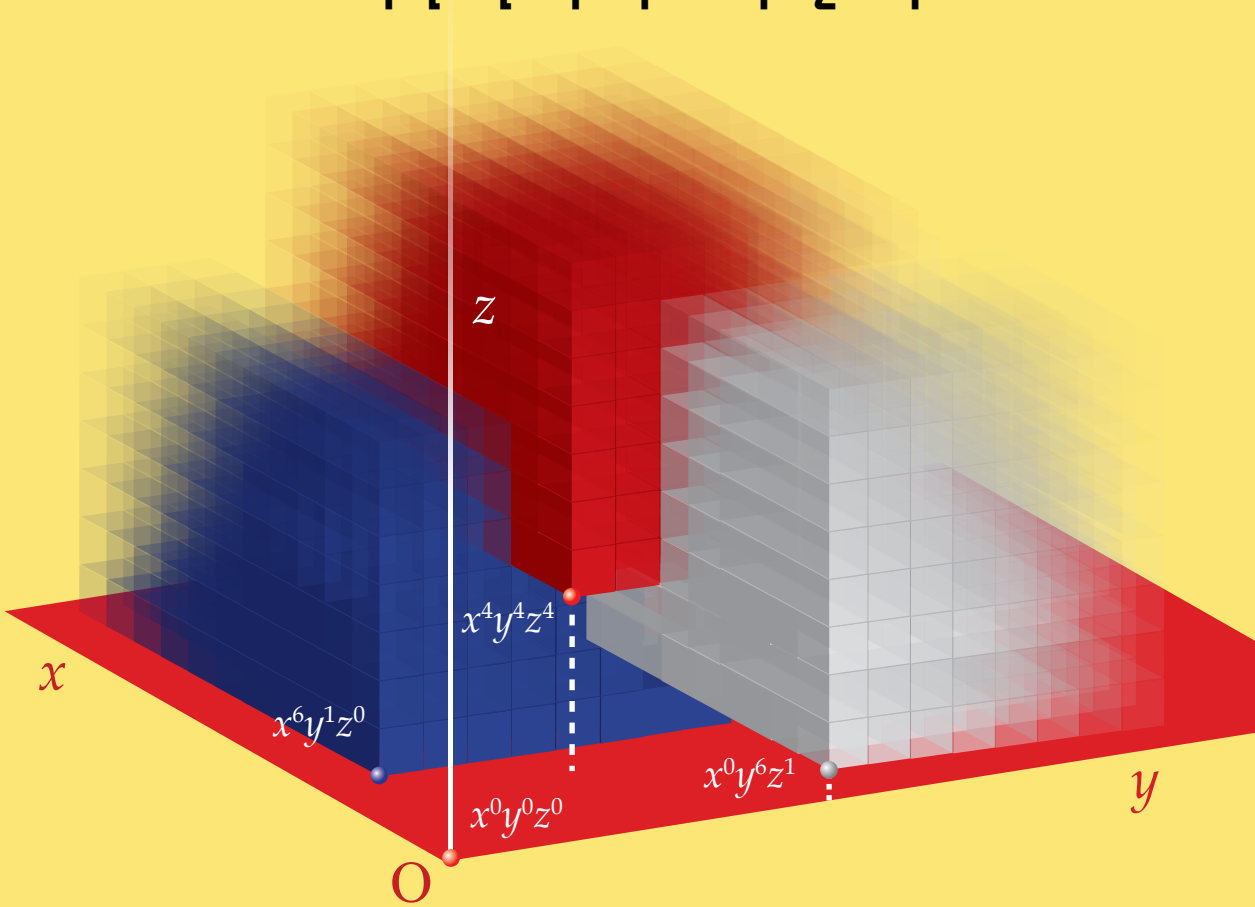
ԵՐԵՎԱՆԻ ՊԵՏԱԿԱՆ
ՀԱՄԱԼՍԱՐԱՆ

Վ. Հ. Միքայելյան

ԱԼԳՈՐԻԹՄԱԿԱՆ ՀԱՆՐԱՀԱՇԻՎ

Կոմուտատիվ օղակներ եւ դաշտեր



Վ. Հ. Միքայելյան

ԱԼԳՈՐԻԹՄԱԿԱՆ ՀԱՆՐԱՀԱՇԻՎ

Կոմուտատիվ օղակներ եւ դաշտեր

Որպես դասագիրք հաստատված է ՀՀ Կրթության եւ գիտության նախարարության կողմից

Երեւան
ԵՊՀ հրատարակչություն
2015

ՀՏԴ 519.6
ԳՄԴ 22.19
Մ 780

Հաստատված է ՀՀ Կրթության եւ գիտության նախարարության կողմից որպես դասագիրք բարձրագույն մասնագիտական կրթություն իրականացնող ուսումնական հաստատությունների համար (17/07/2015):

Երաշխավորված է Երեւանի պետական համալսարանի գիտական խորհրդի կողմից որպես բուհական դասագիրք (7/05/2015):

Երաշխավորված է ԵՊՀ ինֆորմատիկայի եւ կիրառական մաթեմատիկայի ֆակուլտետի գիտական խորհրդի կողմից որպես բուհական դասագիրք (3/12/2014):

Մ 780 Միքայելյան Վ. Հ.
Ալգորիթմական հանրահաշիվ, կոմուտատիվ օղակներ եւ դաշտեր/ Վ. Հ. Միքայելյան.- Եր.: ԵՊՀ հրատ., 2015,.- 374 էջ:

Ալգորիթմական (կոմպյուտերային) հանրահաշիվը մաթեմատիկայի արդի ճյուղ է, որն ընկած է ժամանակակից հանրահաշվի եւ ինֆորմատիկայի հատման տիրույթում: Գրքը ներկայացնում է առարկայի այնպիսի շարադրանք, որտեղ ալգորիթմների կառուցումը հենվում է հանրահաշվական խիստ հիմնավորման վրա: Շարադրանքը ներառում է էվկլիդյան եւ ֆակտորիալ օղակները, օղակների վրա թվային գնահատականները, դաշտերի ընդլայնումները, մնացքների մասին թեորեմը, վերջավոր դաշտերի վրա տրված տարածությունները, բազմանդամի ֆակտորիզացիան ներառյալ Բեռլեկեմպի եւ Յեսենհաուզի ալգորիթմները, նյոտերյան օղակները եւ մոնոմիալ իդեալները, Գրյոբների բազաները եւ Բուխբերգերի ալգորիթմը, արտաքսման իդեալները եւ ոչ գծային հավասարումների համակարգերի լուծումը: Գիրքը նախատեսված է բուհերի ուսանողների, ասպիրանտների, ինչպես նաեւ ալգորիթմական հանրահաշվով, օղակների տեսությամբ եւ հանրահաշվի ալգորիթմական կիրառություններով բոլոր զբաղվողների համար:

Կազմի պատկերը՝ $I = \langle x^6y^1z^0,\ x^4y^4z^4,\ x^0y^6z^1\rangle$ մոնոմիալ իդեալը $\mathbb{R}[x,y,z]$ նյոտերյան օղակում (տես 296 էջի 8.3.7 օրինակը):

V. H. Mikaelian, *Algorithmic Algebra, Commutative Rings and Fields,* YSU Press, Yerevan, 2015, 374pp. (see English annotation on page 370). Cover image: the monomial ideal $I = \langle x^6y^1z^0,\ x^4y^4z^4,\ x^0y^6z^1\rangle$ in the Noetherian ring $\mathbb{R}[x,y,z]$ (see example 8.3.7 on page 296).

В. Г. Микаелян, *Алгоритмическая алгебра, коммутативные кольца и поля,* Издательство ЕГУ, Ереван, 2015, 374 стр. (см. русскую аннотацию на стр. 372). На обложке: мономиальный идеал $I = \langle x^6y^1z^0,\ x^4y^4z^4,\ x^0y^6z^1\rangle$ в нётеровом кольце $\mathbb{R}[x,y,z]$ (см. пример 8.3.7 на стр. 296).

ISBN 978-5-8084-1994-0

ՀՏԴ 519.6
ԳՄԴ 22.19

Բովանդակություն

Նախաբան

Ալգորիթմական (կոմպյուտերային) հանրահաշիվը արդի մաթեմատիկայի մի ճյուղ է, որն ընկած է ժամանակակից հանրահաշվի եւ ինֆորմատիկայի հատման տիրույթում: Նրա նպատակը այնպիսի հանրահաշվական տեսության զարգացումն է, որով հնարավոր է ալգորիթմների կառուցման մեթոդներ մշակել: Այդ ալգորիթմների հիման վրա գրվում են ինչպես առանձին ծրագրեր, այնպես էլ ծրագրային ապահովման փաթեթներ:

Ալգորիթմական հանրահաշվի մոտեցումները ինչ-որ առումով «հակադիր» են թվային մեթոդների կամ մաթեմատիկական անալիզի մոտեցումներին. որեւէ մաթեմատիկական օբյեկտի որոնելի արժեքը գտնելու համար այստեղ կիրառվում են ոչ թե մոտարկումներ (օրինակ, արժեքի ներկայացումը որպես հաջորդականության սահման, շարքի գումար, ինտեգրալ եւլն), այլ օգտագործվում են տվյալ օբյեկտի հանրահաշվական հատկությունները (դիտարկվում են դրա պատկերները ըստ հոմոմորֆիզմների, վերլուծությունը ծնիչների կամ պարզ արտադրիչների արտադրյալի եւլն):

Ալգորիթմական հանրահաշիվը զարգացել է երկու ուղղություններով, որոնք կարելի է բաժանել երկու խմբի: Առաջինը (որին պատկանում է նաեւ մեր աշխատանքը) տեսական հանրահաշվական նոր մեթոդների զարգացումն է, որոնց վրա հենվելով՝ կարելի է կառուցել ավելի արդյունավետ ալգորիթմներ: Այս ուղղությունների կարեւոր մենագրություններ են, օրինակ՝ (von zur Gathen & Gerhard, 2003), (Mishra, 1993), (Mignotte, 1992), (Davenport, et al., 1993), (Панкратьев, 2007) եւլն: Սրա վրա հենվելով՝ զարգանում են երկրորդ խմբի ուղղությունները՝ ալգորիթմների ներկայացումը ծրագրավորման լեզուներով եւ դրանց միջոցով համակարգչային ծրագրային ապահովման մշակումը: Այս ուղղությանը ծանոթանալու համար տես (Tan, et al., 2000), (Grabmeier, et al., 2003): Այս երկու խմբերն իրարից արդեն այնքան են հեռացել, որ ընդունված է դրանք կոչել առանձին անվանումներով՝ **ալգորիթմական հանրահաշիվ** (algorithmic algebra, computer algebra, algebraic algorithms կամ symbolic computation) եւ **համակարգչային հանրահաշվի համակարգեր** (computer algebra systems): Հետաքրքիր է, որ ալգորիթմական հանրահաշվի ամենավաղ հետազոտություններից մեկն է 1953 թ. Ֆիլադելֆիայում Հ. Ղահրիմանյանի հրապարակած «Analytic diferentation by a digital computer» աշխատանքը (Kahrimanian, 1953):

Մի քանի խոսքով բացատրենք հայերեն «ալգորիթմական հանրահաշիվ» թարգմանության ընտրությունը: Computer algebra անվանման մեջ «computer» բառն օգտագործվում է ոչ այնքան «համակարգչային», որքան «հաշվարկային» իմաստով՝ «to compute»: Ֆրանսերենում, օրինակ, ընդունված է «calcul formel» անվանումը (ֆորմալ հաշիվ): Computer algebra անվանումը չի օգտագործվել նաեւ Կնուտի

կողմից (Knuth, 1969): Ռուսաց լեզվին այս առարկայի անվանումն անցել է «компьютерная алгебра» տեսքով (ավելի հազվադեպ օգտագործվում է «алгоритмическая алгебра» ձեւը): Հայերեն երբեմն օգտագործում են «կոմպյուտերային հանրահաշիվ» ձեւը (մեզ հանդիպել է անգամ «քոմփյութերային հանրահաշիվ» թարգմանությունը), ինչն անընդունելի է, քանի որ «computer» եւ «компьютер» բառերի համար որպես հայերեն գրական թարգմանություն ընդունված է «համակարգիչ» բառը: Հայերեն տերմինի ընտրությունն ավելի դյուրին կդառնա, եթե այն կապենք ոչ թե «computer algebra», այլ «algorithmic algebra» անվանման հետ, որը տարածված է բազմաթիվ աղբյուրներում (տես, օրինակ, (Mishra, 1993), (Yap, 1999), (Bokut' & Kukin, 2012), (Matzat, et al., 1999), (Pohst & Zassenhaus, 1997) եւլն): Հաշվի առնելով այս ամենը՝ նպատակահարմար է թվում հայերենում կիրառել հետեւյալ անվանումները՝ **ալգորիթմական հանրահաշիվ** տերմինը օգտագործել որպես անգլերեն algorithmic algebra, computer algebra, algebraic algorithms, symbolic computation հոմանիշների եւ ռուսերեն компьютерная алгебра տերմինի թարգմանություն (որպես տեսական հանրահաշվի ճյուղի անվանում): Իսկ **համակարգչային հանրահաշվի համակարգեր** տերմինը կարելի է օգտագործել որպես անգլերեն computer algebra systems եւ ռուսերեն системы компьютерной алгебры տերմինների թարգմանություն (որպես ծրագրավորման ուղղության անվանում):

Ալգորիթմական հանրահաշվի վաղ շրջանի աղբյուրներում քիչ չեն հանրահաշվական հասկացությունների եւ տերմինների ոչ հստակ, երբեմն սխալ կիրառությունները: Որոշ դեպքերում այդ վրիպումները ալգորիթմական սխալների չեն բերում, քանի որ ապացույցների թերի հատվածները հնարավոր է լրացնել, բայց երբեմն էլ դրանք հանգեցնում են լուրջ սխալների. կառուցված ալգորիթմները միշտ չէ, որ աշխատում են: Բերենք մի քանի տիպական օրինակներ:

Տարբեր խնդիրներ լուծելու տարածված եղանակներից են մոդուլյար մեթոդները: Օրինակ, ամբողջ գործակիցներով $f(x)$ եւ $g(x)$ բազմանդամների ամենամեծ ընդհանուր բաժանարարը հաշվելու համար նպատակահարմար է դիտարկել նրանց $f_p(x) = \varphi_p\big(f(x)\big)$ եւ $g_p(x) = \varphi_p\big(g(x)\big)$ պատկերները $\varphi_p : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ օղակային հոմոմորֆիզմի դեպքում: Նախ հաշվվում է $f_p(x)$ եւ $g_p(x)$ բազմանդամների ամենամեծ ընդհանուր բաժանարարը, եւ դրա միջոցով վերականգնվում է $f(x)$ եւ $g(x)$ բազմանդամների ամենամեծ ընդհանուր բաժանարարը (տես 3-րդ գլխի ալգորիթմները): Սակայն որոշ աղբյուրներում հասկացված չէ φ_p օղակային հոմոմորֆիզմի դերը. հեղինակները պարզապես «դիտարկում են բազմանդամները ըստ p մոդուլի», այսինքն, յուրաքանչյուր գործակից մնացորդով բաժանում են p-ի վրա՝ առանց օղակի կամ հոմոմորֆիզմի հասկացությունը օգտագործելու: Սա չի կարելի համարել պարզապես ոճաբանական մանրուք. նախքան $f_p(x)$ եւ $g_p(x)$ բազմանդամների ամենամեծ ընդհանուր բաժանարարի մասին խոսելը պետք է պարզել, արդյո՞ք $\mathbb{Z}_p[x]$ օղակի բոլոր ոչ զրոյական տարրերի համար իսկապես գոյություն

ունի դրանց ամենամեծ ընդհանուր բաժանարարը: Բարեբախտաբար, այս բացթողումը ալգորիթմական սխալի չի հանգեցնում, քանի որ p պարզ թվի համար $\mathbb{Z}_p[x]$-ն էվկլիդյան օղակ է, եւ նրանում ամենամեծ ընդհանուր բաժանարարի գոյությունն ապահովված է Էվկլիդեսի ալգորիթմով: Այնուամենայնիվ, դա կարիք ունի ապացույցի, քանի որ դժվար չէ կառուցել այնպիսի բազմանդամային օղակ, որտեղ երկու բազմանդամների ամենամեծ ընդհանուր բաժանարարը գոյություն չունի:

Մի փոքր ավելի մանրամասնորեն կանգ առնենք այնպիսի բացթողումների վրա, որոնք բերում են լուրջ ալգորիթմական սխալների: Հաճախակի հանդիպող թերություն է այն փաստի անտեսումը, որ օղակից դաշտին անցման ընթացքում էապես փոխվում է հակադարձելի տարրերի քանակը: Օրինակ, $\varphi_p\colon \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ հոմոմորֆիզմը կիրառելիս պետք է հաշվի առնել, որ $\mathbb{Z}[x]$-ում հակադարձելի են միայն $-1,\ 1$ թվերը, իսկ $\mathbb{Z}_p[x]$-ում հակադարձելի է ցանկացած ոչ զրոյական թիվ, այսինքն՝ $\mathbb{Z}_p^* = \mathbb{Z}_p\backslash\{0\}$ բազմության բոլոր տարրերը: Հակադարձելի տարրով բազմապատկումը չի ազդում բաժանելիության վրա: Ուստի, եթե, ասենք, $\mathbb{Z}_p[x]$ օղակում Էվկլիդեսի ալգորիթմով հաշվվել է $f_p(x)$ եւ $g_p(x)$ բազմանդամների $h(x)$ ամենամեծ ընդհանուր բաժանարարը, ապա ցանկացած $a \in \mathbb{Z}_p^* = \mathbb{Z}_p\backslash\{0\}$ տարրի համար $a \cdot h(x)$ արտադրյալը նույնպես $f_p(x)$ եւ $g_p(x)$ բազմանդամների ամենամեծ ընդհանուր բաժանարարն է: Բայց a-ի որոշ արժեքների դեպքում $a \cdot h(x)$-ը $f(x)$ եւ $g(x)$ բազմանդամների ամենամեծ ընդհանուր բաժանարարի պատկերը չէ՝ անկախ այն բանից, թե ինչ p ենք քննարկել: Երբեմն այս երեւույթը տեղի ունի նաեւ $a = 1$ դեպքում: Նման օրինակ կառուցել ենք 3.4 պարագրաֆում (տես 3.4.2 օրինակը եւ դրան հաջորդող քննարկումը):

Այլ հաճախակի հանդիպող սխալի է հանգեցնում վերջավոր դաշտերի վրա կատարվող հաշվարկների արդյունքի վրա դաշտի բնութագրիչի ազդեցության անտեսումը: Օրինակ, բազմանդամը քառակուսիներից ազատ արտադրիչների վերլուծելու խնդիրը շատ պարզ է զրոյական բնութագրիչի դաշտի վրա, բայց p պարզ բնութագրիչին անցնելիս կարող են առաջանալ շատ ավելի բարդ դեպքեր (տես 4.5 պարագրաֆը): Ալգորիթմներ կառուցելիս անհրաժեշտ է կամ հիմնավորել բարդություններ առաջացնող p բնութագրիչի դեպքը, կամ էլ շրջանցել այն (տես 7.4 պարագրաֆը), ինչը վաղ շրջանի որոշ ալգորիթմների հիմնավորումներում միշտ չէ, որ արվում էր. ալգորիթմներ էին կառուցվում ենթադրելով՝ որ եթե քառակուսիներից ազատ է $f(x)$-ը, ապա այդպիսին կլինի նաեւ $f_p(x)$-ը:

Այս բնույթի բացթողումները գրականության մեջ վերացվել են համեմատաբար ուշ շրջանի հետազոտական հոդվածներում եւ մենագրություններում՝ հանրահաշվական հստակ ապարատի կիրառման միջոցով: Պատրաստելով այս աշխատանքը՝ մենք որոշ դեպքերում օգտվել ենք այդ աղբյուրներից, որոշ դեպքերում էլ ներկայացրել ենք մեր սեփական լուծումները: Նման օրինակ է վերջավոր դաշտի վրա բազմանդամի ֆակտորիզացիայի ալգորիթմի հիմնավորումը 7.3 պարագրաֆում: Գրականության մեջ այդ ալգորիթմը ներկայացվում է Կնուտի առաջարկած տար-

բերակով, քանի որ այն օգտագործում է քառակուսիներից ազատ արտադրիչները, ինչը թեթեւացնում է ալգորիթմը: Բայց Կնուտի շարադրանքը շրջանցում է ապացույցի որոշ հատվածներ, եւ մենք գերադասեցինք վերադառնալ Բեռլեկեմպի սկզբնական ապացույցին՝ այն ադապտացնելով քառակուսիներից ազատ բազմանդամների համար (տես 7.3.19 դիտողությունը):

Գիրքը պարունակում է մի քանի հարյուր վարժություններ եւ խնդիրներ: Շատ խնդիրների կցված են ցուցումներ:

Աշխատանքի կարեւոր առանձնահատկությունն է բազմաթիվ մանրամասն օրինակների քննարկումը: Դրանք ուղեկցում են բոլոր հիմնական հասկացությունները եւ ալգորիթմները: Այդ օրինակները երկարացնում են շարադրանքը, բայց ըստ մեր դասավանդման փորձի՝ էապես նպաստում են նյութի ընկալմանը: Բերված գրեթե բոլոր վարժությունները, խնդիրները եւ օրինակները կազմվել են հատուկ այս աշխատանքի համար՝ ԵՊՀ ԻԿՄ ֆակուլտետում դասավանդման տարիների ընթացքում:

Եթե գրականության մեջ նշված որեւէ անգլիալեզու աղբյուր ունի ռուսերեն թարգմանություն, ապա այն եւս օգտագործվում է հղումներում: Գրականության ցանկում հիշատակված բոլոր հրապարակումները կամ դրանց պատճենները առկա են հեղինակի մոտ եւ կարող են տրամադրվել բոլոր ցանկացողներին:

Հեղինակի կողմից

Ալգորիթմական հանրահաշվի հետ առաջին անգամ առնչվելու առիթ եմ ունեցել 1993 թվականին Մ. Վ. Լոմոնոսովի անվան Մոսկվայի պետական համալսարանում, երբ իմ ուսուցչի՝ պրոֆ. Ա. Յու. Օլշանսկու խորհրդով компьютерная алгебра մասնագիտությունն ընտրեցի որպես ասպիրանտուրայի արտաքին քննության թեմա՝ պրոֆ. Ա. Վ. Միխալյովի եւ (այժմ երջանկահիշատակ) Ե. Վ. Պանկրատյեվի մոտ: Հնարավորություն ունեցա նաեւ մասնակցելու ՄՊՀ բարձրագույն հանրահաշվի ամբիոնի Компьютерная алгебра սեմինարին[1]:

ԵՊՀ ԻԿՄ ֆակուլտետում աշխատելու տարիների ընթացքում, 1990-ականների կեսերից սկսած ալգորիթմական հանրահաշիվը կիրառել եմ, նախ, որպես դիպլո-

[1] Մոսկվայի պետական համալսարանն առաջատար դեր ունի ալգորիթմական հանրահաշվի տարածման մեջ: ՄՊՀ մեխ.-մաթ. ֆակուլտետում Прикладные вопросы алгебры ծրագիրը բակալավրիատի պարտադիր դասընթացներից է, իսկ Алгебраические алгоритмы и их сложность ծրագիրը՝ բակալավրիատի հատուկ դասընթացներից: Դրանից բացի, Компьютерная алгебра ծրագիրը մագիստրատուրայի հիմնական դասընթացներից է: ՄՊՀ մեխ.-մաթ. ֆակուլտետի բարձրագույն հանրահաշվի ամբիոնում գործում է Компьютерная алгебра հատուկ սեմինարը: ՄՊՀ հաշվողական մաթեմատիկայի և կիբեռնետիկայի ֆակուլտետի բակալավրիատում դասավանդվում է Прикладная алгебра պարտադիր դասընթացը: Իսկ ալգորիթմական լեզուների ամբիոնում գործում է նաեւ Компьютерная алгебра и теория формальных языков հատուկ սեմինարը:

մային եւ ավարտական աշխատանքների թեմա, ապա նաեւ՝ որպես մագիստրատուրայի եւ բակալավրիատի դասընթացների նյութ: Այդ ընթացքում են հայտնաբերվել ալգորիթմների տեսական հիմնավորման այն վրիպակները, որոնց մասին հիշատակվեց վերեւում: Տարիների ընթացքում հավաքված նոր ապացույցները, ալգորիթմները, հատկանշական նոր օրինակները գրի են առնվել եւ օգտագործվել առանձին դասախոսությունների տեսքով, հատկապես՝ սկսած 2013 թվականից, երբ արդեն պատրաստ էին տեքստի 2-ից 5-րդ գլուխների հիմնական մասերը: Այդ տեքստերով դասավանդման ընթացքում պարզ դարձավ, որ օղակների եւ դաշտերի տեսության բազային հասկացությունների համար տարբեր դասագրքերի վրա հաճախակի հղումներ տալն արդյունավետ չէ: Ուստի ավելացվեցին նախապատրաստական 2.1-2.3, 2.5, 2.6, 3.3, 4.1, 4.2, 5.1, 6.1, 7.2 պարագրաֆները:

Դասագրքի վերջնական տարբերակի մասնագիտական մանրամասն խմբագրությունն իրականացրել է պրոֆ. Հ. Ս. Միքայելյանը: Տեքստի լեզվական վրիպակները սրբագրվել են դոցենտ Մ. Ա. Միքայելյանի կողմից:

Խորին երախտագիտությունս եմ հայտնում ոչ միայն հիշատակված բոլոր գիտնականներին, այլեւ բոլոր նրանց, ովքեր նպաստել են Հայաստանում ալգորիթմական հանրահաշվի տարբեր ճյուղերի ուսումնասիրությանը: Շնորհակալ եմ նաեւ ԵՊՀ ԻԿՄ ֆակուլտետի ուսանողներին. ալգորիթմական հանրահաշվի գրականության մեջ առկա այն անհարթությունները, որոնց մասին ակնարկվեց վերեւում, գտնվել եւ լուծում են ստացել նրանց հարցերին պատասխանելու ընթացքում:

Այս աշխատանքը ամբողջացնում է ալգորիթմական հանրահաշվի հետ իմ արդեն ավելի քան քսանամյա ծանոթությունը: Հուսով եմ, որ այն կնպաստի Հայաստանում հանրահաշվի այս ճյուղի ավելի լայն դասավանդմանն ու ուսումնասիրությանը:

Վահագն Հ. Միքայելյան, Երեւան, 2014:

1 Պարզագույն նախնական հասկացություններ

1.1 Միջանկյալ արժեքների ուռճացման երեւույթը

Իր «The art of computer programming» մենագրության երկրորդ հատորում Դ. Կնուտը ալգորիթմական խնդիրներում հանրահաշվական մոտեցումների կարեւորությունը հիմնավորելու համար բերում է միջանկյալ արժեքների ուռճացման օրինակը (Knuth, 1969): Մենք սկսում ենք այս օրինակից, քանի որ այն շատ պարզ եւ համոզիչ օրինակ է այն բանի, թե ինչպես հաշվողական եւ անգամ տեխնիկական բարդությունները կարող են հաղթահարվել հանրահաշվի մեթոդների կիրառությամբ: Մենք այս գլխում բաց ենք թողնում բազմանդամի սահմանումը եւ տարրական հատկությունները. դրանք կարելի է գտնել հանրահաշվի ցանկացած ներածության մեջ. (Garrett, 2008), (Cohn, 2003), (Cohn, 2000), (Lang, 2002), (Кострикин, 1977), (Кострикин, 2004), (ван дер Варден, 1979):

Կնուտի օրինակը կապված է Էվկլիդեսի ալգորիթմով հետեւյալ երկու բազմանդամների ամենամեծ ընդհանուր բաժանարարի հաշվման հետ.

$$f(x) = x^8 + x^6 - 3x^4 - 3x^3 + 8x^2 + 2x - 5$$
$$g(x) = 3x^6 + 5x^4 - 4x^2 - 9x + 21: \tag{1.1}$$

Էվկլիդեսի ալգորիթմի միջոցով $f(x)$ եւ $g(x) \neq 0$ ամբողջ գործակիցներով բազմանդամների $d(x) = \big(f(x), g(x)\big)$ ամենամեծ ընդհանուր բաժանարարը հաշվելու ալգորիթմը լավ ծանոթ է հանրահաշվի դասընթացներից: Նախքան Կնուտի օրինակը քննարկելը համառոտ հիշեցնենք ալգորիթմի քայլերը:

Եթե $f(x)$ եւ $g(x) \neq 0$ ամբողջ գործակիցներով բազմանդամներ են, ապա, ըստ մնացորդով բաժանման կանոնի, գոյություն ունեն ռացիոնալ գործակիցներով այնպիսի $q(x)$ եւ $r(x)$ բազմանդամներ, որ

$$f(x) = q(x)g(x) + r(x),$$

որտեղ $r(x) = 0$ կամ $r(x) \neq 0$ եւ $\deg r(x) < \deg g(x)$: Եթե $r(x) = 0$, ապա ակնհայտորեն $d(x) = \big(f(x), g(x)\big) = g(x)$: Եթե $r(x) \neq 0$, ապա կրկնենք քայլերը մինչեւ ստացվի առաջին զրոյական մնացորդով բաժանումը.

$$
\begin{aligned}
f(x) &= q(x)g(x) + r(x), && r(x) \neq 0 \text{ եւ } \deg r(x) < \deg g(x),\\
g(x) &= q_1(x)r(x) + r_1(x), && r_1(x) \neq 0 \text{ եւ } \deg r_1(x) < \deg r(x),\\
r(x) &= q_2(x)r_1(x) + r_2(x), && r_2(x) \neq 0 \text{ եւ } \deg r_2(x) < \deg r_1(x),\\
r_1(x) &= q_3(x)r_2(x) + r_3(x), && r_3(x) \neq 0 \text{ եւ } \deg r_3(x) < \deg r_2(x),
\end{aligned}
\tag{1.2}
$$

$$
\begin{aligned}
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
r_{n-3}(x) &= q_{n-1}(x)r_{n-2}(x) + r_{n-1}(x), && r_{n-1}(x) \neq 0 \text{ եւ } \deg r_{n-1}(x) < \deg r_n(x),\\
r_{n-2}(x) &= q_n(x)r_{n-1}(x) + r_n(x), && r_n(x) \neq 0 \text{ եւ } \deg r_n(x) < \deg r_{n-1}(x),\\
r_{n-1}(x) &= q_{n+1}(x)r_n(x) + 0, && r_{n+1}(x) = 0:
\end{aligned}
$$

Ալգորիթմը կանգ է առնում $r_{n+1}(x) = 0$ զրոյական մնացորդ ստանալու դեպքում (այն չի կարող անվերջ շարունակվել, քանի որ $r_i(x)$ բազմանդամների աստիճանները չեն կարող անվերջ նվազել): Որոնելի ամենամեծ ընդհանուր բաժանարարը վերջին ոչ զրոյական մնացորդն է.

$$d(x) = \big(f(x), g(x)\big) = r_n(x):$$

Ալգորիթմի հիմնավորումը հեշտությամբ հետեւում է (1.2) հավասարությունների համակարգից. դրա վերջին տողից բխում է, որ $r_{n-1}(x) \vdots r_n(s)$ (այսինքն՝ $r_{n-1}(x)$ բազմանդամը բաժանվում է $r_n(s)$ բազմանդամի վրա, տես օգտագործված նշանակումների ցանկը էջ 358-ում): Դրանից եւ նախավերջին տողից բխում է, որ $r_{n-2}(x) \vdots r_n(s)$: Շարունակելով քայլերը կստանանք. $r_{n-3}(x) \vdots r_n(x)$, $r_{n-4}(x) \vdots r_n(x)$,... Իսկ առաջին հավասարություններից կստանանք $r_1(x) \vdots r_n(x)$, $r(x) \vdots r_n(x)$, $g(x) \vdots r_n(x)$, $f(x) \vdots r_n(x)$: Այսպիսով, $r_n(x)$-ը $f(x)$ եւ $g(x)$ բազմանդամների ընդհանուր բաժանարար է:

Մյուս կողմից, ենթադրենք՝ որեւէ $h(x)$ բազմանդամ նույնպես $f(x)$-ի եւ $g(x)$-ի ընդհանուր բաժանարար է: $f(x) = q(x)g(s) + r(x)$ հավասարությունից բխում է, որ $r(x) \vdots h(x)$: Սրանից եւ (1.2) համակարգի երկրորդ տողից բխում է, որ $r_1(x) \vdots h(x)$: Շարունակելով քայլերը՝ կստանանք. $r_{n-1}(x) \vdots h(x)$ եւ $r_n(x) \vdots h(x)$: Ուստի $r_n(x)$-ը բաժանվում է $f(x)$ եւ $g(x)$ բազմանդամների ընդհանուր բաժանարարներից կամայականի վրա: Այսինքն՝ $d(x) = \big(f(x), g(x)\big)$:

Թվում է, թե այս ալգորիթմով Կնուտի օրինակի (1.1) բազմանդամների ամենամեծ ընդհանուր բաժանարարը կարելի է հաշվել մի քանի րոպեում: Բայց հաշվարկները այլ բան են ցույց տալիս. չնայած (1.1) բազմանդամները մեծ գործակիցներ չեն պարունակում, նրանց ամենամեծ ընդհանուր բաժանարարի հաշվման

ընթացքում այնքան խոշոր թվեր են ստացվում (մինչեւ 35-նիշանի), որ հաշվարկը ձեռքով կատարելը շատ դժվար է: Ավելին, ալգորիթմի վերջնական պատասխանն այնպիսին է, որ հաշվարկի ընթացքում ստացված խոշոր թվերը էական տեղեկություն չեն բերում խնդրի համար. այս բազմանդամները փոխադարձաբար պարզ են, եւ վերջնական պատասխանն է $d(x) = \big(f(x), g(x)\big) = 1$:

Ներկայացնենք այդ քայլերը՝ համառոտության համար բաց թողնելով հաշվողական մասը.

$$f(x) = q(x)g(x) + r(x) = \left(\frac{1}{3}x^2 - \frac{2}{9}\right)g(x) - \frac{5}{9}x^4 + \frac{1}{9}x^2 - \frac{1}{3}: \tag{1.3}$$

Հաջորդ մնացորդները կլինեն.

$$r_1(x) = -\frac{117}{25}x^2 - 9x + \frac{441}{25},$$

$$r_2(x) = \frac{233150}{19773}x + \frac{102500}{6591},$$

$$r_3(x) = -\frac{1288744821}{543589225}:$$

Քանի որ համակարգիչն իրականում միայն ամբողջ թվերի հետ է աշխատում, ներկայացնենք նույն հաշվարկն ամբողջ թվերով: Հիշենք, որ բազմանդամային հավասարման երկու կողմերը ոչ զրոյական սկալյար թվով բազմապատկելը չի փոխում դրանց բաժանելիությունը: Բազմապատկելով (1.3) հավասարման երկու կողմերը 27-ով՝ կստանանք.

$$r'(x) = -15x^4 + 3x^2 - 9:$$

Այս բազմապատկումից հետո (կատարելով մնացորդով բաժանումը եւ ամեն բաժանումից հետո համապատասխան ամբողջ թվով բազմապատկելուց հետո) կստանանք մնացորդների հետեւյալ շարքը.

$$r'_1(x) = 15795x^2 + 30375x - 59535,$$

$$r'_2(x) = 1254542875143750x - 1654608338437500,$$

$$r'_3(x) = 1259333879550074310093114199218750 0.$$

Մեր ստացած երկու թվերն էլ՝ $r_3(x) = -\frac{1288744821}{543589225}$ ռացիոնալ կոտորակը եւ $r'_3(x) = 1259333879550074310093114199218750 0$ թիվը խնդրի համար օգտակար միայն մի տեղեկություն են պարունակում. $f(x)$ եւ $g(x)$ բազմանդամներ փոխադարձաբար պարզ են, եւ հաշվարկի ընթացքում ստացված խոշոր թվերը ոչ միայն դանդաղեցնում են ալգորիթմը, այլեւ դրա վերջնական պատասխանի համար քիչ

էական տեղեկություն են պարունակում: Հենց այս երեւույթն է կոչվում միջանկյալ արժեքների ուռճացում:

Դ. Կնուտն առաջարկում է այս օրինակը շատ ավելի արագ լուծել մոդուլյար մեթոդներով (Knuth, 1969): Կնուտի մեթոդին մենք կանդրադառնանք 1.3 պարագրաֆում: Իսկ մինչ այդ նշենք բազմանդամների հետ ըստ մոդուլի գործողությունների մի շարք հատկություններ:

1.2 Թվային եւ բազմանդամային գործողություններ ըստ մոդուլի

Վերհիշենք հանրահաշվի ընդհանուր դասընթացից լավ ծանոթ *բաղդատման* հասկացությունը. կգրենք $a \equiv b (\mathrm{mod}\ m)$ եւ կասենք՝ $a, b \in \mathbb{Z}$ ամբողջ թվերը բաղդատելի են ըստ $m \in \mathbb{Z}$ մոդուլի, եթե $(a-b) \vdots m$ (այսինքն՝ եթե m-ի վրա բաժանելիս a եւ b թվերը երկուսն էլ տալիս են միեւնույն մնացորդը): m-ը կոչվում է բաղդատման *մոդուլ*: Հեշտ է ստուգել, որ եթե $a \equiv b (\mathrm{mod}\ m)$ եւ $a' \equiv b' (\mathrm{mod}\ m)$, ապա

$$a + a' \equiv b + b' (\mathrm{mod}\ m),$$
$$a - a' \equiv b - b' (\mathrm{mod}\ m),$$
$$aa' \equiv bb' (\mathrm{mod}\ m)$$

Երրորդ առնչությունից բխում է նաեւ $ax \equiv bx (\mathrm{mod}\ m)$ եւ

$$ax^n \equiv bx^n (\mathrm{mod}\ m)$$

կամայական $n \in \mathbb{N}$ աստիճանի համար, քանի որ ակնհայտորեն $x \equiv x (\mathrm{mod}\ m)$: Տրված m մոդուլի եւ կամայական

$$f(x) = a_0 x^n + \cdots + a_n$$

ամբողջ գործակիցներով բազմանդամի համար նշանակենք $f_m(x)$-ով այն բազմանդամը, որը ստացվում է $f(x)$-ի յուրաքանչյուր a_i գործակից փոխարինելով a_i' գործակցով այնպես, որ $a_i \equiv a_i' (\mathrm{mod}\ m)$ եւ $a_i' \in \{0, 1, \ldots, m-1\}$: Տրված $f(x)$ բազմանդամից $f_m(x)$-ին անցնելու այս քայլը անվանենք մոդուլյար անցում (հաջորդ գլխում կտրվի այս անցման ավելի հանրահաշվական սահմանումը):

Այժմ անցնենք բազմանդամների հետ գործողություններին:

(1.4) $$f(x) = a_0 x^n + \cdots + a_n \quad \text{եւ} \quad g(x) = b_0 x^k + \cdots + b_k$$

($a_0 \neq 0$ եւ $b_0 \neq 0$) բազմանդամներից ստացված $f_m(x)$ եւ $g_m(x)$ բազմանդամների $f_m(x) + g_m(x)$ գումարը կարելի է ստանալ երկու ճանապարհներով: Նախ, այն $f(x) + g(x)$ գումարից ստացված մոդուլյար անցման արդյունքն է.

$$f_m(x) + g_m(x) = \big(f(x) + g(x)\big)_m$$

(այսինքն՝ $f(x)$ եւ $g(x)$ բազմանդամները նախ գումարում ենք ավանդական ձեւով, ապա նոր՝ մոդուլյար անցում կատարում): Մյուս կողմից, բաղդատման վերը բերված տարրական հատկություններից բխում է, որ միեւնույն արդյունքը կստացվի, եթե գումարվեն միանգամից $f_m(x)$ եւ $g_m(x)$ բազմանդամները, ընդ որում, միեւնույն i աստիճանին համապատասխան անդամների գործակիցները գումարվեն ըստ մոդուլի

$$a_{n-i,m}x^i + b_{k-i,m}x^i = c_{n-i,m}x^i, \tag{1.5}$$

որտեղ

$$c_{n-i,m} \equiv a_{n-i,m} + b_{k-i,m} (\mathrm{mod}\, m), \qquad c_{n-i,m} \in \{0, \dots, m-1\}$$

(պարզության համար ենթադրենք, որ եթե բազմանդամներից մեկն ավելի ցածր աստիճանի է, ապա (1.5) բանաձեւում նրա «պակասող» գործակիցների փոխարեն մասնակցում է զրոն):

Նույն կերպ երկու ճանապարհներով կարելի է ստանալ $f_m(x)$ եւ $g_m(x)$ բազմանդամների $f_m(x)g_m(x)$ արտադրյալը: Մի կողմից

$$f_m(x)g_m(x) = \big(f(x)g(x)\big)_m,$$

իսկ, մյուս կողմից, $f_m(x)g_m(x)$ արտադրյալը կստացվի, եթե միանգամից բազմապատկվեն $f_m(x)$ եւ $g_m(x)$ բազմանդամները՝ փակագծերը բացելու եւ նման անդամները միավորելու կանոնով (համապատասխան գործակիցները կբազմապատկվեն եւ կգումարվեն ըստ m մոդուլի):

Ըստ մոդուլի բաժանելիության հասկացությունը նման է սովորական բաժանելիությանը: a ամբողջ թիվը բաժանվում է b ամբողջ թվի վրա ըստ m մոդուլի, եթե գոյություն ունի մի c ամբողջ թիվ այնպիսին, որ $a \equiv bc \pmod m$: Նույն կերպ $f(x)$ բազմանդամը բաժանվում է $g(x)$ բազմանդամի վրա ըստ m մոդուլի, եթե գոյություն ունի մի $h(x)$ բազմանդամ այնպիսին, որ $f_m(x) = g_m(x)h_m(x)$:

Նկատենք ամբողջ թվերի բաժանելիության եւ բազմանդամների բաժանելիության միջեւ մի տարբերություն: Ամբողջ թվերի շարքում միակ հակադարձելի (այսինքն՝ հակադարձ ունեցող) թվերն են 1 եւ -1 թվերը: Եւ այդ թվերով բազմա-

պատկելը չի ազդում բաժանելիության հատկության վրա. եթե տեղի ունի ամբողջ թվերի $a \vdots b$ բաժանումը, ապա տեղի ունեն նաեւ $a \vdots -b$, $-a \vdots b$, $-a \vdots -b$ բաժանումները:

Ռացիոնալ թվերի մեջ հակադարձելի են զրոյից տարբեր բոլոր թվերը: Ուստի, ասենք, $x^3 + x$ բազմանդամը չի բաժանվի $2x^2 + 2$ բազմանդամի վրա, եթե սահմանափակվենք միայն ամբողջ գործակիցներով բազմանդամներով, բայց կբաժանվի դրա վրա, եթե դիտարկենք նաեւ ռացիոնալ գործակիցներով բազմանդամներ. $x^3 + x = (2x^2 + 2) \cdot (x/2)$: Այստեղ դարձյալ բաժանումը կատարվում է շնորհիվ 2 ռացիոնալ թվի հակադարձելիության: Տրված k թվի հակադարձելիության փաստը նշանակենք $k \approx 1$ տեսքով:

Ըստ մոդուլի ամբողջ թվեր բազմապատկելիս եւս կարող ենք հանդիպել 1 եւ -1 թվերից տարբեր հակադարձելի թվերի, որոնց հակադարձելիությունը, սակայն, ոչ թե ռացիոնալ կոտորակների շնորհիվ է կատարվում, այլ ըստ մոդուլի բազմապատկման: Օրինակ՝ $m = 5$ մոդուլով բազմապատկման գործողության համար $2 \approx 1$, քանի որ $3 \cdot 2 = 6 \equiv 1 (\mathrm{mod}\ 5)$): Ուստի եւ $x^3 + x = (2x^2 + 2) \cdot 3x$:

Կասենք, որ $d_m(x)$ բազմանդամը $f_m(x)$ եւ $g_m(x)$ բազմանդամների (մոդուլյար) ամենամեծ ընդհանուր բաժանարար է, եթե դրանք երկուսն էլ բաժանվում են $d_m(x)$-ի վրա, եւ եթե գոյություն ունի մի $t_m(x)$ բազմանդամ, որի վրա նույնպես բաժանվում են $f_m(x)$-ը եւ $g_m(x)$-ը, ապա $d_m(x)$-ը բաժանվում է $t_m(x)$-ի վրա: Սա կնշանակենք $d_m(x) = \big(f_m(x), g_m(x)\big)$: Ըստ հակադարձելի թվերի մասին վերը ասվածի, ամենամեծ ընդհանուր բաժանարարը միակը չէ, եւ $k \cdot d_m(x)$ տեսքի ամեն մի բազմանդամ նույնպես $f_m(x)$ եւ $g_m(x)$ բազմանդամների ամենամեծ ընդհանուր բաժանարար է կամայական $k \approx 1$ թվի համար: Կասենք, որ $f_m(x)$ եւ $g_m(x)$ բազմանդամները փոխադարձաբար պարզ են, եւ դա կնշանակենք $\big(f_m(x), g_m(x)\big) = 1$, եթե $d_m(x) = c \approx 1$:

1.2.1 Օրինակ. Եթե $m = 2$, $f_2(x) = x^2 + 1$, $g_2(x) = x + 1$, ապա հեշտ է ստուգել, որ $\big(f_2(x), g_2(x)\big) = x + 1 = g_2(x)$, քանի որ.

$$x^2 + 1 = (x + 1)(x + 1) \ \vdots \ x + 1:$$

1.2.2 Օրինակ. Եթե $m = 5$, ապա $g_5(x) = x + 3$ եւ $h_5(x) = x + 2$ բազմանդամները փոխադարձաբար պարզ են, քանի որ

$$x + 3 = d_5(x)u_5(x) \quad \text{եւ} \quad x + 2 = d_5(x)v_5(x)$$

հավասարություններից բխում է, որ եթե $d_5(x) \not\approx 1$, այսինքն՝ եթե $d_5(x)$-ը հաստատուն թիվ չէ եւ նրա $\deg\big(d_5(x)\big)$ աստիճանը մեծ է 0-ից, ապա $\deg\big(d_5(x)\big) = \deg(x+3) = \deg(x+2) = 1$:

1.3 Կնուտի մոդուլյար մեթոդը

Դ. Կնուտն առաջարկում է 1.1 պարագրաֆում բերված միջանկյալ արժեքների ուռճացման օրինակը շատ ավելի դյուրին լուծել մոդուլյար մեթոդներով (Knuth, 1969): Բազմանդամների մոդուլյար ամենամեծ բաժանարարը հաշվելու կանոնը նման է Էվկլիդեսի ալգորիթմի միջոցով ամբողջ գործակիցներով բազմանդամների ամենամեծ ընդհանուր բաժանարարը հաշվելու կանոնին, որ բերեցինք 1.1 պարագրաֆում (1.2) համակարգից անմիջապես հետո: Իրոք, բաղդատման տարրական հատկությունների եւ ըստ մոդուլի գումարման ու բազմապատկման մասին վերը ասվածից բխում է, որ եթե $f(x), q(x), g(x)$ եւ $r(x)$ բազմանդամները կապված են

$$f(x) = q(x)g(x) + r(x)$$

հավասարությամբ, ապա ցանկացած m մոդուլի համար տեղի ունի նաեւ

$$f_m(x) = q_m(x)g_m(x) + r_m(x)$$

հավասարությունը: Մասնավորապես, սա կարելի է կիրառել եւ (1.2) համակարգի բոլոր տողերի վրա: Օրինակ՝ n-րդ տողը կստանա հետեւյալ տեսքը.

$$r_{n-3,m}(x) = q_{n-1,m}(x)r_{n-2,m}(x) + r_{n-1,m}(x):$$

(1.2) համակարգի տողերի քանակը կարող է եւ նվազել, քանի որ որեւէ k-րդ քայլում ($k < n$) կարող ենք արդեն իսկ ստանալ վերջին ոչ զրոյական մնացորդը.

$$r_{k,m}(x) \neq 0 \text{ եւ } \deg r_{k,m}(x) < \deg r_{k-1,\mathrm{m}}(x), \text{ բայց } r_{k+1}(x) = 0:$$

Կրկնելով (1.2) համակարգին անմիջապես հաջորդող փաստարկները՝ կարող ենք ստանալ, որ

$$d_m(x) = r_{k,m}(x) = \big(f_m(x), g_m(x)\big):$$

Այժմ վերադառնանք Կնուտի օրինակին: 1.1 պարագրաֆում բերված (1.1) բազմանդամների եւ $m = 5$ մոդուլի համար կատարելով մոդուլյար անցում՝ կստանանք

$$f_5(x) = x^8 + x^6 + 2x^4 + 2x^3 + 3x^2 + 2x$$
$$g_5(x) = 3x^6 + x^2 + x + 1: \tag{1.6}$$

Էվկլիդեսի ալգորիթմը կիրառելու համար օգտագործենք բազմանդամներն իրար վրա «անկյունով բաժանելու կանոնի» մոդուլյար տարբերակը՝ հիշելով, որ, քանի որ $m=5$ մոդուլը պարզ թիվ է, ապա ցանկացած $a,b\in\{1,2,3,4\}$ թվերի համար միշտ կա (սա հեշտ է ստուգել) մի $c\in\{1,2,3,4\}$ թիվ այնպիսին, որ $a=bc$.

$$\begin{array}{l|l} x^8+x^6+2x^4+2x^3+3x^2+2x & 3x^6+x^2+x+1 \\ \hline x^8+2x^4+2x^3+2x^2 & 2x^2+2 \\ \hline x^6+x^2+2x & \\ x^6+2x^2+2x+2 & \\ \hline 4x^2+3 & \end{array}$$

Այստեղ աջ մասի $2x^2$ միանդամն ընտրված է այնպես, որ այս բաժանման $g_5(x)$ բաժանարարի առաջին անդամի հետ բազմապատկվելիս ստացվի

$$2x^2\cdot 3x^6=6x^8\equiv x^8 (\mathrm{mod}\ 5)$$

միանդամը, որը կկրճատվի $f_5(x)$ բաժանելու x^8 ավագ անդամի հետ: Շարունակենք բաժանումները.

$$\begin{array}{l|l} 3x^6+x^2+x+1 & 4x^2+3 \\ \hline 3x^6+x^4 & 2x^4+x^2+2 \\ \hline 4x^4+x^2+x+1 & \\ 4x^4+3x^2 & \\ \hline 3x^2+x+1 & \\ 3x^2+1 & \\ \hline x & \end{array}$$

$$\begin{array}{l|l} 4x^2+3 & x \\ \hline 4x^2 & 4x \\ \hline 3 & \end{array}$$

Այսինքն՝ $f_5(x)$ եւ $g_5(x)$ բազմանդամները փոխադարձաբար պարզ են (վերջին ոչ զրոյական մնացորդն է 3-ը, որը հակադարձելի է ըստ 5 մոդուլի՝ $3\cdot 2=6\equiv 1(\mathrm{mod}\ 5)$): Այստեղից դեռ չի հետեւում, որ փոխադարձաբար պարզ են $f(x)$ եւ $g(x)$ բազմանդամները. ինչպես ցույց է տալիս հետեւյալ պարզ օրինակը, $\big(f_m(x),g_m(x)\big)=1$ պայմանից չի բխում $\big(f(x),g(x)\big)=1$ պայմանը:

1.3.1 Օրինակ. $h(x)=7x^2+8x+1$ եւ $l(x)=7x^2+15x+2$ բազմանդամները փոխադարձաբար պարզ չեն, քանի որ $h(x)=(x+1)(7x+1)$, $l(x)=(x+2)(7x+1)$ եւ $\big(h(x),l(x)\big)=7x+1$: Բայց $m=7$ մոդուլի համար $h_7(x)=x+1$, $l_7(x)=x+2$: Ուստի $\big(h_7(x),l_7(x)\big)=1$ (սա հեշտ է ցույց տալ 1.2.2 օրինակի նմանությամբ):

Կնուտի մոդուլյար մեթոդը ավարտելու համար մնացել է ցույց տալ, որ կոնկրետ հենց այդ օրինակում $\big(f_5(x),g_5(x)\big)=1$ պայմանից իսկապես բխում է, որ $\big(f(x),g(x)\big)=1$: Ենթադրենք՝ ամբողջ գործակիցներով որեւէ $t(x)$ բազմանդամ հանդիսանում է $f(x)$, $g(x)$ բազմանդամների ընդհանուր բաժանարար.

(1.7) $$f(x)=t(x)f^*(x) \quad \text{եւ} \quad g(x)=t(x)g^*(x):$$

Համարենք, որ $t(x)$ բազմանդամի աստիճանն է՝ $k\geq 0$, իսկ ավագ գործակիցն է՝ c_0: Մեր օրինակի (1.1) բազմանդամների ավագ անդամների տեսքից պարզ է, որ $1\vdots c_0$ եւ $3\vdots c_0$ (եթե $f(x)$, $g(x)$ բազմանդամները բաժանվում են $t(x)$-ի վրա, ապա նրանց ավագ գործակիցներն էլ պիտի բաժանվեն $t(x)$-ի ավագ գործակցի վրա): Միակ հնարավորություններն են՝ $c_0=\pm 1$, բայց քանի որ -1 թվով բազմապատկելը չի փոխում բազմանդամների բաժանելիությունը, կարող ենք համարել $c_0=1$, եւ $t(x)$-ի ավագ անդամն է $c_0x^k=x^k$: Ըստ (1.7) պայմանների, $t_5(x)\approx 1$, քանի որ $f_5(x)$ եւ $g_5(x)$ բազմանդամները փոխադարձաբար պարզ են, եւ նրանց երկուսին էլ բաժանող բազմանդամը պիտի հաստատուն լինի: Մյուս կողմից, $t(x)$-ի ավագ գործակիցը 1 է, ուստի $m=5$ մոդուլով դիտարկելիս այն անփոփոխ է մնում. $t_5(x)$ մոդուլյար բազմանդամի ավագ գործակիցը եւս 1 է: Ուստի $k=0$ եւ $t(x)=1$: Ուրեմն $f(x)$ եւ $g(x)$ բազմանդամները փոխադարձաբար պարզ են:

Կնուտի օրինակը մի քանի առումներով շատ օգտակար լինելով հանդերձ, ունի այն հարաբերական թերությունը, որ ողջ քննարկումը իրականացնում է միայն (1.1) երկու բազմանդամների համար: Հետագայում մենք կառաջարկենք մեթոդներ, որոնք ոչ միայն իրականացնում են դա, այլեւ կամայական երկու բազմանդամների համար հաշվում են նրանց ամենամեծ ընդհանուր բաժանարարը՝ ելնելով նրանց մոդուլյար ամենամեծ ընդհանուր բաժանարարից:

2 Օղակներ եւ հոմոմորֆիզմներ

2.1 Օղակներ, ամբողջության տիրույթներ եւ դաշտեր

Առաջին գլխում մենք խուսափեցինք շարադրանքը տանել հանրահաշվական համակարգերի լեզվով (օղակներ, դաշտեր, հոմոմորֆիզմներ եւլն), եւ մեր օգտագործած տեխնիկան չէր անցնում թվերի եւ բազմանդամների հետ ըստ մոդուլի գործողություններ կատարելու սահմանը: Դրա նպատակն այն էր, որ այս դասընթացի սկիզբը, հատկապես Կնուտի օրինակը, ձեւակերպվեն առավել պարզ հասկացությունների միջոցով. մինչդեռ օղակների տեսության, հոմոմորֆիզմների օգտագործումը կարող էր տպավորություն ստեղծել, որ առաջարկվող մեթոդները ավելի բարդ են, քան դրանք իրականում կան:

Դժբախտաբար, հնարավոր չի լինելու հետագա շարադրանքը եւս այդպես տանել, քանի որ դասընթացի վերջում մենք գործ ենք ունենալու այնպիսի օբյեկտների հետ (գծային օպերատորներ վերջավոր դաշտի վրա տրված գծային տարածություններում, դրանց սեփական արժեքներն ու վեկտորներ, նյոտերյան օղակներ եւլն), որոնք չեն կարող նկարագրվել առանց խիստ հանրահաշվական լեզվի: Ավելին՝ հանրաշվական համակարգերի կիրառումը հաճախ կարճացնում է ալգորիթմների կառուցումը (տես 5.1.14 դիտողությունը):

Ուստի հետագա շարադրանքի համար մեզ որոշակի ծանոթություն պետք կլինի օղակների եւ դաշտերի տեսության հիմունքներից: Նյութին կարելի է ծանոթանալ (Кострикин, 1977), (Кострикин, 2004), (Ленг, 1968), (ван дер Варден, 1979) (Cohn, 2003), (Cohn, 2000), (Cohn, 1965), (Garrett, 2008) դասագրքերով: Այստեղ կսահմանափակվենք միայն հիմնական սահմանումների, օրինակների եւ մի քանի թեորեմների ձեւակերպմամբ, որպեսզի դասընթացի հետագա մասում կարողանանք օգտագործել դրանք մեր նշանակումներով:

Որեւէ A բազմության վրա տրված $\circ$ *հանրահաշվական գործողություն* է կոչվում A բազմության կամայական $a, b \in A$ տարրերի (կարգավորված) զույգին նույն բազմության որեւէ $a \circ b$ տարրի համապատասխանեցումը կամ, այլ խոսքերով,

$\circ\colon A \times A \to A$ արտապատկերումը $A \times A$ դեկարտյան արտադրյալից A բազմության մեջ: Այստեղ $a \circ b$ տարրը $(a, b) \in A \times A$ զույգի պատկերն է: A բազմությունն իր վրա տրված $\circ$ հանրահաշվական գործողության հետ միասին նշանակվում է $\langle A, \circ \rangle$ տեսքով եւ կոչվում *հանրահաշվական համակարգ* (կամ պարզապես համակարգ, եթե համատեքստից հասկանալի է, թե խոսքը որ հանրահաշվական համակարգի մասին է): Եթե միեւնույն բազմության վրա սահմանված են մի քանի հանրահաշվական գործողություններ, օրինակ $\circ$, $*$, $+$, $\cdot$ եւ այլն, ապա կարելի է սահմանել նաեւ մի քանի գործողությամբ հանրահաշվական համակարգ, օրինակ՝ $\langle A, \circ, *, +, \cdot \rangle$:

2.1.1 Օրինակներ. Հանրահաշվական համակարգերի հայտնի օրինակներ են.

$$\langle \mathbb{N}, + \rangle, \quad \langle \mathbb{Q}, - \rangle, \quad \langle \mathbb{R}, \cdot \rangle, \quad \langle \mathbb{Z}, +, \cdot \rangle, \quad \langle \mathbb{R}, +, -, \cdot \rangle, \ \langle \mathbb{C}, +, -, \cdot \rangle:$$

Այն դեպքերում, երբ հասկանալի է, թե որ գործողությունների հետ գործ ունենք տվյալ հանրահաշվական համակարգում, համառոտության համար ընդունված է բաց թողնել փակագծերն ու գործողությունների նշանները, եւ համակարգը նշանակել միայն մի տառով՝ A: Տվյալ $\langle A, \circ \rangle$ համակարգի համար A բազմությունը կոչվում է նրա *կրիչ*: Երկու գործողություններով հանրահաշվական համակարգերի կարեւորագույն օրինակներից է օղակը:

2.1.2 Օղակի սահմանումը. Ենթադրենք՝ ոչ դատարկ R բազմության վրա տրված են $+$ (գումարում) եւ $\cdot$ (բազմապատկում) հանրահաշվական գործողությունները, որոնք կամայական $a, b, c \in R$ տարրերի համար բավարարում են հետեւյալ պայմաններին.

O.1 $a + b = b + a$,

O.2 $(a + b) + c = a + (b + c)$,

O.3 գոյություն ունի այնպիսի $0 \in R$ տարր, որ $0 + a = a$,

O.4 գոյություն ունի $-a \in R$ տարր այնպիսին, որ $-a + a = 0$,

O.5 $(ab)c = a(bc)$,

O.6 $(a + b)c = ac + bc$ եւ $a(b + c) = ab + ac$:

Այդ դեպքում $\langle R, +, \cdot \rangle$ հանրահաշվական համակարգը կոչվում է *օղակ*:

Այստեղ եւ հետագայում օղակի երկու տարրերի արտադրյալի նշանակման մեջ բազմապատկման «$\cdot$» նշանը հաճախ բաց կթողնենք (ինչպես դա արվում է թվերի բազմապատկման դեպքում): **O.2** եւ **O.5** պայմանները կոչվում են գումարման եւ բազմապատկման գործողությունների ասոցիատիվություն: **O.1** պայմանը կոչվում է գումարման կոմուտատիվություն (կամ տեղափոխականություն): **O.3** պայմանում նշված 0 տարրը կոչվում է գումարման զրոյական տարր: **O.4** պայմանում նշված

$-a$ տարրը կոչվում է a տարրի հակադիր տարր: **O.6** պայմանները կոչվում են բաշխականության կանոններ: Խմբերի տեսության տարրերին ծանոթ ընթերցողը կնկատի, որ **O.1** - **O.4** պայմանները նշանակում են, որ $\langle R, + \rangle$ հանրահաշվական համակարգը աբելյան խումբ է (տես խմբերի տեսության (Каргаполов & Мерзляков, 1996), (Robinson, 1996), (Rotman, 1995) դասագրքերը կամ ընդհանուր հանրահաշվի (Cohn, 2003), (Кострикин, 1977), (Ленг, 1968), (ван дер Варден, 1979) դասագրքերը):

Օղակների դեպքում նույնպես ընդունված է $\langle R, +, \cdot \rangle$ օղակը նշանակել միայն R տառով եւ բաց թողնել գումարման ու բազմապատկման նշանները: Օղակների ակնհայտ օրինակներ են $\langle \mathbb{Z}, +, \cdot \rangle$ եւ $\langle \mathbb{R}, +, \cdot \rangle$ համակարգերը: $\langle R, +, \cdot \rangle$ օղակը կոչվում է *կոմուտատիվ* (կամ տեղափոխական) օղակ, եթե կամայական $a, b \in R$ տարրերի համար $ab = ba$: Իսկ եթե օղակում գոյություն ունի այնպիսի $1 \in R$ տարր, որ $1 \cdot a = a \cdot 1 = a$ կամայական $a \in R$ տարրի համար, ապա օղակը կոչվում է *միավորով օղակ*, իսկ 1 տարրը կոչվում է R օղակի միավոր: Երբեմն հարկ կլինի շեշտել, թե տրված 0 կամ 1 տարրը որ R օղակից են վերցված: Այդ դեպքում դրանք գրի կառնենք 0_R եւ 1_R տեսքով: Օղակի a, b տարրերի տարբերությունը ներմուծվում է հետեւյալ կերպ՝ $a - b = a + (-b)$:

2.1.3 Վարժություն. Ստուգել, որ կամայական $a, b \in R$ տարրերի եւ n ամբողջ թվի համար.

1) **O.3** պայմանում նշված 0 զրոյական տարրը միակն է:
2) **O.4** պայմանում նշված $-a \in R$ տարրը միակն է:
3) $a0 = 0 = 0a$:
4) $(-a)(-b) = ab$:
5) $(-a)b = a(-b) = -ab$:
6) $(n \cdot a)b = a\,(n \cdot b) = n \cdot (ab)$, որտեղ $n \cdot a$ նշանակում է $n \cdot a = \underbrace{a + \cdots + a}_{n}$:
7) Եթե օղակում գոյություն ունի 1 միավոր, ապա $(-1)a = a(-1) = -a$ եւ $(-1)(-a) = (-a)(-1) = a$:
8) $(a - b)c = ac - bc$ եւ $a(b - c) = ab - ac$:

Տրված R կոմուտատիվ օղակի a եւ b տարրերի համար կասենք, որ a-ն բաժանվում է b-ի վրա (սա կնշանակենք է $a \vdots b$), կամ որ b-ն բաժանում է a-ն (սա կնշանակենք է $b \mid a$), եթե գոյություն ունի $c \in R$ տարր այնպիսին, որ $a = bc$ կամ $a = cb$: Այս պայմաններում b-ն նաեւ կոչվում է a-ի բաժանարար, իսկ a-ն կոչվում է b-ի բազմապատիկ: Եթե b-ն չի բաժանում a-ն, ապա դա նշանակվում է $b \nmid a$:

Եթե R կոմուտատիվ օղակի c տարրը բաժանում է այդ օղակի միաժամանակ երկու a եւ b տարրերը, ապա այն կոչվում է դրանց ընդհանուր բաժանարար: c-ն կոչվում է a եւ b տարրերի ամենամեծ ընդհանուր բաժանարար, եթե այն դրանց

ընդհանուր բաժանարար է, եւ եթե օղակի t տարրը նույնպես a եւ b տարրերի ընդհանուր բաժանարար է, ապա c-ն բաժանվում է t-ի վրա (նկատենք, որ ամեն մի օղակի յուրաքանչյուր տարրերի համար չէ, որ գոյություն ունի ամենամեծ ընդհանուր բաժանարար, տես 2.5.3 թեորեմը): Նույն կերպ օղակում սահմանվում են օղակի տարրերի բազմապատիկի, ընդհանուր բազմապատիկի եւ ամենափոքր ընդհանուր բազմապատիկի հասկացությունները:

a եւ b տարրերի *ամենամեծ ընդհանուր բաժանարարը* նշանակվում է (a,b) կամ $\mathrm{GCD}(a,b)$: Իսկ *ամենափոքր ընդհանուր բազմապատիկը* նշանակվում է $[a,b]$ կամ $\mathrm{LCM}(a,b)$:

2.1.4 Օրինակներ. $\mathbb{Z}$ օղակում ունենք՝ $(6,8)=2$ եւ $(6,8)=-2$: $\mathbb{Z}[x]$ օղակում ունենք՝ $(x^2+3x,5x)=x$ եւ $(x^2+3x,5x)=-x$: Իսկ $\mathbb{Q}$-ի վրա տրված $\mathbb{Q}[x]$ օղակում այդ նույն բազմանդամների համար ունենք՝ $(x^2+3x,5x)=x$, $(x^2+3x,5x)=-7x$ եւ $(x^2+3x,5x)=\frac{11}{7}x$, քանի որ բոլոր երեք՝ x, $-7x$ եւ $\frac{11}{7}x$ բազմանդամներն էլ բավարարում են ամենամեծ ընդհանուր բաժանարարի սահմանմանը:

Նախորդ գլխում կիրառված “$\approx$” սիմվոլը միավորով կամայական R օղակի վրա տարածելով գրենք $a\approx 1$, եթե a տարրը հակադարձելի է. գոյություն ունի այնպիսի $a^{-1}\in R$ տարր, որ $aa^{-1}=1_R$: R օղակի a եւ b տարրերը կոչվում են *փոխադարձաբար պարզ* տարրեր, եթե $(a,b)\approx 1$, այսինքն՝ եթե նրանց ամենամեծ ընդհանուր բաժանարարը R օղակի հակադարձելի տարր է: Ավանդաբար ընդունված նշանակումը չխախտելու համար այս փաստը կնշանակենք $(a,b)=1$ տեսքով, չմոռանալով, որ, ասենք, $(3,8)=1$ եւ $(3,8)=-1$ պայմանները երկուսն էլ նշանակում են, որ 3 եւ 8 թվերը փոխադարձաբար պարզ են $\mathbb{Z}$ օղակում:

2.1.5 Դիտողություն. Բացառելով ակնհայտ դեպքերը, երբ a,b տարրերից մեկը կամ երկուսն էլ զրոյական են, (a,b)-ն ու $[a,b]$-ն հաշվելիս մենք ստորեւ կհամաբենք, որ a,b տարրերը ոչ զրոյական են:

Բերված հասկացությունները կարող են ընդհանրացվել մի քանի տարրերի դեպքի համար: $a_1,\dots,a_n\in R$ տարրերի համար սահմանվում է նրանց ընդհանուր բաժանարը, $(a_1,\dots,a_n)$ ընդհանուր ամենամեծ բաժանարը եւ $[a_1,\dots,a_n]$ ընդհանուր ամենափոքր բազմապատիկը: $a_1,\dots,a_n\in R$ տարրերը կոչվում են փոխադարձաբար պարզ տարրեր, եթե $(a_1,\dots,a_n)\approx 1$: Նրանք կոչվում են զույգ առ զույգ փոխադարձաբար պարզ տարրեր, եթե $(a_i,a_j)\approx 1$ կամայական $i,j=1,\dots,n$, $i\neq j$ ինդեքսների համար: Հասկանալի է, որ սա ավելի ուժեղ պայման է, քան $(a_1,\dots,a_n)\approx 1$ պայմանը:

2.1.6 Սահմանում. $\langle R,+,\cdot\rangle$ օղակի L ենթաբազմությունը կոչվում է R-ի ենթաօղակ, եթե այն օղակ է R-ում սահմանված գումարման եւ բազմապատկման $+$, $\cdot$ գործողությունների նկատմամբ:

2.1.7 Խնդիր. Ապացուցել, որ $\langle R, +, \cdot\rangle$ օղակի ոչ դատարկ L ենթաբազմությունը ենթաօղակ է այն եւ միայն այն դեպքում, երբ կամայական $a, b \in L$ տարրերի համար $a - b \in L$ եւ $ab \in L$: *Յուցում.* ոչ դատարկ L ենթաբազմությունը պարունակում է որեւէ $a \in L$ տարր: Դիտարկել $a - a$, $0 - a$ տարբերությունները:

2.1.8 Սահմանում. R օղակի I ենթաօղակը կոչվում է R-ի իդեալ, եթե կամայական $a \in I$ եւ $b \in R$ տարրերի համար $ba \in I$ եւ $ab \in I$:

2.1.9 Խնդիր. Ապացուցել, որ $\langle R, +, \cdot\rangle$ օղակի ոչ դատարկ I ենթաբազմությունը իդեալ է այն եւ միայն այն դեպքում, երբ կամայական $a, b \in I$ եւ $c \in R$ տարրերի համար $a - b \in I$ եւ $ac \in I$, $ca \in I$: *Յուցում.* օգտվել 2.1.7 խնդրից:

Օղակներ կառուցելու հարմար միջոց է ուղիղ արտադրյալի գաղափարը: Տրված $R_1, \dots, R_n$ օղակների համար դիտարկենք նրանց կրիչների (բազմությունների) դեկարտյան արտադրյալը՝

$$R = R_1 \times \cdots \times R_n = \{(a_1, \dots, a_n) \mid a_i \in R_i, i = 1, \dots, n\}:$$

R բազմության վրա կարելի է մտցնել նրա տարրերի (n-յակների) միջեւ գումարման եւ բազմապատկման գործողություններ հետեւյալ կերպ. R-ի $(a_1, \dots, a_n)$ եւ $(b_1, \dots, b_n)$ տարրերի համար սահմանենք՝

$$(a_1, \dots, a_n) + (b_1, \dots, b_n) = (a_1 + b_1, \dots, a_n + b_n),$$
$$(a_1, \dots, a_n) \cdot (b_1, \dots, b_n) = (a_1 b_1, \dots, a_n b_n):$$

Հեշտ է ստուգել, որ այս գործողությունների նկատմամբ R-ը օղակ է: Այն կոչվում է $R_1, \dots, R_n$ օղակների *ուղիղ արտադրյալ* եւ նշանակվում է $R = R_1 \times \cdots \times R_n$ կամ $R = \prod_{i=1}^{n} R_i$ տեսքով: Հնարավոր թյուրիմացություններից խուսափելու համար նշենք, որ գրականության մեջ սա երբեմն կոչվում է նաեւ օղակների *ուղիղ գումար* (եթե օղակը դիտարկենք որպես միայն ադիտիվ աբելյան խումբ, ապա տերմինները պիտի ներմուծվեն ըստ գումարման գործողության):

Տարրական մաթեմատիկայի ամենաբնական թվացող սկզբունքներից մեկն այն է, որ եթե երկու արտահայտությունների արտադրյալը 0 է, ապա արտադրիչներից որեւէ մեկը նույնպես հավասար է 0-ի: Դժվար չէ կառուցել օրինակ, որը ցույց կտա, որ հանրահաշվում դա միշտ չէ, որ այդպես է:

2.1.10 Օրինակ. Վերցնենք հետեւյալ մատրիցները $A = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}$: Այդ դեպքում $A \neq 0$ եւ $B \neq 0$, բայց $AB = 0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$:

2.1.11 Սահմանում. Եթե R օղակի $a, b \neq 0$ տարրերի համար $ab = 0$, ապա a եւ b տարրերը կոչվում են *զրոյի բաժանարարներ*:

Հաճախ տարբերակումը շեշտելու համար a-ն անվանում են *զրոյի ձախ բաժանարար*, իսկ b-ն՝ *զրոյի աջ բաժանարար*:

2.1.12 Սահմանում. R օղակը կոչվում է *ամբողջության տիրույթ*, եթե այն կոմուտատիվ է, ունի $1 \neq 0$ միավոր, եւ եթե այն ազատ է զրոյի բաժանարարներից՝ նրա կամայական a եւ b տարրերի համար $ab = 0$ հավասարությունից բխում է, որ $a = 0$ կամ $b = 0$:

2.1.13 Խնդիր. Զրոյի բաժանարարներից ազատ լինելու պայմանը կապված է իրար հավասար երկու արտահայտություններում աջից կամ ձախից նույն ոչ զրոյական արտադրիչը կրճատելու կանոնի հետ: Ցույց տալ, որ կոմուտատիվ եւ $1 \neq 0$ միավոր ունեցող օղակն ամբողջության տիրույթ է այն եւ միայն այն ժամանակ, երբ նրանում $ba = ca$ եւ $a \neq 0$ պայմաններից բխում է, որ $b = c$ (այսինքն՝ կատարվում է կրճատում a-ի վրա):

2.1.14 Սահմանում. R օղակը կոչվում է *դաշտ*, եթե այն կոմուտատիվ է, ունի $1 \neq 0$ միավոր, եւ եթե նրա կամայական a ոչ զրոյական տարր հակադարձելի է՝ գոյություն ունի $a^{-1} \in R$ այնպիսին, որ $aa^{-1} = 1$:

Ինչպես ցույց են տալիս հետեւյալ խնդիրները, բոլոր դաշտերի բազմությունը բոլոր ամբողջության տիրույթների բազմության սեփական ենթաբազմություն է:

2.1.15 Խնդիր. Ցույց տալ, որ յուրաքանչյուր դաշտ ամբողջության տիրույթ է: *Յուցում.* բավական է համեմատել միայն վերջին պայմանները եւ ցույց տալ, որ $a \neq 0$ հակադարձելի տարրը չի կարող լինել զրոյի բաժանարար: Ենթադրենք հակառակը եւ վերցնենք $b \neq 0$ տարրը, որի համար $ab = 0$: Մնում է 2.1.13 խնդիրը կիրառել հետեւյալ հավասարության վրա՝ $ab = 0 = a \cdot 0$:

2.1.16 Խնդիր. Գտնել այնպիսի մի ամբողջության տիրույթի օրինակ, որը դաշտ չէ: *Յուցում.* օգտվել 2.1.30 վարժությունից:

2.1.17 Վարժություն. Ցույց տալ, որ եթե դաշտի իդեալը զրոյական չէ, ապա այն համընկնում է ողջ դաշտի հետ: Յուրաքանչյուր դաշտ ունի ճիշտ երկու իդեալ:

Առաջին գլխում բերված “$\approx$” առնչությունը ամբողջության տիրույթներում ունի հետեւյալ կարեւոր ընդհանրացումը.

2.1.18 Սահմանում. R ամբողջության տիրույթի $a, b \in R$ տարրերը կոչվում են *ասոցացված տարրեր*, եթե գոյություն ունի մի $\varepsilon \in R^*$ հակադարձելի տարր այնպիսին, որ $a = \varepsilon \cdot b$: Այս փաստը նշանակվում է $a \approx b$:

2.1.19 Վարժություն. Ստուգել որ «$\approx$» սիմվոլի կիրառությունը երկու հասկացությունների նշանակման համար հակասություն չի առաջացնում. $a \approx 1$ գրությունը

նշանակում է «a եւ 1 տարրերն ասոցացված են» այն եւ միայն այն ժամանակ, երբ a տարրը հակադարձելի է:

2.1.20 Հատկություն. Հեշտ է ստուգել, որ ասոցացվածության առընչությունը *համարժեքության հարաբերություն* է:

2.1.21 Խնդիր. Ցույց տալ, որ R ամբողջության տիրույթի $a, b \in R$ տարրերի համար $a \approx b$ այն եւ միայն այն դեպքում, երբ $a \vdots b$ եւ $b \vdots a$:

Օղակների տեսության առանցքային հասկացություններից է.

2.1.22 Սահմանում. R ամբողջության տիրույթի ոչ զրոյական եւ ոչ հակադարձելի p տարրը կոչվում է *պարզ տարր* (կամ չբերվող տարր, անվերլուծելի տարր), եթե կամայական $p = b \cdot c$ ներկայացումից բխում է, որ $b \approx 1$ կամ $c \approx 1$:

Օղակների տեսության մեջ «պարզ տարր» եւ «չբերվող տարր» տերմիններով կարող են եւ տարբեր հասկացություններ նշանակվել. երբեմն պարզ տարրը սահմանվում է այսպես. p-ն պարզ է, եթե $bc \vdots p$ պայմանից բխում է, որ $b \vdots p$ կամ $c \vdots p$: Սա ընդհանուր դեպքում տարբեր է 2.1.22 սահմանումից, բայց ամբողջության տիրույթներում դրանք նույն բանն են նշանակում, եւ մենք օգտագործելու ենք «պարզ տարր», «չբերվող տարրեր», «անվերլուծելի տարր» տերմինները որպես հոմանիշներ, քանի որ դրանք կիրառելու ենք միայն ամբողջության տիրույթներում:

Օղակների, ինչպես եւ ամբողջության տիրույթների ու դաշտերի օրինակները հանրահաշվում բազմազան են: Ստորեւ նշենք միայն այն օրինակները, որոնք մեզ պետք են գալու ալգորիթմների կառուցման համար:

2.1.23 Թվային օրինակներ. Օղակների թվային օրինակներ են $\langle \mathbb{Z}, +, \cdot \rangle$, $\langle \mathbb{Q}, +, \cdot \rangle$, $\langle \mathbb{R}, +, \cdot \rangle$, $\langle \mathbb{C}, +, \cdot \rangle$ համակարգերը:

2.1.24 Վարժություն. Ֆիքսված k ամբողջ թվի համար դիտարկենք $k\mathbb{Z} = \{kz \mid z \in \mathbb{Z}\}$ բազմությունը, որն ակնհայտորեն բաղկացած է k-ի վրա բաժանվող բոլոր ամբողջ թվերից: Ցույց տալ, որ $\langle k\mathbb{Z}, +, \cdot \rangle$ համակարգն օղակ է: Հանդիսանու՞մ է այն ամբողջության տիրույթ կամ դաշտ:

2.1.25 Մոդուլյար օրինակներ. Տրված m դրական ամբողջ թվի համար $\mathbb{Z}_m$-ով նշանակենք $\{0, 1, \dots, m-1\}$ բազմությունը: Այս բազմության վրա սահմանենք մնացորդով գումարման եւ բազմապատկման գործողություններ հետեւյալ կերպ. եթե $a, b \in \mathbb{Z}_m$, ապա գոյություն ունի միակ r թիվ, որը պատկանում է $\mathbb{Z}_m$-ին, եւ որը բաղդատելի է $a + b$ գումարին: Դա այն մնացորդն է, որը ստացվում է $a + b$ գումարը m-ի վրա բաժանելիս: Հենց այս r թիվն էլ անվանենք a, b թվերի ըստ m մոդուլի գումար կամ մոդուլյար գումար: Սովորական գումարից տարբերելու համար երբեմն կնշա-

նակենք այն $+_m$ սիմվոլով՝ $r = a +_m b$, բայց ավելի հաճախ կօգտագործենք սովորական «+» նշանը, քանի որ, որպես կանոն, համատեքստից հասկանալի է լինում, թե որ գումարի հետ գործ ունենք: Նույն կերպ սահմանվում է ըստ m մոդուլի արտադրյալը, կամ մոդուլյար արտադրյալը՝ $r = a \cdot_m b$, որտեղ r-ը այն միակ թիվն է, որը պատկանում է $\mathbb{Z}_m$-ին եւ որը բաղդատելի է $a \cdot b$ արտադրյալին. դա այն մնացորդն է, որը ստացվում է $a \cdot b$ արտադրյալը m-ի վրա բաժանելիս: $a \cdot_m b$ արտադրյալը նույնպես հաճախ կնշանակենք պարզապես $a \cdot b$ կամ ab, եթե հասկանալի է, թե որ արտադրյալի մասին է խոսքը: Օրինակ՝ $3 +_6 4 = 1$ եւ $6 \cdot_7 3 = 4$:

Հետեւյալ հայտնի փաստը բերենք առանց ապացույցի.

2.1.26 Թեորեմ. *$\mathbb{Z}_m$ մնացքների օղակը դաշտ է այն եւ միայն այն դեպքում, երբ m-ը պարզ թիվ է:*

2.1.27 Մատրիցային օրինակներ. Կամայական կոմուտատիվ R օղակի եւ m, n բնական թվերի համար դիտարկենք R-ի տարրերից կազմված, m տողերից եւ n սյուներից բաղկացած բոլոր մատրիցների $M_{m,n}(R)$ բազմությունը.

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \in M_{m,n}(R); \;\; a_{ij} \in R; \;\; i = 1, \dots, m; \;\; j = 1, \dots, n:$$

Համառոտ կնշանակենք $A = \|a_{ij}\|_{m,n}$ կամ պարզապես $A = \|a_{ij}\|$, եթե m, n արժեքները նշելը անհրաժեշտ չէ: Այսպիսի մատրիցների հետ գործողությունները սահմանվում են նույն կերպ, ինչ սովորական թվային մատրիցների միջեւ: Եթե տրված է միեւնույն կարգի եւս մի $B = \|b_{ij}\|$ մատրից, ապա $A + B = C = \|c_{ij}\|$, որտեղ

$$c_{ij} = a_{ij} + b_{ij}, \qquad i = 1, \dots, m; \;\; j = 1, \dots, n:$$

Իսկ արտադրյալը սահմանվում է «տողերը սյուներով բազմապատկելու» կանոնով. $AB = C = \|c_{ij}\|$, որտեղ

$$c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}, \qquad i = 1, \dots, m; \;\; j = 1, \dots, n:$$

Երբ մատրիցները քառակուսային են, այսինքն, երբ $m = n$, ապա ընդունված է ավելի կարճ նշանակումներ օգտագործել. $M_n(R)$ եւ $\|a_{ij}\|_n$:

$\langle M_n(R), +, \cdot \rangle$ համակարգն օղակ է: Այն կոչվում է R օղակի վրա տրված *լրիվ մատրիցային օղակ*: Այս դասընթացում մեզ պետք են գալու առաջին հերթին $M_n(\mathbb{Z})$ եւ $M_n(\mathbb{Z}_p)$ մատրիցային օղակները (p-ն որեւէ պարզ թիվ է):

2.1.28 Օրինակ. Ենթադրենք՝ $R = \mathbb{Z}_7$: Այդ դեպքում $M_3(\mathbb{Z}_7)$ օղակում տեղի ունի.

$$\begin{pmatrix} 1 & 2 & 0 \\ 0 & 6 & 0 \\ 2 & 3 & 4 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 4 & 1 \\ 3 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 2 & 2 \\ 0 & 3 & 6 \\ 5 & 5 & 0 \end{pmatrix}:$$

Այս արտադրյալում, օրինակ, $c_{32}=5$, քանի որ $\mathbb{Z}_7$ օղակում $2\cdot 1+3\cdot 4+4\cdot 3=5$: Իսկ $c_{33}=0$, քանի որ $2\cdot 0+3\cdot 1+4\cdot 1=0$:

2.1.29 Վարժություն. $M_2(\mathbb{Z}_5)$ օղակում հաշվել հետեւյալ արտադրյալները.

$$\begin{pmatrix}1&0\\3&3\end{pmatrix}\begin{pmatrix}3&1\\2&4\end{pmatrix},\quad \begin{pmatrix}3&1\\2&3\end{pmatrix}\begin{pmatrix}2&1\\0&2\end{pmatrix},\quad \begin{pmatrix}4&1\\1&3\end{pmatrix}\begin{pmatrix}1&0\\0&1\end{pmatrix}:$$

Դիտարկենք որեւէ R ամբողջության տիրույթ եւ R-ի վրա սահմանենք բազմանդամներ որպես

$$f(x)=a_0x^n+a_1x^{n-1}+\cdots+a_{n-1}x+a_n$$

տեսքի ձեւական (ֆորմալ) արտահայտություններ, որտեղ $a_0,\dots,a_n$ տարրերը R-ից են ($a_0\neq 0$) եւ կոչվում են բազմանդամի *գործակիցներ*, x սիմվոլը կոչվում է *փոփոխական*, իսկ $x^n,x^{n-1},\dots,x$ արտահայտությունները ոչ բացասական ամբողջ $n,n-1,\dots,1,0$ թվերի համար ձեւական արտահայտություններ են, որոնք կոչվում են *x-ի աստիճաններ* (համարենք, որ $x^1=x$, այսինքն՝ $a_{n-1}x=a_{n-1}x^1$ եւ, որ $x^0=1$, այսինքն՝ $a_n=a_nx^0$): n թիվը կոչվում է $f(x)$ բազմանդամի աստիճան եւ նշանակվում՝ $n=\deg f(x)$: Մասնավորապես, եթե $f(x)=a_0\neq 0$, ապա $n=\deg f(x)=0$: Բացառություն է կազմում $f(x)=a_0=0$ զրոյական բազմանդամը, որի համար աստիճանի հասկացություն չի սահմանվում: a_ix^{n-i} տեսքի ձեւական արտահայտությունները ($i=0,\dots,n$) կոչվում են $f(x)$ բազմանդամի անդամներ, դրանցից a_0x^n-ը կոչվում է բազմանդամի ավագ անդամ, իսկ a_0 գործակիցն՝ ավագ գործակից: a_n-ը կոչվում է բազմանդամի ազատ անդամ: R ամբողջության տիրույթի վրա տրված բոլոր բազմանդամների բազմությունը նշանակվում է $R[x]$ սիմվոլով: 6.2 պարագրաֆում մենք կբերենք բազմանդամի ձեւական սահմանումը մի քանի փոփոխականների դեպքի համար: Ենթադրենք R-ի վրա տրված է եւս մի բազմանդամ.

$$g(x)=b_0x^m+\cdots+b_m\in R[x]:$$

$f(x)$ եւ $g(x)$ բազմանդամների $f(x)+g(x)$ գումարը սահմանվում է «նման անդամների միացման» կանոնով, այսինքն իրար են գումարվում հավասար աստիճաններին համապատասխան անդամները. եթե $n-i=m-j$, ապա

$$a_ix^{n-i}+b_jx^{m-j}=(a_i+b_j)x^{n-i}=(a_i+b_j)x^{m-j},$$

ընդ որում, եթե որեւէ աստիճանի համապատասխան անդամ կա բազմանդամներից միայն մեկում (այդպես կլինի այդպես, երբ $\deg f(x)\neq\deg g(x)$), ապա մյուս բազմանդամի «պակասող» գումարելու փոխարեն վերցնում ենք զրոյական գումարելի: Օրինակ՝ $2x^3+x$ եւ x^2+3x+5 բազմանդամների գումարի ավագ գործակիցն է $2+0=2$, իսկ ազատ անդամը՝ $0+5=5$: Հասկանալի է, որ

$$\deg\big(f(x)+g(x)\big)\leq\max\{n,m\},$$

որտեղ խիստ անհավասարություն տեղի ունի, միայն, երբ բազմանդամների աստիճանները հավասար են եւ $a_0=-b_0$ (ավագ անդամները կրճատվում են):

$f(x)$ եւ $g(x)$ բազմանդամների $f(x)g(x)$ արտադրյալը սահմանվում է «փակագծերի բացման, ապա նման անդամների միացման» կանոնով, այսինքն.

$$f(x)g(x) = c_0x^{n+m} + \cdots + c_{n+m} \in R[x],$$

որտեղ

$$c_k = \sum_{\substack{i,j \\ i+j=k}} a_i\, b_j\,, \quad k = 0, \dots, n+m:$$

Սահմանված երկու գործողությունների հետ միասին $R[x]$-ը հանրահաշվական համակարգ է: Ավելին, $\langle R[x], +, \cdot\rangle$ համակարգը օղակ է: Այն կոչվում է R օղակի վրա տրված *բազմանդամային օղակ*:

2.1.30 Վարժություն. Տրված R ամբողջության տիրույթի համար դիտարկենք $R[x]$ բազմանդամային օղակը: Արդյո՞ք այն ամբողջության տիրույթ է: Արդյո՞ք այն դաշտ է: Համեմատել սա 2.1.16 խնդրի հետ:

Հետեւյալ օրինակը նշում է օղակի մի կարեւոր տեսակ, որը մենք բազմիցս օգտագործելու ենք ալգորիթմների կառուցման համար:

2.1.31 Օրինակ. Քանի որ ըստ 2.1.26 թեորեմի $\mathbb{Z}_p$ մնացքների օղակը դաշտ է (եւ, ուրեմն, ամբողջության տիրույթ է), ապա նրա վրա կարելի է սահմանել $\mathbb{Z}_p[x]$ օղակը, որը կանվանենք *մոդուլար բազմանդամների օղակ*: $\mathbb{Z}_p[x]$ օղակի տարրերը $f(x) = a_0x^n + \cdots + a_n$ տեսքի բազմանդամներն են, որոնց գործակիցները $\mathbb{Z}_p$ դաշտից են, եւ որոնց հետ գումարման եւ բազմապատկման գործողություններ կատարելիս գործակիցները գումարվում եւ բազմապատկվում են ըստ մոդուլի: Այժմ հեշտ է նկատել, որ 1.2 պարագրաֆում քննարկվող $f_m(x)$ բազմանդամները $\mathbb{Z}_m[x] = \mathbb{Z}_p[x]$ օղակից են: 1.2 պարագրաֆի նյութի եւ այս օղակի հետ կապված՝ տես նաեւ 2.3.6 եւ 2.3.7 կարեւոր հոմոմորֆիզմների օրինակները:

Այժմ տեսնենք, թե ինչու են բազմանդամները սահմանվում ոչ թե կամայական օղակների, այլ ամբողջության տիրույթների (մասնավորապես, դաշտերի) վրա: Եթե R օղակում չպահանջենք կոմուտատիվության պայմանը, ապա

$$a_ix^{n-i} \cdot b_jx^{m-j} = a_i(x^{n-i}b_j)x^{m-j} = a_i(b_jx^{n-i})x^{m-j} = a_ib_jx^{n+m-i-j}$$

հավասարություններից երկրորդը կարող է եւ խախտվել, եթե x-ի փոխարեն R օղակում վերցնենք որեւէ տարր: Այսինքն՝ «փոփոխականի փոխարեն արժեք տեղադրելու» սկզբունքը բազմանդամներում բնական իմաստ ունի միայն կոմուտատիվ օղակների վրա:

R օղակում 1 միավորի գոյությունը անհրաժեշտ է, քանի որ առանց դրա չենք կարող համարել, որ $R[x]$ օղակը պարունակում է x-ի աստիճանները. $x^k = 1 \cdot x^k \in R[x]$: Իսկ զրոյի բաժանարարներից ազատ լինելու պայմանը երաշխավորում է, որ եթե ցանկացած երկու բազմանդամների $a_i x^{n-i}$ եւ $b_j x^{m-j}$ անդամները զրոյական չեն ($a_i, b_j \neq 0$), ապա զրոյական չէ նաեւ նրանց $a_i b_j x^{n+m-i-j}$ արտադրյալը:

Հետեւյալ երկու փաստերը մենք կօգտագործենք մի քանի ալգորիթմներում:

2.1.32 Լեմմա. $\mathbb{Z}_p$ դաշտի կամայական a, b տարրերի համար տեղի ունի $(a+b)^p = a^p + b^p$ հավասարությունը:

Ապացույց: Սա հեշտ է ստուգել Նյուտոնի բինոմական բանաձեւը $\mathbb{Z}_p$-ում կիրառելով: Իրոք $(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^{p-i} b^i$, որտեղ աջ մասի $p+1$ հատ գումարելիներից առաջինը a^p է, վերջինը՝ b^p, իսկ մնացած $p-1$ հատ գումարելիներից յուրաքանչյուրը բաժանվում է p-ի վրա, այսինքն՝ հավասար է 0-ի $\mathbb{Z}_p$-ում: ■

Քանի որ 2.1.32 լեմմայի հավասարությունը տեղի ունի $\mathbb{Z}_p$ դաշտի կամայական տարրերի համար, եւ քանի որ $\mathbb{Z}_p[x]$ օղակի կամայական $f(x)$ բազմանդամի փոփոխականի փոխարեն տեղադրելով կամայական $x' \in \mathbb{Z}_p$ արժեք՝ դարձյալ ստանում ենք $f(x')$ արժեք $\mathbb{Z}_p$ դաշտից, ապա 2.1.32 լեմման՝ որպես «կետ առ կետ հավասարություն» բազմանդամային արտահայտությունների վրա կիրառելով՝ կստանանք.

2.1.33 Հետեւանք. $\mathbb{Z}_p[x]$ օղակի կամայական $f(x)$, $g(x)$ բազմանդամների համար տեղի ունի $\big(f(x)+g(x)\big)^p = f(x)^p + g(x)^p$ հավասարությունը:

2.2 Գլխավոր իդեալներ եւ բաղդատումներ, ծնիչ բազմություններ

1.2 պարագրաֆում մենք սահմանեցինք $a, b \in \mathbb{Z}$ ամբողջ թվերի $a \equiv b \pmod m$ բաղդատումները եւ նշեցինք դրանց տարրական հատկությունները: Մեր ալգորիթմներում պետք է գալու բաղդատման հասկացության ընդհանրացումը բազմանդամների համար: Այս պարագրաֆում բազմանդամների բաղդատումը սահմանվելու է օղակի գլխավոր իդեալների միջոցով: Բայց քանի որ աբստրակտ հանրահաշվական սահմանումը կարող է դյուրընկալելի չլինել, ապա առաջին ընթերցման ժամանակ բավարար է հիշել միայն այն, որ $f(x)$, $g(x)$, $m(x)$ ամբողջ կամ մոդուլյար գործակիցներով բազմանդամների համար

$$f(x) \equiv g(x) \big(\mathrm{mod}\, m(x)\big)$$

գրառումը (կարդացվում է՝ «$f(x)$-ը բաղդատելի է $g(x)$-ի հետ ըստ $m(x)$ մոդուլի») նշանակում է, որ $f(x) - g(x)$ տարբերությունը բաժանվում է $m(x)$-ի վրա, եւ որ այս

բաղդատումը ունի այն նույն հատկությունները, որ ամբողջ թվերի համար բերեցինք 1.2 պարագրաֆի սկզբում:

Քանի որ բաժանելիության հասկացությունը կա բոլոր օղակներում, ապա ամեն մի R օղակի a, b, m տարրերի համար էլ կարելի է դիտարկել $(a-b) \vdots m$ պայմանը: Սակայն ամեն մի օղակում չէ, որ կարելի է դրա շնորհիվ սահմանել այնպիսի օղակային բաղդատում, որը ունենա նույն տարրական հատկությունները, որոնք բերված են 1.2 պարագրաֆի սկզբում ամբողջ թվերի համար:

Բայց միավորով կոմուտատիվ օղակներում դա կարելի է իրականացնել գլխավոր իդեալի հասկացության միջոցով: Տրված R օղակի m տարրի համար սահմանենք $mR = \{ma | a \in R\} \subseteq R$ ենթաբազմությունը: Օրինակ՝ 2.1.24 վարժության $k\mathbb{Z}$ բազմությունը սրա մասնավոր դեպք է $R = \mathbb{Z}$ օղակի համար:

2.2.1 Խնդիր. Ստուգել, որ եթե R օղակը կոմուտատիվ է եւ ունի միավոր, ապա նրա կամայական m տարրի համար mR ենթաբազմությունը կհանդիսանա R-ի ենթաօղակ (եւ իդեալ) ու կպարունակի m-ը: *Ցուցում.* աջ իդեալ լինելու պայմանն ակնհայտ է, իսկ ձախ իդեալ լինելու պայմանի համար օգտվել R-ի կոմուտատիվությունից:

R միավորով կոմուտատիվ օղակի mR իդեալը կոչվում է m տարրով ծնված *գլխավոր իդեալ*: Կամայական R օղակի a, b տարրերը կոչվում են բաղդատելի ըստ I իդեալի, եւ դա նշանակվում է $a \equiv b (\mathrm{mod}\, I)$, եթե $a - b \in I$: Մասնավորապես, եթե R օղակը կոմուտատիվ է եւ ունի միավոր, ապա իմաստ ունի $a \equiv b (\mathrm{mod}\, mR)$ բաղդատումը, քանի որ mR-ը նույնպես իդեալ է ըստ 2.2.1 խնդրի: Այս բաղդատումն ընդունված է նշանակել $a \equiv b (\mathrm{mod}\, m)$ տեսքով (բաց է թողնված «R» տառը) եւ ասել. «R օղակի a, b տարրերը բաղդատելի են ըստ m մոդուլի»:

2.2.2 Օրինակ. $\mathbb{Z}_3[x]$ օղակում տեղի ունի. $x^3 + 1 \equiv x + 1 (\mathrm{mod}\, 2x^2 + 1)$:

2.2.3 Օրինակ. 1.3 պարագրաֆում Կնուտի մոդուլյար մեթոդը կիրառելիս մենք երեք անգամ կատարեցինք բազմանդամների անկյունով բաժանում: Դրանց $\mathbb{Z}_5[x]$ օղակում համապատասխանում են հետեւյալ երեք բաղդատումները՝

$$x^8 + x^6 + 2x^4 + 2x^3 + 3x^2 + 2x \equiv 4x^2 + 3 (\mathrm{mod}\, 3x^6 + x^2 + x + 1),$$
$$3x^6 + x^2 + x + 1 \equiv x (\mathrm{mod}\, 4x^2 + 3),$$
$$4x^2 + 3 \equiv 3 (\mathrm{mod}\, x):$$

2.2.4 Խնդիր. Ստուգել R միավորով կոմուտատիվ օղակում բաղդատումների տարրական հատկությունները. եթե $a \equiv b (\mathrm{mod}\, m)$ եւ $a' \equiv b' (\mathrm{mod}\, m)$ տրված $a, b, a', b', m \in R$ տարրերի համար, ապա.

$$a + a' \equiv b + b' (\mathrm{mod}\, m), \quad a - a' \equiv b - b' (\mathrm{mod}\, m), \quad aa' \equiv bb' (\mathrm{mod}\, m):$$

2.2.5 Խնդիր. Ստուգել, որ R միավորով կոմուտատիվ օղակում տարրերի՝ իրար հետ ըստ m մոդուլի բաղդատելի լինելու հարաբերությունը համարժեքության հարաբերություն է: Մասնավորապես, R-ի կրիչ բազմությունը տրոհվում է համարժեքության դասերի, որտեղ յուրաքանչյուր դաս բաղկացած է այդ դասի որեւէ տարրին համարժեք բոլոր տարրերից:

Օղակների մի կարեւոր տեսակ են այն օղակները, որոնց բոլոր իդեալները գլխավոր են: Այդ օղակների ալգորիթմական հնարավորություններից մեկն այն է, որ դրանցում ըստ յուրաքանչյուր I իդեալի բաղդատումը հանգում է ըստ որեւէ տարրի բաղդատման. ըստ այն m տարրի, որի համար $I = mR$:

2.2.6 Սահմանում. R ամբողջության տիրույթը կոչվում է *գլխավոր իդեալների օղակ*, եթե նրա յուրաքանչյուր I իդեալ գլխավոր է, այսինքն՝ I իդեալի համար գոյություն ունի $m \in R$ տարր այնպիսին, որ $I = mR$:

2.2.7 Խնդիր. Ցույց տալ, որ $\mathbb{Z}$ օղակը գլխավոր իդեալների օղակ է: *Ցուցում.* $\mathbb{Z}$ օղակի կամայական ոչ զրոյական I իդեալի համար դիտարկել այն ոչ զրոյական $m \in I$ տարրը, որը բացարձակ արժեքով չի գերազանցում I իդեալի մնացած տարրերին:

Անցնենք օղակների, ենթաօղակների եւ իդեալների ծնիչ բազմությունների սահմանմանը: Ինչպես կտեսնենք քիչ հետո, գլխավոր իդեալի հասկացությունը դրանց մի մասնավոր դեպքն է:

2.2.8 Սահմանում. R օղակի ոչ դատարկ A *ենթաբազմությամբ ծնված ենթաօղակ* է կոչվում R-ի այն մինիմալ ենթաօղակը, որը պարունակում է A-ն: Այդ ենթաօղակը նշանակվում է $R[A]$:

Մինիմալությունը այստեղ հասկացվում է տեսաբազմական իմաստով՝ $R[A]$-ն պարունակվում է R-ի ցանկացած S ենթաօղակում, եթե S-ը պարունակում է A-ն: Սահմանումը կոռեկտ է, քանի որ գոյություն ունի A-ն պարունակող գոնե մեկ ենթաօղակ՝ $S = R$: A-ն կոչվում է $R[A]$ *ենթաօղակի ծնիչ*:

2.2.9 Օրինակ. $\mathbb{Z}$ օղակում վերցնենք $A = \{4, 6\}$: Զույգ թվերի $2\mathbb{Z}$ ենթաօղակը պարունակում է A-ն: Մյուս կողմից, եթե որեւէ S ենթաօղակ պարունակում է A-ն, ապա այն պարունակում է $6 - 4 = 2$ տարբերությունը: Իսկ եթե S-ը պարունակում է 2-ը, ապա այն պարունակում է նաեւ բոլոր զույգ թվերը: Ուստի $\mathbb{Z}[4, 6] = 2\mathbb{Z}$:

2.2.10 Սահմանում. R օղակի ոչ դատարկ A *ենթաբազմությամբ ծնված իդեալ* է կոչվում R-ի այն մինիմալ իդեալը, որը պարունակում է A-ն: Այդ իդեալը նշանակվում է $\langle A \rangle$:

Կրկին մինիմալությունը հասկացվում է տեսաբազմական իմաստով: Սահմանումը կոռեկտ է, քանի որ գոյություն ունի A-ն պարունակող գոնե մեկ իդեալ՝ R-ը: A-ն կոչվում է $\langle A \rangle$ *իդեալի ծնիչ*: Առանձնապես կարեւոր է այն դեպքը, երբ $\langle A \rangle$-ն

համընկնում է ողջ R օղակի հետ: Այդ դեպքում նշանակվում է $\langle A\rangle = R$, իսկ A-ն կոչվում է *օղակի ծնիչ:*

2.2.11 Օրինակ. Միավորով կոմուտատիվ R օղակում վերցնենք որեւէ m տարր: Ըստ սահմանման, $\langle m\rangle$ իդեալը պարունակվում է mR գլխավոր իդեալի մեջ, քանի որ mR-ը պարունակում է $m = m \cdot 1$ տարրը: Մյուս կողմից, ցանկացած $m \cdot r$ արտադրյալ $\langle m\rangle$-ից է, քանի որ $\langle m\rangle$-ը իդեալ է: Ուրեմն՝ $\langle m\rangle = mR$: Մասնավորապես, $\mathbb{Z}$ օղակում ունենք՝ $\langle k\rangle = k\mathbb{Z}$:

Հետեւյալ բնութագրումը մենք հետագայում հաճախ ենք օգտագործելու.

2.2.12 Թեորեմ. *Ենթադրենք միավորով կոմուտատիվ R օղակում տրված է A ոչ դատարկ ենթաբազմությունը: Այդ դեպքում*

$$\langle A\rangle = \left\{ \sum_{i=1}^{n} a_i r_i \;\middle|\; a_i \in A;\ r_i \in R;\ i = 1, \dots, n;\ n \in \mathbb{N} \right\}. \tag{2.1}$$

Ըստ թեորեմի՝ $\langle A\rangle$ իդեալը գտնելու համար պետք է վերցնել A-ի տարրերի $a_1, \dots, a_n$ վերջավոր հաջորդականությունները, դրանցից a_i անդամները R-ի որեւէ r_i տարրերով բազմապատկել ($i = 1, \dots, n$), եւ ստացված արտադրյալները գումարել իրար: Պարզ է, որ երբ R-ը բաղկացած է մեկ տարրից, ստանում ենք գլխավոր իդեալի սահմանումը:

2.2.12 թեորեմի ապացույցը: (2.1)-ի աջ կողմի բազմությունը նշանակենք A^*: Պարզ է, որ $\sum_{i=1}^{n} a_i r_i$ տեսքի գումարներն իրար գումարելիս այդ տեսքի գումար է ստացվում: Քանի որ կամայական $t \in R$ տարրի համար $(\sum_{i=1}^{n} a_i r_i) \cdot t = \sum_{i=1}^{n} a_i (r_i t)$ գումարը նույնպես այդ տեսքի է, հեշտ է ստուգել, որ A^* բազմությունը իդեալ է: Այն պարունակում է A-ն, քանի որ կամայական $a \in A$ տարր կարելի է ներկայացնել $a \cdot 1$ տեսքով: Ուրեմն, ըստ 2.2.10 սահմանման, $\langle A\rangle \subseteq A^*$: Մյուս կողմից, քանի որ $\langle A\rangle$-ն իդեալ է, այն պարունակում է բոլոր $a_i r_i$ ($i = 1, \dots, n$) արտադրյալները եւ դրանց գումարները: Այսինքն՝ $A^* \subseteq \langle A\rangle$: ■

2.3 Օղակների հոմոմորֆիզմներ, մոդուլյար անցում, ֆակտոր-օղակներ

2.3.1 Սահմանում. Տրված $\langle R, +, \cdot\rangle$ եւ $\langle K, +, \cdot\rangle$ օղակների հոմոմորֆիզմ է կոչվում այն

$$\varphi : R \to K$$

արտապատկերումը, որը համաձայնեցված է օղակներում սահմանված գումարման եւ բազմապատկման գործողությունների հետ, այսինքն՝ եթե ցանկացած $a, b \in R$ տարրերի համար տեղի ունեն հետեւյալ պայմանները.

H.1 $\varphi(a+b)=\varphi(a)+\varphi(b)$,
H.2 $\varphi(ab)=\varphi(a)\varphi(b)$:

Հաշվի առնելով սահմանմանը նախորդող դիտողությունը՝ նկատենք, որ **H.1** եւ **H.2** հավասարությունների աջ եւ ձախ մասերում մասնակցող գումարման ու բազմապատկման գործողությունները կարող են տարբեր գործողություններ լինել:

2.3.2 Օրինակ. Եթե $R=\mathbb{C}$ եւ $K=\mathbb{R}$, ապա յուրաքանչյուր $z=a+ib$ կոմպլեքս թվի իր իրական մասը համապատասխանեցնող $\varphi(z)=\Re(z)=a$ արտապատկերումը, ինչպես եւ կեղծ մասի մոդուլը համապատասխանեցնող $\phi(z)=|\Im(z)|=b$ արտապատկերումը հոմոմորֆիզմներ են:

2.3.3 Վարժություն. Արդյոք հոմոմորֆի՞զմ են $\varphi\colon\mathbb{C}\to\mathbb{C}$ եւ $\psi\colon\mathbb{C}\to\mathbb{C}$ արտապատկերումները, որոնք կոմպլեքս թվերի վրա տրված են $\varphi(z)=|z|$ եւ $\psi(z)=\bar{z}$ կանոններով ($\bar{z}$-ը կոմպլեքս z թվի համալուծն է):

Օղակների $\varphi\colon R\to K$ հոմոմորֆիզմը կոչվում է սյուրյեկտիվ հոմոմորֆիզմ, եթե այն սյուրյեկտիվ արտապատկերում (վրա արտապատկերում) է R բազմությունից K բազմության վրա: Այսինքն՝ եթե կամայական $b\in K$ տարրի համար գոյություն ունի $a\in R$ տարր այնպիսին, որ $\varphi(a)=b$: Իսկ $\varphi\colon R\to K$ հոմոմորֆիզմը կոչվում է ինյեկտիվ հոմոմորֆիզմ, եթե այն ինյեկտիվ արտապատկերում (միարժեք արտապատկերում) է R բազմությունից K բազմության մեջ: Այսինքն՝ կամայական $a_1,a_2\in R$ տարրերի համար, եթե $a_1\neq a_2$, ապա նաեւ $\varphi(a_1)\neq\varphi(a_2)$:

2.3.4 Սահմանում. R եւ K օղակների $\varphi\colon R\to K$ հոմոմորֆիզմը կոչվում է *իզոմոմորֆիզմ*, եթե այն սյուրյեկտիվ եւ ինյեկտիվ է: Այսինքն, եթե այն բիյեկտիվ (փոխմիարժեք) արտապատկերում է: Այս փաստը գրի է առնվում $R\cong K$տեսքով:

$\varphi\colon R\to K$ հոմոմորֆիզմի *միջուկ* է կոչվում R-ի հետեւյալ ենթաբազմությունը՝

$$\ker\varphi=\{a\in R\mid\varphi(a)=0\}$$

(նշանակումը ծագում է «kernel» բառից): Իսկ այդ հոմոմորֆիզմի *պատկեր* է կոչվում K-ի հետեւյալ ենթաբազմությունը՝

$$\operatorname{im}\varphi=\{b\in K\mid\exists\, a\in R,\ \ \varphi(a)=b\}$$

(նշանակումը ծագում է «image» բառից): Որոշ աղբյուրներում պատկերը նշանակում են նաեւ $\operatorname{im}_\varphi(R)$:

2.3.5 Խնդիր. Ցույց տալ, որ կամայական $\varphi\colon R\to K$ հոմոմորֆիզմի համար $\ker\varphi$-ն R օղակի իդեալ է: Ստուգել՝ արդյո՞ք $\operatorname{im}\varphi$-ն ենթաօղակ է, արդյո՞ք $\operatorname{im}\varphi$-ն իդեալ է:

Յուցում. եթե $\varphi(a) = 0$ ապա կամայական $c \in R$ տարրի համար $\varphi(ac) = \varphi(a)\varphi(c) = 0 \cdot \varphi(c) = 0$:

Այժմ անցնենք հոմոմորֆիզմի այն օրինակներին, որոնք առավել հաճախ ենք օգտագործելու:

2.3.6 Օրինակ (թվային մոդուլյար անցում). Դիտարկենք

$$\varphi\colon \mathbb{Z} \to \mathbb{Z}_m$$

արտապատկերումը ամբողջ թվերի $\mathbb{Z}$ օղակից մնացքների որեւէ $\mathbb{Z}_m$ օղակի մեջ հետեւյալ կանոնով. յուրաքանչյուր ամբողջ թվի համապատասխանեցվում է այդ թիվը m-ի վրա բաժանելիս ստացված մնացորդը (հասկանալի է, որ այն միակն է): 1.2 պարագրաֆի սկզբում բերված բաղդատումների տարրական հատկություններից անմիջապես երեւում է, որ φ արտապատկերումը հոմոմորֆիզմ է: Մենք կանվանենք այն թվային մոդուլյար անցում (կամ ռեդուկցիա) ըստ m մոդուլի եւ կնշանակենք φ_m տեսքով: Մասնավորապես, երբ $m = p$ պարզ թիվ է, կունենանք φ_p նշանակումը: Հեշտ է ստուգել, որ այս հոմոմորֆիզմի համար՝

$$\ker \varphi_m = m\mathbb{Z} = \{mn \,|n \in \mathbb{Z}\} \quad \text{եւ} \quad \operatorname{im} \varphi_m = \mathbb{Z}_m\colon$$

2.3.7 Օրինակ (բազմանդամային մոդուլյար անցում). Իսկ այժմ դիտարկենք

$$\varphi\colon \mathbb{Z}[x] \to \mathbb{Z}_p[x]$$

արտապատկերումը, որն ամբողջ գործակիցներով կամայական $f(x) = a_0x^n + \cdots + a_n$ բազմանդամի համապատասխանեցնում է

$$\varphi\big(f(x)\big) = \varphi_p(a_0)x^n + \cdots + \varphi_p(a_n) \in \mathbb{Z}_p[x]$$

մոդուլյար բազմանդամը (տես 2.1.31 օրինակը): 1.2 պարագրաֆի նյութից, մասնավորապես, բաղդատման տարրական կանոններից բխում է, որ այս արտապատկերումը հոմոմորֆիզմ է: Հեշտ է ստուգել, որ այս φ հոմոմորֆիզմի համար $\ker\varphi$-ն բաղկացած է այն $f(x) \in \mathbb{Z}[x]$ բազմանդամներից, որոնց բոլոր գործակիցները բաժանվում են p-ի վրա: Պարզ է նաեւ, որ $\operatorname{im}\varphi = \mathbb{Z}_p[x]$:

Այն, ինչ մենք 1.2 պարագրաֆում նշանակեցինք $f_p(x)$, այստեղ հանդիսանում է $f(x) \in \mathbb{Z}[x]$ բազմանդամի պատկերը՝ $\varphi\big(f(x)\big) = f_p(x)$: Անվանենք այս հոմոմորֆիզմը բազմանդամային մոդուլյար անցում (կամ ռեդուկցիա) ըստ p մոդուլի, եւ այն նույնպես նշանակենք φ_p տեսքով (մեր շարադրանքում սա թյուրիմացություն չի առաջացնում, քանի որ թվերն ու բազմանդամները միշտ տարբեր տառերով են

նշանակվում, ուստի միշտ հասկանալի է, որ $\varphi_p(a)$-ն թիվ է, իսկ $\varphi_p\big(f(x)\big)$-ը՝ բազմանդամ): 1.2 պարագրաֆի շարադրանքի հետ զուգահեռները էլ ավելի են շեշտվում հետեւյալ նշանակմամբ.

$$f_p(x) = \varphi_p\big(f(x)\big):$$

$\mathbb{Z}_p[x]$ օղակի ամեն մի բազմանդամի նշանակման մեջ չէ, որ մենք պարտավոր ենք կիրառել p ինդեքսը: Երբ դա թյուրիմացության տեղիք չի տա, մոդուլյար բազմանդամները նույնպես կնշանակենք $f(x)$ տեսքով (օրինակ՝ երբ տվյալ խնդրում չի մասնակցում այնպիսի մի $f(x) \in \mathbb{Z}[x]$ բազմանդամ, որի պատկերը անհրաժեշտ է նշանակել $f_p(x)$ տեսքով):

Այժմ պարզ է, որ 1.2–1.3 պարագրաֆների շարադրանքը (ներառյալ Կնուտի մոդուլյար մեթոդը) կարող էր ձեւակերպվել նաեւ օղակների հոմոմորֆիզմների լեզվով, եւ այդ տեսքով այն անգամ ավելի համառոտ տեսք կունենար: Այնուամենայնիվ, այս գլխի ամենասկզբում նշված պատճառներով, 1.2–1.3 պարագրաֆները ձեւակերպված են ավելի պարզ լեզվով:

Օղակների հոմոմորֆիզմները սերտորեն կապված են *ֆակտոր-օղակի* կարեւոր հասկացության հետ: Ենթադրենք տրված են R օղակը եւ նրա I իդեալը: Ըստ I իդեալի օղակի a տարրին համապատասխան *հարակից դաս* է կոչվում R-ի հետեւյալ ենթաբազմությունը $a + I = \{a + c \mid c \in I\}$: Հարակից դասերի միջոցով կարելի է տալ R օղակի *տրոհում*, այսինքն օղակի ներկայացում այնպիսի ոչ դատարկ ենթաբազմությունների միավորման տեսքով, որոնցից կամայական երկուսը հատում ունեն միայն երբ համընկնում են:

2.3.8 Օրինակ. Եթե վերցնենք $R = \mathbb{Z},\ I = 5\mathbb{Z},\ a = 3$, ապա

$$a + I = 3 + 5\mathbb{Z} = \{3 + 5n \mid n \in \mathbb{Z}\} = \{3, 3 \pm 5, 3 \pm 10, 3 \pm 15, \dots\}:$$

Այսինքն՝ $3 + 5\mathbb{Z}$ հարակից դասը այն ամբողջ թվերի բազմությունն է, որոնք 5-ի վրա բաժանելիս ստացվող մնացորդը 3 է:

Եթե R օղակը ներկայացված է ըստ իր I իդեալի հարակից դասերի միավորման տեսքով՝

$$R = \bigcup_{a \in R} (a + I), \tag{2.2}$$

ապա յուրաքանչյուր հարակից դասից կամայական մեկ տարր ֆիքսելով անվանենք այն *հարակից դասի ներկայացուցիչ*: Բնականաբար $a + I$ դասի համար դա

կարող է լինել հենց a տարրը, կամ ցանկացած այլ a' տարր, որը բավարարում է $a'-a\in I$ պայմանին:

(2.2) ներկայացման մեջ որոշ $a+I$ հարակից դասեր կարող են կրկնվել, այսինքն՝ մասնակցել մեկից ավելի անգամներ: Այդ դեպքում, կրկին, նրանց ներկայացուցիչների տարբերությունը կպատկանի I-ին: Բոլոր չկրկնվող հարակից դասերի ներկայացուցիչների բազմությունը կոչվում է R օղակի *ներկայացուցիչների համակարգ* կամ *տրանսվերսալ* ըստ I իդեալի: Երբ a-ն վազանցում է R օղակի բոլոր տարրերը, ստացված $a+I$ հարակից դասերը վազանցում են բոլոր հարակից դասերի բազմությունը (հնարավոր կրկնություններով):

2.3.9 Վարժություն. Ստուգել, որ $a+I=a'+I$ պայմանը իրոք համարժեք է $a'-a\in I$ պայմանին:

Ըստ I իդեալի R օղակի հարակից դասերի միջեւ հնարավոր է ներմուծել գումարման եւ բազմապատկման գործողություններ. կամայական $a,b\in R$ տարրերի համար սահմանենք՝

$$(a+I)+(b+I)=(a+b)+L,\qquad (a+I)\cdot(b+I)=ab+L: \tag{2.3}$$

Չնայած օղակի կամայական $a,b\in R$ տարրերի համար էլ գոյություն ունեն $(a+b)+L$ եւ $ab+L$ հարակից դասեր, այնուամենայնիվ, նախքան (2.3) արտահայտություններն օգտագործելն անհրաժեշտ է ապացուցել դրանց կոռեկտությունը: Ի նկատի ունենք այն, որ նշված հարակից դասերը որոշ $a',b'\in R$ տարրերի համար կարող են ունենալ նաեւ այլ տեսք $a+I=a'+I$ եւ $b+I=b'+I$ (օրինակ՝ $2+5\mathbb{Z}=7+5\mathbb{Z}=1002+5\mathbb{Z}$): Ուստի պետք է ցույց տալ, որ (2.3) գործողությունների սահմանումները կախված չեն այն բանից, թե տվյալ հարակից դասերի ո՛ր ներկայացուցիչներն ենք ընտրել:

2.3.10 Խնդիր. Ստուգել, որ վերը բերված պայմաններում՝

$$(a+b)+L=\left(a'+b'\right)+L,\qquad ab+L=a'b'+L,$$

այսինքն՝ (2.3) գործողությունների սահմանումները կոռեկտ են (կախված չեն հարակից դասերի ներկայացուցիչների ընտրությունից):

Տրված R օղակի եւ նրա I իդեալի համար հարակից դասերի $\{a+I\mid a\in R\}$ բազմության վրա (2.3) կանոններով մեր կառուցած հանրահաշվական համակարգը օղակ է: Այն կոչվում է R օղակի *ֆակտոր-օղակ* ըստ I իդեալի, եւ նշանակվում է R/I.

$$\langle\{a+I\mid a\in R\},+,\cdot\rangle:$$

2.3.11 Վարժություն. Ապացուցել, որ $\mathbb{Z}$ օղակի $m\mathbb{Z}$ իդեալի համար (m-ը որեւէ բնական թիվ է) տեղի ունի $\mathbb{Z}/m\mathbb{Z} = \langle\{m\mathbb{Z}, 1+m\mathbb{Z}, \dots, (m-1)+m\mathbb{Z}\}, +, \cdot\rangle$, ընդ որում, $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_m$:

2.3.12 Օրինակ. Որեւէ p պարզ թվի համար $\mathbb{Z}[x]$ բազմանդամային օղակում վերցնենք բոլոր այնպիսի բազմանդամների P ենթաբազմությունը, որոնց բոլոր գործակիցները բաժանվում են p-ի վրա: Հեշտ է տեսնել, որ, եթե $f(x), g(x) \in P$, ապա նաեւ $f(x) - g(x) \in P$ (p-ի վրա բաժանվող թվերի տարբերությունը բաժանվում է p-ի վրա): Հեշտ է նաեւ տեսնել, որ եթե $h(x)$-ը կամայական բազմանդամ է $\mathbb{Z}[x]$ օղակից, ապա $f(x)h(x) \in P$ (քանի որ $f(x)$-ի բոլոր գործակիցները բաժանվում են p-ի վրա, ապա, անկախ $h(x)$-ի գործակիցների բաժանելությունից, $f(x)h(x)$ արտադրյալի յուրաքանչյուր գործակից բաժանվում է p-ի վրա): Ըստ 2.1.7 խնդրի սա նշանակում է, որ P ենթաբազմությունը $\mathbb{Z}[x]$ օղակի ենթաօղակ եւ իդեալ է: Ըստ P իդեալի $\mathbb{Z}[x]$-ը տրոհվում է հարակից դասերի միավորման, ընդ որում, $f(x), g(x)$ երկու բազմանդամներ միեւնույն ենթաբազմությունից են, եթե $f(x) - g(x) \in P$ (տես 2.3.9 վարժությունը), այսինքն՝ եթե $f(x) - g(x)$ տարբերության բոլոր գործակիցները բաժանվում են p-ի վրա: Այս $\mathbb{Z}[x]/P$ ֆակտոր-օղակում գումարման եւ բազմապատկման գործողություններն են $(f(x)+P)+(g(x)+P) = t(x)+P$, որտեղ $t(x)$ բազմանդամը ստացվում է $f(x)+g(x)$ գումարի վրա 2.3.7 օրինակի բազմանդամային մոդուլյար անցումը կիրառելու միջոցով, եւ $(f(x)+P)\cdot(g(x)+P) = l(x)+P$, որտեղ $l(x)$ բազմանդամը ստացվում է նույն մոդուլյար անցումը $f(x)g(x)$ արտադրյալի վրա կիրառելու միջոցով:

Վերջին օրինակների եւ վարժությունների մեջ շատ ընդհանրություններ կային: Դրանցից մեկը հետեւյալ կարեւոր փաստն է, որը ցույց է տալիս օղակների հոմոմորֆիզմների եւ իդեալների միջեւ կապը:

2.3.13 Թեորեմ (օղակների հոմոմորֆիզմների հիմնական թեորեմը). *Ենթադրենք տրված է R եւ K օղակների $\varphi: R \to K$ հոմոմորֆիզմը: Այդ դեպքում նրա* $\ker\varphi$ *միջուկն իդեալ է R օղակում, իսկ* $\operatorname{im}\varphi$ *պատկերը ենթաօղակ է K օղակում: Ընդ որում.*

$$R/\ker\varphi \cong \operatorname{im}\varphi:$$

Թեորեմում նշված իզոմորֆիզմը տրվում է $\theta(a+\ker\varphi) = \varphi(a) \in K$ կանոնով: Ճիշտ է եւ հակառակը՝ R օղակի կամայական I իդեալի համար $\nu(a) = a + I \in R/I$ կանոնով տրվող արտապատկերումը հոմոմորֆիզմ է: Ընդ որում, $\ker\nu = I$ եւ $\operatorname{im}\nu = R/I$: Այս $\nu: R \to R/I$ հոմոմորֆիզմն անվանում են I իդեալին համապատասխանող *բնական* հոմոմորֆիզմ (կամ *կանոնական* հոմոմորֆիզմ): Թեորեմի ապացույցը մենք բաց ենք թողնում, քանի որ այն առկա է հանրահաշվի ներածական դասընթացներում:

Հետագայում մեզ պետք են գալու օղակի *մաքսիմալ իդեալի* եւ օղակում ըստ մաքսիմալ իդեալի ֆակտոր-օղակի հասկացությունները:

2.3.14 Սահմանում. R օղակի M իդեալը կոչվում է R-ի մաքսիմալ իդեալ, եթե այն սեփական իդեալ է, եւ R-ում գոյություն չունի M իդեալը խիստ պարունակող որեւէ սեփական I իդեալ. $M \neq R$ եւ եթե $M \subset I$, ապա $I = R$:

Այլ խոսքերով՝ M իդեալը սեփական է, եւ R օղակում չկան M-ի եւ R-ի «միջեւ ընկած» իդեալներ: Հեշտ է ստուգել, որ.

2.3.15 Թեորեմ. *R կոմուտատիվ միավորով օղակի M իդեալը մաքսիմալ է այն եւ միայն այն դեպքում, երբ R/M ֆակտոր-օղակը դաշտ է:*

2.3.16 Օրինակներ. $\mathbb{Z}$ օղակում մաքսիմալ է $p\mathbb{Z}$ տեսքի ցանկացած իդեալ, որտեղ p-ն որեւէ պարզ թիվ է: Միաժամանակ, ըստ 2.1.26 թեորեմի, $\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}_p$ օղակը դաշտ է այն եւ միայն այն դեպքում, երբ p-ն պարզ է: Մյուս կողմից, բաղադրյալ $m = nk$ թվի համար $m\mathbb{Z}$ օղակը մաքսիմալ չէ, քանի որ $m\mathbb{Z} \subset n\mathbb{Z} \subset \mathbb{Z}$:

Կամայական դաշտի կամ, ավելի ընդհանուր, կոմուտատիվ օղակի վրա տրված A մատրիցի որոշիչը մեզ բազմիցս պետք է գալու հետագա գլուխներում: 2.1.27 կետում մենք արդեն սահմանել ենք R կոմուտատիվ օղակի վրա տրված n-րդ կարգի քառակուսային մատրիցների $M_n(R)$ օղակը: Ենթադրենք տրված է

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \in M_n(R) \tag{2.4}$$

տեսքի որեւէ A մատրից: Նրա $\det A$ որոշիչը $n!$ հատ գումարելիների գումար է.

$$\det A = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)}, \tag{2.5}$$

որտեղ σ տեղադրությունը վազանցում է n-րդ կարգի բոլոր $n!$ հատ տեղադրությունների S_n խումբը, իսկ $a_{1\sigma(1)} \cdots a_{n\sigma(n)}$ արտադրյալը A մատրիցի յուրաքանչյուր տողից ու յուրաքանչյուր սյունից մեկական վերցրած n հատ տարրերի արտադրյալ է: $\operatorname{sgn}(\sigma)$ արժեքը հավասար է 1-ի, եթե σ տեղադրությունը զույգ է, եւ -1-ի եթե σ տեղադրությունը կենտ է: Որոշիչի տարրական հատկությունների ապացույցը մենք բաց ենք թողնում, քանի որ դրանք մանրամասնորեն ուսումնասիրվում են հանրահաշվի ներածական դասընթացներում, եւ այդ հիմնական հատկություններն

առանց դժվարության տարածվում են կամայական դաշտի կամ կոմուտատիվ օղակի վրա տրված մատրիցների համար: Որպես ինքնուրույն աշխատանք կարելի է ապացուցել հետեւյալ հատկությունները.

2.3.17 Վարժություններ. (2.5) բանաձեւից ստանալ $A \in M_n(R)$ մատրիցի $\det A$ որոշիչի հետեւյալ հատկությունները.

ա. A մատրիցի երկու տողերը (կամ սյուները) դիրքափոխելիս $\det A$ որոշիչը փոխում է նշանը:

բ. Երկու հավասար տող (կամ սյուն) ունեցող ցանկացած A մատրիցի որոշիչը հավասար է զրոյի:

գ. A մատրիցի որեւէ տող (կամ սյուն) $a \in R$ տարրով բազմապատկելիս $\det A$ որոշիչը նույնպես բազմապատկվում է այդ տարրով:

դ. Գծորեն կախված տողեր (կամ սյուներ) (տես 7.2 պարագրաֆը) ունեցող ցանկացած A մատրիցի որոշիչը հավասար է զրոյի:

ե. Եթե A մատրիցի որեւէ տողի (կամ սյան) գումարենք նրա մի այլ տող (կամ սյուն)՝ նախապես վերջինս $a \in R$ տարրով բազմապատկելով, ապա $\det A$ որոշիչը դրանից չի փոխվի:

զ. Եթե A մատրիցը եռանկյունի է, այսինքն՝ նրա գլխավոր անկյունագծից ներքեւ ընկած բոլոր տարրերը զրոյական են, ապա $\det A = a_{11} \cdots a_{nn}$:

Ենթադրենք տրված են R եւ L կոմուտատիվ օղակները եւ $\varphi: R \to L$ հոմոմորֆիզմը: R եւ L օղակների վրա տրված $M_n(R)$ եւ $M_n(L)$ մատրիցային օղակների համար կարելի է սահմանել $\varphi: M_n(R) \to M_n(L)$ հոմոմորֆիզմը հետեւյալ կերպ. եթե

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \in M_n(R), \tag{2.6}$$

$(a_{ij} \in R, i, j = 1, \dots, n)$, ապա A մատրիցի համար նրա $\varphi(A)$ պատկերը տրվում է

$$\varphi(A) = \begin{pmatrix} \varphi(a_{11}) & \cdots & \varphi(a_{1n}) \\ \cdots & \cdots & \cdots \\ \varphi(a_{n1}) & \cdots & \varphi(a_{nn}) \end{pmatrix} \in M_n(L)$$

բանաձեւով: Մասնավորապես, եթե սկզբնական հոմոմորֆիզմը $\varphi_p: \mathbb{Z} \to \mathbb{Z}_p$ մոդուլյար անցումն է, ապա պայմանավորվենք նշանակել $\varphi_p(A) = A_p$, ընդ որում, $\varphi_p: M_n(\mathbb{Z}) \to M_n(\mathbb{Z}_p)$ հոմոմորֆիզմը նույնպես անվանենք մոդուլյար անցում:

2.3.18 Վարժություն. Հաշվել $\varphi_p\colon M_n(\mathbb{Z}) \to M_n(\mathbb{Z}_p)$ մոդուլյար անցման պատկերը եւ միջուկը:

Ինչպես բազմանդամների դեպքում, այնպես էլ այժմ մատրիցների համար $\varphi_p\colon M_n(\mathbb{Z}) \to M_n(\mathbb{Z}_p)$ մոդուլյար անցումը միշտ չէ, որ «բավարար» ինֆորմացիա է պահպանում մատրիցի մասին:

2.3.19 Օրինակ. Վերցնենք

$$A = \begin{pmatrix} 1 & 10 & 3 \\ 0 & 0 & 14 \\ 2 & 0 & 7 \end{pmatrix} \in M_3(\mathbb{Z}):$$

Պարզ է, որ $\det A = 280 \neq 0$: Սակայն

$$A_7 = \varphi_7(A) = \begin{pmatrix} 1 & 3 & 3 \\ 0 & 0 & 0 \\ 2 & 0 & 0 \end{pmatrix} \in M_3(\mathbb{Z}_7)$$

մատրիցն ունի հավասար սյուներ, ուստի $\det A_7 = 0$, եւ այս զրոյական արժեքը այլեւս քիչ ինֆորմացիա է տալիս սկզբնական մատրիցի որոշիչի մասին, քանի որ մոդուլյար անցումը չի պահպանել մատրիցի տարրերի գծային անկախությունը: Արժե համեմատել այս օրինակը 2.4.1 կետի հետ:

2.3.20 Օրինակ. Եթե նախորդ օրինակի մատրիցի համար վերցնենք $p = 19$, ապա φ_{19} անցումն արդեն չի փոխում A մատրիցի արտաքին տեսքը.

$$A_{19} = \varphi_{19}(A) = \begin{pmatrix} 1 & 10 & 3 \\ 0 & 0 & 14 \\ 2 & 0 & 7 \end{pmatrix} \in M_3(\mathbb{Z}_{19}),$$

բայց չնայած դրան՝ մատրիցի որոշիչը դարձյալ չի պահպանվում $\det A_{19} = 14 \neq 280$:

Հաջորդ հարցը, որ կարող է առաջանալ, նախապատկերի միարժեք վերականգնման խնդիրն է, որը բազմանդամների դեպքի համար կքննարկենք 2.4.2 կետում: $\varphi_p\colon \mathbb{Z} \to \mathbb{Z}_p$ եւ $\varphi_p\colon M_n(\mathbb{Z}) \to M_n(\mathbb{Z}_p)$ մոդուլյար անցումներից ոչ մեկը բիյեկտիվ չէ, ուստի ինչ-որ խնդիր $M_n(\mathbb{Z}_p)$-ում լուծելուց հետո (օրինակ՝ մատրիցի որոշիչը հաշվելուց հետո) միշտ չէ, որ պարզ է, թե լուծումն ինչպես պիտի վերականգնել $M_n(\mathbb{Z})$-ի համար: Նախորդ օրինակում մենք, բավականաչափ մեծ p վերցնելով, կարողացանք հասնել այն բանին, որ A եւ A_{19} մատրիցների տեսքերը իրարից չտարբերվեն: Սակայն, եթե մատրիցը *բացասական* տարրեր ունի, ապա միայն մեծ p վերցնելը դեռ թույլ չի տալիս լուծել նախապատկերի միակության հարցը:

2.3.21 Օրինակ. Եթե φ_{19} մոդուլյար անցումից հետո ունենք

$$A_{19} = \varphi_{19}(A) = \begin{pmatrix} 1 & 10 & 3 \\ 0 & 0 & 14 \\ 2 & 0 & 7 \end{pmatrix},$$

ապա սրա համար նախապատկեր կհանդիսանա հետեւյալ մատրիցներից կամայականը.

$$\begin{pmatrix} 1 & 10 & 3 \\ 0 & 0 & 14 \\ 2 & 0 & 7 \end{pmatrix}, \quad \begin{pmatrix} -18 & 10 & 3 \\ 0 & 0 & -5 \\ 2 & 0 & 7 \end{pmatrix}, \quad \begin{pmatrix} -18 & -9 & -16 \\ 0 & 0 & -5 \\ -17 & 0 & -12 \end{pmatrix}:$$

Հետագայում մենք մի քանի անգամ կանդրադառնանք մատրիցներում մոդուլյար անցման եւ վերջավոր դաշտերի վրա որոշիչների հաշվման հետ կապված խնդիրների (մասնավորապես, տես 5.2 պարագրաֆը):

2.4 Մոդուլյար անցման ալգորիթմական կիրառությունները

$\varphi_m: \mathbb{Z} \to \mathbb{Z}_m$, $\varphi_p: \mathbb{Z} \to \mathbb{Z}_p$, $\varphi_p: \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ եւ $\varphi_p: M_n(\mathbb{Z}) \to M_n(\mathbb{Z}_p)$ մոդուլյար անցումները (օղակային հոմոմորֆիզմները) ալգորիթմներ կառուցելու հիմնական մեր գործիքներից են: Այդ ալգորիթմներից մեկին (Կնուտի օրինակին) ծանոթացանք 1.3 պարագրաֆում: Օղակների հոմոմորֆիզմների լեզվի կիրառությամբ այդ ալգորիթմը կարող է վերաձեւակերպվել այսպես. 1.1 պարագրաֆում բերված (1.1) բազմանդամների ամենամեծ ընդհանուր բաժանարարը Էվկլիդեսի ալգորիթմով հաշվելիս առաջանում է միջանկյալ արժեքների ուռճացման պրոբլեմը. հաշվարկների ընթացքում ստացվում են շատ մեծ (մինչեւ 35 նիշանի) թվեր, որոնք ոչ միայն դանդաղեցնում են հաշվարկը, այլեւ շատ քիչ էական ինֆորմացիա են պարունակում վերջնական պատասխանի համար: Դա հաղթահարելու համար դիտարկվում է

$$\varphi_5: \mathbb{Z}[x] \to \mathbb{Z}_5[x]$$

մոդուլյար անցումը, եւ այդ հոմոմորֆիզմի նկատմամբ (1.1) բազմանդամները ունեն $f_5(x)$ եւ $g_5(x)$ պատկերները (տես (1.6) բազմանդամները 1.3 պարագրաֆում): Այդ պատկերները փոխադարձաբար պարզ են, ընդ որում, այդ փաստը պարզելը անհամեմատ ավելի հեշտ է, քան $f(x)$ եւ $g(x)$ բազմանդամների փոխադարձաբար պարզությունը հաշվելը, քանի որ այս դեպքում հաշվարկները կատարվում են ոչ թե $\mathbb{Z}$-ում, որտեղ կարող են անսպասելիորեն մեծ՝ «ուռճացած» թվեր հանդիպել, այլ $\mathbb{Z}_5 = \{0, \dots, 4\}$ օղակում, որտեղ ընդամենը հինգ հատ թիվ կա: Վերջին քայլում $\big(f_5(x), g_5(x)\big) = 1$ պայմանից հակասող ենթադրությամբ բխեցվում է $\big(f(x), g(x)\big) = 1$ պայմանը՝ շնորհիվ $f(x)$ եւ $g(x)$ բազմանդամների ավագ գործակիցների եւ $m = 5$

մոդուլի փոխադարձ պարզության: Իրոք, եթե $\big(f(x), g(x)\big) = d(x) \not\equiv 1$, ապա $d(x)$-ի պատկերը հանդիսացող $d_5(x) = \varphi_5\big(d(x)\big)$ մոդուլյար բազմանդամը $f_5(x)$ եւ $g_5(x)$ փոխադարձաբար պարզ մոդուլյար բազմանդամների (միգուցե ոչ ամենամեծ) ընդհանուր բաժանարար է, ուստի $d_5(x) \approx 1$: Մյուս կողմից, քանի որ $d(x)$-ը բաժանում է $f(x)$ եւ $g(x)$ բազմանդամներից յուրաքանչյուրին, ապա նրա c_0 ավագ գործակիցն էլ բաժանում է $f(x)$ բազմանդամի ավագ գործակիցը (որը հավասար է 1-ի), ինչպես եւ $g(x)$ բազմանդամի ավագ գործակիցը (որը հավասար է 3-ի): Սա հնարավոր է, միայն երբ $c_0 = \pm 1$, համարենք $c_0 = 1$: Քանի որ φ_5 հոմոմորֆիզմը անփոփոխ է թողնում 1 թիվը, $d_5(x)$ եւ $d(x)$ բազմադամների ավագ անդամները նույնն են: Իսկ սա հնարավոր է միայն, երբ $d_5(x) = d(x) \approx 1$:

Այս օրինակի էֆեկտիվությունը ապահովվում է $\mathbb{Z}$ օղակը $\mathbb{Z}_5$ օղակով փոխարինելու մեթոդով: Հետագայում մենք գործ կունենանք էլ ավելի հետաքրքիր ալգորիթմների հետ, որոնցում մասնակցում է ոչ միայն $\mathbb{Z}_p$-ն, այլեւ $\mathbb{Z}_p$ վերջավոր դաշտի վրա տրված տրված $V = \mathbb{Z}_p^n$ գծային տարածությունները, $\mathbb{Z}_p$-ի հանրահաշվական ընդլայնումները եւլն: Ի տարբերություն ավանդական իրական կամ ռացիոնալ տարածությունների (որոնք պարունակում են հաշվելի կամ կոնտինուալ քանակությամբ վեկտորներ/կետեր), վերջավոր դաշտի վրա տրված վերջավոր չափանի գծային տարածությունները իրենք նույնպես վերջավոր են (օրինակ՝ $\mathbb{Z}_5^3$ եռաչափ տարածությունը ունի ընդամենը $5^3 = 125$ հատ վեկտոր/կետ), եւ նրանցում ալգորիթմական կամ հաշվողական շատ խնդիրներ շատ ավելի արագ են լուծվում:

$\varphi_p\colon \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ մոդուլյար անցման ալգորիթմական արժանիքներից մյուսին կծանոթանանք 2.5 պարագրաֆում: $\mathbb{Z}_p[x]$-ն Էվկլիդյան օղակ է, եւ նրանում գործում են էվկլիդյան օղակների ալգորիթմները, ներառյալ 2.5.3, 2.5.5 եւ 2.5.7 ալգորիթմները: Մինչդեռ $\mathbb{Z}[x]$ օղակը էվկլիդյան չէ (տես 2.5.9 օրինակը), եւ նրանում այդ ալգորիթմները ոչ միշտ են գործում: Ուստի մենք հավելյալ ալգորիթմական հնարավորություններ կստանանք, եթե որեւէ խնդիր լուծելիս՝ հարցը φ_p մոդուլյար անցումով տեղափոխենք $\mathbb{Z}_p[x]$ օղակ, ապա լուծենք այն որեւէ մոդուլյար էվկլիդյան ալգորիթմով: Տես նաեւ կարեւոր 2.5.17 դիտողությունը 2.5 պարագրաֆի վերջում:

Մոդուլյար անցումների օգնությամբ կառուցվող մեր ալգորիթմները հիմնականում ունենալու են հետեւյալ տեսքը: Նախ, խնդիրը ձեւակերպվելու է ամբողջ թվերի օգնությամբ, եւ ընտրվելու է այն մոդուլը, ըստ որի կատարվելու է մոդուլյար անցումը (գրեթե միշտ դա մի p պարզ թիվ է հանդիսանալու): Այնուհետեւ կատարվելու է φ_p մոդուլյար անցումը եւ խնդիրը վերաձեւակերպվելու է $\mathbb{Z}_p$ դաշտի, $\mathbb{Z}_p[x]$ օղակի կամ $\mathbb{Z}_p$-ի վրա տրված գծային տարածության մեջ (հարմարության համար սա կանվանենք մոդուլյար խնդիր): Այն լուծվելու է վերջավոր թվերի վրա (ալգո-

րիթմի արդյունավետությունը ձեռք է բերվելու սրա միջոցով եւ էվկլիդյան օղակների մասին քիչ առաջ բերված դիտողությամբ): Վերջում մոդուլյար խնդրի արդեն գտնված լուծման միջոցով գտնվելու է նաեւ ընդհանուր խնդրի լուծումը:

Քննարկենք մի քանի տիպական բարդություններ, որոնք առաջանում են խնդիրների մոդուլյար լուծման ժամանակ: Հետագայում դրանք բոլորն էլ պատասխաններ կստանան եւ կհաղթահարվեն:

Ենթադրենք՝ մեր խնդիրը կապված է $f(x) \in \mathbb{Z}[x]$ բազմանդամի $h(x) \in \mathbb{Z}[x]$ բաժանարարի հաշվման հետ. սա կարող է հանդիպել, ասենք, երկու բազմանդամների ամենամեծ ընդհանուր բաժանարարը հաշվելու ալգորիթմում, տրված բազմանդամի բոլոր բաժանարարները թվարկելու ալգորիթմում, տրված բազմանդամի ֆակտորիզացիայի (պարզ արտադրիչների վերլուծության) ալգորիթմում եւլն: $\varphi_p\colon \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ մոդուլյար անցումը կարտապատկերի այդ բազմանդամները $f_p(x)$ եւ $h_p(x)$ պատկերներին:

2.4.1 Գործակիցների պահպանման հարցը. Մոդուլյար անցման ժամանակ $f(x)$ բազմանդամի կամ նրա բաժանարարների գործակիցները կարող են փոխվել, կրճատվել, եւ $f_p(x)$ բազմանդամի բաժանարարները կարող են շատ քիչ կապված լինել $f(x)$ բազմանդամի բաժանարարների հետ, քանի որ մոդուլյար անցման ժամանակ $f(x)$-ի գործակիցների մասին շատ ինֆորմացիա է կորսվում: Օրինակ՝ $f(x) = 7x^2 + 22$ բազմանդամի համար $f_7(x) = 1$, իսկ վերջինս $f(x)$-ի բաժանարարների մասին այլեւս որեւէ էական ինֆորմացիա չի պարունակում φ_7 մոդուլյար անցումից հետո: Կնուտի օրինակում նույնպես գործակիցների կրճատում կամ կորուստ էր տեղի ունենում, սակայն մենք $m = 5$ մոդուլն ընտրել էինք այնպես, որ վերջնական պատասխանի վրա գործակիցների կորուստը չազդի:

2.4.2 Նախապատկերի միակության հարցը. Ենթադրենք՝ տրված $f(x)$ բազմանդամի համար ըստ p մոդուլի հաշվել ենք $f_p(x)$ մոդուլյար բազմանդամը եւ նրա համար մոդուլյար մեթոդներով գտել $h_p(x)$ բաժանարարը: Անգամ եթե այս մոդուլյար անցման ժամանակ ինչ-որ կերպ լուծվել է գործակիցների պահպանման հարցը, ապա դարձյալ պարզ չէ, թե $f(x)$-ի որ բաժանարարն է համապատասխանում $h_p(x)$-ին, քանի որ մոդուլյար անցումը բիյեկտիվ արտապատկերում չէ: Օրինակ՝ եթե $\mathbb{Z}_7[x]$ օղակում ունենք $f_7(x) = (x + 1)(x + 5)$, ապա $x + 1$ պարզ արտադրիչի նախապատկեր կարող է լինել ինչպես $x + 1$, այնպես էլ $x + 8$ բազմանդամը: Մեզ անհրաժեշտ է մի մեխանիզմ, որով միարժեքորեն կվերականգնվի նրա հավանական նախապատկեր բազմանդամը, որը բաժանարար է $f(x)$ բազմանդամի համար:

Հավելյալ բարդություն է առաջանում նաեւ *բացասական* գործակիցների համար. չէ՞ որ $x+1$ արտադրիչի նախապատկեր կարող է լինել նաեւ $x-6$ բազմանդամը:

2.4.3 Բաժանելիության հարցը. Այս հարցը պակաս ակնհայտ է, քան նախորդ երկու հարցերը: Եթե անգամ մոդուլյար անցման ժամանակ գործակիցների պահպանությունը բարդություն չի առաջացնում, եւ եթե նախապատկերների միակության հարցը նույնպես չի ծագում, ապա դարձյալ $f_p(x)$-ի $h_p(x)$ բաժանարարը կարող է շատ քիչ ինֆորմացիա պարունակել $f(x)$-ի բաժանարարների մասին:

Նախքան սա օրինակի վրա ցույց տալը, կատարենք տերմինների մի հստակեցում: Բազմանդամի սահմանումից ակնհայտ է, որ բազմանդամային միեւնույն $R[x]$ օղակի երկու բազմանդամներ իրար հավասար են այն եւ միայն այն դեպքում, երբ հավասար են նրանց համապատասխան աստիճանների գործակիցները: Մինչդեռ, օրինակ՝ $x^2+1 \in \mathbb{Z}[x]$ եւ $x^2+1 \in \mathbb{Z}_2[x]$ բազմանդամներն իրար հավասար չեն, քանի որ դրանք այնպիսի օղակներից են, որոնց կրիչները չեն հատվում: Այսպիսի բազմանդամները բնութագրելու համար կասենք, որ նրանք նույն գրությամբ բազմանդամներ են:

Եթե $f(x)$ եւ $h(x)$ բազմանդամների բոլոր գործակիցները դրական են, իսկ p մոդուլն ընտրված է դրանցից բոլորից ավելի մեծ, այդ դեպքում $f(x)$ եւ $f_p(x)$ բազմանդամները կունենան միեւնույն գրությունը, իսկ $h_p(x)$-ի $\varphi_p^{-1}(h_p(x))$ նախապատկերը պարտավոր է ունենալ նույն գրությունը, ինչ $h_p(x)$-ը: Սակայն այն կարող է $f(x)$-ի բաժանարար չլինել, ավելին՝ $f(x)$-ի բաժանարար կառուցելու համար որեւէ էական տեղեկություն չկրել:

Իսկապես, վերցնենք $f(x)=x^2+1$ բազմանդամը եւ կատարենք $\varphi_2\colon \mathbb{Z}[x] \to \mathbb{Z}_2[x]$ մոդուլյար անցումը՝ $f_2(x)=x^2+1$: Այս բազմանդամը ունի նույն գրությունը, ինչ $f(x)$-ը, եւ այն $\mathbb{Z}_2[x]$-ում պարզ չէ, քանի որ ներկայացվում է

$$f_2(x)=x^2+1=x^2+1^2=(x+1)(x+1)$$

տեսքով (տես 2.1.32 լեմման եւ 2.1.33 հետեւանքը): Ունենք

$$f_2(x) \vdots x+1=h_2(x):$$

Մինչդեռ $f(x) \in \mathbb{Z}[x]$ բազմանդամը պարզ է, քանի որ եթե այն ունենար առաջին աստիճանի (գծային) բաժանարար, ապա $x^2+1=0$ հավասարումը կունենար որեւէ արմատ: Այսինքն՝ $h_2(x)$ բազմանդամի օգնությամբ $f(x)$-ի որեւէ սեփական բաժանարար հնարավոր չէ ստանալ:

2.4.1, 2.4.2 եւ 2.4.3 հարցերը առաջանալու են առաջիկայում մեր կողմից քննարկվելիք բոլոր ալգորիթմներում, եւ դրանցից յուրաքանչյուրում ստանալու են յուրովի լուծում:

2.5 Էվկլիդյան օղակներ

Էվկլիդյան օղակի սահմանումն ընդհանրացնում է մնացորդով բաժանելու գաղափարը, որը ծանոթ է ամբողջ թվերի մնացորդով բաժանման կամ բազմանդամների մնացորդով բաժանման հասկացությունից:

Տրված m, n ամբողջ թվերի համար ($n \neq 0$) գոյություն ունեն q, r ամբողջ թվեր այնպիսիք, որ $m = qn + r$, ընդ որում, $r = 0$ կամ $r \neq 0$ եւ $|r| < |n|$: Նույն կերպ՝ տրված $f(x)$, $g(x)$ ռացիոնալ (իրական, կոմպլեքս) գործակիցներով բազմանդամների համար ($g(x) \neq 0$) գոյություն ունեն $q(x)$, $r(x)$ ռացիոնալ (իրական, կոմպլեքս) գործակիցներով բազմանդամներ այնպիսիք, որ $f(x) = q(x)g(x) + r(x)$, ընդ որում, $r(x) = 0$ կամ $r(x) \neq 0$ եւ $\deg\big(r(x)\big) < \deg(g(x))$:

Այս օրինակներում ամբողջ թվի բացարձակ արժեքի եւ բազմանդամի աստիճանի խաղացած դերերը շատ նման են: Ընդհանրացնենք դրանք՝ օղակի ոչ զրոյական a տարրին $\delta(a)$ մի ամբողջ թիվ համապատասխանեցնելով հետեւյալ կերպ.

2.5.1 Սահմանում. R ամբողջության տիրույթը կոչվում է *էվկլիդյան օղակ*, եթե տրված է այնպիսի մի $\delta: R\backslash\{0\} \to \mathbb{N} \cup \{0\}$ արտապատկերում, որ.

E.1 R օղակի ցանկացած $a, b \neq 0$ տարրերի համար $\delta(ab) \geq \delta(a)$:

E.2 Կամայական a, b տարրերի համար, եթե $b \neq 0$, ապա գոյություն ունեն $q, r \in R$ տարրեր այնպիսիք, որ $a = qb + r$, ընդ որում, կամ $r = 0$, կամ էլ $r \neq 0$ եւ $\delta(r) < \delta(b)$:

Երբեմն $\delta(a)$ ֆունկցիան անվանում են Էվկլիդեսի ֆունկցիա, աստիճանի ֆունկցիա կամ նորմի ֆունկցիա, իսկ $\delta(a) \in \mathbb{N} \cup \{0\}$ արժեքը երբեմն անվանում են $a \in R$ տարրի նորմ կամ էվկլիդյան նորմ:

2.5.2 Օրինակ. Սահմանումից առաջ բերված օրինակներում, վերցնելով $\delta(n) = |n|$ կամ $\delta(f(x)) = \deg f(x)$ (այստեղ $f(x) \in \mathbb{Q}[x]$), կստանանք էվկլիդյան օղակի առաջին օրինակները. ամբողջ թվերի $\mathbb{Z}$ օղակը եւ ռացիոնալ բազմանդամների $\mathbb{Q}[x]$ օղակը: Այն, որ $\mathbb{Q}[x]$ օղակը էվկլիդյան է, հետեւում է բազմանդամների մնացորդով բաժանման կանոններից եւ այն բանից, որ այդ ընթացքում ռացիոնալ թվերի հետ

գործողությունների ընթացքում ստացվում են միայն ռացիոնալ թվեր: Ստորեւ մենք կստանանք էվկլիդյան օղակների այլ օրինակներ եւս:

Պայմանավորվենք **E.2** կետում նշված $a = qb + r$ հավասարությունն անվանել *մնացորդով բաժանում*, q-ն՝ *քանորդ*, իսկ r-ը՝ *մնացորդ*:

Էվկլիդյան օղակների նշանակությունը պայմանավորված է այն բանով, որ նրանցում գործում են մեզ թվաբանությունից ծանոթ մի շարք սկզբունքներ եւ, առաջին հերթին, *Էվկլիդեսի ալգորիթմը*, որը թույլ է տալիս լուծել տարրերի ամենամեծ ընդհանուր բաժանարարի եւ ամենափոքր ընդհանուր բազմապատիկի գոյության խնդիրը: Ընդ որում, հաշվի առնելով 2.1.5 դիտողությունը, մենք կարող ենք հարցը քննարկել միայն *ոչ զրոյական* տարրերի համար:

2.5.3 Թեորեմ (Էվկլիդեսի թեորեմը). *Էվկլիդյան R օղակում նրա կամայական ոչ զրոյական a, b տարրերի համար գոյություն ունի դրանց (a, b) ամենամեծ ընդհանուր բաժանարարը եւ $[a, b]$ ամենափոքր ընդհանուր բազմապատիկը:*

Ապացույցը կրկնում է 1.1 պարագրաֆի (1.2) համակարգի հետ բերված փաստարկները: Ուստի բերենք այն առանց մանրամասների: Ենթադրենք $a, b \neq 0$: Ըստ էվկլիդյան օղակի սահմանման, գոյություն ունեն $q, r \in R$ տարրեր այնպիսիք, որ $a = qb + r$, որտեղ կամ $r = 0$, կամ $r \neq 0$ եւ $\delta(r) < \delta(b)$: Եթե $r = 0$, ապա ակնհայտորեն $(a, b) = b$: Եթե $r \neq 0$, ապա կրկնենք քայլերը՝ մինչեւ ստացվի առաջին զրոյական մնացորդով բաժանումը.

$$
\begin{aligned}
&a = qb + r, && r \neq 0 \text{ եւ } \delta(r) < \delta(b),\\
&b = q_1 r + r_1, && r_1 \neq 0 \text{ եւ } \delta(r_1) < \delta(r),\\
&r = q_2 r_1 + r_2, && r_2 \neq 0 \text{ եւ } \delta(r_2) < \delta(r_1),\\
&r_1 = q_3 r_2 + r_3, && r_3 \neq 0 \text{ եւ } \delta(r_3) < \delta(r_2),\\
&\qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots && \qquad (2.7)\\
&r_{n-3} = q_{n-1} r_{n-2} + r_{n-1}, && r_{n-1} \neq 0 \text{ եւ } \delta(r_{n-1}) < \delta(r_n),\\
&r_{n-2} = q_n r_{n-1} + r_n, && r_n \neq 0 \text{ եւ } \delta(r_n) < \delta(r_{n-1}),\\
&r_{n-1} = q_{n+1} r_n + 0, && r_{n+1} = 0:
\end{aligned}
$$

Կրկնելով (1.2) համակարգին անմիջապես հաջորդող դիտարկումները՝ ստանում ենք, որ (2.7) համակարգում հանդիպող վերջին ոչ զրոյական մնացորդը $a, b \in R$ տարրերի ամենամեծ ընդհանուր բաժանարարն է.

$$d = r_n = (a, b):$$

Ամբողջ թվերի դեպքի համար $[a, b]$ ամենափոքր ընդհանուր բազմապատիկը հաշվվում է (a, b) ամենամեծ ընդհանուր բաժանարարի օգնությամբ

$$(a, b)[a, b] = ab$$

բանաձեւից: Դա արվում է ամենամեծ ընդհանուր բաժանարարի մասին մի քանի տարրական հատկությունների միջոցով (օրինակ՝ $(as, bs) = (a, b)s$ հատկությունը), որոնք հայտնի են ամբողջ թվերի դեպքի համար եւ որոնք հեշտ է ապացուցել նաեւ օղակների համար: Շարադրանքը չերկարացնելու համար բաց թողնենք դրանք: ■

Եթե (2.7) համակարգում վերանվանենք. $r_0 = r$, $r_{-1} = b$, $r_{-2} = a$, ապա տողերը կստանան ավելի միանման տեսք.

(2.8) $$r_{k-3} = q_{k-1}r_{k-2} + r_{k-1};\ \ r_{k-1} \neq 0 \text{ եւ } \delta(r_{k-1}) < \delta(r_k);\quad k = 1, \dots, n+2:$$

Մասնավորապես, $k = 1$ ինդեքսի համար կստացվի համակարգի առաջին տողը՝

$$r_{1-3} = r_{-2} = a = qb + r = q_0 r_{-1} + r_0 = q_{1-1}r_{1-1} + r_{1-1}:$$

Այս նշանակումներով ձեւակերպենք ստացված ալգորիթմը.

2.5.4 Ալգորիթմ (Էվկլիդեսի ալգորիթմը). Տրված են R էվկլիդյան օղակի $a, b \in R$ ոչ զրոյական տարրերը: Գտնել դրանց (a, b) ամենամեծ ընդհանուր բաժանարարը:

1. Նշանակենք $r_{-2} = a$ եւ $r_{-1} = b$:

2. Նշանակենք $k = 1$:

3. K էվկլիդյան օղակի r_{k-3} տարրը ներկայացնենք $r_{k-3} = q_{k-1}r_{k-2} + r_{k-1}$ տեսքով;

4. Եթե $r_{k-1} \neq 0$

5. նշանակենք $k = k + 1$;

6. վերադառնանք 3-րդ քայլին:

7. Դուրս գրենք $(a, b) = r_{k-2}$ ամենամեծ ընդհանուր բաժանարարը:

Հետեւյալ փաստը հաճախ անվանում են նաեւ *Էվկլիդեսի ընդլայնված ալգորիթմ*: Այն, լրացնելով նախորդ թեորեմը, պնդում է, որ (a, b) ամենամեծ ընդհանուր բաժանարարը ոչ միայն գոյություն ունի, այլեւ արտահայտվում է a, b տարրերի պատիկների գումարի միջոցով: Կրկին, ըստ 2.1.5 դիտողության, քննարկում ենք միայն ոչ զրոյական տարրերի դեպքը:

2.5.5 Թեորեմ. *Էվկլիդյան R օղակում նրա կամայական ոչ զրոյական $a, b \in R$ տարրերի համար գոյություն ունեն $u, v \in R$ տարրեր այնպիսիք, որ տեղի ունի հետեւյալ հավասարությունը.*

$$ua + vb = (a, b):$$

Ապացույց: Նշանակենք $(a, b) = d$: Նախորդ ապացույցի մեջ կառուցված (2.7) համակարգի նախավերջին տողից հետեւում է, որ

(2.9) $$d = r_n = r_{n-2} - q_n r_{n-1}:$$

Իսկ ըստ (2.7) համակարգի ներքեւից երրորդ տողի՝

$$r_{n-1} = r_{n-3} - q_{n-1}r_{n-2},$$

որտեղից r_{n-1}արժեքը տեղադրելով (2.9) հավասասության մեջ՝ կստանանք

$$d = r_{n-2} - q_n r_{n-1} = r_{n-2} - q_n(r_{n-3} - q_{n-1}r_{n-2})$$
$$= (1 + q_n q_{n-1}) \cdot r_{n-2} - q_n \cdot r_{n-3}:$$

d-ի այս ներկայացումը տարբերվում է (2.9) ներկայացումից այն բանով, որ այս գրառման մեջ արդեն բացակայում է r_{n-1}-ը, եւ d-ն ներկայացված է որպես r_{n-2} եւ r_{n-3} տարրերի պատիկների գումար: Հաջորդ քայլում այս հավասարության մեջ կտեղադրենք r_{n-2}-ի արժեքն ըստ (2.7) համակարգի ներքեւից չորրորդ տողի եւ կստանանք d-ի ներկայացում որպես r_{n-3} եւ r_{n-4} տարրերի պատիկների գումար: Այսպես բարձրանալով (2.7) համակարգի տողերով՝ վերջին քայլում կստանանք d-ի ներկայացում որպես a եւ b տարրերի պատիկների գումար, որի գործակիցները եւ կլինեն պահանջվող u, v տարրերը: ■

Այս ապացույցում մենք (2.7) համակարգի տողերը քննարկեցինք ներքեւից վերեւ, բայց կոնկրետ խնդիրներ լուծելիս ավելի հարմար է գնալ վերեւից ներքեւ. Էվկլիդեսի ալգորիթմի ամեն քայլը անելուց հետո հերթական մնացորդը ներկայացնենք որպես a եւ b տարրերի կոմբինացիա: Ձեւակերպենք սա ալգորիթմի տեսքով, ընդ որում, կրկին օգտվենք $r_0 = r, r_{-1} = b, r_{-2} = a$ նշանակումներից.

2.5.6 Ալգորիթմ (Էվկլիդեսի ընդլայնված ալգորիթմը). Տրված են R էվկլիդյան օղակի $a, b \in R$ ոչ զրոյական տարրերը: Գտնել դրանց (a, b) ամենամեծ ընդհանուր բաժանարարը եւ այնպիսի $u, v \in R$ տարրեր, որոնց համար, $ua + vb = (a, b)$:

1. Նշանակենք $r_{-2} = a$ եւ $r_{-1} = b$:

2. Նշանակենք $u' = 1, v' = 0$ եւ $u = 0, v = 1$:

3. Նշանակենք $k = 1$:

4. r_{k-3} եւ r_{k-2} մնացորդները ներկայացնենք $r_{k-3} = u'r_{-2} + v'r_{-1}$ եւ $r_{k-2} = ur_{-2} + vr_{-1}$ տեսքով:

5. K էվկլիդյան օղակի r_{k-3} տարրը ներկայացնենք $r_{k-3} = q_{k-1}r_{k-2} + r_{k-1}$ տեսքով;

6. Եթե $r_{k-1} \neq 0$

7. r_{k-3} եւ r_{k-2} մնացորդների՝ 4-րդ քայլում ստացված արժեքները տեղադրելով $r_{k-1} = r_{k-3} - q_{k-1}r_{k-2}$ ներկայացման մեջ, ստանանք $r_{k-1} = (u' - q_{k-1}u)r_{-2} + (v' - q_{k-1}v)r_{-1}$ ներկայացումը;

8. u, v փոփոխականներին շնորհենք նոր $u = u' - q_{k-1}u$ եւ $v = v' - q_{k-1}v$ արժեքներ;

9. $u,\ v$ փոփոխականների նախկին արժեքները շնորհենք u', v' փոփոխականներին;

10. նշանակենք $k = k + 1$;

11. վերադառնանք 4-րդ քայլին:

12. Դուրս գրենք $(a, b) = r_{k-2}$ ամենամեծ ընդհանուր բաժանարարը:

13. Դուրս գրենք $u,\ v$ արժեքները:

2.5.7 Հետեւանք. *Էվկլիդյան R օղակում նրա կամայական փոխադարձաբար պարզ $a, b \in R$ տարրերի համար գոյություն ունեն $u, v \in R$ տարրեր այնպիսիք, որ տեղի ունի հետեւյալ հավասարությունը.*

$$ua + vb = 1:$$

Էվկլիդյան օղակները եւ Էվկլիդեսի ալգորիթմը գլխավոր իդեալների օղակներ (տես 2.2.6 սահմանումը) կառուցելու հարմար միջոց են: Տեղի ունի.

