7. ŽIEDO $\mathbb{Z}_n$ VIENETŲ GRUPĖ

6.7 pastabos. Žinome (žr. 6.5 pavyzdį, 1), kad $U(\mathbb{Z}) = (\{-1, 1\}, \cdot)$ yra 2-osios eilės ciklinė grupė.

Jeigu K – kūnas, tai grupė $U(K) = K - \{0\} = K^*$ yra vadinama multiplikacine kūno K grupe.

Atskirai panagrinėkime likinių klasių žiedą $\mathbb{Z}_n$ ir šio žiedo elementų, turinčių atvirkštinius elementus, grupę $U(\mathbb{Z}_n) = U_n$.

Iš 6.3 pavyzdžių žinome, kad ne visiems n nenuliniai žiedo $\mathbb{Z}_n$ elementai turi atvirkštinius. Pavyzdžiui, žiede $\mathbb{Z}_8$ elementai $\overline{2}$, $\overline{4}$, $\overline{6}$ neturi atvirkštinių, o elementai $\overline{1}$, $\overline{3}$, $\overline{5}$, $\overline{7}$ turi atvirkštinius. Priežastis ta, kad skaičiai 1, 3, 5, 7 yra tarpusavyje pirminiai skaičiui 8, o skaičiai 2, 4, 6 – ne.

6.8 teiginys. *1.* $U_n = \{\overline{a} \mid \text{DBD}\,(a, n) = 1\}$.

2. $|U_n| = \varphi(n)$, *kai* φ *– Oilerio funkcija.*

Įrodymas. 1. Jeigu $\overline{a} \in U_n$, tai egzistuoja toks $\overline{b} \in U_n$, kad $\overline{a}\overline{b} = \overline{1}$, t.y. $a \cdot b \equiv 1 \pmod n \iff a \cdot b = 1 + n \cdot k, k \in \mathbb{Z}$, $a \cdot b + n(-k) = 1$.

Jeigu būtų $\text{DBD}(a, n) = d > 1$, tai egzistuotų tokie c ir m, kad $a = dc$, $n = dm$ ir $d\big(cb + m(-k)\big) = 1$, t.y. 1 turėtų dalytis iš $d > 1$. Ši prieštara ir rodo, kad $\text{DBD}\,(a, n) = 1$.

Priešingai, jeigu $\text{DBD}\,(a, n) = 1$, tai atvirkštiniu Euklido[1] algoritmu galima rasti tokius skaičius b ir k, kad

$$\begin{aligned}
&a \cdot b + n \cdot k = 1,\\
&a \cdot b = 1 - n \cdot k,\\
&a \cdot b \equiv 1 \pmod n,\\
&\overline{a} \cdot \overline{b} = \overline{1} \quad \text{ir } \overline{a} \in U_n.
\end{aligned}$$

2. Įrodymas išplaukia iš Oilerio funkcijos apibrėžimo (žr. 2.17 pavyzdį).

[1] $E\upsilon\kappa\lambda\varepsilon\iota\delta\eta\varsigma$, III a. pr. Kr., – senovės graikų matematikas.

$\triangle$

Remiantis paskutiniu teiginiu įrodomi žymiųjų teoremų analogai grupei U_n.

6.9 Oilerio–Ferma teorema. *Jeigu* $\overline{a} \in U_n$, *tai* $\overline{a}^{\varphi(n)} = \overline{1}$.

Išvada. *Jeigu* $\overline{a} \in U_n$, *tai* $\overline{a}^{-1} = (\overline{a})^{\varphi(n)-1}$.

6.10 Mažoji Ferma teorema. *Jeigu* p *yra pirminis skaičius, tai visiems* $\overline{a} \in U_p$, $\overline{a}^{\,p-1} = \overline{1}$.

Išvada. *Jeigu* p *yra pirminis skaičius, tai visiems* $\overline{a} \in \mathbb{Z}_p$, $a \neq 0$, $\overline{a}^{\,-1} = \overline{a}^{\,p-2}$.

6.11 išvada. *Tegu* $n = p_1 p_2 \ldots p_r$ *yra natūralusis skaičius, čia* $p_1, p_2, \ldots, p_r$ *– skirtingi pirminiai skaičiai. Tada visiems* $\overline{a} \in \mathbb{Z}_n$ *teisinga lygybė* $\overline{a}^{\,\varphi(n)+1} = \overline{a}$, φ *– Oilerio funkcija.*

Įrodymas. Mūsų nagrinėjamu atveju $\varphi(n) = (p_1-1)(p_2-1)\ldots(p_r-1)$. Tegu $\overline{a} \in \mathbb{Z}_n$. Pirminiam skaičiui p_i, $1 \leqslant i \leqslant r$, galimi du variantai:

a) DBD $(a, p_i) = 1$, tai $a^{p_i-1} \equiv 1 \pmod{p_i}$,

$$a^{\varphi(n)} = \left(a^{p_i-1}\right)^{\frac{\varphi(n)}{p_i-1}} \equiv 1 \pmod{p_i},$$
$$a^{\varphi(n)+1} \equiv a \pmod{p_i}.$$

b) DBD $(a, p_i) > 1$, t.y. a dalijasi iš p_i ir todėl $a \equiv 0 \pmod{p_i}$,

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

Taigi visiems p_i, $1 \leqslant i \leqslant r$, $a^{\varphi(n)+1} \equiv a \pmod{p_i}$, t.y. $a^{\varphi(n)+1} - a$ dalijasi iš visų pirminių p_i, $1 \leqslant i \leqslant r$, kartu iš šių pirminių skaičių sandaugos $p_1 p_2 \ldots p_r = n$:

$$a^{\varphi(n)+1} \equiv a \pmod{n},$$
$$\overline{\mathrm{a}}^{\varphi(\mathrm{n})+1} = \overline{\mathrm{a}}.$$

$\triangle$

Remdamiesi bendrais teiginiais apie komutatyviąsias grupes, ištirsime, kokios gali būti grupės U_n elementų eilių reikšmės.

