Baigtiniai kūnai

2010

Priminimas: daugianarių veiksmai

Čia ir toliau p – pirminis skaičius.

Teorema. Daugianarių aibės $\mathbb{F}_{p,n}[x], \mathbb{F}_p[x]$ yra tiesinės erdvės virš kūno $\mathbb{F}_p$.

Daugianarius galime ir dauginti: tiesiog naudokimės įprastinėmis sudėties, daugybos asociatyvumo, komutatyvumo ir distributyvumo savybėmis ir laipsnių daugybos taisyklėmis $x^n \cdot x^m = x^{n+m}$.
Teisinga tokia laipsnių kitimo taisyklė:

$$\deg(f \cdot g) = \deg(f) + \deg(g), \quad f, g \in \mathbb{F}_p[x].$$

Daugianarių dalyba

Teorema. Tegu $f, g \in \mathbb{F}_p[x]$ yra du daugianariai, $\deg(g) < \deg(f)$. Tada egzistuoja vienintelė daugianarių pora $q, r \in \mathbb{F}_p[x]$, kad

$$f(x) = q(x)g(x) + r(x), \quad 0 \leq \deg(r) < \deg(g).$$

Kaip ir sveikųjų skaičių atveju, daugianarį $q(x)$ vadinsime f dalybos iš g dalmeniu, o r – liekana.

Daugianarių dalikliai

Jeigu dalydami daugianarį $f(x)$ iš $g(x)$, gauname nulinę liekaną, t. y. $r(x) = 0$, tai sakome, kad f dalijasi iš g, arba – g yra f daliklis. Tada

$$f(x) = q(x)g(x).$$

Kiekvienas daugianaris dalijasi iš pats savęs ir iš nenulinių $\mathbb{F}_p$ elementų – nulinio laipsnio daugianarių:

$$f(x) = \alpha q(x), \quad q(x) = \alpha^{-1} f(x), \quad \alpha \neq 0.$$

Tokius $f(x)$ daliklius vadinsime trivialiaisiais.

Neskaidūs daugianariai

Teorema. Kiekvienam $n \geq 1$ yra n-ojo laipsnio daugianarių, neturinčių netrivialiųjų daliklių.

Tokie daugianariai daugeliu savybių (bet ne visomis) panašūs į pirminius skaičius.

Apibrėžimas. Daugianarį $f \in \mathbb{F}_p[x]$, neturintį netrivialiųjų daliklių vadinsime neskaidžiu.

Pavyzdžiui, visi pirmojo laipsnio daugianariai yra neskaidūs. Yra bet kokio laipsnio neskaidžių daugianarių.

Daugianarių dalikliai

Jeigu du daugianariai f_1, f_2 dalijasi iš to paties daugianario

$$d(x) = a_k x^k + \ldots + a_1 x + a_0, \ (a_k \neq 0)$$

t. y. $f_1(x) = g_1(x)d(x), f_2(x) = g_2(x)d(x)$, tai jie dalijasi ir iš daugianario su vyriausiuoju koeficientu, lygiu 1.

$$\begin{aligned} f_1(x) &= (a_k g_1(x))(a_k^{-1} d(x)), \\ f_2(x) &= (a_k g_2(x))(a_k^{-1} d(x)), \end{aligned}$$

daugianario $a_k^{-1}d(x)$ laipsnis lygus k, o vyriausiasis koeficientas lygus 1.

Daugianarių dalikliai

Apibrėžimas. Tegu $f_1, f_2 \in \mathbb{F}_p[x]$ yra du daugianariai. Jų didžiausiuoju bendruoju dalikliu vadiname didžiausiojo laipsnio daugianarį su vienetiniu vyriausiuoju koeficientu, iš kurio dalijasi ir f_1, ir f_2.

Bendrąjį didžiausiąjį daliklį žymėsime (f_1, f_2).
Bendrąjį didžiausią daliklį galima rasti Euklido algoritmu.

