Vilius Stakėnas,
Gediminas Stepanauskas

Analizinės skaičių teorijos apžvalga

„Visi, kam tenka užsiimti skaičių teorija, tolydžio užsidega aistra šiai sričiai,“ – kažkada pastebėjo K. Gausas. Tai tiesa. Daug stiprių protų siekė jos gelmės, daug perdėm savimi pasitikėjusių žmonių vilčių sužlugo. Daug sužinota, daug naujų klausimų iškelta.

Šioje apžvalgoje bandome aptarti dalį problemų, kurias įprasta priskirti analizinei skaičių teorijai. Jos uždaviniai natūraliai kyla iš sveikųjų skaičių tarpusavio ryšių, rezultatai neretai irgi formuluojami gan paprastomis formulėmis, tačiau jiems įrodyti pasitelkiama sudėtinga analizinė technika: realaus ir kompleksinio kintamojo funkcijos, diferencijavimo ir integravimo operacijos ir kita. Tačiau tai – jau moderniųjų laikų dvasia. Pirmųjų įžvalgų autoriai galėjo kliautis tik savo mintimis.

Suprantama, jog nieko negalime pasakyti apie tuos (be abejo, labai talentingus!) mąstytojus, kuriems pirmiesiems kilo mintis, jog egzistuoja ne vien tik trys (penki, šeši, ...) akmenys, medžiai ar avys, bet ir skaičius trys (penki, šeši,..). Žinoma, šis atradimas nelaikytinas skaičių teorijos pradžia. Atradėjai neturėjo nei laiko šioms mintims išplėtoti, nei galimybių jas paskelbti. Pirmosios Senovės pasaulio civilizacijos – šumerų, Babilono, Egipto turėjo gan gilių žinių apie skaičius, naudojo jas turtui, nuostoliams, laikui ir kitiems dalykams skaičiuoti bei matuoti, tačiau savo skaičių teoriją kažin ar turėjo.

Užtat ją tikrai turėjo Pitagoras (572–497 m. pr. Kr.), bene pirmasis šaltiniuose minimas žmogus, pradėjęs nuosekliai tirti natūraliųjų skaičių savybes. Pitagoras buvo, kaip įprasta tais veržliais žmonijos intelekto jaunystės laikais, universalas – filosofas, mokslininkas ir politikas. Savo mokiniams jis dar buvo pusdievis, dabartinių mokyklų mokiniams jis – teoremos apie stačiojo trikampio kraštines autorius, paaukojęs dievams už šį atradimą jaučių. Kai kas mano, kad Pitagoras dar buvęs olimpiados kumštynių čempionas, bet čia, matyt, įsismaginus perlenkta. Diogenas Laertietis, parašęs savotišką enciklopedinį žinyną apie Graikijos mąstytojus, nemažai įvairių žinių pateikęs ir apie Pitagorą, aiškiai nurodo, kad tas didvyris buvo kitas Pitagoras.

Mes čia nesame linkę išsamiai dėstyti skaičių teorijos istorijos. Mums knieti kuo greičiau pereiti prie jos problemų, nes Gauso pastebėjimo atžvilgiu nesame išimtis. Skaičių teorija mūsų moderniame pasaulyje žmones jaudina ne mažiau, bet tikrai daugiau, negu bet kada.

• • • $\alpha + \omega$ • • •

Tikrai galėtume sutikti su U. Dadliu (U. Dudley), kuris sako, jog mūsų laikui labiau nei bet kuriam ankstesniam tinka apibūdinimas: „matematikos aukso amžius". Taigi ir skaičių teorijos. Kartais apie skaičių teorijos pasiekimus parašo net didieji sensacijų ištroškę laikraščiai. Tose publikacijose matematikai neretai randa smagaus, tik jiems suprantamo humoro.*

Pirminiai skaičiai ir pagrindinė aritmetikos teorema

Natūraliųjų skaičių dalumas

Kiekvienas natūralusis skaičius a yra vienetų suma

$$a = 1 + 1 + \ldots + 1.$$

Jei a galime gauti sumuodami natūraliuosius skaičius b

$$a = b + b + \ldots + b,$$

tai sakysime, kad a *dalijasi* iš b (arba b dalija a); rašysime $b|a$. Skaičių b vadinsime a *dalikliu*, o a – b *kartotiniu*. Natūralusis skaičius b dalija natūralųjį skaičių a tada ir tik tada, kai egzistuoja c, kad

$$a = bc. \tag{1}$$

Šia lygybe paranku apibrėžti ir sveikųjų skaičių dalumą:

$b|a$ *tada ir tik tada, kai egzistuoja sveikas skaičius* c, *su kuriuo (1) lygybė teisinga.*

Vien tik sveikųjų skaičių dalumo apibrėžimo pakanka šioms dalumo savybėms įrodyti.

Teorema. *Bet kokiems sveikiems skaičiams* a, b, c *teisingi šie teiginiai:*

1) $1|a, \quad a|a$;
2) *jei* $a|b$ *ir* $b|c$ *tai* $a|c$;
3) *jei* $a|b$ *ir* $b|a$ *tai* $a = \pm b$;
4) *jei* $a|b$ *ir* $a|c$ *tai bet kokiems sveikiems* u, v $a|ub + cv$.

Tegu $a > b > 1$ yra du natūralieji skaičiai. Tada neneigiami skaičiaus b kartotiniai

$$0, \ b, \ 2b, \ 3b, \ \ldots$$

sudaro aritmetinę progresiją, nesutampančią su visa natūraliųjų skaičių aibe. Tegul qb yra didžiausias b kartotinis, kuriam $qb \leq a$. Tada skirtumas $r = a - qb$ tenkina nelygybę $0 \leq r < b$. Taigi

$$a = qb + r, \quad 0 \leq r < b. \tag{2}$$

* *American Mathematical Monthly. 1994, January. P.2*

Šios išraiškos egzistavimas ir vienatis konstatuojami vienoje Euklido „Elementų" teoremoje.

Euklido dalybos su liekana teorema. *Bet kokiai natūraliųjų skaičių porai* a, b *egzistuoja vieninteliai* q, r *, tenkinantys (2) sąlygą.*

Pagrindinė aritmetikos teorema

Koks bebūtų natūralusis skaičius a, jis dalijasi iš 1 ir a. Šie dalikliai vadinami *trivialiaisiais*. Yra natūraliųjų skaičių, kurie kitokių daliklių ir neturi. Juos vadinsime pirminiais. Taigi

natūralusis skaičius p *vadinamas pirminiu, jei jis turi tik du skirtingus daliklius:* 1 *ir* p.

Natūralieji skaičiai, turintys bent vieną netrivialųjį daliklį, vadinami *sudėtiniais*. Skaičius 1 ir yra vienas: jis nėra nei pirminis, nei sudėtinis. Iš pirminio skaičiaus apibrėžimo bei dalumo savybių nesunkiai gaunamos tokios išvados:

- *mažiausias netrivialusis sudėtinio skaičiaus daliklis yra pirminis skaičius;*
- •• *bet kuris sudėtinis skaičius* n *turi bent vieną pirminį daliklį* $p \leq \sqrt{n}$;
- ••• *jeigu natūralusis skaičius* n *neturi netrivialiųjų daliklių* $d \leq \sqrt{n}$, *tai jis yra pirminis.*

Šių teiginių įrodymai labai paprasti, tačiau labai „matematiški": parodoma, jog prielaida apie jų klaidingumą veda prie loginės prieštaros. Tikrai, jei mažiausias netrivialusis skaičiaus n daliklis d nebūtų pirminis skaičius, tai jis, kartu ir n, dalytųsi iš r, $1 < r < d$. Bet tada d nebūtų mažiausias n daliklis! Tad pirmoji išvada turi būti teisinga.

Jeigu n yra sudėtinis skaičius, tai egzistuoja netrivialiųjų daliklių pora d_1, d_2, kad $n = d_1 d_2$. Jeigu būtų $d_1, d_2 > \sqrt{n}$, tai gautume $n = d_1 d_2 > n$. Todėl bent vienas iš skaičių d_1, d_2 neviršija $\sqrt{n}$ ir mažiausiam jo netrivialiajam dalikliui teisinga nelygybė $p \leq \sqrt{n}$. Skaičius p yra pirminis ir dalo n, tad antroji išvada teisinga.

Pagaliau tarę, jog trečioji išvada nėra teisinga, gautume, jog antroji nėra teisinga taip pat. Šitaip negali būti, nes visa, kas matematikoje įrodyta – tas jau teisinga visiems laikams!

Trečiąją išvadą pravartu prisiminti, kai tikriname, ar tam tikras skaičius yra pirminis. Pavyzdžiui, norėdami patikrinti, ar skaičius 281 yra pirminis, turime patikrinti tik teiginių

$$2 \not| 281, \quad 3 \not| 281, \quad 5 \not| 281, \quad 7 \not| 281, \quad 11 \not| 281, \quad 13 \not| 281,$$

teisingumą, nes kiti pirminiai skaičiai jau didesni už $\sqrt{281} < 17$.

Jeigu n yra sudėtinis skaičius, tai egzistuoja mažiausias netrivialusis jo daliklis p_1, kuris pagal pirmąją išvadą yra pirminis skaičius. Tada $n = p_1 n_1, n > n_1 > 1$. Jeigu n_1 yra pirminis skaičius, tai gauname sudėtinio skaičiaus n skaidinį dviejų pirminių sandauga. Jeigu n_1 yra sudėtinis, tai, pasirėmę tuo pačiu samprotavimu skaičiui n_1, gausime

$$n = p_1 p_2 n_2, \quad n > n_1 > n_2 > 1, \quad p_1 \leq p_2.$$

••• $\alpha + \omega$ •••

Arba gavome n skaidinį pirminiais, arba procesą galime tęsti. Šiaip ar taip jis turi nutrūkti, nes skaičiai n_i griežtai mažėja. Tad galų gale gausime n išraišką pirminių skaičių sandauga

$$n = p_1 p_2 \cdot \ldots \cdot p_m, \quad p_1 \leq p_2 \leq \ldots \leq p_m.$$

Jeigu n yra pats pirminis, tai $m = 1$. Teiginys apie šio skaidinio egzistavimą ir vienatį vadinamas pagrindine aritmetikos teorema. Tačiau ji reikšminga ne tik natūraliųjų skaičių teorijoje. Jinai – daugelio matematikos teiginių apie įvairios prigimties elementų aibių struktūrą prototipas. Vienoms aibėms įrodoma, kad analogiškas teiginys teisingas, o kitoms – kad taip nėra.

Pagrindinė aritmetikos teorema. *Kiekvienam natūraliajam skaičiui $n > 1$ egzistuoja vienintelis skaidinys pirminių skaičių sandauga*

$$n = p_1 p_2 \cdot \ldots \cdot p_m, \quad p_1 \leq p_2 \leq \ldots \leq p_m. \tag{3}$$

Įrodymas.* Skaidinio egzistavimą jau parodėme. Dabar įrodysime, kad toks skaidinys yra vienintelis.