2.5.8 Թեորեմ. *Կամայական էվկլիդյան օղակ գլխավոր իդեալների օղակ է:*

Ապացույց: Ենթադրենք տրված է R էվկլիդյան օղակը $\delta: R\backslash\{0\} \to \mathbb{N} \cup \{0\}$ արտապատկերման հետ միասին: R օղակի կամայական I իդեալի համար վերցնենք նրա որեւէ m ոչ զրոյական տարր, որի համար $\delta(m) \leq \delta(a)$ կամայական $a \in I$ տարրի համար: Սա միշտ էլ հնարավոր է անել, քանի որ $\delta(a)$ արժեքները ոչ բացասական ամբողջ թվեր են, եւ դրանցից միշտ էլ կարելի է ընտրել փոքրագույնը:

Այժմ վերցնենք կամայական $b \in I$ տարր եւ այն մնացորդով բաժանենք m-ի վրա ըստ էվկլիդյան օղակի սահմանման՝ $b = qm + r$, որտեղ $r = 0$ կամ $r \neq 0$ եւ $\delta(r) < \delta(m)$: Եթե $r \neq 0$, ապա ստանում ենք, որ $r = b - qm \in I$ տարրը I իդեալի ոչ զրոյական տարր է, որի համար $\delta(r) < \delta(m)$: Ստացված հակասությունը ցույց է տալիս, որ $r = 0$ եւ $b = qm + 0 = mq \in mR$: Ուստի $I = mR$: ■

Կան օղակներ, որոնք էվկլիդյան չեն:

2.5.9 Օրինակ. Ամբողջ գործակիցներով բազմանդամների $\mathbb{Z}[x]$ օղակը էվկլիդյան չէ: Իրոք, եթե այն էվկլիդյան օղակ լիներ, ապա, անկախ այն բանից, թե ինչպես է սահմանվել $\delta: \mathbb{Z}[x] \backslash\{0\} \to \mathbb{N} \cup \{0\}$ արտապատկերումը, այդ օղակի $f(x) = 2$ եւ $g(x) = x$ բազմանդամների համար, ըստ էվկլիդեսի ընդլայնված ալգորիթմի, պիտի գոյություն ունենան $u(x), v(x) \in \mathbb{Z}[x]$ բազմանդամներ այնպիսիք, որ

$$\begin{aligned} u(x)f(x) + v(x)g(x) &= u(x) \cdot 2 + v(x) \cdot x \\ &= \big(f(x), g(x)\big) = d(x) = 1: \end{aligned} \tag{2.10}$$

Վերջին հավասարությունն ակնհայտ է, քանի որ՝ անկախ δ արտապատկերման սահմանման եղանակից, ունենք $(2, x) = 1$: Մնում է նկատել, որ $v(x) \cdot x$ բազմանդամն ազատ անդամներ չունի, եւ (2.10) առնչության կատարման միակ հնարավորությունն այն է, որ $v(x) \cdot x$ բազմանդամը ամբողջությամբ կրճատվի $u(x) \cdot 2$ բազմանդամի այն գործակիցների հետ, որոնք տարբեր են ազատ անդամից, իսկ մնացած ազատ անդամն էլ հավասար լինի 1-ի: Բայց սա անհնար է, քանի որ $u(x) \cdot 2$ բազմանդամի ազատ անդամը, եթե այն գոյություն ունի, պիտի լինի ամբողջ զույգ թիվ:

2.5.10 Օրինակ. Հետեւյալ օրինակը հետաքրքիր է նրանով, որ այն ոչ էվկլիդյան օղակ է, որը միաժամանակ գլխավոր իդեալների օղակ է հանդիսանում: Վերցնենք $\alpha = {}^1\!/_2\,(1 + \sqrt{-19}) = {}^1\!/_2\,(1 + i\sqrt{19})$ կոմպլեքս թիվը եւ դիտարկենք $\mathbb{C}$ դաշտի հետեւյալ ենթաբազմությունը՝ $\mathbb{Z}(\alpha) = \{a + \alpha b \,|\, a, b \in \mathbb{Z}\}$: Սա գլխավոր իդեալների օղակ է, եւ նրա համար հնարավոր չէ սահմանել այնպիսի $\delta\colon \mathbb{Z}(\alpha) \setminus \{0\} \to \mathbb{N} \cup \{0\}$ արտապատկերում, որը էվկլիդյան օղակ կդարձներ $\mathbb{Z}(\alpha)$-ն (մանրամասները տես, օրինակ, (Ալեքսանյան, 2006) եւ (Dummit & Foote, 2004) դասագրքում):

2.5.11 Լեմմա. *Եթե R էվկլիդյան օղակի a, b, h տարրերի համար ունենք $a \cdot b \vdots h$ եւ $(a, h) = 1$, ապա $b \vdots h$:*

Ապացույց: Ըստ 2.5.7 հետեւանքի, ինչ-որ $u, v \in R$ տարրերի համար $ua + vh = 1$: Ուրեմն՝ $ua \cdot b + vh \cdot b = 1 \cdot b = b$ տարրը նույնպես բաժանվում է h-ի վրա: ■

2.5.12 Հետեւանք. Եթե R էվկլիդյան օղակի a, b տարրերի համար ունենք $a \cdot b \vdots p$, որտեղ p-ն պարզ է եւ a-ն չի բաժանվում p-ի վրա, ապա b-ն բաժանվում է p-ի վրա:

Հետեւյալ թեորեմը ոչ միայն էվկլիդյան օղակներ կառուցելու հեշտ միջոց է, այլեւ հետագայում օգտագործվելու է ալգորիթմներ կառուցելու համար:

2.5.13 Թեորեմ. *Յանկացած R դաշտի վրա տրված $R[x]$ բազմանդամային օղակը էվկլիդյան օղակ է:*

Ապացույց: 2.5.1 սահմանման **E.1** պայմանը ստուգվում է անմիջապես: Սահմանման **E.2** պայմանը ստուգելու համար ենթադրենք $f(x), g(x) \in R[x]$ եւ $g(x) \neq 0$:

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n \quad \text{եւ} \quad g(x) = b_0x^m + b_1x^{m-1} + \cdots + b_m\colon$$

Կիրառենք ինդուկցիա ըստ n աստիճանի: Երբ $n = 0$, ապա $m = 0$ դեպքում ունենք

$$f(x) = a_0 = \left(\frac{a_0}{b_0}\right) b_0 = \frac{a_0}{b_0}\, g(x) + 0,$$

այսինքն՝ $q(x) = \frac{a_0}{b_0}$ եւ $r(x) = 0$: Եթե $m > 0$, ապա

$$f(x) = 0 \cdot\ g(x) + f(x), \tag{2.11}$$

այսինքն՝ $q(x) = 0,\ r(x) = f(x),$ եւ $\delta\big(r(x)\big) < \delta\big(g(x)\big)$: Այժմ ենթադրենք թեորեմն ապացուցվել է n-ից ցածր աստիճանի բոլոր բազմանդամների համար: Եթե $m > n$,

ապա դարձյալ ապացույցն ավարտվում է (2.11) հավասարությամբ: Համարենք $m \le n$: Այդ դեպքում $n-m \ge 0$, ուրեմն՝ $f(x)$-ը ինչ-որ $f_1(x)$ բազմանդամի համար կարելի է ներկայացնել

$$f(x) = \frac{a_0}{b_0} x^{n-m} g(x) + f_1(x) \tag{2.12}$$

տեսքով, որտեղ $\delta\big(f_1(x)\big) < \delta\big(f(x)\big)$: Իրոք, քանի որ $\frac{a_0}{b_0} x^{n-m} g(x)$ բազմանդամն ունի նույն աստիճանը եւ նույն ավագ անդամը, ինչ $f(x)$-ը, ապա նրանց տարբերության մեջ կրճատում է կատարվում, եւ $f_1(x)$ բազմանդամն ունի ավելի ցածր աստիճան, քան $f(x)$ բազմանդամը: Ըստ ինդուկցիայի՝ թեորեմը ճիշտ է $f_1(x)$-ի համար. գոյություն ունեն $q_1(x)$ եւ $r_1(x)$ բազմանդամներ այնպիսիք, որ $f_1(x) = q_1(x)g(x) + r_1(x)$ եւ $\delta\big(r_1(x)\big) < \delta\big(g(x)\big)$: Մնում է $f_1(x)$-ը տեղադրել (2.12) հավասարության մեջ ու ստանալ $q(x) = \frac{a_0}{b_0} x^{n-m} + q_1(x)$ եւ $r(x) = r_1(x)$, ընդ որում, ունենք $\delta\big(r(x)\big) = \deg r_1(x) < \delta\big(g(x)\big)$: ■

Մեր ալգորիթմներում հաճախակի օգտագործվելու է հետեւյալ փաստը, որը անմիջապես հետեւում է քիչ առաջ ապացուցված 2.5.13 թեորեմից եւ մնացքների օղակների մասին 2.1.26 թեորեմից.

2.5.14 Հետեւանք. *Կամայական p պարզ թվի համար $\mathbb{Z}_p$ դաշտի վրա տրված $\mathbb{Z}_p[x]$ բազմանդամային օղակը էվկլիդյան օղակ է:*

Իսկ հետեւյալ նդումը հետեւում է 2.5.13 եւ 2.5.8 թեորեմներից:

2.5.15 Հետեւանք. *Կամայական R դաշտի վրա տրված $R[x]$ բազմանդամային օղակը գլխավոր իդեալների օղակ է:*

Այս տեսության հետագա զարգացումներ կարելի է գտնել 8-րդ գլխում: Տես 8.4.12 Հիլբերտի թեորեմը եւ 8.4.13 դիտողությունը: Տես նաեւ 6.3.12 օրինակը:

$c \in R$ տարրը կոչվում է $f(x) = a_0x^n + \cdots + a_n \in R[x]$ բազմանդամի արմատ, եթե R օղակում, եթե $f(c) \overset{\text{def}}{=} a_0c^n + \cdots + a_n = 0$: Տրված $f(x)$ բազմանդամը ոչ զրոյական $x-c$ բազմանդամի վրա մնացորդով բաժանելով հեշտ է ապացուցել.

2.5.16 Բեզուի թեորեմը. *Եթե $R[x]$ օղակն էվկլիդյան է, ապա $f(x) \in R[x]$ բազմանդամի համար $c \in R$ տարրն արմատ է այն եւ միայն այդ դեպքում, երբ $f(x) \vdots (x-c)$: Այսինքն՝ երբ որեւէ $q(x) \in R[x]$ բազմանդամի համար տեղի ունի $f(x) = (x-c)q(x)$ ներկայացումը:*

Ըստ 2.5.15 հետեւանքի, Բեզուի թեորեմը տեղի ունի դաշտի վրա տրված կամայական բազմանդամային օղակում:

2.5.17 Դիտողություն. Քանի որ $\mathbb{Z}_p[x]$-ն էվկլիդյան է, նրա համար գործում են էվկլիդյան 2.5.3, 2.5.5 եւ 2.5.7 ալգորիթմները: Անդրադառնալով $\varphi_p\colon \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ ան-

ցումների միջոցով կառուցվող ալգորիթմներին՝ նկատենք, որ $\mathbb{Z}_p[x]$ օղակը $\mathbb{Z}[x]$ օղակից շատ ավելի հարմար միջավայր է ալգորիթմներ կառուցելու համար: Ոչ միայն այն պատճառով, որ $\mathbb{Z}_p$-ում գործ ունենք միայն վերջավոր քանակությամբ թվերի հետ (ինչը կարճացնում է հաշվարկները եւ թույլ չի տալիս, որ առաջանա, ասենք, միջանկյալ արժեքների ուռճացման երեւույթը), այլեւ այն պատճառով, որ $\mathbb{Z}_p[x]$ օղակը էվկլիդյան է: Խնդիրներ լուծելիս նպատակահարմար է φ_p մոդուլյար անցումով խնդիրը $\mathbb{Z}[x]$ օղակից տեղափոխել $\mathbb{Z}_p[x]$ օղակ, լուծել այն էվկլիդյան մեթոդներով, եւ լուծումը «հետ բերել» $\mathbb{Z}[x]$: Այս ընթացքում առաջանում են հարցեր, որոնց մի մասին անդրադարձանք 2.4 պարագրաֆի 2.4.1, 2.4.2 եւ 2.4.3 կետերում:

2.6 Բազմանդամի բովանդակություն, կեղծ բաժանումներ

2.6.1 Սահմանում. Եթե R ամբողջության տիրույթի վրա տրված $f(x) \in R[x]$ բազմանդամի բոլոր գործակիցների ամենամեծ ընդհանուր բաժանարարը գոյություն ունի, ապա այն կոչվում է $f(x)$-ի *բովանդակություն* եւ նշանակվում $\mathrm{cont}\big(f(x)\big)$: Եթե $f(x) = a_0x^n$, ապա ընդունված է համարել $\mathrm{cont}(a_0x^n) = a_0$: Մասնավորապես, հաստատուն $f(x) = c$ բազմանդամի համար $\mathrm{cont}(c) = c$, իսկ զրոյական բազմանդամի համար $\mathrm{cont}(0) = 0$: Հետագայում մենք կհանդիպենք այնպիսի օղակների, որոնց որոշ տարրերի համար ամենամեծ ընդհանուր բաժանարար գոյություն չունի, ուստի 2.6.1 սահմանման մեջ ամենամեծ ընդհանուր բաժանարարի գոյության նախապայմանը, իրոք, անհրաժեշտ է: Օղակներում տարրերի ամենամեծ ընդհանուր բաժանարարը սահմանվում է հակադարձելի տարրի ճշտությամբ, ուստի $\mathrm{cont}\big(f(x)\big)$-ը նույնպես սահմանվում է այդ ճշտությամբ:

2.6.2 Սահմանում. R ամբողջության տիրույթի վրա տրված $f(x) \in R[x]$ բազմանդամը կոչվում է *նորմավորված*, եթե նրա ավագ գործակիցը հավասար է 1-ի:

Եթե $f(x)$-ի a_0 ավագ գործակիցը հակադարձելի տարր է R ամբողջության տիրույթում, ապա $f(x)$-ը կարելի է *նորմավորել*, այսինքն՝ $f(x)$-ից անցում կատարել $a_0^{-1} \cdot f(x)$ բազմանդամին, որն արդեն նորմավորված է: Հասկանալի է, որ եթե R-ը դաշտ է, ապա կարելի է նորմավորել $R[x]$-ի բոլոր ոչ զրոյական բազմանդամները: Եթե սահմանափակվենք $R = \mathbb{Z}$ դեպքով, ապա, հաշվի առնելով, որ $\mathbb{Z}$-ում ամենամեծ ընդհանուր բաժանարարը սահմանված է, իսկ հակադարձելի տարրերն են միայն -1 եւ 1, կունենանք.

2.6.3 Սահմանում. $f(x) \in \mathbb{Z}[x]$ ոչ զրոյական բազմանդամի *բովանդակություն* է կոչվում նրա բոլոր գործակիցների ամենամեծ ընդհանուր բաժանարարը: Այն նշանակվում է $\mathrm{cont}\big(f(x)\big)$ (եւ սահմանվում է նշանի ճշտությամբ):

2.6.4 Օրինակ. Եթե $f(x) = 2x^2 + 6x - 4 \in \mathbb{Z}[x]$, ապա $\mathrm{cont}\big(f(x)\big) = 2$ (կամ էլ $\mathrm{cont}\big(f(x)\big) = -2$):

2.6.5 Սահմանում. $f(x) \in R[x]$ բազմանդամը կոչվում է *պրիմիտիվ* բազմանդամ, եթե $\mathrm{cont}\big(f(x)\big) \approx 1$:

Բազմանդամի բովանդակությունը միշտ սահմանված է, եթե այն տրված է էվկլիդյան օղակի վրա. դրանցում տարրերի ամենամեծ ընդհանուր բաժանարարը գոյություն ունի: Կան օղակների ավելի լայն դասեր եւս, որոնց վրա նույնպես բովանդակությունը միշտ սահմանված է (տես 6.3 պարագրաֆը): Եթե ոչ զրոյական $f(x)$ բազմանդամի համար սահմանված է $\mathrm{cont}\big(f(x)\big)$-ը, ապա $f(x)$-ը կարելի է ներկայացնել

$$f(x) = \mathrm{cont}\big(f(x)\big)\ f_0(x)$$

տեսքով, որտեղ $f_0(x)$-ը պրիմիտիվ բազմանդամ է. բավական է վերցնել $f_0(x) = f(x)/\mathrm{cont}\big(f(x)\big)$:

2.6.6 Սահմանում. Եթե $f(x) \in R[x]$ ոչ զրոյական բազմանդամի համար սահմանված է նրա $\mathrm{cont}\big(f(x)\big)$ բովանդակությունը, ապա $f(x)$-ի *պրիմիտիվ մաս* է կոչվում $f(x)/\mathrm{cont}\big(f(x)\big)$ պրիմիտիվ բազմանդամը: Այն նշանակվում է $\mathrm{pp}\big(f(x)\big)$:

Ըստ վերը ասվածի, $\mathrm{pp}\big(f(x)\big)$-ը սահմանվում է հակադարձելի տարրի ճշտությամբ: Մասնավորապես, կամայական ոչ զրոյական $f(x) \in \mathbb{Z}[x]$ բազմանդամի համար $\mathrm{pp}\big(f(x)\big)$-ը միշտ գոյություն ունի եւ սահմանվում է նշանի ճշտությամբ:

2.6.7 Օրինակ. 2.6.4 օրինակի $f(x)$ բազմանդամի համար ունենք $\mathrm{pp}\big(f(x)\big) = (2x^2 + 6x - 4)/2 = x^2 + 3x - 2$: Կամ էլ $\mathrm{pp}\big(f(x)\big) = -x^2 - 3x + 2$:

Գաուսի լեմմայի ամենաընդհանուր տեսքը եւ դրա հետ կապված ֆակտորիալ օղակների հատկությունները մեզ պետք կգան 6-րդ գլխում՝ բազմանդամների ֆակտորիզացիայի ալգորիթմներ կառուցելու համար: Քանի որ մինչ այդ ֆակտորիալ օղակների վերաբերյալ մեզ ընդամենը մի քանի փաստ է պետք գալու, առայժմ բերենք Գաուսի լեմմայի միայն մասնավոր դեպքը $\mathbb{Z}[x]$ օղակի համար:

2.6.8 Գաուսի լեմման $\mathbb{Z}[x]$ օղակի համար. *Կամայական $f(x),\ g(x) \in \mathbb{Z}[x]$ բազմանդամների համար.*

$$\mathrm{cont}\big(f(x) \cdot g(x)\big) \approx \mathrm{cont}\big(f(x)\big) \cdot \mathrm{cont}\big(g(x)\big): \tag{2.13}$$

Մասնավորապես, պրիմիտիվ բազմանդամների արտադրյալը պրիմիտիվ բազմանդամ է:

Ապացույց: նախ ապացուցենք երկրորդ պնդումը: Ենթադրենք $f(x),\ g(x)$ բազմանդամները պրիմիտիվ են, բայց նրանց $h(x)=f(x)\cdot g(x)$ արտադրյալը պրիմիտիվ չէ. կա մի p պարզ թիվ, որի վրա բաժանվում են $h(x)$-ի բոլոր գործակիցները: Եթե $f(x),\ g(x)$ բազմանդամների գործակիցների մի մասը բաժանվում են p-ի վրա, ապա, ըստ պրիմիտիվության պայմանի, այդ բազմանդամներից յուրաքանչյուրն ունի գոնե մի գործակից, որը p-ի վրա չի բաժանվում: Ենթադրենք $f(x)$-ում այդպիսի գործակիցներից առաջինը a_s-ն է, իսկ $g(x)$-ում՝ b_t-ն.

$$f(x)=a_0x^n+\cdots+a_sx^{n-s}+\cdots+a_n,$$
$$g(x)=b_0x^m+\cdots+b_tx^{m-t}+\cdots+b_m, \tag{2.14}$$

$p|a_0,\dots,p|a_{s-1}$ բայց $p\nmid a_s$, եւ $p|b_0,\dots,p|b_{t-1}$ բայց $p\nmid b_t$: Պարզ է, որ $h(x)$ բազմանդամի մեջ $x^{(n-s)+(m-t)}$ աստիճանի գործակիցը կլինի.

$$c_{s+t}=a_sb_t+[a_{s+1}b_{t-1}+a_{s+2}b_{t-2}+\cdots]+[a_{s-1}b_{t+1}+a_{s-2}b_{t+2}+\cdots]: \tag{2.15}$$

Ըստ b_t-ի ընտրության, $b_{t-1},b_{t-2},\cdots$ գործակիցները բոլորը բաժանվում են p-ի վրա: Ուստի (2.15) արտահայտության առաջին քառակուսի փակագծի գումարը բաժանվում է p-ի վրա: Հաշվի առնելով a_s-ի ընտրությունը՝ p-ի վրա բաժանվում է նաեւ (2.15) հավասարության երկրորդ քառակուսի փակագծի գումարը: Եւ քանի որ $p\nmid a_sb_t$, ապա նաեւ $p\nmid c_{s+t}$: Հակասություն:

Անցնելով ընդհանուր դեպքին՝ ներկայացնենք բազմանդամները

$$f(x)=\operatorname{cont}\big(f(x)\big)\operatorname{pp}\big(f(x)\big),\ g(x)=\operatorname{cont}\big(g(x)\big)\operatorname{pp}\big(g(x)\big)$$

տեսքով, որտեղ $\operatorname{pp}\big(f(x)\big)$ եւ $\operatorname{pp}\big(g(x)\big)$ բազմանդամները պրիմիտիվ են (տրիվիալ դեպքը, երբ բազմանդամներից որեւէ մեկը զրոյական է, ակնհայտ է, եւ այն կարելի է բացառել): Ուրեմն $f(x)g(x)=\operatorname{cont}\big(f(x)\big)\operatorname{cont}\big(g(x)\big)\cdot\operatorname{pp}\big(f(x)\big)\operatorname{pp}\big(g(x)\big)$: Քանի որ $\operatorname{pp}\big(f(x)\big)\operatorname{pp}\big(g(x)\big)$ արտադրյալը, ըստ քիչ առաջ ապացուցվածի, պրիմիտիվ բազմանդամ է, ապա հավասարության աջ մասի բովանդակությունն է $\operatorname{cont}\big(f(x)\big)\operatorname{cont}\big(g(x)\big)$: Մնում է համեմատել դա հավասարության ձախ մասի բովանդակության հետ: ■

2.6.9 Հետեւանք. $\mathbb{Z}[x]$ օղակում պրիմիտիվ բազմանդամի բաժանարարը նույնպես պրիմիտիվ բազմանդամ է: Մասնավորապես, պրիմիտիվ բազմանդամների ամենամեծ ընդհանուր բաժանարարը պրիմիտիվ բազմանդամ է:

Չնայած տարբեր օղակներ երբեմն կարող են պարունակել ընդհանուր տարրեր, այդ տարրերի բաժանելիությունը կարող է, տվյալ օղակից կախված, տարբեր իմաստ ունենալ:

2.6.10 Օրինակ. 2 եւ 3 թվերը պատկանում են $\mathbb{Z}$ եւ $\mathbb{Q}$ օղակներին, բայց դրանց բաժանելիությունը տեղի ունի այդ օղակներից միայն երկրորդում՝ $2 \vdots 3$, քանի որ $2 = 3 \cdot \frac{2}{3}$: Նույն կերպ՝ $f(x) = x^2 + 3x$ բազմանդամը բաժանվում է $g(x) = 2x + 6$ բազմանդամի վրա $\mathbb{Q}[x]$ օղակում, բայց ոչ $\mathbb{Z}[x]$ օղակում $f(x) = x^2 + 3x = \frac{1}{2}x \cdot (2x + 6)$:

$\mathbb{Q}$ դաշտի վրա տրված բազմանդամների համար տարբեր ալգորիթմական խնդիրներ կարելի է հանգեցնել $\mathbb{Z}$ օղակի վրա տրված բազմանդամների համար համանման խնդիրների քննարկմանը, եւ հակառակը:

2.6.11 Լեմմա. *Ենթադրենք $f(x)$, $g(x) \in \mathbb{Z}[x]$, ընդ որում, $g(x)$ բազմանդամը պրիմիտիվ է: Եթե $f(x)$-ը բաժանվում է $g(x)$-ի վրա $\mathbb{Q}[x]$ օղակում, ապա այն բաժանվում է դրա վրա նաեւ $\mathbb{Z}[x]$ օղակում:*

Ապացույց: Վերցնենք այն $h(x) \in \mathbb{Q}[x]$ բազմանդամը, որի համար $f(x) = g(x)h(x)$: Այդ բազմանդամի գործակիցները ռացիոնալ են.

$$h(x) = \frac{u_0}{v_0}x^m + \cdots + \frac{u_m}{v_m}:$$

Բնական $v_0, \dots, v_m$ հայտարարների ամենափոքր ընդհանուր բազմապատիկը նշանակենք v: Այդ դեպքում $v \cdot h(x)$ բազմանդամը $\mathbb{Z}[x]$-ից է եւ կարելի է դիտարկել դրա բոլոր գործակիցների u ամենամեծ ընդհանուր բաժանարարը՝ $u = \mathrm{cont}\big(v \cdot h(x)\big)$: Նշանակելով $a = \mathrm{cont}\big(f(x)\big)$՝ հաշվենք.

$$v \cdot f(x) = v \cdot a \cdot \mathrm{pp}\big(f(x)\big) = g(x) \cdot\ v \cdot h(x) = g(x) \cdot\ u \cdot \mathrm{pp}\big(v \cdot h(x)\big): \tag{2.16}$$

Այս հավասարության ձախ մասի բովանդակությունն է $v \cdot a$, իսկ աջ մասինը՝ u, քանի որ $g(x)$ եւ $\mathrm{pp}\big(v \cdot h(x)\big)$ պրիմիտիվ բազմանդամների արտադրյալը պրիմիտիվ է ըստ Գաուսի լեմմայի: Ուստի $v \cdot a \approx u$ եւ (2.16) հավասարությունների բոլոր մասերն էլ բաժանվում են $v \cdot a$-ի վրա: Ուրեմն $\mathrm{pp}\big(f(x)\big) = g(x)\ \frac{u}{v \cdot a}\mathrm{pp}\big(v \cdot h(x)\big)$ եւ

$$f(x) = a \cdot \mathrm{pp}\big(f(x)\big) = a \cdot g(x)\frac{u}{v \cdot a}\mathrm{pp}\big(v \cdot h(x)\big):$$

Այսինքն՝ $f(x) = g(x)k(x)$, որտեղ $k(x) = a\frac{u}{v}\mathrm{pp}\big(v \cdot h(x)\big) \in \mathbb{Z}[x]$: ■

2.6.12 Խնդիր. Ցույց տալ, որ $\mathbb{Z}[x]$ օղակի կամայական $f(x)$ պարզ տարր ունի հետեւյալ երկու տիպերից մեկը.

1) կամ $\deg f(x) = 0$ եւ այդ դեպքում $f(x) = c$ հաստատուն բազմանդամը պարզ է այն եւ միայն այն դեպքում, երբ c-ն պարզ է որպես ամբողջ թիվ (որպես $\mathbb{Z}$ օղակի ոչ զրոյական տարր),

2) կամ էլ $\deg f(x) > 0$ եւ այդ դեպքում $f(x)$ բազմանդամը պարզ է այն եւ միայն այն դեպքում, երբ այն պրիմիտիվ պարզ բազմանդամ է:

2.6.13 Թեորեմ. *$\mathbb{Z}[x]$ օղակի կամայական ոչ զրոյական $f(x)$ բազմանդամ կարելի է ներկայացնել հետեւյալ տեսքով.*

$$f(x) = \varepsilon \cdot p_1 \cdots p_u \cdot g_1(x) \cdots g_s(x), \tag{2.17}$$

որտեղ $\varepsilon = \pm 1$, $p_1, \dots, p_m$ տարրերը ամբողջ պարզ թվեր են, իսկ $g_1(x), \dots, g_s(x)$ տարրերը՝ 0-ից բարձր աստիճանի պրիմիտիվ պարզ բազմանդամներ: Ընդ որում, (2.17) ներկայացումը միակն է այն իմաստով, որ եթե գոյություն ունի $f(x)$ բազմանդամի նման մի այլ ներկայացում եւս՝

$$f(x) = \epsilon \cdot q_1 \cdots q_v \cdot h_1(x) \cdots h_r(x), \tag{2.18}$$

ապա $u = v$, $s = r$ եւ (միգուցե արտադրիչների որոշ վերադասավորությունից հետո) տեղի ունեն. $p_i \approx q_i$ $(i = 1, \dots, u)$ եւ $g_j(x) \approx h_j(x)$ $(j = 1, \dots, s)$:

Ապացույց: Ենթադրենք $\deg f(x) > 0$ եւ $f(x) = \operatorname{cont}\big(f(x)\big) \operatorname{pp}\big(f(x)\big)$: Ըստ թվաբանության հիմնական թեորեմի $\operatorname{cont}\big(f(x)\big)$-ը ներկայացնենք պարզ թվերի $p_1 \cdots p_u$ արտադրյալի տեսքով: Եթե $\operatorname{pp}\big(f(x)\big)$ պրիմիտիվ մասը պարզ բազմանդամ չէ, ներկայացնենք այն $\operatorname{pp}\big(f(x)\big) = f_1(x) f_2(x)$ տեսքով (որտեղ $f_1(x), f_2(x) \not\approx 1$): Եթե $f_1(x), f_2(x)$ պրիմիտիվ բազմանդամներից որեւէ մեկը դարձյալ պարզ չէ, այն ներկայացնենք ոչ տրիվիալ արտադրյալի տեսքով: Քանի որ պրոցեսն անվերջ շարունակվել չի կարող, մի քանի քայլից կստանանք $\operatorname{pp}\big(f(x)\big) = g_1(x) \cdots g_s(x)$ ներկայացումը պրիմիտիվ պարզ բազմանդամների արտադրյալի տեսքով:

Ներկայացման միակությունը ցույց տալու համար ենթադրենք $f(x)$ բազմանդամը ներկայացվել է նաեւ (2.18) տեսքով: 2.5.11 լեմման եւ 2.5.12 հետեւանքը հեշտությամբ կարելի է ընդհանրացնել երկուսից ավել արտադրիչների դեպքի համար. $\mathbb{Q}[x]$ օղակում $h_1(x)$ պարզ բազմանդամի վրա է բաժանվում $p_1, \dots, p_u, g_1(x), \dots, g_s(x)$ արտադրիչներից որեւէ մեկը: Ըստ 2.6.11 լեմմայի այդ բաժանումը տեղի ունի նաեւ $\mathbb{Z}[x]$ օղակում: Քանի որ $\deg h_1(x) > 0$, ապա համարենք բաժանվող արտադրիչը $g_1(x)$-ն է: Կրճատելով դրա վրա եւ կրկնելով այս քայլը մի քանի անգամ կստանանք ներկայացման միակությունը: ■

2.6.13 թեորեմի (2.17) ներկայացումը անվանում են նաեւ բազմանդամի *ֆակտորիզացիա*: (2.17) ներկայացման մեջ կարելի է կատարել «նման անդամների միացում»: Եթե p_i պարզ թվերի մեջ կան իրար ասոցացված թվեր կամ եթե $g_j(x)$ բազմանդամների մեջ կան իրար ասոցացված բազմանդամներ, դրանք կարելի է իրար

միացնել՝ անհրաժեշտության դեպքում փոխելով ε արտադրիչի նշանը (եթե միացվող ասոցացված տարրերը ունեն հակառակ նշաններ): Կստանանք.

$$f(x) = \nu \cdot p_1^{\alpha_1} \cdots p_n^{\alpha_n} \cdot g_1^{\beta_1}(x) \cdots g_m^{\beta_m}(x), \tag{2.19}$$

որտեղ $p_1, \dots, p_n$; $g_1(x), \dots, g_m(x)$ տարրերը զույգ առ զույգ ասոցացված չեն եւ $\nu = \pm 1$:

2.6.14 Օրինակ. $f(x) = 270x^3 + 990x^2 + 1170x + 450$ բազմանդամի (2.17) ներկայացումն է $f(x) = 90 \cdot (3x^3 + 11x^2 + 13x + 5) = 1 \cdot 2 \cdot 3 \cdot 3 \cdot 5 \cdot (x+1)(x+1)(3x+5)$, որի (2.19) տեսքը «նման անդամների միացումից» հետո կլինի $f(x) = 1 \cdot 2 \cdot 3^2 \cdot 5 \cdot (x+1)^2(3x+5)$: Այս տեսքերը միակն են թեորեմում նշված իմաստով. $f(x)$ բազմանդամն, օրինակ, կարելի է ներկայացնել նաեւ հետեւյալ տեսքով՝ $f(x) = (-1) \cdot 2 \cdot (-3)^2 \cdot 5 \cdot (-x-1)^2(-3x-5)$:

Պրիմիտիվ բազմանդամների համար (2.17) եւ (2.19) ներկայացումները ավելի պարզ տեսք ունեն.

2.6.15 Հետեւանք. $\mathbb{Z}[x]$ օղակի կամայական պրիմիտիվ $f(x)$ բազմանդամ կարելի է ներկայացնել հետեւյալ տեսքով.

$$f(x) = \varepsilon \cdot g_1(x) \cdots g_s(x), \tag{2.20}$$

որտեղ $\varepsilon = \pm 1$, իսկ $g_1(x), \dots, g_s(x)$ տարրերը 0-ից բարձր աստիճանի պրիմիտիվ պարզ բազմանդամներ են: Ընդ որում, (2.17) ներկայացումը միակն է 2.6.13 թեորեմում նշված իմաստով:

2.6.13 թեորեմի մի այլ կարեւոր հետեւանքն էլ այն է, որ, չնայած $\mathbb{Z}[x]$ օղակը էվկլիդյան չէ (տես 2.5.9 օրինակը) եւ չնայած այդ օղակում ամենամեծ ընդհանուր բաժանարարի գոյությունը չի կարելի ապահովել 2.5.13 թեորեմի միջոցով, այնուամենայնիվ, $\mathbb{Z}[x]$-ում ցանկացած ոչ զրոյական տարրերի ամենամեծ ընդհանուր բաժանարարը միշտ գոյություն ունի.

2.6.16 Հետեւանք. Կամայական $f(x), g(x) \in \mathbb{Z}[x]$ բազմանդամների համար, որոնք միաժամանակ զրոյական չեն, գոյություն ունի նրանց

$$d(x) = \big(f(x), g(x)\big) \in \mathbb{Z}[x]$$

ամենամեծ ընդհանուր բաժանարարը: $d(x)$-ը որոշվում է ± 1 արտադրիչի (նշանի) ճշտությամբ:

Ապացույց: Եթե $f(x), g(x)$ բազմանդամներից մեկը զրոյական է, ապա պնդումը տրիվիալ է: Եթե $f(x), g(x)$ բազմանդամները երկուսն էլ ոչ զրոյական են, վերցնենք դրանց (2.19) ներկայացումները.

$$f(x) = \nu \cdot p_1^{\alpha_1} \cdots p_n^{\alpha_n} \cdot g_1^{\beta_1}(x) \cdots g_m^{\beta_m}(x),$$
$$g(x) = \nu' \cdot p_1^{\alpha'_1} \cdots p_n^{\alpha'_n} \cdot g_1^{\beta'_1}(x) \cdots g_m^{\beta'_m}(x): \tag{2.21}$$

Նկատենք, որ այստեղ մենք երկու ներկայացումներում էլ օգտագործել ենք միեւնույն $p_1, \dots, p_n$; $g_1(x), \dots, g_m(x)$ արտադրիչները: Հասկանալի է, որ $f(x), g(x)$ բազմանդամները պարտավոր չեն ունենալ միեւնույն պարզ արտադրիչները: Սակայն, առանց այս ապացույցի կոռեկտությունը խախտելու, մեր ներկայացումների մեջ կարող ենք ավելացնել «պակասող» պարզ տարրերը՝ զրոյական աստիճաններով: Այս պայմանավորվածության պարագայում հեշտ է ստուգել, որ

$$\big(f(x), g(x)\big) = \kappa \cdot p_1^{\gamma_1} \cdots p_n^{\gamma_n} \cdot g_1^{\delta_1}(x) \cdots g_m^{\delta_m}(x), \tag{2.22}$$

որտեղ $\kappa = \pm 1$, $\gamma_i = \min\{\alpha_i, \alpha'_i\}$, $\delta_j = \min\{\beta_j, \beta'_j\}$ $(i = 1, \dots, n;\ j = 1, \dots, m)$: ■

2.6.17 Խնդիր. Ցույց տալ, որ կամայական $f(x), g(x) \in \mathbb{Z}[x]$ բազմանդամների համար, որոնցից ոչ մեկը զրոյական չէ, գոյություն ունի նրանց $[f(x), g(x)] \in \mathbb{Z}[x]$ ամենափոքր ընդհանուր բազմապատիկը: Ցույց տալ նաեւ, որ

$$\big(f(x), g(x)\big) \cdot [f(x), g(x)] \approx f(x) \cdot g(x):$$

2.6.18 Դիտողություն. $\mathbb{Z}[x]$ եւ $\mathbb{Q}[x]$ օղակներում միեւնույն տարրերի ամենամեծ ընդհանուր բաժանարարները կարող են տարբեր լինել: Օրինակ, $\mathbb{Z}[x]$ օղակում $f(x) = 12x^2 + 24x + 12$ եւ $g(x) = 8x + 8$ բազմանդամների ամենամեծ բաժանարար են հանդիսանում միայն $4x + 4$ եւ $-4x - 4$ բազմանդամները, քանի որ $\mathbb{Z}[x]$-ի միակ հակադարձելի տարրերն են $\{1, -1\}$: Իսկ $x + 1$ կամ $2x + 2$ բազմանդամներից ոչ մեկը ամենամեծ ընդհանուր բաժանարար չէ, քանի որ դրանք չեն բաժանվում $4x + 4$ ընդհանուր բաժանարարի վրա: Մինչդեռ $\mathbb{Q}[x]$ օղակում որպես $\big(f(x), g(x)\big)$ կարելի է վերցնել, ասենք, $x + 1$ կամ $2x + 2$ բազմանդամները:

Չնայած 2.6.16 հետեւանքն ապահովում է $\mathbb{Z}[x]$ օղակում ամենամեծ ընդհանուր բաժանարարի գոյությունը, այն, ի տարբերություն Էվկլիդեսի ալգորթմի (տես 2.5.3 թեորեմը), չի տալիս դրա հաշվման արդյունավետ եղանակ: $\mathbb{Z}[x]$-ում բազմանդամների ամենամեծ ընդհանուր բաժանարարի հաշվումը կարելի է կատարել $\mathbb{Z}[x]$-ը պարունակող $\mathbb{Q}[x]$ օղակի Էվկլիդյանության եւ այսպես կոչված «կեղծ բաժանումների» միջոցով: Նախ, $f(x)$, $g(x) \in \mathbb{Z}[x]$ բազմանդամները համարենք $\mathbb{Q}[x]$ Էվկլիդյան օղակի տարրեր եւ հաշվենք դրանց $h(x) \in \mathbb{Q}[x]$ ամենամեծ ընդհանուր բաժանարարը Էվկլիդեսի ալգորիթմով:

2.6.19 Օրինակ. Ենթադրենք $f(x)=2x^3-14x+14$ եւ $g(x)=6x^2-14$: Այս բազմանդամների համար $\mathbb{Q}[x]$ էվկլիդյան օղակում ունենք՝

$$\begin{array}{l|l} 2x^3-14x+14 & 6x^2-14 \\ \hline 2x^3-14/3\,x & 1/3\,x \\ \hline -28/3\,x+14 & \end{array}$$

Այսինքն՝ $2x^3-14x+14=1/3\,x\cdot(6x^2-14)-28/3\,x+14$: Հաջորդ քայլում՝

$$6x^2-14=(-9/14\,x-27/98)(-28/3\,x+14)-632/49:$$

Քանի որ ստացվեց զրոյական աստիճանի մնացորդ, ապա $\mathbb{Q}[x]$ օղակում $\big(f(x),g(x)\big)=-632/49\approx 1$, եւ $f(x)$, $g(x)$ բազմանդամները փոխադարձաբար պարզ են $\mathbb{Q}[x]$-ում: Այս պահին չգիտենք՝ որն է դրանց ամենամեծ ընդհանուր բաժանարարը $\mathbb{Z}[x]$ օղակում, բայց $f(x)$, $g(x)$ բազմանդամները երկուսն էլ $\mathbb{Z}[x]$-ում բաժանվում են $h(x)=2$ հաստատուն բազմանդամի վրա, որը ասոցացված չէ 1-ին ոչ $\mathbb{Z}$ օղակում, ոչ էլ $\mathbb{Z}[x]$ օղակում: Այսինքն՝ $\mathbb{Z}[x]$ օղակում $f(x),g(x)$ բազմանդամները փոխադարձաբար պարզ չեն:

$h(x)\in\mathbb{Q}[x]$ ամենամեծ ընդհանուր բաժանարարից Գաուսի լեմմայով հեշտ է ստանալ ամենամեծ ընդհանուր բաժանարարը նաեւ $\mathbb{Z}[x]$ օղակում: Ինչ-որ $q_1(x)$, $q_2(x)\in\mathbb{Q}[x]$ բազմանդամների համար $\mathbb{Q}[x]$-ում ունենք. $f(x)=h(x)\cdot q_1(x)$ եւ $g(x)=h(x)\cdot q_2(x)$ (այն պարզ դեպքը, երբ բազմանդամներից մեկը զրոյական է, կարելի է բացառել): Եթե $h(x)$ բազմանդամի բոլոր գործակիցների հայտարարների ամենափոքր ընդհանուր բազմապատիկը նշանակենք s, իսկ $q_1(x)$, $q_2(x)$ բազմանդամների բոլոր գործակիցների հայտարարների ամենափոքր ընդհանուր բազմապատիկը՝ s, ապա

$$stf(x)=sh(x)\cdot tq_1(x)\quad\text{եւ}\quad stg(x)=sh(x)\cdot tq_2(x)$$

հավասարությունների թե աջ եւ թե ձախ մասերը կլինեն $\mathbb{Z}[x]$-ից: $sh(x)$ բազմանդամը կլինի $stf(x)$ եւ $stg(x)$ բազմանդամների ընդհանուր բաժանարարը $\mathbb{Z}[x]$-ում:

Հաշվարկների ընթացքում ստացված «ավելորդ» s եւ st սկալյար արտադրիչներից կարելի է ազատվել հետեւյալ կերպ. նախ նկատենք, որ եթե $f(x)$, $g(x)$ բազմանդամները լինեին պրիմիտիվ $\mathbb{Z}[x]$-ում, ապա, ըստ 2.6.9 հետեւանքի, պրիմիտիվ կլիներ նաեւ դրանց ամենամեծ ընդհանուր բաժանարարը եւ կունենայինք

$$\big(f(x),g(x)\big)=\mathrm{pp}\big(sh(x)\big):$$

Իսկ եթե այդ բազմանդամները պրիմիտիվ չեն, ապա խնդիրը կարելի է հանգեցնել նախորդ դեպքին. գրենք

$$f(x) = \mathrm{cont}\big(f(x)\big)\,\mathrm{pp}\big(f(x)\big), \qquad g(x) = \mathrm{cont}\big(g(x)\big)\,\mathrm{pp}\big(g(x)\big)$$

եւ նշանակենք $r = \Big(\mathrm{cont}\big(f(x)\big), \mathrm{cont}\big(g(x)\big)\Big)$: Ընդ որում, $\mathrm{cont}\big(f(x)\big)$ եւ $\mathrm{cont}\big(g(x)\big)$ արժեքներն ու նրանց r ամենամեծ ընդհանուր բաժանարարը $\mathbb{Z}$ օղակում կարելի է հաշվել Էվկլիդեսի ալգորիթմով ($\mathbb{Z}$-ը Էվկլիդյան օղակ է):

Իսկ $\mathrm{pp}\big(f(x)\big)$ եւ $\mathrm{pp}\big(g(x)\big)$ պրիմիտիվ բազմանդամների համար կարելի է դրանց պրիմիտիվ ամենամեծ ընդհանուր բաժանարարը հաշվել քիչ առաջ բերված կանոնով՝ $\mathrm{pp}\big(sh(x)\big)$, որտեղ $h(x)$-ը այդ բազմանդամների ամենամեծ ընդհանուր բաժանարարն է $\mathbb{Q}[x]$-ում ($\mathbb{Q}[x]$-ը Էվկլիդյան օղակ է): Վերջնական պատասխանը կունենա $r \cdot \mathrm{pp}\big(sh(x)\big)$ տեսքը: Այսպիսով, ստանում ենք հետեւյալ ալգորիթմը .

2.6.20 Ալգորիթմ ($\mathbb{Z}[x]$ օղակում ամենամեծ ընդհանուր բաժանարարի հաշվումը «կեղծ բաժանումների» միջոցով). Տրված են $f(x),\ g(x) \in \mathbb{Z}[x]$ ոչ զրոյական բազմանդամները: Հաշվել նրանց $\big(f(x),\ g(x)\big)$ ամենամեծ ընդհանուր բաժանարարը:

1. $\mathbb{Z}$ օղակում Էվկլիդեսի ալգորիթմով հաշվենք $\mathrm{cont}\big(f(x)\big)$ եւ $\mathrm{cont}\big(g(x)\big)$ բովանդակությունները:

2. $\mathbb{Z}$ օղակում Էվկլիդեսի ալգորիթմով հաշվենք այդ բովանդակությունների $r = \Big(\mathrm{cont}\big(f(x)\big),\ \mathrm{cont}\big(g(x)\big)\Big)$ ամենամեծ ընդհանուր բաժանարարը:

3. Անցում կատարենք բազմանդամների պրիմիտիվ մասերին. $f(x) = \mathrm{pp}\big(f(x)\big)$ եւ $g(x) = \mathrm{pp}\big(g(x)\big)$:

4. $f(x),\ g(x)$ բազմանդամները դիտարկենք որպես Էվկլիդյան $\mathbb{Q}[x]$ օղակի տարրեր, եւ Էվկլիդեսի ալգորիթմով հաշվենք դրանց $h(x) \in \mathbb{Q}[x]$ ամենամեծ ընդհանուր բաժանարարը (բազմանդամները «անկյունով» բաժանելիս կարող են առաջանալ կոտորակային գործակիցներ):

5. $h(x)$ բազմանդամը որեւէ s սկալյարով բազմապատկելով՝ ստանանք $sh(x) \in \mathbb{Z}[x]$: Որպես s կարելի է վերցնել, օրինակ, $h(x)$ բազմանդամի բոլոր գործակիցների հայտարարների ամենափոքր ընդհանուր բազմապատիկը:

6. Հաշվենք դրա $\mathrm{pp}\big(sh(x)\big)$ պրիմիտիվ մասը:

7. Որոնելի ամենամեծ ընդհանուր բաժանարարը դուրս գրենք $r \cdot \mathrm{pp}\big(sh(x)\big)$ տեսքով:

2.6.21 Օրինակ. 2.6.19 օրինակի բազմանդամների համար հաշվենք՝

$$\mathrm{cont}\big(f(x)\big) = \mathrm{cont}(2x^3 - 14x + 14\,) = 2,$$
$$\mathrm{cont}\big(g(x)\big) = \mathrm{cont}(6x^2 - 14\,) = 2:$$

Ուրեմն, $r = (2{,}2) = 2$: Ունենք $\mathrm{pp}\big(f(x)\big) = x^3 - 7x + 7$ եւ $\mathrm{pp}\big(g(x)\big) = 3x^2 - 7$:

$$\begin{array}{l|l} x^3-7x+7 & 3x^2-7 \\ \hline x^3-7/3\,x & 1/3\,x \\ \hline -14/3\,x+7 & \end{array}$$

Այսինքն՝ $x^3-7x+7 = 1/3\,x\cdot(3x^2-7)-14/3\,x+7$: Հաջորդ քայլում $3x^2-7 = (-9/14\,x-27/28)(-14/3\,x+7)-1/4$: Ուրեմն՝ $\mathbb{Q}[x]$ օղակում տեղի ունի՝ $h(x) = \big(f(x),g(x)\big) = -1/4 \approx 1$: Ստացված $-1/4$ մնացորդը $\mathbb{Z}[x]$ օղակի մեջ բերելու համար բազմապատկենք այն -4-ով: Խնդրի պատասխանն է $d(x) = r\cdot \mathrm{pp}\big(ah(x)\big) = 2\cdot \mathrm{pp}((-4)(-1/4)) = 2$: Համեմատե՛լ սա 2.6.19 օրինակի արդյունքի հետ:

Քանի որ ռացիոնալ թվերի հետ գործողությունների ժամանակ կոտորակների համարիչներն ու հայտարարները աճում են, երբեմն հարմար է $\mathbb{Q}[x]$ օղակում մնացորդով հերթական բաժանումը կատարելուց հետո ստացված արդյունքը բազմապատկել այնպիսի արտադրիչով, որը կփոքրացնի կոտորակները: Օրինակ՝ կարելի է յուրաքանչյուր քայլից հետո նորմավորել հերթական բազմանդամը:

2.6.22 Օրինակ. Դիտարկենք 2.6.19 օրինակի բազմանդամները, բայց ամեն մի բաժանումից հետո նորմավորենք արդյունքը: $3x^2-7$ բազմանդամը կփոխարինվի $x^2-7/3$-ով: Հաջորդ մնացորդը կլինի $x-3/2$, իսկ վերջին ոչ զրոյական նորմավորված մնացորդը կլինի 1: Ուստի $d(x) = r\cdot \mathrm{pp}\big(ah(x)\big) = 2\cdot \mathrm{pp}(1) = 2$:

2.6.23 Վարժություն. $\mathbb{Z}[x]$ օղակում «կեղծ բաժանումների» միջոցով հաշվել հետեւյալ բազմանդամների ամենամեծ ընդհանուր բաժանարարը:

$$f(x) = 90x^4+330x^3+330x^2+30x-60,\quad g(x) = 40x^3+20x^2+20x:$$

2.6.24 Վարժություն. Հաշվել 2.6.23 վարժության բազմանդամների ամենափոքր ընդհանուր բազմապատիկը $\mathbb{Z}[x]$ օղակում:

2.6.20 ալգորիթմը $\mathbb{Z}[x]$ օղակում ամենամեծ ընդհանուր բաժանարաի հաշվման լավագույն եղանակը չէ. այն կարող է հանգեցնել միջանկյալ արժեքների ուռճացման պրոբլեմին: Հետագայում մենք կծանոթանանք ավելի արդյունավետ մեթոդների հետ (տես 3.4, 3.6 եւ 5.3 պարագրաֆները):

2.7 Ամենամեծ ընդհանուր բաժանարարի աստիճանը

Այժմ անցնենք բազմանդամների ամենամեծ ընդհանուր բաժանարարի աստիճանի ուսումնասիրությանը, որը մեզ պետք կգա ալգորիթմներ կառուցելիս: Տարրական մաթեմատիկայում $\big(f(x),\ g(x)\big)$-ը հաճախ սահմանվում է այսպես. «$f(x)$, $g(x)$ բազմանդամների ամենամեծ ընդհանուր բաժանարարը այդ բազմանդամների առավելագույն աստիճանի ընդհանուր բաժանարարն է»: Մենք արդեն ունենք

օրինակներ, որոնք ցույց են տալիս ընդհանուր օղակների վրա այդ ձեւակերպման ոչ կոռեկտությունը. 2.6.18 դիտողության մեջ բերված $f(x)=12x^2+24x+12$ եւ $g(x)=8x+8$ բազմանդամների ամենամեծ ընդհանուր բաժանարարի աստիճանը 1 է, սակայն $\mathbb{Z}[x]$ օղակում $f(x),\ g(x)$ բազմանդամների $x+1$ բաժանարարը դրանց ամենամեծ ընդհանուր բաժանարարը չէ:

Եթե $f(x),g(x)\in\mathbb{Z}[x]$ բազմանդամները տրված են իրենց (2.21) ներկայացում-ներով, իսկ $h(x)$-ը այդ բազմանդամների որեւէ ընդհանուր բաժանարար է, ապա (2.21) ներկայացումների միակությունից բխում է, որ $h(x)$-ը ունի հետեւյալ (2.19) ներկայացումը

$$h(x)=\sigma\cdot p_1^{\rho_1}\cdots p_n^{\rho_n}\cdot g_1^{\mu_1}(x)\cdots g_m^{\mu_m}(x), \tag{2.23}$$

որտեղ $\sigma=\pm1$, $\rho_i\le\gamma_i=\min\{\alpha_i,\alpha_i'\}$, $\mu_j\le\delta_j=\min\{\beta_j,\beta_j'\}$ $(i=1,\dots,n;\ j=1,\dots,m)$: Պարզ է, որ $\sigma\cdot p_1^{\rho_1}\cdots p_n^{\rho_n}=\operatorname{cont}\big(h(x)\big)$ եւ $g_1^{\mu_1}(x)\cdots g_m^{\mu_m}(x)=\operatorname{pp}\big(h(x)\big)$: Այստեղից բխում է, որ հնարավոր ամենաբարձր աստիճանի $d(x)$ բաժանարարը կստանանք, եթե վերցնենք $\mu_j=\delta_j=\min\{\beta_j,\beta_j'\}$ $(j=1,\dots,m)$, իսկ ρ_i արժեքները $d(x)$-ի աստիճանի վրա չեն ազդում: Այսինքն՝

$$\deg d(x)=\deg[g_1^{\delta_1}(x)\cdots g_m^{\delta_m}(x)]\ =\sum_{t=1,\dots,m}\delta_t\cdot\deg g_t(x):$$

$f(x),\ g(x)$ բազմանդամների հնարավոր բոլոր $h(x)$ ընդհանուր բաժանարարների աստիճանների մաքսիմումն է $\deg\big(f(x),g(x)\big)$, եւ եթե $f(x),g(x)$ բազմանդամների որեւէ $d(x)$ ընդհանուր բաժանարարի աստիճանը հավասար է $\deg\big(f(x),g(x)\big)$-ի, ապա $d(x)$-ը բաժանվում է $\operatorname{pp}\big(d(x)\big)=\operatorname{pp}\big(f(x),g(x)\big)=g_1^{\delta_1}(x)\cdots g_m^{\delta_m}(x)$ արտադրյալի վրա:

Որպեսզի $\deg d(x)=\deg\big(f(x),g(x)\big)$ պայմանին բավարարող $d(x)$ ընդհանուր բաժանարարը լինի $\big(f(x),g(x)\big)$ *ամենամեծ* ընդհանուր բաժանարարը, պետք է, որ $\operatorname{cont}\big(d(x)\big)$-ը բաժանվի $\operatorname{cont}\big(h(x)\big)=\sigma\cdot p_1^{\rho_1}\cdots p_n^{\rho_n}$ բովանդակության վրա: Դա հնարավոր է միայն, երբ $\operatorname{cont}\big(d(x)\big)=\kappa\cdot p_1^{\gamma_1}\cdots p_n^{\gamma_n}$, որտեղ $\kappa=\pm1$, $\gamma_i=\min\{\alpha_i,\alpha_i'\}$ $(i=1,\dots,n)$: Ըստ թվաբանության հիմնական թեորեմի, դա համարժեք է

$$\operatorname{cont}\big(d(x)\big)\approx\Big(\operatorname{cont}\big(f(x)\big),\operatorname{cont}\big(g(x)\big)\Big)$$

պայմանին: Մենք ստացանք.

2.7.1 Լեմմա. *$f(x),g(x)\in\mathbb{Z}[x]$ ոչ զրոյական բազմանդամների $d(x)$ ընդհանուր բաժանարարը նրանց $\big(f(x),g(x)\big)$ ամենամեծ ընդհանուր բաժանարարն է այն եւ միայն այն դեպքում, երբ $d(x)$-ի աստիճանը $f(x),\ g(x)$ բազմանդամների ընդհանուր բաժանարարների աստիճանների մաքսիմումն է, եւ $d(x)$-ի բովանդակությունը ստացված է $f(x),\ g(x)$ բազմանդամների բովանդակությունների ամենամեծ ընդհանուր բաժանարարին.*

$$d(x)=\big(f(x),g(x)\big)\ \Leftrightarrow\ \begin{cases}\deg d(x)=\max\{\deg h(x)\mid f(x),g(x)\vdots h(x)\},\\ \mathrm{cont}\big(d(x)\big)\approx\Big(\mathrm{cont}\big(f(x)\big),\mathrm{cont}\big(g(x)\big)\Big):\end{cases}$$

2.7.2 Օրինակ. Եթե 2.6.18 դիտողության $f(x)=12x^2+24x+12$ եւ $g(x)=8x+8$ բազմանդամների համար վերցնենք $d(x)=x+1$ ընդհանուր բաժանարարը, ապա 2.7.1 լեմմայի պայմաններից առաջինը, իրոք, կատարվում է. $\deg(x+1)=\max\{\deg h(x)\mid f(x),g(x)\vdots h(x)\}=1$: Սակայն երկրորդ պայմանը չի կատարվում՝ $\mathrm{cont}(x+1)=1$, իսկ այն չի բաժանվում $\Big(\mathrm{cont}\big(f(x)\big),\mathrm{cont}\big(g(x)\big)\Big)=(12,8)=\pm4$ արժեքի վրա: Ուստի $x+1\neq\big(f(x),g(x)\big)$: Մյուս կողմից, եթե վերցնենք $d(x)=4x+4$ կամ $d(x)=-4x-4$ բազմանդամներից որեւէ մեկը, ապա, ըստ 2.7.1 լեմմայի, $d(x)=\big(f(x),g(x)\big)$, քանի որ $\deg d(x)=1$ եւ նաեւ $\mathrm{cont}\big(d(x)\big)\approx4=(12,8)$:

2.7.1 լեմման առանձնապես պարզ տեսք ունի պրիմիտիվ բազմանդամների դեպքի համար.

2.7.3 Լեմմա. *$f(x),g(x)\in\mathbb{Z}[x]$ պրիմիտիվ բազմանդամների $d(x)$ ընդհանուր բաժանարարը նրանց $\big(f(x),g(x)\big)$ ամենամեծ ընդհանուր բաժանարարն է այն եւ միայն այն դեպքում, երբ $d(x)$-ի աստիճանը $f(x)$, $g(x)$ բազմանդամների ընդհանուր բաժանարարների աստիճանների մաքսիմումն է, եւ $d(x)$-ը նույնպես պրիմիտիվ է.*

$$d(x)=\big(f(x),g(x)\big)\ \Leftrightarrow\ \begin{cases}\deg d(x)=\max\{\deg h(x)\mid f(x),g(x)\vdots h(x)\},\\ \mathrm{cont}\big(d(x)\big)\approx1:\end{cases}$$

Հետագա ալգորիթմներում ավելի հաճախ անհրաժեշտ է լինելու 2.7.1 լեմմայի հենց այս 2.7.3 մասնավոր դեպքը: Հնարավոր է ստանալ 2.7.1 լեմմայի անալոգը նաեւ $\mathbb{Q}[x]$ օղակի համար: 2.6.13 թեորեմը վերաբերում էր միայն $\mathbb{Z}[x]$ օղակին, եւ այն $\mathbb{Q}[x]$-ում ուղղակիորեն կիրառել հնարավոր չէ:

Վերցնենք $f(x)$, $g(x)$, $h(x)\in\mathbb{Q}[x]$ եւ ենթադրենք $f(x)$, $g(x)\vdots h(x)$: Այսինքն՝ գոյություն ունեն $q_1(x)$, $q_2(x)\in\mathbb{Q}[x]$, որոնց համար $f(x)=h(x)q_1(x)$ եւ $g(x)=h(x)q_2(x)$: Այս հավասարությունները բազմապատկելով որեւէ ամբողջ թվով (օրինակ՝ $f(x)$, $h(x)$, $q_1(x)$, $q_2(x)$ բազմանդամների բոլոր գործակիցների հայտարարների ամենափոքր ընդհանուր բազմապատիկով)՝ կստանանք հավասարություններ ամբողջ գործակիցներով բազմանդամների միջեւ: Այսինքն՝ $f(x)$, $g(x)\vdots h(x)$ բաժանումները $\mathbb{Q}[x]$-ում կատարվում են այն եւ միայն այն դեպքում, երբ որեւէ c ամբողջ թվի համար $cf(x)\vdots ch(x)$ եւ $cg(x)\vdots ch(x)$ բաժանումները կատարվում են $\mathbb{Z}[x]$-ում: $cf(x)$, $cg(x)$, $ch(x)$ բազմանդամների վրա կիրառենք 2.6.13 թեորեմը եւ ստանանք դրանց (2.19) ներկայացումները.

$$cf(x)=\nu\cdot p_1^{\alpha_1}\cdots p_n^{\alpha_n}\cdot g_1^{\beta_1}(x)\cdots g_m^{\beta_m}(x),$$
$$cg(x)=\nu'\cdot p_1^{\alpha'_1}\cdots p_n^{\alpha'_n}\cdot g_1^{\beta'_1}(x)\cdots g_m^{\beta'_m}(x),$$
$$ch(x)=\sigma\cdot p_1^{\rho_1}\cdots p_n^{\rho_n}\cdot g_1^{\mu_1}(x)\cdots g_m^{\mu_m}(x),$$

որտեղ, կրկին ըստ (2.19) ներկայացման միակության, ունենք $\rho_i \le \gamma_i = \min\{\alpha_i, \alpha_i'\}$, $\mu_j \le \delta_j = \min\{\beta_j, \beta_j'\}$ $(i = 1, \dots, n;\ j = 1, \dots, m)$:

Քանի որ c ոչ զրոյական հաստատունով բազմապատկելը չի փոխում բազմանդամների աստիճանը, ապա այս դեպքում եւս $ch(x)$ բազմանդամը $cf(x)$ եւ $cg(x)$ բազմանդամների ամենամեծ ընդհանուր բաժանարար լինելու համար անհրաժեշտ է, որ $\mu_j = \delta_j$ $(j = 1, \dots, m)$: Այսինքն՝ անհրաժեշտ է, որ $ch(x)$-ի աստիճանը հավասար լինի $\mathbb{Z}[x]$-ում $cf(x)$ եւ $cg(x)$ բազմանդամների ընդհանուր բաժանարարների աստիճանների մաքսիմումին: Անհրաժեշտության դեպքում c-ն մեծացնելով՝ կարող ենք պնդել, որ այդ մաքսիմումը հավասար է $\mathbb{Q}[x]$-ում $f(x)$ եւ $g(x)$ բազմանդամների բոլոր ընդհանուր բաժանարարների աստիճանների մաքսիմումին:

Անցնենք բովանդակությունների գնահատմանը: Քանի որ $\mathbb{Q}$ դաշտում յուրաքանչյուր ոչ զրոյական թիվ հակադարձելի է, ապա դրանով բազմապատկումը չի փոխում բազմանդամների բաժանելիությունը $\mathbb{Q}[x]$ օղակում: Այսինքն՝ վերն օգտագործված

$$c, \operatorname{cont}\big(cf(x)\big) = \nu \cdot\ p_1^{\alpha_1} \cdots p_n^{\alpha_n},\ \operatorname{cont}\big(cg(x)\big) = \nu' \cdot\ p_1^{\alpha_1'} \cdots p_n^{\alpha_n'}$$

եւ

$$\operatorname{cont}\big(ch(x)\big) = \sigma \cdot p_1^{\rho_1} \cdots p_n^{\rho_n}$$

հաստատուն արտադրիչները, $\mathbb{Q}[x]$ օղակ անցում կատարելուց հետո, այլեւս չեն ազդում բաժանելիության վրա.

2.7.4 Լեմմա. *$f(x),\ g(x) \in \mathbb{Q}[x]$ ոչ զրոյական բազմանդամների $d(x)$ ընդհանուր բաժանարարը նրանց $\big(f(x), g(x)\big)$ ամենամեծ ընդհանուր բաժանարարն է այն եւ միայն այն դեպքում, երբ $d(x)$-ի աստիճանը $f(x)$, $g(x)$ բազմանդամների ընդհանուր բաժանարարների աստիճանների մաքսիմումն է.*

$$d(x) = \big(f(x), g(x)\big) \ \Leftrightarrow\ \deg d(x) = \max\{\deg h(x) \mid f(x), g(x) \vdots h(x)\}:$$

Այսպիսով, $\mathbb{Q}[x]$ օղակում ամենամեծ ընդհանուր բաժանարարի սահմանումը (հակադարձելի արտադրիչի ճշտությամբ) համընկնում է տարրական մաթեմատիկայում տրվող ամենամեծ ընդհանուր բաժանարարի սահմանմանը, որը հիշատակեցինք վերը: Մենք 2.7.4 լեմման բխեցրինք 2.7.1 լեմմայից, որը $\mathbb{Z}[x]$ ոչ Էվկլիդյան օղակում Գաուսի լեմմայի մի կիրառություն էր: Կարելի ստանալ նաեւ 2.7.4 լեմմայի ընդհանրացումը ցանկացած K դաշտի վրա տրված $K[x]$ օղակի համար՝ օգտվելով Էվկլիդյան օղակների հատկություններից եւ 2.6.13 թեորեմի անալոգից:

2.7.5 Թեորեմ. *Ցանկացած K դաշտի վրա տրված $K[x]$ օղակի կամայական ոչ զրոյական $f(x)$ բազմանդամ կարելի է ներկայացնել հետեւյալ տեսքով.*

$$f(x) = \varepsilon \cdot g_1(x) \cdots g_s(x), \tag{2.24}$$

որտեղ $\varepsilon \in K^* = K \setminus \{0\}$, *իսկ* $g_1(x), \dots, g_s(x)$ *տարրերը 0-ից բարձր աստիճանի պարզ բազմանդամներ են: Ընդ որում, (2.24) ներկայացումը միակն է այն իմաստով, որ եթե գոյություն ունի* $f(x)$ *բազմանդամի նման մի այլ ներկայացում եւս՝*

$$f(x) = \epsilon \cdot h_1(x) \cdots h_r(x), \tag{2.25}$$

ապա $s = r$ *եւ (միգուցե արտադրիչների որոշ վերադասավորությունից հետո) տեղի ունեն.* $g_i(x) \approx h_i(x)$ $(i = 1, \dots, s)$:

Ապացույց: Նախ, ոչ զրոյական $f(x) \in K[x]$ բազմանդամի համար ստանանք (2.24) տեսքի ֆակտորիզացիայի գոյությունը: Եթե $f(x)$-ն ինքը պարզ չէ եւ հաստատուն չէ (բոլոր հաստատուն ոչ զրոյական բազմանդամները K-ում հակադարձելի տարրեր են), ապա այն կարելի է ներկայացնել երկու՝ ավելի ցածր աստիճանի բազմանդամների արտադրյալի միջոցով: Եթե դրանցից որեւէ մեկը նույնպես պարզ չէ, ապա այն նույնպես կարելի է տրոհել: Վերջավոր քայլերից հետո կստանանք (2.24) տեսքի ներկայացումը, որտեղ $g_i(x)$ բազմանդամները պարզ են եւ ε-ը կարելի է համարել 1: Եթե կա նաեւ (2.25) ներկայացումը, ապա 2.5.12 հետեւանքի օգնությամբ հեշտ է ստանալ, որ $h_1(x)$ պարզ արտադրիչը մասնակցում է առաջին ներկայացման մեջ եւս: Հեռացնելով այն երկու ներկայացումներից եւ կրկնելով քայլը՝ մենք կստանանք որոնելի միակությունը: ■

(2.24) ֆակտորիզացիայի մեջ կատարելով նման անդամների միացում՝ կստանանք (2.19) ներկայացման անալոգը $K[x]$ օղակում.

$$f(x) = \nu \cdot g_1^{\beta_1}(x) \cdots g_m^{\beta_m}(x): \tag{2.26}$$

Իսկ սրանից հեշտ է բխեցնել 2.7.1 եւ 2.7.4 լեմմաների անալոգը.

2.7.6 Լեմմա. *Յանկացած* K *դաշտի վրա տրված* $K[x]$ *օղակի կամայական* $f(x)$, $g(x)$ *ոչ զրոյական բազմանդամների* $d(x)$ *ընդհանուր բաժանարարը նրանց* $\big(f(x), g(x)\big)$ *ամենամեծ ընդհանուր բաժանարարն է այն եւ միայն այն դեպքում, երբ* $d(x)$*-ի աստիճանը* $f(x)$, $g(x)$ *բազմանդամների ընդհանուր բաժանարարների աստիճանների մաքսիմումն է.*

$$d(x) = \big(f(x), g(x)\big) \;\Leftrightarrow\; \deg d(x) = \max\{\deg h(x) \mid f(x), g(x) \vdots h(x)\}:$$

Այստեղ, վերցնելով $K = \mathbb{Q}$, ստանում ենք 2.7.4 լեմման: Իսկ $K = \mathbb{Z}_p[x]$ դեպքը հետագայում մի քանի անգամ կօգտագործվի մոդուլյար ալգորիթմներում:

3 Թվային գնահատականներ օղակների վրա

3.1 Լանդաու-Մինյոտի գնահատականները

Այս գլխում մենք համադրելու ենք էվկլիդյան օղակների եւ Գաուսի լեմմայի օգնությամբ ստացված հանրահաշվական տեսական կառուցվածքները տարբեր թվային գնահատականների հետ (Լանդաու-Մինյոտի գնահատականներ, ռեզուլտանտի արժեքներ, Ադամարի բանաձեւ եւլն): Այդ համադրությունների միջոցով կառուցելու ենք բազմանդամների պարզ բաժանարարների կառուցման, ամենամեծ ընդհանուր բաժանարարի հաշվման, փոխադարձ պարզության որոշման եւ այլ ալգորիթմներ:

Ներկա պարագրաֆի նպատակն է ստանալ տրված բազմանդամի բոլոր հնարավոր բաժանարարների բոլոր գործակիցների գնահատման բանաձեւեր, որոնք տեխնիկական նշանակություն են ունենալու հետագա մի շարք ալգորիթմների կառուցման համար:

Ենթադրենք տրված են $f(x),\ g(x) \in \mathbb{Z}[x]$ բազմանդամները, ընդ որում, $g(x)$-ը $f(x)$-ի բաժանարար է՝ $f(x) = g(x)h(x)$: Այդ դեպքում $f(x)$ բազմանդամի գործակիցները ստացվում են $g(x)$ եւ $h(x)$ բազմանդամների համապատասխան գործակիցների արտադրյալների գումարի տեսքով: Մասնավորապես, $f(x)$-ի ավագ գործակիցը $g(x)$ եւ $h(x)$ բազմանդամների ավագ գործակիցների արտադրյալն է, եւ, ուստի, բացարձակ արժեքով մեծ կամ հավասար է նրանցից երկուսից էլ: Սրանից սակայն չի բխում, թե $g(x)$-ը չի կարող ունենալ $f(x)$-ի բոլոր գործակիցներին գերազանցող որեւէ գործակից:

3.1.1 Օրինակ. $f(x) = x^4 + x^3 + x + 1$ բազմանդամի բոլոր գործակիցները հավասար են 1-ի, սակայն $f(x)$-ը ունի $g(x) = (x+1)^2 = x^2 + 2x + 1$ բաժանարարը, որի երկրորդ գործակիցը 2 է:

3.1.2 Վարժություն. Նույն օրինաչափությունը նկատել հետեւյալ բազմանդամներում եւս.

$f(x) = x^3 + x^2 - x - 1$ եւ $g(x) = (x+1)^2$:
$f(x) = x^5 + 3x^4 + 2x^3 - 2x^2 - 3x - 1$ եւ $g(x) = (x+1)^4$:
$f(x) = x^6 + 3x^5 + 3x^4 + 2x^3 + 3x^2 + 3x + 1$ եւ $g(x) = (x+1)^4$:

3.1.3 Օրինակ. Մասնավորապես, $f(x) = x^4 + x^3 + x + 1$ եւ $g(x) = x^3 + x^2 - x - 1$ բազմանդամներն ունեն ընդհանուր $d(x) = x^2 + 2x + 1$ բաժանարարը, որի մի գործակիցը երկու անգամ գերազանցում է $f(x)$ եւ $g(x)$ բազմանդամների բոլոր գործակիցների մոդուլները:

3.1.4 Օրինակ. Էլ ավելի անսպասելի օրինակ կարելի է կառուցել *ցիկլոտոմիկ բազմանդամների* միջոցով: n-րդ $\phi_n(x)$ ցիկլոտոմիկ բազմանդամն այն միակ պարզ բազմանդամն է $\mathbb{Z}[x]$-ում, որը բաժանում է $x^n - 1$ բազմանդամը, բայց չի բաժանում $x^k - 1$ բազմանդամը, եթե $k < n$: Պարզ է, որ.

$\phi_1(x) = x - 1$,
$\phi_2(x) = x + 1$ (քանի որ $x^2 - 1 = (x+1)(x-1)$),
$\phi_3(x) = x^2 + x + 1$,
$\phi_4(x) = x^2 + 1$,
$\phi_5(x) = x^4 + x^3 + x^2 + x + 1$
եւ այլն...

Ցիկլոտոմիկ բազմանդամի ընդհանուր բանաձեւն է.

$$\phi_n(x) = \prod_{\substack{k=1,\dots,n \\ (k,n)=1}} \left(x - e^{\frac{2i\pi k}{n}}\right):$$

Մինչեւ $n = 104$ արժեքը բոլոր ցիկլոտոմիկ բազմանդամների բոլոր գործակիցները բացարձակ արժեքով չեն գերազանցում 1-ը: Բայց $n = 105$ թիվը առաջին բնական թիվն է, որը կարելի է ներկայացնել իրարից տարբեր երեք կենտ պարզ թվերի արտադրյալի տեսքով. $105 = 3 \cdot 5 \cdot 7$:

$$\begin{aligned}\phi_{105}(x) = {} & x^{48} + x^{47} + x^{46} - x^{43} - x^{42} - 2x^{41} - x^{40} - x^{39} + x^{36} + x^{35} + x^{34} + x^{33} \\ & + x^{32} + x^{31} - x^{28} - x^{26} - x^{24} - x^{22} - x^{20} + x^{17} + x^{16} + x^{15} + x^{14} + x^{13} \\ & + x^{12} - x^9 - x^8 - 2x^7 - x^6 - x^5 + x^2 + x + 1:\end{aligned}$$

Նկատում ենք, որ $\phi_{105}(x)$ բազմանդամն ունի անդամներ, որոնց գործակիցները -2 են: Մյուս կողմից, $\phi_{105}(x)$-ը բաժանարար է $x^{105} - 1$ բազմանդամի համար, իսկ վերջինիս միակ գործակիցներն են՝ $-1,\ 1$:

3.1.5 Դիտողություն. Առանց ապացույցի նշենք այն կարեւոր փաստը, որ ցիկլոտոմիկ բազմանդամների գործակիցները անվերջորեն աճում են: Այսինքն՝ կամայական մեծ M թվի համար կա մի k բնական թիվ այնպիսին, որ x^k-1 բազմանդամի բաժանարար հանդիսացող $\phi_k(x)$ ցիկլոտոմիկ բազմանդամի գործակիցներից որեւէ մեկը մոդուլով գերազանցում է M-ը:

Տրված $f(x)$ բազմանդամի բոլոր հնարավոր բաժանարարների բոլոր գործակիցները բացարձակ արժեքով սահմանափակ են, եւ Լանդաու-Մինյոտի բանաձեւը հնարավորություն է տալիս գնահատելու դրանք:

3.1.6 Թեորեմ (Լանդաու-Մինյոտի բանաձեւը). *Ենթադրենք $\mathbb{Z}[x]$ բազմանդամային օղակում տրված է $f(x)=a_0x^n+\cdots+a_n$ բազմանդամը եւ նրա կամայական $g(x)=b_0x^m+\cdots+b_m$ բաժանարարը: Այդ դեպքում տեղի ունի հետեւյալ առնչությունը.*

$$\sum_{i=0}^{m}|b_i|\le 2^m\left|\frac{b_0}{a_0}\right|\sqrt{\sum_{i=0}^{n}a_i^2}:$$

Թեորեմի ապացույցը կբերենք քիչ հետո: Գրառումները կարճացնելու համար նշենք, որ ընդհանրապես $\|f(x)\|=\sqrt{\sum_{i=0}^{n}a_i^2}$ բանաձեւով (ոչ միայն $\mathbb{Z}[x]$ օղակի տարրերի, այլ կամայական բազմանդամների համար) ընդունված է սահմանել *բազմանդամային մետրիկան* (բազմանդամների գծային տարածության մեջ բազմանդամի նորմը կամ երկարությունը): Ըստ այդմ՝ թեորեմի անհավասարությունը կարելի է ներկայացնել

$$\sum_{i=0}^{m}|b_i|\le 2^m\left|\frac{b_0}{a_0}\right|\|f(x)\| \tag{3.1}$$

տեսքով: Տրված $f(x)$ բազմանդամի համար այն, իրոք, թույլ է տալիս վերին գնահատական հաշվել նրա կամայական $g(x)$ բաժանարարի ցանկացած b_i գործակցի մոդուլի համար, եթե անգամ $g(x)$-ի տեսքի մասին մեզ ոչինչ հայտնի չէ (մասնավորապես, եթե հայտնի չեն բանաձեւում օգտագործված m եւ b_0 արժեքները): Իրոք, $|b_i|\le\sum_{i=0}^{m}|b_i|$, իսկ աջ մասում՝ $2^m\le 2^n$ եւ $\left|\frac{b_0}{a_0}\right|\le 1$, քանի որ կոտորակի համարիչը հայտարարի բաժանարարն է: Այսինքն՝ $|b_i|\le 2^n\|f(x)\|$: Այս գնահատականը կարելի է բարելավել: Իրոք, եթե $f(x)$ բազմանդամի $g(x)$ բաժանարարի աստիճանը $n-1$ է, ապա

$$|b_i| \le \sum_{i=0}^{n-1} |b_i| \le 2^{n-1} \left|\frac{b_0}{a_0}\right| \|f(x)\| \le 2^{n-1}\|f(x)\|:$$

Այսինքն՝ $|b_i| \le 2^{n-1}\|f(x)\|$ գնահատականը ճիշտ է $f(x)$ բազմանդամի բոլոր այն բաժանարարների համար, որոնց աստիճանը չի գերազանցում $n-1$ թիվը:

Մյուս կողմից, եթե $f(x)$-ի $g(x)$ բաժանարարի աստիճանը n է, ապա $g(x)$-ը կամ հավասար է $f(x)$-ին, կամ էլ ստացվում է $f(x)$-ը որեւէ ոչ զրոյական ամբողջ թվի վրա բաժանելիս: Երկու դեպքերում էլ $g(x)$-ի b_i գործակիցները բացարձակ արժեքով չեն գերազանցում $\max\{|a_i| \mid i = 0, \dots, n\}$ մաքսիմումը: Հեշտ է տեսնել, որ

$$|b_i| \le \max\{|a_i| \mid i = 0, \dots, n\} \le \sqrt{\sum_{i=0}^{n} a_i^2} = \|f(x)\|:$$

Ուրեմն՝ քիչ առաջ ստացած գնահատականը ճիշտ է $f(x)$-ի *բոլոր* բաժանարարների բոլոր գործակիցների համար: Հետագայում այն մեզ պետք է գալու ալգորիթմական կառուցումներում, ուստի ապագա հղումների համար նշանակենք

$$N_f = 2^{n-1}\|f(x)\|: \tag{3.2}$$

Ձեւակերպենք ստացված փաստը որպես.

3.1.7 Հետեւանք. $\mathbb{Z}[x]$ օղակի $f(x) = a_0x^n + \dots + a_n$ բազմանդամի կամայական $g(x) = b_0x^m + \dots + b_m$ բաժանարարի ցանկացած b_i գործակցի համար $(i = 1, \dots, m)$.

$$|b_i| \le N_f = 2^{n-1}\|f(x)\|:$$

Եթե $\mathbb{Z}[x]$-ում տրված են $f(x)$ եւ $g(x)$ բազմանդամները, իսկ $h(x)$-ը դրանց որեւէ ընդհանուր բաժանարար է, ապա 3.1.7 հետեւանքը երկու անգամ կիրառելով՝ կստանանք.

3.1.8 Հետեւանք. $\mathbb{Z}[x]$ օղակի $f(x) = a_0x^n + \dots + a_n$ եւ $g(x) = b_0x^m + \dots + b_m$ բազմանդամների կամայական $h(x) = c_0x^k + \dots + c_k$ ընդհանուր բաժանարարի ցանկացած c_i գործակցի համար $(i = 1, \dots, k)$.

$$|c_i| \le \min\{N_f, N_g\} = \min\{2^{n-1}\|f(x)\|,\ 2^{m-1}\|g(x)\|\}:$$

3.1.8 հետեւանքի գնահատականը կարելի է բարելավել.

3.1.9 Հետեւանք. $\mathbb{Z}[x]$ օղակի $f(x) = a_0x^n + \dots + a_n$ եւ $g(x) = b_0x^m + \dots + b_m$ բազմանդամների կամայական $h(x) = c_0x^k + \dots + c_k$ ընդհանուր բաժանարարի ցանկացած c_i գործակցի համար $(i = 1, \dots, k)$.

$$|c_i| \le N_{f,g} = 2^{\min\{n,m\}}(a_0, b_0) \min\left\{\frac{\|f(x)\|}{|a_0|}, \frac{\|g(x)\|}{|b_0|}\right\}: \tag{3.3}$$

Ապացույց: (3.1) բանաձեւը նախ կիրառենք $f(x)$, $h(x)$ զույգի, ապա $g(x)$, $h(x)$ զույգի համար: Պարզ է, որ $k \le \min\{n,m\}$: Մյուս կողմից, քանի որ c_0-ն բաժանում է $a_0,\ b_0$ ավագ գործակիցները, այն բաժանում է եւ դրանց (a_0,b_0) ամենամեծ ընդհանուր բաժանարարը: Ուստի $\left|\frac{c_0}{a_0}\right|$ եւ $\left|\frac{c_0}{b_0}\right|$ կարելի է վերեւից գնահատել $\left|\frac{(a_0,b_0)}{a_0}\right|$ եւ $\left|\frac{(a_0,b_0)}{b_0}\right|$ արժեքներով: ■

3.1.10 Վարժություն. Հաշվել N_f գնահատականը 3.1.1 օրինակի եւ 3.1.2 վարժության բազմանդամների համար:

3.1.11 Վարժություն. (3.3) բանաձեւով հաշվել $N_{f,g}$ գնահատականը $f(x)=x^5+3x^4+2x^3-2x^2-3x-1$ եւ $(x)=x^3+x^2-x-1$ բազմանդամների զույգի համար:

3.1.12 Վարժություն. (3.2) բանաձեւով հաշվել N_{ϕ_i} գնահատականը առաջին հինգ ցիկլոտոմիկ բազմանդամների համար:

3.1.13 Խնդիր. Գտնել դեպքեր, երբ 3.1.9 հետեւանքի գնահատականն ավելի ստույգ է, քան 3.1.8 հետեւանքի գնահատականը: *Յուցում.* գտնել $f(x)$ եւ $g(x)$ բազմանդամների օրինակ, որոնց համար 3.1.9 հետեւանքի գնահատականը բացարձակ արժեքով ավելի փոքր է:

3.1.6 թեորեմի ապացույցը: Այս ապացույցը ստորեւ կառուցվելիք ալգորիթմներում մեզ պետք չի գալու. մենք այն բերում ենք միայն շարադրանքի ամբողջականության համար:

Նախ, հեշտ է ստուգել, որ կամայական $z\in\mathbb{C}$ կոմպլեքս թվի համար տեղի ունի

$$\|(x-z)f(x)\| = \|(\bar{z}x-1)f(x)\| \tag{3.4}$$

հավասարությունը (ապացուցելու համար բավական է հավասարության երկու կողմերն էլ քառակուսի բարձրացնել):

Ենթադրենք $f(x)$ բազմանդամի բոլոր արմատներն են $z_1,\dots,z_n$ կոմպլեքս թվերը՝ $f(x)=a_0\prod_{i=1}^{n}(x-z_i)$: Նշանակենք.

$$M(f)=|a_0|\prod_{i=1}^{n}\max\{1,|z_i|\}:$$

Ցույց տանք, որ $M(f)\le\|f(x)\|$: Համարենք, որ $z_1,\dots,z_n$ կոմպլեքս արմատներից առաջին k հատն են, որ մոդուլով մեծ են 1-ից: Այդ դեպքում $M(f)=|a_0z_1\cdots z_k|$: Վերցնենք հետեւյալ օժանդակ բազմանդամը.

$$t(x) = a_0 \prod_{i=1}^{k} (\overline{z_i}x - 1) \prod_{i=k+1}^{n} (x - z_i) \in \mathbb{C}[x],$$

եւ ենթադրենք c_0-ն նրա ավագ գործակիցն է: Այդ դեպքում

$$M(f)^2 = |a_0 z_1 \cdots z_k|^2 = |a_0 \overline{z_1} \cdots \overline{z_k}|^2 = c_0^2$$

(վերջին հավասարությունը ստացվում է վերեւի $a_0 \prod_{i=1}^{k} (\overline{z_i}x - 1)$ արտահայտության մեջ փակագծերի բացում կատարելով): Մյուս կողմից, $c_0^2 \le \|t(x)\|^2$: Մնում է $t(x)$ բազմանդամի վրա k անգամ կիրառելով (3.4) բանաձեւը՝ ստանալ

$$\left\| a_0 \prod_{i=1}^{k} (\overline{z_i}x - 1) \prod_{i=k+1}^{n} (x - z_i) \right\| = \left\| a_0 \prod_{i=1}^{n} (x - z_i) \right\| = \|f(x)\|:$$

Այսպիսով. $M(f)^2 = c_0^2 \le \|t(x)\|^2 = \|f(x)\|^2$, եւ $M(f) \le \|f(x)\|$ անհավասարությունն ապացուցված է: $g(x) = b_0 x^m + \cdots + b_m$ բաժանարարի համար նույնպես դիտարկենք համապատասխան $M(g)$-ն: Դժվար չէ Վիետի բանաձեւերի օգնությամբ ստանալ $|b_i| \le \binom{m}{i} M(g)$, որտեղից եւ՝

$$\sum_{i=0}^{m} |b_i| \le M(g) \sum_{i=0}^{m} \binom{m}{i} = M(g) 2^m:$$

Քանի որ $g(x)$ բազմանդամի ամեն մի լուծում արմատ է նաեւ $f(x)$ բազմանդամի համար, ապա $M(g) \le |a_0/b_0| M(f)$, որտեղից եւ.

$$\sum_{i=0}^{m} |b_i| \le M(g) 2^m \le 2^m \left|\frac{a_0}{b_0}\right| M(f) \le 2^m \left|\frac{a_0}{b_0}\right| \|f(x)\|:$$

Թեորեմն ապացուցված է: ■

3.1.14 Խնդիր. Վիետի բանաձեւերի օգնությամբ ստանալ նախորդ ապացույցի վերջում օգտագործված $|b_i| \le \binom{m}{i} M(g)$ անհավասարությունը:

3.2 Գործակիցների գնահատականի պարզագույն կիրառությունները

Սկսենք Լանդաու-Մինյոտի բանաձեւի միջոցով բազմանդամների բաժանելիության վերաբերյալ ոչ բարդ ալգորիթմներից: Այդ ալգորիթմները առայժմ շատ անկատար կլինեն այն առումով, որ դրանցում չափազանց շատ քայլեր պիտի կատարել որոնելի պատասխանը գտնելու համար: Մենք հետագայում դրանք կփոխարինենք անհամեմատ ավելի արագ աշխատող ալգորիթմներով, իսկ հետեւյալ ալգորիթմնե-

րը բերում ենք միայն որպես Լանդաու-Մինյոտի բանաձեւի պարզ կիրառությունների օրինակներ:

Տրված $f(x) \in R[x]$ բազմանդամի $p(x)$ *պարզ բաժանարարի պատիկություն* է կոչվում այն $\alpha \in \mathbb{N}$ բնական աստիճանը, որի համար $p^{\alpha}(x) \mid f(x)$, բայց $p^{\alpha+1}(x) \nmid f(x)$: Երբեմն բաժանարարի պատիկություն հասկացությունը ներմուծվում է նաեւ ոչ անպայման պարզ բաժանարարների համար: Երբեմն էլ $\mathbb{N}$-ը փոխարինում են $\mathbb{N} \cup \{0\}$ բազմությամբ եւ համարում, որ $p(x)$-ը $f(x)$-ի *զրոյական* պատիկության բաժանարար է, եթե $p(x) \nmid f(x)$:

Ըստ 3.1.7 հետեւանքի, տրված $f(x) = a_0x^n + \cdots + a_n \in \mathbb{Z}[x]$ բազմանդամի բաժանարարն ունի $g(x) = b_0x^k + \cdots + b_k$ տեսքը, որտեղ $k \le n$ եւ $|b_i| \le N_f = 2^{n-1}\|f(x)\|$: Տրված k-ի համար այդ պայմանին բավարարող բոլոր հնարավոր գումարներն ընդամենը վերջավոր հատ են, եւ դրանց քանակն է $2N_f\big(2N_f+1\big)^k$:

3.2.1 Վարժություն. Ստուգել, որ $f(x) \in \mathbb{Z}[x]$ բազմանդամի k-րդ աստիճանի բոլոր բաժանարարների քանակությունը չի գերազանցում $2N_f\big(2N_f+1\big)^k$ թիվը:

Բազմանդամների ցանկերի կարգավորման համար մեզ պետք կգա բազմանդամների վրա սահմանված որեւէ գծային կարգի հարաբերություն: Տրված այբուբենի վրա սահմանված բառերի (տառերի վերջավոր հաջորդականությունների) կարգավորման հայտնի *աստիճանային լեքսիկոգրաֆիական* սկզբունքը կարելի է տարածել եւ բազմանդամների վրա: $g(x) = b_0x^k + \cdots + b_k$ եւ $h(x) = c_0x^m + \cdots + b_m$ բազմանդամների համար սահմանենք $g(x) < h(x)$ այն եւ միայն այն դեպքում, երբ $k < m$ կամ $k = m$ եւ $g(x) - h(x)$ տարբերության ավագ անդամը բացասական է: Ինչպես կտեսնենք հետագայում 8.2 պարագրաֆում, սա $grlex$ մոնոմիալ կարգավորվածության մասնավոր դեպքն է: Մենք կարող էինք ստորեւ բերվող շարադրանքը մի փոքր կարճացնել՝ օգտվելով $grlex$-ի տերմինաբանությունից: Սակայն, տեքստն ավելի դյուրընկալելի դարձնելու համար օգտագործում ենք միայն ավանդական տերմինները, առավել եւս, որ մինչեւ 8-րդ գլուխը մեզ որեւէ այլ մոնոմիալ կարգավորվածություն չի հանդիպելու:

Աստիճանային լեքսիկոգրաֆիական սկզբունքը նշանակում է, որ մենք նախ համեմատում ենք բազմանդամների աստիճանները (եւ մեծ համարում ավելի բարձր աստիճանի բազմանդամը), իսկ հավասար աստիճանի բազմանդամները համեմատում ենք ըստ b_i, c_i գործակիցների՝ փնտրելով առաջին գործակիցը, որը միեւնույնը չէ երկու բազմանդամներում էլ: Մոնոմիալ կարգավորման տեսակներին ավելի մանրամասնորեն կանդրադառնանք 8.2 պարագրաֆում:

3.2.2 Վարժություն. Ստուգել, որ $\mathbb{Z}[x]$-ի վրա մեր սահմանած կարգավորվածությունը *գծային* է, այսինքն, կամայական $g(x), h(x), f(x) \in \mathbb{Z}[x]$ բազմանդամների համար տեղի ունեն հետեւյալ պայմանները.

1) $g(x) \le h(x)$ կամ $h(x) \le g(x)$,

2) եթե $g(x) \le h(x)$ եւ $h(x) \le g(x)$, ապա $g(x) = h(x)$,

3) եթե $g(x) \le h(x)$ եւ $h(x) \le g(x)$, ապա $g(x) \le f(x)$:

Վերհիշենք, որ նախորդ գլխում ոչ զրոյական բազմանամի *ֆակտորիզացիա* անվանեցինք նրա (2.17) ներկայացումը իր պարզ արտադրիչների արտադրյալի տեսքով: «Նման անդամների միացման» միջոցով կարելի է ֆակտորիզացիան բերել (2.19) տեսքին: Հասկանալի է, որ (2.19) ֆակտորիզացիան ունեցող $f(x)$ բազմանդամի p_i պարզ արտադրիչի պատիկությունն է α_i, իսկ $g_j(x)$ պարզ արտադրիչի պատիկությունն է β_j, որտեղ $i = 1, \dots, n$ եւ $j = 1, \dots, m$: Բազմանդամի ֆակտորիզացիան գտնելը համարժեք է նրա բոլոր պարզ արտադրիչների $\mathcal{P}$ ցանկի (հաջորդականության) ստացմանը, ընդ որում, յուրաքանչյուր արտադրիչ նշված է այնքան անգամ, որքան իր պատիկությունն է: Ընդ որում, $\mathcal{P}$-ն անվանում ենք ոչ թե բազմություն, այլ ցանկ, քանի որ բազմությունները չեն կարող պարունակել կրկնվող տարրեր:

Ունենալով բազմանդամների ֆակտորիզացիան՝ կարող ենք լուծել դրանց հետ կապված տարբեր խնդիրներ. գտնել բազմանդամների ամենամեծ ընդհանուր բաժանարարը, ամենափոքր ընդհանուր բազմապատիկը, լուծել բազմանդամի պարզության հարցը, հաշվել դրա արմատները եւլն: Որպես Լանդաու-Մինյոտի բանաձեւի պարզագույն կիրառություն՝ ձեւակերպենք բազմանդամի ֆակտորիզացիայի մի ալգորիթմ.

3.2.3 Ալգորիթմ (Լանդաու-Մինյոտի բանաձեւի միջոցով բազմանդամի ֆակտորիզացիան). Տրված է $f(x) \in \mathbb{Z}[x]$ ոչ զրոյական բազմանդամը: Գտնել նրա ֆակտորիզացիան:

1. Նշանակենք $n = \deg f(x)$:

2. Ըստ Լանդաու-Մինյոտի բանաձեւի 3.1.7 հետեւանքի հաշվենք $N_f = 2^{n-1}\|f(x)\|$:

3. Սահմանենք բազմանդամների $\mathcal{P}$ դատարկ ցանկը:

4. $(k = 0;\ k \le n;\ k++)$ արժեքների համար

5. վերցնենք $g(x) = b_0x^k + \dots + b_k$ տեսքի բոլոր $2N_f\big(2N_f+1\big)^k$ հատ ամբողջ գործակիցներով բազմանդամների $\mathcal{G}_k$ բազմությունը, որտեղ $|b_k| \le N_f$ եւ $b_0 \ne 0$;

6. որեւէ եղանակով, օրինակ, աստիճանային լեքսիկոգրաֆիական սկզբունքով կարգավորենք $\mathcal{G}_k$-ն;

7. $\mathcal{P}$ ցանկին ավելացնենք $\mathcal{G}_k$-ն;

8. $\mathcal{G}_k$-ի յուրաքանչյուր $g(x)$ բազմանդամ մնացորդով բաժանենք $\mathcal{P}$ ցանկի մնացած բոլոր բազմանդամների վրա եւ, եթե այդ բաժանումներից գոնե մեկի մնացորդը զրոյական է, $g(x)$-ը դեն նետենք $\mathcal{P}$-ից;

9. Յուրաքանչյուր $g(x) \in \mathcal{P}$ բազմանդամի համար

10. $i = 0$;

11. եթե $f(x) \vdots g^{i+1}(x)$

12. նշանակենք $i = i + 1$;

13. վերադառնանք 11-րդ քայլին;

14. եթե $i = 0$

15. $\mathcal{P}$ ցանկից դեն նետենք $g(x)$ բազմանդամը;

16. հակառակ դեպքում

17. $\mathcal{P}$ ցանկում $g(x)$ բազմանդամը փոխարինենք իրեն հավասար i հատ անդամներով;

18. անցնենք $\mathcal{P}$ ցանկի հաջորդ բազմանդամին:

19. Դուրս գրենք $\mathcal{P}$ ցանկի բազմանդամները:

Եթե խմբավորենք պարզ արտադրիչները՝ նախ գրելով պարզ սկալյարները, ապա պարզ պրիմիտիվ բազմանդամները, ապա կստանանք (2.19) վերլուծությունը (տվյալ դեպքում $\nu = 1$): Եթե սկզբնական $f(x) = c \neq 0$ բազմանդամը հաստատուն է, ապա 3.2.3 ալգորիթմի 6-րդ կետում մենք կստանանք c *թվի* վերլուծությունը *պարզ թվերի* աստիճանների (եւ $\nu = 1$ հակադարձելի տարրի) արտադրյալի: Իսկ եթե $c = \pm 1$, ապա կստանանք $f(x) = \nu = \pm 1$ բազմանդամի վերլուծությունը «զրո հատ» պարզ արտադրիչների (տես 2.6.13 թեորեմը եւ (2.19) վերլուծությունը):

Որպես 3.2.3 ալգորիթմի պարզ կիրառություն՝ կարելի է ստանալ տրված $f(x),\ g(x) \in \mathbb{Z}[x]$ բազմանդամների ամենամեծ ընդհանուր բաժանարարը եւ ամենափոքր ընդհանուր բազմապատիկը հաշվելու հասկանալի, բայց շատ աշխատատար եղանակ 2.6.16 հետեւանքի մեթոդով: Տրված $f(x),\ g(x) \in \mathbb{Z}[x]$ ոչ զրոյական բազմանդամներն ըստ 3.2.3 ալգորիթմի կարելի է վերլուծել պարզ արտադրիչների աստիճանների արտադրյալի: Եթե որեւէ $p(x)$ պարզ արտադրիչ բաժանում է այս բազմանդամներից միայն մեկը, ապա այն $p^0(x) = 1$ զրոյական աստիճանով ավելացնենք մյուսի վերլուծությանը: Կարելի է համարել, որ երկու բազմանդամներն

էլ հանդիսանում են պարզ արտադրիչների միեւնույն ցանկի տարրերի որոշ աստիճանների արտադրյալներ, ինչպես (2.21) բանաձեւերում: Այդ դեպքում $\big(f(x), g(x)\big)$-ը կհաշվվի (2.22) բանաձեւով: Վերջապես $[f(x), g(x)] = f(x)g(x)/\big(f(x), g(x)\big)$: Այս լուծման թերությունն ակնհայտ է. մենք կազմում ենք բազմանդամների մի մեծ ցանկ, որի տարրերը պիտի հերթով իրար վրա բաժանել: Հետագայում մենք կստանանք բազմանդամի պարզ արտադրիչների եւ բազմանդամների ամենամեծ ընդհանուր բաժանարարների հաշվման շատ ավելի կատարյալ ալգորիթմներ:

Այժմ անցնենք Լանդաու-Մինյոտի բանաձեւի մի քանի այլ կարեւոր կիրառությունների, որոնք հետագայում օգտագործելու ենք ալգորիթմներում: 2.4 պարագրաֆում մոդուլյար անցման ալգորիթմական կիրառությունները քննարկելիս մենք թվարկեցինք մի քանի տիպական բարդություններ, որոնք առաջանում են մոդուլյար անցման ժամանակ, մասնավորապես, 2.4.1 եւ 2.4.2 հարցերը:

Նախ, դիտարկենք մոդուլյար անցման ժամանակ *գործակիցների պահպանման հարցը* (տես 2.4.1 կետը): Ենթադրենք տրված $f(x)$ բազմանդամի համար մոդուլյար մեթոդներով լուծում ենք բաժանելիության հետ կապված որեւէ խնդիր, օրինակ՝ տվյալ բազմանդամի պարզ արտադրիչների կամ բազմանդամների ամենամեծ ընդհանուր բաժանարարի հաշվման խնդիրը: $\varphi_p\colon \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ մոդուլյար անցումը իզոմորֆիզմ չէ, եւ եթե այդ խնդիրը լուծենք մոդուլյար $f_p(x) = \varphi_p\big(f(x)\big)$ բազմանդամի համար, ապա դրանից հետո միշտ չէ, որ կարող ենք նույն խնդրի լուծումը վերականգնել $f(x) \in \mathbb{Z}[x]$ բազմանդամի համար: Ինչպես տեսանք 2.4.1 կետի օրինակում, $f(x) = 7x^2 + 22$ բազմանդամի համար $f_7(x) = 1$, եւ $f(x)$-ի բաժանարարների մասին φ_7 մոդուլյար անցումից հետո այլեւս որեւէ գործնական ինֆորմացիա չի պահպանվում: Իսկ, ասենք, φ_{11} մոդուլյար անցումից հետո կստանայինք $f_{11}(x) = 7x^2$, որն արդեն վերլուծված է պարզ արտադրիչների, բայց որի պարզ արտադրիչները կապված չեն $f(x)$ բազմանդամի պարզ արտադրիչի հետ (դրա պատկեր չեն հանդիսանում մոդուլյար անցման ժամանակ):

Թվում է, թե այս հարցը կարելի է լուծել այնպիսի մի մեծ p պարզ թիվ վերցնելով, որը գերազանցի $f(x)$-ի բոլոր գործակիցները: Օրինակ՝ եթե $p = 37$, ապա

$$\varphi_{37}\big(f(x)\big) = f_{37}(x) = 7x^2 + 22$$

մոդուլյար բազմանդամն ունի նույն գործակիցները, ինչ $f(x)$-ը, եւ թվում է, թե $f_{37}(x)$-ի բաժանարարները հաշվելով՝ մենք կստանանք նաեւ $f(x)$-ի բաժանարարները: Բայց, ինչպես տեսանք 3.1.1 տարրական օրինակում, $f(x)$ բազմանդամի որեւէ $g(x)$ բաժանարար կարող է ավելի մեծ գործակիցներ ունենալ, քան $f(x)$-ի

գործակիցներն են, եւ մեր ընտրած p պարզ թիվը կարող է փոքր լինել $g(x)$-ի որեւէ գործակցից: 3.1.1 օրինակում դիտարկված $f(x) = x^4 + x^3 + x + 1$ բազմանդամի բոլոր գործակիցները փոքր են $p = 2$ պարզ թվից, եւ φ_2 մոդուլյար անցումը չի փոխում դրանք. $f_2(x) = x^4 + x^3 + x + 1$: Բայց $f(x)$-ը ունի $g(x) = (x+1)^2 = x^2 + 2x + 1$ բաժանարարը, որը փոփոխվում է մոդուլյար անցման ընթացքում՝ $g_2(x) = x^2 + 1$: Այս $g_2(x)$ բազմանդամը $\mathbb{Z}_2[x]$ օղակում, իրոք, բաժանարար է $f_2(x)$-ի համար, բայց $g_2(x)$-ը պատկեր չի հանդիսանում $f(x)$-ի որեւէ բաժանարարի համար:

Լանդաու-Մինյոտի բանաձեւից հետո ստացվող (3.2) գնահատականը՝

$$N_f = 2^{n-1}\|f(x)\|,$$

հնարավորություն է տալիս շրջանցելու այդ բարդությունը: Եթե անգամ $f(x)$ բազմանդամի $g(x)$ բաժանարարներից եւ ոչ մեկը մեզ հայտնի չէ, ապա մեր ալգորիթմում կարող ենք օգտագործել այն փաստը, որ $g(x)$-ի յուրաքանչյուր գործակից բացարձակ արժեքով փոքր է N_f գնահատականից: Ուստի $\varphi_p\colon \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ մոդուլյար անցման ժամանակ $g(x)$-ի գործակիցների մասին ինֆորմացիան պահպանվում է. այդ գործակիցները կամ անփոփոխ են մնում (եթե նրանք բացասական չեն), կամ էլ նրանց p է գումարվում (եթե դրանք բացասական են): Տես նաեւ 3.2.7 լեմման ստորեւ:

3.2.4 Օրինակ. Վերը նշված $f(x) = x^4 + x^3 + x + 1$ բազմանդամի համար

$$N_f = 2^{4-1}\|f(x)\| = 8\sqrt{1^2 + 1^2 + 1^2 + 1^2} = 16:$$

Կարելի է ընտրել $p = 17 > 16$ պարզ թիվը եւ $\varphi_{17}\colon \mathbb{Z}[x] \to \mathbb{Z}_{17}[x]$ մոդուլյար անցումը, որը կպահպանի $f(x)$-ի բոլոր բաժանարարների բոլոր գործակիցները:

3.2.5 Դիտողություն. Այս մեթոդը կարող է ունենալ տարբեր կատարելագործումներ: Օրինակ՝ եթե հաշվում ենք տրված $f(x)$ եւ $g(x)$ բազմանդամների $d(x) = \big(f(x)\,,g(x)\big)$ ամենամեծ ընդհանուր բաժանարարը, ապա, քանի որ $d(x)$-ը բաժանարար է միաժամանակ այդ երկու բազմանդամների համար էլ, կարելի է օգտվել (3.3) բանաձեւի $N_{f,g}$ գնահատականից եւ վերցնել

$$p > N_{f,g}$$

պարզ թիվը: Այդ դեպքում $\big(f_p(x)\,,g_p(x)\big)$ մոդուլյար ամենամեծ ընդհանուր բաժանարարը ավելի շատ օգտակար տեղեկություն է պարունակում $d(x)$-ի մասին, քանի որ $\big(f_p(x)\,,g_p(x)\big)$ բազմանդամում մոդուլյար անցման ժամանակ գործակիցների կրճատում տեղի չի ունեցել: Նկատենք, որ այստեղից դեռ չի հետեւում, որ

$\big(f_p(x)\,,g_p(x)\big)$ բազմանդամը հավասար է $d(x)$-ին: Ավելին՝ $\big(f_p(x)\,,g_p(x)\big)$-ը կարող է անգամ չլինել $d(x)$-ի պատկերը φ_p մոդուլյար անցման ժամանակ, քանի որ, ինչպես տեսանք 2.4.3 կետում, մոդուլյար անցման ժամանակ կարող է խախտվել եւ նախապատկերների բաժանելիությունը (այս հարցին մենք կանդրադառնանք նաեւ 3.4 պարագրաֆում):

Հաջորդ խնդիրը, որը կարելի է լուծել Լանդաու-Մինյոտի բանաձեւով, *միակ նախապատկերի վերականգնման* հարցն է, որին անդրադարձանք 2.4.2 կետում: Քանի որ $\varphi_p\colon \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ մոդուլյար անցումը ոչ մի p մոդուլի համար բիյեկտիվ չէ, ապա եթե մոդուլյար անցումից հետո լուծել ենք բաժանելիության հետ կապված որեւէ խնդիր եւ ստացել, ասենք, $f_p(x)$ բազմանդամի մոդուլյար $h_p(x)$ բաժանարարը, ապա այն $\mathbb{Z}[x]$ օղակում կարող է ունենալ անվերջ քանակությամբ նախապատկերներ (տես 2.4.2 կետը): Այդ նախապատկերներից ո՞րը վերցնենք որպես $h_p(x)$-ի $h(x)$ նախապատկեր:

Եթե այս խնդրում, նախ, $f(x)$-ի համար հաշվենք N_f գնահատականը, ապա φ_p մոդուլյար անցումը կատարենք ըստ որեւէ $p > N_f$ պարզ թվի, ապա

$$h_p(x) = b_{0,p}x^m + \cdots + b_{m,p} \in \mathbb{Z}_p[x]$$

մոդուլյար բաժանարարը կհանդիսանա այնպիսի մի

$$h(x) = b_0x^m + \cdots + b_m \in \mathbb{Z}[x]$$

բազմանդամի պատկերը, որի գործակիցներից ոչ մեկը չի կրճատվել φ_p մոդուլյար անցման ընթացքում: Ըստ N_f գնահատականի ընտրության.

$$b_i \in \{-N_f, -N_f+1, \dots, -1, 0, 1, \dots, N_f-1, N_f\}, \quad i = 0, \dots, m\text{:}$$

Ընդ որում, ոչ բացասական գործակիցներն անփոփոխ են մնում մոդուլյար անցման ընթացքում. $b_{i,p} = \varphi_p(b_i) = b_i$, իսկ բացասական գործակիցները մեծանում են p-ով՝ $b_{i,p} = \varphi_p(b_i) = b_i + p$: Այս $b_i + p$ արժեքներից որեւէ մեկը կարող է եւ համընկնել դրական b_j արժեքներից մեկի հետ: Ուստի $h_p(x)$ մոդուլյար բազմանդամի որեւէ $b_{i,p} \in \mathbb{Z}_p$ գործակցի համար առայժմ չենք կարող ասել.

- արդյո՞ք այն $h(x)$-ի որեւէ ոչ բացասական գործակցի պատկեր է, որն անփոփոխ է մնացել մոդուլյար անցման ժամանակ,
- թե՞ այն $h(x)$-ի որեւէ բացասական գործակցի պատկեր է. $b_{i,p} = \varphi_p(b_i) = b_i + p$:

3.2.6 Օրինակ. $f(x) = x^2 - 2x + 1 = (x-1)^2$ բազմանդամի բոլոր գործակիցները, ինչպես եւ այդ բազմանդամի բոլոր բաժանարարների բոլոր գործակիցները մոդու-

լով չեն գերազանցում 2 թիվը: Ըստ վերը նշվածի, կարող ենք վերցնել $p = 3 > 2$ պարզ թիվը եւ կատարել $\varphi_3 \colon \mathbb{Z}[x] \to \mathbb{Z}_3[x]$ մոդուլյար անցումը.

$$f_3(x) = \varphi_3\big(f(x)\big) = x^2 + x + 1:$$

$f(x)$-ի բոլոր դրական գործակիցներն, իրոք, անփոփոխ են մնացել, իսկ $a_1 = -2$ գործակիցը արտապատկերվել է $\varphi_3(-2) = 1 \in \mathbb{Z}_3$ թվին: Նույնը վերաբերում է $h(x) = x - 1$ բաժանարարին. $h_3(x) = x + 2$: Ուստի, եթե որեւէ խնդրի լուծման ժամանակ մենք ստացել ենք $f_3(x)$ բազմանդամի $h_3(x) = x + 2$ բաժանարարը, ապա, եթե մեզ հայտնի չէ $h(x)$ բազմանդամը, մենք չենք կարող ասել, թե $h_3(x)$-ի գործակիցներից որո՞նք են դրական գործակիցների պատկերներ եւ որոնք՝ բացասական գործակիցների. $h_3(x)$-ի համար ունենք չորս հնարավոր նախապատկերներ.

$$x + 2, \quad x - 1, \quad -2x + 2, \quad -2x - 1:$$

Բացասական գործակիցների հետ կապված այս այլընտրանքը հեշտ է լուծել N_f գնահատականը բարձրացնելով: Մոդուլյար անցումն իրականացնենք ըստ

$$p > 2 \cdot N_f: \tag{3.5}$$

պայմանի ընտրված p պարզ թվի: Ոչ բացասական b_i գործակիցները դարձյալ անփոփոխ են մնում φ_p-ի ազդեցության տակ: Ավելին, քանի որ $b_i \in \{0, \dots, N_f\}$ եւ $p > 2 \cdot N_f$, ստանում ենք, որ ոչ բացասական b_i գործակիցները պատկանում են $[0, p/2)$ միջակայքին:

Բացասական գործակիցներն արտապատկերվում են $b_{i,p} = \varphi_p(b_i) = b_i + p$ կանոնով: Բայց, քանի որ $p > 2 \cdot N_f$, իսկ b_i-ն բացասական է, ապա $b_{i,p} = b_i + p \geq p - N_f > p/2$, այսինքն՝ բացասական b_i գործակիցների պատկերները պատկանում են $(p/2, p)$ միջակայքին: Այսպիսով ստանում ենք.

3.2.7 Լեմմա. *Ենթադրենք $\mathbb{Z}[x]$ բազմանդամային օղակում տրված է $f(x) = a_0x^n + \dots + a_n$ բազմանդամը եւ նրա համար* (3.2) *բանաձեւով հաշվված է N_f գնահատականը: Եթե $p > 2N_f$, ապա $f(x)$-ի կամայական $h(x) = b_0x^m + \dots + b_m$ բաժանարարի $h_p(x) = \varphi_p\big(h(x)\big) = b_{0,p}x^m + \dots + b_{m,p} \in \mathbb{Z}_p[x]$ պատկերի գործակիցների համար համար տեղի ունի հետեւյալ այլընտրանքը.*

1. *կամ $b_i = b_{i,p} \geq 0$, եւ սա տեղի ունի այն եւ միայն այն դեպքում, երբ $b_{i,p} < p/2$,*
2. *կամ էլ $b_i = b_{i,p} - p < 0$, եւ սա տեղի ունի այն եւ միայն այն դեպքում, երբ $b_{i,p} > p/2$:*

Այսինքն՝ ունենալով $h_p(x)$-ը՝ կարելի է $h(x)$-ը վերականգնել հետեւյալ պարզ ալգորիթմով.

3.2.8 Ալգորիթմ (բազմանդամի մոդուլյար բաժանարարի նախապատկերի վերականգնումը). Տրված է $f(x) \in \mathbb{Z}[x]$ բազմանդամը, եւ նրա $h(x)$ անհայտ բաժանարարի համար կարող ենք կառուցել նրա $h_p(x) = \varphi_p\big(h(x)\big)$ մոդուլյար պատկերը ըստ կամայական պարզ թվի: Գտնել $h(x)$ բաժանարարը:

1. $f(x)$ բազմանդամի համար Լանդաու-Մինյոտի (3.2) բանաձեւով հաշվենք N_f գնահատականը:

2. Ընտրենք $p > 2 \cdot N_f$ պայմանին բավարարող որեւէ p պարզ թիվ:

3. Կառուցենք ըստ φ_p մոդուլյար անցումի ստացված $h_p(x) = b_{0,p}x^m + \cdots + b_{m,p}$ մոդուլյար բազմանդամը:
4. $(i = 0;\ i \le m;\ \ i++)$ արժեքների համար

5. եթե $b_{i,p} < p/2$

6. նշանակենք $b_i = b_{i,p}$;

7. հակառակ դեպքում

8. նշանակենք $b_i = b_{i,p} - p$:

9. Դուրս գրենք $h(x) = b_0x^m + \cdots + b_m$ բազմանդամը:

Հետագայում խնդիրներ լուծելիս մենք միշտ կարող ենք համարել, որ մոդուլյար անցումն իրականացրել ենք ըստ բավականաչափ մեծ պարզ թվի, եւ համապատասխան նախապատկերը հնարավոր է հաշվել ըստ այս ալգորիթմի:

Իսկ եթե ինչ-որ խնդրում պետք է գնահատել միանգամից ըստ երկու բազմանդամների (օրինակ՝ $f(x)$ եւ $g(x)$ բազմանդամների ամենամեծ ընդհանուր բաժանարարի հաշվման խնդրում), ապա կարող ենք օգտվել (3.3) բանաձեւի $N_{f,g}$ գնահատականից եւ ընտրել այնպիսի մի պարզ $p > 2 \cdot N_{f,g}$ թիվ, որը բավականաչափ մեծ է միաժամանակ երկու բազմանդամների համար էլ:

3.3 Բազմանդամների ռեզուլտանտը

Տրված երկու բազմանդամների *ռեզուլտանտի* հասկացությունը մեզ անհրաժեշտ է լինելու միայն ալգորիթմների կառուցման համար որոշ գնահատականներ ստանալու նպատակով: Ուստի առաջին ընթերցման ժամանակ կարելի է բաց թողնել այս պարագրաֆի ապացույցները եւ հիշել միայն 3.3.6 թեորեմը, որը կապ է հաստատում երկու բազմանդամների փոխադարձ պարզության եւ ռեզուլտանտի միջեւ:

3.3.1 Լեմմա. *Տրված $f(x),\ g(x) \in R[x]$ ոչ զրոյական բազմանդամները փոխադարձաբար պարզ չեն այն եւ միայն այն դեպքում, երբ գոյություն ունեն $u(x),\ v(x) \in R[x]$ ոչ զրոյական բազմանդամներ այնպիսիք, որ.*
1) $u(x)f(x) + v(x)g(x) = 0$,
2) $\deg u(x) < \deg g(x)$ *եւ* $\deg v(x) < \deg f(x)$*:*

Ապացույց: Նախ, ենթադրենք

$$\big(f(x), g(x)\big) = d(x) \not\approx 1:$$

Քանի որ $\deg d(x) > 0$, ապա $\deg\big(f(x)/d(x)\big) < \deg f(x)$ եւ $\deg\big(g(x)/d(x)\big) < \deg g(x)$: Ուստի պայմանի բավարարությունն ապացուցելու համար կարելի է վերցնել $u(x) = -g(x)/d(x)$ եւ $v(x) = f(x)/d(x)$:

Անհրաժեշտության ապացույցի համար ենթադրենք, թե տրված են լեմմայի պայմանին բավարարող $u(x),\ v(x) \in R[x]$ ոչ զրոյական բազմանդամներ, որոնց համար $u(x)f(x) = -v(x)g(x)$: Եթե $f(x),\ g(x)$ բազմանդամները փոխադարձաբար պարզ լինեին, ապա $u(x)f(x) \vdots g(x)$ պայմանից պիտի բխեր, որ $u(x) \vdots g(x)$: Սա հանգեցնում է հակասության, քանի որ $\deg u(x) < \deg g(x)$: ■

3.3.1 լեմման կարելի է ներկայացնել վեկտորական տարածությունների մեջ գծային օպերատորների միջոցով: Կառուցենք այդ ներկայացումը:

Գծային տարածության հայտնի օրինակներից է տրված R դաշտի վրա սահմանված բազմանդամների $R[x]$ բազմությունը, որի վրա վեկտորների (բազմանդամների) գումարը սահմանվում է նույն կերպ, ինչպես $R[x]$ օղակում, իսկ $\alpha \in R$ սկալյարի եւ $f(x) = a_0x^n + \cdots + a_n \in R[x]$ վեկտորի (բազմանդամի) արտադրյալը սահմանվում է

$$\alpha(a_0x^n + \cdots + a_n) = (\alpha \cdot a_0)x^n + \cdots + (\alpha \cdot a_n)$$

կանոնով (տես նաեւ 7.2 պարագրաֆը, որտեղ ավելի մանրամասնորեն ենք կանգ առել կամայական դաշտերի վրա տրված գծային տարածությունների եւ օպերատորների վրա):

3.3.2 Վարժություն. Ստուգել, որ $R[x]$ օղակը քիչ առաջ սահմանված գործողությունների նկատմամբ, իրոք, R դաշտի վրա տրված գծային տարածություն է:

Տրված n բնական թվի համար վերցնենք

$$P_n = P_n(R) = \{f(x) \in R[x] \mid \deg f(x) \le n\}$$

ենթաբազմությունը: Սահմանենք նաեւ $P_0 = \{0\}$:

3.3.3 Վարժություն. Ստուգել, որ P_n ենթաբազմությունը նույնպես գծային տարածություն է նույն գործողությունների նկատմամբ, եւ, հետեւաբար, P_n-ը $R[x]$-ի ենթատարածություն է:

3.3.4 Խնդիր. Ցույց տալ, որ P_n տարածության բազիս է հետեւյալ վեկտորների (բազմանդամների) համակարգը.

$$e_0 = x^n, e_1 = x^{n-1}, \dots, e_n = x^0 = 1,$$

եւ նկատել, որ $\dim P_n = n + 1$: *Յուցում.* $e_0, e_1, \dots, e_n$ համակարգի գծային անկախությունն ապացուցելու համար հիշել, որ կամայական ոչ զրոյական բազմանդամ ունի ոչ ավել, քան վերջավոր քանակությամբ արմատներ:

Այժմ ենթադրենք, թե 3.3.1 լեմմայի մեջ դիտարկված $f(x)$ եւ $g(x)$ բազմանդամների աստիճաններն են համապատասխանաբար n եւ m: Այս դեպքում $u(x) \in P_{m-1}$, $v(x) \in P_{n-1}$, եւ մենք կարող ենք դիտարկել

$$\Psi_{f,g}: P_{m-1} \oplus P_{n-1} \to P_{m+n-1}$$

արտապատկերումը տարածությունների $P_{m-1} \oplus P_{n-1}$ ուղիղ գումարից P_{m+n-1} տարածության վրա, որ տրված է

$$\Psi_{f,g}: \big(u(x), v(x)\big) \to u(x)f(x) + v(x)g(x)$$

կանոնով. բազմանդամների $\big(u(x), v(x)\big) \in P_{m-1} \oplus P_{n-1}$ զույգին համապատասխանեցվում է 3.3.1 լեմմայում նշված գումարը: Այս սահմանման կոռեկտությունն ակնհայտ է, քանի որ

$$\deg\big(u(x)f(x) + v(x)g(x)\big) \le m + n - 1:$$

Հեշտ է ստուգել նաեւ, որ $\Psi_{f,g}$ արտապատկերումը գծային է: Ավելին.

$$\dim(P_{m-1} \oplus P_{n-1}) = m + n = \dim(P_{m+n-1}):$$

Այսինքն՝ $\Psi_{f,g}$-ն գծային օպերատոր է միեւնույն չափողականության տարածությունների միջեւ: $\Psi_{f,g}$-ն իզոմորֆիզմ է այն եւ միայն այն դեպքում, երբ նրա $\ker \Psi_{f,g}$ միջուկը զրոյական է: Ըստ 3.3.1 լեմմայի, դա հնարավոր է այն եւ միայն այն դեպքում, երբ $\big(f(x), g(x)\big) = 1$: Սա տալիս է 3.3.1 լեմմայի մի նոր ձեւակերպում.

3.3.5 Լեմմա. *Վերը բերված նշանակումներում $\Psi_{f,g}$ օպերատորն իզոմորֆիզմ է այն եւ միայն այն դեպքում, երբ $\big(f(x), g(x)\big) = 1$:*

Լեմմայի այս տեսքը թույլ է տալիս ստանալ այն մատրիցային բանաձեւը, որը եւ օգտագործելու ենք հետագայում: $P_{m-1} \oplus P_{n-1}$ գծային տարածության համար բազիս է հանդիսանում հետեւյալ համակարգը.

$$(x^{m-1},0),(x^{m-2},0),\dots,(1,0);$$
$$(0,x^{n-1}),(0,x^{n-2}),\dots,(0,1):$$

Ըստ այդ բազիսի՝ $\Psi_{f,g}$ օպերատորի $S_{f,g}$ մատրիցը հաշվելու համար պետք է $\Psi_{f,g}$ օպերատորը հերթով կիրառել բազիսի վեկտորների վրա.

$$\Psi_{f,g}\colon (x^{m-1},0)\to x^{m-1}f(x),$$
$$\dots\dots\dots\dots\dots\dots\dots\dots$$
$$\Psi_{f,g}\colon (1,0)\to f(x);$$
$$\Psi_{f,g}\colon (0,x^{n-1})\to x^{n-1}g(x),$$
$$\dots\dots\dots\dots\dots\dots\dots\dots$$
$$\Psi_{f,g}\colon (0,1)\to g(x):$$

$x^if(x)$ եւ $x^jg(x)$ տեսքի բազմանդամների գործակիցները դասավորելով տողերով՝ ստանում ենք հետեւյալ մատրիցը՝

$$S_{f,g}=\begin{pmatrix} a_0 & a_1 & \cdots & a_n & & \\ & a_0 & a_1 & \cdots & a_n & \\ & \dots\dots & \dots\dots & \dots\dots & \dots\dots & \\ & & a_0 & a_1 & \cdots & a_n \\ b_0 & b_1 & \cdots & b_m & & \\ & b_0 & b_1 & \cdots & b_m & \\ & \dots\dots & \dots\dots & \dots\dots & \dots\dots & \\ & & b_0 & b_1 & \cdots & b_m \end{pmatrix}, \tag{3.6}$$

որտեղ մատրիցի տարրերը $f(x)=a_0x^n+\cdots+a_n$ եւ $g(x)=b_0x^m+\cdots+b_m$ բազմանդամների գործակիցներն են, իսկ բոլոր դատարկ թողած տեղերում զրոներ են: $S_{f,g}$ մատրիցն ունի $m+n$ սյուն եւ $m+n$ տող, ընդ որում, առաջին m տողերում դասավորված են $f(x)$-ի գործակիցները (յուրաքանչյուր հաջորդ տողում մի քայլ դեպի ավելի աջից գրված), իսկ հաջորդ n տողերում դասավորված են $g(x)$-ի գործակիցները (դարձյալ յուրաքանչյուր հաջորդ տողում մի քայլ դեպի ավելի աջից գրված):

$S_{f,g}$ մատրիցն ընդունված է անվանել $f(x)$ եւ $g(x)$ բազմանդամների *Սիլվեստրի մատրից*, իսկ նրա որոշիչը՝ $f(x)$ եւ $g(x)$ բազմանդամների *ռեզուլտանտ*՝

$$\operatorname{res}\big(f(x),g(x)\big)=\det S_{f,g}: \tag{3.7}$$

Նախորդ լեմմայից անմիջապես բխում է հետեւյալ օգտակար հայտանիշը.

3.3.6 Թեորեմ. *Տրված $f(x),\ g(x)\in R[x]$ ոչ զրոյական բազմանդամները փոխադարձաբար պարզ են այն եւ միայն այն դեպքում, երբ* $\operatorname{res}\big(f(x),g(x)\big)\neq 0$:

3.3.7 Օրինակ. Վերցնենք $f(x)=x^2-1$ եւ $g(x)=x^3-4x$: Այս բազմանդամները փոխադարձաբար պարզ են, քանի որ

$$f(x)=(x+1)(x-1) \text{ եւ } g(x)=x(x+2)(x-2):$$

Մյուս կողմից,

$$\operatorname{res}\big(f(x),g(x)\big)=\det\begin{pmatrix}1&0&-1&0&0\\0&1&0&-1&0\\0&0&1&0&-1\\1&0&-4&0&0\\0&1&0&-4&0\end{pmatrix}=-9\neq 0:$$

3.3.8 Օրինակ. Վերցնենք $f(x)=x^2-1$ եւ $g(x)=x^2+x$: Հեշտ է տեսնել, որ $\big(f(x),g(x)\big)=x+1$, քանի որ

$$f(x)=(x+1)(x-1) \text{ եւ } g(x)=x(x+1):$$

Մյուս կողմից,

$$\operatorname{res}\big(f(x),g(x)\big)=\det\begin{pmatrix}1&0&-1&0\\0&1&0&-1\\1&1&0&0\\0&1&1&0\end{pmatrix}=0:$$

Երկու բազմանդամների ռեզուլտանտի հաշվման համար կան եւս մի քանի բանաձեւեր, որոնք կնշենք ստորեւ առանց ապացույցի, քանի որ դրանք ուղղակիորեն չեն օգտագործվելու մեր ալգորիթմների մեջ: Մենք այդ բանաձեւերը նույնպես բերում ենք, քանի որ դրանք ռեզուլտանտի հաշվման ավելի հարմար մեթոդներ են, քան (3.7) բանաձեւը, հատկապես այն դեպքերում, երբ բազմանդամների արմատները հայտնի են:

Այդ բանաձեւերի ձեւակերպման համար անհրաժեշտ է ընդլայնել հետեւյալ պայմանավորվածությունը: Այս պարագրաֆի սկզբում մենք վերցրինք ցանկացած R ամբողջության տիրույթի կամ դաշտի վրա տրված $R[x]$ բազմանդամային օղակ, եւ ռեզուլտանտը սահմանեցինք նրա կամայական $f(x),\ g(x)\in R[x]$ ոչ զրոյական բազմանդամների համար: Պայմանավորվենք այս պարագրաֆի հետագա մասում R-ը համարել իրական թվերի դաշտը՝ $R=\mathbb{R}$: Իրական գործակիցներով, հաստատունից տարբեր կամայական բազմանդամ ունի արմատներ, որոնք ընդհանուր դեպքում կոմպլեքս են, եւ որոնց քանակը (հաշվի առնելով պատիկ արմատների պատիկությունը եւս) հավասար է բազմանդամի աստիճանին: Ենթադրենք

$$f(x)=a_0x^n+\cdots+a_n \text{ եւ } g(x)=b_0x^m+\cdots+b_m$$

բազմանդամների արմատներն են համապատասխանաբար $\alpha_1,\dots,\alpha_n$ եւ $\beta_1,\dots,\beta_m$: Այս դեպքում իրավացի է հետեւյալ կարեւոր բանաձեւը.

(3.8) $$\operatorname{res}\big(f(x),g(x)\big)=a_0^m b_0^n\prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i-\beta_j):$$

Քանի որ միշտ տեղի ունի

$$g(x)=b_0\prod_{j=1}^{m}(x-\beta_j)$$

հավասարությունը, ապա, դրա մեջ $x=\alpha_i$ արժեքը տեղադրելով եւ վերեւի արտահայտությունը ձեւափոխելով, կունենանք ռեզուլտանտի հաշվման մի այլ բանաձեւ.

(3.9) $$\operatorname{res}\big(f(x),g(x)\big)=a_0^m\prod_{i=1}^{n}g(\alpha_i):$$

Նույն կերպ՝

$$f(x)=a_0\prod_{i=1}^{n}(x-\alpha_i)$$

վերլուծությունից ստացվում է եւս մի բանաձեւ.

(3.10) $$\operatorname{res}\big(f(x),g(x)\big)=(-1)^{n\cdot m}b_0^n\prod_{j=1}^{m}f(\beta_j):$$

Մասնավորապես՝

(3.11) $$\operatorname{res}\big(f(x),g(x)\big)=(-1)^{n\cdot m}\operatorname{res}\big(g(x),f(x)\big):$$

3.3.9 Օրինակ. Կիրառենք այս երեք բանաձեւերից առաջինը 3.3.7 օրինակում դիտարկված բազմանդամների համար: $f(x)=x^2-1$ բազմանդամի արմատներն են $\alpha_1=1,\ \alpha_2=-1,$ իսկ $g(x)=x^3-4x$ բազմանդամինը՝ $\beta_1=0,\ \beta_2=2,\ \beta_3=-2$: Ուստի

$$\operatorname{res}\big(f(x),g(x)\big)=1^3 1^2\cdot(1-0)(1-2)(1+2)\cdot(-1-0)(-1-2)(-1+2)=-9:$$

Այն փաստը, որ վերջին բանաձեւերում ռեզուլտանտը սահմանափակել ենք $R=\mathbb{R}$ դեպքի համար, չի փոխում այս բանաձեւերի ալգորիթմական արժեքը մեր համար, քանի որ (3.8) – (3.11) բանաձեւերը կիրառելու ենք միայն իրական (ամբողջ, ռացիոնալ) գործակիցներով բազմանդամների համար (դրանք չեն կիրառվելու, օրինակ, $\mathbb{Z}_p[x]$ օղակի մոդուլյար բազմանդամների համար):

Իրականում (3.8) – (3.11) բանաձեւերը ճիշտ են ցանկացած դաշտի համար, քանի որ կամայական դաշտ կարելի է ներդնել իր այնպիսի ընդլայնման մեջ, որ-

տեղ $f(x)$ եւ $g(x)$ բազմանդամներն արմատներ ունեն (տես 4.2.31 թեորեմը): Մենք, դաշտերի հանրահաշվորեն փակ ընդլայնումներին պատրաստվում ենք անդրադառնալ հետագայում, մասնավորապես, 4.2 պարագրաֆում, իսկ այստեղ մեր նպատակների համար բավարար է իրական գործակիցների դեպքը, որոնց համար հանրահաշվորեն փակ դաշտը տվյալ դեպքում $\mathbb{C}$-ն է:

3.4 Ամենամեծ ընդհանուր բաժանարարի մեծ պարզ թվի ալգորիթմը

Օգտվելով մոդուլյար անցումից, Գաուսի լեմմայից, Լանդաու-Մինյոտի բանաձեւից եւ ռեզուլտանտի հատկություններից՝ մենք արդեն կարող ենք կառուցել կամայական $f(x),\ g(x) \in \mathbb{Z}[x]$ բազմանդամների $d(x) = \big(f(x),\ g(x)\big)$ ամենամեծ ընդհանուր բաժանարարը մոդուլյար մեթոդներով հաշվելու ալգորիթմը:

Ըստ 2.5.13 թեորեմի՝ $\mathbb{Z}_p[x]$ օղակն էվկլիդյան է ցանկացած p պարզ թվի համար: Նրա ցանկացած տարրերի համար, ըստ 2.5.3 թեորեմի, կարելի է էվկլիդեսի ալգորիթմով հաշվել դրանց ամենամեծ ընդհանուր բաժանարարը: Տրված p-ի համար դիտարկենք φ_p մոդուլյար անցումը, այսինքն՝ $\varphi_p\colon \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ օղակային հոմոմորֆիզմը: Կամայական $f(x),\ g(x) \in \mathbb{Z}[x]$ բազմանդամների համար, ըստ նրանց $f_p(x),\ g_p(x) \in \mathbb{Z}_p[x]$ պատկերների, գտնենք դրանց $\big(f_p(x),\ g_p(x)\big)$ ամենամեծ ընդհանուր բաժանարարը: Մի շարք պատճառներով այն կարող է տարբեր լինել $d_p(x) = \varphi_p\big(d(x)\big) = \varphi_p\Big(\big(f(x), g(x)\big)\Big)$ բազմանդամից: Ավելին, ինչպես արդեն տեսել ենք 2.4.1, 2.4.2 եւ 2.4.3 կետերում, $\big(f_p(x),\ g_p(x)\big)$ մոդուլյար բազմանդամը կարող է ընդհանրապես որեւէ էական ինֆորմացիա չպարունակել $d(x)$-ի մասին կամ էլ կարող է անհնար լինի էֆեկտիվորեն հաշվել դրա նախապատկերը:

Այդ բարդությունները շրջանցելու համար մոդուլյար անցումը իրականացնենք ըստ բավականաչափ մեծ p պարզ թվի: Նախ, օգտվենք (3.3) բանաձեւից. եթե

$$p > N_{f,g},$$

ապա φ_p մոդուլյար անցումը որոշակի ինֆորմացիա է պահպանում $f(x)$ բազմանդամի կամայական բաժանարարի ցանկացած գործակցի մասին. այն կամ անփոփոխ է մնում մոդուլյար անցման ընթացքում (եթե տվյալ գործակիցը ոչ բացասական է), կամ էլ մոդուլյար անցման ժամանակ պարզապես դրան զուգադրվում է p թիվը (եթե տվյալ գործակիցը բացասական է):

Առայժմ լուծված չէ նաեւ նախապատկերի հաշվման միարժեքության ապահովման խնդիրը (տես 3.2.6 օրինակը եւ 3.2.7 լեմմային նախորդող քննարկումը): Բայց, ինչպես տեսանք, վերցնելով

$$p > 2 \cdot N_{f,g} \tag{3.12}$$

պայմանին բավարարող p պարզ թիվ (տես (3.3) բանաձեւը), կարող ենք համարել, որ $\varphi_p\colon \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ մոդուլար անցման ժամանակ $f(x)$, $g(x)$ բազմանդամների կամայական $h(x)$ ընդհանուր բաժանարարի պատկերն է

$$h_p(x) = \varphi_p\big(h(x)\big) = b_{0,p}x^k + \cdots + b_{k,p} \in \mathbb{Z}_p[x]$$

բազմանդամը, որի գործակիցների համար՝

1. կամ $b_{i,p} = b_i$, եւ սա տեղի ունի այն եւ միայն այն դեպքում, երբ $b_i \geq 0$,
2. կամ էլ $b_{i,p} = b_i + p$, եւ սա տեղի ունի այն եւ միայն այն դեպքում, երբ $b_i < 0$:

Այսինքն՝ ունենալով $h_p(x)$ ընդհանուր բաժանարարը՝ մենք միշտ կարող ենք միարժեքորեն վերականգնել նրա որոնելի $h(x)$ նախապատկերը 3.2.8 ալգորիթմով. կամ $b_i = b_{i,p}$, եթե $b_{i,p} < p/2$, կամ էլ $b_i = b_{i,p} - p$, եթե $b_{i,p} > p/2$:

3.4.1 Դիտողություն. Կարելի՞ է արդյոք տրված $f(x),\ g(x) \in \mathbb{Z}[x]$ բազմանդամների համար հաշվել $N_{f,g}$ սահմանը, վերցնել դրան երկու անգամ գերազանցող $p > 2 \cdot N_{f,g}$ պարզ թիվ, հետո էվկլիդյան $\mathbb{Z}_p[x]$ օղակում հաշվել $\big(f_p(x),\ g_p(x)\big)$ մոդուլար ամենամեծ ընդհանուր բաժանարարը եւ ըստ 3.2.8 ալգորիթմի վերականգնել դրա $d(x)$ նախապատկերը՝ որպես $\big(f(x),\ g(x)\big)$ ամենամեծ ընդհանուր բաժանարար: Այս հարցը նախանշում է մեր կառուցելիք ալգորիթմի հիմնական սկզբունքը, բայց այն երկու կարեւոր պատճառներով առայժմ բացասական պատասխան ունի: Դրանցից առաջինը կապված է *«ավելորդ» սկալյար արտադրիչների*, իսկ երկրորդը՝ *բաժանելիության պահպանման* հետ:

Դիտողության մեջ հիշատակված առաջին պատճառը տեսնելու համար դիտարկենք հետեւյալ պարզ օրինակը.

3.4.2 Օրինակ. Վերցնենք $f(x) = x^2 + 4x + 3$ եւ $g(x) = x^2 + 2x + 1$: Բոլոր գործակիցները դրական են, եւ կամայական $p > 4$ պարզ թվի համար φ_p մոդուլար անցումը չի փոխում բազմանդամների տեսքը. $f_p(x) = x^2 + 4x + 3$ եւ $g_p(x) = x^2 + 2x + 1$: Կիրառենք Էվկլիդեսի ալգորիթմը.

$$\begin{array}{l|l} x^2+4x+3 & x^2+2x+1 \\ \hline x^2+2x+1 & 1 \\ \hline 2\,x+2 & \end{array}$$

այսինքն՝ $f_p(x) = 1 \cdot g_p(x) + 2\,x + 2$: Հաջորդ քայլում $g_p(x) = q(x) \cdot (2\,x+2) + 0$, քանի որ $g_p(x)$-ը $\mathbb{Z}_p[x]$ օղակում բաժանվում է $2x+2$ բազմանդամի վրա: Ուրեմն այդ օղակում, ըստ Էվկլիդեսի ալգորիթմի, $\big(f_p(x),\ g_p(x)\big) = 2x+2$: Իսկ մյուս կողմից՝ $x^2+4x+3 = (x+1)(x+3)$, այսինքն՝ $\mathbb{Z}[x]$ օղակում

$$\big(f(x),\ g(x)\big) = \big((x+1)(x+3),\ (x+1)^2\big) = x+1:$$

Ինչպիսի $p > 4$ պարզ թիվ էլ վերցնենք, $\big(f_p(x),\ g_p(x)\big) = 2x+2$ բազմանդամը չի հանդիսանա $\big(f(x),\ g(x)\big)$ ամենամեծ ընդհանուր բաժանարարի պատկերը. $\varphi_p(x+1) \neq 2x+2$, քանի որ $a_0 = 1$ ավագ գործակիցը հավասար չէ 2-ի ըստ ոչ մի p մոդուլի: 2 թիվն այստեղ «ավելորդ» սկալյար արտադրիչ է:

3.4.2 օրինակում նկատված երեւույթի պատճառն այն է, որ $\mathbb{Z}[x]$ օղակում միակ հակադարձելի տարրերն են $1, -1$ թվերը, ուստի ամենամեծ ընդհանուր բաժանարարը որոշվում է միայն նշանի ճշտությամբ. $\big(f(x),\ g(x)\big)$-ի միակ հնարավոր արժեքներն են միայն $x+1$ եւ $-x-1$: Իսկ $\mathbb{Z}_p[x]$ օղակում հակադարձելի է կամայական ոչ զրոյական $t \in \mathbb{Z}_p$ թիվ: Ուստի $\mathbb{Z}_p[x]$ օղակում $\big(f_p(x),\ g_p(x)\big)$-ի հետ միասին $f_p(x), g_p(x)$ բազմանդամների ամենամեծ ընդհանուր բաժանարար է նաեւ դրա կամայական $t \cdot \big(f_p(x),\ g_p(x)\big)$ պատիկը ($t \neq 0$): Մեր 3.4.2 օրինակում Էվկլիդեսի ալգորիթմը հաշվարկել էր $2(x+1)$ պատիկը, որը $x+1$ բազմանդամի պատկերը չէ: $t \cdot \big(f_p(x),\ g_p(x)\big)$ տեսքի ոչ զրոյական պատիկները $\mathbb{Z}_p[x]$ օղակում $p-1$ հատ են, եւ դրանցից միայն մեկն է, որ $d(x)$-ի $d_p(x)$ պատկերն է:

3.4.3 Վարժություն. 3.4.2 օրինակի բազմանդամների համար վերցնել, օրինակ, $p = 151$ եւ, «անկյունով» բաժանելով, ստուգել, որ $f_{151}(x) = x^2+4x+3$ եւ $g_{151}(x) = x^2+2x+1$ բազմանդամների համար ամենամեծ ընդհանուր բաժանարար են հանդիսանում $2x+2$ եւ $100\,x+100$ բազմանդամները:

«Ավելորդ» սկալյար արտադրիչից կարելի է ազատվել պրիմիտիվ բազմանդամների ու Գաուսի լեմմայի օգնությամբ: Որպես հաշվարկի առաջին քայլ (դեռ նախքան Լանդաու-Մինյոտի բանաձեւը կիրառելը) մեր բազմանդամները ներկայացնենք իրենց բովանդակությունների ու պրիմիտիվ մասերի արտադրյալների տեսքով.

$$f(x) = \operatorname{cont}\big(f(x)\big)\operatorname{pp}\big(f(x)\big), \qquad g(x) = \operatorname{cont}\big(g(x)\big)\operatorname{pp}\big(g(x)\big)$$

եւ նշանակենք $r = \Big(\operatorname{cont}\big(f(x)\big),\ \operatorname{cont}\big(g(x)\big)\Big)$: Քանի որ այս բովանդակությունները որոշվում են նշանի ճշտությամբ, առանց ընդհանրությունը խախտելու համարենք, որ $\operatorname{pp}\big(f(x)\big)$, $\operatorname{pp}\big(g(x)\big)$ բազմանդամների ավագ գործակիցները *դրական են*: Եթե մեզ հաջողվի գտնել դրանց $\Big(\operatorname{pp}\big(f(x)\big),\ \operatorname{pp}\big(g(x)\big)\Big)$ ամենամեծ ընդհանուր բաժանարարը, ապա որոնելի $d(x)$-ը կհաշվվի

$$d(x) = \big(f(x), g(x)\big) = r \cdot \Big(\operatorname{pp}\big(f(x)\big), \operatorname{pp}\big(g(x)\big)\Big)$$

տեսքով (տես 2.6.8 Գաուսի լեմման, 2.6.9 եւ 2.6.16 հետեւանքները):

Ուստի նշանակումների պարզության համար ֆիքսենք r թիվը, անցում կատարենք նոր $f(x) = \operatorname{pp}\big(f(x)\big)$ եւ $g(x) = \operatorname{pp}\big(g(x)\big)$ բազմանդամներին եւ ստորեւ համարենք, որ $f(x)$, $g(x)$ բազմանդամները պրիմիտիվ են: Հաշվելով այս նոր բազմանդամների $d(x)$ ամենամեծ ընդհանուր բաժանարարը՝ մենք վերջնական պատասխանը կստանանք $r \cdot d(x)$ տեսքով: Նկատենք, որ այս անցման հաշվողական առավելություններից մեկն էլ այն է, որ բազմանդամների գործակիցները նվազում են, ուստի Լանդաու-Մինյոտի բանաձեւն այս անցումից հետո կիրառելով՝ մենք կստանանք զգալիորեն ավելի փոքր $N_{f,g}$ գնահատական:

Նշանակենք $w = (a_0, b_0)$, որտեղ $a_0, b_0 \in \mathbb{Z}$ դրական թվերը $f(x)$, $g(x)$ բազմանդամների ավագ գործակիցներն են: $d(x) = \big(f(x),\ g(x)\big)$ բազմանդամի c_0 ավագ գործակիցը, որը նույնպես կարելի է համարել դրական, w-ի որեւէ բաժանարար է: Կամայական p պարզ թվի համար $f_p(x)$ եւ $g_p(x)$ մոդուլյար բազմանդամների $a_{0,p} = \varphi_p(a_0)$ եւ $b_{0,p} = \varphi_p(b_0)$ ավագ գործակիցները բաժանվում են $d_p(x)$-ի $c_{0,p} = \varphi_p(c_0)$ ավագ գործակցի վրա: Եւ եթե այժմ $p > 2 \cdot \max\{N_f, N_g\}$, ապա

$$0 \le a_0,\ b_0,\ c_0 < p \qquad \text{եւ} \qquad a_0 = a_{0,p},\ \ b_0 = b_{0,p},\ \ c_0 = c_{0,p}:$$

Համարենք, որ մեր ընտրած p-ն արդեն այնպիսին է, որ $\deg d(x) = \deg\Big(f_p(x),\ g_p(x)\Big)$: Քանի որ, ըստ p-ի ընտրության, φ_p-ն չի զրոյացնում $d(x)$-ի ավագ գործակիցը, ապա $\deg d(x) = \deg d_p(x)$: Եւ, քանի որ $d_p(x)$-ի աստիճանը $f_p(x)$, $g_p(x)$ բազմանդամների ամենամեծ ընդհանուր բաժանարարի աստիճանին է հավասար, ապա, ըստ 2.7.6 լեմմայի, $d_p(x)$-ը $f_p(x)$, $g_p(x)$ բազմանդամների ամենամեծ ընդհանուր բաժանարարներից մեկն է. $d_p(x) \approx \Big(f_p(x),\ g_p(x)\Big)$: Հետեւաբար՝ $\mathbb{Z}_p[x]$ օղակում $f_p(x)$, $g_p(x)$ բազմանդամների՝ $t \cdot \Big(f_p(x),\ g_p(x)\Big)$ ընդհանուր տեսքով տրվող ամենամեծ ընդհանուր բաժանարարների շարքում $d(x) = \big(f(x),\ g(x)\big)$ բազման-

դամի $d_p(x)$ պատկերը կառանձնանա այն հատկությամբ, որ իր ավագ գործակիցը կլինի w-ի որոշակի (մեզ անհայտ) բաժանարար:

Այստեղից $d_p(x)$-ը եւ $d(x)$-ը կարելի է հաշվել՝ օգտվելով $f(x)$, $g(x)$ բազմանդամների պրիմիտիվությունից: Էվկլիդեսի ալգորիթմով հաշվենք $\big(f_p(x),\ g_p(x)\big)$-ը եւ այն բազմապատկենք այնպիսի մի $t \in \mathbb{Z}_p$ թվով, որ $t \cdot \big(f_p(x),\ g_p(x)\big)$ արտադրյալի ավագ գործակիցը հավասար լինի w-ի: Ըստ ասվածի, $t \cdot \big(f_p(x),\ g_p(x)\big)$ արտադրյալը կամ $d_p(x) = \varphi_p\big(d(x)\big)$ պատկերն է, կամ էլ այդ պատկերի որեւէ սկալյար պատիկը (ընդ որում, ըստ w-ն չգերազանցող ինչ-որ սկալյարի): 3.2.8 ալգորիթմով հաշվենք $t \cdot \big(f_p(x),\ g_p(x)\big)$-ի $k(x) \in \mathbb{Z}[x]$ նախապատկերը, որը կլինի $f(x)$, $g(x)$ բազմանդամների ինչ-որ պատիկների ամենամեծ ընդհանուր բաժանարարը: Մնում է հիշել, որ պրիմիտիվ $f(x)$, $g(x)$ բազմանդամների ամենամեծ ընդհանուր բաժանարարը նույնպես պրիմիտիվ է, ուրեմն, եթե մեզ հայտնի է $k(x)$-ը, ապա

$$d(x) = \mathrm{pp}\big(k(x)\big):$$

3.4.4 Օրինակ. Կիրառենք այս կանոնը 3.4.2 օրինակի դեպքում: Այնտեղ ստացել էինք, որ $\big(f_p(x),\ g_p(x)\big) = 2\,x + 2$: Մյուս կողմից, $w = (1, 1) = 1$: Ուրեմն՝ $t \cdot \big(f_p(x),\ g_p(x)\big)$ բազմանդամի ավագ գործակիցը 1 դարձնելու համար վերցնենք $t = 2$ եւ հաշվենք $2(2\,x + 2) = x + 1$: Ըստ 3.2.8 ալգորիթմի՝ սրա նախապատկերն է $k(x) = x + 1$, իսկ $\mathrm{pp}(x + 1) = x + 1 = \big(f(x), g(x)\big)$:

Այսպիսով, 3.4.1 դիտողության մեջ նշված «ավելորդ» սկալյար արտադրիչների հետ կապված բարդությունը կարելի է շրջանցել Գաուսի լեմմայի օգնությամբ: Իսկ 3.4.2 օրինակի ոչ բարդ դեպքում մեր կառուցումներն արդեն իսկ վերջնական պատասխանի են բերում:

Նշենք, որ այս ընթացքում մենք արեցինք մի քայլ, որի համար p-ն չէր նախատեսված: Նախապատկերի վերականգնումն ապահովելու համար p-ն ավելի քան երկու անգամ մեծ է $f(x)$, $g(x)$ բազմանդամների բոլոր բաժանարարների գործակիցների բացարձակ արժեքներից: Վերջին քայլում, սակայն, մենք վերականգնեցինք մոդուլյար բաժանարարի $t \cdot \big(f_p(x),\ g_p(x)\big)$ *պատիկի* նախապատկերը: p թվով այդ պատիկի գործակիցների գնահատման հարցը այստեղ էական չէ, քանի որ կառուցվող ալգորիթմի աշխատանքի ընթացքում p-ն քայլ առ քայլ մեծանալու է:

Մենք $d(x) = \mathrm{pp}\big(k(x)\big)$ լուծումը ստացանք՝ ենթադրելով, որ $\deg d(x) = \deg\big(f_p(x),\ g_p(x)\big)$: Ազատվենք այս հավելյալ պայմանից: Նախ դիտարկենք մի օրինակ, որը ցույց է տալիս, որ այդ հավասարությունը միշտ չէ, որ տեղի ունի:

3.4.5 Օրինակ. Ենթադրենք $f(x) = x^2 + 1$ եւ $g(x) = x + 1$: Ակնհայտ է, որ այս բազմանդամները պրիմիտիվ եւ պարզ են $\mathbb{Z}[x]$ օղակում. $d(x) = \big(f(x), g(x)\big) = 1$: Նրանց բոլոր հնարավոր բաժանարարների բոլոր գործակիցները հավասար են 1-ի: Վերցնենք այն երկու անգամ գերազանցող $p = 2$ պարզ մոդուլը: $\varphi_2\colon \mathbb{Z}[x] \to \mathbb{Z}_2[x]$ անցումից հետո կրկին $f_2(x) = x^2 + 1$ եւ $g_2(x) = x + 1$ (այսինքն՝ բազմանդամների գրությունները նույնիսկ չեն էլ փոխվել): Բայց $\mathbb{Z}_2[x]$-ում տեղի ունի $f_2(x) = x^2 + 1 = x^2 + 1^2 = (x + 1)(x + 1)$: Ուստի $\big(f_2(x), g_2(x)\big) = x + 1 \in \mathbb{Z}_2[x]$: Հասկանալի է, որ $d(x) = 1$ ամենամեծ ընդհանուր բաժանարարի համար նրա $\varphi_p\big(d(x)\big) = d_p(x) = 1$ պատկերը ոչ մի p մոդուլի համար $x + 1$ չի լինի՝ $1 = \deg d(x) < \deg\big(f_2(x),\ g_2(x)\big) = 2$:

Այս անսպասելի «անհամապատասխանության» պատճառն այն է, որ բաժանելիությունը $\mathbb{Z}[x]$ եւ $\mathbb{Z}_2[x]$ օղակներում էապես տարբեր հատկություն է, եթե անգամ $f(x)$ եւ $f_2(x)$ կամ $g(x)$ եւ $g_2(x)$ բազմանդամների գրությունները համընկնում են: Իսկապես, $\mathbb{Z}_2[x]$-ում տեղի ունի

$$\begin{array}{r|l} x^2 + 1 & x + 1 \\ \cline{2-2} x^2 + x & x + 1 \\ \cline{1-1} x + 1 & \\ x + 1 & \\ \cline{1-1} 0 & \end{array}$$

«անկյունով» բաժանումը, որին $\mathbb{Z}[x]$-ում կհամապատասխանի հետեւյալ բաժանումը.

$$\begin{array}{r|l} x^2 + 1 & x + 1 \\ \cline{2-2} x^2 + x & x - 1 \\ \cline{1-1} -x + 1 & \\ -x - 1 & \\ \cline{1-1} 2 & \end{array}$$

իսկ դրա արդյունքում ստացվում է $r = 2 \neq 0$ մնացորդը:

Ուստի ընդհանուր դեպքում առայժմ չենք կարող պնդել, թե նախորդ քայլերում մեր ստացած $d(x) = \mathrm{pp}\big(k(x)\big)$ բազմանդամը կլինի $\big(f(x),\ g(x)\big)$ ամենամեծ ընդհա-

նուր բաժանարարը, քանի որ այն կարող է եւ ընդհանրապես չբաժանել $f(x),\ g(x)$ պրիմիտիվ բազմանդամներից որեւէ մեկը: Սակայն մեր ստացած սահմանափակումները արդեն թույլ են տալիս ասել, որ մենք գտնվում ենք հետեւյալ երկու իրավիճակներից մեկում. կամ $d(x)$-ը $f(x),\ g(x)$ բազմանդամների ընդհանուր բաժանարարն է, եւ այդ դեպքում դա նրանց *ամենամեծ* ընդհանուր բաժանարարն է, կամ էլ $d(x)$-ը չի բաժանում $f(x),\ g(x)$ բազմանդամներից որեւէ մեկը, եւ այդ դեպքում մենք գործ ունենք բաժանելիության պահպանման խնդրի հետ:

Իսկապես, ենթադրենք $f(x),\ g(x) \vdots d(x)$: Ըստ p-ի ընտրության, այն գերազանցում է նաեւ $d(x)$-ի ավագ գործակցի բացարձակ արժեքը, ուստի φ_p անցումը չի փոքրացնում $d(x)$-ի աստիճանը.

$$\deg d(x) = \deg d_p(x):$$

Քննարկելով $\mathbb{Z}[x]$ օղակում բազմանդամների ամենամեծ ընդհանուր բաժանարարի աստիճանի հարցը, մենք ապացուցել ենք, որ $f(x),\ g(x)$ պրիմիտիվ բազմանդամների ամենաբարձր աստիճանի $d(x)$ ընդհանուր բաժանարարն ասոցացված է $\big(f(x), g(x)\big)$-ին այն եւ միայն այն դեպքում, երբ $d(x)$-ը նույնպես պրիմիտիվ է (տես 2.7.3 եւ 2.7.1 լեմմաները): Քանի որ $d(x) = \mathrm{pp}\big(k(x)\big)$ բաժանարարը պրիմիտիվ է, ապա $d(x) \approx \big(f(x), g(x)\big)$ ըստ 2.7.3 լեմմայի:

Այդ իրավիճակի միակ հնարավոր այլընտրանքը կստացվի, եթե $f(x)$-ը կամ $g(x)$-ը չբաժանվի $d(x) = \mathrm{pp}\big(k(x)\big)$ բազմանդամի վրա, չնայած տվյալ p-ի համար $f_p(x)$-ը եւ $g_p(x)$-ը բաժանվում են $\varphi_p\big(d(x)\big) = \Big(f_p(x), g_p(x)\Big)$ բազմանդամի վրա: Այսինքն, բախվել ենք բաժանելիության պահպանման խնդրին:

Ի մի բերենք մեր հավաքած փաստերը. ըստ $f(x)$ եւ $g(x)$ պրիմիտիվ բազմանդամների p պարզ թիվն ընտրելով (3.12) պայմանով, հաշվելով $t \cdot \Big(f_p(x), g_p(x)\Big)$ մոդուլար բազմանդամը եւ կառուցելով նրա $k(x)$ նախապատկերի $d(x)$ պրիմիտիվ մասը՝ մենք կարող ենք պնդել, որ կամ $d(x)$-ը բաժանում է $f(x),\ g(x)$ բազմանդամները (եւ հանդիսանում է դրանց ամենամեծ ընդհանուր բաժանարարը), կամ էլ տվյալ p-ի համար բախվել ենք բաժանելիության պահպանման խնդրին: Այդ երկրորդ այլընտրանքային դեպքը շրջանցելու համար օգտվենք բազմանդամների ռեզուլտանտի հատկություններից:

3.4.6 Լեմմա. *Եթե p պարզ թիվը չի բաժանում $f(x),\ g(x) \in \mathbb{Z}[x]$ բազմանդամների $a_0,\ b_0$ ավագ գործակիցներից գոնե մեկը եւ $d(x) = \big(f(x),\ g(x)\big)$, ապա* $\deg d(x) \le \deg\Big(f_p(x), g_p(x)\Big)$*: Իսկ եթե p-ն չի բաժանում նաեւ*

(3.13) $$R = \operatorname{res}(f(x)/d(x), g(x)/d(x))$$

ռեզուլտանտը, ապա նաեւ

$$\deg d(x) = \deg d_p(x) = \deg\big(f_p(x), g_p(x)\big).$$

Ապացույց: $f(x)/d(x)$ եւ $g(x)/d(x)$ բազմանդամները փոխադարձաբար պարզ են: $d(x)$-ի ավագ գործակիցը բաժանում է $f(x)$, $g(x)$ բազմանդամների a_0, b_0 ավագ գործակիցներից երկուսն էլ: Ուստի, ըստ p-ի ընտրության, $d(x)$-ի ավագ գործակիցը չի բաժանվում p-ի վրա, $d_p(x)$ պատկերը զրոյական չէ, եւ կոռեկտ է դիտարկել $f_p(x)/d_p(x)$ եւ $g_p(x)/d_p(x)$ քանորդները: Հեշտ է նկատել, որ

$$\big(f_p(x), g_p(x)\big) = d_p(x)\big(f_p(x)/d_p(x), g_p(x)/d_p(x)\big).$$

Իսկ այստեղից պարզ է, որ $\deg d_p(x) \neq \deg\big(f_p(x), g_p(x)\big)$ անհավասարությունը կարող է տեղի ունենալ միայն, երբ $\big(f_p(x)/d_p(x), g_p(x)/d_p(x)\big) \not\approx 1$ կամ որ նույնն է՝

$$\deg\big(f_p(x)/d_p(x), g_p(x)/d_p(x)\big) > 0,$$

այսինքն՝ երբ $f_p(x)/d_p(x)$ եւ $g_p(x)/d_p(x)$ բազմանդամները ունեն մի ոչ տրիվիալ ընդհանուր բաժանարար (գործ ունենք մոդուլյար անցման ժամանակ բաժանելիության խախտման հետ):

Ըստ 3.3.6 թեորեմի՝ $\mathbb{Z}_p$ դաշտի վրա տրված $f_p(x)/d_p(x)$ եւ $g_p(x)/d_p(x)$ բազմանդամները փոխադարձաբար պարզ չեն այն եւ միայն այն դեպքում, երբ

$$\operatorname{res}\big(f_p(x)/d_p(x), g_p(x)/d_p(x)\big) = 0.$$

Վերը նշված ռեզուլտանտը հանդիսանում է $S_{f_p/d_p,\, g_p/d_p}$ Սիլվեստրի մատրիցի որոշիչը: Հաշվի առնելով *մատրիցային* մոդուլյար անցման ժամանակ φ_p հոմոմորֆիզմի ազդեցությունը մատրիցների տարրերի վրա՝ հեշտ է տեսնել, որ $S_{f_p/d_p,\, g_p/d_p}$ մատրիցը ստացվում է $f(x)/d(x)$ եւ $g(x)/d(x)$ բազմանդամների $S_{f/d,g/d}$ Սիլվեստրի մատրիցից՝ նրա յուրաքանչյուր տարրի վրա կիրառելով φ_p *թվային* մոդուլյար անցումը:

Մյուս կողմից, քանի որ մատրիցի որոշիչը հանդիսանում է այդ մատրիցի որոշ տարրերի արտադրյալների գումար եւ տարբերություն (եւ քանի որ այդ գործողությունները ժառանգական են φ_p հոմոմորֆիզմի նկատմամբ), պարզ է, որ.

$$\operatorname{res}\big(f_p(x)/d_p(x), g_p(x)/d_p(x)\big) = \varphi_p\big(\operatorname{res}(f(x)/d(x), g(x)/d(x))\big) = \varphi_p(R) = R_p.$$

Իսկ այստեղից պարզ է, որ հավասարության ձախ կողմի ռեզուլտանտը զրոյական է $\mathbb{Z}_p$ դաշտում միայն, երբ հավասարության աջ կողմի R ռեզուլտանտը բաժանվում է p

պարզ թվի վրա: Ըստ մեր լեմմայի պայմանների՝ դա կարող է տեղի ունենալ միայն, երբ $R = 0$, բայց այդ դեպքն էլ բացառվում է, քանի որ $f(x)/d(x)$ եւ $g(x)/d(x)$ բազմանդամները փոխադարձաբար պարզ են: ■

3.4.7 Դիտողություն. Նկատենք, որ այս լեմմայում p պարզ թվի վրա դրված առաջին պայմանը ($p \nmid a_0$ կամ $p \nmid b_0$) արդեն իսկ կատարվում է (3.12) պայմանի կատարման դեպքում:

Վերադառնանք ամենամեծ ընդհանուր բաժանարարի ալգորիթմին: 3.4.6 լեմման պնդում է, որ բաժանելիության պահպանման խնդրի հետ կապված երկրորդ այլընտրանքը կարող է տեղի ունենալ միայն, երբ p-ն բաժանում է R ռեզուլտանտը: Մենք, դժբախտաբար, չենք կարող հաշվել R-ը, քանի որ մեզ հայտնի չէ $d(x)$ արտադրիչը (3.4.6 լեմմայի (3.13) բանաձեւում մասնակցող $d(x)$-ը ոչ թե մեր կառուցած $d(x) = \mathrm{pp}\big(k(x)\big)$-ն է, այլ $f(x), g(x)$ ամենամեծ ընդհանուր բաժանարարը, որն առայժմ հայտնի չէ): Այնուամենայնիվ, 3.4.6 լեմման հուշում է, որ մեր հաշված $d(x) = \mathrm{pp}\big(k(x)\big)$ բազմանդամը կարող է տարբեր լինել $d(x) = \big(f(x),\ g(x)\big)$ ամենամեծ ընդհանուր բաժանարարից *միայն վերջավո՛ր քանակությամբ p պարզ մոդուլների համար*: Ավելին, խոսքի ազատություն թույլ տալով, կարող ենք ասել, որ $d(x) \not\approx \big(f(x),\ g(x)\big)$ անհավասարությունը տեղի ունի միայն «քիչ քանակությամբ» p պարզ թվերի համար, քանի որ R ռեզուլտանտի պարզ բաժանարարների քանակը մեծ չէ (տես 3.5 պարագրաֆը):

Ալգորիթմի կառուցումը կարելի է եզրափակել հետեւյալ քայլերով. ենթադրենք ըստ (3.12) պայմանի ընտրված p պարզ մոդուլի հաշվել ենք $d(x)$ բազմանդամը: Եթե $f(x),\ g(x)$ բազմանդամներից գոնե մեկը չի բաժանվում $d(x)$-ի վրա, ապա ընտրենք մի այլ, ավելի մեծ p եւ կրկնենք քայլերը ըստ այդ նոր մոդուլի: Ոչ ավել, քան վերջավոր քանակությամբ քայլերից հետո անպայման կհասնենք մի p-ի, ըստ որի ստացված $d(x)$ բազմանդամի համար $f(x) \vdots d(x)$ եւ $g(x) \vdots d(x)$: Ուրեմն եւ՝ $d(x) = \big(f(x),\ g(x)\big)$:

Մնում է ստացվածը բազմապատկել ամենասկզբում ֆիքսված $r = \Big(\mathrm{cont}\big(f(x)\big), \mathrm{cont}\big(g(x)\big)\Big)$ սկալյարով եւ ստանալ վերջնական բազմանդամը $r \cdot d(x)$ տեսքով:

Ձեւակերպենք մեր կառուցած ալգորիթմը.

