$\alpha + \omega$, 2003, Nr. 3, 45–48

Lyginiai

Svajūnas Sajavičius
svajunas.sajavicius@mif.vu.lt

Straipsnyje nagrinėjami uždaviniai, kuriuos galima išspręsti pasinaudojus lyginių savybėmis.

Jeigu sveikųjų skaičių a ir b skirtumas $a - b$ dalijasi iš m, $m \in N$, tai sakoma, kad *a lygsta b moduliu m* ir rašoma $a \equiv b (\mathrm{mod}\, m)$. Priešingu atveju, jei $a - b$ nesidalija iš m, sakoma, kad *a nelygsta b moduliu m* ir rašoma $a \not\equiv b (\mathrm{mod}\, m)$. Kai $a \equiv 0 (\mathrm{mod}\, m)$, tai skaičius a dalijasi iš m (žymima $a \vdots m$ arba $m|a$). Reiškiniai $a \equiv b (\mathrm{mod}\, m)$ vadinami *lyginiais* (angl. *congruence*; rus. *сравнение*). Lyginio sąvoką pirmą kartą 1801 metais pavartojo K. F. Gausas[1] savo veikale „Aritmetiniai tyrinėjimai“.

Pavyzdžiui: $14 \equiv 5 (\mathrm{mod}\, 3)$, $-17 \equiv 4 (\mathrm{mod}\, 7)$, $9 \not\equiv 6 (\mathrm{mod}\, 2)$, $4 \not\equiv -3 (\mathrm{mod}\, 6)$ ir t. t.

Matematikai tokius sąryšius, pavyzdžiui, sveikųjų skaičių aibėje $\boldsymbol{Z}$ apibrėžtą sąryšį $\equiv$, vadina ekvivalentumo sąryšiais. Šie sąryšiai turi refleksyvumo, simetriškumo ir tranzityvumo savybes. Iš tikrųjų lengva įsitikinti, kad sąryšis $\equiv$ yra:

- refleksyvus: $a \equiv a (\mathrm{mod}\, m)$;
- simetriškas: jei $a \equiv b (\mathrm{mod}\, m)$, tai $b \equiv a (\mathrm{mod}\, m)$;
- tranzityvus: jei $a \equiv b (\mathrm{mod}\, m)$ ir $b \equiv c (\mathrm{mod}\, m)$, tai $a \equiv c (\mathrm{mod}\, m)$.

Lyginyje $a \equiv b (\mathrm{mod}\, m)$ skaičius m vadinamas *moduliu*. Skaičiai a ir b vadinami *palyginamais pagal modulį m*.

Lyginių savybės

Susipažinsime su dar keliomis svarbiausiomis lyginių savybėmis. Pateikiamų savybių ir teoremų įrodymus galima rasti skaičių teorijos vadovėliuose, pavyzdžiui, [1].

1 savybė. Jei $a_1 \equiv b_1 (\mathrm{mod}\, m)$ ir $a_2 \equiv b_2 (\mathrm{mod}\, m)$, tai $a_1 + a_2 \equiv b_1 + b_2 (\mathrm{mod}\, m)$, $a_1 - a_2 \equiv b_1 - b_2 (\mathrm{mod}\, m)$ ir $a_1 \cdot a_2 \equiv b_1 \cdot b_2 (\mathrm{mod}\, m)$.

2 savybė. Jei $a \equiv b (\mathrm{mod}\, m)$, tai $a \equiv b + mk (\mathrm{mod}\, m)$ ir $a + mk \equiv b (\mathrm{mod}\, m)$, $k \in \boldsymbol{Z}$.

3 savybė. Jei $a \equiv b + c (\mathrm{mod}\, m)$, tai $a - c \equiv b (\mathrm{mod}\, m)$.

4 savybė. Jei $a \equiv b (\mathrm{mod}\, m)$, tai $a^n \equiv b^n (\mathrm{mod}\, m)$, $n \in N$.

5 savybė. Jei $P(x)$ yra daugianaris, kurio koeficientai sveikieji skaičiai, ir $a \equiv b (\mathrm{mod}\, m)$, tai $P(a) \equiv P(b) (\mathrm{mod}\, m)$.