6.12 teiginys. *Tegu* $(A, \cdot)$ *yra komutatyvioji grupė, kurios eilė* $|A| = n$, *o laisvai pasirinktų grupės* A *elementų* a *ir* b *eilės yra* $\mathrm{ord}_A(a) = l$ *ir* $\mathrm{ord}_A(b) = m$. *Tada:*

1) $a^k = e_A$ tada ir tik tada, kai k dalijasi iš l;

2) jeigu DBD $(l, m) = 1$, *tai* $\mathrm{ord}_A(a \cdot b) = l \cdot m$;

3) grupėje A visada galima rasti tokį elementą c, kurio eilė yra lygi bendrajam mažiausiam skaičių l ir m kartotiniui: $\mathrm{ord}_A(c) = \mathrm{BMK}\,(l, m)$.

Įrodymas. 1) Padalijęskaičių k iš l su liekana, gausime $k = l \cdot q + r$, $0 \leqslant r < l$. Tada

$$e_A = a^k \iff e_A = \left(a^l\right)^q \cdot a^r \iff e_A = \left(e_A\right)^q a^r \iff e_A = a^r,$$
$$0 \leqslant r < l \iff r = 0.$$

2) Kai DBD $(l, m) = 1$, tai $(a \cdot b)^{l \cdot m} = \left(a^l\right)^m \cdot \left(b^m\right)^l = e_A^m \cdot e_A^l = e_A$, ir todėl remiantis 1) sandauga $l \cdot m$ dalijasi iš $\mathrm{ord}_A(a \cdot b) = s$.

Priešingai,

$$e_A = (a \cdot b)^s = a^s \cdot b^s,$$
$$a^s = \left(b^s\right)^{-1} = \left(b^{-1}\right)^s,$$
$$e_A = \left(a^l\right)^s = a^{l \cdot s} = \left(b^{-1}\right)^{l \cdot s} = \left(b^{l \cdot s}\right)^{-1} \iff e_A = b^{l \cdot s}$$

ir pagal 1) $l \cdot s$ dalijasi iš m. Bet DBD $(l, m) = 1$ ir todėl s turi dalytis iš m.

Panašiai galime įsitikinti ir tuo, kad skaičius s dalijasi iš l. Taigi $s = \mathrm{ord}_A(a \cdot b)$ dalijasi iš $m \cdot l$ (nes DBD $(l, m) = 1$). Apibendrinę gausime, kad $\mathrm{ord}_A(a \cdot b) = m \cdot l$.

3) Užrašykime skaičius l ir m skirtingų pirminių skaičių sandauga:

$$l = p_1^{\alpha_1} \ldots p_t^{\alpha_t},$$
$$m = p_1^{\beta_1} \ldots p_t^{\beta_t}.$$

Taip skaidant, gali atsitikti, kad kai kuriems i, $1 \leqslant i \leqslant t$, $\alpha_i = 0$, o kai kuriems j, $1 \leqslant j \leqslant t$, $\beta_j = 0$.

Gerai žinome, kad:

a) BMK $(l, m) = p_1^{\max\,(\alpha_1, \beta_1)} \ldots p_t^{\max\,(\alpha_t, \beta_t)}$,

b) DBD $(l, m) = p_1^{\min\,(\alpha_1, \beta_1)} \ldots p_t^{\min\,(\alpha_t, \beta_t)}$,

c) BMK $(l, m) \cdot$ DBD $(l, m) = l \cdot m$.

Nagrinėjamus skaičių l ir m skaidinius sutvarkykime taip:

$$l = p_1^{\alpha_1} \ldots p_r^{\alpha_r} p_{r+1}^{\alpha_{r+1}} \ldots p_t^{\alpha_t},$$
$$m = p_1^{\beta_1} \ldots p_r^{\beta_r} p_{r+1}^{\beta_{r+1}} \ldots p_t^{\beta_t};$$

čia

$$\alpha_i \leqslant \beta_i, \quad \text{kai} \quad 1 \leqslant i \leqslant r,$$
$$\alpha_i > \beta_i, \quad \text{kai} \quad r+1 \leqslant i \leqslant t.$$

Pažymėję $k_1 = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, $k_2 = p_{r+1}^{\beta_{r+1}} \dots p_t^{\beta_t}$, gausime

$$k_1 \cdot k_2 = p_1^{\alpha_1} \dots p_r^{\alpha_r} p_{r+1}^{\beta_{r+1}} \dots p_t^{\beta_t} = p_1^{\min\,(\alpha_1 \beta_1)} \dots p_t^{\min\,(\alpha_t \beta_t)} = \text{DBD}\,(l, m),$$

$$\operatorname{ord}\bigl(a^{k_1}\bigr) = \frac{l}{\text{DBD}\,(l, k_1)} = \frac{l}{k_1},$$
$$\operatorname{ord}\bigl(a^{k_2}\bigr) = \frac{m}{\text{DBD}\,(m, k_2)} = \frac{m}{k_2},$$
$$\operatorname{ord}\bigl(a^{k_1} \cdot a^{k_2}\bigr) = \frac{l}{k_1} \cdot \frac{m}{k_2} = \frac{l \cdot m}{\text{DBD}\,(l, m)} = \text{BMK}\,(l, m), \quad \text{nes}$$
$$\text{DBD}\left(\frac{l}{k_1}, \frac{m}{k_2}\right) = \text{DBD}\bigl(p_{r+1}^{\alpha_{r+1}} \dots p_t^{\alpha_t}, p_1^{\beta_1} \dots p_r^{\beta_r}\bigr) = 1.$$