3.4.8 Ալգորիթմ (ամենամեծ ընդհանուր բաժանարարի հաշվման մեծ պարզ թվի մեթոդը). Տրված են $f(x),\ g(x) \in \mathbb{Z}[x]$ ոչ զրոյական բազմանդամները: Հաշվել նրանց $\big(f(x),\ g(x)\big)$ ամենամեծ ընդհանուր բաժանարարը:

1. $f(x)$, $g(x)$ բազմանդամների համար Էվկլիդեսի ալգորիթմով հաշվենք նրանց $\operatorname{cont}\big(f(x)\big)$ եւ $\operatorname{cont}\big(g(x)\big)$ բովանդակությունները: Դրանց նշաններն ընտրենք այնպես, որ $f(x)/\operatorname{cont}\big(f(x)\big) = \operatorname{pp}\big(f(x)\big)$ եւ $g(x)/\operatorname{cont}\big(g(x)\big) = \operatorname{pp}\big(g(x)\big)$ հարաբերությունների ավագ գործակիցները դրական լինեն:

2. Էվկլիդեսի ալգորիթմով հաշվենք $r = \Big(\operatorname{cont}\big(f(x)\big),\ \operatorname{cont}\big(g(x)\big)\Big)$ ամենամեծ ընդհանուր բաժանարարը:

3. Նշանակենք $f(x) = \operatorname{pp}\big(f(x)\big)$ եւ $g(x) = \operatorname{pp}\big(g(x)\big)$:

4. a_0-ով նշանակենք $f(x)$-ի ավագ գործակիցը, b_0-ով նշանակենք $g(x)$-ի ավագ գործակիցը (դրանք դրական են ըստ մեր կառուցման):

5. Էվկլիդեսի ալգորիթմով հաշվենք $w = (a_0, b_0)$ դրական ամենամեծ ընդհանուր բաժանարարը:

6. Լանդաու-Մինյոտի բանաձեւի (3.3) հետեւանքով հաշվենք $N_{f,g}$ գնահատականը:

7. Ընտրենք մի $p > 2 \cdot N_{f,g}$ պարզ թիվ, որը չի օգտագործվել նախորդ քայլերում:

8. φ_p մոդուլյար անցումն իրականացնենք ըստ p մոդուլի եւ հաշվենք $f(x),\ g(x) \in \mathbb{Z}[x]$ բազմանդամների $f_p(x), g_p(x) \in \mathbb{Z}_p[x]$ պատկերները:

9. $\mathbb{Z}_p[x]$ օղակում Էվկլիդեսի ալգորիթմով հաշվենք $\Big(f_p(x),\ g_p(x)\Big)$ ամենամեծ ընդհանուր բաժանարարը:

10. Ստացված $\Big(f_p(x),\ g_p(x)\Big)$-ը p մոդուլով բազմապատկենք այնպիսի մի $t \in \mathbb{Z}_p$ թվով, որ $t \cdot \Big(f_p(x),\ g_p(x)\Big)$ արտադրյալի ավագ գործակիցը հավասար լինի w-ին:

11. Ըստ 3.2.8 ալգորիթմի հաշվենք $t \cdot \Big(f_p(x),\ g_p(x)\Big)$ բազմանդամի $k(x) \in \mathbb{Z}[x]$ նախապատկերը:

12. $\mathbb{Z}$ օղակում Էվկլիդեսի ալգորիթմով հաշվենք $\operatorname{cont}\big(k(x)\big)$ բովանդակությունը:

13. Նշանակենք $d(x) = k(x)/\operatorname{cont}\big(k(x)\big) = \operatorname{pp}\big(k(x)\big)$:

14. Եթե $f(x) \vdots d(x)$ եւ $g(x) \vdots d(x)$

15. անցնենք ալգորիթմի 18-րդ քայլին;

16. հակառակ դեպքում

17. վերադառնանք ալգորիթմի 7-րդ քայլին:

18. Որոնելի ամենամեծ ընդհանուր բաժանարարը դուրս գրենք $r \cdot d(x)$ տեսքով:

Այս ալգորիթմն անվանում են ամենամեծ ընդհանուր բաժանարարի հաշվման «մեծ պարզ թվի» ալգորիթմ, որպեսզի տարբերեն այն ընդհանուր բաժանարարի հաշվման այլ ալգորիթմներից, մասնավորապես, «կեղծ բաժանումների» 2.6.20 ալգորիթմից կամ «փոքր պարզ թվերի» 5.3.10 ալգորիթմից, որին կծանոթանանք ավելի ուշ, եւ որի աշխատանքի սկզբունքն է ոչ թե հաշվարկն ըստ բավականաչափ մեծ պարզ թվի, այլ հաշվարկն ըստ մի քանի տարբեր փոքր պարզ թվերի (տես 5.3 պարագրաֆը): Տես նաեւ 3.5.3 եւ 3.5.7 դիտողությունները 3.4.8 ալգորիթմի որոշ գնահատականների ճշտման մասին:

Քիչ հետո այս ալգորիթմը կկիրառենք 1.3 պարագրաֆում բերված այն բազմանդամների համար, որոնց վրա քննարկել ենք միջանկյալ արժեքների ուռճացման երեւույթը եւ այն շրջանցելու Կնուտի մոդուլյար մեթոդը.

$$f(x) = x^8 + x^6 - 3x^4 - 3x^3 + 8x^2 + 2x - 5$$
$$g(x) = 3x^6 + 5x^4 - 4x^2 - 9x + 21: \tag{3.14}$$

Մինչ այդ կրկին նկատենք, որ 1.3 պարագրաֆի ապացույցը, ըստ էության, հանգում էր $\varphi_5\colon \mathbb{Z}[x] \to \mathbb{Z}_5[x]$ մոդուլյար անցմանը: Մենք ստանում էինք

$$\varphi_5\big(f(x)\big) = f_5(x) = x^8 + x^6 + 2x^4 + 2x^3 + 3x^2 + 2x,$$
$$\varphi_5\big(g(x)\big) = g_5(x) = 3x^6 + x^2 + x + 1 \tag{3.15}$$

մոդուլյար բազմանդամները եւ ցույց տալիս, որ դրանք փոխադարձաբար պարզ են, եւ որ դրանց փոխադարձ պարզությունից բխում է նաեւ $f(x)$ եւ $g(x)$ բազմանդամների փոխադարձ պարզությունը:

Այս բազմանդամների համար նույն արդյունքը կստանանք նաեւ 3.4.8 ալգորիթմի միջոցով, ընդ որում, ստիպված կլինենք օգտվել 5-ից ավելի մեծ p պարզ թվից: Բայց, նախ, բերենք մի օրինակ, որը մեզ կհամոզի, որ միշտ չէ, որ հնարավոր է հարցը լուծել շատ փոքր պարզ թվերի միջոցով (ինչպես Կնուտի օրինակում էր, որտեղ ունեինք $p = 5$).

3.4.9 Օրինակ. Վերցնենք Կնուտի օրինակում բերված (3.14) բազմանդամները, բայց որպես պարզ մոդուլ վերցնենք $p = 2$: Այս դեպքում.

$$\varphi_2\big(f(x)\big) = f_2(x) = x^8 + x^6 + x^4 + x^3 + 1,$$
$$\varphi_2\big(g(x)\big) = g_2(x) = x^6 + x^4 + x + 1: \tag{3.16}$$

Այս օրինակում $f_2(x)$ եւ $g_2(x)$ բազմանդամներն արդեն փոխադարձաբար պարզ չեն, քանի որ.

$$\begin{array}{l|l} x^8+x^6+x^4+x^3+1 & x^6+x^4+x+1 \\ \cline{2-2} x^8+x^6+x^3+x^2 & x^2 \\ \cline{1-1} x^4+x^2+1 & \end{array}$$

$$\begin{array}{l|l} x^6+x^4+x+1 & x^4+x^2+1 \\ \cline{2-2} x^6+x^4+x^2 & x^2 \\ \cline{1-1} x^2+x+1 & \end{array}$$

$$\begin{array}{l|l} x^4+x^2+1 & x^2+x+1 \\ \cline{2-2} x^4+x^3+x^2 & x^2+x+1 \\ \cline{1-1} x^3+1 & \\ x^3+x^2+x & \\ \cline{1-1} x^2+x+1 & \\ x^2+x+1 & \\ \cline{1-1} 0 & \end{array}$$

Ունենք $1 \approx \big(f_2(x),\ g_2(x)\big) = x^2+x+1 \in \mathbb{Z}_2[x]$: Մինչդեռ, ինչպես արդեն ցույց ենք տվել 1.3 պարագրաֆում, $f(x)$ եւ $g(x)$ բազմանդամները $\mathbb{Z}[x]$-ում փոխադարձաբար պարզ են: Այսինքն՝ Կնուտի օրինակի մոտեցումը այլեւս չի գործի, եթե վերցնենք ոչ թե $p=5$, այլ $p=2$: Հետեւաբար, երբեմն չենք կարող խուսափել մեծ պարզ թվեր կիրառելուց:

3.4.10 Օրինակ. Կրկին դիտարկենք Կնուտի օրինակի (3.14) բազմանդամները, եւ դրանց վրա կիրառենք 3.4.8 ալգորիթմը: $f(x)$ եւ $g(x)$ բազմանդամները պրիմիտիվ են եւ $r = \big(\mathrm{cont}\big(f(x)\big),\ \mathrm{cont}\big(g(x)\big)\big) = (1,1) = 1$: Ունենք.

$$\|f(x)\| = \sqrt{1+1+9+9+64+4+25} = \sqrt{113} < 11,$$

$$\|g(x)\| = \sqrt{9+25+14+81+441} = \sqrt{570} < 24:$$

Ըստ (3.3) բանաձեւի՝

$$N_{f,g} = 2^{\min\{8,6\}}\,(1{,}3)\min\left\{\frac{\sqrt{113}}{1}, \frac{\sqrt{570}}{3}\right\} < 2^6 \cdot 1 \cdot \frac{24}{3} = 512:$$

Ըստ (3.12) պայմանի՝ որպես մոդուլ կարող ենք ընտրել $p = 1031 > 2 \cdot 512$ պարզ թիվը:

Գնահատականների տարբերությունը տեսնելու համար փորձենք գնահատել նաեւ ըստ (3.2) բանաձեւի: Ունենք.

$$N_f = 2^{8-1} \cdot \sqrt{113} < 2^{8-1} \cdot 11 = 1408,$$
$$N_g = 2^{6-1} \cdot \sqrt{570} < 2^{6-1} \cdot 24 = 768:$$

Որպես մոդուլ կարող ենք ընտրել $p = 2819 > 2 \cdot 1408$ պարզ թիվը: Ինչպես տեսնում ենք, երկրորդ գնահատականն ավելի կոպիտ է: Մոդուլյար անցումը կարող ենք իրականացնել ըստ դրանցից կամայականի, ենթադրենք, երկրորդի. $\varphi_p = \varphi_{2819}$: Կստանանք՝

$$\begin{aligned} \varphi_{2819}\big(f(x)\big) &= f_{2819}(x) \\ &= x^8 + x^6 + 2816x^4 + 2816x^3 + 8x^2 + 2x + 2814, \\ \varphi_{2819}\big(g(x)\big) &= g_{2819}(x) = 3x^6 + 5x^4 + 2815x^2 + 2810x + 21: \end{aligned} \tag{3.17}$$

Կիրառենք Էվկլիդեսի ալգորիթմի քայլերը (համառոտության համար այստեղ բաց ենք թողնում «անկյունով բաժանումները»).

$$f_{2819}(x) = (940x^2 + 313) \cdot g_{2819}(x) + 2192x^4 + 1253x^2 + x^2 + 1879,$$

$$\begin{aligned} g_{2819}(x) = (1686x^2 + 892) \cdot (2192x^4 + 1253x^2 + x^2 + 1879) \\ +2025x^2 + 2810x + 1258, \end{aligned}$$

$$\begin{aligned} 2192x^4 + 1253x^2 + x^2 + 1879 \\ = (2447x^2 + 2667x + 1928) \cdot (2025x^2 + 2810x + 1258) \\ +2781x + 817, \end{aligned}$$

$$2025x^2 + 2810x + 1258 = (466x + 2675) \cdot (2781x + 817) + 508,$$

$$2781x + 817 = 1587x \cdot 508 + 855,$$

$$508 = 2813 \cdot 855 + 0:$$

Վերջին ոչ զրոյական մնացորդն է $\big(f_{2819}(x),\ g_{2819}(x)\big) = 855$ հաստատունը, որը զրոյական չէ եւ հակադարձելի է $\mathbb{Z}_{2819}$ օղակում: Ըստ 3.2.8 ալգորիթմի՝ 855-ի նախապատկերն է $k(x) = 855 \in \mathbb{Z}[x]$ բազմանդամը, քանի որ $855 < 2819/2$: Քանի որ $\mathrm{cont}\big(k(x)\big) = \mathrm{cont}(855) = 855$, ապա $\mathrm{pp}\big(k(x)\big) = 855/855 = 1$: Վերջնական պատասխանն է $\big(f(x),\ g(x)\big) = r \cdot \mathrm{pp}\big(k(x)\big) = 1 \cdot 1 = 1$:

3.4.11 Վարժություն. Կատարել 3.4.10 օրինակի հաշվարկը նաեւ ըստ $p = 1031$ մոդուլի: Համեմատել հաշվարկի բարդությունը 3.4.10 օրինակի հետ:

3.4.12 Վարժություններ. Հաշվել $f(x)$, $g(x)$ բազմանդամների ամենամեծ ընդհանուր բաժանարարը մեծ պարզ թվի ալգորիթմով.

1) $f(x) = 3x^3 - 8x^2 + 5x - 2$ եւ $g(x) = 2x^3 - 5x^2 + 3x - 2$,
2) $f(x) = 4x^3 - 13x^2 + 4x - 3$ եւ $g(x) = 2x^3 - 9x^2 + 10x - 3$,
3) $f(x) = 2x^4 - 2x^3 - 2x^2 + 3x - 1$ եւ $g(x) = x^4 - x^3 - 2x^2 + 2x$:

3.5 Ռեզուլտանտի պարզ բաժանարարների գնահատականներ

Այս պարագրաֆում մենք կստանանք $R = \operatorname{res}(f(x)/d(x), g(x)/d(x))$ ռեզուլտանտի մի քանի հատկություններ, որոնք ոչ միայն հավելյալ գնահատականներ են տալիս 3.4.8 ալգորիթմի մասին, այլեւ օգտագործվելու են հաջորդ պարագրաֆում՝ նոր ալգորիթմ կառուցելիս:

3.4.8 ալգորիթմի կառուցման ընթացքում R ռեզուլտանտի դերը կարեւոր էր այն առումով, որ եթե p-ն ըստ $p > N_{f,g}$ բանաձեւի ընտրված բավականաչափ մեծ պարզ թիվ էր, ապա $\varphi_p\colon \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ մոդուլյար անցման ժամանակ կարող էինք բախվել (նախապատկերի) բաժանելիության պահպանման խնդրին միայն այն դեպքում, երբ p-ն R-ի բաժանարար էր: Այսինքն՝ այդ դեպքում $f(x)$, $g(x)$ պրիմիտիվ բազմանդամների պատկերների համար հաշվված $t \cdot \big(f_p(x), g_p(x)\big)$ մոդուլյար ամենամեծ բաժանարարի $k(x)$ նախապատկերի $d(x) = \operatorname{pp}\big(k(x)\big)$ պրիմիտիվ մասը կարող էր $\big(f(x), g(x)\big)$ ամենամեծ ընդհանուր բաժանարարը չլինել: Ինչպես նշեցինք 3.4 պարագրաֆում, R-ը հաշվել չենք կարող, քանի որ մեզ հայտնի չէ $d(x)$-ը:

Այնուամենայնիվ, կարելի է գնահատել ինչպես R-ի արժեքը, այնպես էլ այն բաժանող պարզ թվերի քանակը: Սկսենք առաջին գնահատականից:

3.5.1 Լեմմա. *Կամայական $f(x),\ g(x) \in \mathbb{Z}[x]$ բազմանդամների եւ նրանց ցանկացած $d(x)$ ընդհանուր բաժանարարի համար տեղի ունի հետեւյալ գնահատականը*

$$|R| = \big|S_{f/d,g/d}\big| \le \sqrt{(n+1)^m (m+1)^n}\, N_f^m N_g^n, \tag{3.18}$$

որտեղ $n = \deg f(x),\ m = \deg g(x)$:

Ապացույց: Ցանկացած $d(x)$-ի համար $\deg f(x)/d(x) \le n$ եւ $\deg g(x)/d(x) \le m$: Քանի որ $f(x)/d(x)$ եւ $g(x)/d(x)$ հարաբերությունները $f(x)$ եւ $g(x)$ բազմանդամների բաժանարարներ են, ապա ըստ (3.2) բանաձեւի՝ դրանց գործակիցները բացարձակ արժեքով սահմանափակ են, համապատասխանաբար, $N_f = 2^{n-1}\|f(x)\|$ եւ $N_g = 2^{m-1}\|g(x)\|$ գնահատականներով: Հետեւաբար,

$$\|f(x)/d(x)\| \le \sqrt{(n+1)N_f^2} = \sqrt{n+1} \cdot N_f,$$

$$\|g(x)/d(x)\| \le \sqrt{(m+1)N_g^2} = \sqrt{m+1}\cdot N_g:$$

R ռեզուլտանտը $f(x)/d(x)$ եւ $g(x)/d(x)$ բազմանդամներին համապատասխանող $S_{f/d,g/d}$ Սիլվեստրի մատրիցի որոշիչն է (տես 3.3 պարագրաֆը): Այդ մատրիցը ոչ ավել, քան $n+m$ կարգի քառակուսի մատրից է, որի առաջին ոչ ավել, քան m տողերում գրված են $f(x)/d(x)$-ի գործակիցները (այդ գործակիցները ոչ ավել, քան $n+1$ հատ են), իսկ վերջին ոչ ավել, քան n տողերում գրված են $g(x)/d(x)$-ի գործակիցները (այդ գործակիցները ոչ ավել, քան $m+1$ հատ են): Տես (3.6) ներկայացումը 3.3 պարագրաֆում:

Կարող ենք օգտվել որոշիչի գնահատման (5.10) Ադամարի անհավասարությունից, որին ավելի մանրամասն կանդրադառնանք որոշիչների հաշվմանը նվիրված 5.2 պարագրաֆում: Քանի որ որոշիչը մատրիցի տրանսպոնացումից չի փոխվում, ապա կիրառենք Ադամարի բանաձեւը $S_{f/d,g/d}$ մատրիցի տողերի վրա՝ հաշվի առնելով նաեւ այն գնահատականները, որ ստացանք $\|f(x)/d(x)\|$ եւ $\|g(x)/d(x)\|$ նորմերի համար՝

$$|R| = \left|S_{f/d,g/d}\right| \le \underbrace{\sqrt{N_f^2+\cdots+N_f^2}^{\,m}}_{n+1}\ \underbrace{\sqrt{N_g^2+\cdots+N_g^2}^{\,n}}_{m+1} = \left(\sqrt{n+1}\cdot N_f\right)^m\left(\sqrt{m+1}\cdot N_g\right)^n,$$

որտեղից եւ ստացվում է լեմմայի գնահատականը: ■

3.5.2 Օրինակ. Ստանանք (3.18) գնահատականը Կնուտի օրինակի (3.14) բազմանդամների համար: Ինչպես հաշվել ենք 3.4.10 օրինակում, $N_f = 1408$, $N_g = 768$: Ուրեմն՝

$$\begin{aligned}|R| = \left|S_{f/d,g/d}\right| &\le \sqrt{(8+1)^6(6+1)^8}\cdot 1408^6\cdot 768^8\\ &= \sqrt{531441\cdot 5764801}\cdot 7791407675257913344\\ &\cdot 12102908786760836815 2576 =\\ &= 1750329\cdot 7791407675257913344\cdot 12102908786760836815 2576\\ &= 1.650537429958211858281024985826 5e+48:\end{aligned}$$

Ստացվում է շատ մեծ մի թիվ, որը ցույց է տալիս, թե ինչքան թույլ է (3.18) գնահատականը:

3.5.3 Դիտողություն. Եթե մենք 3.4.8 ալգորիթմում p պարզ թվի վրա դնեինք $p > 2\cdot\sqrt{(n+1)^m(m+1)^n}\,N_f^m N_g^n$ պայմանը, ապա $R = \det S_{f/d,g/d}$ ռեզուլտանտը չէր բաժանվի պարզ p-ի վրա, ու մենք պրիմիտիվ $f(x),\ g(x)$ բազմանդամների համար միանգամից կունենայինք $\mathrm{pp}\big(k(x)\big) = \big(f(x), g(x)\big)$: Այսինքն՝ վերջնական պատասխանը կստացվեր *միայն մեկ անգամ* պարզ p թիվ կիրառելով (կարիք չէր լինի նոր p վերցնելու եւ ալգորիթմի քայլերը կրկնելու դրա համար): Սակայն 3.5.2 օրինակը բացատրում է, թե ինչու մենք 3.4.8 ալգորիթմում չօգտագործեցինք (3.18) գնա-

հատականը: Ինչպես տեսանք այդ օրինակում, (3.18) գնահատականը կարող է շատ մեծ լինել, եւ դրա կիրառումն արդյունավետ չէ: Ավելի հեշտ է 3.4.8 ալգորիթմի քայլը կրկնելը, քան $1.650537429958211858281024985826 5e+48$ թիվը հաշվելը, այն երկու անգամ գերազանցող պարզ թիվ գտնելն ու մոդուլյար հաշվարկներն ըստ այդ պարզ թվի տանելը:

Այնուամենայնիվ, (3.18) գնահատականը կարող է օգտագործվել այլ կերպ, եթե մենք հիշենք, որ 3.4.8 ալգորիթմում մեզ հետաքրքրում էր ոչ թե կոնկրետ $|R| = |S_{f/d,g/d}|$ արժեքի մեծությունը, այլ դրա պարզ բաժանարարների քանակը:

$p_k\#$ սիմվոլով ընդունված է նշանակել առաջին k պարզ թվերի արտադրյալը.

$$p_k\# = p_1 \cdots p_k,$$

(որտեղ $p_1, \cdots, p_k$ թվերը առաջին k հատ պարզ թվերն են՝ $p_1 = 2$, $p_2 = 3$... եւլն): Օրինակ՝ $p_5\# = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 2310$: Երբեմն $p_k\#$ արժեքն անվանում են «k-րդ պրիմորիալ» (k-th primorial), բայց մենք կխուսափենք այդ տերմինի օգտագործումից, քանի որ «primorial» բառի հայերեն լավագույն թարգմանության պատասխանատվությունը չենք ուզում վերցնել: Այդ արժեքները շատ արագ են աճում. $p_{10}\#$ արժեքը մեծ է 6 միլիարդից՝

$$p_{10}\# = 6.469.693.230:$$

3.5.4 Լեմմա. *Տրված n բնական թվի՝ զույգ առ զույգ տարբեր պարզ բաժանարարների քանակը չի գերազանցում k-ն, որտեղ k-ն այն մեծագույն բնական թիվն է, որի համար $n \geq p_k\#$:*

Ապացույց: $p_k\#$ արժեքն ունի ճիշտ k հատ իրարից զույգ առ զույգ տարբեր պարզ բաժանարարներ՝ $p_1, \cdots, p_k$: Ընդ որում, k հատ տարբեր պարզ բաժանարարներ ունեցող թվերի մեջ $p_k\#$ արժեքը նվազագույնն է, քանի որ $p_1, \cdots, p_k$ պարզ թվերից կամայականը մի նոր պարզ թվով փոխարինելով՝ մենք կմեծացնենք դրանց արտադրյալը: Ուրեմն, եթե $n < p_k\#$, ապա n-ի պարզ բաժանարարների քանակը փոքր է k-ից: ■

3.5.5 Հետեւանք. Կամայական $f(x),\ g(x) \in \mathbb{Z}[x]$ բազմանդամների եւ նրանց ցանկացած $d(x)$ ընդհանուր բաժանարարի համար $R = S_{f/d,g/d}$ ռեզուլտանտի՝ զույգ առ զույգ տարբեր պարզ բաժանարարների քանակը չի գերազանցում k-ն, որտեղ k-ն այն մեծագույն բնական թիվն է, որի համար

$$\sqrt{(n+1)^m (m+1)^n}\, N_f^m N_g^n \geq p_k\#$$

(այստեղ $n = \deg f(x), m = \deg g(x), N_f = 2^{n-1}\|f(x)\|$ եւ $N_g = 2^{m-1}\|g(x)\|$):

3.5.6 Օրինակ. Վերադառնալով 3.5.2 օրինակի դեպքին՝ դժվար չէ հաշվել, որ

$$p_{30}\# = 3.161005464041760778814520629154 4e + 46 < 1.650537429958211858281024985826 5e + 48,$$

բայց $k = 31$ արժեքի համար արդեն.

$$p_{31}\# = 4.014476939333036189094441199026e + 48 > 1.650537429958211858281024985826 5e + 48:$$

Այսինքն՝ $S_{f/d,g/d}$-ի պարզ բաժանարարների քանակը ոչ ավել, քան 30 է, եւ 3.4.8 ալգորիթմը Կնուտի օրինակի (3.14) բազմանդամների համար կիրառելիս, ինչ պարզ թվեր էլ ընտրենք, մենք վերջնական ճշգրիտ պատասխանը կստանանք ոչ ավե,լ քան $30 + 1 = 31$ հատ պարզ թվեր դիտարկելուց հետո (կամայական 31 հատ պարզ թվերից գոնե մեկը չի լինի R-ի բաժանարար):

3.5.7 Դիտողություն. 3.5.5 հետեւանքը եւ 3.5.6 օրինակը ցույց են տալիս, որ, չնայած (3.18) գնահատականի մեծությանը, այն ալգորիթմներ կառուցելիս կարող է արդյունավետ լինել շնորհիվ այն հանգամանքի, որ $p_k\#$ արժեքը նույնպես շատ արագ է աճում՝ k-ից կախված (տես նաեւ 3.6.4 եւ 3.6.5 օրինակները, որտեղ k-ի փոքր արժեքներ են ստացվում): 3.4.8 ալգորիթմը կիրառելիս մենք միշտ վերջնական պատասխանը կստանանք ոչ ավել, քան $k + 1$ հատ պարզ թվեր օգտագործելուց հետո, որտեղ k-ն այն մեծագույն բնական թիվն է, որի համար $p_k\#$ արժեքը մեծ չէ

$$\sqrt{(n+1)^m(m+1)^n}\, N_f^m N_g^n$$

գնահատականից:

Կա մի մասնավոր դեպք, երբ այս դիտարկումը առանձնապես արդյունավետ է ալգորիթմ կառուցելիս: Դա կամայական $f(x),\ g(x) \in \mathbb{Z}[x]$ բազմանդամների փոխադարձ պարզության որոշման ալգորիթմն է, որին կանդրադառնանք հաջորդ պարագրաֆում:

3.6 Փոխադարձ պարզության ալգորիթմը եւ մեթոդի ընդհանրացումները

Նախորդ պարագրաֆի գնահատականների հիման վրա կարելի է ձեւափոխել 3.4.8 ալգորիթմի ընդհանուր սկզբունքը եւ ստանալ բազմանդամների փոխադարձ պարզության որոշման ավելի պարզ ալգորիթմ:

Ինչպես մենք նկատեցինք ավելի վաղ, φ_p մոդուլյար անցման ժամանակ բազմանդամի պատկերը կարող է այնքան փոքրանալ, որ այլեւս որեւէ էական ինֆորմացիա չպարունակի բազմանդամի մասին: Մասնավորապես, երկու փոխադարձաբար ոչ պարզ բազմանդամների ամենամեծ ընդհանուր բաժանարարի պատկերը կարող է հավասար լինել 1-ի:

3.6.1 Օրինակ. Վերցնենք $f(x) = 5x^2 + 11x + 2$ եւ $g(x) = 10x^2 - 3x - 1$: Այդ դեպքում $d(x) = \big(f(x), g(x)\big) = 5x + 1$: Բայց $\varphi_5\colon \mathbb{Z}[x] \to \mathbb{Z}_5[x]$ մոդուլյար անցման ժամանակ $f_5(x) = x + 2$ եւ $g_5(x) = 2x + 4$: Ուրեմն եւ $\big(f_5(x), g_5(x)\big) = x + 2 \neq 1$: Մյուս կողմից, $d_5(x) = \varphi_5(5x + 1) = 1$: Այսինքն՝ մոդուլյար անցումից հետո տրիվիալ է $d(x)$-ի $d_5(x)$ պատկերը, բայց ոչ $\big(f_5(x), g_5(x)\big)$ մոդուլյար ամենամեծ ընդհանուր բաժանարարը, եւ $d(x)$-ի մասին էական ինֆորմացիա չի պարունակում ոչ $d_5(x)$-ը, ոչ էլ $\big(f_5(x), g_5(x)\big)$-ը:

3.4.8 ալգորիթմում մենք խուսափում էինք նման խնդիրներից՝ վերցնելով $p > 2 \cdot N_{f,g}$: Դա բերում էր մեծ պարզ թվերի քննարկման, որոնցից կարելի է խուսափել, երբ մեր խնդիրն է միայն բազմանդամների փոխադարձ պարզության որոշումը:

Ինչպես տեսանք 3.4.6 լեմմայում, եթե p պարզ թիվը չի բաժանում $f(x),\ g(x) \in \mathbb{Z}[x]$ բազմանդամների $a_0,\ b_0$ ավագ գործակիցներից գոնե մեկը, ապա $\deg d(x) \leq \deg\big(f_p(x), g_p(x)\big)$: Այսինքն՝ նշված դեպքում բազմանդամների պատկերների ամենամեծ ընդհանուր բաժանարարի աստիճանը փոքր չէ բազմանդամների ամենամեծ ընդհանուր բաժանարարի աստիճանից:

3.4.6 լեմմայի հետեւյալ պարզ հետեւանքը հետաքրքիր է համեմատել 1.3 պարագրաֆում բերված Կնուտի մոդուլյար մեթոդի հետ.

3.6.2 Հետեւանք. Եթե p պարզ թիվը չի բաժանում տրված $f(x),\ g(x) \in \mathbb{Z}[x]$ պրիմիտիվ բազմանդամներից գոնե մեկի ավագ գործակիցը, եւ $f_p(x),\ g_p(x)$ բազմանդամները փոխադարձաբար պարզ են, ապա փոխադարձաբար պարզ են նաեւ $f(x)$ եւ $g(x)$ բազմանդամները:

Ապացույց: Եթե $\big(f_p(x), g_p(x)\big) = 1$, ապա

$$0 = \deg\big(f_p(x), g_p(x)\big) \geq \deg\big(f(x), g(x)\big),$$

այսինքն՝ $\big(f(x), g(x)\big) = c \neq 0$: Բայց քանի որ ըստ 2.6.9 հետեւանքի $\big(f(x), g(x)\big)$-ը նույնպես պրիմիտիվ է, ապա $c = \pm 1$: ■

Այս հետեւանքը թույլ է տալիս սկսել կամայական $f(x)$, $g(x)$ բազմանդամների փոխադարձ պարզության որոշման ալգորիթմի կառուցումը: Եթե, ըստ (3.12) պայմանի, բավականաչափ *մեծ* p պարզ թիվ գտնելու փոխարեն մենք որեւէ *փոքր* p պարզ թվի համար (որը չի բաժանում $f(x)$ եւ $g(x)$ պրիմիտիվ բազմանդամներից գոնե մեկի ավագ գործակիցը) պարզենք, որ $\big(f_p(x), g_p(x)\big) = 1$, ապա, ըստ 3.6.2 հետեւանքի, առանց 3.4.8 ալգորիթմի քայլերի էլ պարզ կլինի, որ $\big(f(x), g(x)\big) = 1$:

Իսկ կամայական (ոչ անպայման պրիմիտիվ) $f(x)$, $g(x) \in \mathbb{Z}[x]$ բազմանդամների դեպքը հեշտությամբ հանգում է սրան: Իսկապես, ներկայացնենք դրանք $f(x) = \mathrm{cont}\big(f(x)\big)\,\mathrm{pp}\big(f(x)\big)$ եւ $g(x) = \mathrm{cont}\big(g(x)\big)\,\mathrm{pp}\big(g(x)\big)$ տեսքերով: Եթե $\mathrm{cont}\big(f(x)\big)$ եւ $\mathrm{cont}\big(g(x)\big)$ բովանդակությունները փոխադարձաբար պարզ չեն, ապա փոխադարձաբար պարզ չեն նաեւ $f(x)$, $g(x)$ բազմանդամները: Իսկ եթե $\Big(\mathrm{cont}\big(f(x)\big),\ \mathrm{cont}\big(g(x)\big)\Big) = 1$, ապա խնդիրը կրկին բերվում է $\mathrm{pp}\big(f(x)\big)$ եւ $\mathrm{pp}\big(g(x)\big)$ պրիմիտիվ բազմանդամների փոխադարձ պարզության որոշմանը:

Միակ հարցը, որ առայժմ բաց է, հետեւյալն է. ի՞նչ անել, եթե մեր ընտրած p պարզ թվի համար $\big(f_p(x), g_p(x)\big) \neq 1$: Սա կարող է նշանակել կամ այն, որ $\big(f(x), g(x)\big) \neq 1$, կամ էլ այն, որ տվյալ p մոդուլով φ_p մոդուլյար անցումը «բավարար ինֆորմացիա չի պահպանել» $f(x),\ g(x)$ պրիմիտիվ բազմանդամների փոխադարձ պարզությունը որոշելու համար: 3.4.8 ալգորիթմի տրամաբանությամբ այս խնդիրը կարող էինք լուծել երկու քայլով՝ նախ պետք էր ի սկզբանե բավականաչափ մեծ p ընտրել, եւ հետո մեծացնել այն այնքան, մինչեւ ճշգրիտ պատասխանը ստացվի: Կարելի է այս խնդիրը ավելի հեշտ լուծել: Ըստ 3.5.5 հետեւանքի, «բավարար ինֆորմացիա չպահպանող» p պարզ թվերի քանակը ոչ ավել, քան k է, որտեղ

$$\sqrt{(n+1)^m (m+1)^n}\, N_f^m N_g^n \geq p_k\#:$$

Հետեւաբար, կարելի է նախապես հաշվել այս անհավասարությանը բավարարող մեծագույն k-ն, եւ $\big(f_p(x), g_p(x)\big) = 1$ պայմանը ստուգել կամայական $k+1$ հատ պարզ թվերի համար, որոնցից յուրաքանչյուրը չի բաժանում $f(x),\ g(x)$ պրիմիտիվ բազմանդամներից գոնե մեկի ավագ գործակիցը. $\big(f(x), g(x)\big) \neq 1$ պայմանը տեղի ունի այն եւ միայն այն դեպքում, եթե $\big(f_p(x), g_p(x)\big) \neq 1$ պայմանը տեղի ունի $k+1$ հատ այդպիսի պարզ թվերի համար: Այս մոտեցման առավելությունը ոչ միայն այն է, որ օգտագործում ենք շատ ավելի փոքր պարզ թվեր, այլեւ այն, որ այլեւս կարիք չկա ամեն քայլից հետո հաշվել $t \cdot \big(f_p(x), g_p(x)\big)$-ի $k(x)$ նախապատկերը, ապա այդ նախապատկերի $d(x) = \mathrm{pp}\big(k(x)\big)$ պրիմիտիվ մասը, ապա ստուգել $f(x) \vdots d(x)$ ու $g(x) \vdots d(x)$ պայմանները: Այս դեպքում, եթե $\big(f_p(x), g_p(x)\big) \neq 1$, ապա միանգամից

անցնում ենք հաջորդ p պարզ թվին եւ ստուգում, որ այս գործողությունը կրկնվի առնվազն $k+1$ անգամ: Ստանում ենք հետեւյալ ալգորիթմը.

3.6.3 Ալգորիթմ (բազմանդամների փոխադարձ պարզության որոշման մոդուլյար ալգորիթմը). Տրված են $f(x),\ g(x) \in \mathbb{Z}[x]$ ոչ զրոյական բազմանդամները: Գտնել փոխադարձաբար պա՞րզ են արդյոք նրանք:

1. $f(x),\ g(x)$ բազմանդամների համար Էվկլիդեսի ալգորիթմով հաշվենք նրանց $\operatorname{cont}\big(f(x)\big)$ եւ $\operatorname{cont}\big(g(x)\big)$ բովանդակությունները:

2. Էվկլիդեսի ալգորիթմով հաշվենք $r = \Big(\operatorname{cont}\big(f(x)\big),\ \operatorname{cont}\big(g(x)\big)\Big)$ ամենամեծ ընդհանուր բաժանարարը:

3. Եթե $r \not\approx 1$

4. $f(x),\ g(x)$ բազմանդամներ փոխադարձաբար պարզ չեն;

5. վերջ:

6. Նշանակենք $f(x) = \operatorname{pp}\big(f(x)\big)$ եւ $g(x) = \operatorname{pp}\big(g(x)\big)$:

7. a_0-ով նշանակենք $f(x)$-ի ավագ գործակիցը, b_0-ով նշանակենք $g(x)$-ի ավագ գործակիցը:

8. Էվկլիդեսի ալգորիթմով հաշվենք $w = (a_0, b_0)$ դրական ամենամեծ ընդհանուր բաժանարարը:

9. Նշանակենք $n = \deg f(x)$ եւ $m = \deg g(x)$:

10. $f(x)$ եւ $g(x)$ բազմանդամների համար (3.2) բանաձեւով հաշվենք $N_f = 2^{n-1}\|f(x)\|$ եւ $N_g = 2^{m-1}\|g(x)\|$ գնահատականները:

11. Նշանակենք $B = \sqrt{(n+1)^m (m+1)^n}\, N_f^m N_g^n$:

12. Առաջին պարզ թվերի $p_1, \cdots, p_k, \cdots$ հաջորդականության տարրերն իրարով բազմապատկելով՝ գտնենք այն վերջին (ամենամեծ) k ինդեքսը, որի համար տեղի ունի $B \geq p_k\# = p_1 \cdots p_k$:

13. Նշանակենք $i = 1$:

14. Ընտրենք մի $p \nmid w$ պարզ թիվ, որը չի օգտագործվել նախորդ քայլերում:

15. φ_p մոդուլյար անցումն իրականացնենք ըստ p մոդուլի եւ հաշվենք $f(x),\ g(x) \in \mathbb{Z}[x]$ բազմանդամների $f_p(x),\ g_p(x) \in \mathbb{Z}_p[x]$ պատկերները:

16. $\mathbb{Z}_p[x]$ օղակում Էվկլիդեսի ալգորիթմով հաշվենք $\big(f_p(x),\ g_p(x)\big)$ ամենամեծ ընդհանուր բաժանարարը:

17. Եթե $\big(f_p(x),\ g_p(x)\big) \approx 1$

18. $f(x),\ g(x)$ բազմանդամներ փոխադարձաբար պարզ են;

19. վերջ:

20. Եթե $i < k + 1$

21. նշանակենք $i = i + 1$;

22. վերադառնանք ալգորիթմի 14-րդ քայլին;

23. հակառակ դեպքում

24. $f(x),\ g(x)$ բազմանդամներ փոխադարձաբար պարզ չեն:

3.6.4 Օրինակ. Վերցնենք $f(x) = x^2 + 2x + 1$ եւ $g(x) = -2x - 6$ բազմանդամները: Դրանցից երկրորդը պրիմիտիվ չէ՝ $\mathrm{cont}\big(g(x)\big) = (-2, -6) = -2$: Քանի որ $r = \big(\mathrm{cont}\big(f(x)\big),\ \mathrm{cont}\big(g(x)\big)\big) = (1, -2) = 1$, ապա պարզապես անտեսենք $\mathrm{cont}\big(g(x)\big) = -2$ բովանդակությունը եւ $g(x)$-ը փոխարինենք $g(x) = \mathrm{pp}\big(g(x)\big) = (-2x - 6)/(-2) = x + 3$ բազմանդամով: Հաշվենք $N_f = 2^{2-1}\sqrt{1^2 + 2^2 + 1^2} = 2\sqrt{6} < 4.9$ եւ $N_g = 2^{1-1}\sqrt{1^2 + 3^2} = \sqrt{10} < 3.2$ գնահատականները (երկար տասնորդական կոտորակներից խուսափելու համար մենք դեպի վերեւ ենք կլորացնում բոլոր կոտորակները): Քանի որ $\deg f(x)/d(x) + \deg g(x)/d(x) \le 2 + 1 = 3$, ապա $S_{f/d,g/d}$ Սիլվեստրի մատրիցը կարող է լինել (ոչ ավել քան) երրորդ կարգի մի մատրից, որի առաջին տողում գրված են (ոչ ավել, քան) երկրորդ աստիճանի որեւէ բազմանդամի գործակիցներ (յուրաքանչյուր գործակիցը 4.9-ից փոքր), իսկ նրա վերջին (ոչ ավել, քան) երկու տողերում գրված են (ոչ ավել, քան) առաջին աստիճանի բազմանդամի գործակիցներ (յուրաքանչյուրը 3.2-ից փոքր): Ըստ Ադամարի բանաձեւի՝ R ռեզուլտանտը բացարձակ արժեքով փոքր է

$$\sqrt{(n+1)^m(m+1)}\, N_f^m N_g^n < \sqrt{3^1 \cdot 2^2} \cdot 4.9^1 \cdot 3.2^2 < 174$$

արժեքից: 174-ի պարզ բաժանարարների հնարավոր քանակը գնահատելու համար հաշվենք առաջին պարզ թվերի արտադրյալը: $2 \cdot 3 = 6 < 174,\ 2 \cdot 3 \cdot 5 = 30 < 174$ բայց $2 \cdot 3 \cdot 5 \cdot 7 = 210 > 174$: Հետեւաբար, ռեզուլտանտի հնարավոր պարզ արտադրիչների քանակը երեքից ավելի չէ, քանի որ կամայական չորս հատ տարբեր պարզ թվերի արտադրյալը մեծ է 174-ից: Եթե մենք ըստ կամայական չորս հատ պարզ թվերի (որոնցից յուրաքանչյուրը չի բաժանում $f(x),\ g(x)$ բազմանդամ-

ներից գոնե մեկի ավագ գործակիցը) ստանայինք, որ $f_p(x),\ g_p(x)$ պրիմիտիվ բազմանդամները փոխադարձ պարզ չեն, ապա փոխադարձաբար պարզ չէին լինի նաեւ $f(x),\ g(x)$ բազմանդամները: Բայց չորս անգամ ստուգելու կարիք չի լինում, քանի որ հակառակ պատասխանն է ստացվում արդեն երկրորդ քայլում: Եթե $p = 2$, ապա $f_2(x) = x^2 + 1$ եւ $g_2(x) = x + 1$: Ինչպես հեշտ է ստուգել Էվկլիդեսի ալգորիթմով, $\big(f_2(x), g_2(x)\big) = x + 1 \neq 1$: Եթե $p = 3$, ապա $f_3(x) = x^2 + 2x + 1$ եւ $g_3(x) = x$: Ունենք $\big(f_3(x), g_3(x)\big) = 1$: Ուրեմն եւ՝ $\big(f(x), g(x)\big) = 1$:

3.6.5 Օրինակ. Փոխենք նախորդ օրինակի երկրորդ բազմանդամը, որպեսզի ունենանք փոխադարձաբար ոչ պարզ բազմանդամների օրինակ եւս. $f(x) = x^2 + 2x + 1$ եւ $g(x) = x + 1$: Երկու բազմանդամներն էլ պրիմիտիվ են: Ունենք $N_f = 2\sqrt{6} < 4.9$ եւ $N_g = 2^{1-1}\sqrt{1^2 + 1^2} = \sqrt{2} < 1.5$: Կրկին, ըստ Ադամարի բանաձեւի, R ռեզուլտանտը բացարձակ արժեքով փոքր է

$$\sqrt{3^1 \cdot 2^2} \cdot 4.9^1 \cdot 1.5^2 < 39$$

արժեքից: 39-ի պարզ բաժանարարների հնարավոր քանակը գնահատելու համար նկատենք, որ $2 \cdot 3 = 6 < 39$, $2 \cdot 3 \cdot 5 = 30 < 39$, բայց $2 \cdot 3 \cdot 5 \cdot 7 = 210 > 39$: Կրկին ռեզուլտանտի հնարավոր պարզ արտադրիչների քանակը ոչ ավել, քան երեք է: Ստուգելու ենք ըստ կամայական չորս հատ պարզ թվերի (որոնցից յուրաքանչյուրը չի բաժանում $f(x),\ g(x)$ բազմանդամներից գոնե մեկի ավագ գործակիցը): Եթե $p = 2$, ապա $f_2(x) = x^2 + 1$ եւ $g_2(x) = x + 1$: Ուրեմն՝ $\big(f_2(x), g_2(x)\big) = x + 1 \neq 1$: Իսկ $p = 3$, $p = 5$ եւ $p = 7$ դեպքերում էլ հեշտ է հաշվել, որ $\big(f_p(x), g_p(x)\big) = x + 1 \neq 1$: Ուրեմն եւ՝ $\big(f(x), g(x)\big) \neq 1$:

Եթե 3.6.3 ալգորիթմը կիրառենք նաեւ Կնուտի օրինակի (3.14) բազմանդամների վրա, ապա 3.5.2 եւ 3.5.6 օրինակների հաշվարկը ցույց է տալիս, որ ստիպված կլինենք ալգորիթմի քայլը կրկնել ոչ ավել, քան 31 անգամ:

3.6.6 Դիտողություն. Ինչպես նշում է Դ. Կնուտը, պատահականորեն ընտրված $f(x),\ g(x) \in \mathbb{Z}[x]$ բազմանդամների համար դրանց փոխադարձ պարզության հավանականությունը ավելի բարձր է, քան պատահականորեն ընտրված $a,\ b \in \mathbb{Z}$ ամբողջ թվերի փոխադարձ պարզության հավանականությունը (Knuth, 1969): Ուստի, եթե տրված $f(x),\ g(x)$ բազմանդամների համար ամենամեծ ընդհանուր բաժանարարի հաշվումը սկսենք դրանց փոխադարձ պարզության ուսումնասիրությունից, ապա մեծ հավանականությամբ խնդրի պատասխանը կստանանք 3.6.3 ալգորիթմի միջոցով, եւ այլեւս կարիք չի լինի կիրառել 3.4.8 ալգորիթմը: Այդ իմաստով

հաճախ գերադասելի է, նախ, կիրառել 3.6.3 ալգորիթմը, ապա, եթե պարզվի, որ բազմանդամները փոխադարձաբար պարզ չեն, անցնել 3.4.8 ալգորիթմին:

Այս պարագրաֆի գնահատականների օգնությամբ կարելի է ամենամեծ բաժանարարի եւս մի քանի ալգորիթմներ կառուցել: Նշենք դրանք առանց մանրամասն շարադրանքի:

Տրված $f(x),\ g(x) \in \mathbb{Z}[x]$ ոչ զրոյական բազմանդամների համար կարելի է անցնել դրանց պրիմիտիվ մասերին, ապա հաշվել $\sqrt{(n+1)^m(m+1)^n}\, N_f^m N_g^n$ գնահատականը, որտեղ $n = \deg f(x)$, $m = \deg g(x)$: Ընտրենք այն ամենամեծ k ինդեքսը, որի համար այդ գնահատականը մեծ կամ հավասար է $p_k\#$ արժեքից: Վերցնենք կամայական $p_1, \cdots, p_{k+1}$ պարզ թվեր, որոնք բոլորը մեծ են $2 \cdot N_{f,g}$-ից: Հաշվենք $\left(f_{p_i}(x),\ g_{p_i}(x)\right)$ մոդուլյար ամենամեծ ընդհանուր բաժանարարները, $i = 1, \dots, k+1$: Մեզ դեռ հայտնի չէ $d(x)$-ը, բայց, ըստ մեր գնահատականների, հայտնի է, որ դիտարկված պարզ թվերի քանակն ավելի մեծ է, քան $R = \mathrm{res}(f(x)/d(x), g(x)/d(x))$ ռեզուլտանտի պարզ բաժանարարների քանակը: Ուստի, ըստ 3.4.6 լեմմայի, $p_1, \cdots, p_{k+1}$ պարզ թվերից գոնե մեկը չի բաժանում R ռեզուլտանտը: Դժվար չէ գտնել այն. համեմատենք $\deg\left(f_{p_i}(x),\ g_{p_i}(x)\right)$ աստիճանները, եւ վերցնենք այն p_i-ն, որի համար այդ աստիճանը մինիմալ արժեք է ընդունում (հնարավոր է, որ մինիմալ արժեքն ընդունվի մի քանի հատ p_i-երի համար. այդ դեպքում ընտրենք դրանցից կամայականը, գերադասելի է՝ փոքրագույնը): Ըստ այդ p_i արժեքի (ինչպես 3.4.8 ալգորիթմում)՝ հաշվենք t թիվը, $t \cdot \left(f_{p_i}(x),\ g_{p_i}(x)\right)$ բազմանդամի $k(x)$ նախապատկերը եւ դրա $\mathrm{pp}\big(k(x)\big)$ պրիմիտիվ մասը: Որոնելի պատասխանը դուրս գրենք $r \cdot d(x)$ տեսքով:

3.6.7 Խնդիր. Ալգորիթմի տեսքով ներկայացնել այս մեթոդի քայլերը:

Բերված մեթոդի առավելությունն այն է, որ ալգորիթմի ցիկլը կրկնվում է միայն մի անգամ՝ 3.4.8 ալգորիթմի 13-18 քայլերի վրայով անցնում ենք միայն մի անգամ: Մյուս կողմից, բերված մեթոդի թերությունն այն է, որ ստիպված ենք $\left(f_{p_i}(x),\ g_{p_i}(x)\right)$ բազմանդամը հաշվել $k+1$ անգամ՝ բավական մեծ p_i արժեքների համար:

Այդ թերությունը կարելի է նվազեցնել հետեւյալ կերպ. նախորդ դատողություններում $p_k\#$ արժեքը հաշվելուց հետո վերցնենք $p_1, \cdots, p_{k+1}$ պարզ թվեր, որոնք բոլորը ոչ թե մեծ են $2 \cdot N_{f,g}$-ից, այլ չեն բաժանում w-ն: Հասկանալի է՝ սա զգալիորեն փոքրացնում է օգտագործվող $p_1, \cdots, p_{k+1}$ թվերը: Վերցնենք $\deg\left(f_{p_i}(x),\ g_{p_i}(x)\right)$ աս-

տիճանների M մինիմումը: Ըստ մեր կառուցումների՝ $M = \deg\big(f(x),\ g(x)\big)$: Ընտրենք $p > 2 \cdot N_{f,g}$ պայմանին բավարարող որեւէ պարզ թիվ եւ հաշվենք $\deg\Big(f_p(x),\ g_p(x)\Big)$ արժեքը: Եթե $\deg\Big(f_p(x),\ g_p(x)\Big) = M$, ապա հաշվենք նաեւ t թիվը, $t \cdot \Big(f_{p_i}(x),\ g_{p_i}(x)\Big)$ բազմանդամի $k(x)$ նախապատկերը, $\mathrm{pp}\big(k(x)\big)$ պրիմիտիվ մասը եւ որոնելի պատասխանը՝ $r \cdot d(x)$ տեսքով: Իսկ եթե $\deg\Big(f_p(x),\ g_p(x)\Big) > M$, ապա ընտրենք մի նոր $p > 2 \cdot N_{f,g}$ պարզ թիվ եւ կրկնենք քայլը:

4 Դաշտերի ընդլայնումներ եւ քառակուսիներից ազատ բազմանդամներ

4.1 Օղակների եւ դաշտերի բնութագրիչները

Այս գլխի հիմնական նպատակն է ավելի մոտիկից ծանոթանալ օղակների ու դաշտերի հատկություններին եւ ստանալ դրանց նոր ալգորիթմական կիրառություններ: Հիմնական տեսական բովանդակությունը կապված է լինելու օղակների ու դաշտերի բնութագրիչների, ընդլայնումների, հանրահաշվական տարրերի, մինիմալ բազմանդամների եւ հանրահաշվական ընդլայնումների հետ:

Իսկ հիմնական ալգորիթմական արդյունքները հանգելու են զրոյական եւ պարզ բնութագրիչի դաշտերի վրա տրված բազմանդամների քառակուսիներից ազատ արտադրիչների հաշվմանը: Այդ ալգորիթմները օգտագործվելու են նաեւ հետագա գլուխներում:

Այն ընթերցողները, ովքեր հետաքրքրված են առաջին հերթին ալգորիթմական կիրառություններով, կարող 4.2 պարագրաֆից հիշել միայն 4.2.3 թեորեմի եւ նրա 4.2.4 հետեւանքի ձեւակերպումները, ինչպես նաեւ 4.2.29 սահմանումը եւ 4.2.31 թեորեմի ձեւակերպումը: Այսինքն՝ այն, որ յուրաքանչյուր ամբողջության տիրույթ կարելի է ներդնել դաշտի մեջ, եւ այդ դաշտն էլ կարելի է ներդնել հանրահաշվորեն փակ դաշտի մեջ (այնպիսի դաշտի մեջ, որտեղ յուրաքանչյուր բազմանդամ արմատ ունի):

4.2, 4.4 եւ 4.5 պարագրաֆներում բերված ապացույցների մանրամասները կհետաքրքրեն միայն նրանց, ովքեր հատուկ նպատակ ունեն ավելի մոտիկից ծանոթանալու մեր օգտագործած տեսության մանրամասն հանրահաշվական հիմնավորումներին: Հետագա գլուխների ալգորիթմների կառուցումներում դրանք չեն պահանջվելու:

Օղակներում եւ դաշտերում կարեւոր նշանակություն ունի դրանց բնութագրիչի հասկացությունը:

4.1.1 Սահմանում. R օղակը կոչվում է n *բնութագրիչի* օղակ, եթե n-ը այն նվազագույն դրական ամբողջ թիվն է, որի համար

$$na = \underbrace{a + \cdots + a}_{n} = 0$$

հավասարությունը տեղի ունի կամայական $a \in R$ տարրի համար: Իսկ եթե այդպիսի դրական ամբողջ թիվ գոյություն չունի, ապա R-ը համարվում է 0 բնութագրիչի օղակ: R օղակի բնութագրիչը նշանակվում է $\mathrm{char}(R)$: Վերը նշված դեպքերում՝ $\mathrm{char}(R) = n$ կամ $\mathrm{char}(R) = 0$:

Եթե R օղակը միավորով օղակ է (դա այդպես է, օրինակ, ամբողջության տիրույթների եւ դաշտերի համար), ապա բնութագրիչի սահմանման պայմանն ավելի պարզ տեսք ունի.

4.1.2 Սահմանում. R միավորով օղակը կոչվում է n բնութագրիչի օղակ, եթե n-ը այն նվազագույն դրական ամբողջ թիվն է, որի համար

$$\underbrace{1 + \cdots + 1}_{n} = 0:$$

Իսկ եթե այդպիսի դրական ամբողջ թիվ գոյություն չունի, ապա R-ը համարվում է 0 բնութագրիչի օղակ:

4.1.3 Վարժություն. Ցույց տալ, որ միավորով օղակի համար 4.1.1 եւ 4.1.2 սահմանումները համարժեք են:

4.1.4 Օրինակներ. Հեշտ է ստուգել, որ $\mathrm{char}(\mathbb{Z}) = \mathrm{char}(\mathbb{Q}) = \mathrm{char}(\mathbb{R}) = \mathrm{char}(\mathbb{C}) = 0$: $\mathrm{char}(\mathbb{Z}_n) = n$: Մասնավորապես, p պարզ թվի համար $\mathbb{Z}_p$-ն դաշտ է եւ $\mathrm{char}(\mathbb{Z}_p) = p$:

Մինչ այժմ մենք գործ ենք ունեցել վերջավոր դաշտերի միայն մեկ տիպի հետ՝ $\mathbb{Z}_p$, որտեղ p-ն պարզ թիվ է: Հետագայում մեզ անհրաժեշտ են լինելու վերջավոր դաշտերի մասին մի քանի փաստեր եւս: Սկսենք $\mathbb{Z}_p$-ից տարբեր վերջավոր դաշտերի օրինակներից:

4.1.5 Օրինակ. $\mathbb{Z}_2[x]$ բազմանդամային օղակում վերցնենք $g(x) = x^2 + x + 1$ բազմանդամը եւ դրանով ծնված $I = g(x)\mathbb{Z}_2[x]$ գլխավոր իդեալը: $K = \mathbb{Z}_2[x]/I$ ֆակտոր-օղակը բաղկացած $f(x) + I$ տեսքի հարակից դասերից, որտեղ $f(x) \in \mathbb{Z}_2[x]$: Ստուգենք, որ այդ դասերը միայն չորս հատ են՝ $0 + I,\ 1 + I,\ x + I,\ x + 1 + I$: Իրոք, նկատենք, որ նշված չորս դասերը իրարից տարբեր են, քանի որ դրանցից ցանկացած երկուսի ներկայացուցիչների տարբերությունը չի պատկանում I իդեալին, քանի որ չի բաժանվում $g(x)$-ի վրա: Մյուս կողմից, եթե $\deg f(x) > 1$, ապա $f(x)$-ը $g(x)$ բազմանդամի վրա բաժանելիս որպես մնացորդ ստացվում են միայն այն բազմանդամ-

ները, որոնք հենց նոր թվարկեցինք: Այսինքն՝ $f(x)+I$ տեսքի յուրաքանչյուր դաս հավասար է նշված չորս դասերից որեւէ մեկին: Մնում է ստուգել, որ K-ն դաշտ է, այսինքն՝ ցույց տալ նրա ոչ զրոյական տարրերի հակադարձելիությունը: Իրոք. $1\cdot 1=1$ եւ

$$x(x+1)=x^2+x=(x^2+x+1)+1\in g(x)\mathbb{Z}_2[x]+1=1_K:$$

Այսինքն՝ հակադարձելի են նաեւ x եւ $x+1$ տարրերը: Հեշտ է նաեւ ստուգել, որ $\mathrm{char}(K)=2$, քանի որ $\mathbb{Z}_2[x]$ օղակում $x+x=2x=0$ եւ $(x+1)+(x+1)=0$:

4.1.6 **Խնդիր.** $\mathbb{Z}_2[x]$ բազմանդամային օղակում վերցնենք $g(x)=x^3+x+1$ բազմանդամով ծնված $I=g(x)\mathbb{Z}_2[x]$ գլխավոր իդեալը: Ցույց տալ, որ $K=\mathbb{Z}_2[x]/I$ ֆակտոր-օղակը 8 տարրից բաղկացած դաշտ է: Ընդ որում, $\mathrm{char}(K)=2$:

4.1.7 **Խնդիր.** Գտնել 9 տարրից բաղկացած դաշտ: Ստուգել, որ դրա բնութագրիչը հավասար է 3-ի: *Յուցում.* դիտարկել $\mathbb{Z}_3[x]$ օղակի ֆակտոր-օղակ ըստ համապատասխան իդեալի:

Վերջին օրինակներն ու խնդիրները հետաքրքիր է համադրել հետեւյալ փաստի հետ. մենք չենք կարող 4, 8 կամ 9 տարրից բաղկացած դաշտեր ստանալ պարզապես վերցնելով $\mathbb{Z}_4$, $\mathbb{Z}_8$ կամ $\mathbb{Z}_9$ օղակները, քանի որ նշված թվերը պարզ չեն. տես 2.1.26 թեորեմը: Մյուս կողմից, դաշտեր են հանդիսանում $\mathbb{Z}_2$, $\mathbb{Z}_3$ օղակները: Դրանց բնութագրիչներն են՝ համապատասխանաբար 2 եւ 3:

Պատահական չէ, որ մեր բերած օրինակներում վերջավոր դաշտի բնութագրիչը որեւէ պարզ թիվ է, իսկ դաշտի հզորությունը՝ այդ պարզ թվի որեւէ աստիճան:

4.1.8 **Խնդիր.** Ստուգել, որ եթե K վերջավոր օղակը դաշտ է, ապա $\mathrm{char}(K)$ բնութագրիչը պարզ թիվ է: *Յուցում.* ենթադրել, որ $\mathrm{char}(K)=mn$ բաղադրյալ թիվ է $(m,n\neq 1)$, եւ ստանալ հակասություն զրոյի բաժանարարներից ազատ լինելու փաստի հետ:

4.1.9 **Խնդիր.** Ստուգել, որ եթե K վերջավոր դաշտի բնութագրիչը p պարզ թիվն է, ապա $|K|=p^k$ որեւէ k բնական թվի համար: *Յուցում.* $\langle K,+,\cdot\rangle$ դաշտը ադիտիվ $\langle K,+\rangle$ աբելյան խումբ է գումարման գործողության նկատմամբ: Համարենք, որ նրա կարգը բաժանվում է իրարից տարբեր q եւ r պարզ թվերի վրա: Ըստ խմբերի տեսությունից հայտնի Կոշու թեորեմի, եթե պարզ թիվը խմբի կարգի բաժանարար է, ապա խումբը պարունակում է այդ պարզ կարգի մի տարր: Մեր դեպքում գոյություն ունեն $a,b\in\langle K,+,\cdot\rangle$ տարրեր այնպիսիք, որ $|a|=q$ եւ $|b|=r$: Հաշվի առնելով գրության ադիտիվությունը՝ սա նշանակում է, որ $qa=0$ եւ $rb=0$: Ստանալ հակասություն՝ սրանք համադրելով 4.1 սահմանման հետ: Այս խնդիրը կարելի է լուծել նաեւ այլ կերպ՝ օգտագործելով վերջավոր դաշտի վրա տրված տարածությունները (տես 7.2 պարագրաֆը):

Մենք ստացանք.

4.1.10 Թեորեմ. *Եթե K դաշտը վերջավոր է, ապա գոյություն ունի այնպիսի մի p պարզ թիվ, որ* $\mathrm{char}(K) = p$ *եւ* $|K| = p^k$ *որեւէ k բնական թվի համար:*

Քանի որ K դաշտի հակադարձելի տարրերի K^* բազմությունը (դաշտի մուլտիպլիկատիվ խումբը) համընկնում է K-ի ոչ զրոյական տարրերի բազմության հետ՝ $K^* = K\backslash\{0\}$, ապա այս թեորեմից բխում է, որ $|K^*| = p^k - 1$: Պարզվում է, որ վերջավոր դաշտերի մուլտիպլիկատիվ խմբերի մասին կարելի է ասել ավելին.

4.1.11 Թեորեմ. *Եթե K դաշտը վերջավոր է,* $\mathrm{char}(K) = p$ *եւ* $|K| = p^k$*, ապա K դաշտի K^* մուլտիպլիկատիվ խումբը $p^k - 1$ կարգի ցիկլիկ խումբ է:*

Ապացույց: Հեշտ է ստուգել (կամ բխեցնել վերջավոր աբելյան խմբերի մասին հիմնական թեորեմից), որ եթե որեւէ աբելյան խմբի a, b տարրի համար $|a| = n$ եւ $|b| = m$, ապա խմբում կա մի c տարր, որի կարգը m, n թվերի ամենափոքր ընդհանուր բազմապատիկն է. $|c| = [m, n]$:

Վերցնենք K^* խմբի տարրերից մեկը, որն ունի մաքսիմալ n կարգ. $|a| = n$ եւ ցանկացած $b \in K^*$ տարրի համար $|a| \geq |b|$: Ըստ նախորդ դիտողության՝ $|b|$-ն պիտի լինի $|a|$-ի բաժանարար, այլապես K^* խմբում գոյություն կունենար ավելի մեծ $[m, n]$ կարգ ունեցող մի c տարր: Սա նշանակում է, որ $f(x) = x^n - 1$ բազմանդամի համար (իրարից տարբեր) արմատներ են հանդիսանում K^* խմբի բոլոր $p^k - 1$ հատ տարրերը: Ըստ Բեզուի թեորեմի՝ $f(x)$-ը կարելի է ներկայացնել գծային արտադրիչների արտադրյալի տեսքով.

$$f(x) = \prod_{\substack{i=1,\dots,p^k-1 \\ x_i \in K^*}} (x - x_i):$$

Բայց աջ կողմում գրված է $p^k - 1$ աստիճանի բազմանդամ, եւ այս հավասարությունը հնարավոր է միայն, երբ $f(x)$-ը նույնպես ունի այդ աստիճանը՝ $n = \deg f(x) = p^k - 1$: Այսինքն՝ a տարրի կարգը $p^k - 1$ է եւ $\langle a \rangle = K^*$. ■

4.2 Օղակների ընդլայնումներ եւ հանրահաշվական ընդլայնումներ

F դաշտն անվանում են K դաշտի ընդլայնում, եթե K-ն իզոմորֆ է F-ի որեւէ K' ենթադաշտի. գոյություն ունի $\theta: K \to K' \subseteq F$ իզոմորֆիզմ: Այդ դեպքում (առանց θ իզո-

մորֆիզմը բացահայտորեն նշանակելու) ընդունված է համարել, որ K դաշտը F-ի ենթաբազմություն է: Օրինակ, իրական թվերի դաշտի կառուցման հայտնի մեթոդներից են իրական թվի ներկայացումը անվերջ տասնորդական կոտորակի տեսքով կամ իրական թվի Կոշու սահմանումը ռացիոնալ թվերից կազմված ֆունդամենտալ հաջորդականությունների լեզվով: Այդ դեպքում ռացիոնալ թվերը, որոնք սահմանվում են որպես m/n տեսքի կոտորակներ ($m, n \in \mathbb{Z}$, $n \neq 0$), որպես իրական թվերի մասնավոր դեպք դիտարկվելիս կարող էին գրի առնվել, օրինակ, իբրեւ անվերջ տասնորդական կոտորակներ, ինչպես.

$$\theta(1/4) = 0{,}2500000\ldots$$

կամ էլ որպես ֆունդամենտալ հաջորդականություններ, ինչպես.

$$\theta(1/4) = \{1/4, 1/4, 1/4, \ldots\},$$

բայց ավելի հարմար է գրել $1/4$ կամ 0,25 առանց իզոմորֆիզմի θ տառը եւ առանց F դաշտի տարրերի ընդհանուր տեսքը ամբողջությամբ գրառելու:

Այն փաստը, որ F դաշտը K դաշտի ընդլայնում է, երբեմն ընդունված է նշանակել F/K սիմվոլով: Սա հարմար նշանակում է, երբ միանգամից մի շարք ընդլայնումներ են դիտարկվում, բայց մենք հազվադեպ կօգտագործենք այս նշանակումը, քանի որ այն կարող է շփոթություն առաջացնել՝ ֆակտոր-օղակի կամ ֆակտոր-խմբի նշանակման հետ:

Ամեն մի օղակ չէ, որ կարելի է ներդնել որեւէ դաշտի մեջ.

4.2.1 Օրինակ. Եթե $R = \mathbb{Z}_{mn}$, որտեղ $m, n \not\approx 1$, ապա R օղակում կան զրոյի բաժանարարներ. $m \cdot n = 0$: Այս հավասարությունը անփոփոխ կմնա, եթե R-ը ներդրվի որեւէ F օղակի մեջ: Ուրեմն, F օղակը չի կարող դաշտ լինել, քանի որ այն պետք է ազատ լինի զրոյի բաժանարարներից (տես 2.1.15 խնդիրը): Եթե R օղակը ներդրվում է որեւէ դաշտի մեջ, ապա R-ը ազատ է զրոյի բաժանարարներից:

4.2.2 Օրինակ. Եթե R օղակը կոմուտատիվ չէ, նրանում կան $a, b \in R$ տարրեր, որոնց համար $ab \neq ba$: Այս հավասարությունը անփոփոխ կմնա, եթե R-ը ներդրվի որեւէ F դաշտի մեջ: Այս հակասությունը ցույց է տալիս, որ եթե R օղակը ներդրվում է որեւէ դաշտի մեջ, ապա R-ը կոմուտատիվ է:

Վերջին երկու օրինակներում նշված անհրաժեշտ պայմանները միասին բավարար պայման են հանդիսանում հետեւյալ կարեւոր պնդման համար.

4.2.3 Թեորեմ. *R օղակը կարելի է ներդնել դաշտի մեջ այն եւ միայն այն դեպքում, երբ R-ը կոմուտատիվ է եւ ազատ է զրոյի բաժանարարներից:*

Ապացույցի սխեման: R կոմուտատիվ, զրոյի բաժանարարներից ազատ օղակը պարունակող F դաշտի կառուցումը նման է ամբողջ թվերի $\mathbb{Z}$ օղակի միջոցով ռացիոնալ թվերի $\mathbb{Q}$ դաշտի կառուցմանը:

Դիտարկենք ձեւական a/b տեսքի քանորդների բազմությունը, որտեղ $a \in R$, $b \in R\backslash\{0\}$: Երկու a/b եւ c/d քանորդները համարենք համարժեք, եթե $ad = cb$: Հեշտ է ստուգել, որ սահմանված հարաբերությունը համարժեքության հարաբերություն է: Ուստի a/b քանորդների բազմությունը տրոհվում է համարժեքության դասերի, որոնց բազմությունը եւ նշանակենք F: Գրառման կարճության համար a/b սիմվոլով նշանակենք նաեւ F-ում a/b տարրը պարունակող համարժեքության դասը: Դասերի գումարն ու արտադրյալը սահմանվում են հետեւյալ կանոններով.

$$a/b + c/d = (ad + cb)/bd \quad \text{եւ} \quad a/b \cdot c/d = ac/bd:$$

Հեշտ է ստուգել, որ այս սահմանումները կոռեկտ են, այսինքն՝ դրանք կախված չեն համարժեքության դասերի a/b եւ c/d ներկայացուցիչների ընտրություններից: Շատ պարզ է նաեւ օղակի 2.1.2 սահմանման **O.1-O.6** պայմանների ստուգումը. դրանք բխում են R օղակում այդ հատկությունների առկայությունից: F-ի աղիտիվ զրոյական տարրն է $0/h$ դասը, որտեղ h-ը կամայական ոչ զրոյական տարր է R օղակից (եթե նման տարր գոյություն չունի, ապա $R = \{0\}$ եւ այս դեպքը կարելի է բացառել թեորեմի ապացույցից, քանի որ զրոյական օղակը միշտ էլ տրիվիալ ներդրում ունի դաշտի մեջ):

F օղակը դաշտ է. այն կոմուտատիվ է, քանի որ R-ը կոմուտատիվ է: F-ի մուլտիպլիկատիվ միավորն է $1 = h/h$ դասը: Եթե $a/b \neq 0 = 0/h$, ապա, ըստ համարժեքության սահմանման, $a \cdot h \neq b \cdot 0 = 0$: Ուրեմն, քանի որ $a \neq 0$, ապա գոյություն ունի b/a դասը, որը եւ կլինի a/b դասի հակադարձը.

$$a/b \cdot b/a = ab/ba = h/h,$$

քանի որ, ըստ սահմանման, $abh = hba$:

Մնում է տեսնել, որ R օղակը ներդրվում է F դաշտի մեջ: Իսկապես, սահմանենք $\theta: R \to F$ հետեւյալ կանոնով. $\theta(a) = ah/h \in F$: Հեշտ է ցույց տալ, որ սա իզոմորֆ ներդրում է: ■

4.2.4 Հետեւանք. *Յանկացած ամբողջության տիրույթ կարելի է ներդնել դաշտի մեջ:*

Այն դեպքում, երբ R օղակը միավոր ունի, ապացույցում հիշատակված θ արտապատկերումը ավելի պարզ տեսք ունի, քանի որ կարելի է վերցնել $h = 1$ եւ այդ դեպքում $\theta(a) = a1/1 = a/1$:

4.2.3 թեորեմի ապացույցի ընթացքում ըստ R օղակի կառուցվող F դաշտը կոչվում է R օղակի *քանորդների դաշտ*: Այն նշանակվում է $\mathrm{Quot}(R)$:

4.2.5 Օրինակներ. Հեշտ է տեսնել, որ $\mathrm{Quot}(\mathbb{Z}) = \mathbb{Q}$: Մյուս կողմից, $\mathrm{Quot}(\mathbb{Q}) = \mathbb{Q}$, $\mathrm{Quot}(\mathbb{R}) = \mathbb{R}$, $\mathrm{Quot}(\mathbb{C}) = \mathbb{C}$: Եւ, ընդհանրապես, կամայական K դաշտի համար $\mathrm{Quot}(K) = K$: Նկատենք, որ այս օրինակներում, համաձայն այս պարագրաֆի սկզբում արված դիտողության, մենք օգտագործում ենք հավասարության, այլ ոչ թե իզոմորֆիզմի նշանը (գրում ենք $\mathrm{Quot}(\mathbb{Z}) = \mathbb{Q}$ այլ ոչ՝ $\mathrm{Quot}(\mathbb{Z}) \cong \mathbb{Q}$):

Քանորդների դաշտի մի հետաքրքիր օրինակ կառուցվում է բազմանդամային օղակների միջոցով.

4.2.6 Օրինակ. Կամայական R ամբողջության տիրույթի համար $R[x]$ բազմանդամային օղակը նույնպես ամբողջության տիրույթ է (տես նաեւ 2.1.30 վարժությունը): Ուրեմն՝ կարելի է դիտարկել

$$\mathrm{Quot}(R[x]) = \{f(x)/g(x) \mid f(x), g(x) \in R[x], g(x) \neq 0\}$$

քանորդների դաշտը: Այն կոչվում է R ամբողջության տիրույթի ռացիոնալ ֆունկցիաների դաշտ եւ նշանակվում է $R(x)$ սիմվոլով: Մասնավորապես, կամայական K դաշտի համար կարելի է դիտարկել նրա ռացիոնալ ֆունկցիաների $K(x) = \mathrm{Quot}(K[x])$ դաշտը:

Մասնավորապես, եթե R-ը իրական թվերի $\mathbb{R}$ դաշտն է, ապա ստանում ենք մաթեմատիկական անալիզից ծանոթ ռացիոնալ ֆունկցիաները. այն կոտորակային ֆունկցիաները, որոնց համարիչն ու հայտարարը իրական բազմանդամներ են (հայտարարը ոչ զրոյական):

4.2.7 Սահմանում. K դաշտը կոչվում է *հանրահաշվորեն փակ դաշտ*, եթե այդ դաշտի վրա տրված $K[x]$ բազմանդամային օղակի յուրաքանչյուր $f(x) \in K[x]$ հաստատունից տարբեր բազմանդամ արմատ ունի K դաշտում:

4.2.8 Օրինակ. Ըստ հանրահաշվի հիմնական թեորեմի՝ հանրահաշվորեն փակ դաշտի օրինակ է կոմպլեքս $\mathbb{C}$ դաշտը: Մյուս կողմից հանրահաշվորեն փակ դաշտ չեն հանդիսանում իրական $\mathbb{R}$ եւ ռացիոնալ $\mathbb{Q}$ դաշտերը, քանի որ դրանցում արմատ չունի, օրինակ, $f(x) = x^2 + 1$ բազմանդամը:

4.2.9 Սահմանում. Ենթադրենք տրված է K դաշտի F ընդլայնումը եւ $a \in F$ տարրը: a-ն կոչվում է *հանրահաշվական* տարր K դաշտի վրա, եթե այն որեւէ $f(x) \in K[x]$ բազմանդամի արմատ է: Իսկ եթե նման բազմանդամ գոյություն չունի, ապա a-ն կոչվում է *տրանսցենդենտ* տարր K դաշտի վրա:

4.2.10 Սահմանում. K դաշտի F ընդլայնումը կոչվում է K-ի *հանրահաշվական* ընդլայնում, եթե կամայական $a \in F$ տարր հանրահաշվական է K դաշտի վրա: Հակառակ դեպքում ընդլայնումը կոչվում է *տրանսցենդենտ* ընդլայնում:

4.2.11 Օրինակ. Իրական $\mathbb{R}$ դաշտի հանրահաշվական ընդլայնում է կոմպլեքս $\mathbb{C}$ դաշտը, իսկ ռացիոնալ $\mathbb{Q}$ դաշտի հանրահաշվական ընդլայնման օրինակ է

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

դաշտը: $\mathbb{Q}$ դաշտի վրա տրանսցենդենտ տարրերի օրինակներ են հայտնի π եւ e թվերը: Ուստի դրանցից յուրաքանչուրով եւ $\mathbb{Q}$-ով ծնվում է $\mathbb{Q}$ դաշտի տրանսցենդենտ ընդլայնում:

Երբ առանց կոնկրետ դաշտը նշելու ասում են՝ «տրանսցենդենտ տարր» կամ «հանրահաշվական տարր», ապա ընդունված է հասկանալ $\mathbb{Q}$ դաշտի վրա տրանսցենդենտ կամ հանրահաշվական տարրերը: Սա այն դեպքն է, որն առավել հաճախ է օգտագործվում մաթեմատիկական անալիզում:

4.2.12 Դիտողություն. Կարող է անսպասելի թվալ, բայց մինչ այժմ անհայտ է՝ տրանսցենդե՞նտ են արդյոք այնպիսի «ոչ բարդ» տեսքով տրվող թվեր, ինչպիսիք են.

$$\pi + e, \quad \pi - e, \quad \pi/e, \quad \pi \cdot e, \quad \pi^{\pi}, \quad e^{e} \text{ եւ այլն...}$$

Ալգորիթմական կառուցումներում մեզ պետք է գալու այն կարեւոր փաստը, որ կամայական K դաշտի համար գոյություն ունի նրա հանրահաշվորեն փակ ընդլայնում (տես 4.2.31 թեորեմը): Նախքան դրա ապացույցը՝ բերենք մի քանի սահմանումներ եւ փաստեր:

Ենթադրենք K դաշտը F դաշտի ենթադաշտ է, եւ a-ն F-ի կամայական տարր է: $K(a)$-ով նշանակենք K դաշտին a տարրի միացումով ստացված դաշտը. F-ի բոլոր այն L ենթադաշտերի հատումը, որոնք պարունակում են K-ն եւ a-ն.

$$K(a) = \bigcap_{K \cup \{a\} \subseteq L} L.$$

Հեշտ է ստուգել, որ սահմանված $K(a)$ բազմությունն իրոք դաշտ է: Մասնավորապես, եթե $a \in K$, ապա $K(a) = K$: Այս $K(a)$ նշանակումը նմանվում է 4.2.6 օրինակում կառուցված քանորդների դաշտի նշանակմանը. եթե K դաշտի համար դի-

տարկենք նրա վրա բազմանդամային $K[x]$ օղակը, ապա դրա քանորդների դաշտը կլինի ռացիոնալ ֆունկցիաների $K(x) = \mathrm{Quot}(K[x])$ դաշտը: Ինչպես կտեսնենք քիչ հետո, $K(a)$ եւ $K(x)$ սիմվոլների միջեւ նմանությունը պատահական չէ, չնայած այդ մաթեմատիկական օբյեկտները մենք սահմանեցինք իրարից շատ տարբեր ձեւերով:

Մեզ պետք կգա եւս մի հասկացություն. եթե K դաշտը F դաշտի ենթադաշտ է, եւ $a \in F$, ապա նշանակենք

$$K[a] = \{b_0a^m + b_1a^{m-1} + \cdots + b_m \in F \mid b_i \in K, m \in \mathbb{N} \cup \{0\}\} \subseteq F:$$

$K[a]$-ն կարելի է բնութագրել որպես F դաշտի այն ենթաբազմությունը, որը ստացվում է $K[x]$ օղակի բազմանդամների մեջ «x փոփոխականի փոխարեն $x = a$ արժեքը տեղադրելով»: Ստույգ սահմանումը հետեւյալն է. կարելի է $\pi\colon K[x] \to F$ օղակային հոմոմորֆիզմ սահմանել հետեւյալ կանոնով. եթե $g(x) = b_0x^m + b_1x^{m-1} + \cdots + b_m \in K[x]$, ապա.

$$\pi\colon g(x) \to g(a) = b_0a^m + b_1a^{m-1} + \cdots + b_m:$$

Հեշտ է ստուգել, որ սա իրոք հոմոմորֆիզմ է եւ

$$K[a] = \mathrm{im}\,\pi = \{g(a) \mid g(x) \in K[x]\}:$$

Ըստ օղակների հոմոմորֆիզմների մասին 2.3.13 հիմնական թեորեմի, այս հոմոմորֆիզմի $\ker\pi$ միջուկը $K[x]$ օղակի իդեալ է: Համաձայն 2.5.13 թեորեմի՝ $K[x]$ օղակն Էվկլիդյան է, որովհետեւ այն տրված է դաշտի վրա: Քանի որ, ըստ 2.5.8 թեորեմի, յուրաքանչյուր Էվկլիդյան օղակ գլխավոր իդեալների օղակ է, ապա $\ker\pi$ իդեալը գլխավոր իդեալ է, այսինքն՝ այն ծնվում է $K[x]$-ի որեւէ $m(x)$ բազմանդամով.

$$\ker\pi = m(x)K[x]:$$

Եթե $\ker\pi = 0$ (այսինքն՝ π-ն իզոմորֆիզմ է), ապա $m(x) = 0$: Իսկ եթե $\ker\pi \neq 0$ (այսինքն՝ π-ն իզոմորֆիզմ չէ), ապա այդ պայմանին բավարարող $m(x)$ ոչ զրոյական բազմանդամներից ընտրենք մինիմալ աստիճան ունեցողը եւ, քանի որ բազմանդամը հաստատունով բազմապատկելն այստեղ չի ազդում նրանով (դաշտի վրա) ծնված բազմանդամային իդեալի վրա, կարող ենք համարել, որ $m(x)$-ը նորմավորված բազմանդամ է, այսինքն՝ նրա ավագ գործակիցը 1 է: Այս պայմաններն ապահովում են $m(x)$ բազմանդամի ընտրության միակությունը, քանի որ, եթե մի այլ նորմավորված $m'(x)$ բազմանդամ նույնպես բավարարում է այս պայմաններին, ապա, ըստ աստիճանի մինիմալության, $\deg m(x) = \deg m'(x)$, իսկ եթե $m(x)$ եւ $m'(x)$ բազմանդամները տարբերվեին գոնե մի գործակցով, ապա այդ գործակիցը պիտի տարբեր լիներ ավագ գործակցից (որը 1 է երկուսի համար էլ), եւ այդ դեպ-

քում $m(x) - m'(x)$ տարբերությունը կլիներ $\deg m(x)$-ից ավելի ցածր աստիճանի բազմանդամ, որը պատկանում է $\ker \pi$-ին: Այստեղից հետեւում է, որ նշված $m(x)$ բազմանդամը միակն է, եւ կարող ենք սահմանել.

4.2.13 Սահմանում. Եթե տրված է K դաշտի F ընդլայնումը, ապա $a \in F$ տարրի *մինիմալ բազմանդամ* է կոչվում $K[x]$ օղակի նվազագույն աստիճանի հաստատունից տարբեր այն նորմավորված $m(x)$ բազմանդամը, որի համար $m(a) = 0$:

Հասկանալի է, որ ամեն մի ընդլայնման եւ ամեն մի տարրի համար չէ, որ գոյություն ունի մինիմալ բազմանդամ: F/K ընդլայնման $a \in F$ տարրի համար ունենք

$$\pi\colon K[x] \to K[a], \tag{4.1}$$

հոմոմորֆիզմը ($\ker \pi = m(x)K[x]$), որի համար բերված քննարկումը իրարից էապես տարբեր երկու դեպքեր է բնորոշում՝ կախված π-ի բնույթից.

1. եթե π-ն իզոմորֆիզմ է, ապա $K[x] \cong K[a]$, իսկ $m(x)K[x]$ իդեալը եւ $m(x)$ բազմանդամը զրոյական են,
2. եւ եթե π-ն իզոմորֆիզմ չէ, ապա $K[x]/(m(x)K[x]) \cong K[a]$, որտեղ $m(x)$-ը $a \in K$ տարրի մինիմալ բազմանդամն է:

Վերադառնալով հանրահաշվական տարրի մասին 4.2.9 սահմանմանը՝ նկատում ենք, որ այս երկընտրանքի առաջին դեպքը տեղի ունի, երբ a-ն տրանսցենդենտ տարր է K-ի վրա, եւ երկրորդ դեպքը տեղի ունի, երբ a-ն հանրահաշվական տարր է K-ի վրա:

4.2.14 Օրինակ. Ենթադրենք $K = \mathbb{Q}$ եւ $a = e$: Ինչպես հայտնի է, e թիվը տրանսցենդենտ թիվ է. այն ռացիոնալ գործակիցներով ոչ մի բազմանդամի արմատ չէ: Ուստի $\mathbb{Q}[e]$ օղակը (որն ամբողջովին բաղկացած է իրական թվերից) իզոմորֆ է ռացիոնալ գործակիցներով բազմանդամների $\mathbb{Q}[x]$ օղակին (որը թվային օղակ չէ): Իզոմորֆիզմը կարելի է բացահայտորեն գրել

$$\pi\colon b_0x^m + b_1x^{m-1} + \cdots + b_m \to b_0e^m + b_1e^{m-1} + \cdots + b_m$$

բանաձեւով: $\mathbb{Q}[e]$ օղակի տարր է, օրինակ, $1/2 + 3e - 4e^2 + e^{10}$ թիվը:

4.2.15 Օրինակ. Ենթադրենք $K = \mathbb{Q}$ եւ $a = \sqrt{2}$: Այդ դեպքում a-ն արմատ է $m(x) = x^2 - 2$ մինիմալ բազմանդամի համար:

$$\mathbb{Q}[\sqrt{2}] \cong \mathbb{Q}[x]/\big((x^2 - 2)\mathbb{Q}[x]\big).$$

Իսկ եթե որպես a վերցնենք $\mathbb{Q}$-ի տարր, օրինակ՝ $a = 3$, ապա այն արմատ է $m(x) = x - 3$ մինիմալ բազմանդամի համար, եւ

$$\mathbb{Q}[3] \cong \mathbb{Q}[x]/\big((x - 3)\mathbb{Q}[x]\big) \cong \mathbb{Q}.$$

4.2.16 Խնդիր. Դիտարկել $K=\mathbb{R}$ եւ $a=i\in\mathbb{C}$: Գտնել, թե ինչ տեսք կստանա (4.1) առնչությունն այս դեպքում:

4.2.17 Խնդիր. Ցույց տալ, որ (4.1) հոմոմորֆիզմով տրվող $m(x)$ մինիմալ բազմանդամը *պարզ* բազմանդամ է $K[x]$-ում: *Ցուցում.* ենթադրենք $m(a)=0$ եւ $m(x)=u(x)v(x)$, որտեղ $u(x),v(x)\not\equiv 1$: Հաշվել $u(a)v(a)$ արժեքը եւ օգտվել այն փաստից, որ $K[x]$ օղակն ազատ է զրոյի բաժանարարներից, իսկ $u(x),v(x)$ բազմանդամների աստիճանները փոքր են $m(x)$-ի աստիճանից:

Մենք արդեն կարող ենք բացատրել $K(a)$ եւ $K(x)$ նշանակումների նմանությունը, որ հիշատակեցինք ավելի վաղ:

4.2.18 Լեմմա. *Եթե F դաշտի a տարրը հանրահաշվական է F-ի K ենթադաշտի վրա, ապա $K[a]$ օղակը դաշտ է եւ, մասնավորապես, $K[a]=K(a)$:*

Ապացույց: Վերցնենք որեւէ ոչ զրոյական $c\in K[a]$ տարր եւ ցույց տանք, որ այն հակադարձ ունի $K[a]$ օղակում: Քանի որ a-ն հանրահաշվական է, ապա տեղի ունի (4.1) առնչությունը որեւէ $m(x)$ մինիմալ բազմանդամի համար: Ինչ-որ $g(x)\in K[x]$ բազմանդամի համար ունենք $c=g(a)=b_0a^m+b_1a^{m-1}+\cdots+b_m$: Քանի որ $c\neq 0$, ապա $g(x)\notin\ker\pi=m(x)K[x]$, եւ $g(x)$-ն չի բաժանվում $m(x)$-ի վրա: Ըստ 4.2.17 խնդրի, $m(x)$-ը պարզ բազմանդամ է $K[x]$-ում եւ, ըստ Էվկլիդեսի ընդհանրացված ալգորիթմի, գոյություն ունեն այնպիսի $u(x),v(x)\in K[x]$ բազմանդամներ, որ

$$u(x)m(x)+v(x)g(x)=\big(m(x),g(x)\big)=1:$$

Այս հավասարությունների բոլոր անդամների վրա կիրառենք π-ն.

$$\pi\big(u(x)m(x)+v(x)g(x)\big)=0+\pi\big(v(x)\big)\pi\big(g(x)\big)=v(a)g(a)=v(a)c=1,$$

Այսինքն՝ $v(a)=c^{-1}$:

Մենք $K(a)$-ով նշանակել էինք F-ի բոլոր այն ենթադաշտերի հատումը, որոնք պարունակում են K-ն եւ a-ն: Այդ ենթադաշտերից յուրաքանչյուրը պարունակում է $K[a]$-ն, քանի որ $K[a]$-ն բաղկացած է $K\cup\{a\}$-ի տարրերի արտադրյալների գումարից: Եւ քանի որ $K[a]$-ն արդեն իսկ դաշտ է, ապա $K[a]=K(a)$: ■

4.2.19 Օրինակ. Վերադառնանք 4.2.15 օրինակին. ունենք՝ $\mathbb{Q}\big[\sqrt{2}\big]=\mathbb{Q}\big(\sqrt{2}\big)=\big\{g\big(\sqrt{2}\big)\mid g(x)\in\mathbb{Q}[x]\big\}$: Նկատենք, որ $g(x)=b_0x^m+\cdots+b_m$ բազմանդամի մեջ $x=\sqrt{2}$ արժեքը տեղադրելիս $\sqrt{2}$-ի բոլոր զույգ աստիճանները ամբողջ թվերի են հավասար, իսկ կենտ աստիճանները հավասար են որեւէ ամբողջ թվերի եւ $\sqrt{2}$-ի արտադրյալի: Ուստի, նման անդամների միավորում կատարելով, ստանում ենք

$\mathbb{Q}[\sqrt{2}] = \mathbb{Q}(\sqrt{2}) = \{u + v\sqrt{2} \mid u, v \in \mathbb{Q}\}$: Իսկ, ասենք, 3 թիվը $\mathbb{Q}$ դաշտին միացնելիս ստանում ենք. $\mathbb{Q}(3) = \mathbb{Q}[3] = \mathbb{Q}$:

4.2.20 Խնդիր. Նախորդ օրինակի նմանությամբ ցույց տալ, որ $\mathbb{C} = \mathbb{R}[i] = \mathbb{R}(i) = \{u + v\,i \mid u, v \in \mathbb{R}\}$:

Մեր ստացած օրինաչափությունը բացատրում է $K(a)$ նշանակման նմանությունը ռացիոնալ ֆունկցիաների դաշտի $K(x)$ նշանակմանը:

$K(a)$ դաշտն անվանում են K *դաշտին a տարրի ավելացում* (F դաշտի մեջ): Եթե F դաշտի մեջ վերցնենք մի քանի $a_1, \dots, a_n \in F$ տարրեր, ապա կարելի է դրանց հաջորդական ավելացումով ստանալ $K(a_1)\cdots(a_n)$ դաշտը, որն ընդունված է նշանակել $K(a_1, \dots, a_n)$ եւ անվանել K *դաշտին $a_1, \dots, a_n$ տարրերի ավելացում* (F դաշտի մեջ):

Նույն սկզբունքով ներմուծվում են $K[x_1, \dots, x_n] = K[x_1]\cdots[x_n]$ եւ $K[a_1, \dots, a_n] = K[a_1]\cdots[a_n]$ օղակները: Դրանցից առաջինը ստացվում է, նախ, K դաշտի վրա դիտարկելով $K[x_1]$ բազմանդամային օղակը, ապա $K[x_1]$ օղակի վրա դիտարկելով $(K[x_1])[x_2]$ բազմանդամային օղակը (այս օղակի բազմանդամների գործակիցները $K[x_1]$-ից են, իսկ փոփոխականն է x_2-ը) եւ այլն: Իսկ $K[a_1, \dots, a_n]$-ն ստացվում է $K[x_1, \dots, x_n]$-ի բազմանդամներում փոփոխականների փոխարեն $a_1, \dots, a_n \in F$ տարրերը տեղադրելով, կամ, որ նույնն է, որպես համապատասխան $\pi\colon K[x_1, \dots, x_n] \to F$ հոմոմորֆիզմի պատկեր:

Դաշտերի ընդլայնումների հետ կապված հաջորդ հասկացությունը առնչվում է գծային տարածությունների հետ: Եթե տրված է F/K ընդլայնումը, ապա հեշտ է ստուգել, որ F-ը K դաշտի վրա տրված գծային տարածություն է, եթե F-ի տարրերի գումարը (համարենք դրանք վեկտորներ) նույնացնենք F օղակում գումարման գործողության հետ, իսկ K-ի տարրերի (համարենք դրանք սկալյարներ) եւ F-ի տարրերի արտադրյալը նույնացնենք F օղակում արտադրյալի գործողության հետ (ցանկացած դաշտի վրա տրված գծային տարածության սահմանումը տես 7.2 պարագրաֆում):

Դաշտերի ընդլայնումների համար դիտարկվում են գծային անկախության, տարածության բազիսի եւ չափողականության հասկացությունները: K դաշտի վրա տրված F գծային տարածության չափողականությունը նշանակենք $\dim_K F$:

$\dim_K F$ չափողականությունն անվանում են նաեւ F/K *ընդլայնման աստիճան* եւ նշանակում $[F\colon K]$: Տրված F/K ընդլայնումը կոչվում է վերջավոր ընդլայնում, եթե $[F\colon K] < \infty$:

4.2.21 Օրինակ. $\mathbb{Q}(\sqrt{2}) = \{u + v\sqrt{2} \mid u, v \in \mathbb{Q}\}$ դաշտը գծային տարածություն է $\mathbb{Q}$-ի վրա: Նրանում գծորեն անկախ վեկտորների օրինակներ են $\vec{a} = 1$ եւ $\vec{b} = \sqrt{2}$: Հեշտ է հաշվել, որ $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}) = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$:

4.2.22 Օրինակ. Կամայական F դաշտ ինքն իր ընդլայնումն է: Նրանում կամայական երկու վեկտորներ գծորեն կախված են: Ուստի՝ $\dim_F F = 1$:

4.2.23 Խնդիր. Ստուգել, որ եթե $a \in F$ տարրը հանրահաշվական է K-ի վրա եւ նրա մինիմալ բազմանդամն է $m(x)$-ը, ապա $[K(a):K] = \dim_K K(a) = \deg m(x)$: *Յուցում.* ունենք $K(a) = K[a] \cong K[x]/(m(x)K[x])$: Հետեւյալ $n = \deg m(x)$ հատ վեկտորները

$$\overrightarrow{e_1} = 1, \overrightarrow{e_2} = x, \dots, \overrightarrow{e_n} = x^{n-1}$$

ակնհայտորեն իրարից տարբեր են ըստ $m(x)$ մոդուլի, քանի որ դրանցից յուրաքանչյուրի աստիճանը փոքր է n-ից (եւ, ուրեմն, դրանցից ցանկացած երկուսի տարբերությունը չի բաժանվում $m(x)$-ի վրա):

Այդ վեկտորները նաեւ գծորեն անկախ են, քանի որ նրանց ոչ տրիվիալ գծային կոմբինացիան չի կարող բաժանվել n-րդ աստիճանի $m(x)$ բազմանդամի վրա, այսինքն՝ չի կարող 0-ի հավասարվել $K[x]/(m(x)K[x])$ օղակում: Մյուս կողմից՝ $\overrightarrow{e_1}, \dots, \overrightarrow{e_n}$ համակարգը բազիս է, քանի, որ ըստ $m(x)K[x]$ մոդուլի, ամեն մի բազմանդամ հավասար է ոչ ավել քան $n-1$-րդ աստիճանի բազմանդամի: Ներկայացնել այդ բազմանդամը $\overrightarrow{e_1}, \dots, \overrightarrow{e_n}$ համակարգի գծային կոմբինացիայի տեսքով (տես նաեւ 7.2 պարագրաֆը):

4.2.24 Թեորեմ. *Եթե F/K եւ L/F ընդլայնումները վերջավոր են, ապա վերջավոր է նաեւ L/K ընդլայնումը, ընդ որում, $[F:K][L:F] = [L:K]$:*

Ապացույց: Ենթադրենք K դաշտի վրա տրված F տարածության բազիսն է $\overrightarrow{e_1}, \dots, \overrightarrow{e_n}$ համակարգը, իսկ F դաշտի վրա տրված L տարածության բազիսն է $\overrightarrow{h_1}, \dots, \overrightarrow{h_s}$ համակարգը: Այս վեկտորները, որպես L-ի տարրեր կարելի է բազմապատկել: Հեշտ է ստուգել, որ ns հատ վեկտորներից բաղկացած

$$\overrightarrow{h_1} \cdot \overrightarrow{e_1}, \dots, \overrightarrow{h_1} \cdot \overrightarrow{e_n}; \dots; \overrightarrow{h_s} \cdot \overrightarrow{e_1}, \dots, \overrightarrow{h_s} \cdot \overrightarrow{e_n}$$

համակարգը բազիս է K դաշտի վրա տրված L տարածության համար: ■

4.2.25 Թեորեմ. *Դաշտերի կամայական F/K վերջավոր ընդլայնում հանրահաշվական է: Ավելին, գոյություն ունեն վերջավոր քանակությամբ $a_1, \dots, a_n \in F$ տարրեր այնպիսիք, որ $F = K(a_1, \dots, a_n) = K[a_1, \dots, a_n]$:*

Ապացույց: Նախ ցույց տանք, որ կամայական $a \in F$ տարր հանրահաշվական է K-ի վրա: a-ի աստիճանների $1, a, a^2, a^3, \ldots$ անվերջ հաջորդականությունը չի կարող գծորեն անկախ լինել վերջավոր չափանի F տարածության մեջ: Ուրեմն, այդ հաջորդականության որեւէ վերջավոր ենթաբազմության տարրերի

$$b_0a^0 + b_1a + \cdots + b_na^n$$

գծային կոմբինացիան (K դաշտից վերցված b_i գործակիցներով) հավասար է 0-ի: Բայց դա նշանակում է, որ a-ն b_i գործակիցներով

$$g(x) = b_0x^0 + b_1x + \cdots + b_nx^n \in K[x]$$

բազմանդամի արմատ է:

Երկրորդ պնդման ապացույցի համար վերցնենք որեւէ $a_1 \in F\backslash K$ տարր (այդպիսի տարր կարող ենք վերցնել, քանի որ այն դեպքում, երբ $F = K$, թեորեմի պնդումն ակնհայտ է, ուրեմն կարող ենք այդ դեպքը բացառել թեորեմի ապացույցից): Կառուցենք $K(a_1)$ ընդլայնումը: $[K(a_1):K] \leq [F:K] < \infty$: Եթե $K(a_1) \neq F$, վերցնենք որեւէ $a_2 \in F\backslash K(a_1)$ տարր եւ կառուցենք $K(a_1, a_2) = K(a_1)(a_2)$ ընդլայնումը:

$$[K(a_1, a_2):K] = [K(a_1, a_2):K(a_1)][K(a_1):K] \leq [F:K] < \infty:$$

Շարունակելով քայլերը՝ մենք ամեն անգամ ստանում ենք 1-ից մեծ աստիճանի ընդլայնումներ: Այս պրոցեսը, ըստ նախորդ թեորեմի, անվերջ չի կարող շարունակվել, քանի որ $[F:K] < \infty$: ■

Եթե F դաշտում տրված են նրա L_1 եւ L_2 ենթադաշտերը, ապա հեշտ է ստուգել, որ F-ի ենթադաշտ է նաեւ $L_1 \cdot L_2 = \{l_1 \cdot l_2 \mid l_1 \in L_1,\ l_2 \in L_2\}$ ենթաբազմությունը:

4.2.26 Լեմմա. *Ենթադրենք տրված է դաշտերի F/K ընդլայնումը, եւ F-ում կան այնպիսի L_1 եւ L_2 ենթադաշտեր, որ L_1/K եւ L_2/K ընդլայնումները վերջավոր են: Այդ դեպքում.*

1. *$(L_1 \cdot L_2)/K$ ընդլայնումը վերջավոր է, եւ $[L_1 \cdot L_2:K] \leq [L_1:K][L_2:K]$,*
2. *եթե $a_1, \ldots, a_n \in L_1$ եւ $b_1, \ldots, b_m \in L_2$ այն տարրերն են, որոնց համար $L_1 = K(a_1, \ldots, a_n) = K[a_1, \ldots, a_n]$ եւ $L_2 = K(b_1, \ldots, b_m) = K[b_1, \ldots, b_m]$, ապա.*

$$L_1 \cdot L_2 = K(a_1, \ldots, a_n; b_1, \ldots, b_m) = K[a_1, \ldots, a_n; b_1, \ldots, b_m]:$$

Ապացույց: Այն, որ L_1 եւ L_2 դաշտերն իրոք ունեն այն ներկայացումները, որ բերված են լեմմայի 2-րդ կետում, բխում է 4.2.25 թեորեմից: Քանի որ բոլոր $a_1, \ldots, a_n$; $b_1, \ldots, b_m$ տարրերը հանրահաշվական են, ապա

$$K(a_1, \ldots, a_n; b_1, \ldots, b_m) = K[a_1, \ldots, a_n; b_1, \ldots, b_m]:$$

Մյուս կողմից $L_1 \cdot L_2$-ը այն մինիմալ ենթադաշտն է, որ ընկած է F-ում եւ պարունակում է L_1 եւ L_2 ենթադաշտերը, այսինքն՝ K-ն եւ $a_1, \dots, a_n; b_1, \dots, b_m$ տարրերը: Ուրեմն $L_1 \cdot L_2 = K(a_1, \dots, a_n; b_1, \dots, b_m)$: Այստեղից ստացվում է նաեւ լեմմայի 1 կետի պնդումը: ■

4.2.27 Լեմմա. *Ենթադրենք տրված է դաշտերի F/K ընդլայնումը, եւ F-ի L ենթադաշտը, որը պարունակում է K-ն: Այդ դեպքում եթե $a \in F$ տարրը հանրահաշվական է K-ի վրա, ապա այն հանրահաշվական է նաեւ L-ի վրա, ընդ որում,*

$$[L(a):L] \le [K(a):K] < \infty:$$

Ապացույց: Քանի որ a-ն հանրահաշվական է K-ի վրա, այն հանրահաշվական է նաեւ L-ի վրա, որովհետեւ $K[x]$-ի ամեն մի բազմանդամ նաեւ $L[x]$-ից է: $[K(a):K]$ աստիճանը հավասար է K-ի վրա a-ի մինիմալ բազմանդամի աստիճանին: Այդ բազմանդամի աստիճանը չի ավելանում, երբ K-ն փոխարինվում է ավելի մեծ L դաշտով: ■

Այժմ մենք կարող ենք ապացուցել հետեւյալ կարեւոր փաստը.

4.2.28 Թեորեմ. *Եթե F/K եւ L/F ընդլայնումները հանրահաշվական են, ապա հանրահաշվական է նաեւ L/K ընդլայնումը:*

Ապացույց: Վերցնենք կամայական $a \in L$ տարր, որը հանրահաշվական է F-ի վրա, եւ ցույց տանք, որ այն հանրահաշվական է նաեւ ավելի փոքր K ենթադաշտի վրա: Ըստ պայմանի, a-ն հանդիսանում է $m(x) \in F[x]$ մինիմալ նորմավորված բազմանդամի արմատ.

$$0 = m(a) = a^m + b_1 a^{m-1} + \cdots + b_m,$$

որտեղ $b_1, \dots, b_m \in F$: Քանի որ F/K ընդլայնումը հանրահաշվական է, ապա այս b_i գործակիցներից յուրաքանչյուրը հանրահաշվական է K-ի վրա, եւ $[K(b_i):K]$ աստիճանը վերջավոր է ցանկացած $i = 0,1, \dots, m$ համար: Կիրառելով 4.2.26 լեմման ստանում ենք, որ վերջավոր է նաեւ $K(b_1, \dots, b_m)/K$ ընդլայնման $[K(b_1, \dots, b_m):K]$ աստիճանը:

Մյուս կողմից, $m(x) \in K(b_1, \dots, b_m)[x]$, քանի որ $m(x)$-ի բոլոր գործակիցները $K(b_1, \dots, b_m)$ դաշտից են: Այսինքն՝ a տարրը հանրահաշվական է ոչ միայն F-ի վրա, այլեւ դրա $K(b_1, \dots, b_m)$ ենթադաշտի վրա: Ուստի վերջավոր է նաեւ

$$K(b_1, \dots, b_m)(a)/K(b_1, \dots, b_m)$$

ընդլայնման աստիճանը: Ուրեմն.

$$[K(b_1,\dots,b_m)(a):K] = [K(b_1,\dots,b_m)(a):K(b_1,\dots,b_m)]\cdot[K(b_1,\dots,b_m):K] < \infty:$$

Այսինքն՝ $a \in K(b_1,\dots,b_m)(a) \subseteq F$ տարրը հանրահաշվական է K-ի վրա: ■

4.2.29 Սահմանում. K դաշտի $\overline{K}$ ընդլայնումը կոչվում է K-ի *հանրահաշվական փակույթ*, եթե $\overline{K}$ դաշտը հանրահաշվորեն փակ է, եւ $\overline{K}$-ի յուրաքանչյուր տարր հանրահաշվական է K-ի վրա:

4.2.30 Օրինակ. Հանրահաշվական փակույթի ծանոթ օրինակ է կոմպլեքս թվերի դաշտը՝ $\mathbb{C} = \overline{\mathbb{R}}$: Այլ օրինակներ հնարավոր կլինի կառուցել 4.2.31 թեորեմի միջոցով:

Նկատենք, որ այս սահմանման երկրորդ պահանջը առաջինի մասնավոր դեպքը չէ: Եթե $\overline{K}$-ն հանրահաշվորեն փակ է, ապա նրա յուրաքանչյուր a տարր $\overline{K}[x]$-ի որեւէ բազմանդամի արմատ է: Սա, իհարկե, վերաբերում է եւ այն դեպքին, երբ $a \in K$: Սահմանման երկրորդ պայմանը պահանջում է, որ այդ դեպքում բազմանդամը կարելի է վերցնել ոչ թե $\overline{K}[x]$, այլ $K[x]$ օղակից: Սա սահմանափակում է $\overline{K}$-ն եւ չի թողնում, որ այն պարունակի, օրինակ, K-ի վրա տրանսցենդենտ տարրեր:

Նախքան հաջորդ թեորեմին անցնելը՝ նշանակումների հետ կապված հետեւյալ պայմանավորվածության կարիքը կա: 4.2.20 խնդրին հաջորդող նշանակումներից մենք արդեն ծանոթ ենք K դաշտի վրա տրված՝ մեկից ավելի փոփոխականներով բազմանդամների $K[x_1,\dots,x_n] = K[x_1]\cdots[x_n]$ օղակին: Այն սահմանվում է որպես բազմանդամային օղակներ կառուցելու հաջորդական պրոցեսի արդյունք. նախ K-ի վրա կառուցվում է $K[x_1]$ օղակը, ապա $K[x_1]$ օղակի վրա կառուցվում է $K[x_1,x_2] = K[x_1][x_2]$ օղակը (որպես x_2 փոփոխականի վրա $K[x_1]$ ամբողջության տիրույթից վերցված գործակիցներով բազմանդամների օղակ) եւ այլն: Այս օղակը դժվար չէ կառուցել նաեւ ուղղակիորեն (որպես $x_1,\dots,x_n$ փոփոխականների $f(x_1,\dots,x_n)$ ֆունկցիաներ). նախ սահմանվում են այդ փոփոխականների վրա տրված $a\cdot x_{i_1}\cdots x_{i_k}$ տեսքի միանդամները (որտեղ $a \in K$ եւ $x_{i_j} \in \{x_1,\dots,x_n\}$), ապա դրանց ձեւական գումարների $K[x_1,\dots,x_n]$ բազմության վրա մտցվում է գումարում եւ բազմապատկում:

Նշված սահմանումներից երկուսն էլ կիրառելի են նաեւ այն դեպքում, եթե փոփոխականների քանակը վերջավոր չէ: I անվերջ հաշվելի բազմությամբ ինդեքսավորված $\{x_i | i \in I\}$ փոփոխականների վրա տրված բազմանդամների

$$K[x_i; i \in I] = K[x_1,\dots,x_i,\dots]$$

բազմանդամային օղակը կարող է սահմանվել թե՛ որպես

$$K[x_1], K[x_1,x_2],\dots,K[x_1,\dots,x_i],\dots$$

օղակների շղթայի միավորման արդյունք եւ թե՛ $a \cdot x_{i_1} \cdots x_{i_k}$ տեսքի միանդամների ձեւական գումարների միջոցով (վերջավոր են ինչպես գումարվող միանդամների քանակը, այնպես էլ՝ յուրաքանչյուր միանդամում մասնակցող փոփոխականների քանակը):

4.2.31 Թեորեմ. *Կամայական K դաշտի համար գոյություն ունի նրա $\bar{K}$ հանրահաշվական փակույթը:*

Ապացույց: Դիտարկենք $K[x]$ օղակում պարզ նորմավորված $h(x)$ բազմանդամների H բազմությունը: Յուրաքանչյուր այդպիսի $h(x)$ բազմանդամի համար դիտարկենք մի առանձին x_h փոփոխական: Քանի որ փոփոխականի վերանվանումից բազմանդամային օղակը չի փոխվում՝ $K[x] \cong K[x_h]$, ապա կարելի է $h(x)$ բազմանդամը նույնացնել $K[x_h]$ բազմանդամային օղակի $h(x_h)$ բազմանդամի հետ:

Դիտարկենք մի ավելի մեծ օղակ, որը պարունակում է բոլոր այս $K[x_h]$ օղակները. $\mathcal{K} = K[x_h; h \in H]$: Սա թեորեմից առաջ բերված օղակն է, որտեղ ինդեքսների I բազմության դերը կատարում է պարզ նորմավորված բազմանդամների H բազմությունը: $\mathcal{H}$-ով նշանակենք $\mathcal{K}$ օղակի այն իդեալը, որը $\mathcal{K}$-ում ծնվում է բոլոր $h(x_h), h \in H$ բազմանդամներով:

Հակասող ենթադրությամբ ստուգենք, որ $\mathcal{H}$-ը $\mathcal{K}$-ի սեփական ենթաբազմություն է: $\mathcal{H} = \mathcal{K}$ պայմանը համարժեք է $1 \in \mathcal{H}$ պայմանին (եթե $\mathcal{H}$ իդեալը պարունակում է $\mathcal{K}$ օղակի 1 միավորը, ապա այն պարունակում է նաեւ $\mathcal{K}$-ի յուրաքանչյուր $f(x_1, \dots, x_n) = 1 \cdot f(x_1, \dots, x_n)$ տարր): Ենթադրենք $\mathcal{K}$-ի ինչ-որ $k_1, \dots, k_s$ բազմանդամների եւ $\mathcal{H}$ իդեալի ինչ-որ $h_1(x_{h_1}), \dots, h_s(x_{h_s})$ բազմանդամների համար 1-ը ներկայացվում է

$$1 = k_1 \cdot h_1(x_{h_1}) + \cdots + k_s \cdot h_s(x_{h_s}) \in \mathcal{H} \tag{4.2}$$

տեսքով, որպես $\mathcal{H}$-ի տարր (պարզության համար $k_1, \dots, k_s$ բազմանդամների գրության մեջ բաց ենք թողել դրանց x_{i_j} փոփոխականները, որոնք այստեղ էական չեն):

Կառուցենք K դաշտի մի քանի հաջորդական ընդլայնումներ: Նախ K_1-ով նշանակենք K-ի այն ընդլայնումը, որտեղ $h_1(x_{h_1})$ բազմանդամը որեւէ r_1 արմատ ունի: K_1-ը կարող է լինել $K[x_{h_1}] / (h_1(x_{h_1})K[x_{h_1}])$ ֆակտոր-օղակը: Այս օղակը կարող է նաեւ հանդիսանալ ռացիոնալ ֆունկցիաների դաշտ կամ պարզապես համընկնել K-ի հետ (տես 4.2.13 սահմանումը, 4.2.14 եւ 4.2.15 օրինակները): K_1-ի բնույթն այս պահին էական չէ, եւ կարեւոր է միայն այն, որ դրանում $h_1(x_{h_1})$ բազմանդամն արմատ ունի: Նույն կերպ K_1-ը կարելի է ընդլայնել այնպիսի մի K_2 դաշտի, որտեղ որեւէ r_2 արմատ ունի $h_2(x_{h_2})$ բազմանդամը: Իհարկե, այս քայլում կարող է այն-

պես պատահել, որ $h_2(x_{h_2})$ բազմանդամը, որը պարզ բազմանդամ էր K-ի վրա, այլեւս պարզ չլինի K_1-ի վրա: Սակայն այդ դեպքում $h_2(x_{h_2})$-ը տրոհվում է պարզ արտադրիչների արտադրյալի, ու մենք կարող ենք այս քայլը կատարել՝ $h_2(x_{h_2})$-ի փոխարեն վերցնելով նշված պարզ արտադրիչներից որեւէ մեկը (պարզ արտադրիչի արմատը արմատ կհանդիսանա նաեւ $h_2(x_{h_2})$-ի համար): Շարունակելով պրոցեսը, s-րդ քայլում կստանանք մի K_s դաշտ որը K_{s-1}-ի ընդլայնում է, եւ որտեղ որեւէ r_s արմատ ունի $h_s(x_{h_s})$ բազմանդամը:

Քանի որ պրոցեսը հաջորդական ընդլայնումներով է ընթացել, ապա K_s դաշտում բոլոր $h_1(x_{h_1}), \dots, h_s(x_{h_s})$ բազմանդամներն համապատասխանաբար ունեն $r_1, \dots, r_s$ արմատները:

Որոնելի հակասությունը ստանալու համար $\mathcal{H}$-ի յուրաքանչյուր բազմանդամի մեջ փոփոխականների փոխարեն K_s դաշտից արժեքներ տեղադրենք հետեւյալ կերպ. x_{h_j}-ի փոխարեն տեղադրենք r_j (երբ $j = 1, \dots, s$) եւ տեղադրենք 0 (մնացած բոլոր փոփոխականների համար): Ստանում ենք $\alpha: \mathcal{H} \to K_s$ հոմոմորֆիզմը: α-ն կիրառելով (4.2) առնչության երկու կողմերի վրա եւ հիշելով, որ օղակների հոմոմորֆիզմների ժամանակ միավոր տարրի պատկերը միշտ միավորն է՝ ստանում ենք.

$$1_{K_s} = \alpha(1_{\mathcal{H}}) = \alpha\left(k_1 \cdot h_1(x_{h_1}) + \dots + k_s \cdot h_s(x_{h_s})\right) = \alpha(k_1) \cdot h_1(r_1) + \dots + \alpha(k_s) \cdot h_s(r_s)$$
$$= \alpha(k_1) \cdot 0_{K_s} + \dots + \alpha(k_s) \cdot 0_{K_s} = 0_{K_s}$$

(հստակության համար այստեղ մենք միավոր եւ զրոյական տարրերի ինդեքսներում նշել ենք, թե որ տարրը որ օղակից է): Հակասությունը ցույց է տալիս, որ $1 \notin \mathcal{H} \neq \mathcal{K}$:

Քանի որ $\mathcal{H}$-ը $\mathcal{K}$-ի սեփական իդեալ է, Յորնի լեմմայից[1] օգտվելով ցույց տանք, որ այն պարունակվում է $\mathcal{K}$-ի որեւէ $\mathcal{M}$ մաքսիմալ իդեալում: Վերցնենք $\mathcal{K}$-ի սեփական իդեալների մի աճող շղթա, որի տարրերը բոլորը պարունակում են $\mathcal{H}$-ը.

$$\mathcal{H} \subset \dots \subset \mathcal{S} \subset \dots \tag{4.3}$$

Այս շղթայի միավորումը նույնպես պարունակում է $\mathcal{H}$-ը, եւ այդ միավորումը նույնպես $\mathcal{K}$-ի սեփական իդեալ է, քանի որ հակառակ դեպքում օղակի 1 միավորը կպատկաներ (4.3) շղթայի իդեալներից մեկին, որը եւ կհամընկներ $\mathcal{K}$-ի հետ: Ուստի, ըստ Յորնի լեմմի, գոյություն ունի $\mathcal{K}$-ի այնպիսի մի մաքսիմալ $\mathcal{M}$ իդեալ, որ $\mathcal{M} \supseteq \mathcal{H}$: Նշանակենք

[1] Յորնի լեմմը կարելի է գտնել հանրահաշվի հիմունքներին վերաբերող դասագրքերում, օրինակ՝ (Cohn, 2003), (Cohn, 1965), (Lang, 2002), (ван дер Варден, 1979), (Ленг, 1968), (Garrett, 2008):

$$\overline{K} = \mathcal{K}/\mathcal{M}:$$

K-ի ներդրումը $\overline{K}$-ի մեջ տրվում է $\theta: a \to a + \mathcal{M}$ կանոնով: Շնորհիվ $\mathcal{M}$-ի մաքսիմալության եւ ըստ 2.3.15 թեորեմի՝ $\mathcal{K}/\mathcal{M}$ ֆակտոր-օղակը դաշտ է:

Հեշտ է տեսնել, որ հաստատունից տարբեր կամայական $f(x) \in K[x]$ բազմանդամ արմատ ունի $\overline{K}$-ի մեջ: Բավական է դա ապացուցել պարզ նորմավորված բազմանդամների համար (բոլոր մյուս բազմանդամները ունեն նման բաժանարարներ): $f(x)$ պարզ նորմավորված բազմանդամը պատկանում է H բազմությանը. ինչ-որ t ինդեքսի համար $f(x)$-ը (փոփոխականի վերանվանումից հետո) համընկնում է $h_t(x_{h_t}) \in H$ բազմանդամի հետ: Ուրեմն, $f(x_{h_t}) = h_t(x_{h_t}) \in \mathcal{H} \subseteq \mathcal{M}$: Հետեւաբար, $\theta(x_{h_t}) = x_{h_t} + \mathcal{M} \in \mathcal{K}/\mathcal{M}$ տարրը $f(x)$-ի արմատ է.

$$f\left(\theta(x_{h_t})\right) = f(x_{h_t} + \mathcal{M}) \in \mathcal{M} = 0 + \mathcal{M} = 0_{\overline{K}},$$

եւ բոլոր x_{h_t} տարրերի $\theta(x_{h_t})$ պատկերները հանրահաշվական են K-ի վրա:

Այստեղից բխում է, որ $\overline{K}$-ի յուրաքանչյուր տարր նույնպես հանրահաշվական է K-ի վրա: Իրոք, $\overline{K}$ դաշտի կամայական c տարր ունի

$$c = \theta\big(g(x_{i_1}, \dots, x_{i_k})\big) = g(x_{i_1}, \dots, x_{i_k}) + \mathcal{M}$$

տեսքը, որտեղ $g(x_{i_1}, \dots, x_{i_k})$-ը մի քանի փոփոխականի որեւէ բազմանդամ է $\mathcal{K} = K[x_h; h \in H]$ օղակից: Ինչպես տեսանք քիչ առաջ, այս $x_{i_1}, \dots, x_{i_k}$ փոփոխականների $\theta(x_{i_1}), \dots, \theta(x_{i_k})$ պատկերները հանրահաշվական են K-ի վրա: Այսինքն՝ c-ն պատկանում է K դաշտի $K[\theta(x_{i_1}), \dots, \theta(x_{i_k})] = K\left(\theta(x_{i_1}), \dots, \theta(x_{i_k})\right)$ ընդլայնմանը: Ըստ նախորդ թեորեմի, այդ ընդլայնումը հանրահաշվական է: Ուրեմն, c-ն հանրահաշվական է K-ի վրա:

Մնում է ապացուցել վերջին կետը. $\overline{K}$ դաշտի վրա տրված կամայական $b(y) \in \overline{K}[y]$ (հաստատունից տարբեր) բազմանդամ արմատ ունի $\overline{K}$-ում (մենք այստեղ փոփոխականը նշանակել ենք y տառով, որ շփոթություն չառաջանա մինչ այժմ օգտագործված x կամ x_{i_j} փոփոխականների հետ): $b(y)$-ի գործակիցները $\overline{K}$-ից են. դրանք ինչ-որ $x_{i_1}, \dots, x_{i_k}$ փոփոխականների վրա տրված $g(x_{i_1}, \dots, x_{i_k})$ բազմանդամների պատկերներ են θ հոմոմորֆիզմի ազդեցության տակ: Ինչպես տեսանք, այդ բոլոր պատկերները հանրահաշվական են K-ի վրա: Ուստի $b(y)$-ը բազմանդամ է նաեւ K դաշտի $K\left(\theta(x_{i_1}), \dots, \theta(x_{i_k})\right)$ ընդլայնման վրա սահմանված

$$K\left(\theta(x_{i_1}), \dots, \theta(x_{i_k})\right)[y]$$

բազմանդամային օղակում: Քանի որ $\theta(x_{i_1}), \dots, \theta(x_{i_k})$ տարրերը հանրահաշվական են K-ի վրա, ապա, ըստ նախորդ թեորեմի եւ 4.2.26 լեմմայի, $K\left(\theta(x_{i_1}), \dots, \theta(x_{i_k})\right)$

ընդլայնումը հանրահաշվական է K-ի վրա: Այսինքն՝ մեր բազմանդամը արմատներ ունի նաեւ K դաշտում: ■

4.2.31 թեորեմի պնդումը կարելի է ուժեղացնել: Մասնավորապես, K դաշտի հանրահաշվորեն փակ $\bar{K}$ ընդլայնումը *միակն* է այն իմաստով, որ թեորեմի պայմանին բավարարող ցանկացած երկու ընդլայնումներ իրար իզոմորֆ են: Ընդ որում, այդ իզոմորֆիզմն այնպիսին է, որ տեղում է թողնում K-ի բոլոր տարրերը (K դաշտը ներդրված է երկու ընդլայնումների մեջ էլ): Մեզ, սակայն, նման հավելյալ պնդումները պետք չեն գալու:

4.2.32 Օրինակներ. Ի հավելումն 4.2.30 օրինակի $\mathbb{C} = \overline{\mathbb{R}}$ հանրահաշվական փակույթի, այժմ արդեն գիտենք, որ հանրահաշվական A փակույթ ունի նաեւ ռացիոնալ $\mathbb{Q}$ դաշտը: Այդ փակույթը մեծ չէ $\mathbb{C}$-ից, քանի որ $\mathbb{Q} \subset \mathbb{R}$: Մյուս կողմից, A-ն խիստ փոքր է $\mathbb{C}$-ից, քանի որ այն չի պարունակում, ասենք, π թիվը (կամ ցանկացած այլ թիվ, որը տրանսցենդենտ է $\mathbb{Q}$-ի վրա): $A = \overline{\mathbb{Q}}$ դաշտն անվանում են *հանրահաշվական թվերի դաշտ*: Ըստ մեր ստացածի, $\mathbb{Q} \subset A \subset \mathbb{C}$ եւ $A \not\subseteq \mathbb{R}$: Նկատենք, որ մենք արդեն կարիք չունենք ստուգելու դաշտի սահմանման պայմանները A-ի համար, քանի որ դրանք ապահովված են նախորդ թեորեմով:

$\mathbb{C}$-ում կարելի է նշել ենթադաշտերի այլ օրինակներ, մասնավորապես.

4.2.33 Խնդիր. Վերցնենք $\mathbb{Q}$-ի վրա որեւէ a տրանսցենդենտ թիվ եւ դիտարկենք $\mathbb{Q}(a)$ դաշտի $\overline{\mathbb{Q}(a)}$ փակույթը: Ցույց տալ, որ այն տարբեր կլինի վերը դիտարկված բոլոր $\mathbb{Q}$, $\mathbb{Q}(a)$, A, $\mathbb{R}$, $\mathbb{C}$ դաշտերից: Սա վերաբերում է, մասնավորապես, $\overline{\mathbb{Q}(\pi)}$ եւ $\overline{\mathbb{Q}(e)}$ դաշտերին:

Վերջավոր $\mathbb{Z}_p$ դաշտը ոչ միայն ինքը հանրահաշվորեն փակ չէ, այլեւ վերջավոր չէ նրա հանրահաշվական փակույթը: Դա բխում է հետեւյալ խնդրից.

4.2.34 Խնդիր. Եթե K դաշտը վերջավոր է, ապա այն հանրահաշվորեն փակ չէ: Մասնավորապես, հանրահաշվորեն փակ չեն $\mathbb{Z}_p$ դաշտը եւ 4.1.5 օրինակում ու 4.1.6, 4.1.7 խնդիրներում բերված դաշտերը: Ըստ 4.2.31 թեորեմի, K-ն ունի հանրահաշվական փակույթ: Այն նույնպես վերջավոր լինել չի կարող: *Յուցում.* ենթադրենք $K = \{0,1,a_1,\dots,a_n\}$ դաշտը վերջավոր է: Դիտարկել հետեւյալ բազմանդամը $f(x) = (x-0)(x-1)(x-a_1)\cdots(x-a_n)+1 \in K[x]$, եւ ստուգել, որ այս բազմանդամն արմատ չունի K-ում:

$\mathbb{Z}_p$ դաշտի $\overline{\mathbb{Z}}_p$ հանրահաշվորեն փակույթի բնույթի մասին պատկերացում է տալիս, օրինակ, 4.2.31 թեորեմի ապացույցը: Այդ փակույթի կոնկրետ տեսքը հետագայում չի օգտագործվելու, բայց քանի որ $\mathbb{Z}_p$-ն, ընդհանրապես, կարեւոր դեր ունի մեր ալգորիթմների կառուցման մեջ, ուրվագծորեն, առանց ապացույցների տանք $\overline{\mathbb{Z}}_p$-ի ավելի դյուրընկալելի ներկայացումը:

4.1.5 օրինակի նմանությամբ հնարավոր է կառուցել p^n տարրից բաղկացած մի K դաշտ կամայական p պարզ թվի եւ n բնական թվի համար: p^n կարգի դաշտն ընդունված է նշանակել $GF(p^n)$ սիմվոլով: Այդ դաշտը կարելի է ստանալ որպես $\mathbb{Z}_p[x]/(m(x)\mathbb{Z}_p[x])$ ֆակտոր-օղակ, որտեղ $m(x)$-ը n-րդ աստիճանի որեւէ պարզ բազմանդամ է (դրանց գոյությունը հեշտ է ցույց տալ): Այդ դեպքում $GF(p^n)$-ը n չափողականության գծային տարածություն է $\mathbb{Z}_p = GF(p)$ դաշտի վրա եւ, ուրեմն,

$$|GF(p^n)| = \left|\mathbb{Z}_p\right|^{[GF(p^n):\mathbb{Z}_p]} = \left|\mathbb{Z}_p\right|^{\deg m(x)} = \left|\mathbb{Z}_p\right|^n = p^n$$

(տես ընդլայնման աստիճանի սահմանումը): Եթե $n_2 \vdots n_1$, ապա $GF(p^{n_1}) \subseteq GF(p^{n_2})$: Ուրեմն կարելի է ստանալ հետեւյալ անվերջ շղթան.

$$GF(p^{1!}) \subseteq GF(p^{2!}) \subseteq \cdots \subseteq GF(p^{n!}) \subseteq \cdots$$

Սահմանենք $\overline{\mathbb{Z}}_p = GF(p^\infty) = \bigcup_{n=1}^{\infty} GF(p^{n!})$: Այսինքն՝ $\overline{\mathbb{Z}}_p$ փակույթը ստացվում է դաշտերի հաջորդական ընդլայնումների մի շղթայի միջոցով, որտեղ յուրաքանչյուր ընդլայնումը կառուցվում է (նախորդ քայլում ստացված դաշտի վրա տրված) բազմանդամային օղակը ֆակտորիզացնելով ըստ համապատասխան պարզ բազմանդամի ծնված գլխավոր իդեալի:

Հավասար կարգի բոլոր վերջավոր դաշտերն իրար իզոմորֆ են: Նշենք այդ կարեւոր փաստն առանց ապացույցի.

4.2.35 Թեորեմ. *Տրված p պարզ թվի եւ n բնական թվի համար p^n կարգի կամայական $GF(p^n)$ դաշտ իզոմորֆ է $\overline{\mathbb{Z}}_p$ փակույթում $x^{p^n} - x$ բազմանդամի p^n հատ արմատներից բաղկացած դաշտին:*

$GF(p^n)$ նշանակումը կապված է Գալուայի դաշտ (Galois Field) բառակապակցության հապավման հետ: Վերջավոր դաշտերը հաճախ անվանում են *Գալուայի դաշտեր*, իսկ $\mathbb{Z}_p$ դաշտն էլ հաճախ նշանակում են $GF(p)$ կամ $\mathbb{F}_p$ սիմվոլներով: Չնայած այդ նշանակումները ավելի են տարածված դաշտերի տեսության մեջ,

մենք այստեղ օգտագործում ենք $\mathbb{Z}_p$ նշանակումը, քանի որ մեր շարադրանքի հիմնական մասը օղակների տեսության եւ խմբերի տեսության լեզվով է կատարվում: Դաշտերի ընդլայնումների տեսությանը կարելի է ավելի հանգամանորեն ծանոթանալ (Cohn, 2003), (Кострикин, 2004), (Кострикин, 1977), (Ленг, 1968), (ван дер Варден, 1979), (Garrett, 2008) դասագրքերով:

4.3 Բազմանդամի տրոհումը քառակուսիներից ազատ արտադրիչների

Ենթադրենք տրված է $f(x) \in R[x]$ բազմանդամը, որտեղ R-ը կամայական ամբողջության տիրույթ է: Կասենք, որ $f(x)$-ը ազատ չէ քառակուսիներից, եթե այն բաժանվում է որեւէ $q^2(x) \in R[x]$ բազմանդամի վրա, որտեղ $q(x) \not\approx 1$: Իսկ եթե նման $q^2(x)$ բաժանարար գոյություն չունի, ապա $f(x)$-ը կոչվում է *քառակուսիներից ազատ* բազմանդամ: Հասկանալի է, որ քառակուսիներից ազատ լինելը պարզ բազմանդամ լինելուց ավելի թույլ հատկություն է:

4.3.1 Օրինակներ. Հետեւյալ բազմանդամները բոլորն էլ $\mathbb{Z}[x]$ օղակից են.

1. $f(x) = x^2 + 3x + 1$ բազմանդամը ազատ է քառակուսիներից, ավելին, այն պարզ է:
2. $f(x) = x^2 + 3x + 2 = (x + 1)(x + 2)$ բազմանդամը ազատ է քառակուսիներից, քանի որ նրա ոչ տրիվիալ բաժանարարներից եւ ոչ մեկը քառակուսի չէ: Միաժամանակ $f(x)$-ը պարզ չէ:
3. $f(x) = x^3 + 2x^2 + x = (x + 1)^2 x$ բազմանդամը ազատ չէ քառակուսիներից, քանի որ այն բաժանվում է $(x + 1)^2$ բազմանդամի վրա: Հասկանալի է, որ $f(x)$-ը պարզ չէ:

Յուրաքանչյուր ֆակտորիալ օղակում (տես 6.1 պարագրաֆը) ամեն մի տարր հակադարձելի արտադրիչի ճշտությամբ միակ ձեւով ներկայացվում է պարզ արտադրիչների արտադրյալի տեսքով: Դա վերաբերում է նաեւ $\mathbb{Z}[x]$ օղակին, որի համար այդ փաստը ստացել ենք ավելի վաղ 2.6.13 թեորեմում: Այստեղից պարզ է, որ, եթե $R[x]$-ը ֆակտորիալ է, ապա յուրաքանչյուր $f(x) \in R[x]$ բազմանդամ ($f(x) \in \mathbb{Z}[x]$ բազմանդամ) կարելի է ներկայացնել քառակուսիներից ազատ բազմանդամների արտադրյալի տեսքով. եթե $f(x)$-ը ազատ չէ քառակուսիներից, ապա նրա

պարզ արտադրիչները կարելի է խմբավորել այնպես, որ յուրաքանչյուր խմբում յուրաքանչյուր պարզ արտադրիչ մասնակցի ոչ ավելի, քան մեկ անգամ: 4.3.1 օրինակի 3-րդ կետի բազմանդամը կարելի է ներկայացնել $f(x) = (x+1)^2x = [(x+1)x] \cdot [x+1]$ տեսքով, որտեղ քառակուսի փակագծերում գրված արտադրիչներից յուրաքանչյուրն ազատ է քառակուսիներից:

4.3.2 Օրինակ. Ավելի պակաս ակնհայտ օրինակ.

$$f(x) = x^{11} + 4x^{10} - 9x^9 - 46x^8 + 23x^7 + 192x^6 - 7x^5 - 358x^4 - 24x^3 + 304x^2 + 16x - 96:$$

Կարելի է ստուգել, որ

$$f(x) = (x-1)^3(x+2)^3(x+1)^2(x-2)^2(x+3),$$

ուստի այս բազմանդամը արտահայտվում է քառակաուսիներից ազատ երեք արտադրիչների արտադրյալի տեսքով $f(x) = g_1(x)g_2(x)g_3(x)$, որտեղ.

$$g_1(x) = (x-1)(x+2)(x+1)(x-2)(x+3),$$

$$g_2(x) = (x-1)(x+2)(x+1)(x-2),$$

$$g_3(x) = (x-1)(x+2):$$

Ընդ որում, քառակուսիներից ազատ արտադրիչների վերլուծությունը կախված է ամբողջության տիրույթից, եւ կարող է փոխվել, երբ R-ը փոխվում է:

4.3.3 Օրինակ. $\mathbb{Q}[x]$ օղակում $f(x) = 9x^3 + 18x^2 + 9x = 9(x+1)^2x$ բազմանդամի 9 արտադրիչն ասոցացված է 1-ին, քանի որ 9-ը հակադարձելի է: Ուստի որպես $f(x)$-ի վերլուծություն կարելի է գրել $f(x) = [9(x+1)x] \cdot [x+1]$: Բայց $\mathbb{Z}[x]$ օղակում $9 \nsim 1$, ուստի քառակուսիներից ազատ արտադրիչների վերլուծություն է, ասենք, $f(x) = [3(x+1)x] \cdot [3(x+1)]$:

Այս օրինակներում բազմանդամի վերլուծությունը քառակուսիներից ազատ արտադրիչների հենվում էր պարզ արտադրիչների վերլուծության վրա: Հետաքրքիր եւ կարեւոր ալգորիթմական նշանակություն ունեցող փաստ է այն, որ քառակուսիներից ազատ արտադրիչների վերլուծությունը կարելի է կառուցել անգամ առանց բազմանդամի պարզ արտադրիչներն իմանալու: Դրան նվիրված կլինեն հաջորդ երկու պարագրաֆները: Հետագայում քառակուսիներից ազատ արտադրիչների վերլուծությունը մեզ անհրաժեշտ կլինի նաեւ 7.3 եւ 7.4 պարագրաֆներում:

Մեզ պետք կգա *բազմանդամի ածանցյալի* հասկացությունը: Կամայական օղակի վրա տրված $f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ բազմանդամի համար սահմանենք նրա $f'(x)$ ածանցյալը, որն այստեղ ներմուծվում է մաթեմատիկական անալիզից հայտնի ածանցյալի գաղափարից անկախ.

$$f'(x) = na_0x^{n-1} + (n-1)a_1x^{n-2} + \cdots + a_{n-1}:$$

Ածանցյալի սովորական սահմանումից օգտվել չենք կարող, քանի որ մեր կառուցումները միշտ չէ, որ իրական դաշտում են կատարվում եւ ֆունկցիայի սահմանի գաղափարը կիրառել չենք կարող:

4.3.4 Օրինակ. $\mathbb{Z}_5[x]$ բազմանդամային օղակում $f(x) = 2x^5 + 3x^4 + 4x + 3$ բազմանդամի ածանցյալն է $f'(x) = 5 \cdot 2x^{5-1} + 4 \cdot 3x^{4-1} + 1 \cdot 4x^{1-1} = 2x^3 + 4$:

4.4 Արտադրիչների կառուցումը. զրոյական բնութագրիչի դեպքը

Դիտարկենք զրոյական բնութագրիչի R ամբողջության տիրույթի վրա տրված $f(x) \in R[x]$ բազմանդամի քառակուսիներից ազատ արտադրիչների կառուցման խնդիրը: R ամբողջության տիրույթն, ըստ 4.2.4 հետեւանքի, կարելի է ներդնել որեւէ K դաշտի մեջ եւ, ըստ 4.2.31 թեորեմի, կարելի է վերցնել K-ի հանրահաշվորեն փակ որեւէ F ընդլայնումը (օրինակ՝ $F = \overline{K}$ հանրահաշվական փակույթը):

Մասնավորապես, $R = \mathbb{Z}$ դեպքում կարելի է վերցնել $K = \mathbb{Q}$ եւ, ասենք, $F = \mathbb{C}$: Կարելի էր վերցնել նաեւ 4.2.32 օրինակում հիշատակված հանրահաշվական թվերի $F = A = \overline{\mathbb{Q}}$ դաշտը, բայց քանի որ F-ի կոնկրետ տեսքը մեր ալգորիթմում էական չէ, պարզության համար վերցնենք $F = \mathbb{C}$ (մենք օգտագործելու ենք միայն այն, որ F-ում ցանկացած $f(x) \in \mathbb{Z}[x]$ բազմանդամ արմատ ունի):

F դաշտի (մասնավոր դեպքում՝ $\mathbb{C}$ դաշտի) հանրահաշվորեն փակ լինելուց եւ Բեզուի թեորեմից հեշտ է բխեցնել, որ

$$f(x) = a_0(x - x_1) \cdots (x - x_n), \tag{4.4}$$

որտեղ $x_1, \ldots, x_n \in F$ տարրերը $f(x)$-ի բոլոր արմատներն են: Այս առնչությունը տեղի ունի $f(x) \in \mathbb{C}[x]$ մասնավոր դեպքի համար նույնպես:

(4.4) ներկայացման մեջ, խմբավորելով նման արտադրիչները, կստանանք.

(4.5) $$f(x) = a_0(x - x_1)^{k_1} \cdots (x - x_s)^{k_s},$$

որտեղ արդեն $x_i \neq x_j$, եթե $i \neq j$: Այստեղից.

(4.6) $$f'(x) = a_0 \sum_{i=1}^{s} [(x - x_1)^{k_1} \cdots (x - x_{i-1})^{k_{i-1}} \cdot k_i(x - x_i)^{k_i - 1} \cdot (x - x_{i+1})^{k_{i+1}} \cdots (x - x_s)^{k_s}]$$

(աջ կողմի գումարի գումարելիները ստացվել են (4.5) արտադրյալը ածանցելով ըստ արտադրյալի ածանցման կանոնի, ինչը ստուգելը դժվար չէ): Այստեղից.

(4.7) $$f'(x) = a_0(x - x_1)^{k_1 - 1} \cdots (x - x_s)^{k_s - 1} \cdot k(x),$$

որտեղ

(4.8) $$k(x) = \sum_{i=1}^{s} [(x - x_1) \cdots (x - x_{i-1}) \cdot k_i \cdot (x - x_{i+1}) \cdots (x - x_s)]:$$

Այստեղից սկսած մեր դատողությունները կախված են լինելու այն փաստից, որ $\mathrm{char}(R) = 0$, այսինքն՝ ոչ մի դրական ամբողջ n թվի եւ օղակի 1 միավորի համար տեղի չունի

$$\underbrace{1 + \cdots + 1}_{n} = 0$$

հավասարությունը (տես 4.1.2 սահմանումը): Ինչպես կտեսնենք հետագայում, սա ամենապարզ եւ ալգորիթմներում ամենակիրառվող դեպքն է:

Հաշվենք, թե $x - x_j$ միանդամի ո՞ր ամենաբարձր աստիճանն է բաժանում (4.7) արտահայտությունը ($j = 1, \ldots, s$): Հասկանալի է, որ $(x - x_j)^{k_j - 1}$ արտադրիչը մտնում է (4.7) արտահայտության մեջ: Մյուս կողմից, $k(x)$ գումարը բաղկացած է s գումարելիներից, որոնցից $s - 1$ հատը պարունակում են $x - x_j$ արտադրիչը, իսկ մեկը (j-րդ գումարելին) պարունակում է ոչ թե $x - x_j$ արտադրիչը, այլ համապատասխան ածանցումից գոյացած k_j թիվը: Քանի որ $\mathrm{char}(R) = 0$, ապա ոչ զրոյական որեւէ արտահայտություն k_j-ով բազմապատկելիս չի զրոյանում: Ուստի $k(x)$-ը չի բաժանվում $x - x_j$ արտադրիչի վրա, քանի որ այն պարունակում է ճիշտ մեկ ոչ զրոյական գումարելի, որը $x - x_j$ արտադրիչի վրա չի բաժանվում:

Այստեղից եւ (4.5) արտահայտությունից բխում է, որ

(4.9) $$\big(f(x), f'(x)\big) = a_0(x - x_1)^{k_1 - 1} \cdots (x - x_s)^{k_s - 1} \approx (x - x_1)^{k_1 - 1} \cdots (x - x_s)^{k_s - 1}:$$

Իսկ սա մեզ հնարավորություն է տալիս հաշվելու $f(x)$ բազմանդամի քառակուսիներից ազատ առաջին $g(x)$ արտադրիչը $K[x]$ օղակում.

$$g(x) = \frac{f(x)}{\big(f(x), f'(x)\big)} \approx (x - x_1) \cdots (x - x_s): \tag{4.10}$$

Հաջորդ քառակուսիներից ազատ արտադրիչը գտնելու համար անցնենք $f(x) = f(x)/g(x)$ բազմանդամին եւ քայլը կրկնենք նրա ածանցյալի համար:

Որպեսզի մենք ամեն քայլում ստիպված չլինենք հաշվի առնել $a_0 \in K$ սկալյարը եւ (4.9) բանաձեւով կրկին ազատվել դրանից, պայմանավորվենք ի սկզբանե անցնել $f(x) = \frac{1}{a_0} f(x)$ նորմավորված բազմանդամին $K[x]$-ում, հաշվել դրա վերլուծությունը քառակուսիներից ազատ արտադրիչների, եւ վերջում a_0-ով բազմապատկել ստացված քառակուսիներից ազատ արտադրիչներից որեւէ մեկը, ասենք, առաջինը: Քառակուսիներից ազատ արտադրիչների գրառման համար սահմանենք բազմանդամների $\mathcal{S}$ ցանկը (հաջորդականությունը), որն ալգորիթմի սկզբում կարելի է համարել դատարկ: Շեշտենք, որ $\mathcal{S}$-ը ցանկ է, այլ ոչ՝ բազմություն, քանի որ բազմության տարրերն, ըստ սահմանման, պետք է իրարից տարբեր լինեն, իսկ քառակուսիներից ազատ արտադրիչները կարող են եւ կրկնվել:

Այն դեպքում, երբ $R = K$ օղակը դաշտ է, մենք արդեն կառուցել ենք հետեւյալ ալգորիթմը.

4.4.1 Ալգորիթմ (քառակուսիներից ազատ արտադրիչների վերլուծումը զրոյական բնութագրիչի դաշտի վրա տրված բազմանդամային օղակում): Տրված է $f(x) \in K[x]$ բազմանդամը, որտեղ K-ն զրոյական բնութագրիչի դաշտ է: Վերլուծել այն քառակուսիներից ազատ արտադրիչների:

1. a_0-ով նշանակենք $f(x)$ բազմանդամի ավագ գործակիցը:

2. Նշանակենք $f(x) = \frac{1}{a_0} f(x)$:

3. Սահմանենք բազմանդամների $\mathcal{S}$ դատարկ ցանկը:

4. Հաշվենք $f'(x)$ ածանցյալը:

5. $K[x]$ օղակում Էվկլիդեսի ալգորիթմով հաշվենք $\big(f(x), f'(x)\big)$ ամենամեծ ընդհանուր բաժանարարը:

6. Նշանակենք $g(x) = \frac{f(x)}{(f(x), f'(x))}$:

7. Նորմավորենք $g(x)$ բազմանդամը:

8. $\mathcal{S}$ ցանկին ավելացնենք $g(x)$ բազմանդամը:

9. Նշանակենք $f(x) = \frac{f(x)}{g(x)}$:

10. Եթե $f(x) = 1$

11. անցնենք 14-րդ քայլին;

12. հակառակ դեպքում

13. վերադառնանք 4-րդ քայլին:

14. $\mathcal{S}$ ցանկի բազմանդամներից որեւէ մեկը, օրինակ, առաջին $g(x)$ բազմանդամը, փոխարինենք $g(x) = a_0 \cdot g(x)$ բազմանդամով:

15. Դուրս գրենք $\mathcal{S}$ ցանկի բազմանդամները՝ որոնելի քառակուսիներից ազատ արտադրիչները:

4.4.2 Վարժություն. $\mathbb{Q}[x]$ բազմանդամային օղակում քառակուսիներից ազատ արտադրիչների վերլուծել հետեւյալ բազմանդամները.

1) $f(x) = x^4 + 6x^3 + 13x^2 + 12x + 4$,
2) $f(x) = 4x^3 + 16x^2 + 13x + 3$:

4.4.3 Վարժություն. $\mathbb{Q}[x]$ բազմանդամային օղակում կիրառել 4.4.1 ալգորիթմն այն դեպքում, երբ $f(x) = c \neq 0$ հաստատուն բազմանդամ է:

Չնայած 4.4.1 ալգորիթմը կիրառելի է հաճախակի օգտագործվող $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ դաշտերի վրա, ալգորիթմի ակնհայտ թերությունն է, որ այն չենք կարող օգտագործել $\mathbb{Z}$-ի վրա: Դա կարելի է հաղթահարել՝ օգտվելով 4.2.4 հետեւանքից:

Ինչպես նշեցինք սկզբում, ցանկացած R ամբողջության տիրույթն, ըստ 4.2.4 հետեւանքի, կարելի է ներդնել քանորդների K դաշտի մեջ, որի վրա արդեն կարելի է կիրառել 4.4.1 ալգորիթմը: Այսինքն՝ ունենք $f(x) \in R[x]$ բազմանդամի վերլուծությունը քառակուսիներից ազատ արտադրիչների, որոնք $K[x]$ օղակից են: Երբ $R = \mathbb{Z}$, այդ արտադրիչները $\mathbb{Q}[x]$-ից են:

$f(x)$-ը վերլուծենք իր բովանդակության եւ պրիմիտիվ մասի արտադրյալին. $f(x) = \mathrm{cont}\big(f(x)\big)\,\mathrm{pp}\big(f(x)\big)$: Քանի որ $\mathrm{cont}\big(f(x)\big) \in \mathbb{Z}$, դուրս գրենք $\mathrm{cont}\big(f(x)\big)$-ի քառակուսիներից ազատ արտադրիչները $\mathbb{Z}$-ում, եւ դրանցից կազմենք $\mathcal{S}$ ցանկը (հետագայում մենք դրան էլի ենք անդամներ ավելացնելու): Անցնենք $f(x) = \mathrm{pp}\big(f(x)\big)$ պրիմիտիվ մասին (տես նաեւ 4.3.3 օրինակը): Ըստ 4.4.1 ալգորիթմի՝ գտնենք $f(x)$-ի քառակուսիներից ազատ արտադրիչները $\mathbb{Q}[x]$ օղակում՝

$$f(x) = g_1(x) \cdots g_r(x) \in \mathbb{Q}[x]:$$

Հասկանալի է, որ դրանք կարող են ունենալ կոտորակային գործակիցներ $\mathbb{Q}$-ից: $g_1(x), \ldots, g_r(x)$ բազմանդամների բոլոր գործակիցների հայտարարների ամենափոքր ընդհանուր բազմապատիկը նշանակենք v-ով: Պարզ է, որ

$$v \cdot f(x) = v \cdot g_1(x) \cdots g_r(x)$$

հավասարության աջ կողմում քառակուսիներից ազատ նոր արտադրիչներ չեն առաջանում ($\mathbb{Q}[x]$ օղակում): Մյուս կողմից, $v \cdot g_i(x) \in \mathbb{Z}[x]$, $i = 1, \dots, r$: Դիտարկենք $\mathrm{pp}\big(v \cdot g_i(x)\big)$ պրիմիտիվ մասը: Ըստ 2.6.11 լեմմայի՝ այն բաժանում է $f(x)$-ը նաեւ $\mathbb{Z}[x]$ օղակում: Քանի որ այն $\mathbb{Z}[x]$-ում քառակուսիներից ազատ է, ստանում ենք, որ որոնելի քառակուսիներից ազատ արտադրիչներն են $\mathrm{pp}\big(v \cdot g_i(x)\big)$, $i = 1, \dots, r$ դրական աստիճանի բազմանդամները, որոնց մենք ավելացնում ենք $\mathcal{S}$ ցանկին:

Ստանում ենք հետեւյալ ալգորիթմը.

4.4.4 Ալգորիթմ (քառակուսիներից ազատ արտադրիչների վերլուծումը $\mathbb{Z}[x]$ օղակում): Տրված է $f(x) \in \mathbb{Z}[x]$ բազմանդամը: Վերլուծել այն քառակուսիներից ազատ արտադրիչների:

1. $f(x)$ բազմանդամի համար $\mathbb{Z}$ օղակում Էվկլիդեսի ալգորիթմով հաշվենք նրա $\mathrm{cont}\big(f(x)\big)$ բովանդակությունը:

2. $\mathcal{S}$-ով նշանակենք $\mathrm{cont}\big(f(x)\big) \in \mathbb{Z}$ թվի քառակուսիներից ազատ արտադրիչների ցանկը:

3. Նշանակենք $f(x) = \mathrm{pp}\big(f(x)\big)$:

4. Համարելով $f(x) \in \mathbb{Q}[x]$, ըստ 4.4.1 ալգորիթմի, գտնենք $f(x)$-ի քառակուսիներից ազատ $g_1(x), \dots, g_r(x)$ արտադրիչները $\mathbb{Q}[x]$ օղակում:

5. v-ով նշանակենք $g_1(x), \dots, g_r(x)$ բազմանդամների բոլոր գործակիցների հայտարարների ամենափոքր ընդհանուր բազմապատիկը, որը $\mathbb{Z}[x]$ օղակում կարելի է հաշվել Էվկլիդեսի ալգորիթմի օգնությամբ:

6. ($i = 1$; $i \le r$; $i++$) արժեքների համար

7. Էվկլիդեսի ալգորիթմով $\mathbb{Z}[x]$ օղակում հաշվենք $\mathrm{cont}\big(v \cdot g_i(x)\big)$ բովանդակությունը;

8. հաշվենք $\mathrm{pp}\big(g_i(x)\big) = g_i(x)/\mathrm{cont}\big(v \cdot g_i(x)\big)$ պրիմիտիվ մասը;

9. $\mathcal{S}$ ցանկին ավելացնենք $\mathrm{pp}\big(g_i(x)\big)$ բազմանդամը:

10. Դուրս գրենք $\mathcal{S}$ ցանկի բազմանդամները՝ որոնելի քառակուսիներից ազատ արտադրիչները:

4.4.5 Օրինակ. Քառակուսիներից ազատ արտադրիչների վերլուծենք $f(x)=x^3+4x^2+5x+2\in\mathbb{Z}[x]$ բազմանդամը: Քանի որ $\operatorname{cont}\big(f(x)\big)$ բովանդակությունը տրիվիալ է, միանգամից $\mathbb{Z}$ օղակից անցնենք $\mathbb{Q}$ դաշտին եւ համարենք, որ $f(x)=x^3+4x^2+5x+2\in\mathbb{Q}[x]$: Քանի որ $f'(x)=3x^2+8x+5\neq 0$, ապա նրանց $\big(f(x),f'(x)\big)$ ամենամեծ ընդհանուր բաժանարարը հաշվենք ըստ Էվկլիդեսի ալգորիթմի.

$$\begin{array}{l|l}
x^3+4x^2+5x+2 & 3x^2+8x+5 \\
\cline{2-2}
x^3+{}^8\!/_3\,x^2+{}^5\!/_3\,x & {}^1\!/_3\,x+{}^4\!/_9 \\
\cline{1-1}
\quad {}^4\!/_3\,x^2+{}^{10}\!/_3\,x+2 & \\
\quad {}^4\!/_3\,x^2+{}^{32}\!/_9\,x+{}^{20}\!/_9 & \\
\cline{1-1}
\qquad -{}^2\!/_9\,x-{}^2\!/_9 &
\end{array}$$

$$\begin{array}{l|l}
3x^2+8x+5 & -{}^2\!/_9\,x-{}^2\!/_9 \\
\cline{2-2}
3x^2+3x & -{}^{27}\!/_2\,x-{}^{45}\!/_2 \\
\cline{1-1}
\quad 5x+5 & \\
\quad 5x+5 & \\
\cline{1-1}
\qquad 0 &
\end{array}$$

Ստանում ենք, որ $\big(f(x),f'(x)\big)=-{}^2\!/_9\,x-{}^2\!/_9\approx x+1=\operatorname{pp}(x+1)$: Վերջին անցումը ամբողջ գործակիցներով բազմանդամի կարելի է կատարել, քանի որ հաշվարկները $\mathbb{Q}[x]$-ում են: Որպես քառակուսիներից ազատ առաջին արտադրիչ՝ ստանում ենք.

$$g_1(x)=\frac{f(x)}{\big(f(x),f'(x)\big)}=\frac{x^3+4x^2+5x+2}{x+1}=x^2+3x+2:$$

$f(x)$-ը փոխարինենք $f(x)/g_1(x)=x+1$ բազմանդամով: Այն քառակուսիներից ազատ է. $g_2(x)=x+1$: Որոնելի վերլուծությունն է $f(x)=g_1(x)g_2(x)=(x^2+3x+2)(x+1)$: Նկատենք, որ մենք մի փոքր շեղվեցինք 4.4.4 ալգորիթմի քայլերից. $\big(f(x),f'(x)\big)$-ը հաշվելուց հետո մենք չօգտագործեցինք $-{}^2\!/_9\,x-{}^2\!/_9$ ամենամեծ ընդհանուր բաժանարարը, այլ միանգամից բերեցինք այն $x+1$ տեսքի: Դա ակնհայտորեն կարելի էր անել: Եթե այդ պարզեցումը չանեինք, ապա երկրորդ քայլում կունենայինք $\frac{x^3+4x^2+5x+2}{-{}^2\!/_9\,x-{}^2\!/_9}$ բազմանդամը: Կոտորակային գործակիցներից կազատվեինք ամենավերջում՝ v արտադրիչի օգնությամբ:

4.4.6 Վարժություն. Ստուգել, որ նախորդ օրինակում ստացված $g_1(x)=x^2+3x+2$ բազմանդամը քառակուսիներից ազատ է:

4.4.7 Վարժություն. $\mathbb{Z}[x]$ օղակում քառակուսիներից ազատ արտադրիչների վերլուծել հետեւյալ բազմանդամները.

1) $f(x) = x^3 + x^2 - 5x + 3$,
2) $f(x) = 8x^3 - 12x^2 + 4$:

4.4.8 Դիտողություն. Նկատենք 4.4.1, 4.4.4 ալգորիթմների եւ հաջորդ պարագրաֆի 4.5.2 ալգորիթմի հետեւյալ կարեւոր առանձնահատկությունը. դրանց հիմնավորման համար մենք օգտագործում ենք այնպիսի հասկացություններ, ինչպիսիք են հանրահաշվական տարրերը դաշտերի ընդլայնումներում, հանրահաշվորեն փակ դաշտերը, դաշտերի փակույթները եւ այլն: Վերջնական ալգորիթմի շարադրանքում, սակայն, դաշտերի տեսության այդ հասկացությունները ներկա չեն, եւ ալգորիթմները շատ ավելի պարզ հասկացությունների վրա են հենվում: Մասնավորապես, 4.4.5 օրինակում մենք կիրառել ենք 4.4.4 ալգորիթմը՝ առանց հիշատակելու հանրահաշվորեն փակ $\mathbb{C}$ դաշտը կամ դաշտերի ընդլայնումները, չնայած դրանք անհրաժեշտ են ալգորիթմի տեսական հիմնավորման համար:

4.5 Արտադրիչների կառուցումը. վերջավոր դաշտի դեպքը

Ենթադրենք մեր R վերջավոր ամբողջության տիրույթն արդեն ներդրված է K վերջավոր դաշտի մեջ, եւ K-ն էլ ներդրված է հանրահաշվորեն փակ F դաշտի մեջ (F-ի վրա արդեն վերջավոր լինելու պայման չի դրվում): Քանի որ գործ ունենք վերջավոր դաշտերի հետ, ապա դաշտի բնութագրիչը որեւէ պարզ թիվ է՝ $\mathrm{char}(K) = \mathrm{char}(F) = p$: Այսինքն՝ կամայական $a \in K \subseteq F$ տարրի համար.

$$pa = p1 \cdot a = \underbrace{(1 + \cdots + 1)}_{p} a = 0 \cdot a = 0:$$

Սրա մասնավոր եւ ալգորիթմերում ամենից հաճախ կիրառվող դեպքն է $R = \mathbb{Z}_p$ օղակը: Այս դեպքում $\mathrm{char}(\mathbb{Z}_p) = p$ եւ $R = K$ եւ, ի տարբերություն նախորդ պարագրաֆի դեպքի, K դաշտին անցնելու համար քանորդների դաշտը քննարկելու կարիք չկա, քանի որ R-ն արդեն իսկ դաշտ է:

Ի տարբերություն $\mathbb{Z}$ օղակի (որի համար որպես հանրահաշվորեն փակ ընդլայնում կարող էինք վերցնել կոմպլեքս թվերի $\mathbb{C}$ դաշտը), $\mathbb{Z}_p$-ի համար մենք չունենք p բնութագրիչի հանրահաշվորեն փակ F դաշտի որեւէ հանրահայտ օրինակ: Ավելին, ինչպես տեսանք, ոչ մի վերջավոր F դաշտ չի կարող հանրահաշվորեն փակ լի-

նել (տես 4.2.34 խնդիրը): Որպես F կարող ենք վերցնել այն դաշտը, որը կառուցվել է 4.2.31 թեորեմի ապացույցի ընթացքում, կամ էլ այն ավելի պարզ $\overline{\mathbb{Z}}_p = GF(p^\infty)$ կառուցվածքը, որը ներկայացվեց 4.2.34 խնդրից հետո: Բոլոր դեպքերում մեր համար էական չէ F դաշտի տեսքը. բավական է իմանալ, որ $\mathbb{Z}_p$-ն ներդրվում է հանրահաշվորեն փակ որեւէ F դաշտի մեջ (տես նաեւ 1.1.1 դիտողությունը):

Վերադառնանք նախորդ պարագրաֆի սկզբի դատողություններին եւ (4.7) արտահայտությանը, որը ճիշտ էր կամայական բնութագրիչի համար: Հասկանալի է, որ, ի տարբերություն նախորդ պարագրաֆի, (4.7) արտահայտության մեջ եւ (4.8) արտահայտության $k(x)$ բազմանդամի մեջ բոլոր $x_1, \dots, x_n$ արժեքներն այս անգամ վերցված են p բնութագրիչի F դաշտից:

Խնդիրներ կարող են առաջանալ $k(x)$ արտադրիչի հետ կապված, քանի որ նրա (4.8) գրության մեջ որոշ գումարելիներ կարող են եւ զրոյանալ k_i արտադրիչի ավելանալու շնորհիվ. k_i-ն կարող է լինել p-ի վրա բաժանվող թիվ: Հնարավոր են հետեւյալ երեք դեպքերը.

