Giedrius Alkauskas

Pirminiai skaičiai aritmetinėse progresijose

Dirichlė teorema

1837 metais L. Dirichlė įrodė tokią teoremą:

1 teorema. *Jei a, d yra du natūralieji skaičiai ir $(a, d) = 1$, tai sekoje*

$$x_n = an + d, \quad n = 1, 2, \ldots,$$

yra be galo daug pirminių skaičių. Jei $s_1 < s_2 < \ldots$ yra šios sekos pirminiai skaičiai, tai dydžiai

$$\frac{1}{s_1} + \frac{1}{s_2} + \ldots + \frac{1}{s_n}$$

neaprėžtai auga, kai $n \to \infty$.

Šios teoremos įrodymas nėra elementarus. Ją lengva įrodyti sekoms $3n+1, 3n+2, 4n+1, 4n+3$. Šiame straipsnyje pateikiamas elementarus Dirichlė teoremos įrodymas visoms aritmetinėms progresijoms, prasidedančioms vienetu ir turinčioms pirminį skirtumą.

Keli svarbūs skaičių teorijos teiginiai

Tegu $\varphi(n)$ yra natūraliųjų skaičių, mažesnių už n ir tarpusavyje su juo pirminių, kiekis. Teisinga Oilerio teorema:

2 teorema. *Jei c yra natūralusis skaičius ir $(n, c) = 1$, tai $c^{\varphi(n)} - 1$ dalijasi iš n.*

Įrodymas. Naudosime įprastinius skaičių teorijos žymenis: jei a dalo b, rašysime $a|b$; jei a ir b dalijant iš c gaunamos tos pačios liekanos, rašysime $a \equiv b (\mathrm{mod}\ c)$. Priminsime, kad iš $a_1 \equiv b_1 (\mathrm{mod}\ c)$ ir $a_2 \equiv b_2 (\mathrm{mod}\ c)$ išplaukia $a_1 a_2 \equiv b_1 b_2 (\mathrm{mod}\ c)$ ir iš $ad \equiv bd (\mathrm{mod}\ c), (d, c) = 1$ išplaukia $a \equiv b (\mathrm{mod}\ c)$.

Tegu $a_1, a_2, \ldots, a_k, k = \varphi(n)$, yra visi natūralieji skaičiai, nedidesni už n ir tarpusavyje su juo pirminiai. Tada skaičiai

$$c \cdot a_1, c \cdot a_2, \ldots, c \cdot a_k$$

yra taip pat tarpusavyje pirminiai su n. Prieštaros metodu nesunkiai įsitikinsime, kad visus juos dalijant iš n gaunamos skirtingos liekanos. Tarkime,

$ca_m \equiv b_m (\mathrm{mod}\ n), 1 \leq m \leq k, 1 \leq b_m < n$. Tačiau tada skaičiai $b_1, b_2, \ldots, b_k$ gaunami tiesiog perstačius skaičius $a_1, a_2, \ldots, a_k$. Taigi

$$ca_1 \cdot ca_2 \cdot \ldots \cdot ca_k \equiv b_1 \cdot b_2 \cdot \ldots \cdot b_k \equiv a_1 \cdot a_2 \cdot \ldots \cdot a_k (\mathrm{mod}\ n).$$

Suprastinę lyginį iš $a_1 \cdot a_2 \cdot \ldots \cdot a_k$, gausime $c^k \equiv 1 (\mathrm{mod}\ n)$, t. y. n dalija $c^k - 1 = c^{\varphi(n)} - 1$.

Pritaikę šią teoremą, kai n yra pirminis skaičius p, gausime Ferma teoremą.

3 teorema. *Jei skaičius p yra pirminis, o natūralusis skaičius c nesidalija iš p, tai $c^{p-1} - 1$ dalijasi iš p.*

Mums dar prireiks tokio teiginio apie sveikaskaičius tiesinės lygties sprendinius.

4 teorema. *Jei a, b yra tarpusavyje pirminiai natūralieji skaičiai, tai atsiras neneigiami sveikieji skaičiai x, y, su kuriais*

$$ax - by = 1.$$

Įrodymas. Prieštaros būdu nesunku įsitikinti, kad skaičius $1 \cdot a, 2 \cdot a, \ldots b \cdot a$ dalijant iš b gaunamos skirtingos liekanos. Tada bent vieno iš jų liekana bus lygi 1. Tarkime, $ax \equiv 1 (\mathrm{mod}\ b)$. Taigi su tam tikru sveikuoju y teisinga lygybė $ax = 1 + by$. Tačiau

$$y = \frac{ax - 1}{b} \geq \frac{a - 1}{b} \geq 0.$$

Teiginys įrodytas.*

Aritmetinės progresijos nq+1

Šiame skyrelyje elementariai įrodysime tokią teoremą.

5 teorema. *Jei q yra pirminis skaičius, tai sekoje $x_n = nq + 1$, $n = 1, 2, \ldots$ yra be galo daug pirminių skaičių.*

Iš pradžių įrodysime pagalbinį teiginį.

Lema. *Jei $q > 1$ yra natūralusis skaičius, tai lygtis*

$$z^{q-1} + z^{q-2} + \ldots + z + 1 = pm$$

su be galo daugeliu pirminių p turi sprendinį natūraliaisiais skaičiais m, z.

Lemą galima ir šitaip suformuluoti:

skaičių $z^{q-1} + z^{q-2} + \ldots + z + 1$, $z = 1, 2, \ldots$ skirtingų pirminių daliklių aibė yra begalinė.

---

* Kaip skaičiams a,b surasti skaičius x, y rašoma „Alfa + omega", 1996, **1**, p. 8.