$\triangle$

6.13 pastaba. Įrodyto teiginio 3) dalį indukcija pagal n galima apibendrinti:

3$'$) *jeigu* $a_1, a_2, \dots, a_r \in A$, *tai grupėje* A *visada galima rasti tokį elementą* c, *kurio eilė*

$$\operatorname{ord}_A(c) = \text{BMK}\,\bigl(\operatorname{ord}_A(a_1), \operatorname{ord}_A(a_2), \dots, \operatorname{ord}_A(a_r)\bigr).$$

Pirmiesiems natūraliesiems n grupės U_n yra ciklinės:

$$n = 1, \quad \varphi(1) = 1, \quad U_1 = \{1\} = \langle 1 \rangle,$$
$$n = 2, \quad \varphi(2) = 1, \quad U_2 = \{1\} = \langle 1 \rangle,$$
$$n = 3, \quad \varphi(3) = 2, \quad U_3 = \{1, 2\} = \langle 2 \rangle.$$

Generuojančio grupę U_3 elemento laipsniai mod 3:

n	$=$	1	2
2^n	$=$	2	1

$n = 4$, $\varphi(4) = 2$, $U_4 = \{1, 3\} = \langle 3 \rangle$.

Generuojančio grupę U_4 elemento laipsniai mod 4:

$$\begin{array}{ccccc} n & = & 1 & 2 \\ \hline 3^n & = & 3 & 1 \end{array}$$

$n = 5$, $\varphi(5) = 4$, $U_5 = \{1, 2, 3, 4\} = \langle 2 \rangle$.

Generuojančio grupę U_5 elemento laipsniai mod 5:

$$\begin{array}{cccccc} n & = & 1 & 2 & 3 & 4 \\ \hline 2^n & = & 2 & 4 & 3 & 1 \end{array}$$

$n = 6$, $\varphi(6) = 2$, $U_6 = \{1, 5\} = \langle 5 \rangle$.

Generuojančio grupę U_6 elemento laipsniai mod 6:

$$\begin{array}{cccc} n & = & 1 & 2 \\ \hline 5^n & = & 5 & 1 \end{array}$$

$n = 7$, $\varphi(7) = 6$, $U_7 = \{1, 2, 3, 4, 5, 6\} = \langle 3 \rangle$.

Generuojančio grupę U_7 elemento laipsniai mod 7:

$$\begin{array}{cccccccc} n & = & 1 & 2 & 3 & 4 & 5 & 6 \\ \hline 3^n & = & 3 & 2 & 6 & 4 & 5 & 1 \end{array}$$

$n = 8$, $\varphi(8) = 4$, $U_8 = \{1, 3, 5, 7\}$.

Grupės U_8 elementų laipsniai mod 8:

$$\begin{array}{cccccc} n & = & 1 & 2 & 3 & 4 \\ \hline 3^n & = & 3 & 1 & 3 & 1 \\ 5^n & = & 5 & 1 & 5 & 1 \\ 7^n & = & 7 & 1 & 7 & 1. \end{array}$$

Taigi U_8 yra pirmoji neciklinė grupė. Žemiau suformuluotas teiginys atsakys mums kodėl.

6.14 teiginys. *Grupė U_n yra ciklinė tik tada, kai $n = 1, 2, 4, p^\alpha, 2p^\alpha$; čia p – nelyginis pirminis skaičius, o α – bet kuris natūralusis skaičius.*

Ciklinę grupę U_n generuojantis elementas vadinamas primityviąja šaknimi moduliu n.

Žinome, jeigu a yra ciklinės grupės U_n primityvioji šaknis mod n, tai $\overline{a}^{\varphi(n)} = \overline{1}$ (Oilerio–Ferma teorema). Priešingai, jeigu U_n nėra ciklinė, t.y. $n \neq 1, 2, 4, p^\alpha$, $2p^\alpha$, $p > 2$ – pirminis skaičius, o $\alpha \in \mathbb{N}$, tai su visais $a \in U_n$

$$a^{\frac{\varphi(n)}{2}} = 1.$$

6.15 pavyzdys. U_{18} yra ciklinė grupė, nes $18 = 2 \cdot 3^2$, $|U_{18}| = \varphi(18) = 6$ ir $U_{18} = \{1, 5, 7, 11, 13, 17\} = \langle 5 \rangle$.

Generuojančio grupę U_{18} elemento laipsniai mod 18:

n	$=$	1	2	3	4	5	6
5^n	$=$	5	7	17	13	11	1.

Kiek iš viso yra primityviųjų šaknų moduliu n? Į šį klausimą atsakys toks teiginys:

6.16 teiginys. *Grupėje U_n yra $\varphi\big(\varphi(n)\big)$ primityviųjų šaknų moduliu n.*

Įrodymas. Jeigu grupėje U_n yra nors viena primityvioji šaknis, pavyzdžiui a, tai U_n – ciklinė grupė: $U_n = \{a, a^2, \ldots, a^{\varphi(n)}\}$, $a^{\varphi(n)} = 1$. Pagal 5.43 teiginio 4b dalį šioje ciklinėje grupėje yra $\varphi\big(\varphi(n)\big)$ generuojančių šią ciklinę grupę elementų, o tai ir yra primityviosios šaknys mod n.

