Skaičių teorijos pradmenys

Ir pirminio skaičiaus daliklių dingimo paslaptis!

Šią teorinę medžiagą paruošė du daliklių detektyvai:
Anton Šerlokas Liutvinas ir Pijus Vatsonas Piekus

2024/10/15

1 Lyginiai ir nelyginiai skaičiai

1.1 Teorija

Apibrėžimas. Sveikąjį skaičių n vadinsime *lyginiu*, jei jį galima užrašyti pavidalu: $n = 2k$, kur k bet koks sveikas skaičius ($n, k \in \mathbb{Z}$).

Apibrėžimas. Sveikąjį skaičių n vadinsime *nelyginiu*, jei jį galima užrašyti pavidalu: $n = 2k + 1$, kur k bet koks sveikas skaičius ($n, k \in \mathbb{Z}$).

Apibrėžimas. Sveikuosius skaičius m ir n vadinsim *vienodo lyginumo*, jeigu jie abu lyginiai arba abu nelyginiai.

Apibrėžimas. Sveikuosius skaičius m ir n vadinsim *skirtingo lyginumo*, jeigu vienas iš jų lyginis, o kitas nelyginis.

1 Pavyzdys Įrodykite, jog bet kokių dviejų lyginių skaičių suma yra lyginė.
Įrodymas: Pažymėkime pirmą skaičių a, o antrą - b, tada pagal lyginio skaičiaus apibrėžimą $a = 2c$, o $b = 2d$, gauname, jog $a+b = 2c+2d = 2(c+d)$, vadovaujantis tuo pačiu apibrėžimu gauname lyginį skaičių.

2 Pavyzdys Įrodykite, jog bet kokio nelyginio skaičiaus kvadratas yra nelyginis.
Įrodymas: Pažymėkime nelyginį skaičių n, tada pagal nelyginio skaičiaus apibrėžimą $n = 2k + 1$. Gauname, jog $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, remiantis nelyginio skaičiaus apibrėžimu gauname, jog n^2 yra nelyginis.

Iki šiol mes pasitelkėme tiesioginį įrodymo būdą, pasiėmėm sąlyga, pritaikėm tam tikrus apibrėžimus ir gavom rezultatą. Deja sudėtingesniuose uždaviniuose tai ne visada pavyks, tačiau nepraraskime vilties, mums į pagalbą ateina kitas įrodymo būdas!

3 Pavyzdys Įrodykite, jog kiekvienam sveikajam skaičiui n, n^2+n+6 yra lyginis.
Įrodymas: Įrodymą galime išskaidyti į du atvejus, nes kiekvienas sveikas skaičius turi būti arba lyginis arba nelyginis, pirmu atveju sakysim, jog n lyginis, o antru, jog n nelyginis.
1 dalis: $n = 2k$, tada $n^2+n+6 = (2k)^2+2k+6 = 4k^2+2k+6 = 2(2k^2+k+3)$, gauname lyginį skaičių.
2 dalis: $n = 2k+1$, tada $n^2+n+6 = (2k+1)^2+(2k+1)+6 = 4k^2+4k+1+2k+1+6 = 4k^2+6k+8 = 2(2k^2+3k+4)$, ir vėl gavome lyginį skaičių.
Abiem atvejais gavome, jog n^2+n+6 yra lyginis ir tai užbaigia mūsų įrodymą.

Toks įrodymo būdas vadinamas įrodymas su atvejais (angl. proof by cases). Jis yra gana dažnai sutinkamas ir neretai praverčia sprendžiant sunkesnius uždavinius.

1.2 Uždaviniai

1. Įrodykite, jog bet kokių dviejų nelyginių skaičių suma yra lyginė.

2. Įrodykite, jog lyginio ir nelyginio skaičių suma visada yra nelyginė.

3. Įrodykite, jog dviejų lyginių skaičių sandauga yra lyginė.

4. Įrodykite, jog dviejų nelyginių skaičių sandauga yra nelyginė.

5. Įrodykite, jog lyginio ir nelyginio skaičių sandauga yra lyginė.

6. Įrodykite, jog lyginio skaičiaus kvadratas yra lyginis.

7. Įrodykite, kad jei n yra lyginis, tai $-n$ bus lyginis, $n+1$ bus nelyginis, $(-1)^n = 1$.

8. Įrodykite, kad jei n yra nelyginis, tai $-n$ bus nelyginis, n^2+4n+9 bus lyginis, n^3 bus nelyginis, o $(-1)^n = -1$.