Tarkime priešingai: ne visi natūralieji skaičiai išskaidomi (3) pirminių skaičių sandauga vieninteliu būdu. Tada egzistuos mažiausias $n > 1$, kuris išskaidomas pirminių skaičių sandauga bent dviem būdais:

$$n = p_1 p_2 \cdot \ldots \cdot p_r = q_1 q_2 \cdot \ldots \cdot q_s; \tag{4}$$

čia p_i, q_j – pirminiai skaičiai, be to, $p_i \neq q_j$, nes priešingu atveju suprastinę abi (4) lygybės puses iš to paties pirminio, gautume dar mažesnį natūralųjį skaičių, kuris išskaidomas pirminių sandauga nevienareikšmiškai. Užrašykime (4) lygybę taip:

$$n = p_1 a = q_1 b,$$

čia $a = p_2 \cdot \ldots \cdot p_r < n$, $b = q_2 \cdot \ldots \cdot q_s < n$. Tarkime $p_1 < q_1$; atvejis $q_1 < p_1$ būtų tiriamas analogiškai. Sudarykime naują skaičių

$$m = n - p_1 b = q_1 b - p_1 b = (q_1 - p_1) b.$$

Kadangi $m < n$, tai m skaidinys pirminiais skaičiais yra vienintelis. Kadangi

$$m = p_1 a - p_1 b = p_1 (a - b),$$

tai į m skaidinį būtinai įeina p_1 . Iš lygybės

$$m = (q_1 - p_1) b = (q_1 - p_1) q_2 \cdot \ldots \cdot q_s$$

---

* *Palyginkite su įrodymu išdėstytu H. Markšaičio straipsnyje „Neapibrėžtinės lygtys: algebrinės skaičių teorijos užuomazga“ (žr. p. 7-17.)*

ir sąlygos $p_1 \neq q_j$ gauname, kad $p_1|q_1 - p_1$, arba $q_1 - p_1 = kp_1$. Tačiau iš šios lygybės išplauktų negalimas dalykas, kad pirminis q_1 dalijasi iš pirminio $p_1, p_1 < q_1$. Todėl prielaida, jog egzistuoja nevienareikšmiškai pirminių sandauga išskaidomi skaičiai, yra neteisinga.

Iš pagrindinės aritmetikos teoremos tesiogiai išplaukia, kad

jeigu p yra pirminis skaičius ir $p|ab$, tai $p|a$ arba $p|b$. *

Skaidinyje (4) tie patys pirminiai gali kartotis. Pakeitę vienodų pirminių sandaugas laipsniais, galėsime (4) skaidinį parašyti taip:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \ldots \cdot p_r^{\alpha_r};$$

čia: p_i yra skirtingi pirminiai skaičiai, o α_i – natūralieji. Ši skaičiaus n išraiška vadinama *kanoniniu skaidiniu*.

Didelių skaičių kanoninio skaidinio ieškojimas (faktorizavimas) – nuo senų laikų mėgiamas matematikų užsiėmimas ir savotiškas „matematinis sportas“. Ypač didelis dėmesys tenka skaičių $2^n \pm 1$ faktorizavimo problemai. Kodėl tokių skaičių? Skaičius 2^n turi labai daug pirminių daugiklių, tikėtina, jog $2^n \pm 1$ jų turės nedaug, o galbūt šis skaičius netgi bus pirminis. Ieškoti pirminio skaičiaus, didesnio už visus žinomus, – čia ir glūdi azartas.

Skaičius

$$F_n = 2^{2^n} + 1, \quad n = 0, 1, \ldots,$$

tyrinėjo P. Ferma (Pierre de Fermat, 1601–1665). Jie ir vadinami Ferma skaičiais. Pastebėjęs, kad skaičiai F_0, F_1, F_2, F_3, F_4 yra pirminiai, jis iškėlė hipotezę, kad skaičius F_n yra pirminis su visais natūraliaisiais n. Kad taip nėra, 1732 metais nustatė L. Oileris (Leonhard Euler, 1707–1783), suradęs skaidinį

$$F_5 = 2^{32} + 1 = 641 \times 6700417.$$

Skaičius F_6 taip pat nėra pirminis; kanoninį skaidinį

$$F_6 = 274177 \times 67280421310721$$

1880 metais surado F. Landri (F. Landry). Šis matematikas visą savo gyvenimą paskyrė skaičių $2^n \pm 1$ tyrimui. Skaičiai F_7, F_8, F_9 taip pat nėra pirminiai. Jų kanoniniai skaidiniai surasti atitinkamai 1970, 1980 ir 1990 metais.

Rekordinių pirminių skaičių medžiotojai paprastai tiria ne Ferma, bet Merseno (Marin Mersenne, 1588–1649) skaičius. Jais vadinami skaičiai

$$M(p) = 2^p - 1;$$

čia p yra pirminis. Merseno skaičiai yra pirminiai, kai

$$p = 2, 3, 5, 7, 13, 17, 19, 31, 61.$$

* *Pastebėkime, jog jau minėtame H. Markšaičio straipsnyje šis teiginys įrodomas anksčiau už pagrindinę aritmetikos teoremą, o pastaroji išplaukia iš jo.*

• • • $\alpha + \omega$ • • •

Amerikos matematikų draugijos susitikime 1903 m. F. Kolė (F. Cole) „perskaitė“ nebylų pranešimą, tačiau susilaukė garsių plojimų. Jis patikrino ant lentos lygybę

$$M(67) = 2^{67} - 1 = 193707721 \times 761838257287,$$

taigi įrodė, jog kitas Merseno skaičius nėra pirminis.

Rekordiniai pirminiai yra Merseno skaičiai. Pirminis skaičius $M(11213)$ buvo 1968 m. rekordas. Jo garbei JAV buvo išleistas pašto ženklas. Kalifornijos studentų L. Nikel (Laura Nickel) ir K. Nolio (Curt Noll) 400 valandų trukę skaičiavimai galingu kompiuteriu 1978 metų lapkričio 18 dieną pasibaigė nauju rekordu: skaičius

$$M(21701) = 2^{21701} - 1$$

yra pirminis. Jis užrašomas 6533 dešimtainiais skaitmenimis. Iš viso žinomi 28 pirminiai Merseno skaičiai (jeigu dabar nerasta daugiau). Dvidešimt aštuntojo pirminio skaičiaus $M(86243)$ atradėjas – D. Slovinskis (D. Slowinski).

Pirminių skaičių dėsniai

Du klasikiniai rezultatai

Pirminiai skaičiai – tai tie elementai, iš kurių sudaryti visi natūralieji skaičiai. Kiek yra pirminių skaičių, ir kaip juos išrinkti? Atsakymus į šiuos klausimus pateikia jau klasikinė graikų matematika.

Euklido teorema. *Pirminių skaičių yra be galo daug.*

Įrodymas. Sakykime, kad pirminių skaičių aibė yra baigtinė, o $p_1, p_2, \ldots, p_r$ yra visi jos elementai. Tada natūralusis skaičius

$$n = p_1 p_2 \ldots p_r + 1$$

yra sudėtinis: didesnis už 1 ir nelygus nė vienam iš pirminių. Bet n nesidalija nei iš p_1, nei iš $p_2, \ldots, p_r$. Priešingu atveju vienetas turėtų dalytis iš bent vieno pirminio skaičiaus. Bet taip nėra! Tada n yra pats pirminis, nes nesidalija iš jokio pirminio skaičiaus. Gautoji prieštara paneigia prielaidą, kad pirminių skaičių aibė yra baigtinė.

Dabar aptarsime pirminių skaičių sekos sudarymo būdą. Metodas buvo žinomas jau graikų matematikui Eratostenui (Eratosthenes, 276–194 m. pr. Kr.). Metodui prigijo Eratosteno rėčio pavadinimas.

Išties idėja labai paprasta ir naudojama ne tik skaičių teorijoje. Tarkime, aibės

$$\mathcal{A} = \{a_1, a_2, \ldots, a_n\}$$

elementai gali turėti savybes $S_1, S_2, \ldots, S_t$. Kaip išskirti tuos aibės $\mathcal{A}$ elementus, kurie neturi nė vienos iš šių savybių? Jeigu aibės $\mathcal{A}$ elementus galime peržiūrėti eilės tvarka, tai elementų, neturinčių nė vienos savybės S_i, poaibį $\mathcal{A}_0$ gausime atlikę šiuos veiksmus:

1) *peržiūrėję* $\mathcal{A}$ *elementus išbraukime tuos, kurie turi savybę* S_1, *o likusių elementų poaibį pažymėkime* $\mathcal{A}_{t-1}$;
2) *peržiūrėję* $\mathcal{A}_{t-1}$ *elementus išbraukime tuos, kurie turi savybę* S_2, *o likusių elementų poaibį pažymėkime* $\mathcal{A}_{t-2}$;

.....

t) *peržiūrėję* $\mathcal{A}_1$ *elementus išbraukime tuos, kurie turi savybę* S_t; *likusių elementų poaibį* $\mathcal{A}_0$ *sudaro tie* $\mathcal{A}$ *elementai, kurie neturi nė vienos savybės* S_i.

Šis algoritmas duoda taip pat formulę $\mathcal{A}_0$ elementų skaičiui reikšti. Susitarkime baigtinės aibės $\mathcal{B}$ elementų skaičių žymėti $|\mathcal{B}|$. Aibės $\mathcal{A}$ elementų, turinčių savybę S_i, poaibį žymėsime $\mathcal{A}(i)$. Analogiškai $\mathcal{A}(i_1,\ldots,i_r)$ reiškia elementų, turinčių visas savybes $S_{i_1},\ldots,S_{i_r}$, poaibį, t. y. $\mathcal{A}(i_1,\ldots,i_r)=\mathcal{A}(i_1)\cap\ldots\cap\mathcal{A}(i_r)$. Atlikdami i-ąjį algoritmo žingsnį, išbraukiame lygiai

$$|\mathcal{A}(i)|-\sum_{1\le i_1<i}|\mathcal{A}(i_1,i)|+\sum_{1\le i_1<i_2<i}|\mathcal{A}(i_1,i_2,i)|-\ldots+(-1)^i|\mathcal{A}(1,2\ldots,i)|$$

elementų; čia į sumą įtraukiami visi tie nariai, kurių indeksai tenkina po sumos ženklu nurodytą nelygybę.

Atlikę visus algoritmo žingsnius, gausime $\mathcal{A}_0$ aibę, kurios elementų skaičius

$$|\mathcal{A}_0|=|\mathcal{A}|-\sum_{1\le i\le t}|\mathcal{A}(i)|+\sum_{1\le i_1<i_2\le t}|\mathcal{A}(i_1,i_2)|-\ldots+(-1)^t|\mathcal{A}(1,2\ldots,t)|.$$

Grįškime prie pirminių skaičių. Jeigu $\mathcal{A}=\{2,3,\ldots,n\}$, $p_1<p_2<\ldots<p_t$ – visi intervalo $[2,\sqrt{n}]$ pirminiai skaičiai, o S_i žymi savybę, kad skaičius dalijasi iš p_i, tai atlikę visus anksčiau aprašyto algoritmo žingsnius, gausime intervalo $(\sqrt{n},n]$ pirminius skaičius. Tai išplaukia iš ankstesnio skyrelio pradžios išvadų. Galime šiek tiek modifikuoti algoritmo aprašymą, kad nereikėtų iš anksto žinoti skaičių p_i, nes jie randami paties proceso metu. Tada gautume visų intervalo $[2,n]$ pirminių skaičių seką.

Eratosteno rėtis – būdas intervalo $[2,n]$ pirminiams skaičiams išrinkti – paprastai aprašomas taip:

1. *Surašykime visus natūraliuosius skaičius nuo 2 iki* n.
2. *Pabraukime skaičių 2, o visus kitus skaičiaus 2 kartotinius išbraukime.*
3. *Tegul* p *yra mažiausias nepabrauktas ir neišbrauktas skaičius. Pabraukime* p, *o visus kitus dar neišbrauktus* p *kartotinius išbraukime.*
4. *Kartokime 3-ąjį žingsnį tol, kol mažiausias nepabrauktas ir neišbrauktas skaičius* p *bus didesnis už* $\sqrt{n}$.
5. *Visi pabrauktieji ir neišbrauktieji skaičiai ir yra visi pirminiai iš skaičių* $2,3,\ldots,n$. *Pabrauktieji yra nedidesni už* $\sqrt{n}$, *o nepabrauktieji – didesni.*

Eratosteno laikais skaičiai būdavo rašomi lentelėse. Atrenkant pirminius skaičius, jų kartotiniai būdavo išduriami. Likdavo skylėta lentelė, primenanti rėtį. Iš čia ir kilęs rėčio pavadinimas.