6 savybė. Jei skaičius d yra skaičių a ir b bendrasis daliklis ir $a \equiv b (\mathrm{mod}\, m)$, tai $\frac{a}{d} \equiv \frac{b}{d} \left(\mathrm{mod}\, \frac{m}{(m,d)}\right)$, čia (m, d) yra didžiausias bendrasis skaičių m ir d daliklis.

[1] Johann Carl Friedrich Gauss (1777–1855) — vokiečių matematikas.

Sprendžiant uždavinius svarbi ir labai naudinga tokia teorema.

Teorema. *Du sveikieji skaičiai lygsta vienas kitam moduliu m tada ir tik tada, kai dalijant juos iš m gaunama ta pati liekana.*

Verta paminėti dar kelis labai gražius skaičių teorijos rezultatus. Prieš tai apibrėžkime Oilerio[2] funkciją.

APIBRĖŽIMAS. Oilerio funkcija $\varphi(n)$ yra lygi skaičiui natūraliųjų skaičių, ne didesnių už n ir tarpusavyje pirminių su n.

Oilerio funkcijos apibrėžimo sritis yra natūraliųjų skaičių aibė. Funkcijos, kurių apibrėžimo sritis yra natūraliųjų skaičių aibė, vadinamos aritmetinėmis. Oilerio funkcija taip pat yra multiplikatyvioji funkcija, t. y., jei m ir n — tarpusavyje pirminiai skaičiai, tai $\varphi(mn) = \varphi(m)\cdot\varphi(n)$. Iš multiplikatyvumo apibrėžimo išplaukia, kad žinant skaičiaus n kanoninį skaidinį $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, čia p_i — skirtingi pirminiai skaičiai, $\alpha_i \in N$, $i = 1, 2, \ldots, k$, rasti funkcijos reikšmę taške n galima pagal formulę $\varphi(n) = \varphi(p_1^{\alpha_1})\cdot\varphi(p_2^{\alpha_2})\cdots\varphi(p_k^{\alpha_k})$. Pabandykite įrodyti, kad $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$, kai p — bet koks pirminis, o α — natūralusis skaičius.

Spręsdami uždavinius taip pat naudosimės šiomis teoremomis.

Oilerio teorema. *Jei a ir m yra tarpusavyje pirminiai skaičiai, tai* $a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m)$.

Kai m — pirminis, tai $\varphi(m) = m - 1$. Galime suformuluoti tokią teoremą.

Mažoji Ferma[3] teorema. *Jei p yra pirminis skaičius ir a su p — tarpusavyje pirminiai skaičiai, tai* $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$. *Be to,* $a^p \equiv a (\mathrm{mod}\, p)$, *kai a — bet koks sveikasis skaičius.*

Uždavinių sprendimo pavyzdžiai

Keliais pavyzdžiais pailiustruosime, kaip naudojantis lyginių savybėmis sprendžiami uždaviniai.

1 pavyzdys. *Įrodykime, kad neegzistuoja daugianaris P(x), kurio koeficientai yra sveikieji skaičiai, kad* $P(256) = 652$ *ir* $P(106) = 601$.

Sprendimas. Kadangi teisingas lyginys $256 \equiv 106 (\mathrm{mod}\, 150)$, tai, remiantis 5-ąja savybe, $P(256) \equiv P(106) (\mathrm{mod}\, 150)$. Tačiau $652 \not\equiv 601 (\mathrm{mod}\, 150)$. Taigi toks daugianaris $P(x)$ neegzistuoja.

2 pavyzdys. *Raskime liekaną, kuri gaunama skaičių* $23^{24} + 24^{23}$ *padalijus iš* 11.

Sprendimas. Kadangi skaičiai 24 ir 23 yra tarpusavyje pirminiai su 11, tai remiantis mažąja Ferma teorema $23^{10} \equiv 1 (\mathrm{mod}\, 11)$, todėl

$$(23^{10})^2 = 23^{20} \equiv 1^2 = 1 (\mathrm{mod}\, 11) \quad \text{ir} \quad 23^{20}\cdot 23^4 = 23^{24} \equiv 1\cdot 23^4 = 23^4 (\mathrm{mod}\, 11).$$

Bet

$$23^4 = 279841 = 25440\cdot 11 + 1, \quad \text{tai} \quad 23^4 \equiv 1 (\mathrm{mod}\, 11) \quad \text{ir} \quad 23^{24} \equiv 1 (\mathrm{mod}\, 11).$$

Taip pat gauname, kad

$$24^{10} \equiv 1 (\mathrm{mod}\, 11), \qquad (24^{10})^2 = 24^{20} \equiv 1^2 = 1 (\mathrm{mod}\, 11)$$

---

[2] Leonard Euler (1707–1771) — šveicarų matematikas, mechanikas ir fizikas.