Daugianariai – funkcijos

Kiekvieną daugianarį

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n$$

galime interpretuoti kaip funkciją $f : \mathbb{F}_p \to \mathbb{F}_p$, priskiriančią argumentams reikšmes taip:

$$\alpha \mapsto a_0 + a_1\alpha + \ldots + a_n\alpha^n.$$

Argumentui α priskiriamą reikšmę žymėsime $f(\alpha)$. Kad išvengtume dviprasmybių, daugianarius visada žymėdami $f(x)$, o reikšmes $f(\alpha), f(\beta), \ldots$

Daugianarių šaknys

Jei $\alpha \in \mathbb{F}_p$, $f(x) \in \mathbb{F}_p[x]$ ir $f(\alpha) = 0$, tai elementą α vadinsime daugianario $f(x)$ šaknimi. Nesudėtinga įsitikinti, kad tada $f(x)$ dalijasi iš $x - \alpha$, t. y.

$$f(x) = (x - \alpha)g(x), \quad g(x) \in \mathbb{F}_p[x].$$

Jeigu

$$f(x) = (x - \alpha)^k h(x), \quad k \geq 1, \quad h(\alpha) \neq 0,$$

tai sakysime, kad šaknies α kartotinumas yra lygus k. Dar galima sakyti, kad toks daugianaris turi k vienodų (lygių α) šaknų.

Daugianarių šaknys

Svarbus teiginys apie daugianario šaknų skaičių.

Teorema. Daugianario $f \in \mathbb{F}_p[x]$ šaknų skaičius yra nedidesnis už jo laipsnį.

Kūnų plėtiniai

Daugianarių žiedai

Dalybos iš pirminio skaičiaus liekanų kūnai yra baigtiniai kūnai. Yra ir kitokių kūnų.

Pasirinkime kokį nors n-ojo laipsnio daugianarį

$$f(x) = a_0 + a_1 x + \ldots + a_n x^n, \quad a_i \in \mathbb{F}_p.$$

Daugianarių aibėje $\mathbb{F}_{p,n}[x]$ apibrėžkime daugybos veiksmą:

jei $g, h \in \mathbb{F}_{p,n}[x]$, tai $g \times_f h = g \cdot h$ dalybos iš f liekana.

Teorema. Tegu f yra n-ojo laipsnio daugianaris. Daugianarių aibė $\mathbb{F}_{p,n}[x]$ su sudėties ir daugybos veiksmais $+, \times_f$ sudaro žiedą.

Nauji kūnai

Teorema. Jeigu $f \in \mathbb{F}_p[x]$ yra neskaidus n-ojo laipsnio daugianaris, tai $\mathbb{F}_{p,n}[x]$ su sudėties ir daugybos veiksmais $+, \times_f$ sudaro kūną.

Naujo kūno elementus užrašome daugianariais. Galima nagrinėti ir daugianarius su koeficientais iš to kūno.

Sukonstruoto kūno elementams žymėti naudosime reiškinius, gautus iš daugianarių, pakeitus simbolį x į α : jei $g \in \mathbb{F}_{p,n}$, tai

$$g(x) = a_0 + \ldots + a_k x^k \mapsto a_0 + \ldots + a_k \alpha^k \mapsto (a_0, a_1, \ldots, a_{n-1});$$

čia $a_l = 0$, kai $l > k$.

Izomorfiški kūnai

Sukonstruotame naudojant neskaidų n-osios eilės daugianarį su koeficientais iš $\mathbb{F}_p$ kūne yra p^n elementų. Kūnas $\mathbb{F}_p$ yra naujojo kūno dalis.

Yra ne vienas neskaidus n-ojo laipsnio daugianaris. Koks ryšys tarp kūnų, gaunamų naudojant skirtingus to paties laipsnio daugianarius?