$\triangle$

6.17 pastaba. Jeigu a yra primityvioji šaknis mod$n$ ir DBD$\big(k, \varphi(n)\big) = 1$, tai ir a^k, yra primityvioji šaknis mod n (žr. 5.42 teiginio 4b) dalį).

6.18 pavyzdys. Iš 6.15 pavyzdžio matėme, kad 5 yra primityvioji šaknis mod 18. Elemento $\overline{5}^k$ eilė grupėje U_{18} lygi

$$\frac{\varphi(18)}{\mathrm{DBD}\,\big(k, \varphi(18)\big)} = \frac{6}{\mathrm{DBD}(k, 6)}.$$

Šis elementas bus primityvioji šaknis mod 18 tik tada, kai $\mathrm{DBD}(k, 6) = 1$, $1 \leqslant k \leqslant 5$.

Vienas iš tokių skaičių k yra 5, todėl $5^5 \equiv 11 \pmod{18}$ – kita primityvioji šaknis (mod 18).

Dabar pateiksime algoritmą, pagal kurį galima rasti primityviąją šaknį mod p, kai $p > 2$ yra pirminis skaičius.

6.19 algoritmas. *Žinoma: p – nelyginis pirminis skaičius.*

Rezultatas: a – primityvioji šaknis mod p.

1. Randame skaičiaus $p-1$ kanoninį skaidinį:

$$p-1 = p_1^{m_1} p_2^{m_2} \dots p_k^{m_k}; \quad \text{priskiriame} \quad a := 1, i := 1.$$

2. Priskiriame $a := a + 1$.
3. Skaičiuojame $b := a^{\frac{p-1}{p_i}}$ (žr. 5.11 algoritmą).
   Jeigu $b = 1$, pereiname prie 2.
   Jeigu $b \neq 1$, tai $i := i + 1$.
4. Jeigu $i > k$, išvedame a.
   Jeigu $i \leqslant k$, pereiname prie 2.

$\triangle$

6.20 pavyzdys. U_{11} yra ciklinė grupė, $U_{11} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. $11 - 1 = 10 = 2 \cdot 5$.

Jeigu $a = 2$, tai

$$2^{\frac{10}{2}} = 2^5 = 32 \equiv 10 \bmod 11 \not\equiv 1 \pmod{11},$$
$$2^{\frac{10}{5}} = 2^2 = 4 \not\equiv 1 \pmod{11}.$$

Taigi 2 yra primityvioji šaknis mod 11. Jeigu $a = 3$, tai $3^{\frac{10}{2}} = 3^5 = 243 \equiv 1 \pmod{11}$ ir todėl 3 nėra primityvioji šaknis mod 11.

Apibendrinkime mūsų samprotavimus apie primityviųjų šaknų mod n paiešką:

Kai $n = 2$ arba $n = 4$, tai $a = n - 1$ yra primityvioji šaknis mod n.

Kai $n = p$, p – pirminis skaičius, tai primityviąsias šaknis galima rasti pagal 6.19 algoritmą.

Kai $n = p^\alpha$ arba $n = 2p^\alpha$, p – pirminis nelyginis skaičius, o $\alpha \in \mathbb{N}$, $\alpha \geqslant 2$, primityviąsias šaknis mod n galima rasti remiantis tokiu teiginiu:

6.21 teiginys. *1. Tegu a yra primityvioji šaknis* mod p, *p – pirminis nelyginis skaičius. Tada:*

a) jeigu $a^{p-1} \not\equiv 1 \pmod{p^2}$, tai a – primityvioji šaknis mod p^α, $\alpha \geqslant 2$;

b) jeigu $(a+p)^{p-1} \not\equiv 1 \pmod{p^2}$, tai $a + p$ – primityvioji šaknis mod p^α, $\alpha \geqslant 2$.

2. Tegu b yra primityvioji šaknis $\bmod p^\alpha$*, p – pirminis skaičius, $\alpha \geqslant 2$. Tada:*

a) jeigu b nelyginis, tai b – primityvioji šaknis $\bmod 2p^\alpha$*;*

b) jeigu $b+p$ nelyginis, tai $b+p^\alpha$ – primityvioji šaknis mod $2p^\alpha$.

6.22 pastabos. 1. Pastebėkime, kad tik vienas iš skaičių b arba $b+p$ yra nelyginis. Paaiškinsime 6.21 teiginio 1 dalies sąlygą:

$$\begin{aligned}(a+p)^{p-1} &= a^{p-1} + (p-1)pa^{p-2} + C_{p-1}^2 p^2 a^{p-3} + \dots \\ &\equiv a^{p-1} + (p-1)pa^{p-2} \pmod{p^2} \equiv a^{p-1} + p^2a^{p-2} - pa^{p-2} \\ &\equiv a^{p-1} - pa^{p-2} \pmod{p^2}.\end{aligned}$$

Jeigu $a^{p-1} \equiv 1 (\bmod p^2)$, tai $(a+p)^{p-1} \equiv 1 - pa^{p-2} (\bmod p^2) \not\equiv 1 (\bmod p^2)$, nes DBD $(a,p)=1$ ir $pa^{p-2} \not\equiv 0 \pmod{p^2}$.

Jeigu $(a+p)^{p-1} \equiv 1 \pmod{p^2}$, tai $1 \equiv a^{p-1} - pa^{p-2} (\bmod p^2)$ ir $a^{p-1} \not\equiv 1 \pmod{p^2}$ (priešingu atveju būtų $pa^{p-2} \equiv 0 \pmod{p^2}$ ir DBD $(a,p) \neq 1$).

