LIETUVOS JAUNŲJŲ MATEMATIKŲ MOKYKLA

II. PIRMINIAI IR SUDĖTINIAI SKAIČIAI

(2024–2026)

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

Skaičių dalumas. Visų sveikųjų skaičių aibėje {..., -2, -1, 0, 1, 2, 3, ...} atlikdami sudėties ir daugybos veiksmus, liksime joje: bet kurių dviejų skaičių suma ir sandauga vėl yra sveikieji skaičiai. Šiems veiksmams priešingi yra atimties ir dalybos veiksmai: atimties $a - b$ rezultatas (skirtumas) yra toks vienintelis x, kuriam $a = b + x$, o dalybos $a{:}\,b$ rezultatas (dalmuo) yra toks vienintelis x, kuriam $a = b \cdot x$ (dalmuo neapibrėžtas, kai $b = 0$). Bet kurių sveikųjų skaičių skirtumas vėl yra sveikasis skaičius. Šiuo požiūriu dalyba yra įdomiausia: sveikųjų skaičių a ir $b \neq 0$ dalmuo $a{:}\,b$ tik kartais yra sveikasis skaičius. Kai taip visgi nutinka, t. y. kai lygties $a = b \cdot x$ sprendinys x yra sveikasis (čia $b \neq 0$), tai sakoma, kad a **dalijasi iš** b. Ėmus tirti šį dalumo sąryšį tarp sveikųjų skaičių bei visa, kas su juo susiję, pamažu radosi viena iš didžiųjų matematikos sričių, vadinama **skaičių teorija**.

Jei a dalijasi iš b, tai (sveikasis) skaičius b vadinamas (sveikojo) skaičiaus a **dalikliu**, o skaičius a – skaičiaus b **kartotiniu**. Jei apie bet kokį sveikąjį $b \neq 0$ paklausime, kokie yra jo kartotiniai a, tai atsakymas nebus sudėtingas: tai skaičiai $a = b \cdot x$, kur x yra bet koks sveikasis skaičius. Dviejų tokių kartotinių suma ir skirtumas vėl yra b kartotiniai: $bx_1 \pm bx_2 = b(x_1 \pm x_2)$. Padauginus b kartotinį $b \cdot x$ iš bet kokio sveikojo c, vėl gaunamas b kartotinis $b \cdot (cx)$. Jei turime skaičiaus b kartotinį $a = b \cdot x$, kur b savo ruožtu yra sveikojo skaičiaus c kartotinis $b = c \cdot y$, tai $a = c \cdot (xy)$, taigi a yra c kartotinis. Pagrindėme tokias ***išvadas*** apie sveikuosius skaičius:

1) jei a_1 ir a_2 dalijasi iš $b(\neq 0)$, tai ir $a_1 \pm a_2$ dalijasi iš b;

2) jei a dalijasi iš $b(\neq 0)$, tai ac dalijasi iš b su kiekvienu sveikuoju c;

3) jei a dalijasi iš $b(\neq 0)$, o b dalijasi iš $c(\neq 0)$, tai a dalijasi iš c.

Tiriant skaičių dalumą, šiomis išvadomis paprastai remiamasi nejučia. Pavyzdžiui, pastebėję, jog $n = 11\,768\,100$ dalijasi iš 3 (pagal skaitmenų sumą), neskaičiuodami sumos $s = n + 3 \cdot 2^{100}$ ar sandaugos $p = n \cdot 95$ suvokiame, kad s ir p dalijasi iš 3, o kadangi n dalijasi iš 100, tai n dalijasi ir iš 4, iš 25 bei iš 50 (iš bet kurio skaičiaus 100 daliklio).

Tarkime, kad skaičius b natūralusis (t. y. teigiamas sveikasis). Visi jo teigiami kartotiniai $b \cdot x$ sudaro didėjančią seką b, $2b$, $3b$, ... Kai $b = 2$, tai šią seką gausime, visų natūraliųjų skaičių sekoje 1, 2, 3, ... imdami kas antrą skaičių; kai $b = 3$, tai kas trečią; ir t. t. Jei natūralusis a yra sekoje b, $2b$, $3b$, ..., tai $a = bx$ yra b kartotinis bei dalijasi iš b. Tuo tarpu kai natūralusis a iš b nesidalija, jis yra tarp dviejų gretimų b kartotinių bx ir $b(x + 1)$ (jei $a < b$, tai $x = 0$). Abiem atvejais įmanoma a dalyba iš b **su liekana**: atitinkamas x yra šios dalybos dalmuo, o skaičius $r = a - bx$, parodantis, kiek a yra didesnis už b kartotinį bx, yra šios dalybos liekana. Čia $0 \leq r \leq b - 1$. Pavyzdžiui, skaičius $a = 325$ yra tarp skaičiaus $b = 7$ gretimų kartotinių $7 \cdot 46$ ir $7 \cdot 47$, tad dalijant a iš b su liekana gaunami dalmuo $x = 46$ ir liekana $r = 325 - 7x = 3$. O jei $a = 322 = 7 \cdot 46$, tai gauname $x = 46$ ir $r = 322 - 7x = 0$.

Visi natūraliojo skaičiaus b teigiami kartotiniai b, $2b$, $3b$, ... yra ne mažesni už b. Taigi kiekvieno natūraliojo skaičiaus a visi teigiami dalikliai yra atitinkamai ne didesni už a, t. y. priklauso aibei $\{1, 2, 3, \ldots, a\}$. Lygybė $a = 1 \cdot a$ parodo, kad mažiausias ir didžiausias šios aibės skaičiai visada yra a dalikliai. Jau matėme, kad natūraliojo b teigiamų kartotinių aibė lengvai nusakoma. Tačiau jei iš eilės didėjimo tvarka imsime natūraliąsias a reikšmes ir kiekvienai nustatysime jos teigiamus daliklius, tai gautos daliklių aibės mainysis gana įmantriai:

$\{1\}$, $\{1, 2\}$, $\{1, 3\}$, $\{1, 2, 4\}$, $\{1, 5\}$, $\{1, 2, 3, 6\}$, $\{1, 7\}$, $\{1, 2, 4, 8\}$, $\{1, 3, 9\}$, $\{1, 2, 5, 10\}$, $\{1, 11\}$, $\{1, 2, 3, 4, 6, 12\}$, ...

Tęsiant šią seką, pasitaikys vis didesnių aibių, tačiau niekur nedings ir mažesnės, įskaitant mažiausias galimas – sudarytas tik iš skaičių 1 ir a, kuriuos visada rasime tarp skaičiaus a daliklių. Natūralieji skaičiai a, turintys lygiai du teigiamus daliklius (taigi daliklius 1 ir a), vadinami **pirminiais**. Jie yra labai svarbūs tiek nusakant kitų sveikųjų skaičių daliklius, tiek skaičių teorijoje apskritai. Didėjimo tvarka jie sudaro seką 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, ...