[3] Pierre de Fermat (1601–1665) — prancūzų matematikas.

ir

$$24^{20} \cdot 24^3 = 24^{23} \equiv 1 \cdot 24^3 = 24^3 (\mathrm{mod}\, 11).$$

Iš lygybės

$$24^3 = 12167 = 1106 \cdot 11 + 1$$

gauname, kad

$$24^3 \equiv 1 (\mathrm{mod}\, 11) \quad \text{ir} \quad 24^{23} \equiv 1 (\mathrm{mod}\, 11).$$

Vadinasi,

$$23^{24} + 24^{23} \equiv 1 + 1 = 2 (\mathrm{mod}\, 11).$$

Atsakymas. 2.

3 pavyzdys. *Raskime paskutinį skaičiaus* 2003^{2004} *skaitmenį.*

Sprendimas. Paskutinis skaičiaus skaitmuo lygus liekanai, gaunamai skaičių dalijant iš 10. Kadangi 2003 ir 10 yra tarpusavyje pirminiai skaičiai, galime taikyti Oilerio teoremą. Apskaičiavę $\varphi(10) = \varphi(2) \cdot \varphi(5) = 1 \cdot 4 = 4$, gauname $2003^{\varphi(10)} = 2003^4 \equiv 1 (\mathrm{mod}\, 10)$. Iš čia $(2003^4)^{501} = 2003^{2004} \equiv 1^{501} = 1 (\mathrm{mod}\, 10)$. Taigi skaičiaus 2003^{2004} paskutinis skaitmuo yra 1.

Atsakymas. 1.

4 pavyzdys. *Įrodykime, kad skaičius* $1^n + 2^n + 3^n + 4^n$ *nesidalija iš* 5, *kai* $n = 4k$, $k \in \mathbf{Z}$.

Sprendimas. Remsimės mažąja Ferma teorema. Kadangi

$$1^4 \equiv 1 (\mathrm{mod}\, 5), \qquad 2^4 \equiv 1 (\mathrm{mod}\, 5), \qquad 3^4 \equiv 1 (\mathrm{mod}\, 5), \qquad 4^4 \equiv 1 (\mathrm{mod}\, 5),$$

tai teisingi ir lyginiai

$$1^{4k} \equiv 1 (\mathrm{mod}\, 5), \qquad 2^{4k} \equiv 1 (\mathrm{mod}\, 5), \qquad 3^{4k} \equiv 1 (\mathrm{mod}\, 5), \qquad 4^{4k} \equiv 1 (\mathrm{mod}\, 5).$$

Iš čia

$$(1^{4k} + 2^{4k} + 3^{4k} + 4^{4k}) \equiv 4 (\mathrm{mod}\, 5).$$

Taigi skaičius $1^n + 2^n + 3^n + 4^n$, $n = 4k$, $k \in \mathbf{Z}$, nesidalija iš 5.

5 pavyzdys. *Įrodykime, kad skaičius* $12^{2n+1} + 11^{n+2}$ *dalijasi iš* 133, *kai* $n \in N$.

Sprendimas. Kadangi

$$12^2 = 144 \equiv 11 (\mathrm{mod}\, 133),$$

tai

$$144^n \equiv 11^n (\mathrm{mod}\, 133) \quad \text{ir} \quad 12 \cdot 144^n = 12^{2n+1} \equiv 12 \cdot 11^n (\mathrm{mod}\, 133).$$

Iš lygybės

$$11^{n+2} = 121 \cdot 11^n, \quad \text{ir} \quad 121 \equiv -12 (\mathrm{mod}\, 133)$$

gauname, kad

$$11^{n+2} \equiv -12 \cdot 11^n (\mathrm{mod}\, 133).$$

Vadinasi,

$$12^{2n+1} + 11^{n+2} \equiv 12 \cdot 11^n - 12 \cdot 11^n = 0 (\mathrm{mod}\, 133).$$

6 pavyzdys. *Įrodykime, kad* $a^4 + b^4 + c^4$ *dalijasi iš* n, *jei* $a + b + c$ *ir* $a^2 + b^2 + c^2$ *dalijasi iš* n; *čia* $n \in N$, $a, b, c \in \mathbf{Z}$.

