VIII. SVEIKŲJŲ SKAIČIŲ LAIPSNIAI

(2023–2025)

Teorinę medžiagą parengė bei aštuntąją užduotį sudarė Vilniaus universiteto docentas Aivaras Novikas

Sveikųjų skaičių laipsnius a^n (su natūraliuoju rodikliu n) ir reiškinius su šiais laipsniais nagrinėsime jų dalumo savybių požiūriu. Lygybė $(-a)^n = (-1)^n \cdot a^n$ parodo, kad daugeliu atveju pakanka nagrinėti natūraliojo skaičiaus a atvejį.

Dalyba su liekana. Nagrinėkime bet kokius sveikąjį skaičių a ir natūraląjį skaičių b. Iš a atimant arba prie a pridedant b bet kiek kartų, gaunami visi įmanomi skaičiai $a - bk$, kur skaičius k sveikasis. Į intervalą $[0; b)$ visada patenka lygiai vienas toks skaičius $r = a - bq$. Šio r bei atitinkamo sveikojo skaičiaus q radimas vadinamas **skaičiaus a dalyba iš skaičiaus b su liekana**. Skaičius q vadinamas šios dalybos **dalmeniu**, o skaičius r – jos **liekana**. Turime lygybę $a = bq + r$, kur r yra vienas iš skaičių 0, 1, 2, ..., $b - 1$. Pavyzdžiui, jei $a = 775$ ir $b = 11$, tai intervale $[0; 11)$ atsidursime, $q = 70$ kartų iš a atėmę b. Taigi padalijus 775 iš 11 su liekana, gaunamas dalmuo $q = 70$ ir liekana $r = 775 - 11 \cdot 70 = 5$. Jei vietoj 775 imsime $a = -775$, tai prie a turėsime 71 kartą pridėti b, kad gautume liekaną $r = (-775) - 11 \cdot (-71) = 6$ (ir dalmenį $q = -71$). Bendruoju atveju pasirinkus bet kurią reikšmę $r = 0, 1, 2, ..., b - 1$, visi skaičiai $bk + r$, kur skaičius k sveikasis, dalijasi iš b su ta pačia liekana r. Kai sveikieji skaičiai skiriasi per natūraliojo b kartotinį, tai dalijasi iš b su ta pačia liekana. Pavyzdžiui, iš 11 su liekana 6 dalijasi skaičiai ..., -27, -16, -5, **6**, 17, 28, 39, 50, 61, ...

Sveikųjų skaičių a_1 ir a_2 sumoje pakeitę skaičių a_1 į jo dalybos iš natūraliojo b liekaną $r_1 = a_1 - bq_1$, pakeisime sumą per b kartotinį bq_1, taigi nepakeisime sumos dalybos iš b liekanos. Tą patį galima pasakyti apie sveikųjų skaičių skirtumą: norint rasti $a_1 - a_2$ dalybos iš b liekaną, tiek a_1, tiek a_2 galima pakeisti jų atitinkamomis liekanomis. Lygybė $(bq_1 + r_1)a_2 = b \cdot (q_1 a_2) + r_1 a_2$ panašiai parodo, kad sveikuosius skaičius galima keisti jų dalybos iš b liekanomis, nagrinėjant sandaugą. Pavyzdžiui, dalijant skaičių $a = 1250^2 \cdot 547 + 7426 - 617^3$ iš 13 su liekana, pakanka iš 13 su liekana padalyti skaičius 1250, 547, 7426, 617 ir juos pakeisti atitinkamomis liekanomis:

$$1250 = 13 \cdot 96 + 2, \quad 547 = 13 \cdot 42 + 1, \quad 7426 = 13 \cdot 571 + 3, \quad 617 = 13 \cdot 47 + 6;$$

$$1250^2 \cdot 547 + 7426 - 617^3 \equiv 2^2 \cdot 1 + 3 - 6^3 \pmod{13}.$$

Čia užrašas $u \equiv v \pmod{m}$ – **lyginys moduliu m** – reiškia, kad u ir v dalijasi iš m su ta pačia liekana (skiriasi per m kartotinį). Jį skaitome „**u lygsta v moduliu m**“. Kaip ir lygybių atveju, galima rašyti nenutrūkstamą lyginių moduliu m seką:

$$2^2 \cdot 1 + 3 - 6^3 \equiv -209 \equiv (-1) \cdot (13 \cdot 16 + 1) \equiv (-1) \cdot 1 \equiv -1 \equiv 12 \pmod{13}.$$

Taigi pradinis skaičius a, kaip ir skaičiai, kuriais jį pakeitėme, dalijasi iš 13 su liekana 12.

1 pavyzdys. Raskime trečiąjį mažiausią natūraląjį x, kuriam skaičius $784\,565^{565\,487} + x$ dalijasi iš 12. Tam raskime $a = 784\,565^{565\,487}$ dalybos iš 12 liekaną:

$$784\,565 = 12 \cdot 65\,380 + 5, \qquad a \equiv 5^{565\,487} \pmod{12}.$$

Čia laipsnio pagrindą 784 565 galime suprastinti moduliu 12, nes kėlimas laipsniu reiškia kartotinę daugybą: turime 565 487-is dauginamuosius, lygius 784 565, kurių kiekvieną galime pakeisti dalybos liekana 5. Tačiau taip pat suprastinti rodiklį 565 487 būtų klaida. Vietoj to pastebėkime, kad $5^2 \equiv 1 \pmod{12}$ ir todėl $a \equiv (5^2)^{282\,743} \cdot 5 \equiv 1^{282\,743} \cdot 5 \equiv 5 \pmod{12}$. Vadinasi, $a + x$ dalijasi iš 12 (su liekana 0) tada ir tik tada, kai iš 12 dalijasi $5 + x_0$, kur x_0 yra x dalybos iš 12 liekana. Tinka tik $x_0 = 7$. Trys tokie mažiausi natūralieji skaičiai x yra 7, $7 + 12 = 19$ ir $7 + 12 \cdot 2 = 31$.

Atsakymas. $x = 31$.

