Paskaita 8

Žiedai, pozicedžiai, idealai

Pagrindinis dėmesys skiriamas baigtiniams žiedams

Apr. Trejetas $(R, +, \cdot)$ yra vadinamas **žiedu**, jeigu:

a) $(R, +)$ yra Abelio grupė,

b) $(R, \cdot)$ yra pusgrupė

c) $x \cdot (y+z) = (x \cdot y) + (x \cdot z)$

$(x+y) \cdot z = (x \cdot z) + (y \cdot z)$

$\forall x, y, z \in R$.

Žiedas yra **komutatyvus**, jeigu pusgrupė $(R, \cdot)$ yra komutatyvi.

$1 = e$.

Vienetinis ~~gra~~ žiedo elementas ~~elementas~~ yra pusgrupės $(R, \cdot)$ neutralus elementas (jis nebūtinai egzistuoja žiede, nes $(R, \cdot)$ tik pusgrupė).

Kadangi $(R, +)$ yra Abelio grupė, tai $\exists 0 \in R$ ir jis yra vienintelis. Taip pat ~~egzistuoja~~ $\forall x \in R \ \exists (-x) \in R$:.

neutralus elementas 0
vienetinis elementas 1.

Pav.

Trupletas $(\mathbb{Z}, +, \cdot)$ yra komutatyvus žiedas, vienetinis elementas 1.

$(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ irgi komutatyvus žiedas, vienetinis elementas $1+m\mathbb{Z}$.

(likėnų klasių žiedas modulio m)

Def

Jeigu R yra <u>baigtinė aibė</u>, tai žiedas <u>vadinamas baigtiniu</u>

Jeigu elementas $a \in R$ turi atvirkštinį a^{-1} (<u>sveikųjų daugybos atžvilgiu</u>), tai a vadinamas <u>vienetu</u> 1 dalijimo. (<u>vienetiniu elementu</u>)

Aišku, kad atvirkštinis elementas a^{-1} yra vienintelis

Paskaita 8 (Tęsinys)

Žiedai, požiedžiai, idealai.

(Liekamų klasių žiedai - pagr. dėmesys -3- CR - nebaigtinai grupė atžvilgiu.)

T. Žiedo R nenulio dalikliai arba gra multiplikacinė ~~dalis~~ grupė. Jeigu žiedas komutatyvus, tai ir ši grupė gra komutatyvi. Ji žymėsime R^*.

$\tilde{e} = 1$

Pav. 1 $\tilde{e} = \tilde{e}^{-1}$, tai gi nenulio dalikliu arba priklauso neutralus elementas $\tilde{e}$.
($\tilde{e}$ - neutralus daugybos atžvilgiu, nenulinis elementas)

Pav. 2 Imkime $a \in R$ nenulį dalikį.
$(a^{-1})^{-1} = a$, tai gi a^{-1} taip pat gra nenulio dalikliu.

$(a^{-1})^{-1} = b$: $\boxed{(a^{-1}) \cdot b = 1}$

bet $(a^{-1}) \cdot a = 1$

Nulio dalikliai

Def. Žiedo R elementas $a \in R$ yra vadinamas *nulio dalikliu*, jei $a \neq 0$ ir $\exists b \neq 0$, $b \in R$, toks kad

$$a \cdot b = 0 \quad (\text{arba } b \cdot a = 0)$$

Pav. 1. Žiedas $\mathbb{Z}$ neturi nulio daliklių.

Pav. 2 Imkime 2×2 matricų žiedą

$$\begin{pmatrix} 1 & 2 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 2 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Turime nulio daliklius

Def. Komutatyvusis žiedas, neturintis nulio daliklių, vadinamas *integraliniu sritimi*.

T. Nagrinėkime likčių klasių žiedą $\mathbb{Z}/m\mathbb{Z}$. ~~Tegul~~ $a + m\mathbb{Z}$ yra nulio dalikliu, $a \not\equiv 0 \bmod m$.

$\Leftrightarrow$ $1 < \gcd(a, m) < m$.