Sudėtiniai skaičiai. Kiekvienas natūralusis nepirminis $a > 1$ turi daugiau nei du teigiamus daliklius, taigi turi daliklį d_1, kuriam $1 < d_1 < a$, ir tuo pačiu daliklį $d_2 = a{:}\,d_1$, kuriam $1 < d_2 < a$. Natūralieji skaičiai, didesni už 1, kurie nėra pirminiai, vadinami **sudėtiniais**. Taigi kiekvienas sudėtinis skaičius yra dviejų mažesnių natūraliųjų skaičių sandauga $d_1 d_2$. Natūraliojo skaičiaus a teigiami dalikliai, nelygūs 1 ir a, vadinami jo **tikriniais dalikliais**. (Kartais tikriniu dalikliu laikomas ir skaičius 1, bet čia laikysimės nurodyto apibrėžimo.)

1 teiginys. Kiekvienas sudėtinis skaičius yra kelių pirminių (nebūtinai skirtingų) skaičių sandauga.

Įrodymas. Tarkime priešingai: kad esama sudėtinių skaičių, kurie nėra pirminių skaičių sandaugos. Sekoje 1, 2, 3, ... pasirinkime patį pirmąjį – mažiausiąjį – iš jų ir pažymėkime a. Tada $a = d_1 d_2$, kur natūralieji skaičiai d_1 ir d_2 yra tarp 1 ir a (neimtinai). Remiantis mūsų prielaida, kiekvienas natūralusis skaičius tarp 1 ir a (neimtinai) yra arba pirminis, arba pirminių skaičių sandauga. Tada ir tokių skaičių d_1 bei d_2 – pirminių skaičių arba jų sandaugų – sandauga $a = d_1 d_2$ yra pirminių skaičių sandauga. Gavome prieštarą, todėl teiginys teisingas. ■

Iš šio teiginio galima išvesti porą ***išvadų***.

1) Kiekvienas sudėtinis skaičius dalijasi iš bent vieno pirminio skaičiaus. Pirminis skaičius visada dalijasi iš savęs paties. ***Vadinasi***, kiekvienas natūralusis skaičius, didesnis už 1, turi pirminį daliklį.

2) Tarkime, kad natūralusis skaičius $n > 1$ sudėtinis. Tada jis yra natūraliųjų $d_1 > 1$ ir $d_2 > 1$ sandauga. Galime laikyti, kad $d_1 \leq d_2$. Skaičius d_1 turi pirminį daliklį $p \leq d_1$. Kadangi $n = d_1 d_2 \geq d_1^2 \geq p^2$, tai $p \leq \sqrt{n}$. ***Vadinasi***,

kiekvienas sudėtinis skaičius n turi pirminį daliklį, ne didesnį už $\sqrt{n}$, o jei natūralusis $n > 1$ tokio daliklio neturi, tai skaičius n pirminis.

1 pavyzdys. Raskime visus pirminius skaičius intervale $[320; 340]$. Intervalo sveikieji skaičiai, kurie baigiasi skaitmeniu 0, 2, 4, 6, 8 arba 5, dalijasi iš 2 arba iš 5, tad yra sudėtiniai. Kiti, kurių skaitmenų suma dalijasi iš 3, patys dalijasi iš 3 ir taip pat yra sudėtiniai (tai skaičiai 321, 327, 333, 339). Lieka skaičiai 323, 329, 331, 337. Jie nesidalija iš 2, 3 arba 5. Kadangi $\sqrt{337} < 19$, tai pakanka tikrinti jų dalumą iš 7, 11, 13 ir 17 (iš pirminių skaičių, mažesnių nei 19, išskyrus 2, 3 ir 5). Jei kuris nors iš likusių intervalo skaičių sudėtinis, tai turės tokį daliklį, o jei neturės, tai jis pirminis. Tikrinant paaiškėja, kad $323 = 17 \cdot 19$ dalijasi iš 17, o $329 = 7 \cdot 47$ iš 7 (sudėtiniai skaičiai). O skaičiai $n = 331$ bei $n = 337$ neturi pirminių daliklių, ne didesnių už $\sqrt{n} < 19$, todėl yra pirminiai.

Atsakymas. 331, 337.

Jei d_1 ir d_2 yra natūralieji skaičiai, didesni už 1, tai skaičius $a = d_1 d_2$ sudėtinis. Juk tada a turi daliklį d_1, kuris ne tik didesnis už 1, bet ir mažesnis už a, nes $d_2 > 1$ (daliklis d_1 tikrinis). Kai skaičius užrašytas reiškiniu, kartais galima tą reiškinį išskaidyti, atliekant algebrinius pertvarkymus, ir taip įrodyti, kad skaičius sudėtinis. **Pavyzdžiui**, $a = 150^{1150} - 11^{132}$ išskaidomas pagal kvadratų skirtumo formulę: natūralusis $a = (150^{575})^2 - (11^{66})^2$ turi daliklį $d_1 = 150^{575} - 11^{66} > 1$, iš kurio padaliję skaičių a gauname $d_2 = 150^{575} + 11^{66} > 1$. Taigi skaičius $a = d_1 d_2$ sudėtinis. Kvadratų skirtumą galima įžvelgti ir skaičiuje $b = 150^{1150} - 121^{131}$, nors šiuo atveju vienas laipsnio rodiklis nelyginis: $b = (150^{575})^2 - (11^{131})^2$ turi (tikrinius) daliklius $150^{575} \pm 11^{131}$. Kvadratų skirtumo formulės naudingai nepritaikysime skaičiui $151^{1151} - 121^{131}$, bet čia to ir nereikia. Šis skaičius sudėtinis, nes tai dviejų nelyginių skaičių skirtumas ir turi tikrinį daliklį 2. Taip pat kvadratų skirtumo formulės nepritaikysime skaičiui $150^{1148} - 11^{133}$, bet čia verta prisiminti bendresnę formulę:

$$a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \cdots + ab^{n-2} + b^{n-1}) \quad \text{(skaičius } n > 1 \text{ natūralusis).}$$

Antruosiuose reiškinio skliaustuose sudėtos visos galimos n sandaugų $a^k b^{n-1-k}$, kur $k = n - 1, n - 2, ..., 1, 0$. Jei čia skaičiai a ir b sveikieji, $a \neq b$, tai sveikasis skaičius $a^n - b^n$ dalijasi iš $a - b$. Tarkime, kad skaičiai a ir b natūralieji, $a > b$. Tada $a^n - b^n = d_1 d_2$, kur $d_1 = a - b \geq 1$ ir $d_2 > 1$. Jei $a - b > 1$, tai skaičius $a^n - b^n$ sudėtinis. Atskiru atveju taip bus, jei $b = 1$ ir $a > 2$. Jei turimoje $a^n - b^n$ formulėje imsime nelyginį n ir vietoj b įrašysime $-b$, tai gausime $a^n + b^n$ formulę, iš kurios išplaukia, kad $a^n + b^n$ dalijasi iš $a + b$ (skaičiai a ir b sveikieji, $a \neq -b$). Jei skaičiai a ir b natūralieji ir bent vienas iš jų didesnis už 1, tai $1 < a + b < a^n + b^n$. Tokiu atveju skaičius $a^n + b^n$ turi tikrinį daliklį $a + b$ bei yra sudėtinis. Pabrėžkime, kad jei laipsnių rodiklis n lyginis, tai $a^n + b^n$ nebūtinai dalijasi iš $a + b$. Pavyzdžiui, $2^2 + 3^2 = 13$ nesidalija iš $2 + 3 = 5$.

