Algebros pratybos. Rimantas Grigutis

**2 pratybos**. *Laipsnio* $a^n \pmod m$ *skaičiavimas .* *Lyginio* $ax \equiv b \pmod m$ *sprendimas.Dalumo požymiai.Atvirkštinio* $a^{-1} \pmod m$ *skaičiavimas, kai* $(a,m)=1$*.Aritmetika* $\mathbf{Z}_m$.

**Laipsnio** $a^n \pmod m$ **skaičiavimas**

1. Laipsnio rodiklis užrašomas dvejetaine sistema: $n = \sum\limits_{i=0}^{k} \alpha_i 2^i$ .

2. $a^n = a^{\sum\limits_{i=0}^{k}\alpha_i 2^i} = a^{\alpha_0 2^0} \cdot a^{\alpha_1 2^1} \cdots a^{\alpha_k 2^k} \cdots$

3. Pasinaudoję lygybe $a^{2^{i+1}} = \left(a^{2^i}\right)^2$ pildoma lentelė

| | | | |
|---|---|---|---|
| $i$ | $0$ | $\cdots$ | $k$ |
| $\alpha_i$ | $\alpha_0$ | $\cdots$ | $\alpha_k$ |
| $a^{2^i}$ | $a^{2^0}$ | $\cdots$ | $a^{2^k}$ |
| $b_i = a^{\sum\limits_{j=0}^{i}\alpha_i 2^j}$ | $b_0$ | $\cdots$ | $b_k = a^n \pmod m$ |

*Pavyzdys.* Suskaičiuosime $7^{39} \pmod{41}$

1. $39 = 2^5 + 2^2 + 2^1 + 2^0 = 100111_2$.

2.

| | | | | | | |
|---|---|---|---|---|---|---|
| $i$ | 0 | 1 | 2 | 3 | 4 | 5 |
| $\alpha_i$ | 1 | 1 | 1 | 0 | 0 | 1 |
| $a^{2^i}$ | 7 | 8 | $-18$ | $-4$ | 16 | 10 |
| $b_i$ | 7 | 15 | 17 | 17 | 17 | **6** |

$7^{39} = 6 \pmod{41}$ .

**Uždaviniai**.

Apskaičiuokite

1) $22^{144} \pmod{73} = 1$ . 2) $498^{451} \pmod{23}$ . 3) $215^{243} \pmod{21}$ .

Atsakymai. 1) 1. 2) 22. 3) 20.

**Lyginio** $ax \equiv b \pmod m$ **sprendimas**.

Šie uždaviniai yra ekvivalentūs:

1. Lygties $ax + my = b$ sprendimas.
2. Lyginių lygties $\bar{a}\bar{x} = \bar{b}$ sprendimas.
3. Lyginio $ax \equiv b \pmod{m}$ sprendimas.

Išnagrinėsime Lyginio $ax \equiv b \pmod{m}$ sprendimą.

Nagrinėkime du atvejus: $(a, m) = 1$ ir $(a, m) = d > 1$.

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

Šiuo atveju, naudodamiesi Euklido algoritmu, galime rasti tokius $c, q \in \mathbf{Z}$, kad

$$ac + mq = 1.$$

Tada

$$\begin{gathered} a\,(bc) + m\,(bq) = b \\ \Rightarrow a\,(bc) = b - m\,(bq) \\ \Rightarrow a\,(bc) \equiv b \pmod{m}. \end{gathered}$$

Gavome, kad $x_0 = bc$ yra lyginio sprendinys.

Tegu dabar $x = x_1$ yra kitas šio lyginio sprendinys, t.y. $ax_1 \equiv b \pmod{m}$.
Tada $\left.\begin{array}{c} ax_0 \equiv ax_1 \pmod{m} \\ (a, m) = 1 \end{array}\right\} \Rightarrow x_0 \equiv x_1 \pmod{m}$.