Izomorfiški kūnai

Apibrėžimas. Tegu K_1 ir K_2 yra du kūnai, kurių sudėties ir daugybos operacijas žymėsime $+_1, \times_1$ ir $+_2, \times_2$. Kūnus vadinsime izomorfiškais, jeigu egzistuoja abipus vienareikšmė atitiktis $\lambda : K_1 \to K_2$, su visais $a, b \in K_1$ tenkinanti sąlygas

$$\lambda(a +_1 b) = \lambda(a) +_2 \lambda(b); \quad \lambda(a \times_1 b) = \lambda(a) \times_2 \lambda(b).$$

Izomorfiški kūnai

Teorema. Jeigu $\mathbb{F}$ yra baigtinis kūnas, tai jo elementų skaičius yra pirminio skaičiaus laipsnis, t. y.

$$|\mathbb{F}| = p^n, \quad p \text{ yra pirminis skaičius, } n \geq 1.$$

Visi tiek pat elementų turintys kūnai yra izomorfiški.

Nesvarbu, kokį neskaidų n-ojo laipsnio daugianarį pasirinksime, sukonstruotas kūnas iš esmės bus tas pats. Todėl jį žymėsime tiesiog $\mathbb{F}_{p^n}$, arba $\mathbb{F}_q$, pabrėždami, kad q yra pirminio skaičiaus laipsnis.

Plėtiniai

Visi kūnai $\mathbb{F}_{p^n}$ yra pagrindinio kūno $\mathbb{F}_p$ plėtiniai, o koks jų tarpusavio ryšys?

Teorema. Jeigu natūrinis skaičius d dalija n, tai egzistuoja kūno $\mathbb{F}_{p^n}$ pokūnis (poaibis, sudarantis kūną), izomorfiškas $\mathbb{F}_{p^d}$.

Taigi, pavyzdžiui, būtų teisinga rašyti

$$\mathbb{F}_3 \subset \mathbb{F}_{3^2} \subset \mathbb{F}_{3^4} \subset \mathbb{F}_{3^{12}},$$

tačiau $\mathbb{F}_{3^4} \subset \mathbb{F}_{3^6}$ – neteisinga.

Kūnų plėtiniai

Kūne $\mathbb{F}_p$ sudėję p vienetų, gauname nulį: $1+1+\ldots+1=0$; kadangi $\mathbb{F}_p \subset \mathbb{F}_{p^m}$ kiekvienam m, tai ši lygybė teisinga visuose $\mathbb{F}_p$ plėtiniuose.
Jeigu sudėtume p kitų elementų, taip pat gautume nulį:

$$a+a+\ldots+a=(1+1+\ldots+1)\cdot a=0\cdot a=0, \quad a\in\mathbb{F}_{p^m}.$$

Teorema. Su bet kokiais elementais $\alpha,\beta\in\mathbb{F}_{p^m}$ teisinga lygybė

$$(\alpha+\beta)^p=\alpha^p+\beta^p.$$

Generuojantys elementai

Elementų eilė

Pažymėkime visų nenulinių kūno $\mathbb{F}_q$ $(q=p^m)$ elementų aibę $\mathbb{F}_q^*$. Šios aibės elementai daugybos veiksmo atžvilgiu sudaro grupę, šios grupės eilė lygi $|\mathbb{F}_q^*|=q-1=p^m-1$.
Jeigu pasirinktume elementą $\alpha\in\mathbb{F}_q^*$ ir sudarytume jo laipsnius

$$\alpha,\ \alpha^2,\ \alpha^3,\ldots$$

gautume periodinę elementų seką.
Periodas – mažiausias skaičius m, kad $\alpha^m=1$.

Apibrėžimas. Elemento $\alpha\in\mathbb{F}_q^*$ eile vadinamas mažiausias natūralusis skaičius m, su kuriuo $\alpha^m=1$. Elemento eilę žymėsime $o(\alpha)$.

Generuojantis elementas

Algebroje įrodoma, kad bet kokio baigtinės grupės elemento eilė dalija grupės eilę. Taigi bet kokiam nenuliniam elementui α skaičius $q-1$ dalijasi iš $o(\alpha)$.

Teorema. Aibėje $\mathbb{F}_q^*$ yra elementų, kurių eilės lygios $q-1$.

Apibrėžimas. Aibės $\mathbb{F}_q^*$ elementą γ, kurio eilė lygi $q-1$, vadinsime generuojančiu (arba primityviuoju) kūno $\mathbb{F}_q$ elementu.