2. Norint rasti primityviąją šaknį mod p^α, $p>2$ – pirminis skaičius, $\alpha \geqslant 2$, reikia:

a) pagal 6.19 algoritmą rasti a – primityviąją šaknį mod p;

b) skaičiuoti $a_1 \equiv a^{p-1} (\bmod p^2)$;

c) jeigu $a_1 \neq 1$, tai a – primityvioji šaknis mod p^α, $\alpha \geqslant 2$;
jeigu $a_1 = 1$, tai $a+p$ – primityvioji šaknis mod p^α, $\alpha \geqslant 2$.

3. Norint rasti primityviąją šaknį mod $2p^\alpha$, $p>2$ – pirminis skaičius, $\alpha \geqslant 2$, reikia:

a) pagal 6.19 algoritmą rasti b – primityviąją šaknį mod p;

b) jeigu b nelyginis, tai b – primityvioji šaknis mod $2p^\alpha$;
jeigu b lyginis, tai $b+p^\alpha$ – primityvioji šaknis mod $2p^\alpha$.

Dabar panagrinėkime neciklines U_n grupes. Natūralu pradėti nuo atvejo, kai $n = 2^\alpha$, $\alpha \geqslant 3$, $\alpha \in \mathbb{N}$.

6.23 teiginys. *$U_{2^\alpha} \approx \mathbb{Z}_2 \times \mathbb{Z}_{2^{\alpha-2}}$, kur $\mathbb{Z}_2$, $\mathbb{Z}_{2^{\alpha-2}}$ yra adicinės ciklinės grupės.*

Grupėje U_{2^α} nesunkiai galime rasti elementą, kurio eilė šioje grupėje yra maksimali. Tai elementas $5 \in U_{2^\alpha}$, nes iš $\operatorname{ord}_{U_{2^\alpha}}(5) = 2^{\alpha-2}$ gauname, kad 2^α dalijasi iš $\operatorname{ord}_{U_{2^\alpha}}(5)$ ir $\operatorname{ord}_{U_{2^\alpha}}(5) \leqslant 2^{\alpha-1}$ (įrodykite!). Tada

$$\begin{aligned} 5^{2^k} \equiv 1 \pmod{2^\alpha} &\iff (5^{2^k} - 1) \equiv 0 \pmod{2^\alpha} \\ &\iff (5-1)(5^{2^0}+1)(5^{2^1}+1)\dots(5^{2^{k-1}}+1) \equiv 0 \pmod{2^\alpha} \\ &\iff (5+1)(5^2+1)(5^{2^2}+1)\dots(5^{2^{k-1}}+1) \equiv 0 \pmod{2^{\alpha-2}}\end{aligned}$$

ir, kai $k = \alpha - 1$,

$$(5+1)(5^2+1)(5^{2^2}+1)\dots(5^{2^{\alpha-2}}+1) \equiv 0 \pmod{2^{\alpha-2}}.$$

6.24 pastaba. Remiantis pastaruoju teiginiu, bet kurį grupės U_{2^α} elementą galima užrašyti taip:

$$(-1)^{\,i}5^j, \quad 0 \leqslant i \leqslant 1, \quad 1 \leqslant j \leqslant 2^{\alpha-1}.$$

Neciklinėse grupėse U_n yra svarbūs tie elementai, kurių eilė šioje grupėje yra maksimali. Tai maksimalios eilės grupės elementai.

6.25 teiginys. *Jeigu a yra maksimalios eilės grupės U_n elementas, tai bet kuriam $b \in U_n$ teisinga*

$$\mathrm{ord}_{U_n}(a) \quad \textit{dalijasi iš} \quad \mathrm{ord}_{U_n}(b).$$

Įrodymas. Iš 6.12 teiginio 3) dalies žinome, kad egzistuoja toks $c \in U_n$, kad $\mathrm{ord}_{U_n}(c) = \mathrm{BMK}\big(\mathrm{ord}_{U_n}(a), \mathrm{ord}_{U_n}(b)\big)$. Bet $\mathrm{ord}_{U_n} a$ yra maksimalus grupėje, todėl

$$\begin{aligned}\mathrm{ord}_{U_n}(c) = &\mathrm{BMK}\ \big(\mathrm{ord}_{U_n}(a), \mathrm{ord}_{U_n}(b)\big) \leqslant \mathrm{ord}_{U_n}(a),\\ &\mathrm{BMK}\ \big(\mathrm{ord}_{U_n}(a), \mathrm{ord}_{U_n}(b)\big) = \mathrm{ord}_{U_n}(a)\end{aligned}$$

ir todėl $\mathrm{ord}_{U_n}(a)$ dalijasi iš $\mathrm{ord}_{U_n}(b)$.

△

6.26 apibrėžimas. *Funkcija $\lambda : \mathbb{N} \to \mathbb{N}$,*

$$\lambda(n) = \max\{\mathrm{ord}_{U_n}(a) \mid a \in U_n\},$$

vadinama maksimalios eilės funkcija.

6.27 pavyzdžiai.