2 pavyzdys. Įrodykime, kad natūralieji skaičiai $a_1 = 3514^{9191} - 1665^{4403}$, $a_2 = 3514^{9190} + 1665^{4405}$, $a_3 = = 100 \ldots 001$ (tarp vienetų yra 220 nulių), $a_4 = 2^{129} - 1$, $a_5 = 1222^{1279} - 1$ sudėtiniai. Tam pakanka nurodyti po tikrinį jų daliklį. Skaičius $9191 = 91 \cdot 101 = 7 \cdot 13 \cdot 101$ dalijasi iš skaičių 7, 13, 101. Iš jų dalydami skaičių 4403, aptinkame ir jo dalumą iš 7. Taigi $a_1 = (3514^{1313})^7 - (1665^{629})^7$ turi tikrinį daliklį $d_1 = 3514^{1313} - 1665^{629}$. Lengva pastebėti skaičių 9190 ir 4405 bendrą nelyginį daliklį 5 bei tikrinį a_2 daliklį $d_2 = 3514^{1838} + 1665^{881}$. Skaičius $a_3 = 10^{221} + 1 = (10^{13})^{17} + 1^{17}$ turi tikrinį daliklį $d_3 = 10^{13} + 1$, skaičius $a_4 = (2^3)^{43} - 1$ – tikrinį daliklį $d_4 = 2^3 - 1 = 7$, o skaičius $a_5 = 1222^{1279} - 1^{1279}$ – tikrinį daliklį $d_5 = 1222 - 1 = 1221$. ■

Jei išnagrinėtame pavyzdyje turėtume skaičių $2^{1279} - 1$, tai negalėtume gauti jo tikrinio daliklio kaip skaičiui a_5, nes tegautume (netikrinį) daliklį $2 - 1 = 1$. Taip pat negalėtume gauti tikrinio daliklio kaip skaičiui a_4, nes skaičius 1279 pirminis, kitaip nei $129 = 3 \cdot 43$. Skaičiai $M_n = 2^n - 1$, kur skaičius n natūralusis, vadinami **Merseno skaičiais** (prancūzų matematikas Marin Mersenne, 1588–1648). Pavyzdyje matėme, kad Merseno skaičius $a_4 = M_{129}$ sudėtinis. Tuo įsitikinti padėjo pastebėjimas, kad indeksas $n = 129 = 3 \cdot 43$ sudėtinis. Esama ir pirminių Merseno skaičių. Jie gaunami imant pirmines n reikšmes: $M_2 = 3$, $M_3 = 7$, $M_5 = 31$, ... Visgi net su pirminiu n skaičius M_n gali būti sudėtinis, pavyzdžiui, $M_{11} = 23 \cdot 89$. Merseno skaičiai svarbūs, ieškant didelių pirminių skaičių. Šiuo metu (2025 m. pradžioje) didžiausias nustatytas pirminis skaičius yra $M_{136\,279\,841}$, turintis 41 024 320 skaitmenų. Neskaitant jo, šeši didžiausi nustatyti pirminiai skaičiai taip pat yra Merseno skaičiai. Nuo 1952 m., kai buvo nustatyta, kad skaičius M_{521}, turintis 157 skaitmenis, yra pirminis, didžiausias nustatytas pirminis skaičius visada buvo Merseno skaičius, išskyrus pertrauką nuo 1989 iki 1992 metų. Dideli pirminiai skaičiai (nors ir ne patys didžiausieji tarp šiuo metu žinomų) yra svarbūs kriptografijoje – informacijos šifravimo ir iššifravimo moksle, nuo kurio priklauso kibernetinis saugumas.

Toliau mums pravers toks pastebėjimas: jei natūralieji skaičiai a ir b dalijasi iš natūraliojo skaičiaus n atitinkamai su liekana 1 ir su liekana r, tai jų sandauga dalijasi iš n su liekana r. Tai išplaukia iš tapatybės $(nk_1 + 1)(nk_2 + r) = = n(nk_1k_2 + rk_1 + k_2) + r$. Tada dauginant bet kiek natūraliųjų skaičių, kurie dalijasi iš n su liekana 1, gautoji sandauga dalijasi iš n su liekana 1. Pavyzdžiui, skaičius 1667 dalijasi iš 5 su liekana 2, bet galima patikrinti, kad 1667^4 dalijasi iš 5 su liekana 1. Skaičius 1667^{4400} yra kelių (1100-o) skaičių, lygių 1667^4, sandauga, tad taip pat dalijasi iš 5 su liekana 1. Tada 1667^{4401}, 1667^{4402} ir 1667^{4403} dalijasi iš 5 atitinkamai su ta pačia liekana kaip 1667^1, 1667^2 ir 1667^3, taigi su liekana 2, 4 ir 3.

3 pavyzdys. Įrodykime, kad natūralieji skaičiai $a_1 = 3514^{9192} - 1667^{4402}$, $a_2 = 3514^{9191} + 1667^{4401}$ ir $a_3 = 3514^{9192} + 1667^{4402}$ sudėtiniai. Skaičiaus a_1 atveju pakanka pastebėti skaičių 9192 ir 4402 bendrą daliklį 2, o tada – skaičiaus a_1 tikrinį daliklį $3514^{4596} - 1667^{2201}$. Skaičiui a_3 šios idėjos nepritaikysime, nes turime laipsnių sumą, o ne skirtumą, tad laipsnių rodiklių bendras lyginis daliklis 2 netinka. Nelyginio bendro daliklio, didesnio už 1, nei skaičiams 9192 ir 4402, nei (skaičiaus a_2 atveju) skaičiams 9191 ir 4401 nerasime. Todėl šiuo atveju mąstykime

kitaip: tikrinkime skaičių a_2 ir a_3 dalumą iš 2, 3, 5, ... Iš 2 jie nesidalija kaip lyginio ir nelyginio skaičių sumos. Skaičiai 3514 ir 1667^2 dalijasi iš 3 su liekana 1, todėl 3514^{9191} dalijasi iš 3 su liekana 1, o $1667^{4401} = (1667^2)^{2200} \cdot 1667$ su ta pačia liekana 2 kaip skaičius 1667. Pažymėję $3514^{9191} = 3k + 1$, $1667^{4401} = 3l + 2$, gauname, kad $a_2 = (3k + 1) + (3l + 2) = 3(k + l + 1)$ turi tikrinį daliklį 3. Pakartoję šiuos samprotavimus su a_3, norimo rezultato negautume: $a_3 = 3514^{9192} + 1667^{4402} = (3k_1 + 1) + (3l_1 + 1) = 3(k_1 + l_1) + 2$. Skaičiai 3514^2 ir 1667^4 dalijasi iš 5 su liekana 1, todėl $3514^{9192} = (3514^2)^{4596}$ dalijasi iš 5 su liekana 1, o $1667^{4402} = (1667^4)^{1100} \cdot 1667^2$ su ta pačia liekana 4 kaip 1667^2. Pažymėję $3514^{9192} = 5k_2 + 1$, $1667^{4402} = 5l_2 + 4$ gauname, kad $a_3 = (5k_2 + 1) + (5l_2 + 4) = 5(k_2 + l_2 + 1)$ turi tikrinį daliklį 5. ■

Mums pasisekė, kad pavyzdyje dideli skaičiai a_2 ir a_3 turi mažus pirminius daliklius. Bendruoju atveju patikrinimas, ar duotas didelis skaičius yra pirminis, ar sudėtinis, gali būti kur kas ilgesnis, per trumpą laiką neįveikiamas net kompiuteriui. Išnagrinėkime dar porą ypatingų – užrašomų išskaidomais reiškiniais – skaičių.

