Skaičių teorijos pradmenys
II dalis
Ir pirminio skaičiaus daliklių dingimo paslaptis!

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

2024/11/05

4 DBD ir MBK

4.1 Teorija

Dvi iš svarbiausių funkcijų skaičių teorijoje yra dbd (didžiausias bendras daliklis) ir mbk (mažiausias bendras kartotinis), nors uždavinių olimpiadose su jomis būna retai, tačiau jos vis tiek praverčia sprendžiant ir įrodinėjant kitus skaičių teorijos uždavinius.

Apibrėžimas. Dviejų ar daugiau skaičių *didžiausiuoju bendru dalikliu* (dbd) vadinsime didžiausią skaičių, iš kurio visi duotieji dalinasi.

Apibrėžimas. Dviejų ar daugiau skaičių *mažiausiuoju bendru kartotiniu* (mbk) vadinsime mažiausią skaičių, kuris dalijasi iš visų duotųjų.

Apibrėžimas. Du skaičius, kurių didžiausiasis bendras daliklis yra lygus 1, vadinsime *tarpusavyje pirminiais.*

Pavyzdys. Raskite skaičių 30 ir 48 didžiausią bendrą daliklį ir mažiausią bendrą kartotinį.

Sprendimas: Ieškant didžiausiojo bendro daliklio ir mažiausiojo bendro kartotinio labai praverčia skaidymas pirminiais dalikliais. $30 = 2 \cdot 3 \cdot 5$, $48 = 2^4 \cdot 3$. Norėdami rasti didžiausią bendrą daliklį turime paimti visus pirminius daliklius, priklausančius abiems skaičiams. Šiuo atveju tai būtų $2 \cdot 3$. Rezultatas užrašomas taip: dbd(30, 48) $= 6$. Norėdami rasti mažiausią bendrą kartotinį, turime paimti kiek įmanoma mažiau pirminių daliklių taip, kad jų būtų nemažiau nei abiejuose skaičiuose atskirai. Šiuo atveju tai būtų $2^4 \cdot 3 \cdot 5$. Rezultatas užrašomas taip: mbk(30, 48) $= 240$.

Teiginys. $\text{dbd}(a,\, b) = \text{dbd}(a - b,\, b)$.

Įrodymas: Tegu $\text{dbd}(a,\, b) = d$. Tuomet $d \mid a$ ir $d \mid b$, o kartu $d \mid (a - b)$. Vadinasi, $\text{dbd}(a - b,\, b)$ bus nemažesnis nei d. Iš kitos pusės – tegu $\text{dbd}(a - b,\, b) = d'$. Kartu $d' \mid (a - b)$ ir $d' \mid b$, o tuo pačiu $d' \mid a$, nes $a = (a - b) + b$. Vadinasi, $\text{dbd}(a,\, b)$ bus nemažesnis nei d'. Kadangi gavome $d \geq d'$ ir $d' \geq d$, tai vadinasi $d = d'$, t.y. $\text{dbd}(a,\, b) = \text{dbd}(a - b,\, b)$.

Pavyzdys. Pasinaudodami įrodyta lygybe raskime $\text{dbd}(2^{100} + 1,\, 2^{100} - 1)$

Sprendimas: $\text{dbd}(2^{100} + 1,\, 2^{100} - 1) = \text{dbd}(2,\, 2^{100} - 1) = \text{dbd}(2,\, 1) = 1$.

Pavyzdys. [IMO 1959] Įrodykite, kad trupmena $\frac{21n+4}{14n+3}$ yra nesuprastinama su visomis natūraliosiomis n reikšmėmis.

Sprendimas: Trupmena bus nesuprastinama, jei didžiausias skaitiklio ir vardiklio bendras daliklis bus lygus vienam. Pasinaudoję $\text{dbd}(a,\, b) = \text{dbd}(a,\, b - a)$ gauname: $\text{dbd}(21n + 4,\, 14n + 3) = \text{dbd}(7n + 1,\, 14n + 3) = \text{dbd}(7n + 1, 7n0 + 2) = \text{dbd}(7n + 1,\, 1) = 1$.