• • • $\alpha+\omega$ • • •

Štai intervalo $[2, 100]$ pirminių skaičių „išsijojimo“ pavyzdys. Išbrauktųjų (kartotinių) skaičių vietose – žvaigždutės.

	2	3	*	5	*	7	*	*	*
11	*	13	*	15	*	17	*	19	*
*	*	23	*	*	*	*	*	29	*
31	*	*	*	*	*	37	*	*	*
41	*	43	*	*	*	47	*	*	*
*	*	53	*	*	*	*	*	59	*
61	*	*	*	*	*	67	*	*	*
71	*	73	*	*	*	*	*	79	*
*	*	83	*	*	*	*	*	89	*
*	*	*	*	*	*	97	*	*	*

Maža gudrybė palengvina tikrinimo-braukymo procesą. Jeigu skaičius nuo 2 iki n surašysime į 6 stulpelius:

	2	3	4	5	6
7	8	9	10	11	12
.	.	.	.	.	.

tai antrąjį, trečiąjį, ketvirtąjį ir šeštąjį stulpelius galima iš karto išbraukti – juose pirminių skaičių nebus.

Kol nebuvo kompiuterių, pirminių skaičių lentelių sudarymas reikalavo daug laiko, kantrybės ir darbo. 1668 m. anglų matematikas D. Pelis (John Pell, 1620–1685) paskelbė pirminių skaičių, neviršijančių 10^7 lentelę, J. Kulikas (J.P. Kulik, 1773–1863) per 20 metų aštuoniuose tomuose (4212 puslapiai!) surašė visų natūraliųjų skaičių iki 100 330 201 skaidinius pirminiais dauginamaisiais. Taigi jis rado ir visus šio intervalo pirminius skaičius. Dabar pirminių skaičių atrinkimą sėkmingai atlieka kompiuteriai. 1959 metais K. Beikeris ir F. Grunbergeris (C. L. Baker, F. J. Gruenberger) paruošė mikrofilmą, kuriame surašyti visi pirminiai, ne didesni už 104 395 301. Jų yra šeši milijonai. Įspūdingas rezultatas minimas P. Ribenboimo (P. Ribenboim) 1988 ir 1990 m. išleistoje knygoje „Pirminių skaičių rekordai“: yra lygiai

$$1\ 075\ 292\ 778\ 753\ 150$$

pirminių skaičių nedidesnių už $4 \cdot 10^{16}$.

Formulės yra bejėgės

Graikų matematika nežinojo nei formulių, nei funkcijų. Tai – naujųjų laikų matematikos sąvokos. Mums, prie jų įpratusiems, natūralu klausti, ar nėra paprastos vieno kintamojo funkcijos, kurios visos reikšmės būtų pirminiai skaičiai. Paprasčiausios funkcijos, kurias šiuo požiūriu galime tirti, yra daugianariai su sveikaisiais koeficientais:

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0, \quad a_n > 0.$$

• • • $\alpha + \omega$ • • •

Yra tikrai įdomių pavyzdžių. L. Oileris nurodė, jog kvadratinio trinario

$$f(x) = x^2 + x + 41$$

reikšmės, kai $x = 0, 1, \ldots, 39$, yra pirminiai skaičiai. Dar įspūdingesnis yra kvadratinis trinaris

$$f(x) = x^2 - 79x + 1601.$$

Jo reikšmės $f(0), f(1), \ldots, f(79)$ yra pirminiai skaičiai!

Tačiau daugianariai yra pernelyg paprastos funkcijos, kad galėtų reikšti pirminių skaičių sekos narius. Teisingas toks teiginys.

Teorema. *Nėra tokio daugianario su sveikaisiais koeficientais*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0, \quad a_n > 0,$$

kad visos jo reikšmės $f(x)$, kai x yra natūralusis skaičius, būtų pirminiai skaičiai.

Įrodymas. Išties teiginys akivaizdus, jei $a_0 = 0$. Jeigu $a_0 > 1$, tai $f(x)$ nebus pirminis skaičius, kai x dalijasi iš a_0.

Tegu $a_0 = 1$. Kadangi vyriausias daugianario koeficientas a_n yra teigiamas, tai $f(x)$ neaprėžtai didėja, kai x didėja. Tada bus toks natūralusis z, kad $f(z) > 1$. Imkime $x = y + z$ ir įstatykime į $f(x)$ išraišką. Pasirėmę Niutono binomo formule

$$(u+v)^m = \sum_{k=0}^{m} C_m^k u^k v^{m-k}, \quad C_m^k = \frac{m!}{(m-k)!k!},$$

galėsime parašyti

$$f(x) = b_n y^n + b_{n-1} y^{n-1} + \ldots + b_0, \quad b_0 = f(z) > 1;$$

čia visi koeficientai b_i yra sveikieji skaičiai. Jau nustatėme, kad lygybės dešinės pusės reiškinio visos reikšmės negali būti pirminiai skaičiai, kai y dalijasi iš b_0, t. y., kai $x = kb_0 + z$.

Tad vargu, ar bus kada rasta „rimta“ vieno kintamojo funkcija, su kuria galėtume gauti naujus pirminius skaičius. Tačiau yra nelabai rimtų formulių. V. Milsas (W. Mills) 1947 m. paskelbė tokį teiginį:

egzistuoja toks skaičius A, kad bet kokiam natūraliajam n $\left[A^{3^n}\right]$ yra pirminis skaičius.

Čia ir kitur $[u]$ žymime skaičiaus u sveikąją dalį, t. y. mažiausią natūralųjį skaičių k, kuriam $k \leq u$. Milso formulė nėra rimta todėl, jog norėdami gauti naują pirminį skaičių, turime sužinoti daugiau skaičiaus A dešimtainės išraiškos narių po kablelio, o tai galime sužinoti tik suradę naują pirminį skaičių. Ratas užsisklendžia!

Panagrinėkime dar vieną panašaus pobūdžio teiginį. Tarkime $p_1 < p_2 < \ldots$ yra visų pirminių skaičių seka. Sudarykime racionaliųjų skaičių seką

$$\alpha_1 = 0.2, \quad \alpha_2 = 0.203, \quad \alpha_3 = 0.203005, \quad \ldots, \alpha_n, \ldots;$$

• • • $\alpha + \omega$ • • •

čia skaičiaus α_n dešimtainė išraiška gaunama pridedant prie α_{n-1} dešimtainės išraiškos skaičiaus p_n dešimtainės išraiškos skaitmenis, papildytus iš kairės nuliais, kad susidarytų lygiai n skaitmenų. Šis skaičių sekos α_n apibrėžimas būtų korektiškas, jeigu n-ojo pirminio skaičiaus dešimtainėje išraiškoje yra ne daugiau kaip n skaitmenų. Tai savo ruožtu išplaukia iš nelygybės $p_n < 10p_{n-1}, n = 2, 3, \ldots$, kurią gausime kitame skyrelyje.

Taigi sudarėme seką α_n, kuri konverguoja į tam tikrą iracionalųjį skaičių β. Dabar galime suformuluoti teiginį, kuriame nuo β grįžtama prie pirminių skaičių.

Teorema. *Egzistuoja toks realus skaičius β, kad n-asis pirminis skaičius lygus $[10^n\beta_n]$; čia skaičiai β_n apibrėžiami taip:*

$$\beta_1 = \beta, \quad \beta_m = 10^{m-1}\beta_{m-1} - [10^{m-1}\beta_{m-1}].$$

Iš teiginio įrodymo aišku, jog pirminiams skaičiams tirti mūsų pirminių skaičių „generavimo algoritmas“ visai nenaudingas.

Nagrinėjome galimybę pirminius skaičius reikšti formulėmis. Dabar pakeiskime požiūrio tašką: kokiomis funkcijomis galima reikšti dydį $\pi(x)$, lygų intervalo $[2, x]$ pirminių skaičių kiekiui? Jeigu žinotume tikslią $\pi(x)$ išraišką, n-ąjį pirminį skaičių galėtume rasti iš lygties $\pi(p_n) = n$. Jei žinoma apytikslė $\pi(x)$ išraiška, ši lygybė gali nurodyti apytikslę p_n pasirodymo vietą.

Tačiau ir $\pi(x)$ funkcijos elgesys yra sudėtingas. Pirmas faktas, kurį pastebėjo dar XVIII a. matematikai, tyrinėdami Eratosteno rėčiu sudarytas pirminių skaičių lenteles, yra toks:

pirminių skaičių dalis intervale $[2, x]$ nykstamai mažėja, kai x didėja.

Analiziškai šį faktą užrašysime taip:

$$\frac{\pi(x)}{x} \to 0, \qquad x \to \infty.$$

Tačiau koks šio nykimo pobūdis? Keli žmonės teisingai spėjo, kaip mažėja $\pi(x)/x$ didėjant x. A. Ležandras (Adrien Marie Legendre, 1752–1833) 1808 m. spėjo, jog

$$\pi(x) \approx \frac{x}{\ln x - 1.08366}.$$

K. Gausas (Karl Friedrich Gauß, 1777–1855), remdamasis paties sudaryta nedidesnių už 3 milijonus pirminių skaičių lentele, manė, kad

$$\pi(x) \approx \int_2^x \frac{dt}{\ln t}.$$

Tai buvo teisingi spėjimai, tačiau įrodymų teko laukti ilgai.

Funkcijos $\pi(x)$ didėjimo rėžiai

Pirmąjį svarų rezultatą apie funkcijos $\pi(x)$ elgesį 1850 m. paskelbė P. Čebyšovas (Пафнутий Чебышев, 1821–1894).

Teorema. *Egzistuoja konstantos $c_1 > 0.9$ ir $c_2 < 1.11$ su kuriomis teisingos nelygybės*

$$c_1 \frac{x}{\ln x} \leq \pi(x) \leq c_2 \frac{x}{\ln x}, \quad x \geq 30.$$

Šio teiginio pakanka *Bertrano postulatui* (Joseph Lois François Bertrand, 1822–1900) įrodyti:

kiekviename intervale $(n, 2n]$ yra bent vienas pirminis skaičius.

Iš tikrųjų pakanka įsitikinti, kad

$$\pi(2x) - \pi(x) > 0, \quad x \geq 1.$$

Kai $x \leq 30$, teiginį galime tiesiogiai patikrinti. Kai $x > 30$, iš Čebyšovo teoremos gausime

$$\pi(2x) - \pi(x) > c_1 \frac{x}{\ln x} - c_2 \frac{x}{\ln x} > 0.$$

Iš Bertrano postulato išplaukia, jog gretimiems pirminiams p_{n-1} ir p_n teisinga nelygybė $p_n < 2p_{n-1}$.*

Čebyšovo įrodyme svarbus vaidmuo tenka funkcijai

$$\theta(x) = \sum_{p \leq x} \ln p;$$

čia p žymi pirminius skaičius. Šią funkciją lengviau analizuoti negu $\pi(x)$.

Įrodysime paprastesnį Čebyšovo teoremos variantą – nelygybes be konstantų įverčių.