2 pavyzdys. Raskime didžiausią natūraląjį triženklį x, kuriam $74^{44^{30}} - x$ dalijasi iš 27. Pažymėkime $a = 74^{44^{30}}$. Tada $74 \equiv 20 \pmod{27}$ ir $a \equiv 20^{44^{30}} \equiv (-7)^{44^{30}} \equiv 7^{44^{30}} \pmod{27}$. Čia 20 verta pakeisti su šia liekana iš 27 besidalijančiu skaičiumi $20 - 27 = -7$, nes $7 < 20$. Minusas prie 7 prapuola, nes laipsnio rodiklis 44^{30} yra lyginis. Toliau iš eilės tikrinkime septyneto laipsnių 7, 7^2, 7^3, … dalybos iš 27 liekanas. Čia, pavyzdžiui, nustačius, kad $7^4 \equiv 25 \pmod{27}$, tiesiogiai apskaičiuoti 7^5 reikšmę ir dalyti ją iš 27 nebūtina. Vietoj to turime

$$7^5 \equiv 7^4 \cdot 7 \equiv 25 \cdot 7 \equiv (-2) \cdot 7 \equiv -14 \equiv 13 \pmod{27},$$

toliau analogiškai $7^6 \equiv 7^5 \cdot 7 \equiv 13 \cdot 7 \equiv 91 \equiv 10 \pmod{27}$, ir t. t.

Taip gauname, kad $7^9 \equiv 1 \pmod{27}$ (tęsdami parodytus veiksmus, patikrinkite savarankiškai!). Jei rodiklis 44^{30} dalytųsi iš 9, tai iš karto gautume $a \equiv (7^9)^{\cdots} \equiv 1^{\cdots} \equiv 1 \pmod{27}$. Nors situacija

sudėtingesnė, vis tiek mėginkime pasiremti gauta parankia skaičiaus 7^9 liekana 1. Tam raskime rodiklio 44^{30} dalybos iš rodiklio 9 liekaną: $44 \equiv -1 \pmod 9$, todėl $44^{30} \equiv (-1)^{30} \equiv 1 \pmod 9$. Tegu $44^{30} = 9k + 1$ (skaičius k natūralusis). Tada $a \equiv 7^{9k+1} \equiv (7^9)^k \cdot 7 \equiv 1^k \cdot 7 \equiv 7 \pmod{27}$. Taigi vietoj $a - x$ galime nagrinėti $7 - x_0$, ir čia x dalybos iš 27 liekana x_0 turi būti lygi 7. Didžiausias triženklis skaičius 999 dalijasi iš 27 su liekana 0. Vadinasi, su liekana 7 iš 27 dalijasi skaičius 1006, o didžiausias toks triženklis skaičius yra $1006 - 27 = 979$.

Pabrėžkime, kad $74^{44^{30}} = 74^{(44^{30})} \neq (74^{44})^{30} = 74^{1320}$. Jei čia nagrinėtume $(74^{44})^{30} - x$, tai sprendime gautume $1320 \equiv 6 \pmod 9$, o tada $a \equiv 7^6 \equiv 10 \pmod{27}$ bei atsakymą $x = 982$.

Atsakymas. $x = 979$.

Laipsniai ir dalybos liekana 1. Išnagrinėtame 2 pavyzdyje buvo svarbu rasti skaičiaus 7 laipsnį, kuris dalytųsi iš 27 su liekana 1. Jį radome tikrindami visus skaičiaus 7 laipsnius (su natūraliaisiais rodikliais). Mums pasisekė, kad tiko jau 7^9 ir neteko tikrinti ilgiau. Ar galima tikrinimo išvengti? Kodėl apskritai galime būti tikri, kad liekaną 1 įmanoma gauti? Čia padeda teoremos, kurios nusako natūralųjį n, kuriam duoto tinkamo sveikojo skaičiaus a laipsnis a^n garantuotai dalijasi iš duoto natūraliojo m su liekana 1. Pirmoji iš jų nusako atvejį, kai skaičius m pirminis.

1 teiginys. Tarkime, kad sveikasis skaičius a nesidalija iš pirminio skaičiaus p. Tada $a^{p-1} - 1$ dalijasi iš p.

Įrodymas. Kadangi joks iš skaičių 1, 2, 3, ..., $p - 1$ nesidalija iš p, kaip ir skaičius a, tai ir aritmetinėje progresijoje $a, 2a, 3a, ..., (p-1)a$ joks narys nesidalija iš p. Analogiškai iš p nesidalija ir jokių dviejų progresijos narių ia ir ja, kur $i \neq j$, skirtumas $(i - j)a$, nes tai yra a sandauga su skaičiumi $i - j$, kuris lygus vienam iš skaičių $\pm 1, \pm 2, \pm 3, ..., \pm(p-2)$. Todėl dalijant nagrinėjamos progresijos narius iš p, visos gaunamos atitinkamos liekanos $r_1, r_2, r_3, ..., r_{p-1}$ yra nenulinės ir skirtingos. Nenulinių dalybos iš p liekanų tėra $p - 1$, todėl liekanos $r_1, r_2, r_3, ..., r_{p-1}$ turi būti tam tikra tvarka surašytos visos galimos nenulinės liekanos 1, 2, 3, ..., $p - 1$. Vadinasi,

$$a \cdot 2a \cdot 3a \cdot ... \cdot (p-1)a \equiv r_1 \cdot r_2 \cdot r_3 \cdot ... \cdot r_{p-1} \equiv 1 \cdot 2 \cdot 3 \cdot ... \cdot (p-1) \pmod p,$$

$a^{p-1}(p-1)! \equiv (p-1)! \pmod p$, $\quad a^{p-1}(p-1)! - (p-1)! = (p-1)!\,(a^{p-1} - 1)$ dalijasi iš p. Vėlgi, skaičiai 1, 2, 3, ..., $p - 1$ nesidalija iš p, todėl nesidalija ir jų sandauga $(p-1)!$. Skaičius $a^{p-1} - 1$ dalijasi iš p, nes priešingu atveju iš p nesidalytų sandauga $(p-1)!\,(a^{p-1} - 1)$. Tai ir reikėjo įrodyti. ■

Įrodytas teiginys vadinamas **Mažąja Ferma teorema** (prancūzų matematikas Pierre de Fermat, 1601–1665; yra ir kita jo vardo teorema, vadinama didžiąja arba paskutiniąja). Dažnai naudojama jos alternatyvi formuluotė, pašalinant sąlygą, kad a dalijasi iš p: jei skaičius p pirminis, tai $a^p - a$ dalijasi iš p kiekvienam sveikajam a (net nesidalijančiam p – juk iš p visada dalijasi vienas iš sandaugos $a \cdot (a^{p-1} - 1)$ dauginamųjų).