Iš kitos pusės, jeigu $y \equiv x_0 \pmod{m}$, tai $ay \equiv ax_0 \equiv b \pmod{m}$ ir todėl $y$ yra lyginio sprendinys.

Taigi, jeigu $x_0$ yra lyginio sprendinys, tai kitais lyginio sprendiniais yra skaičiai iš ${}_mK_{x_0}$ ir tik jie.

2. $(a, m) = d > 1$.

Tam, kad lyginys $ax \equiv b \pmod{m}$ turėtų sprendinį būtina, kad $b$ dalytųsi iš $d$.

Tikrai, jeigu $x = x_1$ yra lyginio sprendinys, tai

$$\left.\begin{array}{c} ax_1 \equiv b \pmod{m} \\ (a, m) = d \end{array}\right\} \Rightarrow \left.\begin{array}{c} ax_1 - b = mq, q \in \mathbf{Z} \\ a \vdots d, m \vdots d \end{array}\right\} \Rightarrow \left.\begin{array}{c} ax_1 - mq = b \\ a = a_1 d; m = m_1 d \end{array}\right\}$$

$\Rightarrow a_1 d x_1 - m_1 d q = b \Rightarrow d\,(a_1 x_1 - m_1 q) = b \Rightarrow b \vdots d$.

Taigi, turime $\left.\begin{array}{c} b = b_1 d \\ m = m_1 d \\ a_1 = a_1 d \end{array}\right\} \Rightarrow a_1 d x \equiv b_1 d \pmod{m_1 d} \Longleftrightarrow a_1 x \equiv b_1 \pmod{m_1}$
ir $(a_1, m_1) = 1$.

Tegu dabar $x = x_1$ yra lyginio $a_1x \equiv b_1 \pmod{m_1}$ sprendinys. Tada lyginio $ax \equiv b \pmod{m}$ skirtingais sprendiniais mod $m$ yra $x_1, x_1 + \frac{m}{d}, x_1 + 2 \cdot \frac{m}{d}, ..., x_1 + (d-1)\frac{m}{d}$, visi sprendiniai yra klasėse ${}_mK_{x_1}, {}_mK_{x_1+\frac{m}{d}}, ..., {}_mK_{x_1+(d-1)\frac{m}{d}}$.

*Pavyzdys.*

$$6x \equiv 3 \pmod{15}, \ (6,15) = 3 = d;$$
$$2x \equiv 1 \pmod{5}, \ (2,5) = 1;$$
$$2 \cdot 3 \equiv 1 \pmod{5}, \text{ nes } 2 \cdot 3 + 5 \cdot (-1) = 1.$$

Gavome, kad lyginio sprendiniai yra $x_1 = 3$, $x_1 + \frac{m}{d} = 3 + 5 = 8, x_1 + 2 \cdot \frac{m}{d} = 3 + 10 = 3 + 10 = 13$. Visi sprendiniai yra klasėse ${}_{15}K_3, {}_{15}K_8, {}_{15}K_{13}$.

**Uždaviniai.**

Išspręskite lyginius.

1) $12x \equiv 5 \pmod{5}$ .2) $11x \equiv 10 \pmod{16}$ .3) $13x \equiv 65 \pmod{78}$ .

4) $8x \equiv 12 \pmod{20}$ .5) $91x \equiv 21 \pmod{56}$ .6) $18x \equiv 16 \pmod{22}$ .

7) $33x \equiv 9 \pmod{39}$ .8) $52x \equiv 28 \pmod{60}$ .9) $74x \equiv 32 \pmod{94}$ .

10) $34 \equiv 24 \pmod{38}$ .11) $60x \equiv 33 \pmod{84}$ .12) $69x \equiv 33 \pmod{84}$13) $54x \equiv 26 \pmod{62}$ .

Atsakymai.