9. Įrodykite, kad jei n bus sveikas skaičius, tai tada n^2+n ir n^2+3n+6 bus lyginiai, o $3n^2+5n+1$ bus nelyginis.

10. Duoti du nelyginiai skaičiai m ir n. Įrodykite, kad $5m-3n$ yra lyginis.

11. Sveikieji skaičiai m ir n yra tokio pačio lyginumo. Įrodyti, kad $7m-3n$ yra lyginis.

12. Įrodykite, kad jei n, m ir t yra sveikieji skaičiai, tai bent vienas iš $m-n$, $m-t$ ir $n-t$ bus lyginis.

13. Įrodykite, jog bet kokį nelyginį skaičių galima išreikšti kaip dviejų kvadratų skirtumą.

2 Dalumas

2.1 Teorija

Apibrėžimas. Sveikasis skaičius b *dalijasi* iš sveikojo nenulinio skaičiaus a, jeigu $b = ak$, kur k yra bet koks sveikas skaičius ($a, b, k \in \mathbb{Z}, a \neq 0$).

Kai b dalijasi iš a, tai užrašysime $a \mid b$ ir sakysime a *dalo* b, kitu atveju rašysime $a \nmid b$ ir sakysime, jog a *nedalo* b.

Apibrėžimas. Jeigu n dalijasi iš k ($k \mid n$), tai k vadinsim skaičiaus n *dalikliu.*

Apibrėžimas. Jeigu K dalijasi iš n ($n \mid K$), tai K vadinsim skaičiaus n *kartotiniu.*

Dalumo savybės (jas olimpiadose galima naudoti be įrodymo):

1 Savybė. Jeigu $x \mid a$ ir $x \mid b$, tai $x \mid a + b$.

Įrodymas: Pagal dalumo apibrėžimą galime teigti, jog $a = xk_1$, o $b = xk_2$, tada $a + b = xk_1 + xk_2 = x(k_1 + k_2)$, $k_1 + k_2$ yra sveikas skaičius, todėl pagal dalumo apibrėžimą galima teigti, jog $x \mid a + b$.

2 Savybė. Jeigu $x \mid a$ ir $x \mid b$, tai $x \mid a - b$.

3 Savybė. Jeigu $n \mid a$ ir $n \mid b$, tai $n \mid ax + by$, visiems sveikiesiems x, y.

4 Savybė. Jeigu $x \mid a$ ir $x \mid b$, tai $x \mid ab$.

5 Savybė. Jeigu $x \mid a$ ir $y \mid b$, tai $xy \mid ab$.

6 Savybė. Jeigu $x \mid y$ ir $y \mid z$, tai $x \mid z$.

Įrodymas: Pagal dalumo apibrėžimą $y = xk_1$ ir $z = yk_2$, Gauname, jog $z = yk_2 = (xk_1)k_2 = xk_1k_2 = x(k_1k_2)$, todėl galime teigti, jog $x \mid z$.

7 Savybė. Jeigu $a \mid b$, tai $an \mid bn$, visiems sveikiesiems n.

8 Savybė. Jeigu $an \mid bn$, tai $a \mid b$ visiems natūraliesiems n.

9 Savybė. Jeigu $a \mid b$, tai $a^n \mid b^n$, visiems natūraliesiems n.

10 Savybė. $m \mid mn$, visiems natūraliesiems n ir m.

11 Savybė. Jeigu $mn \mid a$, tai $m \mid a$ ir $n \mid a$.

12 Savybė. Jeigu $x \mid y$ ir $y \mid x$, tai $|x| = |y|$.

13 Savybė. Jeigu $a \mid b$, tai $|a| \leqslant |b|$ arba $b = 0$.

Dalybos su liekana teorema. Visiems sveikiesiems skaičiams a ir m ($a, m \in \mathbb{Z}, m > 0$), egzistuoja tokie unikalūs sveikieji skaičiai q ir r ($q, r \in \mathbb{Z}$), kad

$$a = mq + r$$

kur $0 \leqslant r < m$.

Šiuo atveju a - *dalinys*, m - *daliklis*, q - *nepilnas dalmuo*, o r yra *liekana*.

