Algebros paskaitos informatikams. Rimantas Grigutis.

3 paskaita. *Klasikinės skaičių teorijos teoremos.*

Primityviųjų klasių multiplikacinė grupė.

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

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

Šios aibės elementų skaičių vadiname Oilerio funkcijos φ m reikšme : $\varphi(m)$. Pavyzdžiui, kai $p \Leftrightarrow$ pirminis skaičius, tai $\varphi(p) = p \Leftrightarrow 1$. Jeigu skaičiaus m kanoninis skaidinys yra $m = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$, tai $\varphi(m) = m\left(1 \Leftrightarrow \frac{1}{p_1}\right) \cdots \left(1 \Leftrightarrow \frac{1}{p_s}\right)$. Čia mes remiamės svarbiausia Oilerio funkcijos savybe - multiplikatyvumo savybe: *jei* $(m, n) = 1$, *tai* $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$.

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

Įrodymas. 1) Tegu $\alpha, \beta \in U_m$ ir $a \in \alpha, b \in \beta$, t.y. $(a, m) = (b, m) = 1$. Tada $(ab, m) = 1$ ir $\alpha\beta = K_{ab} \in U_m$.

2) Visoms likinių klasėms galioja sandaugos asociatyvumo savybė. Todėl $\alpha(\beta\gamma) = (\alpha\beta)\gamma$ su visais $\alpha, \beta, \gamma \in U_m$.

3) Akivaizdu, kad $K_1 \in U_m$.

4) Jei $\alpha \in U_m$, tai $\alpha \cdot \alpha^{-1} = K_1$. Tada $\alpha = (\alpha^{-1})^{-1}$ it todėl $\alpha^{-1} \in U_m$.

Įrodyta.

Dabar pateiksime klasikines skaičių teoremas.

Apibrėžimai. *Tegu* $m > 1 \Leftrightarrow$ *fiksuotas skaičius. Skaičių* $a_0 \in K_0, a_1 \in K_1, ..., a_{m-1} \in K_{m-1}$ *aibė* $\{a_0, a_1, ..., a_{m-1}\}$ *vadinama* **pilnąja likinių sistema mod** m. *Skaičiai* $r_1, r_2, ..., r_s$ *, paimti po vieną iš kiekvienos primityviosios likinių klasės mod* m *sudaro* **redukuotąją likinių sistemą mod** m. Pastebėsime, kad $s = \varphi(m)$.

Lema. *Tegu* $r_1, r_2, ..., r_s \Leftrightarrow$ *redukuotoji likinių sistema mod* m *ir skaičius* a *yra tarpusavyje pirminis* $m : (a, m) = 1$. *Tada skaičių sistema* $ar_1, ar_2, ..., ar_s$ *irgi yra redukuotoji likinių sistema mod* m.

Įrodymas. Skaičiai $r_1, r_2, ..., r_s$ yra redukuotoji likinių sistema mod m, todėl $(r_i, m) = 1$ su visais $i = 0, 1, 2, ..., s$ Tada ir $(ar_i, m) = 1$ su visais $i = 0, 1, 2, ..., s$ ir todėl jie visi yra primityviose klasėse. Parodysime, kad skaičiai sekoje $ar_0, ar_1, ..., ar_s$ yra tarpusavyje skirtingi mod m ir todėl jie visi yra *skirtingose* primityviose klasėse Sakykime, kad $ar_i \equiv ar_j \pmod{m}$. Tada $ar_i \Leftrightarrow ar_j = a(r_i \Leftrightarrow r_j)$ dalijasi iš m. Bet $(a, m) = 1$, todėl $r_i \Leftrightarrow r_j$ dalijasi iš m ir $r_i \equiv r_j \pmod{m}$, taigi $i = j$. Gavome, kad skaičiai sekoje $ar_0, ar_1, ..., ar_s$ yra skirtingose primityviose klasėse. Ir skaičių sekoje ir primityviųjų klasių yra po lygiai (po $s = \varphi(m)$). Taigi $ar_0, ar_1, ..., ar_s$ yra redukuotoji likinių sistema mod m.

Įrodyta.