Sąlyga, kad p yra pirminis skaičius, teoremoje esminė. Įrodyme ja rėmėmės, kelis kartus pasinaudoję tokia pirminių skaičių **savybe**, skiriančia juos nuo kitų natūraliųjų skaičių: jei keli sveikieji skaičiai nesidalija iš pirminio p, tai nesidalija ir jų sandauga. Ši savybė taip pat formuluojama dviem ar keliems skaičiams „atbulu“ būdu: jei sveikųjų skaičių sandauga dalijasi iš p, tai dalijasi bent vienas iš dauginamųjų. Ji vadinama **Euklido lema** (senovės graikų matematikas Euklidas Aleksandrietis, apie 300 m. pr. Kr.) ir yra stipriai susijusi su dar vienu teiginiu – **Pagrindine aritmetikos teorema**: kiekvienas natūralusis skaičius $n > 1$ užrašomas pirminių skaičių sandauga lygiai vienu būdu (nekreipiant dėmesio į dauginamųjų tvarką). Čia pirminiai skaičiai sandaugoje nebūtinai skirtingi. Be to, leidžiamos sandaugos iš vieno pirminio dauginamojo (lygios jam pačiam).

Du sveikieji skaičiai, neturintys bendro daliklio, didesnio už 1, vadinami **tarpusavyje pirminiais**. Tarkime, kad kiekvienas iš natūraliųjų skaičių $b_1, b_2, b_3, ..., b_k$, išskyrus nebent b_1, yra tarpusavyje pirminis su natūraliuoju m. Tarkime, kad m ir sandauga $B = b_1 b_2 b_3 ... b_k$ turi bendrą daliklį $d > 1$ (taigi nėra tarpusavyje pirminiai). Tada $b_1 b_2 b_3 ... b_k = dc$ (skaičius c natūralusis). Abiejose lygybės pusėse vietoj kiekvieno dauginamojo galima įrašyti jam lygią pirminių skaičių sandaugą arba skaičių 1, ir tada abiejose lygybės pusėse turi būti tie patys pirminiai skaičiai, gali skirtis nebent jų tvarka (Pagrindinė aritmetikos teorema). Pirminiai skaičiai, įrašyti vietoj d, yra skaičiaus m dalikliai, todėl gali būti nebent vietoj b_1 įrašytoje išraiškoje. Tada b_1 dalijasi iš d, tad nėra tarpusavyje pirminis su m. Jei atskiru atveju $d = m$ (t. y. B dalijasi iš m), tai b_1 dalijasi iš m. ***Vadinasi***, jei natūraliųjų skaičių sandaugos kiekvienas dauginamasis, nebent išskyrus vieną, yra tarpusavyje pirminis su duotu natūraliuoju m, o tas likęs dauginamasis nesidalija iš m, tai ir visa

sandauga iš m nesidalija. ***Be to***, jei ir tas likęs dauginamasis yra tarpusavyje pirminis su m, tai tokia yra visa sandauga. Šias išvadas lengva apibendrinti sveikiesiems (nebūtinai natūraliesiems) skaičiams. Jas vietoj Euklido lemos naudojant Mažosios Ferma teoremos įrodyme, gaunamas teoremos apibendrinimas, kai vietoj pirminio p imamas natūralusis m.

Iš tiesų, tarkime, kad $m > 1$ ir a yra tarpusavyje pirminiai sveikieji skaičiai. Mažosios Ferma teoremos įrodyme iš a padauginkime ne 1, 2, 3, ..., $p-1$, o natūraliuosius skaičius nuo 1 iki m, tarpusavyje pirminius su m. Juos pažymėkime t_1, t_2, t_3, ..., t_k. Tada kiekviena gautoji sandauga $t_i a$ yra tarpusavyje pirminė su m. Tokia yra ir $t_i a$ dalybos iš m liekana r_i (pamąstykite kodėl!). Toliau kaip ankstesniame įrodyme pastebime, kad dviejų skirtingų sandaugų skirtumas $(t_i - t_j)a$ nesidalija iš m ir todėl liekanos r_i yra skirtingos bei tiesiog yra tam tikra tvarka surašyti pradiniai skaičiai t_1, t_2, t_3, ..., t_k. Pagaliau analogiškai nagrinėdami sandaugų $t_i a$ sandaugą moduliu m, gauname: $t_1 t_2 t_3 \dots t_k(a^k - 1)$, taigi ir $a^k - 1$ dalijasi iš m.

Kiekvienam natūraliajam m atitinkamą k – su m tarpusavyje pirminių natūraliųjų skaičių nuo 1 iki m kiekį – **pažymėkime $\varphi(m)$**. Mažiausioms m reikšmėms skaičių t_i aibės iš eilės lygios
$\{1\}, \{1\}, \{1,2\}, \{1,3\}, \{1,2,3,4\}, \{1,5\}, \{1,2,3,4,5,6\}, \{1,3,5,7\}, \{1,2,4,5,7,8\}, \{1,3,7,9\}, \dots$.
Taigi turime reikšmes $\varphi(1) = \varphi(2) = 1$, $\varphi(3) = \varphi(4) = \varphi(6) = 2$, $\varphi(5) = \varphi(8) = \varphi(10) = 4$, $\varphi(7) = \varphi(9) = 6$, ... Visose aibėse yra skaičius 1, tad kiekvienam natūraliajam m priskiriama reikšmė $\varphi(m)$ natūralioji. Gauname funkciją $\varphi : \mathbb{N} \to \mathbb{N}$, vadinamą **Oilerio funkcija** (šveicarų matematikas Leonhard Euler, 1707–1783). Pagaliau galime suformuluoti **Oilerio teoremą** – Mažosios Ferma teoremos apibendrinimą, kurio įrodymą aptarėme.

2 teiginys. Tarkime, kad $m \geq 1$ ir a yra tarpusavyje pirminiai sveikieji skaičiai. Tada skaičius $a^{\varphi(m)} - 1$ dalijasi iš m.

Ši teorema teisinga ne tik aptartu atveju $m > 1$, bet ir trivialiu atveju $m = 1$. Jei skaičius $m = p$ pirminis, tai su juo tarpusavyje pirminiai visi sveikieji skaičiai, nesidalijantys iš p (prisiminkime pirminio skaičiaus apibrėžimą). Nuo 1 iki m tai skaičiai $\{t_1, t_2, t_3, \dots, t_k\} = \{1, 2, 3, \dots, p-1\}$, taigi šiuo atveju $\varphi(m) = p - 1$, ir gauname Mažąją Ferma teoremą kaip atskirą Oilerio teoremos atvejį.

Oilerio teoremoje sąlyga, kad a ir m yra tarpusavyje pirminiai, esminė: priešingu atveju jie turi bendrą daliklį $d > 1$, iš kurio dalijasi visi a laipsniai a, a^2, a^3, ... Tada joks skaičius $a - 1$, $a^2 - 1$, $a^3 - 1$, ... nesidalija nei iš d, nei tuo labiau iš d kartotinio m. Vadinasi, sekoje a, a^2, a^3, ... iš m su liekana 1 nesidalija ne tik $a^{\varphi(m)}$, bet ir apskritai joks narys. Tuo tarpu jei a yra tarpusavyje pirminis su m, tai tinkamų sekos narių esama be galo daug: tai ne tik $a^{\varphi(m)}$, bet ir $a^{2\varphi(m)}$, $a^{3\varphi(m)}$, ... Net ir $a^{\varphi(m)}$ neprivalo būti pirmasis toks narys: 2 pavyzdyje matėme, kad tinka a^9, kai $a = 7$, $m = 27$, nors Oilerio teorema mums nurodo, kad tinka $a^{\varphi(27)} = a^{18}$.