Generuojantis elementas

Jeigu $\alpha = \gamma$ yra generuojantis elementas, tai

$$\alpha,\ \alpha^2,\ \alpha^3, \ldots$$

seka prasideda visų $\mathbb{F}_q^*$ elementų eile, kuri toliau kartojasi. Bet kuris nenulinis kūno elementas α gali būti užrašytas kaip generuojančio elemento laipsnis:

$$\alpha = \gamma^j, \quad 0 \le j < q-1.$$

Generuojantis elementas

Kaip rasti generuojančius elementus?
Teorema. Jeigu kiekvienam $q-1$ dalikliui d $(d < q-1)$ elementas $\gamma \in \mathbb{F}_q^*$ tenkina sąlygą

$$\gamma^d \neq 1,$$

tai γ – primityvusis elementas.

Pavyzdžiui, patikrinkime, ar $\gamma = 2$ yra generuojantis elementas kūne $\mathbb{F}_{23}$. Kadangi $23-1 = 2 \cdot 11$, tai pakaks apskaičiuoti tik du laipsnius:

$$2^2 = 4, \quad 2^{11} = 2(2^5)^2 = 2 \cdot 9^2 = 8,$$

taigi $\gamma = 2$ yra generuojantis elementas.

Sudėtingesnis pavyzdys

Pasirinkę neskaidų virš $\mathbb{F}_2$ daugianarį $f(x) = x^4 + x + 1$, sukonstruokime kūno $\mathbb{F}_{2^4}$ kopiją

0000	0	1000	α^3
0001	1	1001	$\alpha^3 + 1$
0010	α	1010	$\alpha^3 + \alpha$
0011	$\alpha + 1$	1011	$\alpha^3 + \alpha + 1$
0100	α^2	1100	$\alpha^3 + \alpha^2$
0101	$\alpha^2 + 1$	1101	$\alpha^3 + \alpha^2 + 1$
0110	$\alpha^2 + \alpha$	1110	$\alpha^3 + \alpha^2 + \alpha$
0111	$\alpha^2 + \alpha + 1$	1111	$\alpha^3 + \alpha^2 + \alpha + 1$

Galima skaičiuojant naudotis lygybe $\alpha^4 + \alpha + 1 = 0$.
Galbūt α yra generuojantis elementas? Kadangi $q - 1 = 15 = 3 \cdot 5$, tai pakanka įsitikinti, kad laipsniai α^3 ir α^5 nelygūs 1 :

$$\alpha^5 = \alpha^4 \cdot \alpha = (\alpha + 1) \cdot \alpha = \alpha^2 + \alpha \neq 1.$$

Elementas α yra generuojantis elementas. Taip būna ne visada.

Primityvieji daugianariai

Apibrėžimas. Jeigu $f(x)$ yra neskaidus virš kūno $\mathbb{F}_p$ daugianaris, o naudojantis juo sukonstruotame kūne $\mathbb{F}_{p^r}$ $(r = \deg(f) > 1)$ elementas α yra primityvusis, tai daugianaris $f(x)$ pats vadinamas primityviuoju.

Teorema. Daugianarių erdvėje $\mathbb{F}_p[x]$ egzistuoja bet kokio laipsnio $r > 1$ primityvieji daugianariai.
r-ojo laipsnio daugianaris $f(x)$ yra primityvus tada ir tik tada, kai jis nėra jokio daugianario $x^m - 1$ su $m < p^r - 1$ daliklis.

Todėl visada galime sukonstruoti baigtinio kūno $\mathbb{F}_q$ kopiją, kad jo nenuliniai elementai būtų reiškiami laipsniais $\alpha^j,\ j = 0, 1, \ldots, q - 2$.