Teorema. *Egzistuoja konstantos c_1 ir c_2, su kuriomis teisingos nelygybės*

$$c_1 \frac{x}{\ln x} \leq \pi(x) \leq c_2 \frac{x}{\ln x}, \quad x \geq 2.$$

Įrodyme remsimės neseniai paskelbto darbo** idėjomis. Pagrindinis mūsų įrodymo instrumentas – ne Čebyšovo funkcija, bet Niutono binomo formulė:

$$(u+v)^m = \sum_{k=0}^{m} C_m^k u^k v^{m-k}, \quad C_m^k = \frac{m(m-1)\dots(m-k+1)}{1 \cdot 2 \cdot \dots \cdot k}.$$

---

* *Taigi, nelygybė $p_n < 10p_{n-1}$, kuria pasinaudojome ankstesniame skyrelyje, taip pat teisinga.*

** *Nair M. A new method in elementary prime number theory // J. London Math. Soc., 1982, 2, P. 385–391.*

Pasinaudosime keliomis paprastomis binominių koeficientų C_m^k savybėmis. Visų pirma pastebėsime, kad

$$C_m^{k+1} = C_m^k \frac{n-k}{k+1}.$$

Iš šios paprastos lygybės išplaukia, kad didėjant k dydžiai C_m^k iš pradžių didėja, o po to pradeda mažėti:

$$C_m^{k+1} \geq C_m^k \quad (0 \leq k \leq (n-1)/2) \text{ ir } C_m^{k+1} \leq C_m^k \quad ((n-1)/2 \leq k \leq n).$$

Pasirėmę šiomis nelygybėmis, gauname: jei $m = 2l$, tai didžiausias binominis koeficientas yra C_{2l}^l; jei $m = 2l+1$, tai yra du didžiausieji binominiai koeficientai – $C_{2l+1}^l = C_{2l+1}^{l+1}$. Įvertinsime šiuos didžiausius binominius koeficientus:

$$(1+1)^{2l+1} = \sum_{k=0}^{2l+1} C_{2l+1}^k > C_{2l+1}^l + C_{2l+1}^{l+1}, \quad (1+1)^{2l} = \sum_{k=0}^{2l} C_{2l}^k > C_{2l}^l,$$

$$(1+1)^{2l} = \sum_{k=0}^{2l} C_{2l}^k < (2l+1)C_{2l}^l.$$

Taigi gauname

$$C_{2l+1}^l, C_{2l+1}^{l+1} < 2^{2l}, \quad C_{2l}^l < 2^{2l}, \quad 2^{2l} < (2l+1)C_{2l}^l. \tag{5}$$

Dar pastebėkime, kad visi pirminiai skaičiai $l+1 < p \leq 2l+1$ dalija reiškinio

$$C_{2l+1}^l = \frac{(2l+1)\cdot\ldots\cdot(l+2)}{l!} < 2^{2l}$$

skaitiklį, tačiau nedalija vardiklio. Todėl

$$\prod_{l+1<p\leq 2l+1} p | C_{2l+1}^l, \quad \text{ir} \quad \prod_{l+1<p\leq 2l+1} p \leq 2^{2l}. \tag{6}$$

Apibrėšime dvi skaičių sekas r_n ir d_n: r_n yra visų pirminių skaičių $1 < p \leq n$ sandauga, o d_n – bendrasis mažiausias skaičių $1, 2, \ldots, n$ kartotinis. Taigi

$$r_n = 2\cdot\ldots\cdot p_N, \quad d_n = 2^{\alpha_1}\cdot\ldots\cdot p_N^{\alpha_N}, \quad N = \pi(n); \tag{7}$$

čia: p_k žymime k-ąjį pirminį skaičių, $\alpha_k \geq 1$ – atitinkamą natūralųjį skaičių. Teorema lengvai išplaukia iš tokio teiginio.

Lema. *Teisingos šios nelygybės*

$$r_n \leq 4^n \quad (n \geq 1); \qquad d_n \geq 2^n \quad (n \geq 7). \tag{8}$$

Lemą įrodysime kiek vėliau, o dabar ja pasirėmę gausime teoremos nelygybes. Iš (7), (8) gauname

$$2^n \leq d_n \leq 2^{\alpha_1}\cdot\ldots\cdot p_N^{\alpha_N} \leq n^{\pi(n)}.$$

• • • $\alpha + \omega$ • • •

Imdami abiejų nelygybės pusių logaritmus, gausime

$$\pi(n) \geq \ln 2 \frac{n}{\ln n}, \quad n \geq 7.$$

Konstantą $\ln 2$ pakeitę pakankamai maža teigiama konstanta c_1, gautume vieną iš teoremos nelygybių.

Dabar fiksuokime kokį nors t, $2 \leq t \leq n$ ir panagrinėkime nelygybes

$$\prod_{t<p\leq n} p < r_n \leq 4^n.$$

Sandaugoje visi pirminiai skaičiai yra didesni už t, taigi

$$t^{\pi(n)-\pi(t)} < 4^n.$$

Vėl imdami abiejų nelygybės pusių logaritmus ir pasirėmę trivialiu įverčiu $\pi(t) < t$, gausime

$$\pi(n) < \pi(t) + \ln 4 \frac{n}{\ln t} < t + \ln 4 \frac{n}{\ln t}.$$

Dabar imkime gautoje nelygybėje $t = n/\ln^2 n$. Pakanka parodyti, kad galime parinkti tokią teigiamą konstantą c_2, kad būtų

$$t + \ln 4 \frac{n}{\ln t} \leq c_2 \frac{n}{\ln n}.$$

Tai nesudėtinga. Taigi teorema teisinga, jeigu teisingos lemos nelygybės.

Tiems, kurie teisingai galvoja, kad matematika be įrodymų tai lyg knygos turinys be pačios knygos puslapių, pateikiame ir lemos įrodymą.

Lemos įrodymas. Matematinės indukcijos metodu įrodysime nelygybę $r_n \leq 4^n$. Akivaizdu, kad ji teisinga, jei $n = 2$. Tarkime ji teisinga su visais $m \leq n-1$, ir įrodykime nelygybę, kai $m = n$. Jei n yra lyginis skaičius, tai $r_n = r_{n-1} < 4^{n-1} < 4^n$, tad nelygybė teisinga. Nagrinėkime nelyginį skaičių $n = 2l+1$. Pasirėmę (6) bei indukcijos prielaida, gausime

$$r_n = r_{l+1} \prod_{l+1<p\leq 2l+1} p < 4^{l+1} 4^l = 4^n.$$

Kiek sudėtingiau įrodyti antrąją lemos nelygybę. Be Niutono binomo formulės, pasinaudosime dar vienu analizės instrumentu – elementariu integralu

$$\int_0^1 (a+bt)^m dt = \frac{(a+b)^{m+1} - a^{m+1}}{(m+1)b}, \quad b \neq 0.$$

Pasinaudoję šia formule $(a = 1, b = y-1)$, gausime

$$\int_0^1 (1-x+xy)^{n-1} dx = \frac{1}{n} \frac{y^n - 1}{y-1} = \frac{1}{n}(1 + y + \ldots + y^{n-1}). \tag{9}$$

• • • $\alpha + \omega$ • • •

Tačiau šį integralą galime integruoti ir kitaip – pirma pritaikę Niutono binomo formulę:

$$\int_0^1 (1-x+xy)^{n-1}dx = \int_0^1 \sum_{m=0}^{n-1} C_{n-1}^m y^m x^m (1-x)^{n-m-1}dx = \sum_{m=0}^{n-1} C_{n-1}^m I(n,m) y^m; \quad (10)$$

čia pažymėjome

$$I(n,m) = \int_0^1 x^m (1-x)^{n-m-1}dx.$$

Sulyginę (9), (10) lygybių koeficientus prie tų pačių y laipsnių gausime

$$\frac{1}{n} = C_{n-1}^m I(n,m), \quad m \le n-1.$$

Po paprastų skaičiavimų gausime

$$I(n,m-1) = \frac{1}{mC_n^m}, \quad m = 1,2,\ldots,n. \quad (11)$$

Dabar panagrinėsime dydį $I(n,m-1)$. Pritaikę Niutono binomo formulę ir po to integruodami, gausime

$$I(n,m-1) = \int_0^1 x^{m-1}(1-x)^{n-m}dx = \sum_{j=0}^{n-m}(-1)^{n-m-j}C_{n-m}^j \int_0^1 x^{n-1-j}dx =$$

$$\sum_{j=0}^{n-m}(-1)^{n-m-j}C_{n-m}^j \frac{1}{n-j} = \frac{s_{m,n}}{d_n}; \quad (12)$$

čia $s_{m,n}$ yra sveikas skaičius. Paskutinę lygybę užrašėme pasirėmę tuo, kad priešpaskutinės sumos dėmenys yra trupmenos, kurių vardikliai dalija d_n. Sulyginę (11) ir (12), gausime

$$\frac{s_{m,n}}{d_n} = \frac{1}{mC_n^m}.$$

Iš čia išplaukia tokia išvada:

$$mC_n^m | d_n, \quad 1 \le m \le n. \quad (13)$$

Pasirėmę (13), gauname

$$nC_{2n}^n | d_{2n}, \quad (n+1)C_{2n+1}^{n+1} = (2n+1)C_{2n}^n | d_{2n+1}.$$

Kadangi n ir $2n+1$ yra tarpusavyje pirminiai skaičiai ir $d_{2n}|d_{2n+1}$, tai

$$n(2n+1)C_{2n}^n | d_{2n+1}, \quad \text{ir} \quad n(2n+1)C_{2n}^n \le d_{2n+1}.$$

Pasinaudosime (5) nelygybe sumažinsime kairiąją gautos nelygybės pusę:

$$n2^{2n} \le d_{2n+1}.$$

• • • $\alpha + \omega$ • • •

Jei $n \geq 2$, tai $d_{2n+1} \geq 2^{2n+1}$, t. y. lemos nelygybė $d_m \geq 2^m$ teisinga nelyginiams $m \geq 5$. Jei $n \geq 4$, tai

$$d_{2n+2} \geq d_{2n+1} \geq n2^{2n} \geq 2^{2n+2},$$

ir nelygybė $d_m \geq 2^m$ teisinga visiems lyginiams $m \geq 10$. Nelygybę, kai $m = 8$, galime tiesiogiai patikrinti. Lema įrodyta.

Nauja senos dramos veikėja

Tai – dzeta funkcija $\zeta(s)$. Ji pirmąsyk pasirodė L. Oilerio (Leonhard Euler, 1707–1783) darbuose:

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}. \tag{14}$$

Begalinės sumos reikšmė yra baigtinė, jei $s > 1$ ir begalinė, jei $s = 1$.

Ryšys su mūsų „drama“ – pirminių skaičių aibės tyrimu – atrodo neįžvelgiamas. Išties jam atskleisti prireiktų gana subtilios analizinės technikos. Pabandysime tik įteigti skaitytojui šio ryšio nuojautą, aukodami, deja, formalų matematinį griežtumą.