Jei bendruoju atveju $a^k \equiv 1 \pmod m$ (skaičiai m ir k natūralieji, skaičius a sveikasis), tai $a^i \equiv a^{i+k} \equiv a^{i+2k} \equiv \dots \pmod m$ kiekvienam sveikajam $i \geq 0$. Gauname **išvadą**: jei sekoje a, a^2, a^3, ... narių a^i ir a^j rodikliai skiriasi per natūraliojo skaičiaus k kartotinį (t. y. i ir j dalijasi iš k su ta pačia liekana), kur $a^k \equiv 1 \pmod m$, tai a^i ir a^j dalijasi iš m su ta pačia liekana. Atskiru atveju a^i dalybos iš m liekana nepakinta, pakeičiant natūralųjį i jo dalybos iš tokio k liekana.

3 pavyzdys. Nustatykime, su kokia liekana skaičius $6^{559^{2025^{955}}} + 26^{5^{732}}$ dalijasi iš 29. Atskirai nagrinėkime $a_1 = 6^{559^{2025^{955}}}$ ir $a_2 = 26^{5^{732}}$. Skaičius 29 pirminis, o skaičiai 6 ir 26 iš jo nesidalija. Todėl $6^{28} \equiv 26^{28} \equiv 1 \pmod{29}$, ir rodiklius $b_1 = 559^{2025^{955}}$ ir $b_2 = 5^{732}$ galima prastinti moduliu 28, t. y. pakeisti jų dalybos iš 28 liekanomis. Suprastinti b_1 gana lengva:
$559 \equiv 27 \equiv -1 \pmod{28}$, $b_1 \equiv (-1)^{2025^{955}} \equiv -1 \equiv 27 \pmod{28}$, $a_1 \equiv 6^{27} \pmod{29}$.
Toliau skaičių 6^{27} galima suprastinti moduliu 29, keliais veiksmais mažinant laipsnio rodiklį:
$a_1 \equiv 6^{27} \equiv 216^9 \equiv 13^9 \equiv 169^4 \cdot 13 \equiv 24^4 \cdot 13 \equiv (-5)^4 \cdot 13 \equiv 8125 \equiv 5 \pmod{29}$.
Prastindami rodiklį b_2 pasinaudokime tuo, kad laipsnio 5^{732} pagrindas 5 yra tarpusavyje pirminis su $28 = 2^2 \cdot 7$ (nesidalija nei iš 2, nei iš 7). Galioja Oilerio teorema: nuo 1 iki 28 yra 12 natūraliųjų skaičių, kurie nesidalija nei iš 2, nei iš 7, todėl $\varphi(28) = 12$ ir $5^{12} \equiv 1 \pmod{28}$. Turime
$732 \equiv 0 \pmod{12}$, $b_2 \equiv 5^0 \equiv 1 \pmod{28}$, $a_2 \equiv 26^1 \equiv 26 \pmod{29}$.
Vadinasi, $a_1 + a_2 \equiv 5 + 26 \equiv 31 \equiv 2 \pmod{29}$.

Atsakymas. 2.

4 pavyzdys. Nustatykime, su kokia liekana $3126^{559^{7201}} + 17^{2809^{289}} + 20^{2^{736}}$ dalijasi iš 81. Su $81 = 3^4$ tarpusavyje pirminiai yra tie sveikieji skaičiai, kurie nesidalija iš 3. Nuo 1 iki 81 iš 3 dalijasi kas trečias natūralusis skaičius, todėl tokių skaičių yra $81:3 = 27$. Taigi $\varphi(81) = 81 - 27 = 54$.

3126 dalijasi iš 3, tad skaičiui $a_1 = 3126^{559^{7201}}$ Oilerio teoremos nepritaikysime. To ir nereikia: laipsnio pagrindas dalus iš 3, todėl a_1 dalijasi iš trejeto didelio laipsnio (iš $3^{559^{7201}}$), tuo labiau iš 3^4.

Skaičius 17 iš 3 nesidalija, todėl taikome Oilerio teoremą laipsniui $a_2 = 17^{2809^{289}}$:

$2809 \equiv 1 \pmod{54}$, $2809^{289} \equiv 1^{289} \equiv 1 \pmod{54}$, $17^{2809^{289}} \equiv 17^1 \equiv 17 \pmod{81}$.

Skaičius 20 iš 3 nesidalija, todėl pagal Oilerio teoremą laipsnio $a_3 = 20^{2^{736}}$ rodiklį 2^{736} galime suprastinti moduliu 54. Laipsniui 2^{736} vėl būtų galima taikyti Oilerio teoremą, tačiau jo pagrindas 2 nėra tarpusavyje pirminis su $54 = 2 \cdot 27$. Visgi jis yra tarpusavyje pirminis su 27. Analogiškai kaip $\varphi(81)$ reikšmę, gauname $\varphi(27) = 27 - 9 = 18$. Tada $736 \equiv 16 \pmod{18}$, $2^{736} \equiv 2^{16} \pmod{27}$. Toliau gauname $2^{16} \equiv 32^3 \cdot 2 \equiv 5^3 \cdot 2 \equiv 250 \equiv 7 \pmod{27}$. Taigi skaičius 2^{736} dalijasi iš 27 su liekana 7 ir priklauso progresijai $7, 7 + 27, 7 + 2 \cdot 27$, ..., kurią galima išskaidyti į dvi progresijas pagal dalumą iš 54: nelyginiai skaičiai $7, 7 + 2 \cdot 27, 7 + 4 \cdot 27$, ... dalijasi iš 54 su liekana 7, o lyginiai skaičiai $34, 34 + 2 \cdot 27, 34 + 4 \cdot 27$, ... dalijasi iš 54 su liekana 34. Skaičius 2^{736} lyginis, todėl $2^{736} \equiv 34 \pmod{54}$, $a_3 \equiv 20^{34} \equiv 400^{17} \equiv 76^{17} \equiv (-5)^{17} \pmod{81}$ ir

$$a_3 \equiv (-25) \cdot 3125^3 \equiv (-25) \cdot 47^3 \equiv (-1) \cdot 2\,595\,575 \equiv -11 \equiv 70 \pmod{81}.$$

Tada $a_1 + a_2 + a_3 \equiv 0 + 17 + 70 \equiv 87 \equiv 6 \pmod{81}$.