Դեպք 1. k_i արտադրիչներից ոչ մեկը չի բաժանվում p-ի վրա: Այդ դեպքում մեր դիտարկումները չի տարբերվում զրոյական բնութագրիչի դեպքից, որ քննարկեցինք նախորդ պարագրաֆում:

Դեպք 2. Ենթադրենք k_i արտադրիչներից մի քանիսը (բայց ոչ բոլորը) բաժանվում են p-ի վրա: Քանի որ մենք կարող ենք վերադասավորել (4.5) ներկայացման արտադրիչները, համարենք, որ p-ի վրա բաժանվող արտադրիչներն են առաջին m հատը ($0 \le m \le s$):

$$p|k_1, \dots, p|k_m; \quad p \nmid k_{m+1}, \dots, p \nmid k_s:$$

Ինչպես տեսանք նախորդ պարագրաֆում, զրոյական բնութագրիչի դեպքը դիտարկելիս (4.8) արտահայտության մեջ բոլոր գումարելիները, բացի մեկից, բաժանվում էին $x - x_j$ միանդամի վրա, եւ դրա շնորհիվ (4.8) գումարը $x - x_j$ միանդամի վրա չէր բաժանվում: Իսկ այժմ (4.8) գումարում բացակայում են (զրոյացել են) այն առաջին m գումարելիները, որոնց շնորհիվ (4.8) արտահայտությունը չէր բաժանվում

$$x - x_1, x - x_2, \dots, x - x_m$$

միանդամների վրա: Այժմ $k(x)$-ը բաժանվում է $x - x_j$ միանդամների վրա այն եւ միայն այն դեպքում, երբ $j \le m$: Ուրեմն.

$$\begin{aligned}\big(f(x),f'(x)\big) &= a_0(x-x_1)^{k_1}\cdots(x-x_m)^{k_m}\cdot(x-x_{m+1})^{k_{m+1}-1}\cdots(x-x_s)^{k_s-1}\\ &\approx (x-x_1)^{k_1}\cdots(x-x_m)^{k_m}\cdot(x-x_{m+1})^{k_{m+1}-1}\cdots(x-x_s)^{k_s-1}:\end{aligned}$$

Քանի որ այս արտահայտության մեջ $s-m>0$ հատ միանդամներ մասնակցում են ավելի ցածր աստիճանով, քան (4.5) արտադրյալում, ապա այս դեպքում եւս (4.10)-ի նմանությամբ կարող ենք ստանալ $f(x)$ բազմանդամի քառակուսիներից ազատ առաջին $g(x)$ արտադրիչը.

$$g(x)=\frac{f(x)}{\big(f(x),f'(x)\big)}\approx(x-x_{m+1})\cdots(x-x_s): \tag{4.11}$$

Անցնենք $f(x)=f(x)/g(x)$ բազմանդամին եւ քայլը կրկնենք նրա համար:

Դեպք 3. Մնացել է այն դեպքը, երբ k_i արտադրիչները բոլորն էլ բաժանվում են p-ի վրա, $i=1,\dots,s$: Այս դեպքը էապես տարբեր է քննարկված դեպքերից, քանի որ $k(x)$ բազմանդամն ու նրա հետ միասին նաեւ $f'(x)$ ածանցյալը ամբողջովին զրոյանում են (տես (4.7) արտահայտությունը): Դա նշանակում է, որ

$$\big(f(x),f'(x)\big)=f(x)$$

եւ

$$g(x)=\frac{f(x)}{\big(f(x),f'(x)\big)}=1$$

հարաբերության դիտարկումն այլեւս հնարավորություն չի տալիս $f(x)$-ի սեփական արտադրիչ գտնել: Դժվար չէ բերել օրինակներ, երբ նման իրավիճակ, իրոք, տեղի ունի:

4.5.1 Օրինակ. Եթե $f(x)=x^p+1$, ապա $\mathbb{Z}_p$ դաշտի վրա $f'(x)=px^{p-1}+0=0$, եւ $f'(x)$ բազմանդամն այլեւս էական ինֆորմացիա չի պարունակում $f(x)$-ի արտադրիչների մասին՝

$$\big(f(x),f'(x)\big)=(f(x),0)=f(x):$$

Մյուս կողմից, $\mathbb{Z}_p$ դաշտի վրա $f(x)$-ն ունի հետեւյալ վերլուծությունը.

$$f(x)=x^p+1=x^p+1^p=(x+1)^p,$$

որը դժվար չէ ստուգել՝ $(x+1)^p$ արտահայտությունը վերլուծելով Նյուտոնի բինոմական բանաձեւով (ստացվում են $p+1$ հատ գումարելիներ, որոնցից բոլորը, բացի առաջինից եւ վերջինից, զրոյանում են, քանի որ ունեն p-ի վրա բաժանվող գործակիցներ):

$f'(x) = 0$ հավասարությունը հնարավոր էր միայն, երբ $f(x)$-ի բոլոր միանդամների աստիճանացույցերը բաժանվում են p-ի աստիճանների վրա, ինչպես 4.5.1 օրինակում ունեինք x^p եւ $1 = x^0$ միանդամները, որոնց աստիճանացույցերն են p եւ 0: Թող p^c-ն լինի p-ի առավելագույն աստիճանը, որը բաժանում է $f(x)$-ի բոլոր միանդամների աստիճանացույցերը:

Ունենք.

(4.12) $$f(x) = a_0 x^{p^c \cdot b_0} + a_1 x^{p^c \cdot b_1} + \cdots + a_n$$

եւ

$$f'(x) = p^c(b_0 \cdot a_0)x^{p^c \cdot b_0 - 1} + p^c(b_1 \cdot a_1)x^{p^c \cdot b_1 - 1} + \cdots + 0 = 0:$$

Մենք R վերջավոր ամբողջության տիրույթից անցում ենք կատարել K վերջավոր դաշտին, ու մեր բազմանդամները $K[x]$-ում են (մասնավորապես, եթե $R = \mathbb{Z}_p$, ապա նաեւ $K = \mathbb{Z}_p$):

Գտնենք այնպիսի մի u ամբողջ թիվ, որ կամայական $a \in K$ ոչ զրոյական տարրի a^u աստիճանի համար տեղի ունենա

$$(a^u)^{p^c} = a^{u \cdot p^c} = a:$$

Սա, իրոք, հնարավոր է, քանի որ K վերջավոր դաշտի ոչ զրոյական (հակադարձելի) տարրերի K^* բազմությունը $p^m - 1$ կարգի մուլտիպլիկատիվ ցիկլիկ խումբ է, որտեղ $p^m = |K|$ (տես 4.1.10 եւ 4.1.11 թեորեմները): Ուրեմն, ոչ զրոյական $a \in K$ տարրի համար ունենք $a^{p^m - 1} = 1$: Հասկանալի է, որ p^c եւ $p^m - 1$ թվերը փոխադարձաբար պարզ են, ուստի, ըստ Էվկլիդեսի ընդհանրացված ալգորիթմի, գոյություն ունեն այնպիսի u, v ամբողջ թվեր, որոնց համար

$$up^c + v(p^m - 1) = 1:$$

Հետեւաբար.

$$\begin{aligned} a = a^1 = a^{up^c + v(p^m - 1)} &= a^{up^c} a^{v(p^m - 1)} \\ &= (a^u)^{p^c}\left(a^{p^m - 1}\right)^v = (a^u)^{p^c}, \end{aligned}$$

եւ որոնելի a^u աստիճանը գտնված է:

(4.12) տեսքով տրված $f(x)$ բազմանդամի համար կառուցենք հետեւյալ $\Phi(x)$ բազմանդամը.

(4.13) $$\Phi(x) = a_0^u x^{b_0} + a_1^u x^{b_1} + \cdots + a_n^u,$$

որը ստացվում է $f(x)$-ի հետ երկու ձեւափոխություն կատարելով. յուրաքանչյուր գործակից բարձրացված է u-րդ աստիճան, եւ x-ի յուրաքանչյուր $x^{p^c \cdot b_i}$ աստիճան փոխարինված է x^{b_i} աստիճանով: Հաշվենք $\Phi^{p^c}(x)$ արժեքը.

$$\Phi^{p^c}(x) = (a_0^u\, x^{b_0} + a_1^u x^{b_1} + \cdots + a_n^u)^{p^c}$$
$$= (a_0^u\, x^{b_0})^{p^c} + (a_1^u x^{b_1})^{p^c} + \cdots + (a_n^u)^{p^c}:$$

Սա մենք ստացել ենք՝ կիրառելով Նյուտոնի (ընդհանրացված) բինոմական բանաձեւը եւ զրոյացնելով p-ի վրա բաժանվող գործակիցներով գումարելիները: Աջ կողմի գումարելիներից յուրաքանչյուրի համար

$$(a_i^u x^{b_i})^{p^c} = a_i^{u \cdot p^c} x^{b_i \cdot p^c} = a_i x^{b_i \cdot p^c}$$

(այստեղ է, որ մեզ պետք եկավ u-ի ընտրությունը), եւ, ուրեմն՝

$$\Phi^{p^c}(x) = f(x), \tag{4.14}$$

այսինքն՝ մեր $f(x)$ բազմանդամը ո՛չ միայն քառակուսիներից ազատ չէ, այլեւ ներկայացվում է $\Phi(x)$ բազմանդամի աստիճանի տեսքով: Մենք չենք կարող պնդել, թե $\Phi(x)$ բազմանդամն ինքը ազատ է քառակուսիներից, սակայն մենք արդեն իսկ ունենք ալգորիթմի հերթական քայլը. $f(x)$ բազմանդամից կարելի է անցում կատարել ավելի ցածր աստիճանի $\Phi(x)$ բազմանդամին, եւ հետագա քննարկումը շարունակել $\Phi(x)$-ի համար: Ընդ որում, $\Phi(x)$ բազմանդամի բացահայտ տեսքը մեզ հայտնի է, քանի որ մենք ունենք c թիվը (այն գտնում ենք $f(x)$-ի աստիճաններից) եւ ունենք u թիվը (այն գտնում ենք Էվկլիդեսի ընդհանրացված ալգորիթմով):

Նշված երեք տիպի քայլերը վերջավոր անգամ կրկնելով՝ մենք քառակուսիներից ազատ արտադրիչների կարող ենք վերլուծել վերջավոր ամբողջության տիրույթի (վերջավոր դաշտի) վրա տրված կամայական բազմանդամ: Քառակուսիներից ազատ արտադրիչների գրության համար սահմանենք բազմանդամների $\mathcal{S}$ ցանկը, որն ալգորիթմի սկզբում դատարկ է:

Կրկին շեշտենք, որ եթե առաջին երկու դեպքերում մենք ալգորիթմի հերթական քայլից հետո ստանում եւ $\mathcal{S}$ ցանկ ենք ներմուծում $f(x)$ բազմանդամի հերթական $g(x)$ քառակուսիներից ազատ արտադրիչը, ապա երրորդ դեպքում ալգորիթմի քայլի ընթացքում անցում ենք կատարում $f(x)$ բազմանդամից դեպի ավելի ցածր աստիճանի $f(x) = \Phi(x)$ բազմանդամին եւ մտապահում p^c թիվը: Եւ երբ հաջորդ քայլերում ստանում ենք քառակուսիներից ազատ հերթական արտադրիչնե-

րը, մենք դրանք $\mathcal{S}$ ցանկ ենք ավելացնում p^c անգամ, քանի որ, եթե $\Phi(x)$-ը ունի, ասենք, քառակուսիներից ազատ $g(x)$ արտադրիչը, ապա $\Phi^{p^c}(x)$ բազմանդամի վերլուծության մեջ դրան կհամապատասխանի $g(x)^{p^c}$ արտադրիչը:

Եթե երրորդ տիպի քայլը ալգորիթմի աշխատանքի ընթացքում մի քանի անգամ է հանդիպում, ապա համապատասխանաբար աճում են եւ աստիճանները (դրանց հաշվառման համար ներմուծենք մի նոր s փոփոխական, որի արժեքը ալգորիթմի սկզբում կարելի է համարել 1):

Բազմանդամների ավագ անդամների հետ կապված խնդիրներից խուսափելու համար հարմար է ալգորիթմի սկզբում մտապահել $f(x)$ բազմանդամի a_0 ավագ գործակիցը, ապա անցնել նորմավորված բազմանդամների եւ ալգորիթմի վերջում a_0-ն վերադարձնել ստացված արտադրիչներից որեւէ մեկին, օրինակ, առաջինին:

Կառուցեցինք հետեւյալ ալգորիթմը.

4.5.2 Ալգորիթմ (քառակուսիներից ազատ արտադրիչների վերլուծումը վերջավոր դաշտի վրա տրված բազմանդամային օղակում): Տրված է $f(x) \in K[x]$ բազմանդամը, որտեղ K-ն վերջավոր դաշտ է: Վերլուծել այն քառակուսիներից ազատ արտադրիչների:

1. a_0-ով նշանակենք $f(x)$ բազմանդամի ավագ գործակիցը:

2. Նշանակենք $f(x) = \frac{1}{a_0} f(x)$ նորմավորված բազմանդամը:

3. Նշանակենք $p = \mathrm{char}(K)$ պարզ բնութագրիչը:

4. Սահմանենք բազմանդամների $\mathcal{S}$ դատարկ ցանկը:

5. $f(x)$-ը ներկայացնենք $f(x) = x^n + a_1 x^{n-1} + \cdots + a_i x^{n-i} + \cdots + a_n$ տեսքով, որտեղ $n = \deg f(x)$:

6. Նշանակենք $s = 1$:

7. Գտնենք այն մեծագույն ամբողջ c-ն, որի համար բոլոր ոչ զրոյական $a_i x^{n-i}$ միանդամների աստիճանացույցերը բաժանվում են p^c-ի վրա՝ $(n-i) \vdots p^c$, երբ $a_i \neq 0$, $i = 1, \ldots, n$:

8. Եթե $c > 0$

9. նշանակենք $p^m = |K|$;

10. Էվկլիդեսի ընդհանրացված ալգորիթմով գտնենք այն u, v ամբողջ թվերը, որոնց համար $up^c + v(p^m - 1) = 1$;

11. նշանակենք $s = s \cdot p^c$;

12. անցնենք $f(x) = x^n + a_1^u x^{(n-1)/p^c} + \cdots + a_i^u x^{(n-i)/p^c} + \cdots + a_n^u$ բազմանդամին:

13. Հաշվենք $f'(x)$ ածանցյալը:

14. $K[x]$ օղակում Էվկլիդեսի ալգորիթմով հաշվենք $\big(f(x), f'(x)\big)$ ամենամեծ ընդհանուր բաժանարարը:

15. Նշանակենք $g(x) = \frac{f(x)}{(f(x), f'(x))}$:

16. Նորմավորենք $g(x)$ բազմանդամը:

17. $\mathcal{S}$ ցանկին s անգամ ավելացնենք $g(x)$ բազմանդամը:

18. Նշանակենք $f(x) = \frac{f(x)}{g(x)}$:

19. Եթե $f(x) = 1$

20. անցնենք 23-րդ քայլին;

21. հակառակ դեպքում

22. վերադառնանք 7-րդ քայլին:

23. $\mathcal{S}$ ցանկի բազմանդամներից որեւէ մեկը, օրինակ առաջին $g(x)$ բազմանդամը, փոխարինենք $g(x) = a_0 \cdot g(x)$ բազմանդամով:

24. Դուրս գրենք $\mathcal{S}$ ցանկի բազմանդամները՝ որոնելի քառակուսիներից ազատ արտադրիչները:

4.5.3 Դիտողություն. Համեմատելով այս ալգորիթմը նախորդ պարագրաֆի կառուցումների հետ՝ նկատում ենք, որ վերջավոր դաշտի դեպքում մենք մի էական առավելություն ունենք. եթե $R = \mathbb{Z}_p$, ապա R-ը արդեն իսկ դաշտ է, իսկ $R[x]$ օղակն արդեն իսկ Էվկլիդյան է: Ուստի 4.5.2 ալգորիթմը կարող է կառուցել բազմանդամի ներկայացումը քառակուսիներից ազատ արտադրիչների սկզբնական $R = \mathbb{Z}_p$ օղակի վրա՝ առանց այն մինչեւ մի նոր դաշտ ընդլայնելու անհրաժեշտության:

4.5.4 Օրինակ. Վերցնենք $f(x) = x^6 + x^5 + x + 1 \in \mathbb{Z}_5[x]$ եւ քառակուսիներից ազատ արտադրիչների վերլուծենք այն՝ ըստ վերեւում բերված քայլերի: Քանի որ

$f'(x) = x^5 + 1 \neq 0$, ապա $\big(f(x), f'(x)\big) = x^5 + 1$: Այստեղ ամենամեծ ընդհանուր բաժանարարը հաշվել ենք ըստ Էվկլիդեսի ալգորիթմի.

$$\begin{array}{r|l} x^6 + x^5 + x + 1 & x^5 + 1 \\ \cline{2-2} x^6 + x & x + 1 \\ \cline{1-1} x^5 + 1 & \\ x^5 + 1 & \\ \cline{1-1} 0 & \end{array}$$

Ուրեմն, որպես քառակուսիներից ազատ առաջին արտադրիչ ստանում ենք.

$$g_1(x) = \frac{f(x)}{\big(f(x), f'(x)\big)} = \frac{x^6 + x^5 + x + 1}{x^5 + 1} = x + 1:$$

Փոխարինենք մեր $f(x)$ բազմանդամը՝

$$f(x) = f(x)/g_1(x) = x^5 + 1:$$

Այս անգամ գործ ունենք ավելի բարդ դեպքի հետ, քանի որ

$$(x^5 + 1)' = 0 + 0 = 0 \in \mathbb{Z}_5[x]:$$

Այս դեպքում $p^c = 5^1$ եւ $m = |\mathbb{Z}_5| = 5$, իսկ $\mathbb{Z}_5^* = \langle 1 \rangle$ ցիկլիկ խմբի կարգն է $m - 1 = 4$: Միանգամից երեւում է, որ որպես u թիվ, որի համար $\mathbb{Z}_5^*$-ում տեղի ունի $a^{u \cdot p^c} = a$ պայմանը, կարելի է վերցնել $u = 1$, քանի որ $a^{1 \cdot 5} = a^{4+1} = 1 \cdot a = a$: Իսկ ընդհանուր դեպքում u-ն կարելի էր հաշվել Էվկլիդեսի ընդհանրացված ալգորիթմով $up^c + v(p^m - 1) = 1$ պայմանից, որը մեր դեպքում ունի

$$u5^1 + v(5^1 - 1) = u5 + v4 = 1$$

տեսքը: Ուստի օժանդակ $\Phi(x)$ բազմանդամը (4.13) բանաձեւով կառուցվում է հետեւյալ կերպ.

$$\Phi(x) = x^{5/5} + 1 = x + 1:$$

Իսկ (4.14) վերլուծությունը ընդունում է հետեւյալ տեսքը.

$$x^5 + 1 = (x + 1)^{p^c} = (x + 1)^{5^1} = (x + 1)^5:$$

Ստանում ենք վերլուծություն քառակուսիներից ազատ հինգ արտադրիչների, որոնցից յուրաքանչյուրն է $x + 1$: Հաշվի առնելով ավելի վաղ ստացված $g_1(x) = x + 1$ արտադրիչը՝ ստանում ենք.

$$f(x) = x^6 + x^5 + x + 1 = (x + 1)^6:$$

4.5.5 Խնդիր. $\mathbb{Z}_3[x]$ օղակում քառակուսիներից ազատ արտադրիչների վերլուծել

$$f(x) = x^{19} + 2x^{18} + x^4 + 2x^3 + 2x + 1$$

բազմանդամը: *Յուցում.* հաշվի առնել, որ $x^{18} + x^3 + 2$ բազմանդամի ածանցյալը $\mathbb{Z}_3[x]$ օղակում զրոյական է:

4.5.6 Դիտողություն. 4.5.2 ալգորիթմը թույլ է տալիս $f(x)$ բազմանդամը քառակուսիներից ազատ արտադրյալների վերլուծել ըստ ցանկացած p մոդուլի: Ընդ որում, ալգորիթմի ընթացքը ավելի բարդ կամ ավելի պարզ քայլեր է պահանջում՝ կախված այն բանից, թե $f(x)$-ի միանդամների աստիճանացույցերը բաժանվո՞ւմ են, թե՞ չեն բաժանվում p պարզ թվի վրա (ընդ որում, որքան ավելի շատ են p-ի վրա բաժանվող աստիճանացույցերը, այնքան ավելի է բարդանում ալգորիթմը): Ավելի վաղ արդեն հանդիպել են այնպիսի ալգորիթմներ, որտեղ մենք ինչ-որ խնդիր լուծելու համար, նախ, ընտրել ենք «հարմար» p պարզ թիվ, եւ հետագա գործողությունները կատարել ըստ այդ մոդուլի: Հետագա գլուխներում եւս մեզ հանդիպելու են նման խնդիրներ: Այդ առումով 4.5.2 ալգորիթմը երբեմն կարելի է կիրառել այնպես, որ քառակուսիներից ազատ արտադրյալների վերլուծման ընթացքում խուսափենք ամենաբարդ դեպքերից: Օրինակ, եթե խնդիրը թույլ է տալիս տրված $f(x)$ բազմանդամի համար նախապես ընտրել p պարզ մոդուլը (տես, օրինակ, 7.4 պարագրաֆը), ապա ընտրենք այն ավելի մեծ, քան $\deg f(x)$ աստիճանը: Այդ դեպքում p-ն մեծ կլինի նաեւ

$$\deg f'(x) \quad \text{եւ} \quad \deg\big(f(x), f'(x)\big)$$

աստիճաններից: Այսինքն՝ (4.7) եւ (4.8) արտահայտությունների մեջ այլեւս չեն լինի ածանցումներից հետո առաջացած եւ p-ի վրա բաժանվող գործակիցներ, եւ մենք երբեք չենք անցնի 4.5.2 ալգորիթմի 8-12 քայլերով:

Եթե նախորդ պարագրաֆում մենք քննարկեցինք 0 բնութագրիչի բոլոր դաշտերը, ապա այս պարագրաֆում կարողացանք դիտարկել p բնութագրիչի միայն վերջավոր դաշտերի դեպքը: K դաշտի վերջավոր լինելը մեզ պետք եկավ այն քայլում, որտեղ հաշվեցինք u արժեքը՝ օգտագործելով K վերջավոր դաշտի $p^m = |K|$ հզորությունը: Քանի որ u արժեքը մեր ապացույցներում միայն օժանդակ դեր էր կատարում, կարող է թվալ, որ մեր ալգորիթմը (որի հիմնական գործիքը $\big(f(x), f'(x)\big)$ ամենամեծ ընդհանուր բաժանարարն է) հնարավոր է ձեւափոխել այն-

պես, որ այն ծածկի p բնութագրիչի բոլոր դաշտերի դեպքը: Սակայն կան օրինակներ, որոնք ցույց են տալիս, որ $f'(x)$ ածանցյալ բազմանդամը կարող է այդ նպատակի համար բավարար ինֆորմացիա չպարունակել, եթե K դաշտը անվերջ է:

4.5.7 Օրինակ. Վերցնենք $K = \mathbb{Z}_2(y)$ ռացիոնալ ֆունկցիաների դաշտը (տես 4.2.6 օրինակը): K-ի տարրերը կոտորակային ֆունկցիաներ են, որոնց համարիչը եւ հայտարարը $\mathbb{Z}_2$-ից վերցված գործակիցներով y փոփոխականի բազմանդամներ են (հայտարարի բազմանդամը ոչ զրոյական է): Դիտարկենք $K[x]$ բազմանդամային օղակի

$$f(x) = yx^2 + 1$$

բազմանդամը, որի փոփոխականը x-ն է, իսկ y-ը ավագ գործակիցն է K դաշտից: Մի կողմից,

$$f'(x) = y2x^{2-1} + 0 = 0$$

եւ, ուրեմն, $\big(f(x), f'(x)\big) = f(x)$: Այսինքն՝ $f'(x)$ ածանցյալը մեր ալգորիթմի համար ինֆորմացիա չի պարունակում:

Մյուս կողմից, կարելի է տեսնել, որ $f(x)$ բազմանդամը պարզ է: Ենթադրենք հակառակը. այն ունի ներկայացում գծային արտադրիչների արտադրյալի տեսքով.

$$f(x) = \big(g_1(y)x + h_1(y)\big)\big(g_2(y)x + h_2(y)\big),$$

որտեղ $g_1(y), g_2(y), h_1(y), h_2(y) \in K$: Քանի որ $g_1(y)g_2(y) = y$ եւ $h_1(y)h_2(y) = 1$, ապա համարենք, որ $g_2(y) = yg_1^{-1}(y)$ եւ $h_2(y) = h_1^{-1}(y)$: Այսինքն՝

$$\begin{aligned} f(x) &= \big(g_1(y)x + h_1(y)\big)\big(yg_1^{-1}(y)x + h_1^{-1}(y)\big) \\ &= g_1(y)yg_1^{-1}(y)x^2 + h_1(y)h_1^{-1}(y) + h_1(y)\cdot yg_1^{-1}(y)x + g_1(y)x\cdot h_1^{-1}(y) \\ &= yx^2 + 1 + x[h_1(y)\cdot yg_1^{-1}(y) + g_1(y)\cdot h_1^{-1}(y)]: \end{aligned}$$

Ուրեմն՝

$$\begin{aligned} &h_1(y)y\cdot g_1^{-1}(y) + g_1(y)\cdot h_1^{-1}(y) \\ &= y\frac{h_1(y)}{g_1(y)} + \frac{g_1(y)}{h_1(y)} = \frac{yh_1^2(y) + g_1^2(y)}{g_1(y)h_1(y)} = 0: \end{aligned}$$

Բայց սա հնարավոր է միայն, երբ $yh_1^2(y) = -g_1^2(y)$: Իսկ սա տեղի չունի: Նախ նկատենք, որ $\mathbb{Z}_2$ դաշտի վրա $-g_1^2(y) = g_1^2(y)$: Ինչպիսին էլ լինեն $g_1(y)$ ռացիոնալ ֆունկցիայի համարիչն ու հայտարարը, $g_1^2(y)$ ֆունկցիայի համարիչի եւ հայտարարի աստիճանները երկուսն էլ զույգ են: Նույնը վերաբերում է $h_1(y)$ ռացիոնալ

ֆունկցիային: Բայց $yh_1^2(y)$ ռացիոնալ ֆունկցիայի համարիչի աստիճանը կենտ է, ուստի $yh_1^2(y) = g_1^2(y)$ հավասարությունն անհնար է:

4.5.7 օրինակն, իհարկե, չի նշանակում, թե $K[x]$ բազմանդամային օղակում $f(x)$ բազմանդամը չի վերլուծվում քառակուսիներից ազատ արտադրիչների արտադրյալի: Ինչպես նշեցինք 4.3 պարագրաֆում, յուրաքանչյուր ֆակտորիալ օղակում ամեն մի տարր ունի ներկայացում պարզ արտադրիչների արտադրյալի տեսքով, որտեղից եւ հեշտ է ստանալ ներկայացումը քառակուսիներից ազատ արտադրիչների արտադրյալի տեսքով: Մասնավորապես, քանի որ $K = \mathbb{Z}_2(x)$ օղակը դաշտ է, ապա $K[x]$ օղակը ֆակտորիալ օղակ է, եւ $f(x)$ բազմանդամն ունի որոնելի վերլուծությունը, որը, սակայն, հնարավոր չէ հաշվել $f'(x)$ ածանցյալի միջոցով:

5 Մոդուլյար անցումներ ըստ մի քանի մոդուլների

5.1 Մնացքների մասին չինական թեորեմը օղակներում

Մինչ այժմ մեր քննարկած ալգորիթմներում յուրաքանչյուր մոդուլյար անցում տեղի էր ունենում ըստ մեկ որոշակի մոդուլի, որը կարող էր լինել որեւէ պարզ թիվ, չբերվող բազմանդամ կամ օղակի գլխավոր իդեալ: Երբեմն մենք կարող էինք փոփոխել այդ մոդուլը՝ ալգորիթմի համար ավելի գերադասելի պայմաններ ստանալու համար, բայց յուրաքանչյուր մոդուլյար անցում կատարվում էր միայն մեկ ֆիքսված մոդուլով: Այս գլխում մենք կծանոթանանք այնպիսի մեթոդների, որտեղ տրված խնդրի լուծման համար մոդուլյար անցումներ են տեղի ունենում ըստ մի քանի մոդուլների. ըստ յուրաքանչյուր մոդուլի ստացվում է մասնակի պատասխան, եւ հետո այդպիսի մասնակի պատասխանների հիման վրա կառուցվում է խնդրի վերջնական պատասխանը: Այսպիսի մեթոդների պատմական հիմքը համարվում է մնացքների մասին չինական թեորեմը, որը ծագել է հետեւյալ բնույթի խնդրից. «Քանի՞ զինվոր կա ջոկատում, եթե ջոկատը երեք սյան բաժանվելիս երկու զինվոր է ազատ մնում, հինգ սյան բաժանվելիս երեք զինվոր է ազատ մնում, իսկ յոթ սյան բաժանվելիս դարձյալ երկու զինվոր է ազատ մնում»:

Ստորեւ մենք նախ ապացուցելու ենք մնացքների մասին չինական թեորեմն Էվկլիդյան օղակների համար, այնուհետեւ 5.2 եւ 5.3 պարագրաֆներում ստանալու ենք դրա կիրառություններ՝ ըստ մի քանի մոդուլների մոդուլյար անցումներ են կատարվելու որոշիչների հաշվման եւ բազմանդամային հաշվարկների համար: Չինական թեորեմի եւս մի կարեւոր կիրառության հետ մենք հետագայում ծանոթանալու ենք 7.3 պարագրաֆում, որտեղ միաժամանակյա մոդուլյար անցումները կօգտագործենք բազմանդամների ֆակտորիզացիայի նպատակով:

Մնացքների մասին չինական թեորեմի զանազան տարբերակներ տեղի ունեն կամայական օղակների, կոմուտատիվ օղակների, կամ Էվկլիդյան օղակների համար (իսկ ավելի ընդհանուր հանրահաշվական համակարգերում՝ խմբերում, չինական թեորեմի նախատիպը հայտնի է որպես Ռեմակի թեորեմը): Սակայն մենք, հե-

տեւելով ալգորիթմական հանրահաշվի հիմնական մենագրությունների եւ դասագրքերի օրինակին, տալիս ենք այս թեորեմը էվկլիդյան օղակների համար: Դրա պատճառն այն է, որ Էվկլիդյան օղակներում հնարավորություն ունենք ալգորիթմորեն հաշվել բոլոր այն արժեքները, որոնց գոյությունը պնդվում է մնացքների մասին չինական թեորեմում: Մինչդեռ ավելի ընդհանուր օղակների համար դա կարող է ալգորիթմորեն անլուծելի խնդիր լինել: Սկսենք ամբողջ թվերի համար մնացքների մասին չինական թեորեմի տեսքից (բերենք առանց ապացույցի, քանի որ այն հետագա ավելի ընդհանուր թեորեմի հետեւանք է).

5.1.1 Թեորեմ (մնացքների մասին չինական թեորեմը ամբողջ թվերի համար). *Ենթադրենք $m_1, \dots, m_k \in \mathbb{Z}$ թվերը զույգ առ զույգ փոխադարձաբար պարզ են՝ $(m_i, m_j) = 1$ կամայական $i, j = 1, \dots, k;\ \ i \neq j$ համար: Այդ դեպքում կամայական $s_1, \dots, s_k \in \mathbb{Z}$ թվերի համար գոյություն ունի $n \in \mathbb{Z}$ թիվ այնպիսին, որ.*

$$\begin{aligned} n &\equiv s_1 (\mathrm{mod}\, m_1), \\ &\dots\dots\dots\dots\dots \\ n &\equiv s_k (\mathrm{mod}\, m_k), \end{aligned} \tag{5.1}$$

ընդ որում, եթե որեւէ t թիվ նույնպես բավարարում է այս համակարգին, ապա

$$t \equiv n (\mathrm{mod}\, m),$$

որտեղ $m = m_1 \cdots m_k$:

Թեորեմի երկրորդ պայմանը նշանակում է, որ n թիվը (5.1) համակարգին բավարարող թվերի մեջ որոշիչ է այն իմաստով, որ եթե մի այլ t թիվ նույնպես բավարարում է համակարգին, ապա t-ն ունի $t = mi + n$ տեսքը որեւէ i ամբողջ թվի համար:

Եթե սահմանափակվենք միայն այն դեպքով, երբ $s_i < m_i$ $(i = 1, \dots, k)$, ապա (5.1) համակարգը կարելի է ձեւակերպել այսպես. գոյություն ունի $n \in \mathbb{Z}$ թիվ, որը m_i-ի վրա բաժանելիս ստացվում է s_i մնացորդ $(i = 1, \dots, k)$: Հասկանալի է, որ վերը նշված սահմանափակումը չի փոխում թեորեմի ընդհանրությունը, քանի որ, եթե, ասենք, $s_1 \geq m_1$, ապա s_1-ը կարելի է մնացորդով բաժանել m_1-ի վրա: Ստացված s_1' մնացորդի համար ունենք $s_1' \equiv s_1 (\mathrm{mod}\, m_1)$, այսինքն, $n \equiv s_1 (\mathrm{mod}\, m_1)$ այն եւ միայն այն դեպքում, երբ $n \equiv s_1' (\mathrm{mod}\, m_1)$, ընդ որում, $s_1' < m_1$:

Այժմ, ենթադրենք, R-ը էվկլիդյան օղակ է, եւ նրա մեջ տրված են $m_1, \dots, m_k \in R$ զույգ առ զույգ փոխադարձաբար պարզ տարրերը: Վերցնենք R-ի

$$I_1 = m_1 R, \dots, I_k = m_k R$$

իդեալները: Դրանց համապատասխան կարելի է կառուցել բնական հոմոմորֆիզմներ (տես 2.3.13 թեորեմին հաջորդող կառուցումները եւ բնական հոմոմորֆիզմի սահմանումը).

$$\begin{aligned} &\pi_1\colon R \to R/I_1, \quad \pi_1(a) = a + I_1, \ \ a \in R, \\ &\qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ &\pi_k\colon R \to R/I_k, \quad \pi_k(a) = a + I_k, \ \ a \in R\colon \end{aligned} \tag{5.2}$$

Կառուցենք մի նոր χ հոմոմորֆիզմ R օղակից R/I_i ֆակտոր-օղակների ուղիղ արտադրյալի մեջ՝

$$\chi\colon R \to R/I_1 \times \cdots \times R/I_k,$$

որտեղ $a \in R$ տարրի համար սահմանվում է՝

$$\chi(a) = \big(\pi_1(a), \ldots, \pi_k(a)\big) = (a + I_1, \ldots, a + I_k)\colon \tag{5.3}$$

5.1.2 Լեմմա. *χ-ը այուրյեկտիվ հոմոմորֆիզմ է, ընդ որում,* $\ker\chi = mR$, *որտեղ* $m = m_1 \cdots m_k$:

Ապացույց: Այն, որ χ-ն հոմոմորֆիզմ է, հեշտ է ստանալ՝ ստուգելով հոմոմորֆիզմի 2.3.1 սահմանման կետերը (5.3) արտապատկերման համար:

Որեւէ $a \in R$ տարր պատկանում է $\ker\chi$ միջուկին այն եւ միայն այն դեպքում, երբ

$$\chi(a) = 0_{R/I_1 \times \cdots \times R/I_k} = (0 + I_1, \ldots, 0 + I_k)\colon$$

Բայց, ըստ (5.3) սահմանման, սա հնարավոր է այն եւ միայն այն դեպքում, երբ

$$a + I_i = 0 + I_i$$

կամայական $i = 1, \ldots, k$ համար: Իսկ դա համարժեք է

$$a \in I_i, \ \ i = 1, \ldots, k$$

պայմանին: $a \in I_i = m_i R$ պայմանը պարզապես նշանակում է, որ $a \vdots m_i$: Եթե a տարրը բաժանվում է բոլոր $m_1, \ldots, m_k$ տարրերի վրա, ապա այն բաժանվում է նաեւ դրանց ամենափոքր ընդհանուր բազմապատիկի վրա: Եւ քանի որ դրանք բոլորը զույգ առ զույգ փոխադարձաբար պարզ են, ապա այդ ամենափոքր ընդհանուր բազմապատիկը $m = m_1 \cdots m_k$ արտադրյալն է: Ուստի՝

$$a \in mR = \ker\chi\colon$$

Սյուրյեկտիվության ապացույցի համար նախ ապացուցենք, որ յուրաքանչյուր

$$e_i = (0 + I_1, \dots, 1 + I_i, \dots, 0 + I_k)$$

տեսքի տարր (բոլոր կոորդինատները զրոյական են, բացի i-րդ կոորդինատից) ունի որեւէ $l_i = \chi^{-1}(e_i)$ նախապատկեր R-ում ($i = 1, \dots, k$): Ըստ 2.5.5 թեորեմի, գոյություն ունեն $u, v \in R$ տարրեր այնպիսիք, որ

$$u\frac{m}{m_i} + vm_i = \left(\frac{m}{m_i}, m_i\right) = 1:$$

Նշանակելով $l_i = u\frac{m}{m_i}$, կունենանք $l_i = (-v)m_i + 1$, այսինքն՝ $l_i \equiv 1 (\mathrm{mod}\, m_i)$ եւ

$$\pi_i(l_i) = 1 + I_i:$$

Մյուս կողմից, ակնհայտորեն $\pi_j(l_i) = 0 + I_i$, եթե $j \neq i$, քանի որ $l_i = u\frac{m}{m_i} \vdots m_j$: Ուրեմն՝ $\chi(l_i) = e_i$:

e_i տեսքի տարրերի l_i նախապատկերների գոյությունից բխում է $R/I_1 \times \cdots \times R/I_k$ ուղիղ արտադրյալի բոլոր տարրերի նախապատկերների գոյությունը: Դիտարկենք

$$f_i = (0 + I_1, \dots, a_i + I_i, \dots, 0 + I_k)$$

տեսքի կամայական տարր: Հեշտ է տեսնել, որ սրա նախապատկերն է $a_i l_i$ տարրը, քանի որ

$$\pi_i(a_i l_i) = \pi_i(a_i)\pi_i(l_i) = (a_i + I_i)(1 + I_i) = a_i + I_i$$

եւ

$$\pi_j(a_i l_i) = \pi_j(a_i)\pi_j(l_i) = \pi_j(a_i)(0 + I_i) = 0 + I_i,$$

եթե $j \neq i$: Նկատենք, որ$R/I_1 \times \cdots \times R/I_k$ ուղիղ արտադրյալի յուրաքանչյուր տարր իրենից ներկայացնում է f_i տեսքի k հատ գումարելիների $f_1 + \cdots + f_k$ գումար: ■

Ապացուցված լեմմից եւ օղակների հոմոմորֆիզմների մասին 2.3.13 հիմնական թեորեմի՝ χ սյուրյեկտիվ հոմոմորֆիզմի վրա կիրառումից անմիջապես ստացվում է.

5.1.3 Թեորեմ (մնացքների մասին չինական թեորեմը էվկլիդյան օղակների համար). *Ենթադրենք R-ը էվկլիդյան օղակ է, եւ նրա մեջ տրված են $m_1, \dots, m_k \in R$ զույգ առ զույգ փոխադարձաբար պարզ տարրերը: Այդ դեպքում տեղի ունի հետեւյալ օղակային հոմոմորֆիզմը*

$$R/mR \cong R/m_1R \times \cdots \times R/m_kR, \tag{5.4}$$

որտեղ $m = m_1 \cdots m_k$:

Ստացված (5.4) արտահայտությունը շատ քիչ է նմանվում մնացքների մասին չինական թեորեմի ավանդական տեսքին (տես 5.1.1 թեորեմը): Դրանց կապն ավելի համոզիչ դարձնելու համար (5.4) առնչությունից դուրս բերենք 5.1.1 թեորեմը: 5.1.1 թեորեմի պայմաններում $m_1, \dots, m_k \in \mathbb{Z}$ թվերին համապատասխանող I_i իդեալներն են՝ $I_i = m_i\mathbb{Z}$ (տես 2.1.24 վարժությունը): Ուստի $\mathbb{Z}/I_i = \mathbb{Z}/m_i\mathbb{Z} \cong \mathbb{Z}_{m_i}$ եւ (5.4) արտահայտությունն ընդունում է

$$\mathbb{Z}_m \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k} \tag{5.5}$$

տեսքը, որը կարելի է մեկնաբանել որպես $(s_1, \dots, s_k) \in \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$ վեկտորին մի $n \in \mathbb{Z}_m$ թվի համապատասխանեցում:

5.1.4 Վարժություն. Այս պարագրաֆի սկզբում հիշատակված զինվորների ջոկատի մասին չինական խնդիրը վերաձեւակերպել ամբողջ թվերի համար մնացքների մասին չինական թեորեմի տեսքով (5.1.1 թեորեմը): Նույն խնդիրը վերաձեւակերպել էվկլիդյան օղակների համար մնացքների մասին չինական թեորեմի տեսքով (5.1.3 թեորեմը):

Քանի որ $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p$ օղակները դաշտեր են եւ, ըստ 2.5.13 թեորեմի, համապատասխան $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$, $\mathbb{Z}_p[x]$ բազմանդամային օղակներն էվկլիդյան են: Մենք հիմա կարող ենք բազմանդամների համար մնացքների մասին չինական թեորեմը դուրս բերել միանգամից մեր քննարկած բոլոր տիպերի բազմանդամների համար՝ ռացիոնալ, իրական, կոմպլեքս եւ մոդուլյար դաշտերի վրա:

5.1.5 Թեորեմ (մնացքների մասին չինական թեորեմը բազմանդամների համար). *Ենթադրենք R դաշտի վրա սահմանված $R[x]$ բազմանդամային օղակում տրված $m_1(x), \dots, m_k(x) \in R[x]$ բազմանդամները զույգ առ զույգ փոխադարձաբար պարզ են՝ $(m_i(x), m_j(x)) = 1$ կամայական $i, j = 1, \dots, k$; $i \neq j$ համար: Այդ դեպքում կամայական $s_1(x), \dots s_k(x) \in R[x]$ բազմանդամների համար գոյություն ունի $f(x) \in R[x]$ բազմանդամ այնպիսին, որ.*

$$\begin{aligned} f(x) &\equiv s_1(x) \big(\mathrm{mod}\, m_1(x)\big), \\ &\dots\dots\dots\dots\dots\dots\dots\dots \\ f(x) &\equiv s_k(x) \big(\mathrm{mod}\, m_k(x)\big), \end{aligned} \tag{5.6}$$

ընդ որում, եթե որեւէ $h(x) \in R[x]$ բազմանդամ նույնպես բավարարում է այս համակարգին, ապա

$$h(x) \equiv f(x) \big(\mathrm{mod}\, m(x)\big),$$

որտեղ $m(x) = m_1(x) \cdots m_k(x)$:

Բազմանդամների վրա մնացքների մասին չինական թեորեմը մեզ հանդիպելու է 5.2, 5.3 պարագրաֆներում եւ 7րդ գլխի 7.3 պարագրաֆում:

5.1.6 Վարժություն. Ձեւակերպել 5.1.5 թեորեմը $\mathbb{Z}_p$ դաշտի վրա տրված մոդուլյար բազմանդամների համար:

5.1.3 թեորեմի ապացույցը կարեւոր է նաեւ իր ալգորիթմական արժեքի շնորհիվ. այն հնարավորություն է տալիս հաշվելու (5.1) համակարգին բավարարող n տարրը:

Ալգորիթմների տեսքով ձեւակերպենք մնացքների մասին չինական թեորեմի առավել հաճախ կիրառվող դեպքերը:

5.1.7 Ալգորիթմ (մնացքների մասին չինական ալգորիթմը ամբողջ թվերի համար). $\mathbb{Z}$ օղակում տրված են զույգ առ զույգ փոխադարձաբար պարզ $m_1, \dots, m_k$ թվերը: Կամայական $s_1, \dots, s_k \in \mathbb{Z}$ թվերի համար գտնել 5.1.1 մնացքների մասին չինական թեորեմի պայմաններին բավարարող n թիվը:

1. Նշանակենք $m = m_1 \cdots m_k$:

2. ($i = 1;\ i \le k;\ i++$) արժեքների համար

3. m_i եւ $\frac{m}{m_i}$ փոխադարձաբար պարզ թվերի համար Էվկլիդեսի ընդհանրացված ալգորիթմով գտնենք այնպիսի $u_i, v_i \in \mathbb{Z}$ թվեր, որոնց համար $u_i \frac{m}{m_i} + v_i m_i = 1$;

4. նշանակենք $l_i = u_i \frac{m}{m_i}$:

5. Նշանակենք $l = \sum_{i=1}^{k} s_i \cdot l_i$:

6. $\mathbb{Z}$ Էվկլիդյան օղակում l-ը մնացորդով բաժանենք m-ի վրա՝ $l = qm + n$, որտեղ $n = 0$ կամ $n \ne 0$ եւ $|n| < |l|$:

7. Դուրս գրենք n մնացորդը:

5.1.8 Օրինակ. Որպես նման կիրառության մի օրինակ ցույց տանք, թե ինչպես կարելի է 5.1.1 թեորեմի պայմաններում գտնել այն n թիվը, որը կբավարարի հետեւյալ համակարգին՝

$$\begin{aligned} n &\equiv 2 \pmod{11}, \\ n &\equiv 7 \pmod{13}, \end{aligned} \tag{5.7}$$

եւ կպատկանի $\mathbb{Z}_{11\cdot 13} = \mathbb{Z}_{143}$ օղակին: Այստեղ ունենք $k = 2$ եւ $m = 11 \cdot 13 = 143$: Նախ, ըստ 2.5.5 թեորեմի, գոյություն ունեն $u_1, v_1 \in \mathbb{Z}$ տարրեր այնպիսիք, որ

$$u_1 \frac{m}{m_1} + v_1 m_1 = u_1 \frac{143}{11} + v_1 11 = u_1 13 + v_1 11 = 1:$$

u_1, v_1 արժեքները հաշվվում են՝ ըստ 2.5.5 թեորեմի ապացույցում բերված Էվկլիդեսի ընդլայնված ալգորիթմի՝

$$6 \cdot 13 + (-7) \cdot 11 = 1:$$

Ուրեմն՝

$$l_1 = u_1 \frac{m}{m_1} = 6 \cdot 13 = 78:$$

Գոյություն ունեն նաեւ $u_2, v_2 \in \mathbb{Z}$ տարրեր այնպիսիք, որ

$$u_2 \frac{m}{m_2} + v_2 m_2 = u_2 \frac{143}{13} + v_2 13 = u_2 11 + v_2 13 = 1,$$

այսինքն՝

$$(-7) \cdot 11 + 6 \cdot 13 = 1,$$

եւ

$$l_2 = u_2 \frac{m}{m_2} = (-7) \cdot 11 = -77:$$

Նշված l_1 եւ l_2 թվերը 2.5.5 թեորեմի ապացույցում հիշատակված այն նախապատկերներն են, որոնց համար

$$l_1 \equiv 1 (\mathrm{mod}\ 11), \qquad l_2 \equiv 0 (\mathrm{mod}\ 11),$$
$$l_1 \equiv 0 (\mathrm{mod}\ 13); \qquad l_2 \equiv 1 (\mathrm{mod}\ 13):$$

Մնում է այս օժանդակ թվերը բազմապատկել s_1, s_2 գործակիցներով եւ որոնելի $n = 46$ թիվը ստանալ որպես գծային կոմբինացիայի բաղդատում ըստ $m = m_1 m_2 = 143$ մոդուլի՝

$$s_1 l_1 + s_2 l_2 = 2 \cdot 78 + 7 \cdot (-77) = -383 \equiv 46 (\mathrm{mod}\ 143):$$

Ստացված պատասխանն իրոք բավարարում է (5.7) համակարգին՝

$$46 = 4 \cdot 11 + 2 = 3 \cdot 13 + 7:$$

Նկատենք, (5.7) համակարգին բավարարում է նաեւ -383 թիվը, սակայն մենք պարտավոր ենք կատարել վերջին մոդուլյար անցումը, որպեսզի ստանանք $n \in \mathbb{Z}_m = \mathbb{Z}_{143}$ արժեքը: Առանց դրա մենք չէինք ունենա 5.1.1 թեորեմի երկրորդ պնդումը:

5.1.9 Վարժություն. Գտնել այն n թիվը, որը բավարարում է

$$n \equiv 1 (\mathrm{mod}\ 3),$$
$$n \equiv 3 (\mathrm{mod}\ 7),$$
$$n \equiv 5 (\mathrm{mod}\ 8)$$

համակարգին եւ պատկանում է $\mathbb{Z}_{168}$ օղակին: *Յուցում.* Էվկլիդեսի ընդլայնված ալգորիթմով գտնել այնպիսի $u_i, v_i \in \mathbb{Z}; i = 1, 2, 3$ թվեր, որոնց համար

$$u_1 \frac{168}{3} + v_1 3 = 1,$$
$$u_2 \frac{168}{7} + v_2 7 = 1,$$
$$u_3 \frac{168}{8} + v_3 8 = 1,$$

եւ նշանակել՝ $l_1 = u_1 \frac{168}{3},\ l_2 = u_2 \frac{168}{7},\ l_3 = u_3 \frac{168}{8}$:

5.1.10 Վարժություն. Գտնել այն թվերը, որոնք բավարարում են 5.1.4 վարժության պայմաններին, այսինքն՝ ջոկատի զինվորների հնարավոր քանակությունները:

5.1.11 Ալգորիթմ (մնացքների մասին չինական ալգորիթմը բազմանդամների համար). R դաշտի վրա սահմանված $R[x]$ բազմանդամային օղակում տրված են $m_1(x), \dots, m_k(x)$ զույգ առ զույգ փոխադարձաբար պարզ բազմանդամները: Կամայական $s_1(x), \dots s_k(x) \in R[x]$ բազմանդամների համար գտնել 5.1.5 մնացքների մասին չինական թեորեմի պայմաններին բավարարող $f(x)$ բազմանդամը:

1. Նշանակենք $m(x) = m_1(x) \cdots m_k(x)$:

2. ($i = 1;\ i \le k;\ i++$) արժեքների համար

3. $m_i(x)$ եւ $m(x)/m_i(x)$ փոխադարձաբար պարզ բազմանդամների համար Էվկլիդեսի ընդհանրացված ալգորիթմով գտնենք այնպիսի $u_i(x), v_i(x) \in R[x]$ բազմանդամներ, որոնց համար $u_i(x)\frac{m(x)}{m_i(x)} + v_i(x)m_i(x) = 1$;

4. նշանակենք $l_i(x) = u_i(x)\frac{m(x)}{m_i(x)}$:

5. Նշանակենք $l(x) = \sum_{i=1}^{k} s_i(x) \cdot l_i(x)$:

6. $R[x]$ Էվկլիդյան օղակում $l(x)$-ը մնացորդով բաժանենք $m(x)$-ի վրա՝ $l(x) = q(x)m(x) + f(x)$, որտեղ $f(x) = 0$ կամ $f(x) \neq 0$ եւ $|f(x)| < |l(x)|$:

7. Դուրս գրենք $f(x)$ մնացորդը:

5.1.12 Օրինակ. Գտնենք այն $f(x) \in \mathbb{R}[x]$ իրական բազմանդամը, որը բավարարում է

$$f(x) \equiv 1 (\mathrm{mod}\ x - 1),$$
$$f(x) \equiv 3 (\mathrm{mod}\ 2x)$$

համակարգին եւ պատկանում է $\mathbb{R}[x]/L$ ֆակտոր-օղակին, որտեղ

$$L = (x-1)2x\mathbb{R}[x] = \{(x-1)2xg(x) \mid g(x) \in \mathbb{R}[x]\}:$$

Այն, որ L-ը իդեալ է, հեշտ է ուղղակիորեն ստուգել, կամ նկատել, որ այն $\mathbb{R}[x]$ օղակի գլխավոր իդեալ է (տես 2.2 պարագրաֆը): Ուրեմն $\mathbb{R}[x]/L$ ֆակտոր-օղակը կոռեկտ է սահմանված:

Էվկլիդեսի ընդլայնված ալգորիթմով դժվար չէ գտնել այնպիսի $u_i(x), v_i(x) \in \mathbb{R}[x]; i = 1,2$ բազմանդամներ, որոնց համար

$$u_1(x)\frac{(x-1)2x}{x-1} + v_1(x)(x-1) = 1,$$
$$u_2(x)\frac{(x-1)2x}{2x} + v_2(x)2x = 1:$$

$u_1(x) = 1/2, v_1(x) = -1, u_2(x) = -1, v_2(x) = 1/2$: Ուստի՝ $l_1(x) = x$ եւ $l_2(x) = 1-x$: Գծային կոմբինացիան կլինի՝

$$1 \cdot x + 3 \cdot (1-x) = -2x + 3 \equiv -2x + 3 (\mathrm{mod}\ (x-1)2x)$$

(նկատենք, որ վերջին բաղդատումը ոչինչ չի փոխում, քանի որ $1 = \deg(-2x+3) < \deg\big((x-1)2x\big) = 2$): Հեշտ է ստուգել, որ $f(x) = -2x + 3$ բազմանդամը բավարարում է օրինակի պահանջին:

5.1.13 Խնդիր. Գտնենք այն $f(x) \in \mathbb{Z}_5[x]$ մոդուլյար բազմանդամը, որը բավարարում է

$$f(x) \equiv x + 1 (\mathrm{mod}\ x+2),$$
$$f(x) \equiv 4x + 2 (\mathrm{mod}\ 3x+1)$$

համակարգին եւ պատկանում է $\mathbb{Z}_5[x]/L$ ֆակտոր-օղակին, որտեղ

$$L = (x+2)(3x+1)\mathbb{Z}_5[x] = \{(x+2)(3x+1)g(x) \mid g(x) \in \mathbb{Z}_5[x]\}:$$

Յուցում. այս խնդրի լուծման քայլերի միակ էական տարբերությունը 5.1.12 օրինակից կայանում է նրանում, որ բոլոր գործողություններն արվում են ըստ $p = 5$ մոդուլի: Նման գործողություններ մենք շատ ենք կատարելու 5.2 պարագրաֆում:

5.1.14 Դիտողություն. Համեմատելով այս պարագրաֆում միանգամից տարբեր օղակների (թվեր, բազմանդամներ, մոդուլյար բազմանդամներ եւլն) համար ստացված ալգորիթմներն առաջին գլխի շարադրանքի հետ (հատկապես 1.2 պարագրաֆի հետ), նկատում ենք, թե օղակային մեթոդներով ինչքան ավելի արագ ենք հասնում որոնելի ալգորիթմների կառուցմանը: Մինչդեռ 1.2 պարագրաֆում ընդամենը Էվկլիդեսի ալգորիթմի անալոգը $\mathbb{Z}_5[x]$-ում կիրառելու համար ստիպված էինք

բավական շատ նախապատրաստական փաստեր թվել ըստ մոդուլի բաժանումների մասին: Մյուս կողմից, եթե մենք դասընթացը սկսեինք միանգամից օղակների տեսական հասկացություններով, ապա մեր նախնական օրինակները (մասնավորապես, Կնուտի օրինակը) կարող էին դյուրընկալելի չլինել: Ուստի առաջին գլուխը կազմել ենք որպես տարրական մաթեմատիկայի լեզվով Էվկլիդյան օղակների կիրառության օրինակ:

5.2 Որոշիչի հաշվման մոդուլյար մեթոդներ

Նախքան մատրիցի որոշիչի հաշվման մոդուլյար մեթոդները նկարագրելը նշենք երկու հարցեր, որոնց պատճառով մեզ բավարար չեն որոշիչի հաշվման ավանդական մեթոդները, օրինակ, Գաուսի հայտնի մեթոդը, ըստ որի զրոյացնում ենք մատրիցի գլխավոր անկյունագծից ներքեւ գտնվող մասը, ապա հաշվում ձեւափոխված մատրիցի անկյունագծի տարրերի արտադրյալը (տես 2.3.17 վարժությունները եւ դրանց հաջորդող դիտողությունը):

Այդ հարցերից առաջինը միջանկյալ արժեքների ուռճացման երեւույթն է, որի դրսեւորումները մենք տեսանք 1.1 եւ 1.3 պարագրաֆներում՝ բազմանդամների ամենամեծ ընդհանուր բաժանարարը հաշվելիս: Մատրիցի որոշիչի հաշվման համար նույնպես հեշտ է բերել օրինակներ, երբ հաշվարկի ընթացքում ստացվում են միջանկյալ արժեքներ, որոնք շատ մեծ են, եւ որոնք, ի վերջո, քիչ ինֆորմացիա են պարունակում խնդրի վերջնական պատասխանի համար:

5.2.1 Օրինակ. Վերցնենք հետեւյալ n-րդ կարգի անկյունագծային մատրիցը

$$A = \begin{pmatrix} a & 0 & & & \mathbf{0} \\ 0 & a & & & \\ & & \cdots & & \\ & & & a & 0 \\ \mathbf{0} & & & 0 & b \end{pmatrix},$$

որի գլխավոր անկյունագծի վրա դասավորված են՝ $n-1$ անգամ ռացիոնալ a թիվը եւ մեկ անգամ ռացիոնալ b թիվը: Հասկանալի է, որ Գաուսի մեթոդով $\det A$ որոշիչը հաշվելիս կստանանք $d = \det A = a^{n-1} \cdot b$: Դժվար չէ ընտրել a, b թվերն այնպիսին, որ a, b, d արժեքները բոլորը լինեն փոքր թվեր, բայց որոշիչի հաշվման ընթացքում հանդիպեն շատ մեծ միջանկյալ արժեքներ: Օրինակ, կարելի է վերցնել $a = 10$ եւ $b = 1/10^{n-1}$: Այդ դեպքում $d = \det A = 1$, բայց որպես միջանկյալ արժեք ունենք

$a^{n-1} = 10^{n-1}$ աստիճանը, որն, ըստ n-ի ընտրության, կարելի է ինչքան ասես մեծ դարձնել: Մինչդեռ, $\det A$ որոշիչը կամայական p պարզ մոդուլով հաշվելիս, կխուսափենք $p-1$ արժեքը գերազանցող բոլոր թվերից:

Հաջորդ հարցը կապված է Գաուսի մեթոդով ամբողջ տարրերով մատրիցի որոշիչի հաշվման ալգորիթմի արագության հետ: Գլխավոր անկյունագծից ներքեւ գտնվող բոլոր տարրերը զրոյացնելու համար մենք մատրիցի տողերին գումարում ենք այլ տողեր՝ նախապես դրանք թվերով բազմապատկելով: Այդ պրոցեսում ստացվում են բազմաթիվ կոտորակային անդամներ, որոնց համարիչը եւ հայտարարը հաշվարկի հաջորդ քայլերում բազմապատկվում են այլ կոտորակներով եւ արդյունքում կարող են շատ արագ աճել:

Ենթադրենք հետեւյալ ընթացիկ մատրիցը ստացվել է Գաուսի մեթոդով մատրիցի որոշիչը հաշվելիս. արդեն զրոյացրել ենք գլխավոր անկյունագծի առաջին $k-1$ տարրերից ներքեւ ընկած մասը.

$$A = \begin{pmatrix} a_{11,1} & * & & & & * \\ 0 & \ddots & & & & \\ & & a_{k-1k-1,k-1} & * & \cdots & * \\ & & 0 & a_{kk,k} & \cdots & a_{kn,k} \\ & & \cdots & \cdots & \cdots & \cdots \\ \mathbf{0} & & 0 & a_{nk,k} & \cdots & a_{nn,k} \end{pmatrix}: \tag{5.8}$$

Յուրաքանչյուր k ինդեքսի համար $a_{ij,k}$ տառերով նշանակենք ձեւափոխված A մատրիցի այն տարրերը, որոնք կգրվեն մատրիցի $k-1$-րդ սյունից աջ այն բանից հետո, երբ արդեն զրոյացվել է $k-1$-րդ սյան՝ գլխավոր անկյունագծից ներքեւ ընկած մասը: Հասկանալի է, որ $i,j = k,\dots,n$ ինդեքսների համար.

$$a_{ij,k} = a_{ij,k-1} - \frac{a_{ik-1,k-1}}{a_{k-1k-1,k-1}} a_{k-1j,k-1}: \tag{5.9}$$

m_k-ով նշանակենք $a_{ij,k}$ կոտորակների բոլոր համարիչների եւ հայտարարների բացարձակ արժեքների մաքսիմումը ($i,j = 1,\dots,n$): Համարենք նաեւ, որ m_0-ն A մատրիցի բոլոր տարրերի բացարձակ արժեքների մաքսիմումն է (նախքան Գաուսի մեթոդով մատրիցը անկյունագծային տեսքի բերելու պրոցեսը սկսելը). $|a_{ij}| \le m_0$:

m_i արժեքների միջոցով վերեւից գնահատելով (5.9) բանաձեւի աջ մասը՝ կստանանք, որ

$$m_k \le 2m_{k-1}^4 \le 4m_{k-2}^{4^2} \le \cdots \le 2^k m_0^{4^k}:$$

Այսինքն՝ Գաուսի մեթոդով որոշիչը հաշվելիս կոտորակների բազմապատկման շնորհիվ չի բացառվում էքսպոնենցյալ արագությամբ աճող արժեքների գոյացումը:

Մինչդեռ, եթե մենք հաշվարկները կատարենք φ_p մոդուլյար անցումից հետո $A_p = \varphi_p(A)$ մատրիցում, ապա կխուսափենք ոչ միայն մեծ թվերից, այլեւ կոտորակներից, քանի որ $\mathbb{Z}_p$-ն դաշտ է, ուստի նրանում կոտորակային արտահայտություններ չեն առաջանա: Նկատենք, որ Գաուսի մեթոդով որոշիչ հաշվելիս երբեմն կարող են գլխավոր անկյունագծին հանդիպել զրոյական տարրեր, որոնց մենք կտեղափոխենք մատրիցի տողերի եւ սյուների դիրքափոխությամբ: Վերջին հաշվարկներում անտեսեցինք նման քայլերը, քանի որ մեր ստացած գնահատականն առանց այդ էլ շատ մեծ էր:

Որոշիչը մոդուլյար մեթոդներով հաշվելիս կտեսնենք, որ մեր կառուցած մոդուլյար ալգորիթմը միայն բազմանդամային արագություն ունի, եւ գործողություններում ներգրավվող արժեքները ոչ ավել, քան բազմանդամային արագությամբ են աճում:

Մինչեւ այս հարցերին պատասխանելը եւ որոշիչի հաշվման մոդուլյար ալգորիթմները կառուցելը՝ ապացուցենք մի բանաձեւ:

5.2.2 Լեմմա (Ադամարի անհավասարությունը). *Ենթադրենք տրված է n-րդ կարգի*

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \tag{5.10}$$

մատրիցը, որի տարրերը կամայական իրական թվեր են: Այդ դեպքում տեղի ունի հետեւյալ անհավասարությունը՝

$$R = |\det A| \le \prod_{i=1}^{n} \sqrt{a_{1i}^2 + \cdots + a_{ni}^2}:$$

Նախքան ապացույցը նկատենք, որ եթե A մատրիցի սյուները դիտարկենք որպես

$$s_1 = \begin{bmatrix} a_{11} \\ \vdots \\ a_{n1} \end{bmatrix}, \cdots, s_n = \begin{bmatrix} a_{1n} \\ \vdots \\ a_{nn} \end{bmatrix}$$

վեկտորներ եւ հիշենք, որ $\|s_i\| = \sqrt{a_{1i}^2 + \cdots + a_{ni}^2}$ տեսքով ընդունված է նշանակել վեկտորի նորմը, ապա լեմմայի անհավասարությունը ստանում է հետեւյալ տեսքը՝

$$|\det A| \le \prod_{i=1}^{n} \|s_i\|: \tag{5.11}$$

Ապացույց: Քանի որ Ադամարի բանաձեւի ապացույցը մեր ալգորիթմներում որեւէ դեր չի կատարում, բերենք այս բանաձեւի հնարավորինս կարճ մի ապացույց, որը հենվում է Շմիդտի օրթոգոնալացման պրոցեսի հատկության վրա:

Եթե $s_1, \dots, s_n$ վեկտորները գծորեն կախված են, ապա լեմմայի պնդումն ակնհայտ է, քանի որ $\det A = 0$: Ուստի ենթադրենք $s_1, \dots, s_n$ համակարգը անկախ է: Դա նաեւ նշանակում է, որ այդ վեկտորներից յուրաքանչյուրը ոչ զրոյական է, ուստի դրանցից ամեն մեկը կարելի է բաժանել իր երկարության վրա եւ ստանալ 1 երկարության վեկտոր $v_i = \frac{1}{\|s_i\|} s_i \quad (i = 1, \dots, n)$: Եթե (5.11)-ի աջ եւ ձախ մասերը բաժանենք $\|s_i\|$ երկարությունների վրա բոլոր $i = 1, \dots, n$ արժեքների համար, ապա (5.11)-ի աջ մասում կստանանք 1, իսկ ձախ մասում՝ v_i վեկտորների կոորդինատներից բաղկացած որոշիչի բացարձակ արժեքը: Ուստի (5.11)-ը ապացուցելու համար բավարար է ցույց տալ, որ նշված բացարձակ արժեքը չի գերազանցում 1-ը:

Գծային հանրահաշվից լավ հայտնի Շմիդտի օրթոգոնալացման պրոցեսը կիրառելով $v_1, \dots, v_n$ վեկտորների վրա կստանանք օրթոնորմավորված $u_1, \dots, u_n$ համակարգը: Ըստ օրթոգոնալացման պրոցեսի հատկության, $v_1, \dots, v_n$ համակարգի կոորդինատներից բաղկացած մատրիցի որոշիչը հավասար է $u_1, \dots, u_n$ համակարգի կոորդինատներից բաղկացած մատրիցի որոշիչին: Բայց նշված օրթոնորմավորված համակարգի վեկտորների վրա ձգված է n չափանի խորանարդը, որի ծավալը 1 է: ■

5.2.3 Հետեւանք. *Եթե n-րդ կարգի (5.10) մատրիցի բոլոր տարրերը բացարձակ արժեքով չեն գերազանցում B դրական թիվը, ապա* $\det A$ *որոշիչը բացարձակ արժեքով չի գերազանցում $n^{n/2}B^n$ թիվը:*

Ապացույց: Քանի որ

$$\|s_i\| = \sqrt{a_{1i}^2 + \dots + a_{ni}^2} \le \sqrt{nB^2} = \sqrt{n}B,$$

ապա, ըստ նախորդ լեմմայի, $|\det A| \le \prod_{i=1}^{n} \|s_i\| \le \left(\sqrt{n}B\right)^n$: ■

5.2.3 հետեւանքը հնարավորություն է տալիս գնահատելու $\det A$ արժեքը՝ առանց այդ որոշիչը հաշվելու: $M_n(R)$ օղակի A մատրիցի որոշիչը, ըստ (2.5) բանաձեւի, իրենից ներկայացնում է R-ի տարրերի արտադրյալների գումար: Քանի որ կամայական $\varphi: R \to L$ հոմոմորֆիզմ համաձայնեցված է օղակում գումարման եւ բազմապատկման գործողությունների նկատմամբ, ունենք.

$$\varphi(\det A) = \varphi\left(\sum_{\sigma\in S_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)}\cdots a_{n\sigma(n)}\right) = \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma)\varphi\big(a_{1\sigma(1)}\cdots a_{n\sigma(n)}\big)$$
$$= \sum_{\sigma\in S_n} \operatorname{sgn}(\sigma)\varphi\big(a_{1\sigma(1)}\big)\cdots\varphi\big(a_{n\sigma(n)}\big) = \det \varphi(A):$$

Մասնավորապես, եթե որպես φ վերցնենք φ_p մոդուլյար անցումը, ապա

$$\varphi_p(\det A) = \det \varphi_p(A) = \det A_p: \tag{5.12}$$

Նշանակենք $M_n = n^{n/2}B^n$: Եթե այժմ մենք վերցնենք որեւէ p պարզ թիվ, որը գերազանցում է $|\det A|$ արժեքը (իսկ դա առանց $\det A$ արժեքն իմանալու հեշտ է անել ըստ 5.2.3 հետեւանքի՝ վերցնելով որեւէ $p > M_n$), ապա $\varphi_p(\det A)$ արժեքի համար տեղի ունի հետեւյալ երկընտրանքը.

1. կամ $\det A$ որոշիչը ոչ բացասական է եւ $\varphi_p(\det A) = \det A$, քանի որ φ_p մոդուլյար անցման ժամանակ $\det A$-ն իրենից ավելի մեծ p թվի վրա բաժանելիս տալիս է $\det A$ մնացորդ,
2. կամ էլ $\det A$ որոշիչը բացասական է եւ $\varphi_p(\det A) = \det A + p$, քանի որ $\det A$-ն իրենից մոդուլով ավելի մեծ p թվի վրա բաժանելիս տալիս է $\det A + p$ մնացորդը:

Այս երկընտրանքը եւ (2.5) հավասարությունը կապ են ստեղծում $\mathbb{Z}_p$ դաշտում հաշվված $\det A_p$ մոդուլյար որոշիչի եւ նրա $\det A$ նախապատկերի միջեւ: $\det A_p$ արժեքը հավասար է կամ $\det A$-ին (եթե $\det A$-ն ոչ բացասական է), կամ էլ հավասար է $\det A + p$ գումարին (եթե $\det A$-ն բացասական է): Բացասական նախապատկերների հետ առաջացող այս բարդությունը մենք կարող ենք շրջանցել այնպես, ինչպես դա արեցինք 3.2.7 լեմմայում կամ 3.2.8 ալգորիթմում. եթե մենք վերցնենք M_n արժեքը երկու անգամ գերազանցող p, ապա $\det A$ եւ $\det A + p$ արժեքները իրարից կզանազանվեն այն հայտանիշով, որ դրանցից առաջինը $p/2$-ից փոքր է, իսկ երկրորդը՝ $p/2$-ից մեծ: Սա նշանակում է, որ եթե մենք պարզ մոդուլն ընտրենք $p > 2 \cdot M_n$ պայմանով, ապա $\det A_p$ մոդուլյար որոշիչի $\det A$ նախապատկերը վերականգնելու համար պետք է համեմատել $\det A_p$ եւ $p/2$ արժեքները. եթե $\det A_p < p/2$, ապա $\det A = \det A_p$, իսկ եթե $\det A_p > p/2$, ապա $\det A = \det A_p - p$:

Հասկանալի է, որ այս մոտեցման առավելությունը կայանում է նրանում, որ A_p մատրիցի որոշիչը մոդուլյար մեթոդներով հաշվելիս մենք խուսափում ենք միջանկյալ արժեքների ուռճացումից եւ կոտորակների հետ գործողություններից:

5.2.4 Ալգորիթմ (մատրիցի որոշիչի հաշվման մեծ պարզ թվի ալգորիթմը). Տրված է $A \in M_n(\mathbb{Z})$ մատրիցը: Հաշվել նրա $\det A$ որոշիչը:

1. A մատրիցի համար հաշվենք նրա տարրերի բացարձակ արժեքների B մաքսիմումը:

2. Ադամարի բանաձեւով ստանանք $|\det A|$ արժեքի $M_n = n^{n/2}B^n$ վերին գնահատականը:

3. Վերցնենք որեւէ p պարզ թիվ, որը բավարարում է $p > 2 \cdot M_n$ պայմանին:

4. Ըստ p մոդուլի իրականացնենք $\varphi_p: M_n(\mathbb{Z}) \to M_n(\mathbb{Z}_p)$ մոդուլյար անցումը եւ հաշվենք $\varphi_p(A) = A_p$ մատրիցը:

5. $\mathbb{Z}_p$ դաշտի վրա հաշվենք A_p մատրիցի $\det A_p$ որոշիչը:

6. Եթե $\det A_p < p/2$

7. դուրս գրենք $\det A = \det A_p$;

8. հակառակ դեպքում

9. դուրս գրենք $\det A = \det A_p - p$:

Այս ալգորիթմն ունի n-ից կախված բազմանդամային արագություն, որը կարելի է ներկայացնել

$$O(n^5(\log n + \log B)^2)$$

բանաձեւով: Ապացույցը, որը մենք բաց ենք թողնում, պարունակում է p պարզ թվի կառուցման հավանականային բանաձեւ եւ կապված է պարզ թվերի բաշխման հետ:

5.2.5 Օրինակ. Հետեւյալ մատրիցի որոշիչը հաշվենք Գաուսի ավանդական մեթոդով եւ ապա մեծ պարզ թվի մեթոդով.

$$A = \begin{pmatrix} 1 & 2 & -2 \\ 0 & 3 & 2 \\ 2 & 2 & 3 \end{pmatrix}:$$

Հաջորդաբար զրոյացնելով այուները՝ կստանանք.

$$\det A = \det \begin{pmatrix} 1 & 2 & -2 \\ 0 & 3 & 2 \\ 0 & -2 & 7 \end{pmatrix} = \det \begin{pmatrix} 1 & 2 & -2 \\ 0 & 3 & 2 \\ 0 & 0 & 25/3 \end{pmatrix} = 25:$$

Այժմ հաշվենք նույն արժեքը մեծ պարզ թվի մեթոդով:

$$M_n = 3^{3/2} \cdot 3^3 = \sqrt{27} \cdot 27 = 140{,}296 \ldots:$$

Ուրեմն, $2 \cdot M_n$ թիվը գերազանցող առաջին պարզ թիվն է՝ $p = 281$: Ուստի.

$$A_{281} = \varphi_{281}(A) = \begin{pmatrix} 1 & 2 & 279 \\ 0 & 3 & 2 \\ 2 & 2 & 3 \end{pmatrix}:$$

Հաջորդաբար զրոյացնելով սյուներն ըստ մոդուլի՝ կստանանք.

$$\det A_{281} = \det \begin{pmatrix} 1 & 2 & 279 \\ 0 & 3 & 2 \\ 0 & 279 & 7 \end{pmatrix} = \det \begin{pmatrix} 1 & 2 & 279 \\ 0 & 3 & 2 \\ 0 & 0 & 102 \end{pmatrix} = 3 \cdot_{281} 102 = 25:$$

Մնում է պարզել հավանական բացասական նախապատկերի հարցը: Քանի որ $25 < 281/2$, ապա վերջնական պատասխանն է՝ $\det A = 25$ (հակառակ անհավասարությունը տեղի կունենար, եթե $\det A$-ն բացասական լիներ, եւ այդ դեպքում մենք կստանայինք վերջնական պատասխանը՝ $\det A_{281}$-ից 281 հանելով):

Մատրիցի որոշիչը հաշվելու հաջորդ ալգորիթմը զգալիորեն ավելի արագ է, քան մատրիցի որոշիչի հաշվման մեծ պարզ թվի ալգորիթմը: Այն օգտագործում է ըստ մի քանի մոդուլների մոդուլյար անցումների մեթոդները եւ մնացքների մասին չինական թեորեմը, որոնք նկարագրեցինք 5.1 պարագրաֆում:

Տրված $A \in M_n(\mathbb{Z})$ մատրիցի համար Ադամարի բանաձեւով կրկին հաշվենք $M_n = n^{n/2}B^n$ արժեքը, որը վերին գնահատական է $|\det A|$-ի համար: Վերցնենք r հատ պարզ թվեր այնպիսիք, որ դրանց արտադրյալը երկու անգամ գերազանցի M_n-ը.

$$p_1 \cdots p_r \geq 2 \cdot M_n:$$

Հասկանալի է, որ ըստ այս պարզ մոդուլներից յուրաքանչյուրի կարող է քիչ ինֆորմացիա պահպանվել $\det A$ որոշիչի մասին: Սակայն $\det A_{p_1}, \dots, \det A_{p_r}$ արժեքների ամբողջությունը թույլ է տալիս վերականգնել $\det A$ արժեքը: Քանի որ $p_1, \dots, p_r$ թվերը զույգ առ զույգ փոխադարձաբար պարզ են, կարող ենք կիրառել 5.1.1 մնացքների մասին չինական թեորեմն ամբողջ թվերի համար. գոյություն ունի $h \in \mathbb{Z}$ թիվ այնպիսին, որ.

$$\begin{aligned} h &\equiv \det A_{p_1} \pmod{p_1}, \\ &\dots\dots\dots\dots\dots\dots\dots \\ h &\equiv \det A_{p_r} \pmod{p_r}, \end{aligned} \tag{5.13}$$

ընդ որում, եթե որեւէ t թիվ նույնպես բավարարում է այս համակարգին, ապա

$$t \equiv h \pmod{p_1 \cdots p_r}:$$

Ընդ որում, h-ը կարելի է հաշվել ըստ 5.1.7 ալգորիթմի: (5.12) բանաձեւը կիրառելով բոլոր $p_1, \dots, p_r$ մոդուլների վրա ստանում ենք, որ $\det A$-ն նույնպես բավարարում է (5.13) համակարգին: Ուրեմն՝ $\det A \equiv h (\mathrm{mod}\, p_1 \cdots p_r)$: Սա հետեւյալ կապն է հաստատում ստացված h արժեքի եւ $\det A$-ի միջեւ: Եթե $\det A$-ն ոչ բացասական է, ապա $h = \det A$, քանի որ եթե $p_1 \cdots p_r$ թիվը չգերազանցող երկու ոչ բացասական ամբողջ թվեր իրար բաղդատելի են այդ մոդուլով, ապա նրանք իրար հավասար են: Ավելին՝ $h = \det A < p_1 \cdots p_r/2$: Իսկ եթե $\det A$-ն բացասական է, ապա $h = \det A + p_1 \cdots p_r$, քանի որ $\det A$-ն $-p_1 \cdots p_r$ թվից ոչ փոքր բացասական ամբողջ թիվ է: Ավելին՝ $h = \det A + p_1 \cdots p_r > p_1 \cdots p_r/2$:

Այս երկընտրանքը կապ է ստեղծում ըստ 5.1.7 ալգորիթմի հաշվված h արժեքի եւ $\det A$ որոշիչի միջեւ: $\det A$ արժեքը հավասար է h-ի, եթե $h < p_1 \cdots p_r/2$, եւ հավասար է $h - p_1 \cdots p_r$, եթե $h > p_1 \cdots p_r/2$:

Ստացված ալգորիթմն ավելի արագ է, քան նախորդը: Այն ունի n-ից կախված բազմանդամային արագություն, որը կարելի է ներկայացնել

$$O(n^4 \log^2(nB)(\log^2 n + (\log\log B)^2))$$

բանաձեւով: Սրա ապացույցը եւս հենվում է $p_1, \dots, p_r$ պարզ թվերի կառուցման հավանականային բանաձեւերի վրա:

5.2.6 Ալգորիթմ (մատրիցի որոշիչի հաշվման փոքր պարզ թվերի ալգորիթմը). Տրված է $A \in M_n(\mathbb{Z})$ մատրիցը: Հաշվել նրա $\det A$ որոշիչը:

1. A մատրիցի համար հաշվենք նրա տարրերի բացարձակ արժեքների B մաքսիմումը:

2. Ադամարի բանաձեւով ստանանք $|\det A|$ արժեքի $M_n = n^{n/2}B^n$ վերին գնահատականը:

3. Վերցնենք որեւէ $p_1, \dots, p_r$ պարզ թվեր, որոնք բավարարում են $p_1 \cdots p_r > 2 \cdot M_n$ պայմանին:

4. $(i = 0;\ i \le r;\ \ i++)$ արժեքների համար

5. ըստ p_i մոդուլի իրականացնենք $\varphi_{p_i}: M_n(\mathbb{Z}) \to M_n(\mathbb{Z}_{p_i})$ մոդուլյար անցումը եւ հաշվենք $\varphi_{p_i}(A) = A_{p_i}$ մատրիցը:

6. $\mathbb{Z}_{p_i}$ դաշտի վրա հաշվենք A_{p_i} մատրիցի $\det A_{p_i}$ որոշիչը:

7. Ըստ 5.1.7 ալգորիթմի հաշվենք այն h թիվը, որը բավարարում է (5.13) համակարգին:

8. Եթե $h < p_1 \cdots p_r/2$

9. դուրս գրենք $\det A = h$;

10. հակառակ դեպքում

11. դուրս գրենք $\det A = h - p_1 \cdots p_r$:

5.2.7 Օրինակ. Այժմ հաշվենք 5.2.5 օրինակի

$$A = \begin{pmatrix} 1 & 2 & -2 \\ 0 & 3 & 2 \\ 2 & 2 & 3 \end{pmatrix}$$

մատրիցի որոշիչը փոքր մեծ պարզ թվերի մեթոդով: Կրկին

$$M_n = 3^{3/2} \cdot 3^3 = \sqrt{27} \cdot 27 = 140{,}296 \ldots:$$

Վերցնելով հետեւյալ չորս պարզ թվերը՝ $2, 3, 5, 11$, նկատում ենք, որ դրանց արտադրյալն արդեն բավականաչափ մեծ է.

$$2 \cdot 3 \cdot 5 \cdot 11 = 330 > 2 \cdot M_n:$$

Նկատենք, որ եթե որպես չորրորդ պարզ թիվ վերցնեինք 7-ը, ապա արտադրյալը բավականաչափ մեծ չէր լինի, եւ մենք ստիպված կլինեինք եւս մի պարզ թիվ վերցնել: Չորս անգամ կիրառենք մոդուլյար անցումներ եւ հաշվենք մոդուլյար որոշիչները.

$$A_2 = \varphi_2(A) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}:$$

Միանգամից երեւում է, որ $\det A_2 = 1$: Այնուհետեւ.

$$A_3 = \varphi_3(A) = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 0 & 2 \\ 2 & 2 & 0 \end{pmatrix}:$$

Բերենք անկյունագծային տեսքի (երկրորդ քայլում զրոյական տարրից խուսափելու համար տեղափոխում ենք տողերը).

$$\det A_3 = \det \begin{pmatrix} 1 & 2 & 0 \\ 0 & 0 & 2 \\ 0 & 1 & 1 \end{pmatrix} = -\det \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \end{pmatrix} = -2 = 1:$$

Երրորդ քայլում.

$$A_5 = \varphi_5(A) = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 3 & 2 \\ 2 & 2 & 3 \end{pmatrix}:$$

Բերենք անկյունագծային տեսքի.

$$\det A_5 = \det \begin{pmatrix} 1 & 2 & 3 \\ 0 & 3 & 2 \\ 0 & 3 & 2 \end{pmatrix} = 0:$$

Չորրորդ քայլում.

$$A_{11} = \varphi_{11}(A) = \begin{pmatrix} 1 & 2 & 9 \\ 0 & 3 & 2 \\ 2 & 2 & 3 \end{pmatrix}:$$

Բերենք անկյունագծային տեսքի.

$$\det A_{11} = \det \begin{pmatrix} 1 & 2 & 9 \\ 0 & 3 & 2 \\ 0 & 9 & 7 \end{pmatrix} = \det \begin{pmatrix} 1 & 2 & 9 \\ 0 & 3 & 2 \\ 0 & 0 & 1 \end{pmatrix} = 3:$$

Այժմ մնացքների մասին 5.1.1 չինական թեորեմով գտնենք այն d ամբողջ թիվը, որը բավարարում է հետեւյալ համակարգին՝

$$d \equiv 1 (\mathrm{mod}\ 2),$$

$$d \equiv 1 (\mathrm{mod}\ 3),$$

$$d \equiv 0 (\mathrm{mod}\ 5),$$

$$d \equiv 3 (\mathrm{mod}\ 11),$$

եւ որը պատկանում է $\mathbb{Z}_{330}$ օղակին: Դա մենք հաշվում ենք նույն կերպ, ինչ 5.1.9 վարժությունը: Բաց թողնելով մանր հաշվարկները՝ $d = 25$: Մնում է համեմատել ստացված 25 արժեքը $330/2$ արժեքի հետ: Քանի որ $25 < 330/2$, ապա վերջնական պատասխանն է՝ $\det A = 25$ (հակառակ անհավասարությունը տեղի կունենար, եթե $\det A$-ն բացասական լիներ, եւ այդ դեպքում մենք կստանայինք վերջնական պատասխանը՝ 25-ից 330 հանելով):

5.2.8 Դիտողություն. Բերված 5.2.4 եւ 5.2.6 ալգորիթմները մենք ձեւակերպեցինք ամբողջ տարրերով մատրիցների համար՝ չնայած պարզ է, որ դրանք ռացիոնալ մատրիցների վրա կիրառելու համար բավական է միայն բազմապատկել մատրիցը իր բոլոր տարրերի հայտարարների ամենափոքր ընդհանուր բազմապատիկով:

5.2.9 Դիտողություն. Իրականում Գաուսի մեթոդը բազմանդամային արագություն ունի նաեւ $M_n(\mathbb{Q})$, $M_n(\mathbb{R})$ եւ $M_n(\mathbb{C})$ օղակներում: Սակայն դրա ապացույցը տեխնիկապես ավելի բարդ է, քան այն, ինչ մենք բերեցինք մոդուլյար մեթոդների կիրառմամբ կառուցված ալգորիթմների համար:

5.3 Ամենամեծ ընդհանուր բաժանարարի փոքր պարզ թվերի ալգորիթմը

5.1 պարագրաֆում բերված ըստ մի քանի մոդուլների հաշվարկի մեթոդները կարող են օգտագործվել 3.4 եւ 3.6 պարագրաֆներում կառուցված ամենամեծ ընդհանուր բաժանարարի հաշվման ալգորիթմներն ուժեղացնելու համար:

Քանի որ այս ալգորիթմի կառուցումն ավելի բարդ է, քան մեծ պարզ թվի ալգորիթմի կառուցումը, ապա նյութն ավելի դյուրընկալելի դարձնելու համար սկսենք համեմատաբար պարզ խնդիրներից: Նախ, ենթադրենք, թե պետք է վերականգնել ինչ-որ $d(x) \in \mathbb{Z}[x]$ բազմանդամ, որի համար մեզ հայտնի է դրա գործակիցների բացարձակ արժեքների N վերին գնահատականը, եւ պարզ թվերի ինչ-որ անվերջ $p_1, p_2, \dots, p_k, \dots$ հաջորդականության համար մեզ տրված են $d(x)$-ի $\varphi_{p_i}\big(d(x)\big) = d_{p_i}(x) \stackrel{\text{def}}{=} s_i(x)$ պատկերները: Այստեղ մենք օգտագործում ենք $s_i(x)$ նշանակումը, որպեսզի խուսափենք «ինդեքսի ինդեքս» պարունակող $d_{p_i}(x)$ նշանակումից, եւ որպեսզի մեր նշանակումները ավելի մոտ լինեն 5.1 պարագրաֆի նշանակումներին:

Վերցնենք $p_1, \dots, p_k$ պարզ թվեր եւ k անգամ կիրառենք 5.1.1 թեորեմը՝ որպես բաղդատման $m_1, \dots, m_k$ մոդուլներ վերցնելով $p_1, \dots, p_k$ արժեքները: Ամեն անգամ հերթական $i = 1, \dots, k$ ինդեքսի համար ստանանք այնպիսի մի n_i թիվ, որ.

$$\begin{gathered} n_i \equiv 0 (\mathrm{mod}\, p_1), \\ \dots\dots\dots\dots\dots\dots \\ n_i \equiv 1 (\mathrm{mod}\, p_i), \\ \dots\dots\dots\dots\dots\dots \\ n_i \equiv 0 (\mathrm{mod}\, p_k), \end{gathered} \tag{5.14}$$

$i = 1, \dots, k$: Ըստ այս n_i թվերի եւ ըստ տրված $s_i(x)$ բազմանդամների կառուցենք

$$S(x) = S_{p_1,\dots,p_k}(x) \stackrel{\text{def}}{=} n_1 \cdot s_1(x) + \dots + n_k \cdot s_k(x) \in \mathbb{Z}[x] \tag{5.15}$$

գումարը (համառոտության համար պայմանավորվենք $S(x)$-ի ինդեքսում գրել $p_1, \dots, p_k$ թվերը միայն այն դեպքում, երբ անհրաժեշտ կլինի շեշտել դրանք)։ Եթե պարզ թվերի բազմությունը նշանակենք $P = \{p_1, \dots, p_k\}$, ապա երբեմն հարմար է գրել նաեւ $S_P(x) = S_{p_1,\dots,p_k}(x)$։

Քանի որ բազմանդամների գումարման ժամանակ գործակիցները գումարվում են ըստ համապատասխան աստիճանների, ապա պարզ է, որ (5.15) գումարում յուրաքանչյուր x^j-ի գործակիցը մի թիվ է, որը p_i մոդուլով բաղդատելի է $s_i(x)$ բազմանդամում x^j-ի գործակցին։ Նշանակում է, որ կամայական p_i-ի համար ($i = 1, \dots, k$) $S(x)$ եւ $d(x)$ բազմանդամները հավասար են ըստ p_i մոդուլի. $\varphi_{p_i}\big(d(x)\big) = \varphi_{p_i}\big(S(x)\big)$։

Նշանակենք $m = p_1 \cdots p_k$ եւ պայմանավորվենք կամայական $f(x) = a_0x^n + \cdots + a_n$ բազմանդամի համար $f_m(x)$-ով նշանակել այն բազմանդամը, որը ստացվում է $f_m(x)$-ի բոլոր գործակիցները «ըստ m մոդուլի դիտարկելիս», այսինքն՝

$$f_m(x) = \varphi_m(a_0)x^n + \cdots + \varphi_m(a_n) \in \mathbb{Z}[x],$$

որտեղ φ_m-ը $\varphi_m\colon \mathbb{Z} \to \mathbb{Z}_m$ թվային օղակների հոմոմորֆիզմն է (տես նաեւ 1.2 պարագրաֆը)։ Նկատենք, որ մենք չէինք կարող պարզապես գրել $f_m(x) = \varphi_m\big(f(x)\big)$, համարելով, որ φ_m-ը $\varphi_m\colon \mathbb{Z}[x] \to \mathbb{Z}_m[x]$ բազմանդամային օղակների հոմոմորֆիզմն է, քանի որ բաղադրյալ m-ի համար $\mathbb{Z}_m$ օղակի վրա $\mathbb{Z}_m[x]$ բազմանդամային օղակ սահմանված չէ ($\mathbb{Z}_m$ օղակն ամբողջության տիրույթ չէ)։ Քանի որ $f_m(x)$ բազմանդամը $f(x)$-ից տարբերվում է միայն մի քանի՝ m-ի վրա բաժանվող գումարելիներով, որոնք զրոյանում են $\varphi_{p_i}\colon \mathbb{Z}[x] \to \mathbb{Z}_{p_i}[x]$ մոդուլյար անցման ժամանակ (հիշենք, որ $m \vdots p_i$), ապա $f(x)$ եւ $f_m(x)$ բազմանդամներն φ_{p_i} մոդուլյար անցման ժամանակ ունեն միեւնույն պատկերը։ Ուրեմն.

$$\varphi_{p_i}\big(d_m(x)\big) = \varphi_{p_i}\big(d(x)\big) = \varphi_{p_i}\big(S(x)\big) = \varphi_{p_i}\big(S_m(x)\big),$$

$i = 1, \dots, k$։ Այսինքն՝ $d(x)$ եւ $S(x)$ բազմանդամները, «ըստ m մոդուլի դիտարկելուց հետո» ունեն նույն $s_i(x)$ պատկերները։ Ըստ 5.1.1 թեորեմի երկրորդ պնդման, $\{0, 1, \dots, m-1\}$ բազմության մեջ կա միայն մի թիվ, որը բավարարում է (5.1) համակարգին։ Կիրառելով դա բազմանդամների յուրաքանչյուր գործակցի վրա՝ ստանում ենք, որ $d_m(x) = S_m(x)$։

5.3.1 Օրինակ. Վերցնենք $d(x) = 5x^2 - 7x - 11$ եւ $k = 2$, $p_1 = 3$, $p_2 = 5$։ Այդ դեպքում $d_3(x) = s_1(x) = 2x^2 + 2x + 1$ եւ $d_5(x) = s_2(x) = 3x + 4$։ Հեշտ է Էվկլիդեսի ընդհանրացված ալգորիթմով հաշվել (5.14) համակարգին բավարարող n_1 եւ n_2 թվերը։ $n_1 = 10$ եւ $n_2 = 6$։ Այդ դեպքում

$$S(x) = S_{3,5}(x) = n_1 \cdot s_1(x) + n_2 \cdot s_2(x) = 10(2x^2 + 2x + 1\,) + 6(3x + 4)$$
$$= 20x^2 + 38x + 34:$$

Քանի որ $m = p_1 \cdot p_2 = 3 \cdot 5 = 15$, ապա $S_m(x) = S_{15}(x) = 5x^2 + 8x + 4$: Այսուս կողմից, $d_m(x) = d_{15}(x) = 5x^2 + 8x + 4$: Այսինքն, իսկապես, $d_m(x) = S_m(x)$:

Ստացված $d_m(x) = S_m(x)$ հավասարությունը նախանշում է $s_i(x)$ բազմանդամների միջոցով $d(x)$ բազմանդամի վերականգնման ուղին: Վերցնենք այնքան շատ $p_1, \dots, p_k$ պարզ թվեր, որ $m = p_1 \cdots p_k$ արտադրյալը մեծ լինի $2N$-ից: Այս դեպքում $d(x)$ եւ $d_m(x)$ բազմանդամների բոլոր *ոչ բացասական* գործակիցները կհամընկնեն, քանի որ դրանք փոքր են N-ից, եւ m մոդուլով դիտարկվելիս չեն փոխվում: Դրանք փոքր կլինեն նաեւ $m/2$-ից, քանի որ $m > 2N$: Իսկ $d(x)$-ի որեւէ *բացասական* գործակից m մոդուլով դիտարկվելիս դրան պարզապես կգումարվի m: Այսինքն՝ $d(x)$-ի բացասական գործակիցներին համապատասխանում են $d_m(x)$-ի այն գործակիցները, որոնք մեծ են $m/2$-ից:

Ստացվում է $d(x)$-ի վերականգնման հետեւյալ եղանակը: Վերցնենք կամայական $p_1, \dots, p_k$ թվեր, որոնց համար $m = p_1 \cdots p_k > 2N$, ապա (5.15) բանաձեւով կառուցենք $S(x) = S_{p_1,\dots,p_k}(x)$ բազմանդամը: Դրա բոլոր գործակիցները ըստ m մոդուլի դիտարկելով՝ ստանանք $S_m(x) = d_m(x)$ բազմանդամը: Իսկ $d_m(x)$-ից $d(x)$ բազմանդամը վերականգնելու համար m-ով փոքրացնենք դրա բոլոր այն գործակիցները, որոնք մեծ են $m/2$-ից:

5.3.2 Օրինակ. Կիրառենք այս կանոնը 3.1.1 օրինակի $d(x) = 5x^2 - 7x - 11$ բազմանդամի համար: Այդ դեպքում $N = \max\{5, |-7|, |-11|\} = 11$: Վերցնենք $k = 3$, $p_1 = 3$, $p_2 = 5$, $p_3 = 7$ եւ $m = 3 \cdot 5 \cdot 7 = 105 > 2 \cdot 11$: Այդ դեպքում $s_1(x) = 2x^2 + 2x + 1$, $s_2(x) = 3x + 4$, $s_3(x) = 5x^2 + 3$: Էվկլիդեսի ընդհանրացված ալգորիթմով հաշվենք (5.14) համակարգին բավարարող n_1, n_2 եւ n_3 թվերը: $n_1 = -35$, $n_2 = 21$ եւ $n_3 = 15$: Այդ դեպքում.

$$S(x) = S_{3,5,7}(x) = -35(2x^2 + 2x + 1\,) + 21(3x + 4) + 15(5x^2 + 3)$$
$$= 5x^2 - 7x + 94:$$

Քանի որ $m = 105$, ապա $S_m(x) = S_{105}(x) = 5x^2 + 98x + 94$: Սրա գործակիցները համեմատենք $m/2 = 105/2 = 52.5$ արժեքի հետ: Քանի որ $S_{105}(x)$ բազմանդամի վերջին երկու գործակիցները մեծ են 52.5-ից, ապա դրանցից հանենք 105: Ստանում ենք $d(x)$ բազմանդամի ճշգրիտ վերականգնումը.

$$d(x) = 5x^2 + (98 - 105)x + (94 - 105) = 5x^2 - 7x - 11:$$

5.3.3 Վարժություն. Պարզ թվերի $p_1, \dots, p_k$ ընտրությունը, իհարկե, միակը չէ: Նախորդ օրինակում մենք պարզապես վերցրինք առաջին պարզ թվերը, որոնք զույգ չեն եւ որոնց արտադրյալը $2 \cdot 11$-ից մեծ է: Դրանք երեք հատ էին: Վերցնել $p_1 = 5$, $p_2 = 7$ պարզ թվերը եւ հաշվարկը տանել դրանց համար: Ճիշտ պատասխանը երաշխավորված է, քանի որ $m = 5 \cdot 7 = 35 > 2 \cdot 11$:

5.3.4 Դիտողություն. Մենք խուսափեցինք $p = 2$ զույգ պարզ թվից, որպեսզի $m/2$ արժեքը ամբողջ թիվ չլինի: Այլապես $S_m(x)$-ի որոշ գործակիցներ կարող էին հավասար լինել $m/2$-ի: Այս պարագրաֆի ալգորիթմի հետ աշխատելու որոշ փորձառություն ձեռք բերելուց հետո կարելի է աշխատել նաեւ $p = 2$ պարզ մոդուլով, քանի որ $m/2$-ի հավասար գործակիցների դեպքը շրջանցելը դժվար չէ:

5.3.5 Խնդիր. Ի՞նչ տեսք կստանա մեր բերած կանոնը, եթե միանգամից վերցնենք մեկ հատ $p_1 > 2 \cdot N$ պարզ թիվ: Այսինքն՝ $k = 1$:

Այժմ մի փոքր բարդացնենք պայմանները: Ենթադրենք.

1) մեզ հայտնի չէ N արժեքը, սակայն հայտնի է, որ որոնելի $d(x)$ բազմանդամը մեզ արդեն տրված $f(x)$ եւ $g(x)$ պրիմիտիվ բազմանդամների ամենամեծ ընդհանուր բաժանարարն է,
2) պարզ թվերի $p_1, \dots, p_k, \dots$ հաջորդականության համար տրված $s_i(x)$ բազմանդամների մասին ունենք ավելի թույլ պայման: Դրանց մասին հայտնի է ոչ թե այն, որ դրանք $d(x)$-ի պատկերներ են, այլ միայն այն, որ դրանք $d(x)$-ի ինչ-որ $e \cdot d(x)$ սկալյար պատիկի պատկերներ են, որտեղ e-ն անհայտ է, բայց ունենք դրա արժեքի $|e| \le E$ գնահատականը:

Նախորդ կառուցումները մի փոքր փոփոխելով՝ մենք կարող ենք վերականգնել $d(x)$ բազմանդամը, եթե հայտնի են $f(x)$, $g(x)$, $s_i(x)$ բազմանդամները ($i = 1,2, \dots$) եւ E գնահատականը: Իսկապես, ըստ 3.1.8 հետեւանքի (3.3) բանաձեւի, կարելի է $d(x)$-ի գործակիցների մոդուլների համար որպես վերին գնահատական վերցնել $N_{f,g}$ արժեքը: Քանի որ $s_i(x)$ բազմանդամները $e \cdot d(x)$-ի պատկերներ են, ապա, համարելով $N = E \cdot N_{f,g}$ եւ վերցնելով

$$p_1 \dots p_k > 2 \cdot N = 2 \cdot E \cdot N_{f,g}$$

պայմանին բավարարող $p_1, \dots, p_k$ պարզ թվեր, մենք կարող ենք կրկնել վերը բերված քայլերը եւ ստանալ $S(x)$ եւ $S_m(x)$ բազմանդամները (դարձյալ $m = p_1 \dots p_k$): $S_m(x)$-ից կարելի է վերականգնել $e \cdot d(x)$ բազմանդամը, որը, սակայն, դեռ $d(x)$-ը չէ (e-ն անհայտ է մեզ): Ըստ 2.6.9 հետեւանքի, $d(x)$-ը պրիմիտիվ է, ուստի կարելի է

վերականգնել այն որպես մեր ստացած $e \cdot d(x)$ բազմանդամի պրիմիտիվ մասը՝ $d(x) = \mathrm{pp}\big(e \cdot d(x)\big)$: Այսինքն՝ $f(x)$, $g(x)$ բազմանդամների պրիմիտիվությունը մեզ թույլ է տալիս $d(x)$-ն նախ «վերականգնել e սկալյար արտադրիչի ճշտությամբ», ապա ազատվել այդ արտադրիչից՝ վերականգնված բազմանդամի պրիմիտիվ մասին անցնելու միջոցով:

Այժմ անցնենք $s_i(x)$, $i = 1, 2, \ldots$ բազմանդամների եւ E գնահատականի կառուցմանը՝ ըստ տրված $f(x)$ եւ $g(x)$ պրիմիտիվ բազմանդամների: Ինչպես տեսանք 3.4 պարագրաֆում (մասնավորապես, 3.4.2 օրինակում), տրված p_i պարզ թվի համար $f_{p_i}(x)$, $g_{p_i}(x)$ բազմանդամների մոդուլյար $z_i(x) = \big(f_{p_i}(x),\ g_{p_i}(x)\big)$ ամենամեծ ընդհանուր բաժանարարը, որը Էվկլիդեսի ալգորիթմով հեշտ է հաշվել $\mathbb{Z}_{p_i}[x]$ Էվկլիդյան օղակում, կարող է ընդհանրապես չհանդիսանալ $d(x)$-ի պատկերը. այն կարող է տրիվիալ լինել կամ նրա աստիճանը կարող է ավելի բարձր լինել, քան $d(x)$-ի աստիճանն է:

2.7.6 լեմման կիրառելով $K = \mathbb{Z}_p$ դաշտի դեպքի համար, ունենք, որ $\mathbb{Z}_p[x]$ *օղակի* $f(x)$, $g(x)$ ոչ զրոյական բազմանդամների $d(x)$ ընդհանուր բաժանարարը նրանց ամենամեծ ընդհանուր բաժանարարն է այն եւ միայն այն դեպքում, երբ $d(x)$-ի աստիճանը այդ բազմանդամների ընդհանուր բաժանարարների աստիճանների մաքսիմումն է:

Ենթադրենք մեզ արդեն հաջողվել է ընտրել այնպիսի $p_1, \ldots, p_k$ պարզ թվեր, որոնց համար $\deg z_i(x) = \deg\big(f_{p_i}(x), g_{p_i}(x)\big) = \deg d(x)$: Ըստ քիչ առաջ նշվածի, սա նշանակում է, որ $s_i(x)$ բազմանդամները կարող ենք որոնել $t_i \cdot z_i(x)$ տեսքով: $t_i \in \mathbb{Z}_{p_i}$ սկալյար արտադրիչի դերը բացատրված է 3.4.1 դիտողության եւ 3.4.2 օրինակի մեջ. $\mathbb{Z}[x]$ օղակում միակ հակադարձելի տարրերն են $1, -1$ թվերը, ուստի $d(x)$ ամենամեծ ընդհանուր բաժանարարը որոշվում է միայն նշանի ճշտությամբ: Իսկ $\mathbb{Z}_{p_i}[x]$ օղակում հակադարձելի է կամայական ոչ զրոյական թիվ: Ուստի $\mathbb{Z}_{p_i}[x]$ օղակում $f_{p_i}(x)$, $g_{p_i}(x)$ բազմանդամների ամենամեծ ընդհանուր բաժանարար է նաեւ $z_i(x)$-ի կամայական $t_i \cdot z_i(x)$ պատիկը ($t_i \neq 0$):

t_i արժեքը կարելի է որոշել հետեւյալ կերպ: Ենթադրենք $f(x)$, $g(x)$ բազմանդամների ավագ գործակիցներն են, համապատասխանաբար, a_0, b_0 թվերը: Նշանակենք $w = (a_0, b_0)$: Ըստ 3.4.6 լեմմայի, եթե $p_i \nmid w$, ապա միշտ $\deg\big(f_p(x), g_p(x)\big) \geq \deg d(x)$: Եթե $p_i \nmid w$, ապա φ_{p_i} մոդուլյար անցման ժամանակ չեն փոփոխվում ոչ w-ն եւ ոչ էլ $d(x)$-ի c_0 ավագ գործակիցը (քանի որ $\mathbb{Z}[x]$ օղակում -1 թվով բազմապատկումը չի ազդում բաժանելիության վրա, կարող ենք

համարել, որ $f(x)$, $g(x)$, $d(x)$ բազմանդամների ավագ գործակիցները դրական են): Ուրեմն, եթե անգամ չգիտենք c_0 ավագ գործակիցը, մեզ հայտնի է, որ այդ արժեքների w/c_0 հարաբերությունը չի փոխվում $\varphi_{p_i}\colon \mathbb{Z}[x] \to \mathbb{Z}_{p_i}[x]$ մոդուլյար անցման ժամանակ: Եթե t_i-ն ընտրենք այնպես, որ $s_i(x) = t_i \cdot z_i(x)$ պատիկի ավագ գործակիցը p_i մոդուլով հավասար լինի w-ի, ապա կարելի է պնդել, որ $s_i(x)$-ը հանդիսանում է $d(x)$-ի ինչ-որ $e \cdot d(x)$ սկալյար պատիկի պատկեր, որտեղ e-ն անհայտ է, բայց ունենք դրա արժեքի $|e| \le w/c_0 \le w$ գնահատականը: Նշանակենք $E = w$ եւ վերականգնենք $d(x)$-ը արդեն բերված եղանակով. վերցնենք այնքան շատ $p_1, \dots, p_k$ թվեր ($p_i \nmid w$), որ բավարարվի

$$p_1 \dots p_k > 2 \cdot N = 2 \cdot E \cdot N_{f,g}$$

պայմանը: Ըստ $p_1, \dots, p_k$ մոդուլների կառուցենք n_i թվերը եւ $z_i(x)$ ու $s_i(x)$ բազմանդամները: Դրանց միջոցով կառուցենք $S(x)$ եւ $S_m(x)$ բազմանդամները: Վերականգնենք $e \cdot d(x)$ բազմանդամը եւ ստանանք $d(x) = \mathrm{pp}\big(e \cdot d(x)\big)$:

5.3.6 Օրինակ. Հետեւյալ բազմանդամները մենք այս պարագրաֆում դիտարկելու ենք մի քանի անգամ՝ ալգորիթմի տարբեր քայլեր մեկնաբանելու ընթացքում.

$$\begin{aligned} f(x) &= 28x^3 + 216x^2 - 193x - 51, \\ g(x) &= 8x^3 + 78x^2 + 33x - 442: \end{aligned} \tag{5.16}$$

$f(x)$, $g(x)$ բազմանդամները պրիմիտիվ են: Ըստ $p_1 = 7$ մոդուլի կունենանք՝

$$\begin{aligned} \varphi_7\big(f(x)\big) &= f_7(x) = 6x^2 + 3x + 5, \\ \varphi_7\big(g(x)\big) &= g_7(x) = x^3 + x^2 + 5x + 6: \end{aligned} \tag{5.17}$$

Հեշտ է ստուգել, որ $z_1(x) = 5x + 4 \in \mathbb{Z}_7[x]$ բազմանդամը $f_7(x)$, $g_7(x)$ զույգի ամենամեծ ընդհանուր բաժանարարներից մեկն է: Մյուս կողմից, դրա 5 ավագ գործակիցը չի բաժանում 28 եւ 8 ավագ գործակիցները: Ուրեմն, $z_1(x)$ բազմանդամը $f(x)$, $g(x)$ բազմանդամների ոչ մի ընդհանուր բաժանարարի պատկեր չի հանդիսանա: Քանի որ $w = (28, 8) = 4$, ապա $\big(f(x),\ g(x)\big)$-ի ավագ գործակիցը պիտի լինի 4-ի որեւէ բաժանարար ($\pm 4, \pm 2, \pm 1$ թվերից մեկը): $5x + 4$ բազմանդամն ըստ 7 մոդուլի բազմապատկելով $t_1 = 5^{-1} \cdot 4 = 5 \in \mathbb{Z}_7$ թվով, կստանանք՝

$$s_1(x) = 5(5x + 4) = 4x + 6$$

ընդհանուր բաժանարարը: Ինչպես հետո կստուգենք 5.3.14 օրինակում, $\big(f(x),\ g(x)\big) = 2x + 17$: Քանի որ $\varphi_7(2x + 17) = 2x + 3$, տեսնում ենք, որ վերը ստացված $4x + 6 = e \cdot (2x + 3)$ բազմանդամը $2x + 3 = \mathrm{pp}(2x + 3)$ պրիմիտիվ բազմանդամի պատիկն է: Դրա պատճառը հասկանալի է. $\big(f(x),\ g(x)\big)$-ի ավագ գործակիցը 4-ի

բաժանարար է, մինչդեռ մենք $5x+4$ բազմանդամը բազմապատկեցինք այնպիսի մի t_1 թվով, որ ստանանք (7 մոդուլով) 4-ին խիստ հավասար ավագ գործակից: Ուրեմն, $t_1(5x+4)$ արտադրյալը, եթե $2x+3$ բազմանդամը չէ, ապա դրա պատիկն է:

Ինչպես տեսնում ենք, $d(x)$-ի վերականգնման գրեթե բոլոր քայլերն արված են: Միակ բաց մնացած հարցն այն է, թե ինչպե՞ս գտնենք $p_1, \dots, p_k, \dots$ պարզ թվեր, որոնց համար $\deg z_i(x) = \deg d(x)$: Այդ թվերի հայտնաբերման եղանակը հանգելու է այնպիսի p_i պարզ թվերի քննարկմանը, ըստ որոնց հաշվվող $z_i(x)$-ի աստիճանները գնալով ավելի ու ավելի փոքր են դառնում, մինչեւ կհավասարվեն $\deg d(x)$-ին:

$f(x),\ g(x) \in \mathbb{Z}[x]$ (պրիմիտիվ) բազմանդամների համար վերցնենք կամայական p_1 կենտ պարզ թիվ, որը չի բաժանում դրանցից գոնե մեկի ավագ գործակիցը, այսինքն՝ $p_1 \nmid w$: Կատարենք φ_{p_1} անցումը եւ հաշվենք $s_1(x) = t_1 \cdot z_1(x)$ արտադրյալը, որտեղ t_1-ն ընտրված է այնպես, որ $s_1(x)$-ի ավագ գործակիցը p_1 մոդուլով հավասար լինի w-ի: Մեկ պարզ թվից բաղկացած $\{p_1\}$ բազմության համար, հասկանալի է, կունենանք $n_1 = 1$ եւ $S(x) = S_{p_1}(x) = 1 \cdot s_{p_1}(x)$: Ապա հաշվենք $S_m(x)$ բազմանդամը եւ վերականգնենք $e \cdot d(x)$ բազմանդամը: Հաշվենք դրա $d(x) = \mathrm{pp}\big(e \cdot d(x)\big)$ պրիմիտիվ մասը: Ստուգենք՝ արդյոք $d(x)$-ն բաժանո՞ւմ է $f(x),\ g(x)$ բազմանդամները: Եթե այո, ապա վերջնական պատասխանն է $\big(f(x), g(x)\big) = d(x)$, քանի որ, ըստ 2.7.3 լեմմայի, պրիմիտիվ բազմանդամների ամենաբարձր աստիճանի ընդհանուր բաժանարարը նաեւ դրանց *ամենամեծ* ընդհանուր բաժանարարն է: Իսկ եթե $d(x) \nmid f(x)$ կամ $d(x) \nmid g(x)$, ապա վերցնենք մի այլ $p_2 \nmid w$ պարզ թիվ, կատարենք φ_{p_2} անցումը եւ հաշվենք $z_2(x)$-ը: Համեմատենք $\deg z_2(x)$ եւ $\deg z_1(x)$ աստիճանները: Հնարավոր են երեք դեպքեր.

ա. Եթե $\deg z_2(x) > \deg z_1(x)$, ապա p_2-ը այնպիսի մի մոդուլ է, ըստ որի հաշվելիս ստացվող $z_2(x)$ ամենամեծ ընդհանուր բաժանարարն «ավելի հեռու» է որոնելի $\big(f(x), g(x)\big)$ պատասխանից, քան $z_1(x)$-ը (այն իմաստով, որ դրա աստիճանն ավելի շատ է տարբերվում $\big(f(x), g(x)\big)$-ի աստիճանից): Ուղղակի անտեսենք p_2-ի այս արժեքը, եւ p_2-ի համար վերցնենք մի այլ պարզ արժեք:

բ. Եթե $\deg z_2(x) = \deg z_1(x)$, ապա ըստ $\{p_1, p_2\}$ զույգի կառուցենք վերը նշված օժանդակ $S(x) = S_{p_1,p_2}(x)$ բազմանդամը եւ հաշվենք $d(x) = \mathrm{pp}\big(e \cdot d(x)\big)$ պրիմիտիվ մասը: Եթե $f(x), g(x) \vdots d(x)$, ապա $\big(f(x), g(x)\big) = d(x)$, քանի որ $\deg d(x) = \deg S(x) = \deg z_2(x) \geq \deg\big(f(x), g(x)\big)$: Հակառակ դեպքում, պահպանելով p_1, p_2 արժեքները, վերցնենք եւս մի նոր $p_3 \nmid w$ պարզ թիվ, եւ կրկնենք քայլը դրա համար:

գ. Եթե $\deg z_2(x) < \deg z_1(x)$, ապա սա նշանակում է, որ մինչ այժմ մեր դիտարկած $z_1(x)$ բազմանդամն ավելի բարձր աստիճանի է եղել, քան $\big(f(x), g(x)\big)$-ը, եւ այժմ մեզ հաջողվել է գտնել մի p_2՝ ըստ որի հաշվելիս ստացվող $z_2(x)$ մոդուլյար ամենամեծ ընդհանուր բաժանարարն «ավելի մոտ» է որոնելի $\big(f(x), g(x)\big)$ պատասխանին, քան $z_1(x)$-ը: Այս դեպքում անտեսենք p_1-ի հին արժեքը, համարենք $p_1 = p_2$, եւ հաշվարկը վերսկսենք այս նոր p_1-ի համար:

5.3.7 Օրինակ. Կրկին դիտարկենք (5.16) բազմանդամները եւ մոդուլյար անցումն իրականացնենք ըստ $p_2 = 3$ արժեքի:

$$\begin{aligned} \varphi_3\big(f(x)\big) &= f_3(x) = x^3 + 2x, \\ \varphi_3\big(g(x)\big) &= g_3(x) = 2x^3 + 2: \end{aligned} \tag{5.18}$$

Հեշտ է հաշվել, որ $z_2(x) = 2x + 2$: Քանի որ ավագ գործակիցը 2 է, ունենք $t_2 = 4/2 = 2$: Եւ $s_2(x) = 2 \cdot z_2(x) = 4x + 4 \cong x + 1 (\mathrm{mod}\ 3)$: Քանի որ $\deg z_2(x) = \deg z_1(x)$, ապա ունենք քիչ առաջ բերված այլընտրանքի երկրորդ դեպքը եւ մենք $\{7, 3\}$ զույգի համար կարող ենք կառուցել այն օժանդակ բազմանդամները, որոնք սահմանվեցին քիչ առաջ: Դրանք հաշվելու համար մեզ պետք են այնպիսի n_1, n_2 թվեր, որ $n_1 \equiv 1 (\mathrm{mod}\ 7)$, $n_1 \equiv 0 (\mathrm{mod}\ 3)$ եւ $n_2 \equiv 0 (\mathrm{mod}\ 7)$, $n_2 \equiv 1 (\mathrm{mod}\ 3)$: Այդպիսի թվեր հեշտ է հաշվել ըստ 5.1.7 ալգորիթմի: Օրինակ՝ $n_1 = -6$ եւ $n_2 = 7$: Ունենք.

$$S_{7,3}(x) = n_1 \cdot s_1(x) + n_2 \cdot s_2(x) = -6(4x + 6) + 7(x + 1) = -17x - 29 \in \mathbb{Z}[x]$$

եւ $S_m(x) = S_{21}(x) = 4x + 13$: Քանի որ այս բազմանդամի երկրորդ գործակիցը մեծ է $m/2 = 21/2$ -ից, ապա $e \cdot d(x) = 4x + (13 - 21) = 4x - 8$: Սա պրիմիտիվ բազմանդամ չէ եւ $d(x) = \mathrm{pp}\big(e \cdot d(x)\big) = \mathrm{pp}(4x - 8) = x - 2$: Հեշտ է հաշվել, որ ստացված արդյունքը չի բաժանում, օրինակ, $f(x)$-ը: Ուստի $d(x)$ բազմանդամը դեռ չի վերականգնված:

Վերադառնանք ալգորիթմի կառուցման պրոցեսին: Պարզ թվերի ընտրությունը շարունակենք ինդուկցիայով. եթե $p_1, \dots, p_k$ պարզ թվերի համար քայլերն արդեն արված են, ապա ընտրենք մի նոր $p_{k+1} \nmid w$ պարզ թիվ, եւ քայլը կատարենք դրա համար: Ըստ բերված երեք այլընտրանքների՝ կամ p_{k+1}-ն պետք է դեն նետվի, կամ այն պիտի ավելացվի պարզ թվերի $p_1, \dots, p_k$ ցանկին (եւ մենք պետք է հաշվենք $d(x) = \mathrm{pp}\big(e \cdot d(x)\big)$ պրիմիտիվ մասն ու ստուգենք՝ արդյոք այն բաժանո՞ւմ է $f(x)$, $g(x)$ բազմանդամները), կամ էլ պետք է անտեսենք մինչ այժմ օգտագործված բոլոր $p_1, \dots, p_k$ թվերն, ու պրոցեսը նորից վերսկսենք $p_1 = p_{k+1}$ արժեքի համար:

Քանի որ w-ն չբաժանող պարզ թվերի քանակն անվերջ է, կարող ենք անվերջ շարունակել այս քայլերը: Ցույց տանք, որ վերջավոր քայլերից հետո այն արդեն կհանգեցնի որոնելի $\big(f(x), g(x)\big)$ պատասխանին:

Ինչպես ռեզուլտանտի հատկություններից օգտվելով ապացուցել ենք 3.4 պարագրաֆում, տրված $f(x)$, $g(x)$ բազմանդամների համար կան ընդամենը վերջավոր քանակությամբ p պարզ թվեր, որոնց համար $\big(f(x), g(x)\big)$ ամենամեծ ընդհանուր բաժանարարը տարբեր է $t \cdot \big(f_p(x), g_p(x)\big)$ մոդուլյար ամենամեծ ընդհանուր բաժանարարի այն նախապատկերից, որը կառուցվում է 3.2.8 ալգորիթմի միջոցով: Ուստի բավականաչափ մեծ $p_{k+1} \nmid w$ պարզ թվի համար մենք կունենանք

$$\deg z_{k+1}(x) = \deg\big(f(x), g(x)\big):$$

Այսինքն՝ վերը նշված այլընտրանքի երրորդ դեպքը միայն վերջավոր անգամ կարող է հանդիպել. մենք միայն մի քանի անգամ կարող է ստիպված լինենք վերսկսելու պրոցեսը $p_1 = p_{k+1}$ արժեքի համար, բայց վաղ թե ուշ կհասնենք $\deg\big(f(x), g(x)\big)$ արժեքին, որից ներքեւ այլեւս չենք իջնի, քանի որ $p_{k+1} \nmid w$: Իսկ եթե հաջորդ $p_{k+1} \nmid w$ արժեքն ավելացնելիս ունենանք այլընտրանքի առաջին դեպքը, ապա պարզապես անտեսենք այդ p_{k+1}-ը:

Համարենք, որ արդեն հասել ենք այնպիսի $P = \{p_1, \dots, p_k\}$ պարզ թվերի, որ հաջորդ $p_{k+1} \nmid w$ արժեքն ավելացնելիս ունենք այլընտրանքի միայն երկրորդ դեպքը, կամ էլ (վերջավոր անգամ) առաջին դեպքը, որը մեզ չի խանգարում համարել, որ $m = p_1 \cdots p_k$ արտադրյալն անվերջ աճում է: Վաղ թե ուշ կունենանք $m = p_1 \cdots p_k > 2 \cdot N = 2 \cdot E \cdot N_{f,g}$: Այդ դեպքում հաշվարկված $d(x) = \mathrm{pp}\big(e \cdot d(x)\big)$ պրիմիտիվ մասն անպայման հավասար է $f(x)$, $g(x)$ պրիմիտիվ բազմանդամների $\big(f(x), g(x)\big)$ ամենամեծ ընդհանուր բաժանարարին:

Իսկ կամայական $f(x)$, $g(x)$ բազմանդամների դեպքը կարելի է հեշտությամբ հանգեցնել նախորդ դեպքին այն մեթոդով, որ արդեն կիրառել ենք 3.4 պարագրաֆում: Բազմանդամները ներկայացնենք

$$f(x) = \mathrm{cont}\big(f(x)\big)\,\mathrm{pp}\big(f(x)\big), \qquad g(x) = \mathrm{cont}\big(g(x)\big)\,\mathrm{pp}\big(g(x)\big)$$

տեսքով եւ նշանակենք $r = \Big(\mathrm{cont}\big(f(x)\big),\ \mathrm{cont}\big(g(x)\big)\Big)$: Քանի որ այս բազմանդամների $\mathrm{cont}\big(f(x)\big)$ եւ $\mathrm{cont}\big(g(x)\big)$ բովանդակությունները որոշվում են նշանի ճշտությամբ, առանց ընդհանրությունը խախտելու համարենք, որ $\mathrm{pp}\big(f(x)\big)$, $\mathrm{pp}\big(g(x)\big)$ բազմանդամների ավագ գործակիցները *դրական են*: Դրանց $\Big(\mathrm{pp}\big(f(x)\big),\ \mathrm{pp}\big(g(x)\big)\Big)$ ամենամեծ ընդհանուր բաժանարարը կարելի է գտնել $d(x) = \mathrm{pp}\big(e \cdot d(x)\big)$ տեսքով,

եւ վերջնական պատասխանը (ըստ 2.6.8 Գաուսի լեմմայի եւ նրա 2.6.9 եւ 2.6.16 հետեւանքների) ստանալ որպես

$$\big(f(x),g(x)\big)=r\cdot\Big(\mathrm{pp}\big(f(x)\big),\mathrm{pp}\big(g(x)\big)\Big)=r\cdot\mathrm{pp}\big(e\cdot d(x)\big):$$

5.3.8 Դիտողություն. p_i պարզ թվերի ընտրության այս եղանակը ունի մի հավելյալ առավելություն: Այն մեզ թույլ է տալիս շրջանցել վերը կառուցված ալգորիթմի որոշ քայլեր: Մենք կարիք չունենք հաշվելու $N_{f,g}$ եւ E արժեքները: Կարիք չունենք նաեւ միանգամից դիտարկելու այնքան շատ $p_1,\dots,p_k$ պարզ թվեր, որոնց համար $m=p_1\cdots p_k>2\cdot N=2\cdot E\cdot N_{f,g}$: Իսկապես, ալգորիթմը աշխատում է նախ մեկ, ապա երկու, երեք, եւլն հատ պարզ թվերի հետ: Վերջնական ստույգ $r\cdot\mathrm{pp}\big(e\cdot d(x)\big)$ պատասխանը կարող է ստացվել անգամ նախքան $p_1\cdots p_k>2\cdot E\cdot N_{f,g}$ արժեքին հասնելը: Կոնկրետ խնդիրներում, որպես կանոն, հենց այդպես էլ ստացվում է:

Մենք արդեն պատրաստ ենք ձեւակերպելու ալգորիթմը, սակայն մինչ այդ պարզեցնենք դրա քայլերից եւս մեկը: Նկատենք, որ $S_{p_1,\dots,p_k,p_{k+1}}(x)$ բազմանդամը կառուցելիս կարիք չկա հաշվելու բոլոր $n_1,\dots,n_{k+1}$ թվերը, քանի որ $S_{p_1,\dots,p_k,p_{k+1}}(x)$ բազմանդամը հաշվելիս կարելի է օգտվել արդեն հաշվված $S_{p_1,\dots,p_k}(x)$ բազմանդամից: Իրոք, մնացքների մասին չինական թեորեմով գտնենք այնպիսի մի n_{k+1}, n^*_{k+1} թվազույգ, որ

$$n_{k+1}\equiv 1(\mathrm{mod}\,p_{k+1}),\ \ n_{k+1}\equiv 0(\mathrm{mod}\,p_1\cdots p_k),$$
$$n^*_{k+1}\equiv 0(\mathrm{mod}\,p_{k+1}),\ \ n^*_{k+1}\equiv 1(\mathrm{mod}\,p_1\cdots p_k)$$

եւ վերցնենք

$$S_{p_1,\dots,p_k,p_{k+1}}(x)=n^*_{k+1}\cdot S_{p_1,\dots,p_k}(x)+n_{k+1}\cdot s_{k+1}(x): \tag{5.19}$$

Հեշտ է ստուգել, որ

$$S_{p_1,\dots,p_k,p_{k+1}}(x)\equiv n_{k+1}\cdot s_{k+1}(x)\equiv s_{k+1}(x)(\mathrm{mod}\,p_{k+1}):$$

Իսկ երբ $i\in P=\{p_1,\dots,p_k\}$, ապա

$$S_{p_1,\dots,p_k,p_{k+1}}(x)\equiv n^*_{k+1}\cdot S_{p_1,\dots,p_k}(x)\equiv S_{p_1,\dots,p_k}(x)\equiv s_i(x)(\mathrm{mod}\,p_i):$$

Քանի որ հաջորդ՝ $S_m(x)$ օժանդակ բազմանդամի գործակիցները հաշվվում են ըստ $m=p_1,\dots,p_k,p_{k+1}$ մոդուլի, ապա այդ բազմանդամի հաշվման ժամանակ միեւնույն արդյունքը կստանանք ինչպես (5.15) բանաձեւով, այնպես էլ (5.19) բանաձեւով հաշվվող $S_{p_1,\dots,p_k,p_{k+1}}(x)$ բազմանդամն օգտագործելով: (5.19) բանաձեւի ալգորիթմական առավելություններն այն են, որ մնացքների մասին չինական թեորեմը կիրառվում է միայն երկու (այլ ոչ $k+1$ հատ) մոդուլների համար եւ, դրանից բացի,

նախորդ քայլում հաշվված $S_{p_1,\dots,p_k}(x)$ բազմանդամն օգտագործվում է հաջորդ քայլի $S_{p_1,\dots,p_k,p_{k+1}}(x)$ բազմանդամի կառուցման մեջ:

5.3.9 Դիտողություն. Ստորեւ ձեւակերպված 5.3.10 ալգորիթմում մենք օգտագործելու ենք $S_{p_1,\dots,p_k}(x)$ բազմանդամի կառուցման երկրորդ, ավելի կարճ եղանակը (5.19) բանաձեւի օգնությամբ: Սակայն ավելեի ուշ 5.3.14 օրինակում մենք կիրառելու ենք երկու եղանակներն էլ՝ դրանց տարբերությունը ցույց տալու համար:

Ձեւակերպենք մեր կառուցած ալգորիթմը.

5.3.10 Ալգորիթմ (ամենամեծ ընդհանուր բաժանարարի հաշվման փոքր պարզ թվերի մեթոդը). Տրված են $f(x),\ g(x) \in \mathbb{Z}[x]$ ոչ զրոյական բազմանդամները: Հաշվել նրանց $\big(f(x),\ g(x)\big)$ ամենամեծ ընդհանուր բաժանարարը:

1. $f(x),\ g(x)$ բազմանդամների համար Էվկլիդեսի ալգորիթմով հաշվենք նրանց $\operatorname{cont}\big(f(x)\big)$ եւ $\operatorname{cont}\big(g(x)\big)$ բովանդակությունները: Դրանց նշաններն ընտրենք այնպես, որ $f(x)/\operatorname{cont}\big(f(x)\big) = \operatorname{pp}\big(f(x)\big)$ եւ $g(x)/\operatorname{cont}\big(g(x)\big) = \operatorname{pp}\big(g(x)\big)$ հարաբերությունների ավագ գործակիցները դրական լինեն:

2. Էվկլիդեսի ալգորիթմով հաշվենք $r = \Big(\operatorname{cont}\big(f(x)\big),\ \operatorname{cont}\big(g(x)\big)\Big)$ ամենամեծ ընդհանուր բաժանարարը:

3. Նշանակենք $f(x) = \operatorname{pp}\big(f(x)\big)$ եւ $g(x) = \operatorname{pp}\big(g(x)\big)$:

4. a_0-ով նշանակենք $f(x)$-ի ավագ գործակիցը, b_0-ով նշանակենք $g(x)$-ի ավագ գործակիցը (դրանք դրական են ըստ մեր կառուցման):

5. Էվկլիդեսի ալգորիթմով հաշվենք $w = (a_0, b_0)$ դրական ամենամեծ ընդհանուր բաժանարարը:

6. Նշանակենք $k = 1$:

7. Նախորդ քայլերում չօգտագործված որեւէ $p_k \nmid w$ պարզ թվի համար սահմանենք $P = \{p_k\}$ բազմությունը:

8. φ_{p_k} մոդուլյար անցումն իրականացնենք ըստ p_k մոդուլի եւ հաշվենք $f(x), g(x) \in \mathbb{Z}[x]$ բազմանդամների $f_{p_k}(x),\ g_{p_k}(x) \in \mathbb{Z}_{p_k}[x]$ պատկերները:

9. $\mathbb{Z}_{p_k}[x]$ օղակում Էվկլիդեսի ալգորիթմով հաշվենք $z_k(x) = \Big(f_{p_k}(x),\ g_{p_k}(x)\Big)$ ամենամեծ ընդհանուր բաժանարարը:

10. m-ով նշանակենք P բազմության թվերի արտադրյալը:

11. t_k թիվն ընտրենք այնպես, որ $s_k(x) = t_k \cdot z_k(x)$ արտադրյալի ավագ գործակիցը p_k մոդուլով հավասար լինի w-ի:

12. Եթե P բազմությունը բաղկացած է միայն մեկ թվից

13. նշանակենք $S_P(x) = s_k(x)$;

14. այլապես

15. մնացքների մասին չինական թեորեմի միջոցով գտնենք այնպիսի մի n_k, n_k^* թվազույգ, որ $n_k \equiv 1 (\mathrm{mod}\, p_k)$, $n_k \equiv 0 (\mathrm{mod}\, m/p_k)$ եւ $n_k^* \equiv 0 (\mathrm{mod}\, p_k)$, $n_k^* \equiv 1 (\mathrm{mod}\, m/p_k)$;

16. կառուցենք $S_P(x) = n_k^* \cdot S_P(x) + n_k \cdot s_k(x)$ բազմանդամը:

17. Կառուցենք $S_m(x)$ բազմանդամը՝ $S_P(x)$-ի գործակիցներից յուրաքանչյուրը փոխարինելով m-ի վրա բաժանելիս ստացվող իր մնացորդով:

18. $S_m(x)$-ից ստանանք $e \cdot d(x)$ բազմանդամը. $S_m(x)$-ի գործակիցները հերթով համեմատենք $m/2$-ի հետ, եւ եթե գործակիցը մեծ է $m/2$-ից, ապա դրանից հանենք m:

19. Նշանակենք $d(x) = \mathrm{pp}\big(e \cdot d(x)\big)$:

20. Եթե $f(x) \vdots d(x)$ եւ $g(x) \vdots d(x)$

21. անցնենք ալգորիթմի 34-րդ քայլին:

22. Նշանակենք $D = \deg z_k(x)$:

23. Նշանակենք $k = k + 1$:

24. Վերցնենք նախորդ քայլերում չօգտագործված որեւէ $p_k \nmid w$ պարզ թիվ:

25. φ_{p_k} մոդուլյար անցումն իրականացնենք ըստ p_k մոդուլի եւ հաշվենք $f(x)$, $g(x) \in \mathbb{Z}[x]$ բազմանդամների $f_{p_k}(x)$, $g_{p_k}(x) \in \mathbb{Z}_{p_k}[x]$ պատկերները:

26. $\mathbb{Z}_{p_k}[x]$ օղակում Էվկլիդեսի ալգորիթմով հաշվենք $z_k(x) = \left(f_{p_k}(x),\ g_{p_k}(x)\right)$ ամենամեծ ընդհանուր բաժանարարը:

27. Եթե $\deg z_k(x) > D$

28. վերադառնանք ալգորիթմի 24-րդ քայլին;

29. այլապես, եթե $\deg z_k(x) = D$

30. p_k թիվն ավելացնենք P բազմությանը;

31. վերադառնանք ալգորիթմի 10-րդ քայլին;

32. այլապես

33. վերադառնանք ալգորիթմի 6-րդ քայլին:

34. Որոնելի ամենամեծ ընդհանուր բաժանարարը դուրս գրենք $r \cdot d(x)$ տեսքով:

5.3.11 Դիտողություն. Նկատենք, որ չնայած ամենամեծ ընդհանուր բաժանարարի հաշվման փոքր պարզ թվերի մեթոդն էապես ավելի երկար տեսական հիմնավորում պահանջեց, քան մեծ պարզ թվի մեթոդը 3.4 պարագրաֆում, այնուամենայնիվ, վերջնական ալգորիթմի քայլերն այստեղ էապես ավելի շատ կամ ավելի բարդ չեն, քան մեծ պարզ թվի մեթոդի քայլերը: Մենք հիմա ստիպված չենք հաշվել Լանդաու-Մինյոտի բանաձեւի սահմանները, եւ հաշվարկները տանում ենք շատ ավելի փոքր պարզ թվերով: Մյուս կողմից, այստեղ մենք ստիպված ենք ամեն քայլում կիրառել մնացքների մասին չինական թեորեմը: Փոքր պարզ թվերի 5.3.10 ալգորիթմն էապես ավելի արագ ալգորիթմ է, քան մեծ պարզ թվի 3.4.8 ալգորիթմը:

Քննարկենք կառուցված ալգորիթմը մի քանի օրինակների համար:

5.3.12 Օրինակ. Դիտարկենք Կնուտի օրինակում քննարկված (3.12) բազմանդամները, որոնց մենք անդրադարձանք նաեւ 3.4.9 օրինակում, որտեղ ստուգեցինք, որ 2 մոդուլով հաշվելիս $\varphi_2\big(f(x)\big) = f_2(x)$ եւ $\varphi_2\big(g(x)\big) = g_2(x)$ բազմանդամները փոխադարձաբար պարզ չեն: Այժմ վերցնենք $p_1 = 3$ (այն բաժանում է $f(x),\ g(x)$ բազմանդամների ավագ գործակիցներից միայն մեկը): Հեշտ է հաշվել, որ

$$\varphi_3\big(f(x)\big) = f_3(x) = x^8 + x^6 + 2x^2 + 2x + 1,$$
$$\varphi_3\big(g(x)\big) = g_3(x) = 2x^4 + 2x^2 \tag{5.20}$$

բազմանդամները փոխադարձաբար պարզ են: Այս օրինակում ալգորիթմը պատասխան է տալիս առաջին իսկ քայլից հետո. $\big(f(x), g(x)\big) = 1$: Այս դեպքում կարիք չեղավ քննարկել մեկից ավելի շատ պարզ թվեր: Դրանից բացի, հենց առաջին քայլում $z_1(x) = \big(f_{p_1}(x),\ g_{p_1}(x)\big)$-ի աստիճանը հավասար ստացվեց $\big(f(x), g(x)\big)$-ի աստիճանին (քանի որ այն զրոյական է), ուրեմն, հարկ չեղավ նաեւ այնպիսի պարզ մոդուլների հետ գործ ունենալ, որոնց պետք է անտեսեինք մեր հաշվարկներում:

5.3.13 Դիտողություն. 1.3 պարագրաֆում Կնուտի մոդուլյար մեթոդը կիրառելիս մենք օգտագործեցինք $p = 5$ մոդուլը: 5.3.12 օրինակը ցույց է տալիս, որ կարելի էր նույն արդյունքը ստանալ ըստ $p = 3$ մոդուլի (այն չի բաժանում $f(x)$-ի ավագ գոր-

ծակիցը՝ չնայած բաժանում է $g(x)$-ի ավագ գործակիցը): Այնուամենայնիվ, Կնուտի օրինակն ավելի հարմար էր դիտարկել $p = 5$ մոդուլի համար (ինչպես եւ Դ. Կնուտն է արել), քանի որ դրա նպատակն էր մոդուլյար մեթոդների կիրառության առավելությունների հնարավորինս պարզ օրինակ կառուցել: Իսկ $p = 3$ մոդուլը հավելյալ բացատրություններ է պահանջում՝ $g(x)$-ի ավագ գործակցի հետ կապված:

Քննարկենք ավելի բարդ օրինակ, որտեղ մեր ալգորիթմի բոլոր հիմնական քայլերն իսկապես հանդիպում են.

5.3.14 Օրինակ. Փոքր պարզ թվերի ալգորիթմով հաշվենք (5.16) բազմանդամների ամենամեծ ընդհանուր բաժանարարը (այդ բազմանդամները մենք արդեն քննարկել ենք 5.3.6 եւ 5.3.7 օրինակներում): Նախ, ինչպես 5.3.6 օրինակում, վերցնենք $p_1 = 7$: Այն չի բաժանում $f(x)$, $g(x)$ բազմանդամների ավագ գործակիցների $w = (28, 8) = 4$ ամենամեծ ընդհանուր բաժանարարը: 5.3.6 օրինակում հաշվել ենք, որ

$$z_1(x) = 5x + 4,\ s_1(x) = 4x + 6$$

եւ այդ դեպքում $\mathrm{pp}\big(e \cdot d(x)\big) = 2x + 3$: Հեշտ է ստուգել, որ $2x + 3 \nmid f(x)$, այսինքն՝ որոնելի $\big(f(x),\ g(x)\big)$ պատասխանը դեռ գտնված չէ:

$p_2 = 3$ դեպքը քննարկել ենք 5.3.7 օրինակում: Այս դեպքում

$$z_2(x) = 2x + 2,\ s_2(x) = x + 1 \ \text{ եւ } \ S_{7,3}(x) = -17x - 29:$$

Ինչպես տեսանք, այս դեպքում $\mathrm{pp}\big(e \cdot d(x)\big) = \mathrm{pp}(4x - 8) = x - 2$, որը չի բաժանում $f(x)$-ը: Ուստի պատասխանը դարձյալ չի գտնված:

Վերցնենք $p_3 = 5$ եւ էվկլիդեսի ալգորիթմով հաշվենք

$$z_3(x) = \big(f_5(x), g_5(x)\big) = (3x^3 + x^2 + 2x + 4, 3x^3 + 3x^2 + 3x + 3) = x^2 + 3x + 2:$$

Քանի որ $\deg z_3(x) = 2 > \deg z_2(x) = 1$, ապա $p_3 = 5$ արժեքը կարող ենք անտեսել մեր հաշվարկներում: Այն որոնելի $\big(f(x),\ g(x)\big)$ պատասխանից «շատ հեռու» մոդուլյար արժեք է պարունակում:

p_3-ի համար վերցնենք մի այլ արժեք, ասենք, $p_3 = 11$ եւ հաշվենք

$$z_3(x) = \big(f_{11}(x), g_{11}(x)\big) = (6x^3 + 7x^2 + 5x + 4, 8x^3 + x^2 + 9) = x + 3:$$

Վերցնելով $t_3 = 4$, ստանում ենք $s_3(x) = t_3 \cdot z_3(x) = 4x + 12 \cong 4x + 1 (\mathrm{mod}\ 11)$:

Օժանդակ $S_{7,3,11}(x)$ բազմանդամը հաշվենք մեր բերած եղանակներից երկուսով էլ (խնդիրներ լուծելիս կարելի է նախապատվությունը տալ երկրորդին, քանի որ այն ավելի կարճ է, բայց այս օրինակում, եղանակների համեմատության համար, կիրառում ենք երկուսն էլ. տես 5.3.9 դիտողությունը): Ըստ առաջին եղանակի՝ (5.15) բանաձեւի համար մեզ պետք են նոր n_1, n_2, n_3 թվեր այնպիսիք, որ

$$n_1 \equiv 1 (\mathrm{mod}\ 7), n_1 \equiv 0 (\mathrm{mod}\ 3), n_1 \equiv 0 (\mathrm{mod}\ 11),$$

$$n_2 \equiv 0 (\mathrm{mod}\ 7), n_2 \equiv 1 (\mathrm{mod}\ 3), n_2 \equiv 0 (\mathrm{mod}\ 11),$$

$$n_3 \equiv 0 (\mathrm{mod}\ 7), n_3 \equiv 0 (\mathrm{mod}\ 3), n_3 \equiv 1 (\mathrm{mod}\ 11):$$

Էվկլիդեսի ընդհանրացված ալգորիթմով հեշտ է հաշվել. $n_1 = 99$, $n_2 = -77$ եւ $n_3 = -21$: Այդ դեպքում

$$S_{7,3,11}(x) = 99(4x + 6) - 77(x + 1) - 21(4x + 1) = 235x + 496:$$

Իսկ ըստ երկրորդ եղանակի՝ $S_{7,3,11}(x)$-ի հաշվումը հանգեցնենք $S_{7,3}(x)$-ի հաշվմանը: (5.19) բանաձեւի համար մեզ պետք է n_3, n_3^* թվազույգ.

$$n_3 \equiv 1 (\mathrm{mod}\ 11), n_3 \equiv 0 (\mathrm{mod}\ 7 \cdot 3),$$

$$n_3^* \equiv 0 (\mathrm{mod}\ 11), n_3^* \equiv 1 (\mathrm{mod}\ 7 \cdot 3):$$

Հեշտ է հաշվել, օրինակ, $n_3 = -21$, $n_3^* = 22$:

$$S_{7,3,11}(x) = 22 \cdot S_{7,3} - 21 \cdot s_{11}(x) = 22(-17x - 29) - 21(4x + 1) = -458x - 659:$$

Օժանդակ $S_{7,3,11}(x)$ բազմանդամի համար ստացանք երկու տարբեր արժեքներ, որոնք, սակայն, բաղդատելի են ըստ $m = 3 \cdot 7 \cdot 11 = 231$ մոդուլի.

$$235x + 496 - (-458x - 659) = 693x + 1155 = 231(3x + 5) \vdots 231:$$

Ուրեմն, այդ երկու օժանդակ բազմանդամներից որն էլ վերցնենք, կստանանք միեւնույն $S_m(x)$ բազմանդամը.

$$S_m(x) = S_{231}(x) = 4x + 34:$$

Այնուհետեւ՝ $e \cdot d(x) = 4x + 34$, քանի որ $S_m(x)$ բազմանդամի երկու արմատներն էլ փոքր են $231/2 = 115.5$ արժեքից, եւ բացասական գործակիցների դեպքը չի հանդիպում: Հաշվենք

$$\mathrm{pp}\big(e \cdot d(x)\big) = \mathrm{pp}(4x + 34) = 2x + 17:$$

Հեշտ է ստուգել, որ $f(x),\ g(x) \vdots 2x + 17$:

Մնում է հիշել, որ $f(x)$, $g(x)$ բազմանդամները պրիմիտիվ են, ուստի դրանց համար $r = \big(\mathrm{cont}\big(f(x)\big),\ \mathrm{cont}\big(g(x)\big)\big) = (1,1) = 1$ արժեքը տրիվիալ է: Ստանում ենք խնդրի վերջնական պատասխանը.

$$\big(f(x), g(x)\big) = r \cdot d(x) = r \cdot \mathrm{pp}\big(e \cdot d(x)\big) = 1 \cdot \mathrm{pp}(4x + 34) = 2x + 17:$$

5.3.15 Խնդիր. Ստուգել, որ t_i արտադրիչների կիրառումն իսկապես անհրաժեշտ է (5.15) բանաձեւում: Դրա համար 5.3.14 օրինակում դիտարկվող բազմանդամների ամենամեծ ընդհանուր բաժանարարը հաշվել առանց t_i արտադրիչների եւ ցույց տալ, որ այդ դեպքում ալգորիթմը ճիշտ պատասխանի չի հանգեցնի:

5.3.16 Վարժություններ. Փոքր պարզ թվերի ալգորիթմով հաշվել հետեւյալ բազմանդամների զույգերի ամենամեծ ընդհանուր բաժանարարները.

1) $f(x) = x^2 + 3x + 2$ եւ $g(x) = x^2 + 4x + 3$;

2) $f(x) = 6x^4 + 2x^3 + 6x^2 - 4x - 2$ եւ $g(x) = 3x^2 + 7x + 2$;

3) $f(x) = 4x^4 + 6x^3 - 4x^2 - 9x - 3$ եւ $g(x) = 6x^4 + 6x^3 - 11x^2 - 9x + 3$:

5.3.17 Խնդիր. Նախորդ վարժության **(2)** կետի բազմանդամների ամենամեծ ընդհանուր բաժանարարը փոքր պարզ թվերի ալգորիթմով հաշվել պարզ թվերի երկու տարբեր հաջորդականությունների համար: Նախ, $p_1 = 5$, $p_2 = 7$, եւլն… Երկրորդ դեպքում վերցնել $p_1 = 7$, $p_2 = 11$, եւլն… Ո՞ր դեպքում է ավելի կարճ հաշվարկ ստացվել եւ ինչո՞ւ:

5.3.18 Վարժություններ. Փոքր պարզ թվերի ալգորիթմով հաշվել 3.4 պարագրաֆի 3.4.12 վարժությունների բազմանդամների ամենամեծ ընդհանուր բաժանարարները: Համեմատել ստացված հաշվարկների բարդությունը մեծ պարզ թվի ալգորիթմի միջոցով նույն բազմանդամների ամենամեծ ընդհանուր բաժանարարների հաշվման բարդության հետ:

5.3.19 Խնդիր. Քննարկել 5.3.8 դիտողության փաստարկը 5.3.12 եւ 5.3.14 օրինակների բազմանդամների համար: Ինչպիսի՞ն կլինեին E եւ $N_{f,g}$ գնահատականներն այդ դեպքերում: Առաջին կենտ պարզ թվերի $p_1, \dots, p_k$ հաջորդականությունն օգտագործելու դեպքում նվազագույնը ինչպիսի՞ k պիտի վերցնել այդ օրինակներից յուրա-

քանչյուրում, որ կատարվի $p_1 \cdots p_k > 2 \cdot E \cdot N_{f,g}$ պայմանը: Համեմատել դա 5.3.12 եւ 5.3.14 օրինակների հաշվարկի հետ, որտեղ մենք ունեինք $k = 1$ եւ $k = 4$:

Հետագայում մենք էլի առիթներ կունենանք առնչվելու ըստ մի քանի մոդուլների մոդուլյար անցումների հետ: Մասնավորապես, ինչպես նշեցինք այս գլխի ամենասկզբում, մնացքների մասին չինական թեորեմը կկիրառենք 7.3 պարագրաֆում բազմանդամների ֆակտորիզացիայի ալգորիթմի համար:

6 Ֆակտորիալ օղակներ եւ մի քանի փոփոխականների բազմանդամներ

6.1 Ֆակտորիալ օղակներ

Այս գլխի նպատակն է ներմուծել ֆակտորիալ օղակի հասկացությունը, եւ կառուցել ալգորիթմներ դրանց վրա տրված մի քանի փոփոխականների $f(x_1, \dots, x_n)$ բազմանդամների համար:

6.1.1 Սահմանում. R ամբողջության տիրույթը կոչվում է *ֆակտորիալ օղակ*, եթե նրա կամայական ոչ զրոյական $a \in R$ տարր կարելի է ներկայացնել

$$a = \varepsilon \cdot p_1 \cdots p_n \tag{6.1}$$

տեսքով, որտեղ $\varepsilon \in R^*$ տարրը հակադարձելի է, իսկ $p_1, \dots, p_n$ տարրերը պարզ են: Ընդ որում, այս ներկայացումը միակն է հետեւյալ իմաստով. եթե a տարրն ունի նաեւ $a = \nu \cdot q_1 \cdots q_m$ ներկայացումը, որտեղ $\nu \in R^*$, իսկ $q_1, \dots, q_m$ տարրերը պարզ են, ապա $m = n$, եւ (միգուցե արտադրիչների վերադասավորումից հետո) համապատասխան պարզ արտադրիչները ասոցացված են իրար.

$$p_1 \approx q_1, \dots, p_n \approx q_n:$$

Ֆակտորիզացիա ունեն նաեւ հակադարձելի տարրերը. նրանց համար պարզապես $n = 0$: Ֆակտորիալ օղակները երբեմն անվանում են նաեւ միարժեք վերլուծությամբ օղակներ:

6.1.2 Օրինակ. $\mathbb{Z}$ օղակը, ըստ թվաբանության հիմնական թեորեմի, ֆակտորիալ է: Նրա $a = 60$ տարրն ունի հետեւյալ վերլուծությունները (6.1) տեսքով.

$$60 = 1 \cdot 2 \cdot 2 \cdot 3 \cdot 5, \qquad 60 = (-1) \cdot 2 \cdot (-2) \cdot (-3) \cdot (-5):$$

Պարզ է, որ $1, -1 \in \mathbb{Z}^*$ եւ $2 \approx -2$, $3 \approx -3$, $5 \approx -5$: Ընդ որում, $\mathbb{Z}$ օղակում պարզ տարրեր են նաեւ $-2, -3, -5$ թվերը:

(6.1) տեսքի վերլուծությունն անվանում են a տարրի վերլուծություն պարզ արտադրիչների արտադրյալի կամ a տարրի *ֆակտորիզացիա*: Մենք հաճախ դիտարկելու ենք այնպիսի ֆակտորիզացիաներ, երբ (6.1) գրության մեջ ε հակադարձելի տարրը միավորն է: Այդ դեպքում $\varepsilon = 1$ արտադրիչը (6.1) տողում կարելի է բաց թողնել:

Բերենք այնպիսի ամբողջության տիրույթի օրինակ, որի որեւէ ոչ զրոյական տարր չի ներկայացվում պարզ արտադրիչների արտադրյալի տեսքով:

6.1.3 Օրինակ. Վերցնենք $\mathbb{Q}[x]$ օղակի հետեւյալ ենթաօղակը՝ $R = x\mathbb{Q}[x] + \mathbb{Z}$: Հեշտ է տեսնել, որ սա բաղկացած է այնպիսի բազմանդամներից, որոնց բոլոր գործակիցները, բացի վերջինից, ռացիոնալ են, իսկ վերջին գործակիցը (ազատ անդամը) ամբողջ թիվ է: Հեշտ է ստուգել նաեւ այն, որ R-ն ամբողջության տիրույթ է, եւ որ նրանում միակ հակադարձելի տարրերն են $1, -1 \in \mathbb{Z}$ թվերը: R օղակի $f(x)$ պարզ տարրը կարող է լինել միայն հետեւյալ տեսքի. $f(x) = p$ կամ $f(x) = -p$ (որտեղ p-ն որեւէ պարզ թիվ է) կամ էլ $f(x)$-ն այնպիսի մի բազմանդամ է, որը պարզ է $\mathbb{Q}[x]$ օղակում, եւ որի ազատ գործակիցը 1 է կամ -1: R օղակի x տարրը չի կարող գրվել պարզ արտադրիչների արտադրյալի տեսքով: Ենթադրենք հակառակը՝ $x = \varepsilon \cdot p_1(x) \cdots p_n(x)$: Համեմատելով այս արտադրյալի բազմանդամների աստիճանները՝ հեշտ է տեսնել, որ այս գրության մեջ մասնակցող պարզ արտադրիչներից միայն մեկն է, որ կարող է լինել առաջին աստիճանի (համարենք $p_1(x) = a_0x \pm 1$ բազմանդամը), իսկ մնացած բոլոր արտադրիչների աստիճանները զրոյական են ($p_i(x) = p_i$ որոշ p_i պարզ թվերի համար, երբ $i > 1$): Հեշտ է ստուգել, որ նման արտադրյալը կլինի մի բազմանդամ, որն անպայման կունենա ոչ զրոյական ազատ անդամ: Մնում է տեսնել, որ x տարրն ինքը պարզ չէ R օղակում: Այն կարելի է ներկայացնել $x = 2 \cdot (0{,}5\, x + 0\,)$ տեսքով: Ստուգենք, որ այս երկու արտադրիչներից ոչ մեկն ասոցացված չէ x-ին: 2 արտադրիչը չի կարող բաժանվել x-ի վրա, քանի որ ավելի ցածր աստիճան ունի: Մյուս կողմից, եթե R օղակում $0{,}5\, x \vdots x$, ապա, շնորհիվ ամբողջության տիրույթներում կրճատման կանոնի (տես 2.1.13 խնդիրը), $0{,}5 \in R$: Հակասություն:

Հաջորդ օրինակը ցույց է տալիս, որ եթե ամբողջության տիրույթում ամեն տարր նույնիսկ ներկայացվում է պարզ տարրերի արտադրյալի տեսքով, այդ ներկայացումը կարող է միակը չլինել:

6.1.4 Օրինակ. Վերցնենք կոմպլեքս թվերից բաղկացած

$$R = \{u + iv\sqrt{5} \mid u, v \in \mathbb{Z}\} \subseteq \mathbb{C}$$

օղակը: Հեշտ է ստուգել, որ սա, իրոք, օղակ եւ ամբողջության տիրույթ է հանդիսանում կոմպլեքս թվերի գումարման ու բազմապատկման նկատմամբ: Ցույց տանք, որ այն ֆակտորիալ օղակ չէ՝ չնայած նրանում կամայական տարր ներկայացվում է պարզ տարրերի արտադրյալի տեսքով: Ցանկացած $a = u + iv\sqrt{5}$ թվի համար դիտարկենք նրա մոդուլի քառակուսին. $|a|^2 = u^2 + v^2 \cdot 5$: Հաշվենք դրա արժեքները փոքր $u,\ v$ թվերի համար.

$|a|^2 = 0$, երբ $u,\ v = 0$,
$|a|^2 = 1$, երբ $u = \pm 1,\ v = 0$,
$|a|^2 = 4$, երբ $u = \pm 2,\ v = 0$,
$|a|^2 = 5$, երբ $u = 0,\ v = \pm 1$,
$|a|^2 \geq 6$, մնացած բոլոր $u,\ v$ արժեքների համար:

Ուրեմն՝ ոչ զրոյական $a \in R$ թվի մոդուլը կամ հավասար է 1-ի ($u = \pm 1,\ v = 0$ դեպքում), կամ էլ մեծ է 1-ից: Քանի որ բազմապատկման ժամանակ կոմպլեքս թվերի մոդուլները բազմապատկվում են, ապա պարզ է, որ $a = u + iv\sqrt{5}$ տեսքի թիվը հակադարձելի է միայն, երբ $a = 1$ կամ $a = -1$:

Եթե ոչ զրոյական a տարրն ունի $a = b \cdot c$ ներկայացումը, ապա կամ b, c տարրերից որեւէ մեկը հակադարձելի է, կամ էլ դրանք երկուսն էլ հակադարձելի չեն եւ միաժամանակ $|a| > |b|$ ու $|a| > |c|$, այսինքն՝ երկու ոչ հակադարձելի տարրերի արտադրյալի մոդուլը խիստ մեծ է արտադրիչների մոդուլներից: Սա հնարավորություն է տալիս ստանալու a տարրի ներկայացումը պարզ արտադրիչների արտադրյալի տեսքով: Իրոք՝ եթե, ենթադրենք, b-ն պարզ տարր չէ, ապա $b = b_1 \cdot b_2$, որտեղ

$$b_1, b_2 \notin R^* \quad \text{եւ} \quad |b| > |b_1|, \quad |b| > |b_2|:$$

Տեղադրենք $b = b_1 \cdot b_2$ արտադրյալը $a = b \cdot c$ ներկայացման մեջ: Շարունակելով այս պրոցեսը՝ մենք ամեն քայլում ստանում ենք խիստ ավելի փոքր մոդուլ ունեցող արտադրիչներ: Բայց, մյուս կողմից, բոլոր ոչ զրոյական $a \in R$ տարրերի մոդուլների քառակուսիները բնական թվեր են, եւ դրանք չեն կարող անվերջ նվազել: Ուստի որեւէ քայլում պրոցեսը կանգ կառնի. կստանանք $a = p_1 \cdots p_n$ ներկայացումը, որտեղ բոլոր $p_1, \dots, p_n$ տարրերը պարզ են:

Չնայած դրան՝ R օղակը ֆակտորիալ չէ, քանի որ պարզ արտադրիչների վերլուծությունը միակը չէ: $6 \in R$ թիվն այս օղակում ունի երկու ներկայացումներ. $6 = 2 \cdot 3$ եւ

$$6 = 1 + 5 = 1^2 - i^2 \cdot 5 = \big(1 + i\sqrt{5}\big)\big(1 - i\sqrt{5}\big):$$

Հեշտ է ստուգել, որ բոլոր $2,\ 3,\ 1+i\sqrt{5},\ 1-i\sqrt{5}$ արտադրիչներն էլ պարզ են (դիտարկե՛լ դրանց մոդուլների քառակուսիները): Բայց, ասենք, 2 արտադրիչը չի կարող ասոցացված լինել $1+i\sqrt{5}$ կամ $1-i\sqrt{5}$ արտադրիչներից որեւէ մեկին, քանի որ

$$\left|1+i\sqrt{5}\right| = \left|1-i\sqrt{5}\right| = \sqrt{6} \neq 2,$$

այնինչ, ասոցացված լինելու դեպքում դրանք պարտավոր էին իրարից տարբերվել մի հակադարձելի արտադրիչով, որի մոդուլը, ըստ մեր կառուցման, պետք է հավասար լիներ 1-ի:

2.2 պարագրաֆից մեզ ծանոթ է գլխավոր իդեալների օղակի հասկացությունը, որն օգնում է ամբողջ թվերի վրա կիրառվող *բաղդատման* հասկացությունն ընդհանրացնելու ընդհանուր օղակների վրա: Այսպիսով, մեզ հայտնի են անբողջության տիրույթների հետեւյալ երեք հիմնական տիպերը. *էվկլիդյան* օղակներ, *գլխավոր իդեալների* օղակներ եւ *ֆակտորիալ* օղակներ: Ցույց տանք, որ օղակների այս երեք տիպերը մեկը մյուսի մասնավոր դեպքեր են. յուրաքանչյուր էվկլիդյան օղակ գլխավոր իդեալների օղակ է, եւ կան գլխավոր իդեալների օղակներ, որոնք էվկլիդյան չեն: Իսկ յուրաքանչյուր գլխավոր իդեալների օղակ ֆակտորիալ օղակ է, եւ կան ֆակտորիալ օղակներ, որոնք գլխավոր իդեալների օղակ չեն: Ֆակտորիալ օղակները մինչ այժմ մեզ հանդիպած հատուկ ամբողջության տիրույթների ամենալայն դասն են:

Ըստ 2.5.8 թեորեմի, յուրաքանչյուր էվկլիդյան օղակ գլխավոր իդեալների օղակ է: Իսկ 2.5.10 օրինակի օղակը ցույց է տալիս, որ էվկլիդյան օղակների բազմությունը գլխավոր իդեալների օղակների բազմության սեփական ենթաբազմություն է:

Հաջորդ քայլի համար մեզ պետք կգան 2.5.11 լեմմայի եւ 2.5.12 հետեւանքի անալոգները ֆակտորիալ օղակների համար: Ֆակտորիալ օղակի սահմանումից հեշտ է ստանալ.