Būtinumas. Tarkime, kad $a + m\mathbb{Z}$ yra nulio dalikliu. Tada $\exists\, b + m\mathbb{Z}$, $b \not\equiv 0 \bmod m$, kad $a \cdot b \equiv 0 \bmod m$ (priešingu atveju $a \not\equiv 0 \bmod m$).

Reiškia m yra ab daliklis,
bet m nėra nei a, nei b daliklis.

Todėl $1 < \gcd(a, m) < m$

(jeigu $\gcd(a,m) = 1$, tai m bent b dalikliu)

Pakankamumas
Iš atvirkščio, jei

$$1 < \gcd(a, m) < m$$

Imkime $b = \dfrac{m}{\gcd(a,m)} \Rightarrow$ Tada $b \not\equiv 0 \mod m$.

nes $1 < b < m$.

Taigi $a \not\equiv 0 \mod m$, $b \not\equiv 0 \mod m$.

Bet

daug $a \cdot b$

$a \cdot b = (\gcd \cdot b) \cdot k$

$= m \cdot k \equiv 0 \mod m$

$a = 6$, $m = 21$, $\gcd(a,m) = 3$, $b = 7$.

$a = \gcd \cdot k$

$m = \gcd \cdot b$

Reiškia $a + m\mathbb{Z}$ yra nulio daliklis

Išvada: Jeigu m yra pirminis skaičius tai žiedas $\mathbb{Z}/m\mathbb{Z}$ nėra nulio daliklių

Def. Jeigu žiedas R yra komutatyvus ir $\forall a \in R$, $a \neq 0$ yra apverčiamas (daugybos atžv.), tai R vadinamas **kūnu** (field).

$(R, \cdot)$ yra Abelio grupė

(▲ žiedui $(R, +)$ yra Abelio grupė),

© $(R, \cdot)$ bendrosios atvejo yra Abelio pusgrupė.

Taigi svarbu patikrinti, kad $\exists$ atvirkštinis elementas a^{-1}, (simetrinis daugybos atžvilgiu)

Def. Jeigu $n = a \cdot b$, tai a yra n daliklis, o n yra a kartotinis (elem.)

Lyginių klasė $a + m\mathbb{Z}$ yra apverčiama žiede $\mathbb{Z}/m\mathbb{Z}$, $\Leftrightarrow$ $a \cdot x \equiv 1 \mod m$ turi sprendinį.

T. $a + m\mathbb{Z}$ yra apverčiamas žiedo $\mathbb{Z}/m\mathbb{Z} \iff \gcd(a, m) = 1$.

Jei a yra apverčiamas, tai a^{-1} yra vienintelis.

Įrodymas. Įrodysime, jeigu $1 \le a < m$, tai $a + m\mathbb{Z}$ yra arba apverčiamas, arba nulio daliklis. ($\Rightarrow 1 < \gcd(a, m) < m$)

Įrodymas (teoremos). Pažymėkime

$g = \gcd(a, m)$ ir $a + m\mathbb{Z}$ yra apverčiamas, t.y. $\exists\, x \in \mathbb{Z}$: $a \cdot x \equiv 1 \pmod m$

Tada 1) g yra m daliklis

2) $\Rightarrow$ g yra $a \cdot x - 1$ daliklis, nes $a \cdot x - 1 = -mk = g \cdot (\ell \cdot k)$

Bet g yra ir a daliklis, todėl (skaičiaus!)

$\Rightarrow$ g yra vienetu daliklis $\Rightarrow g = 1$.

nes ($\gcd > 0$)

$12 \times 16 = 192 + 9 = 201$

$16 \times 8 = 128 + 13 = 141$

Atvirkščiai, tarkime, kad $\underline{g = 1}$. Tada iš Euklido algoritmo teoremos žinom

~~a~~ $\exists x, y \in \mathbb{Z}$, ~~tokie~~ kad

$$ax + my = 1.$$

$$\Rightarrow ax - 1 = m(-y),$$ taigi

x yra lygties $\boxed{ax \equiv 1 \mod m.}$ sprendinys. (Euklido algoritmas leidžia rasti efektyviai tokį x.) $\underline{g}$-gal

Taigi $x + m\mathbb{Z}$ yra ~~elementas~~ galime a nesakyti

$a + m\mathbb{Z}$ atitinkamos ~~žiedo~~ žiedo $\mathbb{Z}/m\mathbb{Z}$.