Atsakymas. 6.

Oilerio funkcija. Remiantis Pagrindine aritmetikos teorema, kiekvienas natūralusis $m > 1$ užrašomas išraiška $p_1^{a_1} p_2^{a_2} p_3^{a_3} \ldots p_k^{a_k}$, kur $p_1, p_2, p_3, \ldots, p_k$ (čia $k \geq 1$) yra skirtingi pirminiai skaičiai, o rodikliai $a_1, a_2, a_3, \ldots, a_k$ yra natūralieji. Be to, tokią išraišką – **skaidinį pirminiais daugikliais** – skaičius m turi vienintelę (nekreipiant dėmesio į dauginamųjų tvarką). Skaičiai $p_1, p_2, p_3, \ldots, p_k$ yra visi pirminiai m dalikliai (kitų nėra pagal Euklido lemą). Jei sveikasis n yra tarpusavyje pirminis su tokiu skaičiumi m, tai nesidalija iš jokio p_i. Kita vertus, jei n nėra tarpusavyje pirminis su m, tai jie turi bendrą daliklį $d > 1$, kuris (būdamas pirminių skaičių sandauga) turi pirminį daliklį p, iš kurio tada dalijasi m ir n. Kadangi iš p dalijasi m, tai p sutampa su vienu iš p_i. ***Vadinasi***, sveikieji skaičiai, tarpusavyje pirminiai su natūraliuoju m, yra visi sveikieji skaičiai, nesidalijantys iš jokio pirminio skaičiaus, kuris yra m skaidinyje pirminiais daugikliais. Šia išvada jau nejučia naudojomės pavyzdžiuose: skaičiai, tarpusavyje pirminiai su $28 = 2^2 \cdot 7$ arba su $81 = 3^4$, – tai skaičiai, nesidalijantys atitinkamai iš 2 ir 7 arba iš 3. Šis pastebėjimas pravers, gaunant Oilerio funkcijos formulę, leidžiančią tiesiogiai neskaičiuoti, keli skaičiai nuo 1 iki m yra tarpusavyje pirminiai su m.

5 pavyzdys. Nustatykime, kaip susijusios reikšmės $\varphi(m)$ ir $\varphi(5m)$, kai $m > 1$ yra bet koks natūralusis skaičius. Nuo 1 iki m yra $\varphi(m)$ natūraliųjų skaičių, tarpusavyje pirminių su m, t. y. tokių, kurie nesidalija iš pirminių skaičių, esančių skaičiaus m skaidinyje pirminiais daugikliais (trumpinsime – SPD). Nuo 1 iki $5m$ analogiškai yra $\varphi(5m)$ natūraliųjų skaičių, kurie nesidalija iš pirminių skaičių, esančių skaičiaus $5m$ SPD. Natūraliuosius skaičius nuo 1 iki $5m$ išskaidykime į 5 aibes: nuo 1 iki m, nuo $m + 1$ iki $2m$, nuo $2m + 1$ iki $3m$, nuo $3m + 1$ iki $4m$, nuo $4m + 1$ iki $5m$. Pasirinkus bet kurį skaičių r iš pirmosios aibės, skaičiai $r, r + m, r + 2m, r + 3m, r + 4m$ arba visi turi pirminį daliklį iš m SPD, arba visi neturi. Todėl penkiose aibėse yra po $\varphi(m)$ skaičių, tarpusavyje pirminių su m, o iš viso jų gauname $5\varphi(m)$. Toliau yra dvi galimybės: arba pirminis skaičius 5 yra skaičiaus m SPD skaidinyje, arba nėra. Pirmuoju atveju su m ir su $5m$ tarpusavyje pirminiai yra tie patys skaičiai, ir $\varphi(5m) = 5\varphi(m)$. Skaičiuodami $\varphi(5m)$ antruoju atveju, dar turime papildomai atmesti tuos iš skaičių $5, 5 \cdot 2, 5 \cdot 3$, ..., $5m$, kurie yra tarpusavyje pirminiai su m (bet ne su $5m$, nes dalijasi iš 5). Tai tie skaičiai $5a$, kur $a = 1, 2, 3, \ldots, m$ yra tarpusavyje pirminis su m. Tokių a yra $\varphi(m)$, todėl šiuo atveju $\varphi(5m) = 5\varphi(m) - \varphi(m) = 4\varphi(m)$. Taigi žinodami, kad $\varphi(28) = 12$, gauname $\varphi(140) = 4 \cdot 12 = 48$, $\varphi(700) = 5 \cdot 48 = 240$, $\varphi(3500) = 5 \cdot 240 = 1200$ ir apskritai $\varphi(28 \cdot 5^n) = 12 \cdot 4 \cdot 5^{n-1}$ (kiekvienam natūraliajam n).

Atsakymas. $\varphi(5m) = 5\varphi(m)$, kai m dalijasi iš 5, ir $\varphi(5m) = 4\varphi(m)$ priešingu atveju.

5 pavyzdyje vietoj $\varphi(5m)$ imdami $\varphi(pm)$, kur skaičius p – bet koks pirminis, analogiškai įrodytume, kad $\varphi(pm) = p\varphi(m)$, kai m dalijasi iš p, ir $\varphi(pm) = (p-1)\varphi(m)$ priešingu atveju. Tada $\varphi(m \cdot p^n) = \varphi(m) \cdot (p-1) \cdot p^{n-1} = \varphi(m) \cdot (p^n - p^{n-1})$ kiekvienam natūraliajam n, kai

natūralusis $m > 1$ nesidalija iš p. Be to, ši formulė teisinga, ir kai $m = 1$, pagal $\varphi(p) = p - 1$ ir $\varphi(p^n) = \varphi(p) \cdot p^{n-1} = p^n - p^{n-1}$ (kai $n > 1$). Taip gauname bendrąją Oilerio funkcijos formulę.

Išvada. Tarkime, kad natūraliojo $m > 1$ skaidinys pirminiais daugikliais yra $p_1^{a_1} p_2^{a_2} p_3^{a_3} \dots p_k^{a_k}$. Tada $\varphi(m) = \left(p_1^{a_1} - p_1^{a_1-1}\right)\left(p_2^{a_2} - p_2^{a_2-1}\right)\left(p_3^{a_3} - p_3^{a_3-1}\right) \dots \left(p_k^{a_k} - p_k^{a_k-1}\right)$.