Išvada. *Tegu* $r_1, r_2, ..., r_s \Leftrightarrow$ *redukuotoji likinių sistema mod* m *ir skaičius* a *yra tarpusavyje pirminis* $m : (a, m) = 1$. *Tada*

$$ar_0 \cdot ar_1 \cdots ar_s \equiv r_0 \cdot r_1 \cdots r_s \pmod{m}.$$

Įrodymas. Turime

$$\begin{gathered} ar_0 \cdot ar_1 \cdots ar_s \equiv r_0 \cdot r_1 \cdots r_s \pmod{m} \Leftrightarrow \\ K_{ar_0} \cdot K_{ar_1} \cdots K_{ar_s} = K_{r_0} \cdot K_{r_1} \cdots K_{r_s}. \end{gathered}$$

Paskutinioji lygybė teisinga, nes tiek kairėje, tiek dešinėje jos pusėje yra visų skirtingų primityviųjų klasių sandaugos.

Įrodyta.

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

Įrodymas. Tegu $r_1, r_2, ..., r_s \Leftrightarrow$ redukuotoji likinių sistema mod m. Tada $(r_i, m) = 1$ su visais $i = 0, 1, 2, ..., s$ ir todėl skaičius $r_1 \cdot r_2 \cdots r_s$ irgi yra tarpusavyje pirminis $m : (r_1 \cdot r_2 \cdots r_s, m) = 1$.

Turime

$$\begin{gathered} ar_0 \cdot ar_1 \cdots ar_s \equiv r_0 \cdot r_1 \cdots r_s \pmod{m} \Leftrightarrow \\ a^s r_0 \cdot r_1 \cdots r_s \equiv r_0 \cdot r_1 \cdots r_s \pmod{m}, (a, m) = 1 \Leftrightarrow \\ a^s \equiv 1 \pmod{m}, \end{gathered}$$

čia $s = \varphi(m)$.

Įrodyta.

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

Mažoji Ferma teorema. *Jeigu* $p\Leftrightarrow$ *pirminis skaičius, o* a *nesidalija iš* p, *tai* $a^{p-1}\equiv 1\,(\operatorname{mod} m)$.

Įrodymas. Tai atskiras Oilerio teoremos atvejis, kai $m=p\Leftrightarrow$ pirminis, nes $\varphi(p)=p\Leftrightarrow 1$.

Įrodyta.

Išvada. *Jeigu* a *nesidalija iš pirminio skaičiaus* p, *tai* $\bar{a}^{-1}=\bar{a}^{p-2}\,(\operatorname{mod} p)$.

Teiginys. *Tegu* $m=p_1\cdot p_2\cdots p_r$ *yra natūralusis skaičius, čia* $p_1,p_2,...,p_r$ - *skirtingi pirminiai skaičiai. Tada visiems* $\bar{a}\in\mathbf{Z}_m$ *teisinga lygybė*

$$\bar{a}^{\varphi(m)+1}=\bar{a}.$$

Įrodymas. Mūsų nagrinėjamu atveju

$$\varphi(m)=(p_1\Leftrightarrow 1)(p_2\Leftrightarrow 1)\cdots(p_r\Leftrightarrow 1).$$

Tegu $\bar{a}\in\mathbf{Z}_m$. Pirminiam skaičiui p_i, $1\leq i\leq r$, galimi du variantai:

a) $(a,p_i)=1$.

Tada pagal Mažąją Ferma teoremą turime $a^{p_i-1}\equiv 1\,(\operatorname{mod} m)$ ir

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

b) $(a,p_i)>1$.

Tada a dalijasi iš p_i, t.y. $a\equiv 0\,(\operatorname{mod} m)$ ir todėl

$$a^{\varphi(m)+1}\equiv 0\equiv a\,(\operatorname{mod} m).$$

Taigi turime, kad skaičius $a^{\varphi(m)+1}\Leftrightarrow a$ dalijasi iš visų pirminių p_i,kartu ir iš šių pirminių skaičių sandaugos m :

$$a^{\varphi(m)+1}\equiv a\,(\operatorname{mod} m)$$
$$\bar{a}^{\varphi(m)+1}=\bar{a}.$$

Įrodyta.

Pateiksime dabar klasikinį pirminio skaičiaus testą.

Vilsono teorema. *Skaičius p yra pirminis tada ir tik tada, kada* $(p \Leftrightarrow 1)! \equiv \Leftrightarrow 1 \pmod p$.