4 pavyzdys. Įrodykime, kad skaičius c sudėtinis, kai a) $c = 625^{673} + 2^{674}$; b) $c = 2 \cdot 3^{990} + 2 \cdot 3^{661} - 3^{330} - 10$.

a) Pastebėkime, kad $c = a^2 + b^2$, kur $a = 25^{673}$ ir $b = 2^{337}$. Kadangi $2ab = (5^{673})^2 \cdot (2^{169})^2$ yra sveikojo skaičiaus kvadratas, tai pridėję ir atėmę jį iš c, gauname kvadratų skirtumą:
$c = (a^2 + 2ab + b^2) - 2ab = (a + b)^2 - (5^{673} \cdot 2^{169})^2 = (25^{673} + 2^{337} - 5^{673} \cdot 2^{169})(25^{673} + 2^{337} + 5^{673} \cdot 2^{169})$.
Čia pirmasis dauginamasis d_1 mažesnis už antrąjį, bet didesnis už 1, nes $25^{673} > 5^{673} \cdot 2^{169}$. Taigi tai tikrinis c daliklis.

b) Turime $c = f(3^{330})$, kur $f(n) = 2n^3 + 6n^2 - n - 10$. Tikrinant sveikąsias n reikšmes, galima pastebėti, kad daugianaris f turi šaknį -2, t. y. $f(-2) = 0$. Jei bet koks daugianaris $p(x)$ turi šaknį c, tai jis lygus $(x - c)p_1(x)$, kur $p_1(x)$ yra daugianaris. Taigi $f(n)$ turi būti įmanoma išskaidyti taip, kad vienas dauginamasis būtų $n - (-2) = n + 2$. Pamėginkime tai atlikti, dirbtinai reiškinyje sudarydami narius, besidalijančius iš $n + 2$:

$$f(n) = 2n^2(n + 2) - 4n^2 + 6n^2 - n - 10 = 2n^2(n + 2) + 2n^2 - n - 10 =$$
$$= 2n^2(n + 2) + 2n(n + 2) - 4n - n - 10 = (2n^2 + 2n)(n + 2) - 5n - 10 = (2n^2 + 2n - 5)(n + 2).$$

Skaičius c lygus $d_1 d_2$, kur $d_1 = 3^{330} + 2 > 1$, $d_2 = 2 \cdot 3^{660} + 2 \cdot 3^{330} - 5 > 1$, taigi yra sudėtinis.

c) Atsakykime į papildomą klausimą apie $f(n)$ iš b dalies: kokios yra pirminės $|f(n)|$ reikšmės, kai n sveikasis? Pirminio p vieninteliai skaidiniai dviem sveikaisiais dauginamaisiais yra $1 \cdot p = p \cdot 1 = (-1) \cdot (-p) = (-p) \cdot (-1)$. Todėl jei skaičius n sveikasis, o skaičius $|f(n)|$ pirminis, tai $n + 2 = \pm 1$ arba $2n^2 + 2n - 5 = \pm 1$. Tada $n = -1$, -3, $\frac{-1 \pm \sqrt{13}}{2}$, 1 arba -2. Trys n reikšmės -1, -3, 1 tinka. Atitinkamos $|f(n)|$ reikšmės sudaro **atsakymą**: 5, 7, 3. ■

5 pavyzdys. Nustatykime visas pirmines $|f(n)|$ reikšmes, kai n sveikasis, $f(n) = 2n^3 + n^2 - n - 4$. Šiuo atveju daugianaris $f(n)$ sveikųjų šaknų neturi, tad jo neišskaidysime, kitaip nei 4 pavyzdyje. Bet tai ir nebūtina. Pastebėkime, kad skaičius $n^2 - n$ visada lyginis (dviejų lyginių arba nelyginių skaičių skirtumas). Todėl lyginės yra ir visos rūpimos $f(n) = 2(n^3 - 2) + (n^2 - n)$ bei $|f(n)|$ reikšmės. Skaičius $|f(n)|$ turi būti pirminis ir lyginis. Kiekvienas pirminis skaičius p dalijasi tik iš ± 1 ir iš $\pm p$, tad jei p lyginis, t. y. turi daliklį 2, tai $p = 2$. Taigi turime ieškoti sveikųjų n, kuriems $f(n) = \pm 2$. Lengva pastebėti, kad $f(1) = -2$. Taigi $|f(n)|$ įgyja vienintelę pirminę reikšmę 2.

Papildykime uždavinį: raskime visus sveikuosius n, kuriems skaičius $|f(n)|$ pirminis. Tada $f(n) = \pm 2$ ir $2n^3 + n^2 - n = 4 \pm 2$. Kadangi $2n^3 + n^2 - n$ dalijasi iš n, tai iš n dalijasi $4 + 2 = 6$ arba $4 - 2 = 2$. Liko tiesiogiai patikrinti galimybes $n = \pm 1, \pm 2, \pm 3, \pm 6$. Gauname **atsakymą**: $|f(1)| = 2$; $|f(n)|$ nepirminis sveikiesiems $n \neq 1$. ■

Pirminiai ir sudėtiniai skaičiai aritmetinėse progresijose. Prisiminkime: aritmetinė progresija yra tokia seka a, $a + d$, $a + 2d$, …, kurios kiekvienas naujas narys gaunamas, prie paskutinio gauto nario pridėjus duotą skaičių d. Čia nagrinėsime tik begalines aritmetines progresijas, kurioms a ir d yra natūralieji skaičiai.

6 pavyzdys. Nagrinėkime aritmetinę progresiją 3, 7, 11, ..., sudarytą iš visų natūraliųjų skaičių, kurie dalijasi iš 4 su liekana 3. Pirminius skaičius joje sunumeruokime didėjimo tvarka: $q_1 = 3$, $q_2 = 7$, $q_3 = 11$, $q_4 = 19$, ...

a) Nustatykime, ar seka q_1, q_2, ... baigtinė, ar begalinė. Mums pravers du pastebėjimai.

1) Natūralieji skaičiai dalijasi iš 4 su liekana 0, 1, 2 arba 3 bei sudaro atitinkamas progresijas 4, 8, 12, ...; 1, 5, 9, ...; 2, 6, 10, ...; 3, 7, 11, ... Trečiojoje iš jų visi skaičiai turi daliklį 2, todėl visi, išskyrus patį skaičių 2, yra sudėtiniai. Analogiškai pirmojoje progresijoje visi skaičiai sudėtiniai. Taigi kiekvienas pirminis skaičius arba dalijasi iš 4 su liekana 1 arba 3, arba yra lygus 2.

2) Sudauginę bet kiek natūraliųjų skaičių, besidalijančių iš 4 su liekana 1, gausime sandaugą, kuri taip pat dalijasi iš 4 su šia liekana. Taigi pirminių skaičių iš progresijos 1, 5, 9, ... sandauga niekada nesidalija iš 4 su liekana 3.