Euklido algoritmas. Rasime $\text{dbd}(a,\, b)$. Nemažindami bendrumo tarkime, kad $a \geq b$. Remiantis dalumo su liekana teorema:
$a = bq_1 + r_1$, kur $0 < r_1 < b$
$b = r_1 q_2 + r_2$, kur $0 < r_2 < r_1$
$r_1 = r_2 q_3 + r_3$, kur $0 < r_3 < r_2$
$\ldots$
$r_{k-2} = r_{k-1} q_k + r_k$, kur $0 < r_k < r_{k-1}$
$r_{k-1} = r_k q_{k+1}$
Iš $r_1 > r_2 > \ldots > r_k$ seka, kad kažkada gausime dalybos liekaną lygią 0. Tuomet, kadangi $\text{dbd}(a,\, b) = \text{dbd}(b,\, r) = \ldots = \text{dbd}(r_{k-2},\, r_{k-1}) = \text{dbd}(r_{k-1},\, r_k)$, tai paskutinioji nenulinė liekana r_k ir bus didžiausias bendrasis daliklis, $\text{dbd}(a,\, b) = r_k$.

Šis algoritmas dažnai naudojamas informatikoje, o matematikoje $-$ rečiau, dažniausiai užtenka kelis kartus pasinaudoti savybe $\text{dbd}(a,\, b) = \text{dbd}(a,\, b - a)$. Tačiau mums svarbi šio algoritmo išvada.

Euklido algoritmo išvada. Jei $\text{dbd}(a,\, b) = d$, tai egzistuoja tokie $x, y \in \mathbb{Z}$, kad $ax + by = d$.

Įrodymas: Iš priešpaskutinės Euklido algoritmo lygybės galime išreikšti r_k per r_{k-1} ir r_{k-2}. Iš dar ankstesnės galima išreikšti r_{k-1} per r_{k-2} ir r_{k-3}. Įstatę į pirmąją išraišką gausime r_k išraišką per r_{k-2} ir r_{k-3}. Taip toliau vis tęsdami gausime r_k išraišką per a, b, t.y. rasime x, y, tenkinančius $ax + by = \text{dbd}(a,\, b)$.

Pavyzdys. Kokius skaičius galime išreikšti suma $8x + 5y$, kur $x, y \in \mathbb{Z}$?

Sprendimas: Pagal Euklido algoritmo išvadą tokiu būdu galima išreikšti $\mathrm{dbd}(8, 5) = 1$, todėl bet kokį skaičių n galima išreikšti vietoje x ir y, naudojamų vieneto išraiškoje, imant nx ir ny.

4.2 Uždaviniai

1. Tarkime a ir b yra natūralūs skaičiai, o $\mathrm{dbd}(a, b) = d$. Įrodykite šias savybes:

(a) Jei $a \mid b$, tai $d = a$.

(b) Jei $d = a$, tai $a \mid b$.

(c) $\mathrm{dbd}(\frac{a}{d}, \frac{b}{d}) = 1$.

(d) $\mathrm{dbd}(an, bn) = dn$ galioja su visais natūraliaisiais n.

2. Tegul a, b, x, y bet kokie sveikieji skaičiai tenkinantys lygtį: $ax + by = n$. Įrodykite, kad $\mathrm{dbd}(a, b)| \; n$

3. Tarkime a, b ir c yra natūralūs skaičiai. Įrodykite, kad, jei $a \mid bc$ ir $\mathrm{dbd}(a, b) = 1$, tai $a \mid c$.

4. Tarkime a, b ir c yra natūralūs skaičiai. Įrodykite, kad, jei $\mathrm{dbd}(a, b) = 1$ ir $\mathrm{dbd}(a, c) = 1$, $\mathrm{dbd}(a, bc) = 1$.

5. Tarkime p yra pirminis skaičius. Įrodykite šias savybes:

(a) $\mathrm{dbd}(a, p) = 1$ arba p su visais natūraliaisiais a.

(b) Jei $p \mid ab$, tai $p \mid a$ ir/arba $p \mid b$ galioja visiems natūraliesiems a ir b.

(c) Jei $p \mid a^2$, tai $p \mid a$ galioja su visais natūraliaisiais a.

6. Tarkime a ir b yra tarpusavyje pirminiai. Įrodykite, kad, jei $a \mid c$ ir $b \mid c$, tai $ab \mid c$.

7. Įrodykite, kad $\mathrm{mbk}(a, b) \cdot \mathrm{dbd}(a, b) = a \cdot b$

8. $\mathrm{dbd}(a, b) = 12$, o $\mathrm{mbk}(a, b) = 360$, raskite a ir b.