Taigi, pavyzdžiui, $\varphi(2^2 \cdot 7) = (2^2 - 2)(7 - 1) = 12$, $\varphi(7^4) = 7^4 - 7^3 = 2058$, $\varphi(3 \cdot 73) = (3 - 1)(73 - 1) = 144$, $\varphi(7^3 \cdot 11^2 \cdot 29) = (7^3 - 7^2)(11^2 - 11)(29 - 1) = 905\,520$, ... Bet $\varphi(9^4) \neq 9^4 - 9^3$ ir $\varphi(3 \cdot 91) \neq (3 - 1)(91 - 1)$ (skaičiai 9 ir 91 ne pirminiai). Iš tiesų $\varphi(9^4) = 3^8 - 3^7$ ir $\varphi(3 \cdot 91) = (3 - 1)(7 - 1)(13 - 1)$. Taip pat $\varphi(3^2 \cdot 3^5) \neq (3^2 - 3)(3^5 - 3^4)$ (SPD pirminiai skaičiai p_i turi būti skirtingi). Taikant Oilerio funkcijos formulę, reikia gauti m SPD.

6 pavyzdys. Apskaičiuokime a) visas galimas $\varphi(75m) : \varphi(m)$ reikšmes; b) $\varphi(579\,768)$.

a) Kadangi $75 = 3 \cdot 5 \cdot 5$, tai $\varphi(75m)$ gauname iš $\varphi(m)$, daugindami iš 2 arba 3 (priklausomai nuo to, ar m dalijasi iš 3), tada iš $4 \cdot 5 = 20$ arba $5 \cdot 5 = 25$ (priklausomai nuo to, ar m dalijasi iš 5).

b) Išskaidykime skaičių $m = 579\,768$ pirminiais daugikliais, vis dalydami iš pirminių skaičių 2, 3, 5, ... (jei dalijasi be liekanos). Pirmiausiai kartotinai dalykime iš 2, kol tai įmanoma, tada iš 3, ir t. t.: $579\,768 : 2 = 289\,884$, $289\,884 : 2 = 144\,942$, $144\,942 : 2 = 72\,471$ (nesidalija iš 2), $72\,471 : 3 = 24\,157$ (nesidalija iš 3, iš 5), $24\,157 : 7 = 3\,451$, $3\,451 : 7 = 493$ (nesidalija iš 7, iš 11, iš 13), $493 : 17 = 29$ (gautas skaičius pirminis). Vadinasi, $m = 2^3 \cdot 3 \cdot 7^2 \cdot 17 \cdot 29$ ir $\varphi(m) = 4 \cdot 2 \cdot 42 \cdot 16 \cdot 28 = 150\,528$.

Atsakymas. a) 40, 50, 60, 75; b) 150 528.

Primityvioji šaknis. Tarkime, kad sveikasis skaičius a nesidalija iš pirminio skaičiaus p. Seką a, a^2, a^3, ... nagrinėkime moduliu p, t. y. dalybos iš p liekanų požiūriu. Jei dvi liekanos sutampa, t. y. jei $a^i \equiv a^j \pmod p$, $i < j$, tai $a^j - a^i = a^i\left(a^{j-i} - 1\right)$ dalijasi iš p. Tada iš p dalijasi $a^{j-i} - 1$, o a^{j-i} dalijasi iš p su liekana 1. Čia $j - i < j$, todėl kol sekoje a, a^2, a^3, ... negausime liekanos 1, jos narių dalybos iš p liekanos negali sutapti. Tegu k yra mažiausias natūralusis skaičius, kuriam $a^k \equiv 1 \pmod p$ (egzistuoja pagal Mažąją Ferma teoremą). Jis vadinamas **skaičiaus a eile moduliu p**. Tada skaičių a, a^2, a^3, ..., a^k dalybos iš p liekanos yra k skirtingų skaičių. Toliau liekanos periodiškai kartojasi: $a^{k+1} \equiv a \cdot a^k \equiv a \cdot 1 \equiv a \pmod p$, panašiai $a^{k+2} \equiv a^2 \pmod p$, $a^{k+3} \equiv a^3 \pmod p$, ir t. t. Negausime kitų liekanų nei skaičių a, a^2, a^3, ..., a^k liekanos. ***Vadinasi***, skaičiaus a laipsniai moduliu p generuoja tiek skirtingų liekanų, kokia yra a eilė moduliu p. Su liekana 1 iš p dalijasi tik laipsniai a^k, a^{2k}, a^{3k}, ... (čia rodikliai yra k kartotiniai). Tarp jų yra a^{p-1} (Mažoji Ferma teorema). ***Vadinasi,*** skaičiaus eilė k moduliu p visada yra skaičiaus $p - 1$ daliklis, ir $k \leq p - 1$. Pavyzdžiui, skaičiaus 3 laipsniai iš eilės generuoja dalybos iš 11 liekanas 3, 9, 5, 4, 1, 3, 9, 5, 4, 1, ... (čia, pvz., $3^4 \equiv 3^3 \cdot 3 \equiv 5 \cdot 3 \equiv 15 \equiv 4 \pmod{11}$). Taigi skaičiaus 3 eilė moduliu 11 yra 5. Nors ji nesutampa su $11 - 1 = 10$, bet yra 10 daliklis. Žinoma, tada eilė moduliu 11 lygi 5 ir skaičiams $3 + 11 = 14$, $14 + 11 = 25$, $3 - 11 = -8$ ir t. t. Tuo tarpu skaičiaus 2 (tuo pačiu skaičių 24, -9 ir t. t) eilė moduliu 11 lygi 10 (yra maksimali). Skaičius 55 eilės moduliu 11 apskritai neturi (dalijasi iš 11), o jo eilė moduliu 13 yra tokia pati kaip skaičiaus $55 - 4 \cdot 13 = 3$ (ši eilė lygi 3).

Pastaba. Vietoj pirminio p imant bet kokį natūralųjį m, analogiškai apibrėžiama eilė moduliu m kiekvienam sveikajam a, tarpusavyje pirminiam su m. Ji yra skaičiaus $\varphi(m)$ daliklis ir vėlgi parodo, kiek skirtingų dalybos iš m liekanų generuoja laipsniai a, a^2, a^3, ... Dar 2 pavyzdyje matėme, kad skaičiaus 7 eilė moduliu 27 lygi 9. Atitinkamos 9 liekanos yra 7, 22, 19, 25, 13, 10, 16, 4, 1.

Yra įrodyta, kad kiekvienam pirminiam p egzistuoja toks sveikasis skaičius g, nedalus iš p, kurio eilė moduliu p lygi $p - 1$. Kiekvienas toks g vadinamas **primityviąja šaknimi moduliu p**. Tokio g laipsniai g, g^2, g^3, ..., g^{p-1} nesidalija iš p ir generuoja $p - 1$ liekaną, tad g yra visų galimų nenulinių liekanų 1, 2, 3, ..., $p - 1$ generatorius (todėl jį ir žymime g). T. y. g, g^2, g^3, ..., g^{p-1} dalybos iš p liekanos yra tam tikra tvarka surašyti skaičiai 1, 2, 3, ..., $p - 1$.