$\lambda(1) = \varphi(1) = 1,$

$\lambda(2) = \varphi(2) = 1,$

$\lambda(4) = \varphi(4) = 2,$

$\lambda(p^\alpha) = \varphi\left(p^\alpha\right) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1), \quad p > 2$ – pirminis skaičius,

$\lambda(2p^\alpha) = \varphi\left(2p^\alpha\right) = (p-1)p^{\alpha-1}, \quad p > 2$ – pirminis skaičius,

$\lambda(2^\alpha) = 2^{\alpha-2}, \quad \alpha \geqslant 3.$

Maksimalios eilės funkcijos λ reikšmėms $\lambda(n)$ skaičiuoti mes pasitelksime skaičiaus n kanoninį skaidinį $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, $p_1, p_2, \dots, p_r$ – skirtingi pirminiai skaičiai, ir funkcijos λ reikšmes $\lambda\bigl(p_1^{\alpha_1}\bigr), \lambda\bigl(p_2^{\alpha_2}\bigr), \lambda\bigl(p_r^{\alpha_r}\bigr)$. Tam talkins

6.28 kinų teorema liekanoms. *Tegu $m_1, m_2, \dots, m_k$ yra poromis tarpusavyje pirminiai skaičiai, t.y.* DBD $(m_i, m_j) = 1$, *kai $i \neq j$, $M = m_1 m_2 \dots m_k$; $a_1, a_2, \dots, a_k$ – bet kurie sveikieji skaičiai. Lyginių sistema*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ x &\equiv a_2 \pmod{m_2}, \\ &\dots\dots\dots\dots\dots\dots \\ x &\equiv a_k \pmod{m_k} \end{aligned} \qquad (*)$$

turi vienintelį sprendinį x moduliu M.

Kitais žodžiais sakant, turime bijekciją $f : \mathbb{Z}_M \to \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \dots \times \mathbb{Z}_{m_k}$, kuri bet kuriam x, $0 \leqslant x < M - 1$, priskiria $f(x) = \bigl(a_1, a_2, \dots, a_k\bigr)$; čia $a_i \equiv x \bmod m_i$, $i = 1, 2, \dots, k$.

Įrodymą pateiksime algoritmais. Iš pradžių nurodysime būdą, kaip išspręsti $(*)$ sistemą, kai $k = 2$.

6.29 algoritmas. *Žinoma: $m_1, m_2 > 1$ – tarpusavyje pirminiai skaičiai; a_1, a_2 – sveikieji skaičiai.*

Rezultatas: toks x, kad $x \equiv a_1 \pmod{m_1}$, $x \equiv a_2 \pmod{m_2}$.

1. Jeigu $a_1 \geqslant 0$, tai $x :=$ LIEKANA (a_1, m_1) [skaičiaus a_1 dalybos su liekana iš m_1 liekanos priskyrimas].
2. $m_1^{-1} := m_1^{-1} \pmod{m_2}$ [žr. 6.8 ir 6.9 algoritmus].
3. $q :=$ LIEKANA $\bigl(m_1^{-1}(a_2 - x), m_2\bigr)$.
4. $x := x + m_1 q$.

△

Remdamiesi šiuo algoritmu, įrodysime kinų teoremą, kai $n = 2$. Lyginys $x \equiv a_1 \pmod{m_1}$ yra visada išsprendžiamas, todėl $x = a_1 + m_1 q$; čia q – sveikasis skaičius. Šį skaičių rasime, naudodamiesi tuo, kad $x \equiv a_2 \pmod{m_2}$ ir todėl $a_1 + m_1 q \equiv a_2 \pmod{m_2}$, $q = (a_2 - a_1) m_1^{-1} \pmod{m_2}$. Taigi $q = m_1^{-1}(a_2 - a_1) + r m_2$, $r \in \mathbb{Z}$ ir

$$\begin{aligned} x &= a_1 + m_1\bigl(m_1^{-1}(a_2 - a_1) + r m_2\bigr) \\ &= a_1 + m_1 m_1^{-1}(a_2 - a_1) + r m_1 m_2 \\ &\equiv a_1 + m_1 m_1^{-1}(a_2 - a_1) \pmod{m_1 m_2} \end{aligned}$$

(išraiškose m_1^{-1} yra mod m_2).

Sprendinio vienatinumas. Tegu x ir y yra du nagrinėjamos lyginių sistemos sprendiniai. Tada

$$x - y \equiv 0 \pmod{m_1},$$
$$x - y \equiv 0 \pmod{m_2}$$

ir $x - y \equiv 0 \pmod{m_1 m_2}$, nes DBD $(m_1, m_2) = 1$.

△

6.30 pavyzdys.

$$x \equiv 15 \pmod{6},$$
$$x \equiv 4 \pmod{11}.$$

1. $15 = 6 \cdot 2 + 3$, todėl pirmasis mūsų sistemos lyginys keičiamas lyginiu $x \equiv 3 \pmod{6}$.

2. $x = 3 + 6q$.

3. DBD $(6, 11) = 1$ – pirminis skaičius, todėl $6^{-1} = 6^{\varphi(11)-1} = 6^9 \equiv 2 \pmod{11}$.

4. $q \equiv 2\,(4 - 3) \pmod{11} = 2 \pmod{11}$ ir
$x = 3 + 6 \cdot 2 = 15 \pmod{6 \cdot 11} = 15 \pmod{66}$.

Patikrinimas.

$$15 = 2 \cdot 6 + 3 \equiv 3 \pmod{6},$$
$$15 = 1 \cdot 11 + 4 \equiv 4 \pmod{11}.$$

Apibendrinsime 6.29 algoritmą.

6.31 algoritmas. *Žinoma:* $a_1, a_2, \ldots, a_k$ *– sveikieji skaičiai;* $m_1, m_2, \ldots, m_k$ *– poromis tarpusavyje pirminiai skaičiai, t.y.* DBD $(m_i, m_j) = 1$, $i \neq j$.