Dabar tarkime, kad progresijoje 3, 7, 11, ... pirminių skaičių kiekis tėra baigtinis. Nagrinėkime visų šių pirminių skaičių sandaugą $Q = q_1 q_2 q_3 \ldots q_k$. Skaičius $4Q - 1$ nesidalija iš q_k (priešingu atveju dalytųsi $4Q - (4Q - 1) = 1$). Analogiškai $4Q - 1$ nesidalija iš q_1, q_2, ..., q_{k-1}, taip pat iš 2. Kadangi skaičius $4Q - 1 = 4(Q - 1) + 3$ nesidalija iš jokio pirminio skaičiaus, kurio dalybos iš 4 liekana yra 3, nei iš 2, tai šis skaičius pats nėra pirminis ir yra pirminių skaičių iš progresijos 1, 5, 9, ... sandauga. Tačiau tada ši sandauga $4(Q - 1) + 3$ dalijasi iš 4 su liekana 1. Gavome prieštarą. Vadinasi, duotojoje progresijoje yra be galo daug pirminių skaičių q_1, q_2, ...

b) Lengviau yra pagrįsti, kad duotojoje progresijoje yra ir be galo daug sudėtinių skaičių. Iš tiesų, jos nariai gaunami prie pirmojo nario 3 kelis kartus pridedant 4, ir tarp jų galima aptikti be galo daug skaičių $3 + 4 \cdot 3$, $3 + 4 \cdot 6$, $3 + 4 \cdot 9$, …, kurie visi dalijasi iš 3, bet yra didesni už 3, tad yra sudėtiniai. Skaičių liks be galo daug, net jei kiek sustiprinsime sąlygą ir ieškosime progresijos narių, kurie turi daugiau nei 6 teigiamus daliklius. Iš eilės perrinkdami narius, randame skaičių $63 = 3^2 \cdot 7$, kuris turi 6 daliklius 1, 3, 7, 9, 21, 63. Prie jo vis pridėdami 4, gauname be galo daug progresijos narių $63 + 4 \cdot 63k$, kur $k = 1, 2, 3, \ldots$. Jie visi dalijasi iš 63, bet yra didesni už 63,

taigi turi tuos pačius 6 skaičiaus 63 daliklius ir dar bent po vieną teigiamą daliklį (patį skaičių). Vadinasi, progresijoje yra be galo daug narių, kurie turi daugiau nei 6 daliklius. ■

7 pavyzdys. Apie pirminius skaičius aritmetinėje progresijoje dar galima klausti, kiek daugiausiai iš eilės einančių progresijos narių gali būti pirminiai skaičiai. Į šį klausimą atsakykime progresijoms a) 3, 7, 11, ...; b) 1, 31, 61, ...

a) Seka prasideda trimis pirminiais skaičiais 3, 7, 11, po kurių eina sudėtinis skaičius 15. Toliau joje negausime daugiau nei dviejų gretimų pirminių narių, nes sudėtinius narius $3 + 4 \cdot 3$, $3 + 4 \cdot 6$, $3 + 4 \cdot 9$, … turime kas trečioje pozicijoje (skaičiuojant nuo antrojo nario), o tarp bet kurių dviejų tokių pozicijų yra tik po du narius.

b) Progresijoje ketvirtasis narys 91 dalijasi iš 7 (yra sudėtinis). Todėl kas septintas narys, skaičiuojant nuo penktojo, yra sudėtinis: tai skaičiai $91 + 30 \cdot 7k$, kur $k = 1, 2, 3, ...$, besidalijantys iš 7. Tarp tokių narių progresijoje yra po 6 narius, todėl joje negali būti daugiau nei 6 iš eilės einantys pirminiai nariai. Kita vertus, tiesiogiai tikrinant galima aptikti 6 pirminius progresijos narius 541, 571, 601, 631, 661, 691.

Atsakymas. a) 3; b) 6.

6 pavyzdyje radome didėjančią progresiją, kurioje yra be galo daug pirminių skaičių. ***Vadinasi***, pirminių skaičių yra be galo daug. Be to, galima įrodyti (nors ir daug sudėtingiau), kad be galo daug pirminių skaičių yra kiekvienoje aritmetinėje progresijoje a, $a + d$, $a + 2d$, …, kur a ir d yra natūralieji skaičiai, neturintys bendro daliklio, didesnio už 1. Šis teiginys vadinamas **Dirichlė teorema apie aritmetines progresijas** (vokiečių matematikas Gustav Lejeune Dirichlet, 1805–1859). Pavyzdžiui, yra be galo daug pirminių skaičių progresijoje 7, 29, 51, ..., t. y. be galo daug pirminių skaičių, kurie dalijasi iš 22 su liekana 7. Taigi lygtis $p = 22n + 7$ turi be galo daug sprendinių (n, p), kur skaičius n natūralusis, o skaičius p pirminis.

Skaidinys pirminiais daugikliais. Skaidant skaičių dauginamaisiais (net ir pirminį), visada galima prirašyti bet kiek daugiklių, lygių 1. Atmetus ypatingąjį – nei pirminį, nei sudėtinį – daugiklį 1, pirminiai skaičiai tampa neišskaidomi (jų vienintelis skaidinys $p = 1 \cdot p = p \cdot 1$). Taigi pagal 1 teiginį visi sudėtiniai skaičiai daugybos požiūriu sudaryti iš pirminių skaičių, kurie yra lyg nedalomos dalelės, natūraliųjų skaičių atomai. Skaičių teorijoje itin svarbus pastebėjimas, kad, turint du šių atomų rinkinius, iš jų sudaryti skaičiai bus skirtingi, nebent patys rinkiniai sutaptų (galbūt elementų tvarkai juose skiriantis). Tai įrodyti mums padės toks pagalbinis teiginys.

2 teiginys. Tarkime, kad natūraliųjų skaičių sandauga $a \cdot b$ dalijasi iš pirminio skaičiaus p. Tada bent vienas iš dauginamųjų a ir b taip pat dalijasi iš p.

Įrodymas. Įsivaizduokime mechaninį laikrodį su viena rodykle, kurio ciferblatas turi p padalų, iš eilės ratu pažymėtų skaičiais 0, 1, 2, ..., $p - 1$. Tarkime, kad pradinė rodyklės padėtis yra padala 0 ir kad vienu ėjimu leidžiama pasukti rodyklę per a padalų pagal laikrodžio rodyklę. Jei po pirmojo ėjimo rodyklė grįžta į pradinę padėtį, tai posūkis per a padalų yra vienas ar keli posūkiai per p padalų. Tada a dalijasi iš p. Toliau tarkime, kad a nesidalija iš p ir tada po pirmojo ėjimo rodyklė atsiduria ties padala r, kur $r > 0$. Turime įrodyti, kad b dalijasi iš p.