9. Duota, kad trupmena $\frac{a}{b}$ yra suprastinama. Ar trupmena $\frac{a-b}{a+b}$ būtinai yra suprastinama? Ir atvirkščiai, jei žinoma, kad trupmena $\frac{a-b}{a+b}$ yra suprastinama, ar trupmena $\frac{a}{b}$ būtinai yra suprastinama?

10. Kiek yra sveikųjų skaičių $1 \leq n \leq 100$, kad $\mathrm{dbd}(n^2 + 1, n + 1) > 1$?

11. Kiek yra sveikųjų skaičių $1 \leq n \leq 100$, kad $\mathrm{dbd}(n^2 + 1, n + 2) > 1$?

12. Jei natūralieji skaičiai a ir b yra tarpusavyje pirminiai, tai $\mathrm{dbd}(a+b, a^2+b^2) = 1$ arba 2.

13. Raskite su kuriomis n reikšmėmis galioja $\mathrm{dbd}(n^2+3n+1, n^2-n+1) > 1$.

13*. Įrodykite, kad reiškinys

$$\frac{\mathrm{dbd}(m,n)}{n}\binom{n}{m}$$

yra natūralusis skaičius, kai $n \geq m \geq 1$

5 Lyginiai

5.1 Teorija

Praeituose skyriuose mes naudojoje du būdus užrašyti skaičių dalumus, vienas iš jų buvo algebrinis ($a = kb$), o kitas buvo per "brūkšnį" ($a \mid b$). Dabar laikas išmokti trečiąjį būdą, kuris ypač naudingas dirbant su skaičių liekanomis.

Apibrėžimas. Jeigu $m \mid a-b$, tai tada sakysime, jog "a lygsta b moduliu m" ir tai užrašysime, kaip $a \equiv b \pmod{m}$, čia $a, b, m \in \mathbb{Z}, m \neq 0$. Tai galioja ir atvirkščiai, jeigu $a \equiv b \pmod{m}$, tai tada $m \mid a-b$.

Pastaba. Užrašas $a \bmod m$, yra lygus liekanai gautai a dalijanti iš m.

Pastaba. Toliau naudosimės tam tikrais matematiniais ženklais. Jeigu galioja P, o tai reiškia, jog galioja ir Q žymėsime: $P \implies Q$, o jeigu P galioja tada ir tik tada, kai galioja Q: $P \iff Q$. Taip pat svarbu žinoti, jog jeigu jūsų prašo įrodyti, kad P galioja tada ir tik tada, kai galioja Q, tai jūs privalote įrodymą skaldyti į du atvejus: pirmu atveju įrodot, kad $P \implies Q$, o antru, jog $Q \implies P$.

Lyginių savybės (jas olimpiadose galima naudoti be įrodymo):

1 Savybė. $a \equiv b \pmod{m}$ tada ir tik tada, kai a dalijant iš m ir b dalijant iš m gauname vienodas liekanas.

Įrodymas: Įrodymą skaldome į du atvejus, pirmu įrodysime, jog a ir b dalijant iš m gauname vienodas liekanas $\implies a \equiv b \pmod{m}$, o antru: $a \equiv b \pmod{m} \implies a$ ir b dalijant iš m gauname vienodas liekanas.

1 atvejis: Kadangi a ir b dalijant iš m gauname vienodas liekanas, tai pagal dalybos su liekana teoremą gauname: $a = mq_1 + r$, $b = mq_2 + r$, tada $a - b = mq_1 + r - mq_2 - r = mq_1 - mq_2 = m(q_1 - q_2)$, kas reiškia, jog $m \mid a - b$, o iš to seka, jog $a \equiv b \pmod{m}$.

2 atvejis: Iš sąlygos $a \equiv b \pmod{m}$ gauname, jog $m \mid a - b$. Taikome dalybos su liekana teoremą: $a = mq_1 + r_1$, $b = mq_2 + r_2$. Iš to gauname, kad $m \mid mq_1 + r_1 - mq_2 - r_2 \implies m \mid r_1 - r_2$. Kadangi $0 \leqslant r_1, r_2 \leqslant m - 1$, tai reiškia, jog $0 \leqslant |r_1 - r_2| \leqslant m - 1$, bet taip pat $m \mid r_1 - r_2$, todėl galima teigti, jog $r_1 - r_2 = 0$ arba $r_1 = r_2$, kas reiškia, jog a ir b dalijant iš m gauname vienodas liekanas.