7 pavyzdys. Nustatykime, kurie iš skaičių 2, 87, -109, 12 569 yra primityviosios šaknys moduliu 19.

Pradėkime nuo skaičiaus 2. Reikia nustatyti, ar jo eilė yra $19 - 1 = 18$, ar mažesnė. Iš Mažosios Ferma teoremos žinome, kad $2^{18} \equiv 1 \pmod{19}$, to netikrinkime. Reikia patikrinti, ar kuris iš skaičių 2^1, 2^2, 2^3, ..., 2^{18} lygsta 1 moduliu 19. Skaičius 18 yra gana mažas, tad būtų galima tiesiogiai patikrinti visus šiuos dvejeto laipsnius. Tačiau žinome, kad skaičiaus eilė yra 18 daliklis, todėl lieka tikrinti 2^1, 2^2, 2^3, 2^6, 2^9. Be to, jei $2^9 \equiv (2^3)^3 \not\equiv 1 \pmod{19}$, tai $2^3 \not\equiv 1 \pmod{19}$, todėl nebūtina tikrinti 2^3 ir analogiškai 2^1, 2^2. Taigi kadangi $2^6 \equiv 7 \not\equiv 1 \pmod{19}$ ir $2^9 \equiv 16^2 \cdot 2 \equiv (-3)^2 \cdot 2 \not\equiv$

$\not\equiv 1 \pmod{19}$, tai skaičiaus 2 eilė moduliu 19 lygi 18, o pats skaičius 2 yra primityvioji šaknis.

Skaičiaus 87 eilė moduliu 19 yra tokia pati kaip skaičiaus $87 - 19 \cdot 4 = 11$. Analogiškai kaip skaičiui 2, pakanka tikrinti laipsnius 11^6 ir 11^9. Kadangi $11^6 \equiv 121^3 \equiv 7^3 \equiv 343 \equiv 1 \pmod{19}$, tai 11^9 galime netikrinti: skaičių 11 ir 87 eilė moduliu 19 yra ne didesnė nei 6, todėl tai nėra primityviosios šaknys moduliu 19.

Skaičius -109 nėra primityvioji šaknis moduliu 19, o skaičius 12569 yra, nes $(-109)^9 \equiv 5^9 \equiv$ $\equiv 125^3 \equiv 11^3 \equiv 1 \pmod{19}$, $12\,569 \equiv 10 \pmod{19}$, $10^6 \equiv 11 \pmod{19}$, $10^9 \equiv 18 \pmod{19}$.

Atsakymas. 2 ir 12569.

Apibendrinkime pavyzdžio pastebėjimus. Jei sveikasis a nesidalija iš pirminio p ir reikia nustatyti, ar a yra primityvioji šaknis moduliu p, tai pakanka patikrinti laipsnius a^d, kur $d < p - 1$ yra teigiamas skaičiaus $p - 1$ daliklis. Dar daugiau, pakanka patikrinti tik $a^{\frac{p-1}{q}}$ kiekvienam skaičiaus $p - 1$ pirminiam dalikliui q, nes skaičių $\frac{p-1}{q}$ teigiami dalikliai yra visos galimos d reikšmės. Jei nė vienas toks laipsnis $a^{\frac{p-1}{q}}$ nesidalija iš p su liekana 1, tai a yra primityvioji šaknis moduliu p. Žinoma, priešingu atveju a nėra primityvioji šaknis moduliu p.

8 pavyzdys. Galima patikrinti, kad mažiausia natūralioji primityvioji šaknis moduliu 41 yra 6. Iš tiesų, $1^1 \equiv 2^{20} \equiv 3^8 \equiv 4^{20} \equiv 5^{20} \equiv 1 \pmod{41}$, bet $6^8 \equiv 10 \pmod{41}$, $6^{20} \equiv 40 \pmod{41}$. Nustatykime skaičių 6^{22}, 6^{23}, 6^{25}, 6^{30} eilę moduliu 41. Taigi, kokiems natūraliesiems k skaičius $(6^{22})^k - 1 = 6^{22k} - 1$ dalijasi iš 41? Kadangi 6 yra primityvioji šaknis, tai tiems ir tik tiems k, kuriems rodiklis $22k$ dalijasi iš $41 - 1 = 40$, taigi kuriems k dalijasi iš 20. Mažiausias toks k yra 20. Jis ir yra skaičiaus 6^{22} eilė. Analogiškai mažiausias k, kuriam $23k$, $25k$, $30k$ dalijasi iš 40, yra atitinkamai 40, 8, 4. Skaičiai 6^{22}, 6^{23}, 6^{25}, 6^{30} dalijasi iš 41 atitinkamai su liekana 5, 30, 14, 9. Taigi tuo pačiu nustatėme ir skaičių 5, 30, 14, 9 eiles moduliu 41. Jos yra atitinkamai 20, 40, 8, 4.

Atsakymas. 20, 40, 8, 4.

9 pavyzdys. Žinodami, kad 2 yra primityvioji šaknis moduliu 19, nustatykime, kurios iš lygčių

$$x^6 = 19y + 5, \qquad x^6 = 19y + 11, \qquad x^5 = 19y + 5$$

turi sveikąjį sprendinį (x, y). Toms lygtims, kurios turi tokį sprendinį, nustatykime visas galimas reikšmes $n = 1, 2, 3, ..., 18$, kurioms lygtis turi sveikąjį sprendinį $(x, y) = (2^n, y)$.

Pirmoji lygtis turi sveikąjį sprendinį (x, y) tada ir tik tada, kai sveikąjį sprendinį x turi lyginys $x^6 \equiv 5 \pmod{19}$. Čia x negali dalytis iš 19, nes priešingu atveju $x^6 \equiv 0 \pmod{19}$. Taigi x dalijasi iš 19 su viena iš liekanų 1, 2, 3, ..., 18 – su ta pačia liekana kaip vienas iš skaičių 2^n, kur $n = 1, 2, 3, ..., 18$. Tada $x^6 \equiv 2^{6n} \equiv 64^n \equiv 7^n \pmod{19}$. Tačiau laipsniai 7^n dalijasi iš 19 tik su liekanomis 7, $11 (\equiv 7^2)$ ir $1 (\equiv 7^3)$. Vadinasi, x^6 negali dalytis iš 19 su liekana 5, o lygtis sprendinių neturi.