Liekanų paprastųjų vienetų. Tarkime turime dar vieną atitinkamą $v + m\mathbb{Z}$. Tada

$$ax \equiv av \mod m.$$ Taigi

m yra $a(x - v)$ daliklis.

Bet $\gcd(a, m) = 1$ todėl $\boxed{x \equiv v \mod m.}$

Pav. 1) Kokios klasės (elementai) $a + 12\mathbb{Z}$ yra apverčiamos?

($m = 12$ $a = 1, 5, 7, 11$)

2) Raskite klasės $5 + 12\mathbb{Z}$ atvirkštinį (atvirkštinė yra $5 + 12\mathbb{Z}$)

T. Žiedas $\mathbb{Z}/m\mathbb{Z}$ yra laukas, $\Leftrightarrow$ m yra pirminis skaičius

Multiplikatyvioji liekanų klasių grupė

Imame tuos elementus $a + m\mathbb{Z}$, kurie turi apverčiamus elementus. Jie sudaro multiplikatyviąją grupę (daugybos atžvilgiu) $(\mathbb{Z}/m\mathbb{Z})^*$. (žymėjimas)

Jos eilė (elementų skaičius) žymima $\varphi(m)$. Funkciją vadiname Eulerio funkcija

$\varphi(m)$ - kiek skaičių aibėje $(1, 2, \ldots, m)$ yra nesikertančių $\gcd(a, m) = 1$.

Išvada 51.

Jei p - pirminis skaičius, tai

$$\varphi(p) = p - 1$$

$\varphi(12) = 4.$

$(\mathbb{Z}/12\mathbb{Z})^{\times} = \{1+12\mathbb{Z},\ 5+12\mathbb{Z},$

$7+12\mathbb{Z},\ 11+12\mathbb{Z}\}.$

Su šiomis lichomy klasių grupėmis susijusios pirminių skaičių teorijos teoremos (jos esminiai naudojamos kriptografijos viešojo rakto algoritmuose!

Eulerio teorema. $a \in \mathbb{Z}$

Jeigu $\gcd(a, m) = 1$, tai

$$a^{\varphi(m)} \equiv 1 \mod m.$$

$m = 12$, $\varphi(m) = 4$

$a = 5$, $5^4 = 625$;

$5^2 \equiv 1 \mod 12 \Rightarrow 5^4 \equiv 1 \mod 1$

(Teorine multiplikatyvi grupes $(\mathbb{Z}/m\mathbb{Z})^*$ elementų.)

$5 + 12\mathbb{Z} \in (\mathbb{Z}/12\mathbb{Z})^*$.

Mažoji Ferma teorema. Jei p - pirminis skaičius, $a \in \mathbb{Z}$ ir $\gcd(a, p) = 1$, tai

$$a^{p-1} \equiv 1 \mod p.$$

$a = 5$
$p = 3$
$5^2 = 25 \equiv 1 \mod 3$

Įrodymas $\Rightarrow$ iš Eulerio teoremos, $m = p$.

Pav. 1 Raskime 5^{121} dalmenį iš 7

$a = 5$, $m = 7$

$\gcd(5, 7) = 1$.

$5^6 \equiv 1 \mod 7$ (Ferma t.)

$5^{120} \equiv 1 \mod 7$

$5^{121} \equiv 5 \mod 7$

Pav. 2 Rasti liekana $5^{100} + 9^{100}$ dalijame iš 14.

$\gcd(5, 14) = 1$, $\gcd(9, 14) = 1$

$14 = 2 \cdot 7$ $\varphi(14) = 1 \cdot 6 = 6$

$5^6 \equiv 1 \mod 14$. $9^6 \equiv 1 \mod 14$.

$5^{96} \equiv 1 \mod 14$ $9^{96} \equiv 1 \mod 14$.

$5^2 \equiv 11 \mod 14$ $9^2 \equiv 11 \mod 14$

$5^4 \equiv 121 \equiv 9 \mod 14$ $9^4 \equiv 121 \equiv 9 \mod 14$.

$5^{100} + 9^{100} \equiv 18 \equiv 4 \mod 14$.