Naudodamas ζ funkciją, L. Oileris įrodė, kad pirminių skaičių yra be galo daug. Rezultatas, žinoma, nėra naujas, tačiau visiškai naujas įrodymo būdas. Dažnai metodas būna svarbesnis už patį rezultatą. Žymėdami p pirminį skaičių ir prisiminę geometrinės progresijos narių sumos formulę, realiajam skaičiui $s > 1$ parašysime

$$1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \ldots = \left(1 - \frac{1}{p^s}\right)^{-1}. \tag{15}$$

Ką gautume formaliai sudauginę dvi tokias lygybes, parašytas dviem skirtingiems pirminiams p_1, p_2 ? Rezultatas būtų šitoks:

$$\sum_{k,l \geq 0} \frac{1}{p_1^{ks} p_2^{ls}} = \left(1 - \frac{1}{p_1^s}\right)^{-1} \left(1 - \frac{1}{p_2^s}\right)^{-1};$$

čia k, l yra sveikieji skaičiai. Kairėje lygybės pusėje gavome dalį (14) sumos dėmenų. Sudauginę (15) lygybes, atitinkančias visus pirminius skaičius, gautume

$$\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}. \tag{16}$$

Pastaroji lygybė vadinama Oilerio sandauga. Jeigu pirminių skaičių aibė būtų baigtinė, tai imdami $s = 1$ dešinėje (16) lygybės pusėje gautume baigtinį skaičių. Tačiau jau minėjome, kad $\zeta(1)$ reikšmė nėra baigtinė. Taigi iš gautos prieštaros išplaukia, kad prielaida, jog pirminių skaičių aibė baigtinė, yra neteisinga. Iš tikrųjų Oilerio metodu galima įrodyti daugiau, nei tvirtinama Euklido teoremoje. Pats L. Oileris įrodė, kad suma

$$\sum_p \frac{1}{p},$$

• • • $\alpha + \omega$ • • •

čia p perbėga visus pirminius skaičius, yra begalinė.

Svarbi naujovė: teiginys apie pirminius skaičius įrodytas, pasinaudojant informacija apie funkcijos $\zeta(s)$ elgesį. Mintis, kad išsamesnė informacija galėtų duoti daugiau žinių apie pirminius skaičius, atrodo labai viliojanti. Išties B. Rymano (Bernhard Riemann, 1826–1866) idėjos atvėrė naujų galimybių šios krypties tyrimams. B. Rymanas pirmasis pradėjo nagrinėti ζ funkciją

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = \prod_{p} \left(1 - \frac{1}{p^s}\right)^{-1}$$

ne tik su realiaisiais, bet ir kompleksiniais s * . Jis susiejo pirminių skaičių pasiskirstymo problemą su ζ funkcijos nulių, t. y. tų skaičių s, kuriems $\zeta(s) = 0$, problema. Tiems, kas teisėtai piktinasi, kai apsiribojama vien bendro pobūdžio pastabomis, pateikiame analizinę šio ryšio formuluotę. Jau minėjome, kad funkcijos $\pi(x)$ elgesys, kai $x \to \infty$, yra glaudžiai susijęs su Čebyšovo funkcijos

$$\psi(x) = \sum_{p \le x} \ln p$$

elgesiu. Pastarąją su ζ funkcija sieja toks ryšys.

Teorema. *Jei x nėra kokio nors pirminio skaičiaus logaritmas, tai*

$$\psi(x) = x - \sum_{\rho} \frac{x^\rho}{\rho} - \frac{\zeta'(0)}{\zeta(0)} - \frac{1}{2}\ln\left(1 - \frac{1}{x^2}\right);$$

čia ρ perbėga visus ζ nulius, kuriems $\operatorname{Re}\rho \ge 0$.

Nustatę, kad nėra ζ funkcijos nulių, kuriems $\operatorname{Re} s = 1$, gautume asimptotikas

$$\psi(x) = x + \varepsilon(x)x, \quad \pi(x) = (1 + \varepsilon(x)) \int_2^x \frac{dt}{\ln t};$$

čia $\varepsilon(x) \to 0$, kai $x \to \infty$. Tai 1896 m. nepriklausomai vienas nuo kito gavo Ž. Adamaras ir Š. Vallė Pussenas (Jacques Hadamard, 1865–1963; Charles Jean de La Vallée Poussin, 1866–1962). Iš tikrųjų nustatyta šiek tiek daugiau: nulių nėra ne tik ant tiesės $\operatorname{Re} s = 1$, bet ir arti jos. Ši informacija įgalino užrašyti pirminių skaičių pasiskirstymo dėsnį tokia forma:

$$\pi(x) = \int_2^x \frac{dt}{\ln t} + \varepsilon(x)x\exp\{-c\sqrt{\ln x}\}, \quad \varepsilon(x) \to 0,\ c > 0,\ x \to \infty.$$

Pats B. Rymanas iškėlė hipotezę, kad visiems ζ funkcijos nuliams, kuriems $\operatorname{Re} s \ge 0$, teisinga $\operatorname{Re} s = 0.5$, t. y. visi dešiniau tiesės $\operatorname{Re} s = 0$ esantys nuliai yra ant vienos tiesės. Jeigu taip iš tikrųjų yra, tai pirminių skaičių pasiskirstymo dėsnį galėtume parašyti taip:

$$\pi(x) = \int_2^x \frac{dt}{\ln t} + \varepsilon(x)\sqrt{x}\ln x;$$

* *Detaliau apie ζ funkciją rašoma J. Kubiliaus straipsnyje „Rymano dzeta funkcija ir jos paslaptys“ (žr. p. 47–54).*

čia $\varepsilon(x)$ aprėžto modulio funkcija.

Šios labai svarbios hipotezės reikšmę ir gilumą matematikai ne iš karto suvokė. Štai ką rašo apie savo matematinių studijų pradžią XX a. pradžioje žymus anglų matematikas Dž. Litlvudas (John Edensor Littlewood, 1885–1977):

„Barnsas iškėlė man naują uždavinį: „įrodyti" Rymano hipotezę. Šis didvyriškas ketinimas vis dėlto neliko visiškai be rezultatų... Aš aptikau ζ funkciją skaitydamas Lindeliofo knygą, bet šioje knygoje visiškai nieko nėra apie pirminius skaičius, tad aš neturėjau nė menkiausio supratimo apie ryšio tarp šių klausimų egzistavimą; man Rymano hipotezė buvo tiesiog reikšminga sveikųjų funkcijų teorijos hipotezė... Net retas kuris iš daug geriau informuotų žmonių girdėjo apie Adamaro darbą, dar mažiau buvo mačiusių Valle-Pusseno darbą belgiškame žurnale...Aš greitai nustačiau, kad jei pagrindinė pirminių skaičių teorema teisinga su $\sqrt{x}$ eilės liekamuoju nariu, tai iš to išplaukia Rymano hipotezė. Reikia atsižvelgti į tai, kad tuo metu niekas iš matematikų neįtarė, kad pirminių skaičių pasiskirstyme slypi kažkokia velniava; taigi $\sqrt{x}$ eilės paklaida atrodė natūrali dėl tos priežasties, kad bet kuris pirminis n daliklis neviršija $\sqrt{n}$. Tad aš ėmiausi darbo su dideliu įkvėpimu ir tikėjimu sėkme, ir tik po kelių savaičių kankynių suvokiau tikrąją padėtį." *

Pridursime, kad Rymano hipotezė neįrodyta iki šiol. Tačiau ir pastangos ją paneigti buvo bergždžios. Skaičiavimai, atlikti pasitelkus kompiuterius, rodo, kad keli milijonai pirmųjų nulių (jei juos išdėstysime modulių didėjimo tvarka), išties yra vienoje tiesėje $\operatorname{Re} s = 0.5$.

Skaičių reiškimo sumomis uždaviniai

Kvadratų sumos ... ir taip toliau

Kiekvieną natūralųjį skaičių galima užrašyti pirminių skaičių sandauga – šį teiginį pavadinome pagrindine aritmetikos teorema. Kiekvienas natūralusis skaičius lygus vienetų sumai – šis trivialus teiginys apie skaičių sandarą nenusipelno, žinoma, atskiro vardo. Tačiau ir apie adicinę, t. y. susijusią su skaičių sudėtimi, skaičių struktūrą galime suformuluoti daug įdomių teiginių.

Bendra forma uždavinį galėtume formuluoti taip. Tegu $\mathcal{A}$ yra kokia nors begalinė sveikų neneigiamų skaičių aibė, $k > 1$ – fiksuotas natūralusis skaičius. Ar bet kokiam natūraliajam n atsiras skaičiai $x_1, \ldots, x_k \in \mathcal{A}$, kad

$$n = x_1 + x_2 + \ldots + x_k? \tag{17}$$

Šio uždavinio istorija siekia (kurgi ne!) Antikos laikus. Jau minėto Diofanto „Aritmetikoje" klausiama, ar (17) lygybė yra teisinga kiekvienam natūraliajam n, jei $k = 2$, $\mathcal{A} = \{0^2, 1^2, 2^2, \ldots\}$, Taigi klausiama: ar kiekvieną natūralųjį skaičių n galima išreikšti dviejų sveikųjų skaičių kvadratų suma

$$n = x^2 + y^2. \tag{18}$$

* *Littlewood J. E. A Mathematicians Miscellany. London, 1957.*

• • • $\alpha + \omega$ • • •

Kodėl domėtasi būtent tokiomis išraiškomis? Aišku, kad tai „geometrinės“ graikų matematikų mąstysenos atgarsis.

Skaičius, kurių šiuo būdu negalima išreikšti, nesunku rasti. Iš tikrųjų bet kokio sveikojo skaičiaus kvadrato dalybos iš 4 liekana yra arba 0, arba 1. Tada dviejų kvadratų sumos dalybos iš 4 liekana negali būti lygi 3. Taigi skaičiams $4k+3$ (18) išraiška neegzistuoja. Visi $4k+3$ pavidalo skaičiai turi savo kanoniniuose skaidiniuose nors vieną pirminį $p = 4t+3$, kuris į skaidinį įeina nelyginiu laipsniu. Tačiau šią savybę turi ne tik skaičiai $4k+3$. Nėra sudėtinga įrodyti, kad visiems tokiems skaičiams (18) išraiška neegzistuoja. Tad į dviejų skaičių kvadratų sumos išraišką gali pretenduoti tik tie skaičiai, į kurių kanoninius skaidinius pirminiai $p = 4k+3$ įeina tik lyginiais laipsniais. Tokius skaičius galima užrašyti taip:

$$n = p_0 p_1 \dots p_s q_1^2 \dots q_t^2; \tag{19}$$

čia: $p_0 = 1$ arba $p_0 = 2$, $p_1, \dots, p_s$ – skirtingi $4k+1$ pavidalo pirminiai skaičiai, $q_1, \dots, q_t$ – bet kokie, nebūtinai skirtingi pirminiai skaičiai. Parodysime, jog skaičiui n (18) išraiška egzistuoja, jeigu ši išraiška egzistuoja pirminiams $p_1, \dots, p_s$. Iš nesunkiai patikrinamos tapatybės

$$(a^2+b^2)(c^2+d^2) = (ac+bd)^2 + (ad-bc)^2$$

išplaukia: jei (18) išraiška egzistuoja skaičiams n_1, n_2, tai ji egzistuoja ir jų sandaugai $n_1 n_2$. Tačiau $2 = 1^2+1^2$, $q^2 = q^2+0^2$. Taigi įrodę, kad kiekvienas pirminis $p = 4t+1$ gali būti išreikštas dviejų kvadratų suma, gautume, kad bet kuris (19) skaičius gali būti išreikštas dviejų kvadratų suma. Aptarėme A. Žiraro (Albert Girard, 1595–1632) teoremos įrodymo kelią.

Teorema. *Skaičių n galima užrašyti dviejų sveikųjų skaičių kvadratų suma tada ir tik tada, jei $4k+3$ pavidalo pirminiai daugikliai į jo kanoninį skaidinį įeina lyginiais laipsniais.*

Taigi yra daug skaičių, kurie negali būti išreikšti dviejų kvadratų suma. K. Gausas 1801 m. įrodė, kad trijų kvadratų taip pat nepakanka.

Teorema. *Skaičių n galima užrašyti sveikųjų skaičių kvadratų suma*

$$n = x^2+y^2+z^2$$

tada ir tik tada, kai $n \neq 4^k(8l+7)$; čia $k, l \geq 0$ yra sveikieji skaičiai.