Panašiai nagrinėjame antrąją lygtį: lyginyje $x^6 \equiv 11 \pmod{19}$ vietoj x įrašome tokį laipsnį 2^n, kad $x \equiv 2^n \pmod{19}$, ir gauname $7^n \equiv 11 \pmod{19}$. Čia $n = 1, 2, 3, ..., 18$. Jau nustatėme, kad tinka $n = 2$, o kadangi skaičiaus 7 eilė moduliu 19 yra 3, tai dar tinka $n = 2 + 3, 2 + 6, 2 + 9, ...$ Vadinasi, nuo 1 iki 18 tinka reikšmės $n = 2, 5, 8, 11, 14, 17$.

Trečioji lygtis analogiškai suvedama į lyginius $x \equiv 2^n \pmod{19}$ ir $13^n \equiv 5 \pmod{19}$. Čia vietoj 7 turime 13, nes $2^{5n} \equiv 32^n \equiv 13^n \pmod{19}$. Vieną po kitos rašykime skaičiaus 13 laipsnių dalybos iš 19 liekanas: 13, 17, 12, 4, 14, 11, 10, 16, 18, ... Čia, pavyzdžiui, $13^7 \equiv 13^6 \cdot 13 \equiv$ $\equiv 11 \cdot 13 \equiv 10 \pmod{19}$. Gavę 9-ąją liekaną $18 = (-1) + 19$, likusias 9 liekanas galime gauti greičiau pagal $13^{9+i} \equiv (-1) \cdot 13^i \pmod{19}$. Pavyzdžiui, $13^{12} \equiv -13^3 \equiv -12 \equiv 7 \pmod{19}$. Jų galime ir nerašyti: svarbu, kad iš penktosios liekanos 14 ir tik iš jos gauname $(5 + 9)$-ąją liekaną $19 - 14 = 5$. Vadinasi, yra lygiai viena tinkama n reikšmė: $13^n \equiv 5 \pmod{19}$, kai $n = 14$.

Atsakymas. Pirmoji lygtis sveikųjų sprendinių neturi; antroji turi, tinka $n = 2, 5, 8, 11, 14, 17$; trečioji turi, tinka $n = 14$.

Pabaigai paminėsime, kad skaičių laipsnių prastinimas moduliu m, Oilerio funkcija ir teorema yra svarbūs **RSA kriptosistemoje** – duomenų šifravimo ir iššifravimo sistemoje, kuri plačiai naudojama, užtikrinant saugų duomenų perdavimą internetu. Ji taikoma, pasirinkus tam tikrus parametrus – skaičius, vadinamus raktais. Kai kurie iš jų turi būti labai dideli, kad sistema iš tiesų būtų saugi, t. y. kad užšifruotų duomenų vagis, neturintis visų raktų, nepajėgtų jų iššifruoti. 10 uždavinyje pateiktas RSA kriptosistemos taikymo pavyzdys su (ne bet kaip parinktais) mažais raktais 391, 31, 159.

AŠTUNTOJI UŽDUOTIS

1. Nustatykite: a) kurie du iš 12-os skaičių 19, 19^2, 19^3, ..., 19^{12} dalijasi iš 39 su mažiausiomis liekanomis; b) 13-ąjį mažiausią natūralųjį skaičių x, kuriam $19^{296\,684} + x$ dalijasi iš 39.

2. Nustatykite: a) mažiausią natūralųjį n, kuriam $138\,847^n$ dalijasi iš 49 su liekana 1; b) mažiausią keturženklį natūralųjį skaičių x, kuriam $138\,847^{300\,011^{263\,741^{2\,711}}} - x$ dalijasi iš 49.

3. Nustatykite $16\,353^{2^{601}} + 83^{681^{78}} + 2^{29^{542}}$ dalybos iš 23 liekaną.

4. Apskaičiuokite a) $\varphi(61) + \varphi(63) + \varphi(625) + \varphi(627)$; b) $\varphi(119\,304\,306)$.

5. Nustatykite visas galimas $\varphi(2250m) : \varphi(m)$ reikšmes (čia skaičius m natūralusis).

6. Nustatykite skaičiaus $917^{457} + 13^{42^{57}}$ dalybos iš 100 liekaną (taigi paskutinius du skaitmenis).

7. Nustatykite $11\,173^{97^{83^{457}}} + 2^{457^{83^{97}}}$ dalybos iš 363 liekaną.
Užuomina. Kelis kartus pritaikius Oilerio teoremą, dviejų dėmenų prastinimą galima tęsti naudojantis tokiais lyginiais kaip $283^7 \equiv -53 \pmod{363}$ ir $2^{36} \equiv 97 \pmod{363}$.

8. a) Nustatykite, kurie iš skaičių 7, -38, 187, 3829 yra primityviosios šaknys moduliu 43.
b) Duota, kad $g = 2$ yra primityvioji šaknis moduliu 13. Nustatykite, kurių iš 12 skaičių 2, 2^2, 2^3, ..., 2^{12} eilė moduliu 13 yra 3, o kurių 4. Tuo remdamiesi nustatykite, kurių iš 12 skaičių 1, 2, 3, ..., 12 eilė moduliu 13 yra 3, o kurių 4.

9. Duota, kad 3 yra primityvioji šaknis moduliu 31. Įrodykite, kad viena iš lygčių
$$x^{10} = 31y + 25, \qquad x^7 = 31y + 10, \qquad x^{10} = 31y + 13$$
neturi sveikųjų sprendinių (x, y). Kitoms dviem lygtims nustatykite visas galimas reikšmes $n = 1, 2, 3, ..., 30$, su kuriomis lygtis turi sveikąjį sprendinį $(x, y) = (3^n, y)$.

10. Skaičius $a < 391$ natūralusis ir tarpusavyje pirminis su 391. Padalijus skaičių a^{31} iš 391 su liekana, gauta liekana b – **pranešimo a šifras**. Padalijus skaičių b^{159} iš 391, gauta liekana c. Įrodykite, kad $c = a$, t. y. kad skaičių a, užšifruotą skaičiumi b, nurodytu būdu galima iššifruoti.
Užuomina. Raskite $\varphi(391)$.

Užduoties sprendimus prašome išsiųsti iki **2025 m. kovo 7 d.** mokyklos adresu: Lietuvos jaunųjų matematikų mokykla, Matematinio švietimo centras, VU Matematikos ir informatikos fakultetas, Naugarduko g. 24, LT-03225 Vilnius. Mūsų mokyklos interneto svetainės adresas: https://mif.vu.lt/matematikos-olimpiados/ljmm/

LIETUVOS JAUNŲJŲ MATEMATIKŲ MOKYKLOS TARYBA