Sprendimas. Pagal sąlygą $a+b+c \equiv 0 (\mathrm{mod}\, n)$ ir $a^2+b^2+c^2 \equiv 0 (\mathrm{mod}\, n)$. Vadinasi,

$$a+b \equiv -c (\mathrm{mod}\, n) \quad \text{ir} \quad (a+b)^2 \equiv (-c)^2 (\mathrm{mod}\, n), \qquad a^2+2ab+b^2 \equiv c^2 (\mathrm{mod}\, n),$$
$$a^2+2ab+b^2-(a^2+b^2+c^2) \equiv c^2 (\mathrm{mod}\, n), \qquad 2ab \equiv 2c^2 (\mathrm{mod}\, n).$$

Pastarojo lyginio abi puses padauginę iš ab, gauname lyginį $2a^2b^2 \equiv 2abc^2 (\mathrm{mod}\, n)$. Tokiu pat būdu gauname lyginius $2a^2c^2 \equiv 2ab^2c (\mathrm{mod}\, n)$ ir $2b^2c^2 \equiv 2a^2bc (\mathrm{mod}\, n)$. Sudėję visus tris lyginius, gauname

$$2a^2b^2+2a^2c^2+2b^2c^2 \equiv 2abc^2+2ab^2c+2a^2bc = 2abc(a+b+c) \equiv 0 (\mathrm{mod}\, n).$$

Prie abiejų lyginio pusių pridėkime $a^4+b^4+c^4$ ir gausime, kad

$$a^4+b^4+c^4 \equiv a^4+b^4+c^4+2a^2b^2+2a^2c^2+2b^2c^2 = (a^2+b^2+c^2)^2 \equiv 0 (\mathrm{mod}\, n).$$

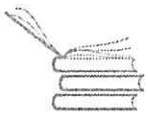
QED (lot. *quod erat demonstrandum* — tai ir reikėjo įrodyti).

Lyginių teorija yra gana plati. Šiame straipsnelyje tik susipažinome su lyginio sąvoka, jų savybėmis, išsprendėme paprasčiausius uždavinius. Daugiau apie lyginius galite rasti skaičių teorijos vadovėliuose.

Uždaviniai savarankiškam darbui

1. Raskite liekaną, gaunamą skaičių N dalijant iš d, kai:
   a) $N = 4554^{454} + 3113^{313}$, $d = 7$;
   b) $N = (1^2+1)(2^2+1)(3^2+1)\cdots(1000^2+1)$, $d = 3$;
   c) $N = 22^{22} + 333^{333} + 4444^{4444}$, $d = 5$.
2. Raskite paskutinį skaičiaus N skaitmenį, kai:
   a) $N = 103^{301} \cdot 107^{701}$;
   b) $N = 9339^{3993} + 3993^{9339}$;
   c) $N = 777^{777} - 888^{888}$.
3. Ar egzistuoja toks daugianaris $P(x)$, kurio koeficientai yra sveikieji skaičiai, kad $P(a) = m$ ir $P(b) = n$, kai:
   a) $a = 33$, $b = 44$, $m = 14$, $n = 41$;
   b) $a = 5$, $b = 9$, $m = 16$, $n = 25$;
   c) $a = 11$, $b = 33$, $m = 2001$, $n = 2003$?
4. Įrodykite, kad bent vienas iš skaičių a^2-b^2, a^2-c^2, b^2-c^2 dalijasi iš 3, jei skaičius $a^2+b^2+c^2$ dalijasi iš 3.
5. Įrodykite, kad , $3^{n+4}+1$ dalijasi iš 10, kai $n \in N$, jei 3^n+1 dalijasi iš 10.

Atsakymai. 1. a) 2; b) 2; c) 3. 2. a) 1; b) 6; c) 1. 3. a) ne; b) ne; c) taip.



1. K. Bulota, P. Survila, *Algebra ir skaičių teorija. II dalis*, Mokslas, Vilnius, 1990.