Tačiau keturių kvadratų jau pakanka. Tai 1770 m. įrodė J. Lagranžas (Joseph Louis Lagrange, 1736–1813).

Teorema. *Bet kokiam natūraliajam n atsiras sveikieji skaičiai x, y, z, w, kad*

$$n = x^2+y^2+z^2+w^2. \tag{20}$$

• • • $\alpha + \omega$ • • •

Panašiai kaip dviejų kvadratų atveju iš tapatybės

$$(x^2+y^2+z^2+w^2)(x'^2+y'^2+z'^2+w'^2)=X^2+Y^2+Z^2+W^2,$$

$$X=xx'+yy'+zz'+ww',\ Y=xy'-yx'+wz'-zw',$$

$$Z=xz'-zx'+yw'-wy',\ W=xw'-wx'+zy'-yz',$$

išplaukia: jeigu skaičiai n_1, n_2 gali būti išreikšti keturių kvadratų suma, tai jų sandauga n_1n_2 – taip pat. Todėl įrodinėjant teoremą pakanka nagrinėti atvejį, kai n (20) lygybėje – nelyginis pirminis skaičius.

Na, o kas gi trukdo nagrinėti kubų, bikvadratų ir aukštesniųjų laipsnių sumas? Hipotezę apie tokias sumas 1770 m. suformulavo anglų matematikas E. Varingas (Edward Waring, 1734–1798):

kiekvienam natūraliajam k egzistuoja skaičius r, kad kiekvienam natūraliajam n atsiras sveikieji neneigiami skaičiai $x_1,\ldots,x_r$, kad

$$n=x_1^k+x_2^k+\ldots+x_r^k. \tag{21}$$

Jeigu natūraliajam k Varingo hipotezė teisinga, tai skaičių r aibė netuščia. Pažymėkime $g(k)$ mažiausiąjį jos elementą. Taigi visiems n egzistuoja (21) išraiška, jei $r=g(k)$, tačiau taip nėra, jei $r=g(k)-1$. Jau matėme, kad $g(2)=4$. E. Varingas taip pat spėjo, kad $g(3)=9$, $g(4)=19$. Varingo hipotezė „kybojo“ beveik 150 metų. 1909 m. vokiečių matematikui D. Hilbertui (David Hilbert, 1862–1943) pavyko ją įrodyti: skaičius $g(k)$ iš tiesų egzistuoja kiekvienam natūraliajam k. Hilberto įrodymas buvo labai sudėtingas. Žymus prancūzų matematikas A. Puankarė (Jules Henri Poincaré, 1854–1912) pareiškė: „Jeigu kada nors bus suprasta, kur glūdi šio įrodymo spyruoklės, didelės reikšmės aritmetiniai rezultatai pasipils, tikriausiai, kaip iš gausybės rago.“ Hilberto darbe nėra jokių žinių apie dydžių $g(k)$ reikšmes, jame tik įrodyta, kad šie dydžiai egzistuoja. Tais pačiais 1909 .m. įrodytas Varingo spėjimas $g(3)=9$, tačiau lygybė $g(4)=19$ įrodyta tik 1986 m.

Reikšmingi aritmetiniai rezultatai, susiję su Varingo problema, iš tikrųjų pasipylė, tačiau ne todėl (kaip tikėjosi A. Puankarė), kad buvo suprastas Hilberto įrodymas. 1920 m. G. Hardis ir J. Litlevudas (Godfrey Harold Hardy 1877–1947, John Edensor Littlewood, 1885–1977) paskelbė naują Varingo hipotezės įrodymą. Naujasis metodas pasirodė esąs labai efektyvus – ir ne tik sprendžiant Varingo problemą.

Tegu $k\geq 1$ yra natūralusis skaičius. Kompleksiniams skaičiams $|z|<1$ apibrėžkime funkciją

$$f(z)=1+z^{1^k}+z^{2^k}+\ldots++z^{m^k}+\ldots. \tag{22}$$

Formaliai sudauginę s (22) vienodų begalinių sumų, gausime

$$(f(z))^s=\sum_{n=0}^{\infty}r(n)z^n. \tag{23}$$

Koeficientas $r(n)$ lygus skirtingų išraiškų

$$n=x_1^k+x_2^k+\ldots+x_s^k$$

• • • $\alpha+\omega$ • • •

skaičiui. Varingo hipotezę įrodysime, jeigu įrodysime, kad egzistuoja toks natūralusis s, kad visi koeficientai $r(n)$ (23) lygybėje yra teigiami. Šiuos koeficientus galima išreikšti pasinaudojus kompleksiniais integralais

$$r(n) = \frac{1}{2\pi i} \int_C \frac{(f(z))^s}{z^{n+1}} dz;$$

čia C žymi apskritimą, kurį sudaro kompleksiniai skaičiai $z, |z| = \rho, \rho < 1$. Parašyti šį integralą – anoks nuopelnas, nes tirti jį sudėtinga. G. Hardis ir J. Litlevudas sugalvojo, kaip tai galima daryti. Čia ir glūdi naujojo metodo esmė. Jis „permeta“ Varingo hipotezę iš skaičių teorijos į kompleksinio kintamojo funkcijų sritį. *

Naudojantis šiuo metodu dydžio $g(k)$ problema irgi beveik išspręsta. Natūraliesiems $4 \leq k \leq 200.000$ teisinga lygybė

$$g(k) = 2^k + \left[\left(\frac{3}{2}\right)^k\right] - 2; \tag{24}$$

čia $[a]$ žymi skaičiaus a sveikąją dalį. Jei $k > 200.000$, tai (24) gali būti neteisinga tik baigtiniam k reikšmių skaičiui.

Pirminių skaičių sumos

Kryžiuočių ainis iš Karaliaučiaus bei Peterburgo mokslų akademijos narys Ch. Goldbachas (Christian Goldbach, 1690–1764) 1742 metų birželio mėnesį parašė laišką L. Oileriui (vieną iš 95 jam parašytų laiškų), kuriame iškėlė vieną hipotezę apie pirminius skaičius. Nors ši hipotezė aptinkama ir kitų to meto matematikų raštuose, tačiau dėl Ch. Goldbacho ir L. Oilerio susirašinėjimo ji patraukė matematikų dėmesį. Dabar įprasta ją vadinti Goldbacho hipoteze ir formuluoti taip:

bet kokį didesnį už 2 lyginį skaičių galima užrašyti dviejų pirminių skaičių suma.

Pastebėkime, kad remdamiesi Goldbacho hipoteze galime suformuluoti ir hipotezę apie nelyginių skaičių reiškimą pirminių skaičių suma. Jei nelyginis skaičius $2n+1$ yra nemažesnis už 7, tai $2n-2 \geq 4$. Jei Goldbacho hipotezė yra teisinga, tai egzistuoja du pirminiai p_1, p_2, kuriems $2n-2 = p_1 + p_2$. Tačiau tada $2n+1 = 3 + p_1 + p_2$. Vadinasi,

nelyginius, didesnius už 7 skaičius galima užrašyti trijų pirminių skaičių suma.

Goldbacho problema pasirodė esanti dar sudėtingesnė ir už Varingo problemą. Ilgą laiką net nebuvo aišku, kaip pradėti ją spręsti. Apsiribota vien jos tikrinimu nedideliems lyginiams skaičiams. G. Kantoras (Georg Cantor, 1845–1918) 1894 m. nustatė Goldbacho hipotezės teisingumą visiems lyginiams $n \leq 1000$. Net ir po Hilberto darbo, kuriame išspręsta Varingo problema, žymus skaičių teoretikas E. Landau (Edmund Georg Landau, 1877–1938) 1912 m. manė, kad Goldbacho hipotezė viršija tuometinės matematikos galimybes.

---

* *Sunku susilaikyti nepacitavus Ž. Adamaro: „Trumpiausias kelias tarp dviejų realiosios srities faktų eina per kompleksinę sritį.“*

Tačiau jau aptartas Hardžio ir Litlvudo metodas davė impulsą ir šiai problemai spręsti. Formaliai žiūrint, kelias tas pats: jei

$$F(z) = z^2 + z^3 + \ldots + z^p + \ldots$$

(čia $|z| < 1$ – kompleksinis, p – pirminis skaičius), tai $R_s(n)$ lygybėje

$$F^s(z) = \sum_{n=1}^{\infty} R_s(n) z^n$$

yra skaičiaus n skirtingų išraiškų $n = p_1 + \ldots + p_s$ (p_i – pirminiai skaičiai) kiekis. Tad Goldbacho hipotezei įrodyti pakanka nustatyti, kad koeficientai $R_2(n)$ yra teigiami visiems lyginiams $n > 4$. Juos, kaip ir Varingo problemos dydžius, galima tirti naudojantis integralu

$$R_s(n) = \frac{1}{2\pi i} \int_C \frac{F^s(z)}{z^{n+1}} dz. \tag{25}$$

Hardžiui ir Litlvudui pavyko įrodyti, kad Goldbacho hipotezė yra teisinga, jeigu teisinga (sustiprinta) Rymano hipotezė. Tačiau daugiausia pavyko pasiekti rusų matematikui I. Vinogradovui (Иван Матвеевич Виноградов, 1891–1983). Jis modifikavo Hardžio ir Litlvudo metodą, sugalvojęs, kaip (25) lygybėje begalines sumas $F(z)$ galima pakeisti specialiomis baigtinėmis trigonometrinėmis sumomis. Tad 1937 m. pasinaudojęs šiais patobulinimais jis beveik išsprendė vadinamąją trinarę Goldbacho problemą.

Teorema. *(I. Vinogradovas) Egzistuoja tokia konstanta n_0, kad bet kurį nelyginį skaičių $n, n > n_0$, galima išreikšti trijų pirminių skaičių suma.*

Goldbacho hipotezė apie lyginio skaičiaus reiškimą pirminių skaičių suma (dvinarė Goldbacho problema) neįrodyta iki šiol. Paminėsime du su ja susijusius rezultatus. 1966 m. J. Čenas (J. Chen) įrodė tokį teiginį.

Teorema. *Egzistuoja tokia konstanta n_0, kad bet kurį lyginį skaičių $n, n > n_0$, galima išreikšti suma*

$$n = p + P_2;$$

čia: p yra pirminis skaičius, o P_2 – arba pirminis, arba dviejų pirminių sandauga.