1) $\overline{0}$ 2) $\overline{14}$ 3) $\overline{5}, \overline{11}, \overline{17}, \overline{23}, \overline{29}, \overline{35}, \overline{41}, \overline{47}, \overline{53}, \overline{59}, \overline{65}, \overline{71}, \overline{77}$

4) $\overline{4}, \overline{9}, \overline{14}, \overline{19}$ 5) $\overline{7}, \overline{15}, \overline{23}, \overline{31}, \overline{39}, \overline{47}, \overline{55}$ 6) $\overline{7}, \overline{18}$ 7) $\overline{5}, \overline{18}, \overline{31}$

8) $\overline{4}, \overline{19}, \overline{34}, \overline{49}$ 9) $\overline{36}, \overline{83}$ 10) $\overline{13}, \overline{32}$ 11) $\varnothing$ 12) $\overline{9}, \overline{37}, \overline{65}$ .

**Dalumo požymiai**.

Tegu

$n = (a_k a_{k-1} ... a_2 a_1 a_0)_{10} = a_k 10^k + \cdots + a_0.$

Pvz. : $3472 = 3 \cdot 10^3 + 4 \cdot 10^2 + 7 \cdot 10^1 + 2 \cdot 10^0$

$Q_s(n) = \sum\limits_{i=0}^{\infty} (a_{is+s-1} ... a_{is+1} a_{is}),$

Pvz.: $Q_3(6154328103) = 103 + 328 + 154 + 006 = 591$

tada $n = \sum\limits_{i=0}^{\infty} (a_{is+s-1} ... a_{is+1} a_{is}) \cdot 10^{is},$

Pvz.: $6154328103 = 103 \cdot 10^{0 \cdot 3} + 328 \cdot 10^{1 \cdot 3} + 154 \cdot 10^{2 \cdot 3} + 6 \cdot 10^{3 \cdot 3}.$

$Q'_s(n) = \sum\limits_{i=0}^{\infty} (-1)^i (a_{is+s-1} ... a_{is+1} a_{is}),$

Pvz.: $Q'_3(6154328103) = 103 - 328 + 154 - 006 = -77.$

1) Įrodyti:
*Teiginys (Dalumo požymiai)*
Su visais $n \in \mathbf{N}, s \in \mathbf{N}$ teisinga
$(i)$ $n \equiv Q_s(n) \pmod{10^s - 1}$,
$(ii)$ $n \equiv Q_s^{'}(n) \pmod{10^s + 1}$.

Uždaviniai
1) Įrodykite teiginį.
2) Raskite dalumo požymius iš
i) 9,99,999; 11,101,1001.
ii) 7,13,37.
iii) 17,19.

**Atvirkštinio $a^{-1} \pmod m$ skaičiavimas, kai $(a, m) = 1$.Aritmetika $\mathbf{Z}_m$.**

1. Turime $(a, m) = 1$.Iš Euklido algoritmo gauname, kad $a \cdot b + m \cdot c = 1$
2. $\bar{a} \cdot \bar{b} = \bar{1}$ ir $a^{-1} \equiv b \pmod m$.
*Pavyzdys.*
Surasime $4^{-1} \pmod{81}$.
1. Iš Euklido algoritmo gauname, kad $4 \cdot (-20) + 81 \cdot (1) = 1$
2. $4^{-1} \equiv -20 \equiv 61 \pmod{81}$.
*Uždaviniai.*
1. Raskite
1) $71^{-1} \pmod{2503}$; 2)$63^{-1} \pmod{3407}$; 3) $67^{-1} \pmod{3631}$.
2. 1) Parašykite sudėties ir daugybos lenteles žieduose $\mathbf{Z}_7$, $\mathbf{Z}_8$, $\mathbf{Z}_9$, $\mathbf{Z}_{11}$, $\mathbf{Z}_{12}$ , $\mathbf{Z}_{13}$.
2) Išspręskite lygtis $x^2 = 1$ ir $x^2 = -1$ minėtuose žieduose.

3. Su kuriais $\bar{a} \in Z_{100}$ teisinga: $\bar{a}^{40} = \bar{1}$ .
Atsakymai
1. 1) 2362 2) 1352 3) 1951.
3. $a$ nelyginis nedalus iš 5.