Daugianarių šaknys

Jeigu sukonstravome kūno $\mathbb{F}_p$ plėtinį $\mathbb{F}_q$ $(q = p^m)$, tai galime nagrinėti daugianarius su koeficientais iš šio kūno. Pažymėkime jų aibę $\mathbb{F}_q[x]$. Akivaizdu, kad $\mathbb{F}_p[x] \subset \mathbb{F}_q[x]$.
Kiekvieną šios aibės daugianarį $f = a_0 + a_1x + \ldots + a_rx^r$ galime suvokti kaip funkciją $f : \mathbb{F}_q \to \mathbb{F}_q$:

$$\beta \mapsto a_0 + a_1\beta + \ldots + a_r\beta^r = f(\beta), \quad \beta \in \mathbb{F}_q.$$

Jei $f(\beta) = 0$, elementą β vadiname daugianario šaknimi. Tada daugianaris $f(x)$ dalijasi iš $x - \beta$. Jeigu jis dalijasi iš $(x - \beta)^m$, bet nesidalija iš $(x - \beta)^{m+1}$, sakome, kad daugianaris turi m vienodų (lygių β) šaknų, arba – šaknies β kartotinumas lygus m.

27 / 35

Daugianarių šaknys

Visiems baigtiniams kūnams teisingas teiginys, kurį suformulavome kūnui $\mathbb{F}_p$.
Teorema. Daugianario $f \in \mathbb{F}_q[x]$ šaknų skaičius nedidesnis už daugianario laipsnį.

Kadangi bet kurio nenulinio $f \in \mathbb{F}_q$ elemento β eilė dalija $q - 1$, tai šis elementas yra daugianario $x^{q-1} - 1$ šaknis. O apskritai visi, neišskiriant nei nulio, kūno elementai yra daugianario

$$g(x) = x^q - x$$

šaknys.

28 / 35

Minimalieji daugianariai

Apibrėžimas. Minimaliuoju elemento $\beta \in \mathbb{F}_q$ daugianariu vadinsime mažiausiojo laipsnio daugianarį $m_\beta(x)$ iš $\mathbb{F}_p[x]$ su vienetiniu vyriausiuoju koeficientu, kad $m_\beta(\beta) = 0$.

Kadangi β yra daugianario $m_\beta(x)$ šaknis, tai šis daugianaris turi dalytis iš $x - \beta$, dalmuo bus daugianaris iš $\mathbb{F}_q[x]$:

$$m_\beta(x) = (x - \beta)g(x), \quad g(x) \in \mathbb{F}_q[x].$$

Jeigu $\beta \in \mathbb{F}_p$, tai $m_\beta(x) = x - \beta$; jeigu β yra primityvusis kūno $\mathbb{F}_q$ elementas, tai $m_\beta(x) = x^{q-1} - 1$.

Minimalieji daugianariai

Kaip surasti elemento $\beta \in \mathbb{F}_q$ minimalųjį daugianarį?

$\mathbb{F}_{p^r}$ galime sutapatinti su tiesine erdve $\mathbb{F}_{p,r}[x]$ (ją sudaro ne didesnio kaip r-ojo laipsnio daugianariai). Ši aibė yra r-matė tiesinė erdvė virš $\mathbb{F}_p$, vadinasi, bet kuris $r+1$-o elemento rinkinys yra tiesiškai priklausomas. Elementus $1, \beta, \beta^2, \ldots, \beta^r$ galime interpretuoti kaip šios erdvės elementus.
Turėtų būti $\mathbb{F}_p$ elementai $a_0, a_1, \ldots, a_r$, kad

$$a_0 + a_1\beta + a_2\beta^2 + \ldots + a_r\beta^r = 0.$$

Suradę tokių elementų rinkinį, kad paskutiniojo nenulinio koeficiento a_j numeris j būtų kuo mažiausias, gautume minimalųjį daugianarį

$$m_\beta(x) = a_0 + a_1x + a_2x + \ldots + a_jx^j.$$

Pavyzdys

Išbandykime šį skaičiavimų būdą su kūnu $\mathbb{F}_{2^4}$ ir $\beta = \alpha^2 + 1$. Tarkime, kūnas buvo sudarytas su primityviuoju daugianariu $f(x) = x^4 + x + 1$, taigi α yra primityvusis elementas, galime naudotis lygybe $\alpha^4 = \alpha + 1$.