Rezultatas: vienintelis $x \pmod{m_1 m_2 \ldots m_k}$, tenkinantis lyginius $x \equiv a_1 \pmod{m_1}$, $x \equiv a_2 \pmod{m_2}, \ldots, x \equiv a_k \pmod{m_k}$.

1. $m := 1$, $x :=$ LIEKANA (a_1, m_1), $i := 1$.
2. $m := m \cdot m_1$; $m^{-1} := m^{-1} \pmod{m_{i+1}}$.
3. $q_{i+1} :=$ LIEKANA $\big(m^{-1}(a_{i+1} - x), m_{i+1}\big)$.
4. $x := x + m q_{i+1}$.
5. $i := i + 1$; jeigu $i \leqslant k - 1$, tai grįžtame prie 2;
   jeigu $i > k - 1$, tai rezultatas yra x.

△

6.32 pastaba. Pastarasis algoritmas grindžiamas 6.29 algoritmo taikymu lyginių poroms: radę lyginių sistemos $x \equiv a_1 \pmod{m_1}$, $x \equiv a_2 \pmod{m_2}$ vienintelį sprendinį $x_1 \pmod{m_1 m_2}$, sprendžiame sistemą $x \equiv x_1 (\mathrm{mod} m_1 m_2)$, $x \equiv a_3 (\mathrm{mod} m_3)$. Išsprendę ją ir suradę vienintelį sprendinį $x_2 \pmod{m_1 m_2 m_3}$, sprendžiame kitą sistemą $x \equiv x_2 \pmod{m_1 m_2 m_3}$, $x \equiv a_4 \pmod{m_4}$ ir t.t.

6.33 pavyzdys.

$$x \equiv -5 \pmod 7,$$
$$x \equiv 6 \pmod 9,$$
$$x \equiv 4 \pmod 8.$$

Sprendžiame lyginių sistemą

$$x \equiv -5 \pmod 7,$$
$$x \equiv 6 \pmod 9.$$

1.1. $-5 = 7 \cdot (-1) + 2$, todėl pirmąjį sistemos lyginį keičiame lyginiu $x \equiv 2 \pmod 7$.

1.2. $x = 2 + 7q_1$, $q_1 \in \mathbb{Z}$.

1.3. DBD $(7, 9) = 1$, todėl $7^{-1} \equiv 7^{\varphi(9)-1} (\mathrm{mod}\, 9) = 7^5 \equiv 4 \pmod 9$.

1.4. $q_1 = 4(6-2) = 16 \equiv 7 \pmod 9$;

$x = 2 + 7 \cdot 7 = 51 \pmod{7 \cdot 9}$.

Sprendžiame lyginių sistemą $x \equiv 51 \pmod{63}$, $x \equiv 4 \pmod 8$.

2.1. $x = 51 + 63q_2$, $q_2 \in \mathbb{Z}$.

2.2. DBD $(63, 8) = 1$, todėl $63^{-1} \equiv 63^{\varphi(8)-1} (\mathrm{mod}\, 8) = 63^3 (\mathrm{mod}\, 8) \equiv 7 \pmod 8$.

2.3. $q_2 = 7(4 - 51) = 7 \cdot (-47) = -329 \equiv -9 \pmod 8 \equiv 7 \pmod 8$,

$x = 51 + 63 \cdot 7 = 492 \pmod{7 \cdot 9 \cdot 8}$.

Patikrinimas:

$$492 = 70 \cdot 7 + 2 \equiv 2 \pmod 7,$$
$$492 = 54 \cdot 9 + 6 \equiv 6 \pmod 9,$$
$$492 = 61 \cdot 8 + 4 \equiv 4 \pmod 8.$$

Sistemos sprendinį $492 \pmod{7 \cdot 9 \cdot 8}$ galima užrašyti ir taip: $492 = 2 + 7 \cdot 7 + 7 \cdot (7 \cdot 9)$.

Bendruoju atveju lyginių sistemos $(*)$ sprendinį galima užrašyti ir taip:

$$x = q_1 + q_2 \cdot m_1 + q_3(m_1 \cdot m_2) + \ldots + q_k(m_1 \cdot m_2 \cdot \ldots \cdot m_{k-1});$$

čia $q_1 = \text{LIEKANA}\,(a_1, m_1)$, o q_i, $i > 1$ iš 6.31 algoritmo.

Baigdami mūsų kinų teoremos liekanoms nagrinėjimą, pastebėsime, kad funkcija $f : \mathbb{Z}_M \to \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \ldots \mathbb{Z}_{m_k}$, $M = m_1 m_2 \ldots m_k$, $\text{DBD}\,(m_i, m_j) = 1$, $i \neq j$, yra ne tik bijekcija, bet ir žiedų izomorfizmas: $\mathbb{Z}_M \approx \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \ldots \times \mathbb{Z}_{m_k}$:

jeigu $x \equiv a_i \pmod{m_i}$,

$y \equiv b_i \pmod{m_i}$, $1 \leqslant i \leqslant k$,

tai $x + y \equiv a_i + b_i \pmod{m_i}$,

$x \cdot y \equiv a_i \cdot b_i \pmod{m_i}$, $1 \leqslant i \leqslant k$,

ir todėl

$$\begin{aligned} f(x+y) &= (a_1 + b_1, a_2 + b_2, \ldots, a_k + b_k) = (a_1, a_2, \ldots, a_k) \\ &\quad + (b_1, b_2, \ldots, b_k), \\ f(x \cdot y) &= (a_1 \cdot b_1, a_2 \cdot b_2, \ldots, a_k \cdot b_k) = (a_1, a_2, \ldots, a_k) \cdot (b_1, b_2, \ldots, b_k). \end{aligned}$$

Panašiai galėtume parodyti, kad

$$U_M \approx U_{m_1} \times U_{m_2} \times \ldots \times U_{m_k};$$

čia U_i yra žiedo $\mathbb{Z}_i$ elementų, turinčių atvirkštinius, grupė.