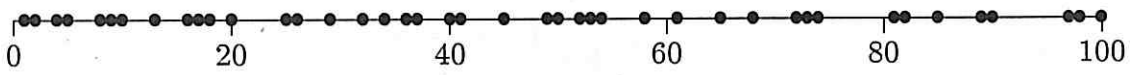
Taip pat žinoma, kad jei ir egzistuoja lyginiai skaičiai, kuriems dvinarė Goldbacho hipotezė nėra teisinga, tai jų negali būti daug. Jei $E(x)$ yra šių skaičių, neviršijančių x, kiekis, tai egzistuoja teigiamos konstantos c, a, kad

$$E(x) \leq c \frac{x}{\ln^a x}, \quad x \geq 4.$$

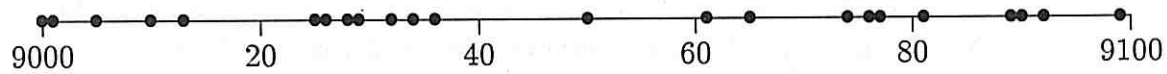
Aritmetinės funkcijos

Įnoringos iš prigimties

Daugelį skaičiaus savybių lemia jo kanoninio skaidinio forma. Pavyzdžiui, skaičių n galima užrašyti dviejų kvadratų suma tada ir tik tada, kai į jo kanoninį skaidinį $4k+3$ pavidalo pirminiai skaičiai įeina tik lyginiu laipsniu. Mums įprasta natūraliuosius skaičius įsivaizduoti kaip sutvarkytą didėjimo tvarka aibę, tad norėtųsi tikėtis, kad ir aritmetinės skaičių savybės „paklūsta“ šiai tvarkai, t. y. jas turintys skaičiai išsidėstę skaičių tiesėje dėsningai. Tačiau nesudėtingi tyrimai sugriauna viltį, kad aritmetinės skaičių savybės gerai „suderintos“ su skaičių tvarka. Panagrinėkime, pavyzdžiui, skaičius, kuriuos galima išreikšti dviejų sveikųjų skaičių kvadratų suma. Žymėdami juos skaičių tiesėje ženklu •, gausime tokį vaizdą:

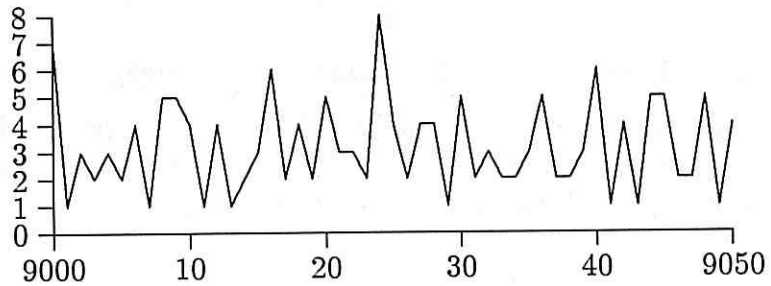


Galbūt tvarka išryškėja toliau, t. y. dideliems skaičiams? Ištyrę palyginti didelių skaičių šimtinę, gausime tokią schemą:



Vienintelė išvada, kurią galbūt galime padaryti palyginę abu brėžinius tėra tokia: didelių skaičių intervaluose natūralieji skaičiai, kuriuos galima išreikšti dviejų kvadratų suma, pasitaiko rečiau.

Panagrinėkime, kaip kinta pirminių daugiklių skaičiaus kanoniniame skaidinyje kiekis, kai tiriamuosius skaičius imame vieną po kito didėjimo tvarka. Tegu $\Omega(n)$ žymi pirminių skaičių kanoniniame n skaidinyje kiekį. Plokštumos koordinačių sistemoje atidėję taškus $\langle n, \Omega(n)\rangle$ bei sujungę juos atkarpomis, gausime itin keistą laužtę:



Brėžinys veikiau atgraso nei skatina ieškoti kokio nors dėsningumo. Tačiau vieną taisyklę visai nesudėtinga įžvelgti: kokie bebūtų natūralieji m, n, visada teisinga lygybė

$$\Omega(mn) = \Omega(m) + \Omega(n).$$

• • • $\alpha + \omega$ • • •

Ši taisyklė nebegalios dydžiui $\omega(n)$, kuris reiškia skirtingų pirminių daliklių kanoniniame n skaidinyje kiekį. Bet jeigu m, n yra tarpusavyje pirminiai natūralieji skaičiai, tai lygybė

$$\omega(mn) = \omega(m) + \omega(n)$$

vėlgi teisinga. Ši savybė būdinga daugeliui skaičių teorijoje pasitaikančių sekų $f(n)$, paprastai vadinamų aritmetinėmis funkcijomis. Jeigu aritmetinė funkcija $f(n)$ yra tokia, kad visiems natūraliesiems tarpusavyje pirminiams m, n teisinga lygybė

$$f(mn) = f(m) + f(n), \tag{26}$$

tai $f(n)$ vadinama adityviąja funkcija, jeigu ji teisinga visiems, ne tik tarpusavyje pirminiams m, n – visiškai adityviąja funkcija. Taigi $\omega(n), \Omega(n)$ – du adityviųjų funkcijų pavyzdžiai.

Tiesiog neįmanoma neapibrėžti tokių aritmetinių funkcijų, kurioms galiotų lygybė (26) su daugybos ženklu vietoje sudėties. Aritmetinę funkciją $g(n) \not\equiv 0$, visiems natūraliesiems tarpusavyje pirminiams m, n tenkinančią lygybę

$$g(mn) = g(m) \cdot g(n),$$

vadinsime multiplikatyviąja funkcija; jeigu lygybė teisinga visiems, ne tik tarpusavyje pirminiams m, n – visiškai multiplikatyviąja funkcija.

Pavyzdžių irgi toli ieškoti nereikia. Tegu $d(n)$ yra skaičiaus n skirtingų daliklių skaičius. Jeigu m, n yra du tarpusavyje pirminiai natūralieji skaičiai, tai kiekvieną sandaugos mn daliklį d vieninteliu būdu galime išskaidyti į sandaugą $d = d_1 d_2$, kad d_1 dalytų m, o d_2 – n. Tad skaičius mn turi tiek skirtingų daliklių, kiek yra skirtingų porų d_1, d_2. Todėl

$$d(mn) = d(m)d(n),$$

ir $d(n)$ yra multiplikatyvioji funkcija.

Grįžkime prie skaičių reiškimo dviejų kvadratų sumomis. Žymėkime $r(n)$ skaičiaus n skirtingų išraiškų

$$n = x^2 + y^2, \quad x \geq 0, y > 0,$$

kiekį; čia x, y, žinoma, – sveikieji skaičiai. Tada $r(n)$ yra aritmetinė funkcija; iš tikrųjų ji yra multiplikatyvioji funkcija.

Adityviosios ar multiplikatyviosios funkcijos reikšmę natūraliajam n visiškai apibrėžia n kanoninis skaidinys. Tiksliau, jei $f(n)$ yra adityvioji, o $g(n)$ multiplikatyvioji funkcijos, ir $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$, tai

$$f(n) = f(p_1^{\alpha_1}) + f(p_2^{\alpha_2}) + \dots + f(p_s^{\alpha_s}), \quad g(n) = g(p_1^{\alpha_1}) g(p_2^{\alpha_2}) \dots g(p_s^{\alpha_s}).$$

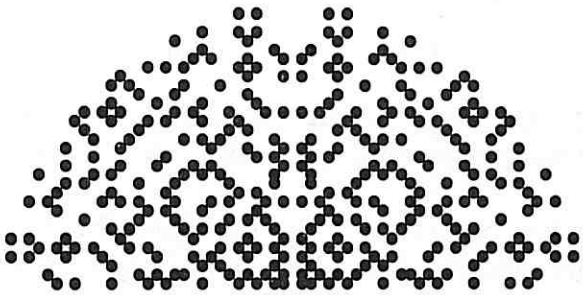
Tad svarbu žinoti adityviosios ar multiplikatyviosios funkcijos reikšmes, įgyjamas pirminių skaičių laipsniams. Pavyzdžiui, galima įrodyti, kad

$$r(p^\alpha) = \begin{cases} 1, & \text{kai } p = 2, \\ \alpha + 1, & \text{kai } p = 4k + 1, \\ 0, & \text{kai } p = 4k + 3 \text{ ir } \alpha \text{ nelyginis}, \\ 1, & \text{kai } p = 4k + 3 \text{ ir } \alpha \text{ lyginis}. \end{cases}$$

• • • $\alpha + \omega$ • • •

Skyrelio pradžios brėžiniai, susiję su tam tikromis aritmetinėmis skaičių savybėmis, kėlė greičiau nedarnos, nei tvarkos jausmą. Pabaigsime pavyzdžiu, kuris byloja visai priešingai.

Plokštumoje, kurioje įvesta stačiakampė koordinačių sistema, atidėkime tas sveikųjų skaičių poras $\langle x, y\rangle$, kurioms x^2+y^2 yra mažesnis už 1000 pirminis skaičius. Vaizduokime tik taškus su teigiamomis y reikšmėmis. Štai ką gausime:



Vidutinės reikšmės

Jau matėme, kad aritmetinė funkcija $f(n)$, kai jos argumentas n perbėga natūraliuosius skaičius $1, 2, \ldots, N$, gali elgtis gana įnoringai. Svarbi aritmetinės funkcijos charakteristika yra jos vidutinė intervale $[1, N]$ reikšmė. Ją mes apibrėšime taip:

$$M(f, N) = \frac{1}{N}\sum_{n=1}^{N} f(n).$$

Kartais vidutinę reikšmę nesudėtinga suskaičiuoti.

Prisiminkime multiplikatyviąją funkciją $r(n)$, kuri reiškia skaičiaus n skirtingų išraiškų $n = x^2 + y^2$ kiekį; čia $x \geq 0, y > 0$ yra natūralieji skaičiai. Įveskime plokštumoje stačiakampę koordinačių sistemą ir žymėkime u, v taško abscisę bei ordinatę. Nagrinėkime skritulius $u^2+v^2 \leq R^2$; juos žymėsime $C(R)$. Jeigu $n \leq N$ ir $n = x^2+y^2, x \geq 0, y > 0$, tai taškas $\langle x, y\rangle$ yra skritulio $C(\sqrt{N})$ viduje bei pirmame koordinačių ketvirtyje (bet ne ant tiesės $v = 0$). Kita vertus, kiekvienam šio skritulio taškui su sveikomis koordinatėmis $x \geq 0, y > 0$, atsiras skaičius $n \leq N$, kad $n = x^2 + y^2$. Taigi skritulio $C(\sqrt{N})$ taškų su sveikomis koordinatėmis $x \geq 0, y > 0$, skaičius lygus skirtingų išraiškų $n = x^2+y^2, n \leq N$, kiekiui, t. y. sumai

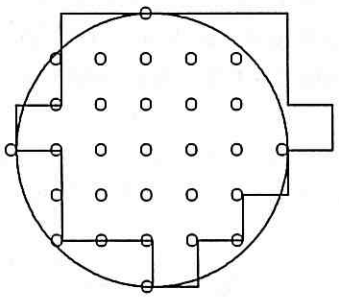
$$r(1) + r(2) + \ldots + r(N) = NM(r, N).$$

Jeigu skaičiuosime visus skritulio $C(\sqrt{N})$ taškus su sveikomis koordinatėmis x, y, (išskyrus tašką $\langle 0, 0\rangle$), tai gautasis dydis $S(\sqrt{N})$ bus keturgubai didesnis:

$$S(\sqrt{N}) = 4NM(r, N). \tag{27}$$

• • • $\alpha + \omega$ • • •

Tad uždavinį apie funkcijos $r(n)$ vidurkį suvedėme į skritulio taškų su sveikomis koordinatėmis skaičiavimo uždavinį. Šį uždavinį nesunku išspręsti pasitelkus geometrinį brėžinį.



Skritulio $C(\sqrt{N})$ taškai su sveikomis koordinatėmis pažymėti o. Kiekvienam iš jų priskirsime vienetinį kvadratą su vertikaliomis ir horizontaliomis kraštinėmis taip, kad taškas būtų apatinė kairioji šio kvadrato viršūnė. Kvadratai sudaro plokščią figūrą, kurios plotas lygus $S(\sqrt{N})+1$ (primename, kad $S(\sqrt{N})$ – skritulio taškų su sveikomis koordinatėmis $x, y, x^2+y^2 \neq 0$, kiekis.) Matome, kad ši figūra nedengia skritulio $C(\sqrt{N})$, taip pat nėra šio skritulio dengiama. Tačiau skritulys $C(\sqrt{N}+\sqrt{2})$ tikrai dengs šią figūrą o skritulys $C(\sqrt{N}-\sqrt{2})$ bus figūros poaibis. Parašę atitinkamą nelygybę plotams, gauname

$$\pi(\sqrt{N}-\sqrt{2})^2 < S(\sqrt{N})+1 < \pi(\sqrt{N}+\sqrt{2})^2.$$

Prisiminę (27) galime suformuluoti tokį tvirtinimą apie aritmetinės funkcijos $r(n)$ vidutinę reikšmę.