6.1.5 Լեմմա. *Եթե R ֆակտորիալ օղակի ոչ զրոյական a տարրի (6.1) ֆակտորիզացիան է $a = \varepsilon \cdot p_1 \cdots p_n$, եւ a-ն բաժանվում է $p \in R$ պարզ տարրի վրա, ապա $p \approx p_i$ որեւէ $i = 1, \ldots, n$ համար:*

Ապացույց: Ենթադրենք $a = bp$, բայց $p \not\approx p_i$ բոլոր $i = 1, \ldots, n$ համար: Քանի որ b-ն ոչ զրոյական է, այն նույնպես ունի ֆակտորիզացիա՝ $b = \nu \cdot q_1 \cdots q_m$: Ուրեմն՝ a-ն ունի $a = \nu \cdot q_1 \cdots q_m \cdot p$ ֆակտորիզացիան, որի p արտադրիչն ասոցացված չէ

$a = \varepsilon \cdot p_1 \cdots p_n$ ֆակտորիզացիայի արտադրիչներից ոչ մեկին: Սա հակասում է ֆակտորիզացիայի միակությանը, ըստ 6.1.1 սահմանման: ■

6.1.6 Հետեւանք. Եթե R ֆակտորիալ օղակի a, b տարրերի համար ունենք $a \cdot b \vdots p$, որտեղ p-ն պարզ է եւ a-ն չի բաժանվում p-ի վրա, ապա b-ն բաժանվում է p-ի վրա:

6.1.7 Հետեւանք. Եթե R ֆակտորիալ օղակի a, b, h տարրերի համար ունենք $a \cdot b \vdots h$ եւ $(a, h) = 1$, ապա $b \vdots h$:

Հետաքրքիր է նկատել, որ 6.1.6 եւ 6.1.7 հետեւանքները ֆակտորիալ օղակների համար պնդում են նույնը, ինչ 2.5.12 հետեւանքը եւ 2.5.11 լեմման՝ էվկլիդյան օղակների համար:

6.1.8 Թեորեմ. *Յուրաքանչյուր գլխավոր իդեալների օղակ ֆակտորիալ օղակ է:*

Ապացույց: Հեշտ է տեսնել, որ եթե R օղակի a, b տարրերով ծնված գլխավոր իդեալներն են $I_a = aR$ եւ $I_b = bR$, ապա $a \vdots b$ պայմանից բխում է, որ $I_a \subseteq I_b$: Ուստի, եթե օղակում գոյություն ունի այնպիսի $a_1, a_2, \dots, a_i, \dots$ տարրերի անվերջ հաջորդականություն, որոնցից յուրաքանչյուրը բաժանվում է իր հաջորդի վրա, ապա մենք կունենանք իրար մեջ ներդրված իդեալների մի անվերջ շարք.

$$I_{a_1} \subseteq I_{a_2} \subseteq \cdots \subseteq I_{a_i} \subseteq \cdots, \tag{6.2}$$

որտեղ $I_{a_i} = a_i R$: Այս իդեալների $I = \bigcup_{i=1}^{\infty} I_{a_i}$ միավորումը նույնպես իդեալ է: Իսկապես, եթե $b \in I$ եւ $r \in R$, ապա $br \in I$, քանի որ որեւէ n ինդեքսի համար $b \in I_{a_n}$ եւ $br \in I_{a_n}$, քանի որ I_{a_n}-ը իդեալ է: Քանի որ I-ն իդեալ է, այն նաեւ գլխավոր իդեալ է՝ $I = cR$ որեւէ $c \in I$ տարրի համար: Գոյություն ունի որեւէ n, որի համար $c \in I_{a_n}$: Այդ n համարից սկսած

$$I_{a_n} = I_{a_{n+1}} = I_{a_{n+2}} = \cdots = I = cR: \tag{6.3}$$

Վերցնենք կամայական ոչ զրոյական, ոչ հակադարձելի $a \in R$ տարր եւ ստանանք նրա միակ ֆակտորիզացիան: Եթե a-ն պարզ չէ, ապա այն կարելի է ներկայացնել a-ին չասոցացված տարրերի $a = a_1 \cdot b_1$ արտադրյալի տեսքով: Եթե, ասենք, a_1-ը նույնպես պարզ չէ, այն կարելի է ներկայացնել $a_1 = a_2 \cdot b_2$ արտադրյալի տեսքով: Այս քայլը կարելի է կրկնել արտադրյալներում հանդիպող բոլոր բաղադրյալ տարրերի համար: Կամ այս պրոցեսը մի քայլում կանգ կառնի (եւ մենք կունենանք a-ի ներկայացում պարզ տարրերի արտադրյալի տեսքով), կամ էլ այն կշարունակվի անվերջ, եւ մենք կստանանք այս ապացույցի սկզբում բերված $a_1, a_2, \dots, a_i, \dots$ անվերջ հաջորդականությունը:

Երկրորդ դեպքում մենք կստանանք իրար մեջ ներդրված իդեալների (6.2) շարքը, որն, ինչպես տեսանք (6.3) տողում, դադարում է աճել որեւէ n համարից սկսած:

Բայց եթե $a_nR = a_{n+1}R$, ապա $a_n \vdots a_{n+1}$ եւ $a_{n+1} \vdots a_n$, այսինքն, $a_n \approx a_{n+1}$, մինչդեռ ամեն քայլում մենք ընտրել էինք այնպիսի բաժանարար, որն ասոցացված չէ համապատասխան բաժանելուն: Այս հակասությունը նշանակում է, որ գլխավոր իդեալների օղակում յուրաքանչյուր ոչ զրոյական, ոչ հակադարձելի a տարրի բաղադրյալ արտադրիչները (եթե դրանք կան) կամայական ձեւով (1-ին չասոցացված) արտադրիչների վերլուծելով, եւ ապա այս քայլն այդ արտադրիչների համար կրկնելով՝ մենք պրոցեսն անվերջ շարունակել չենք կարող, եւ ինչ-որ քայլում կստանանք a-ի ներկայացումը պարզ արտադրիչների արտադրյալի տեսքով.

$$a = p_1 \cdots p_n: \tag{6.4}$$

Մնում է ցույց տալ այս ներկայացման միակությունը 6.1.1 սահմանման իմաստով (կարելի է համարել, որ (6.4) տողում ունենք $\varepsilon = 1$): Ենթադրենք a-ն ունի նաեւ

$$a = \nu \cdot q_1 \cdots q_m \tag{6.5}$$

ներկայացումը, որտեղ $\nu \in R^*$, իսկ $q_1, \dots, q_m$ տարրերը պարզ են: Ենթադրենք p_1-ը չի բաժանվում q_1-ի վրա: Քանի որ $J = p_1R + q_1R$ ենթաբազմությունն իդեալ է, այն գլխավոր իդեալ է՝ $J = cR$: Քանի որ c-ի վրա բաժանվում են միաժամանակ p_1, q_1 տարրերը, $c \approx 1$ եւ $J = R$: Ուստի ինչ-որ u, v տարրերի համար $p_1u + q_1v = 1$: Ուստի

$$p_1 \cdot p_2 \cdots p_n \cdot u + q_1v \cdot p_2 \cdots p_n = p_2 \cdots p_n$$

եւ, ուրեմն, $p_2 \cdots p_n \vdots q_1$: Կրկնելով սա՝ ի վերջո կգտնենք մի p_i տարր, որը բաժանվում է q_1-ի վրա, այսինքն, $p_1 \approx q_1$: (6.4) եւ (6.5) ներկայացումների աջ մասերը կրճատենք q_1-ի վրա: Մի քանի անգամ կրկնելով այս քայլեր կստանանք որոնելի միակությունը: ■

Մնում է բերել այնպիսի մի ֆակտորիալ օղակի օրինակ, որը գլխավոր իդեալների օղակ չէ:

6.1.9 Օրինակ. Այն փաստը, որ $\mathbb{Z}[x]$ օղակը ֆակտորիալ օղակ է, բխում է 2.6.13 թեորեմից: $f(x) \in \mathbb{Z}[x]$ բազմանդամի ֆակտորիզացիան (2.17) ներկայացումն է. պարզ ամբողջ թվերը եւ պարզ պրիմիտիվ բազմանդամները $\mathbb{Z}[x]$ օղակի պարզ տարրերն են, եւ այդ օղակում (2.17)-ը համընկնում է (6.1) ֆակտորիզացիայի հետ: $\mathbb{Z}[x]$-ը գլխավոր իդեալների օղակ չէ. ցույց տանք, որ նրա այն I իդեալը, որը ծնվում է $\{x, 2\}$ տարրերով, գլխավոր իդեալ չէ: Իսկապես, ենթադրենք որեւէ $f(x) \in \mathbb{Z}[x]$ բազմանդամի համար $I = f(x)\mathbb{Z}[x]$: Քանի որ $2 \in I$, ապա $2 = f(x) \cdot g(x)$ որեւէ $g(x)$ բազմանդամի համար: Սա հնարավոր է միայն, երբ $f(x) \approx 2$ կամ $f(x) \approx 1$: Առաջին դեպքն անհնար է, քանի որ այդ դեպքում I-ի բոլոր բազմանդամները

կբաժանվեին 2-ի, մինչդեռ $x \in I$ բազմանդամն այդ պայմանին չի բավարարում: Իսկ եթե $f(x) \approx 1$, ապա $I = \mathbb{Z}[x]$: Իսկ սա հնարավոր չէ, քանի որ $1 \notin I$: Հետաքրքիր է համեմատել 6.1.9 օրինակը 2.5.9 օրինակի հետ, որտեղ տեսանք, որ $\mathbb{Z}[x]$ օղակն էվկլիդյան չէ: Տես նաեւ 6.3.12 օրինակը:

Ըստ 2.1.22 սահմանման, ոչ զրոյական, ոչ հակադարձելի p տարրը կոչվում է պարզ տարր (կամ չբերվող տարր, անվերլուծելի տարր), եթե կամայական $p = b \cdot c$ ներկայացումից բխում է, որ $b \approx 1$ կամ $c \approx 1$: Իսկ «չբերվող տարր» եւ «անվերլուծելի տարր» տերմիններն օգտագործվում են որպես «պարզ տարր» տերմինի հոմանիշներ: Մյուս կողմից, ըստ 6.1.6 հետեւանքի, R ֆակտորիալ օղակում պարզ տարրը կարող է սահմանվել նաեւ այսպես. *ոչ զրոյական, ոչ հակադարձելի p տարրը կոչվում է պարզ տարր, եթե կամայական $a, b \in R$ տարրերի համար $a \cdot b \vdots p$ պայմանից բխում է, որ $a \vdots p$ կամ $b \vdots p$*: Ավելի վաղ 2.5.12 հետեւանքում նույն օրինաչափությունը նկատել էինք էվկլիդյան օղակների համար: Ասվածից, սակայն, չի բխում, թե ընդհանրապես բոլոր օղակներում տարրի պարզությունը համարժեք է վերը բերված պայմանին: Ցույց տանք դա հետեւյալ օրինակով.

6.1.10 Օրինակ. Ոչ ֆակտորիալ օղակ մենք արդեն կառուցել ենք 6.1.4 օրինակում՝ $R = \{u + iv\sqrt{5} \mid u, v \in \mathbb{Z}\} \subseteq \mathbb{C}$: Եթե վերցնենք $a = 2 + i\sqrt{5}$ եւ $b = 2 - i\sqrt{5}$, ապա

$$ab = \left(2 + i\sqrt{5}\right)\left(2 - i\sqrt{5}\right) = 4 - i^2 5 = 9:$$

$9 \vdots 3$, բայց $2 + i\sqrt{5}$ եւ $2 - i\sqrt{5}$ թվերից ոչ մեկը չի բաժանվում $p = 3$ պարզ թվի վրա: Այսինքն՝ 6.1.6 հետեւանքի օրինաչափությունը կարող է եւ խախտվել ոչ ֆակտորիալ օղակներում:

Քանի որ դաշտի վրա բազմանդամային օղակները էվկլիդյան են, ապա ստանում ենք ֆակտորիալ օղակների եւս մի դաս.

6.1.11 Հետեւանք. *Յանկացած R դաշտի վրա տրված $R[x]$ բազմանդամային օղակը ֆակտորիալ օղակ է:*

Այսինքն՝ ֆակտորիալ օղակներ են $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$ օղակները: Քանի որ, ըստ մնացքների օղակների մասին 2.1.26 թեորեմի, $\mathbb{Z}_p$-ն նույնպես դաշտ է, ապա ստանում ենք ֆակտորիալ օղակի եւս մի օրինակ, որը ներկայացնենք առանձին հետեւանքի տեսքով, քանի որ հետագայում հղումներ ենք անելու այս փաստի վրա.

6.1.12 Հետեւանք. *Յանկացած p պարզ թվի համար $\mathbb{Z}_p[x]$ բազմանդամային օղակը ֆակտորիալ օղակ է:*

Հետագայում մենք կստանանք վերջին երկու հետեւանքների ընդհանրացումը 6.3.8 թեորեմում. R-ի վրա դրվող պայմանը կարելի է թուլացնել: Այն կարող է լինել ոչ թե դաշտ, այլ կամայական ֆակտորիալ օղակ:

R ֆակտորիալ օղակի a ոչ զրոյական տարրի $a = \varepsilon \cdot p_1 \cdots p_n$ ֆակտորիզացիայում կարող են մասնակցել իրար ասոցացված տարրեր: Եթե այդպիսիք կան, ապա կարելի է դրանք իրար միացնել եւ գրել որպես պարզ տարրի աստիճան՝ անհրաժեշտության դեպքում փոխելով ε արտադրիչը (եթե միացվող ասոցացված տարրերն իրար հավասար չեն): Կստանանք.

$$a = \nu \cdot p_1^{\alpha_1} \cdots p_m^{\alpha_m}, \tag{6.6}$$

որտեղ $p_1, \dots, p_n$ տարրերն արդեն զույգ առ զույգ ասոցացված չեն, $\alpha_1, \dots, \alpha_m \in \mathbb{N}$ եւ $\nu \in R^*$:

6.1.13 Օրինակ. 6.1.2 օրինակում բերված ֆակտորիզացիաները կարող են գրվել հետեւյալ կերպ

$$60 = 1 \cdot 2 \cdot 2 \cdot 3 \cdot 5 = 1 \cdot 2^2 \cdot 3 \cdot 5 = 2^2 \cdot 3 \cdot 5,$$
$$60 = (-1) \cdot 2 \cdot (-2) \cdot (-3) \cdot (-5) = 1 \cdot 2^2 \cdot (-3) \cdot (-5) = 2^2 \cdot (-3) \cdot (-5):$$

Երկրորդ տողում 2 եւ -2 իրար ասոցացված պարզ տարրերի միացումից հետո մենք -1 հակադարձելի տարրը ստիպված էինք փոխարինել 1 հակադարձելի տարրով:

6.1.14 Թեորեմ. *R ֆակտորիալ օղակի կամայական ոչ զրոյական a, b տարրերի համար R-ում գոյություն ունի նրանց (a, b) ամենամեծ ընդհանուր բաժանարարը եւ $[a, b]$ ամենափոքր ընդհանուր բազմապատիկը: Դրանք որոշվում են հակադարձելի տարրի ճշտությամբ:*

Ապացույց: Ենթադրենք a տարրը ասոցացված պարզ արտադրիչների միացումից հետո ունի (6.6) ֆակտորիզացիան, իսկ b տարրը՝

$$b = \nu' \cdot p_1^{\alpha'_1} \cdots p_m^{\alpha'_m} \tag{6.7}$$

ֆակտորիզացիան: Նկատենք, որ (6.6) եւ (6.7) ֆակտորիզացիաների մեջ մենք օգտագործել ենք միեւնույն $p_1, \dots, p_m$ պարզ տարրերը, քանի որ, (6.6) եւ (6.7) ներկայացումների մեջ կարող ենք ավելացնել «պակասող» պարզ տարրերը՝ զրոյական աստիճաններով: Հեշտ է ստուգել, որ

$$(a, b) = \kappa \cdot p_1^{\gamma_1} \cdots p_m^{\gamma_m} \cdot, \tag{6.8}$$

որտեղ $\kappa \in R^*$, $\gamma_i = \min\{\alpha_i, \alpha'_i\}$ $(i = 1, \dots, m)$: Իրոք, այդ արտադրյալը բաժանում է a, b տարրերը: Մյուս կողմից, եթե այդ տարրերն ունեն որեւէ c ընդհանուր բաժա-

նարար, ապա ֆակտորիզացիայի միակությունից բխում է, որ c-ի պարզ արտադրիչները պետք է ասոցացված լինեն $p_1, \dots, p_m$ պարզ տարրերից որոշներին (տես նաեւ 6.1.5 լեմման): Ընդ որում, պարզ արտադրիչները c-ի ներկայացման մեջ չեն կարող մասնակցել γ_i արժեքները գերազանցող աստիճաններով, քանի որ դա կբերեր a-ի (կամ b-ի) ֆակտորիզացիայի միակության խախտմանը:

Նույն կերպ՝

(6.9) $$[a, b] = \theta \cdot p_1^{\rho_1} \cdots p_m^{\rho_m} \cdot,$$

որտեղ $\theta \in R^*$, $\rho_i = \max\{\alpha_i, \alpha_i'\}$ $(i = 1, \dots, m)$: ■

6.1.15 Հետեւանք. R ֆակտորիալ օղակի կամայական ոչ զրոյական a, b տարրերի համար $(a, b)[a, b] = a \cdot b$:

6.1.16 Դիտողություն. Նկատենք, որ 6.1.14 թեորեմն ապահովում է ֆակտորիալ օղակում կամայական ոչ զրոյական տարրերի ամենամեծ ընդհանուր բաժանարարի գոյությունը, ինչպես Էվկլիդեսի ալգորիթմը՝ Էվկլիդյան օղակներում: Բայց, ի տարբերություն Էվկլիդեսի ալգորիթմի, 6.1.14 թեորեմը ամենամեծ ընդհանուր բաժանարարի (եւ ամենափոքր ընդհանուր բազմապատիկի) հաշվման էֆեկտիվ եղանակ չէ, քանի որ թեորեմը կիրառելու համար պահանջվում են (6.6) եւ (6.7) ֆակտորիզացիաները: Մինչդեռ տարրերի ֆակտորիզացիաները գտնելը շատ ավելի բարդ խնդիր է, քան դրանց ամենամեծ ընդհանուր բաժանարարը: Օրինակ, չնայած այն բանին, որ $\mathbb{Z}[x]$ օղակը ֆակտորիալ է (տես 6.1.9 օրինակը), մենք 3-րդ գլխում բավական շատ բարդություններ հաղթահարեցինք՝ այդ օղակում ամենամեծ ընդհանուր բաժանարարը հաշվելու ալգորիթմներ գտնելու համար (ի տարբերություն, ասենք, $\mathbb{Z}_p[x]$ Էվկլիդյան օղակի, որտեղ ֆակտորիզացիայի թե գոյությունը եւ թե բացահայտ տեսքը միանգամից ստացվում են Էվկլիդեսի ալգորիթմով):

6.2 Մի քանի փոփոխականների բազմանդամներ

Մի քանի փոփոխականների բազմանդամներին մենք արդեն անդրադարձել ենք 4.2 պարագրաֆում: Այս գլխում մեզ անհրաժեշտ են լինելու դրանց երկու տարբեր մեկնաբանություններ: Սկսենք այն մեկնաբանությունից, որն ավելի մոտ է սովորական (մեկ փոփոխականի) բազմանդամների ձեւական սահմանմանը:

Վերցնենք որեւէ R ամբողջության տիրույթ եւ R-ին չպատկանող, տարբեր $x_1, \dots, x_n$ սիմվոլների (դրանց անվանենք *փոփոխականներ*) կարգավորված n-յակը: R-ի վրա $x_1, \dots, x_n$ փոփոխականների *միանդամ* է կոչվում

$$a_{k_1,\dots,k_n} x_1^{k_1} \cdots x_n^{k_n} \tag{6.10}$$

տեսքի ձեւական (ֆորմալ) արտահայտությունը, որտեղ $k_1, \dots, k_n$ *աստիճանները* կամայական ոչ բացասական ամբողջ թվեր են, իսկ $a_{k_1,\dots,k_n}$ *գործակիցը* R օղակի կամայական տարր է: (6.10) միանդամի համար նրա աստիճանների $\alpha = (k_1, \dots, k_n)$ կարգավորված n-յակը կոչվում է նրա *աստիճանային վեկտոր*: Երբեմն ընդունված է (6.10) միանդամը նշանակել $a_\alpha x^\alpha$. մենք այս նշանակումը կօգտագործենք 8-րդ գլխում:

R-ի վրա $x_1, \dots, x_n$ փոփոխականների *բազմանդամ* է կոչվում (6.10) տեսքի միանդամներց կազմված հետեւյալ ձեւական գումարը

$$f(x_1, \dots, x_n) = \sum_{(k_1,\dots,k_n)\in S} a_{k_1,\dots,k_n} x_1^{k_1} \cdots x_n^{k_n}, \tag{6.11}$$

որտեղ S-ը $(k_1, \dots, k_n)$ տեսքի աստիճանային վեկտորների մի վերջավոր բազմություն է: Եթե կարիք չկա հիշատակելու $x_1, \dots, x_n$ փոփոխականները, ապա (6.11)-ը կոչվում է n *փոփոխականների բազմանդամ* կամ էլ պարզապես *բազմանդամ*: (6.11) տեսքի բոլոր n փոփոխականների բազմանդամների բազմությունը նշանակենք $R[x_1, \dots, x_n]$:

n փոփոխականների բազմանդամների համար, ի տարբերություն սովորական բազմանդամների, սահմանվում են երկու տիպի deg ֆունկցիաներ՝ ըստ առանձին փոփոխականի եւ ըստ բոլոր փոփոխականների: (6.11) միանդամի x_i-*աստիճանը* սահմանվում է $\deg_{x_i}\left(a_{k_1,\dots,k_n} x_1^{k_1} \cdots x_i^{k_i} \cdots x_n^{k_n}\right) = k_i$ կանոնով: Իսկ ըստ բոլոր փոփոխականների աստիճանը սահմանվում է $\deg\left(a_{k_1,\dots,k_n} x_1^{k_1} \cdots x_n^{k_n}\right) = k_1 + \cdots + k_n$ կանոնով: Նույն կերպ $f(x_1, \dots, x_n)$ բազմանդամի x_i-*աստիճանը*՝ $\deg_{x_i} f(x_1, \dots, x_n)$ սահմանվում է որպես նրա բոլոր միանդամների x_i-աստիճաններից ամենամեծը: Իսկ $\deg f(x_1, \dots, x_n)$ աստիճանը սահմանվում է որպես նրա բոլոր միանդամների $\deg\left(a_{k_1,\dots,k_n} x_1^{k_1} \cdots x_n^{k_n}\right)$ աստիճաններից ամենամեծը: Հասկանալի է, որ բազմանդամի երկու միանդամներ չեն կարող ունենալ հավասար աստիճանային վեկտորներ, քանի որ S-ը բազմություն է եւ չի կարող պարունակել հավասար տարրեր: Մենք կասենք, որ երկու միանդամներ *ունեն միեւնույն աստիճանները*, եթե նրանք ունեն միեւնույն աստիճանային վեկտորը կամ, որ նույնն է, նրանց x_i-աստիճանները համընկնում են բոլոր x_i, $i = 1, \dots, n$ փոփոխականների համար:

Եթե (6.10) միանդամում x_i փոփոխականը մասնակցում է $k_i = 1$ աստիճանով, ապա համառոտության համար պայմանավորվենք x_i^1-ի փոխարեն գրել x_i: Եթե x_i-ն մասնակցում է $k_i = 0$ աստիճանով, ապա պայմանավորվենք միանդամի գրության մեջ x_i^0-ն բաց թողնել: Իսկ եթե $\deg\left(a_{k_1,\dots,k_n}x_1^{k_1}\cdots x_n^{k_n}\right) = 0$, ապա այդ միանդամը հավասար համարենք իր $a_{0,\dots,0} \in R$ գործակցին: Դրանից բացի, պայմանավորվենք $0 \in R$ զրոյին հավասար համարել այն միանդամները, որոնց գործակիցը զրոյական է: Այդպիսի միանդամները պայմանավորվենք բաց թողնել բազմանդամի գրությունից, եթե, իհարկե, բազմանդամը միայն մեկ (զրոյական) միանդամից չի բաղկացած: Եթե (6.10) միանդամի աստիճանը զրո չէ եւ $a_{k_1,\dots,k_n} = 1$, ապա այդ գործակիցը նույնպես բաց թողնենք միանդամի գրությունից: Այս պայմանավորվածությունները միայն գրառման համառոտություն չէ, որ նշանակում են (տես 6.2.1 օրինակները): Եթե կամայական երկու բազմանդամ համարենք հավասար այն եւ միայն այն դեպքում, երբ դրանցից՝ նշված գործողությունների կատարումից հետո նույն արտահայտությունն է ստացվում, ապա $R[x_1, \dots, x_n]$-ի վրա սահմանած կլինենք, ինչպես դժվար չէ ստուգել, բազմանդամների *համարժեքության* հարաբերություն: Հետագա կառուցումները տանելով այս հավասարության ճշտությամբ՝ մենք ոչ միայն ավելի համառոտ գրառումներ կունենանք, այլեւ զերծ կլինենք հետեւյալ տիպի հարցերից՝ արդյոք իրար հավասա՞ր են $0x_1^2x_2$, $0x_1x_2^2$ եւ 0 բազմանդամները, կամ՝ $1x_1x_2$ եւ x_1x_2 բազմանդամները կամ էլ՝ $2x_1^0x_2^0$, $2x_1^0$ եւ 2 բազմանդամները: Նշանակումները չբարդացնելու համար պայմանավորվենք նույն $f(x_1, \dots, x_n)$ սիմվոլով նշանակել նաեւ $R[x_1, \dots, x_n]$-ի համապատասխան դասը՝ ըստ այդ համարժեքության, իսկ $R[x_1, \dots, x_n]$-ը նույնացնենք համարժեքության դասերի բազմության հետ: Մասնավորապես, 0, x_1x_2, 2 տեսքի նշանակումները $R[x_1, x_2]$-ում համարենք (6.10) տեսքի միանդամների համառոտ գրություններ:

6.2.1 Օրինակներ. $\mathbb{Z}[x_1, \dots, x_4]$-ում տեղի ունեն հետեւյալ հավասարությունները.

ա. $f(x_1, \dots, x_4) = 2x_1^3x_2^0x_3^0x_4^2 + 5x_1^0x_2^0x_3^0x_4^0 = 2x_1^3x_4^2 + 5$,

բ. $f(x_1, \dots, x_4) = 2x_1^3x_4^1 + 0x_2^4x_3^1 + 0x_1^7x_3^2 = 2x_1^3x_4 + 0 + 0 = 2x_1^3x_4$,

գ. $f(x_1, \dots, x_4) = 0x_1^5x_3^2x_4^2 + 7x_1^0x_2^0x_3^0x_4^0 = 0 + 7 = 7$:

Երբ դիտարկվող փոփոխականների քանակը փոքր է, ավելի հարմար է դրանք նշանակել ոչ թե $x_1, x_2, x_3, \dots$, այլ $x, y, z, \dots$: Ըստ այդմ՝ դիտարկվում են, ասենք, $\deg_x 2x^3y^7$, $\deg_y f(x, y)$-ը եւլն: Գրության համառոտության համար երբեմն $f(x_1, \dots, x_n)$ բազմանդամը կնշանակենք միայն f տառով:

6.2.2 Օրինակներ. $R = \mathbb{Z}$ օղակի վրա դիտարկենք երկու փոփոխականների $f(x, y) = 2x^2y^4 + 6x^5 - 4x^3y + 3xy^4 + 5y^7 + 2y^4 + 2y + 7 \in \mathbb{Z}[x, y]$ բազմանդամը: Այստեղ $a_{2,4} = 2$, $a_{5,0} = 6$ եւլն: Պարզ է, որ $\deg_x(2x^2y^4) = 2$, $\deg_y(2x^2y^4) = 4$,

$\deg_x(6x^5) = \deg_x f(x,y) = 5$ եւ $\deg_y(5y^7) = \deg_y f(x,y) = 7$: Պարզ է նաեւ, որ $\deg_x(5y^7) = \deg_x(7) = \deg_y(7) = 0$ եւ $\deg f(x,y) = \deg(5y^7) = 7 > \deg(2x^2y^4) = 6$:

Նկատենք, որ մի քանի փոփոխականների բազմանդամների համար բացակայում է ավագ անդամի հասկացությունը, քանի որ տարբեր միանդամներ կարող են ունենալ միեւնույն deg աստիճանը: Օրինակ՝ $f(x,y) = 5x^3y^4 + 6x^7 - 4xy^6 + x$ բազմանդամի առաջին երեք միանդամների աստիճաններն էլ հավասար են 7-ի: *Ըստ x_i փոփոխականի* $f(x_1, \dots, x_n)$ *բազմանդամի ավագ անդամ* է կոչվում նրա այն միանդամը, որի x_i-աստիճանը հավասար է $\deg_{x_i} f$-ին: Մեկ փոփոխականի բազմանդամների համար դա համընկնում է սովորական իմաստով ավագ անդամի հասկացությանը, եւ մենք կարող ենք կարգավորել միանդամները ըստ աստիճանի: Սա է պատճառը, թե ինչու մեկ փոփոխականի բազմանդամների օղակում ավելի հարմար է գրառումը սկսել ավագ անդամից, եւ նրա գործակիցն անվանել ոչ թե a_n, այլ a_0, այսինքն, $f(x) = a_0x^n + \dots + a_n$:

$R[x_1, \dots, x_n]$-ն կարելի է վերածել օղակի, եթե նրա վրա սահմանենք տարրերի գումարման ու բազմապատկման գործողություններ: Դրանք, նախ, սահմանվում են միանդամների վրա: Եթե $a_{k_1,\dots,k_n}x_1^{k_1}\cdots x_n^{k_n}$ եւ $b_{k_1,\dots,k_n}x_1^{k_1}\cdots x_n^{k_n}$ միանդամները ունեն միեւնույն աստիճանները, ապա դրանց գումարը սահմանվում է

$$a_{k_1,\dots,k_n}x_1^{k_1}\cdots x_n^{k_n} + b_{k_1,\dots,k_n}x_1^{k_1}\cdots x_n^{k_n} \stackrel{\text{def}}{=} \left(a_{k_1,\dots,k_n} + b_{k_1,\dots,k_n}\right)x_1^{k_1}\cdots x_n^{k_n} \tag{6.12}$$

բանաձեւով, որտեղ աջ կողմում փակագծերի մեջ գումարումը կատարվում է R ամբողջության տիրույթում: Օրինակ՝ $4x^3y + 7x^3y = 11x^3y$: Ընդ որում, եթե $a_{k_1,\dots,k_n} + b_{k_1,\dots,k_n} = 0$, ապա, ըստ մեր պայմանավորվածության, զրոյական է նաեւ միանդամների գումարը: Կամայական (միգուցե տարբեր աստիճաններ ունեցող) $a_{k_1,\dots,k_n}x_1^{k_1}\cdots x_n^{k_n}$ եւ $b_{j_1,\dots,j_n}x_1^{j_1}\cdots x_n^{j_n}$ միանդամների արտադրյալը սահմանվում է

$$a_{k_1,\dots,k_n}x_1^{k_1}\cdots x_n^{k_n} \cdot b_{j_1,\dots,j_n}x_1^{j_1}\cdots x_n^{j_n} \stackrel{\text{def}}{=} \left(a_{k_1,\dots,k_n}\cdot b_{j_1,\dots,j_n}\right)x_1^{k_1+j_1}\cdots x_n^{k_n+j_n} \tag{6.13}$$

բանաձեւով, որտեղ աջ կողմում՝ փակագծերի մեջ, բազմապատկումը կատարվում է R ամբողջության տիրույթում, իսկ աստիճանները գումարվում են որպես ամբողջ թվեր: Օրինակ՝ $4x^3y \cdot 5x^8y^3 = 20x^{11}y^4$:

(6.11) տեսքի գրությամբ տրված $f(x_1, \dots, x_n) = \sum_{(k_1,\dots,k_n)\in S} a_{k_1,\dots,k_n}x_1^{k_1}\cdots x_n^{k_n}$ եւ $g(x_1, \dots, x_n) = \sum_{(j_1,\dots,j_n)\in S'} b_{j_1,\dots,j_n}x_1^{j_1}\cdots x_n^{j_n}$ բազմանդամների $f + g$ գումարը սահմանվում է «նման անդամների միացման» կանոնով. $\sum_{(k_1,\dots,k_n)\in S} a_{k_1,\dots,k_n}x_1^{k_1}\cdots x_n^{k_n} + \sum_{(j_1,\dots,j_n)\in S'} b_{j_1,\dots,j_n}x_1^{j_1}\cdots x_n^{j_n}$ ձեւական գումարի մեջ իրար են գումարվում հավասար աստիճաններ ունեցող միանդամները: Իսկ այդ բազմանդամների $f \cdot g$ արտադրյալը սահմանվում է «փակագծերը բացելու եւ ապա նման անդամների միացման» կա-

նոնով. f-ի միանդամներից յուրաքանչյուրը բազմապատկվում է g-ի միանդամներից յուրաքանչյուրի հետ, եւ ապա ստացված միանդամների մեջ իրար են միացվում հավասար աստիճաններ ունեցողները: Հեշտ է ստուգել, որ սահմանված գործողությունները համաձայնեցված են վերը սահմանված հավասարության (համարժեքության հարաբերության) հետ: Մասնավորապես, $R[x_1,\dots,x_n]$-ի վրա սահմանված գործողությունների սահմանափակումը R օղակի վրա համընկնում է R-ի օղակային գործողությունների հետ: Եթե $a,b\in R$, ապա

$$a+b=a\,x_1^0\cdots x_n^0+b\,x_1^0\cdots x_n^0\overset{\text{def}}{=}(a+b)x_1^0\cdots x_n^0=a+b\in R,$$
$$a\cdot b=a\,x_1^0\cdots x_n^0\ \cdot\ b\,x_1^0\cdots x_n^0\overset{\text{def}}{=}(a\cdot b)x_1^{0+0}\cdots x_n^{0+0}=a\cdot b\in R:$$

6.2.3 Օրինակ. $R=\mathbb{Z}_5$ օղակի վրա դիտարկենք երեք փոփոխականի $f(x,y,z)=2x^5y^3z^2+3xz$ եւ $g(x,y,z)=4x^5y^5z+3xy^2+4xz$ բազմանդամները: Այդ դեպքում $f(x,y,z)+g(x,y,z)=2x^5y^3z^2+2xz+4x^5y^5z+3xy^2$, քանի որ հավասար աստիճաններ ունեցող միանդամները միայն երկու հատ են, եւ $\mathbb{Z}_5$ օղակի վրա դրանց գումարն է $3xz+4xz=2xz$: Իսկ արտադրյալը կհաշվվի այսպես՝

$$\begin{aligned}f(x,y,z)\cdot g(x,y,z)&=3x^{10}y^8z^3+x^6y^5z^2+3x^6y^3z^3+4x^6y^5z^2+4x^2y^2z^1+2x^2z^2\\&=3x^{10}y^8z^3+3x^6y^3z^3+4x^2y^2z^1+2x^2z^2:\end{aligned}$$

6.2.4 Վարժություն. Նախորդ օրինակի f եւ g բազմանդամների համար հաշվել $f^2=f\cdot f$ եւ $g^2=g\cdot g$ քառակուսիները: Հաշվել f^2+g եւ f^2+g^2 գումարները: Գտնել $\deg_x f^2$ եւ $\deg(f^2+g^2)$ արժեքները:

6.2.5 Խնդիր. Ցույց տալ, որ R ամբողջության տիրույթի վրա տրված n փոփոխականների բազմանդամների $R[x_1,\dots,x_n]$ բազմությունը օղակ է նրա վրա սահմանված գումարման եւ բազմապատկման գործողությունների նկատմամբ: Այն նաեւ ամբողջության տիրույթ է: *Յուցում.* որպես $R[x_1,\dots,x_n]$-ի միավոր կարելի է վերցնել $1\in R$ միանդամը: Որպես զրոյական տարր կարելի է վերցնել $0\in R$ միանդամը: Եթե $f(x_1,\dots,x_n)$ եւ $g(x_1,\dots,x_n)$ բազմանդամները երկուսն էլ զրոյական չեն, ապա զրոյական չէ նաեւ դրանց արտադրյալը: Դա ստուգելու համար համեմատել, ասենք, $\deg_{x_i}f$, $\deg_{x_i}g$ եւ $\deg_{x_i}(f\cdot g)$ արժեքները x_i փոփոխականների համար:

6.2.6 Վարժություն. Կամայական $f(x_1,\dots,x_n),\ g(x_1,\dots,x_n)\in R[x_1,\dots,x_n]$ բազմանդամների համար համեմատել $\deg f,\ \deg g$ եւ $\deg(f\cdot g)$ արժեքները:

Այժմ անցնենք $R[x_1,\dots,x_n]$ օղակի այն մեկնաբանությանը, որն օգտագործել ենք 4.2 պարագրաֆում: Սկսենք հետեւյալ օրինակից.

6.2.7 Օրինակ. Դիտարկենք $\mathbb{Z}[x,y]$ օղակի այն $f(x,y)$ բազմանդամը, որը քննարկեցինք 6.2.2 օրինակում: «Նման անդամների միացում» կատարելով՝ կարելի է ներկայացնել այն

(6.14) $$f(x,y)=5y^7+(2x^2+3x+2)y^4-(4x^3-2)y+(6x^5+7)y^0$$

տեսքով: Հասկանալի է, որ սա սովորական (մեկ փոփոխականի) բազմանդամ է, որի փոփոխականն է y-ը, եւ որի $a_0=5$, $a_1=2x^2+3x+2$, $a_2=-(4x^3-2)$ եւ $a_3=6x^5+7$ գործակիցները $\mathbb{Z}[x]$ ամբողջության տիրույթից են: (6.14) բազմանդամը $\mathbb{Z}[x][y]$ բազմանդամային օղակից է: Նույն կերպ $f(x,y)$-ը կարելի էր ներկայացնել

(6.15) $$f(x,y)=6x^5-4yx^3+2y^4x^2+3y^4x+(5y^7+2y^4+2y+7)$$

Տեսքով՝ որպես x փոփոխականի բազմանդամ $\mathbb{Z}[y]$ օղակի վրա, այսինքն՝ որպես $\mathbb{Z}[y][x]$ օղակի տարր: $\mathbb{Z}[x,y]$, $\mathbb{Z}[x][y]$ եւ $\mathbb{Z}[y][x]$ բազմանդամային օղակներն իրար հավասար չեն, քանի որ դրանք ընդհանրապես տարբեր օղակների վրա են սահմանված: Բայց դրանք իրար իզոմորֆ են. $\mathbb{Z}[x][y]$ օղակի բազմանդամի մեջ փակագծերի բացում իրականացնելով՝ մենք կստանանք $a_{ij}y^ix^j$ տեսքի գումարելիներ, որոնք կարելի է համապատասխանեցնել $\mathbb{Z}[x,y]$ օղակի՝ նույն գրությունն ունեցող միանդամներին: Այս արտապատկերումը շարունակվում է մինչեւ $\mathbb{Z}[x][y]\cong\mathbb{Z}[x,y]$ իզոմորֆիզմ, քանի որ այն համաձայնեցված է օղակային գործողությունների հետ. փակագծերի բացում կամ տարրերի խմբավորում միեւնույն կերպ է կատարվում $\mathbb{Z}[x][y]$ եւ $\mathbb{Z}[x,y]$ օղակներում:

Այս սկզբունքը կարելի է ինդուկցիայով տարածել փոփոխականների ցանկացած քանակի համար: $R[x_1,\dots,x_n]$ օղակն իզոմորֆ է ինչպես $R[x_1,\dots,x_{n-1}][x_n]$ օղակին (սա մեկ x_n փոփոխականի բազմանդամների օղակն է $R[x_1,\dots,x_{n-1}]$-ի վրա), այնպես էլ $R[x_1][x_2,\dots,x_n]$ օղակին (սա $n-1$ հատ $x_2,\dots,x_n$ փոփոխականների բազմանդամների օղակն է $R[x_1]$-ի վրա) կամ $R[x_1,\dots,x_{m-1}][x_m,\dots,x_n]$ օղակին՝ ցանկացած $m=2,\dots,n-1$ թվի համար: Ավելին, շարունակելով 4.2 պարագրաֆի նյութը՝ նշենք, որ $R[x_1,\dots,x_n]$ օղակն իզոմորֆ է $R[x_1]\cdots[x_n]$ օղակին (սա մեկ x_n փոփոխականի բազմանդամների օղակն է $R[x_1]\cdots[x_{n-1}]$-ի վրա, որն, իր հերթին, մեկ x_{n-1} փոփոխականի բազմանդամների օղակն է $R[x_1]\cdots[x_{n-2}]$-ի վրա եւլն):

6.2.8 Խնդիր. Կամայական R ամբողջության տիրույթի համար հիմնավորել վերը նշված $R[x_1,\dots,x_n]\cong R[x_1,\dots,x_{m-1}][x_m,\dots,x_n]$ իզոմորֆիզմը, որտեղ $m=2,\dots,n-1$ ցանկացած թիվ է: *Յուցում.* օգտվել 6.2.7 օրինակից եւ կիրառել ինդուկցիա:

6.2.9 Խնդիր. Հիմնավորել վերը նշված $R[x_1,\dots,x_n]\cong R[x_1]\cdots[x_n]$ իզոմորֆիզմը: *Յուցում.* օգտվել նախորդ խնդրից եւ 4.2 պարագրաֆից:

6.2.10 Դիտողություն. Օգտագործելով տրանսցենդենտ ընդլայնումների մասին 4.2 պարագրաֆի փաստերը (տես 4.2.25 թեորեմը եւ հաջորդող քննարկումը)՝ կարելի էր տալ մի քանի փոփոխականների բազմանդամի ավելի կարճ սահմանում: Ենթադրենք R ամբողջության տիրույթը ներդրված է K դաշտի մեջ, եւ K-ն պարունակում է այնպիսի $x_1, \dots, x_n$ տարրեր, որ յուրաքանչյուր x_i-ն տրանսցենդենտ է K-ի մեջ R-ով եւ մնացած $\{x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n\}$ տարրերով ծնված ենթադաշտում ($x_1, \dots, x_n$ համակարգը *հանրահաշվորեն անկախ* է R-ի վրա): Այդ դեպքում K-ի մեջ $R \cup \{x_1, \dots, x_n\}$ միավորմամբ ծնված օղակն անվանենք R ամբողջության տիրույթի վրա տրված $x_1, \dots, x_n$ փոփոխականների բազմանդամների $R[x_1, \dots, x_n]$ օղակ: 4.2 պարագրաֆում արդեն ապացուցել ենք, որ այն իզոմորֆ է $R[x_1] \cdots [x_n]$ օղակին:

6.3 Գաուսի լեմման ֆակտորիալ օղակներում

2.6 պարագրաֆում մենք R ամբողջության տիրույթի վրա տրված ոչ զրոյական $f(x) \in R[x]$ բազմանդամի $\mathrm{cont}\big(f(x)\big)$ բովանդակությունը սահմանեցինք այն դեպքերի համար, երբ բազմանդամի բոլոր գործակիցների ամենամեծ ընդհանուր բաժանարարը R-ում գոյություն ունի: Ըստ 6.1.14 թեորեմի, այդ ամենամեծ ընդհանուր բաժանարարը միշտ գոյություն ունի, եթե R-ը ֆակտորիալ օղակ է: Ուստի R ֆակտորիալ օղակի վրա տրված $f(x) \in R[x]$ ոչ զրոյական բազմանդամի համար $\mathrm{cont}\big(f(x)\big)$-ը միշտ սահմանված է: Հիշենք նաեւ, որ, որպես ամենամեծ ընդհանուր բաժանարար, $\mathrm{cont}\big(f(x)\big)$-ը սահմանվում է $\varepsilon \in R^*$ հակադարձելի տարրի ճշտությամբ:

6.3.1 Օրինակ. Ինչպես տեսանք 2.6.4 օրինակում, եթե $f(x) = 2x^2 + 6x - 4 \in \mathbb{Z}[x]$, ապա $\mathrm{cont}\big(f(x)\big) = 2$ (կամ էլ $\mathrm{cont}\big(f(x)\big) = -2$, այստեղ $\varepsilon = \pm 1$): Իսկ նույն $f(x)$ բազմանդամը $\mathbb{Q}[x]$ օղակում դիտարկելիս (այն ֆակտորիալ է ըստ 6.1.11 հետեւանքի) որպես $\mathrm{cont}\big(f(x)\big)$ կարելի է վերցնել զրոյից տարբեր ցանկացած $r \in \mathbb{Q}$ ռացիոնալ թիվ, քանի որ դրանք բոլորն էլ բաժանում են բազմանդամի գործակիցները եւ հակադարձելի են: $2, 6, -4$ թվերի համար $\mathbb{Q}$-ում ամենամեծ ընդհանուր բաժանարար են ոչ միայն $2, -2$ թվերը, այլեւ, ասենք, $r = 100 \in \mathbb{Q}^*$ թիվը:

Վերհիշենք, որ, ըստ 2.6.5 սահմանման, $f(x) \in R[x]$ բազմանդամը պրիմիտիվ է, եթե $\mathrm{cont}\big(f(x)\big) \approx 1$: Իսկ ըստ 2.6.6 սահմանման, $f(x)$-ի պրիմիտիվ մաս է կոչվում $\mathrm{pp}\big(f(x)\big) = f(x)/\mathrm{cont}\big(f(x)\big)$ պրիմիտիվ բազմանդամը (այն նույնպես որոշվում է հակադարձելի տարրի ճշտությամբ):

6.3.2 Օրինակ. $\mathbb{Z}_2$ դաշտի վրա երկու փոփոխականների բազմանդամների $\mathbb{Z}_2[x,y]$ օղակում դիտարկենք $f(x,y)=x^2y+xy^2+y^2+y$ բազմանդամը: Ինչպես տեսանք նախորդ պարագրաֆում, $\mathbb{Z}_2[x,y]\cong\mathbb{Z}_2[x][y]$, այսինքն՝ $f(x,y)$ բազմանդամը կարելի է համարել $\mathbb{Z}_2[x]$-ի վրա տրված y փոփոխականի բազմանդամ.

$$f(y)=(x+1)y^2+(x^2+1)y\ =a_0y^2+a_1y\in\mathbb{Z}_2[x][y]:$$

$f(y)$-ի $a_0=x+1$ եւ $a_1=x^2+1$ գործակիցները $\mathbb{Z}_2[x]$ էվկլիդյան օղակից են, եւ դրանց ամենամեծ ընդհանուր բաժանարարը հեշտ է հաշվել Էվկլիդեսի ալգորիթմով: Դա մենք արդեն արել ենք 3.4.5 օրինակում. $x^2+1=x^2+1^2=(x+1)(x+1)$: Ուրեմն եւ $\mathrm{cont}\big(f(y)\big)=(x^2+1,x+1)=x+1\in\mathbb{Z}_2[x]$: Ուստի $\mathrm{pp}\big(f(y)\big)=f(y)/\mathrm{cont}\big(f(y)\big)\ =y^2+(x+1)y$: Իսկ եթե օգտվենք $\mathbb{Z}_2[x,y]\cong\mathbb{Z}_2[y][x]$ իզոմորֆիզմից, նույն $f(x,y)$ բազմանդամը կարելի է դիտարկել որպես $\mathbb{Z}_2[y]$-ի վրա տրված x փոփոխականի բազմանդամ $f(x)=yx^2+y^2x\ +(y^2+y)\in\mathbb{Z}_2[x]$, որի երեք գործակիցների համար $\mathrm{cont}\big(f(x)\big)=(y,y^2,y^2+y)=y\in\mathbb{Z}_2[y]$: Ուստի $\mathrm{pp}\big(f(x)\big)=f(x)/\mathrm{cont}\big(f(x)\big)\ =x^2+yx\ +(y+1)$:

6.3.3 Դիտողություն. Նախորդ օրինակում մենք օգտվեցինք այն բանից, որ $\mathbb{Z}_2[x]$-ն էվկլիդյան օղակ է: Դա ոչ միայն ապահովում էր $\mathbb{Z}_2[x][y]$ օղակի ոչ-զրոյական բազմանդամի բովանդակության եւ պրիմիտիվ մասի գոյությունը (այսինքն՝ $\mathbb{Z}_2[x]$-ին պատկանող գործակիցների ամենամեծ ընդհանուր բաժանարարի գոյությունը), այլեւ տալիս էր դրանց հաշվման հարմար մեթոդ՝ Էվկլիդեսի ալգորիթմը: Ինչպես մենք տեսանք նախորդ պարագրաֆում, $R[x,y]\cong R[x][y]$ (եւ, ընդհանրապես, $R[x_1,\dots,x_n]\cong R[x_1,\dots,x_{m-1}][x_m,\dots,x_n]$) իզոմորֆիզմը տեղի ունի կամայական R ամբողջության տիրույթի համար: Մասնավորապես, $\mathbb{Z}[x,y]\cong\mathbb{Z}[x][y]$ եւ մենք $\mathbb{Z}$-ի վրա տրված երկու փոփոխականների ոչ զրոյական բազմանդամը նույնպես կարող ենք (6.3.2 օրինակի նմանությամբ) ներկայացնել որպես $\mathbb{Z}[x]$ օղակի վրա տրված՝ y փոփոխականի բազմանդամ: Քանի որ այդ բազմանդամի գործակիցները $\mathbb{Z}[x]$ օղակի տարրեր են, ապա, ըստ 6.1.9 օրինակի եւ 6.1.14 թեորեմի, գոյություն ունի դրանց ամենամեծ ընդհանուր բաժանարարը (բազմանդամի բովանդակությունը): Կարեւոր է նկատել, որ ամենամեծ ընդհանուր բաժանարարի գոյության փաստը դեռ չի նշանակում, որ մենք ունենք դրա *հաշվման մեթոդը*:

Ավելի վաղ մենք ծանոթացել էինք 2.6.8 Գաուսի լեմմային միայն ամբողջ գործակիցներով բազմանդամների համար: Դրա ընդհանրացումը տեղի ունի նաեւ ֆակտորիալ օղակների համար.

6.3.4 Գաուսի լեմման ֆակտորիալ օղակի համար. *Կամայական R ֆակտորիալ օղակի վրա տրված $f(x),\ g(x) \in R[x]$ բազմանդամների համար*

$$\operatorname{cont}\big(f(x)\cdot g(x)\big) \approx \operatorname{cont}\big(f(x)\big)\cdot \operatorname{cont}\big(g(x)\big): \tag{6.16}$$

Մասնավորապես, պրիմիտիվ բազմանդամների արտադրյալը պրիմիտիվ բազմանդամ է:

Ապացույց: Քանի որ փաստարկները մեծ մասամբ կրկնում են 2.6.8 լեմմայի ապացույցը, ապա բերենք միայն ապացույցի սխեման: Նախ, ենթադրենք $f(x)$, $g(x)$ բազմանդամները պրիմիտիվ են, բայց նրանց $h(x)=f(x)\cdot g(x)$ արտադրյալը պրիմիտիվ չէ: Այդ դեպքում կա մի $p\in R$ պարզ տարր, որի վրա բաժանվում են $h(x)$-ի բոլոր գործակիցները: $f(x)$, $g(x)$ բազմանդամները ներկայացնենք (2.14) տեսքով՝ համարելով, որ a_s տարրը $f(x)$-ի առաջին գործակիցն է, որը չի բաժանվում p տարրի վրա, իսկ b_t տարրը նույն կանոնով ընտրված գործակիցն է $g(x)$-ի համար: Կրկին, $h(x)$ բազմանդամի մեջ $x^{(n-s)+(m-t)}$ աստիճանի գործակիցը կլինի.

$$c_{s+t}=a_sb_t+[a_{s+1}b_{t-1}+a_{s+2}b_{t-2}+\cdots]+[a_{s-1}b_{t+1}+a_{s-2}b_{t+2}+\cdots]: \tag{6.17}$$

Կրկնելով 2.6.8 լեմմայի ապացույցի փաստարկը՝ ստանում ենք, որ (6.17) հավասարության երկու քառակուսի փակագծերի գումարներն էլ բաժանվում են p-ի վրա: Այն փաստը, որ $p\nmid a_sb_t$, 2.6.8 լեմմայի ապացույցում օգտագործվում էր որպես ամբողջ թվերի մասին հայտնի հատկություն: Իսկ այստեղ մենք դա ստանում ենք որպես 6.1.6 հետեւանքի կիրառություն. եթե R ֆակտորիալ օղակի a_s, b_t տարրերի արտադրյալը բաժանվում է p պարզ տարրի վրա, ապա այդ տարրերից գոնե մեկը նույնպես բաժանվում է p-ի վրա: Ուրեմն, ըստ a_s, b_t տարրերի ընտրության՝ $p\nmid a_sb_t$: Դրանից եւ (6.17) հավասարությունից ստանում ենք, որ $p\nmid c_{s+t}$: Հակասություն:

Ընդհանուր դեպքում բազմանդամները ներկայացնենք

$$f(x)=\operatorname{cont}\big(f(x)\big)\operatorname{pp}\big(f(x)\big),\qquad g(x)=\operatorname{cont}\big(g(x)\big)\operatorname{pp}\big(g(x)\big)$$

տեսքով, որտեղ $\operatorname{pp}\big(f(x)\big)$ եւ $\operatorname{pp}\big(g(x)\big)$ բազմանդամները պրիմիտիվ են, եւ ավարտենք ապացույցը 2.6.8 լեմմայի ապացույցի նմանությամբ: ■

6.3.5 Հետեւանք. R ֆակտորիալ օղակի վրա տրված $R[x]$ բազմանդամային օղակում պրիմիտիվ բազմանդամի բաժանարարը նույնպես պրիմիտիվ է: Մասնավորապես, պրիմիտիվ բազմանդամների ամենամեծ ընդհանուր բաժանարարը պրիմիտիվ բազմանդամ է:

4.2 պարագրաֆում մենք ծանոթացանք ամբողջության տիրույթները քանորդների միջոցով դաշտի մեջ ներդնելու եղանակին (տես 4.2.3 թեորեմի 4.2.4 հետեւանքը). R ամբողջության տիրույթի համար կառուցվում է նրա տարրերի a/b տեսքի ձեւական քանորդների բազմությունը ($a \in R$, $b \in R\backslash\{0\}$): Այդ քանորդների բազմության վրա մտցվում է համարժեքության հարաբերություն, եւ ըստ դրա կազմված համարժեքության դասերի միջեւ գումար եւ արտադրյալ սահմանելով՝ ստացվում է R օղակը պարունակող $F = \mathrm{Quot}(R)$ քանորդների դաշտը: Օրինակ, ըստ 4.2.5 օրինակի, $\mathbb{Z}$ օղակի համար այդ դաշտն է $\mathrm{Quot}(\mathbb{Z}) = \mathbb{Q}$: Հետեւյալ լեմման է 2.6.11 լեմմայի ընդհանրացում է ֆակտորիալ օղակների համար.

6.3.6 Լեմմա. *Ենթադրենք R-ը կամայական ֆակտորիալ օղակ է եւ $f(x)$, $g(x) \in R[x]$, ընդ որում, $g(x)$ բազմանդամը պրիմիտիվ է: Եթե $f(x)$-ը բաժանվում է $g(x)$-ի վրա $F[x]$ օղակում, որտեղ $F = \mathrm{Quot}(R)$, ապա $f(x)$-ը բաժանվում է $g(x)$-ի վրա նաեւ $R[x]$ օղակում:*

Ապացույց: Ապացույցը կրկնելու է 2.6.11 լեմմայի ապացույցի հիմնական կետերը: Գոյություն ունի $h(x) \in F[x]$ բազմանդամ, որի համար $f(x) = g(x)h(x)$.

$$h(x) = u_0/v_0\, x^m + \cdots + u_m/v_m,$$

որտեղ $u_0/v_0, \ldots, u_m/v_m \in F = \mathrm{Quot}(R)$ եւ $v_0, \ldots, v_m \neq 0$: Քանի որ R օղակը ֆակտորիալ է, ըստ 6.1.14 թեորեմի, նրա $v_0, \ldots, v_m$ ոչ զրոյական տարրերի համար գոյություն ունի դրանց v ամենափոքր ընդհանուր բազմապատիկը: $v \cdot h(x)$ բազմանդամը $R[x]$-ից է եւ, կրկին ըստ 6.1.14 թեորեմի, կարելի է դիտարկել դրա բոլոր գործակիցների u ամենամեծ ընդհանուր բաժանարարը՝ $u = \mathrm{cont}\big(v \cdot h(x)\big)$: Նշանակելով $a = \mathrm{cont}\big(f(x)\big)$՝ հաշվենք.

$$v \cdot f(x) = v \cdot a \cdot \mathrm{pp}\big(f(x)\big) = g(x) \cdot\ v \cdot h(x) = g(x) \cdot\ u \cdot \mathrm{pp}\big(v \cdot h(x)\big): \tag{6.18}$$

Այս հավասարության ձախ մասի բովանդակությունն է $v \cdot a$, իսկ աջ մասինը՝ u, քանի որ $g(x)$ եւ $\mathrm{pp}\big(v \cdot h(x)\big)$ պրիմիտիվ բազմանդամների արտադրյալը պրիմիտիվ է ըստ Գաուսի 6.3.4 լեմմայի: Ուստի $v \cdot a \approx u$ եւ (6.18) հավասարությունների բոլոր մասերն էլ բաժանվում են $v \cdot a$-ի վրա: Ուրեմն՝ $\mathrm{pp}\big(f(x)\big) = g(x)\, \frac{u}{v \cdot a} \mathrm{pp}\big(v \cdot h(x)\big)$ եւ $f(x) = a \cdot \mathrm{pp}\big(f(x)\big) = a \cdot g(x) \frac{u}{v \cdot a} \mathrm{pp}\big(v \cdot h(x)\big)$: Այսպիսով՝ $f(x) = g(x)k(x)$, որտեղ $k(x) = \frac{u}{v} \mathrm{pp}\big(v \cdot h(x)\big) \in R[x]$: ■

6.3.7 Հետեւանք. Եթե R օղակը ֆակտորիալ է, ապա $R[x]$ բազմանդամային օղակի կամայական $f(x)$ պարզ տարր ունի հետեւյալ երկու տիպերից մեկը.

1) կամ $\deg f(x) = 0$, եւ այդ դեպքում $f(x) = c$ հաստատուն բազմանդամը պարզ է այն եւ միայն այն դեպքում, երբ c-ն պարզ է որպես R օղակի տարր,
2) կամ էլ $\deg f(x) > 0$, եւ այդ դեպքում $f(x)$ բազմանդամը պարզ է այն եւ միայն այն դեպքում, երբ այն պրիմիտիվ պարզ բազմանդամ է:

Հետեւյալ կարեւոր թեորեմն ընդհանրացնում է մինչ այժմ մեր ստացած մի շարք փաստեր, ներառյալ 2.6.13 թեորեմը, 6.1.11 եւ 6.1.12 հետեւանքները:

6.3.8 Գաուսի թեորեմը. *Եթե R օղակը ֆակտորիալ է, ապա նրա վրա տրված $R[x]$ բազմանդամային օղակը նույնպես ֆակտորիալ է:*

Ապացույց: Հիմնավորումը կրկնելու է 2.6.13 թեորեմի ապացույցի քայլերը: Կամայական ոչ զրոյական $f(x) \in R[x]$ բազմանդամ կարելի է ներկայացնել

$$f(x) = \varepsilon \cdot p_1 \cdots p_u \cdot g_1(x) \cdots g_s(x) \tag{6.19}$$

տեսքով, որտեղ $\varepsilon \in R^*$, $p_1, \dots, p_m$ տարրերը պարզ են R-ում, իսկ $g_1(x), \dots, g_s(x)$ տարրերը 0-ից բարձր աստիճանի պրիմիտիվ պարզ բազմանդամներ են $R[x]$-ում (տես 6.3.7 հետեւանքը): Ընդ որում, (6.19) ներկայացումը միակն է. եթե գոյություն ունի մի այլ ներկայացում՝

$$f(x) = \epsilon \cdot q_1 \cdots q_v \cdot h_1(x) \cdots h_r(x), \tag{6.20}$$

ապա $u = v$, $s = r$ եւ (գուցե արտադրիչների վերադասավորությունից հետո) $p_i \approx q_i$ $(i = 1, \dots, u)$ եւ $g_j(x) \approx h_j(x)$ $(j = 1, \dots, s)$: ■

(6.19) ներկայացման մեջ կարելի է կատարել «նման անդամների միացում»: Եթե p_i պարզ տարրերի մեջ կան միմյանց ասոցացված տարրեր կամ եթե $g_j(x)$ բազմանդամների մեջ կան միմյանց ասոցացված բազմանդամներ, դրանք կարելի է իրար միացնել՝ անհրաժեշտության դեպքում փոխելով ε արտադրիչի նշանը.

$$f(x) = \nu \cdot p_1^{\alpha_1} \cdots p_n^{\alpha_n} \cdot g_1^{\beta_1}(x) \cdots g_m^{\beta_m}(x), \tag{6.21}$$

որտեղ $p_1, \dots, p_n$; $g_1(x), \dots, g_m(x)$ տարրերը զույգ առ զույգ ասոցացված չեն եւ $\nu \in R^*$: 6.1.14 թեորեմից եւ 6.3.8 թեորեմից բխում է.

6.3.9 Հետեւանք. R ֆակտորիալ օղակի վրա տրված կամայական ոչ զրոյական $f(x)$, $g(x)$ բազմանդամների համար $R[x]$-ում գոյություն ունի նրանց $\big(f(x), g(x)\big)$ ամենամեծ ընդհանուր բաժանարարը եւ $[f(x), g(x)]$ ամենափոքր ընդհանուր բազմապատիկը: Դրանք որոշվում են հակադարձելի տարրի ճշտությամբ:

Անդրադառնալով մի քանի փոփոխականների բազմանդամների օղակներին՝ հեշտությամբ ստանում ենք այս պնդումների ընդհանրացումները դրանց համար.

6.3.10 Գաուսի թեորեմը մի քանի փոփոխականների բազմանդամների համար. *Եթե R օղակը ֆակտորիալ է, ապա նրա վրա տրված $R[x_1, \dots, x_n]$ բազմանդամային օղակը նույնպես ֆակտորիալ օղակ է ցանկացած բնական n-ի համար:*

6.3.11 Հետեւանք. R ֆակտորիալ օղակի վրա տրված կամայական ոչ զրոյական $f(x_1, \dots, x_n)$, $g(x_1, \dots, x_n)$ n փոփոխականների բազմանդամների համար $R[x_1, \dots, x_n]$ օղակում գոյություն ունի նրանց (f, g) ամենամեծ ընդհանուր բաժանարարը եւ $[f, g]$ ամենափոքր ընդհանուր բազմապատիկը: Դրանք որոշվում են հակադարձելի տարրի ճշտությամբ:

Որպես 6.3.10 թեորեմի կիրառություն՝ պարագրաֆն ավարտենք հետեւյալ օրինակով:

6.3.12 Օրինակ. Վերցնենք կամայական R ֆակտորիալ օղակի վրա տրված $R[x, y]$ օղակը: Այն ֆակտորիալ է՝ ըստ 6.3.10 թեորեմի: Ցույց տանք, որ այն գլխավոր իդեալների օղակ չի հանդիսանում: Դիտարկենք $R[x, y]$-ի այն I իդեալը, որը ծնվում է $\{x,\ y\}$ տարրերով: Ենթադրենք հակառակը. $I = f(x, y)R[x, y]$ որեւէ $f(x, y)$-ի համար: Քանի որ $x,\ y \in I$, ապա $x \vdots f(x, y)$ եւ $y \vdots f(x, y)$: Սա հնարավոր է միայն, երբ $f(x, y) = \varepsilon \in R^*$: Բայց այդ դեպքում $I = R[x, y]$, իսկ դա անհնար է, քանի որ $\{x,\ y\}$ տարրերով ծնված իդեալը չի կարող պարունակել զրոյական աստիճանի ոչ մի բազմանդամ: Համեմատելով այս օրինակը 6.1.9 օրինակի հետ՝ տեսնում ենք, որ $R[x, y]$-ը գլխավոր իդեալների օղակ չէ, եթե անգամ R-ը դաշտ է:

Հետագա զարգացումների համար տես 8.4.12 Հիլբերտի թեորեմը եւ 8.4.13 դիտողությունը:

6.4 Ալգորիթմներ մի քանի փոփոխականների բազմանդամների համար

Ֆակտորիալ օղակի վրա մի քանի փոփոխականների բազմանդամների օղակը ֆակտորիալ է, եւ դրա շնորհիվ նրանում հնարավոր է քննարկել այնպիսի հասկացություններ, ինչպիսիք են՝ կամայական ոչ զրոյական տարրերի ամենամեծ ընդհանուր բաժանարարը, ամենափոքր ընդհանուր բազմապատիկը, տարրերի փոխադարձ պարզությունը եւլն: Այս պարագրաֆում մենք կտեսնենք, թե ինչպես կարելի է ալգորիթմների կառուցման համար ֆակտորիալ օղակների հետ հավելյալ օժանդակ դաշտեր քննարկել: Այս պարագրաֆի ալգորիթմները օգտագործելու են

$\mathrm{Quot}(R)$ քանորդների դաշտի մեջ R ամբողջության տիրույթի ներդրումը (տես 4.2 պարագրաֆի 4.2.3 թեորեմը, 4.2.4 հետեւանքը, 4.2.5 եւ 4.2.6 օրինակները):

Սկսենք K-ն դաշտի վրա տրված երկու փոփոխականների $K[x,y]$ բազմանդամային օղակի դեպքից: Մասնավորապես, K-ն կարող է լինել $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p$ դաշտերից որեւէ մեկը: $K[x,y] \cong K[x][y]$ իզոմորֆիզմը մեզ թույլ է տալիս դիտարկել $K[x,y]$-ի բազմանդամները՝ որպես $R = K[x]$ օղակի վրա տրված y փոփոխականի բազմանդամներ (տես 6.2.7 օրինակը եւ 6.2.8 խնդիրը): Չնայած K-ի դաշտ լինելը ապահովում է $K[x]$ օղակի էվկլիդյանությունը, եւ նրա վրա կարելի է կիրառել Էվկլիդեսի ալգորիթմը, $R[y] \cong K[x,y]$ օղակը կարող է այլեւս էվկլիդյան չլինել: Այն անգամ գլխավոր իդեալների օղակ չէ՝ ըստ 6.3.12 օրինակի: Այնուամենայնիվ, Էվկլիդեսի ալգորիթմի ընձեռած առավելություններից $R[y]$-ում օգտվելու համար փորձենք ներդնել $R[y]$ օղակը որեւէ էվկլիդյան օղակի մեջ: Ընդհանրապես, եթե R օղակը ներդրվում է որեւէ L օղակի մեջ (այսինքն՝ L-ն ունի R-ին իզոմորֆ ենթաօղակ), ապա $R[y]$ օղակն էլ ներդրվում է $L[y]$ օղակի մեջ:

Ըստ 4.2.3 թեորեմի 4.2.4 հետեւանքի, կամայական R ամբողջության տիրույթ ներդրվում է դաշտի մեջ: Դա R օղակի $F = \mathrm{Quot}(R)$ քանորդների դաշտն է, որը կառուցվում է R-ի տարրերի ձեւական հարաբերությունների միջոցով: Ինչպես տեսանք 4.2.6 օրինակում, եթե քանորդների դաշտը կառուցվում է բազմանդամային օղակի համար, ապա $\mathrm{Quot}(K[x])$-ը K-ի վրա տրված ռացիոնալ ֆունկցիաների դաշտն է, որը նշանակվում է $K(x)$: Որպես L վերցնենք $K(x)$-ը եւ ներդնենք $K[x][y]$-ը $K(x)[y]$ օղակի մեջ: Նկատենք, որ չնայած գրառման որոշ նմանությանը՝ $K[x][y]$ եւ $K(x)[y]$ օղակներն իրարից էապես տարբեր են: Առաջինն իզոմորֆ է $K[x,y]$-ին, մինչդեռ երկրորդը բաղկացած է

$$\frac{c_0(x)}{d_0(x)}y^n + \cdots + \frac{c_n(x)}{d_n(x)} \tag{6.22}$$

տեսքի բազմանդամներից, որոնց գործակիցները ռացիոնալ ֆունկցիաներ են. $\frac{c_i(x)}{d_i(x)} \in K(x)$, $i = 0, \ldots, n$ (այսինքն՝ $c_i(x), d_i(x) \in K[x]$ եւ $d_i(x) \neq 0$): Քանի որ $K(x)$-ը դաշտ է, $K(x)[y]$ օղակն էվկլիդյան է, եւ նրանում արդեն կարելի է կիրառել Էվկլիդեսի ալգորիթմը եւ բազմանդամների «անկյունով բաժանելու» գործողությունը:

6.4.1 Օրինակ. $\mathbb{Z}_3[x,y]$ օղակում վերցնենք $f(x,y) = xy + 2y + 2x + 1$ եւ $g(x,y) = xy + 2x$ բազմանդամները: Ներկայացնենք դրանք որպես $\mathbb{Z}_3[x][y]$ օղակի բազմանդամներ. $f(y) = (x+2)y + (2x+1) = a_0(x)y + a_1(x)$ եւ $g(y) = xy + 2x = b_0(x)y + b_1(x)$: Ներդնենք $\mathbb{Z}_3[x]$ օղակը $\mathbb{Z}_3(x)$ դաշտի մեջ եւ $\mathbb{Z}_3(x)[y]$ էվկլիդյան օղակի մեջ եւ կատարենք ըստ Էվկլիդեսի ալգորիթմի մնացորդով բաժանումը.

$$\begin{array}{l|l} (x+2)y+(2x+1) & xy+2x \\ \hline (x+2)y+\dfrac{(x+2)\cdot 2x}{x} & \dfrac{x+2}{x} \\ \hline 0 & \end{array}$$

Վերջին քայլում տարբերությունը 0 է ստացվել, քանի որ $\mathbb{Z}_3(x)$ քանորդների օղակում ունենք $\frac{(x+2)\cdot 2x}{x} = \frac{2x^2+x}{x} = 2x+1$: Այսինքն՝ $\mathbb{Z}_3(x)[y]$ օղակում մեր բազմանդամների ամենամեծ ընդհանուր բաժանարարն է $h(y) = \big(f(y), g(y)\big) = xy + 2x$: Մյուս կողմից, $h(y)$-ը չի բաժանում $f(y)$-ը $\mathbb{Z}_3[x][y]$ օղակում, քանի որ $h(y)$-ի ավագ գործակից x-ը չի բաժանում $f(y)$-ի ավագ գործակիցը՝ $x+2$: Այսինքն՝ $\mathbb{Z}_3(x)[y]$ եւ $\mathbb{Z}_3[x][y]$ օղակներում բազմանդամների ամենամեծ ընդհանուր բաժանարները կարող են եւ տարբեր լինել, եւ առաջին օղակում դրա հաշվումը դեռ չի ապահովում խնդրի լուծումը երկրորդ օղակում: Այս բարդությունը կշրջանցենք քիչ հետո:

Վերցնենք $f(x,y), g(x,y) \in K[x,y] \cong K[x][y]$ բազմանդամների զույգը: Բաց թողնենք պարզագույն դեպքը, երբ դրանցից մեկը զրոյական է: Համարենք նաեւ, որ բազմանդամները պրիմիտիվ են որպես $K[x][y]$ օղակի տարրեր, այսինքն, դրանց գործակիցների (որպես $K[x]$-ի տարրերի) ամենամեծ ընդհանուր բաժանարարը K^*-ից է: Քանի որ $K[x][y]$-ը ներդրված է $K(x)[y]$-ի մեջ, համարենք $f(y), g(y) \in K[x][y]$ բազմանդամները նաեւ $K(x)[y]$ էվկլիդյան օղակի տարրեր, եւ 6.4.1 օրինակի նմանությամբ հաշվենք դրանց $h(y)$ ամենամեծ ընդհանուր բաժանարարը $K(x)[y]$-ում: Ունենք $f(y) = h(y)\cdot q_1(y)$ եւ $g(y) = h(y)\cdot q_2(y)$, որտեղ $q_1(y), q_2(y) \in K(x)[y]$: Ներկայացնենք $h(y)$-ը (6.22) տեսքով՝

$$h(y) = \frac{c_0(x)}{d_0(x)}y^n + \cdots + \frac{c_n(x)}{d_n(x)}:$$

Շնորհիվ $K[x]$ օղակի էվկլիդյանության, $d_i(x)$ ոչ զրոյական հայտարարների համար գոյություն ունի դրանց ամենափոքր ընդհանուր բազմապատիկը՝

$$s(x) = [d_0(x), \dots, d_n(x)] \in K[x]:$$

$t(x)$-ով նշանակենք $q_1(y)$, $q_2(y)$ բազմանդամների բոլոր գործակիցների հայտարարների ամենափոքր ընդհանուր բազմապատիկը: Կունենանք

$$\begin{aligned} s(x)t(x)\cdot f(y) &= s(x)h(y)\cdot t(x)q_1(y), \\ s(x)t(x)\cdot g(y) &= s(x)h(y)\cdot t(x)q_2(y): \end{aligned} \tag{6.23}$$

Քանի որ $s(x)$-ը բաժանվում է $h(y)$-ի բոլոր գործակիցների հայտարարների վրա, իսկ $t(x)$-ը բաժանվում է $q_1(y)$-ի եւ $q_2(y)$-ի բոլոր գործակիցների հայտարարների

վրա, ապա (6.23)-ի երկու հավասարությունների աջ մասերն էլ կպատկանեն $K[x][y]$ օղակին, եւ $s(x)h(y)$ բազմանդամը կլինի $s(x)t(x)\cdot f(y)$ եւ $s(x)t(x)\cdot g(y)$ բազմանդամների ընդհանուր բաժանարարը $K[x][y]$-ում:

$K[x][y]$ օղակում $f(y)$ եւ $g(y)$ բազմանդամները չեն կարող ունենալ ավելի բարձր աստիճանի ընդհանուր բաժանարար, քան $K(x)[y]$ օղակում ($K[x][y]$-ում բազմանդամների բաժանելիությունից բխում է $K(x)[y]$-ում նույն բազմանդամների բաժանելիությունը): Քանի որ $K(x)[y]$-ում դրանց *ամենամեծ* ընդհանուր բաժանարարը $h(y)$-ն է, ապա $s(x)\cdot h(y)$-ի y-աստիճանը հավասար է $K[x][y]$ օղակում $f(y)$ եւ $g(y)$ բազմանդամների ամենամեծ ընդհանուր բաժանարարի y-աստիճանին: Քանի որ $f(y)$ եւ $g(y)$ բազմանդամները պրիմիտիվ են, ապա, ըստ 6.3.5 հետեւանքի, պրիմիտիվ է եւ նրանց ամենամեծ ընդհանուր բաժանարարը: Ուրեմն՝

$$\big(f(x,y),g(x,y)\big)=\big(f(y),g(y)\big)=\mathrm{pp}\big(s(x)\cdot h(y)\big):$$

Ընդհանուր դեպքը, երբ բազմանդամները պրիմիտիվ չեն, հեշտությամբ բերվում է քննարկված դեպքին: Վերցնենք

$$f(y)=\mathrm{cont}\big(f(y)\big)\mathrm{pp}\big(f(y)\big)\quad\text{եւ}\quad g(y)=\mathrm{cont}\big(g(y)\big)\mathrm{pp}\big(g(y)\big)$$

ներկայացումները եւ Էվկլիդեսի ալգորիթմով հաշվենք $\mathrm{cont}\big(f(y)\big)$, $\mathrm{cont}\big(g(y)\big)\in K[x]$ բովանդակությունների (որպես K դաշտի վրա տրված մեկ փոփոխականի բազմանդամների) ամենամեծ ընդհանուր բաժանարարը.

$$r(x)=\Big(\mathrm{cont}\big(f(y)\big),\mathrm{cont}\big(g(y)\big)\Big)\in K[x]:$$

Քանի որ $\mathrm{pp}\big(f(y)\big)$ եւ $\mathrm{pp}\big(g(y)\big)$ բազմանդամները պրիմիտիվ են, ապա քիչ առաջ բերված եղանակով հաշվենք դրանց

$$\Big(\mathrm{pp}\big(f(y)\big),\mathrm{pp}\big(g(y)\big)\Big)=\mathrm{pp}\big(s(x)\cdot h(y)\big)$$

ամենամեծ ընդհանուր բաժանարարը: Վերջնական պատասխանը ստացվում է հետեւյալ տեսքով՝ $\big(f(x,y),g(x,y)\big)=\big(f(y),g(y)\big)=r(x)\cdot\mathrm{pp}\big(s(x)\cdot h(y)\big)\in K[x][y]$:

6.4.2 Խնդիր. Համեմատել բերված կառուցումները 2.6.20 ալգորիթմի հիմնավորման հետ:

Այսպիսով մենք կառուցեցինք հետեւյալ ալգորիթմը.

6.4.3 Ալգորիթմ (դաշտի վրա տրված երկու փոփոխականների բազմանդամային օղակում ամենամեծ ընդհանուր բաժանարարի հաշվման ալգորիթմը). Տրված են $f(x,y),\ g(x,y)\in K[x,y]$ ոչ զրոյական բազմանդամները, որտեղ K-ն կամայական դաշտ է: Հաշվել նրանց $\big(f(x,y),\ g(x,y)\big)$ ամենամեծ ընդհանուր բաժանարարը:

1. Ըստ $K[x,y] \cong K[x][y]$ իզոմորֆիզմի՝ խմբավորենք $f(x,y)$ եւ $g(x,y)$ բազմանդամների միանդամները ըստ y-ի աստիճանների եւ ներկայացնենք դրանք $f(x,y) = a_0(x)y^n + \cdots + a_n(x) \in K[x][y]$ եւ $g(x,y) = b_0(x)y^m + \cdots + b_m(x) \in K[x][y]$ տեսքով, որտեղ $a_0(x), \dots, a_n(x); b_0(x), \dots, b_m(x) \in K[x]$:

2. $K[x]$ օղակում էվկլիդեսի ալգորիթմով հաշվենք $\operatorname{cont}\big(f(y)\big) = \big(a_0(x), \dots, a_n(x)\big)$ եւ $\operatorname{cont}\big(g(y)\big) = \big(b_0(x), \dots, b_m(x)\big)$ բովանդակությունները:

3. $K[x]$ օղակում էվկլիդեսի ալգորիթմով հաշվենք $r(x) = \Big(\operatorname{cont}\big(f(y)\big),\ \operatorname{cont}\big(g(y)\big)\Big) \in K[x]$ ամենամեծ ընդհանուր բաժանարարը:

4. Նշանակենք $f(y) = \operatorname{pp}\big(f(y)\big)$ եւ $g(y) = \operatorname{pp}\big(g(y)\big)$:

5. $K[x]$ ամբողջության տիրույթն, ըստ 4.2.4 հետեւանքի, ներդնենք $\operatorname{Quot}(K[x])$ քանորդների դաշտի, այսինքն, K դաշտի վրա ռացիոնալ ֆունկցիաների $K(x)$ դաշտի մեջ:

6. $f(y)$ եւ $g(y)$ բազմանդամների համար $K(x)$ դաշտի վրա տրված $K(x)[y]$ օղակում Էվկլիդեսի ալգորիթմով հաշվենք դրանց $h(y) = \big(f(y), g(y)\big) \in K(x)[y]$ ամենամեծ ընդհանուր բաժանարարը:

7. $h(y) \in K(x)[y]$ բազմանդամի գործակիցների (ռացիոնալ ֆունկցիաների) հայտարարները ոչ զրոյական բազմանդամներ են $K[x]$ օղակից: $K[x]$-ում էվկլիդեսի ալգորիթմով հաշվենք այդ հայտարարների $s(x)$ ամենափոքր ընդհանուր բազմապատիկը:

8. $K[x]$ օղակում էվկլիդեսի ալգորիթմով հաշվենք $s(x) \cdot h(y)$-ի $\operatorname{cont}\big(s(x) \cdot h(y)\big) \in K[x]$ բովանդակությունը (ըստ $s(x)$-ի ընտրության, $s(x) \cdot h(y) \in K[x][y]$):

9. Նշանակենք $d(y) = \operatorname{pp}\big(s(x) \cdot h(y)\big) = s(x) \cdot h(y) / \operatorname{cont}\big(s(x) \cdot h(y)\big)$:

10. Որոնելի ամենամեծ ընդհանուր բաժանարարը դուրս գրենք $r(x) \cdot d(y)$ տեսքով:

6.4.4 Օրինակ. $\mathbb{Z}_5[x,y]$ օղակում դիտարկենք $f(x,y) = 3x^2y^2 + 3x^3y + 4x^4$ եւ $g(x,y) = xy^2 + 2x^2y + 2x^2 + xy$ բազմանդամները: Ներկայացնենք դրանք $f(y) = 3x^2y^2 + 3x^3y + 4x^4 \in \mathbb{Z}_5[x][y]$ եւ $g(y) = xy^2 + (2x^2 + x)y + 2x^2 \in \mathbb{Z}_5[x][y]$ տեսքով, այսինքն, $a_0(x) = 3x^2$, $a_1(x) = 3x^3$, $a_2(x) = 4x^4$; $b_0(x) = x$, $b_1(x) = 2x^2 + x$, $b_2(x) = 2x^2$: Հեշտ է հաշվել, որ $\operatorname{cont}\big(f(y)\big) = (3x^2,\ 3x^3,\ 4x^4) = x^2$ եւ $\operatorname{cont}\big(g(y)\big) = (x,\ 2x^2 + x,\ 2x^2) = x$: Այսինքն՝ $r(x) = (x^2,\ x) = x \in \mathbb{Z}_5[x]$ եւ կարող ենք անցում կատարել պրիմիտիվ մասերին. $f(y) = \operatorname{pp}\big(f(y)\big) = f(y)/x^2 = 3y^2 + 3xy + 4x^2$,

$g(y)=\mathrm{pp}\big(g(y)\big)=g(y)/x=y^2+(2x+1)y+2x$: Կիրառենք Էվկլիդեսի ալգորիթմը նոր $f(y),\ g(y)$ բազմանդամների վրա $\mathbb{Z}_5(x)[y]$ օղակում.

$$\begin{array}{l|l} 3y^2+3xy+4x^2 & y^2+(2x+1)y+2x \\ \hline 3y^2+(x+3)y+x & 3 \\ \hline (2x+2)y+(4x^2+4x) & \end{array}$$

$$\begin{array}{l|l} y^2+(2x+1)y+2x & (2x+2)y+(4x^2+4x) \\ \hline y^2+\dfrac{2x^2+2x}{x+1}y & \dfrac{1}{2x+2}y+\dfrac{1}{2x+2} \\ \hline y+2x & \\ \hline y+2x & \\ \hline 0 & \end{array}$$

Վերջին բաժանման մեջ, օրինակ, $(4x^2+4x)\frac{1}{2x+2}y=\frac{2x^2+2x}{x+1}y$, իսկ $(2x+1)y-\frac{2x^2+2x}{x+1}y=\frac{(2x+1)(x+1)-(2x^2+2x)}{x+1}y=\frac{2x^2+3x+1-(2x^2+2x)}{x+1}y=\frac{x+1}{x+1}y=y$: Այսինքն՝ $\mathbb{Z}_5(x)[y]$ օղակում որոնելի ամենամեծ ընդհանուր բաժանարարն է $h(y)=(2x+2)y+(4x^2+4x)$ բազմանդամը: Այս օրինակում, բարեբախտաբար, բոլոր գործակիցները արդեն իսկ $\mathbb{Z}_5[x]$-ից են (ռացիոնալ ֆունկցիաների հայտարարները տրիվիալ են), ուստի կարելի է վերցնել $s(x)=1$: Քանի որ

$$\mathrm{cont}\big(s(x)h(y)\big)=\mathrm{cont}\big(h(y)\big)=(2x+2,4x^2+4x)=2x+2,$$

ապա $\mathrm{pp}\big(s(x)\cdot h(y)\big)=\big((2x+2)y+(4x^2+4x)\big)/(2x+2)=y+2x$: Իսկ վերջնական պատասխանը կհաշվվի հետեւյալ տեսքով՝

$$\big(f(x,y),g(x,y)\big)=r(x)\cdot\mathrm{pp}\big(s(x)\cdot h(y)\big)=x(y+2x)=xy+2x^2:$$

6.4.5 Վարժություն. 6.4.1 օրինակում, նախքան 6.4.3 ալգորիթմի կառուցումը, մենք կարողացանք հաշվել $f(x,y)=xy+2y+2x+1$ եւ $g(x,y)=xy+2x$ բազմանդամների $xy+2x$ ամենամեծ ընդհանուր բաժանարարը միայն $\mathbb{Z}_3(x)[y]$ էվկլիդյան օղակում: Տեսանք նաեւ, որ այն այլեւս ամենամեծ ընդհանուր բաժանարար չէ $\mathbb{Z}_3[x][y]$ օղակում: Կիրառել 6.4.3 ալգորիթմը եւ գտնել $\big(f(x,y),g(x,y)\big)$-ը $\mathbb{Z}_3[x][y]$-ում:

Քանի որ այս պարագրաֆում մինչ այժմ բերված բոլոր օրինակները վերջավոր բնութագրիչի դաշտերի վրա էին ($p=3$ կամ $p=5$), հակիրճ բերենք նաեւ մի օրինակ զրոյական բնութագրիչի $K=\mathbb{Q}$ դաշտի համար:

6.4.6 Օրինակ. $\mathbb{Q}[x,y] \cong \mathbb{Q}[x][y]$ օղակում դիտարկենք $f(x,y) = xy^3 + 2xy^2 + y^2 + 2y = xy^3 + (2x+1)y^2 + 2y$ եւ $g(x,y) = 3x^2y^2 + x^2y + 3xy + x = 3x^2y^2 + (x^2 + 3x)y + x$ բազմանդամները: Ակնհայտորեն $\mathrm{cont}\big(f(y)\big) = 1$ եւ $\mathrm{cont}\big(g(y)\big) = (3x^2,\, x^2 + 3x, x) = x$: Ուստի ունենք $r(x) = (1,x) = 1 \in \mathbb{Q}[x]$ եւ $f(y) = \mathrm{pp}\big(f(y)\big)$, $\mathrm{pp}\big(g(y)\big) = g(y)/x = 3xy^2 + (x+3)y + 1$: Կիրառենք Էվկլիդեսի ալգորիթմը $\mathbb{Q}(x)[y]$ օղակում.

$$\begin{array}{l|l} xy^3 + (2x+1)y^2 + 2y & 3xy^2 + (x+3)y + 1 \\ \cline{2-2} xy^3 + \dfrac{x+3}{3}y^2 + \dfrac{1}{3}y & \dfrac{1}{3}y + \dfrac{5}{9} \\ \cline{1-1} \dfrac{5x}{3}y^2 + \dfrac{5}{3}y & \\ \dfrac{5x}{3}y^2 + \dfrac{5x+15}{9}y + \dfrac{5}{9} & \\ \cline{1-1} -\dfrac{5x}{9}y - \dfrac{5}{9} & \end{array}$$

$$\begin{array}{l|l} 3xy^2 + (x+3)y + 1 & -\dfrac{5x}{9}y - \dfrac{5}{9} \\ \cline{2-2} 3xy^2 + 3y & -\dfrac{27}{5}y - \dfrac{5}{9} \\ \cline{1-1} xy + 1 & \\ xy + 1 & \\ \cline{1-1} 0 & \end{array}$$

Այսինքն՝ $\mathbb{Q}(x)[y]$ օղակում $h(y) = -\frac{5x}{9}y - \frac{5}{9}$: Վերցնենք $s(x) = 9$: Այդ դեպքում $d(y) = \mathrm{pp}\big(s(x)\cdot h(y)\big) = (-5xy - 5)/(-5) = xy + 1$: Վերջնական պատասխանն է

$$\big(f(x,y), g(x,y)\big) = r(x)\cdot d(y) = 1\cdot(xy+1) = xy+1:$$

Հասկանալի է, որ $\mathbb{Q}$-ում 5-ը կամ -5-ը հակադարձելի են: Այսինքն՝ ճիշտ էր նաեւ $5xy + 5$ կամ $-5xy - 5$ պատասխանը: Դրանք ասոցացված են $xy + 1$ բազմանդամին: Մենք, սակայն, ընտրեցինք ամենապարզ գրությամբ պատասխանը:

6.4.7 Վարժություն. Քննարկված 6.4.1, 6.4.4 եւ 6.4.6 օրինակներում մենք օգտվեցինք, համապատասխանաբար, $\mathbb{Z}_3[x,y] \cong \mathbb{Z}_3[x][y]$, $\mathbb{Z}_5[x,y] \cong \mathbb{Z}_5[x][y]$ եւ $\mathbb{Q}[x,y] \cong \mathbb{Q}[x][y]$ իզոմորֆիզմներից: Ամենամեծ բաժանարարը հաշվել նույն օրինակների բազմանդամների համար՝ օգտվելով $\mathbb{Z}_3[x,y] \cong \mathbb{Z}_3[y][x]$, $\mathbb{Z}_5[x,y] \cong \mathbb{Z}_5[y][x]$ եւ $\mathbb{Q}[x,y] \cong \mathbb{Q}[y][x]$ իզոմորֆիզմներից: Այսինքն՝ բազմանդամների միանդամների

խմբավորում կատարել ոչ թե ըստ y, այլ ըստ x փոփոխականի: Օրինակ՝ 6.4.6 օրինակներում քննարկել $f(x,y)=xy^3+2xy^2+y^2+2y=(y^3+2y^2)x+(y^2+2y)$ եւ $g(x,y)=3x^2y^2+x^2y+3xy+x=(3y^2+y)x^2+(3y+1)x$ բազմանդամները:

6.4.8 Վարժություն. Կոմպլեքս թվերի դաշտի վրա տրված երկու փոփոխականների բազմանդամների $\mathbb{C}[x,y]$ օղակում գտնել հետեւյալ բազմանդամների ամենամեծ ընդհանուր բաժանարարը.

$$f(x,y)=(9+6i)x^4y+3x^2y^2+(6i-4)x^3+2ixy,$$
$$g(x,y)=6ix^2y^2+3x^3y-4xy+2ix^2:$$

Չնայած 6.4.3 ալգորիթմը գործում է ցանկացած դաշտի, այդ թվում եւ՝ հաճախ օգտագործվող $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p$ դաշտերի համար, նրա ակնհայտ թերությունն այն է, որ այն չի գործում ամբողջ թվերի $\mathbb{Z}$ օղակի համար: Ալգորիթմի հիմնավորումը փոխելով՝ կարելի է այն տարածել նաեւ $\mathbb{Z}$-ի համար: Մեզ պետք կգա հետեւյալ դաշտը.

6.4.9 Օրինակ. Եթե $R=\mathbb{Z}[x]$, ապա համապատասխան $\mathbb{Z}(x)=\mathrm{Quot}(\mathbb{Z}[x])$ քանորդների դաշտը բաղկացած է

$$\frac{a_0x^n+\cdots+a_n}{b_0x^m+\cdots+b_m} \tag{6.24}$$

տեսքի կոտորակներից, որտեղ $a_0,\dots,a_n;b_0,\dots,b_m$ գործակիցներն ամբողջ թվեր են, եւ $b_0\neq 0$: Սա ավելի մեծ օղակ է, քան ռացիոնալ գործակիցներով բազմանդամների $\mathbb{Q}[x]$ օղակը: Յուրաքանչյուր $\frac{c}{d}\in\mathbb{Q}$ ռացիոնալ թիվ (6.24) տեսքի է, երբ $n=m=0$: Ավելին, ռացիոնալ գործակիցներով յուրաքանչյուր $f(x)=\frac{c_0}{d_0}x^n+\cdots+\frac{c_n}{d_n}\in\mathbb{Q}[x]$ բազմանդամ կարելի է բերել (6.24) տեսքի: Իսկապես, $d_0,\dots,d_n$ հայտարարների ամենափոքր ընդհանուր բազմապատիկը նշանակենք s: Այդ դեպքում

$$f(x)=\frac{1}{s}\left(\frac{sc_0}{d_0}x^n+\cdots+\frac{sc_n}{d_n}\right)=\frac{l_0x^n+\cdots+l_n}{s}\in\mathbb{Z}(x),$$

քանի որ բոլոր $\frac{sc_i}{d_i}=l_i$ կոտորակներն ամբողջ են $i=1,\dots,n$: Այսինքն՝ $\mathbb{Q}[x]$-ը բաղկացած է $\mathbb{Z}(x)$-ի այն (6.24) տեսքի ռացիոնալ ֆունկցիաներից, որոնց հայտարարի աստիճանը զրոյական է: $\mathbb{Z}(x)$-ը դաշտ է: Օրինակ՝ $(2x+3)^{-1}=\frac{1}{2x+3}\in\mathbb{Z}(x)$:

Վերցնենք ոչ զրոյական $f(x,y),g(x,y)\in\mathbb{Z}[x,y]\cong\mathbb{Z}[x][y]$ բազմանդամները: Կրկին, նախ, համարենք, որ բազմանդամները պրիմիտիվ են: Քանի որ $\mathbb{Z}[x][y]$-ը ներդրված է $\mathbb{Z}(x)[y]$-ի մեջ, համարենք, որ $f(y),g(y)\in\mathbb{Z}[x][y]$ բազմանդամները $\mathbb{Z}(x)[y]$ օղակի տարրեր են, եւ Էվկլիդեսի ալգորիթմով հաշվենք դրանց $h(y)\in\mathbb{Z}(x)[y]$ ամենամեծ ընդհանուր բաժանարարը: $f(y)=h(y)\cdot q_1(y)$ եւ $g(y)=h(y)\cdot$

$q_2(y)$, որտեղ $q_1(y), q_2(y) \in \mathbb{Z}(x)[y]$: Ունենք $h(y) = \frac{c_0(x)}{d_0(x)} y^n + \cdots + \frac{c_n(x)}{d_n(x)}$: Հայտարարների $d_i(x)$ ոչ զրոյական բազմանդամների համար վերցնենք $s(x) = [d_0(x), \dots, d_n(x)] \in \mathbb{Z}[x]$: Իսկ $t(x)$-ով նշանակենք $q_1(y)$, $q_2(y)$ բազմանդամների բոլոր գործակիցների հայտարարների ամենափոքր ընդհանուր բազմապատիկը $\mathbb{Z}[x]$-ում: $s(x)$-ի եւ $t(x)$-ի հաշվման համար այլեւս չենք կարող օգտվել Էվկլիդեսի ալգորիթմից (ի տարբերություն նախորդ ալգորիթմի հիմնավորումների), քանի որ $\mathbb{Z}[x]$-ն Էվկլիդյան օղակ չէ: Այնուամենայնիվ, 3-րդ գլխում մենք մի շարք էֆեկտիվ ալգորիթմներ ենք կառուցել, որոնցից յուրաքանչյուրով կարելի է հաշվել $\mathbb{Z}[x]$-ի ոչ զրոյական $d_0(x), \dots, d_n(x)$ բազմանդամների $\big(d_0(x), \dots, d_n(x)\big)$ ամենամեծ ընդհանուր բաժանարարը եւ

$$[d_0(x), \dots, d_n(x)] = d_0(x) \cdots d_n(x) / \big(d_0(x), \dots, d_n(x)\big)$$

ամենափոքր ընդհանուր բազմապատիկը: Այստեղ կիրառենք դրանցից կամայականը, օրինակ, Մեծ պարզ թվի 3.4.8 ալգորիթմը կամ էլ 2.6.20 ալգորիթմը, որն ավելի պարզ հիմնավորում ունի՝ չնայած այն պակաս արդյունավետ է եւ կապված է միջանկյալ արժեքների ուռճացման խնդրի հետ: Նշված ալգորիթմները մենք ձեւակերպել էինք միայն *երկու* բազմանդամների դեպքի համար, սակայն եթե բազմանդամների քանակն ավելի շատ է, ապա դարձյալ կարելի է դրանց ամենամեծ ընդհանուր բաժանարարը հաշվել այդ ալգորիթմների հաջորդական կիրառության միջոցով: Օրինակ՝ նախ կարելի է հաշվել $h_1(x) = \big(d_0(x), d_1(x)\big)$, ապա $h_2(x) = \big(d_0(x), d_1(x), d_2(x)\big) = \big(h_1(x), d_2(x)\big)$, եւ վերջին քայլում ինդուկցիայով ստանալ

$$h_n(x) = \big(d_0(x), \dots, d_n(x)\big) = \big(h_{n-1}(x), d_n(x)\big):$$

Հաշվված $s(x)$ եւ $t(x)$ բազմանդամների օգնությամբ այստեղ եւս ստանում ենք (6.23) հավասարությունները, որտեղ երկու հավասարությունների աջ մասերն էլ կպատկանեն $\mathbb{Z}[x][y]$ օղակին, եւ $s(x)h(y)$ բազմանդամը կլինի $s(x)t(x) \cdot f(y)$ եւ $s(x)t(x) \cdot g(y)$ բազմանդամների ընդհանուր բաժանարարը $\mathbb{Z}[x][y]$-ում: $\mathbb{Z}[x][y]$ օղակում $f(y)$ եւ $g(y)$ բազմանդամները չեն կարող ունենալ ավելի բարձր աստիճանի ընդհանուր բաժանարար, քան $\mathbb{Z}(x)[y]$ օղակում: Քանի որ $f(y)$ եւ $g(y)$ բազմանդամները պրիմիտիվ են, ապա, ըստ 6.3.5 հետեւանքի, պրիմիտիվ է եւ նրանց ամենամեծ ընդհանուր բաժանարարը.

$$\big(f(x,y), g(x,y)\big) = \big(f(y), g(y)\big) = \mathrm{pp}\big(s(x) \cdot h(y)\big):$$

Ընդհանուր դեպքը բերվում է նախորդ դեպքին նույն սկզբունքով, ինչ $K[x][y]$ օղակի համար: Բազմանդամները նախ ներկայացնենք $f(y) = \mathrm{cont}\big(f(y)\big)\mathrm{pp}\big(f(y)\big)$

եւ $g(y) = \mathrm{cont}\big(g(y)\big)\mathrm{pp}\big(g(y)\big)$ տեսքով, որտեղ $\mathrm{cont}\big(f(y)\big)$, $\mathrm{cont}\big(g(y)\big) \in \mathbb{Z}[x]$ բովանդակությունները (որպես $\mathbb{Z}$-ի վրա տրված մեկ փոփոխականի բազմանդամների ամենամեծ ընդհանուր բաժանարարը) կարելի է հաշվել 3.4.8 կամ 2.6.20 ալգորիթմներից որեւէ մեկով: Նույն ալգորիթմներից որեւե մեկով հաշվենք նաեւ

$$r(x) = \Big(\mathrm{cont}\big(f(y)\big), \mathrm{cont}\big(g(y)\big)\Big) \in \mathbb{Z}[x]:$$

Քանի որ $\mathrm{pp}\big(f(y)\big)$ եւ $\mathrm{pp}\big(g(y)\big)$ բազմանդամները պրիմիտիվ են, ապա վերը բերված եղանակով հաշվենք $\Big(\mathrm{pp}\big(f(y)\big), \mathrm{pp}\big(g(y)\big)\Big) = \mathrm{pp}\big(s(x) \cdot h(y)\big)$: Վերջնական պատասխանը ստացվում է հետեւյալ տեսքով.

$$\big(f(x,y), g(x,y)\big) = \big(f(y), g(y)\big) = r(x) \cdot \mathrm{pp}\big(s(x) \cdot h(y)\big) \in \mathbb{Z}[x][y]:$$

Ձեւակերպենք կառուցված ալգորիթմը.

6.4.10 Ալգորիթմ ($\mathbb{Z}[x,y]$ բազմանդամային օղակում ամենամեծ ընդհանուր բաժանարարի հաշվման ալգորիթմը). Տրված են $f(x,y)$, $g(x,y) \in \mathbb{Z}[x,y]$ ոչ զրոյական բազմանդամները: Հաշվել նրանց $\big(f(x,y),\ g(x,y)\big)$ ամենամեծ ընդհանուր բաժանարարը:

1. Ըստ $\mathbb{Z}[x,y] \cong \mathbb{Z}[x][y]$ իզոմորֆիզմի՝ խմբավորենք $f(x,y)$ եւ $g(x,y)$ բազմանդամների միանդամներն ըստ y-ի աստիճանների եւ ներկայացնենք դրանք $f(x,y) = a_0(x)y^n + \cdots + a_n(x) \in \mathbb{Z}[x][y]$ եւ $g(x,y) = b_0(x)y^m + \cdots + b_m(x) \in \mathbb{Z}[x][y]$ տեսքով, որտեղ $a_0(x), \dots, a_n(x); b_0(x), \dots, b_m(x) \in \mathbb{Z}[x]$:

2. $\mathbb{Z}[x]$ օղակում 3.4.8 կամ 2.6.20 ալգորիթմներից որեւէ մեկով հաշվենք $\mathrm{cont}\big(f(y)\big) = \big(a_0(x), \dots, a_n(x)\big)$ եւ $\mathrm{cont}\big(g(y)\big) = \big(b_0(x), \dots, b_m(x)\big)$ բովանդակությունները:

3. $\mathbb{Z}[x]$ օղակում 3.4.8 կամ 2.6.20 ալգորիթմներից որեւէ մեկով հաշվենք $r(x) = \Big(\mathrm{cont}\big(f(y)\big),\ \mathrm{cont}\big(g(y)\big)\Big) \in \mathbb{Z}[x]$ ամենամեծ ընդհանուր բաժանարարը:

4. Նշանակենք $f(y) = \mathrm{pp}\big(f(y)\big)$ եւ $g(y) = \mathrm{pp}\big(g(y)\big)$:

5. $\mathbb{Z}[x]$ ամբողջության տիրույթն, ըստ 4.2.4 հետեւանքի, ներդնենք $\mathrm{Quot}(\mathbb{Z}[x])$ քանորդների դաշտի, այսինքն, $\mathbb{Z}$-ի վրա ռացիոնալ ֆունկցիաների $\mathbb{Z}(x)$ դաշտի մեջ:

6. $f(y)$ եւ $g(y)$ բազմանդամների համար $\mathbb{Z}(x)$ դաշտի վրա տրված $\mathbb{Z}(x)[y]$ օղակում Էվկլիդեսի ալգորիթմով հաշվենք դրանց $h(y) = \big(f(y), g(y)\big) \in \mathbb{Z}(x)[y]$ ամենամեծ ընդհանուր բաժանարարը:

7. $h(y) \in \mathbb{Z}(x)[y]$ բազմանդամի գործակիցների (ռացիոնալ ֆունկցիաների) հայտարարները ոչ զրոյական բազմանդամներ են $\mathbb{Z}[x]$ օղակից: $\mathbb{Z}[x]$-ում 3.4.8 կամ 2.6.20 ալգորիթմներից որեւէ մեկի հաջորդական կիրառությամբ հաշվենք այդ հայտարարների $s(x)$ ամենափոքր ընդհանուր բազմապատիկը:

8. $\mathbb{Z}[x]$ օղակում 3.4.8 կամ 2.6.20 ալգորիթմներից որեւէ մեկի հաջորդական կիրառությամբ հաշվենք $s(x) \cdot h(y)$ բազմանդամի $\operatorname{cont}\big(s(x) \cdot h(y)\big) \in \mathbb{Z}[x]$ բովանդակությունը (ըստ $s(x)$-ի ընտրության, $s(x) \cdot h(y) \in \mathbb{Z}[x][y]$):

9. Նշանակենք $d(y) = \operatorname{pp}\big(s(x) \cdot h(y)\big) = s(x) \cdot h(y)/\operatorname{cont}\big(s(x) \cdot h(y)\big)$:

10. Որոնելի ամենամեծ ընդհանուր բաժանարարը դուրս գրենք $r(x) \cdot d(y)$ տեսքով:

6.4.11 Օրինակ. Անդրադառնանք 6.4.6 օրինակում $\mathbb{Q}[x,y] \cong \mathbb{Q}[x][y]$ օղակի մեջ վերցված բազմանդամներին: Դրանց գործակիցները, որոնք նաեւ $\mathbb{Z}[x]$-ից էին, պարզ տեսք ունեին, եւ ամենամեծ ընդհանուր բաժանարարները եւ ամենափոքր ընդհանուր բազմապատիկները կարելի էր հաշվել նաեւ 3.4.8 կամ 2.6.20 ալգորիթմներից որեւէ մեկով:

6.4.12 Վարժություն. Օգտվելով 6.4.10 ալգորիթմից՝ հաշվել $\mathbb{Z}[x,y]$ օղակի հետեւյալ բազմանդամների ամենամեծ ընդհանուր բաժանարարը.

$$f(x,y) = 2x^3 + 6x^2 + x^3y + 5x^2y + 6xy + x^2y^2 + 3xy^2,$$
$$g(x,y) = 2x^2y^2 + 6xy^2 + x^2y^3 + 3xy^3 + 4x^2 + 12x + 2x^2y + 6xy:$$

Այս պարագրաֆի մնացած մասում L տառն օգտագործենք կամայական ֆիքսված K դաշտը (մասնավորապես, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p$ դաշտերից որեւէ մեկը) կամ $\mathbb{Z}$ օղակը նշանակելու համար: 6.4.3 եւ 6.4.10 ալգորիթմներով մենք կարող ենք L-ի վրա տրված երկու փոփոխականների բազմանդամների $L[x,y]$ օղակում ամենամեծ ընդհանուր բաժանարարի հաշվման խնդիրը հանգեցնել $L[x]$ օղակում համանման խնդրի լուծմանը: Շարունակելով քայլերը ինդուկցիայով՝ մենք կարող ենք L-ի վրա տրված $x_1, \dots, x_n$ փոփոխականների $L[x_1, \dots, x_n]$ օղակում ամենամեծ ընդհանուր բաժանարարի հաշվման խնդիրը հանգեցնել նման խնդրի լուծմանը $L[x_1, \dots, x_{n-1}]$ օղակում, այսինքն, բերել ավելի քիչ փոփոխականներ պարունակող բազմանդամների դեպքին: Իսկապես, ենթադրենք արդեն ունենք $L[x_1, \dots, x_{n-1}]$-ում ամենամեծ ընդհանուր բաժանարարի հաշվման ալգորիթմը: Օգտվելով $L[x_1, \dots, x_n] \cong L[x_1, \dots, x_{n-1}][x_n]$ իզոմորֆիզմից՝ տրված

$$f(x_1, \dots, x_n), g(x_1, \dots, x_n) \in L[x_1, \dots, x_n]$$

պրիմիտիվ բազմանդամներում ըստ x_n փոփոխականի, միանդամների միացում կատարելով, ներկայացնենք f-ը եւ g-ն որպես $L[x_1, \dots, x_{n-1}][x_n]$-ի բազմանդամներ, որոնց գործակիցները $L[x_1, \dots, x_{n-1}]$ օղակից են:

$L[x_1, \dots, x_{n-1}]$ ամբողջության տիրույթը, ըստ 4.2.4 հետեւանքի, ներդնենք

$$\mathrm{Quot}(L[x_1, \dots, x_{n-1}]) \cong L(x_1, \dots, x_{n-1})$$

քանորդների դաշտի մեջ, որի տարրերը L-ի վրա ռացիոնալ ֆունկցիաներ են ըստ $x_1, \dots, x_{n-1}$ փոփոխականների (կոտորակներ, որոնց համարիչն ու հայտարարը $L[x_1, \dots, x_{n-1}]$-ից են): $L(x_1, \dots, x_{n-1})$ դաշտի վրա տրված $L(x_1, \dots, x_{n-1})[x_n]$ էվկլիդյան օղակում Էվկլիդեսի ալգորիթմով հաշվենք $f,\ g$ բազմանդամների ամենամեծ ընդհանուր $h \in L(x_1, \dots, x_{n-1})[x_n]$ բաժանարարը: h-ի գործակիցները կոտորակներ են, որոնց հայտարարները $L[x_1, \dots, x_{n-1}]$-ից են: Իսկ այդ օղակում արդեն ունենք ամենամեծ ընդհանուր բաժանարարի հաշվման ալգորիթմը, որի միջոցով կարող ենք հաշվել նշված հայտարարների

$$s = s(x_1, \dots, x_{n-1}) \in L[x_1, \dots, x_{n-1}]$$

ամենամեծ ընդհանուր բաժանարարը: Կրկնելով 6.4.3 եւ 6.4.10 ալգորիթմների հիմնավորման փաստարկը՝ ստանում ենք, որ $(f, g) = \mathrm{pp}(s \cdot h)$:

Կամայական ոչ զրոյական $f, g \in L[x_1, \dots, x_n]$ բազմանդամների դեպքը բերվում է քննարկվածին: $L[x_1, \dots, x_{n-1}]$-ում ամենամեծ ընդհանուր բաժանարարի հաշվման ալգորիթմը հաջորդաբար կիրառելով f, g բազմանդամների գործակիցների վրա, կստանանք $\mathrm{cont}(f),\ \mathrm{cont}(g) \in L[x_1, \dots, x_{n-1}]$ բովանդակությունները: Նշանակենք

$$r = \big(\mathrm{cont}(f), \mathrm{cont}(g)\big) \in L[x_1, \dots, x_{n-1}]:$$

Քանի որ $\mathrm{pp}(f)$ եւ $\mathrm{pp}(g)$ բազմանդամները պրիմիտիվ են, ապա վերը բերված եղանակով հաշվենք $\big(\mathrm{pp}(f), \mathrm{pp}(g)\big) = \mathrm{pp}(s \cdot h)$: Վերջնական պատասխանը ստացվում է հետեւյալ տեսքով $(f, g) = \big(f(x_1, \dots, x_n), g(x_1, \dots, x_n)\big) = r \cdot \mathrm{pp}(s \cdot h) \in L[x_1, \dots, x_n]$: Ստացանք հետեւյալ ալգորիթմը.

6.4.13 Ալգորիթմ (դաշտի կամ $\mathbb{Z}$ օղակի վրա տրված n փոփոխականների բազմանդամային օղակում ամենամեծ ընդհանուր բաժանարարի հաշվման ալգորիթմը). Տրված են $f = f(x_1, \dots, x_n),\ g = g(x_1, \dots, x_n) \in L[x_1, \dots, x_n]$ ոչ զրոյական բազմանդամները, որտեղ L-ը կամ ցանկացած դաշտ է կամ էլ $\mathbb{Z}$ օղակն է: Տրված է $n-1$ փոփոխականների $L[x_1, \dots, x_{n-1}]$ օղակում ամենամեծ ընդհանուր բաժանարարի հաշվման ալգորիթմը: Հաշվել $(f,\ g)$ ամենամեծ ընդհանուր բաժանարարը:

1. Համաձայն $L[x_1,\dots,x_n]\cong L[x_1,\dots,x_{n-1}][x_n]$ իզոմորֆիզմի՝ խմբավորենք f եւ g բազմանդամների միանդամներն ըստ x_n-ի աստիճանների եւ ներկայացնենք դրանք $f=a_0y^n+\dots+a_n\in L[x_1,\dots,x_{n-1}][x_n]$ եւ $g=b_0y^m+\dots+b_m\in L[x_1,\dots,x_{n-1}][x_n]$ տեսքով, որտեղ $a_0,\dots,a_n;b_0,\dots,b_m\in L[x_1,\dots,x_{n-1}]$:

2. $L[x_1,\dots,x_{n-1}]$ օղակում ամենամեծ ընդհանուր բաժանարարի հաշվման ալգորիթմի հաջորդական կիրառությամբ հաշվենք $\mathrm{cont}(f)=(a_0,\dots,a_n)$ եւ $\mathrm{cont}(g)=(b_0,\dots,b_m)$ բովանդակությունները:

3. $L[x_1,\dots,x_{n-1}]$ օղակում ամենամեծ ընդհանուր բաժանարարի հաշվման ալգորիթմով հաշվենք այդ բովանդակությունների $r=\big(\mathrm{cont}(f),\ \mathrm{cont}(g)\big)\in L[x_1,\dots,x_{n-1}]$ ամենամեծ ընդհանուր բաժանարարը:

4. Նշանակենք $f=\mathrm{pp}(f)$ եւ $g=\mathrm{pp}(g)$:

5. $L[x_1,\dots,x_{n-1}]$ ամբողջության տիրույթն, ըստ 4.2.4 հետեւանքի, ներդնենք $\mathrm{Quot}(L[x_1,\dots,x_{n-1}])$ քանորդների դաշտի, այսինքն, L-ի վրա ռացիոնալ ֆունկցիաների $L(x_1,\dots,x_{n-1})$ դաշտի մեջ:

6. f եւ g բազմանդամների համար $L(x_1,\dots,x_{n-1})$ դաշտի վրա տրված էվկլիդյան $L(x_1,\dots,x_{n-1})[x_n]$ օղակում Էվկլիդեսի ալգորիթմով հաշվենք դրանց $h=(f,g)\in L(x_1,\dots,x_{n-1})[x_n]$ ամենամեծ ընդհանուր բաժանարարը:

7. $h\in L(x_1,\dots,x_{n-1})[x_n]$ բազմանդամի գործակիցների ($x_1,\dots,x_{n-1}$ փոփոխականների ռացիոնալ ֆունկցիաների) հայտարարները ոչ զրոյական բազմանդամներ են $L[x_1,\dots,x_{n-1}]$ օղակից: $L[x_1,\dots,x_{n-1}]$-ում ամենամեծ ընդհանուր բաժանարարի հաշվման ալգորիթմի հաջորդական կիրառությամբ հաշվենք այդ հայտարարների s ամենափոքր ընդհանուր բազմապատիկը:

8. $L[x_1,\dots,x_{n-1}]$ օղակում ամենամեծ ընդհանուր բաժանարարի հաշվման ալգորիթմի հաջորդական կիրառությամբ հաշվենք $s\cdot h$ բազմանդամի $\mathrm{cont}(s\cdot h)\in L[x_1,\dots,x_{n-1}]$ բովանդակությունը (ըստ s-ի ընտրության, $s\cdot h\in L[x_1,\dots,x_{n-1}][x_n]$):

9. Նշանակենք $d=\mathrm{pp}(s\cdot h)=s\cdot h/\mathrm{cont}(s\cdot h)$:

10. Որոնելի ամենամեծ ընդհանուր բաժանարարը դուրս գրենք $r\cdot d$ տեսքով:

6.4.14 Վարժություն. Օգտվելով 6.4.13 ալգորիթմից՝ հաշվել $L[x,y,z]$ օղակի հետեւյալ բազմանդամների ամենամեծ ընդհանուր բաժանարարը.

$f(x,y,z)=2x^2y^2+6xy^2+x^2y^3+3xy^3$, $g(x,y,z)=xy^2z+3x^2y+2y^2z+6xy$,

որտեղ L-ը հետեւյալ դաշտն է.

1) $L=\mathbb{Q}$, **2)** $L=\mathbb{Z}_7$, **3)** $L=\mathbb{Z}$:

7 Բազմանդամների ֆակտորիզացիան եւ արմատները

7.1 Բազմանդամի ֆակտորիզացիայի խնդիրը

Այս գլխում ուսումնասիրվելու են բազմանդամի ֆակտորիզացիայի եւ բազմանդամների արմատների հաշվման խնդիրները վերջավոր, ռացիոնալ, իրական, կոմպլեքս դաշտերի եւ ամբողջ թվերի օղակի վրա:

$f(x)$ ոչ զրոյական բազմանդամի ֆակտորիզացիան հասկացվում է 6.1.1 սահմանման իմաստով՝ $f(x)$-ը ներկայացվում է իր $p_i(x)$ տեսքի պարզ արտադրիչների եւ մի հակադարձելի ε տարրի արտադրյալի տեսքով: Եթե $\varepsilon = 1$, ապա այն կարելի է բաց թողնել ֆակտորիզացիայի գրությունից: Իսկ $p_i(x)$ արտադրիչները, կախված դիտարկվող օղակի բնույթից, կարող են լինել կամ միայն դրական աստիճանի որոշ պարզ բազմանդամներ, կամ էլ ցանկացած աստիճանի պարզ բազմանդամներ (ներառյալ զրոյական աստիճանը, երբ $p_i(x)$-ը հաստատուն է):

Պարզ է, որ 6.1.1 սահմանման մեջ տրված ֆակտորիզացիան միշտ գոյություն ունի $f(x) \in R[x]$ բազմանդամի համար, եթե R-ը որեւէ ֆակտորիալ օղակ է (տես 6.3.8 թեորեմը): Մասնավորապես, R-ը կարող է լինել ամբողջ թվերի $\mathbb{Z}$ օղակը կամ էլ կամայական դաշտ (ներառյալ $\mathbb{Z}_p$ դաշտը, կամայական վերջավոր K դաշտ կամ $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ դաշտերից որեւէ մեկը): Մենք հենց այս դեպքերն ենք թվարկում՝ շեշտելու համար, որ ֆակտորիզացիան տեղի ունի «հաճախակի օգտագործվող» բազմանդամների բոլոր հիմնական տիպերի համար:

Կարեւոր է նաեւ այն, որ ֆակտորիզացիան կապված է բազմանդամի արմատների հետ: Եթե $a \in R$ տարրը $f(x) \in R[x]$ բազմանդամի արմատ է, ապա քննարկվող հիմնական օղակներում $f(x)$-ը, ըստ Բեզուի թեորեմի, բաժանվում է $x - a$ գծային բազմանդամի վրա: Վերջինս ակնհայտորեն պարզ է, եւ շնորհիվ $R[x]$-ի ֆակտորիալության, ասոցացված է 6.1.1 սահմանման մեջ հիշատակված պարզ արտադրիչներից որեւէ մեկին: Այսինքն՝ տվյալ բազմանդամի ֆակտորիզացիան բացահայտորեն հաշվելով՝ մենք գտած կլինենք նաեւ նրա բոլոր արմատները R-ում:

Դժբախտաբար, ֆակտորիզացիայի գոյության փաստի ապացույցը միշտ չէ, որ նշանակում է, թե կարող ենք տալ այդ ֆակտորիզացիայի բացահայտ հաշվման որեւէ ալգորիթմ: Այսինքն՝ ֆակտորիզացիայի խնդիրն էապես տարբեր է, ասենք, ամենամեծ ընդհանուր բաժանարարի հաշվման կամ քառակուսիներից ազատ արտադրիչների հաշվման խնդիրներից, որոնց համար մենք միշտ կարող էինք կոնկրետ հաշվարկի ալգորիթմներ առաջարկել:

Ավելին, ամենամեծ ընդհանուր բաժանարարի կամ քառակուսիներից ազատ արտադրիչների հաշվման ալգորիթմներն էապես ոչնչով չէին փոխվում, երբ մենք, ասենք, $\mathbb{Q}[x]$ օղակից անցնում էինք $\mathbb{R}[x]$ կամ $\mathbb{C}[x]$ օղակներին: Այդ ալգորիթմները հենվում էին այն փաստի վրա, որ $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ դաշտերը երեքն էլ ունեն զրոյական բնութագրիչ: Իրավիճակն այլ է ֆակտորիզացիայի խնդրում: $\mathbb{Q}[x]$ օղակում ֆակտորիզացիայի ալգորիթմը կառուցվում է $\mathbb{Z}[x]$ օղակում ֆակտորիզացիայի ալգորիթմի օգնությամբ, իսկ $\mathbb{Z}[x]$ օղակում ֆակտորիզացիայի ալգորթիմը կառուցվում է ըստ $\mathbb{Z}_p[x]$ օղակում ֆակտորիզացիայի ալգորիթմի: Վերջինս էլ, իր հերթին, հնարավոր է կառուցել՝ օգտվելով վերջավոր դաշտի վրա գծային հանրահաշվի որոշ մեթոդներից: Իսկ $\mathbb{R}[x], \mathbb{C}[x]$ օղակներում տրված բազմանդամի ֆակտորիզացիայի հարցը կարող է լինել հանրահաշվորեն անլուծելի խնդիր, այսինքն, համապատասխան հանրահաշվական ալգորիթմն ընդհանուր դեպքում գոյություն չունի:

Վերջավոր դաշտի վրա օպերատորների եւ գծային հավասարումների համակարգերի մասին անհրաժեշտ փաստերը ստորեւ հավաքել ենք 7.2 պարագրաֆում: 7.3, 7.4 եւ 7.5 պարագրաֆներում ներկայացված են վերջավոր դաշտերի, $\mathbb{Z}$ օղակի եւ $\mathbb{Q}$ դաշտի վրա բազմանդամի ֆակտորիզացիայի ալգորիթմների կառուցումը:

Այդ մեթոդներն ընդհանրացնում են մոդուլյար անցումների մասին դեռ 2.4 պարագրաֆից հայտնի փաստերը: Թվային $\varphi_p \colon \mathbb{Z} \to \mathbb{Z}_p$, բազմանդամային $\varphi_p \colon \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ եւ մատրիցային $\varphi_p \colon M_n(\mathbb{Z}) \to M_n(\mathbb{Z}_p)$ մոդուլյար անցումներն օգնում են մեզ խնդիրը տեղափոխել $\mathbb{Z}_p$ դաշտի վրա: Ընդ որում, $\mathbb{Z}_p$-ի վրա մենք մինչ այժմ կիրառում էինք Էվկլիդյան օղակի ստրուկտուրան եւ մատրիցային հաշիվը: Այս գլխում ավելի ենք խորացնելու վերջավոր դաշտի վրա դիտարկվող մաթեմատիկական օբյեկտների ցանկը՝ ներգրավելով գծային տարածությունները, գծային օպերատորները, գծային հավասարումների համակարգերը եւլն:

Եզրափակիչ 7.6 պարագրաֆում քննարկվում են Գալուայի խմբի որոշ հատկություններ եւ դրանց օգնությամբ ցույց է տրվում, թե ինչո՞ւ է բազմանդամի ֆակ-

տորիզացիայի խնդիրը ընդհանուր դեպքում հանրահաշվորեն անլուծելի $\mathbb{R}$ եւ $\mathbb{C}$ դաշտերի վրա, եթե բազմանդամի աստիճանը մեծ է չորսից:

7.2 Գծային օպերատորներ վերջավոր դաշտի վրա

Գծային հանրահաշվի այնպիսի հասկացություններ, ինչպիսիք են գծային տարածությունը, գծային անկախությունն ու կախվածությունը, տարածության բազիսը եւ չափողականությունը, գծային օպերատորները, գծային հավասարումների համակարգերը ելլն, ծանոթ են հանրահաշվի ներածական դասընթացներից, եւ այստեղ այդ հասկացություններն օգտագործում ենք առանց սահմանելու (մենք արդեն մի քանի անգամ օգտագործել ենք դրանք նախորդ գլուխներում): Չնայած շատ դասընթացներում այդ հասկացությունները հաճախ դիտարկվում են միայն իրական եւ կոմպլեքս դաշտերի համար՝ կամայական դաշտի վրա դրանց քննարկումը որեւէ հավելյալ բարդություն չի առաջացնում: Որոշ տարբերություններ ծագում են՝ կապված վերջավոր դաշտերի հետ: Քանի որ հաջորդ պարագրաֆներում մեզ պետք են գալու վերջավոր դաշտերի վրա տրված տարածություններում օպերատորների եւ գծային հավասարաումների համակարգերի հետ առնչվող մի շարք այդպիսի փաստեր, այս պարագրաֆում համառոտ ներկայացնենք դրանց մի քանի հատկություններ:

Կամայական դաշտի վրա տրված տարածությունների եւ օպերատորների մասին հավելյալ տեղեկություններ կարելի է գտնել, օրինակ, (Cohn, 2003), (Dummit & Foote, 2004), (Garrett, 2008), (Hoffman & Kunze, 1971), (Кострикин, 1977), (Кострикин, 2000), (Кострикин & Манин, 1980), (Мальцев, 1970) դասագրքերում:

Ենթադրենք K-ն վերջավոր է եւ ունի $\mathrm{char}(K) = p$ պարզ բնութագրիչը: Ըստ 4.2.35 թեորեմի՝ $K = GF(p^n)$ եւ K-ի տարրերի քանակն է $|K| = p^n$: Վերջավոր K դաշտի վրա տրված վերջավոր չափողականության տարածությունները վերջավոր են, ի տարբերություն գծային հանրահաշվի դասընթացներում ավելի հաճախ քննարկվող իրական եւ կոմպլեքս դաշտերի վրա տրված տարածությունների, որոնք բոլորն անվերջ են (բացի այն տրիվիալ դեպքից, երբ տարածությունը բաղկացած է մեկ՝ զրոյական վեկտորից): Իսկապես, ըստ հավասար չափողականության տարածությունների իզոմորֆիզմի մասին թեորեմի, ցանկացած K դաշտի վրա տրված V եւ U տարածություններն իզոմորֆ են այն եւ միայն այն դեպքում, երբ $\dim V = \dim U$: Ցանկացած բնական m-ի համար K դաշտի վրա տրված տարածություններից մեկը m-յակների $K^m = \{(a_1, \dots, a_m) \mid x_i \in K,\ i = 1, \dots, m\}$ տարածությունն է, որի վրա վեկ-

տորների գումարումն ու սկալյարով բազմապատկումը սահմանվում է կոորդինատ-առ-կոորդինատ՝

$$(a_1, \dots, a_m) + (a'_1, \dots, a'_m) = (a_1 + a'_1, \dots, a_m + a'_m) \in K^m,$$
$$b(a_1, \dots, a_m) = (ba_1, \dots, ba_m) \in K^m \text{ ցանկացած } b \in K \text{ համար:}$$

$(a_1, \dots, a_m)$ տեսքի m-յակների քանակն է $|K|^m$: Հաշվի առնելով նաեւ K-ի տարրերի քանակը՝ ունենք.

7.2.1 Թեորեմ. *$K = GF(p^n)$ դաշտի վրա տրված m վերջավոր չափողականության ցանկացած V գծային տարածության տարրերի քանակն է $|V| = |K|^m = p^{nm}$:*

Մասնավորապես, եթե U-ն V-ի r չափողականության ենթատարածություն է ($r \le m$), ապա $|U| = |K|^r = p^{nr}$: Իսկ երբ $\dim U = 1$, ունենք $|U| = |K| = p^n$: Այսինքն՝ այն, ինչը իրական տարածություններում ընկալվում էր որպես երկու ուղղություններով «անվերջ շարունակվող» ուղիղ գիծ (մեկ չափողականության ենթատարածություն), $K = GF(p^n)$ դաշտի վրա բաղկացած է ընդամենը վերջավոր p^n քանակությամբ կետերից: Նույն կերպ՝ վերջավոր քանակությամբ կետերից է բաղկացած նաեւ հարթությունը. եթե $K = GF(p^n)$ եւ $\dim U = 2$, ապա $|U| = |K|^2 = p^{2n}$: Իսկ եթե $\dim U = 3$, ապա $|U| = |K|^3 = p^{3n}$ եւլն:

Ամենապարզ դեպքում, երբ $n = 1$ եւ K-ն $\mathbb{Z}_p$ դաշտն է, ունենք.

7.2.2 Հետեւանք. $\mathbb{Z}_p$ դաշտի վրա տրված m վերջավոր չափողականության ցանկացած V գծային տարածության տարրերի քանակն է $|V| = p^m$:

Մասնավորապես՝ $\mathbb{Z}_p$-ի վրա մեկ, երկու, երեք չափողականության տարածությունների տարրերի քանակն է, համապատասխանաբար, p, p^2, p^3: Ասենք, $K = \mathbb{Z}_3$ դեպքում երեք չափողականության $V = \mathbb{Z}_3^3$ տարածությունը «նման է» հայտնի խաղի Ռուբիկի խորանարդին եւ բաղկացած է միայն 27 կետերից: Սա հուշում է, որ այսպիսի տարածության մեջ ինչ-որ վեկտոր որոնելը անհամեմատ ավելի պարզ խնդիր է, քան իրական կամ կոմպլեքս դաշտերի վրա տրված տարածություններում, քանի որ, ենթադրենք 27 կետերից որոնելի կետը կարելի է գտնել՝ ինչ-որ հայտանիշ վերջավոր անգամ կիրառելով (տես 7.2.10 դիտողությունը):

7.2.3 Օրինակ. Վերջավոր դաշտի վրա տրված տարածության կարեւոր օրինակ են նաեւ վերջավոր դաշտերի ընդլայնումները: Ինչպես տեսանք 4.2 պարագրաֆում, դաշտերի K/L ընդլայնումը կարելի է մեկնաբանել որպես L դաշտի վրա տրված K գծային տարածություն: Եթե $K = GF(p^n)$, ապա կարելի է վերցնել $L = \mathbb{Z}_p$, եւ այդ դեպքում $|K| = p^n$, քանի որ $K \cong \mathbb{Z}_p^n$:

Շնորհիվ $V \cong K^m$ ($\dim V = m$) իզոմորֆիզմի, անհրաժեշտության դեպքում միշտ կարող ենք V տարածության v վեկտորը նույնացնել $v = (a_1, \dots, a_m)$ m-յակին, որտեղ $a_1, \dots, a_m \in K$ սկալյարները v-ի կոորդինատներն են ըստ որեւէ $e_1, \dots, e_m \in V$ բազիսի: Երբեմն բազիսը շեշտելու համար մենք m-յակի գրությանը կավելացնենք e տառը՝ $v = (a_1, \dots, a_m)_e$:

Կամայական տարածություններում գծային կախվածության եւ անկախության սահմանումը պայմանավորված չէ դաշտի տարրերի քանակով: Սակայն գծային կախվածության եւ վեկտորների կոորդինատներից կազմված մատրիցի որոշիչի միջեւ առկա կապն արդեն մի փոքր այլ տեսք ունի, քանի որ վերջավոր դաշտի վրա որոշիչի հաշվման գործողությունները տարբեր են: V գծային տարածության կամայական

(7.1) $$v_1 = (a_{11}, \dots, a_{1m}), \dots, v_k = (a_{k1}, \dots, a_{km}),$$

վեկտորների կոորդինատներից կազմենք

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \cdots & \cdots & \cdots \\ a_{k1} & \cdots & a_{km} \end{pmatrix} \in M_{k,n}(K)$$

մատրիցը: Վեկտորների (7.1) համակարգի մաքսիմալ գծորեն անկախ ենթահամակարգի հզորությունն ակնհայտորեն հավասար է A մատրիցի տողային ռանգին, քանի որ մատրիցի տողերը հենց (7.1) համակարգի վեկտորներն են: Կամայական մատրիցի տողային, սյունային եւ մինորային ռանգերի հավասարության մասին հայտնի լեմմայի ապացույցը կախված չէ K դաշտի անվերջությունից: Այդ ապացույցը բարդ չէ, եւ մենք այն բերում ենք որպես խնդիր.

7.2.4 Խնդիր. Ցույց տալ, որ կամայական K դաշտի վրա տրված ցանկացած մատրիցի տողային, սյունային եւ մինորային ռանգերն իրար հավասար են: *Յուցում*՝ կրկնել $\mathbb{R}$ դաշտի վրա տրված մատրիցների համար այդ լեմմայի ապացույցի քայլերը (ռանգի անփոփոխությունը մատրիցի տողերի ու սյուների հետ տարրական ձեւափոխությունների ժամանակ), նկատել, որ դրանք կախված չեն դիտարկվող դաշտի հզորությունից:

Մատրիցի տողային եւ սյունային ռանգերի սահմանումը նույնպես կախված չէ կոնկրետ դաշտի բնույթից: Իսկ մինորային ռանգը կարող է մի փոքր այլ հաշվարկ պահանջել, քանի որ, ինչպես տեսանք, որոշիչի հաշվարկը կախված է դաշտի գործողություններից:

7.2.5 Օրինակներ. $V=\mathbb{Z}_3^3$ տարածության մեջ $v_1=(2,1,0)$, $v_2=(0,2,2)$, $v_3=(0,2,1)$ համակարգը գծորեն անկախ է, քանի որ

$$\begin{vmatrix}2&1&0\\0&2&2\\0&2&1\end{vmatrix}=2\cdot2+0+0-0-0-2\cdot2\cdot2=1-2=2\neq0\in\mathbb{Z}_3:$$

Եթե երկրորդ վեկտորը փոխարինենք $v_2'=(0,1,2)$ վեկտորով, ապա կստանանք գծորեն կախված համակարգ, քանի որ

$$\begin{vmatrix}2&1&0\\0&1&2\\0&2&1\end{vmatrix}=2+0+0-0-0-2\cdot2\cdot2=2-2=0\in\mathbb{Z}_3:$$

Սա անսովոր է թվում, քանի որ $(2,1,0)$, $(0,1,2)$, $(0,2,1)$ համակարգը գծորեն անկախ է $\mathbb{R}$ դաշտի վրա: Այնուամենայնիվ, համակարգը կախված է $\mathbb{Z}_3$-ում. v_2'-ը v_3-ի պատիկն է: Իրոք, $2\cdot v_3=2\cdot(0,2,1)=(0,1,2)=v_2'$: Որպես v_1, v_2', v_3 համակարգի մաքսիմալ անկախ ենթահամակարգ կարելի է վերցնել, ասենք v_1,v_2' զույգը, քանի որ համապատասխան մատրիցի մաքսիմալ ոչ զրոյական մինորներից մեկը գտնըվում է նրա վերին ձախ երկու տողերում եւ սյուներում՝ $\begin{vmatrix}2&1\\0&1\end{vmatrix}=2-0=2\neq0\in\mathbb{Z}_3$:

7.2.6 Վարժություն. Գտնել $V=\mathbb{Z}_5^4$ տարածության հետեւյալ վեկտորների համակարգի մաքսիմալ գծորեն անկախ որեւէ ենթահամակարգ.

$$v_1=(4,1,2,1,3),\ v_2=(2,1,0,1,2),\ v_3=(0,2,1,1,3),\ v_4=(4,3,3,2,1):$$

Վերջավոր դաշտերի վրա է տեղափոխվում նաեւ գծային հավասարումների համակարգերի լուծման Գաուսի մեթոդը: Իսկապես, գծային հավասարումների

$$\begin{cases}a_{11}x_1+\cdots+a_{1k}x_k=b_1\\\cdots\cdots\cdots\cdots\cdots\\a_{m1}x_1+\cdots+a_{mk}x_k=b_m\end{cases}\tag{7.2}$$

համակարգը ($a_{ij}\in K,\ b_i\in K,\ i=1,\dots,m;\ j=1,\dots,k$) կարելի է վեկտորների լեզվով վերաձեւակերպել հետեւյալ կերպ.

$$\vec{v}_1=(a_{11},\dots,a_{m1}),\dots,\vec{v}_k=(a_{1k},\dots,a_{mk}),\ \vec{b}=(b_1,\dots,b_m)\in K^m$$

վեկտորների եւ $x_1,\dots,x_k\in K$ սկալյար փոփոխականների համար տեղի ունի

$$x_1\vec{v}_1+\cdots+x_k\vec{v}_k=\vec{b}\tag{7.3}$$

հավասարումը: Այստեղից միանգամից ստացվում է Կրոնեկեր-Կապելլիի թեորեմը ցանկացած դաշտերի համար. (7.2) համակարգը համատեղելի է (ունի լուծում) այն եւ միայն այն դեպում, երբ լուծում ունի (7.3) հավասարումը, այսինքն, երբ b վեկ-

տորն արտահայտվում է $v_1, \dots, v_k$ վեկտորների գծային կոմբինացիայի տեսքով, այսինքն, երբ $v_1, \dots, v_k, b$ եւ $v_1, \dots, v_k$ համակարգերի մաքսիմալ գծորեն անկախ ենթահամակարգերի հզորությունները հավասար են (ինչպես պայմանավորվել ենք ավելի վաղ, վեկտորների նշանակման մեջ սլաքները կարող ենք բաց թողնել եւ դրանք օգտագործել միայն այն դեպքերում, երբ ցանկանանք շեշտել վեկտորների եւ սկալյարների տարբերությունը): Ուրեմն, եթե (7.2) համակարգի մատրիցը եւ ընդլայնված մատրիցն են, համապատասխանաբար,

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1k} \\ \cdots & \cdots & \cdots \\ a_{m1} & \cdots & a_{mk} \end{pmatrix} \quad \text{եւ} \quad \bar{A} = \begin{pmatrix} a_{11} & \cdots & a_{1k} & b_1 \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & \cdots & a_{mk} & b_m \end{pmatrix},$$

ապա (7.2) համակարգը համատեղելի է այն եւ միայն այն դեպքում, երբ $\operatorname{rank} A = \operatorname{rank} \bar{A}$:

Եթե նշված ռանգերը հավասար են, ապա համակարգի ընդհանուր լուծումը գտնվում է նույն քայլերով, ինչպես $\mathbb{R}$-ի կամ $\mathbb{C}$-ի դեպքում: A մատրիցում գտնում ենք մաքսիմալ ոչ զրոյական M մինորը, եւ համակարգից դեն ենք նետում այն տողերը, որոնց համապատասխան տողերը A մատրիցում չեն անցնում M մինորով: Ենթադրենք $\operatorname{rank} A = r$: Այդ դեպքում նոր համակարգի սյուներից r հատն անցնում են M մինորով, իսկ մնացած $k - r$ հատն ընկած են դրանից դուրս: Այդ $k - r$ հատ սյուները տեղափոխենք հավասարման նշանից աջ, դրանց տանք կամայական արժեքներ K դաշտից: Կստանանք մի համակարգ, որի տողերի եւ սյուների քանակն է r, եւ որի մատրիցի որոշիչը (M մինորը) զրոյական չէ: Այդպիսի համակարգը միշտ ունի միակ լուծում, ըստ, օրինակ, Կրամերի կանոնի: Այդ լուծման կոորդինատներն ավելացնելով աջ մաս տարված փոփոխականների արժեքներին՝ կստանանք (7.2) համակարգի $\vec{u} = (x'_{01}, \dots, x'_{0m}) \in K^m$ որեւէ լուծումը: Այնուհետեւ անցնում ենք (7.2) համակարգին համապատասխան *համասեռ* համակարգին, որը (7.2)-ից տարբերվում է միայն նրանով, որ $b_1, \dots, b_m = 0$: Այդ համակարգի համար $k - r$ անգամ կրկնում ենք վերը բերված քայլերը՝ ամեն անգամ աջ մաս տարված $k - r$ հատ փոփոխականներին տալով այնպիսի արժեքներ, որ արդյունքում համասեռ համակարգի համար ստացվող լուծումները գծորեն անկախ լինեն (ստանում ենք համասեռ համակարգի լուծումների *ֆունդամենտալ* համակարգը): Որպես այդպիսի արժեքներ կարելի է վերցնել, օրինակ՝ $1, 0, \dots, 0$, ապա $0, 1, \dots, 0$ եւլն… $0, 0, \dots, 1$: Եթե լուծումների ֆունդամենտալ համակարգը նշանակենք $\vec{e}_1 = (x'_{11}, \dots, x'_{1m})$, … , $\vec{e}_{k-r} = (x'_{k-r\,1}, \dots, x'_{k-r\,m}) \in K^m$, ապա (7.2) համակարգի ընդհանուր $\vec{v} = (x'_1, \dots, x'_m)$ լուծումը նկարագրվում է հետեւյալ տեսքով

(7.4) $\vec{v} = (x'_1, \dots, x'_m) = \alpha\vec{u} + \beta_1\vec{e}_1 + \cdots + \beta_{k-r}\vec{e}_{k-r} \in K^m$, որտեղ $\alpha, \beta_1, \dots, \beta_{k-r} \in K$:

7.2.7 Օրինակ. $\mathbb{Z}_3$ դաշտի վրա լուծենք հետեւյալ համակարգը՝

$$\begin{cases} 2x_1 + x_2 = 1 \\ x_2 + 2x_3 = 1 \\ 2x_2 + x_3 = 2 \end{cases}:$$

Համակարգի մատրիցը արդեն քննարկվել է 7.2.5 օրինակներում: Այն բավարարում է Կրոնեկեր-Կապելլիի պայմանին, եւ նրա մաքսիմալ ոչ զրոյական $\begin{vmatrix} 2 & 1 \\ 0 & 1 \end{vmatrix}$ մինորը կարելի է վերցնել մատրիցի վերին ձախ անկյունում: Այստեղ $r = 2$ եւ $k - r = 3 - 2 = 1$: Դեն ենք նետում համակարգի երրորդ տողը եւ աջ մաս տանում երրորդ սյունը՝

$$\begin{cases} 2x_1 + x_2 = 1 \\ x_2 = 1 - 2x_3 \end{cases}:$$

x_3-ին տանք կամայական արժեք, ենթադրենք $x_3 = 0$: Այդ դեպքում $\vec{u} = (0, 1, 0) \in \mathbb{Z}_3^3$: Համապատասխան համասեռ համակարգի հետ նշված քայլերը կատարելուց հետո այն կունենա հետեւյալ տեսքը՝

$$\begin{cases} 2x_1 + x_2 = 0 \\ x_2 = -2x_3 \end{cases}:$$

x_3-ին միայն մեկ անգամ ենք արժեքներ շնորհելու: Ենթադրենք $x_3 = 1$: Այդ դեպքում $\vec{e}_1 = (1, 1, 1) \in \mathbb{Z}_3^3$: Ուստի համակարգի ընդհանուր լուծումը կունենա հետեւյալ տեսքը՝

$$\vec{v} = (x'_1, x'_2, x'_3) = \alpha\vec{u} + \beta\vec{e}_1 = \alpha(0, 1, 0) + \beta(1, 1, 1) \in \mathbb{Z}_3^3, \text{ որտեղ } \alpha, \beta \in \mathbb{Z}_3:$$

Այդ լուծումների բազմությունը կարելի է տալ նաեւ $\{(\beta, \alpha + \beta, \beta) \mid \alpha, \beta \in \mathbb{Z}_3\}$ տեսքով:

7.2.8 Վարժություն. $\mathbb{Z}_5$ դաշտի վրա լուծել հետեւյալ համակարգը՝

$$\begin{cases} 4x_1 + x_2 + 2x_3 + x_4 + x_5 = 1 \\ x_1 + x_2 + 3x_3 + x_4 + x_5 = 2 \\ 3x_1 + 2x_2 + 4x_3 + 2x_4 + 2x_5 = 2 \\ 2x_2 + 2x_4 + 2x_5 = 3 \end{cases}:$$

7.2.9 Դիտողություն. Իրական կամ կոմպլեքս դաշտերի վրա գծային հավասարումների համակարգերի լուծման հիմնական դեպքերը երեքն են. կամ $r = \operatorname{rank} A < \operatorname{rank} \bar{A}$ եւ համակարգը լուծումներ չունի, կամ $r = \operatorname{rank} A = \operatorname{rank} \bar{A} = k$ եւ համակարգն ունի ճիշտ մեկ լուծում, կամ էլ $r = \operatorname{rank} A = \operatorname{rank} \bar{A} < k$ եւ համակարգն ունի *անվերջ* քանակությամբ լուծումներ: Առաջին երկու դեպքերը նույնն են

նաեւ $K = GF(p^n)$ վերջավոր դաշտի համար: Իսկ երրորդ դեպքը փոխվում է, քանի որ համակարգին համապատասխանող համասեռ համակարգի լուծումների $k - r$ չափողականության ենթատարածությունն ունի $|K|^{k-r} = p^{n(k-r)}$ հատ վեկտոր: Ուստի այդքան է նաեւ ընդհանուր համակարգի բոլոր լուծումների քանակը: Իսկ պարզագույն $K = \mathbb{Z}_p$ դեպքում լուծումների քանակն է p^{k-r}:

Վերջավոր դաշտերով պայամանավորված հաջորդ տարբերությունը կապված է տարածության գծային օպերատորների (գծային արտապատկերումների հետ): Մենք դրանց համառոտ անվանենք օպերատորներ: Ենթադրենք $K = GF(p^n)$ դաշտի վրա տրված m չափողականության V տարածության վրա ունենք $A: V \to V$ օպերատորը (այսինքն, ցանկացած $v_1, v_2 \in V$ վեկտորների եւ $a_1, a_2 \in K$ սկալյարների համար տեղի ունի $(a_1v_1 + a_2v_2)A = a_1(v_1A) + a_2(v_2A)$ պայմանը): Օպերատորի $\operatorname{im} A = \{u \in V \mid \exists\, v \in V;\ vA = u\}$ *պատկերը* եւ $\ker A = \{v \in V \mid vA = \vec{0}\}$ միջուկը V տարածության ենթատարածություններ են: Այդ փաստի ստուգումը պարզ է եւ կախված չէ K-ի բնույթից: Դաշտից կախված չէ նաեւ այն հայտնի թեորեմի ապացույցը, ըստ որի՝ ցանկացած A օպերատորի համար նրա միջուկի չափողականության (որն անվանում են օպերատորի *դեֆեկտ*) եւ պատկերի չափողականաության (օպերատորի *ռանգի*) գումարը հավասար է տարածության չափողականությանը՝ $\dim \operatorname{im} A + \dim \ker A = \dim V$: Նշանակենք $\dim \operatorname{im} A = r$: Այդ դեպքում $\dim \ker A = m - r$ եւ վերջավոր դաշտի համար $|\operatorname{im} A| = |K|^r = p^{nr}$, իսկ $|\ker A| = |K|^{m-r} = p^{n(m-r)}$: Պարզագույն $K = \mathbb{Z}_p$ դեպքում կունենանք $|\operatorname{im} A| = |\mathbb{Z}_p|^r = p^r$ եւ $|\ker A| = |\mathbb{Z}_p|^{m-r} = p^{m-r}$: Օպերատորի պատկերը եւ միջուկը վերջավոր դաշտերի համար կարելի է ոչ միայն նկարագրել բազիսի միջոցով, այլեւ կարելի է քննարկել դրանք վեկտոր-առ-վեկտոր, քանի որ դրանց վեկտորների քանակը վերջավոր է:

Տվյալ e բազիսում A օպերատորի A_e մատրիցի սահմանումը նույնպես կախված չէ կոնկրետ դաշտի բնույթից: Եթե ֆիքսենք V-ի որեւէ $e_1, \dots, e_m$ բազիս, ապա $A_e = \|a_{ij}\|_m \in M_m(K)$, որտեղ a_{ij} տարրերը ստացվում են՝ A օպերատորը հերթով բազիսի վեկտորների վրա կիրառելով.

$$\begin{aligned} e_1A &= a_{11}e_1 + \dots + a_{1m}e_m, \\ &\dots\dots\dots\dots\dots \\ e_mA &= a_{m1}e_1 + \dots + a_{mm}e_m: \end{aligned}$$

Տարածության կամայական $v \in V$ վեկտորի համար vA պատկերի կոորդինատները կստացվեն, եթե v-ի կոորդինատների $v = (x_1, \dots, x_m)_e$ վեկտորը (որպես մեկ տողից

բաղկացած մատրից) բազմապատկվի A_e մատրիցով՝ $vA = (x_1, \dots, x_m)_e A_e$: Քանի որ հասկանալի է, թե ըստ որ բազիսի են դիտարկվում կոորդինատները եւ մատրիցը, պայմանավորվենք բաց թողնել e ինդեքսը եւ գրել $vA = (x_1, \dots, x_m)A$: Այս դեպքում A օպերատորն ու իր մատրիցը նշանակված կլինեն միեւնույն տառով, բայց դա թյուրիմացություն չի առաջացնի:

Եթե $vA = \lambda v$, որտեղ v-ն ոչ զրոյական վեկտոր է, իսկ λ-ն սկալյար է K-ից, ապա λ-ն կոչվում է A օպերատորի *սեփական արժեք*, իսկ v-ն՝ λ սեփական արժեքին համապատասխան *սեփական վեկտոր:* Այս սահմանումը նույնպես կախված չէ K դաշտի բնույթից: Սակայն K-ից կարող է կախված լինել v-ի հաշվման եղանակը: Եթե արդեն հայտնի է λ-ն, ապա նրան համապատասխան սեփական վեկտորը որոնենք անհայտ կոորդինատներից բաղկացած $v = (x_1, \dots, x_m)$ վեկտորի տեսքով: Ունենք.

$$vA = (x_1, \dots, x_m)\|a_{ij}\|_m = \left(\sum_{i=1,\dots,m} x_i a_{i1} \quad \cdots \quad \sum_{i=1,\dots,m} x_i a_{im} \right)$$

եւ $\lambda v = (\lambda x_1, \dots, \lambda x_m)$: Ուստի $vA = \lambda v$ հավասարումը համարժեք է

$$\begin{cases} a_{11}x_1 + \cdots + a_{m1}x_1 = \lambda x_1 \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ a_{m1}x_1 + \cdots + a_{mm}x_1 = \lambda x_m \end{cases} \quad \text{եւ} \quad \begin{cases} (a_{11} - \lambda)x_1 + \cdots + a_{m1}x_1 = 0 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ a_{m1}x_1 + \cdots + (a_{mm} - \lambda)x_1 = 0 \end{cases}$$

համակարգերին: Դրանցից երկրորդը նշանակում է, որ $(x_1, \dots, x_m)$-ն կարելի է որոնել որպես համապատասխան գծային հավասարումների համակարգի լուծում կամ էլ որպես

$$\begin{pmatrix} a_{11} - \lambda & \cdots & a_{m1} \\ \cdots\cdots\cdots\cdots & & \\ a_{m1} & \cdots & a_{mm} - \lambda \end{pmatrix}$$

մատրիցին համապատասխանող օպերատորի միջուկի վեկտոր: Մենք քննարկել ենք այդ երկու օբյեկտներն էլ: Երկու դեպքերում էլ վերջավոր դաշտի դեպքում ստացվում են ընդամենը $|K|^{k-r} = p^{n(k-r)}$ հատ լուծումներ կամ էլ նույն քանակությամբ վեկտորներ օպերատորի միջուկում:

7.2.10 Դիտողություն. Քննարկված բոլոր խնդիրներում վերջավոր դաշտերի համար մենք ստանում էինք վերջավոր քանակությամբ վեկտորների կամ լուծումների բազմություններ: Սրանով է պայմանավորված վերջավոր դաշտերի վրա գծային հանրահաշվի մեթոդների կարեւոր ալգորիթմական պոտենցիալը. եթե որեւէ խնդիր (իրական կամ կոմպլեքս դաշտերի համար լուծելիս) մենք ստանում էինք, որ որոնելի պատասխանը ինչ-որ համակարգի լուծում կամ ինչ-որ ենթատարա-

ծության վեկտոր է, ապա դա դեռ վերջնական պատասխան չէր, քանի որ նշված բազմությունները կարող էին անվերջ քանակությամբ տարրեր պարունակել: Իսկ վերջավոր դաշտի դեպքում, ինչպես տեսանք, գործ ունենք միայն վերջավոր քանակությամբ օբյեկտների հետ, որոնցից կարելի է վերջնական պատասխանն ընտրել՝ որեւէ հավելյալ հայտանիշ վերջավոր անգամ կիրառելով: Էլ ավելի հետաքրքիր են այն դեպքերը, երբ որեւէ խնդիր, որը տրված չէ վերջավոր դաշտի վրա, նախ բերում են այդ դեպքին մոդուլյար անցումների օգնությամբ, ապա լուծում վերջավոր դաշտերի վրա՝ «շատ փոքրիկ» տարածությունների մեջ, եւ վերջում վերականգնում լուծումն ընդհանուր դեպքում: Նման մոտեցման լավ օրինակ են բազմանդամի ֆակտորիզացիայի եւ արմատների հաշվման խնդիրների լուծումները 7.3, 7.4, 7.5 պարագրաֆներում:

7.3 Բեռլեկեմպի ալգորիթմը

Այս պարագրաֆում կծանոթանանք կամայական K վերջավոր դաշտի վրա տրված $f(x) \in K[x]$ բազմանդամի ֆակտորիզացիայի Բեռլեկեմպի ալգորիթմին:

Համարենք, որ K-ն p պարզ բնութագրիչի վերջավոր դաշտ է: Ինչպես տեսանք 4.1.10 թեորեմում, $K = GF(p^n)$, այսինքն՝ K դաշտը բաղկացած է p^n տարրերից, որտեղ $p = \mathrm{char}(K)$: Ըստ 4.2.35 թեորեմի՝ p^n տարրերից բաղկացած դաշտը (իզոմորֆիզմի ճշտությամբ) միակն է: Չնայած K-ի միակությունը ալգորիթմի կառուցման մեջ չի օգտագործվելու, նշենք այս փաստը, որպեսզի հասկանալի լինի, որ ստորեւ դիտարկվող $V = K^k$ գծային տարածությունը նույնպես միակն է: Մասնավորապես, եթե $n = 1$, ապա $K = GF(p) = \mathbb{Z}_p$: Վերջին դեպքը մեզ պետք կգա նաեւ 7.4 պարագրաֆում:

Վերցնենք կամայական դրական m աստիճանի $f(x) \in K[x]$ բազմանդամ: Քանի որ K-ն դաշտ է, կարելի է համարել, որ $f(x)$-ը նորմավորված է, այսինքն, նրա ավագ գործակիցը 1 է (հակառակ դեպքում պարզապես բազմանդամը կբազմապատկենք նրա a_0 ավագ գործակցի հակադարձով, ինչը չի ազդի ֆակտորիզացիայի կառուցման վրա):

Որպես $f(x)$ բազմանդամի ֆակտորիզացիայի առաջին քայլ նկատենք, որ եթե $f(x)$-ը ներկայացված է այնպիսի բազմանդամների արտադրյալի տեսքով, որոնցից յուրաքանչյուրի ֆակտորիզացիան մենք արդեն ունենք, ապա կունենանք նաեւ

$f(x)$-ի ֆակտորիզացիան: Ինչպես տեսանք 4.5 պարագրաֆում, վերջավոր դաշտի վրա տրված կամայական դրական աստիճանի բազմանդամ կարելի է 4.5.2 ալգորիթմով վերլուծել այն քառակուսիներից ազատ արտադրիչների, այսինքն՝ այնպիսի արտադրիչների, որոնք չունեն $q^2(x)$ տեսքի դրական աստիճանի բաժանարարներ (տես նաեւ 4.3 պարագրաֆը): Ուստի ֆակտորիզացիայի խնդիրը բավական է լուծել միայն քառակուսիներից ազատ բազմանդամների համար, եւ ստորեւ մենք կենթադրենք, որ $f(x)$-ն այդպիսի բազմանդամ է:

Ենթադրենք $f(x)$ քառակուսիներից ազատ, նորմավորված բազմանդամի ֆակտորիզացիան ունի

$$f(x) = p_1(x)\cdots p_k(x) \tag{7.5}$$

տեսքը, որտեղ դրական աստիճանի $p_i(x)$ բազմանդամները պարզ են, $i = 1, \dots, k$: Ունենք $\big(p_i(x), p_j(x)\big) = 1$, եթե $i \neq j$: Վերցնենք կամայական $s_1, \dots s_k \in K$ տարրեր: Ըստ մնացքների մասին չինական թեորեմի բազմանդամային 5.1.5 տարբերակի՝ գոյություն ունի այնպիսի մի $v(x) \in K[x]$ բազմանդամ, որ

$$\begin{aligned} v(x) &\equiv s_1 \big(\mathrm{mod}\, p_1(x)\big), \\ &\dots\dots\dots\dots\dots\dots\dots\dots \\ v(x) &\equiv s_k \big(\mathrm{mod}\, p_k(x)\big), \end{aligned} \tag{7.6}$$

ընդ որում, եթե որեւէ $v'(x) \in K[x]$ բազմանդամ նույնպես բավարարում է (7.6) համակարգին, ապա $v'(x) \equiv v(x)\big(\mathrm{mod}\, f(x)\big)$: Մասնավորապես, այս համակարգին բավարարող $v(x)$ բազմանդամներից միայն մեկն է, որի աստիճանը ցածր է $f(x)$-ի աստիճանից: Քանի որ $s_1, \dots s_k$ արժեքների հնարավոր ընտրությունների քանակը $|K|^k = (p^n)^k = p^{nk}$ է, ստանում ենք, որ m-ից ավելի ցածր աստիճանի եւ (7.6) համակարգին բավարարող $v(x)$ բազմանդամների քանակը ճիշտ p^{nk} է:

(7.6) համակարգը մեզ տալիս է (7.5) ֆակտորիզացիայի հաշվման հիմնական քայլը: Իսկապես, ենթադրենք մենք արդեն ունենք $v(x)$ բազմանդամը, իսկ $s_1, \dots s_k$ տարրերը զույգ առ զույգ տարբեր են: Այդ դեպքում Էվկլիդեսի ալգորիթմով հաշվենք

$$\big(v(x) - s_j, f(x)\big) \tag{7.7}$$

ամենամեծ ընդհանուր բաժանարարը կամայական $j = 1, \dots, k$ ինդեքսի համար: Քանի որ (7.7)-ը բաժանում է $f(x)$ բազմանդամը, ապա այն մի քանի $p_i(x)$ բազմանդամների արտադրյալ է՝ շնորհիվ $K[x]$ օղակի ֆակտորիալության:

Մյուս կողմից, եթե j-ից տարբեր i ինդեքսի համար $\big(v(x)-s_j\big)\vdots p_i(x)$, ապա $v(x)\equiv s_j\big(\mathrm{mod}\, p_i(x)\big)$: Ըստ (7.6) համակարգի՝ մենք արդեն իսկ ունենք $v(x)\equiv s_i\big(\mathrm{mod}\, p_i(x)\big)$: Բայց $v(x)$-ը չի կարող ըստ $p_i(x)$ մոդուլի բաղդատելի լինել միաժամանակ s_j եւ s_i տարրերին, քանի որ դրանից կբխեր $\big(s_j-s_i\big)\vdots p_i(x)$, ինչն անհնար է. սկալյարը չի կարող բաժանվել դրական աստիճանի բազմանդամի վրա: Ուրեմն՝ $v(x)-s_j$ տարբերությունը բաժանվում է (7.5) արտադրիչներից միայն մեկի՝ $p_j(x)$-ի վրա, եւ

$$\Big(v(x)-s_j, f(x)\Big)\approx p_j(x): \tag{7.8}$$

Քանի որ (7.5) արտադրիչները նույնպես կարելի է համարել նորմավորված, ապա $p_j(x)$ արտադրիչը կարելի է ստանալ՝ նորմավորելով $\Big(v(x)-s_j, f(x)\Big)$-ը:

Մինչեւ $v(x)\in K[x]$, $k\in\mathbb{N}$ եւ $s_1,\dots s_k\in K$ արժեքների քննարկմանն անցնելը նկատենք, որ պարզագույն $K=\mathbb{Z}_p$ դեպքում $v(x)$-ը կլինի $\mathbb{Z}_p$-ից ընտրված գործակիցներով մոդուլար բազմանդամ, իսկ $s_1,\dots s_k$ սկալյարները կլինեն թվեր $\{0,\dots,p-1\}$-ից:

Հետեւյալ պնդումը Ֆերմայի փոքր թեորեմի մասնավոր դեպքերից է.

7.3.1 Լեմմա. *$K=GF(p^n)$ դաշտի ցանկացած s տարրի համար $s^{p^n}=s$:*

Ապացույց: Ըստ 4.1.11 թեորեմի՝ եթե $|K|=p^n$, ապա K^* մուլտիպլիկատիվ խումբը p^n-1 կարգի ցիկլիկ խումբ է, այսինքն՝ $s^{p^n}=s^{p^n-1}\cdot s=1\cdot s=s$: ■

(7.6) համակարգի որեւէ տողը p^n-րդ աստիճան բարձրացնելով՝ կստանանք

$$v(x)^{p^n}\equiv s_i^{p^n}\big(\mathrm{mod}\, p_i(x)\big):$$

Ըստ 7.3.1 լեմմայի, $s_i^{p^n}=s_i$: Այսինքն՝ $v(x)^{p^n}\equiv s_i\big(\mathrm{mod}\, p_i(x)\big)$, որտեղ $i=1,\dots,k$: Ըստ 5.1.5 թեորեմի երկրորդ պնդման՝

$$v(x)^{p^n}\equiv v(x)\big(\mathrm{mod}\, f(x)\big): \tag{7.9}$$

Մենք ստացանք.

7.3.2 Լեմմա. *Եթե զույգ առ զույգ փոխադարձաբար պարզ $p_1(x),\dots,p_k(x)\in K[x]$ բազմանդամների եւ կամայական $s_1,\dots s_k\in K$ տարրերի համար $v(x)\in K[x]$ բազմանդամը բավարարում է (7.6) համակարգին, ապա այն բավարարում է նաեւ (7.9) բաղդատմանը, որտեղ $p^n=|K|$:*

Բեռլեկեմպի մեթոդը օգտագործում է այն փաստը, որ (7.9) բաղդատումը, ի տարբերություն (7.6) համակարգի, այլեւս չի պարունակում $p_1(x),\dots,p_k(x)$; $s_1,\dots s_k$

անհայտները, եւ $v(x)$-ը կախման մեջ է միայն $f(x)$-ից եւ p^n-ից, որոնք մեզ հայտնի են: Տեղի ունի 7.3.2 լեմմայի «մասնակի» հակադարձը.

7.3.3 Լեմմա. *Եթե $v(x) \in K[x]$ բազմանդամը բավարարում է (7.9) բաղդատմանը, ապա ինչ-որ $s_1, \dots s_k \in K$ տարրերի համար $v(x)$-ը բավարարում է նաեւ (7.6) համակարգին:*

Ապացույց: K դաշտի ցանկացած s տարր, ըստ 7.3.1 լեմմայի, $x^{p^n} - x$ բազմանդամի արմատ է: Ըստ 2.5.16 Բեզուի թեորեմի՝ $\left(x^{p^n} - x\right) \vdots (x - s)$: Ուրեմն՝ նաեւ $\left(x^{p^n} - x\right) \vdots \prod_{s \in K}(x - s)$, քանի որ $K[x]$-ը ֆակտորիալ է, եւ եթե $s_1 \neq s_2$, ապա $(x - s_1, x - s_2) = 1$: Մյուս կողմից, $\prod_{s \in K}(x - s)$ արտադրյալի աստիճանը նույնպես p^n է, ուրեմն, $x^{p^n} - x = \prod_{s \in K}(x - s)$ (երկու բազմանդամներն էլ նորմավորված են եւ ավագ գործակիցները համեմատելու խնդիր չի առաջանում): Մասնավորապես, x-ի փոխարեն վերցնելով $v(x)$ արժեքը, կունենանք

$$v(x)^{p^n} - v(x) = \prod_{s \in K}(v(x) - s).$$

Մյուս կողմից, ըստ (7.9) բաղդատման, $v(x)^{p^n} - v(x)$ տարբերությունը բաժանվում է $f(x)$-ի եւ նրա բոլոր $p_1(x), \dots, p_k(x)$ պարզ արտադրիչների վրա: Եթե ենթադրենք $p_1(x)$-ը որեւէ $s_1 \in K$ համար, ըստ 6.1.6 հետեւանքի, բաժանում է $v(x) - s_1$ արտադրիչը, ապա այն չի կարող բաժանել որեւէ $v(x) - s_2$ արտադրիչ, եթե $s_1 \neq s_2$: Սա նշանակում է, որ $p_1(x), \dots, p_k(x)$ արտադրիչներից յուրաքանչյուրը բաժանում է $v(x) - s$ տեսքի արտադրիչներից միայն մեկը: Հակառակը պնդել չենք կարող. $v(x) - s$ տեսքի որեւէ արտադրիչ կարող է եւ բաժանվել $p_1(x), \dots, p_k(x)$ արտադրիչներից մի քանիսի վրա:

Ստանում ենք, որ $\prod_{s \in K}\big(f(x), (v(x) - s)\big)$ արտադրյալի յուրաքանչյուր արտադրիչ կամ ասոցացված է միավորին, կամ ասոցացված է $p_1(x), \dots, p_k(x)$ արտադրիչներից մեկին, կամ էլ՝ դրանցից մի քանիսի արտադրյալին: Անհրաժեշտության դեպքում նորմավորելով այդ արտադրյալը՝ ստանում ենք

$$\prod_{s \in K}\big(f(x), (v(x) - s)\big) = f(x) = p_1(x) \cdots p_k(x) \tag{7.10}$$

(գրառման մեջ ավելորդ բարդություն չմտցնելու համար նորմավորված արտադրիչների համար նոր նշանակումներ չենք մտցնում): Մնում է նկատել, որ եթե $(v(x) - s) \vdots p_i(x)$, ապա $v(x) \equiv \mathrm{s}\big(\mathrm{mod}\, p_i(x)\big)$, որտեղից եւ ստացվում են լեմմայի $s_1, \dots s_k \in K$ տարրերը: ■

7.3.4 Օրինակ. (7.9) բաղդատմանը բավարարող բազմանդամներից է $v(x)=1$ հաստատուն բազմանդամը, քանի որ $1^{p^n}-1=0\vdots f(x)$: Այդ դեպքում $s=1\in K$ տարրի համար $(f(x),v(x)-s)=(f(x),1-1)=(f(x),0)=f(x)$: Իսկ ցանկացած այլ s-ի համար $(f(x),s-1)=1$, քանի որ ոչ զրոյական $s-1$ սկալյարը չի կարող բաժանվել դրական աստիճանի $p_1(x),\dots,p_k(x)$ բազմանդամներից որեւէ մեկի վրա: Այսինքն՝ տվյալ դեպքում (7.10) հավասարության ձախ մասի արտադրյալը ունի հետեւյալ տեսքը՝

$$f(x)\cdot\underbrace{1\cdots1}_{p^n-1}$$

(եւ ոչ մի էական ինֆորմացիա չի բերում $f(x)$-ի ֆակտորիզացիայի համար):

Մեր նպատակն է գտնել այնպիսի $v(x)$ բազմանդամ (կամ բազմանդամներ), որ (7.10) արտադրյալն ըստ դրանց կառուցելու դեպքում ստանանք *բոլոր* $p_1(x),\dots,p_k(x)$ արտադրիչները:

7.3.5 Դիտողություն. Պարզագույն $K=\mathbb{Z}_p$ դեպքում $|K|=p$ եւ (7.10) արտադրյալը կընդունի հետեւյալ տեսքը՝

$$\prod_{i=0}^{p-1}\big(f(x),(v(x)-i)\big)=f(x)=p_1(x)\cdots p_k(x): \tag{7.11}$$

$v(x)$ բազմանդամի հնարավոր արժեքների հաշվման համար մեզ պետք կգան վերջավոր դաշտի վրա (գծային) օպերատորների մեթոդներ: $K[x]$ բազմության վրա կարելի է սահմանել K դաշտի վրա տրված գծային տարածություն, եթե որպես վեկտորների գումարման գործողություն վերցնենք բազմանդամների գումարումը, իսկ որպես սկալյարով բազմապատկում՝ բազմանդամի բազմապատկումը K-ի տարրով: Քանի որ բազմանդամների գումարի աստիճանը մեծ չէ գումարելիների աստիճաններից առավելագույնից, ապա տվյալ թվից ոչ ավելի բարձր աստիճանի բազմանդամների ենթաբազմությունը կազմում է $K[x]$-ի ենթատարածություն: Դիտարկենք $V=\{u(x)\in K[x]\mid \deg u(x)\le m-1\}$ ենթատարածությունը, որտեղ $\deg f(x)=m$: Ըստ (7.6) համակարգի կառուցման՝ V տարածության մեջ կա միայն մեկ $v(x)$ բազմանդամ, որը (ֆիքսված $s_1,\dots s_k$ արժեքների համար) բավարարում է այդ համակարգին. մնացած $v'(x)$ բազմանդամները բաղդատելի են $v(x)$-ին ըստ $f(x)$ մոդուլի, այսինքն, դրանց աստիճանները մեծ են $(m-1)$-ից:

p^n-րդ աստիճան բարձրացնելու գործողությունը (գծային) օպերատոր է $K[x]$ տարածությունում. ցանկացած $a,b\in K$ սկալյարների եւ $u(x),l(x)\in K[x]$ բազմանդամների համար

$$(a\cdot u(x)+\ b\cdot l(x))^{p^n}=(a\cdot u(x))^{p^n}+(b\cdot l(x))^{p^n}$$
$$=a^{p^n}\cdot u(x)^{p^n}+b^{p^n}\cdot l(x)^{p^n}=a\cdot u(x)^{p^n}+b\cdot l(x)^{p^n}: \tag{7.12}$$

Այստեղ առաջին հավասարության համար կրկին օգտվել ենք Նյուտոնի բինոմական բանաձեւից, իսկ վերջին հավասարության համար՝ Ֆերմայի փոքր թեորեմից: Այս գործողությունը, սակայն, օպերատոր չէ V ենթատարածության համար, քանի որ V-ի որեւէ բազմանդամ p^n-րդ աստիճան բարձրացնելով՝ կարող ենք ստանալ $(m-1)$-ից ավելի բարձր աստիճանի բազմանդամ, որը V-ին չի պատկանում:

Հեշտ է ստուգել, որ մնացորդով բաժանման գործողությունը նույնպես օպերատոր է: Քանի որ օպերատորների արտադրյալը կրկին օպերատոր է, ապա հետեւյալ Q կանոնը V տարածության վրա օպերատոր է սահմանում. *կամայական $u(x)\in V$ բազմանդամ նախ բարձրացնենք p^n-րդ աստիճան, ապա ստացված $u(x)^{p^n}$ արդյունքը մնացորդով բաժանենք $f(x)$-ի վրա: Ստացված $r(x)$ մնացորդն էլ համարենք $u(x)Q$ արժեքը:*

(7.9) բաղդատումը V տարածության եւ Q օպերատորի տերմիններով ստանում է հետեւյալ տեսքը.

$$v(x)Q=v(x)=1\cdot v(x), \tag{7.13}$$

այսինքն, $v(x)\in V$ վեկտորը Q օպերատորի սեփական վեկտորն է $\lambda=1$ սեփական արժեքի համար: Բազմանդամի ֆակտորիզացիայի եւ վերջավոր դաշտի վրա օպերատորների միջեւ այս անսպասելի եւ գեղեցիկ կապը թույլ է տալիս մեր խնդրի լուծման մեջ օգտագործել գծային հանրահաշվի մեթոդները:

$v(x)$ բազմանդամը կարելի է մեկնաբանել նաեւ այլ կերպ: Եթե E-ով նշանակենք V տարածության միավոր օպերատորը, ապա կամայական $u(x)\in V$ բազմանդամի համար տեղի ունի $u(x)E=u(x)$, ապա (7.13) հավասարությունից կստանանք

$$v(x)Q=v(x)E\ \text{ եւ }\ v(x)(Q-E)=0: \tag{7.14}$$

Այսինքն՝ (7.9) բաղդատումը նշանակում է, որ $v(x)\in V$ վեկտորը $Q-E$ օպերատորի $\ker(Q-E)$ միջուկի տարր է: Հակառակն ակնհայտորեն նույնպես ճիշտ է:

7.3.6 Լեմմա. *$v(x)\in V$ բազմանդամը բավարարում է (7.9) բաղդատմանը այն եւ միայն այն դեպքում, երբ $v(x)\in\ker(Q-E)$:*

Քանի որ $\dim V=(m-1)+1=m$, ապա որպես տարածության e բազիս կարելի է ընտրել, ասենք,

(7.15) $$e_1 = 1 = x^0,\ e_2 = x, \dots, e_m = x^{m-1}$$

վեկտորների համակարգը: K դաշտի վրա տրված միեւնույն չափողականության տարածություններն իզոմորֆ են: Մասնավորապես, կամայական $u(x) \in V$ բազմանդամի կարելի է համապատասխանեցնել է m-յակների K^m տարածության միակ տարր՝ $u(x)$-ի գործակիցներից բաղկացած վեկտորը:

Ինչպես պայմանավորվել ենք ավելի վաղ, V-ի վրա գործող կամայական A օպերատորի մատրիցն ըստ e բազիսի նշանակենք A_e: Մասնավորապես, E միավոր օպերատորի համար՝

$$E_e = \begin{pmatrix} 1 & \cdots & 0 \\ \cdots & \cdots & \cdots \\ 0 & \cdots & 1 \end{pmatrix}:$$

7.3.7 Հետեւանք. (7.9) բաղդատմանը բավարարող $v(x)$ բազմանդամների բազմությունը m չափողականության V տարածության $m-r$ չափողականության ենթատարածություն է, որտեղ $r = \operatorname{rank}(Q_e - E_e)$:

Ապացույց: Օգտվում ենք գծային հանրահաշվից հայտնի այն փաստից, որ կամայական V տարածության վրա գործող A օպերատորի միջուկը ենթատարածություն է, որի չափողականությունը (օպերատորի դեֆեկտը) հավասար է $\dim(V) - \dim(\operatorname{im}(A))$, որտեղ A օպերատորի $\operatorname{im}(A)$ պատկերի չափողականությունը հավասար է A_e մատրիցի $\operatorname{rank} A_e$ ռանգին: Մեր դեպքում $(Q-E)_e = Q_e - E_e$: ■

7.3.8 Հետեւանք. (7.9) բաղդատմանը բավարարող $v(x)$ բազմանդամների քանակը $p^{n(m-r)}$ է:

Ապացույց: K դաշտի տարրերի քանակը p^n է, ուստի դրա վրա $m-r$ չափողականության տարածության հզորությունը կլինի $|K|^{m-r} = (p^n)^{m-r} = p^{n(m-r)}$: ■

Այստեղից արդեն կարող ենք որոշել (7.5) ֆակտորիզացիայի մեջ մասնացող պարզ արտադրիչների k քանակը: Մենք տեսել էինք, որ m-ից ցածր աստիճանի, (7.6) համակարգին բավարարող $v(x)$ բազմանդամների քանակը p^{nk} է: Բայց այդ բազմանդամները կազմում են $\ker(Q-E)$ միջուկը, եւ դրանց քանակը $p^{n(m-r)}$ է: Ստանում ենք $f(x)$-ի ֆակտորիզացիային վերաբերող հետեւյալ փաստը.

