Algebros paskaitos informatikams

Rimantas Grigutis

3 Paskaita. Primityviųjų klasių multiplikacinė grupė.
Eulerio ir mažoji Fermat teorema ir atvirkštinės klasės radimas.
Wilsono teorema ir pirminio skaičiaus testas.
Kinų teorema liekanoms.

Primityviųjų klasių multiplikacinė grupė.

3.1 **Apibrėžimas**. *Tegu U_m yra primityviųjų klasių moduliu m aibė, t.y.*

$$U_m = \{\bar{a} |\, (a, m) = 1, 0 \leq a \leq m-1\}.$$

Aibėje U_m esančių klasių skaičius apibrėžia Eulerio funkciją φ. Žymėsime $\varphi(m)$.

Aibėje U_m yra tik atvirkštines klases turinčios $\mathbf{Z}_m$ klasės.

3.2 **Faktas.** *Eulerio funkcija pasižymi multiplikatyvumo sąvybe: jei $(m, n) = 1$, tai $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$.*

3.3 **Pavyzdžiai**. 1) Jei $p-$ pirminis skaičius, tai $\varphi(p) = p-1$, n es visi skaičiai $1, 2, ..., p-1$ yra tarpusavyje pirminiai su p.

2) $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha \left(1 - \frac{1}{p}\right)$, nes intervale $[0, p^\alpha - 1]$ tik p kartotiniai: $0, 1 \cdot p, 2 \cdot p, ..., (p^{\alpha-1} - 1) \cdot p$ nėra tarpusavyje pirminiai p.

3) Jeigu skaičiaus m kanoninis skaidinys yra $m = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$, tai $\varphi(m) = m\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_s}\right)$. Čia mes remiamės Eulerio funkcijos multiplikatyvumo savybe(3.2 Faktas).

4) $\varphi(120) = \varphi(8 \cdot 3 \cdot 5) = \varphi(2^3) \cdot \varphi(3) \cdot \varphi(5) = (2^3 - 2^2)(3-1)(5-1) = 32.$

$\varphi(120) = 120 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 32.$

3.4 **Teiginys.** *Aibė U_m sudaro multiplikacinę grupę klasių sandaugos atžvilgiu.*

Įrodymas. 1) Tegu $\bar{a}, \bar{b} \in U_m$. Tada$(a, m) = (b, m) = 1$ ir iš *1.13 Teiginio* turime, kad $(ab, m) = 1$ ir $\bar{a} \cdot \bar{b} = \overline{ab} \in U_m$.

2) Visoms likinių klasėms galioja sandaugos asociatyvumo savybė. Todėl $\bar{a}\left(\bar{b}\bar{c}\right) = \left(\bar{a}\bar{b}\right)\bar{c}$ su visais $\bar{a}, \bar{b}, \bar{c} \in U_m$.

3) $\bar{1} \in U_m$, nes $(1, m) = 1$ su visais m.

4) Jei $\bar{a} \in U_m$, tai klasė $\bar{a}$ turi atvirkštinę ir $\bar{a} \cdot \bar{a}^{-1} = \bar{1}$. Tada klasė $\bar{a}^{-1}$ irgi turi atvirkštinę $\left(\bar{a}^{-1}\right)^{-1} = \bar{a}$ ir todėl $\bar{a}^{-1} \in U_m$.

Įrodyta.

Eulerio ir mažoji Fermat teorema ir atvirkštinės klasės radimas

3.5 **Apibrėžimai.** *Skaičiai* $a_0, a_1, ..., a_{m-1}$ *paimti po vieną iš kiekvienos* Z_m *klasės vadinami* **pilnąja likinių sistema mod** m.

Skaičiai $r_1, r_2, ..., r_s$ *, paimti po vieną iš kiekvienos primityviosios* Z_m *klasės vadinami* **redukuotąja likinių sistema mod** m. Čia $s = \varphi(m)$.

3.6 **Lema.** *Tegu* $r_1, r_2, ..., r_s-$ *redukuotoji likinių sistema mod* m *ir skaičius* a *yra tarpusavyje pirminis su* m. *Tada skaičiai* $ar_1, ar_2, ..., ar_s$ *irgi yra redukuotoji likinių sistema mod* m.