1 Pavyzdys Įrodykite, kad jei $n \mid 5a + 3b$ ir $n \mid 3a + 2b$, tai $n \mid a$ ir $n \mid b$.

Įrodymas: Remsimės skaičių dalumo 2-ąja savybę: $n \mid 5a + 3b - (3a + 2b) \implies n \mid 2a + b$, tada $n \mid 3a + 2b - (2a + b) \implies n \mid a + b$, iš to seka, jog $n \mid 2a + b - (a + b) \implies n \mid a$, kadangi $n \mid a + b$ ir $n \mid a$, tai $n \mid a + b - a \implies n \mid b$.

2 Pavyzdys Duota, kad skaičius $a + 4b$ dalijasi iš 13. Įrodykite, kad ir $10a + b$ dalijasi iš 13.

Įrodymas: Remiantis 10 dalumo savybe gauname, jog $13 \mid 13a + 13b$. Tada pagal 9 dalumo savybe ($x = 1, y = -3$) gauname, jog $n \mid 13a + 13b - 3(a + 4b) \implies n \mid 10a + b$.

3 Pavyzdys Duotas sveikasis skaičius x. Įrodykite, jog x^2 dalijant iš 4 gaunama liekana gali būti tik 1 arba 0.

Įrodymas: ir vėl pasinaudosime įrodymu su atvejais. Pirmu atveju tegul x lyginis, o antru - nelyginis.

<u>1 atvejis:</u> Kadangi x lyginis, tai $x = 2k$, tada $x^2 = (2k)^2 = 4k^2$, gauname, jog $4 \mid x$, todėl liekana dalijant iš keturių yra 0.

<u>2 atvejis:</u> Kadangi x nelyginis, tai $x = 2k+1$, tada $x^2 = (2k+1)^2 = 4k^2+4k+1 = 4(k^2+k)+1$, remiantis dalybos su liekana teorema gauname, jog x^2 dalijant iš keturių liekana yra 1.

2.2 Uždaviniai

1. Kiekvienai iš duotų skaičių porų raskite nepilnąjį dalmenį ir liekaną, kai a dalijamas iš m: $(a, m) = (15, 4); (-7, 3); (-1, 15); (4, 15); (65, 11); (0, 4)$.
2. Įrodykite 1-13 dalumo savybes (jau įrodytų spręsti nebūtina).
3. Duota, kad $n \mid 3a$ ir $n \mid 12a + 5b$. Įrodykite, kad $n \mid 10b$.
4. Duota, kad $n \mid 3a + 7b$ ir $n \mid 2a + 5b$. Įrodykite, kad $n \mid a$ ir $n \mid b$.
5. Duota, kad $n \mid a + b$. Įrodykite, kad $n \mid a^3 + 2a + b^3 + 2b$.
6. Duota, kad $11 \mid 3x + 7y$ ir $11 \mid 2x + 5y$. Įrodykite, kad $121 \mid x^2 + 3y^2$.

7. Įrodykite, kad $m^{12} \mid t$, jeigu $m^3 \mid n$ ir $n^4 \mid t$.

8. Duotas sveikasis skaičius n. Įrodykite, kad jei $n^2 \mid n$, tai n lygus 0, 1 arba -1.

9. Duota, kad dviejų natūraliųjų skaičių m ir n sandauga dalijasi iš jų sumos. Įrodykite, kad $m + n \leqslant n^2$.

10. Duotas natūralusis skaičius n. Įrodyti, jog $4 \mid 1 + (-1)^n(2n-1)$.

11. Įrodykite, kad dviejų nelyginių kvadratų skirtumas dalijas iš 8.

12. Įrodykite, jog jeigu skaičiaus paskutinis skaitmuo yra 5, tai jo kvadrato paskutiniai du skaitmenys yra 25.

13. Išspręskite lygtį natūraliaisiais skaičiais: $x^2 + y^2 = 2023$.

14. Suraskite visus tokius natūraliuosius skaičius m ir n, kad $n \mid 2m-1$ ir $m \mid 2n-1$.

3 Pirminiai ir sudėtiniai skaičiai

3.1 Teorija

Apibrėžimas. Skaičius, kuris dalinasi tik iš vieneto ir savęs, vadinamas *pirminiu*. Vienetas nėra laikomas pirminiu.

Apibrėžimas. Skaičius, kuris be vieneto ir savęs, turi kitų daliklių, vadinamas *sudėtiniu*.