7.3.9 Հետեւանք. Մեր նշանակումներում (7.5) ֆակտորիզացիայի $p_1(x), \dots, p_k(x)$ պարզ արտադրիչների քանակն է $k = m - r = m - \operatorname{rank}(Q_e - E_e)$:

$v(x)$ բազմանդամների հաշվման համար օգտագործենք օպերատորի միջուկի նկարագրությունը գծային հավասարումների համակարգի միջոցով: e բազիսում Q օպերատորի Q_e մատրիցի տողերը բաղկացած են բազիսի վեկտորների $e_1Q, \dots, e_nQ$ պատկերների կոորդինատներից: Եթե տեղի ունի.

(7.16) $e_iQ = x^{i-1}Q = q_{i1}e_1 + \cdots + q_{im}e_m = q_{i1}x^0 + \cdots + q_{im}x^{m-1}, \qquad i = 1, \ldots, m,$

ապա

$$Q_e = \begin{pmatrix} q_{11} & \cdots & q_{1m} \\ \cdots & \cdots & \cdots \\ q_{m1} & \cdots & q_{mm} \end{pmatrix} \quad \text{եւ} \quad Q_e - E_e = \begin{pmatrix} q_{11}-1 & \cdots & q_{1m} \\ \cdots & \cdots & \cdots \\ q_{m1} & \cdots & q_{mm}-1 \end{pmatrix}:$$

Քանի որ e-ն այստեղ քննարկվող միակ բազիսն է, պայմանավորվենք բաց թողնել այն մատրիցների ինդեքսից: Այս մատրիցները կնշանակենք Q եւ E, իսկ համատեքստից միշտ հասկանալի կլինի, թե ինչ ի նկատի ունենք՝ օպերատորը, թե նրա մատրիցը: Q մատրիցի առաջին տողը միշտ կլինի $1\ 0 \cdots 0$, քանի որ $e_1Q = 1Q$ վեկտորը կստացվի որպես $1^{p^n} = 1$ բազմանդամի՝ $f(x)$-ի վրա բաժանելուց ստացվող $r(x) = 1 = 1e_1$ մնացորդ: Իսկ երկրորդ տողը կստացվի x^{p^n} բազմանդամը $f(x)$-ի վրա բաժանելու միջոցով եւլն: Մասնավորապես, եթե $p^n < m$, ապա երկրորդ տողը կունենա $0\ \cdots 0\ 1\ 0 \cdots 0$ տեսքը, որտեղ միակ ոչ զրոյական տարրը (p^n+1)-րդ տեղում է:

7.3.10 Օրինակ. Վերցնենք $K = \mathbb{Z}_7$ եւ $f(x) = x^3 + 3x^2 + 2x \in \mathbb{Z}_7[x]$: Հեշտ է ստուգել, որ սա քառակուսիներից ազատ բազմանդամ է: $\mathbb{Z}_7[x]$ տարածության V ենթատարածությունն այս դեպքում բաղկացած կլինի ոչ ավել, քան $\deg f(x) - 1 = 2$ աստիճան ունեցող բազմանդամներից: $\dim(V) = 3$ եւ V-ի բազիս է $e_1 = 1,\ e_2 = x,\ e_3 = x^2$ համակարգը: Հաշվենք $e_1Q,\ e_2Q,\ e_3Q$ վեկտորները: $e_1Q = e_1 = 1$: Իսկ e_2Q-ն ստանալու համար x^7-ը մնացորդով բաժանենք $f(x)$-ի վրա: Ստացվում է $e_2Q = x$: Ապա e_3Q-ն ստանալու համար $f(x)$-ի վրա մնացորդով բաժանենք x^{14}-ը: Ստացվում է $e_3Q = 3x^2 + 2x$: Համապատասխան մատրիցները կլինեն.

$$Q = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 2 & 3 \end{pmatrix} \quad \text{եւ} \quad Q - E = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 2 & 2 \end{pmatrix}:$$

Վերադառնանք ընդհանուր դեպքին: $\lambda = 1$ սեփական արժեքի համար Q օպերատորի սեփական վեկտորները (կամ, որ նույնն է, $Q - E$ օպերատորի միջուկը) գտնելու համար լուծենք $(x_1, \ldots, x_m)Q = (x_1, \ldots, x_m)$ մատրիցային հավասարումը, այսինքն, գծային հավասարումների հետեւյալ համակարգը

$$\begin{cases} q_{11}x_1 + \cdots + q_{m1}x_m = x_1 \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ q_{1m}x_1 + \cdots + q_{mm}x_m = x_m \end{cases},$$

որը համարժեք է

(7.17)
$$\begin{cases} (q_{11}-1)x_1 + \cdots + q_{m1}x_m = 0 \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ q_{1m}x_1 + \cdots + (q_{mm}-1)x_m = 0 \end{cases}$$

(համասեռ) համակարգին: Համակարգի լուծումների բազմությունը կազմում է $m-r$ չափողականության ենթատարածություն K^m տարածության մեջ: Դրա վեկտորները գտնելու համար, ըստ համակարգը լուծելու հայտնի կանոնի, նախ գտնում ենք $Q-E$ մատրիցի մաքսիմալ ոչ զրոյական M մինորը, եւ համակարգից դեն ենք նետում այն տողերը, որոնք չեն անցնում M մինորով: Այնուհետեւ հավասարման նշանից դեպի աջ ենք տեղափոխում այն x_i փոփոխականները, որոնց սյուները չեն անցնում M մինորով: Այդ փոփոխականների քանակն է

$$m-\operatorname{rank} M=m-\operatorname{rank}(Q-E)=m-r=\dim\ker(Q-E):$$

Աջ կողմ տարված փոփոխականներին $m-r$ անգամ շնորհում ենք կամայական (գծորեն անկախ) արժեքներ, եւ ըստ դրանց՝ հաշվում ձախ մասում մնացած փոփոխականների արժեքները: Ստանում ենք $m-r$ հատ գծորեն անկախ լուծումներ՝ (7.17) համասեռ համակարգի լուծումների $v_1,\dots,v_{m-r}\in K^m$ ֆունդամենտալ համակարգը: Ըստ $K^m\cong V$ իզոմորֆիզմի՝ V տարածության մեջ դրանց կհամապատասխանեն

$$v_1(x),\dots,v_{m-r}(x) \tag{7.18}$$

գծորեն անկախ բազմանդամներ: Կիրառենք սա 7.3.10 օրինակի բազմանդամների համար.

7.3.11 Օրինակ. Օգտագործելով 7.3.10 օրինակի $Q-E$ մատրիցի արժեքը՝ ստանում ենք հետեւյալ համակարգը.

$$\begin{cases}0x_1+0x_2+0x_3=0\\0x_1+0x_2+2x_3=0\\0x_1+0x_2+2x_3=0\end{cases}:$$

Որպես M մինոր կարելի է վերցնել, ասենք, երրորդ տողի երրորդ տարրը պարունակող ոչ զրոյական $|2|$ մինորը: Դեն են նետվում առաջին երկու տողերը: Աջ կողմ տարվող x_1, x_2 փոփոխականներին շնորհելով նախ 1, 0 արժեքները՝ կստանանք համակարգի $v_1=(1,0,0)$ լուծումը: Դրան կհամապատասխանի $v_1(x)=1$ բազմանդամը ((7.9) բաղդատման լուծումը): Ինչպես տեսանք 7.3.4 օրինակում, զրոյական աստիճանի $v_1(x)$ բազմանդամի միջոցով ֆակտորիզացիան կառուցել չենք կարող:

Երկրորդ քայլում x_1, x_2 փոփոխականներին շնորհելով 0, 1 արժեքները՝ կստանանք համակարգի $v_2=(0,1,0)$ լուծումը, որին կհամապատասխանի $v_2(x)=x$ բազմանդամը: (7.10) հավասարությունը ստանալու համար Էվկլիդեսի ալգորիթմով հերթով հաշվենք $\big(f(x),(v_2(x)-i)\big)$ ամենամեծ ընդհանուր բաժանարարները $i=0,\dots,6$ թվերի համար:

$$(f(x), x-0) = (x^3+3x^2+2x, x) = x = p_1(x),$$
$$(f(x), x-1) = (x^3+3x^2+2x, x+6) = 6 \approx 1,$$
$$(f(x), x-2) = (x^3+3x^2+2x, x+5) = 3 \approx 1,$$
$$(f(x), x-3) = (x^3+3x^2+2x, x+4) = 4 \approx 1,$$
$$(f(x), x-4) = (x^3+3x^2+2x, x+3) = 1,$$
$$(f(x), x-5) = (x^3+3x^2+2x, x+2) = x+2 = p_2(x),$$
$$(f(x), x-6) = (x^3+3x^2+2x, x+1) = x+1 = p_3(x):$$

Յոթ տողերից չորսում ստացվող ամենամեծ ընդհանուր բաժանարարները հակադարձելի են, ու դրանցով պարզ արտադրիչներ չեն առաջանում: Իսկ մնացած երեք տողերից ծնվում են $p_1(x) = x$, $p_2(x) = x+2$ եւ $p_3(x) = x+1$ բազմանդամները: Հեշտ է ստուգել, որ դրանք իսկապես պարզ են, եւ $x(x+2)(x+1) = f(x)$:

7.3.12 Վարժություն. Կատարել 7.3.10 եւ 7.3.11 օրինակների բոլոր հաշվարկները:

Անցնենք ալգորիթմի կառուցման վերջին քայլին՝ ֆակտորիզացիայի համար անհրաժեշտ $v(x)$ բազմանդամների որոշմանը: Ինչպես տեսանք 7.3.4 եւ 7.3.11 օրինակներում, $v(x)$-ի որոշ արժեքներ $f(x)$-ի ֆակտորիզացիայի չեն բերում: Ըստ 7.3.8 հետեւանքի՝ $v(x)$ բազմանդամների հնարավոր բոլոր արժեքների քանակը $p^{n(m-r)}$ է: Կա՞ն արդյոք այնպիսի «վատ» բազմանդամներ, որոնց ֆակտորիզացիան կառուցելու համար մենք ստիպված լինենք չափազանց շատ $v(x)$ արժեքներ կիրառել (p-ի մեծ արժեքների դեպքում սա իսկապես շատ կծանրացնի ալգորիթմը, առավել եւս, հաշվի առնելով այն, որ 7.4 պարագրաֆում մեզ պետք են գալու p-ի մեծ արժեքներ): Այս հարցը Բեռլեկեմպի մեթոդով պատասխան է ստանում հետեւյալ կերպ:

$\ker(Q-E)$-ի բազիսի՝ (7.18) համակարգի յուրաքանչյուր $v_i(x)$ բազմանդամի համար s_{ij}-ով նշանակենք K-ի այն տարրը, որի համար $v_i(x) \equiv s_{ij} \left(\mathrm{mod}\, p_j(x)\right)$: Կազմենք հետեւյալ մատրիցը.

$$S = \begin{pmatrix} s_{11} & \cdots & s_{1k} \\ \cdots\cdots\cdots & & \\ s_{k1} & \cdots & s_{kk} \end{pmatrix}:$$

7.3.13 Լեմմա. S մատրիցը չվերասերվող է՝ $\det S \neq 0$:

Ապացույց: Եթե S-ի տողերի միջեւ որեւէ $\alpha_i \in K$ սկալյարների համար տեղի ունենա $\sum_{i=1}^{k} \alpha_i s_{ij} = 0$, $j = 1, \ldots, k$ գծային կախվածությունը, ապա

$$\sum_{i=1}^{k} \alpha_i v_i(x) \equiv \sum_{i=1}^{k} \alpha_i s_{ij} \equiv 0 \left(\mathrm{mod}\, p_j(x)\right), \quad j = 1, \ldots, k:$$

Մյուս կողմից, զրոյական բազմանդամի համար մենք նույնպես ունենք $0 \equiv 0 \left(\mathrm{mod}\, p_j(x)\right)$, $j = 1, \dots, k$ համակարգը: Ըստ մնացքների մասին չինական թեորեմի՝ $\sum_{i=1}^{k} \alpha_i v_i(x) \equiv 0 \left(\mathrm{mod}\, f(x)\right)$, այսինքն՝ $\sum_{i=1}^{k} \alpha_i v_i(x) \vdots f(x)$: Քանի որ այս գումարի բոլոր գումարելիների աստիճանները $\deg f(x)$-ից փոքր են, այդ բաժանումը հնարավոր է միայն, երբ $\sum_{i=1}^{k} \alpha_i v_i(x) = 0$: Բայց $v_i(x)$ բազմանդամները գծորեն անկախ են, ուստի $\alpha_i = 0, i = 1, \dots, k$: ■

Ենթադրենք, թե որեւէ $v_i(x)$-ի համար $\left(f(x), (v_i(x) - s)\right)$-ը բաժանվում է միաժամանակ երկու $p_{j_1}(x)$ եւ $p_{j_2}(x)$ արտադրիչների վրա: Այդ դեպքում S մատրիցի i-րդ տողի j_1-րդ եւ j_2-րդ տարրերը իրար հավասար կլինեն: Իսկ եթե դա տեղի ունենա բոլոր $v_i(x)$, $i = 1, \dots, k$ բազմանդամների համար, ապա S մատրիցի j_1-րդ եւ j_2-րդ սյուները նույնը կլինեն: Դա հնարավոր չէ, քանի որ $\det S \neq 0$: Ուրեմն՝ կամայական երկու սյուների համար (7.18) համակարգում կան $v_{i_1}(x)$ եւ $v_{i_2}(x)$, որոնց համապատասխանող տողերում այդ սյուների տարրերը տարբեր են:

7.3.13 լեմման թույլ է տալիս ալգորիթմի կառուցումը եզրափակել հետեւյալ քայլերով. $Q - E$ օպերատորի $\ker(Q - E)$ միջուկի (7.18) բազիսի տարրերից մեկը, ասենք, $v_1(x)$-ը, կարելի է համարել հավասար 1-ի, քանի որ $1^{p^n} = 1$: Ինչպես տեսանք, այդ բազիսային վեկտորը $f(x)$-ի ֆակտորիզացիայի չի բերում: Ուստի անտեսենք $v_1(x)$-ը եւ անցնենք բազիսի հաջորդ վեկտորներին (դրանք բոլորն արդեն դրական աստիճան ունեն, քանի որ հաստատուն լինելու դեպքում գծորեն կախված կլինեին $v_1(x)$-ից):

Ըստ $v_2(x)$ բազմանդամի՝ հերթով հաշվելով $\left(f(x), (v_2(x) - s)\right)$ ամենամեծ ընդհանուր բաժանարարները բոլոր $s \in K$ տարրերի համար՝ դուրս գրենք դրական աստիճանի բոլոր $\left(f(x), (v_2(x) - s)\right)$ բազմանդամները: Նշանակենք դրանց

$$g_1(x), \dots, g_l(x)$$

ցանկը (հաջորդականությունը) $\mathcal{P}$ տառով: Ալգորիթմի աշխատանքի ավարտին $\mathcal{P}$-ն բաղկացած է լինելու որոնելի ֆակտորիզացիայի $p_1(x), \dots, p_k(x)$ արտադրիչներից: Եթե $l = m - r$, ապա արդեն գտել ենք $f(x)$-ի բոլոր $k = m - r$ հատ պարզ արտադրիչները: Իսկ եթե $l < m - r$, ապա $s \in K$ տարրերից որեւէ մեկի համար $\left(f(x), (v_2(x) - s)\right)$-ը բաժանվում է $p_1(x), \dots, p_k(x)$ պարզ արտադրիչներից առնվազն երկուսի վրա:

Այդ դեպքում վերցնենք հաջորդ՝ $v_3(x)$ բազմանդամը, հերթով հաշվենք $\left(g_t(x), (v_3(x) - s)\right)$ ամենամեծ ընդհանուր բաժանարարները բոլոր $s \in K$ տարրերի եւ $g_t(x)$, $t = 1, \dots, l$ արտադրիչների համար: Դրանցից դեն նետենք զրոյական աս-

տիճան ունեցողները: Հասկանալի է, որ եթե որեւէ $g_t(x)$ բազմանդամ պարզ է, ապա կամայական s-ի համար $\big(g_t(x), (v_3(x) - s)\big)$-ը ասոցացված է կամ $g_t(x)$-ին, կամ 1-ին, այսինքն՝ արդյունքում նոր արտադրիչ չի ստացվում: Իսկ եթե այդ $g_t(x)$-ը պարզ չէ, ապա $\big(g_t(x), (v_3(x) - s)\big)$-ը s փոփոխականի արժեքներից որեւէ մեկի համար կարող է բաժանվել $g_t(x)$-ի որեւէ ոչ տրիվիալ բաժանարարի վրա (վերջինս կունենա $\deg g_t(x)$-ից ավելի ցածր դրական աստիճան): $\mathcal{P}$ ցանկում յուրաքանչյուր $g_t(x)$ բազմանդամ փոխարինենք դրական աստիճանի $\big(g_t(x), (v_3(x) - s)\big)$ բաժանարարներով, ըստ բոլոր $s \in K$ արժեքների: Վերահամարակալենք $\mathcal{P}$ ցանկը եւ համարենք, որ այն արդեն բաղկացած է նոր բազմանդամներից (նրա բազմանդամների l քանակը կարող է աճել): Եթե արդեն $l = m - r$, ապա գտել ենք $f(x)$-ի բոլոր $k = m - r$ հատ պարզ արտադրիչները: Իսկ եթե դեռեւս $l < m - r$, ուրեմն՝ անցնենք հաջորդ $v_4(x)$ բազմանդամին եւ քայլը կրկնենք դրա համար:

7.3.13 լեմման պնդում է, որ այս քայլերը ստիպված կլինենք կրկնել ոչ ավել, քան $m - r$ անգամ: Ինչ-որ քայլում կունենանք $l = k = m - r$: Քանի որ $f(x)$-ը նորմավորված բազմանդամ է, որպես եզրափակիչ քայլ նորմավորենք վերջնական $\mathcal{P}$ ցանկի բոլոր բազմանդամները:

Ձեւակերպումն ավելի միանման դարձնելու համար նախապես կարող էինք համարել $l = 1$ եւ $g_1(x) = f(x)$: Այսինքն՝ $i = 2, 3, \dots$ արժեքների համար հաշվում ենք $\big(g_t(x), (v_i(x) - s)\big)$ ամենամեծ ընդհանուր բաժանարարները, $t = 1, \dots, l$ եւ $s \in K$ ($i = 2$ դեպքում $\mathcal{P}$ ցանկում ունենք միայն մեկ $g_t(x) = g_1(x) = f(x)$) բազմանդամ:

Մենք կառուցել ենք հետեւյալ ալգորիթմը.

7.3.14 Ալգորիթմ (վերջավոր դաշտի վրա տրված քառակուսիներից ազատ, նորմավորված բազմանդամի ֆակտորիզացիայի ալգորիթմը). Տրված է $f(x) \in K[x]$ քառակուսիներից ազատ, նորմավորված, ոչ զրոյական բազմանդամը, որտեղ K-ն կամայական վերջավոր դաշտ է: Գտնել $f(x)$-ի ֆակտորիզացիայի պարզ արտադրիչները:

1. Նշանակենք $m = \deg f(x)$:

2. Նշանակենք $j = 0$:

3. Քանի դեռ $j < m$

4. $r(x)$-ով նշանակենք $K[x]$ էվկլիդյան օղակում x^j բազմանդամը $f(x)$-ի վրա բաժանելիս ստացվող մնացորդը;

5. ($i = 1$; $i \le m$; $i++$) արժեքների համար

6. q_{ji}-ով նշանակենք $r(x)$ բազմանդամի $(i-1)$-րդ աստիճանի միանդամի գործակիցը ($q_{ji}=0$, եթե այդ միանդամը բացակա է);

7. վերցնենք $j=j+1$:

8. $M_m(K)$ մատրիցային օղակում վերցնենք $Q=\|q_{ji}\|,\ \ i,j=1,\dots,m$, մատրիցը:

9. Հաշվենք $k=m-\mathrm{rank}(Q-E)$, որտեղ E-ն միավոր մատրիցն է:

10. $q_{ji},\ \ i,j=1,\dots,m$ գործակիցներով կազմենք գծային համասեռ հավասարումների (7.17) համակարգը:

11. Գաուսի մեթոդով հաշվենք (7.17) համակարգի լուծումների $v_1,\dots,v_k\in K^m$ ֆունդամենտալ համակարգը: Որպես առաջին լուծում վերցնենք $v_1=(1,0,\dots,0)$:

12. $(i=1;\ i\le k;\ \ i++)$ արժեքների համար

13. վերցնենք $v_i(x)\in V$ բազմանդամը, որի $(j-1)$-րդ աստիճանի միանդամի գործակիցը հավասար է $v_i\in K^m$ վեկտորի j-րդ կոորդինատին, $j=1,\dots,m$:

14. Նշանակենք $l=1$:

15. Նշանակենք $g_l(x)=f(x)$:

16. Սահմանենք բազմանդամների $\mathcal{P}=\{g_t(x)\mid t=1,\dots,l\}$ ցանկը (մասնավորապես, եթե $l=1$, ապա $P=\{f(x)\}$):

17. Նշանակենք $i=2$:

18. $(t=1;\ t\le l;\ \ t++)$ արժեքների համար

19. $\mathcal{P}$ ցանկում $g_t(x)$-ն փոխարինենք դրական աստիճանի $\big(g_t(x),(v_i(x)-s)\big)$ բազմանդամներով՝ ըստ բոլոր $s\in K$ տարրերի;

20. վերահամարակալենք $\mathcal{P}$ ցանկի բազմանդամները եւ l-ով նշանակենք դրանց քանակը:

21. Եթե $l<k$

22. նշանակենք $i=i+1$;

23. վերադառնանք 18-րդ քայլին;

24. այլապես

25. նորմավորենք $\mathcal{P}$ ցանկի բոլոր բազմանդամները;

26. դուրս գրենք $\mathcal{P}$ ցանկի բազմանդամները:

4.5 պարագրաֆում մենք արդեն կառուցել ենք 4.5.2 ալգորիթմը, որը քառակուսիներից ազատ արտադրիչների է վերլուծում վերջավոր դաշտի (կամ վերջավոր ամբողջության տիրույթի) վրա տրված կամայական $f(x)$ բազմանդամ: Այդ ալգորիթմի եւ 7.3.14 ալգորիթմի օգնությամբ հեշտ է ֆակտորիզացնել K վերջավոր դաշտի վրա տրված կամայական դրական աստիճանի բազմանդամ.

7.3.15 Ալգորիթմ (վերջավոր դաշտի վրա տրված բազմանդամի ֆակտորիզացիայի ալգորիթմը). Տրված է $f(x) \in K[x]$ ոչ զրոյական բազմանդամը, որտեղ K-ն կամայական վերջավոր դաշտ է: Գտնել $f(x)$-ի ֆակտորիզացիայի պարզ արտադրիչները:

1. a_0-ով նշանակենք $f(x)$-ի ավագ անդամը:

2. Անցնենք $f(x) = \frac{1}{a_0} f(x)$ նորմավորված բազմանդամին:

3. 4.5.2 ալգորիթմով $f(x)$-ը վերլուծենք քառակուսիներից ազատ $f_1(x), \dots, f_r(x)$ բազմանդամների արտադրյալի՝ $f(x) = f_1(x) \cdots f_r(x)$:

4. Նորմավորենք $f_1(x), \dots, f_r(x)$ բազմանդամները:

5. Սահմանենք բազմանդամների $\mathcal{P}$ (դատարկ) ցանկը:

6. $(i = 1;\ i \le r;\ \ i++)$ արժեքների համար

7. $f_i(x)$ բազմանդամի համար 7.3.14 ալգորիթմով գտնենք նրա ֆակտորիզացիայի պարզ արտադրիչները եւ ավելացնենք դրանք $\mathcal{P}$ ցանկին;

8. $\mathcal{P}$ ցանկի առաջին բազմանդամը բաժանենք $a_0 \in K$ ոչ զրոյական տարրի վրա:

9. Դուրս գրենք $\mathcal{P}$ ցանկի բազմանդամները:

Նկատենք, որ երկու ալգորիթմներում էլ $\mathcal{P}$-ն անվանեցինք ոչ թե բազմանդամների բազմություն, այլ բազմանդամների ցանկ (հաջորդականություն): Բազմության մեջ որեւէ տարր չի կարող հանդիպել մեկից ավելի անգամ, իսկ հաջորդականության մեջ հնարավոր են անդամների կրկնություններ: Այս տարբերությունը չի դրսեւորվում 7.3.14 ալգորիթմում, քանի որ $f(x)$ բազմանդամը քառակուսիներից ազատ է, եւ $g_1(x), \dots, g_l(x)$ բազմանդամները ամեն քայլում զույգ առ զույգ տարբեր են: Բայց 7.3.15 ալգորիթմում տարբերությունը կարող է էական լինել: Օրինակ, $f(x) = x^3 + x^2 = x^2(x+1)$ բազմանդամը քառակուսիներից ազատ չէ: Նրա համար $\mathcal{P}$ ցանկը կլինի $x,\ x,\ x+1$:

7.3.16 Օրինակ. Հետեւյալ օրինակը Բեռլեկեմպի օրիգինալ (Berlekamp, 1967) հոդվածից է: $f(x)=x^{12}+x^8+x^7+x^6+x^2+x+1\in\mathbb{Z}_2[x]$: Բերենք այն առանց մանրամասների: Այս դեպքում V տարածությունը բաղկացած է $\mathbb{Z}_2$ դաշտի վրա տրված մինչեւ 11-րդ աստիճանի բազմանդամներից: $1,x,\dots,x^{11}$ բազիսի վրա Q օպերատորի ազդեցությունն է.

$$\begin{aligned}
1Q &= 1^2 = 1,\\
xQ &= x^2,\\
x^2Q &= x^4,\\
x^3Q &= x^6,\\
x^4Q &= x^8,\\
x^5Q &= x^{10},\\
x^6Q &= x^8+x^7+x^6+x^2+x+1,\\
x^7Q &= x^{10}+x^9+x^8+x^4+x^3+x^2,\\
x^8Q &= x^{11}+x^{10}+x^8+x^7+x^5+x^4+x^2+x+1,\\
x^9Q &= x^{10}+x^7+x^4+x^2+1,\\
x^{10}Q &= x^9+x^8+x^7+x^4+x+1,\\
x^{11}Q &= x^{11}+x^{10}+x^9+x^6+x^3+x^2:
\end{aligned}$$

Ըստ այդմ $Q-E$ մատրիցը կլինի.

$$R=\begin{pmatrix}
0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&1&0&0&0&0&0&0&0&0&0\\
0&0&1&0&1&0&0&0&0&0&0&0\\
0&0&0&1&0&0&1&0&0&0&0&0\\
0&0&0&0&1&0&0&0&1&0&0&0\\
0&0&0&0&0&1&0&0&0&0&1&0\\
1&1&1&0&0&0&0&1&1&0&0&0\\
0&0&1&1&1&0&0&1&1&1&1&0\\
1&1&1&0&1&1&0&1&0&0&1&1\\
1&0&1&0&1&0&0&1&0&1&1&0\\
1&1&0&0&1&0&0&1&1&1&1&0\\
0&0&1&1&0&0&1&0&0&1&1&0
\end{pmatrix}:$$

Սրա օգնությամբ կազմվում է համասեռ հավասարումների համակարգ, որի օգնությամբ ստացվում է $f(x)$-ի հետեւյալ ֆակտորիզացիան՝

$$f(x)=(x^5+x^3+x^2+x+1)(x^7+x^5+x^4+x^3+1):$$

7.3.17 Վարժություն. Կատարել նախորդ օրինակի հաշվարկները:

7.3.18 Վարժություն. Ֆակտորիզացնել հետեւյալ բազմանդամները $\mathbb{Z}_5[x]$ օղակում.

1) $f(x)=x^3+5x^2+4x$,

2) $f(x)=x^3+2x+5$:

7.3.19 Դիտողություն. Մեր շարադրանքը մի փոքր տարբերվում է Բեռլեկեմպի ալգորիթմի սկզբնական (Berlekamp, 1967) տարբերակից, որը չի օգտագործում $f(x)$ բազմանդամի վերլուծությունը քառակուսիներից ազատ արտադրիչների: $f(x)$-ը կարող է ունենալ մեկից բարձր պատիկության արտադրիչներ, այսինքն, (7.5) ներկայացման մեջ կարող են հանդիպել հավասար $p_i(x)$, $p_j(x)$, $i \neq j$ արտադրիչներ: (7.6) համակարգը այդ դեպքում պետք է կառուցել ոչ թե ըստ պարզ արտադրիչների մոդուլների, այլ ըստ դրանց մաքսիմալ աստիճանների մոդուլների: Ալգորիթմի հիմնավորումը այդ դեպքում գրեթե չի փոխվում: Այնումենայնիվ, քառակուսիներից ազատ արտադրիչների վերլուծությունը ավելի նախընտրելի է հաշվողական տեսակետից. որքան փոքրացնում ենք ֆակտորիզացիայի ենթարկվող $f(x)$ բազմանդամի աստիճանը, այնքան փոքրանում են V տարածությունը, Q եւ $Q - E$ մատրիցները, ինչը թեթեւացնում է ալգորիթմի ամենաաշխատատար մասը: Սա է պատճառը, թե ինչու Կնուտը իր (Knuth, 1969) մենագրության երկրորդ հատորի 4.6.2 պարագրաֆում նախքան բազմանդամի ֆակտորիզացիան վերլուծում է այն քառակուսիներից ազատ արտադրիչների: Այնուամենայնիվ, Կնուտի շարադրանքում շրջանցված է ալգորիթմի հիմնավորման երկրորդ մասը, որտեղ հաշվվում է ֆակտորիզացիայի համար անհրաժեշտ $v_i(x)$ բազմանդամների քանակը (ներառյալ 7.3.13 լեմման): Դրանից բացի, Կնուտի ապացույցը վերաբերում է ոչ թե կամայական վերջավոր դաշտերին, այլ միայն $\mathbb{Z}_p$-ին: (Knuth, 1969)-ի շարադրանքը առանց որեւէ էական փոփոխության օգտագործվել է մի շարք այլ մենագրություններում եւ դասագրքերում: Մենք հարմար համարեցինք վերադառնալ Բեռլեկեմպի սկզբնական հիմնավորմանը՝ այն ադապտացնելով քառակուսիներից ազատ բազմանդամների դեպքին:

7.4 Ցեսենհաուզի ֆակտորիզացիայի ալգորիթմը

Այս պարագրաֆում կներկայացվի $\mathbb{Z}[x]$ օղակում ֆակտորիզացիայի խնդրի լուծումը Ցեսենհաուզի մեթոդով: Հաշվի առնելով կամայական $f(x) \in \mathbb{Z}[x]$ ոչ զրոյական բազմանդամի $f(x) = \mathrm{cont}\big(f(x)\big)\mathrm{pp}\big(f(x)\big)$ ներկայացումը՝ կարելի է նախ ֆակտորիզացնել $\mathrm{cont}\big(f(x)\big) \in \mathbb{Z}$ բովանդակությունը, ապա անցնել պրիմիտիվ $\mathrm{pp}\big(f(x)\big)$ բազմանդամի ֆակտորիզացիային: Եթե $\mathrm{cont}\big(f(x)\big)$-ի պարզ արտադրիչների ցանկն է $\mathcal{C}$, իսկ $\mathrm{pp}\big(f(x)\big)$-ի պարզ արտադրիչների ցանկը՝ $\mathcal{F}$, ապա $f(x)$-ի ֆակտորիզացիան կստանանք $\mathcal{C}$ եւ $\mathcal{F}$ ցանկերի միացումով: Ուստի ենթադրենք, թե $\mathcal{C}$-ն արդեն հաշվված է, եւ, անցնելով $f(x) = \mathrm{pp}\big(f(x)\big)$ պրիմիտիվ բազմանդամին, ստորեւ հա-

մարենք, որ $f(x)$-ը պրիմիտիվ է (եթե հակառակը նշված չի լինի): Քանի որ բազմանդամի բովանդակությունը որոշվում է նշանի ճշտությամբ, համարենք նաեւ, որ $f(x)$-ի ավագ գործակիցը դրական է: Հիշեցնենք, որ $\mathcal{C}$-ն կամ $\mathcal{F}$-ը մենք անվանում ենք ցանկ (հաջորդականություն), այլ ոչ բազմություն, քանի որ դրանք կարող են ունենալ կրկնվող անդամներ:

7.4.1 Օրինակ. $f(x) = 12x^2 + 36x + 24 \in \mathbb{Z}[x]$ բազմանդամի ֆակտորիզացիան բաղկացած է հինգ արտադրիչներից $f(x) = 12(x^2 + 3x + 2) = 2^2 \cdot 3 \cdot (x + 1) \cdot (x + 2)$, որտեղ $\operatorname{cont}\big(f(x)\big) = 12$ բովանդակության համար $\mathcal{C}$ ցանկի բազմանդամներն են՝ $2,\ 2,\ 3$ եւ $\operatorname{pp}\big(f(x)\big)$-ի համար $\mathcal{F}$ ցանկի բազմանդամներն են՝ $x + 1,\ x + 2$:

7.4.2 Վարժություն. Քանի՞ պարզ արտադրիչից է բաղկացած 7.4.1 օրինակի $f(x)$ բազմանդամի ֆակտորիզացիան $\mathbb{Q}[x]$ օղակում:

$\mathbb{Z}[x]$ օղակի կամայական բազմանդամի ֆակտորիզացիայի խնդիրը կարելի է հանգեցնել որեւէ p պարզ թվի համար $K = \mathbb{Z}_p$ վերջավոր դաշտի վրա $\mathbb{Z}_p[x]$ բազմանդամային օղակում նույն խնդրի դիտարկմանը, որն, ինչպես տեսանք նախորդ պարագրաֆում, կարելի է լուծել Բեռլեկեմպի 7.3.14 եւ 7.3.15 ալգորիթմներով:

Ենթադրենք տրված է $\varphi_p\colon \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ մոդուլյար անցումը: Նախ, պայմանավորվենք նշանակումների մասին, քանի որ մոդուլյար անցումը կարող է փոխել ոչ միայն բազմանդամների գործակիցները, այլեւ դրանց պարզ արտադրիչների քանակը:

7.4.3 Օրինակ. $f(x) = x^3 + x^2 + x + 1 \in \mathbb{Z}[x]$ բազմանդամի ֆակտորիզացիան ունի երկու հատ պարզ, իրարից տարբեր արտադրիչներ՝ $f(x) = (x + 1)(x^2 + 1) = p_1(x)p_2(x)$: Ըստ $p = 2$ մոդուլի φ_2 անցումից հետո

$$f_2(x) = x^3 + x^2 + x + 1 = (x + 1)(x^2 + 1^2) = (x + 1)(x + 1)(x + 1) = q_1(x)q_2(x)q_3(x),$$

այսինքն, պարզ արտադրիչները երեք հատ են:

Ստանում ենք, որ եթե $f(x)$-ի ֆակտորիզացիան է

$$f(x) = p_1(x) \cdots p_s(x), \tag{7.19}$$

ապա $f_p(x)$-ի ֆակտորիզացիան կարող է եւ չունենալ $f_p(x) = p_{1,p}(x) \cdots p_{s,p}(x)$ տեսքը, որտեղ $p_{i,p}(x) = \varphi_p\big(p_i(x)\big)$: Ուստի պայմանավորվենք $f_p(x)$-ի ֆակտորիզացիան նշանակել

$$f_p(x) = q_1(x) \cdots q_k(x), \tag{7.20}$$

որտեղ k-ն կարող է տարբերվել s-ից, իսկ $q_i(x)$ արտադրիչը պարտավոր չէ լինել $p_i(x)$ արտադրիչի (կամ էլ՝ (7.19) ֆակտորիզացիայի անդամներից մի ուրիշի) պատկերը: (7.20) նշանակումը հարմար է նաեւ այն բանով, որ խուսափում ենք «p» տառի կրկնվող օգտագործումից՝ «$p_{i,p}(x)$»: Մյուս կողմից, պետք է հաշվի առնել, որ գրելով, ասենք՝ $q_2(x)$, մենք այս դեպքում ի նկատի ունենք ոչ թե ինչ-որ $q(x)$ բազմանդամի պատկերը φ_2 անցման ժամանակ, այլ (7.20) ֆակտորիզացիայի երկրորդ արտադրիչը: (7.20)-ի արտադրիչները կազմում են նախորդ պարագրաֆում հիշատակված $\mathcal{P}$ ցանկը:

Հաջորդ երկու հարցերը, որոնց կարող ենք միաժամանակ պատասխանել, *գործակիցների կրճատման* եւ *նախապատկերի վերականգնման* խնդիրներն են, որոնց մանրամասնորեն անդրադարձել ենք 2.4, 3.2 եւ 3.4 պարագրաֆներում:

7.4.4 Օրինակ. $f(x) = 7x^2 + 22$ բազմանդամի համար $f_7(x) = 1$, որը $f(x)$-ի բաժանարարների մասին այլեւս որեւէ էական ինֆորմացիա չի պարունակում φ_7 մոդուլյար անցումից հետո:

7.4.5 Օրինակ. Եթե $\mathbb{Z}_7[x]$ օղակում տրված է $f_7(x) = (x + 1)(x + 5)$ բազմանդամը, ապա $h(x) = x + 1$ պարզ արտադրիչի նախապատկեր կարող է լինել ինչպես $x + 1$, այնպես էլ $x + 8$ բազմանդամը: Մեզ անհրաժեշտ է մի մեխանիզմ, որով միարժեքորեն կվերականգնվի նրա այն հավանական նախապատկերը, որ բաժանարար է $f(x)$ բազմանդամի համար: Հավելյալ բարդություն է առաջանում *բացասական* գործակիցների համար. չէ՞ որ $x + 1$ արտադրիչի նախապատկեր կարող է լինել նաեւ $x - 6$ բազմանդամը:

Այս հարցերը լուծվում են Լանդաու-Մինյոտի գնահատականներով, որոնց անդրադարձել ենք 3.1 եւ 3.2 պարագրաֆներում: Եթե տրված $f(x) \in \mathbb{Z}[x]$ բազմանդամի համար ըստ (3.2) բանաձեւի հաշվենք $N_f = 2^{n-1}\|f(x)\|$ սահմանը եւ վերցնենք $p > 2 \cdot N_f$ պայմանին բավարարող ցանկացած p պարզ թիվ, ապա $f(x)$-ի կամայական բաժանարարի բոլոր գործակիցները մոդուլով փոքր կլինեն $p/2$-ից: Ուրեմն՝ φ_p անցման ժամանակ այդ գործակիցներից ոչ մեկը չի կրճատվի. այն կամ անփոփոխ կմնա, եթե դրական է (ուրեմն՝ փոքր է $p/2$-ից), կամ էլ դրան կգումարվի p, եթե այն բացասական է (գումարման արդյունքը մեծ կլինի $p/2$-ից): $f_p(x)$ մոդուլյար բազմանդամի $h(x)$ բաժանարարի նախապատկերը կարելի է վերականգնել՝ դրա գործակիցները հերթով $p/2$-ի հետ համեմատելով, այսինքն, ըստ 3.2.8 ալգորիթմի: Ուստի ենթադրենք, որ $p > 2 \cdot N_f$:

Նկատենք, որ բազմանդամի պրիմիտիվ մասին անցումը նպատակահարմար քայլ էր նաեւ p-ի հաշվման իմաստով, քանի որ որքան փոքրացնում ենք քննարկվող բազմանդամի գործակիցները, այնքան փոքրանում է N_f գնահատականը, փոքրանում է p-ն: Իսկ դա, իր հերթին, թեթեւացնում է 7.3.14 եւ 7.3.15 ալգորիթմների հաշվարկը:

Հաջորդ խնդիրը կապված է *քառակուսիներից ազատ* արտադրիչների հետ: $\mathbb{Z}_p[x]$ օղակում $f_p(x)$-ի ֆակտորիզացիայի 7.3.14 ալգորիթմը կիրառելուց առաջ, անհրաժեշտ է նախ այդ բազմանդամը վերլուծել քառակուսիներից ազատ արտադրիչների: Դա կարելի է անել 4.5.2 ալգորիթմով, ընդ որում, ինչպես տեսանք 4.5 պարագրաֆում, վերջավոր դաշտի վրա քառակուսիներից ազատ արտադրիչների վերլուծության խնդիրը, p-ի արժեքից կախված, երեք դեպքերի է տրոհվում: Այդ դեպքերից երրորդն անհամեմատ ավելի բարդ է, եւ ցանկալի է խուսափել դրանից: Մինչդեռ զրոյական բնութագրիչի դաշտի դեպքում քառակուսիներից ազատ արտադրիչների վերլուծությունը շատ ավելի հեշտ խնդիր է (տես 4.4 պարագրաֆը):

Այդ բարդությունները կարելի է շրջանցել, եթե $f(x)$-ը քառակուսիներից ազատ $f(x) = f_1(x) \cdots f_r(x)$ արտադրյալի վերլուծենք $\mathbb{Z}[x]$ օղակում, նախքան φ_p անցումը, եւ ապա $p = p(i)$ մոդուլը տվյալ $f_i(x)$ արտադրիչի համար ընտրենք այնպես, որ նրա $f_{i,p}(x) = \varphi_p\big(f_i(x)\big)$ պատկերը քառակուսիներից ազատ լինի $\mathbb{Z}_p[x]$-ում: Նշանակումների պարզության համար քառակուսիներից ազատ $f_i(x)$ բազմանդամը նույնպես նշանակենք $f(x)$-ով:

Ըստ 4.4 պարագրաֆի, որեւէ $f(x) \in \mathbb{Z}[x]$ բազմանդամի քառակուսիներից ազատ արտադրիչը ստացվում է $g(x) = \frac{f(x)}{(f(x),f'(x))}$ կանոնով: Ընդ որում, քառակուսիներից ազատ $f(x)$-ի համար $\big(f(x), f'(x)\big) = 1$: Իսկ եթե $\big(f(x), f'(x)\big) \not\approx 1$, ապա $g(x)$-ն $f(x)$-ից ավելի ցածր աստիճանի է:

Ենթադրենք $f_p(x) \in \mathbb{Z}_p[x]$ բազմանդամը, ի տարբերություն $f(x)$-ի, քառակուսիներից ազատ չէ: Ինչպես տեսանք 4.5 պարագրաֆում, դա հնարավոր է երեք դեպքերում, որոնցից առաջին երկուսում ունենք $\big(f_p(x), f_p'(x)\big) \not\approx 1$ եւ սրա շնորհիվ ստացվում էր քառակուսիներից ազատ $\frac{f_p(x)}{\left(f_p(x),f_p'(x)\right)}$ արտադրիչը: Իսկ երրորդ դեպքում p-ն բաժանում է $f_p(x)$-ի բոլոր (անդամների) աստիճանացույցերը, ինչի արդյունքում այդ բազմանդամը ներկայացվում է $f_p(x) = \Phi^{p^c}(x)$ տեսքով (տես (4.14) բանաձեւը):

$f_p(x)$-ի անդամների աստիճանացույցերը կարող են տարբերվել $f(x)$-ի աստիճանացույցերից, քանի որ մոդուլար անցման ժամանակ միանդամներից մի քանիսը կարող են կրճատվել: Բայց, հաշվի առնելով $p > 2 \cdot N_f$ պայմանը, դա մեր դեպքում տեղի չի ունենա. $f_p(x)$ եւ $f(x)$ բազմանդամների անդամներն ունեն միեւնույն աստիճանացույցերը: Ավելին, եթե $p > 2 \cdot N_f$, ապա p-ն մեծ է, քան $f(x)$-ի ավագ անդամի աստիճանացույցը, ուստի աստիճանացույցերի մասին պայմանը կարող ենք այլեւս չհիշատակել, քանի որ p-ն $f_p(x)$-ի աստիճանացույցերը չի բաժանում, եւ վերը հիշատակված երրորդ դեպքը տեղի չունի:

Հետեւաբար, եթե քառակուսիներից ազատ $f(x)$ բազմանդամի համար $p > 2 \cdot N_f$ պարզ թիվն այնպիսին է, որ $\left(f_p(x), f_p'(x)\right) = 1$, ապա $f_p(x)$-ը նույնպես քառակուսիներից ազատ է: $f(x)$ եւ $f'(x)$ բազմանդամների վրա 3.4.6 լեմման կիրառելով՝ կստանանք, որ եթե p-ն չի բաժանում $f(x)$ եւ $f'(x)$ բազմանդամների ավագ գործակիցներից գոնե մեկը եւ $R = \operatorname{res}\big(f(x), f'(x)\big)$ ռեզուլտանտը, ապա $\deg\big(f(x), f'(x)\big) = \deg\left(f_p(x), f_p'(x)\right)$, այսինքն, $f_p(x)$-ը նույնպես քառակուսիներից ազատ է: Այդ պայմաններից առաջինը միշտ կատարվում է, քանի որ, եթե $p > 2 \cdot N_f$, ապա p-ն մեծ է $f(x)$-ի ավագ գործակցի մոդուլից:

R ռեզուլտանտը բաժանող պարզ թվերի քանակը վերջավոր է, եւ $f_p(x)$-ը քառակուսիներից ազատ է անվերջ քանակությամբ p պարզ թվերի համար: Ստանում ենք.

7.4.6 Լեմմա. *Եթե $f(x) \in \mathbb{Z}[x]$ ոչ զրոյական բազմանդամն ազատ է քառակուսիներից, եւ $p > 2 \cdot N_f$ պարզ թիվը չի բաժանում $R = \operatorname{res}\big(f(x), f'(x)\big)$ ռեզուլտանտը, ապա $f_p(x) = \varphi_p\big(f(x)\big) \in \mathbb{Z}_p[x]$ բազմանդամը նույնպես ազատ է քառակուսիներից:*

Հաջորդ բարդությունը, որ պիտի շրջանցենք, կապված է *«ավելորդ» սկալյար արտադրիչների* հետ: Դրանց հանդիպել ենք նաեւ ամենամեծ ընդհանուր բաժանարարի ալգորիթմների կառուցման ժամանակ (տես 3.4.2 օրինակը): $\mathbb{Z}_p[x]$ օղակում կամայական ոչ զրոյական $t \in \mathbb{Z}_p$ տարր հակադարձելի է: Ուստի, եթե $f_p(x)$ բազմանդամի բաժանարարներից մեկը $h(x)$-ն է, ապա $t \cdot h(x)$-ը նույնպես բաժանարար է, որը, ենթադրենք, կարող է $f(x)$-ի բաժանարարներից ավելի մեծ գործակիցներ ունենալ (ուստի՝ դրանցից ոչ մեկի պատկերը չլինել):

7.4.7 Օրինակ. Վերցնենք 3.4.2 օրինակի $f(x) = x^2 + 4x + 3$ բազմանդամը: Կամայական $p > 4$ պարզ թվի համար $f_p(x) = x^2 + 4x + 3$, եւ այն ունի $f_p(x) = (x + 1)(x + 3)$ ֆակտորիզացիան: Միաժամանակ $p = 7$ դեպքում այն ունի նաեւ $f_7(x) = (4x + 4)(2x + 6)$ ֆակտորիզացիան: Եթե որեւէ ալգորիթմով գտնենք $f_7(x)$-ի

$q_1(x) = 4x + 4$ պարզ արտադրիչը, այն $f(x)$-ի որեւէ բաժանարարի պատկեր չի լինի, քանի որ $f(x)$-ի ավագ անդամը 4-ի վրա չի բաժանվում: Բայց $q_1(x)$-ը 2-ով բազմապատկելով՝ կստանանք $2(4x + 4) = x + 1$: Տվյալ դեպքում 4-ը «ավելորդ» արտադրիչ է, որը կարողացանք շրջանցել՝ բազմանդամը 2-ով բազմապատկելով:

7.4.8 Վարժություն. Գտնել նախորդ օրինակի $f(x)$ բազմանդամի բոլոր ֆակտորիզացիաները $\mathbb{Z}[x]$ օղակում: Գտնել նրա բոլոր ֆակտորիզացիաները $\mathbb{Z}_7[x]$ օղակում:

Ենթադրենք $\mathbb{Z}_p[x]$ օղակում $h(x)$-ը $f_p(x)$-ի «ավելորդ» սկալյար արտադրիչով բաժանարար է: Այսինքն՝ այն $f(x)$-ի որեւէ բաժանարարի պատկեր չէ, բայց ինչ-որ (մեզ անհայտ) $t \in \mathbb{Z}_p$ սկալյարի համար նրա $t \cdot h(x)$ պատիկը $f(x)$ բազմանդամի որեւէ $g(x)$ բաժանարարի պատկերն է՝ $g_p(x) = t \cdot h(x)$: Ունենք

(7.21) $$f(x) = g(x)u(x),$$

(7.22) $$f_p(x) = h(x)v(x):$$

Քանի որ t-ն հակադարձելի է, այս հավասարություններից երկրորդը կարելի է ձեւափոխել՝

(7.23) $$f_p(x) = \big(t \cdot h(x)\big)\big(t^{-1} \cdot v(x)\big) = g_p(x)\big(t^{-1} \cdot v(x)\big):$$

Եթե $f(x)$, $g(x)$, $u(x)$ բազմանդամների (դրական) ավագ գործակիցները նշանակենք, համապատասխանաբար, a_0, b_0, c_0, ապա, ըստ (7.21)-ի, $a_0 = b_0 \cdot c_0$: Ըստ p թվի ընտրության՝ այդ ավագ գործակիցները չեն փոխվում φ_p մոդուլյար անցման ժամանակ՝ $a_0 = a_{0,p}$, $b_0 = b_{0,p}$ եւ $c_0 = c_{0,p}$: Նշանակում է, որ (7.23) հավասարության ձախ մասի ավագ գործակիցը կրկին a_0 է, իսկ նրա աջ մասի արտադրիչների ավագ գործակիցները դարձյալ b_0 եւ c_0 են: (7.23)-ը կարելի է հասկանալ այսպես. $f_p(x)$-ի a_0 ավագ գործակիցը (7.22) հավասարության մեջ տրոհվել է $h(x)$ եւ $v(x)$ բազմանդամների ավագ գործակիցների արտադրյալին: (7.22)-ի մեջ $v(x)$-ի ավագ գործակցի «ավելորդ» t բաժանարարը փոխանցել ենք $h(x)$-ին եւ ստացել (7.23) հավասարությունը, որտեղ արտադրիչներից մեկն արդեն $g(x)$-ի պատկերն է:

Ասվածը սահմանափակում է դնում t-ի վրա: Այն ոչ թե կամայական ոչ զրոյական թիվ է $\mathbb{Z}_p$-ից, այլ b_0-ի ինչ-որ բաժանարար է: Մեզ հայտնի չէ b_0-ն, ուստի սահմանափակվենք ավելի թույլ պնդումով՝ t-ն a_0-ի ինչ-որ բաժանարար է: Նշանակում է, որ եթե t-ն ընտրենք այնպես, որ $t \cdot h(x)$-ի ավագ գործակիցը լինի a_0, եւ 3.2.8 ալգորիթմով հաշվենք $t \cdot h(x)$-ի $k(x)$ նախապատկերը, ապա $a_0 \cdot f(x)$-ը կբաժանվի $k(x)$-ի վրա: Մյուս կողմից, $f(x)$-ը պրիմիտիվ բազմանդամ է, եւ նրա բաժանարարները նույնպես պրիմիտիվ են: Ուստի մնում է ստուգել՝ արդյոք $f(x)$-ը բաժանվո՞ւմ է $\mathrm{pp}\big(k(x)\big)$-ի վրա:

Ստանում ենք «ավելորդ» սկալյար արտադրիչներից ազատվելու պարզ եղանակ: $f_p(x)$-ի $h(x)$ բաժանարարը բազմապատկենք այնպիսի մի t-ով, որ $t\cdot h(x)$-ի ավագ գործակիցը հավասարվի $f(x)$-ի ավագ գործակցին: Ըստ 3.2.8 ալգորիթմի՝ հաշվենք $t\cdot h(x)$-ի $k(x)$ նախատիպերը $\mathbb{Z}[x]$ օղակում: Ստուգենք՝ արդյո՞ք $f(x)$-ը բաժանվում է $\mathrm{pp}\big(k(x)\big)$ պրիմիտիվ մասի վրա: Եթե այո, ապա արդեն ազատվել ենք հավանական «ավելորդ» սկալյար արտադրիչից եւ գտել $f(x)$-ի $\mathrm{pp}\big(k(x)\big)$ բաժանարարը: Եթե ոչ, ապա $h(x)$ բազմանդամի $t\cdot h(x)$ պատիկներից *եւ ոչ մեկը* $f(x)$-ի որեւէ բաժանարարի պատկեր չէ ոչ մի $t\in\mathbb{Z}_p$ ոչ զրոյական արժեքի համար:

7.4.9 Վարժություն. «Ավելորդ» սկալյար արտադրիչներից ազատվելու բերված եղանակը կիրառել 7.4.7 օրինակի ֆակտորիզացիաների վրա:

Նախորդ քայլը պահանջում է փոխել p-ի գնահատականը: Պարզ p թիվը պետք է երկու անգամ մեծ լինի բոլոր այն բազմանդամների գործակիցների մոդուլներից, որոնց համար կիրառում ենք 3.2.8 ալգորիթմը: Մինչ այժմ մենք այն կիրառել էինք միայն $f(x)$-ի բաժանարարների համար: Բայց վերջին քայլում դիտարկեցինք նաեւ $a_0\cdot f(x)$-ի բաժանարարները: Ուստի N_f-ի փոխարեն վերցնենք $a_0\cdot N_f$: Հաշվի առնելով նաեւ ռեզուլտանտի հետ կապված պայմանը՝ այս պահին p-ի վրա դրվող պահանջն է՝

$$p>2\cdot a_0\cdot N_f \quad \text{եւ} \quad p\nmid R=\mathrm{res}\big(f(x),f'(x)\big): \tag{7.24}$$

Այս պայմանների մեջ a_0-ն եւ $\mathrm{res}\big(f(x),f'(x)\big)$-ն օգտագործելիս ենթադրվում էր, որ $f(x)$-ը քառակուսիներից ազատ է: Եթե դա այդպես չէ եւ $f(x)$-ը վերլուծված է r հատ քառակուսիներից ազատ բազմանդամների $f(x)=f_1(x)\cdots f_r(x)$ արտադրյալին, ապա յուրաքանչյուր $f_i(x)$ արտադրիչի համար դիտարկենք նրա $a_0=a_0(i)$ ավագ գործակիցը, N_{f_i} գնահատականը եւ $R=\mathrm{res}\left(f_i(x),{f_i}'(x)\right)$ ռեզուլտանտը եւ (7.24) պայմանը ձեւակերպենք ըստ դրանց:

Մեր դրած սահմանափակումների պայմաններում այժմ արդեն ավելի սերտ կապ ունենք (7.19) եւ (7.20) ֆակտորիզացիաների միջեւ: Եթե (7.19)-ի $f(x)$ բազմանդամը քառակուսիներից ազատ է, ապա այդպիսին է նաեւ (7.20)-ի $f_p(x)$ բազմանդամը: Դրանից բացի, (7.19)-ի $p_1(x),\dots,p_s(x)$ արտադրիչներից ոչ մեկը չի կրճատվել φ_p անցման ժամանակ: Իհարկե, հնարավոր է, որ այդ պարզ արտադրիչներից որեւէ մեկի պատկերն այլեւ պարզ չէ, եւ այն $\mathbb{Z}_p[x]$-ում, իր հերթին, վերլուծվել է այլ պարզ արտադրիչների արտադրյալի: 7.4.3 օրինակում $p_1(x)=x+1$ պարզ արտադրիչը արտապատկերվել է $p_{1,2}(x)=q_1(x)=x+1$ արտադրիչին, որը պարզ է նաեւ $\mathbb{Z}_2[x]$-ում: Իսկ $p_2(x)=x^2+1$ պարզ արտադրիչն արտապատկերվել է

$p_{2,2}(x)=x^2+1$ արտադրիչին, որն այլեւս պարզ չէ $\mathbb{Z}_2[x]$-ում. այն վերլուծվում է $q_2(x)q_3(x)$ արտադրյալին: Այսպիսով, չնայած մենք գիտենք, որ $p_i(x)$ բազմանդամներն առանց կրճատման արտապատկերվել են $\mathbb{Z}_2[x]$ օղակի մեջ, այնուամենայնիվ, դրանց պատկերները կարող են կրկին տրոհվել, եւ (7.20) ֆակտորիզացիայի տեսքից չի երեւում, թե դրա $q_i(x)$ արտադրիչներից որն ինչպես է ստացվել: Ավելին, ինչպես տեսանք 7.4.3 օրինակում, $q_i(x)$ արտադրիչները կարող են անգամ իրար հավասար լինել, բայց դրանց մի մասը որոշ $p_i(x)$ պարզ արտադրիչների պարզ պատկերներ են, մինչդեռ մնացածները ստացվել են $p_i(x)$ պարզ արտադրիչների բաղադրյալ պատկերների ֆակտորիզացիայից:

Ենթադրենք $f(x)$-ը քառակուսիներից ազատ, պրիմիտիվ, դրական ավագ գործակցով բազմանդամ է $\mathbb{Z}[x]$ օղակում, իսկ p-ն (7.24) պայմաններին բավարարող որեւէ պարզ թիվ է: Կիրառենք $\varphi_p\colon \mathbb{Z}[x]\to\mathbb{Z}_p[x]$ մոդուլյար անցումը, եւ $f_p(x)\in\mathbb{Z}_p[x]$ քառակուսիներից ազատ բազմանդամի համար 7.3.14 ալգորիթմով կառուցենք նրա (7.20) ֆակտորիզացիան ($\mathcal{P}$ ցանկը): Ցույց տանք, թե ինչպես դրանից կարելի է ստանալ $f(x)$-ի (7.19) ֆակտորիզացիան (այսինքն՝ ստանալ $\mathcal{F}$ ցանկը):

Ստուգենք, արդյո՞ք $q_1(x)\in\mathcal{P}$ արտադրիչը (7.19)-ի որեւէ պարզ արտադրիչի պատկեր է: Դրա համար $q_1(x)$-ը $\mathbb{Z}_p[x]$ օղակում բազմապատկենք այնպիսի $t\in\mathbb{Z}_p$ թվով, որ $t\cdot q_1(x)$-ի ավագ գործակիցը հավասար լինի $f(x)$-ի a_0 ավագ գործակցին: Հաշվենք $t\cdot q_1(x)$-ի $k(x)$ նախապատկերն՝ ըստ 3.2.8 ալգորիթմի: Ստուգենք՝ արդյո՞ք $f(x)\vdots \operatorname{pp}\big(k(x)\big)$: Եթե այո, ապա գտել ենք $f(x)$-ի առաջին պարզ արտադրիչը՝ $p_1(x)=\operatorname{pp}\big(k(x)\big)$: Ընդ որում, եթե $q_1(x)$-ը «ավելորդ» սկալյար արտադրիչ է ունեցել, մենք դրանից արդեն ազատվել ենք: Այդ դեպքում $p_1(x)$-ը ներմուծենք $f(x)$-ի պարզ բաժանարարների $\mathcal{F}$ ցանկի մեջ, $q_1(x)$-ը հեռացնենք $\mathcal{P}$ ցանկից, եւ $f(x)$-ը փոխարինենք $f(x)/p_1(x)$-ով: Իսկ հակառակ դեպքում եզրակացնում ենք, որ $q_1(x)$-ը $f(x)$-ի որեւէ բաժանարարի (մասնավորապես՝ պարզ բաժանարարի) պատկեր չէ: Այն առաջացել է $\mathbb{Z}_p[x]$-ում որեւէ այլ արտադրիչի ֆակտորիզացիայից:

Նույնը կրկնելով $q_2(x),\dots,q_k(x)$ արտադրիչների համար՝ մենք ամեն քայլում կամ $f(x)$-ի հերթական պարզ արտադրիչն ենք ստանում (եւ փոխարինում $f(x)$-ը իր բաժանարարով), կամ էլ ստանում ենք, որ տվյալ արտադրիչը $f(x)$-ի (պարզ) բաժանարարի պատկեր չէ: Եթե բոլոր k քայլերի ընթացքում միայն առաջին հնարավորությունն է հանդիպում, ապա $\mathcal{P}$ ցանկը դատարկվում է, եւ $f(x)$-ի ֆակտորիզացիան դրանով ավարտված է. որոնելի ցանկն է $\mathcal{F}$-ը:

Ենթադրենք $\mathcal{P}$ ցանկում մնացել են մի քանի արտադրիչներ: Ուրեմն՝ (7.19) ֆակտորիզացիայի ինչ-որ արտադրիչի պատկերը φ_p անցումից հետո այլեւս պարզ

չէ, եւ այն $\mathbb{Z}_p[x]$ օղակում տրոհվում է, ենթադրենք, *k հատ երկու հատ* պարզ արտադրիչների արտադրյալի: Ըստ $\mathbb{Z}_p[x]$-ի ֆակտորիալության՝ այդ պարզ արտադրիչները պարտավոր են լինել $\mathcal{P}$ ցանկում (հակադարձելի սկալյարի ճշտությամբ): Վերցնենք այդ ցանկի կամայական երկու $q_i(x)$, $q_j(x)$, $i \neq j$ բազմանդամներ եւ ստուգենք, արդյո՞ք $q_i(x)q_j(x)$ արտադրյալը (7.19)-ի որեւէ արտադրիչի պատկեր է: Դրա համար վերցնենք մի $t \in \mathbb{Z}_p$, որի համար $t \cdot q_i(x)q_j(x)$-ի ավագ գործակիցը հավասար լինի a_0-ին: Հաշվենք $t \cdot q_i(x)q_j(x)$-ի $k(x)$ նախապատկերն՝ ըստ 3.2.8 ալգորիթմի: Ստուգենք՝ արդյո՞ք $f(x) \vdots \mathrm{pp}\big(k(x)\big)$: Եթե այո, ապա $f(x)$-ի $\mathrm{pp}\big(k(x)\big)$ բաժանարարը նաեւ պարզ բաժանարար է: Իսկապես, եթե $\mathrm{pp}\big(k(x)\big)$-ը արտադրյալի վերլուծվեր, ապա նրա արտադրիչների պատկերները, իրենց հերթին, $\mathbb{Z}_p[x]$-ում կվերլուծվեին պարզ արտադրիչների արտադրյալի: Բայց, շնորհիվ $\mathbb{Z}_p[x]$-ի ֆակտորիալության, նման պարզ արտադրիչները (հակադարձելի սկալյարի ճշտությամբ) միայն երկուսն են՝ $q_i(x)$-ը եւ $q_j(x)$-ը: Ստացվում է, որ $\mathrm{pp}\big(k(x)\big)$-ի արտադրիչները միայն երկու հատ են, եւ դրանց պատկերներն են $q_i(x)$-ն եւ $q_j(x)$-ն: Բայց այդ դեպքում մենք արդեն ստացած կլինեինք այս արտադրիչները նախորդ քայլերից մեկում: Ուրեմն՝ $\mathrm{pp}\big(k(x)\big)$-ը պարզ է, եւ մենք կարող ենք ներմուծել այն $\mathcal{F}$ ցանկի մեջ, $\mathcal{P}$ ցանկից հեռացնել երկու $q_i(x)$ եւ $q_j(x)$ բազմանդամները, իսկ $f(x)$-ը փոխարինել $f(x)/\mathrm{pp}\big(k(x)\big)$-ով:

Նույն քայլերը կրկնելով $q_i(x)q_j(x)$, $i \neq j$ տեսքի բոլոր արտադրյալների համար՝ մենք ամեն քայլում կամ $f(x)$-ի հերթական պարզ արտադրիչն ենք ստանում (եւ փոխարինում $f(x)$-ը իր բաժանարարով), կամ էլ ստանում ենք, որ տվյալ $q_i(x)q_j(x)$ արտադրյալը $f(x)$-ի (պարզ) բաժանարարի պատկեր չէ: Եթե բոլոր զույգերի քննարկման ընթացքում միայն առաջին հնարավորությունն է կատարվում, ապա $\mathcal{P}$ ցանկը դատարկվում է, եւ $f(x)$-ի ֆակտորիզացիան դրանով ավարտված է:

Ենթադրենք $\mathcal{P}$ ցանկում դեռ մնացել են որոշ արտադրիչներ: Եթե (7.19)-ի ինչ-որ արտադրիչի պատկերը պարզ չէ $\mathbb{Z}_p[x]$-ում, ապա այն չի կարող տրոհվել երկու պարզ արտադրիչների արտադրյալի, քանի որ դրանց մենք քիչ առաջ հեռացրեցինք $\mathcal{P}$ ցանկից: Հավանական է, որ այն տրոհվում է *k հատ երեք հատ* պարզ արտադրիչների արտադրյալի: Դիտարկենք $q_i(x)q_j(x)q_s(x)$ տեսքի բոլոր եռյակների արտադրյալները, եւ քայլերը դրանց համար կրկնելով, դարձյալ որոշ բազմանդամներ ավելացնենք $\mathcal{F}$ ցանկին եւ որոշ բազմանդամներ պակասեցնենք $\mathcal{P}$ ցանկից:

Նույն կերպ կարելի է դիտարկել հնարավոր բոլոր քառյակները եւ այլն: Ինչ-որ քայլում $\mathcal{P}$ ցանկը կպարպվի, եւ $\mathcal{F}$ ցանկում կուտակված կլինեն որոնելի ֆակտորզացիայի դրական աստիճանի բոլոր պարզ արտադրիչները: Մնում է միայն ավե-

լացնել զրոյական աստիճանի պարզ արտադրիչները, որոնք մենք ամենասկզբում կուտակել էինք $\mathrm{cont}(f(x))$ բովանդակության ֆակտորիզացիայի $\mathcal{C}$ ցանկում:

Մենք կառուցեցինք հետեւյալ ալգորիթմը.

7.4.10 Ալգորիթմ ($\mathbb{Z}$ օղակի վրա տրված բազմանդամի ֆակտորիզացիայի ալգորիթմը). Տրված է $f(x) \in \mathbb{Z}[x]$ ոչ զրոյական բազմանդամը: Գտնել $f(x)$-ի ֆակտորիզացիայի պարզ արտադրիչները:

1. $f(x)$ բազմանդամի համար $\mathbb{Z}$ օղակում Էվկլիդեսի ալգորիթմով հաշվենք նրա $\mathrm{cont}(f(x))$ բովանդակությունը: Ընդ որում, նշանն ընտրենք այնպես, որ $f(x)/\mathrm{cont}(f(x)) = \mathrm{pp}(f(x))$ հարաբերության ավագ գործակիցը դրական լինի:

2. $\mathcal{C}$-ով նշանակենք $\mathrm{cont}(f(x)) \in \mathbb{Z}$ թվի ֆակտորիզացիայի պարզ արտադրիչների ցանկը:

3. Նշանակենք $f(x) = \mathrm{pp}(f(x))$:

4. Սահմանենք բազմանդամների $\mathcal{F}$ դատարկ ցանկը:

5. Ըստ 4.4.4 ալգորիթմի՝ $f(x)$-ը վերլուծենք քառակուսիներից ազատ $f_1(x), \dots, f_r(x)$ բազմանդամների արտադրյալի:

6. ($i = 1;\ i \le r;\ i++$) արժեքների համար

7. հաշվենք $R = \mathrm{res}\left(f_i(x), f_i'(x)\right)$ ռեզուլտանտը;

8. Լանդաու-Մինյոտի բանաձեւի (3.2) հետեւանքով հաշվենք N_{f_i} գնահատականը;

9. a_0-ով նշանակենք $f_i(x)$-ի ավագ գործակիցը;

10. ընտրենք այնպիսի մի p պարզ թիվ, որը բավարարում է $p > 2 \cdot a_0 \cdot N_{f_i}$ եւ $p \nmid R$ պայմաններին:

11. φ_p մոդուլյար անցումն իրականացնենք ըստ p մոդուլի եւ հաշվենք $f_i(x) \in \mathbb{Z}[x]$ բազմանդամի $f_{i,p}(x) \in \mathbb{Z}_p[x]$ պատկերը;

12. ըստ Բեռլեկեմպի 7.3.14 ալգորիթմի՝ կառուցենք $f_{i,p}(x)$ բազմանդամի ֆակտորիզացիայի պարզ արտադրիչների $\mathcal{P}$ ցանկը;

13. նշանակենք $n = 1$;

14. քանի դեռ $\mathcal{P}$ ցանկը դատարկ չէ

15. $\mathcal{P}$ ցանկի բազմանդամների յուրաքանչյուր $q_{i_1}(x), \dots, q_{i_n}(x)$ n-յակի համար

16. հաշվենք $q(x) = q_{i_1}(x) \cdots q_{i_n}(x)$ արտադրյալը;

17. $q(x)$-ը բազմապատկենք այնպիսի մի $t \in \mathbb{Z}_p$ թվով, որ $t \cdot q(x)$ արտադրյալի ավագ գործակիցը հավասար լինի a_0-ին;

18. ըստ 3.2.8 ալգորիթմի հաշվենք $t \cdot q(x)$-ի $k(x) \in \mathbb{Z}[x]$ նախապատկերը;

19. եթե $f_i(x) \vdots \mathrm{pp}\big(k(x)\big)$

20. $\mathcal{F}$ ցանկին ավելացնենք $\mathrm{pp}\big(k(x)\big)$ բազմանդամը;

21. $\mathcal{P}$ ցանկից հեռացնենք $q_{i_1}(x), \dots, q_{i_n}(x)$ բազմանդամները;

22. նշանակենք $f_i(x) = f_i(x)/\mathrm{pp}\big(k(x)\big)$:

23. Նշանակենք $n = n + 1$:

24. Վերադառնանք 15-րդ քայլին:

25. Դուրս գրենք $\mathcal{C}$ եւ $\mathcal{F}$ ցանկի բազմանդամները:

7.4.11 Դիտողություն. Հասկանալի է, որ 7.3.14, 7.3.15 եւ 7.4.10 ալգորիթմները լրացնում են միմյանց, ու կարելի է, ասենք, 7.3.14 եւ 7.4.10 ալգորիթմները միավորված տեսքով ներկայացնել՝ որպես $\mathbb{Z}[x]$-ում ֆակտորիզացիայի ալգորիթմ:

7.4.12 Օրինակ. Եթե 7.4.10 ալգորիթմի 12–24 քայլերը կիրառենք 7.4.3 օրինակի $f(x)$ եւ $f_2(x)$ բազմանդամների համար, ապա $\mathcal{P}$ ցանկը սկզբում բաղկացած կլինի երեք հատ $q_1(x) = q_2(x) = q_3(x) = x + 1$ բազմանդամներից: Վերցնենք $n = 1$: Քանի որ $f(x)$ եւ $q_i(x)$ բազմանդամները նորմավորված են, ապա $t = 1$: Պարզ է, որ $t \cdot (x + 1) = x + 1$ բազմանդամի նախապատկերն է $k(x) = x + 1$: Քանի որ $f(x) = x^3 + x^2 + x + 1$ բազմանդամը բաժանվում է $\mathrm{pp}\big(k(x)\big) = x + 1$ պրիմիտիվ մասի վրա, $x + 1$ արտադրիչը ներմուծենք $\mathcal{F}$ ցանկ, իսկ $\mathcal{P}$ ցանկում ջնջենք $q_1(x)$-ը: Իսկ $f(x)$-ը փոխարինենք $f(x) = (x^3 + x^2 + x + 1)/(x + 1) = x^2 + 1$ բազմանդամով: $\mathrm{pp}\big(k(x)\big)$-ը հաշվելով $q_2(x)$ եւ $q_3(x)$ արտադրիչների համար՝ մենք տեսնում ենք, որ այս դեպքում արդեն $f(x) = x^2 + 1$ բազմանդամը չի բաժանվի $x + 1$ պրիմիտիվ մասի վրա: Այսինքն՝ երկրորդ եւ երրորդ քայլերում $\mathcal{F}$ եւ $\mathcal{P}$ ցանկերը չեն փոխվում: Հաջորդ քայլի համար վերցնում ենք $n = n + 1 = 2$ եւ քննարկում $\mathcal{P}$ ցանկի զույգերը: Բայց մնացել է միայն մեկ զույգ՝ $q_2(x)$, $q_3(x)$: Քանի որ $q_2(x) \cdot q_3(x) = x^2 + 1$ եւ

$t=1$, ապա $\mathrm{pp}\big(k(x)\big)=x^2+1$: Քանի որ $f(x)=x^2+1$ բազմանդամը բաժանվում է դրա վրա, ապա չորրորդ քայլում x^2+1 արտադրիչը ներմուծենք $\mathcal{F}$ ցանկ, իսկ $\mathcal{P}$ ցանկում ջնջենք $q_2(x)$ եւ $q_3(x)$ արտադրիչները: $\mathcal{P}$ ցանկը պարպվում է, իսկ $\mathcal{F}$ ցանկում կուտակված արտադրիչներն են $p_1(x)=x+1$ եւ $p_2(x)=x^2+1$: Իսկապես, $x^3+x^2+x+1=(x+1)(x^2+1)\in\mathbb{Z}[x]$:

7.4.13 Օրինակ. Ենթադրենք տրված է $f(x)=15x^4+45x^3+75x^2+30x$ բազմանդամը: Նախ, ներկայացնենք այն $f(x)=\mathrm{cont}\big(f(x)\big)\mathrm{pp}\big(f(x)\big)=15(x^4+3x^3+5x^2+2x)$ տեսքով: $\mathrm{cont}\big(f(x)\big)=15$ բովանդակության համար $\mathcal{C}$ ցանկի պարզ արտադրիչներն են 3, 5 սկալյարները: Անցում կատարենք պրիմիտիվ $f(x)=\mathrm{pp}\big(f(x)\big)=x^4+3x^3+5x^2+2x$ բազմանդամին: Ունենք՝ $f'(x)=4x^3+12x^2+10x+2$: Քառակուսիներից ազատ արտադրիչը ստանալու համար $\mathbb{Q}[x]$ օղակում Էվկլիդեսի ալգորիթմով հաշվենք $\big(f(x),f'(x)\big)$-ը (գրառման համառոտության համար բաց ենք թողնում անկյունով բաժանումների քայլերը).

$$f(x)=\left(\frac{1}{4}x+\frac{1}{4}\right)f'(x)+\left(-\frac{1}{2}x^2-x-\frac{1}{2}\right),$$
$$f'(x)=(-8x-8)\left(-\frac{1}{2}x^2-x-\frac{1}{2}\right)+(-2x-2)$$
$$-\frac{1}{2}x^2-x-\frac{1}{2}=\left(\frac{1}{4}x+\frac{1}{4}\right)(-2x-2)+0:$$

Ստացանք $d(x)=-2x-2$ամենամեծ ընդհանուր բաժանարարը $\mathbb{Q}[x]$ օղակում: Այն $f(x)$-ի բաժանարար չէ $\mathbb{Z}[x]$ օղակում: Ըստ 4.4.4 ալգորիթմի՝ ավելորդ արտադրիչներից կարող ենք ազատվել՝ օգտվելով $f(x)$-ի պրիմիտիվությունից: $d(x)$-ն փոխարինենք $d(x)=\mathrm{pp}\big(d(x)\big)=(-2x-2)/(-2)=x+1$ բազմանդամով (իսկ կոտորակային գործակիցներից ազատվելու հարկ չկա, քանի որ նման գործակիցներ չեն առաջացել): $\big(f(x),f'(x)\big)=x+1$, եւ քառակուսիներից ազատ առաջին արտադրիչն է $f_1(x)=f(x)/(x+1)=x^3+3x^2+2x$: Հաշվելով $f(x)/f_1(x)=x+1$ արժեքը՝ միանգամից նկատում ենք, որ քառակուսիներից ազատ երկրորդ արտադրիչն է $f_2(x)=x+1$: Ակնհայտորեն $f_2(x)$-ը նաեւ պարզ է, եւ նրա համար հատուկ հաշվարկների կարիք չկա: Ուրեմն՝ անցնենք $f_1(x)$-ին եւ համառոտության համար նշանակենք $f(x)=f_1(x)$: Հեշտ է հաշվել, որ

$$R=\mathrm{res}\big(f(x),f'(x)\big)=\det\begin{pmatrix}1&3&2&0&0\\0&1&3&2&0\\3&6&2&0&0\\0&3&6&2&0\\0&0&3&6&1\end{pmatrix}=-4:$$

Քանի որ $N_f = 2^{3-1}\|f(x)\| = 4\sqrt{1+9+4} < 14.967$, ապա որպես p պարզ թիվ կարելի է վերցնել $p = 31 > 2 \cdot a_0 \cdot 14.967 = 29.934$: Մենք այժմ պիտի օգտագործենք φ_{31} մոդուլյար անցումը, բայց նկատենք, որ $f(x) = x^3 + 3x^2 + 2x$ բազմանդամի $\mathbb{Z}_7[x]$ օղակում ունեցած մոդուլյար $f_7(x)$ պատկերի համար 7.3.10 եւ 7.3.11 օրինակներում արդեն ստացել ենք, որ $f_7(x) = x^3 + 3x^2 + 2x = x(x+2)(x+1)$: Ստուգենք՝ արդյո՞ք այդ վերլուծությունը կարելի է օգտագործել այս դեպքում եւս (շատ ավելի հեշտ է դա ստուգելը, քան 7.3.14 ալգորիթմը $p = 31$ արժեքի համար կրկին կիրառելը): 7-ը չի բաժանում $R = -4$ ռեզուլտանտը: Դրանից բացի, $x(x+2)(x+1)$ արտադրյալի բոլոր գործակիցները շատ փոքր են, ու դրանք $p = 31$ մոդուլով բազմապատկվում են նույն կերպ, ինչ $p = 7$ մոդուլով. $x(x+2)(x+1) = x^3 + 3x^2 + 2x$ հավասարությունը տեղի ունի $\mathbb{Z}_7$, $\mathbb{Z}_{31}$ եւ $\mathbb{Z}$ օղակներից յուրաքանչյուրում: Վերջապես, x, $x+2$ եւ $x+1$ արտադրիչներից յուրաքանչյուրը առաջին աստիճանի է, եւ, ըստ $p = 31$ մոդուլի, չի կարող ունենալ ինչ-որ սեփական արտադրիչներ: Այդ երեք բազմանդամներից յուրաքանչյուրի համար հեշտ է անցնել 7.4.10 ալգորիթմի 12–24 քայլերով (ինչպես նախորդ օրինակում) եւ ստանալ, որ դրանցից յուրաքանչյուրի նախապատկերը բաժանում է $f(x)$-ը $\mathbb{Z}[x]$ օղակում: Այսինքն՝ դրանք ավելանում են $\mathcal{F}$ ցանկին ալգորիթմի երեք քայլերի ընթացքում եւ $n = 2$ դեպքին չենք հասնում: Այդ ցանկին ավելանում է նաեւ $f_2(x) = x + 1$ պարզ բազմանդամը: Հաշվի առնելով նաեւ $\mathcal{C}$ ցանկը՝ ստանում ենք որոնելի ֆակտորիզացիան.

$$f(x) = 15x^4 + 45x^3 + 75x^2 + 30x = 3 \cdot 5 \cdot x(x+2)(x+1)^2:$$

7.4.14 Վարժություններ. $\mathbb{Z}[x]$ օղակում ֆակտորիզացնել բազմանդամները.

1) $f(x) = 2x^3 + 13x^2 + 24x + 9$,

2) $f(x) = 6x^4 - 3x^3 - 12x^2 + 9x$:

7.4.15 Դիտողություն. 7.4.10 ալգորիթմը 7.3.14 ալգորիթմի հետ միասին երբեմն անվանում են Ցեսենհաուզ-Բեռլեկեմպի ալգորիթմ: Դա ֆակտորիզացիայի շատ արագ ալգորիթմ է, ինչը նշում է նաեւ Կնուտը (Knuth, 1969): Ալգորիթմի գնահատականներ կարելի է գտնել նաեւ ֆոն ցուր Գատենի մենագրության մեջ (von zur Gathen & Gerhard, 2003):

Այս ալգորիթմը ունի մի քանի տարբերակներ եւ բարելավումներ, ինչպիսին է, օրինակ, Հենզելի մեթոդը, որը թույլ է տալիս p-ն փոքրացնելու միջոցով թեթեւացնել Բեռլեկեմպի ալգորիթմի հաշվարկները: $f(x)$ բազմանդամի $f_p(x)$ պատկերի մոդուլյար ֆակտորիզացիան, նախ, ըստ փոքր p թվի արվում է $\mathbb{Z}_p[x]$ օղակում: Ապա ցույց է տրվում, թե ինչպես, ըստ p մոդուլի ֆակտորիզացիայից ելնելով, ստանալ

ֆակտորիզացիան ըստ p^2, p^3, ... մոդուլների: Ինչ-որ k-ի համար p^k-ն ավելի մեծ է, քան Լանդաու-Մինյոտի բանաձեւերով կամ ռեզուլտանտի միջոցով թելադրվող բոլոր անհրաժեշտ գնահատականները: Տես (von zur Gathen & Gerhard, 2003):

Պարագրաֆն ավարտենք $\mathcal{P}$ ցանկի երկարության վերաբերյալ գնահատականով: Կարելի՞ էր արդյոք p մոդուլն ընտրել այնպես, որ կարիք չլիներ դիտարկել $q_i(x)$ բազմանդամների զույգերը, եռյակները եւլն, եւ $f(x)$-ի բոլոր պարզ ֆակտորները ստացվեին որպես $q_i(x)$ բազմանդամների նախապատկերներ: Այլ խոսքերով՝ արդյո՞ք յուրաքանչյուր $f(x)$ բազմանդամի համար կա այնպիսի p, որի համար (7.19) եւ (7.20) ֆակտորիզացիաները հավասար քանակությամբ արտադրիչներ են պարունակում եւ (գուցե արտադրիչների վերադասավորությունից հետո) $q_i(x) = \varphi_p\big(p_i(x)\big)$: Սա շատ կպարզեցներ խնդիրը, բայց նման p ընդհանուր դեպքում գոյություն չունի: Մասնավորապես, կա այնպիսի $f(x) \in \mathbb{Z}[x]$ պարզ բազմանդամ, որի $f_p(x)$ պատկերը բաղադրյալ է *կամայական* p պարզ թվի համար:

7.4.16 Օրինակ. Ցույց տանք, որ $f(x) = x^4 + 1 \in \mathbb{Z}[x]$ պարզ բազմանդամը ունի նշված հատկությունը: Եթե $p = 2$, ապա $f_2(x) = x^4 + 1 = x^4 + 1^4 = (x + 1)^4$: Մնացած պարզ թվերի դեպքերը քննարկենք՝ օգտվելով պարզ թվի $p = 8k + i$ ներկայացումից, ընդ որում, $i = 0, 2, 4, 6$ դեպքերը բացառվում են, քանի որ p-ն զույգ չէ:

Առանց մանրամասների նշենք վերջավոր դաշտի մի քանի հատկություններ: Ըստ 4.1.11 թեորեմի՝ $\mathbb{Z}_p$ դաշտի մուլտիպլիկատիվ $\mathbb{Z}_p^* = \mathbb{Z}_p \backslash \{0\}$ խումբը $p - 1$ տարրից բաղկացած ցիկլիկ խումբ է: Հեշտ է ստուգել, որ նրա մեջ յուրաքանչյուր տարրը քառակուսի բարձրացնող σ արտապատկերումը (խմբի) հոմոմորֆիզմ է: Քանի որ մեր դեպքում խմբի $p - 1$ կարգը զույգ է, ապա $\{-1, 1\} \in \ker \sigma$: Հեշտ է ստուգել, որ σ-ի միջուկն այլ տարրեր չի պարունակում: Քանի որ $|\ker \sigma| = 2$, ապա $|\operatorname{im} \sigma| = |\mathbb{Z}_p^*|/|\ker \sigma| = (p - 1)/2$: Այսինքն՝ $\mathbb{Z}_p$ օղակում 0-ից բացի քառակուսի են հանդիսանում $(p - 1)/2$ հատ ոչ զրոյական թվեր:

Եթե $p = 8k + 1$, ապա, ինչպես դժվար չէ ստուգել, 2 թիվը քառակուսի է: Ենթադրենք $2 = s^2$: Այդ դեպքում $\mathbb{Z}_p[x]$ օղակում $x^4 + 1 = (x^2 - (2/s)x + 1)(x^2 + (2/s)x + 1)$:

Եթե $p = 8k + 3$, ապա քառակուսի է $-2 = p - 2$ թիվը: Ենթադրենք $-2 = s^2$: Այդ դեպքում $x^4 + 1 = (x^2 - (2/s)x - 1)(x^2 + (2/s)x - 1)$:

Եթե $p = 8k + 5$, ապա քառակուսի է $-1 = p - 1$ թիվը: Ենթադրենք $-1 = s^2$: Այդ դեպքում $x^4 + 1 = (x^2 - s)(x^2 + s)$:

Եթե $p = 8k + 7$, ապա կրկին քառակուսի է 2 թիվը, եւ այս դեպքում ֆակտորիզացիան ստացվում է $p = 8k + 1$ դեպքի նման:

7.4.17 Դիտողություն. Ինչպես տեսանք բազմանդամների ամենամեծ ընդհանուր բաժանարարի ուսումնասիրության ընթացքում, $f(x),\ g(x) \in \mathbb{Z}[x]$ բազմանդամների համար միշտ գոյություն ունի այնպիսի p պարզ թիվ, որ $\big(f(x), g(x)\big)$ ամենամեծ ընդհանուր բաժանարարը կարելի էր հաշվել՝ իմանալով միայն $\Big(f_p(x), g_p(x)\Big)$-ը: Ըստ 3.5.2 օրինակի՝ չնայած նման p գոյություն ունի, բայց հաշվարկն ըստ դրա տանելը կարող է արդյունավետ չլինի, քանի որ p-ն կարող է շատ մեծ թիվ լինել: 7.4.16 օրինակը ցույց է տալիս, որ նման օրինաչափություն ֆակտորիզացիայի խնդրում գոյություն չունի:

7.5 Ֆակտորիզացիան ռացիոնալ գործակիցներով

$\mathbb{Q}[x]$ օղակում բազմանդամի ֆակտորիզացիայի խնդիրը հեշտությամբ բերվում է այդ խնդրի լուծմանը $\mathbb{Z}[x]$ օղակում: Նախ նկատենք, որ միևնույն $f(x)$ բազմանդամի ֆակտորիզացիան $\mathbb{Q}[x]$ եւ $\mathbb{Z}[x]$ օղակներում կարող է տարբեր լինել, եթե անգամ $f(x)$-ի բոլոր գործակիցներն ամբողջ թվեր են: Դա պայմանավորված է բազմանդամի $\mathrm{cont}\big(f(x)\big)$ բովանդակության խաղացած դերով: Եթե $f(x) \in \mathbb{Z}[x]$, ապա $\mathrm{cont}\big(f(x)\big)$ բովանդակությունը, որպես $\mathbb{Z}$-ի ոչ հակադարձելի տարր, կարող է, իր հերթին, վերլուծվել պարզ արտադրիչների, որոնք մտնում են նաեւ $f(x)$-ի պարզ արտադրիչների ցանկի մեջ: Իսկ $\mathbb{Q}[x]$ օղակում բոլոր ոչ զրոյական թվերը հակադարձելի էն, եւ, ուրեմն, $\mathrm{cont}\big(f(x)\big)$-ը խաղում է 6.1.1 սահմանման (6.1) ֆակտորիզացիայի $\varepsilon \in \mathbb{Q}^*$ հակադարձելի տարրի դերը:

7.5.1 Օրինակ. Ինչպես տեսանք 7.4.1 օրինակում, $f(x) = 12x^2 + 36x + 24$ բազմանդամի ֆակտորիզացիան $\mathbb{Z}[x]$ օղակում ունի հինգ պարզ արտադրիչ՝ $f(x) = 12(x^2 + 3x + 2) = 2^2 \cdot 3 \cdot (x+1) \cdot (x+2)$: Իսկ $\mathbb{Q}[x]$ օղակում նույն բազմանդամը դիտարկելիս ստանում ենք միայն երկու պարզ արտադրիչ՝ $f(x) = 12 \cdot (x+1) \cdot (x+2)$, որտեղ $\varepsilon = 12$ թիվը պարզ արտադրիչ չէ, քանի որ այն հակադարձելի է $\mathbb{Q}$ դաշտում: Նույն $f(x)$ բազմանդամը կարելի էր ներկայացնել նաեւ, ասենք, $f(x) = (x/12 + 1/12) \cdot (x+2)$ տեսքով, որտեղ $\varepsilon = 1$, կամ էլ՝ $f(x) = (7/5) \cdot (x/12 + 1/12) \cdot (5/7x + 10/7)$, որտեղ $\varepsilon = 7/5$: Բոլոր երեք ներկայացումներն էլ, ըստ 6.1.1 սահմանման, բավարարում են ֆակտորիզացիայի միակության պահանջին. պարզ արտադրիչների քանակը երկու է. $x + 1 \approx x/12 + 1/12$ եւ $x + 2 \approx 5/7x + 10/7$: Համեմատել սա 7.4.2 վարժության հետ:

Ուրեմն՝ որպես $f(x) \in \mathbb{Q}[x]$ բազմանդամի ֆակտորիզացիայի առաջին քայլ, նկատենք, որ նրա $\mathrm{cont}\big(f(x)\big)$ բովանդակությունը (կամ նրա գործակիցներից ընդհանուր հանված ցանկացած ռացիոնալ սկալյար արտադրիչ) կարելի է համարել ֆակտորիզացիայի ε հակադարձելի տարր, որը չի մտնում պարզ արտադրիչների ցանկի մեջ: Ենթադրենք

$$f(x) = a_0x^n + \cdots + a_n \in \mathbb{Q}[x],$$

որտեղ $a_i \in \mathbb{Q}$, $i = 0, \dots, n$: Եթե v-ով նշանակենք $a_0, \dots, a_n$ գործակիցների հայտարարների ամենափոքր ընդհանուր բազմապատիկը, որը $\mathbb{Z}$ օղակում կարելի է հաշվել Էվկլիդեսի ալգորիթմի օգնությամբ, ապա

$$v \cdot f(x) = va_0x^n + \cdots + va_n \in \mathbb{Z}[x]:$$

Նշանակենք $g(x) = \mathrm{pp}\big(v \cdot f(x)\big) = v \cdot f(x)/\mathrm{cont}\big(v \cdot f(x)\big)$, ընդ որում, բովանդակության նշանն ընտրենք այնպես, որ $g(x)$-ի ավագ գործակիցը դրական լինի: Քանի որ $g(x)$ բազմանդամը $\mathbb{Z}[x]$-ից է, նրա վրա արդեն կարելի է կիրառել ֆակտորիզացիայի 7.4.10 ալգորիթմը: Ընդ որում, քանի որ $g(x)$-ի բովանդակությունը 1 է, ապա համապատասխան $\mathcal{C}$ ցանկը դատարկ կլինի, իսկ $\mathcal{F}$ ցանկը բաղկացած կլինի $p_1(x), \dots, p_s(x)$ պարզ եւ պրիմիտիվ բազմանդամներից՝

$$g(x) = p_1(x) \cdots p_s(x):$$

$p_i(x) \in \mathbb{Z}[x]$ բազմանդամները պարզ են նաեւ $\mathbb{Q}[x]$ օղակում: Մյուս կողմից, $g(x)$-ը $f(x)$-ից տարբերվում է միայն ռացիոնալ սկալյար արտադրիչով, քանի որ այն ստացել ենք $f(x)$-ը v-ով բազմապատկելով եւ $\mathrm{cont}\big(v \cdot f(x)\big)$-ի վրա բաժանելով: Այդ թվերին վերադառնալու հարկ չկա, քանի որ կարելի է համեմատել երկու բազմանդամների ավագ անդամները: Եթե $g(x)$-ի ավագ գործակիցը b_0-ն է, ապա $f(x) = \frac{a_0}{b_0} \cdot g(x)$: Մնում է $g(x)$-ի ֆակտորներից որեւէ մեկը, օրինակ, առաջինը, բազմապատկել $\frac{a_0}{b_0}$-ով: Որոնելի ֆակտորիզացիան կլինի՝

$$f(x) = \left[\frac{a_0}{b_0}p_1(x)\right] \cdot p_2(x) \cdots p_s(x):$$

Այսպիսով ստացանք հետեւյալ ալգորիթմը.

7.5.2 Ալգորիթմ ($\mathbb{Q}$ դաշտի վրա տրված բազմանդամի ֆակտորիզացիայի ալգորիթմը). Տրված է $f(x) \in \mathbb{Q}[x]$ ոչ զրոյական բազմանդամը: Գտնել $f(x)$-ի ֆակտորիզացիայի պարզ արտադրիչները:

1. $f(x)$ բազմանդամի համար $\mathbb{Z}$ օղակում Էվկլիդեսի ալգորիթմով հաշվենք նրա գործակիցների հայտարարների ամենափոքր ընդհանուր v բազմապատիկը:

2. a_0-ով նշանակենք $f(x)$-ի ավագ գործակիցը:

3. $\mathbb{Z}$ օղակում Էվկլիդեսի ալգորիթմով հաշվենք $v \cdot f(x)$ արտադրյալի $\operatorname{cont}\big(v \cdot f(x)\big)$ բովանդակությունը: Ընդ որում, նշանն ընտրենք այնպես, որ $\big(v \cdot f(x)\big)/\operatorname{cont}\big(v \cdot f(x)\big)$ հարաբերության ավագ գործակիցը դրական լինի:

4. Նշանակենք $g(x) = \operatorname{pp}\big(v \cdot f(x)\big)$:

5. Ըստ 7.4.10 ալգորիթմի՝ գտնենք $g(x) \in \mathbb{Z}[x]$ բազմանդամի $g(x) = p_1(x) \cdots p_s(x)$ ֆակտորիզացիան:

6. b_0-ով նշանակենք $g(x)$-ի ավագ գործակիցը:

7. Նշանակենք $p_1(x) = \frac{a_0}{b_0} p_1(x)$:

8. Դուրս գրենք $f(x)$-ի ֆակտորիզացիայի $p_1(x), \dots, p_s(x)$ պարզ արտադրիչները:

7.5.3 Վարժություններ. Ֆակտորիզացնել $\mathbb{Q}[x]$-ի հետեւյալ բազմանդամները.
1) $f(x) = x^3 + 13/2x^2 + 12x + 9/2$,
2) $f(x) = x^4 - 0.5x^3 - 2x^2 + 3/2x$,
3) $f(x) = 1/3x^4 + x^3 + 15/9x^2 + 2/3x$:
Յուցում՝ օգտվել 7.4.14 վարժություններից եւ 7.4.13 օրինակից:

Վերջավոր K դաշտի վրա տրված $K[x]$ օղակում կամ $\mathbb{Z}[x]$ եւ $\mathbb{Q}[x]$ օղակներում տրված $f(x)$ բազմանդամի ֆակտորիզացիայի խնդիրը լուծելիս մենք որեւէ սահմանափակում չունեինք $f(x)$-ի $p_i(x)$ պարզ արտադրիչների աստիճանների վրա: Դրանից բացի, մենք կարիք չունեցանք պարզելու, թե արդյո՞ք $f(x)$ բազմանդամը արմատներ ունի: Քանի որ $\mathbb{R}[x]$ եւ $\mathbb{C}[x]$ օղակներում ֆակտորիզացիայի խնդիրը էապես կախված է լինելու պարզ արտադրիչների աստիճանների սահմանափակությունից եւ $f(x)$-ի լուծումներից (տես 7.6.28 եւ 7.6.27 թեորեմները հաջորդ պարագրաֆում), այս պարագրաֆը եզրափակենք՝ ուսումնասիրելով $K[x]$, $\mathbb{Z}[x]$ եւ $\mathbb{Q}[x]$ օղակներում պարզ բազմանդամների աստիճանների անսահմանափակությունը եւ քննարկելով այդ օղակին պատկանող $f(x)$ բազմանդամի արմատները:

7.5.4 Թեորեմ (Էյզենշտեյնի հայտանիշը). *Ենթադրենք տրված է դրական աստիճանի $f(x) = a_0x^n + \cdots + a_n \in \mathbb{Z}[x]$ բազմանդամը եւ մի այնպիսի p պարզ թիվ, որ $p \nmid a_0$, $p|a_i$, երբ $i = 1, \dots, n$ եւ $p^2 \nmid a_n$: Այդ դեպքում $f(x)$-ը պարզ բազմանդամ է $\mathbb{Q}[x]$ օղակում:*

Ապացույց: Ենթադրենք հակառակը. $f(x)$-ը բերվող բազմանդամ է $\mathbb{Q}[x]$ օղակում՝ գոյություն ունեն դրական աստիճանի $g(x), h(x) \in \mathbb{Q}[x]$ բազմանդամներ, ո-

րոնց համար $f(x) = g(x)h(x)$: Նախ, Գաուսի լեմմայի օգնությամբ ցույց տանք, որ այդ դեպքում $f(x)$-ը բերվող է նաեւ $\mathbb{Z}[x]$ օղակում: Եթե v-ով նշանակենք $g(x),\ h(x)$ բազմանդամների բոլոր գործակիցների հայտարարների ամենափոքր ընդհանուր բազմապատիկը, ապա $v \cdot f(x) = v \cdot g(x)h(x)$ հավասարությունը տեղի կունենա նաեւ $\mathbb{Z}[x]$ օղակում: Երկու կողմերում էլ, անցնելով պրիմիտիվ մասերին եւ բազմապատկելով $\mathrm{cont}\big(f(x)\big)$-ով, կստանանք՝

$$f(x) = \mathrm{cont}\big(f(x)\big)\mathrm{pp}\big(v \cdot f(x)\big) = \mathrm{cont}\big(f(x)\big)\mathrm{pp}\big(v \cdot g(x)h(x)\big):$$

Նոր նշանակումներ չմտցնելու համար ենթադրենք, որ $g(x), h(x) \in \mathbb{Z}[x]$, ապա $f(x) = g(x)h(x)$ հավասարության երկու կողմերի վրա կիրառենք φ_p մոդուլյար անցումը: Ըստ թեորեմի պայմանի՝ $f_p(x) = a_{0,p}x^n$, որտեղ $a_{0,p} = \varphi_p(a_0)$-ն ոչ զրոյական թիվ է $\mathbb{Z}_p$-ից (մնացած բոլոր գործակիցների պատկերները զրոյացել են): $g(x)$, $h(x)$ բազմանդամների պատկերների արտադրյալը բաժանում է $f_p(x)$-ը, ուրեմն, ըստ $\mathbb{Z}_p[x]$-ի ֆակտորիալության, $g_p(x) = b_{0,p}x^k$ եւ $h_p(x) = c_{0,p}x^s$ (որտեղ $k + s = n$, իսկ $b_{0,p}$ եւ $c_{0,p}$ թվերը a_0-ի որեւէ b_0 եւ c_0 բաժանարարների պատկերներ են): Քանի որ $g(x)$ եւ $h(x)$ բազմանդամների բոլոր գործակիցները, բացի առաջինից, զրոյանում են φ_p անցման ժամանակ, դրանք բաժանվում են p-ի վրա: Բայց եթե այդ բազմանդամների *ազատ* անդամները նույնպես բաժանվեն p-ի վրա, ապա $f(x)$-ի a_n ազատ անդամը կբաժանվի p^2 վրա: Հակասություն: ■

7.5.5 Օրինակ. Որեւէ p պարզ թվի համար վերցնենք

$$f(x) = x^n + px^{n-1} + px^{n-2} + \cdots + px + b$$

բազմանդամը, որտեղ b ազատ անդամը բաժանվում է p-ի եւ չի բաժանվում p^2 վրա: Այդ դեպքում $f(x)$-ը պարզ բազմանդամ է $\mathbb{Z}[x]$ եւ $\mathbb{Q}[x]$ օղակներում: Որպես b կարելի է վերցնել, ասենք, $b = pq$ արտադրյալը, որտեղ q-ն p-ից տարբեր մի այլ պարզ թիվ է:

7.5.6 Հետեւանք. Ցանկացած n բնական թվի համար $\mathbb{Z}[x]$ եւ $\mathbb{Q}[x]$ օղակներում գոյություն ունի n-րդ աստիճանի չբերվող բազմանդամ:

Վերջավոր դաշտի վրա պարզ բազմանդամների գոյության հարցին մենք անդրադարձել ենք 4.2 պարագրաֆում: Եթե տրված է K դաշտի F ընդլայնումը, ապա $a \in F$ տարրի $m(x)$ մինիմալ բազմանդամն, ըստ 4.2.17 խնդրի, պարզ բազմանդամ է: Իսկ մինիմալ բազմանդամի աստիճանը հավասար է K դաշտի $K(a)$ ընդլայնման աստիճանին: Արդյո՞ք յուրաքանչյուր n բնական թվի եւ K դաշտի համար գոյութ-

յուն ունի նրա n-րդ աստիճանի F ընդլայնում, որի համար $K(a) = F$ որեւէ $a \in F$ տարրի համար (նման դեպքում a-ն կոչվում է F դաշտում K ենթադաշտի *պրիմիտիվ տարր*): Այս հարցին պատասխան է տալիս պրիմիտիվ տարրերի մասին Արթինի թեորեմը: Բերենք այն առանց ապացույցի.

7.5.7 Թեորեմ (Արթինի թեորեմը). *Եթե F-ը K դաշտի վերջավոր ընդլայնում է, ապա F դաշտում K ենթադաշտի պրիմիտիվ տարր գոյություն ունի այն եւ միայն այն դեպքում, երբ F դաշտում K-ն պարունակող ենթադաշտերի քանակը վերջավոր է:*

Թեորեմի ապացույցը կարելի է գտնել, օրինակ (Garrett, 2008) դասագրքի 22.3 պարագրաֆում: Եթե $|K| = p^m$, ապա $p^{m \cdot n}$ տարրից բաղկացած F դաշտ գոյություն ունի՝ ըստ 4.2.35 թեորեմի: Այն պարունակում է K-ն, եւ համապատասխան ընդլայնման աստիճանը n է, քանի որ $p^{m \cdot n}/p^m = p^n$: Ընդ որում, Արթինի թեորեմի պայմանը կատարվում է, քանի որ F-ը ոչ միայն K-ի վերջավոր ընդլայնում է (տարածության վերջավոր $[F, K]$ չափողականության իմաստով), այլեւ պարզապես վերջավոր է (որպես բազմություն), եւ F դաշտում K-ն պարունակող ենթադաշտերի քանակը անվերջ լինել չի կարող:

7.5.8 Հետեւանք. Ցանկացած n բնական թվի եւ K վերջավոր դաշտի համար $K[x]$ օղակում գոյություն ունի n-րդ աստիճանի չբերվող բազմանդամ:

Բազմանդամի ֆակտորիզացիան լուծում է նաեւ նրա *արմատների* հաշվման հարցը: Եթե տրված է $f(x) \in \mathbb{Q}[x]$ բազմանդամի

$$f(x) = p_1(x) \cdots p_s(x) \tag{7.25}$$

ֆակտորիզացիան, ապա յուրաքանչյուր $p_i(x)$ *գծային* արտադրիչի համապատասխանում է $f(x)$-ի մի արմատ. երբ $p_i(x) = c_o x + c_1$, այդ արմատն է $x_i = -\frac{c_1}{c_0}$: Եթե համարենք, որ (7.25) ֆակտորիզացիայում գծային են k հատ արտադրիչներ, ապա կստանանք համապատասխան $x_1, \dots, x_k$ արմատները: Ճիշտ է նաեւ հակառակը. եթե որեւէ $x_0 \in \mathbb{Q}$ թիվ $f(x)$-ի արմատ է, ապա, ըստ $\mathbb{Q}[x]$ օղակի էվկլիդյանության եւ Բեզուի թեորեմի, $f(x)$-ը բաժանվում է $x - x_0$ բազմանդամի վրա: Ըստ $\mathbb{Q}[x]$ օղակի ֆակտորիալության՝ այդ բազմանդամը ասոցացված է $p_1(x), \dots, p_k(x)$ գծային արտադրիչներից որեւէ մեկին՝ $x - x_0 = t \cdot p_i(x)$, ուստի այն կհաշվվի վերը նշված ճանապարհով: Ստացվում է ռացիոնալ գործակիցներով բազմանդամների ռացիոնալ արմատների հաշվման հետեւյալ մեթոդը. տրված $f(x) \in \mathbb{Q}[x]$ բազմանդամի հա-

մար 7.4.10 ալգորիթմով գտնենք նրա (7.25) ֆակտորիզացիան, եւ նրա յուրաքանչյուր $p_i(x)$ գծային արտադրիչից ստանանք համապատասխան արմատը: Իսկ $f(x) \in \mathbb{Z}[x]$ բազմանդամի համար նույն քայլերը կարելի է կիրառել $\mathbb{Q}$ դաշտի վրա, եւ ապա դրանցից առանձնացնել $\mathbb{Z}$-ին պատկանող լուծումները: Մենք այս մեթոդը ալգորիթմի տեսքով դուրս չենք գրում, քանի որ այն արդյունավետ է միայն այն խնդիրներում, որտեղ բազմանդամի ֆակտորիզացիան կամ արդեն հաշվված է, կամ էլ Ցեսենհաուզ-Բեռլեկեմպի ալգորիթմի քայլերի զգալի մասն արդեն արված են:

Կան ռացիոնալ գործակիցներով բազմանդամի արմատները հաշվելու այլ, շատ ավելի թեթեւ ալգորիթմներ: Դրանցից մեկը կարելի է ստանալ «ռացիոնալ արմատների մասին» թեորեմից.

7.5.9 Թեորեմ. *Ենթադրենք տրված է $f(x) = a_0x^n + \cdots + a_n \in \mathbb{Z}[x]$ բազմանդամը, ընդ որում, նրա a_0 ավագ եւ a_n ազատ անդամները ոչ զրոյական են: Եթե $f(x)$-ի x_0 ռացիոնալ արմատը ներկայացված է $x_0 = \frac{u}{v}$ անկրճատելի կոտորակի տեսքով ($u \in \mathbb{Z}$ եւ $v \in \mathbb{N}$), ապա $a_n \vdots u$ եւ $a_0 \vdots v$:*

Ապացույց: Ապացուցենք օգտվելով Գաուսի լեմմայից: Քանի որ $\mathbb{Z}[x]$ եւ $\mathbb{Q}[x]$ օղակներում բազմանդամների բաժանելիությունը տարբերվում է միայն սկալյար արտադրիչով եւ, քանի որ $f(x)$-ի գործակիցներն ամբողջ են, $\mathrm{pp}\big(f(x)\big)$ պրիմիտիվ մասը $\mathbb{Z}[x]$ եւ $\mathbb{Q}[x]$ օղակներում ունի միեւնույն ֆակտորիզացիան: Պարզ է նաեւ, որ $\mathrm{pp}\big(f(x)\big)$ եւ $f(x)$ բազմանդամներն ունեն միեւնույն արմատները: $x_0 = \frac{u}{v}$ թիվը $\mathrm{pp}\big(f(x)\big)$-ի արմատ է այն եւ միայն այն դեպքում, երբ $\mathbb{Z}[x]$ օղակում $\mathrm{pp}\big(f(x)\big)$-ի ֆակտորիզացիայում կա $\pm(vx - u)$ արտադրիչը (սա այն արտադրիչն է, որին $\mathbb{Q}[x]$ օղակում ասոցացված է $x - x_0 = x - \frac{u}{v}$ արտադրիչը): $\mathrm{pp}\big(f(x)\big)$-ի ավագ անդամը ստացվում է՝ ֆակտորիզացիայի մնացած պարզ արտադրիչների ավագ անդամների հետ vx-ը բազմապատկելով: Հետեւաբար $\mathrm{pp}\big(f(x)\big)$-ի (ուրեմն՝ նաեւ $f(x)$-ի) ավագ գործակիցը բաժանվում է v-ի վրա: Նույն կերպ՝ $\mathrm{pp}\big(f(x)\big)$-ի (ուրեմն՝ նաեւ $f(x)$-ի) ազատ անդամը բաժանվում է u-ի վրա: ■

Ըստ այս թեորեմի՝ $f(x) \in \mathbb{Q}[x]$ բազմանդամի արմատները կարելի է գտնել հետեւյալ կանոնով: Եթե բոլոր գործակիցները չէ, որ ամբողջ են, ապա բազմանդամը կարելի է բազմապատկել նրա գործակիցների հայտարարների ամենափոքր ընդհանուր բաժանարարով եւ ստանալ $\mathbb{Z}[x]$ օղակի բազմանդամ: Անցնենք նրա պրիմիտիվ մասին (սա նպատակահարմար է նաեւ հետագա հաշվարկները փոքրացնելու համար): Նոր նշանակում չմտցնելու համար ենթադրենք, թե այդ պրիմիտիվ մասն է $f(x) = a_0x^n + \cdots + a_n$: Եթե $a_n \neq 0$, ապա կազմենք բոլոր $\frac{u}{v}$ տեսքի անկրճատելի կոտորակների ցանկը, որտեղ $a_n \vdots u$ եւ $a_0 \vdots v$: Հերթով ստուգենք, թե դրանցից որոնք են $f(x)$-ի արմատ: Ընդ որում, պատիկ արմատների հետ թյուրիմացություն

չստանալու համար ամեն անգամ, երբ $\frac{u}{v}$ տեսքի որեւէ արմատ է հայտնաբերվում, $f(x)$-ը փոխարինենք $f(x)/\left(x-\frac{u}{v}\right)$ հարաբերությամբ: Իսկ եթե $a_n=0$, ապա $f(x)$-ի բոլոր անդամները բաժանվում են x-ի վրա, եւ $f(x)$-ի արմատներից մեկն է $x_0=0$: Այդ դեպքում 0-ն ներմուծենք $f(x)$-ի արմատների ցանկի մեջ եւ $f(x)$-ը փոխարինենք $f(x)/x$ հարաբերությամբ: Կրկնենք քայլը: Չի բացառվում, որ $f(x)/x$-ի ավագ անդամը կրկին զրոյական է (այդ դեպքում $x_0=0$ արմատն ունի մեկից ավելի պատիկություն):

7.5.10 Օրինակ. Դիտարկենք $f(x)=x^3+\frac{7}{2}x^2+3x$ բազմանդամը: Կոտորակային գործակցից խուսափելու համար անցնենք $f(x)=2\cdot f(x)=2x^3+7x^2+6x$ բազմանդամին: Ազատ անդամը զրոյական է: Ուստի 0-ն ներմուծենք արմատների ցանկի մեջ եւ անցնենք $f(x)=f(x)/x=2x^2+7x+6$ բազմանդամին: $a_2=6$ ազատ անդամի u բաժանարարի հնարավոր ամբողջ արժեքներն են $u=\pm6,\ \pm3,\ \pm2,\ \pm1$: Իսկ $a_0=2$ ազատ անդամի v բաժանարարի հնարավոր բնական արժեքներն են $v=2,\ 1$: Ուստի լուծումները որոնում ենք հետեւյալ 16 թվերի ցանկից.

$$\pm6/2, \pm3/2, \pm2/2, \pm1/2, \pm6, \pm3, \pm2, \pm1:$$

Երկրորդ քայլում ստանում ենք $-3/2$ լուծումը եւ հետագա բաժանումները ստուգում $f(x)/(x+3/2)=x+2$ բազմանդամի համար: Վերջինիս $x=-2$ արմատը կամ միանգամից նկատում ենք իր տեսքից, կամ էլ ստանում ենք մեր ցանկի 7-րդ քայլում: Որոնելի արմատներն են՝ 0, $-3/2$ եւ -2: Հետաքրքիր է, որ այս դեպքում ստանում ենք նաեւ նախնական $f(x)$ բազմանդամի $f(x)=2x(x+3/2)(x+2)=x(2x+3)(x+2)$ ֆակտորիզացիան: Ընդհանուր դեպքում, իհարկե, այս մեթոդով ֆակտորիզացիան ստանալ չի կարելի, քանի որ $f(x)$-ը կարող է ունենալ ոչ զծային արտադրիչներ: Եթե մեր բազմանդամի համար անհրաժեշտ է գտնել նրա արմատները $\mathbb{Z}$-ում, ապա պարզապես անտեսում ենք $-3/2$ արմատը:

Մենք բերեցինք $\mathbb{Z}[x]$ եւ $\mathbb{Q}[x]$ օղակներում կամայական բազմանդամի արմատները հաշվելու երկու եղանակներ՝ ըստ Ցեսենհաուզ-Բեռլեկեմպի ալգորիթմի եւ ըստ ռացիոնալ արմատների մասին թեորեմի: Երկու եղանակներն էլ բաղկացած են ընդամենը մեկ քայլից, եւ դրանք ալգորիթմների տեսքով ներկայացնելը դժվար չէ.

7.5.11 Խնդիր. Դուրս գրել $\mathbb{Z}[x]$ օղակի կամայական բազմանդամի արմատների հաշվման ալգորիթմը՝ հենվելով Ցեսենհաուզ-Բեռլեկեմպի ալգորիթմի ֆակտորիզացիայի վրա: Ալգորիթմի անալոգը ստանալ $\mathbb{Q}[x]$ օղակի համար:

7.5.12 Խնդիր. Դուրս գրել $\mathbb{Z}[x]$ օղակի կամայական բազմանդամի արմատների հաշվման ալգորիթմը՝ օգտվելով ռացիոնալ արմատների մասին թեորեմից: Ալգորիթմի անալոգը ստանալ $\mathbb{Q}[x]$ օղակի համար:

Մենք մինչ այժմ չենք դիտարկել K վերջավոր դաշտի վրա բազմանդամի արմատների հաշվման հարցը: Բայց դա տարրական խնդիր է, քանի որ K-ն վերջավոր է, եւ ցանկացած բազմանդամի արմատները կարելի է գտնել՝ դաշտի բոլոր տարրերը բազմանդամի մեջ տեղադրելով:

7.5.13 Խնդիր. Դուրս գրել K վերջավոր դաշտի վրա տրված $K[x]$ օղակի կամայական բազմանդամի արմատների հաշվման ալգորիթմը՝ օգտվելով K-ի վերջավորությունից:

7.6 Գալուայի խումբը, իրական եւ կոմպլեքս ֆակտորիզացիան

$\mathbb{R}$ եւ $\mathbb{C}$ դաշտերում առկա *անընդհատության* գաղափարն այդ դաշտերի վրա ֆակտորիզացիայի հարցը հիմնովին տարբեր է դարձնում $\mathbb{Z}$-ի եւ $\mathbb{Q}$-ի վրա ֆակտորիզացիայի խնդրից: Անսպասելի է, բայց $\mathbb{R}[x]$ կամ $\mathbb{C}[x]$ օղակներում որոշ բազմանդամների հանրահաշվորեն ճշգրիտ ֆակտորիզացիան գտնելը կարող է ալգորիթմորեն անլուծելի խնդիր լինել, եւ այն կարելի է իրականացնել միայն որոշ ճշտությամբ՝ մոտարկման բանաձեւերի օգնությամբ:

Մինչեւ դրան անդրադառնալը հստակեցնենք, թե ինչ ի նկատի ունենք՝ «անլուծելի խնդիր» ասելով: Քանի որ $\mathbb{R}[x]$ եւ $\mathbb{C}[x]$ օղակներն Էվկլիդյան են, ըստ Բեզուի թեորեմի, դրանց պատկանող $f(x)$ բազմանդամը ունի x_i արմատը այն եւ միայն այն դեպքում, երբ $f(x)$-ը բաժանվում է $x - x_i$ գծային արտադրիչի վրա: Քանի որ այդ արտադրիչն ակնհայտորեն պարզ է, ապա բազմանդամի բացահայտ ֆակտորիզացիայի խնդիրն իր մեջ ներառում է նաեւ բազմանդամի արմատների բացահայտ հաշվման խնդիրը. եթե $f(x)$-ն ունի x_i արմատը, ապա $x - x_i$ պարզ արտադրիչը գտնելը համարժեք է x_i-ն հաշվելուն: Ինչպես տեսանք 7.5 պարագրաֆի վերջում, մենք այդ հարցին իսկապես կարող ենք պատասխանել $\mathbb{Z}[x]$, $\mathbb{Q}[x]$ եւ $K[x]$ օղակներից յուրաքանչյուրում (K-ն կամայական վերջավոր դաշտ է):

Իրավիճակն այլ է $\mathbb{R}[x]$ եւ $\mathbb{C}[x]$ օղակներում: Նախ հիշենք, որ տրված $f(x) = a_0x^2 + a_1x + a_2 = 0$ քառակուսի հավասարումը ավանդական մեթոդով դիսկրիմինանտի օգնությամբ լուծելիս մենք $f(x)$-ի արմատները ստանում ենք որպես $f(x)$-ի գործակիցների հետ գործողությունների կատարման՝ գումարման, հանման, բազմապատկման, բաժանման եւ ինչ-որ աստիճանի արմատ հանման գործողությունների մի շղթայի արդյունք՝ $x_{1,2} = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$: *Կարդանոյի բանաձեւով* եւ *Կարդանոյի ընդհանրացված բանաձեւով* կարելի է ստանալ նաեւ երրորդ եւ չորրորդ աստի-

ճանի բազմանդամների արմատները: Այդ բանաձեւերը շատ ավելի խրթին տեսք ունեն, բայց դրանք կրկին ստացվում են նշված գործողությունների շղթայի արդյունքով, այսինքն՝ *ստացվում են ռադիկալներով*: Գոյություն ունեն հինգ եւ ավելի բարձր աստիճանի բազմանդամներ, որոնց արմատները ռադիկալներով չեն ստացվում, այսինքն՝ ինչպիսի բանաձեւեր էլ մենք կառուցենք վերը թվարկված գործողություններով, դրանցով բազմանդամի արմատը չի հաշվվի: Այդ փաստը ստացվել է Ռուֆինիի ու Աբելի, եւ նրանցից անկախ՝ Գալուայի կողմից: Ստորեւ կբերենք նման բազմանդամի օրինակ:

7.6.1 Դիտողություն. 4.2 պարագրաֆում մենք մանրամասնորեն շարադրեցինք դաշտերի ընդլայնումների եւ հանրահաշվական փակույթի կառուցման տեսությունը: Դա անհրաժեշտ էր 4-րդ գլխի 4.4 եւ 4.5 պարագրաֆների ալգորիթմների, 7-րդ գլխի 7.3 եւ 7.4 պարագրաֆների ալգորիթմների եւ հետագայում 8-րդ գլխի ալգորիթմների ամբողջական հիմնավորումը ունենալու համար: Ստորեւ մեզ պետք է գալու 4.2 պարագրաֆի տեսության զարգացումը՝ Գալուայի խմբի սահմանումը եւ մի քանի հատկությունները: Օգտագործելու ենք նաեւ լուծելի խմբի հասկացությունը եւ լուծելի խմբի մի քանի օրինակներ: Սակայն, ի տարբերություն 4.2 պարագրաֆի, այստեղ մենք բաց ենք թողնելու հիմնական ապացույցները, քանի որ դրանք պետք են ոչ թե հետագա ալգորիթմների տեսական հիմնավորման, այլ միայն մեկ կարեւոր օրինակի կառուցման համար. գոյություն ունի բազմանդամ, որի արմատները հնարավոր չէ հաշվել ռադիկալներով, ուստի $\mathbb{R}[x]$ եւ $\mathbb{C}[x]$ օղակներում բազմանդամի ֆակտորիզացիայի խնդիրը նույնպես անլուծելի է: Գալուայի տեսությանը վերաբերող ապացույցների մանրամասները կարելի է գտնել (Rotman, 1995), (Artin, 1997), (Garrett, 2008), (Lang, 2002), (Кострикин, 1977), (Кострикин, 2004), (Beachy & Blair, 2006), (Cohn, 2003), (Dummit & Foote, 2004) դասագրքերում: Ստորեւ մենք առանց ապացույցի օգտագործելու ենք նաեւ խմբերի տեսության մի շարք փաստեր, որոնց ապացույցները կարելի է գտնել, օրինակ, (Robinson, 1996), (Rotman, 1995), (Каргаполов & Мерзляков, 1996), (Курош, 1967), (Garrett, 2008), (Lang, 2002), (Кострикин, 1977), (Beachy & Blair, 2006), (Cohn, 2003), (Dummit & Foote, 2004) դասագրքերում:

Ենթադրենք տրված է K դաշտի F ընդլայնումը: Մենք պայմանավորվել էինք այս փաստը համառոտ նշանակել F/K: Ընդ որում, սա շփոթություն չի առաջացնում ըստ իդեալի ֆակտոր-օղակի հասկացության հետ կապված, քանի որ դաշտերն ունեն միայն տրիվիալ իդեալներ, եւ ըստ դրանց ֆակտոր-դաշտեր չեն

քննարկվում: Եթե $f(x) \in K[x]$, ապա $f(x)$-ը կարող է որեւէ x_i արմատ ունենալ F-ում, բայց ոչ K-ում: Դրա օրինակները շատ են 4.2 պարագրաֆում (մասնավորապես, տես 4.2.15 օրինակը եւ 4.2.16 խնդիրը): Ավելին, անհրաժեշտության դեպքում K-ին հավելյալ տարրեր ավելացնելով՝ կարելի է այնքան մեծացնել F-ը, որ այն պարունակի $f(x)$-ի բոլոր արմատները: Ըստ Բեզուի թեորեմի՝ $f(x)$-ը F-ի վրա կվերլուծվի գծային արտադրիչների արտադրյալի՝

$$f(x) = a_0(x - x_1) \cdots (x - x_n), \tag{7.26}$$

որտեղ $n = \deg f(x)$, իսկ a_0-ն $f(x)$-ի ավագ գործակիցն է: Տարրեր ավելացնելու պրոցեսը կարող ենք իրականացնել 4.2.31 թեորեմի օգնությամբ. K-ի $\overline{K}$ հանրահաշվական փակույթը պարունակում է $f(x)$-ի բոլոր արմատները: Սակայն $F = \overline{K}$ դաշտը խրթին կառուցվածք է, եւ մենք կարող ենք որպես ավելի փոքր դաշտ վերցնել $\overline{K}$-ի այն F ենթադաշտը, որը ծնվում է K-ով եւ բոլոր $x_1, \dots, x_n \in \overline{K}$ տարրերով: Այդ դեպքում F-ը կլինի K-ն եւ $f(x)$-ի բոլոր արմատները պարունակող *մինիմալ* եւ իզոմորֆիզմի ճշտությամբ *միակ* դաշտը (այս փաստի ոչ բարդ ապացույցը կարելի է գտնել ցիտված գրականության մեջ): F-ի միակությունը թույլ է տալիս ձեւակերպել հետեւյալ սահմանումը.

7.6.2 Սահմանում. Ենթադրենք K դաշտի վրա տրված է $f(x) = a_0x^n + \cdots + a_n \in K[x]$ դրական աստիճանի բազմանդամը: Այդ դեպքում K-ի F ընդլայնումը կոչվում է K դաշտի վրա $f(x)$ բազմանդամի *վերլուծության դաշտ*, եթե գոյություն ունեն այնպիսի $x_1, \dots, x_n \in F$ տարրեր, որոնց համար $f(x) = a_0(x - x_1) \cdots (x - x_n)$ եւ $F = K(x_1, \dots, x_n)$:

F-ը միակն է, եւ այն ստացվում է՝ K-ին $x_1, \dots, x_n$ տարրերի ավելացման միջոցով (տես 4.2.12 դիտողությանը հաջորդող կառուցումները): Հասկանալի է, որ իր վերլուծության դաշտի վրա յուրաքանչյուր բազմանդամի ֆակտորիզացիան ունի (7.26) տեսքը:

7.6.3 Վարժություններ. Օգտվելով 4.2.15 օրինակից՝ գտնել $\mathbb{Q}$-ի վրա $f(x) = x^2 - 2$ եւ $f(x) = x - 3$ բազմանդամների վերլուծության դաշտերը: Օգտվելով 4.2.16 խնդրից, գտնել $\mathbb{R}$-ի վրա $f(x) = x^2 + 1$ բազմանդամի վերլուծության դաշտը:

Վերհիշենք, որ կամայական F դաշտի համար նրա հոմոմորֆիզմը կամ իզոմորֆիզմը հասկացվում են 2.3.1 եւ 2.3.4 սահմանումների իմաստով, այսինքն՝ որպես օղակային հոմոմորֆիզմ եւ իզոմորֆիզմ (դաշտը նաեւ օղակ է): Հեշտ է ստուգել, որ F-ի բոլոր իզոմորֆիզմների բազմությունը խումբ է արտապատկերումների

սովորական արտադրյալի գործողության նկատմամբ: Այն նշանակվում է $\mathrm{Aut}(F)$ եւ կոչվում F-ի *ավտոմորֆիզմների խումբ:*

7.6.4 Վարժություն. Ստուգել, որ $\mathrm{Aut}(F)$-ը իսկապես խումբ է արտապատկերումների արտադրյալի գործողության նկատմամբ: Ո՞ր իզոմորֆիզմը կլինի այդ խմբի միավորը:

Ենթադրենք տրված է դաշտերի կամայական F/K ընդլայնումը, եւ $\psi \in \mathrm{Aut}(F)$ իզոմորֆիզմն այնպիսին է, որ այն «անշարժ է թողնում» K ենթադաշտը այն իմաստով, որ ցանկացած $a \in K$ տարրի համար $\psi(a) = a$: Նման իզոմորֆիզմների բազմությունը նշանակենք $\mathrm{Aut}(F/K)$: Հեշտ է ստուգել, որ այն նույնպես խումբ է եւ հանդիսանում է $\mathrm{Aut}(F)$-ի ենթախումբը.

7.6.5 Վարժություններ. Ստուգել, որ $\mathrm{Aut}(F/K)$-ը խումբ է արտապատկերումների արտադրյալի գործողության նկատմամբ, եւ որ այն $\mathrm{Aut}(F)$-ի ենթախումբ է:

7.6.6 Սահմանում. Ենթադրենք տրված է դաշտերի F/K ընդլայնումը: Այդ դեպքում $\mathrm{Aut}(F/K)$ խումբը կոչվում է K դաշտի վրա F *ընդլայնման Գալուայի խումբ:* Այն նշանակվում է $\mathrm{Gal}(F/K)$:

Մասնավորապես, եթե F դաշտը տրված $f(x)$ բազմանդամի վերլուծության դաշտն է, ունենք հետեւյալ կարեւոր դեպքը.

7.6.7 Սահմանում. Ենթադրենք տրված է $f(x) \in K[x]$ բազմանդամը եւ K-ի վրա $f(x)$-ի վերլուծության F դաշտը: Այդ դեպքում $\mathrm{Gal}(F/K) = \mathrm{Aut}(F/K)$ խումբը կոչվում է K դաշտի վրա $f(x)$ *բազմանդամի Գալուայի խումբ:*

Բազմանդամի Գալուայի խմբի համար նոր նշանակում չենք մտցնում, այն դարձյալ նշանակվում է $\mathrm{Gal}(F/K)$՝ ի նկատի ունենալով, որ F-ը տվյալ դեպքում կամայական չէ, այլ $f(x)$-ի վերլուծության դաշտն է:

$f(x)$ բազմանդամի Գալուայի խումբը մի կարեւոր եւ գեղեցիկ նկարագրություն ունի $f(x)$-ի արմատների բազմության վրա տրված տեղադրությունների լեզվով: Դրա ներկայացման համար օգտվենք դաշտի վրա հանրահաշվական հավասարումներից: K-ի վրա տրված *հանրահաշվական հավասարում* է կոչվում

$$A(x_1, \dots, x_n) = B(x_1, \dots, x_n) \tag{7.27}$$

տեսքի հավասարումը, որտեղ $A(x_1, \dots, x_n)$-ը եւ $B(x_1, \dots, x_n)$-ը $K[x_1, \dots, x_n]$ օղակի n-փոփոխականների կամայական բազմանդամներ են (այն դեպքերում, երբ հայտնի

է, թե որ հանրահաշվական հավասարման մասին է խոսքը. համառոտության համար երբեմն բաց կթողնենք «հանրահաշվական» բառը): Ենթադրենք (7.27) հավասարումն այնպիսին է, որ $f(x)$-ի արմատները բավարարում են դրան (գրառման միօրինակության համար մենք նույն տառերով ենք նշանակել այդ արմատները եւ A, B բազմանդամների փոփոխականները):

Դիտարկենք $f(x)$-ի $x_1, \dots, x_n$ արմատների բազմության վրա տրված

$$\theta = \begin{pmatrix} x_1 & \cdots & x_n \\ x_{i_1} & \cdots & x_{i_n} \end{pmatrix}$$

տեղադրությունը (բիյեկտիվ արտապատկերումը): θ տեղադրությունը ազդում է (7.27) հավասարման փոփոխականների վրա՝ վերածելով այն մի նոր հավասարման.

(7.28) $$A\big(x_{i_1}, \dots, x_{i_n}\big) = B\big(x_{i_1}, \dots, x_{i_n}\big):$$

Ընդ որում, $x_1, \dots, x_n$ փոփոխականների կոնկրետ արժեքների համար θ-ի ազդեցությունից հետո դրանք կարող են կրկին բավարարել (7.27) հավասարմանը կամ այլեւս չբավարարել դրան:

7.6.8 Օրինակ. Եթե $K = \mathbb{Q}$ եւ $f(x) = x^2 - 4x + 1 \in \mathbb{Q}[x]$, ապա $f(x)$-ի արմատներն են $x_1 = 2 + \sqrt{3}$ եւ $x_2 = 2 - \sqrt{3}$: Եթե վերցնենք $A(x_1, x_2) = x_1 \cdot x_2 \in \mathbb{Q}[x_1, x_2]$ եւ $B(x_1, x_2) = 1 \in \mathbb{Q}[x_1, x_2]$, ապա նշված արմատները բավարարում են $x_1 \cdot x_2 = 1$ հանրահաշվական հավասարմանը՝ $\big(2 + \sqrt{3}\big)\big(2 - \sqrt{3}\big) = 4 - 3 = 1$: Եթե այդ հավասարման վրա ազդենք $\theta = \begin{pmatrix} x_1 & x_2 \\ x_2 & x_1 \end{pmatrix}$ տեղադրությամբ, կստանանք $x_2 \cdot x_1 = 1$ հավասարումը, որին այդ արմատները նույնպես բավարարում են՝ $\big(2 - \sqrt{3}\big)\big(2 + \sqrt{3}\big) = 1$:

7.6.9 Վարժություն. Ցույց տալ, որ այդ նույն օրինաչափությունը նախորդ օրինակի բազմանդամի արմատների եւ θ տեղադրության համար կատարվում է նաեւ $x_1 + x_2 = 4$ հավասարման դեպքում:

Ավելի ուշ մենք կբերենք հակառակ բնույթի օրինակ եւս (տես 7.6.26 օրինակը): Մեզ համար ավելի կարեւոր են այն տեղադրությունները, որոնց ազդեցությունից հետո $f(x)$ բազմանդամի արմատները շարունակում են բավարարել (7.27) հավասարմանը, այսինքն՝ (7.28)-ին: Տրված $f(x) \in K[x]$ բազմանդամի համար այդպիսի θ տեղադրությունների այլ օրինակներ կարելի է ստանալ նրա $\mathrm{Gal}(F/K)$ Գալուայի խմբի միջոցով: Ընդ որում, այդ տեղադրություններն այնպիսին են, որ չեն փոփոխում K դաշտի տարրերը: Իսկապես, ենթադրենք $f(x)$-ի $x_1, \dots, x_n$ արմատները բավարարում են (7.27) հավասարմանը: A եւ B բազմանդամները ներկայացնենք (6.17) տեսքով.

$$A = \sum_{(k_1,\dots,k_n)\in S} a_{k_1,\dots,k_n} x_1^{k_1}\cdots x_n^{k_n} = \sum_{(k_1,\dots,k_n)\in S} b_{k_1,\dots,k_n} x_1^{k_1}\cdots x_n^{k_n} = B: \tag{7.29}$$

Քանի որ $a_{k_1,\dots,k_n}$ եւ $b_{k_1,\dots,k_n}$ գործակիցները K-ից են, ապա F դաշտի $\psi \in \mathrm{Gal}(F/K)$ իզոմորֆիզմը անփոփոխ է թողնում դրանց՝ $\psi(a_{k_1,\dots,k_n}) = a_{k_1,\dots,k_n}$ եւ $\psi(b_{k_1,\dots,k_n}) = b_{k_1,\dots,k_n}$ կամայական $(k_1,\dots,k_n) \in S$ համար: Իսկ $x_1^{k_1}\cdots x_n^{k_n}$ տեսքի արտադրյալի վրա ψ-ն, ըստ հոմոմորֆության պայմանի, ազդում է

$$\psi(x_1^{k_1}\cdots x_n^{k_n}) = \psi(x_1)^{k_1}\cdots\psi(x_n)^{k_n}$$

կանոնով: Քանի որ ψ-ն բիյեկտիվ է, տարբեր x_i եւ x_j արժեքների համար տարբեր են նաեւ դրանց $\psi(x_i)$ եւ $\psi(x_j)$ պատկերները: Այսինքն՝ ψ-ն սահմանում է $x_1,\dots,x_n$ արմատների բազմության *տեղադրություն*: Նշանակելով $x_{i_1} = \psi(x_1),\dots,x_{i_n} = \psi(x_n)$ ստանում ենք

$$\theta_\psi = \begin{pmatrix} x_1 & \cdots & x_n \\ x_{i_1} & \cdots & x_{i_n} \end{pmatrix}$$

տեղադրությունը, որը բավարարում է ցանկալի պայմանին՝ եթե $f(x)$-ի արմատները բավարարում են որեւէ (7.27) հանրահաշվական հավասարման, ապա նրանք բավարարում են դրան նաեւ θ_ψ տեղադրությամբ դիրքափոխվելուց հետո:

Մյուս կողմից, կամայական $\psi \in \mathrm{Gal}(F/K)$ իզոմորֆիզմ միակ կերպով վերականգնվում է իրեն համապատասխանող θ_ψ տեղադրության միջոցով, քանի որ ψ-ն որոշվում է F-ի վրա իր արժեքներով, իսկ F վերլուծության դաշտը ծնվում է K-ով եւ $x_1,\dots,x_n \in F$ տարրերով: Մեզ արդեն հայտնի է, որ ψ-ն անփոփոխ է թողնում K-ն, իսկ $x_1,\dots,x_n$ տարրերի վրա ազդում է θ_ψ տեղադրության նման: Գալուայի դաշտի այս մեկնաբանությունն է, որ մենք օգտագործելու ենք ստորեւ:

7.6.10 Օրինակ. Հաշվենք 7.6.8 օրինակի $f(x) = x^2 - 4x + 1 \in \mathbb{Q}[x]$ բազմանդամի $\mathrm{Gal}(F/\mathbb{Q})$ Գալուայի խումբը: Քանի որ նրա x_1, x_2 արմատներից ոչ մեկը $\mathbb{Q}$-ին չի պատկանում, F ընդլայնումը խիստ մեծ է $\mathbb{Q}$-ից: F-ը ստացվում է $\mathbb{Q}$-ին $2+\sqrt{3}$ եւ $2-\sqrt{3}$ տարրերը միացնելով: Հեշտ է ստուգել, որ $F = \mathbb{Q}(2+\sqrt{3},\ 2-\sqrt{3}) = \mathbb{Q}(\sqrt{3})$: Քանի որ $\sqrt{3}$-ի քառակուսին $\mathbb{Q}$-ից է, F-ը $\mathbb{Q}$-ի երկրորդ աստիճանի ընդլայնում է՝ $[\mathbb{Q}(\sqrt{3}), \mathbb{Q}] = 2$: Այս ընդլայնումը նման է 4.2.11, 4.2.19 եւ 4.2.21 օրինակների ընդլայնմանը: $\mathrm{Gal}(\mathbb{Q}(\sqrt{3})/\mathbb{Q})$ Գալուայի խումբը բաղկացած է երկու տարրից, քանի որ ունենք միայն երկու արմատներ: Իզոմորֆիզմներից առաջինը նույնական արտապատկերումն է, որը որոշվում է միավոր տեղադրությամբ՝ $(1) = \begin{pmatrix} x_1 & x_2 \\ x_1 & x_2 \end{pmatrix}$: Իսկ երկրորդը որոշվում է $\theta = \begin{pmatrix} x_1 & x_2 \\ x_2 & x_1 \end{pmatrix}$ տեղադրությամբ հետեւյալ բանաձեւով $\psi(u +$

$v\sqrt{3}) = u - v\sqrt{3}$, որտեղ $u, v \in \mathbb{Q}$: Երկու տարրերից բաղկացած ցանկացած խումբ իզոմորֆ է $\mathbb{Z}_2$ ցիկլիկ խմբին: Ուրեմն՝ $\mathrm{Gal}\big(\mathbb{Q}(\sqrt{3})/\mathbb{Q}\big) \cong \mathbb{Z}_2$:

Անցնենք ռադիկալներով լուծում ունենալու հասկացության խիստ սահմանմանը: Եթե $f(x) = a_0x^n + \cdots + a_n \in K[x]$ բազմանդամի գործակիցներից ելնելով հնարավոր արտահայտություններ (բանաձեւեր) կազմենք միայն գումարման, հանման, բազմապատկման ու բաժանման գործողություններով (առանց արմատ հանելու գործողության), ապա, այդ արտահայտությունների արդյունքը K դաշտին միացնելով, մենք երբեք դուրս չենք գա K-ի սահմաններից: Բայց արմատ հանելու գործողությունը (ի նկատի ունենք ոչ թե միայն քառակուսի արմատ, այլ ցանկացած աստիճանի արմատ) կարող է էապես մեծացնել K դաշտը (ինչպես $\mathbb{R}$-ին $\sqrt{-1}$ արմատն ավելացնելով՝ ստանում ենք $\mathbb{C}$ դաշտը):

7.6.11 Սահմանում. K դաշտի F ընդլայնումը կոչվում է *ռադիկալ ընդլայնում*, եթե գոյություն ունեն այնպիսի $x_1, \dots, x_n \in F$ տարրեր եւ $k_1, \dots, k_n \in \mathbb{Z}$ թվեր, որոնց համար՝

1) $F = K(x_1, \dots, x_n)$ եւ

2) $x_1^{k_1} \in K$, $x_i^{k_i} \in K(x_1, \dots, x_{i-1})$ երբ $i = 2, \dots, n$:

Այսպիսով, ռադիկալ ընդլայնումը ստացվում է սկզբնական K դաշտին մի քանի անգամ այնպիսի տարրեր միացնելով, որոնցից ամեն մեկի որեւէ աստիճանը պատկանում է նախորդ քայլում ստացված դաշտին:

7.6.12 Սահմանում. $f(x) \in K[x]$ բազմանդամի համար կասենք, որ նրա արմատները հնարավոր է հաշվել ռադիկալներով (կամ որ $f(x) = 0$ հավասարումը կարելի է լուծել ռադիկալներով), եթե գոյություն ունի այնպիսի մի F/K ռադիկալ ընդլայնում, որ F-ը պարունակում է $f(x)$-ի բոլոր արմատները:

Հաջորդ քայլի համար անհրաժեշտ է լուծելի խմբի հասկացության սահմանումը, որը մենք կբերենք մի քանի ոչ բարդ օրինակների հետ միասին: Այդ օրինակները ոչ միայն լուծելի խմբի հասկացությունն ավելի պարզ բացատրելու համար են, այլեւ հետագայում օգտագործվելու են ռադիկալներով հաշվելի եւ ոչ հաշվելի արմատներով բազմանդամների կառուցման համար:

Ենթադրենք G-ն կամայական խումբ է: Նրա $a, b \in G$ տարրերի *կոմուտատոր* է կոչվում եւ $[a, b]$ տեսքով է նշանակվում $[a, b] = a^{-1}b^{-1}a\,b$ արտադրյալը: G խմբի

կոմուտատոր (կամ *կոմուտանտ*) է կոչվում նրա բոլոր տարրերի կոմուտատորներով ծնված ենթախումբը, որը նշանակվում է G' կամ $[G,G]$՝

$$[G,G]=G'=\langle [a,b]\mid a,b\in G\rangle:$$

7.6.13 Վարժություն. Ցույց տալ, որ եթե G խումբն աբելյան է, ապա $G'=1$, այսինքն՝ կոմուտատորը բաղկացած է միայն տրիվիալ տարրից:

7.6.14 Վարժություն. Ստուգել, որ կամայական G խմբի G' կոմուտատորը *նորմալ* ենթախումբ է, այսինքն, ցանկացած $a\in G'$ եւ $g\in G$ տարրերի համար $g^{-1}a\,g\in G'$:

Տրված n բնական թվի համար S_n-ով նշանակվում է n-րդ աստիճանի բոլոր տեղադրությունների խումբը (*լրիվ սիմետրիկ խումբը*), իսկ A_n-ով նշանակվում է n-րդ աստիճանի բոլոր զույգ տեղադրությունների խումբը (*նշանափոխ խումբը*):

7.6.15 Վարժություն. Ստուգել, որ $S_2'=A_3'=1$: Ցույց տալ, որ A_4' խումբը բաղկացած է չորս տարրերից:

7.6.16 Խնդիր. Օգտվելով վերը ցիտված գրականությունից՝ ցույց տալ, որ $A_5'=A_5$ եւ $S_5'=A_5$: *Յուցում*՝ տես նաեւ 7.6.23 օրինակին նախորդող քննարկումը:

G խմբի G' ենթախմբի համար կարելի է, իր հերթին, դիտարկել դրա $(G')'=[[G,G],[G,G]]$ կոմուտատորը, որը կոչվում է G խմբի *երկրորդ կոմուտատոր* եւ նշանակվում է G'': Նույն կերպ կարելի է սահմանել նաեւ խմբի երրորդ, չորրորդ, k-րդ կոմուտատորները: Նշանակումների հարմարության համար խմբի k-րդ կոմուտատորը նշանակվում է $G^{(k)}$ սիմվոլով (այլ ոչ թե k հատ շտրիխներով): Մասնավորապես, $G^{(2)}=G''$, $G^{(1)}=G'$ եւ $G^{(0)}=G$: Հասկանալի է, որ $G^{(k+1)}\le G^{(k)}$, այսինքն՝ երբ k-ն աճում է, $G^{(k)}$ կոմուտատորները կամ փոքրանում են, կամ անփոփոխ են մնում: Որոշ խմբերի համար դրանք ինչ-որ քայլում հավասարվում են G-ի 1 միավոր ենթախմբին: Իսկ որոշ խմբերի համար՝ $G^{(k)}$-ն միշտ մեծ է 1-ից ցանկացած k-ի համար:

7.6.17 Սահմանում. G-ն կոչվում է *լուծելի խումբ*, եթե որեւէ k-ի համար $G^{(k)}=1$: Այդ դեպքում G-ի *լուծելիության երկարություն* (կամ *լուծելիության աստիճան*) է կոչվում այն մինիմալ k-ն, որի համար տեղի ունի $G^{(k)}=1$:

7.6.18 Խնդիր. Օգտվելով վերը ցիտված գրականությունից եւ նախորդ խնդիրներից՝ ցույց տալ, որ $S_3'=A_3\ne 1$, բայց $S_3''=A_3'=1$: Նաեւ $S_4''=A_4'\ne 1$, բայց $S_4^{(3)}=A_4''=1$: Իսկ, մյուս կողմից, $S_5'=A_5\ne 1$ եւ կամայական բնական k-ի համար $S_5^{(k)}=A_5\ne 1$: Այսինքն՝ $k=5$ թիվն այն առաջին աստիճանն է, որի համար S_5 խումբը լուծելի չէ: S_4-ի լուծելիության երկարությունը 3 է, S_3-ի լուծելիության երկա-

րությունը՝ 2, իսկ S_2-ի լուծելիության երկարությունը՝ 1: Պարզ է նաեւ, որ S_1 եւ A_1 խմբերը տրիվիալ են, ուստի $S_1^{(0)} = A_1^{(0)} = 1$, այսինքն՝ S_1 եւ A_1 խմբերի լուծելիության երկարությունը 0 է:

Գալուայի տեսության կարեւորագույն արդյունքներից է հետեւյալ թեորեմը, որը բերում ենք առանց ապացույցի.

7.6.19 Թեորեմ. *Եթե $f(x) \in K[x]$ բազմանդամը տրված է զրոյական բնութագրիչի K դաշտի վրա, ապա նրա արմատները հնարավոր է հաշվել ռադիկալներով այն եւ միայն այն դեպքում, երբ նրա* $\mathrm{Gal}(F/K)$ *Գալուայի խումբը լուծելի է:*

Այս թեորեմը բացատրում է նաեւ «լուծելի խումբ» տերմինի ծագումը. $f(x) = 0$ հավասարումը կարելի է *լուծել* ռադիկալներով այն եւ միայն այն դեպքում, երբ $\mathrm{Gal}(F/K)$ Գալուայի խումբը *լուծելի* է:

7.6.20 Օրինակ. Ինչպես տեսանք 7.6.10 օրինակում, $x^2 - 4x + 1$ քառակուսի եռանդամի Գալուայի խումբն է $\mathrm{Gal}\left(\mathbb{Q}\left(\sqrt{3}\right)/\mathbb{Q}\right) \cong \mathbb{Z}_2$: Այն լուծելի է՝ $\mathbb{Z}_2' = 0$ (միավոր ենթախումբը նշանակում ենք ոչ թե 1, այլ 0, քանի որ խումբն ադիտիվ է): Ըստ 7.6.19 թեորեմի՝ նրա արմատները կարելի է հաշվել ռադիկալներով: Դա, իրոք, այսպես է՝ ըստ դիսկրիմինանտի հաշվման հանրահայտ բանաձեւի:

7.6.21 Օրինակ. Ավելի հետաքրքիր եւ շատ ավելի ոչ տրիվիալ եզրակացություն կարելի է անել 7.6.18 խնդրի օգնությամբ: Ենթադրենք $f(x) \in \mathbb{Q}[x]$ բազմանդամի աստիճանը n է, որտեղ $n \in \{1, 2, 3, 4\}$: Այդ դեպքում $f(x)$-ն ունի n հատ արմատ (հաշվի առնելով պատիկ արմատների կրկնությունները): Այսինքն՝ $f(x)$ բազմանդամի $\mathrm{Gal}(F/\mathbb{Q})$ Գալուայի խումբը S_1, S_2, S_3 կամ S_4 խմբերից որեւէ մեկի ենթախումբն է: Ինչպես տեսանք, այդ խմբերը լուծելի են: Շատ հեշտ է ստուգել, որ լուծելի խմբի կամայական ենթախումբ նույնպես լուծելի է: Ուրեմն՝ $\mathrm{Gal}(F/\mathbb{Q})$-ը լուծելի է, եւ առաջին, երկրորդ, երրորդ կամ չորրորդ աստիճանի յուրաքանչյուր բազմանդամի համար նրա արմատները կարելի է գտնել ռադիկալներով: Այսինքն՝ գոյություն ունեն գումարման, հանման, բազմապատկման, բաժանման եւ ցանկացած աստիճանի արմատ հանման գործողությունների միջոցով կառուցված ինչ-որ բանաձեւեր, որոնց արդյունքում ստացվում են $f(x)$-ի արմատները: Դրանք այս պարագրաֆի ամենասկզբում հիշատակված բանաձեւերն են:

Այժմ անցնենք հակառակ բնույթի օրինակին՝ ցույց տանք *հինգերորդ* աստիճանի այնպիսի բազմանդամ, որի արմատները հնարավոր չէ հաշվել ռադիկալներով: Մեզ պետք է գալու հետեւյալ թեորեմը, որ նույնպես բերում ենք առանց ապացույցի.

7.6.22 Թեորեմ. *Ենթադրենք K-ն կամայական դաշտ է, իսկ $f(x) \in K[x]$ դրական աստիճանի բազմանդամի պարզ արտադրիչներից ոչ մեկը չունի պատիկ արմատներ $f(x)$-ի վերլուծության F դաշտում: Այդ դեպքում* $\mathrm{Gal}(F/K)$ *Գալուայի խմբի կարգը հավասար է F/K ընդլայնման աստիճանին* $|\mathrm{Gal}(F/K)| = [F/K]$:

Թեորեմի ձեւակերպման մեջ կարող է շփոթեցնող թվալ «պարզ արտադրիչներից ոչ մեկը չունի պատիկ արմատներ» արտահայտությունը: Պարզ արտադրիչը, ըստ Բեզուի թեորեմի, իհարկե, չունի պատիկ արմատներ (եւ ընդհանրապես արմատներ, եթե այն գծային չէ) K դաշտի վրա: Բայց F ընդլայնման մեջ $f(x)$-ը կարող է պատիկ արմատներ ունենալ:

Դիտարկենք $f(x) = x^5 - 4x + 2$ բազմանդամը: Ըստ 7.5.4 Էյզենշտեյնի հայտանիշի՝ այն պարզ բազմանդամ է, քանի որ $p = 2$ պարզ թվի համար $p|4$ եւ $p \nmid 2$: Դժվար չէ ստուգել, որ $f(x)$-ն ունի ճիշտ երեք հատ իրական եւ երկու հատ կոմպլեքս արմատներ: Իսկապես, հաշվենք բազմանդամի արժեքները $\{-2, -1, 0, 1, 2\}$ կետերում՝

$$f(-2) = -22, \quad f(-1) = 5, \quad f(0) = 2, \quad f(1) = -1, \quad f(2) = 26:$$

Ըստ Կոշու առաջին թեորեմի՝ $f(x)$-ն առնվազն երեք տարբեր իրական x_1, x_2, x_3 արմատներ ունի $(-2, 2)$ բաց ինտերվալում, քանի որ այն դրա վրա երեք անգամ փոխում է իր արժեքը: Մյուս կողմից, $f'(x) = 5x^4 - 4$ ածանցյալը զրոյական արժեք է ընդունում իրական առանցքի միայն $\left(\frac{4}{5}\right)^{\frac{1}{4}} = 0.4096$ եւ $-\left(\frac{4}{5}\right)^{\frac{1}{4}} = -0.4096$ կետերում: Այսինքն՝ $(-2, 2)$ ինտերվալից դուրս $f(x)$ ֆունկցիան մոնոտոն աճող է եւ այլ արմատներ չունի: Ըստ հանրահաշվի հիմնական թեորեմի՝ $f(x)$-ը ունի $\deg f(x) = 5$ հատ արմատ, որոնցից երեքը $(-2, 2)$ ինտերվալում են, իսկ մնացած երկուսը իրական առանցքից դուրս ընկած կոմպլեքս արմատներ են: Նշանակենք վերջին երկուսը՝ $z_1, z_2 \in \mathbb{C}\backslash\mathbb{R}$: Հասկանալի է, որ դրանք իրար համալուծ են, քանի որ $f(\overline{z}_1) = \overline{f(z_1)} = \overline{0} = 0$ (կոմպլեքս թվերի գումարի կամ արտադրյալի համալուծը հավասար է գումարելիների կամ արտադրիչների համալուծների գումարին կամ արտադրյալին): Ուրեմն՝ $\overline{z}_1 = z_2$, եւ, որպես $f(x)$ բազմանդամի $\{x_1, x_2, x_3, z_1, z_2\}$ արմատները դիրքափոխող եւ միաժամանակ $\mathbb{Q}$-ն անփոփոխ թողնող տեղադրություն, կարող ենք վերցնել

$$\theta = \begin{pmatrix} x_1 & x_2 & x_3 & z_1 & z_2 \\ x_1 & x_2 & x_3 & z_2 & z_1 \end{pmatrix}$$

տեղադրությունը, որը ծնվում է $\mathbb{C}$ հարթության արտացոլումից:

Հաջորդ տեղադրությունը որոնենք $f(x)$ բազմանդամի $\mathrm{Gal}(F/\mathbb{Q})$ Գալուայի խմբի կարգի վերաբերյալ գնահատականով: Քանի որ $f(x)$-ը հինգերորդ աստիճա-

նի պարզ բազմանդամ է եւ չունի կրկնվող արմատներ, ապա, ըստ 7.6.22 թեորեմի, $|\mathrm{Gal}(F/\mathbb{Q})| = [F/\mathbb{Q}]$:

$\mathbb{Q}$ դաշտին $f(x)$ պարզ բազմանդամի արմատներից որեւէ մեկը միացնելով՝ կստանանք $\mathbb{Q}(x_i)$ կամ $\mathbb{Q}(z_i)$ տեսքի մի ընդլայնում, որի աստիճանն է $5 = \deg f(x)$: Հետեւաբար, F վերլուծության դաշտի $[F/\mathbb{Q}]$ աստիճանը նույնպես բաժանվում է 5-ի վրա: Ուրեմն՝ 5-ի վրա բաժանվում է նաեւ $\mathrm{Gal}(F/\mathbb{Q})$ Գալուայի խմբի կարգը: Բայց ըստ Սիլովի առաջին թեորեմի՝ եթե խմբի կարգը բաժանվում է որեւէ p պարզ թվի վրա, ապա այն պարունակում է p-րդ կարգի որեւէ տարր: Ուրեմն՝ $\mathrm{Gal}(F/\mathbb{Q})$ խմբում կա 5-րդ կարգի որեւէ δ տարր:

Ըստ սիմետրիկ խմբի ծնիչների մասին հայտնի փաստի՝ յուրաքանչյուր S_n սիմետրիկ խումբ ծնվում է ցանկացած n երկարության ցիկլով եւ տրանսպոզիցիայով (2 երկարության ցիկլով): Որպես այդպիսի ցիկլեր վերցնելով δ-ն եւ θ-ն՝ ստանում ենք

$$S_5 = \langle \delta, \theta \rangle \subseteq \mathrm{Gal}(F/\mathbb{Q}) \subseteq S_5:$$

Ուրեմն՝ $\mathbb{Q}$-ի վրա $f(x)$ բազմանդամի Գալուայի խումբն է $\mathrm{Gal}(F/\mathbb{Q}) = S_5$:

Մնում է ստուգել, որ S_5 խումբը լուծելի չէ (տես նաեւ 7.6.18 խնդիրը): Կամայական $n \geq 3$ թվի համար $S_n' = [S_n, S_n] = A_n$, որտեղ A_n-ը n-աստիճանի զույգ տեղադրությունների նշանափոխ խումբն է: Ըստ նշանափոխ խմբերի մասին Գալուայի թեորեմի՝ եթե $n \neq 4$, ապա A_n-ը պարզ խումբ է, այսինքն՝ նրա միակ նորմալ ենթախմբերն են ինքը եւ իր տրիվիալ ենթախումբը: Հասկանալի է, որ ոչ աբելյան պարզ խումբը համընկնում է իր կոմուտատորին, քանի որ կոմուտատորը նորմալ ենթախումբ է: Ուրեմն՝ $A_5' = A_5 \neq 1$ եւ $S_5'' = A_5' = A_5 \neq 1$: Նույն կերպ՝ S_5-ի կամայական k-րդ կոմուտատորի համար $S_5^{(k)} = A_5 \neq 1$, երբ $k > 1$: Ստանում ենք.

7.6.23 Օրինակ. $f(x) = x^5 - 4x + 2$ բազմանդամի $\mathrm{Gal}(F/\mathbb{Q})$ Գալուայի խումբը համընկնում է S_5 սիմետրիկ խմբին, քանի որ $\mathrm{Gal}(F/\mathbb{Q})$-ը պարունակում է թե 5 երկարության եւ թե 2 երկարության ցիկլեր, որոնք ծնում են S_5 խումբը: S_5-ը լուծելի խումբ չէ, քանի որ ցանկացած $k = 1, 2, \ldots$ համար ունենք $S_5^{(k)} = A_5 \neq 1$: Ուրեմն, ըստ 7.6.19 թեորեմի, $f(x)$-ի արմատները $\mathbb{Q}$-ի վրա հնարավոր չէ հաշվել ռադիկալներով: $f(x)$-ի լուծումը հնարավոր չէ դուրս բերել իր գործակիցներից՝ դրանց գումարման, հանման, բազմապատկման, բաժանման եւ ցանկացած աստիճանի արմատ հանման գործողությունների ոչ մի շղթայի միջոցով:

Նկատենք նաեւ, որ մենք իրականում ապացուցել ենք ավելին, քան միայն $x^5 - 4x + 2$ բազմանդամի վերաբերյալ այս օրինակը: Տեղի ունի.

7.6.24 Թեորեմ. *Ենթադրենք տրված է կամայական $f(x) \in \mathbb{Q}[x]$ պարզ բազմանդամ: Եթե այն ունի ճիշտ երեք հատ իրական արմատ, ապա $f(x)$-ի արմատները $\mathbb{Q}$-ի վրա հնարավոր չէ հաշվել ռադիկալներով:*

Հասկանալի է, որ թեորեմում հիշատակված իրական արմատները ռացիոնալ չեն, քանի որ $f(x)$-ը պարզ է $\mathbb{Q}$-ի վրա: 7.6.24 թեորեմի օգնությամբ հեշտ է կառուցել նաեւ այլ օրինակներ.