Kartojant ėjimus, rodyklė pradžioje sustoja ties padala $r > 0$, o toliau gali sustoti ir ties kitomis padalomis. Mažiausią teigiamą skaičių, ties kurio padala sustoja taip sukama rodyklė, pažymėkime r_0. Tarkime, kad rodyklė atsiduria ties r_0 po k ėjimų. Tada bet kurie k ėjimų prilygsta rodyklės posūkiui per r_0 padalų. Kartojant tokį posūkį (pradėjus ties 0), po kelių posūkių atliksime pirmą pilną apsisukimą apie ciferblato centrą, pasiekę ir galbūt prašokę 0. Jei rodyklė sustoja tiksliai ties 0, tai p dalijasi iš r_0. Kadangi $0 < r_0 < p$, o skaičius p pirminis, tai $r_0 = 1$. Priešingu atveju rodyklė, prieš prašokdama padalą 0, būtų mažiau nei per r_0 padalų nuo jos, o kitu posūkiu prašokusi ją, atsidurtų ties padala r_1, kur $0 < r_1 < r_0$. Tai prieštarauja mūsų užfiksuoto skaičiaus r_0 minimalumui. Vadinasi, $r_0 = 1$.

Pradžioje atlikus $k \cdot b$ ėjimų, rodyklė pasukama per $a \cdot k \cdot b = kab$ padalų. Čia ab dalijasi iš p, todėl kab dalijasi iš p, o per tiek padalų pasukta rodyklė sustoja ties 0. Kita vertus, k ėjimų prilygsta rodyklės posūkiui per $r_0 = 1$ padalą, todėl atlikus $k \cdot b$ ėjimų rodyklė pasukama per b padalų. Taigi posūkis per b padalų grąžina rodyklę į pradinę padėtį 0 ir prilygsta vienam ar keliems posūkiams per p padalų. Tada b dalijasi iš p – tai ir reikėjo įrodyti. ■

Įrodyme gautas tarpinis rezultatas $r_0 = 1$ reiškia, kad duotas natūralusis a visada turi kartotinį $ka > 0$, kuris dalijasi iš duoto pirminio p su liekana 1. Išspręsime susijusį uždavinį, susišaukiantį su 2 teiginio įrodymo idėjomis.

8 pavyzdys. Intervale $[0; 826]$ raskime natūraliuosius k ir l, kuriems $227k$ dalijasi iš (pirminio) skaičiaus 827 su liekana 1, o $227l$ su liekana 48. Nagrinėkime ciferblatą su 827 padalomis 0, 1, ..., 826 ir viena rodykle, kurios pradinė padėtis yra 0. Po $k_1 = 4$ ėjimų, kai rodyklė sukama per 227 padalas, jos padėtis bus $4 \cdot 227 - 827 = 81$. Po $k_2 = 11$ posūkių per 81 padalą (kiekvienas toks posūkis gaunamas per k_1 ėjimų) rodyklė bus ties $11 \cdot 81 - 827 = 64$. Po $k_3 = 13$ posūkių per 64 padalas ji bus ties $13 \cdot 64 - 827 = 5$; po $k_4 = 166$ posūkių per 5 padalas – ties $166 \cdot 5 - 827 = 3$; pagaliau po $k_5 = 276$ posūkių per 3 padalas – ties $276 \cdot 3 - 827 = 1$. Taigi atliekant ėjimus, kai sukama per 227 padalas, po $k_1k_2k_3k_4k_5 = 26\,206\,752$ ėjimų rodyklė atsidurs ties 1. Kaskart atlikus 827 ėjimus, rodyklė grįžta į pradinę padėtį. Todėl vietoj $26\,206\,752 = 827 \cdot 31\,688 + 776$ pakanka atlikti $k = 776$ ėjimus. Po tiek ėjimų rodyklė atsiduria padėtyje 1, tad padėtį 48 gausime po $776 \cdot 48 = 37\,248 = 827 \cdot 45 + 33$ arba po $l = 33$ ėjimų.

Atsakymas. $k = 776$, $l = 33$.

2 teiginys vadinamas **Euklido lema** (senovės graikų matematikas Euklidas Aleksandrietis, apie 300 m. pr. Kr.). Jis nusako esminę pirminių skaičių savybę, kuri juos išskiria tarp sudėtinių skaičių. Jokiam sudėtiniam skaičiui p šis teiginys negalioja. Pavyzdžiui, jei $p = 6$, tai $12 = 4 \cdot 3$ dalijasi iš p, bet nei $a = 4$, nei $b = 3$ nesidalija. Iš Euklido lemos išplaukia jos ***apibendrinimas***: sudauginus **bet kiek** natūraliųjų skaičių ir jų sandaugai dalijantis iš pirminio skaičiaus p, iš jo turi dalytis bent vienas dauginamasis. Iš to savo ruožtu išplaukia, kad kelių natūraliųjų skaičių, nesidalijančių iš pirminio p, sandauga iš p niekada nesidalija. Jokie du skirtingi pirminiai skaičiai vienas iš kito

nesidalija (pirminio skaičiaus apibrėžimas), tad atskiru atveju gauname tokią ***išvadą***: kelių (nebūtinai skirtingų) pirminių skaičių sandauga nesidalija iš jokių pirminių skaičių, išskyrus sudaugintuosius.

Pavyzdžiui, nedalydami skaičiaus $a = 2 \cdot 2 \cdot 2 \cdot 13 \cdot 41 \cdot 41 = 2^3 \cdot 13 \cdot 41^2$ iš 7 su liekana, ir taip galime būti tikri, kad jis iš 7 nesidalija. Taip pat galime būti tikri, kad a nesidalija iš $91 = 7 \cdot 13$: jei a dalytųsi iš 91, o 91 – iš 7, tai a dalytųsi iš 7. Matome, kad a dalijasi iš 41 ir iš 41^2. Ar jis gali dalytis iš 41^3 ar skaičiaus 41 dar didesnio laipsnio? Jei dalytųsi, tai turėtume $a = 41^3 \cdot b$, kur skaičius b sveikasis. Padaliję šią lygybę iš 41^2, gautume $2^3 \cdot 13 = 41 \cdot b$. Ši lygybė klaidinga, nes jos dešinioji pusė vis dar dalijasi iš pirminio skaičiaus 41, o kairioji (kaip kitokių pirminių skaičių sandauga) nesidalija. Analogiškai įrodoma, kad a dalijasi iš $2^0 (= 1)$, 2^1, 2^2, 2^3, bet ne iš 2^4, 2^5, … ir apskritai kad pirminių skaičių sandauga, kurioje dauginamasis p sutinkamas lygiai n kartų, dalijasi iš p^0, p^1, p^2, …, p^n, bet ne iš p^{n+1}, p^{n+2}, … (įskaitant atvejį $n = 0$). Vadinasi, jei dvi pirminių skaičių sandaugos yra lygios, tai joks pirminis skaičius kaip dauginamasis negali būti sutinkamas vienoje iš jų daugiau kartų nei kitoje (kitaip viena sandauga dalytųsi iš tokio pirminio skaičiaus didesnio laipsnio nei kita). Taigi lygiose pirminių skaičių sandaugose kiekvienas pirminis skaičius kaip dauginamasis pasikartoja po tiek pat kartų. Tai įrodo 3 teiginį.

3 teiginys. Dvi (nebūtinai skirtingų) pirminių skaičių sandaugos yra lygios tada ir tik tada, kai skiriasi nebent dauginamųjų tvarka.