Įrodymas. Tegu $p \Leftrightarrow$ pirminis skaičius. Nagrinėkime baigtinį kūną $\mathbf{Z}_p$. Šiame kūne visos *nenulinės* likinių klasės turi atvirkštines:

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

čia $\psi \Leftrightarrow$ bijekcija aibėje $\{1, 2, ..., p \Leftrightarrow 1\}$.

Klasių aibėje $K_{\psi(1)}, ..., K_{\psi(p-1)}$ yra visos nenulinės $\mathbf{Z}_p$ klasės. Turime, kad skaičių aibė $1, 2, ..., p \Leftrightarrow 1$ susiskaido poromis $\{1, \psi(1)\}, ..., \{p \Leftrightarrow 1, \psi(p \Leftrightarrow 1)\}$. Raskime poras, kuriose $i = \psi(i)$, t.y. $K_i^{-1} = K_i$ ir $1 \leq i < p$. Tada

$$\begin{gathered} K_i^2 = K_1 \\ \Leftrightarrow i^2 = 1 \pmod p \\ \Leftrightarrow (i \Leftrightarrow 1)(i+1) \equiv 0 \pmod p \\ \Leftrightarrow (i \Leftrightarrow 1)(i+1) \text{ dalijasi iš pirminio } p \Leftrightarrow \\ \text{arba } i \Leftrightarrow 1 \text{ dalijasi iš } p, \text{ arba } i+1 \text{ dalijasi iš } p. \end{gathered}$$

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

Tada turime

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

Tegu dabar $p \Leftrightarrow$ sudėtinis skaičius: $p = a \cdot b$, čia $1 < a, b < p$ ir todėl $(p \Leftrightarrow 1)! \vdots a, b$. Taigi $(p \Leftrightarrow 1)! \equiv 0 \pmod p$.

Įrodyta.

Naudodamiesi Vilsono teorema galima sukonstruoti funkciją

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

Tai savotiškas pirminio skaičiaus testas, tiesa praktiškai netaikomas, nes tenka skaičiuoti $(m \Leftrightarrow 1)!$, o tai labai didelis skaičius net esant pakankamai mažiems m.

Baigsime šį skyrių lyginių sistemų sprendimu.

Teorema(kinų teorema liekanoms). Tegu $m_1, m_2, ..., m_k$ yra poromis tarpusavyje pirminiai skaičiai > 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 $\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \qquad \cdots \\ x \equiv a_k \pmod{m_k} \end{cases}$ turi sprendinį $x = x_0$;

(2) jeigu $x = x_2$ yra kitas sistemos sprendinys, tai $x_2 \equiv x_0 \pmod{M}$.

Teoremos įrodymas remiasi tokiomis lemomis.

Lema 1. *Tegu* $a \equiv b \pmod{m_i}$, *čia* $m_1, m_2, ..., m_n \Leftrightarrow$ *poromis tarpusavyje pirminiai skaičiai. Tada* $a \equiv b \pmod{m_1 m_2 \cdots m_n}$.

Įrodymas. Tegu $a \equiv b \pmod{m_1}$ ir $a \equiv b \pmod{m_2}$,čia $(m_1, m_2) = 1$, t.y. $xm_1 + ym_2 = 1$ ir

$$\underbrace{\underbrace{(a \Leftrightarrow b)}_{\vdots\, m_2} xm_1}_{\vdots\, m_1 m_2} + \underbrace{\underbrace{(a \Leftrightarrow b)}_{\vdots\, m_1} ym_2}_{\vdots\, m_1 m_2} = a \Leftrightarrow b$$

Taigi $a \Leftrightarrow b$ dalijasi iš $m_1 m_2$.

Lemoje esantis teiginys įrodomas indukcija pagal n.

Įrodyta.

Lema 2. *Jeigu* $a \equiv b \pmod{m}$ *ir* m *dalijasi iš* d, *tai ir* $a \equiv b \pmod{d}$.

Įrodymas akivaizdus (aš tikuosi).

Teoremos įrodymas. Apibrėžkime skaičius M_i ir N_i iš šių sąlygų:

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

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

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

t.y. x_0 yra sistemos sprendinys,ir todėl sistema

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

ekvivalenti sistemai

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

Remiantis Lema 1 ir Lema 2 paskutinioji sistema yra ekvivalenti lyginiui

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

Įrodyta.