Įrodymas. Su visais i, *1*$\leq i \leq s$, turime $(r_i, m) = 1$ ir $(a, m) = 1$. Pagal *1.13 teiginį* $(ar_i, m) = 1$ visais i. Skaičiai $ar_1, ..., ar_s$ yra skirtingose primityviose klasėse, nes, jei $ar_i \equiv ar_j \pmod{m}$, tai pagal *2.4.7 savybę* turime, kad $r_i \equiv r_j \pmod{m}$ ir pagal r_i ir r_j parinkimą $r_i = r_j$. Taigi, skaičiai $ar_1, ..., ar_s$, paimti po vieną iš kiekvienos primityviosios Z_m klasės, sudaro redukuotąją likinių sistemą.

Įrodyta**.**

3.7 **Išvada**. *Tegu* $r_1, ..., r_s-$ *redukuotoji likinių sistema mod* m *ir skaičius* a *yra tarpusavyje pirminis su* m. *Tada*

$$ar_1 \cdots ar_s \equiv r_1 \cdots r_s \pmod{m}.$$

Įrodymas. Iš *3.6 Lemos* turime, kad

$$U_m = \{\overline{r_1}, ..., \overline{r_s}\} = \{\overline{ar_1}, ..., \overline{ar_s}\}.$$

Todėl

$$\overline{ar_1} \cdot \cdots \cdot \overline{ar_s} = \overline{r_1} \cdot ... \cdot \overline{r_s}$$

arba

$$ar_1 \cdots ar_s \equiv r_1 \cdots r_s \pmod{m}.$$

Įrodyta.

3.8 **Eulerio teorema.** *Jeigu* $(a, m) = 1,$ *tai* $a^{\varphi(m)} \equiv 1 \pmod{m}.$

Įrodymas. Tegu $r_1, r_2, ..., r_s-$ redukuotoji likinių sistema mod m. Iš *3.7 Išvados* turime, kad

Turime

$$ar_1 \cdots ar_s \equiv r_1 \cdots r_s \pmod{m}$$

arba

$$a^s r_1 \cdots r_s \equiv r_1 \cdots r_s \pmod{m}$$

ir pagal 2.4.7 sąvybę turime, kad

$$a^s \equiv 1 \pmod{m}$$

ir

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

Įrodyta.

3.9 **Išvada.** *Jeigu* $(a, m) = 1,$ *tai* $a^{-1} \equiv a^{\varphi(m)-1} \pmod{m}.$

3.10 **Mažoji Fermat teorema.** *Jeigu* $p-$ *pirminis skaičius, o* a *nesidalija iš* p, *tai* $a^{p-1} \equiv 1 \pmod{m}.$

Įrodymas. Tai atskiras Eulerio teoremos atvejis, kai $m = p-$ pirminis, nes tada $\varphi(p) = p - 1.$

Įrodyta.

3.11 **Išvada.** *Jeigu* a *nesidalija iš pirminio skaičiaus* p, *tai* $a^{-1} \equiv a^{p-2} \pmod{p}.$

3.12 **Teiginys.** *Jeigu skaičiaus m kanoninis skaidinys yra $m = p_1 \cdot \cdots \cdot p_r$ čia $p_1, ..., p_r$ - skirtingi pirminiai skaičiai, tai su visais $a \in \mathbf{Z}$ teisinga*

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

Įrodymas. Turime

$$\varphi(m) = \varphi(p_1 \cdot \cdots \cdot p_r) = (p_1 - 1) \cdot \cdots \cdot (p_r - 1).$$

Tegu $a \in \mathbf{Z}$. Su kiekvienu pirminiu skaičiumi p_i, $1 \leq i \leq r$, galimi du atvejai:
(i) $(a, p_i) = 1$.
Tada pagal 3.10 Mažąją Fermat teoremą turime

$$a^{p_i-1} \equiv 1 \pmod{p_i}$$
$$a^{\varphi(m)} = \left(a^{p_i-1}\right)^{\frac{\varphi(m)}{p_i-1}} \equiv 1 \pmod{p_i}$$

ir padauginę iš a

$$a^{\varphi(m)+1} \equiv a \pmod{p_i}.$$

(ii) $(a, p_i) > 1$.
Tada a dalijasi iš p_i, t.y.

$$a \equiv 0 \pmod{p_i}$$

ir todėl

$$a^{\varphi(m)+1} \equiv 0 \equiv a \pmod{p_i}.$$

Abiem atvejais turime, kad skaičius $a^{\varphi(m)+1} - a$ dalijasi iš visų pirminių p_i ir pagal 1.20 Teiginį iš šių pirminių skaičių sandaugos $m = p_1 \cdot \cdots \cdot p_r$:

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

Įrodyta.