Prisiminkime 1 teiginį: sudėtiniai skaičiai yra pirminių skaičių sandaugos. 3 teiginys nurodo, kad kiekvienam sudėtiniam skaičiui tokia sandauga yra vienintelė dauginamųjų tvarkos tikslumu (t. y. nekreipiant dėmesio į dauginamųjų tvarką). Turint pirminių skaičių sandaugą, visus vienodus pirminius skaičius joje galima sugrupuoti ir užrašyti skaičių laipsniais (pvz., $5 \cdot 5 \cdot 7 \cdot 5 \cdot 2 \cdot 7 = 2 \cdot 5^3 \cdot 7^2$). Tokiu būdu gaunama kiekvieno sudėtinio skaičiaus išraiška skirtingų pirminių skaičių laipsniais – to skaičiaus **skaidinys pirminiais daugikliais** (trumpinsime **SPD**). Dabar galime apjungti 1 ir 3 teiginius bei taip ***performuluoti***: **kiekvienas sudėtinis skaičius turi lygiai vieną skaidinį pirminiais daugikliais dauginamųjų tvarkos tikslumu**. Šis teiginys vadinamas **Pagrindine aritmetikos teorema** (trumpinsime **PAT**). Jo svarbą sunku pervertinti: SPD egzistavimas ir vienatis leidžia efektyviai analizuoti skaičių dalumo savybes ir išspręsti įvairius skaičių teorijos uždavinius.

Nagrinėkime baigtinius pirminių skaičių rinkinius, kuriuose elementai gali kartotis, o elementų tvarka nesvarbi. Iš esmės Pagrindinė aritmetikos teorema nusako abipus vienareikšmį atitikimą tarp natūraliųjų skaičių ir tokių rinkinių. Kiekvieną sudėtinį skaičių a atitinka jo unikalus ir vienintelis rinkinys – keli (daugiau nei vienas) pirminiai skaičiai, kurių sandauga lygi a. Pirminius skaičius atitinka rinkiniai iš vieno skaičiaus, o ypatingąjį skaičių 1 – ypatingasis tuščias rinkinys (turintis 0 elementų). Formaliai galima laikyti, kad pirminiai skaičiai yra pirminių skaičių sandaugos iš vieno dauginamojo, o skaičius 1 – tokia „sandauga“ iš 0 dauginamųjų.

Skaičiaus n SPD bendruoju atveju atrodo taip: $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$. Čia p_1, p_2, ..., p_k – skirtingi pirminiai skaičiai (kurių yra $k \geq 1$), skaičiai a_1, a_2, ..., a_k – natūralieji. Galima neatmesti ir atvejo $k = 1$, $a_1 = 1$: tada skaičius $n = p_1$ yra pirminis, ir jo skaidiniu pirminiais daugikliais laikykime jį patį (formali sandauga iš vieno pirminio dauginamojo). Galime ***pakeisti PAT formuluotę***, išplėsdami skaičių, kuriems teorema teisinga, aibę: po lygiai vieną SPD turi ne tik sudėtiniai, bet apskritai visi natūralieji $n > 1$. Tarkime, kad natūraliojo $n > 1$ SPD yra $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$. Tada visi skaičiai $p_1^{b_1} p_2^{b_2} \dots p_k^{b_k}$, kur kiekvienas b_i yra bet koks sveikasis skaičius tarp 0 ir a_i (imtinai), yra skaičiaus n teigiami dalikliai. Kitų teigiamų daliklių skaičius n neturi (jei turėtų, tai n turėtų ir antrą, kitokį SPD), ir jokios dvi $p_1^{b_1} p_2^{b_2} \dots p_k^{b_k}$ reikšmės nesutampa (jei sutaptų, tai išraiškose nubraukę nereikalingus daugiklius p_i^0, vėlgi gautume dviejų SPD lygybę, prieštaraujančią PAT). Kadangi n teigiamo daliklio $p_1^{b_1} p_2^{b_2} \dots p_k^{b_k}$ išraiškoje kiekvienas rodiklis b_i gali įgyti bet kurią iš $a_i + 1$ reikšmių 0, 1, …, a_i nepriklausomai nuo kitų rodiklių, tai skaičius n turi lygiai $(a_1 + 1)(a_2 + 1) \dots (a_k + 1)$ teigiamų daliklių. Pavyzdžiui, skaičius $2 \cdot 5^3 \cdot 7^2$ turi $(1 + 1)(3 + 1)(2 + 1) = 24$ teigiamus daliklius (ir atitinkamai dar 24 neigiamus).

9 pavyzdys. Tarkime, kad natūraliojo n SPD yra $3^{1000} \cdot p^3$ (čia skaičius $p \neq 3$ pirminis). Įrodykime, kad yra be galo daug p reikšmių, kurioms n visų teigiamų daliklių suma dalijasi iš 13, ir nustatykime 7-ąją mažiausią tokią reikšmę. Skaičiaus n teigiami dalikliai yra skaičiai $3^x \cdot p^y$, kur $x = 0, 1, 2, \dots, 1000$ ir $y = 0, 1, 2, 3$. Kai $y = 0$, gauname daliklius, kurių suma s_0 yra $1 + 3 + 3^2 + \dots + 3^{1000}$. Ją galima apskaičiuoti pagal geometrinės progresijos sumos formulę arba pastebėjus, kad $3s_0 = s_0 - 1 + 3^{1001}$ ir todėl $s_0 = \frac{3^{1001} - 1}{2}$. Sudėję visus daliklius, kuriems $y = 1$, gauname $s_1 = p + 3 \cdot p + 3^2 \cdot p + \dots + 3^{1000} \cdot p = s_0 \cdot p$. Analogiškai gauname likusių daliklių sumas $s_2 = s_0 \cdot p^2$ ir $s_3 = s_0 \cdot p^3$ bei visų teigiamų daliklių sumą

$$s = s_0 + s_1 + s_2 + s_3 = s_0 \cdot (1 + p + p^2 + p^3) = \frac{3^{1001} - 1}{2} \cdot (1 + p + p^2 + p^3).$$

Jei s dalijasi iš pirminio skaičiaus 13, tai bent vienas iš dauginamųjų $1 + p + p^2 + p^3$ ir $s_0 = \frac{3^{1001} - 1}{2}$ dalijasi iš 13 (Euklido lema). Jei skaičius s_0 dalijasi iš 13 (tokiu atveju s dalumas iš 13 nuo p nepriklausytų), tai ir jo kartotinis $2s_0 = 3^{1001} - 1$ dalijasi iš 13, t. y. 3^{1001} dalijasi iš 13 su liekana 1. Tikrindami reikšmes 3, 3^2, 3^3, …, pastebime, kad 3^3 dalijasi iš 13 su liekana 1. Todėl $3^{1001} = (3^3)^{333} \cdot 3^2$ dalijasi iš 13 su liekana 9 (kaip skaičius 3^2). Vadinasi, iš 13 būtinai turi dalytis $1 + p + p^2 + p^3$. Pažymėkime $p = 13k + r$, kur r – atitinkamos dalybos iš 13 liekana. Šią p išraišką įrašę reiškinyje $1 + p + p^2 + p^3$ ir jį atskliautę, gauname $13 \cdot \dots + 1 + r + r^2 + r^3$, kur vietoj daugtaškio yra sveikasis skaičius (priklausantis nuo k ir r). Taigi iš 13 turi dalytis $1 + r + r^2 + r^3$. Patikrinę visas galimas liekanos reikšmes $r = 0, 1, \dots, 12$, gauname: tinka visi pirminiai $p \neq 3$, kurie dalijasi iš 13 su liekana 5, 8 arba 12.