7.6.25 Օրինակ. $h(x) = x(x^2 - 4)(x^2 + 4) = x^5 - 16x$ բազմանդամի երեք իրական արմատներն են $0, 2, -2$: Հասկանալի է, որ $h(x)$-ի գրաֆիկը երեք անգամ հատում է Ox առանցքը, ընդ որում, ունի մեկ լոկալ մաքսիմումի եւ մեկ լոկալ մինիմումի կետեր, որոնք $(-2, 2)$ ինտերվալում են: Քանի որ $h(-1) = 15$ եւ $h(1) = -15$, ապա այդ մաքսիմումի եւ մինիմումի կետերում ընդունած արժեքները բավական մեծ են, եւ բազմանդամը կշարունակի երեք արմատներ ունենալ, եթե դրան գումարվի 2: Մյուս կողմից, $f(x) = h(x) + 2 = x^5 - 16x + 2$ բազմանդամը պարզ է $\mathbb{Q}[x]$-ում՝ ըստ Էյզենշտեյնի հայտանիշի: Ուստի, ըստ 7.6.24 թեորեմի, $f(x)$-ի արմատները հնարավոր չէ հաշվել ռադիկալներով:

Այժմ կարող ենք բերել այն օրինակը, որը խոստացանք 7.6.9 վարժությունից հետո:

7.6.26 Օրինակ. Կրկին դիտարկենք $f(x) = x^5 - 4x + 2$ բազմանդամը: Արդեն գիտենք, որ այն ունի զույգ առ զույգ տարբեր $\{x_1, x_2, x_3, z_1, z_2\}$ արմատները, որոնցից իրական են միայն առաջին երեք հատը, ընդ որում, z_1, z_2 արմատները իրար համալուծ են: r-ով նշանակենք դրանց իրական մասը՝ $r = \Re(z_1) = \Re(z_2)$: Վերցնենք 5 փոփոխականների

$$A(x_1, x_2, x_3, z_1, z_2) = 0x_1 + 0x_2 + 0x_3 + z_1 + z_2 = z_1 + z_2 \in \mathbb{Q}[x_1, x_2, x_3, z_1, z_2],$$
$$B(x_1, x_2, x_3, z_1, z_2) = 2r \in \mathbb{Q}[x_1, x_2, x_3, z_1, z_2]$$

բազմանդամները ու կազմենք $z_1 + z_2 = 2r$ հանրահաշվական հավասարումը: Պարզ է, որ $\{x_1, x_2, x_3, z_1, z_2\}$ արմատները բավարարում են դրան: Մյուս կողմից, եթե այդ հավասարման վրա կիրառենք

$$\theta = \begin{pmatrix} x_1 & x_2 & x_3 & z_1 & z_2 \\ z_1 & x_2 & x_3 & x_1 & z_2 \end{pmatrix}$$

տեղադրությունը, ապա կստանանք $x_1 + z_2 = 2r$ հավասարումը, որին $f(x)$-ի արմատները չեն բավարարում:

Այն դեպքերի համար, երբ հինգերորդ աստիճանի բազմանդամի արմատները հնարավոր է հաշվել ռադիկալներով (այսինքն՝ նրա Գալուայի խումբը լուծելի է), ստացված են բազմանդամի արմատների հաշվման բացահայտ եղանակներ եւ բանաձեւեր: Նման նկարագրությունը տվել է Յանգը (Young, 1888), իսկ համեմատաբար վերջերս Լազարը ներկայացրել է այդ արմատների հաշվման բացահայտ բանաձեւերը, որոնք մոտ երեք էջ երկարություն ունեն (Lazard, 2004):

Այժմ անցնենք $\mathbb{C}$ եւ $\mathbb{R}$ դաշտերի վրա բազմանդամի ֆակտորիզացիայի ուսումնասիրմանը՝ ի նկատի ունենալով, որ դա նույնպես ռադիկալներով անլուծելի խնդիր է: Պարզվում է, որ բազմանդամների արմատների հաշվման հարցը ֆակտորիզացիայի խնդրում հանդիպող միակ լուրջ արգելքն է, եւ բազմանդամի արմատների առկայության դեպքում ֆակտորիզացիան շատ հեշտ է կառուցել, քանի որ $\mathbb{R}[x]$ եւ $\mathbb{C}[x]$ օղակներում պարզ բազմանդամները անհամեմատ հեշտ են նկարագրվում, քան $\mathbb{Z}[x]$ եւ $\mathbb{Q}[x]$ օղակներում:

Համաձայն $\mathbb{C}$ դաշտի հանրահաշվական փակության (կամ ըստ հանրահաշվի հիմնական թեորեմի)՝ ցանկացած $f(x) \in \mathbb{C}[x]$ բազմանդամ ունի (7.26) տեսքի վերլուծություն մեկ սկալյարի եւ $n = \deg f(x)$ հատ գծային արտադրիչների արտադրյալի (ներառյալ $n = 0$ դեպքը, երբ գծային արտադրիչները բացակայում են): Մասնավորապես, այս դեպքում $\mathrm{Gal}(\mathbb{C}/\mathbb{C}) = 1$, քանի որ $\mathbb{C}$-ի վրա ցանկացած բազմանդամի վերլուծության դաշտը կրկին $\mathbb{C}$-ն է: Ակնհայտ է, որ $x - x_i$ արտադրիչները պարզ են: Իսկ a_0-ն հակադարձելի տարր է $\mathbb{C}$-ում: Այսինքն՝ 6.1.1 սահմանման տերմիններով $\varepsilon = a_0$, իսկ $f(x)$-ի միակ ֆակտորիզացիայի արտադրիչներն են $p_i(x) = x - x_i$.

7.6.27 Թեորեմ. *Կամայական $f(x) \in \mathbb{C}[x]$ բազմանդամ ունի միակ*

$$f(x) = a_0(x - x_1) \cdots (x - x_n) \tag{7.30}$$

ֆակտորիզացիան, որտեղ a_0 հակադարձելի տարրը $f(x)$-ի ավագ գործակիցն է, իսկ $x - x_i$ պարզ արտադրիչները ստացվում են ըստ $f(x)$-ի բոլոր $x_1, \dots, x_n$ արմատների, $i = 1, \dots, n$:

Հասկանալի է, որ «միակ» բառն այստեղ օգտագործված է այն իմաստով, որը տրված է ֆակտորիզացիայի 6.1.1 սահմանման մեջ. $f(x)$-ի ֆակտորիզացիաները *հավասար* են, եթե բաղկացած են հավասար քանակությամբ պարզ արտադրիչներից, եւ համապատասխան արտադրիչներն իրար ասոցացված են:

Այժմ ենթադրենք տրված է կամայական $f(x) = a_0x^n + \cdots + a_n \in \mathbb{R}[x]$ բազմանդամ, որի իրական արմատներն են $x_1, \dots, x_k \in \mathbb{R}$: Այստեղ $0 \le k \le n = \deg f(x)$, այ-

սինքն՝ հնարավոր է նաեւ այն դեպքը, երբ $f(x)$-ի արմատներից ոչ մեկն իրական չէ: Եթե z-ը $f(x)$-ի որեւէ կեղծ, ոչ իրական արմատ է, ապա, ինչպես տեսանք քիչ առաջ,

$$f(\overline{z}) = a_0\overline{z}^n + \cdots + a_n = \overline{a}_0\overline{z}^n + \cdots + \overline{a}_n = \overline{a_0x^n + \cdots + a_n} = \overline{0} = 0,$$

այսինքն՝ z-ի $\overline{z}$ համալուծը նույնպես արմատ է (եւ տարբեր է z-ից, քանի որ նրա կեղծ մասը զրոյական չէ): Եթե յուրաքանչյուր z, $\overline{z}$ զույգից ընտրենք մեկ արմատ, եւ $f(x)$-ը դիտարկենք $\mathbb{C}$ դաշտի վրա, ապա $f(x)$-ի n հատ բոլոր կոմպլեքս արմատները կարելի է խմբավորել այսպես.

$$x_1, \dots, x_k; z_1, \overline{z}_1, \dots, z_s, \overline{z}_s, \quad \text{որտեղ } k + 2s = n:$$

$\mathbb{C}$-ի վրա $f(x)$ բազմանդամը կունենա հետեւյալ ֆակտորիզացիան.

$$f(x) = a_0(x - x_1)\cdots(x - x_k)\cdot(x - z_1)(x - \overline{z}_1)\cdots(x - z_s)(x - \overline{z}_s):$$

Եթե յուրաքանչյուր z_m ներկայացնենք $z_m = \alpha_m + i\beta_m$ տեսքով, $m = 1, \dots, s$, եւ նշանակենք $q_m(x) = (x - z_m)(x - \overline{z}_m)$, ապա

$$q_m(x) = x^2 - xz_m - x\overline{z}_m + z_m\overline{z}_m = x^2 - 2\alpha_m x + (\alpha_m^2 + \beta_m^2) \in \mathbb{R}[x]:$$

$q_m(x)$-ը երկրորդ աստիճանի նորմավորված բազմանդամ է, որ $\mathbb{C}[x]$ օղակում ունի $(x - z_m)(x - \overline{z}_m)$ վերլուծությունը եւ որը պարզ է $\mathbb{R}[x]$ օղակում: Իսկապես, եթե $q_m(x)$-ը $\mathbb{R}[x]$ օղակում ունենար որեւէ $h(x)$ արտադրիչ, ապա այն արտադրիչ կլիներ նաեւ $\mathbb{C}[x]$ օղակում: Շնորհիվ $\mathbb{C}[x]$-ի ֆակտորիալության՝ այն պետք է ասոցացված լիներ $x - z_m$ կամ $x - \overline{z}_m$ բազմանդամներից որեւէ մեկին: Բայց դրանցից ոչ մեկը հնարավոր չէ բազմապատկել մի այնպիսի կոմպլեքս թվով, որ ստացվի իրական գործակիցներով բազմանդամ: Ստանում ենք 7.6.27 թեորեմի անալոգը իրական դաշտի համար.

7.6.28 Թեորեմ. *Կամայական $f(x) \in \mathbb{R}[x]$ բազմանդամ ունի միակ*

$$f(x) = a_0(x - x_1)\cdots(x - x_k)\cdot(x^2 + b_1x + c_1)\cdots(x^2 + b_sx + c_s) \tag{7.31}$$

ֆակտորիզացիան, որտեղ a_0 հակադարձելի տարրը $f(x)$-ի ավագ գործակիցն է, $x - x_i$ պարզ արտադրիչները ստացվում են ըստ $f(x)$-ի բոլոր $x_1, \dots, x_k$ իրական արմատների, $i = 1, \dots, k$, իսկ $x^2 + b_mx + c_m$ պարզ արտադրիչները ստացվում են ըստ $f(x)$-ի բոլոր $z_1, \overline{z}_1, \dots, z_s, \overline{z}_s$ կեղծ, ոչ իրական արմատների, $m = 1, \dots, s$ ($b_m = -2\alpha_m$, $c_m = \alpha_m^2 + \beta_m^2$, որտեղ $z_m = \alpha_m + i\beta_m$):

Այստեղ եւս «միակ» բառն օգտագործված է ֆակտորիզացիայի 6.1.1 սահմանման մեջ նշված իմաստով:

7.6.29 Դիտողություն. $\mathbb{C}[x]$ օղակում պարզ են միայն գծային բազմանդամները, իսկ $\mathbb{R}[x]$-ում պարզ են գծային բազմանդամները եւ այն քառակուսի բազմանդամները, որոնց դիսկրիմինանտը բացասական է (այսինքն՝ նրանք, որոնք ունեն ճիշտ երկու կեղծ, ոչ իրական արմատ): Հետաքրքիր է սա համեմատել $\mathbb{Z}[x]$-ի, $\mathbb{Q}[x]$-ի եւ K վերջավոր դաշտի վրա տրված $K[x]$ օղակի պարզ բազմանդամների հետ: Այդ օղակներում գոյություն ունեն կամայական աստիճանի պարզ բազմանդամներ (տես 7.5.6 եւ 7.5.8 հետեւանքները): $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $K[x]$ օղակների համար կան կամայական բազմանդամի ֆակտորիզացիայի եւ արմատների հաշվման ալգորիթմներ: Իսկ $\mathbb{R}[x]$, $\mathbb{C}[x]$ օղակներում նման հանրահաշվական ալգորիթմներ գոյություն չունեն: Սակայն կոնկրետ բազմանդամի արմատների առկայության դեպքում դրա ֆակտորիզացիան դառնում է հեշտությամբ լուծվող խնդիր:

7.6.30 Դիտողություն. Հետաքրքիր է նաեւ համեմատել բազմանդամի ֆակտորիզացիայի խնդիրը բազմանդամների ամենամեծ ընդհանուր բաժանարարի հաշվման խնդրի հետ: Չնայած երկու խնդիրներն էլ հանգում են բազմանդամի բաժանարարների հաշվմանը, բայց ամենամեծ ընդհանուր բաժանարարի հաշվումը $\mathbb{R}[x]$, $\mathbb{C}[x]$ օղակներում ավելի բարդ խնդիր չէ, քան $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $K[x]$ օղակներում: Ավելին, անգամ մի քանի փոփոխականների բազանդամների համար ամենամեծ ընդհանուր բաժանարարի հաշվումը չի բարդանում, երբ $\mathbb{Q}$ դաշտից անցնում ենք $\mathbb{R}$ կամ $\mathbb{C}$ դաշտերին (տես 6.4.3 եւ 6.4.13 ալգորիթմները):

$\mathbb{R}$ կամ $\mathbb{C}$ դաշտերի վրա տրված $f(x)$ բազմանդամի արմատների մոտավոր հաշվման տարբեր մեթոդներ մշակվել են մաթեմատիկական անալիզի, թվային մեթոդների, հաշվողական համակարգերի միջոցով.

7.6.31 Օրինակ. Նյուտոնի մեթոդը որպես մոտարկման «գործիք» օգտագործում է $f(x)$ բազմանդամի գրաֆիկի շոշափողը: Կամայական x_0 թվի համար $f'(x_0)$ ածանցյալը $(x_0, f(x_0))$ կետում $f(x)$-ի գրաֆիկին տարված շոշափողի եւ Ox առանցքի կազմած անկյան սինուսն է: Այդ շոշափողը հատվում է Ox առանցքին $(x_1, 0)$ կետում, որտեղ

$$x_1 = x_0 - f(x_0)/f'(x_0):$$

Քանի որ $f(x)$-ի վարքագիծը x_0 կետի շրջակայքում «նման» է շոշափողի վարքագծին, հնարավոր է, որ x_1 կետում $f(x)$-ի արժեքն ավելի է մոտ 0-ին, քան x_0 կետում: Քայլերը ինդուկցիայով կրկնելով՝ հաշվենք

$$x_k = x_{k-1} - f(x_{k-1})/f'(x_{k-1})$$

արժեքը: Հաճախ այս x_k հաջորդականությունը զուգամիտում է $f(x)$-ի որեւէ արմատի, եւ դա թույլ է տալիս գտնել $f(x)$-ի մոտավոր ֆակտորիզացիան:

Բազմանդամների արմատների մոտավոր հաշվման այլ մեթոդներ են Լագերի մեթոդը (տես, օրինակ (Forman, 1970), (Ralston & Rabinowitz, 1978)) եւ Ջենկինս-Տրաուբի ալգորիթմը (Jenkins & Traub, 1970):

8 Գրյոբների բազաներ

8.1 Իդեալի ծնիչ բազմությունները եւ Գրյոբների բազաները

Գրյոբների բազաները ժամանակակից հանրահաշվի ամենաարդյունավետ ալգորիթմական կառուցվածքներից են: Նրանք լայնորեն ընդհանրացնում են մի քանի հանրահայտ ալգորիթմներ, այդ թվում՝ բազմանդամների ամենամեծ ընդհանուր բաժանարարի հաշվման Էվկլիդեսի ալգորիթմը եւ գծային հավասարումների համակարգը փոփոխականների արտաքսման մեթոդով լուծելու ալգորիթմը: Նշված երկու ալգորիթմներն իրարից արտաքուստ շատ տարբեր են, ուստի սկսենք դրանց համեմատությունից եւ աշխատենք նկատել այնպիսի ընդհանրություններ, որոնք հանգեցրել են Գրյոբների բազայի հասկացությանը:

Դիտարկենք K դաշտի վրա տրված $K[x]$ օղակի $f(x), g(x)$ բազմանդամների $d(x) = \big(f(x), g(x)\big)$ ամենամեծ ընդհանուր բաժանարարը Էվկլիդեսի ալգորիթմով հաշվելու քայլերը (տես 2.5 պարագրաֆը): Քանի որ $f(x), g(x)$ բազմանդամները երկուսն էլ բաժանվում են $d(x)$-ի վրա, նրանք պատկանում են $d(x)$-ով ծնված $I = \langle d(x)\rangle = d(x)K[x]$ գլխավոր իդեալին, որը բաղկացած է $K[x]$ օղակի բոլոր այն բազմանդամներից, որոնք բաժանվում են $d(x)$-ի վրա: Մյուս կողմից, 2.5 պարագրաֆի (2.7) աղյուսակի առաջին տողից հեշտ է տեսնել, որ $f(x), g(x)$ բազմանդամներով ծնված $\langle f(x), g(x)\rangle$ իդեալը պարունակում է $f(x)$-ը $g(x)$-ի վրա բաժանելիս ստացվող $r(x)$ մնացորդը. եթե $f(x) = q(x)g(x) + r(x)$, ապա $r(x) = f(x) - q(x)g(x) \in \langle f(x), g(x)\rangle$: Նույն կերպ՝ (2.7) աղյուսակի մնացած տողերից կստանանք, որ $\langle f(x), g(x)\rangle$-ին են պատկանում նաեւ մեր ստացած բոլոր $r(x)$, $r_1(x)$, $r_2(x), \dots, r_{n-1}(x)$, $r_n(x)$ մնացորդները, որտեղ $r_n(x) = d(x)$: Ստանում ենք

$$\langle f(x), g(x)\rangle = I = \langle d(x)\rangle = d(x)K[x] \tag{8.1}$$

հավասարությունը, որը թույլ է տալիս երկու բազմանդամների ամենամեծ ընդհանուր բաժանարարի հաշվումը մեկնաբանել հետեւյալ կերպ: Տրված է $f(x), g(x) \in K[x]$ բազմանդամներով ծնված $I = \langle f(x), g(x)\rangle$ իդեալը, եւ մենք այդ իդեալի համար գտնում ենք «ավելի լավ» $\{d(x)\}$ ծնիչ բազմություն: $\{d(x)\}$-ն ավելի գերադասելի է,

քան $\{f(x), g(x)\}$ ծնիչ բազմությունը, քանի որ այն միայն մեկ տարրից է բաղկացած, եւ I իդեալի ցանկացած $h(x)$ բազմանդամի համար կարելի է միանգամից ասել՝ արդյո՞ք այն պատկանում է I-ին, թե ոչ (դա կախված է այն բանից, թե արդյոք $h(x)$-ը $d(x)$-ի վրա բաժանելիս ստացվող մնացորդը զրոյական է):

Այժմ քննարկենք K դաշտի վրա տրված գծային հավասարումների

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = b_1 \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = b_m \end{cases} \tag{8.2}$$

համակարգի լուծումը փոփոխականների արտաքսման մեթոդով: Ենթադրենք այս համակարգի տողերի տարրական ձեւափոխությունների միջոցով, այսինքն՝ տողերը տեղափոխելով, տողերը ինչ-որ ոչ զրոյական սկալյարներով բազմապատկելով եւ տողերին այլ տողեր գումարելով (նախապես դրանք ինչ-որ սկալյարներով բազմապատկելով)՝ կարողացել ենք համակարգը բերել այնպիսի տեսքի, որ ձեւափոխված տողերը գնալով ավելի ու ավելի քիչ փոփոխականներ են պարունակում: Պարզության համար ենթադրենք, որ վերջին տողում մնացել է միայն մեկ փոփոխական, նախավերջին տողում մնացել են միայն երկու փոփոխականներ եւ այլն.

$$\begin{cases} c_{11}x_1 + c_{12}x_2 + \cdots\cdots\cdots\cdots + c_{1n}x_n = d_1 \\ \qquad\quad c_{22}x_2 + \cdots\cdots\cdots\cdots + c_{2n}x_n = d_2 \\ \qquad\qquad\qquad \cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \qquad\qquad\qquad\qquad c_{m-1\,n-1}x_{k-1} + c_{m-1\,n}x_n = d_{m-1} \\ \qquad\qquad\qquad\qquad\qquad\qquad c_{mn}x_n = d_m \end{cases} : \tag{8.3}$$

Այստեղից համակարգի լուծումը գտնվում է հանրահայտ եղանակով. վերջին տողից հաշվվում է x_n փոփոխականի արժեքը, այն տեղադրվում է նախավերջին տողի մեջ եւ հաշվվում է x_{n-1} փոփոխականի արժեքը: Այսպես, շարժվելով ներքեւից վերեւ, մենք կստանանք բոլոր $x_1, \ldots, x_n$ փոփոխականների արժեքները: 8.8 պարագրաֆում մենք այս պրոցեսը կնկարագրենք ավելի ընդհանուր դեպքի համար, սակայն այստեղ մեզ պետք է միայն ընդհանուր սկզբունքը բացատրող այս օրինակը:

Այժմ նկատենք, որ (8.2) համակարգի տողերը կարելի է մեկնաբանել K դաշտի վրա տրված n փոփոխականների $K[x_1, \ldots, x_n]$ օղակի գծային բազմանդամների լեզվով: Եթե սահմանենք $f_i(x_1, \ldots, x_n) = a_{i1}x_1 + \cdots + a_{in}x_n - b_i$ (որտեղ $i = 1, \ldots, m$), ապա (8.2) համակարգը համարժեք է

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ \cdots\cdots\cdots\cdots \\ f_m(x_1, \ldots, x_n) = 0 \end{cases} \tag{8.4}$$

համակարգին: Նույն կերպ, եթե $g_i(x_1, \dots, x_n)$-ով նշանակենք (8.3) համակարգի i-րդ տողից ստացվող $g_i(x_1, \dots, x_n) = c_{ii}x_i + \cdots\cdots\cdots\cdots + c_{in}x_n - d_i$ բազմանդամը, ապա (8.3) համակարգն էլ համարժեք կլինի

$$\begin{cases} g_1(x_1, \dots, x_n) = 0 \\ \cdots\cdots\cdots\cdots \\ g_m(x_1, \dots, x_n) = 0 \end{cases} \tag{8.5}$$

համակարգին: Դիտարկենք $K[x_1, \dots, x_n]$ օղակի $I = \langle f_1, \dots, f_m \rangle$ իդեալը: Հասկանալի է, որ վերը նշված երեք տիպի ձեւափոխությունները՝ տողերի տեղափոխությունները, տողերը ինչ-որ ոչ զրոյական սկալյարներով բազմապատկելը, տողերին այլ տողեր գումարելը (նախապես դրանք ինչ-որ սկալյարներով բազմապատկելով) տալիս են միայն այնպիսի բազմանդամներ, որոնք կրկին I իդեալից են: Ուստի նաեւ $g_i \in I$ ցանկացած $i = 1, \dots, m$ համար: Մյուս կողմից, բոլոր երեք տիպերի ձեւափոխությունները հակադարձելի են, այսինքն՝ նման ձեւափոխություններով $g_1, \dots, g_m$ բազմանդամներից կարելի է ստանալ $f_1, \dots, f_m$ բազմանդամները: Մենք ստանում ենք հետեւյալ հավասարությունը՝

$$\langle f_1, \dots, f_m \rangle = I = \langle g_1, \dots, g_m \rangle, \tag{8.6}$$

որը շատ նման է (8.1)-ին եւ որը թույլ է տալիս գծային հավասարումների լուծումը մեկնաբանել հետեւյալ կերպ: Տրված է $f_1, \dots, f_m \in K[x_1, \dots, x_n]$ բազմանդամներով ծնված $I = \langle f_1, \dots, f_m \rangle$ իդեալը, եւ մենք այդ իդեալի համար գտնում ենք «ավելի լավ» $\{g_1, \dots, g_m\}$ ծնիչ բազմություն, որն ավելի գերադասելի է, քան $\{f_1, \dots, f_m\}$ ծնիչ բազմությունը, քանի որ նրանցում $x_1, \dots, x_n$ փոփոխականները դասավորված են այնպես, որ որքան մեծանում է i ինդեքսը, այնքան g_i բազմանդամում ավելի քիչ փոփոխականներ են մասնակցում: Սա հնարավորություն է տալիս, նախ, լուծել ավելի քիչ փոփոխականներով հավասարումները, ապա՝ ավելի շատ փոփոխականներով հավասարումներում տեղադրել արդեն գտնված փոփոխականների արժեքները:

8.1.1 Դիտողություն. Թե ամենամեծ ընդհանուր բաժանարարի հաշվման էվկլիդեսի ալգորիթմը եւ թե փոփոխականների արտաքսման մեթոդով գծային հավասարումների համակարգի լուծումը հանգում են $K[x_1, \dots, x_n]$ օղակում տրված I իդեալի համար «ավելի լավ» ծնիչների բազմության կառուցմանը: Այդ ալգորիթմները երկուսն էլ Գրյոբների բազաների կառուցման ալգորիթմների մասնավոր դեպքերն են: Մենք այս երկու մասնավոր ալգորիթմներին կրկին կանդրադառնանք 8.7 պարագրաֆի վերջում եւ 8.8 պարագրաֆում:

Նշված երկու ալգորիթմները ունեն նաեւ մի այլ կարեւոր ընդհանրություն: Էվկլիդեսի ալգորիթմի առաջին քայլում մենք $f(x)$ «գագաթի» օգնությամբ նվազեցնում

ենք $g(x)$ բազմանդամը՝ այն փոխարինում ենք զրոյական կամ ավելի ցածր աստիճանի $r(x)$ մնացորդով: Եթե անգամ $g(x)$-ի աստիճանը հավասար է $f(x)$-ի աստիճանին, ապա $r(x)$-ի աստիճանը հաստատ ավելի ցածր է: Հաջորդ քայլում $g(x)$ «գագաթի» օգնությամբ ստանում ենք $r_1(x)$ մնացորդը, որի աստիճանն ավելի ցածր է $r(x)$-ի աստիճանից: Այսպիսով, մենք ելնում ենք x-ի աստիճանների «բնական»

$$x^n > x^{n-1} > \cdots > x^2 > x > x^0 = 1$$

կարգավորվածությունից եւ աշխատում ենք նոր $r_i(x)$ բազմանդամները ստանալ ըստ ավելի ու ավելի ցածր կարգերի:

Նույն կերպ՝ գծային հավասարումների համակարգը լուծելիս մենք, նախ, $f_2, \dots, f_m$, բազմանդամները f_1 «գագաթի» օգնությամբ փոխարինում ենք այնպիսի բազմանդամներով, որոնք չեն պարունակում x_1 փոփոխականը: Վերջում ստանում ենք $g_1, \dots, g_m$ բազմանդամները, որոնք ավելի ու ավելի ցածր «գագաթներ» կարելի է համարել: Այդ ընթացքում մենք ելնում ենք $x_1, \dots, x_n$ փոփոխականների «բնական»

$$x_n > x_{n-1} > \cdots > x_2 > x_1$$

կարգավորվածությունից: Ինչպես կտեսնենք հաջորդ պարագրաֆում, սրանք մոնոմիալ կարգավորվածության մասնավոր դեպքեր են: Ընդհանուր դեպքում եւս մենք աշխատելու ենք $K[x_1, \dots, x_n]$ օղակի կամայական բազմանդամները դասավորել ըստ նման կարգավորվածության եւ իդեալների նոր ծնիչներ կառուցել՝ աստիճանաբար իջեցնելով դրանց աստիճանները:

Նշված հարցերը մենք ուսումնասիրելու ենք հետեւյալ ավելի ընդհանուր հանրահաշվական խնդիրների լուծման միջոցով: Ենթադրենք ֆիքսված K դաշտի վրա տրված է $R = K[x_1, \dots, x_n]$ բազմանդամային օղակը: Դիտարկենք.

Իդեալների հավասարության խնդիրը: Տրված են R օղակի I եւ J իդեալները: Պարզել՝ արդյո՞ք $I = J$:

Ենթահիդեալ լինելու խնդիրը: Տրված են R օղակի I եւ J իդեալները: Պարզել՝ արդյո՞ք $I \subseteq J$:

Իդեալին պատկանելության խնդիրը: Տրված է R օղակի I իդեալը եւ f տարրը: Պարզել՝ արդյո՞ք $f \in I$:

Այս խնդիրների լուծմանը մենք հասնելու ենք մոնոմիալ կարգավորվածության, մոնոմիալ իդեալների, Դիքսոնի թեորեմի, վերջավոր բազայի մասին Հիլբերտի թեորեմի եւ Բուխբերգերի ալգորիթմի միջոցով: Այդ ընթացքում մենք ստանալու ենք մեզ հայտնի հանրահաշվական փաստերի խորը ընդհանրացումներ: Դրանցից

մի քանիսը հայտնի մեթոդների հետաքրքիր ընդհանրացումներ են: Օրինակ՝ 8.4 պարագրաֆում մենք կծանոթանանք մի բազմանդամը մի քանի բազմանդամների հաջորդականության վրա բաժանելու մեթոդին, որն ընդհանրացնում է բազմանդամները անկյունով բաժանելու հանրահայտ մեթոդը: Հետաքրքիր է, որ, չնայած նման բաժանման ալգորիթմներ Էվկլիդեսից սկսած հայտնի են արդեն դարեր շարունակ, բազմանդամների հաջորդականության վրա բաժանելու մեթոդը հայտնաբերվել է միայն 1960-ական թվականներին:

Հարցի հիմնական տեսական կողմը հենվում է բազմանդամային օղակների նյոտերյանության վրա, ինչն ուսումնասիրվել է Դ. Հիլբերտի կողմից դեռ 1890-ականներին (Hilbert, 1890): Գրյոբների բազաների տեսությունը եւ դրանք հաշվելու Բուխբերգերի ալգորիթմը առաջարկվել են Բ. Բուխբերգերի կողմից եւ այդպես են կոչվել իր ուսուցչի՝ Վ. Գրյոբների պատվին (Buchberger, 1965): Գրեթե միաժամանակ նմանատիպ կառուցվածք է առաջարկվել նաեւ Հ. Հիրոնակայի կողմից (դրանք նա անվանել է ստանդարտ բազաներ) (Hironaka, 1964): Գրյոբների բազաների սկզբունքները ներկա են նաեւ Ն. Մ. Գյունտերի ավելի վաղ հոդվածներում (տես (Гюнтер, 1941), (Renschuch, et al., 2003)):

Այս գլխի նպատակն է տալ Գրյոբների բազաների տեսական ամբողջական հիմնավորումը՝ ներառյալ Դիքսոնի լեմման եւ Հիլբերտի թեորեմը: Դրանց վրա հենվելով՝ ստանում ենք Բուխբերգերի ալգորիթմը, Գրյոբների բազաները եւ արտաքսման իդեալները: Գրյոբների բազաների տեսության այլ զարգացումներ կարելի է գտնել հետեւյալ մենագրություններում եւ դասագրքերում. (Cox, et al., 2008), (Fröberg, 1997), (Becker, et al., 1993), (Adams & Loustaunau, 1994), (von zur Gathen & Gerhard, 2003), (Buchberger, 1985), (Buchberger, et al., 1983), (Латышев, 1988), (Панкратьев, 2007):

8.2 Մոնոմիալ կարգավորվածություն

Ենթադրենք K դաշտի վրա տրված է n փոփոխականների $K[x_1, \dots, x_n]$ օղակը, որը սահմանեցինք 6.2 պարագրաֆում: Պայմանավորվենք $x_1, \dots, x_n$ փոփոխականների *մոնոմիալ* անվանել

(8.7) $$x_1^{k_1} \cdots x_n^{k_n}$$

արտադրյալը, որտեղ $k_1, \dots, k_n$ աստիճանացույցերը կամայական ոչ բացասական ամբողջ թվեր են: Ըստ 6.2 պարագրաֆի սահմանումների՝ (8.7) մոնոմիալը կարելի է համարել 1 գործակցով միանդամ: Նշանակենք $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$: 6.2 պարագրաֆում պայմանավորվեցինք $\alpha = (k_1, \dots, k_n) \in \mathbb{N}_0^n$ կարգավորված n-յակն անվանել աստիճանային վեկտոր: (8.7) մոնոմիալը համառոտության համար նշանակենք x^α: Հաշվի ենք առնում այն, որ մոնոմիալը միարժեքորեն որոշվում է իր $\alpha = (k_1, \dots, k_n)$ աստիճանային վեկտորով, եւ երբ հարկ է, մենք միշտ կարող ենք x^α-ն բերել (8.7) տեսքի:

8.2.1 Օրինակ. Եթե $\alpha = (3, 2, 4)$, ապա $x^\alpha = x_1^3 x_2^2 x_3^4$: Իսկ եթե $\beta = (1, 0, 2)$, ապա $x^\beta = x_1^1 x_2^0 x_3^2 = x_1 x_3^2$, այսինքն՝ աստիճանային վեկտորի գրության մեջ կարող են մասնակցել եւ զրոյական կոորդինատներ, որոնց համապատասխան մոնոմիալում տվյալ փոփոխականը մասնակցում է զրոյական աստիճանով՝ այն «բացակայում է»:

Նախորդ պարագրաֆում բերված օրինակներում անբացահայտ տեսքով մասնակցում էր *մոնոմիալների կարգավորվածության* կամ *կարգի հարաբերության* հասկացությունը: Երբ գծային հավասարումների (8.2) համակարգում մենք, նախ, x_1 փոփոխականն արտաքսում էինք երկրորդ, երրորդ տողերից, հետո x_2 փոխականն արտաքսում էինք երրորդ, չորրորդ տողերից եւլն, մենք ի նկատի ունեինք, որ նախապես սահմանված է $x_1, \dots, x_n$ մոնոմիալների «դասավորություն», այսինքն՝ կարգի հարաբերություն

$$x_1 > x_2 > \cdots > x_{n-1} > x_n,$$

ըստ որի մեր արտաքսման գործողությունը գնում է մեծ մոնոմիալներից դեպի փոքր մոնոմիալները: Նույն կերպ, երբ մեկ x փոփոխականի բազմանդամների համար Էվկլիդեսի ալգորիթմում մնացորդների վրա հաջորդաբար բաժանելով գնում ենք ավելի բարձր աստիճաններից դեպի ավելի ցածր աստիճանները, անբացահայտորեն հենվում ենք x-ի աստիճաններից կազմված մոնոմիալների վրա կարգի հարաբերության վրա՝

(8.8) $$\cdots > x^d > x^{d-1} > \cdots > x > 1:$$

Նշված երկու դեպքերում էլ կարգի հարաբերությունը «ինքնաբերաբար հասկանալի» է: Սակայն մի քանի փոփոխականների դեպքում միշտ չէ, որ պարզ է, թե ո՞ր միանդամները կամ մոնոմիալները պետք է ավելի մեծ համարել: Ենթադրենք $K[x_1, x_2, x_3]$ օղակում տրված են

(8.9) $$x_1 x_2^2 x_3, \quad x_1 x_2 x_3, \quad x_3^2, \quad x_1 x_2^2, \quad x_1^3, \quad x_2^2 x_3$$

մոնոմիալները: Կարող է բնական թվալ, որ դրանցից առաջինը մեծ է երկրորդից, բայց ինչպե՞ս համեմատել մյուսները: Հենց այդ պատճառով է, որ մի քանի փոփո-

խականի բազմանդամների համար ընդհանուր դեպքում չկա ավագ անդամի հասկացություն, ինչպես նշեցինք նաեւ 6.2 պարագրաֆում: Քիչ հետո կտեսնենք, որ գոյություն ունեն նշված մոնոմիալները կարգավորելու տարբեր ձեւեր, ըստ որոնց կարելի է կառուցել իրարից տարբերվող ալգորիթմներ:

Վերհիշենք, որ, եթե $\alpha = (k_1, \dots, k_n) \in \mathbb{N}_0^n$, ապա ըստ 6.2 պարագրաֆում սահմանված $\deg_{x_i}$ եւ deg հասկացությունների՝

$$\deg_{x_i}\left(x_1^{k_1} \cdots x_n^{k_n}\right) = \deg_{x_i} x^\alpha = k_i \quad \text{եւ} \quad \deg\left(x_1^{k_1} \cdots x_n^{k_n}\right) = \deg x^\alpha = k_1 + \cdots + k_n:$$

Ավելացնենք աստիճանի հետ կապված երրորդ նշանակումը՝

$$\operatorname{multideg}\left(x_1^{k_1} \cdots x_n^{k_n}\right) = \operatorname{multideg} x^\alpha = \alpha = (k_1, \dots, k_n)$$

($\operatorname{multideg}\alpha$-ն ոչ թե թիվ է, այլ վեկտոր):

8.2.2 Վարժություններ. Հաշվել $\deg_{x_i}$ $(i = 1, 2, 3)$, deg եւ multideg աստիճանները (8.9) մոնոմիալներից յուրաքանչյուրի համար:

8.2.3 Վարժություն. Ցույց տալ, որ կամայական x^α եւ x^β մոնոմիալների համար $\operatorname{multideg} x^\alpha = \operatorname{multideg} x^\beta$ հավասարությունից բխում է $\deg_{x_i} x^\alpha = \deg_{x_i} x^\beta$ հավասարությունը ըստ ցանկացած x_i փոփոխականի: Իսկ դրանց համակարգից էլ բխում է $\deg x^\alpha = \deg x^\beta$ հավասարությունը: Ճի՞շտ են արդյոք հակառակ պնդումները:

Քանի որ n փոփոխականների x^α մոնոմիալը միարժեքորեն որոշվում է ըստ իր α աստիճանային վեկտորի, մոնոմիալների բազմության վրա կարգի հարաբերություն սահմանելը հանգում է աստիճանային վեկտորների $\mathbb{N}_0^n$ բազմության վրա կարգավորվածության սահմանման: Բազմության վրա տրված մասնակի կարգավորվածության, գծային կարգավորվածության ու լիովին կարգավորվածության սահմանումները մենք այստեղ չենք բացատրելու, քանի որ դրանք հայտնի են հանրահաշվի եւ դիսկրետ մաթեմատիկայի ներածական դասընթացներից (տես նաեւ (Beachy & Blair, 2006), (Cohn, 2003), (Cohn, 1965), (Кон, 1968), (Кострикин, 1977), (Кострикин, 2004), (Ленг, 1968), (van der Waerden, 1991)):

8.2.4 Սահմանում. $\mathbb{N}_0^n$ բազմության վրա տրված $<$ հարաբերությունը կոչվում է *մոնոմիալ կարգավորվածություն (մոնոմիալ կարգի հարաբերություն)*, եթե

M.1 $<$ հարաբերությունը *լիովին* կարգավորվածություն է, այսինքն՝

1) $<$ հարաբերությունը *գծային* կարգավորվածություն է. կամայական $\alpha, \beta \in \mathbb{N}_0^n$ աստիճանային վեկտորների համար տեղի ունի $\alpha < \beta$, $\alpha = \beta$ կամ $\beta < \alpha$ հարաբերություններից մեկը եւ միայն մեկը,

2) $\mathbb{N}_0^n$-ի ցանկացած ոչ դատարկ A ենթաբազմություն ունի *նվազագույն* տարր, այսինքն՝ գոյություն ունի այնպիսի մի $\mu \in A$ աստիճանային վեկտոր, որ ցանկացած այլ $\alpha \in A$ աստիճանային վեկտորի համար $\mu < \alpha$:

M.2 Եթե $\alpha < \beta$, ապա կամայական $\gamma \in \mathbb{N}_0^n$ աստիճանային վեկտորի համար $\alpha + \gamma < \beta + \gamma$ (որտեղ աստիճանային վեկտորների գումարը հասկացվում է կոորդինատ-առ-կոորդինատ գումարման իմաստով):

Համարենք նաեւ $x^\alpha < x^\beta$ այն եւ միայն այն դեպքում, երբ $\alpha < \beta$:

Սահմանման **M.1** կետը նշանակում է, որ մենք միշտ կարող ենք համեմատել ցանկացած երկու աստիճանային վեկտորներ (եւ մոնոմիալներ), ընդ որում, եթե որեւէ ալգորիթմի աշխատանքի ընթացքում մենք անընդհատ շարժվում ենք ավելի մեծ մոնոմիալներից դեպի ավելի փոքր մոնոմիալները, ապա այդ պրոցեսն ինչ-որ քայլում անպայման կանգ կառնի:

Սահմանման **M.2** կետը նշանակում է, որ $<$ հարաբերությունը համաձայնեցված է մոնոմիալների բազմապատկման գործողության հետ հետեւյալ իմաստով: Եթե $x^\alpha < x^\beta$, ապա կամայական x^γ մոնոմիալի համար տեղի ունի նաեւ $x^{\alpha+\gamma} = x^\alpha x^\gamma < x^\beta x^\gamma = x^{\beta+\gamma}$ (պարզ է, որ մոնոմիալների բազմապատկման ժամանակ աստիճանացույցերի կոորդինատները գումարվում են):

8.2.5 Վարժություն. Ցույց տալ, որ սահմանման **M.1** կետում հիշատակված նվազագույն տարրը միակն է:

Որոշ բանաձեւերում գրառման հարմարության համար կարելի է $\alpha < \beta$ կամ $x^\alpha < x^\beta$ հարաբերությունները գրել նաեւ $\beta > \alpha$ կամ $x^\alpha > x^\beta$ տեսքերով:

8.2.6 Օրինակ. Մոնոմիալ կարգավորվածության ամենապարզ օրինակը տրված է մեկ փոփոխականի մոնոմիալների վրա (8.8) բանաձեւերով: x^i տեսքի աստիճանները ($i = 0, 1, 2, \ldots$) լիովին կարգավորված են եւ, եթե $x^i < x^j$, ապա նաեւ $x^{i+k} < x^{j+k}$:

8.2.7 Վարժություն. Նախորդ օրինակի մոնոմիալների կարգավորվածությանը ինչպիսի՞ կարգավորվածություն է համապատասխանում $\mathbb{N}_0^1$ բազմության վրա:

Այժմ անցնենք մոնոմիալ կարգավորվածության երեք կարեւոր օրինակների սահմանումներին:

8.2.8 Սահմանում. $\mathbb{N}_0^n$ բազմության α, β աստիճանային վեկտորների համար սահմանենք $\alpha <_{lex} \beta$, եթե $\alpha - \beta$ վեկտորական տարբերության առաջին ոչ զրոյական

կոորդինատը բացասական է (աստիճանային վեկտորների տարբերությունը հասկացվում է կոորդինատ-առ-կոորդինատ հանման իմաստով): Համապատասխան մոնոմիալների համար սահմանենք $x^\alpha <_{lex} x^\beta$, երբ $\alpha <_{lex} \beta$: Այս կարգի հարաբերությունն անվանենք *լեքսիկոգրաֆիական* կարգավորվածություն (համառոտ՝ lex):

«Լեքսիկոգրաֆիական» տերմինի իմաստը հասկանալի է. վեկտորները համեմատում ենք այնպես, ինչպես բառարանի բառերը՝ երկու վեկտորներից մեծ է այն, որի առաջին կոորդինատն ավելի մեծ է: Իսկ եթե վեկտորներն ունեն միեւնույն առաջին կոորդինատը (այսինքն՝ դրանց տարբերությունը զրոյական է), ապա համեմատում ենք երկրորդ կոորդինատները եւլն: Այսպես դիտարկելով բոլոր կոորդինատները՝ մենք կամ կպարզենք, թե որ վեկտորն է ավելի մեծ, կամ էլ կստանանք, որ վեկտորներն հավասար են:

8.2.9 Օրինակ. $K[x_1, x_2, x_3]$ օղակի համար աստիճանային վեկտորների բազմությունը կլինի $\mathbb{N}_0^3$: Ուստի (8.9) մոնոմիալների աստիճանային վեկտորները կլինեն $(1,2,1),\ (1,1,1), (0,0,2),\ (1,2,0), (3,0,0), (0,2,1)$: Դասավորենք դրանք ըստ lex-ի նվազման՝

$$(3,0,0) >_{lex} (1,2,1) >_{lex} (1,2,0) >_{lex} (1,1,1) >_{lex} (0,2,1) >_{lex} (0,0,2):$$

Ըստ այդմ՝ $x_1^3 >_{lex} x_1x_2^2x_3 >_{lex} x_1x_2^2 >_{lex} x_1x_2x_3 >_{lex} x_2^2x_3 >_{lex} x_3^2$: Բառարանի տերմիններով սա կարելի է հասկանալ այսպես. եթե համապատասխանեցնենք x_1-ին «ա» տառը, x_2-ին «բ» տառը, x_3-ին «գ» տառը, ապա հայերեն բառարանում համապատասխան հինգ բառերը կդասավորվեն

ասա
աբբգ
աբբ
աբգ
բբգ
գգ

հաջորդականությամբ:

8.2.10 Խնդիր. Ցույց տալ, որ lex-ը մոնոմիալ կարգավորվածություն է: *Յուրքում՝* եթե $\alpha <_{lex} \beta$, ապա $\alpha + \gamma <_{lex} \beta + \gamma$, քանի որ, γ-ի կոորդինատները հերթով α-ի եւ β-ի կոորդինատներին ավելացնելով, մենք չենք փոխում տարբերության ամենաառաջին ոչ զրոյական կոորդինատի նշանը: Լիովին կարգավորվածությունը ցույց տալիս հաշվի առնել, որ n-ը վերջավոր է, իսկ $\mathbb{N}_0$-ի վրա սովորական $\leq$ հարաբերությունը լիովին կարգավորվածություն է:

Ըստ lex կարգավորվածության մոնոմիալները համեմատվում են ըստ իրենց «սկզբնական մասերի», ընդ որում, մոնոմիալի աստիճանը որոշիչ դեր չի կատարում: 8.2.9 օրինակում չորս փոփոխական պարունակող $x_1x_2^2x_3$ բառը (x_2-ը երկու անգամ է մասնակցում) ավելի փոքր էր, քան ավելի ցածր աստիճանի՝ երեք փոփոխական պարունակող x_1^3 բառը: Ավելին՝ $x_2^{10}x_3^{10} <_{lex} x_1$: Սակայն որոշ ալգորիթմների կառուցման համար անհրաժեշտ է ավելի մեծ դեր շնորհել մոնոմիալի աստիճանին: Դա արվում է աստիճանային լեքսիկոգրաֆիական կարգավորվածության միջոցով: Եթե $\alpha = (k_1, \dots, k_n)$, ապա պայմանավորվենք նշանակել $|\alpha| = k_1 + \cdots + k_n$: Այդ դեպքում $\deg x^\alpha = \deg x^{(k_1,\dots,k_n)} = |\alpha|$:

8.2.11 Սահմանում. $\mathbb{N}_0^n$ բազմության α, β աստիճանային վեկտորների համար սահմանենք $\alpha <_{grlex} \beta$, եթե $|\alpha| < |\beta|$ կամ $|\alpha| = |\beta|$ եւ $\alpha <_{lex} \beta$: Համապատասխան մոնոմիալների համար սահմանենք $x^\alpha <_{grlex} x^\beta$, երբ $\alpha <_{grlex} \beta$: Այս կարգի հարաբերությունն անվանենք *աստիճանային լեքսիկոգրաֆիական* կարգավորվածություն (համառոտ՝ $grlex$):

Ըստ $grlex$ կարգավորվածության՝ նախ, համեմատվում են մոնոմիալների աստիճանները, եւ ավելի մեծ են համարում ավելի բարձր աստիճան ունեցող մոնոմիալը: Եթե աստիճանները հավասար են, ապա մոնոմիալները համեմատվում են ըստ lex կարգավորվածության: Հասկանալի է, որ $x_2^{10}x_3^{10} >_{grlex} x_1$:

8.2.12 Վարժություն. (8.9) մոնոմիալները դասավորել ըստ $grlex$ կարգավորվածության՝ նվազման կարգով:

8.2.13 Խնդիր. Ցույց տալ, որ $grlex$-ը մոնոմիալ կարգավորվածություն է: *Ցուցում*՝ օգտվել 8.2.10 խնդրի ցուցումից:

Շատ խնդիրներում օգտակար է նաեւ կարգի հետեւյալ հարաբերությունը.

8.2.14 Սահմանում. $\mathbb{N}_0^n$ բազմության α, β աստիճանային վեկտորների համար սահմանենք $\alpha <_{grevlex} \beta$, եթե $|\alpha| < |\beta|$ կամ $|\alpha| = |\beta|$ եւ $\alpha >_{lex} \beta$: Համապատասխան մոնոմիալների համար սահմանենք $x^\alpha <_{grevlex} x^\beta$, երբ $\alpha <_{grevlex} \beta$: Այս կարգի հարաբերությունն անվանենք *աստիճանային հակադարձ լեքսիկոգրաֆիական* կարգավորվածություն (համառոտ՝ $grevlex$):

Ըստ $grevlex$ կարգավորվածության, ինչպես $grlex$-ի դեպքում, կրկին նախ համեմատվում են մոնոմիալների աստիճանները, եւ ավելի մեծ է համարվում ավելի բարձր աստիճան ունեցող մոնոմիալը: Բայց եթե աստիճանները հավասար են, ապա մոնոմիալները համեմատվում են ըստ lex-ի *հակադարձ* կարգավորվածութ-

յան. ավելի մեծ է համարվում այն մոնոմիալը, որն ավելի *փոքր* է ըստ lex-ի: $grevlex$-ն ավելի հարմար է այն դեպքերում, երբ մոնոմիալները համեմատելիս անհրաժեշտ է ուշադրությունը կենտրոնացնել դրանց վերջին մասերի վրա:

8.2.15 Վարժություն. (8.9) մոնոմիալները դասավորել ըստ $grevlex$-ի՝ նվազման կարգով:

8.2.16 Վարժություն. 8.2.9 օրինակում բերված բառերը դասավորել ըստ $grlex$-ի, ապա ըստ $grevlex$-ի՝ նվազման կարգով:

8.2.17 Խնդիր. Ցույց տալ, որ $grevlex$-ը մոնոմիալ կարգավորվածություն է: *Յուղում*՝ օգտվել 8.2.10 խնդրի ցուցումից:

Եթե $grlex$-ից բացի դիտարկվում է նրա հակադարձ $grevlex$ կարգավորվածությունը, ապա կարող է սպասելի թվալ նաեւ lex կարգավորվածության հակադարձի քննարկումը: Սակայն lex-ի հակադարձն ընդհանուր դեպքում մոնոմիալ կարգավորվածություն չէ:

8.2.18 Խնդիր. Ապացուցել, որ lex-ի հակադարձը լիովին կարգավորվածություն չէ: *Յուղում*՝ գտնել իրարից տարբեր աստիճանային վեկտորների նվազող անվերջ հաջորդականություն:

Գրառման համառոտության համար պայմանավորվենք այսուհետեւ կարգի հարաբերության անունը չգրել $>$ եւ $<$ սիմվոլների ինդեքսում: Օրինակ, եթե նախապես նշված է, որ գործ ունենք $grevlex$ կարգի հարաբերության հետ, կգրենք ոչ թե $<_{grevlex}$, այլ $<$:

Հասկանալի է, որ բերված կարգի հարաբերություններից յուրաքանչյուրը կախված է նաեւ այն բանից, թե ինչ հերթականությամբ ենք ի սկզբանե դասավորել փոփոխականները. եթե համարենք, որ $x_1 > x_2 > x_3 > \cdots$ կամ $x > y > z > \cdots$, ապա կստանանք lex, $grlex$ եւ $grevlex$ կարգավորվածությունների մի տարբերակ, իսկ եթե ընդունենք $x_1 < x_2 < x_3 < \cdots$ կամ $x < y < z < \cdots$, ապա համապատասխան կարգավորվածություններն էլ այլ կլինեն: Ամեն անգամ փոփոխականների դասավորության մասին չկրկնելու համար պայմանավորվենք, որ եթե տվյալ խնդրում այդ մասին հատուկ չի նշված, ապա $x_1 > x_2 > x_3 > \cdots$ եւ $x > y > z > \cdots$:

Բերված կարգի հարաբերությունները, ի թիվս այլ խնդիրների, օգտագործվում են տվյալ բազմանդամի միանդամները կարգավորելու համար: Ինչպես նշեցինք 6.2 պարագրաֆում, $\alpha = (k_1, \dots, k_n)$ աստիճանային վեկտորի համար (6.10) միանդամը կարելի է նշանակել $a_\alpha x^\alpha$, ինչը ավելի նման է x^α տեսքի մոնոմիալներին, որոնք

քննարկվում են այս պարագրաֆում: Ըստ այդմ՝ (6.11) ընդհանուր տեսքի բազմանդամը կարտագրվի

$$f = f(x_1, \dots, x_n) = \sum_{\alpha \in S} a_\alpha x^\alpha \tag{8.10}$$

տեսքով, որտեղ S-ը աստիճանային վեկտորների մի վերջավոր բազմություն է: $\mathbb{N}_0^n$ բազմության կամայական վերջավոր S ենթաբազմության համար սահմանվում է (8.10) տեսքի մի բազմանդամ եւ հակառակը: Եթե $a_\alpha x^\alpha$-ն f-ի միանդամն է, ապա x^α-ն կանվանենք f-ի մոնոմիալ: f-ի $a_\alpha x^\alpha$ միանդամները նվազման կարգով դասավորենք ըստ համապատասխան x^α մոնոմիալների կարգավորվածության:

8.2.19 Օրինակ. Ենթադրենք մեզ տրված է $f = 7y^5 - 3xy + 2x + y^2z^3 + 2yz + 3 \in K[x, y, z]$ բազմանդամը: Ըստ lex կարգավորվածության՝ $f = -3xy + 2x + 7y^5 + y^2z^3 + 2yz + 3$: Առաջին տեղում է $-3xy$ միանդամը, քանի որ $xy = x^1y^1z^0 > x^1y^0z^0 = x$: Վերջին տեղում է 3-ը, քանի որ $x^0y^0z^0$-ը մոնոմիալներից փոքրագույնն է: Ընդ որում, f բազմանդամն ունի երրորդ աստիճանի երկու հատ միանդամներ, որոնք այս գրության մեջ հանդիպում են երկրորդ եւ առաջին աստիճանի միանդամներից հետո, քանի որ վերջիններս սկսվում են x-ով: Եթե անցնենք $grlex$-ին, կունենանք արդեն $f = 7y^5 + y^2z^3 - 3xy + 2yz + 2x + 3$, ինչն ավելի «բնական» է թվում, քանի որ ավելի բարձր աստիճաններով միանդամները գրված են սկզբից: Իսկ ըստ $grevlex$-ի կստանանք $f = y^2z^3 + 7y^5 + 2yz - 3xy + 2x + 3$:

Այժմ արդեն կարող ենք ներմուծել մի քանի փոփոխականի բազմանդամի ավագ անդամի, ավագ գործակցի եւլն հասկացությունները, որոնք չկարողացանք սահմանել 6.2 պարագրաֆում: Այդ հասկացությունները սահմանվելու են ըստ նախապես ֆիքսված $<$ մոնոմիալ կարգավորվածության, որը կարող է լինել, մասնավորապես, $<_{lex}$, $<_{grlex}$, $<_{grevlex}$ կարգավորվածություններից որեւէ մեկը:

8.2.20 Սահմանում. Ենթադրենք սահմանված է K դաշտի վրա տրված $K[x_1, \dots, x_n]$ օղակի (եւ $\mathbb{N}_0^n$ բազմության) որեւէ $<$ մոնոմիալ կարգավորվածություն: Այդ դեպքում $f = \sum_{\alpha \in S} a_\alpha x^\alpha$ ոչ զրոյական բազմանդամի՝ ըստ տվյալ կարգավորվածության *ավագ մոնոմիալ* է կոչվում այն x^α մոնոմիալը, որը բազմանդամի մոնոմիալներից մեծագույնն է ըստ $<$ կարգավորվածության: Այն նշանակվում է $\mathrm{lm} f$: Եթե x^α-ն f բազմանդամի ավագ մոնոմիալն է, ապա համապատասխան $a_\alpha x^\alpha$ միանդամը կոչվում է *ավագ միանդամ* եւ նշանակվում $\mathrm{lt} f$: Իսկ համապատասխան a_α գործակիցը կոչվում է *ավագ գործակից* եւ նշանակվում $\mathrm{lc} f$: Եթե $\alpha = \mathrm{multideg}\, x^\alpha = (k_1, \dots, k_n)$, ապա նշանակվում է՝ $\mathrm{multideg}\, f = \alpha = (k_1, \dots, k_n)$:

Պարզ է, որ $\mathrm{lc} f \cdot \mathrm{lm} f = \mathrm{lt} f$ ցանկացած ոչ զրոյական f-ի համար: lm, lt եւ lc նշանակումները «leading monomial», «leading term» եւ «leading coefficient» տերմինների հապավումներն են: Երբեմն, երբ հարկ լինի շեշտել, թե ըստ որ կարգի հարաբերության են ներմուծվել այդ նշանակումները, կգրենք, օրինակ՝ $\mathrm{lc}_{\prec} f$ կամ $\mathrm{lt}_{grlex} f$ եւլն: 8.2.20 սահմանումը բերվեց ոչ զրոյական բազմանդամի համար: Երբեմն որոշ խնդիրներում ավելի միօրինակ ձեւակերպումներ ստանալու համար սահմանում են $\mathrm{lt} 0 = 0$:

8.2.21 Վարժություն. 8.2.19 օրինակի բազմանդամի համար նշել $\mathrm{lm} f$, $\mathrm{lt} f$, $\mathrm{lc} f$ եւ $\mathrm{multideg}\, f$ արժեքներն ըստ lex, $grlex$ եւ $grevlex$ կարգավորվածությունների:

8.2.22 Վարժություն. f-ով նշանակել (8.9) մոնոմիալների գումարը եւ դրա համար հաշվել $\mathrm{lm} f$, $\mathrm{lt} f$, $\mathrm{lc} f$ եւ $\mathrm{multideg}\, f$ արժեքներն ըստ lex, $grlex$ եւ $grevlex$ կարգավորվածությունների:

8.2.23 Վարժություն. Բերել f բազմանդամի օրինակ, որի միանդամի դասավորությունը միեւնույնն է lex, $grlex$ եւ $grevlex$ կարգավորվածությունների դեպքում: Մասնավորապես, $\mathrm{lm} f$, $\mathrm{lt} f$, $\mathrm{lc} f$ արժեքները անկախ կլինեն դրանց ընտրությունից:

Հետեւյալ երեք պնդումներն ապացուցելը հեշտ է, եւ մենք դրանք բերում ենք խնդրի տեսքով.

8.2.24 Խնդիր. Տրված են $K[x_1, \dots, x_n]$ օղակի կամայական f, g ոչ զրոյական բազմանդամները, իսկ $K[x_1, \dots, x_n]$-ի վրա սահմանված է որեւէ մոնոմիալ կարգավորվածություն: Այդ դեպքում.
1) Տեղի ունի $\mathrm{multideg}(f \cdot g) = \mathrm{multideg}\, f + \mathrm{multideg}\, g$ հավասարությունը: *Յուցում՝* ինչպե՞ս են իրար հետ բազմապատկվում f, g բազմանդամների ավագ անդամները:
2) Եթե $f \neq -g$, ապա $\mathrm{multideg}(f + g) \leq \max\{\mathrm{multideg}\, f, \mathrm{multideg}\, g\}$: *Յուցում՝* ինչի՞ հավասար կլինի $f + g$ գումարի ավագ անդամը: $f \neq -g$ պայմանը բերված է, որպեսզի խուսափենք $f + g = 0$ դեպքից:
3) Եթե $\mathrm{multideg}\, f \neq \mathrm{multideg}\, g$, ապա $\mathrm{multideg}(f + g) = \max\{\mathrm{multideg}\, f, \mathrm{multideg}\, g\}$:

8.3 Դիքսոնի լեմման մոնոմիալ իդեալներում

Գրյոբների բազաների տեսական հիմնավորման հիմնական փաստերից մեկը վերջավոր բազայի մասին Հիլբերտի թեորեմն է, որը դաշտի վրա մեկ փոփոխականի բազմանդամների գլխավոր իդեալների մասին 2.5.8 թեորեմի լայն ընդհանրացում է

(տես նաեւ 2.5.13 թեորեմը): Հիլբերտի թեորեմի ապացույցի հիմնական մասը հենվում է մոնոմիալ իդեալների եւ Դիքսոնի լեմմայի վրա:

8.3.1 Սահմանում. K դաշտի վրա տրված $K[x_1, \dots, x_n]$ բազմանդամային օղակի I իդեալը կոչվում է *մոնոմիալ իդեալ*, եթե այն ծնվում է մոնոմիալների որեւէ բազմությամբ. գոյություն ունի $\mathbb{N}_0^n$-ի այնպիսի մի A ենթաբազմություն, որ $I = \langle x^\alpha \mid \alpha \in A \rangle$:

$I = \langle x^\alpha \mid \alpha \in A \rangle$ հավասարությունը նշանակում է, որ կամայական $f \in I$ բազմանդամի համար գոյություն ունեն վերջավոր քանակությամբ $\alpha_1, \dots, \alpha_s$ աստիճանային վեկտորներ եւ $h_1, \dots, h_s \in K[x_1, \dots, x_n]$ բազմանդամներ, որ

$$f = \sum_{i=1}^{s} h_i x^{\alpha_i}, \tag{8.11}$$

Քանի որ յուրաքանչյուր x^{α_i} մոնոմիալի եւ ցանկացած $a_{\alpha_i} \in K$ սկալյարի համար $a_{\alpha_i} x^{\alpha_i}$ միանդամը $\langle x^\alpha \mid \alpha \in A \rangle$-ից է, իսկ (8.11) տեսքի գումարի յուրաքանչյուր գումարելու արտադրյալը բացելուց հետո դարձյալ x^{α_i}-ի վրա բաժանվող մոնոմիալներ են ստացվում, դեռ հստակ չէ, թե ինչով են մոնոմիալ իդեալները տարբերվում մնացած իդեալներից: Ուստի բերենք իդեալների օրինակներ, որոնք մոնոմիալ են կամ ոչ.

8.3.2 Օրինակ. $K[x_1, \dots, x_n]$ օղակում վերցնենք $I = x_1 K[x_1, \dots, x_n]$ գլխավոր իդեալը: Ակնհայտորեն այն բաղկացած է զրոյական բազմանդամից եւ այնպիսի բազմանդամներից, որոնց բոլոր միանդամներում ոչ զրոյական աստիճանով մասնակցում է x_1-ը: Հասկանալի է, որ I-ն x_1 մոնոմիալով ծնված իդեալն է: Այլ օրինակներ կարելի է ստանալ x_1-ը կամայական x^α մոնոմիալով փոխարինելու դեպքում:

Ավելի հետաքրքիր է ստանալ հակառակ բնույթի օրինակ.

8.3.3 Օրինակ. $K[x_1, x_2]$ օղակում վերցնենք $f = x_1 - x_2$ բազմանդամով ծնված $I = \langle f \rangle = (x_1 - x_2) K[x_1, x_2]$ գլխավոր իդեալը: Քանի որ I-ն պարունակում է f-ը, ապա մոնոմիալ իդեալ լինելու դեպքում I-ն պիտի պարունակեր նաեւ այնպիսի $x^{\alpha_1}, \dots, x^{\alpha_s}$ մոնոմիալներ, որ f-ը որոշ $h_1, \dots, h_s \in K[x_1, x_2]$ բազմանդամների համար արտահայտվեր (8.11) գումարի տեսքով՝ $x_1 - x_2 = h_1 x^{\alpha_1} + h_2 x^{\alpha_2}$: Սա կարող էր հնարավոր լինել միայն չորս դեպքերում.

1) երբ $h_1 = x_1,\ x^{\alpha_1} = 1, h_2 = -x_2,\ x^{\alpha_2} = 1,$
2) երբ $h_1 = 1,\ x^{\alpha_1} = x_1, h_2 = -x_2,\ x^{\alpha_2} = 1,$
3) երբ $h_1 = x_1,\ x^{\alpha_1} = 1, h_2 = -1,\ x^{\alpha_2} = x_2,$
4) երբ $h_1 = 1,\ x^{\alpha_1} = x_1, h_2 = -1,\ x^{\alpha_2} = x_2$:

Առաջին երեք դեպքերը միանգամից կարելի է անտեսել, քանի որ եթե I-ն պարունակի 1 միավորը, ապա $I = K[x_1, x_2]$, ինչն անհնար է, քանի որ I-ն ակնհայտորեն չի պարունակում զրոյից տարբեր սկալյար բազմանդամներ: Մնացած դեպքում ունենք, որ I-ն պարունակում է x_1 կամ x_2 մոնոմիալները: Դա նույնպես անհնար է, քանի որ $f = x_1 - x_2$ բազմանդամով ծնված գլխավոր իդեալի բոլոր տարրերը պիտի բաժանվեն f-ի վրա: Հակասությունները ցույց են տալիս, որ I-ն մոնոմիալ իդեալ չէ:

8.3.4 Վարժություն. Տրված է $K[x_1, \dots, x_n]$ օղակի ոչ զրոյական I իդեալը, ընդ որում, հայտնի է, որ յուրաքանչյուր $f \in I$ բազմանդամի հետ միասին I-ն պարունակում է նրա բոլոր միանդամները: Մոնոմիալ իդեա՞լ է արդյոք I-ն:

Հետեւյալ կարեւոր լեմման ոչ միայն նկարագրում է մոնոմիալ իդեալների բազմանդամները, այլեւ շեշտում է այն յուրահատկությունը, որի շնորհիվ մոնոմիալ իդեալները հարմար օժանդակ գործիք են դառնում մնացած իդեալների ուսումնասիրման համար: Ինչպես տեսել ենք նախորդ գլուխների բազմաթիվ օրինակներում, եթե I իդեալը ծնվում է որոշ $g_1,\ g_2 \dots \in K[x_1, \dots, x_n]$ բազմանդամներով (ոչ անպայման մոնոմիալներով), ապա որեւէ $f \in I$ բազմանդամի միանդամները կարող են շատ քիչ կապված լինել $g_1, g_2 \dots$ բազմանդամների եւ դրանց միանդամների հետ, քանի որ բազմանդամների բազմապատկման եւ նման անդամների միացման ընթացքում շատ բան կրճատվում է: Պարզվում է, որ մոնոմիալ իդեալների դեպքում այդ կապը ավելի սերտ է.

8.3.5 Լեմմա. *$K[x_1, \dots, x_n]$ օղակի $I = \langle x^\alpha \mid \alpha \in A \rangle$, $A \subseteq \mathbb{N}_0^n$ մոնոմիալ իդեալի ցանկացած $f = \sum_{\beta \in S} a_\beta x^\beta$ բազմանդամի յուրաքանչյուր x^β մոնոմիալը բաժանվում է որեւէ x^α մոնոմիալի վրա ($\alpha \in A$):*

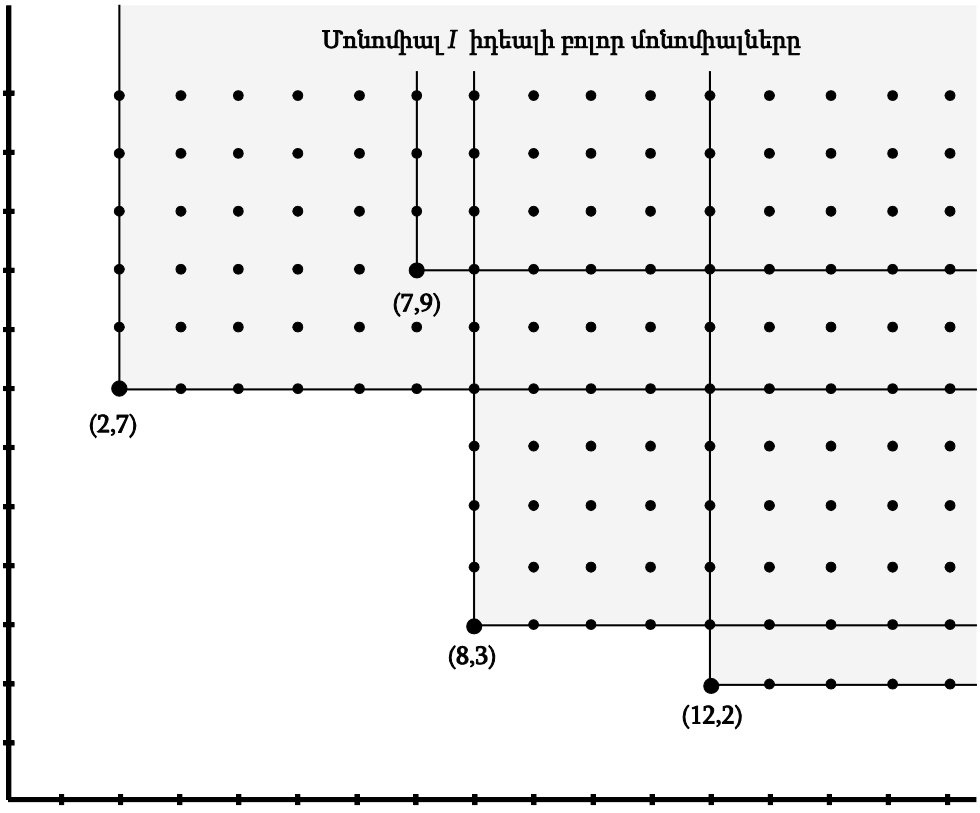
Ըստ լեմմայի՝ f բազմանդամը ստացվում է՝ մի քանի x^α, $\alpha \in A$, մոնոմիալներ $K[x_1, \dots, x_n]$ օղակի այլ մոնոմիալներով բազմապատկելով, եւ վերցնելով ստացված արտադրյալների գծային կոմբինացիան ըստ K դաշտի սկալյարների: Մասնավորապես, եթե f-ն ինքը մոնոմիալ է, ապա.

8.3.6 Հետեւանք. $K[x_1, \dots, x_n]$ օղակի $I = \langle x^\alpha \mid \alpha \in A \rangle$ մոնոմիալ իդեալին ($A \subseteq \mathbb{N}_0^n$) պատկանող ցանկացած x^β մոնոմիալ բաժանվում է որեւէ x^α մոնոմիալի ($\alpha \in A$) վրա:

8.3.5 լեմմայի ապացույցը: Ըստ (8.11) բանաձեւի ունենք $f = \sum_{i=1}^{s} h_i x^{\alpha_i}$, որտեղ $h_1, \dots, h_s \in K[x_1, \dots, x_n]$ եւ $\alpha_1, \dots, \alpha_s \in \{x^\alpha \mid \alpha \in A\}$: Բոլոր i-երի համար h_i բազմանդամների միանդամները հերթով բազմապատկելով համապատասխան x^{α_i} մոնո-

միալներով՝ կստանանք վերջավոր քանակությամբ միանդամներ, որոնցից յուրաքանչյուրը բաժանվում է $\{x^\alpha \mid \alpha \in A\}$ մոնոմիալներից առնվազն մեկի վրա: f-ը ստանալու համար դեռ պետք է այդ միանդամների գումարի մեջ նման անդամների միացում կատարել: Այդ ընթացքում կարող են փոխվել միանդամների գործակիցները, իսկ որոշ միանդամներ կարող են անգամ կրճատվել: Բայց այդ ընթացքում նոր մոնոմիալներ չեն ստացվում: ■

8.3.5 լեմման թույլ է տալիս մոնոմիալ իդեալները նկարագրել հետեւյալ գրաֆիկական եղանակով: Եթե $I = \langle x^\alpha \mid \alpha \in A\rangle$, ապա x^α մոնոմիալի հետ միասին I իդեալը պարունակում է նաեւ բոլոր $x^\alpha x^\gamma = x^{\alpha+\gamma}$ մոնոմիալները: Եթե x^α մոնոմիալը ներկայացնենք որպես n չափողականության տարածության մեջ մի գագաթ, որի կոորդինատների n-յակը հավասար է α աստիճանային վեկտորին, ապա $x^{\alpha+\gamma}$ մոնոմիալները կներկայացվեն այն կետերով, որոնց բոլոր կոորդինատները մեծ կամ հավասար են x^α-ի կոորդինատներից՝ $\alpha + \gamma \in \alpha + \mathbb{N}_0^n$:



Օրինակ՝ երկու փոփոխականների դեպքում $x^{\alpha+\gamma}$ մոնոմիալները կներկայացվեն այն կետերով, որոնք ընկած են x^{α}-ի գագաթից «դեպի աջ եւ վերեւ» (տես վերը բերված պատկերը)։ $\{x^{\alpha} \mid \alpha \in A\}$ բազմության յուրաքանչյուր մոնոմիալի համար նշենք x^{α} գագաթը եւ դրանցից յուրաքանչյուրի համար նշենք իրենից «դեպի աջ եւ վերեւ» ընկած կետերի բազմությունը։ Ամեն կետին համապատասխանում է մի մոնոմիալ I իդեալում։ Այդ մոնոմիալը բազմապատկելով K դաշտի հնարավոր բոլոր սկալյարներով՝ կստանանք միանդամների մի բազմություն։ Ըստ 8.3.5 լեմմայի՝ I իդեալը բաղկացած է նման միանդամների հնարավոր բոլոր գումարներից։

Վերեւի նկարում պատկերված են $K[x,y]$ օղակում $\{x^2y^7,\ x^7y^9,\ x^8y^3,\ x^{12}y^2\}$ մոնոմիալների բազմությամբ ծնված մոնոմիալ I իդեալի բոլոր մոնոմիալները։ Նշված չորս մոնոմիալներից ամեն մեկին համապատասխանեցված է մի գագաթ։ Ամեն գագաթի համար նշված է այն կետերի բազմությունը, որոնք գտնվում են իրենից «դեպի աջ եւ դեպի վերեւ»։ Այդ չորս բազմությունների ստվերագծված միավորումն է, որ բաղկացած է I-ի բոլոր մոնոմիալներից։ Ընդ որում, x^7y^9 մոնոմիալին համապատասխանող գագաթն ինքը ընկած է ստվերագծված հատվածում, ուստի նրա շնորհիվ նոր գագաթներ չեն ավելանում։

8.3.7 Օրինակ. Մոնոմիալ իդեալը եռաչափ պատկերելու մի օրինակ փորձել ենք ներկայացնել այս գրքի կազմին։ $\mathbb{R}[x,y,z]$ օղակում դիտարկենք $I = \langle x^6y^1z^0,\ x^4y^4z^4,\ x^0y^6z^1\rangle$ իդեալը։ $x^4y^4z^4 + \mathbb{N}_0^3$ կետերի բազմությունը պատկերված է կարմիր գույնով. դա այն «անվերջ մեծ խորանարդի մի անկյունն» է, որը հենվում է $x^4y^4z^4$ գագաթին։ $x^6y^1z^0 + \mathbb{N}_0^3$ կետերի բազմությունը նշված է կապույտով, իսկ $x^0y^6z^1 + \mathbb{N}_0^3$ կետերի բազմությունը՝ սպիտակով։ Դրանց միավորումը I իդեալի բոլոր մոնոմիալների բազմությունն է։ Իդեալը բաղկացած է $\mathbb{R}$-ից վերցված գործակիցներով՝ կարմիր, կապույտ եւ սպիտակ գագաթների վերջավոր գծային կոմբինացիաներից։

Ըստ 8.3.5 լեմմայի՝ մոնոմիալ իդեալը կարելի է միարժեքորեն վերականգնել՝ ելնելով իր մոնոմիալներից։ Ուստի ստանում ենք.

8.3.8 Հետեւանք. Մոնոմիալ իդեալները համընկնում են այն եւ միայն այն դեպքում, երբ նրանք պարունակում են միեւնույն մոնոմիալները։

8.3.9 Խնդիր. Նկարագրել մեկ փոփոխականի բազմանդամների $K[x]$ օղակի բոլոր մոնոմիալ իդեալները։ Դրանից օգտվելով պարզել՝ մոնոմիա՞լ է արդյոք $x^2 + 1$ բազմանդամով ծնված իդեալը։

Այժմ մենք կարող ենք անցնել հետեւյալ փաստի ապացույցին.

8.3.10 Լեմմա (Դիքսոնի լեմման). *K դաշտի վրա տրված $K[x_1,\dots,x_n]$ օղակի կամայական $I=\langle x^\alpha \mid \alpha\in A\rangle$, $A\subseteq \mathbb{N}_0^n$ մոնոմիալ իդեալի համար A բազմությունը պարունակում է այնպիսի $\alpha_1,\dots,\alpha_s\in A$ աստիճանային վեկտորներ, որ $I=\langle x^{\alpha_1},\dots,x^{\alpha_s}\rangle$: Մասնավորապես, կամայական մոնոմիալ իդեալ վերջավոր ծնված է:*

Ապացույց: Կիրառենք ինդուկցիա ըստ բազմանդամների n աստիճանի: $n=1$ դեպքում պնդումն ակնհայտ է, քանի որ մոնոմիալ իդեալում կարելի է վերցնել նվազագույն աստիճանի մոնոմիալը (տես 8.3.9 խնդիրը):

Ենթադրենք, լեմման ապացուցված է n-ի համար եւ համարենք, որ I-ն $n+1$ փոփոխականների $K[x_1,\dots,x_n,y]$ բազմանդամային օղակից է (նոր ավելացված փոփոխականը նշանակում ենք ոչ թե x_{n+1}, այլ y): I-ի մոնոմիալները ունեն $x^\alpha y^d$ տեսքը, որտեղ $\alpha\in\mathbb{N}_0^n$ եւ $d\in\mathbb{N}_0$: Բոլոր այդպիսի մոնոմիալների α աստիճանային վեկտորների բազմությունը նշանակենք B եւ դիտարկենք $L=\langle x^\alpha \mid \alpha\in B\rangle$ մոնոմիալ իդեալը: Ըստ ինդուկցիայի՝ կարելի է ընտրել վերջավոր հատ $\alpha_1,\dots,\alpha_s\in B$ աստիճանային վեկտորներ, որ $L=\langle x^{\alpha_1},\dots,x^{\alpha_s}\rangle$: Յուրաքանչյուր x^{α_i} մոնոմիալի համար կա մի $d_i\in\mathbb{N}_0$, որի համար $x^{\alpha_i}y^{d_i}\in I$: Նշանակենք մեծագույնը՝ $h=\max\{d_i,\ i=1,\dots,s\}$:

Վերցնենք որեւէ $k=\{0,\dots,h-1\}$ թիվ եւ դիտարկենք բոլոր այն $\alpha\in\mathbb{N}_0^n$ աստիճանային վեկտորների B_k բազմությունը, որոնց համար $x^\alpha y^k\in I$: Նշանակենք $L_k=\langle x^\alpha \mid \alpha\in B_k\rangle$: Կրկին ըստ ինդուկցիայի հիպոթեզի՝ յուրաքանչյուր k-ի համար $L_k=\langle x^{\alpha_{k1}},\dots,x^{\alpha_{ks_k}}\rangle$: Կառուցենք մոնոմիալների հետեւյալ համակարգը՝

$$
\begin{aligned}
&x^{\alpha_1}y^h,\dots,x^{\alpha_s}y^h,\\
&x^{\alpha_{h-1\,1}}y^{h-1},\dots,x^{\alpha_{h-1\,s_{h-1}}}y^{h-1},\\
&x^{\alpha_{h-2\,1}}y^{h-2},\dots,x^{\alpha_{h-2\,s_{h-2}}}y^{h-2},\\
&\dots\dots\dots\dots\dots\dots\dots\\
&x^{\alpha_{11}}y,\dots,x^{\alpha_{1\,s_1}}y,\\
&x^{\alpha_{01}},\dots,x^{\alpha_{0\,s_0}}:
\end{aligned}
\tag{8.12}
$$

Այս համակարգը կազմված է այնպես, որ I իդեալի կամայական մոնոմիալ բաժանվի (8.12)-ի մոնոմիալներից գոնե մեկի վրա: Իսկապես, վերցնենք որեւէ $x^\alpha y^d\in I$ մոնոմիալ: Եթե d-ն $0,\dots,h-1$ թվերից որեւէ մեկն է, ապա $x^\alpha\in L_d=\langle x^{\alpha_{d1}},\dots,x^{\alpha_{ds_d}}\rangle$: Ուստի x^α-ն բաժանվում է $x^{\alpha_{d1}},\dots,x^{\alpha_{ds_d}}$ մոնոմիալներից որեւե մեկի վրա, իսկ $x^\alpha y^d$-ն բաժանվում է (8.12) համակարգի $x^{\alpha_{d1}}y^d,\dots,x^{\alpha_{ds_d}}y^d$ մոնոմիալներից որեւե մեկի վրա:

Իսկ եթե $d \geq h-1$, ապա օգտվենք (8.12) համակարգի առաջին տողից: Քանի որ $x^{\alpha} \in L = \langle x^{\alpha_1}, \dots, x^{\alpha_s} \rangle$, ապա x^{α}-ն բաժանվում է $x^{\alpha_1}, \dots, x^{\alpha_s}$ մոնոմիալներից, ասենք, x^{α_i}-ի վրա: Նախորդ քայլերում x^{α_i}-ն ներառվել էր L-ի մեջ, քանի որ այն որեւէ y^t-ով բազմապատկելիս ստանում էինք I իդեալի տարր, ընդ որում, t-ն չի գերազանցում $h-1$ թիվը: Քանի որ դիտարկվող $x^{\alpha}y^{d}$ մոնոմիալում y-ը մասնակցում է h-ից ավելի բարձր աստիճանով, ապա $x^{\alpha}y^{d}$-ն բաժանվում է $x^{\alpha_i}y^{h}$-ի վրա:

Չնայած (8.12) վերջավոր համակարգը ծնում է I իդեալը՝ այն դեռեւս լեմմայում խոստացված ծնիչը չէ, քանի որ (8.12) համակարգի մոնոմիալների աստիճանային վեկտորները կարող են A-ին չպատկանել: Ըստ 8.3.5 լեմմայի՝ (8.12) համակարգի ցանկացած մոնոմիալ բաժանվում է I իդեալի $\{x^{\alpha} \mid \alpha \in A\}$ ծնիչի որեւէ մոնոմիալի վրա: Համակարգի յուրաքանչյուր մոնոմիալ փոխարինենք իր այդ բաժանարարով եւ նշանակենք ստացված համակարգը $x^{\beta_1}, \dots, x^{\beta_r}$, որտեղ $r = s + s_{h-1} + \cdots + s_1 + s_0$: Քանի որ $x^{\alpha} \in \langle x^{\beta_1}, \dots, x^{\beta_r} \rangle$, ապա $I \subseteq \langle x^{\beta_1}, \dots, x^{\beta_r} \rangle$ (կամայական իդեալի ծնիչի տարրը իր բաժանարարով փոխարինելով՝ մենք չենք փոքրացնում ծնիչով ծնվող իդեալը): Մյուս կողմից, բոլոր $x^{\beta_1}, \dots, x^{\beta_r}$ մոնոմիալները $\{x^{\alpha} \mid \alpha \in A\}$-ից էին: Ուստի $\langle x^{\beta_1}, \dots, x^{\beta_r} \rangle \subseteq \langle x^{\alpha} \mid \alpha \in A \rangle = I$: Լեմման ապացուցված է: ■

8.3.11 Դիտողություն. Դիքսոնի լեմման ունի երկրաչափական ծագում եւ կապված է վերը բերված գծագրի հետ: Լեմման առնչվում է $\mathbb{N}_0^n$ տեսքի բազմություններում որոշակի պայմանների բավարարող կարգավորվածության նկատմամբ որոշակի բազմությունների մինիմալ տարրերի քանակի վերջավորության հետ: Օրինակ, գծագրում ստվերագծված մասից խիստ դեպի ձախ եւ դեպի ներքեւ գտնվող գագաթների թիվը վերջավոր է: Որոշ աղբյուրներում այս լեմման կոչվում է նաեւ Ջորդանի լեմմա:

Որպես Դիքսոնի լեմմայի կիրառություն՝ կարելի է պարզեցնել մոնոմիալ կարգավորվածության 8.2.4 սահմանման պահանջներից մեկը: Այդ պարզեցումն ունի կարեւոր ալգորիթմական իմաստ, քանի որ որոշ դեպքերում շատ ավելի հեշտ է տվյալ $<$ հարաբերության համար ստուգել ոչ թե սահմանման **M.1** պահանջի երկրորդ կետը, այլ միայն այն փաստը, որ ըստ $<$ կարգավորվածության մինիմալ աստիճանային վեկտորը զրոյական է (զրոյական ենք անվանում $0 = (0, \dots, 0) \in \mathbb{N}_0^n$ աստիճանային վեկտորը):

8.3.12 Հետեւանք. $\mathbb{N}_0^n$ բազմության վրա տրված $<$ մոնոմիալ կարգավորվածության 8.2.4 սահմանման **M.1** պահանջի երկրորդ կետը կարելի է փոխարինել հետեւյալ կետով.

2*) կամայական ոչ զրոյական $\alpha \in \mathbb{N}_0^n$ աստիճանային վեկտորի համար $0 < \alpha$:

Ապացույց: Եթե տեղի ունեն 8.2.4 սահմանման կետերը, ապա $\mathbb{N}_0^n$ բազմությունը նույնպես ունի նվազագույն μ տարր: Եթե այն զրոյական չէ, ապա $\mu < 0$: Ուրեմն՝ $2\mu = \mu + \mu < 0 + \mu = \mu$: Սա հակասում է μ-ի մինիմալությանը:

Ենթադրենք տեղի ունեն **(2*)** կետը եւ 8.2.4 սահմանման բոլոր կետերը, բացի **M.1** պահանջի երկրորդ կետից: $\mathbb{N}_0^n$ բազմության կամայական A ոչ դատարկ ենթաբազմության համար դիտարկենք $I = \langle x^\alpha \mid \alpha \in A \rangle$ մոնոմիալ իդեալը: Ըստ Դիքսոնի լեմմայի այն վերջավոր ծնված է՝ $I = \langle x^{\alpha_1}, \dots, x^{\alpha_s} \rangle$: Վերցնենք կամայական $\alpha \in A$ աստիճանային վեկտոր: Ըստ 8.3.5 լեմմայի՝ x^α-ն որեւէ i-ի համար բաժանվում է x^{α_i} մոնոմիալի վրա: Այսինքն՝ $x^\alpha = x^{\alpha_i} x^\beta = x^{\alpha_i + \beta}$: Քանի որ, ըստ **(2*)** կետի $\beta \geq 0$, ապա $\alpha = \alpha_i + \beta \geq \alpha_i + 0 = \alpha_i$: Հետեւաբար, մնում է իրար հետ համեմատել վերջավոր քանակությամբ $\alpha_1, \dots, \alpha_s$ աստիճանային վեկտորները, դրանցից ընտրել (ըստ $<$ հարաբերության) փոքրագույնը, որը եւ կլինի A ենթաբազմության նվազագույն μ տարրը: ■

8.3.13 Դիտողություն. Մենք արդեն ավարտել ենք Հիլբերտի թեորեմի ապացույցի համար անհրաժեշտ քայլերի մեծ մասը: Վերջին քայլի համար մեզ անհրաժեշտ է միայն մոնոմիալ կարգավորվածությամբ բազմանդամների հաջորդականության վրա բաժանման ալգորիթմը, որին կանցնենք հաջորդ պարագրաֆում:

8.4 Բաժանման ալգորիթմը եւ Հիլբերտի թեորեմը

Բազմանդամների հաջորդականության վրա բաժանման ալգորիթմն ընդհանրացնում է մնացորդով բաժանման սովորական հասկացությունը եւ անկյունով բաժանման մեթոդը, որոնց շատ ենք առնչվել նախորդ գլուխներում: Հիշենք, որ դաշտի վրա տրված $K[x]$ օղակի f, g բազմանդամների համար ($g \neq 0$) գոյություն ունի q քանորդ եւ r մնացորդ, այնպես, որ $f = qg + r$, ընդ որում, կամ $r = 0$, կամ էլ $r \neq 0$ եւ $\deg r < \deg g$: Իսկ անկյունով բաժանման հայտնի մեթոդն օգնում է մեզ հաշվել այդ q եւ r բազմանդամները:

Մեր նպատակն է գտնել մնացորդով բաժանման անալոգը $K[x_1, \dots, x_n]$ օղակում մի քանի բազմանդամների հաջորդականության վրա բաժանելու համար եւ ստանալ անկյունով բաժանման մեթոդի ընդհանրացումը: $f \in K[x_1, \dots, x_n]$ բազմանդամի եւ ոչ զրոյական բազմանդամների $g_1, \dots, g_s$ վերջավոր հաջորդականության համար կարելի է կառուցել $f = q_1 \cdot g_1 + \dots + q_s \cdot g_s + r$ ներկայացումը, որի հատկությունները «նման են» սովորական մնացորդով բաժանումների հատկություններին: r-ի

վրա դրվող պայմանը ձեւակերպվում է հետեւյալ կերպ. նախ՝ $K[x_1, \dots, x_n]$ օղակի վրա ֆիքսվում է որեւէ $<$ մոնոմիալ կարգավորվածություն եւ յուրաքանչյուր g_i բաժանարարի համար ըստ այդմ ընտրվում է նրա $\mathrm{lt} g_i$ ավագ անդամը: Պահանջվում է, որ կամ $r = 0$, կամ էլ $r \neq 0$ եւ r-ի միանդամներից ոչ մեկը չբաժանվի $\mathrm{lt} g_i$-ի վրա, $i = 1, \dots, s$:

Բնականաբար, ակնհայտ չէ, թե յուրաքանչյուր մոնոմիալ կարգավորվածության եւ f եւ $g_1, \dots, g_s$ բազմանդամների համար նման ներկայացում միշտ գոյություն ունի: Սկսենք մի մանրամասն օրինակից, որը ոչ միայն կբացատրի անկյունով բաժանման մեթոդը, այլեւ կնախապատրաստի 8.4.3 թեորեմի ապացույցը:

8.4.1 Օրինակ. $K[x, y]$ օղակում որպես մոնոմիալ կարգի հարաբերություն ընդունենք lex կարգավորվածությունը: $f = 2x^3y + x^2y + xy^2 + y^2$ բազմանդամը բաժանենք հետեւյալ երեք բազմանդամների հաջորդականության վրա՝ $g_1 = x^3$, $g_2 = xy - 1$, $g_3 = y^2 - 1$: Քննարկվող բոլոր բազմանդամների միանդամները պետք է դասավորված լինեն ըստ lex կարգավորվածության, ինչն արդեն արված է: Շեշտենք, որ g_1, g_2, g_3 բաժանարարների հաջորդականության դասավորությունը կապված չէ lex-ի կամ այլ մոնոմիալ կարգի հետ. դրանք մենք կարող ենք դասավորել ինչպես ցանկանում ենք, սակայն, ֆիքսելով այդ բազմանդամների որեւէ դասավորություն, մենք չենք կարող խնդրի լուծման ընթացքում փոխել այն: Անկյունով բաժանումը սկսելու համար նախ f, g_1, g_2 եւ g_3 բազմանդամները դասավորենք հետեւյալ կերպ.

$$\begin{array}{r|l} 2x^3y + x^2y + xy^2 + y^2 & \begin{array}{l} x^3 \\ xy - 1 \\ y^2 - 1 \end{array} \quad \begin{array}{l} \\ \\ r \end{array} \\ \hline & \end{array}$$

Նկատում ենք, որ այս դասավորությունը սովորական անկյունով բաժանումից տարբերվում է իր երեք մասերով: Նախ՝ վերին աջ մասում գրված են ոչ թե մեկ, այլ երեք g_1, g_2, g_3 բաժանարարներ (նույն հաջորդականությամբ, որը ֆիքսվել էր սկզբում): Ապա՝ քանորդների մասում (բաժանարարներից ներքեւ) սովորականից մեծ դատարկ տեղ է թողնված. այդտեղ իրար տակ գրվելու են q_1, q_2, q_3 քանորդները: Վերջապես՝ աջ մասում ավելացված է մի նոր սյունակ, որը անվանված է «r»: Սա մնացորդի («reminder») սյունակն է: Սովորական անկյունով բաժանումների դեպքում մնացորդը հանդես էր գալիս բաժանման եզրափակիչ քայլերում եւ գրվում նախավերջին տողում: Իսկ այս դեպքում մնացորդի համար առանձին սյունակ է հատկացված:

f բազմանդամի $\mathrm{lt} f$ ավագ անդամը համեմատենք g_1 բաժանարարի $\mathrm{lt} g_1$ ավագ անդամի հետ. արդյո՞ք $\mathrm{lt} f$-ը բաժանվում է $\mathrm{lt} g_1$-ի վրա: Եթե այո, ապա քանորդների

մասի *առաջին* տողում գրենք $\mathrm{lt}f/\mathrm{lt}g_1$ միանդամը (առաջին տողում, քանի որ ստացվել է g_1-ի օգնությամբ): Հասկանալի է, որ $(\mathrm{lt}f/\mathrm{lt}g_1)\cdot g_1$ արտադրյալը կունենա նույն ավագ անդամը, ինչ f-ը: Ուստի f-ի ներքեւում գրենք $(\mathrm{lt}f/\mathrm{lt}g_1)\cdot g_1$ բազմանդամը եւ f-ից հանենք այն: Իսկ եթե $\mathrm{lt}f$-ը չբաժանվեր $\mathrm{lt}g_1$-ի վրա, ապա կանցնեինք g_2 բաժանարարին: Մեր դեպքում բաժանումը կատարվում է՝ $\mathrm{lt}f/\mathrm{lt}g_1 = 2y$: Ստանում ենք.

$$\begin{array}{l|l} 2x^3y + x^2y + xy^2 + y^2 & x^3 \\ & xy - 1 \\ & y^2 - 1 \qquad r \\ \hline 2x^3y & 2y \\ \hline x^2y + xy^2 + y^2 & \end{array}$$

Վերջին տողի $x^2y + xy^2 + y^2$ բազմանդամի միանդամները դասավորում ենք ըստ lex-ի (տվյալ դեպքում վերադասավորելու կարիք չկա, քանի որ միանդամները արդեն իսկ ըստ lex-ի են դասավորված): Ապա նույն հերթականությամբ ստուգում ենք՝ արդյոք բաժանվո՞ւմ է ստացված բազմանդամի ավագ անդամը g_1, g_2, g_3 բաժանարարների ավագ անդամների վրա: Այս անգամ ավագ անդամը $\mathrm{lt}g_1$-ի վրա չի բաժանվում, բայց բաժանվում է $\mathrm{lt}g_2$-ի վրա: Քանի որ $x^2y = x\cdot \mathrm{lt}g_2$, ապա քանորդների մասի *երկրորդ* տողում գրենք x միանդամը (երկրորդ տողում, քանի որ ստացվել է g_2-ի օգնությամբ): Հաջորդ քայլում, ըստ lex-ի վերադասավորումից հետո կստացվի $xy^2 + x + y^2$ տարբերությունը: Այն չի բաժանվում $\mathrm{lt}g_1$-ի վրա, բայց բաժանվում է $\mathrm{lt}g_2$-ի վրա՝ $xy^2 = y\cdot \mathrm{lt}g_2$: Շեշտենք, որ այն բաժանվում է նաեւ $\mathrm{lt}g_3$-ի վրա, մենք պարտավոր ենք դիտարկել $\mathrm{lt}g_2$-ը, քանի որ պետք է հետեւենք բաժանարարների դասավորությանը: Ուստի կրկին քանորդների մասի *երկրորդ* տողում գումարում ենք y միանդամը: Հաջորդ հանումից եւ ըստ lex-ի վերադասավորումից հետո կունենանք.

$$\begin{array}{l|l} 2x^3y + x^2y + xy^2 + y^2 & x^3 \\ & xy - 1 \\ & y^2 - 1 \qquad r \\ \hline 2x^3y & 2y \\ & x + y \\ \hline x^2y + xy^2 + y^2 & \\ x^2y - x & \\ \hline xy^2 + x + y^2 & \\ xy^2 - y & \\ \hline x + y^2 + y & \end{array}$$

Այստեղ արդեն այլ իրավիճակ ունենք, քանի որ վերջին $x + y^2 + y$ տարբերության x ավագ անդամը չի բաժանվում $\mathrm{lt}g_1$, $\mathrm{lt}g_2$, $\mathrm{lt}g_3$ ավագ անդամներից ոչ մեկի

վրա: Միաժամանակ մենք դեռ չենք ստացել վերջնական մնացորդը, քանի որ $x + y^2 + y$ տարբերության երկրորդ անդամը բաժանվում է $\mathrm{lt} g_3$-ի վրա. պարզապես նրանից առաջ կանգնած x ավագ անդամը «խանգարում է» մեզ կատարել այդ բաժանումը: Ազատվենք x-ից $x + y^2 + y$ բազմանդամը երկու մասի ճեղքելու միջոցով. x-ը տեղափոխենք «r» սյունակ, իսկ մնացած $y^2 + y$ գումարը իջեցնենք եւս մի տող.

$2x^3y + x^2y + xy^2 + y^2$	x^3 $xy - 1$ $y^2 - 1$	r
$2x^3y$	$2y$ $x + y$	
$x^2y + xy^2 + y^2$		
$x^2y - x$		
$xy^2 + x + y^2$		
$xy^2 - y$		
$x + y^2 + y$		
$y^2 + y$		x

Շարունակելով այս քայլերը, ստանում ենք.

$2x^3y + x^2y + xy^2 + y^2$	x^3 $xy - 1$ $y^2 - 1$	r
$2x^3y$	$2y$ $x + y$ 1	
$x^2y + xy^2 + y^2$		
$x^2y - x$		
$xy^2 + x + y^2$		
$xy^2 - y$		
$x + y^2 + y$		
$y^2 + y$		x
$y^2 - 1$		
$y + 1$		
1		$x + y$
0		$x + y + 1$

Ինչպես տեսնում ենք, $y + 1$ բազմանդամի ավագ գործակիցը նույնպես չի բաժանվում $\mathrm{lt} g_1$, $\mathrm{lt} g_2$, $\mathrm{lt} g_3$ ավագ գործակիցների վրա, ուստի նրա y ավագ գործակիցը

գումարվել է «r» սյունակում արդեն եղած x բազմանդամին: Իսկ հաջորդ քայլում «r» սյունակ է գնացել նաեւ 1-ը: Վերջում ձախ կողմում մնացել է 0, իսկ «r» սյունակում ստացվել է մնացորդի արժեքը՝ $r = x + y + 1$: Ստանում ենք հետեւյալ վերլուծությունը.

$$\begin{aligned} 2x^3y + x^2y + xy^2 + y^2 = f &= q_1 \cdot g_1 + q_2 \cdot g_2 + q_3 \cdot g_3 + r \\ &= 2y \cdot x^3 + (x + y) \cdot (xy - 1) + 1 \cdot (y^2 - 1) + x + y + 1: \end{aligned} \tag{8.13}$$

8.4.2 Վարժություն. Պարզեցնել (8.13)-ի երկրորդ տողը եւ ստուգել, որ ստացվող բազմանդամն իսկապես հավասար է $f = 2x^3y + x^2y + xy^2 + y^2$ բազմանդամին:

Հետեւյալ թեորեմի ապացույցի փուլերը նման են 8.4.1 օրինակի քայլերին.

8.4.3 Թեորեմ. *Ենթադրենք K դաշտի վրա տրված $K[x_1, \dots, x_n]$ օղակում սահմանված է որեւէ $<$ մոնոմիալ կարգավորվածություն եւ տրված է ոչ զրոյական բազմանդամների վերջավոր $g_1, \dots, g_s$ հաջորդականությունը: Այդ դեպքում ցանկացած $f \in K[x_1, \dots, x_n]$ բազմանդամի համար գոյություն ունեն այնպիսի $q_1, \dots, q_s, r \in K[x_1, \dots, x_n]$ բազմանդամներ, որ*

$$f = q_1 \cdot g_1 + \cdots + q_s \cdot g_s + r, \tag{8.14}$$

ընդ որում, կամ $r = 0$, կամ էլ $r \neq 0$ եւ r-ի միանդամներից ոչ մեկը չի բաժանվում $\mathrm{lt}g_1, \dots, \mathrm{lt}g_s$ ավագ անդամների վրա:

Ապացույց: Որպես r մնացորդի սկզբնական արժեք ընդունենք $r = 0$: Ստուգենք, թե արդյո՞ք $\mathrm{lt}f$-ը բաժանվում է որեւէ $\mathrm{lt}g_i$-ի վրա, $i = 1, \dots, s$: Ենթադրենք բաժանումը կատարվում է եւ ընտրենք առաջին i-ն, որի համար $\mathrm{lt}f \vdots \mathrm{lt}g_i$:

Քանի որ ընտրած կարգավորվածությունը մոնոմիալ է, ապա $(\mathrm{lt}f/\mathrm{lt}g_i) \cdot g_i$ արտադրյալի ավագ անդամը կլինի $(\mathrm{lt}f/\mathrm{lt}g_i) \cdot \mathrm{lt}g_i$: Իսկապես՝ $\mathrm{lt}g_i$-ն մեծ է g_i-ի մնացած միանդամներից, իսկ մի այլ միանդամով բազմապատկումը չի խախտում դա՝ ըստ 8.2.4 սահմանման **M.2** կետի: Բայց $(\mathrm{lt}f/\mathrm{lt}g_i) \cdot \mathrm{lt}g_i = \mathrm{lt}f$, այսինքն՝ f եւ $(\mathrm{lt}f/\mathrm{lt}g_i) \cdot g_i$ բազմանադամներն ունեն նույն ավագ անդամը: $f_1 = f - (\mathrm{lt}f/\mathrm{lt}g_i) \cdot g_i$ տարբերության մեջ դրանք կրճատվում են. f_1-ի ավագ անդամը խիստ փոքր է $\mathrm{lt}f$-ից:

Կրկնենք քայլը f_1-ի համար: Եթե դարձյալ i-ն առաջին ինդեքսն է, որի համար $\mathrm{lt}f_1 \vdots \mathrm{lt}g_i$, ապա կանցնենք

$$f_2 = f_1 - (\mathrm{lt}f_1/\mathrm{lt}g_i) \cdot g_i = f + [-(\mathrm{lt}f/\mathrm{lt}g_i) - (\mathrm{lt}f_1/\mathrm{lt}g_i)]g_i \tag{8.15}$$

բազմանդամին: Իսկ եթե բաժանումը կատարվում է մի այլ $j \neq i$ ինդեքսի համար, ապա կանցնենք

$$f_2 = f_1 - (\mathrm{lt} f_1/\mathrm{lt} g_j) \cdot g_j = f - (\mathrm{lt} f/\mathrm{lt} g_i) \cdot g_i - (\mathrm{lt} f_1/\mathrm{lt} g_j) \cdot g_j \tag{8.16}$$

բազմանդամին: Երկու դեպքում էլ ավագ անդամները կրճատվում են, ուրեմն, $\mathrm{lt} f_2 < \mathrm{lt} f_1$:

Հնարավոր է նաեւ այն դեպքը, երբ f_1 բազմանդամում դեռեւս կան $\mathrm{lt} g_i$ ավագ անդամներից որեւէ մեկի վրա բաժանվող միանդամներ, բայց f_1-ի ավագ միանդամը դրանց շարքին չի պատկանում, եւ մենք նախորդ քայլերի նման կրճատում չենք կարող իրականացնել: Այդ դեպքում f_1-ը փոխարինենք $f_2 = f_1 - \mathrm{lt} f_1$ բազմանդամով եւ միաժամանակ r-ը փոխարինենք $r = r + \mathrm{lt} f_1$ բազմանդամով (f_1-ը ճեղքում ենք երկու մասի՝ մի մասը շնորհելով մնացորդին): Պարզ է, որ $\mathrm{lt} f_2 < \mathrm{lt} f_1$:

Այս երեք տիպի քայլերը կրկնելով՝ կստանանք նվազող բազմանդամների $f > f_1 > f_2 > f_3 > \cdots$ հաջորդականություն: Քանի որ մոնոմիալ կարգավորվածությունը լիովին կարգավորվածություն է, ապա այս պրոցեսն անվերջ շարունակվել չի կարող: Այն կանգ կառնի, երբ հերթական f_k բազմանդամի միանդամներից ոչ մեկը չբաժանվի $\mathrm{lt} g_i$ ավագ անդամներից որեւէ մեկի վրա:

Յուրաքանչյուր g_i բազմանդամի համար (8.15) եւ (8.16) տեսքի հավասարումների մեջ $-(\mathrm{lt} f/\mathrm{lt} g_i)$ գումարելիներից առաջացող արտադրիչը նշանակենք q_i: Իսկ եթե g_i բազմանդամներից որեւէ մեկը պրոցեսին ընդհանրապես չի մասնակցել, նրա համար վերցնենք $q_i = 0$: Ստացանք որոնելի (8.14) ներկայացումը: ■

Նկատենք ապացույցից բխող մի առանձնահատկություն.

8.4.4 Հետեւանք. Եթե նախորդ թեորեմի (8.14) ներկայացման մեջ որեւէ i ինդեքսի համար $q_i \cdot g_i \neq 0$, ապա $\mathrm{multideg}\, f \geq \mathrm{multideg}\,(q_i \cdot g_i)$:

8.4.3 թեորեմը ցույց է տալիս, որ 8.4.1 օրինակում ստացված (8.13) վերլուծությունը պատահական հաջողություն չէր, եւ նման բաժանում կարելի է իրականացնել ոչ զրոյական բազմանդամների ցանկացած վերջավոր հաջորդականության վրա: Ապացույցը բացատրում է նաեւ, թե բաժանման ընթացքում ինչու էր անհրաժեշտ մոնոմիալ կարգավորվածություն կիրառել:

(8.14) ներկայացումն ընդունված է անվանել *f բազմանդամի բաժանում $g_1, \ldots, g_s$ բազմանդամների վրա:* $q_1, \ldots, q_s$ բազմանդամները կոչվում են բաժանման *քանորդներ*, իսկ r-ը՝ բաժանման *մնացորդ:* Եթե բաժանարարների կարգավորված s-յակը նշանակենք $G = (g_1, \ldots, g_s)$, ապա (8.14)-ը կարելի է անվանել նաեւ f-ի բա-

ժանում G-ի վրա: Գրյոբների բազաներին անցնելուց հետո մենք նման բաժանումների հետ շատ ենք գործ ունենալու, ուստի նպատակահարմար է մնացորդի համար նշանակում մտցնել՝ $r = f_G$:

Ալգորիթմի տեսքով ձեւակերպենք բազմանդամների հաջորդականության վրա բաժանման մեթոդը.

8.4.5 Ալգորիթմ (բազմանդամների հաջորդականության վրա բաժանման ալգորիթմը: $K[x_1, \dots, x_n]$ օղակում ֆիքսված է որեւէ մոնոմիալ կարգավորվածություն եւ տրված է ոչ զրոյական բազմանդամների $g_1, \dots, g_s$ հաջորդականությունը: Տրված $f \in K[x_1, \dots, x_n]$ բազմանդամը ներկայացնել $f = q_1 \cdot g_1 + \cdots + q_s \cdot g_s + r$ տեսքով, որտեղ կամ $r = 0$, կամ էլ $r \neq 0$ եւ r-ի միանդամներից ոչ մեկը չի բաժանվում $\mathrm{lt}g_1, \dots, \mathrm{lt}g_s$ ավագ անդամների վրա:

1. Նշանակենք $r = 0$:

2. Նշանակենք $q_1 = 0, \dots, q_s = 0$:

3. Նշանակենք $h = f$:

4. Քանի դեռ $h \neq 0$

5. նշանակենք $i = 1$;

6. քանի դեռ $i \leq s$

7. եթե $\mathrm{lt}h \vdots \mathrm{lt}g_i$

8. $q_i = q_i + \mathrm{lt}h/\mathrm{lt}g_i$;

9. $h = h - (\mathrm{lt}h/\mathrm{lt}g_i) \cdot g_i$;

10. վերադառնանք 4-րդ քայլին;

11. այլապես

12. նշանակենք $i = i + 1$;

13. $h = h - \mathrm{lt}h$;

14. $r = r + \mathrm{lt}h$:

15. Դուրս գրենք $f = q_1 \cdot g_1 + \cdots + q_s \cdot g_s + r$ ներկայացումը:

Վարժություններ. 8.4.5 ալգորիթմը կիրառել 8.4.1, 8.4.6 եւ 8.4.9 օրինակների բազմանդամների համար:

Կրկին շեշտենք, որ մեր օգտագործած $g_1, \dots, g_s$ բաժանարարները ֆիքսված հաջորդականությամբ են դասավորված, եւ դրանց վերադասավորությունից հետո մնացորդը կարող է եւ փոխվել: Այս դիտողության էականությունը ցույց տալու համար դիտարկենք 8.4.1 օրինակի բազմանդամի բաժանումը նույն բաժանարարների վրա, բայց այլ դասավորությամբ.

8.4.6 Օրինակ. $K[x,y]$ օղակում ընդունենք lex կարգավորվածությունը եւ $f = 2x^3y + x^2y + xy^2 + y^2$ բազմանդամը բաժանենք $g_1 = x^3$, $g_2 = y^2 - 1$, $g_3 = xy - 1$: Այս օրինակը 8.4.1 օրինակից տարբերվում է միայն բաժանարարների դասավորությամբ: Առանց մանրամասները բացատրելու՝ բերենք անկյունով բաժանման արդյունքը.

$$
\begin{array}{l|l|l}
2x^3y + x^2y + xy^2 + y^2 & x^3 & \\
 & y^2 - 1 & \\
 & xy - 1 & r \\
\hline
2x^3y & 2y & \\
 & x + 1 & \\
 & x & \\
\hline
x^2y + xy^2 + y^2 & & \\
x^2y - x & & \\
\hline
xy^2 + x + y^2 & & \\
xy^2 - x & & \\
\hline
2x + y^2 & & \\
\hline
y^2 & & 2x \\
y^2 - 1 & & \\
\hline
1 & & \\
\hline
0 & & 2x + 1
\end{array}
$$

Ստանում ենք, որ

$$
\begin{aligned}
2x^3y + x^2y + xy^2 + y^2 = f &= q_1 \cdot g_1 + q_2 \cdot g_2 + q_3 \cdot g_3 + r \\
&= 2y \cdot x^3 + (x+1) \cdot (y^2 - 1) + x \cdot (xy - 1) + 2x + 1:
\end{aligned} \tag{8.17}
$$

8.4.7 Դիտողություն. (8.13) եւ (8.17) բաժանումները համեմատելով՝ տեսնում ենք, որ միեւնույն մոնոմիալ կարգավորվածության պայմաններում տվյալ բազմանդամը միեւնույն բաժանարարների վրա բաժանելիս կարող են տարբեր մնացորդներ ստացվել՝ կախված բաժանարարների դասավորությունից: Էվկլիդյան օղակում սովորական մնացորդով բաժանում կատարելիս մենք այս բարդություններին չէինք բախվում, քանի որ բաժանարարների քանակը 1 էր, իսկ մոնոմիալ կարգավորվածությունն էլ միշտ ֆիքսված էր:

8.4.8 Վարժություն. Հիմնավորել 8.4.6 օրինակի բաժանման բոլոր քայլերի մանրամասները:

Բազմանդամների վրա մնացորդով բաժանումը կարող է օգտագործվել 8.1 պարագրաֆում հիշատակված կարեւոր խնդիրներից մեկի՝ իդեալին պատկանելության խնդրի ուումնասիրման համար: Այդ խնդրի լուծումը հետագայում կստանանք Գրյոբների բազաների օգնությամբ, բայց այս պարագրաֆում արդեն կարող ենք լուծման առաջին քայլերն անել:

Ենթադրենք $I \subseteq K[x_1, \dots, x_n]$ իդեալը ծնվում է $g_1, \dots, g_s$ բազմանդամներով եւ տրված է կամայական $f \in K[x_1, \dots, x_n]$ բազմանդամ: Փորձենք պարզել, արդյո՞ք $f \in I$: Դրա համար f-ը բաժանենք $g_1, \dots, g_s$ բազմանդամների վրա: Եթե (8.14) ներկայացման մեջ մնացորդը լինի զրոյական, այսինքն, եթե

$$f = q_1 \cdot g_1 + \cdots + q_s \cdot g_s, \tag{8.18}$$

ապա այստեղից անմիջապես կբխի, որ $f \in \langle g_1, \dots, g_s \rangle = I$ (տես 2.2.12 թեորեմը): Եթե ճիշտ լիներ նաեւ հակառակը, ապա մենք ստացած կլինեինք $g_1, \dots, g_s$ բազմանդամներով ծնված իդեալին պատկանելության խնդրի լուծումը: Բայց, ինչպես մենք տեսանք 8.4.7 դիտողության մեջ, բազմանդամների վրա բաժանելիս ստացվող մնացորդը միարժեքորեն չի որոշվում: Այսինքն՝ f-ը միեւնույն $g_1, \dots, g_s$ բազմանդամների այլ դասավորության վրա բաժանելիս (8.18) վերլուծության մեջ կարող է ոչ զրոյական մնացորդ առաջանալ: Եթե մենք բերենք նման բացահայտ օրինակ, ապա պարզ կդառնա, որ բազմանդամների վրա բաժանումը դեռ բավարար չէ իդեալին պատկանելության խնդրի լուծման համար:

8.4.9 Օրինակ. $K[x, y]$ օղակում ընդունենք lex կարգավորվածությունը: $f = xy^2 - x$ բազմանդամը բաժանելով $g_1 = xy + 1$ եւ $g_2 = y^2 - 1$ ստանում ենք

$$f = xy^2 - x = y \cdot (xy + 1) + 0 \cdot (y^2 - 1) - x - y:$$

Մյուս կողմից, նույն բազմանդամը (g_2, g_1) զույգի վրա բաժանելով՝ ստանում ենք

$$f = xy^2 - x = x \cdot (y^2 - 1) + 0 \cdot (xy + 1) + 0:$$

Ըստ երկրորդ բաժանման՝ $f \in I = \langle g_2, g_1 \rangle = \langle g_1, g_2 \rangle$: Բայց առաջին բաժանման ընթացքում ստացվում է ոչ զրոյական մնացորդ: Այդ փաստը, իհարկե, չի նշանակում, թե $f \notin I$ (ծնիչների տեղափոխությունից դրանցով ծնված իդեալը չի փոխվում): Պարզապես առաջին բաժանումը մեզ դեռ բավարար ինֆորմացիա չի տալիս պարզելու, թե արդյո՞ք f-ը I իդեալից է:

8.4.10 Վարժություն. Ստանալ 8.4.9 օրինակի երկու ներկայացումները անկյունով բաժանման միջոցով:

8.4.11 Դիտողություն. Բերված օրինակները ցույց են տալիս, թե ինչքան ցանկալի կլիներ ունենալ I իդեալի ծնիչների այնպիսի մի $g_1, \dots, g_s$ բազմություն, որի վրա ցանկացած $f \in I$ բազմանդամը բաժանելիս ստացվող r մնացորդը կախված չլիներ ծնիչների դասավորությունից: Մասնավորապես, ցանկալի կլիներ, որ $r = 0$ այն եւ միայն այն դեպքում, երբ $f \in I$: Ինչպես կտեսնենք հետագայում, այս հատկություններով օժտված ծնիչներ են Գրյոբների բազաները, որոնց միջոցով կարելի է լուծել ոչ միայն իդեալին պատկանելության խնդիրը, այլեւ շատ այլ հարցեր:

Որպես նախորդ պարագրաֆի պնդումների եւ 8.4.3 թեորեմի ոչ բարդ կիրառություն՝ արդեն կարող ենք ապացուցել.

8.4.12 Թեորեմ (Հիլբերտի թեորեմը վերջավոր բազայի մասին). *K դաշտի վրա տրված $K[x_1, \dots, x_n]$ բազմանդամային օղակի ցանկացած I իդեալ վերջավոր ծնված է. գոյություն ունեն այնպիսի $g_1, \dots, g_s \in I$ բազմանդամներ, որ $I = \langle g_1, \dots, g_s \rangle$:*

Ապացույց: Եթե $I = \{0\}$, ապա թեորեմն ակնհայտ է: Ուստի ենթադրենք, որ I-ն պարունակում է ոչ զրոյական բազմանդամներ: I իդեալում ֆիքսենք որեւէ մոնոմիալ կարգավորվածություն, եւ I^*-ով նշանակենք I իդեալի բոլոր բազմանդամների (ըստ այդ կարգավորվածության) ավագ անդամներով ծնված իդեալը: Քանի որ միանդամը մոնոմիալից տարբերվում է միայն սկալյար արտադրիչով, ապա I^*-ը մոնոմիալ իդեալ է: Ըստ 8.3.10 Դիքսոնի լեմմայի՝ այն ծնվում է որոշ վերջավոր քանակությամբ մոնոմիալներով: Ըստ I^*-ի կառուցման եւ Դիքսոնի լեմմայի՝ այդ մոնոմիալները I իդեալի որոշ $g_1, \dots, g_s$ բազմանդամների ավագ մոնոմիալներն են: Ցույց տանք, որ $I = \langle g_1, \dots, g_s \rangle$:

Վերցնենք կամայական $f \in I$ բազմանդամ, ֆիքսենք $g_1, \dots, g_s$ բազմանդամների որեւէ դասավորություն եւ, ըստ 8.4.3 թեորեմի, f-ը բաժանենք $g_1, \dots, g_s$ բազմանդամների վրա՝ $f = q_1 \cdot g_1 + \dots + q_s \cdot g_s + r$: Նկատենք, որ այս դեպքում $r = 0$, ուրեմն եւ՝ $f \in I$: Իսկապես, եթե $r \neq 0$, ապա $r = f - (q_1 \cdot g_1 + \dots + q_s \cdot g_s)$ տարբերութունը կլիներ ոչ զրոյական բազմանդամ I իդեալում: Ուստի նրա $\mathrm{lt}\, r$ ավագ անդամը պատկանում է I^* մոնոմիալ իդեալին: Ըստ 8.3.5 լեմմայի 8.3.6 հետեւանքի՝ $\mathrm{lt}\, r$-ը բաժանվում է I^*-ը ծնող մոնոմիալների ցանկացած բազմության որեւէ անդամի վրա: Որպես այդպիսի բազմություն վերցնենք $g_1, \dots, g_s$ բազմանդամների ավագ մոնոմիալների բազմությունը: Ստանում ենք հակասություն 8.4.3 թեորեմի պնդմանը: ■

8.4.13 Դիտողություն. Հիլբերտի թեորեմն ընդհանրացնում է կամայական K դաշտի վրա տրված մեկ փոփոխականի $K[x]$ բազմանդամային օղակի մասին 2.5.15 հետեւանքը: Ըստ այդ հետեւանքի $K[x]$-ը գլխավոր իդեալների օղակ է, այսինքն՝ նրա յուրաքանչյուր I իդեալ ծնվում է միայն մեկ տարրով՝ $I = g(x)K[x] = \langle g(x) \rangle$: Ինչպես տեսանք 6.3.12 օրինակում, այդ օրինաչափությունը չի պահպանվում մեկից ավելի փոփոխականի բազմանդամների օղակում. այնտեղ կան իդեալներ, որոնք միայն մեկ տարրով չեն ծնվում: Հիլբերտի թեորեմը պնդում է, որ դրանք բոլորը ծնվում են եթե ոչ մեկ, ապա *վերջավոր* քանակությամբ տարրերով: 2.5.15 հետեւանքը նշում է Հիլբերտի թեորեմի մի մասնավոր դեպքը, երբ ծնիչների քանակը 1 է:

Հիլբերտի թեորեմը ունի եւս մի կիրառություն, որը մեզ պետք կգա 8.6 պարագրաֆում: Նախ՝ ներմուծենք նյոտերյան օղակի գաղափարը: Կամայական R օղակում տրված իդեալների աճող

$$I_1 \subseteq I_2 \subseteq \cdots \subseteq I_k \subseteq I_{k+1} \subseteq \cdots \tag{8.19}$$

հաջորդականությունը կոչվում է R-ի իդեալների *աճող շղթա:* Այն կարող է բաղկացած լինել վերջավոր կամ անվերջ (հաշվելի) քանակությամբ իդեալներից: Աճող շղթայում իրար հարեւան $I_k \subseteq I_{k+1}$ իդեալները կարող են եւ իրար հավասար լինել:

Կասենք, որ (8.19) շղթան *կայունանում է*, եթե ինչ-որ k_0 համարից սկսած նրա բոլոր իդեալներն իրար հավասար են՝

$$I_{k_0} = I_{k_0+1} = \cdots = I_{k_0+i} = \cdots: \tag{8.20}$$

Կայունացող շղթայում իրարից տարբեր կարող են լինել միայն առաջին որոշ անդամները, իսկ դրանց, ինչ-որ տեղից սկսած, հաջորդում են կրկնվող (8.20) անդամները: Հասկանալի է, որ վերջավոր շղթան միշտ կայունանում է:

8.4.14 Օրինակ. Աճող շղթաների օրինակներ հեշտ է կառուցել՝ օգտվելով ծնիչ բազմություններից: Կամայական R օղակում վերցնենք նրա ցանկացած տարրերի $a_1, \dots, a_k, \dots \in R$ բազմություն եւ սահմանենք $I_k = \langle a_1, \dots, a_k \rangle$: Հասկանալի է, որ $I_k \subseteq I_{k+1}$ ցանկացած $k = 1,2, \dots$ ինդեքսի համար: Ընդ որում, եթե անգամ բոլոր $a_1, \dots, a_k, \dots$ տարրերն իրարից տարբեր են, որեւէ k ինդեքսի համար կարող է տեղի ունենալ $I_k = I_{k+1}$ հավասարությունը:

8.4.15 Խնդիր. Կառուցել նախորդ օրինակում հիշատակված $a_1, \dots, a_k, \dots \in R$ զույգ առ զույգ տարբեր տարրերի այնպիսի հաջորդականություն, որոնց համար կատարվում է $I_k = I_{k+1}$ հավասարությունը: *Յուցում.* $R = K[x_1, \dots, x_n]$ օղակում վերցնել իրարից տարբեր մի քանի $f_1, \dots, f_k$ բազմանդամներ: Հաջորդ $f_{k+1}, f_{k+2}, \dots$ բազմանդամնե-

րը կառուցել որպես առաջին k բազմանդամների գծային կոմբինացիաներ: Այս շղթան կայունանում է:

Պարզվում է, որ շատ օղակներում գոյություն չունեն անվերջ քանակությամբ տարբեր անդամներից բաղկացած իդեալների անվերջ աճող շղթաներ, այսինքն՝ դրանցում իդեալների յուրաքանչյուր աճող շղթա կայունանում է: Այս հատկությունը կոչվում է *իդեալների աճող շղթայի հատկություն* կամ *նյոտերյան հատկություն* (Էմմի Նյոտերի պատվին): Այդ հատկությանը բավարարող օղակը կոչվում է *նյոտերյան օղակ*:

8.4.16 Թեորեմ. *Կամայական R օղակ նյոտերյան է այն եւ միայն այն դեպքում, երբ նրա ցանկացած I իդեալ վերջավոր ծնված է:*

Ապացույց: Ենթադրենք R-ի ցանկացած I իդեալ վերջավոր ծնված է եւ R-ում տրված է կամայական (8.19) շղթան: Ցույց տանք, որ այդ շղթան կայունանում է: Սահմանենք $I = \bigcup_{k=1}^{\infty} I_k$ բազմությունը (մենք կարող ենք համարել, որ (8.19) շղթան անվերջ է, քանի որ վերջավորի դեպքում ապացույցն ակնհայտ է): 2.1.9 խնդրի օգնությամբ հեշտ է ստուգել, որ I-ն իդեալ է: Իսկապես, վերցնենք $a, b \in I$ եւ $c \in R$: Ըստ I-ի կառուցման՝ գոյություն ունեն k_1 եւ k_2 ինդեքսներ, որոնց համար $a \in I_{k_1}$ եւ $b \in I_{k_2}$: Ենթադրենք $k_1 \le k_2$: Քանի որ (8.19) շղթան աճող է, ապա $I_{k_1} \subseteq I_{k_2}$ եւ a, b տարրերը երկուսն էլ I_{k_2}-ից են: Քանի որ I_{k_2}-ն իդեալ է, ապա $a - b \in I_{k_2} \subseteq I$ եւ $ac,\ ca \in I_{k_2} \subseteq I$:

Քանի որ I-ն իդեալ է, այն ծնված է որոշ $a_1, \dots, a_k$ տարրերով: Դրանցից յուրաքանչյուրը պատկանում է որեւէ I_{k_i} իդեալի: k_i ինդեքսներից մեծագույնը նշանակենք k_0: Քանի որ շղթան աճող է, բոլոր $a_1, \dots, a_k$ տարրերն ընկած են I_{k_0} իդեալում: Ուրեմն՝ $I_{k_0} = I_{k_0+1} = \cdots = I$:

Այժմ ենթադրենք, որ R-ի ցանկացած շղթա կայունանում է, բայց R-ում կա մի այնպիսի I իդեալ, որը վերջավոր ծնված չէ: Վերցնենք R-ի ցանկացած a_1 տարր եւ նշանակենք $I_1 = \langle a_1 \rangle$: Քանի որ I-ն վերջավոր ծնված չէ, $I_1 \neq I$, այսինքն՝ գոյություն ունի որեւէ $a_2 \in I \backslash I_1$ տարր, եւ կարելի է դիտարկել I_1-ից խիստ մեծ $I_2 = \langle a_1, a_2 \rangle$ իդեալը: Եթե ինդուկցիայով արդեն սահմանված է $I_k = \langle a_1, \dots, a_k \rangle$ իդեալը, ապա կրկին $I_k \neq I$ եւ կարող ենք վերցնել որեւէ $a_{k+1} \in I \backslash I_k$ տարր եւ սահմանել I_k-ից խիստ մեծ $I_{k+1} = \langle a_1, \dots, a_k, a_{k+1} \rangle$ իդեալը: Ստացված իդեալների աճող շղթան երբեք չի կայունանում: Հակասություն: ■

Ապացուցված թեորեմից եւ Հիլբերտի թեորեմից բխում է.

8.4.17 Հետեւանք. K դաշտի վրա տրված $K[x_1,\dots,x_n]$ բազմանդամային օղակում իդեալների ցանկացած աճող շարք կայունանում է, այսինքն՝ $K[x_1,\dots,x_n]$-ը նյոտերյան օղակ է:

Այս հետեւանքը ցույց է տալիս, որ եթե 8.4.15 խնդրում վերցնենք $R = K[x_1,\dots,x_n]$, ապա որպես $f_1,\dots,f_k,\dots$ բազմանդամները կարելի է ընտրել ցանկացած բազմանդամների հաջորդականությունը. դրանցով ծնված իդեալների շղթան միշտ կայունանում է: 8.4.17 հետեւանքը մեզ պետք կգա նաեւ 8.6 պարագրաֆում Բուխբերգերի ալգորիթմի կառուցման մեջ:

8.5 Գրյոբների բազաներ

Ենթադրենք K դաշտի վրա տրված $K[x_1,\dots,x_n]$ բազմանդամային օղակում տրված է որեւէ $<$ մոնոմիալ կարգավորվածություն: $K[x_1,\dots,x_n]$ օդակի ոչ զրոյական I իդեալի համար $\mathrm{lt}I$-ով նշանակվում է I-ի բոլոր բազմանդամների (ըստ այդ կարգավորվածության) ավագ անդամների $\{\mathrm{lt}f \mid f \in I\}$ բազմությունը: Այդ բազմությամբ ծնված $\langle \mathrm{lt}I\rangle$ իդեալը կոչվում է I իդեալի *ավագ իդեալ* (նրա համար երբեմն մտցվում է հատուկ նշանակում՝ $\mathrm{in}I$ ըստ «initial ideal» անվանման):

Քանի որ միանդամը մոնոմիալից տարբերվում է միայն սկալյար արտադրիչով, ապա հասկանալի է, որ $\langle \mathrm{lt}I\rangle$ ավագ իդեալը մոնոմիալ իդեալ է:

Ըստ 8.4.12 Հիլբերտի թեորեմի՝ I իդեալի համար միշտ գոյություն ունեն վերջավոր քանակությամբ այնպիսի $g_1,\dots,g_s \in I$ բազմանդամներ, որ $\langle g_1,\dots,g_s\rangle = I$: Գրյոբների բազաների նկարագրումը հարմար է սկսել $\langle \mathrm{lt}I\rangle$ իդեալի եւ $g_1,\dots,g_s$ բազմանդամների ավագ գործակիցներով ծնված $\langle \mathrm{lt}g_1,\dots,\mathrm{lt}g_s\rangle$ իդեալի համեմատությունից: Քանի որ $\mathrm{lt}g_1,\dots,\mathrm{lt}g_s \in \mathrm{lt}I$, ապա

$$\langle \mathrm{lt}g_1,\dots,\mathrm{lt}g_s\rangle \subseteq \langle \mathrm{lt}I\rangle: \tag{8.21}$$

Պարզվում է, որ չնայած $\langle g_1,\dots,g_s\rangle = I$ հավասարության, (8.21)-ի երկու կողմերի միջեւ հավասարությունը միշտ չէ, որ տեղի ունի.

8.5.1 Օրինակ. $K[x,y]$ օղակում ընդունենք $grlex$ մոնոմիալ կարգավորվածությունը եւ դիտարկենք $g_1 = xy^2 + 3y^2 + 2x$ եւ $g_2 = x^2y + 3xy$ բազմանդամներով ծնված $I = \langle g_1, g_2\rangle$ իդեալը: Հեշտ է հաշվել, որ

$$x \cdot g_1 - y \cdot g_2 = x^2y^2 + 3xy^2 + 2x^2 - (x^2y^2 + 3xy^2) = 2x^2 \in I,$$

այսինքն՝ $\langle \mathrm{lt} I \rangle$ իդեալին պատկանում են ոչ միայն $\mathrm{lt} g_1 = xy^2$ եւ $\mathrm{lt} g_2 = x^2y$, այլեւ $\mathrm{lt}\, 2x^2 = 2x^2$ միանդամը, որը $\langle \mathrm{lt} g_1, \mathrm{lt} g_2 \rangle$ մոնոմիալ իդեալից չէ, քանի որ չի բաժանվում xy^2 եւ x^2y մոնոմիալներից ոչ մեկի վրա (տես 8.3.5 լեմման եւ նրա հետեւանքը): Այսինքն՝ $\langle \mathrm{lt} g_1, \mathrm{lt} g_2 \rangle$ իդեալը խիստ պարունակվում է $\langle \mathrm{lt} I \rangle$ իդեալի մեջ՝ չնայած այն բանին, որ $\langle g_1, g_2 \rangle = I$: Այս «անհամապատասխանության» պատճառն այն է, որ g_1 բազմանդամի $2x$ միանդամը I օղակում կատարվող գործողությունների եւ կրճատումների արդյունքում ազատվում է իրեն նախորդող (իրենից ավելի մեծ) միանդամներից, եւ $2x^2$ միանդամի կազմում հանդես է գալիս որպես մի նոր ավագ անդամ, որը $\langle \mathrm{lt} g_1, \mathrm{lt} g_2 \rangle$-ից չէ:

Հետագայում 8.5.1 օրինակի բազմանդամները մենք մի քանի անգամ օգտագործելու ենք Գրյոբների բազաների, Բուխբերգերի ալգորիթմի, Գրյոբների մինիմալ եւ բերված բազաների կառուցման քայլերի բացատրության համար[1]:

8.5.2 Խնդիր. Ենթադրենք $g_1 = x^2$ եւ $g_2 = xy + y^2$: Ցույց տալ, որ $\langle \mathrm{lt} g_1, \mathrm{lt} g_2 \rangle$ իդեալը խիստ փոքր է $\langle \mathrm{lt} I \rangle$ իդեալից, որտեղ $I = \langle g_1, g_2 \rangle$: *Յուցում*՝ տես 8.5.13 խնդիրը:

8.5.3 Վարժություն. Բերել այնպիսի $g_1, \dots, g_s$ բազմանդամների օրինակ, որոնց համար (8.22)-ում տեղի ունի $I = \langle g_1, \dots, g_s \rangle$ հավասարությունը:

8.5.4 Դիտողություն. Կարեւոր է նկատել, որ եթե անգամ (8.22)-ում խիստ անհավասարություն տեղի ունի, ապա գոյություն ունի I օղակի այնպիսի $h_1, \dots, h_t$ բազմանդամների բազմություն, որ $\langle \mathrm{lt} h_1, \dots, \mathrm{lt} h_1 \rangle = \langle \mathrm{lt} I \rangle$: Սա բխում է Դիքսոնի լեմմայից (կամ Հիլբերտի թեորեմից): Սա նաեւ նշանակում է, որ I օղակը ծնող բազմանդամների կամայական $g_1, \dots, g_s$ բազմություն կարելի է «լրացնել» վերջավոր քանակությամբ այնպիսի վեկտորներով, որ (8.21)-ը դառնա հավասարություն: Իսկապես, բավական է $\{g_1, \dots, g_s\}$-ին հերթով ավելացնել $h_1, \dots, h_t$ բազմանդամները:

Այժմ մենք կարող ենք տալ այս գլխի առանցքային սահմանումը.

8.5.5 Սահմանում. K դաշտի վրա տրված եւ կամայական մոնոմիալ կարգավորվածություն ունեցող $K[x_1, \dots, x_n]$ բազմանդամային օղակի ոչ զրոյական I իդեալի $G = \{g_1, \dots, g_s\}$ վերջավոր ենթաբազմությունը կոչվում է I-ի *Գրյոբների բազա*, եթե $\langle \mathrm{lt} g_1, \dots, \mathrm{lt} g_s \rangle = \langle \mathrm{lt} I \rangle$:

---

[1] Տես 8.5.8, 8.6.1, 8.6.5, 8.6.11, 8.7.1, 8.7.7, 8.7.9, 8.7.14, 8.9.11 օրինակները: Գրքի վրա աշխատելիս մենք իրականացրել ենք այս եւ մնացած օրինակների մանրամասն հաշվարկները: Դրանք էջեր են զբաղեցնում եւ տեղի խնայողության համար չեն ներառվել այս տպագիր տեքստի մեջ: Հաշվարկի ձեռագիր տարբերակները առկա են, սակայն Գրյոբների բազաներին ավելի դյուրին վարժվելու համար խորհուրդ ենք տալիս անձամբ կատարել նշված օրինակների բոլոր հաշվարկները:

Քանի որ զրոյական բազմանդամները կարելի է հեռացնել ծնիչ բազմություններից, պայմանավորվենք Գրյոբների բազաները համարել բաղկացած միայն ոչ զրոյական բազմանդամներից: Սա հարմար է այն իմաստով, որ հետագայում մենք հաճախակի ենք տարբեր բազմանդամներ բաժանելու Գրյոբների բազաների վրա, եւ ցանկալի է զրոյական բաժանարարներ չունենալ:

Համաձայն 8.5.4 դիտողության, յուրաքանչյուր I իդեալ ունի Գրյոբների բազա: Ըստ 8.5.1 օրինակի, եթե $g_1, \dots, g_s$ բազմանդամները ծնում են I-ն, ապա նրանց ավագ անդամները կարող են եւ I-ի Գրյոբների բազա չլինել, սակայն նրանց մի քանի բազմանդամ ավելացնելով՝ միշտ էլ կարելի է Գրյոբների բազա ստանալ:

Հիլբերտի թեորեմի ապացույցից բխում է.

8.5.6 Հետեւանք. Եթե $G = \{g_1, \dots, g_s\}$ բազմությունը I իդեալի Գրյոբների բազա է, ապա այն նաեւ I-ի ծնիչ է՝ $I = \langle g_1, \dots, g_s \rangle$:

Ապացույց: Կրկնենք Հիլբերտի թեորեմի ապացույցի վերջին մասը. ֆիքսենք $g_1, \dots, g_s$ բազմանդամների որեւէ դասավորություն, եւ կամայական $f \in I$ բազմանդամ բաժանենք դրա վրա՝ $f = q_1 \cdot g_1 + \cdots + q_s \cdot g_s + r$: Եթե $r = 0$, ապա արդեն իսկ ունենք $f \in I$: Իսկ եթե $r \neq 0$, ապա հակասություն ենք ստանում նույն եղանակով, ինչպես Հիլբերտի թեորեմի ապացույցում: ■

8.3.5 լեմմայից եւ Գրյոբների բազայի սահմանումից բխում է մի հետեւանք, որով հաճախ շատ հարմար է ստուգել, թե արդյո՞ք տվյալ բազմությունը Գրյոբների բազա է.

8.5.7 Հետեւանք. I իդեալի $G = \{g_1, \dots, g_s\}$ ենթաբազմությունը I-ի Գրյոբների բազա է այն եւ միայն այն դեպքում, երբ այդ իդեալի յուրաքանչյուր բազմանդամի ավագ անդամը բաժանվում է g_i բազմանդամերից որեւէ մեկի $\mathrm{lt} g_i$ ավագ անդամի վրա, $i = 1, \dots, s$:

8.5.8 Օրինակ. Այս հետեւանքից միանգամից բխում է, որ 8.5.1 օրինակի $g_1 = xy^2 + 3y^2 + 2x$ եւ $g_2 = x^2y + 3xy$ բազմանդամները $I = \langle g_1, g_2 \rangle$ իդեալի Գրյոբների բազա չեն. այդ իդեալի $2x^2$ բազմանդամի ավագ անդամը չի բավարարում 8.5.7 հետեւանքի պայմանին:

8.5.9 Օրինակ. $K[x_1, \dots, x_n]$ օղակում վերցնենք միանդամների կամայական վերջավոր $g_1, \dots, g_s$ բազմությունը: Այդ դեպքում $I = \langle g_1, \dots, g_s \rangle$ իդեալի Գրյոբների բազա է $G = \{g_1, \dots, g_s\}$ բազմությունը: Սա հեշտ է ստուգել՝ օգտվելով 8.3.5 լեմմայից:

Այժմ մենք կարող ենք Գրյոբների բազաների համար ստանալ այն օգտակար հատկությունը, որի մասին հիշատակեցինք նախորդ պարագրաֆի 8.4.11 դիտողության մեջ.

8.5.10 Թեորեմ. *Ենթադրենք K դաշտի վրա տրված $K[x_1, \dots, x_n]$ օղակում տրված է որևէ մոնոմիալ կարգավորվածություն, ըստ որի՝ օղակի ոչ զրոյական I իդեալն ունի $G = \{g_1, \dots, g_s\}$ Գրյոբների բազան: Այդ դեպքում կամայական $f \in K[x_1, \dots, x_n]$ բազմանդամի եւ G-ի տարրերի ցանկացած $g_1, \dots, g_s$ դասավորության դեպքում f-ը $g_1, \dots, g_s$ հաջորդականության վրա բաժանելիս ստացվում է միեւնույն r մնացորդը. գոյություն ունեն այնպիսի $q_1, \dots, q_s, r \in K[x_1, \dots, x_n]$ բազմանդամներ, որ $f = q_1 \cdot g_1 + \dots + q_s \cdot g_s + r$, որտեղ կամ $r = 0$, կամ էլ $r \neq 0$ եւ r-ի միանդամներից ոչ մեկը չի բաժանվում $\mathrm{lt} g_1, \dots, \mathrm{lt} g_s$ ավագ անդամների վրա: Ընդ որում, r-ն անկախ է G-ի տարրերի դասավորությունից:*

Ապացույց: Այն, որ որոնելի բաժանումը G-ի տարրերի ցանկացած $g_1, \dots, g_s$ դասավորության համար տեղի ունի, բխում է 8.4.3 թեորեմից: Ենթադրենք այդ տարրերի մի այլ՝ $g_{i_1}, \dots, g_{i_s}$ դասավորության համար ստացվել է

$$f = q'_1 \cdot g_{i_1} + \dots + q'_s \cdot g_{i_s} + r'$$

բաժանումը, որտեղ կամ $r' = 0$, կամ էլ $r' \neq 0$ եւ r'-ի միանդամներից ոչ մեկը չի բաժանվում $\mathrm{lt} g_{i_1}, \dots, \mathrm{lt} g_{i_s}$ ավագ անդամների վրա: Քանի որ բազմանդամների վերադասավորությունը չի փոխում դրանց ավագ անդամների բազմությունը, ապա վերջին կետը նշանակում է, որ r'-ի միանդամներից ոչ մեկը չի բաժանվում $\mathrm{lt} g_1, \dots, \mathrm{lt} g_s$ ավագ անդամների վրա: Իրարից հանելով երկու ներկայացումները՝ ստանում ենք

$$0 = f - f = \left[(q_1 \cdot g_1 + \dots + q_s \cdot g_s) - \left(q'_1 \cdot g_{i_1} + \dots + q'_s \cdot g_{i_s}\right)\right] - (r - r').$$

Հավասարության աջ մասում քառակուսի փակագծերի մեջ գտնվող արտահայտությունն ակնհայտորեն I իդեալից է: Ուրեմն, եթե $r \neq r'$, ապա $r - r'$ տարբերությունը I իդեալի ոչ զրոյական տարր է: Այդ տարբերության մեջ նման անդամների միացումը կատարվում է ըստ այն մոնոմիալների, որոնք համընկնում են r եւ r' բազմանդամների միանդամներում: Եթե անգամ որոշ միանդամներ կրճատվում են, պարզ է, որ $r - r'$ տարբերության մեջ կարող են մասնակցել միայն այն մոնոմիալները, որոնք մասնակցում են r-ի կամ r'-ի մեջ (նման անդամների միացման ժամանակ կարող են առաջանալ նոր գործակիցներ, բայց ոչ նոր մոնոմիալներ): $I^* = \langle \mathrm{lt} g_1, \dots, \mathrm{lt} g_s \rangle$ իդեալը մոնոմիալ իդեալ է, ուստի որեւէ միանդամ կարող է պատ-

կանել նրան, միայն երբ այն բաժանվում է $\mathrm{lt}g_1, \dots, \mathrm{lt}g_s$ միանդամներից որեւէ մեկի վրա (տես 8.3.5 լեմման եւ 8.3.6 հետեւանքը):

Մյուս կողմից, G-ն Գրյոբների բազա է, ուրեմն՝ $g_1, \dots, g_s$ բազմանդամներով ծընված իդեալի ցանկացած բազմանդամի ավագ անդամը պարտավոր է պատկանել I^* իդեալին եւ, ըստ վերն ասվածի, բաժանվել $\mathrm{lt}g_1, \dots, \mathrm{lt}g_s$ միանդամներից որեւէ մեկի վրա: Բայց, ըստ ընդհանուր մոնոմիալների մասին դիտողության, սա կնշանակեր, որ r-ի կամ r'-ի անդամներից մեկը նույնպես բաժանվում է $\mathrm{lt}g_1, \dots, \mathrm{lt}g_s$ միանդամներից որեւէ մեկի վրա: Ստացված հակասությունն ավարտում է թեորեմի ապացույցը: ■

Թեորեմից ստացվում է մի հետեւանք, որն արդեն հնարավորություն է տալիս լուծել իդեալին պատկանելության խնդիրը, եթե տվյալ իդեալի համար հայտնի է նրա Գրյոբների բազան: Վերհիշենք 8.4 պարագրաֆի նշանակումներից մեկը. եթե տրված է $g_1, \dots, g_s$ բազմանդամների ինչ-որ $G = (g_1, \dots, g_s)$ դասավորություն, ապա f բազմանդամն այդ հաջորդականության վրա բաժանելիս ստացվող r մնացորդը նշանակեցինք $r = f_G$: Եթե G-ն Գրյոբների բազա է, ապա ըստ 8.5.10 թեորեմի՝ բազմանդամների դասավորութունը մնացորդի վրա չի ազդում, եւ կարելի է դիտարկել f բազմանդամը G Գրյոբների բազայի վրա բաժանելիս ստացվող $r = f_G$ մնացորդը:

8.5.11 Հետեւանք. Ենթադրենք $K[x_1, \dots, x_n]$ օղակում տրված է նրա կամայական I ոչ զրոյական իդեալի որեւէ $G = \{g_1, \dots, g_s\}$ Գրյոբների բազան: Այդ դեպքում տրված $f \in K[x_1, \dots, x_n]$ բազմանդամը պատկանում է I-ին այն եւ միայն այն դեպքում, երբ f-ը G-ի վրա բաժանելիս ստացվող մնացորդը զրոյական է՝ $r = f_G = 0$:

Ապացույց: Եթե $f \in I$, ապա ըստ 2.2.12 թեորեմի՝ գոյություն ունեն այնպիսի $q_1, \dots, q_s \in K[x_1, \dots, x_n]$ բազմանդամներ, որ $f = q_1 \cdot g_1 + \dots + q_s \cdot g_s$: Այսինքն՝ f-ը տվյալ $g_1, \dots, g_s$ դասավորության վրա բաժանելիս ստացվում է զրոյական մնացորդ: Ըստ 8.5.10 թեորեմի՝ նույն $f_G = 0$ մնացորդը կստացվի նաեւ ցանկացած այլ դասավորության վրա բաժանելիս: ■

8.5.12 Օրինակ. Եթե I իդեալը տրված է K դաշտի վրա մեկ փոփոխականի $K[x]$ բազմանդամային օղակում, ապա այն գլխավոր իդեալների օղակ է ըստ 2.5.15 հետեւանքի. որեւէ $g = a_0x^n + \dots + a_n$ բազմանդամի համար ունենք $I = \langle g \rangle = gK[x]$: Համարենք, որ $I \neq 0$ եւ $g \neq 0$: Պարզ է, որ $\mathrm{lt}g = a_0x^n$: Քանի որ $gK[x]$ իդեալի բոլոր բազմանդամներն ունեն $g \cdot f$ տեսքը, որտեղ $f \in K[x]$, ապա $\langle \mathrm{lt}g \rangle$ ավագ իդեալը

բաղկացած է զրոյից եւ այնպիսի ոչ զրոյական միանդամներից, որոնց աստիճանները փոքր չեն n-ից: Այդ իդեալը ծնվում է ինչպես x^n մոնոմիալով, այնպես էլ $\mathrm{lt} g = a_0 x^n$ միանդամով ($a_0 \neq 0$): Ուստի $G = \{g\}$ բազմությունը I իդեալի Գրյոբների բազա է: Ըստ 8.5.10 թեորեմի՝ յուրաքանչյուր բազմանդամ g-ի վրա բաժանելիս ստացվում է միարժեքորեն որոշված մնացորդ (այսինքն՝ ստանում ենք $K[x]$ օղակի էվկլիդյան լինելու 2.5.1 սահմանումը): Այդ մնացորդը զրոյական է այն եւ միայն այն դեպքում, երբ բաժանվող բազմանդամը I իդեալից է:

Նկատենք, որ 8.5.10 թեորեմը կամ 8.5.11 հետեւանքը չեն նշանակում, թե $g_1, \dots, g_s$ բաժանարարների դասավորությունից անփոփոխ են նաեւ $q_1, \dots, q_s$ քանորդները: Դրանք կարող են փոփոխվել, եթե անգամ անփոփոխ է r-ը:

8.5.13 Խնդիր. Ցույց տալ, ոչ 8.5.2 խնդրի մեջ բերված $g_1 = x^2$ եւ $g_2 = xy + y^2$ բազմանդամների զույգը Գրյոբների բազա չէ իրենցով ծնված իդեալի համար (որպես մոնոմիալ կարգավորվածություն կարելի է վերցնել, ասենք, lex-ը): $f = x^2 y$ բազմանդամը բաժանել բազմանդամների նախ՝ g_1, g_2, ապա նաեւ՝ g_2, g_1 դասավորությունների վրա, եւ համեմատել արդյունքները (ինչպես հետո հեշտ կլինի ստուգել Բուխբերգերի հայտանիշով, այս զույգը Գրյոբների բազա դարձնելու համար պետք է դրան ավելացնել նաեւ $g_3 = y^3$ բազմանդամը): f-ը բաժանել նոր եռյակի g_1, g_2, g_3 եւ g_3, g_1, g_2 դասավորությունների վրա, համեմատել արդյունքները:

Գրյոբների բազաները մեզ թույլ են տալիս պատասխանել իդեալին պատկանելության խնդրին: Առայժմ պակասում է տվյալ I իդեալի համար Գրյոբների բազայի հաշվման էֆեկտիվ մեթոդը: Դա մենք կիրականացնենք Բուխբերգերի ալգորիթմի միջոցով:

8.6 Բուխբերգերի ալգորիթմը

Այս պարագրաֆում մենք կկառուցենք Բուխբերգերի ալգորիթմը, որի օգնությամբ կարելի է $K[x_1, \dots, x_n]$ օղակի իդեալների համար կառուցել Գրյոբների բազաներ: K դաշտի վրա տրված $K[x_1, \dots, x_n]$ բազմանդամային օղակում ֆիքսենք որեւէ մոնոմիալ կարգավորվածություն եւ վերցնենք f եւ g ոչ զրոյական բազմանդամները: Եթե նշանակենք

$$\mathrm{lt} f = \mathrm{lc} f \cdot \mathrm{lm} f = a_\alpha x^\alpha = a_\alpha x_1^{k_1} \cdots x_n^{k_n} \quad \text{եւ} \quad \mathrm{lt} g = \mathrm{lc} g \cdot \mathrm{lm} g = a_\beta x^\beta = a_\beta x_1^{l_1} \cdots x_n^{l_n}$$

ապա $\mathrm{lm}f$ եւ $\mathrm{lm}g$ ավագ մոնոմիալների ամենափոքր ընդհանուր բազմապատիկը կունենա հետեւյալ տեսքը՝

$$[\mathrm{lm}f, \mathrm{lm}g] = \left[x_1^{k_1}\cdots x_n^{k_n},\ x_1^{l_1}\cdots x_n^{l_n}\right] = x_1^{\max\{k_1,l_1\}}\cdots x_n^{\max\{k_n,l_n\}} \tag{8.22}$$

(սա $K[x_1,\dots,x_n]$ օղակի ֆակտորիալության պարզ հետեւանք է. տես 6.3 եւ 6.4 պարագրաֆները): (8.22) հավասարության աջ մասի

$$\mathrm{multideg}([\mathrm{lm}f, \mathrm{lm}g]) = (\max\{k_1,l_1\},\dots,\max\{k_n,l_n\})$$

աստիճանային վեկտորը նշանակելով γ՝ համառոտ գրենք՝ $[\mathrm{lm}f, \mathrm{lm}g] = x^\gamma$: Քանի որ x^γ-ն բաժանվում է $\mathrm{lt}f$ եւ $\mathrm{lt}g$ միանդամների վրա, կոռեկտ է դիտարկել $\frac{x^\gamma}{\mathrm{lt}f}$ եւ $\frac{x^\gamma}{\mathrm{lt}g}$ հարաբերությունները: Պարզ է, որ $\left(\frac{x^\gamma}{\mathrm{lt}f}\right)f$ բազմանդամը կստացվի f-ից հետեւյալ երկու քայլերով՝ նախ f-ը նորմավորում ենք (բաժանում ավագ գործակցի վրա), ապա f-ի ավագ մոնոմիալի յուրաքանչյուր $x_i^{k_i}$ արտադրիչ համեմատում ենք g-ի ավագ մոնոմիալի համապատասխան $x_i^{l_i}$ արտադրիչի հետ, $i = 1,\dots,n$: Եթե $k_i < l_i$, ապա նորմավորված f-ը բազմապատկում ենք $x_i^{l_i-k_i}$-ով: Արդյունքում $\left(\frac{x^\gamma}{\mathrm{lt}f}\right)f$ եւ $\left(\frac{x^\gamma}{\mathrm{lt}g}\right)g$ բազմանդամները կունենան միեւնույն ավագ անդամը:

Բուխբերգերի ալգորիթմում կարեւոր դեր են կատարելու *S-բազմանդամները*, որոնք տրված f, g ոչ զրոյական բազմանդամների համար սահմանվում են հետեւյալ կերպ՝

$$S(f,g) = \left(\frac{x^\gamma}{\mathrm{lt}f}\right)f - \left(\frac{x^\gamma}{\mathrm{lt}g}\right)g: \tag{8.23}$$

Այսպիսով, f, g զույգի համար S-բազմանդամը կառուցվում է այնպես, որ այդ զույգի $\mathrm{lt}f$ եւ $\mathrm{lt}g$ ավագ անդամները անպայման ներգրավվեն կրճատման մեջ: Մասնավորապես՝

$$\mathrm{multideg}\big(S(f,g)\big) < \mathrm{multideg}\left(\left(\frac{x^\gamma}{\mathrm{lt}f}\right)f\right): \tag{8.24}$$

8.6.1 Օրինակ. Հաշվենք 8.5.1 օրինակի բազմանդամների S-բազմանդամը (կրկին ըստ $grlex$ մոնոմիալ կարգավորվածության): Քանի որ $x^\gamma = x^2y^2$, ապա 8.5.1 օրինակի հաշվարկը պարզապես նշանակում է, որ $S(g_1,g_2) = 2x^2$:,

8.6.2 Վարժություն. Հաշվել S-բազմանդամը 8.5.2 խնդրի բազմանդամների զույգի համար:

8.6.3 Լեմմա. *Ենթադրենք $g_1,\dots,g_s \in K[x_1,\dots,x_n]$ բազմանդամների ավագ անդամներն ունեն միեւնույն աստիճանային վեկտորը, այսինքն՝ գոյություն ունի $\nu \in \mathbb{N}_0^n$,*

որ multideg $g_i = \nu$, $i = 1, \dots, n$: *Եթե ըստ* $a_1, \dots, a_s \in K$ *սկալյարների կազմված* $f = a_1 g_1 + \cdots + a_s g_s$ *գծային կոմբինացիայի* multideg f *աստիճանը փոքր է* ν*-ից (այսինքն, եթե կոմբինացիայի ավագ անդամը կրճատվում է), ապա* f*-ը կարելի է ներկայացնել* $S(g_i, g_j)$ *տեսքի* S*-բազմանդամների գծային կոմբինացիայի տեսքով,* $i, j = 1, \dots, n$*:*

Ըստ (8.24) գնահատականի, $S(g_i, g_j)$ տեսքի S-բազմանդամներից յուրաքանչյուրի աստիճանն ավելի փոքր է, քան ν-ն: Իսկ $a_1 g_1 + \cdots + a_s g_s$ գծային կոմբինացիայի յուրաքանչյուր գումարելու աստիճանը ստույգ ν է (առանց ընդհանրությունը խախտելու կարող ենք համարել, որ $a_1, \dots, a_s$ սկալյարները ոչ զրոյական են): Ուստի 8.6.3 լեմման պնդում է, որ եթե $a_1, \dots, a_s \in K$ սկալյարներն ընտրված են այնպես, որ $f = a_1 g_1 + \cdots + a_s g_s$ գումարում ավագ անդամի կրճատում է տեղի ունենում, ապա այդ կրճատմանը կարելի է հասնել «մի քայլ ավելի վաղ»՝ նախ անցնում ենք $S(g_i, g_j)$ տեսքի S-բազմանդամներին, որոնցում ν աստիճանի ավագ անդամներն արդեն իսկ կրճատված են, ապա f-ը ստանում ենք որպես մի քանի այդպիսի S-բազմանդամների գծային կոմբինացիա:

8.6.3 լեմմայի ապացույցը: g_i բազմանդամի ավագ գործակիցը նշանակենք d_i-ով, $i = 1, \dots, n$: Քանի որ multideg $f < \nu$, ապա նման անդամների միացումից հետո $a_1 g_1 + \cdots + a_s g_s$ գումարի առաջին սկալյար գործակիցը զրոյական կլինի՝

$$a_1 d_1 + \cdots + a_s d_s = 0: \tag{8.25}$$

Եթե h_i-ով նշանակենք g_i բազմանդամի $h_i = g_i / d_i$ նորմավորումը, ապա հեշտ է ստուգել, որ

$$S(g_i, g_j) = \left(\frac{x^\nu}{\mathrm{lt} g_i}\right) g_i - \left(\frac{x^\nu}{\mathrm{lt} g_j}\right) g_j = h_i - h_j: \tag{8.26}$$

Մյուս կողմից, հեշտ է հաշվել, որ

$$\begin{aligned} a_1 g_1 + \cdots + a_s g_s &= a_1 d_1 \cdot h_1 + \cdots + a_s d_s \cdot h_s \\ &= a_1 d_1 (h_1 - h_2) + (a_1 d_1 + a_2 d_2)(h_2 - h_3) + \cdots \\ &\quad + (a_1 d_1 + \cdots + a_{s-1} d_{s-1})(h_{s-1} - h_s) + (a_1 d_1 + \cdots + a_s d_s) h_s: \end{aligned}$$

Գումարելիներից ամենավերջինը զրոյական է ըստ (8.25) հավասարության: Իսկ մնացած գումարը իրենից ներկայացնում է S-բազմանդամների գծային կոմբինացիա ըստ (8.26)-ի: ■

$S(g_i, g_j)$ S-բազմանդամը, ինչպես $K[x_1, \dots, x_n]$-ի ցանկացած բազմանդամ, կարելի է բաժանել բազմանդամների $G = (g_1, \dots, g_s)$ հաջորդականությաւն վրա: Օգտագործելով ավելի վաղ մտցված նշանակումը՝ ստացվող մնացորդը նշանակենք

$S(g_i, g_j)_G$: Նախորդ լեմման օգտագործվում է հետեւյալ կարեւոր հայտանիշն ապացուցելու համար.