Wilsono teorema ir pirminio skaičiaus testas

3.13 **Wilsono teorema.** *Skaičius p yra pirminis tada ir tik tada, kada*

$$(p-1)! \equiv -1 \pmod{p}.$$

Įrodymas. Nagrinėkime du atvejus.

1. Tegu p - pirminis skaičius. Kūne $\mathbf{Z}_p$ visos *nenulinės* likinių klasės turi atvirkštines:

$$K_1^{-1} = K_{\psi(1)}, ..., K_{p-1}^{-1} = K_{\psi(p-1)}.$$

Nagrinėkime skaičių poras $\{1, \psi(1)\}, ..., \{p-1, \psi(p-1)\}$ ir raskime tokias, kuriose $i = \psi(i)$, t.y. $K_i^{-1} = K_i$. Turėtų būti

$$K_i^2 = K_i \cdot K_i^{-1} = K_1$$

arba

$$\begin{gathered} i^2 = 1 \pmod{p} \\ (i^2 - 1) \equiv 0 \pmod{p} \\ (i-1)(i+1) \equiv 0 \pmod{p}, \end{gathered}$$

t.y. $(i-1)(i+1)$ dalijasi iš pirminio p, o tai reiškia, kad arba $i-1$ dalijasi iš p, arba $i+1$ dalijasi iš p.

Pirmuoju atveju $i-1=0$ ir $i=1$, antruoju atveju $i+1=p$ ir $i=p-1$.

Tada turime

$$\begin{gathered} K_1 \cdot K_2 \cdots K_{p-1} = \\ K_1 \cdot \left(K_2 \cdot K_{\psi(2)}\right) \cdot \cdots \cdot \left(K_{p-2} \cdot K_{\psi(p-2)}\right) \cdot K_{p-1} = \\ K_1 \cdot K_{p-1} = K_{p-1} \end{gathered}$$

t.y.

$$K_{1 \cdot 2 \cdot \cdots \cdot (p-1)} = K_{p-1}$$

Atsižvelgus į lyginį $p-1 \equiv -1 \pmod{p}$ turėsime

$$K_{(p-1)!} = K_{-1}$$

ir

$$(p-1)! \equiv -1 \pmod{p}.$$

2. Tegu dabar $m-$ sudėtinis skaičius: $m = a \cdot b$. Nagrinėsime tris atvejus.

(1) jei $1 < a < b < m$, tai $(m-1)! = 1 \cdots a \cdots b \cdots (m-1)$ dalijasi iš $a \cdot b$ ir $(m-1)! = 0 \neq -1 \pmod{m}$;

(2) jei $m = a \cdot a = a^2$ ir $a > 2$, o $m > 4$, tai $(m-1)! = 1 \cdots (1 \cdot a) \cdots (2 \cdot a) \cdots (m-1)$ dalijasi iš a^2 ir $(m-1)! = 0 \neq -1 \pmod{m}$;

(3) jei $m = 4$, tai $(4-1)! = 3! = 6 \equiv 2 \pmod{4} \neq -1 \pmod{4}$.

Įrodyta.

Naudodamiesi Wilsono teorema galima sukonstruoti funkciją

$$f(m) = \sin\left(\frac{\pi \cdot ((m-1)! + 1)}{m}\right) = \left[\begin{array}{c} 0, \text{ jeigu } m- \text{ pirminis} \\ \neq 0, \text{ jeigu } m- \text{ sudėtinis} \end{array}\right. .$$

Tai savotiškas pirminio skaičiaus testo funkcija. Šis testas praktiškai netaikomas, nes tekų skaičiuoti $(m-1)!$, o tai labai didelis skaičius net esant pakankamai mažiems m. Pavyzdžiui jau 100! yra 128-ženklis skaičius.