Lemos įrodymas. Tarkime priešingai: visų skaičių $z^{q-1}+z^{q-2}+\ldots+z+1$, $z=1,2,\ldots$, pirminiai dalikliai yra iš aibės $\{p_1,p_2,\ldots,p_s\}$. Imkime $z=p_1\cdot p_2\cdot\ldots\cdot p_s$. Tuomet

$$z^{q-1}+z^{q-2}+\ldots+z+1$$

nesidalija iš jokio skaičiaus p_i. Gavome prieštarą. Taigi daliklių aibė negali būti baigtinė. Lema įrodyta.

Turbūt pastebėjote, kad lemos įrodymas primena garsųjį Euklido įrodymą, kad pirminių skaičių yra be galo daug. Akivaizdu, kad lemos teiginys teisingas su bet kokiu ne mažesnio už 1 laipsnio daugianariu sveikais koeficientais.

5 teoremos įrodymas. Imkime pirminį skaičių p, tokį, kad $p\neq q$ $(p-1,q)=1$. Tada visų skaičių

$$1^q,2^q,\ldots,(p-1)^q$$

dalybos iš p liekanos yra skirtingos. Iš tikrųjų, jei būtų

$$k^q\equiv l^q(\mathrm{mod}\ p),\quad 1\leq k<l\leq p-1,$$

tai su bet kokiu natūraliuoju x taip pat gautume $k^{xq}\equiv l^{xq}(\mathrm{mod}\ p)$. Remiantis 4 teorema, egzistuoja sveikieji neneigiami skaičiai x,y, su kuriais $qx=(p-1)y+1$. Tačiau tada

$$k^{qx}=k^{(p-1)y+1}\equiv k\cdot(k^{(p-1)})^y\equiv k(\mathrm{mod}\ p),$$

$$l^{qx}=l^{(p-1)y+1}\equiv l\cdot(l^{(p-1)})^y\equiv l(\mathrm{mod}\ p);$$

čia pasinaudojome 3 teoremos tvirtinimu. Taigi iš $k^q\equiv l^q(\mathrm{mod}\ p)$ gautume prieštarą: $k\equiv l(\mathrm{mod}\ p)$.

Iš to išplaukia, kad pirminiam skaičiui $p, p\neq q, (p-1,q)=1$, lygybė $z^q\equiv 1(\mathrm{mod}\ p)$ teisinga tada ir tik tada, kai $z\equiv 1(\mathrm{mod}\ p)$, t. y. $p|z^q-1$ tada ir tik tada, kai $p|z-1$. Panagrinėkime lygybę

$$z^q-1=(z-1)(z^{q-1}+z^{q-2}+\ldots+z+1). \tag{1}$$

Jei p yra pirminis, $p\neq q, (p-1,q)=1$ ir $z\equiv 1(\mathrm{mod}\ p)$, tai

$$z^{q-1}+z^{q-2}+\ldots+z+1\equiv q(\mathrm{mod}\ p)$$

ir p negali dalyti skaičiaus $z^{q-1}+z^{q-2}+\ldots+z+1$. Jei $z\not\equiv 1(\mathrm{mod}\ p)$, ir p dalija $z^{q-1}+z^{q-2}+\ldots+z+1$, tai iš (1) gauname, kad $p|z^q-1$ ir todėl $z\equiv 1(\mathrm{mod}\ p)$. Iš šių samprotavimų gauname tokią svarbią išvadą:

• • • $\alpha+\omega$ • • •

Išvada. *Jei p yra toks pirminis skaičius, kad $p \neq q, (p-1,q) = 1$, tai su bet kokiu natūraliuoju z p negali dalyti $z^{q-1} + z^{q-2} + \ldots + z + 1$.*

Tačiau lema tvirtina, kad skaičių $z^{q-1} + z^{q-2} + \ldots + z + 1$ daliklių aibė yra begalinė. Todėl egzistuoja be galo daug pirminių p, kurie netenkina sąlygos $(p-1,q) = 1$. Tačiau tokiems skaičiams $(p-1,q) = q$, arba $p = 1 + nq$, su tam tikru natūraliuoju n. Teorema įrodyta.

Taigi sekoje $nq + 1$ yra be galo daug pirminių skaičių. Kadangi jie yra nelyginiai, tai iš tiesų visi jie yra posekyje $2mq + 1$.

Kas toliau?

Ar galima šį įrodymo metodą patobulinti, kad jis tiktų progresijoms $qn+a$? Čia q – pirminis skaičius, o $1 < a < q$. Šiam tikslui reiktų sudaryti daugianarį $P(z)$, kurio laipsnis būtų mažesnis už q, ir kuris turėtų savybę:

> *jei $P(z) \equiv 0 \pmod{p}$, tai arba $p \equiv a \pmod{q}$, arba p priklauso tam tikrai baigtinei pirminių skaičių aibei.*

Tokio daugianario net $q = 3, a = 2$ atveju nežinau.

Redaktoriaus prierašas. Giedrius Alkauskas pats sugalvojo čia išdėstytą 5 teoremos (specialaus Dirichlė teoremos atvejo) įrodymą. Po to jis ieškojo, ar tokio įrodymo nėra skaičių teorijos literatūroje. Ir rado: I. M. Vinogradovo „Skaičių teorijos pagrindų“ paskutiniame uždavinių skyriuje ši teorema suformuluota ir nurodytas jos įrodymo kelias. Teorema taip pat dėstoma H. Hasės knygoje „Skaičių teorijos paskaitos“ (vertimas į rusų kalbą išleistas 1950 m.). Šią nuorodą taip pat pateikė straipsnio autorius.