Teorema. *Kiekvienam* $N \geq 1$ *teisingos nelygybės*

$$\frac{1}{4}\pi - \frac{\pi}{\sqrt{2N}} + \frac{2\pi-1}{4N} < M(r,N) < \frac{1}{4}\pi + \frac{\pi}{\sqrt{2N}} + \frac{2\pi-1}{4N}. \tag{28}$$

Iš (28) gauname tokią vidutinės reikšmės asimptotiką

$$M(r,N) = \frac{1}{4}\pi + \frac{c(N)}{\sqrt{N}}, \quad N \to \infty;$$

čia $c(N)$ – aprėžto modulio funkcija: egzistuoja tam tikra konstanta A, kad $|c(N)| < A$.

Aritmetinių funkcijų vidurinių reikšmių asimptotikų tyrimas – svarbus analizinės skaičių teorijos uždavinys. Paminėsime dar keletą rezultatų. Formulėse dydis B yra konstanta, funkcijos $c_i(N)$ – aprėžto modulio funkcijos. Daliklių funkcijai $d(n)$ teisinga lygybė

$$M(d,N) = \ln N + (2B-1) + \frac{c_1(N)}{\sqrt{N}};$$

kanononio skaidinio daugiklių skaičiui $\Omega(n)$

$$M(\Omega,N) = \ln\ln N + B + \frac{c_2(N)}{\ln N}.$$

$\bullet\bullet\bullet\ \alpha+\omega\ \bullet\bullet\bullet$

Aritmetinės funkcijos, dažniai, arba tikimybinė skaičių teorija

Tikimybių teorijos raida prasidėjo nuo klausimų: kaip dažnai tas ar kitas įvykis vyksta, nuo ko tai priklauso. Mes taip pat galime klausti kaip dažnai pasitaiko koks nors „aritmetinis įvykis". Kaip dažnai pasitaiko pirminiai skaičiai arba natūralieji skaičiai, kuriuos galima išreikšti dviejų kvadratų suma ir taip toliau.

Tarkime, mums rūpi intervalo $[1, x]$ natūralieji skaičiai, turintys kokią nors aritmetinę savybę $\mathcal{S}$. Jų aibę pažymėję S_x, o jos elementų kiekį – $|S_x|$, galime taip apibrėžti šios „savybės dažnį":

$$\nu_x\{S_x\} = \frac{|S_x|}{x}.$$

Paprastai tiriama, kaip dažnis $\nu_x\{S_x\}$ elgiasi, kai $x \to \infty$. Štai visai paprastas pavyzdys:

$$\nu_x\{n \le x, p|n\} = \frac{1}{x}\left[\frac{x}{p}\right] = \frac{1}{p} + \frac{c_x}{x};$$

čia c_x yra aprėžto modulio funkcija, o $[v]$ žymi skaičiaus sveikąją dalį.

Dažnai aritmetinės skaičių savybės reiškiamos aritmetinėmis funkcijomis – prisiminkime adityviąsias funkcijas $\omega(n), \Omega(n)$ bei multiplikatyviąsias $r(n), d(n)$. Galime tirti, pavyzdžiui, tokių dažnių asimptotinį elgesį:

$$\nu_x\{n \le x, \omega(n) = k\}, \quad \nu_x\{n \le x, \omega(n) \in A_x\};$$

čia k – fiksuotas natūralusis skaičius, o A_x atitinkamu būdu pasirinkta aibė.

Pirmuosius tokio pobūdžio rezultatus gavo 1917 m. G. Hardis ir S. Ramanudžanas (Srinivasa Ramanujan, 1887–1920). Jie įrodė, kad

$$\nu_x\{n \le x, \omega(n) = k\} < c_1 \frac{(\ln\ln x + c_2)^{k-1}}{(k-1)!\ln x},$$

$$\nu_x\{n \le x, |\omega(n) - \ln\ln x| > \psi(x)\sqrt{\ln\ln x}\} \to 0, \quad x \to \infty; \tag{29}$$

čia: c_1, c_2 teigiamos konstantos, o $\psi(x)$ bet kokia neaprėžtai didėjanti, kai $x \to \infty$, funkcija.

Šie rezultatai gauti analizinės skaičių teorijos metodais, tačiau juose glūdi skaičių teorijos ir tikimybių teorijos idėjų sintezės grūdas. Bet tvirto matematinio pamato tokiai sintezei teko laukti dar ilgai. Tik J. Kubiliaus darbai apie mūsų amžiaus vidurį nustatė naują kryptį skaičių teorijoje, kurią imta vadinti tikimybine skaičių teorija.

Panagrinėkime, kaip šios teorijos šviesoje atrodo Hardžio–Ramanudžano (29) rezultatas, kuris, skyrium imant, teatspindi savotišką pavienės aritmetinės funkcijos elgesį.

Tegu $f(n)$ yra kokia nors adityvioji funkcija. Apibrėžkime

$$A(x) = \sum_{p \le n} \frac{f(p)}{p}, \quad D^2(x) = \sum_{p^\alpha \le n} \frac{f(p^\alpha)}{p^\alpha};$$

čia: p žymi pirminius skaičius, o p^α – jų laipsnius su natūraliaisiais rodikliais.

Kubilius įrodė nelygybę, kuri teisinga visoms be išimties adityviosioms funkcijoms:

egzistuoja konstanta $c > 0$, *kad*

$$\sum_{n \le x} |f(n) - A(x)|^2 \le cxD^2(x). \tag{30}$$

Imkime kokią nors teigiamą ir neaprėžtai didėjančią funkciją $\psi(x)$ ir sumažinkime (30) Kubiliaus nelygybės kairiąją pusę, palikdami joje tik tuos dėmenis, kuriems

$$|f(n) - A(x)| > \psi(x)D(x).$$

Kadangi tokių dėmenų yra $|\{n \le x, |f(n) - A(x)| > \psi(x)D(x)\}|$ ir visi jie nemažesni negu $\psi(x)D(x)$, tai

$$\psi^2(x)D^2(x)|\{n \le x, |f(n) - A(x)| > \psi(x)D(x)\}| \le cxD^2(x),$$

arba

$$\nu_x\{n \le x, |f(n) - A(x)| > \psi(x)D(x)\} \le \psi^{-2}(x),$$

$$\nu_x\{n \le x, |f(n) - A(x)| > \psi(x)D(x)\} \to 0, \quad x \to \infty. \tag{31}$$

Hardžio ir Ramanudžano (29) rezultatas yra atskiras (31) dėsnio atvejis: pakanka imti $f(n) = \omega(n)$ ir suskaičiuoti $A(x), D(x)$. Tikimybių teorijos požiūriu, (31) yra didžiųjų skaičių dėsnis: jeigu atsitiktinai rinksimės natūraliuosius skaičius iš „ilgo" intervalo $[1, x]$, tai retai pasitaikys atvejai, kad pasirinktajam n būtų teisinga $|f(n) - A(x)| > \psi(x)D(x)$.

Dėsnis (31) – vienas iš paprasčiausiųjų tikimybinėje skaičių teorijoje. Paminėsime sudėtingesnį, įrodytą P. Erdiošo ir M. Kaco (Pál Erdös, Marc Kac), o vėliau apibendrintą Kubiliaus:

bet kokiems skaičiams $a < b$

$$\nu_x\left\{n \le x, a < \frac{\omega(n) - \ln\ln x}{\sqrt{\ln\ln x}} < b\right\} \to \frac{1}{2\pi}\int_a^b e^{-0.5u^2}du, \quad x \to \infty.$$

Pabaigoje įprasta pateikti literatūros sąrašą. Literatūra skaičių teorijos klausimais yra gausi, bet ją dažniausiai leidžia užsienio knygų leidyklos. Kažin ar jų sąrašas skaitytojui būtų naudingas. Gi Lietuvoje skaičių teorijos monografijų ir vadovėlių išleista nedaug. Galbūt todėl jas ir verta paminėti.

Paminėsime ir vieną užsieninę knygą – jos pavadinimas daug pasako.

Literatūra

1. *Bulota K., Survila P.* Algebra ir skaičių teorija. Vilnius, Mokslas, 1990. D.1-2.
2. *Kubilius J.* Tikimybiniai metodai skaičių teorijoje. Vilnius, 1959, 1962. Rusų k.
3. *Laurinčikas A.* Rymano dzeta funkcijos teorijos pagrindai. VU leidykla, 1992.
4. *Manstavičius E.* Tikimybinė skaičių teorija. VU leidykla, 1987.
5. *Schroeder M.* Number Theory in Science and Communication. With Applications in Cryptography, Physics, Digital Information, Computing and Self-Similarity. Springer Verlag, 1986.

• • • $\alpha + \omega$ • • •

Bernardas Rymanas (1826–1866) gimė mažo kaimelio pastoriaus šeimoje. Šešių vaikų būryje jis buvo antras: turėjo brolį ir keturias seseris. Šeimą skynė ankstyvos mirtys: jaunas mirė brolis, jaunos – trys seserys, motina taip pat mirė anksti.

Vaikystėje Bernardą labiau traukė istorija negu matematika. Ypač domėjosi Lenkijos istorija. Tačiau matematika greitai užvaldė. Gimnazijoje gavo paskaityti 900 puslapių Ležandro skaičių teorijos kursą. Perskaitė kaip detektyvą – per 6 dienas.

Ketino sekti tėvu – 1846 m. įstojo į Getingeno universiteto teologijos fakultetą. Getingene dėstė „Mathematicorum Princeps" – K. Gausas. B. Rymanas pasuko į matematiką.

Po metų išvyko į Berlyno universitetą. Dveji metai Berlyne – itin svarbus tarpsnis. Užsimezgė draugystė su L. Dirichle – visam gyvenimui.

1849 m. B. Rymanas grįžo į Getingeną, 1851 m. pristatė disertaciją „Kompleksinio kintamojo funkcijų teorijos pagrindai". K. Gausas, kuris retai gyrė jaunuosius, labai vertino šį Rymano darbą.

1853 m. pabaigtas habilitacijos darbas „Apie funkcijų reiškimą trigonometrinėmis eilutėmis". Dar reikėjo parengti habilitacijos paskaitą. Pasiūlė tris temas. K. Gausas išrinko antrąją – iš geometrijos. B. Rymano habilitacijos paskaita „Apie geometrijos pagrindų hipotezes" labai sujaudino K. Gausą. Jis tik vienas galėjo įvertinti Rymano minčių gilumą ir reikšmę.

Nors darbai buvo genialūs – tai nedaug reiškė universiteto vadovybei. Gyvenimas buvo sunkus, tik 1857 m. B. Rymanas tapo ekstraordinariniu profesorium. Tačiau pripažinimas atėjo. Po L. Dirichle mirties 1859 m. B. Rymanas perėmė katedrą, kuriai iš eilės vadovavo K. Gausas bei L. Dirichle.

1862 m. B. Rymanas vedė, bet tais pačiais metais persišaldė ir sunkiai susirgo tuberkulioze. Vokietijos klimatas buvo jau nebepakeliamas, tad B. Rymano šeima dažniausia gyveno Italijoje. Ten prabėgo ir paskutiniai gyvenimo mėnesiai.

„Jo jėgos greitai seko, ir jis pats aiškiai jautė artėjančią mirtį. Bet dieną prieš mirtį jis dar rašė paskutinį, taip ir nepabaigtą darbą, ilsėdamasis po figmedžiu ir žvelgdamas į nuostabų kraštovaizdį." – R. Dedekindas.