Kinų teorema liekanoms ir lyginių sistemos

3.14 **Teorema(Kinų teorema liekanoms)**. Tegu $m_1, m_2, ..., m_k$ yra poromis tarpusavyje pirminiai skaičiai didesni už 1 , t.y. $(m_i, m_j) = 1$, kai $i \neq j$, ir tegu $M = m_1 \cdot m_2 \cdots m_k$. Tada

(1) lyginių sistema $\left\{\begin{array}{c} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \cdots \\ x \equiv a_k \pmod{m_k} \end{array}\right.$ yra suderinta ;

(2) Jei x_0 yra atskiras (1) sistemos sprendinys, tai visi sistemos sprendiniai yra klasėje ${}_M K_{x_0}$.

Teoremos įrodymas remiasi tokiomis lemomis.

3.15 **Lema.** *Jei* $a \equiv b \pmod{m_i}$, $1 \leq i \leq k$, *čia* $m_1, m_2, ..., m_k-$ *poromis tarpusavyje pirminiai skaičiai, tai* $a \equiv b \pmod{m_1 m_2 \cdots m_k}$.

Įrodymas. Lema įrodoma indukcija pagal n ir remiasi 1.15 teiginiu. Paliekama skaitytojui.

3.16 **Lema**. *Jeigu* $a \equiv b \pmod m$ *ir* m *dalijasi iš* d, *tai ir* $a \equiv b \pmod d$.

Įrodymas akivaizdus (aš tikuosi).

3.14 **Teoremos įrodymas**. Apibrėžkime skaičius M_i ir N_i taip

$$M_i = \frac{M}{m_i},$$
$$N_i \equiv M_i^{-1} \pmod{m_i},$$

t.y.

$$M_i N_i \equiv 1 \pmod{m_i}, \; i = 1, 2, ..., k.$$

Tai galima padaryti, nes $(M_i, m_i) = 1$.

Tegu dabar

$$x_0 = M_1 N_1 a_1 + \cdots + M_k N_k a_k.$$

Tada su visais $i, 1 \le i \le k$, teisinga

$$x_0 = M_1 N_1 a_1 + \cdots + M_k N_k a_k \equiv M_i N_i a_i \equiv a_i \pmod{m_i},$$

t.y. x_0 yra sistemos sprendinys ir sistema

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad \cdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

ekvivalenti sistemai

$$\begin{cases} x \equiv x_0 \pmod{m_1} \\ x \equiv x_0 \pmod{m_2} \\ \quad \cdots \\ x \equiv x_0 \pmod{m_k} \end{cases}.$$

Remiantis *3.15* ir *3.16 Lemomis* paskutinioji sistema yra ekvivalenti lyginiui

$$x = x_0 \pmod{m_1 m_2 \cdots m_k}.$$

Įrodyta.

3.17 **Pavyzdys**. Matyt pirmasis lyginių sistemą išsprendė kinų meistras Sun (Sun Tsu Suan-Čing, 4 a.po Kr.). Tai buvo sistema

$$\begin{cases} x \equiv 2 \bmod 3 \\ x \equiv 3 \bmod 5 \\ x \equiv 2 \bmod 7 \end{cases}$$

Išspręskime šią sistemą.
1. $M = 3 \cdot 5 \cdot 7 = 105$
2. $M_1 = \frac{105}{3} = 35, M_2 = \frac{105}{5} = 21; M_3 = \frac{105}{7} = 15.$
3. $N_1 \equiv 35^{-1} \pmod 3 = 2; N_2 \equiv 21^{-1} \pmod 5 = 1; N_3 = 15^{-1} \pmod 7 = 1.$
4. $x_0 = 35 \cdot 2 \cdot 2 + 21 \cdot 1 \cdot 3 + 15 \cdot 1 \cdot 2 = 233 \equiv 23 \pmod{105}.$
Gavome, kad visi sistemos sprendiniai yra klasėje ${}_{105}K_{23} = \{23 + 105t | t \in Z\}.$