Grįžkime prie maksimalios eilės funkcijos λ. Tegu $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ yra kanoninis skaičiaus n skaidinys, o a_i – maksimalios eilės $\lambda\big(p_i^{\alpha_i}\big) = \varphi\left(p_i^{\alpha_i}\right) = p_i^{\alpha_i} - p_i^{\alpha_i - 1}$ elementas grupėje $U_{p_i^{\alpha_i}}$, $1 \leqslant i \leqslant k$ (šį elementą a_i jau mokame rasti).

Lyginių sistemos

$$\begin{aligned} &x \equiv 1 \pmod{p_1^{\alpha_1}}, \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ &x \equiv 1 \pmod{p_{i-1}^{\alpha_{i-1}}}, \\ &x \equiv a_i \pmod{p_i^{\alpha_i}}, \\ &x \equiv 1 \pmod{p_{i+1}^{\alpha_{i+1}}}, \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ &x \equiv 1 \pmod{p_k^{\alpha_k}} \end{aligned}$$

vienintelio sprendinio $x_i \pmod{n}$ eilė grupėje U_n yra

$$\text{ord}_{U_n} x_i = \text{ord}_{U_{p_i{}^{\alpha_i}}}(a_i) = \lambda\big(p_i^{\alpha_i}\big).$$

Atsižvelgę į 6.13 pastabą, galime rasti tokį $b \in U_n$, kad

$$\text{ord}_{U_n}(b) = \text{BMK}\big(\lambda(p_1^{\alpha_1}), \lambda(p_2^{\alpha_2}), \ldots, \lambda\big(p_k^{\alpha_k}\big)\big).$$

Taigi $\lambda(n) \geqslant \text{BMK}\big(\lambda(p_1^{\alpha_1}), \lambda(p_2^{\alpha_2}), \ldots, \lambda(p_k^{\alpha_k})\big)$.

Priešingai, jeigu $a \in U_n$, tai žinome, kad

$$\text{ord}_{U_{p_i{}^{\alpha_i}}}(a) \quad \text{dalo} \quad \lambda(p_i^{\alpha_i}), \quad 1 \leqslant i \leqslant k,$$

ir todėl $\text{ord}_{U_{p_i{}^{\alpha_i}}}(a)$ dalo $\text{BMK}\big(\lambda(p_1^{\alpha_1}), \lambda(p_2^{\alpha_2}), \ldots, \lambda(p_k^{\alpha_k})\big) = s$.

Tada

$$a^s \equiv 1 \ (\text{mod}\ p_i^{\alpha_i}), \quad 1 \leqslant i \leqslant k$$

ir

$$a^s \equiv 1 \ (\text{mod}\ n),$$

$$\text{ord}_{U_n}(a) \leqslant s,$$

$$\lambda(n) \leqslant s = \text{BMK}\big(\lambda(p_1^{\alpha_1}), \lambda(p_2^{\alpha_2}), \ldots, \lambda(p_k^{\alpha_k})\big).$$

Taigi $\lambda(n) = \text{BMK}\big(\lambda(p_1^{\alpha_1}), \lambda(p_2^{\alpha_2}), \ldots, \lambda(p_k^{\alpha_k})\big)$.

6.34 pavyzdys. $\lambda(120) = \text{BMK}\big(\lambda(2^3), \lambda(3), \lambda(5)\big) = \text{BMK}\,(2, 2, 4) = 4$.

Apibendrinsime mūsų žinias apie grupių U_n maksimalios eilės funkciją λ.

6.35 teiginys. *1. Funkcijos λ reikšmės:*

$$\lambda(n) = \begin{cases} 1, & \textit{kai} \ \ n = 1, 2, \\ 2, & \textit{kai} \ \ n = 4, \\ p^{\alpha-1}(p-1), & \textit{kai} \ \ n = p^\alpha, p - \textit{nelyginis} \\ & \textit{pirminis skaičius}, \\ 2^{\alpha-2}, & \textit{kai} \ \ n = 2^\alpha, \alpha \geqslant 3, \\ \textit{BMK}\,\big(\lambda(p_1^{\alpha_1}), \lambda(p_2^{\alpha_2}), \ldots, \lambda(p_k^{\alpha_k})\big), & \textit{kai} \ \ n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k} - \\ & \textit{kanoninis skaičiaus}\ n \\ & \textit{skaidinys}. \end{cases}$$

2. Oilerio–Ferma teoremos analogas funkcijai λ:

Kai DBD $(a, n) = 1$, *tai* $a^{\lambda(n)} \equiv 1 \ (\text{mod}\ n)$.

3. Kai $n = p_1 p_2 \ldots p_k$ yra bekvadratis skaičius ($p_1, p_2, \ldots, p_k$ – skirtingi pirminiai skaičiai), tai su visais $a \in \mathbb{Z}_n$ teisinga lygybė $a^{\lambda(n)+1} \equiv a \ (\text{mod}\ n)$.

Įrodymas. 2. Kai $a \in U_n$, tai $\text{ord}_{U_n}(a)$ dalo $\lambda(n)$, t.y. $\lambda(n) = \text{ord}_{U_n}(a) \cdot l$ ir

$$a^{\lambda(n)} = \big(a^{\text{ord}_{U_n}(a)}\big)^l \equiv 1 \ (\text{mod}\ n).$$