Teiginys. Kiekvieną skaičių n galima vieninteliu būdu išskaidyti pirminiais dauginamaisiais:

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}.$$

Mažus skaičius skaidyti pirminiais dauginamaisiais nesunku – tiesiog iš eilės tikriname pirminius skaičius ir skaičiuojame, kiek kartų iš jų galima padalinti. Pavyzdžiui,

$$120 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 = 2^3 \cdot 3 \cdot 5.$$

Teiginys. Jei skaičius n dalijasi iš skaičiaus a ir

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k},$$

tai tuomet

$$a = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$$

ir

$$b_i \leq a_i$$

su visais $i = 1, \ldots, k$.

Įrodymas: Jei n dalijasi iš a, tai tuomet egzistuoja toks sveikasis skaičius b, kad $n = ab$. Skaičių n sudarys skaičių a ir b pirminiai, todėl į n pirminius įeis visi a pirminiai su nemažesniais laipsnių rodikliais.

Teiginys. Skaičius $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ turi $(a_1 + 1)(a_2 + 1) \cdots (a_k + 1)$ daliklių.

Įrodymas: Kiekvienas n daliklis bus užrašomas kaip $p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$, kur $b_i \leq a_i$ su visais $i = 1, \ldots, k$. Skirtingus daliklius gausime imdami skirtingus pirminių skaičių laipsnius. Parinkti b_i galime $a_i + 1$ būdais (nepamirškime nulio!), todėl iš viso galėsime sudaryti $(a_1 + 1)(a_2 + 1) \cdots (a_k + 1)$ skirtingų laipsnių rinkinių, todėl tiek bus ir skirtingų daliklių.

Laikas naujam įrodymo būdui! Jis veikia labai paprastai, jeigu mums reikia įrodyti, kad galioja P, tai mes tarsime, jog P negalioja ir iš to darysim išvadas. Jeigu išvados yra nesąmoningos, tai P privalo galioti (čia P tai koks nors faktas, teorema ar savybė).

Teorema. Pirminių skaičių yra be galo daug.

Įrodymas: Tarkime priešingai, kad pirminių skaičių yra baigtinis skaičius. Sudauginkime juos visus ir pridėkime vienetą: $p_1 p_2 \cdots p_n + 1$. Šis skaičius nesidalija iš nė vieno pirminio $p_1, \ldots, p_n$, todėl pats yra pirminis. Gavome naują pirminį - prieštara.

Tokį įrodymo būdą vadinsime prieštaros metodu.

Teiginys. Jei skaičius n nesidalija iš jokio pirminio skaičiaus, mažesnio (arba lygaus) už $\sqrt{n}$, tai jis pirminis.

Įrodymas: Tarkime priešingai, kad skaičius n nesidalija iš jokio pirminio skaičiaus, mažesnio (arba lygaus) už $\sqrt{n}$, bet jis turi daliklį $a > \sqrt{n}$, tai $n = a \cdot b$, $b < \sqrt{n}$ ir $b | n$, todėl gauname prieštarą. Tai reiškia, kad skaičius n neturės kitų daliklių, todėl bus pirminis.

3.2 Uždaviniai

1. Raskite visus pirminius skaičius iš intervalo [180, 200].

2. Su kuriomis natūraliosiomis n reikšmėmis skaičius $n^2 + 5n + 6$ pirminis?

3. Įrodykite, kad skaičius turi nelyginį daliklių skaičių tada ir tik tada, kai jis yra sveikojo skaičiaus kvadratas.

4. Duotas pirminis skaičius p didesnis už 3. Įrodykite, jog p skiriasi per 1 nuo 6 kartotinio.

5. Tarkime $n > 4$ yra sudėtinis skaičius. Įrodykite, kad $n|(n-1)!$.

6. Duotas pirminis skaičius p ir du natūralieji skaičiai m ir n. Įrodykite, kad $p < m$, jei $p^2 + m^2 = n^2$.

7. Duoti natūralieji skaičiai n ir r. Tarkime kad

$$1 + 2 + ... + (n-1) = (n+1) + (n+2) + ... + (n+r)$$

Įrodykite, kad n yra sudėtinis.

8. Duotas nelyginis skaičius $n > 3$. Tegul $M = n^2 + 2n - 7$. Įrodykite, kad M turi bent 6 daliklius.

9. Suraskite mažiausiąjį tokį natūralųjį n, kad n turėtų lygiai 24 daliklius.

10. Įrodykite, jog bet kokiam natūraliajam n egzistuoja n iš eilės einančių natūraliųjų, kurie visi yra sudėtiniai.

11. Raskite visus pirminius skaičius p ir q, tenkinančius $p|q+6$ ir $q|p+7$.