$1 = 1$	$1 = 0001$
$\beta = \alpha^2 + \alpha$	$\beta = 0110$
$\beta^2 = \alpha^4 + \alpha^2 = \alpha^2 + \alpha + 1$	$\beta^2 = 0111$
$\beta^3 = (\alpha^2 + \alpha + 1)(\alpha^2 + \alpha) = 1$	$\beta^3 = 0001$
$\beta^4 = \beta$	$\beta^4 = 0110$

Dydžių β^3, β^4, neprireiks. Ieškokime koeficientų $a_0, a_1, a_2 \in \mathbb{F}_p$, kad būtų

$$a_0 \cdot 0001 + a_1 \cdot 0110 + a_2 \cdot 0111 = 0000.$$

Tikrai netruksime juos surasti: $a_0 = a_1 = a_2 = 1$. Taigi minimalus daugianaris yra $m_\beta(x) = 1 + x + x^2$.

Kitas požiūris

Tegu elemento β minimalus daugianaris yra

$$m_\beta(x) = a_0 + a_1 x + \ldots + a_j x^j, \text{ t. y. } m_\beta(\beta) = a_0 + a_1\beta + \ldots + a_j\beta^j = 0.$$

Pakėlę pastarąją lygybę laipsniu p ir pasinaudoję tuo, kad $(u + v)^p = u^p + v^p$ ir $w^p = w$, kai $w \in \mathbb{F}_p$, gausime

$$m_\beta(\beta^p) = a_0 + a_1\beta^p + a_2(\beta^p)^2 + \ldots + a_j(\beta^p)^j = 0.$$

Taigi elemento β minimalaus daugianario $m_\beta(x)$ šaknis yra ir β^p, ir visi sekos

$$\beta,\ \beta^p, (\beta^p)^p = \beta^{p^2},\ \beta^{p^3},\ \beta^{p^4}, \ldots$$

skaičiai. Tačiau ne visi jie skirtingi. Kiek gi jų yra?

Minimalieji daugianariai

Pažymėkime $b = o(\beta)$, taigi m yra mažiausias natūrinis skaičius, su kuriuo $\beta^b = 1$. Tada

$$\beta,\ \beta^p, (\beta^p)^p = \beta^{p^2},\ \beta^{p^3},\ \beta^{p^4}, \dots$$

bus tiek skirtingų narių, kiek skirtingų dalybos iš b liekanų duoda skaičiai $1, p, p^2, \dots$ Šis skirtingų liekanų skaičius savo ruožtu lygus mažiausiam natūraliajam skaičiui m, su kuriuo

$$p^m \equiv 1 \pmod{b}.$$

Tada visi skaičiai $\beta, \beta^p, \beta^{p^2}, \dots, \beta^{p^{m-1}}$ bus skirtingi, o daugianaris $m_\beta(x)$ dalysis iš sandaugos

$$(x-\beta)(x-\beta^p)\cdots(x-\beta^{p^{m-1}}).$$

Minimalusis daugianaris

Teorema. Tegu $\beta \in \mathbb{F}_{p^r}$, b yra šio elemento eilė, o m yra mažiausias natūralusis skaičius, su kuriuo $p^m \equiv 1 \pmod{b}$. Tada minimalus elemento β daugianaris yra

$$m_\beta(x) = (x-\beta)(x-\beta^p)\cdots(x-\beta^{p^{m-1}}).$$

Pavyzdys

Išbandykime naująjį minimalaus elemento skaičiavimo būdą, vėl imdami kūną $\mathbb{F}_{2^4}$ ir $\beta = \alpha^2 + 1$. Skaičiuodami jau įsitikinome, kad $b = 3$. Dabar iš $2^1 \equiv 2 \pmod{3}$ ir $2^2 \equiv 1 \pmod{3}$ gauname, kad $m = 2$. Taigi

$$\begin{aligned} m_\beta(x) &= (x-\beta)(x-\beta^2) \\ &= (x-(\alpha^2+\alpha))(x-(\alpha^2+\alpha+1)) \\ &= x^2+x+1. \end{aligned}$$

Skaičiuoti reikia pasinaudojant lygybe $\alpha^4 = \alpha + 1$.