8.6.4 Թեորեմ (Բուխբերգերի հայտանիշը). *$K[x_1, \dots, x_n]$ օղակի I իդեալի $G = \{g_1, \dots, g_s\}$ ծնիչն այդ իդեալի Գրյոբների բազա է այն եւ միայն այն դեպքում, երբ ցանկացած $i, j = 1, \dots, s$ զույգի համար $S(g_i, g_j)$ S-բազմանդամը G-ի որեւէ $g_1, \dots, g_s$ դասավորության վրա բաժանելիս ստացվող $S(g_i, g_j)_G$ մնացորդը զրոյական է:*

Ապացույց: $S(g_i, g_j)$-ն պատկանում է I իդեալին: Եթե G-ն Գրյոբների բազա է, ապա $S(g_i, g_j)_G = 0$ ըստ 8.5.11 հետեւանքի:

Բավարարության ապացույցի համար վերցնենք կամայական $f \in I$ բազմանդամ եւ ցույց տանք, որ եթե ցանկացած $i, j = 1, \dots, s$ զույգի համար $S(g_i, g_j)_G = 0$, ապա $\mathrm{lt} f \in \langle \mathrm{lt} g_1, \dots, \mathrm{lt} g_s \rangle$:

Քանի որ $\{g_1, \dots, g_s\}$ ենթաբազմությունը I-ի ծնիչ է, ապա ըստ 2.2.12 թեորեմի՝ գոյություն ունեն այնպիսի $r_i \in K[x_1, \dots, x_n]$ բազմանդամներ, որ

$$f = \sum_{i=1}^{t} g_i r_i: \tag{8.27}$$

Քանի որ նման անդամների միացումը կատարվում է ըստ հավասար մոնոմիալներ ունեցող միանդամների, պարզ է, որ (8.27) հավասարության ձախ կողմի f բազմանդամի $\mathrm{multideg}\, f$ աստիճանը չի գերազանցում աջ կողմի $g_i r_i$ բազմանդամների $\mathrm{multideg}(g_i r_i)$ աստիճանների μ մաքսիմումը՝

$$\mathrm{multideg}\, f \le \mu = \max\{\mathrm{multideg}(g_i r_i) \mid i = 1, \dots, t\}: \tag{8.28}$$

Նկատենք, որ եթե (8.28) տողում հավասարություն տեղի ունենա, ապա թեորեմի ապացույցը դրանով կավարտվի: Իրոք, եթե որեւէ $i = 1, \dots, t$ ինդեքսի համար ունենք $\mathrm{multideg}\, f = \mathrm{multideg}(g_i r_i)$, ապա f եւ $g_i r_i$ բազմանդամների ավագ անդամներն իրարից տարբերվում են ոչ զրոյական սկալյար արտադրիչով, ուստի $\mathrm{lt} f$-ը բաժանվում է $\mathrm{lt}(g_i r_i)$-ի վրա: Բայց $\mathrm{lt}(g_i r_i)$-ն էլ բաժանվում է $\mathrm{lt} g_i$-ի վրա: Ուստի

$$\mathrm{lt} f \in \langle \mathrm{lt} g_i \rangle \subseteq \langle \mathrm{lt} g_1, \dots, \mathrm{lt} g_s \rangle:$$

Ցույց տանք, որ եթե $\mathrm{multideg}\, f < \mu$, ապա, (8.27) հավասարության աջ մասում փոփոխություններ կատարելով, կարելի է իջեցնել μ արժեքը: Նախ կարելի է երկու խմբերի բաժանել $g_i r_i$, $i = 1, \dots, t$, գումարելիները. վերադասավորենք դրանք՝ նախ գրելով ամենաբարձր μ աստիճանի գումարելիները: Եթե ենթադրենք, որ դրանք m հատ են, կունենանք

$$f = \sum_{i=1}^{m} g_i r_i + \sum_{i=m+1}^{t} g_i r_i = \sum_{i=1}^{m} g_i \mathrm{lt} r_i + \sum_{i=1}^{m} g_i (r_i - \mathrm{lt} r_i) + \sum_{i=m+1}^{t} g_i r_i: \tag{8.29}$$

Այս հավասարությունների երկրորդ տողի գումարները խմբավորել ենք այնպես, որ ամենաբարձր աստիճանի գումարելիները կուտակվեն միայն առաջին գումարի մեջ, որը պայմանավորվենք նշանակել Γ: Քանի որ $\mathrm{multideg}\, r_i = \mathrm{multideg}(\mathrm{lt} r_i)$, ապա Γ-ի յուրաքանչյուր գումարելու համար $\mathrm{multideg}(g_i \mathrm{lt} r_i) = \mu$: Երկրորդ գումարի գումարելիների աստիճանները խիստ փոքր են μ-ից, քանի որ $r_i - \mathrm{lt} r_i$ բազմանդամի աստիճանը r_i-ի աստիճանից խիստ փոքր է: Իսկ վերջին գումարի մեջ $g_i r_i$ գումարելիների աստիճանները խիստ փոքր են μ-ից ըստ կառուցման:

Քանի որ $\mathrm{multideg}\, f < \mu$ եւ քանի որ (8.29) հավասարությունների երկրորդ տողի վերջին երկու գումարներում մասնակցում են միայն μ-ից ցածր աստիճանի բազմանդամներ, ապա (8.27) հավասարությունը կարող է կատարվել միայն, երբ μ աստիճանի գումարելիներից բաղկացած Γ գումարում տեղի է ունենում կրճատում՝ $\mathrm{multideg}(\Gamma) < \mu$: Ըստ 8.6.3 լեմմայի՝ սա նշանակում է, որ Γ գումարը կարելի է արտահայտել $g_i \mathrm{lt} r_i$ տեսքի ($i = 1, \dots, m$) բազմանդամների որեւէ S-բազմանդամների գծային կոմբինացիայի միջոցով: Ըստ (8.23) սահմանման կառուցենք դրանցից որեւէ մեկը՝

$$S\big(g_i \mathrm{lt} r_i, g_j \mathrm{lt} r_j\big) = \frac{x^{\mu}}{\mathrm{lt}(g_i \mathrm{lt} r_i)} \cdot g_i \mathrm{lt} r_i - \frac{x^{\mu}}{\mathrm{lt}\big(g_j \mathrm{lt} r_j\big)} \cdot g_j \mathrm{lt} r_j: \tag{8.30}$$

Աջ կողմի համարիչներում (8.23) բանաձեւի x^{γ}-ի փոխարեն այստեղ մասնակցում է x^{μ}, քանի որ բոլոր $\mathrm{lt}(g_i \mathrm{lt} r_i)$ արտադրյալների աստիճանը μ է: Պարզ է, որ $\mathrm{lt} r_i$ եւ $\mathrm{lt} r_j$ միանդամների գործակիցները ($\mathrm{lc}\, r_i$ եւ $\mathrm{lc}\, r_j$ սկալյարները) որեւէ ազդեցություն չեն ունենում այս S-բազմանդամի վրա, քանի որ տարբերության մեջ մասնակցող բազմանդամները նորմավորվում են: Մի փոքր այլ է $\mathrm{lm} r_i$ եւ $\mathrm{lm} r_j$ մոնոմիալների դերը: $g_i \mathrm{lt} r_i$ եւ $g_j \mathrm{lt} r_j$ արտադրյալներն ունեն միեւնույն x^{μ} ավագ մոնոմիալը: Իսկ g_i եւ g_j բազմանդամների S-բազմանդամը կազմելիս g_i-ն եւ g_j-ն բազմապատկվում են այնպիսի «օժանդակ» մոնոմիալներով, որ երկուսի արտադրյալների ավագ մոնոմիալները հավասարվեն: Քանի որ այդ ճանապարհով ստացվում է նման հնարավոր ավագ մոնոմիալներից փոքրագույնը, ապա

$$S\big(g_i \mathrm{lt} r_i, g_j \mathrm{lt} r_j\big) = x^{\mu_{ij}} \cdot S\big(g_i, g_j\big),$$

որտեղ $x^{\mu_{ij}}$-ն x^{μ}-ի որեւէ բաժանարար է: Այսպիսով, Γ գումարը վերլուծվում է

$$\Gamma = \sum_{c_{ij} \in K} c_{ij} \cdot x^{\mu_{ij}} \cdot S(g_i, g_j) \tag{8.31}$$

գծային կոմբինացիայի, որտեղ $c_{ij} \in K$, իսկ յուրաքանչյուր գումարելու աստիճանը խիստ փոքր է μ-ից:

Ըստ թեորեմի ենթադրության՝ յուրաքանչյուր $S(g_i, g_j)$ S-բազմանդամը $g_1, \dots, g_s$ հաջորդականության վրա բաժանելիս ստանում ենք $S(g_i, g_j)_G = 0$ մնացորդը: Նշանակում է՝ ինչ-որ $l_{ijk} \in K[x_1, \dots, x_n]$ բազմանդամների (բաժանման քանորդների) համար

$$S(g_i, g_j) = \sum_k l_{ijk} \cdot g_k,$$

ընդ որում, շնորհիվ 8.4.4 հետեւանքի, $\operatorname{multideg}(l_{ijk} \cdot g_k) \le \operatorname{multideg} S(g_i, g_j)$: Հետեւաբար նաեւ՝

$$\operatorname{multideg}(c_{ij} \cdot x^{\mu_{ij}} \cdot l_{ijk} \cdot g_k) \le \operatorname{multideg}\left(c_{ij} \cdot x^{\mu_{ij}} \cdot S(g_i, g_j)\right) < \mu:$$

Ուրեմն, եթե $S(g_i, g_j)$ բազմանդամի վերջին ներկայացումը տեղադրենք (8.31) տողում եւ ստացվածն էլ տեղադրենք (8.29) հավասարությունների մեջ, ապա կունենանք f բազմանդամի մի նոր ներկայացում $f = \sum_{i=1}^{u} g_i w_i$ տեսքով, որտեղ $w_i \in K[x_1, \dots, x_n]$ եւ յուրաքանչյուր գումարելու աստիճանը խիստ փոքր է μ-ից՝ $\operatorname{multideg}(g_i w_i) < \mu,\ i = 1, \dots, u$:

Ստացված ներկայացումը սկզբնական (8.27) ներկայացումից տարբերվում է նրանով, որ դրա բոլոր $g_i w_i$ գումարելիների աստիճանները խիստ փոքր են μ-ից: Եթե $\max\{\operatorname{multideg}(g_i w_i) \mid i = 1, \dots, u\} = \operatorname{multideg} f$, ապա թեորեմի ապացույցը կավարտվի նույն քայլերով, որ կիրառեցինք ապացույցի սկզբում (8.27) ներկայացման համար: Իսկ եթե $g_i w_i$ գումարելիներից գոնե մեկի աստիճանը դեռեւս մեծ է f-ի աստիճանից, ապա կրկնենք ապացույցի քայլերը եւ ստանանք (8.29) տեսքի մի նոր վերլուծություն էլ ավելի փոքր աստիճանի գումարելիներով:

Քանի որ $K[x_1, \dots, x_n]$-ի վրա քննարկվող կարգավորվածությունը մոնոմիալ է, ապա այն նաեւ լիովին կարգավորվածություն է, եւ ապացույցի քայլերն անվերջ անգամ կրկնվել չեն կարող: Ինչ-որ քայլում կունենանք (8.27) տեսքի մի ներկայացում, որի ամենամեծ գումարելու աստիճանը $\operatorname{multideg} f$ է: ■

8.6.5 Օրինակ. Վերադառնալով 8.5.1 եւ 8.6.1 օրինակներին՝ տեսնում ենք, որ 8.6.1 օրինակում մենք փաստորեն ստուգել ենք, որ g_1, g_2 բազմանդամների զույգը Գրյոբների բազա չէ: Իսկապես, մենք ստացել ենք, որ $S(g_1, g_2) = 2x^2$: Մյուս կողմից,

$\mathrm{lt}(2x^2) = 2x^2$ ավագ անդամը չի բաժանվում $\mathrm{lt}g_1 = xy^2$ եւ $\mathrm{lt}g_2 = x^2y$ ավագ անդամներից ոչ մեկի վրա: Ուրեմն՝ $S(g_1, g_2)$-ը g_1, g_2 զույգի վրա բաժանելիս կստացվի $r = S(g_1, g_2)_{(g_1,g_2)} = 2x^2 \neq 0$ ոչ զրոյական մնացորդը: Ըստ Բուխբերգերի հայտանիշի՝ g_1, g_2 զույգը Գրյոբների բազա չէ:

8.6.6 Վարժություն. Բուխբերգերի հայտանիշի օգնությամբ ստուգել, թե արդյո՞ք Գրյոբների բազա է 8.5.2 խնդրի բազմանդամների զույգը:

Բուխբերգերի հայտանիշը առանձնապես հեշտ է կիրառել երկու բազմանդամներից կազմված համակարգերի համար, քանի որ անհրաժեշտ է ստուգել միայն մեկ հատ S-բազմանդամ:

8.6.7 Վարժություն. Կառուցել երկու բազմանդամից բաղկացած Գրյոբների բազա:

8.6.8 Վարժություն. Կառուցել երկու բազմանդամից բաղկացած համակարգ, որը Գրյոբների բազա չէ:

Ենթադրենք տրված է բազմանդամների որեւէ $G = (g_1, \dots, g_s)$ հաջորդականություն (եթե G-ն Գրյոբների բազա է, բազմանդամների դասավորությունը ֆիքսելը պարտադիր չէ, բայց ընդհանուր դեպքում դա անհրաժեշտ է): Տրված r բազմանդամը G-ի ամենավերջում ավելացնելով՝ ստացվող $(g_1, \dots, g_s, r)$ հաջորդականությունը համառոտության համար նշանակենք $G + r$:

8.6.9 Լեմմա. *Ենթադրենք $f \in K[x_1, \dots, x_n]$ բազմանդամը $G = (g_1, \dots, g_s)$ հաջորդականության վրա բաժանելիս ստացվող մնացորդն է $f_G = r$: Այդ դեպքում f-ը $G + r$ հաջորդականության վրա բաժանելիս ստացվում է զրոյական մնացորդ՝ $f_{G+r} = 0$:*

Ապացույց: Անկյունով բաժանման պրոցեսի ամեն քայլում (տես 8.4 պարագրաֆը) կամ ընթացիկ f_i բազմանդամի ավագ անդամը բաժանվում է բաժանարարներից մեկի ավագ անդամի վրա (եւ այդ դեպքում համապատասխան կրճատման միջոցով անցնում ենք հաջորդ f_{i+1} ընթացիկ բազմանդամին), կամ էլ բաժանում տեղի չի ունենում, եւ ընթացիկ f_i բազմանդամը ճեղքվում է երկու մասի (նրա $\mathrm{lt}f_i$ ավագ անդամը միացվում է մնացորդին, եւ մենք պրոցեսը շարունակում ենք $f_{i+1} = f_i - \mathrm{lt}f_i$ ընթացիկ բազմանդամի համար):

Համեմատենք, թե ինչ կստացվի f բազմանդամը $(g_1, \dots, g_s)$ եւ $(g_1, \dots, g_s, r)$ հաջորդականությունների վրա անկյունով բաժանելիս: Բաժանման առաջին մի քանի քայլերում մենք կարող ենք այնպիսի ընթացիկ f_i բազմանդամների հանդիպել, որ $\mathrm{lt}f_i$-ն բաժանվի $\mathrm{lt}g_1, \dots, \mathrm{lt}g_s$ ավագ անդամներից որեւէ մեկի վրա: Այդ դեպքում բա-

ժանման պրոցեսը միանման է ընթանում թե $(g_1, \dots, g_s)$ եւ թե $(g_1, \dots, g_s, r)$ հաջորդականությունների վրա բաժանելիս: r բաժանարարը այդ քայլերի վրա չի ազդում:

Ենթադրենք հասել ենք այն առաջին f_i-ին, որի համար $\mathrm{lt} f_i$-ն չի բաժանվում $\mathrm{lt} g_1, \dots, \mathrm{lt} g_s$ ավագ անդամներից ոչ մեկի վրա: Այդ դեպքում $g_1, \dots, g_s$ հաջորդականության վրա բաժանելիս $\mathrm{lt} f_i$-ն տեղափոխվում է մնացորդների r սյունակ, իսկ $(g_1, \dots, g_s, r)$ հաջորդականության վրա բաժանելիս $\mathrm{lt} f_i$-ն բաժանվում է $\mathrm{lt} r$-ի վրա (պարզ է, որ $\mathrm{lt} r = \mathrm{lt} f_i$, ընդ որում, r-ը կարող է ունենալ $\mathrm{lt} f_i$-ից բացի էլի մի քանի անդամներ): Ուստի որպես q_{s+1} քանորդ վերցնում ենք $q_{s+1} = 1$ արժեքը եւ անցնում $f_{i+1} = f_i - r$ բազմանդամին: Այս քայլում f_i-ից հանվում է ոչ միայն $\mathrm{lt} f_i$ միանդամը, այլ r-ի բոլոր միանդամները: Նկատենք, որ ըստ r-ի կառուցման, այդ միանդամներից ոչ մեկը չի բաժանվում $\mathrm{lt} g_1, \dots, \mathrm{lt} g_s$ ավագ անդամներից որեւէ մեկի վրա, այսինքն, երբ հաջորդ քայլում մենք ստուգենք, թե արդյո՞ք $\mathrm{lt} f_{i+1}$ ավագ անդամը բաժանվում է $\mathrm{lt} g_1, \dots, \mathrm{lt} g_s$ ավագ անդամների վրա, ապա դա կախված չի լինի r-ի այն միանդամներից, որոնք հանվել են f_i-ից: Բաժանման մնացած բոլոր քայլերի ընթացքում մենք հերթական f_{i+j} բազմանդամի ավագ անդամը միշտ էլ կկարողանանք բաժանել $\mathrm{lt} g_1, \dots, \mathrm{lt} g_s$ ավագ անդամներից որեւէ մեկի վրա: ■

Հավաքված փաստերը մեզ արդեն հնարավորություն են տալիս ստանալ *Բուխբերգերի ալգորիթմը*, որով կարելի է Գրյոբների բազա կառուցել K դաշտի վրա տրված $K[x_1, \dots, x_n]$ բազմանդամային օղակի ցանկացած $I = \langle g_1, \dots, g_s \rangle$ իդեալի համար: Նկատենք, որ ըստ Հիլբերտի թեորեմի, $K[x_1, \dots, x_n]$ օղակի ցանկացած I իդեալ վերջավոր ծնված է եւ ուստի, իրոք, ունի նշված $I = \langle g_1, \dots, g_s \rangle$ ներկայացումը:

Եթե g_i բազմանդամներից գոնե մեկը ոչ զրոյական է, ապա I իդեալը նույնպես ոչ զրոյական է: Այսինքն՝ $I = \{0\}$ դեպքը հնարավոր է միայն, երբ բոլոր ծնիչները զրոյական են: Այս տրիվիալ դեպքը բացառենք մեր քննարկումներից եւ ենթադրենք, որ I-ն զրոյական չէ եւ բոլոր g_i բազմանդամները նույնպես ոչ զրոյական են, $i = 1, \dots, s$:

Ֆիքսենք ծնիչի բազմանդամների որեւէ $G = (g_1, \dots, g_s)$ հաջորդականություն: Ինդեքսների որեւէ $i, j = 1, \dots, s$ զույգի համար (8.23) բանաձեւով հաշվենք $S(g_i, g_j)$ բազմանդամը եւ անկյունով բաժանենք այն G-ի վրա: Եթե ստացված $r_{ij} = S(g_i, g_j)_G$ մնացորդները բոլորը զրոյական են, ապա G-ն Գրյոբների բազա է ըստ 8.6.4 Բուխբերգերի հայտանիշի: Իսկ եթե տվյալ i, j զույգի համար $r_{ij} \neq 0$, ապա դիտարկենք $G + r_{ij}$ հաջորդականությունը: Ըստ 8.6.9 լեմմայի՝ $S(g_i, g_j)$-ը $G + r_{ij}$ հաջորդականության վրա բաժանելիս ստացվող մնացորդը զրոյական է՝

$$S(g_i, g_j)_{G+r_{ij}} = 0:$$

Եթե G-ն փոխարինենք $G + r_{ij}$ հաջորդականությամբ, ապա բազմանդամների նույն (g_i, g_j) զույգն այժմ արդեն կբավարարի Բուխբերգերի հայտանիշում նշված պայմանին: Մյուս կողմից, քանի որ r_{ij}-ն պատկանում է I իդեալին, ապա G-ով ծնված իդեալն անփոփոխ է մնացել՝ $\langle G\rangle = I$:

Կրկնենք քայլը՝ (g_i, g_j) զույգի բազմանդամներն այժմ վերցնելով նոր G հաջորդականությունից (ընդ որում, g_i, g_j բազմանդամներից որեւէ մեկը կարող է հավասար լինել նախորդ քայլում ստացած մնացորդին): Եթե հայտնաբերվի մի նոր i, j զույգ, որի համար $r_{ij} = S(g_i, g_j)_G \neq 0$, ապա այս մնացորդը եւս վերջից ավելացնենք G-ին: Ընդ որում, պարզ է, որ նախորդ քայլում արդեն զրոյացված մնացորդը կշարունակի զրոյական մնալ այս քայլից հետո եւս (հեշտ է ստուգել, որ եթե անկյունով բաժանման ալգորիթմում որեւէ բազմանդամ ինչ-որ հաջորդականության վրա բաժանելիս ստացվում է զրոյական մնացորդ, ապա այդ հաջորդականության վերջից եւս մի բաժանարար ավելացնելով՝ մենք դարձյալ կստանանք զրոյական մնացորդ):

Շարունակենք այս պրոցեսը, քանի դեռ հանդիպում են ոչ զրոյական r_{ij} բաժանարարներ: Ամեն քայլում մենք, մի կողմից, եւս մի բազմանդամ ենք ավելացնում G-ին, մյուս կողմից, զրոյացնում ենք $S(g_i, g_j)_G$ մնացորդը: Ընդ որում, ամեն քայլում G-ն մեծացնելով՝ մենք խիստ մեծացնում ենք G-ի բազմանդամների ավագ անդամներով ծնված $\langle \mathrm{lt} g \mid g \in G\rangle$ իդեալը: Իսկապես, այդ իդեալը մոնոմիալ է, իսկ ըստ 8.3.5 լեմմայի՝ որեւէ բազմանդամ պատկանում է մոնոմիալ իդեալին միայն, երբ նրա բոլոր միանդամները բաժանվում են այդ իդեալը ծնող մոնոմիալների վրա: Մեր դեպքում ամեն քայլում G-ին ավելացվում է այնպիսի մի r_{ij} բազմանդամ, որի ոչ մի անդամ *չի բաժանվում* G-ի բազմանդամների ավագ անդամներից որեւէ մեկի վրա (ուստի եւ՝ ավագ մոնոմիալներից ոչ մեկի վրա): Ուրեմն՝ ամեն քայլում $\langle \mathrm{lt} g \mid g \in G\rangle$ իդեալը խիստ մեծանում է:

Եթե այս պրոցեսն անվերջ շարունակվեր, մենք կստանայինք $K[x_1, \dots, x_n]$ օղակի իդեալների խիստ աճող անվերջ շղթա: Սակայն, ըստ Հիլբերտի թեորեմի 8.4.17 հետեւանքի, $K[x_1, \dots, x_n]$ օղակի իդեալների յուրաքանչյուր աճող շղթա կայունանում է: Սա նշանակում է, որ ինչ-որ քայլում մենք կստանանք այնպիսի G հաջորդականություն, որի ցանկացած g_i, g_j անդամների համար $r_{ij} = S(g_i, g_j)_G = 0$: Այսինքն՝ ըստ 8.6.4 Բուխբերգերի հայտանիշի, կստանանք G Գրյոբների բազան: Եթե պայմանավորվենք $\mathcal{S}$-ով նշանակել տվյալ պահին քննարկվող բազմանդամների զույգերի (g_i, g_j) բազմությունը, ապա պարզ է, որ պրոցեսի առաջին քայլում կունե-

նանք $\mathcal{S} = \{(g_i, g_j) \mid 1 \le i < j \le s\}$, իսկ վերջում՝ $\mathcal{S} = \emptyset$: Այսպիսով մենք կառուցեցինք հետեւյալ ալգորիթմը.

8.6.10 Ալգորիթմ (Գրյոբների բազայի կառուցման Բուխբերգերի ալգորիթմը). K դաշտի վրա տրված $K[x_1, \dots, x_n]$ բազմանդամային օղակում ունենք $g_1, \dots, g_s$ ոչ զրոյական բազմանդամներով ծնված $I = \langle g_1, \dots, g_s \rangle$ իդեալը: Հաշվել I իդեալի որեւէ G Գրյոբների բազա:

1. Ֆիքսելով $g_1, \dots, g_s$ բազմանդամների որեւէ դասավորություն՝ սահմանենք $G = (g_1, \dots, g_s)$ հաջորդականությունը:

2. Սահմանենք բազմանդամների զույգերի $\mathcal{S} = \{(g_i, g_j) \mid 1 \le i < j \le s\}$ բազմությունը:

3. Քանի դեռ $\mathcal{S} \neq \emptyset$

4. ընտրենք որեւէ (g_i, g_j) զույգ $\mathcal{S}$-ից;

5. վերագրենք $\mathcal{S} = \mathcal{S} \setminus \{(g_i, g_j)\}$;

6. նշանակենք $x^\nu = [\mathrm{lm} g_i, \mathrm{lm} g_j]$ (g_i, g_j բազմանդամների ավագ մոնոմիալների ամենափոքր ընդհանուր բազմապատիկը);

7. նշանակենք $S(g_i, g_j) = \left(\frac{x^\nu}{\mathrm{lt} g_i}\right) g_i - \left(\frac{x^\nu}{\mathrm{lt} g_j}\right) g_j$;

8. $S(g_i, g_j)$-ը բաժանենք G-ի վրա եւ մնացորդը նշանակենք $r = S(g_i, g_j)_G$;

9. եթե $r \neq 0$

10. G հաջորդականությանը վերջից ավելացնենք r բազմանդամը;

11. վերագրենք $\mathcal{S} = \mathcal{S} \cup \{(r, g) \mid g \in G\}$:

12. Դուրս գրենք G հաջորդականությունը:

8.6.11 Օրինակ. Վերադառնանք 8.5.1 օրինակի բազմանդամներին: 8.6.5 օրինակում մենք Բուխբերգերի հայտանիշով արդեն ստուգել ենք, որ $g_1 = xy^2 + 3y^2 + 2x$ եւ $g_2 = x^2y + 3xy$ զույգը Գրյոբների բազա չէ: Որպես սկզբնական հաջորդականություն վերցնենք $G = (g_1, g_2)$: Քանի որ արդեն ստացել ենք $S(g_1, g_2)_G = 2x^2 \neq 0$, ապա նշանակենք $g_3 = 2x^2$ եւ անցնենք $G = (g_1, g_2, g_3)$ հաջորդականությանը: Այժմ արդեն $S(g_1, g_2)_G = 0$: Հաշվենք

$$S(g_1, g_3) = xg_1 - \frac{1}{2}y^2 g_3 = x^2y^2 + 3xy^2 + 2x^2 - x^2y^2 = 3xy^2 + 2x^2:$$

Անկյունով բաժանելով $S(g_1, g_3)$-ը G-ի վրա՝ ստանում ենք

$$S(g_1, g_3) = 3g_1 + 0g_2 + 1g_3 + (-9y^2 - 6x):$$

Նշանակենք $g_4 = -9y^2 - 6x$ եւ անցնենք $G = (g_1, g_2, g_3, g_4)$ հաջորդականությանը: Ինչպես նշեցինք ալգորիթմի կառուցման ընթացքում, ըստ այս նոր G-ի, զրոյական կլինի ոչ միայն $S(g_1, g_3)_G$ մնացորդը, այլեւ նախորդ քայլի $S(g_1, g_2)_G$ մնացորդը: Պայմանավորվենք մնացած քայլերում այլեւս չհիշատակել արդեն զրոյացված մնացորդները, քանի որ դրանք շարունակում են զրոյական մնալ նոր բաժանարարների ավելացումից հետո եւս: Հաշվենք

$$S(g_1, g_4) = g_1 - \frac{1}{-9}xg_4 = xy^2 + 3y^2 + 2x - xy^2 - \frac{2}{3}x^2 = -\frac{2}{3}x^2 + 3y^2 + 2x$$

(նկատենք, որ անդամների կրճատումից հետո մենք նաեւ վերադասավորել ենք մնացած միանդամները ըստ $grlex$ կարգավորվածության): Բաժանելով $S(g_1, g_4)$-ը G-ի վրա՝ ստանում ենք

$$S(g_1, g_4) = 0g_1 + 0g_2 - \frac{1}{3}g_3 - \frac{1}{3}g_4 + 0,$$

Այսինքն՝ այս քայլում $S(g_1, g_4)_G = 0$ եւ նոր ծնիչ ավելացնելու հարկ չկա: Հաշվենք

$$S(g_2, g_3) = g_2 - \frac{1}{2}yg_3 = x^2y + 3xy - x^2y = 3xy:$$

Բաժանելով $S(g_2, g_3)$-ը G-ի վրա՝ ստանում ենք

$$S(g_2, g_3) = 0g_1 + 0g_2 + 0g_3 + 0g_4 + S(g_2, g_3) = 3xy,$$

քանի որ $3xy$-ն արդեն իսկ չի բաժանում g_1, g_2, g_3, g_4 բազմանդամներից ոչ մեկի ավագ անդամը: Նշանակենք $g_5 = 3xy$ եւ անցնենք $G = (g_1, g_2, g_3, g_4, g_5)$ հաջորդականությանը: Սա վերջին հավելումն է G-ին, քանի որ մնացած բոլոր հաշվումներում ստացվում են միայն զրոյական մնացորդներ: Իսկապես,

$$S(g_1, g_5) = g_1 - \frac{1}{3}yg_5 = xy^2 + 3y^2 + 2x - xy^2 = 3y^2 + 2x:$$

Բաժանելով $S(g_1, g_5)$-ը G-ի վրա՝ ստանում ենք

$$S(g_1, g_5) = 0g_1 + 0g_2 + 0g_3 - \frac{1}{3}g_4 + 0g_5 + 0:$$

Այնուհետեւ

$$S(g_2, g_5) = g_1 - \frac{1}{3}xg_5 = x^2y + 3xy - x^2y = 3xy:$$

$S(g_2, g_5)$-ը G-ի վրա բաժանելը հեշտ է, քանի որ $3xy = g_5$: Ուստի եւ $S(g_2, g_5)_G = 0$: Հաջորդ քայլում

$$S(g_2,g_4)=yg_2-\frac{1}{-9}x^2g_4=x^2y^2+3xy^2-x^2y^2-\frac{2}{3}x^3=-\frac{2}{3}x^3+3xy^2$$

(կրճատումից հետո վերադասավորել ենք միանդամները ըստ $grlex$-ի)։ Բաժանելով $S(g_2,g_4)$-ը G-ի վրա՝ ստանում ենք

$$S(g_1,g_5)=3g_1+0g_2+\left(-\frac{1}{3}x+1\right)g_3+0g_4+0g_5+0:$$

Այնուհետեւ

$$S(g_3,g_4)=\frac{1}{2}y^2g_3-\frac{1}{-9}x^2g_4=x^2y^2-x^2y^2-\frac{2}{3}x^3=-\frac{2}{3}x^3:$$

Քանի որ ստացված բազմանդամը բաժանվում է g_3-ի վրա, միանգամից ունենք $S(g_3,g_4)_G=0$։ Հաջորդ քայլում

$$S(g_3,g_5)=\frac{1}{2}yg_3-\frac{1}{3}xg_5=x^2y-x^2y=0:$$

Վերջապես

$$S(g_4,g_5)=\frac{1}{-9}xg_4-\frac{1}{3}yg_5=xy^2+\frac{2}{3}x^2-xy^2=\frac{2}{3}x^2:$$

Ստացված բազմանդամը բաժանվում է g_3-ի վրա, ուստի $S(g_4,g_5)_G=0$։ Կատարված հաշվարկը ցույց է տալիս, որ $I=\langle g_1,g_2\rangle$ իդեալի Գրյոբների բազա է հետեւյալ բազմանդամների G բազմությունը.

$$\begin{aligned}g_1&=xy^2+3y^2+2x,\\ g_2&=x^2y+3xy,\\ g_3&=2x^2,\\ g_4&=-9y^2-6x,\\ g_5&=3xy:\end{aligned}\tag{8.32}$$

Եզրափակելով օրինակը՝ նկատենք, որ եթե մինչեւ վերջին քայլը մենք G-ն համարում էինք հաջորդականություն եւ պահպանում նրա անդամների դասավորությունը, ապա սկսած այն պահից, երբ պարզվեց, որ G-ն Գրյոբների բազա է, բազմանդամների դասավորությունն այլեւս էական չէ, եւ մենք կարող ենք դիտարկել այդ հինգ բազմանդամների ցանկացած հաջորդականություն։

8.6.12 Վարժություն. Կատարել նախորդ օրինակի բոլոր հաշվարկները՝ ներառյալ անկյունով բաժանումները։

8.6.13 Վարժություն. Բուխբերգերի ալգորիթմի միջոցով որեւէ Գրյոբների բազա կառուցել 8.5.2 խնդրի բազմանդամների զույգով ծնված իդեալի համար։

8.6.14 Վարժություններ. Բուխբերգերի ալգորիթմի միջոցով Գրյոբների բազաներ կառուցել հետեւյալ իդեալների համար: Ընդ որում, նախ կառուցումները կատարել ըստ lex կարգավորվածության, ապա ըստ՝ $grlex$ կարգավորվածության.

1) $I = \langle x - z^4, y - z^5 \rangle$,

2) $I = \langle x^2y - 1, xy^2 - x \rangle$,

3) $I = \langle x^2 + y, x^4 + 2x^2y + y^2 + 3 \rangle$:

8.6.15 Դիտողություն. Նկատենք, որ մենք արդեն կարող ենք լուծել իդեալին պատկանելության խնդիրը, որը ձեւակերպեցինք 8.1 պարագրաֆում: Եթե տրված է $K[x_1, \dots, x_n]$ օղակի $I = \langle g_1, \dots, g_s \rangle$ իդեալը եւ որեւէ $f \in K[x_1, \dots, x_n]$ բազմանդամ, ապա կարելի է պարզել, թե արդյո՞ք f-ը պատկանում է I-ին: Դրա համար բավական է հաշվել I-ի որեւէ G Գրյոբների բազա եւ ստուգել, թե արդյո՞ք f-ը G-ի վրա բաժանելիս ստացվում է զրոյական մնացորդ (ընդ որում, G-ի բազմանդամների դասավորությունն էական չէ): Մենք սա դեռեւս ալգորիթմի տեսքով չենք ձեւակերպում եւ կանդրադառնանք այս հարցին 8.7 պարագրաֆում, երբ Գրյոբների բազաների մասին կունենանք այնպիսի հավելյալ փաստեր, որոնք թույլ կտան լուծել նաեւ իդեալների հավասարության եւ ենթաիդեալների խնդիրները:

8.7 Մինիմալ եւ բերված Գրյոբների բազաներ

Բուխբերգերի ալգորիթմով կարելի է $G = \{g_1, \dots, g_s\}$ Գրյոբների բազա կառուցել $K[x_1, \dots, x_n]$ օղակի ցանկացած ոչ զրոյական I իդեալի համար: Սակայն I-ն կարող է նաեւ այլ Գրյոբների բազաներ ունենալ: Նման օրինակներ հեշտ է ստանալ, ասենք, G-ի g_i բազմանդամները կամայական ոչ զրոյական c_i սկալյարներով բազմապատկելով, $i = 1, \dots, s$: Քանի որ այդ սկալյարներով բազմապատկումը չի փոխում ոչ բազմանդամերի ավագ մոնոմիալները, ոչ էլ I իդեալը, $G = \{c_1g_1, \dots, c_sg_s\}$ բազմությունը նույնպես I-ի Գրյոբների բազա է: Դժվար չէ կառուցել նաեւ ավելի պակաս տրիվիալ օրինակներ.

8.7.1 Օրինակ. Մենք 8.6.11 օրինակում $I = \langle g_1, g_2 \rangle$ իդեալի համար հինգ տարրերից բաղկացած $G = \{g_1, \dots, g_5\}$ Գրյոբների բազան ստացանք (8.32) համակարգի տեսքով: Նկատենք, որ այդ օրինակի I իդեալը չի փոխվի, եթե G-ին ավելացնենք, ասենք, $g_6 = g_2 + g_3 = (x^2y + 3xy) + 2x^2 = x^2y + 2x^2 + 3xy$ բազմանդամը: Մյուս կողմից, g_6 բազմանդամի ավագ անդամը համընկնում է g_2-ի ավագ անդամի հետ,

այսինքն՝ $\{\mathrm{lt}g_1, \dots, \mathrm{lt}g_6\}$ ավագ անդամները ծնում են նույն մոնոմիալ իդեալը, ինչ $\{\mathrm{lt}g_1, \dots, \mathrm{lt}g_5\}$-ը: Ուրեմն՝ $\{g_1, \dots, g_6\}$ բազմությունը նույնպես I-ի Գրյոբների բազա է:

Հասկանալի է, որ մեզ հետաքրքրում են ոչ թե այն դեպքերը, երբ տրված Գրյոբների բազան ավելի է մեծացվում, այլ այն դեպքերը, երբ կարելի է *հնարավորինս քիչ* բազմանդամներից կազմված Գրյոբների բազա ստանալ: Հետեւյալ լեմման թույլ է տալիս Գրյոբների բազայից որոշ տարրեր հեռացնել:

8.7.2 Լեմմա. *Ենթադրենք $G = \{g_1, \dots, g_s\}$ բազմությունը I իդեալի Գրյոբների բազա է, իսկ նրա $g_i \in G$ բազմանդամն այնպիսին է, որ $\mathrm{lt}g_i \in \langle \mathrm{lt}(G\backslash\{g_i\})\rangle$, այսինքն՝ g_i-ի ավագ անդամը պատկանում է G-ի մնացած բազմանդամների ավագ անդամներով ծնված իդեալին: Այդ դեպքում $G\backslash\{g_i\}$ բազմությունը նույնպես I իդեալի Գրյոբների բազա է:*

Ապացույց: Օգտվելով 8.5.7 հետեւանքից՝ բավական է ցույց տալ, որ ցանկացած $f \in I$ բազմանդամի $\mathrm{lt}f$ ավագ անդամը բաժանվում է $G\backslash\{g_i\}$-ի բազմանդամներից որեւէ մեկի ավագ անդամի վրա:

Քանի որ G-ն I-ի Գրյոբների բազա է, ըստ 8.5.7 հետեւանքի՝ գոյություն ունի $g_j \in G$, որ $\mathrm{lt}f \vdots \mathrm{lt}g_j$: Եթե g_j-ն տարբեր է G-ից հեռացված g_i բազմանդամից, ապա g_i-ի հեռացումը այդ բաժանման վրա չի ազդել: Իսկ եթե $g_j = g_i$, ապա օգտվենք այն փաստից, որ $\langle \mathrm{lt}(G\backslash\{g_i\})\rangle$-ն մոնոմիալ իդեալ է: Քանի որ, ըստ լեմմայի պահանջի, $\mathrm{lt}g_i$ միանդամը պատկանում է այդ մոնոմիալ իդեալին, ապա ըստ 8.3.5 լեմմայի՝ այն բաժանվում է մոնոմիալ իդեալի ծնիչներից որեւէ մեկի վրա, այսինքն, որեւէ $\mathrm{lt}g_j$ ավագ անդամի վրա, որտեղ $g_j \in G\backslash\{g_i\}$: Ուստի նաեւ $\mathrm{lt}f \vdots \mathrm{lt}g_i$:

Հասկանալի է, որ $G\backslash\{g_i\}$ բազմությունը ծնում է I-ն: Իրոք, եթե $f \in I$ բազմանդամը անկյունով բաժանենք $G\backslash\{g_i\}$-ի վրա, ապա կստացվի զրոյական մնացորդ, քանի որ բաժանման ամեն քայլում կգտնվի $G\backslash\{g_i\}$-ի որեւէ բազմանդամ, որը կբաժանի ընթացիկ բազմանդամի ավագ անդամը ըստ վերն ասվածի: ■

8.7.3 Դիտողություն. Մենք ստացել ենք Գրյոբների բազայի հետեւյալ օգտակար հատկությունը. $g_i \in G$ բազմանդամի համար $\mathrm{lt}g_i$-ն պատկանում է $\langle \mathrm{lt}(G\backslash\{g_i\})\rangle$ իդեալին այն եւ միայն այն դեպքում, երբ $\mathrm{lt}g_i$-ն բաժանվում է մնացած բազմանդամներից որեւէ մեկի ավագ անդամի վրա: Ընդ որում, այդ դեպքում, G-ից հեռացնելով g_i-ն, մենք ստանում ենք $G\backslash\{g_i\}$ Գրյոբների բազան միեւնույն I իդեալի համար:

Վերը բերված հատկությունները, բնականաբար, ճիշտ չեն բազմանդամների կամայական բազմությունների (ոչ անպայման Գրյոբների բազաների) համար:

8.7.4 Օրինակ. Դիտարկենք $F = \{x^2 + 1\,, x^2\}$ բազմանդամների զույգը $K[x]$ օղակում: Քանի որ $(x^2 + 1) - x^2 = 1$, ապա $I = \langle F\rangle$ իդեալը պարունակում է 1 միավորը եւ, ուրեմն, $I = K[x]$: Մյուս կողմից, $\mathrm{lt}(x^2 + 1) = \mathrm{lt}x^2 = x^2$: Բայց եթե F-ից հեռացնենք առաջին բազմանդամը, կմնա x^2-ն, որը ծնում է $x^2K[x]$ իդեալը: Իսկ վերջինս տարբեր է $I = K[x]$ իդեալից:

8.7.5 Խնդիր. Բուխբերգերի ալգորիթմով գտնել նախորդ օրինակի F բազմությամբ ծնված իդեալի G Գրյոբների բազան: Ստուգել, որ այդ բազայից $x^2 + 1$ բազմանդամը հեռացնելու դեպքում G-ով ծնված իդեալը չի փոխվի:

8.7.6 Սահմանում. $K[x_1, \dots, x_n]$ օղակի I իդեալի $G = \{g_1, \dots, g_s\}$ Գրյոբների բազան կոչվում է *մինիմալ Գրյոբների բազա*, եթե ցանկացած $i = 1, \dots, s$ ինդեքսի համար

1) $\mathrm{lc}g_i = 1$,

2) $\mathrm{lt}g_i \notin \langle \mathrm{lt}(G\backslash\{g_i\})\rangle$:

Այսինքն՝ մինիմալ Գրյոբների բազայի բոլոր բազմանդամները նորմավորված են, եւ դրանցից ոչ մեկի ավագ անդամը չի բաժանվում մնացած բազմանդամներից որեւէ մեկի ավագ անդամի վրա:

8.7.2 լեմման եւ 8.7.3 դիտողությունը ոչ միայն ապացուցում են մինիմալ Գրյոբների բազաների գոյությունը, այլեւ տալիս են դրանց կառուցման եղանակը. բավական է վերցնել I իդեալի որեւէ G Գրյոբների բազա, նորմավորել նրա բազմանդամները եւ համեմատել դրանց ավագ անդամները: Եթե որեւէ g_i բազմանդամի ավագ անդամը բաժանվում է մի այլ g_j բազմանդամի ավագ անդամի վրա, ապա G-ից դեն նետենք g_i-ն: Ըստ 8.7.2 լեմմայի՝ մենք կրկին կունենանք Գրյոբների բազա, ընդ որում, դրանով ծնված I իդեալն անփոփոխ է: Վերջավոր անգամ կրկնելով այս քայլերը՝ մենք ի վերջո կստանանք մինիմալ Գրյոբների բազա: Կիրառենք այս կանոնը 8.6.11 օրինակում կառուցված բազայի վրա:

8.7.7 Օրինակ. 8.6.11 օրինակի $G = \{g_1, \dots, g_5\}$ Գրյոբների բազան նորմավորելուց հետո կստանանք

$$h_1 = xy^2 + 3y^2 + 2x,$$
$$h_2 = x^2y + 3xy,$$
$$h_3 = x^2,$$
$$h_4 = y^2 + \frac{2}{3}x,$$
$$h_5 = xy:$$

Քանի որ $\mathrm{lt} h_1 \mid \mathrm{lt} h_4$ եւ $\mathrm{lt} h_2 \mid \mathrm{lt} h_3$, ապա կարելի է դեն նետել առաջին երկու բազմանդամները: Կմնան երեք բազմանդամներ, որոնցից ոչ մեկի ավագ անդամը մյուսների ավագ անդամների վրա չի բաժանվում: Վերանվանելով բազմանդամները՝ կստանանք միեւնույն I իդեալի հետեւյալ *մինիմալ* Գրյոբների բազան. $f_1 = x^2,\ f_2 = y^2 + \frac{2}{3}x,\ f_3 = xy$:

Քանի որ մինիմալ Գրյոբների բազայի կառուցման քայլերը բարդ չեն, համապատասխան ալգորիթմի ձեւակերպումը թողնենք որպես պարզ խնդիր.

8.7.8 Խնդիր. Ձեւակերպել մինիմալ Գրյոբների բազայի կառուցման ալգորիթմը՝ համարելով, որ տրված I իդեալի համար Բուխբերգերի ալգորիթմի միջոցով արդեն գտնված է G Գրյոբների բազան: *Յուցում.* տես նաեւ 8.7.13 ալգորիթմը:

I իդեալը կարող է ունենալ տարբեր մինիմալ Գրյոբների բազաներ:

8.7.9 Օրինակ. Հեշտ է ստանալ 8.6.11 օրինակի իդեալի (այսինքն՝ 8.5.1 օրինակի $I = \langle g_1, g_2 \rangle$ իդեալի) տարբեր մինիմալ Գրյոբների բազաներ: Իսկապես, դիտարկենք $f_1 = x^2 + k \cdot xy,\ f_2 = y^2 + \frac{2}{3}x,\ f_3 = xy$ բազմանդամների եռյակը, որտեղ k-ն որեւէ ամբողջ թիվ է: Սրանք ստացվում են 8.7.7 օրինակի բազմանդամների եռյակից, եթե f_1 բազմանդամին k անգամ գումարենք f_3-ը: Պարզ է, որ այդ ընթացքում չի փոխվում բազմանդամների եռյակով ծնված I իդեալը, որը ոչ այլ ինչ է, քան 8.5.1 օրինակի $I = \langle g_1, g_2 \rangle$ իդեալը: Մյուս կողմից, $k \cdot xy$-ի գումարումը չի ազդում բազմանդամի ավագ անդամի վրա, ուստի մենք կրկին մինիմալ Գրյոբների բազա ենք ստանում:

8.7.10 Լեմմա. *$K[x_1, \dots, x_n]$ օղակի ոչ զրոյական I իդեալի ցանկացած երկու մինիմալ Գրյոբների բազաներ բաղկացած են հավասար քանակությամբ բազմանդամներից:*

Ապացույց: Ենթադրենք I իդեալն ունի $G = \{g_1, \dots, g_s\}$ եւ $H = \{h_1, \dots, h_k\}$ մինիմալ Գրյոբների բազաները: Դիտարկենք որեւէ $g_i \in G$: Քանի որ $g_i \in I$ եւ H-ը Գրյոբների բազա է, գոյություն ունի այնպիսի մի h_j, որ $\mathrm{lt} g_i \mid \mathrm{lt} h_j$: Քանի որ G-ն նույնպես Գրյոբների բազա է, այդ h_j-ի համար գոյություն ունի այնպիսի մի g_l, որ $\mathrm{lt} h_j \mid \mathrm{lt} g_l$: Ուրեմն՝ տեղի ունի նաեւ $\mathrm{lt} g_i \mid g_l$: Քանի որ G-ն մինիմալ է, սա հնարավոր է միայն, երբ $i = l$: Այսինքն՝ $\mathrm{lt} g_i$ եւ $\mathrm{lt} h_j$ ավագ անդամները բաժանվում են իրար վրա: Քանի որ երկուսի գործակիցն էլ 1 է, ապա $\mathrm{lt} g_i = \mathrm{lt} h_j$: Ստանում ենք, որ G եւ H բազաների բազմանդամների ավագ գործակիցների բազմությունները համընկնում են: Ուրեմն եւ՝ $s = k$: ■

8.7.11 Սահմանում. $K[x_1,\dots,x_n]$ օղակի I իդեալի $G=\{g_1,\dots,g_s\}$ Գրյոբների բազան կոչվում է *բերված Գրյոբների բազա*, եթե ցանկացած $i=1,\dots,s$ ինդեքսի համար

1) $\mathrm{lc} g_i = 1$,

2) g_i-ի միանդամներից ոչ մեկը չի պատկանում $\langle \mathrm{lt}(G\backslash\{g_i\})\rangle$ իդեալին:

Հասկանալի է, որ բերված Գրյոբների բազան նաեւ մինիմալ է:

8.7.12 Թեորեմ. *$K[x_1,\dots,x_n]$ օղակի կամայական I իդեալ ունի միակ բերված Գրյոբների բազա:*

Հասկանալի է, որ այստեղ միակությունը ի նկատի ունենք ֆիքսված մոնոմիալ կարգավորվածության պարագայում:

Ապացույց: Վերցնենք I իդեալի կամայական $G=\{g_1,\dots,g_s\}$ մինիմալ Գրյոբնեբի բազա եւ որեւէ $i=1,\dots,s$ ինդեքսի համար r_i-ով նշանակենք g_i բազմանդամը $G\backslash\{g_i\}$-ի վրա բաժանելիս ստացվող $r_i=(g_i)_{G\backslash\{g_i\}}$ մնացորդը: Քանի որ $G\backslash\{g_i\}$-ն I իդեալի Գրյոբների բազա չէ, բաժանման մնացորդը կարող է եւ կախված լինել բազմանդամների դասավորությունից: $G\backslash\{g_i\}$-ի դասավորությունն էական չէ ապացույցի համար, ուստի պարզության համար ընտրենք նրա դասավորություններից որեւէ մեկը: Նշանակենք $G'=(G\backslash\{g_i\})\cup r_i$ եւ նկատենք, որ այս բազմությունն ունի հետեւյալ հատկությունները.

g_i-ի ավագ անդամը չի բաժանվում $G\backslash\{g_i\}$-ի բազմանդամներից ոչ մեկի ավագ անդամի վրա: Ուստի անկյունով բաժանման ընթացքում $\mathrm{lt} g_i$-ն նույնաբար տեղափոխվում է մնացորդների սյունակ եւ դառնում r_i մնացորդի ավագ անդամը՝ $\mathrm{lt} r_i = \mathrm{lt} g_i$: Հետեւաբար, G-ի եւ G'-ի բազմանդամների ավագ անդամների բազմությունները համընկնում են: $G'\subseteq I$ եւ G'-ը ծնում է I-ն, քանի որ, եթե ինչ-որ $f\in I$ բազմանդամ G-ի վրա բաժանելիս ստացվում է զրոյական մնացորդ, ապա զրոյական մնացորդ է ստացվում նաեւ այն նաեւ G'-ի վրա բաժանելիս, քանի որ $\mathrm{lt}(G)=\mathrm{lt}(G')$: Պարզ է, որ G'-ը Գրյոբների բազա է, քանի որ ունի նույն ավագ անդամները, ինչ G-ն: Նույն պատճառով G'-ը նաեւ *մինիմալ* բազա է:

Քանի որ r_i-ն կազմված է այն միանդամներից, որոնք $G\backslash\{g_i\}$-ի վրա անկյունով բաժանման պրոցեսում տեղափոխվել են մնացորդների սյունակ, ապա պարզ է, որ r_i-ի միանդամներից ոչ մեկը չի բաժանվում $G\backslash\{g_i\}$-ի բազմանդամների ավագ անդամներից որեւէ մեկի վրա:

Կրկնենք նախորդ քայլերը մի այլ g_j բազմանդամի համար եւ, այն r_j մնացորդով փոխարինելով, ստանանք G'' բազմությունը: r_j մնացորդի միանդամները չեն բաժանվում $G''\backslash\{r_j\}$-ի բազմանդամների ավագ անդամներից որեւէ մեկի վրա:

Պարզ է նաեւ, որ նախորդ քայլում ստացված r_i-ի միանդամները եւս չեն բաժանվում $G''\backslash\{r_i\}$-ի բազմանդամների ավագ անդամների վրա, քանի որ $\mathrm{lt}(G'') = \mathrm{lt}(G')$:

Շարունակելով այս քայլերը Գրյոբների բազայի բոլոր բազմանդամների համար՝ կստանանք որոնելի բերված Գրյոբների բազան: Նոր նշանակում չմտցնելու համար բերված բազան նույնպես նշանակենք $G = \{g_1, \dots, g_s\}$:

Անցնենք G-ի միակության ապացույցին: Ենթադրենք I-ն ունի նաեւ $G^* = \{h_1, \dots, h_m\}$ բերված Գրյոբների բազան: Ըստ 8.7.10 լեմմայի՝ $m = s$: Ավելին, ըստ 8.7.10 լեմմայի ապացույցի, G եւ G^* բազաների բազմանդամներն ունեն միեւնույն ավագ անդամները՝ $\mathrm{lt}(G^*) = \mathrm{lt}(G)$: Վերցնենք որեւէ $g_i \in G$ բազմանդամ եւ նրա համար ֆիքսենք այն $h_j \in G^*$ բազմանդամը, որ $\mathrm{lt}g_i = \mathrm{lt}h_j$: Ցույց տանք, որ $g_i = h_j$:

Իրոք, քանի որ $h_j \in I$, ապա նաեւ $g_i - h_j \in I$: Ուրեմն՝ այդ տարբերությունը G Գրյոբների բազայի վրա բաժանելիս ստացվում է զրոյական $(g_i - h_j)_G = 0$ մնացորդ: Քանի որ $\mathrm{lt}g_i = \mathrm{lt}h_j$, ապա $g_i - h_j$ տարբերության մեջ ավագ անդամները կրճատվում են: Այդ տարբերության մնացած միանդամները ստացվում են g_i-ի եւ h_j-ի միանդամների միջեւ նման անդամների միացում կատարելով (ըստ հավասար մոնոմիալների): $g_i - h_j$ տարբերության, ասենք, երկրորդ գումարելին G-ի վրա բաժանելիս կարող է զրոյանալ միայն, երբ այն բաժանվում է G-ի բազմանդամներից մեկի ավագ անդամի վրա: Այդ բազմանդամը չի կարող լինել g_i-ն, քանի որ $g_i - h_j$ տարբերության աստիճանը խիստ փոքր է g_i-ի աստիճանից: Իսկ եթե այդ բազմանդամը լինի մի այլ $g_l \in G$, մենք կունենանք, որ g_i-ի մոնոմիալներից մեկը բաժանվում է միայն $g_l \in G$ բազմանդամի ավագ մոնոմիալի վրա: Ըստ բերված Գրյոբների բազայի սահմանման սա անհնար է, եւ հակասությունից խուսափելու միակ հնարավորությունն է. $g_i - h_j$ տարբերության բոլոր միանդամները զրոյական են: Այսինքն՝ $g_i = h_j$: ■

Տրված G մինիմալ Գրյոբների բազայի հիման վրա բերված Գրյոբների բազա կառուցելու համար պետք է յուրաքանչյուր $g_i \in G$ բազմանդամ բաժանել $G\backslash\{g_i\}$-ի վրա: Եթե $r_i = (g_i)_{G\backslash\{g_i\}}$ մնացորդը զրոյական չէ, g_i-ն փոխարինվում է r_i-ով:

Բերենք բերված Գրյոբների բազայի կառուցման ալգորիթմը՝ համարելով, որ տրված ոչ զրոյական I իդեալի համար (8.6.10 Բուխբերգերի ալգորիթմով կամ ցանկացած այլ եղանակով) արդեն գտնված է G Գրյոբների բազան:

8.7.13 Ալգորիթմ (բերված Գրյոբների բազայի կառուցման ալգորիթմը). K դաշտի վրա որոշված $K[x_1, \dots, x_n]$ բազմանդամային օղակում տրված են I իդեալը եւ նրա G Գրյոբների բազան: Կառուցել I իդեալի բերված Գրյոբների բազան:

1. G Գրյոբների բազայի յուրաքանչյուր g բազմանդամի համար

2. վերագրենք $g = \frac{1}{\mathrm{lt} g} g$;

3. $G \backslash \{g\}$ բազմության յուրաքանչյուր g' տարրի համար

4. եթե $\mathrm{lt} g \vdots \mathrm{lt} g'$

5. վերագրենք $G = G \backslash \{g\}$:

6. G մինիմալ Գրյոբների բազայի յուրաքանչյուր g տարրի համար

7. ֆիքսենք $G \backslash \{g\}$ բազմության որեւէ դասավորություն;

8. g-ն բաժանենք $G \backslash \{g\}$-ի այդ դասավորության վրա եւ ստացված $g_{G \backslash \{g\}}$ մնացորդը նշանակենք r;

9. եթե $r \neq 0$

10. վերագրենք $G = (G \backslash \{g\}) \cup r$:

11. Դուրս գրենք G բերված Գրյոբների բազան:

8.7.14 Օրինակ. Հեշտ է ստուգել, որ 8.7.7 օրինակում ստացված $f_1 = x^2$, $f_2 = y^2 + \frac{2}{3}x$, $f_3 = xy$ բազմանդամներից կազմված մինիմալ Գրյոբների բազան նաեւ բերված Գրյոբների բազա է 8.5.1 օրինակի $I = \langle g_1, g_2 \rangle$ իդեալի համար: Իսկ 8.7.9 օրինակի $f_1 = x^2 + k \cdot xy$, $f_2 = y^2 + \frac{2}{3}x$, $f_3 = xy$ մինիմալ Գրյոբների բազան բերված չէ, եթե $k \neq 0$, քանի որ $k \cdot xy$ միանդամը բաժանվում է $\mathrm{lt} f_3 = xy$ ավագ անդամի վրա: Եթե, ասենք, $k = 2$ դեպքում կիրառենք 8.7.13 ալգորիթմը, ապա $f_1 = x^2 + 2 \cdot xy$ բազմանդամը ալգորիթմի 8-րդ քայլում կբաժանվի (f_2, f_3) հաջորդականության վրա եւ կստացվի $r = x^2$ մնացորդը: Ալգորիթմի 10-րդ քայլում f_1-ը կփոխարինվի $r = x^2$ բազմանդամով:

$K[x_1, \dots, x_n]$ օղակում ֆիքսված մոնոմիալ կարգավորվածության դեպքում կամայական I իդեալի համար *միակ* G բերված Գրյոբների բազայի գոյության փաստը ալգորիթմական շատ կարեւոր նշանակություն ունի: Մասնավորապես, դրա օգնությամբ կարող ենք լուծել 8.1 պարագրաֆում ձեւակերպված խնդիրները:

Իդեալների հավասարության խնդիրը հանգում է բերված Գրյոբների բազաների հաշվմանը: Իսկապես, ենթադրենք $K[x_1, \dots, x_n]$ օղակում տրված են $I = \langle g_1, \dots, g_s \rangle$ եւ $J = \langle h_1, \dots, h_m \rangle$ իդեալները: Այն դեպքը, երբ իդեալներից մեկը կամ երկուսն էլ զրոյական են, շատ հեշտ է պարզել (իդեալը զրոյական է այն եւ միայն այն դեպքում, երբ նրա բոլոր ծնիչները զրոյական են): Ուստի բացառենք այդ դեպքը եւ ենթադրենք, որ ծնիչների բազմանդամները նույնպես ոչ զրոյական են: $K[x_1, \dots, x_n]$-ում ֆիքսենք որեւէ մոնոմիալ կարգավորվածություն եւ, 8.6.10 Բուխբերգերի ալգո-

րիթմի միջոցով ինչ-որ բազմանդամներ ավելացնելով իդեալների ծնիչներին, ստանանք դրանց $G = \{g_1, \dots, g_{s'}\}$ ու $H = \{h_1, \dots, h_{m'}\}$ Գրյոբների բազաները (այստեղ $s' \geq s$ եւ $m' \geq m$): Այդ բազաների վրա կիրառելով 8.7.13 ալգորիթմը՝ կառուցենք I եւ J իդեալների G' եւ H' *բերված* Գրյոբների բազաները: Ըստ 8.7.12 թեորեմի՝ I եւ J իդեալները հավասար են այն եւ միայն այն դեպքում, երբ $G' = H'$:

Ստանում ենք հետեւյալ ալգորիթմը.

8.7.15 Ալգորիթմ (իդեալների հավասարության որոշման ալգորիթմը բերված Գրյոբների բազաների օգնությամբ). K դաշտի վրա որոշված $K[x_1, \dots, x_n]$ բազմանդամային օղակում տրված են $I = \langle g_1, \dots, g_s \rangle$ եւ $J = \langle h_1, \dots, h_m \rangle$ ոչ զրոյական իդեալները: Պարզել, թե արդյո՞ք I եւ J իդեալները հավասար են:

1. $K[x_1, \dots, x_n]$ օղակում սահմանել որեւէ մոնոմիալ կարգավորվածություն:

2. 8.6.10 Բուխբերգերի ալգորիթմով կառուցենք I իդեալի $G = \{g_1, \dots, g_{s'}\}$ Գրյոբների բազան ($s' \geq s$):

3. 8.6.10 Բուխբերգերի ալգորիթմով կառուցենք J իդեալի $H = \{h_1, \dots, h_{m'}\}$ Գրյոբների բազան ($m' \geq m$):

4. 8.7.13 ալգորիթմով կառուցենք G Գրյոբների բազային համապատասխան G' բերված Գրյոբների բազան:

5. 8.7.13 ալգորիթմով կառուցենք H Գրյոբների բազային համապատասխան H' բերված Գրյոբների բազան:

6. Եթե $G' = H'$

7. դուրս գրենք. I եւ J իդեալները հավասար են;

8. այլապես

9. դուրս գրենք. I եւ J իդեալները տարբեր են:

8.7.16 Վարժություններ. Ենթադրենք I-ն 8.5.1 օրինակի $I = \langle g_1, g_2 \rangle$ իդեալն է: Արդյո՞ք $I = J$, որտեղ.

1) $J = \langle x^2 + 2xy,\ y^2 + \frac{2}{3}x,\ xy \rangle$,

2) $J = \langle 7x^2 + 777xy,\ y^2 + \frac{2}{3}x,\ xy \rangle$,

3) $J = \langle x^2,\ y^2 + \frac{2}{3}x \rangle$,

4) $J = \langle x^2 + 2x,\ 3y^2 + 2xy + 2x, -2xy \rangle$:

Ինչպես նշեցինք 8.6.15 դիտողության մեջ, մենք արդեն ունենք նաեւ *իդեալին պատկանելության խնդրի* լուծումը: Եթե տրված է $K[x_1,\dots,x_n]$ օղակի $I=\langle g_1,\dots,g_s\rangle$ իդեալը եւ որեւէ $f\in K[x_1,\dots,x_n]$ բազմանդամ, ապա ֆիքսելով որեւէ մոնոմիալ կարգավորվածություն՝ կառուցենք I-ի որեւէ G Գրյոբների բազա եւ հաշվենք f-ը G-ի վրա բաժանելիս ստացվող r մնացորդը: f-ը պատկանում է I-ին այն եւ միայն այն դեպքում, երբ $r=0$: Այս ալգորիթմի համար անհրաժեշտ չէ, որ G-ն լինի մինիմալ կամ բերված Գրյոբների բազա: Սակայն G-ն նման տիպերի Գրյոբների բազա վերցնելը հաճախ ավելի հարմար է, քանի որ այդ դեպքում G-ի տարրերի քանակն ավելի փոքր կարող է լինել, իսկ որքան քիչ են բաժանարարները, այնքան պարզ է անկյունով բաժանման ալգորիթմը:

8.7.17 Խնդիր. Դուրս գրել $K[x_1,\dots,x_n]$ օղակի I իդեալին պատկանելության խնդրի լուծման ալգորիթմը բերված Գրյոբների բազայի միջոցով: *Յուցում.* տես 8.7.13 ալգորիթմը:

8.7.18 Վարժություններ. Պարզել արդյո՞ք $f=\frac{3}{2}xy^3+x^2y^2+x^2y$ կամ $f=3x^2y^3+x^3y^2$ բազմանդամները պատկանում են 8.7.16 վարժությունների J իդեալներից որեւէ մեկին:

Բերվող Գրյոբների բազաների միջոցով հնարավոր է լուծել նաեւ *ենթաիդեալ լինելու խնդիրը*. $K[x_1,\dots,x_n]$ օղակի I եւ J իդեալների համար հնարավոր է պարզել, թե արդյո՞ք նրանցից մեկը մյուսի ենթաիդեալ է, եւ եթե այո, ապա արդյո՞ք այդ ենթաիդեալը սեփական է: Նախ, 8.6.10 Բուխբերգերի ալգորիթմով եւ 8.7.15 ալգորիթմով գտնենք այդ իդեալների G' եւ H' բերված Գրյոբների բազաները: Եթե դրանք հավասար են, ապա I եւ J իդեալները նույնպես հավասար են: Հակառակ դեպքում G'-ի բազմանդամները բաժանենք H'-ի վրա: Եթե բոլոր բաժանումներում զրոյական մնացորդ ստացվի, ապա I-ն J-ի սեփական ենթաիդեալ է: Հակառակ դեպքում H'-ի բազմանդամները բաժանենք G'-ի վրա: Եթե բոլոր բաժանումներում զրոյական մնացորդ ստացվի, ապա J-ն I-ի սեփական ենթաիդեալ է: Այլապես I եւ J իդեալները անհամեմատելի են (ոչ մեկը մյուսի մեջ ընկած չէ):

8.7.19 Խնդիր. Դուրս գրել $K[x_1,\dots,x_n]$ օղակի I եւ J իդեալների *ենթաիդեալ լինելու* խնդրի լուծման ալգորիթմը բերված Գրյոբների բազայի միջոցով:

8.7.20 Վարժություններ. Պարզել, թե 8.7.16 վարժությունների J իդեալներից որո՞նք են մեկը մյուսի սեփական ենթաիդեալ:

Այս պարագրաֆն ավարտենք Գրյոբների բազաների եւ Էվկլիդեսի ալգորիթմի միջեւ այն կապի նկարագրությամբ, որի մասին հիշատակեցինք 8.1 պարագրաֆում: Ենթադրենք ունենք K դաշտի վրա տրված $K[x]$ օղակի ոչ զրոյական $f = a_0x^n + \cdots + a_n$ եւ $g = b_0x^m + \cdots + b_m$ բազմանդամները: Քանի որ նորմավորումը չի ազդում բազմանդամների ամենամեծ ընդհանուր բաժանարարի վրա, գրառման պարզության համար համարենք, որ $a_0, b_0 = 1$: Համարենք նաեւ, որ $n > m$:

Բուխբերգերի ալգորիթմով կառուցենք $I = \langle f, g\rangle$ իդեալի Գրյոբների բազան: $S(f, g)$-ն հաշվելու համար մեզ պետք է $x^\gamma = [\mathrm{lm}f, \mathrm{lm}g]$ ամենափոքր ընդհանուր բազմապատիկը, որն այս դեպքում հավասար է $x^\gamma = [x^n, x^m] = x^n$: Ուստի (8.23) բանաձեւը կընդունի հետեւյալ տեսքը՝

$$S(f, g) = f - x^{n-m}g:$$

Հաջորդ քայլում $S(f, g)$-ն պետք է անկյունով բաժանել բազմանդամների $G = (f, g)$ զույգի վրա: Քանի որ $S(f, g)$-ի աստիճանը խիստ փոքր է f-ի աստիճանից, պարզ է, որ անկյունով բաժանման յուրաքանչյուր քայլում ընթացիկ բազմանդամը երբեք չի բաժանվի f-ի վրա, այլ կբաժանվի միայն g-ի վրա: Այսինքն՝ $S(f, g)$-ը (f, g) զույգի վրա բաժանելիս կստացվի այն նույն r մնացորդը, որը ստացվում է $S(f, g)$-ը ավանդական եղանակով միայն g-ի վրա բաժանելիս՝ $S(f, g) = q \cdot g + r$ եւ $\deg r < \deg g$ (եթե $r \neq 0$): Քանի որ

$$f - x^{n-m}g = S(f, g) = q \cdot g + r,$$

ապա

$$f = (x^{n-m} + q)g + r = q'g + r,$$

որտեղ $\deg r < \deg g$, եթե $r \neq 0$: Իսկ սա նշանակում է, որ $r = S(f, g)_G$ մնացորդը ոչ այլ ինչ է, եթե ոչ f-ը g-ի վրա բաժանելիս ստացվող մնացորդը ըստ Էվկլիդյան օղակի սահմանման: Ըստ Բուխբերգերի ալգորիթմի՝ միացնենք r-ը G-ին՝ $G = (f, g, r)$: Հաջորդ քայլում պետք է հաշվել $S(f, g)_G$, $S(f, r)_G$ եւ $S(g, r)_G$ մնացորդները: Առայժմ քննարկենք դրանցից միայն երրորդը: Կրկնելով նախորդ քայլերը՝ ստանում ենք, որ $S(g, r)_G = r_1$, որտեղ r_1-ը այն մնացորդն է, որ ստացվում է g-ն r-ի վրա բաժանելիս: Այն նույնպես ավելացնենք G-ին՝ $G = (f, g, r, r_1)$: Շարունակելով այս քայլերը՝ մենք G բազմությանը կավելացնենք 2.5 պարագրաֆի (2.7) համակարգի բոլոր $r, r_1, \ldots, r_{k-1}, r_k$ ոչ զրոյական մնացորդները: Քանի որ r_k-ն f, g բազմանդամների d ամենամեծ ընդհանուր բաժանարարն է, ապա G-ով ծնված իդեալը պարունակում է d-ով ծնված $dK[x]$ գլխավոր իդեալը: Մյուս կողմից, քանի որ բոլոր

$r, r_1, \dots, r_{k-1}, r_k$ մնացորդները $I = \langle f, g \rangle$ իդեալից են, ունենք $I = dK[x]$: Այժմ հիշենք, որ նախորդ քայլերում մենք բաց թողեցինք $S(f,r)_G$ տիպի մնացորդները: Հասկանալի է, որ դրանք նույնպես I-ից են, եւ դրանց ավելացումը չի փոխում I-ն:

Ստանում ենք, որ Բուխբերգերի ալգորիթմով f, g զույգի համար Գրյոբների բազա կառուցելը իր մեջ ներառում է նրանց d ամենամեծ ընդհանուր բաժանարարի հաշվումը: G բազան պարունակում է d-ն եւ էլի մի շարք բազմանդամներ (այդ թվում եւ f, g բազմանդամները), որոնք բոլորը $I = dK[x]$ իդեալից են:

Նշված բազմանդամները բաժանվում են d-ի վրա: Ուստի G Գրյոբների բազայից *մինիմալ* Գրյոբների բազային անցնելու ընթացքում դրանք բոլորը դեն կնետվեն, բացի d-ից: Այսինքն՝ $I = \langle f, g \rangle$ իդեալի մինիմալ Գրյոբների բազան է $G = \{d\}$: Հեշտ է ստուգել, որ սա նաեւ բերված Գրյոբների բազա է: Այսպիսով՝ Էվկլիդեսի ալգորիթմով բազմանդամների ամենամեծ ընդհանուր բաժանարարի հաշվումը մինիմալ Գրյոբների բազայի հաշվման մասնավոր դեպքն է:

8.7.21 Խնդիր. Ստանալ նախորդ դիտարկման ընդհանրացումը մեկից ավելի բազմանդամների ամենամեծ ընդհանուր բաժանարարի համար:

8.8 Գրյոբների բազաները գծային հավասարումների համակարգերում

Սկսենք մի պարզ օրինակից, որը ոչ միայն ցույց կտա Գրյոբների բազայի կապը գծային հավասարումների համակարգերի լուծման հետ, այլեւ կբացատրի հաջորդ պարագրաֆում ավելի բարձր աստիճանի հավասարումների համակարգերի համար կրճատման իդեալների կիրառության ընդհանուր սկզբունքը (տես 8.8.5 դիտողությունը):

8.8.1 Օրինակ. Լուծենք հետեւյալ հավասարումների համակարգը փոփոխականների արտաքսման Գաուսի մեթոդով, այսինքն՝ մինորների մեթոդից մի փոքր տարբերվող եղանակով (մինորների մեթոդը նույնպես կապվում է Գաուսի անվան հետ, եւ մենք այդ մեթոդին անդրադարձել ենք 7.2 պարագրաֆում): Համակարգի փոփոխականները դասավորենք այնպես, որ համապատասխան փոփոխականները բոլոր տողերում գրվեն իրար տակ.

(8.33)
$$\begin{cases} 2x_1 + 2x_2 + 2x_3 - 2x_4 + 2x_5 = 2 \\ 2x_1 + 2x_2 + 3x_3 + x_4 + 2x_5 = 2 \\ -x_1 - x_2 + x_3 + x_5 = 0 \\ x_1 + x_2 + 2x_3 + 2x_4 + x_5 = 1 \end{cases}:$$

Մենք կարող ենք առաջին տողի առաջին գործակիցը հավասարեցնել մեկի: Դա կարելի է անել՝ առաջին տողը 2-ի վրա բաժանելով, ինչը, հասկանալի է, չի ազդի համակարգի լուծումների վրա: Դրանից բացի, մենք կարող ենք նախորդ քայլում ստացված 1 գործակցից ներքեւ (առաջին սյան մեջ) ստանալ միայն զրոյական գործակիցներ: Դա կարելի է անել՝ մնացած տողերին գումարելով առաջին տողը՝ նախապես այն ինչ-որ սկալյարներով բազմապատկելով: Դա նույնպես չի ազդում լուծումների վրա, եւ մենք կունենանք հետեւյալ համակարգը.

$$\begin{cases} x_1 + x_2 + x_3 - x_4 + x_5 = 1 \\ x_3 + 3x_4 = 0 \\ 2x_3 - x_4 + 2x_5 = 1 \\ x_3 + 3x_4 = 0 \end{cases}:$$

Նկատենք, որ այս ընթացքում արեցինք մի քայլ, որը չէինք կատարում մատրիցի որոշիչը հաշվելիս. մենք համակարգի մի տողը բազմապատկեցինք սկալյարով: Այդ քայլը փոխում է համակարգի մատրիցի որոշիչը, բայց մեր նպատակը որոշիչը չէ, այլ լուծումները, որոնք անփոփոխ մնացին այդ ընթացքում:

Հաջորդ քայլը նույնպես կտարբերվի որոշիչը եռանկյունի տեսքի բերելու մեթոդով հաշվելու եղանակից (տես 2.3.17 վարժությունները). որոշիչը հաշվելիս մենք աշխատում էինք հնարավորինս շատ ոչ զրոյական տարրեր բերել մատրիցի գլխավոր անկյունագծի վրա, իսկ դրանցից ներքեւ ստանալ միայն զրոներ: Այդ ընթացքում մենք կարող էինք տեղափոխել ինչպես տողերը, այնպես էլ սյուները (հաշվի առնելով, որ դրանով փոխում ենք միայն որոշիչի նշանը): Սակայն այժմ մենք երբեք *չենք տեղափոխում սյուները*, քանի որ դրանից հետո կխառնվեն $x_1, \dots, x_n$ փոփոխականները: Հետեւաբար, մենք չենք դիրքափոխում երկրորդ եւ երրորդ սյուները եւ, գլխավոր անկյունագծի երկրորդ գործակիցը 0 թողնելով, անցնում ենք երրորդ սյանը:

Ինչպես նշեցինք քիչ առաջ, մեր նպատակն է բոլոր ոչ տրիվիալ տողերի առաջին գործակիցը հավասարեցնել 1-ի: Երկրորդ տողում դա արդեն իսկ այդպես է, եւ մենք կարող ենք անցնել երրորդ սյան վերջին երկու գործակիցների զրոյացման: Դա կրկին կարելի է անել՝ երրորդ ու չորրորդ տողերին գումարելով երկրորդ տողը՝ նախապես այն սկալյարներով բազմապատկելով.

$$\begin{cases} x_1 + x_2 + x_3 - x_4 + x_5 = 1 \\ x_3 + 3x_4 = 0 \\ -7x_4 + 2x_5 = 1 \\ 0 = 0 : \end{cases}$$

Վերջում ստացանք մի տող, որը միայն զրոներից է բաղկացած: Հասկանալի է, որ կարելի է դեն նետել այն՝ առանց համակարգի լուծումները փոփոխելու: Դրանից բացի, համակարգի երրորդ տողի առաջին գործակիցը դեռեւս 1 չէ: Ուստի որպես հաջորդ քայլ կստանանք՝

$$\begin{cases} x_1 + x_2 + x_3 - x_4 + x_5 = 1 \\ x_3 + 3x_4 = 0 \\ x_4 - 2/7x_5 = -1/7 : \end{cases} \tag{8.34}$$

Առաջին, երրորդ եւ չորրորդ սյուներում կանգնած են x_1, x_3 եւ x_4 փոփոխականները: Դրանք այն փոփոխականներն են, որոնք, ըստ մեր կառուցման, «գլխավորում են» համակարգի տողերը եւ ունեն 1 գործակից: Համակարգի ձախ մասում թողնենք դրանք, իսկ մնացած x_2 եւ x_5 փոփոխականները տեղափոխենք հավասարման նշանից աջ՝

$$\begin{cases} x_1 + x_3 - x_4 = 1 - x_2 - x_5 \\ x_3 + 3x_4 = 0 \\ x_4 = -1/7 + 2/7x_5 : \end{cases}$$

Ձախ կողմում մենք ունենք մի քառակուսի համակարգ, որի որոշիչը 1 է: Այս համակարգը աջ կողմի արտահայտությունների ցանկացած արժեքների դեպքում ունի միակ լուծում: Ուստի մենք կարող ենք ցանկացած $x_2 = \alpha$ եւ $x_5 = \beta$ արժեքներ շնորհել աջ կողմ տարված փոփոխականներին եւ ըստ այդմ լուծել

$$\begin{cases} x_1 + x_3 - x_4 = 1 - \alpha - \beta \\ x_3 + 3x_4 = 0 \\ x_4 = -1/7 + 2/7\beta \end{cases}$$

համակարգը: Նախ $x_4 = -1/7 + 2/7\beta$, ապա $x_3 = -3x_4 = 3/7 - 6/7\beta$, այնուհետեւ

$$x_1 = 1 - \alpha - \beta - 3/7 + 6/7\beta - 1/7 + 2/7\beta = 3/7 - \alpha + 1/7\beta:$$

Այսինքն՝ (8.33) համակարգի ընդհանուր լուծումն է՝

$$\{(3/7 - \alpha + 1/7\beta, \alpha, 3/7 - 6/7\beta, -1/7 + 2/7\beta, \beta) \mid \alpha, \beta \in K\}:$$

(8.33) համակարգը լուծելու եղանակը մեզ համար նորույթ չի պարունակում: Շատ ավելի հետաքրքիր եւ անսպասելի է այն, որ (8.34) համակարգի տողերում

գրված է հետեւյալ երեք բազմանդամներից բաղկացած Գրյոբների բազան ըստ lex կարգավորվածության.

$$g_1 = x_1 + x_2 + x_3 - x_4 + x_5 - 1, \qquad g_2 = x_3 + 3x_4, \qquad g_3 = x_4 - 2/7x_5 + 1/7:$$

Համակարգի (8.34) տեսքը կոչվում է *աստիճանաձեւ տողերով* տեսք: Ինչպես տեսնում ենք, այդ մեթոդով համակարգի լուծումը հանգում է որոշակի Գրյոբների բազայի հաշվման: Սա առայժմ ստացել ենք մեկ օրինակի համար, իսկ ընդհանուր դեպքին կանդրադառնանք քիչ հետո:

8.8.2 Վարժություն. Ստուգել, որ նախորդ օրինակի $G = \{g_1, g_2, g_3\}$ բազմանդամների համար կատարվում է 8.6.4 Բուխբերգերի հայտանիշը՝ $S(g_i, g_j)_G = 0$: Ստուգել նաեւ, որ G Գրյոբների բազան մինիմալ Գրյոբների բազա է:

Շարունակենք նախորդ օրինակի համակարգի քննարկումը.

8.8.3 Օրինակ. 8.8.1 օրինակի (8.33) համակարգը (8.34) տեսքի բերելուց հետո կարելի էր լուծումը ավարտին հասցնել մի փոքր այլ կերպ: 8.8.1 օրինակում մենք շեշտեցինք x_1, x_3 եւ x_4 փոփոխականների դերը, որոնք «գլխավորում են» համակարգի տողերը: Համապատասխան տողում այդ փոփոխականներից ձախ գրված են միայն զրոներ: Ուստի մենք կարող ենք զրոյացնել նաեւ այդ փոփոխականներից վերեւ ընկած գումարելիները: (8.34) համակարգը կարելի է բերել նախ հետեւյալ տեսքին.

$$\begin{cases} x_1 + x_2 - 4x_4 + x_5 = 1 \\ x_3 + 3x_4 = 0 \\ x_4 - 2/7x_5 = -1/7 \end{cases}$$

(զրոյացվել է x_3-ից վերեւ ընկած գումարելին), ապա նաեւ հետեւյալ տեսքին.

$$\begin{cases} x_1 + x_2 - 1/7x_5 = 3/7 \\ x_3 + 6/7x_5 = 3/7 \\ x_4 - 2/7x_5 = -1/7 \end{cases} \tag{8.35}$$

(զրոյացվել են x_4-ից վերեւ ընկած գումարելիները): Եթե հիմա կրկին x_2 եւ x_5 փոփոխականները տեղափոխենք հավասարման նշանից աջ, ապա նրանց շնորհենք $x_2 = \alpha$ եւ $x_5 = \beta$ արժեքները, ապա մնացած երեք փոփոխականների արժեքները կհաշվվեն միանգամից.

$$\begin{cases} x_1 = 3/7 - \alpha + 1/7\beta \\ x_3 = 3/7 - 6/7\beta \\ x_4 = -1/7 + 2/7\beta : \end{cases}$$

Լուծման այս եղանակը ունի մի անսպասելի հատկություն. (8.36) համակարգի տողերը ներկայացնող

$$g_1 = x_1 + x_2 - 1/7x_5 - 3/7, \quad g_2 = x_3 + 6/7x_5 - 3/7, \quad g_3 = x_4 - 2/7x_5 + 1/7$$

բազմանդամները ոչ միայն մինիմալ Գրյոբների բազա, այլեւ բերված Գրյոբների բազա են:

8.8.4 Վարժություն. Ստուգել, որ նախորդ օրինակի g_1, g_2, g_3 բազմանդամների բազմությունը բերված Գրյոբների բազա է:

8.8.5 Դիտողություն. Քննարկված օրինակները հուշում են այն օրինաչափությունը, որը մենք կիրառելու ենք ցանկացած (ոչ անպայման գծային) հավասարումների համակարգի լուծման ուսումնասիրության համար: Մենք աշխատելու ենք հավասարումների համակարգից նախ դեն նետել ավելորդ տողերը (ինչպես նախորդ օրինակում զրոյական տողը), ապա Գրյոբների բազաների օգնությամբ աստիճանաբար արտաքսել փոփոխականները: Այսինքն՝ ստանալ համակարգի այնպիսի տողեր, որոնք ավելի ու ավելի քիչ քանակությամբ փոփոխականներ են պարունակում: Եթե այդ պրոցեսում ստանանք մի տող, որը միայն մեկ փոփոխական է պարունակում, ապա դրա լուծումը (եթե կարողանանք այն ալգորիթմորեն հաշվել) կարելի է տեղադրել այնպիսի մի տողի մեջ, որը միայն երկու փոփոխական է պարունակում եւլն…

Դիտողության մեջ նշված պրոցեսին մենք կանցնենք հաջորդ պարագրաֆում: Բայց, նախքան այդ, ընդհանուր դեպքի համար ձեւակերպենք այն հասկացությունները, որ վերը բերեցինք 8.8.1, 8.8.3 օրինակների եւ 8.8.2, 8.8.4 վարժությունների համակարգերի համար:

Ցանկացած K դաշտի վրա տրված գծային հավասարումների

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = b_1 \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = b_m \end{cases} \tag{8.36}$$

համակարգը կանվանենք *աստիճանաձեւ տողերով* համակարգ, եթե.

1) յուրաքանչյուր տողի առաջին ոչ զրոյական գումարելու գործակիցը 1 է (այն կոչվում է *գլխավոր* գումարելի),
2) ցանկացած երկու հաջորդական, ոչ զրոյական տողերից երկրորդում գլխավոր գումարելու փոփոխականի համարն ավելի մեծ է, քան առաջինում,
3) եթե համակարգում կան զրոյական (միայն զրոյական գործակիցներ եւ զրոյական ազատ անդամներ ունեցող) տողեր, ապա դրանք համակարգի վերջին տողերն են:

(8.36) համակարգը կանվանենք *բերված աստիճանաձեւ տողերով* համակարգ, եթե այն, ի հավելումն նախորդ երեք պայմանների, բավարարում է հետեւյալին.

4) եթե որեւէ սյուն պարունակում է որեւէ գլխավոր գումարելի, ապա այդ սյան բոլոր մնացած գումարելիները զրոյական են (նախորդ կետերից արդեն բխում է, որ գլխավոր գումարելուց ներքեւ ընկած բոլոր գումարելիները զրոյական են, եւ մենք այստեղ ավելացնում ենք, որ զրոյական են նաեւ դրանից վերեւ ընկած գումարելիները):

8.8.6 Օրինակներ. Աստիճանաձեւ տողերով համակարգի օրինակ է (8.34) համակարգը: Իսկ բերված աստիճանաձեւ տողերով համակարգի օրինակ է (8.35)-ը:

K դաշտի վրա տրված (8.36) գծային հավասարումների համակարգի *տողերի տարրական ձեւափոխություններ* անվանենք հետեւյալ ձեւափոխությունները.

1) համակարգի որեւէ տողի բազմապատկումը K դաշտի որեւէ սկալյարով,

2) համակարգի երկու տողերի դիրքափոխումը,

3) համակարգի մի տողին մի այլ տողի գումարումը՝ նախապես վերջինս K դաշտի որեւէ սկալյարով բազմապատկելուց հետո:

8.8.7 Խնդիր. Ստուգել, որ տողերի տարրական ձեւափոխություններից ոչ մեկը չի փոխում (8.37) համակարգի լուծումները:

8.8.8 Խնդիր. Ցույց տալ, որ (8.36) գծային հավասարումների համակարգը տողերի տարրական ձեւափոխությունների միջոցով կարելի է բերել աստիճանաձեւ տողերով տեսքի եւ բերված աստիճանաձեւ տողերով տեսքի: *Ցուցում.* կրկնել 8.8.1, 8.8.3 օրինակների քայլերը: Հաշվի առնել, որ համակարգը կարող է պարունակել միայն զրոներից բաղկացած սյուներ: Զրոյական կարող է լինել նաեւ առաջին սյունը: Ինչո՞ւ նման դեպքերում մենք չենք կարող տեղափոխել սյուները: Զրոյական սյանը համապատասխանում է փոփոխական, որը կարող է ընդունել կամայական արժեք:

8.8.9 Վարժություններ. Աստիճանաձեւ տողերով եւ բերված աստիճանաձեւ տողերով տեսքի բերելու միջոցով լուծել 7.2.7 օրինակի եւ 7.2.8 վարժության համակարգերը:

8.8.10 Խնդիր. Դուրս գրել գծային հավասարումների համակարգը աստիճանաձեւ տողերով եւ բերված աստիճանաձեւ տողերով ներկայացնելու ալգորիթմը:

8.8.11 Թեորեմ. *Եթե գծային հավասարումների (8.37) համակարգը ունի աստիճանաձեւ տողերով տեսք, ապա ըստ նրա տողերի ստացված գծային* $g_i = a_{i1}x_1 + \cdots + a_{in}x_n - b_i,\ \ i = 1, \dots, m,$ *բազմանդամներից կազմված* $G = \{g_1, \dots, g_m\}$ *բազմությունը մինիմալ Գրյոբների բազա է:*

Ապացույց: Նշանակենք $I = \langle g_1, \dots, g_m \rangle$ եւ վերցնենք այդ իդեալի կամայական $f \in I$ բազմանդամ: Ցույց տանք, որ նրա ավագ անդամը բաժանվում է $\{\mathrm{lt}g_1, \dots, \mathrm{lt}g_m\}$ ավագ անդամներից որեւէ մեկի վրա:

Պարզության համար ենթադրենք, որ g_1-ի ավագ անդամն է $a_{11}x_1 = x_1$: Եթե $\mathrm{lt} f$-ը բաժանվում է x_1-ի վրա, ապա թեորեմն ապացուցված է: Ենթադրենք $\mathrm{lt} f$-ը x_1-ի վրա չի բաժանվում: Քանի որ համակարգը աստիճանաձեւ տողերով տեսքի է, ապա $a_{11} = 1$, իսկ առաջին սյան մնացած բոլոր $a_{21}, \dots, a_{m1}$ գործակիցները զրոյական են, այսինքն՝ $g_2, \dots, g_m$ բազմանդամներում x_1 փոփոխականը բացակայում է:

Ըստ 2.2.12 թեորեմի f-ը կարելի է ներկայացնել որպես (2.1) տեսքի

$$f = \sum_{j=1}^{m} g_{i_j} r_j \tag{8.37}$$

գումար, որտեղ $g_{i_j} \in G$ եւ $r_j \in K[x_1, \dots, x_n]$: Այդ g_{i_j} բազմանդամները կարող են պարունակել x_1-ը միայն, երբ հավասար են g_1-ին: Եթե (8.37) գումարի ավագ անդամը չի բաժանվում x_1-ի վրա, ապա զրոյի է հավասար բոլոր այն գումարելիների գումարը, որոնցում մասնակցում է g_1-ը.

$$\sum_{\substack{j=1,\dots,m \\ g_{i_j}=g_1}} g_{i_j} r_j = 0:$$

Այս գումարից ընդհանուր հանելով $g_{i_j} = g_1$ արտադրիչը՝ տեսնում ենք, որ գումարը զրոյանում է միայն, երբ համապատասխան r_j-երի գումարը զրոյական է, այսինքն՝ (8.37) գումարից կարելի է դեն նետել g_1-ով մասնակցող գումարելիները:

Պարզության համար ենթադրենք, որ g_2-ի ավագ անդամն է $a_{21}x_2 = x_2$: Կրկին, եթե $\mathrm{lt} f$-ը բաժանվում է x_2-ի վրա, ապացույցն ավարտված է: Հակառակ դեպքում (8.38) գումարի մեջ խմբավորենք եւ ապա դեն նետենք g_2-ով մասնակցող գումարելիները: Կամ մենք ինչ-որ քայլում կստանանք, որ $\mathrm{lt} f \vdots \mathrm{lt} g_i$, կամ էլ կհաշվարկենք, որ $f = 0$, ինչը հակասության է բերում: ■

8.8.12 Խնդիր. Ստուգել, որ եթե գծային հավասարումների (8.36) համակարգը ունի *բերված* աստիճանաձեւ տողերով տեսք, ապա ըստ նրա տողերի ստացված $G = \{g_1, \dots, g_m\}$ մինիմալ Գրյոբների բազան *բերված* Գրյոբների բազա է:

8.8.13 Վարժություններ. Համապատասխան մինիմալ Գրյոբների բազաններն ու բերված Գրյոբների բազաները գտնել 7.2.7 օրինակի եւ 7.2.8 վարժության գծային հավասարումների համակարգերի համար:

8.9 Աֆինական բազմաձեւություններ եւ արտաքսման իդեալներ

Հավասարումների համակարգերի լուծումների ուսումնասիրության ընթացքում Գրյոբների բազաները օգտագործելու համար (տես 8.8.5 դիտողությունը) մեզ պետք են գալու բազմանդամներով եւ իդեալներով սահմանված աֆինական բազմաձեւությունները: K դաշտի վրա տրված n-յակների $K^n = \{(x_1, \dots, x_n) \mid x_i \in K,\ i =$

$1, \dots, n\}$ գծային տարածությանը մենք հանդիպել ենք ավելի վաղ, մասնավորապես, 7.2 պարագրաֆում:

8.9.1 Սահմանում. Ենթադրենք K դաշտի վրա տրված է K^n գծային տարածությունը եւ n փոփոխականի բազմանդամների $K[x_1, \dots, x_n]$ օղակը: Այդ օղակի $f_1, \dots, f_s$ բազմանդամներով սահմանված *աֆինական բազմաձեւություն* է կոչվում K^n-ի հետեւյալ ենթաբազմությունը՝

$$V(f_1, \dots, f_s) = \{(a_1, \dots, a_n) \in K^n \mid f_i(a_1, \dots, a_n) = 0, \qquad i = 1, \dots, s\}: \tag{8.38}$$

Այսինքն՝ $V = V(f_1, \dots, f_s)$ աֆինական բազմաձեւությունը

$$\begin{cases} f_1(x_1, \dots, x_n) = 0 \\ \dots\dots\dots\dots\dots \\ f_s(x_1, \dots, x_n) = 0 \end{cases} \tag{8.39}$$

համակարգի *լուծումների* բազմությունն է: Մենք համառոտության համար սա հաճախ կանվանենք պարզապես *բազմաձեւություն* եւ բաց կթողնենք բազմանդամների հիշատակումը, երբ համատեքստից պարզ է, թե որ բազմանդամներին են քննարկվում: Բազմաձեւությունները հանրահաշվական երկրաչափության հիմնական հասկացություններից են, եւ դրանք ընդգրկում են երկրաչափական օբյեկտների շատ լայն դասեր:

8.9.2 Օրինակ. Եթե $K = \mathbb{R}$ եւ $n = 2$, ապա, վերցնելով $K[x, y]$ օղակի $f(x, y) = x^2 + y^2 - R^2$ բազմանդամը, մենք որպես $V(f)$ աֆինական բազմաձեւություն կստանանք $\mathbb{R}^2$ իրական հարթության վրա $(0,0)$ կենտրոնով եւ R շառավղով շրջանագիծը: Իսկ եթե ավելացնենք նաեւ $g(x, y) = x - y$ բազմանդամը, ապա կստանանք $V(f, g)$ բազմաձեւությունը, որը բաղկացած է միայն երկու կետերից՝ նշված շրջանագծի եւ $y = x$ ուղղի հատման կետերից:

Աֆինական բազմաձեւություններ են նաեւ էլիպսները, հիպերբոլները, պարաբոլները եւ, ավելի ընդհանուր՝ բոլոր բազմանդամային ֆունկցիաների գրաֆիկները: Իսկապես.

8.9.3 Օրինակ. Եթե $K = \mathbb{R}$ դաշտի վրա տրված է $f(x) = a_0x^m + \dots + a_m \in \mathbb{R}[x]$ բազմանդամը, ապա $\mathbb{R}[x, y]$ օղակի $g(x, y) = a_0x^m + \dots + a_m - y$ բազմանդամով սահմանված $V(g)$ բազմաձեւությունը համընկնում է $\mathbb{R}^2$ իրական հարթության վրա $f(x)$-ի գրաֆիկի հետ:

8.9.4 Խնդիր. Ցույց տալ, որ բազմաձեւություններ են նաեւ ռացիոնալ ֆունկցիաների գրաֆիկները:

8.9.5 Վարժություն. Քննարկելով $f(x) = x^2$ պարաբոլի գրաֆիկը $\mathbb{R}^2$ հարթության վրա՝ նկարագրել $V(y - x^2 - z)$ բազմաձեւությունը $\mathbb{R}^3$ տարածության մեջ:

Աֆինական բազմաձեւությունների այլ բնույթի օրինակներ կարելի է ստանալ գծային հավասարումների համակարգերի լուծումներից: Մենք դրանց անդրադարձել ենք 7.2 եւ 8.8 պարագրաֆներում:

8.9.6 Օրինակ. Կամայական K դաշտի վրա տրված գծային հավասարումների

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = b_1 \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = b_m \end{cases} \tag{8.40}$$

համակարգը կարելի է ներկայացնել

$$\begin{cases} f_1(x_1, \dots, x_n) = 0 \\ \cdots\cdots\cdots\cdots \\ f_m(x_1, \dots, x_n) = 0 \end{cases}$$

տեսքով, որտեղ $f_i(x_1, \dots, x_n) \in K[x_1, \dots, x_n]$ գծային բազմանդամը սահմանվում է հետեւյալ կերպ

$$f_i(x_1, \dots, x_n) = a_{i1}x_1 + \cdots + a_{in}x_n - b_i, \qquad i = 1, \dots, m:$$

Այդ դեպքում (8.40) համակարգի լուծումները ոչ այլ ինչ են, քան $V = V(f_1, \dots, f_m)$ աֆինական բազմաձեւությունը: Մասնավորապես, երբ բոլոր $b_1, \dots, b_m$ ազատ անդամները զրոյական են, V բազմաձեւությունը նաեւ ենթատարածություն է:

Շատ կարեոր է աֆինական բազմաձեւությունների կապը $K[x_1, \dots, x_n]$ օղակի իդեալների հետ: Նախ նկատենք, որ եթե $(a_1, \dots, a_n) \in K^n$ n-յակը լուծում է տվյալ $f(x_1, \dots, x_n) = 0$ եւ $h(x_1, \dots, x_n) = 0$ հավասարումների համար, ապա այն լուծում է նաեւ $f(x_1, \dots, x_n) + h(x_1, \dots, x_n) = 0$ հավասարման համար: Ավելին, վերցնելով ցանկացած $r(x_1, \dots, x_n) \in K[x_1, \dots, x_n]$ բազմանդամ, հեշտ է ստուգել, որ $(a_1, \dots, a_n)$-ը լուծում է նաեւ $f(x_1, \dots, x_n) \cdot r(x_1, \dots, x_n) = 0$ հավասարման համար (քանի որ, եթե $f(a_1, \dots, a_n) = 0$, ապա այդ արտադրյալը զրոյական է անկախ $r(a_1, \dots, a_n)$ արժեքից):

Ցանկացած $f_1, \dots, f_s \in K[x_1, \dots, x_n]$ բազմանդամների համար նրանցով ծնված $I = \langle f_1, \dots, f_s \rangle$ իդեալը, ըստ 2.2.12 թեորեմի, կարելի է ներկայացնել որպես $f_i r_i$ տեսքի արտադրյալների (2.1) գումարների բազմություն (r_i բազմանդամները կամայական են $K[x_1, \dots, x_n]$-ից): Սրանից եւ վերն ասվածից բխում է, որ եթե $g(x_1, \dots, x_n)$-ը

ցանկացած բազմանդամ է I իդեալից, ապա նրա համար նույնպես տեղի ունի $g(a_1, \dots, a_n) = 0$: Այսինքն՝ $V = V(f_1, \dots, f_s)$ բազմաձեւության n-յակները արմատ են նաեւ ցանկացած $g \in I$ բազմանդամի համար:

8.9.7 Սահմանում. Ենթադրենք K դաշտի վրա տրված է K^n գծային տարածությունը եւ n փոփոխականի բազմանդամների $K[x_1, \dots, x_n]$ օղակը: Այդ օղակի I *իդեալով սահմանված աֆինական բազմաձեւություն* է կոչվում K^n-ի հետեւյալ ենթաբազմությունը՝

$$V(I) = \{(a_1, \dots, a_n) \in K^n \mid f(a_1, \dots, a_n) = 0, \text{ ցանկացած } f \in I\}: \tag{8.41}$$

Եթե $I = \langle f_1, \dots, f_s \rangle$, ապա սահմանմանը նախորդող քննարկումից պարզ է, որ $f_1, \dots, f_s$ բազմանդամներով սահմանված $V(f_1, \dots, f_s)$ աֆինական բազմաձեւությունը ընկած է $V(I)$-ի մեջ: Մյուս կողմից, քանի որ $\{f_1, \dots, f_s\} \subseteq I$, ապա I-ի բոլոր բազմանդամների համար արմատ հանդիսացող n-յակները արմատ կհանդիսանան նաեւ $f_1, \dots, f_s$ բազմանդամների համար՝ $V(f_1, \dots, f_s) \supseteq V(I)$: Այսինքն, եթե $I = \langle f_1, \dots, f_s \rangle$, ապա

$$V(I) = V(f_1, \dots, f_s): \tag{8.42}$$

Իդեալներով սահմանված $V(I)$ բազմաձեւությունները ավելի ընդհանուր հասկացություն են թվում թեկուզ միայն այն պատճառով, որ $V(f_1, \dots, f_s)$ տեսքի բազմաձեւությունները սահմանվում են բազմանդամների վերջավոր բազմությունների համար, մինչդեռ $V(I)$ տեսքի բազմաձեւությունը սահմանող I իդեալը կարող է անվերջ լինել:

Այնուամենայնիվ, վերջավոր բազայի մասին 8.4.12 Հիլբերտի թեորեմի միջոցով դժվար չէ ցույց տալ, որ իրականում յուրաքանչյուր $V(I)$ բազմաձեւություն կարելի է ներկայացնել $V(f_1, \dots, f_s)$ տեսքով: Իսկապես, $K[x_1, \dots, x_n]$ օղակի ցանկացած I իդեալ վերջավոր ծնված է: Եթե նրա ծնիչների վերջավոր բազմությունն է $\{f_1, \dots, f_s\}$, ապա կարելի է վերցնել $V(f_1, \dots, f_s)$ բազմաձեւությունը, որը հավասար է $V(I)$ բազմաձեւությանը, ինչպես տեսանք քիչ առաջ: Մենք ապացուցեցինք.

8.9.8 Լեմմա. *K դաշտի վրա տրված $K[x_1, \dots, x_n]$ օղակի ցանկացած I իդեալի համար $V(I) = V(f_1, \dots, f_s)$, որտեղ $\{f_1, \dots, f_s\}$-ը I-ի ծնիչների ցանկացած բազմություն է: Մասնավորապես, ցանկացած I իդեալով սահմանված աֆինական բազմաձեւություն կարող է սահմանվել բազմանդամների վերջավոր բազմությամբ:*

8.9.9 Դիտողություն. Այս լեմման ընդհանրացնում է գծային հավասարումներից հայտնի հետեւյալ փաստը: Երբեմն (ինչպես 8.8.1 օրինակում) մենք կարող ենք դեն նետել «ավելորդ» հավասարումները: Դրանք այն հավասարումներն են, որոնք գծորեն կախված են մյուսներից եւ համակարգի լուծման ընթացքում զրոյանում են: Ավելին, եթե դիտարկենք n փոփոխականներով գծային հավասարումների որեւէ *անվերջ* համակարգ

$$\begin{cases} a_{11}x_1 + \cdots + a_{1n}x_n = b_1 \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ a_{m1}x_1 + \cdots + a_{mn}x_n = b_m \\ \cdots\cdots\cdots\cdots\cdots\cdots, \end{cases}$$

ապա հեշտ է տեսնել, որ այս համակարգի գծորեն անկախ տողերի քանակը ոչ ավել, քան n է, եւ այս անվերջ քանակությամբ տողերը հանդիսանում են որոշ վերջավոր քանակությամբ տողերի գծային կոմբինացիաներ: Այսինքն՝ համակարգի բոլոր տողերը, բացի որոշ վերջավոր քանակությամբ տողերից, կարելի է դեն նետել: 8.9.8 լեմման ցույց է տալիս, որ նույնը կարելի է ասել ցանկացած $V(I)$ բազմաձեւության համար:

Իդեալների օգտագործումը թույլ է տալիս գործի մեջ ներգրավել այնպիսի «զենքեր», ինչպիսիք են Գրյոբների բազաները: Տրված $V(f_1, \dots, f_s)$ աֆինական բազմաձեւությունը ուսումնասիրելու համար կարելի է անցնել $I = \langle f_1, \dots, f_s \rangle$ իդեալով սահմանված $V(I)$ բազմաձեւությանը, իսկ դրանից էլ՝ I իդեալի $G = \{g_1, \dots, g_s\}$ Գրյոբների բազայով (կամ մինիմալ, բերված Գրյոբների բազաներով) սահմանված $V(G)$ բազմաձեւությանը: G-ի ալգորիթմական հնարավորությունները կարող են օգտագործվել $V(G) = V(g_1, \dots, g_s)$ բազմաձեւության նկարագրության համար:

8.9.10 Օրինակ. 8.8.1 օրինակում մենք (8.33) համակարգի լուծման համար կառուցեցինք $g_1 = x_1 + x_2 + x_3 - x_4 + x_5 - 1$, $g_2 = x_3 + 3x_4$, $g_3 = x_4 - 2/7x_5 + 1/7$ մինիմալ Գրյոբների բազան եւ $g_1 = x_1 + x_2 - 1/7x_5 - 3/7$, $g_2 = x_3 + 6/7x_5 - 3/7$, $g_3 = x_4 - 2/7x_5 + 1/7$ բերված Գրյոբների բազան:

Այժմ անցնենք *փոփոխականների արտաքսման* սկզբունքին, որը հիշատակեցինք 8.8.5 դիտողության մեջ:

8.9.11 Օրինակ. Դիտարկենք այն $V(g_1, g_2)$ բազմաձեւությունը, որը տրվում է 8.5.1 օրինակի բազմանդամներով: Այլ խոսքերով՝ լուծենք *ոչ գծային* հավասարումների

$$\begin{cases} xy^2 + 3y^2 + 2x = 0 \\ x^2y + 3xy = 0 \end{cases}$$

համակարգը: $V(g_1, g_2)$ բազմաձեւությունից կարելի է անցնել $I = \langle g_1, g_2 \rangle$ իդեալով սահմանված $V(I)$ բազմաձեւությանը: Հիշենք, որ 8.6.5 օրինակում մենք արդեն ստուգել ենք, որ $\{g_1, g_2\}$-ը Գրյոբների բազա չէ: 8.6.11 օրինակում մենք I իդեալի համար ստացանք հինգ տարրերից բաղկացած $G = \{g_1, \dots, g_5\}$ Գրյոբների բազան, որը 8.7.7 օրինակում փոխարինեցինք հետեւյալ երեք տարրից բաղկացած մինիմալ Գրյոբների բազայով (ինչպես ստուգեցինք 8.7.14 օրինակում, այն նաեւ բերված Գրյոբների բազա է).

$$f_1 = x^2, \quad f_2 = y^2 + \frac{2}{3}x, \quad f_2 = xy:$$

Ըստ այս $G = \{f_1, f_2, f_3\}$ բազայի՝ կառուցենք

$$\begin{cases} x^2 = 0 \\ y^2 + 2/3x = 0 \\ xy = 0 \end{cases}$$

համակարգը: Ըստ մեր կառուցումների՝

$$V(g_1, g_2) = V(I) = V(G):$$

Այժմ մնում է «պատահաբար» նկատել, որ նոր համակարգի առաջին տողից արտաքսված է y փոփոխականը: Իսկ $x^2 = 0$ հավասարումը ունի միայն $x = 0$ արմատը: Տեղադրելով այս արժեքը մնացած տողերում, ստանում ենք.

$$\begin{cases} x = 0 \\ y^2 = 0 \\ 0 \cdot y = 0, \end{cases}$$

որտեղ երրորդ տողը ոչ մի պայման չի դնում y-ի վրա, իսկ երկրորդ տողը պահանջում է, որ $y = 0$: Այսինքն՝ համակարգի միակ լուծումը զրոյական է՝ $V(g_1, g_2) = \{(0, 0)\}$: Նկատենք, որ այս օրինակում որպես մոնոմիալ կարգավորվածություն ընտրված էր $grlex$-ը: Ինչպես կտեսնենք ստորեւ, եթե որպես մոնոմիալ կարգավորվածություն ընտրենք lex-ը, ապա փոփոխականների արտաքսումը կարելի է իրականացնել ցանկացած համակարգի համար:

Մեզ անհրաժեշտ է փոփոխականների արտաքսման հասկացության տեսական ստույգ ձեւակերպումը.

8.9.12 Սահմանում. K դաշտի վրա տրված $K[x_1, \dots, x_n]$ օղակի $I = \langle f_1, \dots, f_s \rangle$ իդեալի k-րդ *արտաքսման իդեալ* է կոչվում $I_k = I \cap K[x_{k+1}, \dots, x_n]$ իդեալը:

Քանի որ իդեալների հատումը իդեալ է, այս սահմանումը կոռեկտ է: Հասկանալի է, որ I_k-ն կազմված է I-ի այն բազմանդամներից, որոնց գրության մեջ բացակայում են $x_1, \dots, x_k$ փոփոխականները: Ընդունված է համարել, որ $I_0 = I$:

Եթե $K[x_1,\dots,x_n]$ օղակի I իդեալն ունի այնպիսի $f_1,\dots,f_s$ ծնիչ, որ, ենթադրենք, $f_s \in I_{n-1}$ եւ $f_{s-1} \in I_{n-2}$, ապա f_s-ը կարող է լինել միայն մեկ՝ x_n փոփոխականի բազմանդամ, որի արմատը հաշվելու դեպքում՝ կարելի է տեղադրել f_{s-1}-ի մեջ: Վերջինս կարող է լինել միայն x_{n-1} եւ x_n փոփոխականների բազմանդամ, եւ նախորդ քայլում գտնված x_n-ի ամեն մի հնարավոր արժեքի դեպքում f_{s-1}-ը վերածվում է մեկ փոփոխականի բազմանդամի: Դրա արմատներն էլ, իրենց հերթին, կարող են տեղադրվել f_{s-2}-ի մեջ, եթե այն պատկանում է I_{n-3}-ին եւլն:

8.9.13 Օրինակ. Գաուսի մեթոդով գծային հավասարումների համակարգերի լուծումը արտաքսման իդեալների կիրառման պարզագույն ձեւն է: 8.8.1 օրինակը մենք լուծեցինք՝ համակարգը բերելով (8.34) տեսքին, որտեղ վերջին $f_3 = x_4 - 2/7x_5 + 1/7$ բազմանդամը I_3-ից է, եւ դրա շնորհիվ հաշվվում է x_4-ի $-1/7 + 2/7\beta$ արժեքը: Իսկ մյուս բազմանդամները I_2-ից եւ I_0-ից են:

8.9.14 Օրինակ. Ոչ գծային հավասարումների 8.9.11 օրինակում մենք ունեինք՝ $f_1 \in K[x]$ եւ $f_1, f_2 \in K[x,y]$: Այս օրինակում միակ անհամապատասխանությունը 8.9.12 սահմանմանը կայանում է նրանում, որ մեկ փոփոխականից բաղկացած ենթաօղակը ստացվեց ոչ թե $K[y]$-ը, այլ $K[x]$-ը: Բայց սա էական չէ, քանի որ փոփոխականների անվանումը ոչինչ չի փոխում: Դրանից բացի, քիչ հետո կտեսնենք, որ *lex* մոնոմիալ կարգավորվածության դեպքում բազմանդամները եւ ենթաօղակները դասավորվում են ճիշտ 8.9.12 սահմանման մեջ բերված տեսքով:

8.9.15 Թեորեմ (արտաքսման թեորեմը). *Ենթադրենք K դաշտի վրա տրված $K[x_1,\dots,x_n]$ օղակի I իդեալը ըստ lex մոնոմիալ կարգավորվածության ունի G Գրյոբների բազան: Այդ դեպքում ցանկացած $k = 0,1,\dots,n-1$ համար*

$$G_k = G \cap K[x_{k+1},\dots,x_n]$$

(ոչ դատարկ) հատումը Գրյոբների բազա է I_k արտաքսման իդեալի համար:

Ապացույց: Դիտարկենք I_k արտաքսման իդեալի որեւէ f ոչ զրոյական բազմանդամ: Քանի որ f-ը նաեւ I-ից է, իսկ G-ն Գրյոբների բազա է, ապա $\mathrm{lt} f$-ը բաժանվում է G-ի որեւէ g բազմանդամի $\mathrm{lt} g$ ավագ անդամի վրա: f-ի գրառման մեջ մասնակցում են միայն $x_{k+1},\dots,x_n$ փոփոխականները, հետեւաբար, միայն նրանք են մասնակցում նաեւ $\mathrm{lt} f$-ի եւ $\mathrm{lt} g$-ի միանդամների մոնոմիալներում: Քանի որ G բազան կառուցվել է ըստ *lex* մոնոմիալ կարգավորվածության, g-ի մնացած բոլոր մոնոմիալներում նույնպես կարող են մասնակցել միայն $x_{k+1},\dots,x_n$ փոփոխականները: Ուրեմն g-ն $K[x_{k+1},\dots,x_n]$-ից է: Հետեւաբար, $g \in G_k$ եւ $\langle \mathrm{lt} I_k \rangle \subseteq \langle \mathrm{lt} G_k \rangle$: Մյուս կողմից, $\langle \mathrm{lt} I_k \rangle \supseteq \langle \mathrm{lt} G_k \rangle$, քանի որ G_k-ն ընկած է I_k-ի մեջ: ■

8.9.16 Դիտողություն. 8.9.15 արտաքսման թեորեմը ցույց է տալիս, թե ինչքան արդյունավետ են Գրյոբների բազաները աֆինական բազմաձեւությունների նկարագրության համար: $f_1, \dots, f_s \in K[x_1, \dots, x_n]$ բազմադամներով սահմանված (8.38) բազմաձեւության նկարագրության, այսինքն՝ (8.39) համակարգի լուծումների ուսումնասիրման համար պետք է ըստ lex-ի հաշվել $I = \langle f_1, \dots, f_s \rangle$ իդեալի որեւէ G Գրյոբների բազա, եւ նրա մեջ փնտրել մինիմալ քանակությամբ փոփոխականներ պարունակող բազմանդամները: Դրանց լուծումները գտնելու դեպքում այդ լուծումները տեղադրում ենք հաջորդ բազմանդամների մեջ եւլն: Այս ընթացքում կարող են պատահել նաեւ դատարկ հատումներ, որոնք լուծման վրա չեն ազդում. 8.9.13 օրինակում $n = 5$, սակայն I_4 արտաքսման իդեալը զրոյական է, քանի որ I իդեալը չի պարունակում միայն x_5-ից կախված բազմանդամներ:

8.9.17 Խնդիր. Լուծել իրական քառակուսային հավասարումների համակարգը.

$$\begin{cases} x^2 + y + z &= 1 \\ x + y^2 + z &= 1 \\ x + y + z^2 &= 1 \end{cases} :$$

Յուցում. ըստ lex մոնոմիալ կարգավորվածության այս համակարգի բազմանդամներով ծնված իդեալն ունի հետեւյալ Գրյոբների բազան.

$$\begin{aligned} g_1 &= x + y + z^2 - 1, \\ g_2 &= y^2 - y - z^2 + z, \\ g_3 &= 2yz^2 + z^2 - z^2, \\ g_4 &= z^6 - 4z^4 + 4z^3 - z^2: \end{aligned}$$

Ամենավերջին բազմանդամը կախված է միայն z-ից, եւ նրա արմատները կարելի է գտնել, քանի որ $z^6 - 4z^4 + 4z^3 - z^2 = z^2(z-1)^2(z^2 - 2z + 1)$: Ուստի z-ը կարող է ընդունել միայն չորս հնարավոր արժեքներ՝ $z \in \{0, 1, -1 - \sqrt{2},\ -1 + \sqrt{2}\}$:

8.9.18 Դիտողություն. Ասվածը, իհարկե, չի նշանակում, թե Գրյոբների բազաների միջոցով մենք կարող ենք լուծել բազմանդամներով տրվող ցանկացած հավասարումների համակարգ: Ինչպես մենք տեսանք 7.6 պարագրաֆում (տես 7.6.23 օրինակը, 7.6.24 թեորեմը եւ հարակից քննարկումը), նույնիսկ ընդամենը մեկ բազմանդամով տրվող հավասարումը կարող է անլուծելի լինել, եթե նրա աստիճանը մեծ է 4-ից: Բայց, անկախ դրանից, Գրյոբների բազաները ունեն ալգորիթմական շատ մեծ նշանակություն եւ կիրառության լայն ոլորտ: Դրանց այլ կիրառությունների կարելի է ծանոթանալ օգտվելով 8.1 պարագրաֆում հիշատակված գրականությունից:

Հավելվածներ

Հավելված 1. Համակարգչային հանրահաշվի համակարգերը

Ալգորիթմական հանրահաշվի մեթոդների կիրառմամբ ստեղծված համակարգչային ծրագրերի քանակն անցնում է երեսունից: Դրանք կարելի է խմբավորել ըստ ժամանակագրական հաջորդականության կամ ըստ օգտագործման նպատակի (դրանցից մի քանիսը ստեղծվել են միայն որոշակի բնույթի խնդիրների լուծման համար, ինչպես, օրինակ, GAP-ը, իսկ մյուսները խնդիրների լայն դասի համար են, ինչպես, օրինակ, Mathematica-ն):

Ներկայացնենք դրանցից միայն մի քանիսը: Մանրամասն տեղեկություններ կարելի է ստանալ ծրագրերի ինտերնետային կայքերից:

Համակարգչային հանրահաշվի հին համակարգերից է **Macsyma**-ն: Զարգացումը սկսվել է 1968-ից MIT-ում: Այն օգտագործում է ինչպես ալգորիթմական հանրահաշվի, այնպես էլ թվային մոտարկման մեթոդներ: Macsyma-ի միջոցով կարելի է հաշվարկներ կատարել հանրահաշվական արտահայտությունների (բանաձեւերի) հետ, ստանալ 2D եւ 3D գրաֆիկներ, հաշվել ածանցյալներ եւ ինտեգրալներ, լուծել հավասարումներ, ֆակտորիզացնել բազմանդամներ եւլն: Ծրագրի զարգացումը շարունակվել է մինչեւ 1982թ.: Այս պահին գործող պաշտոնական կայք չունի (նախկին macsyma.com կայքն այս տողերը գրելու պահին չէր գործում):

Առաջին համակարգերից է նաեւ IBM-ի նախաձեռնած **Scratchpad**-ը, որը ստեղծվել է 1965-ին եւ հետագայում փոխարինվել է Axiom-ով (տես ստորեւ): Այս պահին գործող պաշտոնական կայք չունի:

muMATH համակարգչային հանրահաշվի համակարգը ստեղծվել է 1970-ականների վերջերին: Հետագայում փոխարինվել է Derive համակարգով, որը Texas Instruments ընկերության կողմից զարգացվել է մինչեւ 2007թ.: Այս պահին գործող պաշտոնական կայք չունի:

Առաջին համակարգերից է նաեւ **Reduce**-ը, որի զարգացումը սկսվել է 1960-ականներին: 2008-ից սկսած այն տարածվում է նաեւ անվճար: Reduce համակարգի միջոցով կարելի է գործողություններ կատարել ռացիոնալ գործակիցներով բազմանդամների հետ, պարզեցնել զանազան բանաձեւեր, կատարել մատրիցային հաշվարկներ, սահմանել նոր ֆունկցիաներ, անալիտիկորեն հաշվել դիֆերենցյալներ եւ ինտեգրալներ, ֆակտորիզացնել բազմանդամներ, լուծել հանրահաշվական հավասարումներ եւլն: Այս պահին գործող կայքն է reduce-algebra.sourceforge.net

Ավելի ուշ ստեղծված համակարգերից է **Mathematica**-ն, որ ստեղծվել է Wolfram Research ընկերության կողմից 1988-ին: Այն իր հնարավորություններով ոչ միայն գերազանցում է նախորդներին, այլեւ ունի օգտագործման համար ավելի հարմար ինտերֆեյս: Mathematica-ի միջոցով կարելի է կատարել սիմվոլիկ եւ թվային հաշվարկի բազմաթիվ տիպեր, այդ թվում՝ օգտվել ներկառուցված ֆունկցիաների մեծ գրադարանից, կատարել գործողություններ մատրիցների հետ, ստեղծել 2D եւ 3D գրաֆիկներ, լուծել հավասարումներ եւ հավասարումների համակարգեր (ներառյալ դիոֆանտյան եւ մասնակի ածանցյալներով հավասարումներ), օգտագործել մի քանի փոփոխականի ֆունկցիաներ, կատարել վիճակագրական հաշվարկներ, մոդելավորել պատահական պրոցեսներ, օգտագործել ֆինանսական հաշվիչներ, կատարել խմբերի տեսության որոշ գործողություններ եւլն: Mathematica-ն անվճար չի տարածվում, սակայն կարելի է գտնել անվճար փորձնական տարբերակը: Ծրագրի կայքն է wolfram.com/mathematica

Maple համակարգը ստեղծվել է 1980թ. Maplesoft ընկերության կողմից Կանադայում: Նրա հնարավորությունների ցանկը մոտ է Mathematica-ի հնարավորություններին, սակայն կան հետեւյալ տարբերությունները. Maple-ը գերազանցում է ինտեգրալ հավասարումների, Գրյոբների բազաների եւ բազմանդամների հետ կապված հաշվարկներում: Mathematica-ն ավելի հզոր է ռեկուրենտ բանաձեւերում, հավասարումների լուծման եւ պարզեցման խնդիրներում: Maple-ն անվճար չէ, սակայն կա անվճար փորձնական տարբերակը: Կա նաեւ անվճար Maple Player անվճար ծրագիրը, որով կարելի է դիտել Maple-ով արդեն կատարված հաշվարկների արդյունքը: Ծրագրի կայքն է maplesoft.com/products/maple

Axiom համակարգը շարունակում է ավելի վաղ հիշատակված Scratchpad-ը: Նրա գործառույթները մոտ են նախորդ երկու համակարգերի հնարավորություններին: Տարբերություններից մեկն ինտերֆեյսի ունիվերսալությունն է: Axiom-ում օգտագործվում են կատեգորիաներ, որոնցով կարելի է տալ մնացած հասկացությունները՝ բազմությունների կատեգորիաները, խմբերի կատեգորիաները, օղակների

կատեգորիաները եւլն: Axiom-ը կարելի է ստանալ անվճար: Ծրագրի կայքն է axiom-developer.org

MuPAD համակարգը ստեղծվել է Գերմանիայում 1989թ. MuPAD research group-ի կողմից, սակայն 1997-ին անցել է SciFace Software GmbH & Co. KG ընկերությանը: Ծրագրի MuPAD Light տարբերակը տարածվել է անվճար, իսկ MuPAD Pro տարբերակը՝ կոմերցիոն հիմունքներով: 2008-ին SciFace-ը անցել է MathWorks ընկերությանը, որը MuPAD-ը միացրել է իր MATLAB ծրագրի Symbolic Math Toolbox հավելվածին: Այսօր MuPAD-ը գործում է հիմնականում այդ տեսքով: Ծրագրի կայքն է mathworks.com/discovery/mupad.html

GAP (Groups, Algorithms and Programming) համակարգի զարգացումը սկսվել է 1986թ. Գերմանիայում: Այս պահին համակարգը ղեկավարվում է Գերմանիայում, Միացյալ Թագավորությունում եւ Միացյալ Նահանգներում գտնվող հինգ կենտրոնների կողմից: Նախորդ համակարգերից այն տարբերվում է նրանով, որ ի սկզբանե GAP-ը ստեղծվել է հիմնականում միայն խմբերի տեսության խնդիրների լուծման համար: Այս համակարգում վերջավոր խումբը ներկայացվում է տեղադրությունների տեսքով, նկարագրվում են խմբի բոլոր ծնիչները, ենթախմբերը, ավտոմորֆիզմները եւլն: Մասնավորապես, GAP-ի տվյալների բազայում տեղադրությունների լեզվով կա մինչեւ 2000 կարգի բոլոր 423164062 խմբերի նկարագրությունը (բացառությամբ 1024-րդ կարգի խմբերի), խորանարդից ազատ կարգ ունեցող մինչեւ 50000 կարգի բոլոր 395703 խմբերի նկարագրությունը եւլն: Իր ստեղծման առաջին օրից մինչ այսօր GAP-ը տարածվել է անվճար: Ծրագրի կայքն է gap-system.org/

Magma համակարգը սկսել է զարգանալ 1990-ականներին Ավստրալիայում: Այն փոխարինում է **Cayley** համակարգին, որը զարգացվել է 1982-ից մինչեւ 1993-ը: Magma-ի կիրառման ոլորտներն են խմբերի տեսությունը, թվերի տեսությունը, հանրահաշվական երկրաչափությունը, կրիպտոգրաֆիան, կոդավորման տեսությունը, օպտիմիզացիան եւլն: Magma-ն անվճար չի տարածվում: Ծրագրի կայքն է magma.maths.usyd.edu.au/

Հավելված 2. Հիմնական ալգորիթմների ցանկ

1. **Ալգորիթմ (Էվկլիդեսի ալգորիթմը).** Տրված են R էվկլիդյան օղակի $a, b \in R$ ոչ զրոյական տարրերը: Գտնել դրանց (a, b) ամենամեծ ընդհանուր բաժանարարը: (Ալգորիթմ 2.5.4, էջ 48):
2. **Ալգորիթմ (Էվկլիդեսի ընդլայնված ալգորիթմը).** Տրված են R էվկլիդյան օղակի $a, b \in R$ ոչ զրոյական տարրերը: Գտնել դրանց (a, b) ամենամեծ ընդհանուր բաժանարարը եւ այնպիսի $u, v \in R$ տարրեր, որոնց համար, $ua + vb = (a, b)$: (Ալգորիթմ 2.5.6, էջ 49):
3. **Ալգորիթմ ($\mathbb{Z}[x]$ օղակում ամենամեծ ընդհանուր բաժանարարի հաշվումը «կեղծ բաժանումների» միջոցով).** Տրված են $f(x),\ g(x) \in \mathbb{Z}[x]$ ոչ զրոյական բազմանդամները: Հաշվել նրանց $\big(f(x),\ g(x)\big)$ ամենամեծ ընդհանուր բաժանարարը: (Ալգորիթմ 2.6.20, էջ 61):
4. **Ալգորիթմ (Լանդաու-Մինյոտի բանաձեւի միջոցով բազմանդամի ֆակտորիզացիան).** Տրված է $f(x) \in \mathbb{Z}[x]$ ոչ զրոյական բազմանդամը: Գտնել նրա ֆակտորիզացիան: (Ալգորիթմ 3.2.3, էջ 74):
5. **Ալգորիթմ (բազմանդամի մոդուլյար բաժանարարի նախապատկերի վերականգնումը).** Տրված է $f(x) \in \mathbb{Z}[x]$ բազմանդամը, եւ նրա $h(x)$ անհայտ բաժանարարի համար կարող ենք կառուցել նրա $h_p(x) = \varphi_p\big(h(x)\big)$ մոդուլյար պատկերը ըստ կամայական պարզ թվի: Գտնել $h(x)$ բաժանարարը: (Ալգորիթմ 3.2.8, էջ 80):
6. **Ալգորիթմ (ամենամեծ ընդհանուր բաժանարարի հաշվման մեծ պարզ թվի մեթոդը).** Տրված են $f(x),\ g(x) \in \mathbb{Z}[x]$ ոչ զրոյական բազմանդամները: Հաշվել նրանց $\big(f(x),\ g(x)\big)$ ամենամեծ ընդհանուր բաժանարարը: (Ալգորիթմ 3.4.8, էջ 94):
7. **Ալգորիթմ (բազմանդամների փոխադարձ պարզության որոշման մոդուլյար ալգորիթմը).** Տրված են $f(x),\ g(x) \in \mathbb{Z}[x]$ ոչ զրոյական բազմանդամները: Գտնել փոխադարձաբար պա՞րզ են արդյոք նրանք: (Ալգորիթմ 3.6.3, էջ 105):
8. **Ալգորիթմ (քառակուսիներից ազատ արտադրիչների վերլուծումը զրոյական բնութագրիչի դաշտի վրա տրված բազմանդամային օղակում):** Տրված է $f(x) \in K[x]$ բազմանդամը, որտեղ K-ն զրոյական բնութագրիչի դաշտ է: Վերլուծել այն քառակուսիներից ազատ արտադրիչների: (Ալգորիթմ 4.4.1, էջ 135):
9. **Ալգորիթմ (քառակուսիներից ազատ արտադրիչների վերլուծումը $\mathbb{Z}[x]$ օղակում):** Տրված է $f(x) \in \mathbb{Z}[x]$ բազմանդամը: Վերլուծել այն քառակուսիներից ազատ արտադրիչների: (Ալգորիթմ 4.4.4, էջ 137):
10. **Ալգորիթմ (քառակուսիներից ազատ արտադրիչների վերլուծումը վերջավոր դաշտի վրա տրված բազմանդամային օղակում):** Տրված է $f(x) \in K[x]$ բազմանդամը, որտեղ K-ն վերջավոր դաշտ է: Վերլուծել այն քառակուսիներից ազատ արտադրիչների: (Ալգորիթմ 4.5.2, էջ 144):

11. **Ալգորիթմ (մնացքների մասին չինական ալգորիթմը ամբողջ թվերի համար).** $\mathbb{Z}$ օղակում տրված են զույգ առ զույգ փոխադարձաբար պարզ $m_1, \dots, m_k$ թվերը: Կամայական $s_1, \dots, s_k \in \mathbb{Z}$ թվերի համար գտնել 6.1.1 մնացքների մասին չինական թեորեմի պայմաններին բավարարող n թիվը: (Ալգորիթմ 5.1.7, էջ 155):

12. **Ալգորիթմ (մնացքների մասին չինական ալգորիթմը բազմանդամների համար).** R դաշտի վրա սահմանված $R[x]$ բազմանդամային օղակում տրված են $m_1(x), \dots, m_k(x)$ զույգ առ զույգ փոխադարձաբար պարզ բազմանդամները: Կամայական $s_1(x), \dots s_k(x) \in R[x]$ բազմանդամների համար գտնել 6.1.5 մնացքների մասին չինական թեորեմի պայմաններին բավարարող $f(x)$ բազմանդամը: (Ալգորիթմ 5.1.11, էջ 157):

13. **Ալգորիթմ (մատրիցի որոշիչի հաշվման մեծ պարզ թվի ալգորիթմը).** Տրված է $A \in M_n(\mathbb{Z})$ մատրիցը: Հաշվել նրա $\det A$ որոշիչը: (Ալգորիթմ 5.2.4164):

14. **Ալգորիթմ (մատրիցի որոշիչի հաշվման փոքր պարզ թվերի ալգորիթմը).** Տրված է $A \in M_n(\mathbb{Z})$ մատրիցը: Հաշվել նրա $\det A$ որոշիչը: (Ալգորիթմ 5.2.6, էջ 166):

15. **Ալգորիթմ (ամենամեծ ընդհանուր բաժանարարի հաշվման փոքր պարզ թվերի մեթոդը).** Տրված են $f(x),\ g(x) \in \mathbb{Z}[x]$ ոչ զրոյական բազմանդամները: Հաշվել նրանց $\big(f(x),\ g(x)\big)$ ամենամեծ ընդհանուր բաժանարարը: (Ալգորիթմ 5.3.10, էջ 179):

16. **Ալգորիթմ (դաշտի վրա տրված երկու փոփոխականների բազմանդամային օղակում ամենամեծ ընդհանուր բաժանարարի հաշվման ալգորիթմը).** Տրված են $f(x,y)$, $g(x,y) \in K[x,y]$ ոչ զրոյական բազմանդամները, որտեղ K-ն կամայական դաշտ է: Հաշվել նրանց $\big(f(x,y),\ g(x,y)\big)$ ամենամեծ ընդհանուր բաժանարարը: (Ալգորիթմ 6.4.3, էջ 208):

17. **Ալգորիթմ ($\mathbb{Z}[x,y]$ բազմանդամային օղակում ամենամեծ ընդհանուր բաժանարարի հաշվման ալգորիթմը).** Տրված են $f(x,y),\ g(x,y) \in \mathbb{Z}[x,y]$ ոչ զրոյական բազմանդամները: Հաշվել նրանց $\big(f(x,y),\ g(x,y)\big)$ ամենամեծ ընդհանուր բաժանարարը: (Ալգորիթմ 6.4.10, էջ 214):

18. **Ալգորիթմ (դաշտի կամ $\mathbb{Z}$ օղակի վրա տրված n փոփոխականների բազմանդամային օղակում ամենամեծ ընդհանուր բաժանարարի հաշվման ալգորիթմը).** Տրված են $f = f(x_1, \dots, x_n),\ g = g(x_1, \dots, x_n) \in L[x_1, \dots, x_n]$ ոչ զրոյական բազմանդամները, որտեղ L-ը կամ ցանկացած դաշտ է կամ էլ $\mathbb{Z}$ օղակն է: Տրված է $n-1$ փոփոխականների $L[x_1, \dots, x_{n-1}]$ օղակում ամենամեծ ընդհանուր բաժանարարի հաշվման ալգորիթմը: Հաշվել $(f,\ g)$ ամենամեծ ընդհանուր բաժանարարը: (Ալգորիթմ 6.4.13, էջ 216):

19. **Ալգորիթմ (վերջավոր դաշտի վրա տրված քառակուսիներից ազատ, նորմավորված բազմանդամի ֆակտորիզացիայի ալգորիթմը).** Տրված է $f(x) \in K[x]$ քառակուսիներից ազատ, նորմավորված, ոչ զրոյական բազմանդամը, որտեղ K-ն կամայական վերջավոր դաշտ է: Գտնել $f(x)$-ի ֆակտորիզացիայի պարզ արտադրիչները: (Ալգորիթմ 7.3.14, էջ 239):

20. **Ալգորիթմ (վերջավոր դաշտի վրա տրված բազմանդամի ֆակտորիզացիայի ալգորիթմը).** Տրված է $f(x) \in K[x]$ ոչ զրոյական բազմանդամը, որտեղ K-ն կամայական վերջավոր դաշտ է: Գտնել $f(x)$-ի ֆակտորիզացիայի պարզ արտադրիչները: (Ալգորիթմ 7.3.15, էջ 241):

21. **Ալգորիթմ ($\mathbb{Z}$ օղակի վրա տրված բազմանդամի ֆակտորիզացիայի ալգորիթմը).** Տրված է $f(x) \in \mathbb{Z}[x]$ ոչ զրոյական բազմանդամը: Գտնել $f(x)$-ի ֆակտորիզացիայի պարզ արտադրիչները: (Ալգորիթմ 7.4.10, էջ 252):

22. **Ալգորիթմ ($\mathbb{Q}$ դաշտի վրա տրված բազմանդամի ֆակտորիզացիայի ալգորիթմը).** Տրված է $f(x) \in \mathbb{Q}[x]$ ոչ զրոյական բազմանդամը: Գտնել $f(x)$-ի ֆակտորիզացիայի պարզ արտադրիչները: (Ալգորիթմ 7.5.2, էջ 258):

23. **Ալգորիթմ (բազմանդամների հաջորդականության վրա բաժանման ալգորիթմը:** $K[x_1, \dots, x_n]$ օղակում ֆիքսված է որեւէ մոնոմիալ կարգավորվածություն եւ տրված է ոչ զրոյական բազմանդամների $g_1, \dots, g_s$ հաջորդականությունը: Տրված $f \in K[x_1, \dots, x_n]$ բազմանդամը ներկայացնել $f = q_1 \cdot g_1 + \cdots + q_s \cdot g_s + r$ տեսքով, որտեղ կամ $r = 0$, կամ էլ $r \neq 0$ եւ r-ի միանդամներից ոչ մեկը չի բաժանվում $\mathrm{lt} g_1, \dots, \mathrm{lt} g_s$ ավագ անդամների վրա: 8.4.5, էջ 305):

24. **Ալգորիթմ (Գրյոբների բազայի կառուցման Բուխբերգերի ալգորիթմը).** K դաշտի վրա սահմանված $K[x_1, \dots, x_n]$ բազմանդամային օղակում տրված է $g_1, \dots, g_s$ ոչ զրոյական բազմանդամներով ծնված $I = \langle g_1, \dots, g_s \rangle$ իդեալը: Հաշվել I իդեալի որեւէ G Գրյոբների բազա: (Ալգորիթմ 8.6.10, էջ 325):

25. **Ալգորիթմ (բերված Գրյոբների բազայի կառուցման ալգորիթմը).** K դաշտի վրա սահմանված $K[x_1, \dots, x_n]$ բազմանդամային օղակում տրված են I իդեալը եւ նրա G Գրյոբների բազան: Կառուցել I իդեալի բերված Գրյոբների բազան: (Ալգորիթմ 8.7.13, էջ 333):

26. **Ալգորիթմ (իդեալների հավասարության որոշման ալգորիթմը բերված Գրյոբների բազաների օգնությամբ).** K դաշտի վրա սահմանված $K[x_1, \dots, x_n]$ բազմանդամային օղակում տրված են $I = \langle g_1, \dots, g_s \rangle$ եւ $J = \langle h_1, \dots, h_m \rangle$ ոչ զրոյական իդեալները: Պարզել, թե արդյո՞ք I եւ J իդեալները հավասար են: (Ալգորիթմ 8.7.15, էջ 335):

Օգտագործված նշանակումներ

$\mathbb{N}$	բնական թվերի բազմությունը
$\mathbb{Z}$	ամբողջ թվերի բազմությունը (օղակը)
$\mathbb{Q}$	ռացիոնալ թվերի բազմությունը (օղակը, դաշտը)
$\mathbb{R}$	իրական թվերի բազմությունը (օղակը, դաշտը)
$\mathbb{C}$	կոմպլեքս թվերի բազմությունը (օղակը, դաշտը)
$\mathbb{Z}_m$	ըստ m մոդուլի մնացքների օղակը
$\mathbb{Z}_p$	ըստ p պարզ մոդուլի մնացքների դաշտը
$a \vdots b$	a թիվը (օղակի տարրը) բաժանվում է b թվի (օղակի տարրի) վրա
$f(x) \vdots g(x)$	$f(x)$ բազմանդամը բաժանվում է $g(x)$ բազմանդամի վրա
$a \mid b$	a թիվը (օղակի տարրը) բաժանում է b թիվը (օղակի տարրը) վրա
$f(x) \mid g(x)$	$f(x)$ բազմանդամը բաժանում է $g(x)$ բազմանդամը
$\deg f(x)$	$f(x)$ բազմանդամի աստիճանը
φ_p	օղակային $\varphi_p\colon \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ հոմոմորֆիզմ, մոդուլյար անցում
$a \equiv b (\mathrm{mod}\, m)$	$a, b \in \mathbb{Z}$ ամբողջ թվերը բաղդատելի են ըստ $m \in \mathbb{Z}$ մոդուլի
$x \equiv y (\mathrm{mod}\, I)$	R օղակի $x, y \in R$ տարրերը բաղդատելի են ըստ I իդեալի
$x \equiv y (\mathrm{mod}\, m)$	R կոմուտատիվ օղակի $x, y \in R$ տարրերը բաղդատելի են ըստ $m \in R$ տարրի մոդուլի
$f(x) \equiv g(x) \big(\mathrm{mod}\, m(x)\big)$	R ամբողջության տիրույթի վրա տրված $R[x]$ բազմանդամային օղակի $f(x),\ g(x) \in R[x]$ տարրերը բաղդատելի են ըստ $m(x) \in R[x]$ մոդուլի
$a \approx 1$	a թիվը (օղակի տարրը) հակադարձելի է, a օղակի տարրը ասոցացված է 1-ին
$a \approx b$	օղակի a եւ b տարրերն ասոցացված են
R^*	R օղակի հակադարձելի տարրերի բազմությունը
$f(x) \approx 1$	$f(x)$ բազմանդամը հակադարձելի է
$\mathrm{char}(R)$	օղակի բնութագրիչ, դաշտի բնութագրիչ
$f_p(x)$	մոդուլյար բազմանդամ
$R[x]$	բազմանդամային օղակ R ամբողջության տիրույթի վրա
$\mathbb{Z}[x]$	ամբողջ բազմանդամների օղակը
$\mathbb{Q}[x]$	ռացիոնալ բազմանդամների օղակը
$\mathbb{R}[x]$	իրական բազմանդամների օղակը

$\mathbb{C}[x]$	կոմպլեքս բազմանդամների օղակը
$\mathbb{Z}_p[x]$	մոդուլյար բազմանդամների օղակը
$+_m$	ըստ m մոդուլի գումար, կամ մոդուլյար գումար
$\cdot_m$	ըստ m մոդուլի արտադրյալը, կամ մոդուլյար արտադրյալը
$\binom{n}{i}$	n-ից i-ական (չկարգավորված) զուգորդությունների քանակը
$M_n(R)$	լրիվ մատրիցային օղակ R օղակի վրա
$\Re(z)$	$z = a + ib$ կոմպլեքս թվի իր իրական մասը
$\Im(z)$	$z = a + ib$ կոմպլեքս թվի իր կեղծ մասը
$\lvert z\rvert$	z կոմպլեքս թվի մոդուլը
N_f	$f(x)$ բազմանդամի բաժանարարների համար Լանդաու-Մինյոտի բանաձեւով հաշվվող գնահատականը
(a, b) կամ $\mathrm{GCD}(a, b)$	a եւ b տարրերի ամենամեծ ընդհանուր բաժանարարը
$[a, b]$ կամ $\mathrm{LCM}(a, b)$	a եւ b տարրերի ամենափոքր ընդհանուր բազմապատիկը
$(a, b) = 1$ կամ $(a, b) \approx 1$	a եւ b տարրերը են փոխադարձաբար պարզ են
$R \cong K$	R, K օղակները իզոմորֆ են
$G \cong H$	G, H խմբերը իզոմորֆ են
$\ker \varphi$	φ հոմոմորֆիզմի միջուկը
$\mathrm{im}\, \varphi$	φ հոմոմորֆիզմի պատկերը
$I = \langle A \rangle$	օղակի A բազմությամբ ծնված իդեալը
$I = \langle a_i \mid i \in I \rangle$	օղակի $\{a_i \mid i \in I\}$ տարրերով ծնված իդեալը
$R_1 \times \cdots \times R_n$ կամ $\prod_{i=1}^{n} R_i$	$R_1, \ldots, R_n$ օղակների ուղիղ արտադրյալը
$\delta(a)$	R Էվկլիդյան օղակի $a \in R$ տարրի նորմը
$\mathrm{cont}\big(f(x)\big)$	$f(x)$ բազմանդամի բովանդակությունը
$\mathrm{pp}\big(f(x)\big)$	$f(x)$ բազմանդամի $f(x)/\mathrm{cont}\big(f(x)\big)$ պրիմիտիվ մասը
$\phi_n(x)$	n-րդ ցիկլոտոմիկ բազմանդամը
$\lVert f(x)\rVert$	բազմանդամայի $\sqrt{\sum_{i=0}^{n} a_i^2}$ մետրիկան (նորմը)
N_f	$f(x)$ բազմանդամի բաժանարարի կամայական գործակցի գնահատականը հաշվված Լանդաու-Մինյոտի բանաձեւով
$N_{f,g}$	$f(x)$, $g(x)$ բազմանդամների ընդհանուր բաժանարարի կամայական գործակցի գնահատականը հաշվված Լանդաու-Մինյոտի բանաձեւով
$S_{f,g}$	$f(x)$ եւ $g(x)$ բազմանդամների Սիլվեստրի մատրիցը
$\mathrm{res}\big(f(x), g(x)\big)$	$f(x)$ եւ $g(x)$ բազմանդամների $\det S_{f,g}$ ռեզուլտանտը

$p_k\#$	առաջին k պարզ թվերի $p_k\# = p_1 \cdots p_k$ արտադրյալը
F/K	K դաշտի F ընդլայնում
a/b	օղակի a, b տարրերի ձեւական հարաբերությունը
$\mathrm{Quot}(R)$	R օղակի քանորդների դաշտը
$K(x) = \mathrm{Quot}(K[x])$	$K(x)$ օղակի քանորդների դաշտը, K դաշտի վրա տրված ռացիոնալ ֆունկցիաների դաշտը
$K(a)$	F/K ընդլայնման մեջ K դաշտին $a \in F$ տարրի ավելացումը
$K(a_1, \dots, a_n)$	F/K ընդլայնման մեջ K դաշտին $a_1, \dots, a_n \in F$ տարրերի ավելացումը
$K[x_i; i \in I]$	K դաշտի վրա $x_i; i \in I$ փոփոխականներով բազմանդամների օղակը
$[F\colon K]$	F/K ընդլայնման աստիճանը
$\overline{K}$	K դաշտի հանրահաշվական փակույթը
$A = \overline{\mathbb{Q}}$	հանրահաշվական թվերի դաշտը
$GF(p)$ կամ $\mathbb{F}_p$	ըստ p պարզ մոդուլի մնացքների $\mathbb{Z}_p$ դաշտի այլ նշանակում
$GF(p^n)$	p^n կարգի Գալուայի դաշտը
$\deg_{x_i}\left(a_{k_1,\dots,k_n} x_1^{k_1} \cdots x_n^{k_n}\right)$	$a_{k_1,\dots,k_n} x_1^{k_1} \cdots x_n^{k_n}$ միանդամի x_i-աստիճանը
$\deg\left(a_{k_1,\dots,k_n} x_1^{k_1} \cdots x_n^{k_n}\right)$	$a_{k_1,\dots,k_n} x_1^{k_1} \cdots x_n^{k_n}$ միանդամի աստիճանը
$\deg_{x_i} f(x_1, \dots, x_n)$	$f(x_1, \dots, x_n)$ բազմանդամի x_i-աստիճանը
$\deg f(x_1, \dots, x_n)$	$f(x_1, \dots, x_n)$ բազմանդամի աստիճանը
$\mathrm{rank}\, A$	A մատրիցի ռանգը
$\mathrm{im}\, A$	A օպերատորի պատկերը
$\ker A$	A օպերատորի միջուկը
$\mathrm{Aut}(F)$	F դաշտի ավտոմորֆիզմների խումբը
$\mathrm{Gal}(F/K)$	F/K ընդլայնման Գալուայի խումբը: $f(x)$ բազմանդամի Գալուայի խումբը, երբ F-ը $f(x)$-ի վերլուծության դաշտն է
θ_ψ	Գալուայի խմբի ψ իզոմորֆիզմին համապատասխան տեղափոխությունը
$[a, b] = a^{-1}b^{-1}a\,b$	$a, b \in G$ տարրերի կոմուտատորը
$[G, G] = G'$	G խմբի կոմուտանտը (կոմուտատորը)
$G^{(k)}$	G խմբի k-րդ կոմուտատորը
S_n	n-րդ աստիճանի լրիվ սիմետրիկ խումբը
A_n	n-րդ աստիճանի նշանափոխ խումբը

$\alpha = (k_1, \dots, k_n)$	աստիճանային վեկտոր
x^α	α աստիճանային վեկտորին համապատասխան մոնոմիալ
$\mathrm{multideg}\left(x_1^{k_1} \cdots x_n^{k_n}\right)$	$x_1^{k_1} \cdots x_n^{k_n}$ մոնոմիալի աստիճանային վեկտորը
$\mathrm{multideg}\, x^\alpha$	x^α մոնոմիալի աստիճանային վեկտորը
$<$	մոնոմիալ կարգավորվածություն
$\mathbb{N}_0$	բնական թվերից եւ զրոյից բաղկացած բազմությունը
$\mathbb{N}_0^n$	$\mathbb{N}_0$-ի տարրերի n-յակների բազմությունը
$<_{lex}$	լեքսիկոգրաֆիական կարգավորվածություն
$<_{grlex}$	աստիճանային լեքսիկոգրաֆիական կարգավորվածություն
$<_{grevlex}$	աստիճանային հակադարձ լեքսիկոգրաֆիական կարգավորվածություն
$\mathrm{lm} f$	f բազմանդամի ավագ մոնոմիալը
$\mathrm{lc} f$	f բազմանդամի ավագ գործակիցը
$\mathrm{lt} f$	f բազմանդամի ավագ անդամը
f_G	f բազմանդամը բազմանդամների $G = (g_1, \dots, g_s)$ հաջորդականության կամ Գրյոբների բազայի վրա բաժանման մնացորդը
$G = \{g_1, \dots, g_s\}$	$g_1, \dots, g_s$ բազմանդամներից բաղկացած Գրյոբների բազա
$\langle \mathrm{lt} I \rangle$	I իդեալի ավագ իդեալը
$I = \langle g_1, \dots, g_s \rangle$	$g_1, \dots, g_s$ տարրերով ծնվող իդեալը
$S(f, g)$	f, g բազմանդամների $\left(\frac{x^\gamma}{\mathrm{lt} f}\right) f - \left(\frac{x^\gamma}{\mathrm{lt} g}\right) g$ S-բազմանդամը
$V(f_1, \dots, f_s)$	$f_1, \dots, f_s$ բազմանդամներով սահմանված աֆինական բազմաձեւություն
$V(I)$	I իդեալով սահմանված աֆինական բազմաձեւություն
$V(G)$	G Գրյոբների բազայով սահմանված աֆինական բազմաձեւություն
I_k	$I = \langle f_1, \dots, f_s \rangle$ իդեալի $I \cap K[x_{k+1}, \dots, x_n]$ արտաքսման իդեալը

Տերմինների ցանկ

Ա

Բ

Գ

Դ

Ե

Զ

Է

Ը

Թ

Ի

Լ

Կ

Հ

Մ

Ն

Ո

Չ

Պ

Ռ

Ս

Վ

Տ

Ց

Փ

Ք

Օ

Ֆ

Գրականություն

Adams, W. W. & Loustaunau, P., 1994. *An introduction to Gröbner Bases.* s.l.:AMS.

Artin, E., 1997. *Galois Theory: Lectures Delivered at the University of Notre Dame.* s.l.:Notre Dame Mathematical Lectures, Number 2.

Beachy, B. A. & Blair, W. D., 2006. *Abstract algebra.* 3rd ed. Long Grove: Waveland Press, Inc..

Becker, T., Weispfennig, V. & Kredel, H., 1993. *Grobner Bases: A Computational Approach to Commutative Algebra.* New York: Springer-Verlag.

Berlekamp, E. R., 1967. Factoring Polynomials Over Finite Fields. *Bell System Technical Journal,* Volume 46, pp. 1853-1859.

Bokut', L. A. & Kukin, G. P., 2012. *Algorithmic and Combinatorial Algebra.* s.l.:Springer Science+Business Media Dordrecht.

Brown, W., 1971. On Euclid's Algorithm and the Computation of Polynomial Greatest Common Divisors. *J. ACM,* Volume 18, pp. 478-504.

Buchberger, B., 1965. *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal.* Innsbruck: Univ. of Innsbruck Math. Inst., Ph.D. thesis.

Buchberger, B., 1985. Gröbner bases: An algorithmic method in polynomial. *Multidimensional Systems Theory (N.K. Bose ed.), Reidel, Dordrecht,* pp. 184-232.

Buchberger, B., Collins, G. & Loos, R., 1983. *Computer Algebra Symbolic and Algebraic Computation.* 2nd ed. Wien, New York: Springer-Verlag.

Cohen, J. S., 2003 . *Computer Algebra and Symbolic Computation: Mathematical Methods.* Natick: A K Peters.

Cohn, P. M., 1965 . *Universal algebra.* New York - London: Harper & Row.

Cohn, P. M., 2000. *Introduction to ring theory.* London: Springer-Verlag .

Cohn, P. M., 2003. *Basic algebra. Groups, rings and fields.* London: Springer-Verlag .

Cohn, P. M., 2003. *Further algebra and applications..* London: Springer-Verlag .

Cox, D. A., Little, J. & O'Shea, D., 2008. *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra.* 3rd ed. New York: Springer.

Davenport, J. H., Siret, Y. & Tournier, E., 1993. *Computer algebra. Systems and algorithms for algebraic computation. Second edition.* London: Academic Press.

Dummit, D. S. & Foote, R. M., 2004. *Abstract Algebra, 3rd Edition.* s.l.:John Wiley and Sons.

Forman, A., 1970. *Numerical Methods that Work.* s.l.:Harper & Row.

Fröberg, R., 1997. *An Introduction to Gröbner Bases.* New York, Weinheim: Wiley.

Galois, É., 1846. OEuvres mathématiques d'Évariste Galois. *Journal de Mathématiques Pures et Appliquées,* Volume 10, p. 381–444.

Garrett, P. B., 2008. *Abstract Algebra.* Boca Raton: Chapman & Hall/CRC.

Grabmeier, J., Kaltofen, E. & Weispfenning, V., 2003. *Computer algebra handbook : foundations, applications, systems.* 2nd. ed. Berlin, Heidelberg, New York: Springer-Verlag.

Hilbert, D., 1890. Ueber die Theorie der algebraischen Formen. *Mathematische Annalen,* 36(4), pp. 473-534.

Hironaka, H., 1964. Resolution of singularities of an algebraic variety over a field of characteristic zero. I. *Ann. of Math.,* Volume 79, pp. 109-203.

Hironaka, H., 1964. Resolution of singularities of an algebraic variety over a field of characteristic zero. II. *Ann. of Math.,* Volume 79, pp. 205-326.

Hoffman, K. & Kunze, R., 1971. *Linear algebra. Second edition.* Englewood Cliffs: Prentice-Hall.

Holt, D. F., Eick, B. & O'Brien, E. A., 2005. *Handbook of computational group theory.* Boca, Raton, London, New York, Washington: Chapman & Hall/CRC Press.

Hulpke, A., 2010. *Notes on Computational Group Theory.* Colorado: Colorado State University.

Jenkins, M. & Traub, J., 1970. A Three-Stage Variables-Shift Iteration for Polynomial Zeros and Its Relation to Generalized Rayleigh Iteration. *Numer. Math.,* Volume 14, p. 252–263.

Kahrimanian, H. G., 1953. *Analytic diferentation by a digital computer.* Philadelphia, Pennsylvania: Thesis, Temple University.

Knuth, D., 1969. *The art of computer programming. Vol. 2. Seminumerical algorithms. Second edition. Addison-Wesley Series in Computer Science and Information Processing.* s.l.:Addison-Wesley.

Lang, S., 2002. *Algebra. Revised third edition. Graduate Texts in Mathematics, 211..* New York: Springer-Verlag.

Lazard, D., 2004. *Solving quintics in radicals, in Olav Arnfinn Laudal, Ragni Piene, The Legacy of Niels Henrik Abel.* Berlin: s.n.

Matzat, H. B., Greuel, G.-M. & Hiss, G., 1999. *Algorithmic Algebra and Number Theory, Selected Papers from a Conference Held at the University of Heidelberg, in October 1997.* Berlin, Heidelberg, New York: Springer-Verlag.

Mignotte, M., 1992. *Mathematics for computer algebra.* New York: Springer-Verlag.

Mishra, B., 1993. *Algorithmic Algebra.* New York, Berlin, Heidelberg: Springer-Verlag.

Pohst, M. & Zassenhaus, H., 1997 . *Algorithmic Algebraic Number Theory.* s.l.:Cambridge University Press .

Ralston, A. & Rabinowitz, P., 1978. *A First Course in Numerical Analysis.* s.l.:McGraw-Hill.

Renschuch, B., Roloff, H., Rasputin, G. G. & Abramson, M., 2003. Contributions to constructive polynomial ideal theory XXIII: forgotten works of Leningrad mathematician N. M. Gjunter on polynomial ideal theory. *ACM SIGSAM Bulletin,* 37(2), pp. 35-48.

Robinson, D. J. S., 1996. *A course in the theory of groups. Second edition. Graduate Texts in Mathematics, 80..* New York: Springer-Verlag.

Rotman, J. J., 1995. *An introduction to the theory of groups. Fourth edition. Graduate Texts in Mathematics, 148..* New York: Springer-Verlag.

Rotman, J. J., 2001. *Galois Theory.* 2nd ed. s.l.:Springer.

Ruffini, P., 1799. *Teoria Generale delle Equazioni, in cui si dimostra impossibile la soluzione algebraica delle equazioni generali di grado superiore al quarto.* Bologne: s.n.

Schreier, O., 1927. Die Untergruppen der freien Gruppen. *Abh. Math. Sem. Hamburg,* Volume 5, pp. 161-83.

Seress, Á., 2003. *Permutation Group Algorithms.* Cambridge: Cambridge University Press.

Sims, C. C., 1994. *Computation with Finitely-presented Groups.* Cambridge: Cambridge University Press.

Tan, K. S., Steeb, W.-H. & Hardy, Y., 2000. *Symbolic C++:An Introduction to Computer Algebra using Object-Oriented Programming.* 2nd extended and rev. ed. ed. s.l.:Springer-Verlag.

van der Waerden, B. L., 1991. *Algebra. Vol. I, Based in part on lectures by E. Artin and E. Noether. Translated from the seventh German edition by Fred Blum and John R. Schulenberger.* New York: Springer-Verlag.

van der Waerden, B. L., 1991. *Algebra. Vol. II. Based in part on lectures by E. Artin and E. Noether. Translated from the fifth German edition by John R. Schulenberger..* New York: Springer-Verlag.

von zur Gathen, J. & Gerhard, J., 2003. *Modern computer algebra.* Cambridge: Cambridge University Press.

von zur Gathen, J. & Gerhard, J., 2003. *Modern Computer Algebra, Solutions to selected exercises.* Cambridge : Cambridge University Press.

Yap, C., 1999 . *Fundamental Problems of Algorithmic Algebra.* Princeton: University Press.

Young, G. P., 1888. Solvable Quintics Equations with Commensurable Coefficients. *American Journal of Mathematics,* Volume 10, p. 99–130.

ван дер Варден, Б., 1979. *Алгебра.* Москва: Наука.

Гюнтер, Н. М., 1941. Sur les modules des formes algebraiques. *Труды тбилисского матем. инст.,* Volume 9, pp. 97-206.

Каргаполов, М. & Мерзляков, Ю. И., 1996. *Основы теории групп.* Москва: Наука.

Кон, П. М., 1968. *Универсальная алгебра.* Москва: Мир.

Кострикин, А., 1977. *Введение в алгебру.* Москва: Наука.

Кострикин, А., 1987. *Сборник задач по алгебре.* Москва: Наука.

Кострикин, А., 2000. *Введение в алгебру. Часть 2. Линейная алгебра.* Москва: ФИЗМАТЛИТ.

Кострикин, А., 2004. *Введение в алгебру. Часть 1. Основы алгебры.* Москва: ФИЗМАТЛИТ.

Кострикин, А., 2004. *Введение в алгебру. Часть 3. Основные структуры.* Москва: ФИЗМАТЛИТ.

Кострикин, А. & Манин, Ю., 1980. *Линейная алгебра и геометрия.* Москва: Наука.

Курош, А., 1965. *Курс высшей алгебры.* Москва: Наука.

Курош, А., 1967. *Теория Групп.* Москва: Наука.

Латышев, В. Н., 1987. *Комбинаторная теория колец: сложность алгебраических алгоритмов.* Москва: Издательство МГУ.

Латышев, В. Н., 1988. *Комбинаторная теория колец. Стандартные базисы.* Москва: Издательство МГУ.

Ленг, С., 1968. *Алгебра.* Москва: Мир.

Мальцев, А., 1970. *Основы линейной алгебры.* Москва: Наука.

Михалев, А. В. & Панкратьев, Е. В., 1989. *Компьютерная алгебра. Вычисления в дифференциальной и разностной алгебре.* Москва: Издательство МГУ.

Панкратьев, Е., 2007. *Элементы компьютерной алгебры.* Москва: МГУ.

Աթաբեկյան, Վ. Ս., 2005. *Հանրահաշվի ներածություն.* Երեւան: Երեւանի համալսարանի հրատարակչություն.

Ալեքսանյան, Ա., 2006. *Հանրահաշիվ Խմբեր, օղակներ, դաշտեր.* Երևան: Երեւանի համալսարանի հրատարակչություն.

Միքայելյան, Հ. Ս., 2004. *Բարձրագույն հանրահաշվի դասընթաց, 1.* Երեւան: Էդիթ Պրինտ.

Միքայելյան, Հ. Ս., 2004. *Բարձրագույն հանրահաշվի դասընթաց, 2.* Երեւան: Էդիթ Պրինտ.

Մովսիսյան, Յ. Մ., 2008. *Բարձրագույն հանրահաշիվ և թվերի տեսություն.* Երեւան: Զանգակ.

Annotation in English

Algorithmic Algebra, Commutative Rings and Fields

Vahagn H. Mikaelian

Algorithmic algebra (computer algebra) is an area of mathematics, lying in intersection of modern algebra and computer science. The first main purpose of this book is to present the subject in a course, where construction of algorithms relies on strictly and systematically presented theoretical algebraic background. In early sources on algorithmic algebra there were some incorrect applications of algebraic notions which sometimes lead to malfunctioning algorithms. Omissions of that type were corrected in literature by research papers and monographs of later period. Preparing this work we in most cases used that research, and in some cases presented our own solutions. We also offer some new algorithms and improvements of known algorithms. Deeper algebraic argumentation sometimes allows us to build the algorithms for more general cases.

Our second main aim is to present an easy-to-read text of algorithmic algebra, which can be used for individual study and for composition of university courses. In particular, the paragraphs presenting construction of algorithms are proceeded by brief introductions to respective sections of commutative rings theory and fields theory: Euclidean rings, extensions and algebraic closure of fields, unique factorization domains, linear spaces and operators on finite fields, Galois groups of fields extensions, monomial ideals, Noetherian polynomial rings, elements of algebraic geometry, etc. In order to make the text more understandable all algebraic notions and algorithms are accompanied by detailed examples. The book contains a few hundreds of examples, exercises and problems, almost all of which are new and are composed during preparation of this work.

Brief description of the chapters

The 1st introductory chapter contains an example of solution of a known problem: the phenomenon of intermediate expression swell and Knuth's method to overcome it. The purpose of this section is to give a preliminary impression about the methods of algorithmic algebra before the construction of algebraic theory is started.

The 2nd chapter briefly presents the main properties of rings and their homomorphisms which will be used in the next chapters.

The 3rd chapter sets a few numeric bounds for Euclidean rings: Landau-Mignotte's limits, bounds connected with the resultant, Sylvester matrix and the nth primorial. Ap-

plying these bounds on Euclidean rings we get a few algorithms, in particular, the big prime number's algorithm to calculate the greatest common divisor, the algorithm of checking coprime polynomials, etc.

The text becomes considerably more complicated from the 4th chapter where we present the fraction fields, algebraic and transcendent elements, minimal polynomials, and construction of the algebraic closure of any field. The theory is used to build algorithms of square-free decompositions for polynomials over finite fields and fields of zero characteristic.

The 5th chapter is devoted to the Chinese reminder theorem and to its usage in construction of algorithms for determinants and polynomials. In particular, Hadamard's bound is used to get the small primes' algorithm for determinant computation. And by combination of the Chinese reminder theorem with the methods of the 3th chapter we get the small primes' algorithm to calculate the greatest common divisor of polynomials.

The 6th chapter presents elements of the theory of unique factorization domains and introduces multivariate polynomials. Consideration of Gauss's lemma and Gauss's theorem on arbitrary unique factorization domains allows us to construct algorithms for multivariate polynomials, in particular, algorithms to compute the greatest common divisor for multivariate polynomials.

The 7th chapter studies polynomial factorization and properties of the roots of polynomials on arbitrary finite field, on the ring $\mathbb{Z}$ and on the field $\mathbb{Q}$ (including constructon of the algorithms of Berlecamp and Zessenhaus). On the fields $\mathbb{R}$ and $\mathbb{C}$ the problem of factorization is not solvable by radicals, as it is explained by the aid of Galois group. For these algorithms we use some extra theoretical background: linear spaces, operators and systems of linear equations on finite fields.

The 8th chapter is devoted to Gröbner bases. By the Buchberger's algorithm we construct the Gröbner bases for ideals of polynomial rings, which allows to solve the problems of equality of ideals, of membership in ideals and of sub-ideals. We present this theory in full, including monomial ideals, Dickson's lemma and Hilbert's theorem on finite base. Gröbner bases also are used for description of elimination ideals and for solution of problems in algebraic geometry.

Аннотация на русском языке

Алгоритмическая алгебра, коммутативные кольца и поля

Ваагн Г. Микаелян

Алгоритмическая алгебра (компьютерная алгебра) – область математики, лежащая в пересечении современной алгебры и информатики. Первая основная цель этой книги – представить этот предмет в таком изложении, где построение алгоритмов опирается на строго и систематически изложенную теоретическую алгебраическую основу. В ранних источниках по алгоритмической алгебры встречались неверные применения алгебраических понятий, что иногда приводило к неправильно работающим алгоритмам. Упущения такого типа в литературе были исправлены в статьях и монографиях более позднего периода. Работая над данным текстом мы в большинстве случаев опирались на эти исследования, а в некоторых случаях представляем и наши собственные решения. Мы также предлогаем некоторые новые алгоритмы и усовершенствования известных алгоритмов. Более глубокая алгебраической аргументация иногда позволяет нам строить алгоритмы для более общих случаев.

Нашей второй основной целью является представление по-возможности доступного текста по алгоритмической алгебры, который может быть использован и для самостоятельного изучения, и для составления университетских курсов. В частности, параграфы, представляющие построение алгоритмов, предшествуются краткими введениями в соответствующие разделы теории коммутативных колец и теории полей: евклидовы кольца, расширения и алгебраическое замыкание полей, факториальные кольца, линейные пространства и операторы над конечными полями, группы Галуа расширений полей, мономиальные идеалы, нётеровые полиномиальные кольца, элементы алгебраической геометрии и т. д.. Для более ясного изложения все алгебраические понятия и алгоритмы сопровождаются подробными примерами. Книга содержит несколько сотен примеров, упражнений и задач, почти все из которых являются новыми и были составлены в ходе подготовки настоящей работы.

Краткое описание глав

1-я вводная глава содержит пример решения конкретного вопроса: проблему разбухания промежуточных значений и метод Кнута для его решения. Цель этой главы – дать первоначальное представление о методах алгоритмической алгебры еще до начала построения алгебраической теории.

2-я глава кратко представляет основные свойства колец и их гомоморфизмов, которые будут использованы в следующих главах.

3-я глава устанавливает некоторые числовые оценки для евклидовых колец: оценки Ландау-Миньотта, границы, связанные с результантом, с матрицей Сильвестра и с n-ым приориалом. Применяя эти оценки над евклидовыми кольцами, мы получаем ряд алгоритмов, в частности, алгоритм большого простого числа для вычисления наибольшего общего делителя, алгоритм проверки взаимной простоты многочленов и т. д..

Изложение значительно усложняется с 4-ой главы, где мы представляем поля частных, алгебраические и трансцендентные элементы, минимальные многочлены, и построение алгебраического замыкания для любого поля. Эта теория используется для конструирования алгоритмов разложения на множители свободные от квадратов для многочленов над конечными полями и над полями нулевой характеристики.

5-я глава посвящена китайской теореме об остатках и его использованию в построении алгоритмов для определителей и полиномов. В частности, используется граница Адамара для получения алгоритма вычисления определителя методом малых простых чисел. А сочетание китайской теоремы с методами 3-й главы дает алгоритм малых простых чисел для вычисления наибольшего общего делителя многочленов.

6-я глава представляет элементы теории факториальных колец и вводит многочлены от нескольких переменных. Рассмотрение леммы Гаусса и теоремы Гаусса на произвольных факториальных кольцах позволяет строить алгоритмы для многочленов от нескольких переменных, в частности, алгоритм вычисления наибольшего общего делителя для многочленов от нескольких переменных.

7-я глава глава изучает полиномиальную факторизацию и свойства корней многочленов над произвольным конечным полем, над кольцом $\mathbb{Z}$ и над полем $\mathbb{Q}$ (в том числе строятся алгоритмы Берлекэмпа и Цессенхауза). А над полями $\mathbb{R}$ и $\mathbb{C}$ проблема факторизации не разрешима в радикалах, как это объясняется с помощью группы Галуа. Для этих алгоритмов мы используем дополнительную теоретическую основу: линейные пространства, операторы и систем линейных уравнений над конечными полями.

8-я глава посвящена базам Грёбнера. С помощью алгоритма Бухбергера для идеалов полиномиальных колец строятся базы Грёбнера, которые позволяют решить проблемы равенства идеалов, принадлежности идеалу, и проблему подидеала. Мы представляем эту теорию в полном объеме, включая мономиальные идеалы, лемму Диксона и теорему Гильберта о конечной базе. Базы Грёбнера также используются для описания идеалов исключения и для решения задач в алгебраической геометрии.

Երեւանի պետական համալսարան

Վ. Հ. Միքայելյան,

ԱԼԳՈՐԻԹՄԱԿԱՆ ՀԱՆՐԱՀԱՇԻՎ

կոմուտատիվ օղակներ եւ դաշտեր

Համակարգչային ձեւավորումը եւ կազմը՝
Վ. Հ. Միքայելյանի

Մասնագիտական խմբագիր՝
Հ. Ս. Միքայելյան

Տեխ. խմբագիր՝
Մ. Ա. Միքայելյան

Չափսը 70x100 1/16: Տպ. Մամուլ 24
Տպաքանակը՝ 100 օրինակ

ԵՊՀ հրատարակչություն
Երեւան, 0025, Ալեք Մանուկյան 1

ՀՐԱՏԱՐԱԿՉՈՒԹՅՈՒՆ
ԵՐԵՎԱՆ 2015