Tinkamų p reikšmių yra be galo daug, nes aritmetinėse progresijose 5, 18, 31, …; 8, 21, 34, …; 12, 25, 38, … yra po be galo daug pirminių skaičių (Dirichlė teorema). Tai ir reikėjo įrodyti. Rašydami didėjimo tvarka trijų progresijų narius (prie 5, 8, 12 vis pridedame po 13) ir pabraukdami tik tuos, kurie yra pirminiai, nustatome 7-ąjį tinkamą p:

5, 8, 12, 18, 21, 25, 31, 34, 38, 44, 47, 51, 57, 60, 64, 70, 73, 77, 83, 86, 90, 96, 99, 103, 109, ...

Atsakymas. $p = 109$.

Pastaba. Pavyzdyje gavome, kad $3^{1000} \cdot p^3$ teigiamų daliklių suma yra skaičiaus 3^{1000} tokių daliklių sumos s_0 ir skaičiaus p^3 tokių daliklių sumos $1 + p + p^2 + p^3$ sandaugai. Šį dėsningumą galima ***apibendrinti***: jei natūraliojo $n > 1$ SPD yra $p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$, tai užrašę kiekvieno laipsnio $p_i^{a_i}$ teigiamų daliklių sumą $1 + p_i + p_i^2 + \dots + p_i^{a_i}$, šias sumas sudauginę ir sandaugą pilnai atskliautę, gausime sandaugų $p_1^{b_1} p_2^{b_2} \dots p_k^{b_k}$ – skaičiaus n visų teigiamų daliklių – sumą. Pavyzdžiui, skaičiui $n = 12\,375 = 3^2 \cdot 5^3 \cdot 11$ sandauga $(1 + 3 + 9)(1 + 5 + 25 + 125)(1 + 11) = 13 \cdot 156 \cdot 12 = 24\,336$ yra skaičiaus n teigiamų daliklių suma, nes trijų sumų sandaugoje visais įmanomais būdais imant po vieną skaičių iš pirmosios, antrosios ir trečiosios sumos, trijų skaičių sandaugos yra visi įmanomi teigiami n dalikliai: $1 \cdot 1 \cdot 1$, $3 \cdot 5^3 \cdot 1$, $3^2 \cdot 5^2 \cdot 11$ ir t. t. Įdomu, kad panašiai galima mąstyti ir apie kai kurias begalines sumas bei sandaugas. Pavyzdžiui, skaičių $\frac{1}{n^2}$, kur $n = 1, 2, 3, \dots$, suma $S = 1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \dots$ gaunama, sudauginant visas įmanomas (geometrinių progresijų) sumas $1 + \frac{1}{p^2} + \frac{1}{p^4} + \frac{1}{p^6} + \dots$, kur skaičius p pirminis. Taigi šių sumų, kurių reikšmės yra $\frac{1}{1-\frac{1}{p^2}} = \frac{p^2}{p^2-1} = \frac{p \cdot p}{(p-1)\cdot(p+1)}$, begalinė sandauga $\frac{2 \cdot 2}{1 \cdot 3} \cdot \frac{3 \cdot 3}{2 \cdot 4} \cdot \frac{5 \cdot 5}{4 \cdot 6} \cdot \frac{7 \cdot 7}{6 \cdot 8} \cdot \frac{11 \cdot 11}{10 \cdot 12} \cdot \dots$ lygi begalinei sumai S. Savo ruožtu yra įrodyta, kad $S = \frac{\pi^2}{6}$, kur $\pi = 3{,}14\dots$ yra garsioji geometrinė konstanta!

ANTROJI UŽDUOTIS

1. Patikrinkite, kad intervale $(2015; 2035)$ trys skaičiai yra pirminiai, o likę 16 sveikųjų skaičių jame yra sudėtiniai.

2. Duota, kad kažkurie du iš skaičių $a_1 = 2^{11\,099} - 1$, $a_2 = 2^{11\,213} - 1$, $a_3 = 2^{11\,213} + 1$, $a_4 = 42^{11\,213} - 1$, $a_5 = 2^{162} + 21^{11\,210}$, $a_6 = 2^{16} + 1$, $a_7 = 2^{80} + 1$ yra pirminiai. Likusiems penkiems skaičiams nustatykite po tikrinį daliklį ir taip įrodykite, kad jie sudėtiniai (dviejų pirminių skaičių nenagrinėkite).

3. Skaičiams $a_1 = 237^{3913} - 10^{817}$, $a_2 = 23^{3913} + 10^{718}$, $a_3 = 81^{815} + 25 \cdot 10^{814}$ nustatykite po tikrinį daliklį ir taip įrodykite, kad jie sudėtiniai. *Užuomina.* Vienam iš skaičių pritaikykite 4 pavyzdžio idėjas.

4. Nustatykite visas galimas pirmines $|f(n)|$ reikšmes, kai skaičius n sveikasis ir $f(n) = n^3 - n^2 - 7n + 3$. *Užuomina.* Atspėkite daugianario $f(n)$ sveikąją šaknį.

5. Skaičius n sveikasis. Nustatykite visas galimas pirmines $|f(n)|$ reikšmes ir visas atitinkamas n reikšmes, kai a) $f(n) = 100 \dots 0729$, čia tarp 1 ir 7 yra $6n - 3$ nulių, $n \geq 1$; b) $f(n) = n^4 + n^3 - 6$.

6. Raskite natūraliuosius k ir l, mažesnius už 929, kuriems $350k$ dalijasi iš (pirminio) skaičiaus 929 su liekana 1, o $350l$ – su liekana 79.

7. Nagrinėkime aritmetinę progresiją 1, 7, 13, ...
a) Įrodykite, kad joje yra be galo daug narių, turinčių daugiau nei 6 teigiamus daliklius.
b) Nustatykite, kiek daugiausiai šioje progresijoje yra iš eilės einančių narių, kurie yra pirminiai skaičiai.

8. Nesinaudodami Dirichlė teorema apie aritmetines progresijas, įrodykite: aritmetinėje progresijoje 5, 11, 17, ... yra be galo daug pirminių skaičių.

9. Natūraliojo skaičiaus n SPD yra $5^{500} \cdot p^2$ (čia skaičius $p \neq 5$ pirminis). Įrodykite, kad yra be galo daug p reikšmių, kurioms skaičiaus n visų teigiamų daliklių suma dalijasi iš 7, ir raskite 9-ąją mažiausią tokią reikšmę.

10. Natūralusis skaičius m vadinamas **tobulu**, jei jo visų teigiamų daliklių, išskyrus patį m, suma $s(m)$ lygi m. Pavyzdžiui, skaičius $m = 28 = 1 + 2 + 4 + 7 + 14$ yra tobulas. Nagrinėkime skaičius $n = 2^a \cdot p$, kur skaičius a natūralusis, o skaičius $p > 2$ pirminis. Nustatykite ketvirtąjį mažiausią tokį skaičių n, kuris yra tobulas. *Užuomina.* Užrašykite $n = 2^a \cdot p$ teigiamų daliklių sumos $s(n) + n$ formulę. Pritaikykite ją atveju, kai n tobulas.

Užduoties sprendimus prašome išsiųsti iki **2025 m. vasario 18 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