2 Savybė. Jeigu $a \equiv b \pmod{m}$ ir $b \equiv c \pmod{m}$, tai tada $a \equiv c \pmod{m}$.

Įrodymas: Pasinaudokime 1 savybe, turime $a \equiv b \pmod{m}$, vadinasi a ir b dalijant iš m gauname vienodas liekanas, tačiau taip pat turime $b \equiv c \pmod{m}$, vadinasi b ir c dalijant iš m gauname vienodas liekanas. Kadangi a, b ir c dalijant iš m gauname vienodas liekanas, tai $a \equiv c \pmod{m}$.

3 Savybė. $a \equiv b \pmod{m}$ tada ir tik tada, kai egzistuoja toks $k \in \mathbb{Z}$, kad $a = b + km$.

Įrodymas: Įrodymą ir vėl turime padalyti į du atvejus. Pirmu atveju įrodysime $a \equiv b \pmod{m} \implies a = b + km$, kažkokiam sveikam k. O antru įrodysime, kad jei $a = b + km \implies a \equiv b \pmod{m}$

1 atvejis: Kadangi $a \equiv b \pmod{m}$, tai reiškia, jog $m \mid a - b$, o iš to seka, jog $a - b = mk \implies a = b + km$ ką ir reikėjo įrodyti.

2 atvejis: Kadangi $a = b + km$, tai $a - b = km$, kas reiškia, jog $m \mid a - b$, o iš to seka, jog $a \equiv b \pmod{m}$

4 Savybė. Jeigu $a \equiv b \pmod{m}$ ir $c \equiv d \pmod{m}$, tai tada $a + c \equiv b + d \pmod{m}$.

Įrodymas: Kadangi $a \equiv b \pmod{m}$ ir $c \equiv d \pmod{m}$, tai galime pasinaudoti 3 lyginių savybe: $a = b + k_1m$ ir $c = d + k_2m$, tada $a + c = b + k_1m + d + k_2m = (b + d) + m(k_1 + k_2)$, ir vėl pagal 3 savybę galima teigti, jog $a + c \equiv b + d \pmod{m}$.

5 Savybė. Jeigu $a \equiv b \pmod{m}$ ir $c \equiv d \pmod{m}$, tai tada $a - c \equiv b - d \pmod{m}$.

6 Savybė. Jeigu $a \equiv b \pmod{m}$ ir $c \equiv d \pmod{m}$, tai tada $a \cdot c \equiv b \cdot d \pmod{m}$.

7 Savybė. Jeigu $a \equiv b \pmod{m}$, tai tada $a^k \equiv b^k \pmod{m}$ su visais $k \in \mathbb{N}$.

Kaip matome lyginių aritmetika yra beveik tokia pati kaip ir paprastoji aritmetika. Sudėtis, atimtis, daugyba, kėlimas laipsniu yra daroma lygiai taip pat. Tačiau išsiskiriant nuo paprastosios aritmetikos lyginiai turi papildomų savybių (1,2) ir su jais galima žymiai daugiau ką nuveikti. Galime sakyti, jog lyginiai yra paprastoji aritmetika "ant steroidų" :). Nepaisant to mums iškyla vienas pavojus ir jis yra, tai kad reikia **LABAI ATSARGIAI** lyginius dalinti!

8 Savybė. Jeigu $ak \equiv bk \pmod{m}$ ir $dbd(k, m) = 1$, tai tada $a \equiv b \pmod{m}$.

Dalumo požymiai

Užrašę skaičių dešimtainėje sistemoje $\overline{a_1a_2...a_n}$, iš jo skaitmenų galime spręsti, ar jis dalijasi iš kai kurių mažų skaičių, ar ne. Naudingiausi dalumo požymiai yra šie:

1 Požymis. Skaičius dalijasi iš 2, jeigu jo paskutinis skaitmuo dalijasi iš 2.

Įrodymas: Išskleidę skaičių $\overline{a_1a_2...a_n}$ gauname $a_1 \cdot 10^{n-1} + a_2 \cdot 10^{n-2} + ... + a_{n-1} \cdot 10 + a_n \equiv a_1 \cdot 0 + a_2 \cdot 0 + ... + a_{n-1} \cdot 0 + a_n \equiv a_n \pmod{2}$

2 Požymis. Skaičius dalijasi iš 3, jeigu jo skaitmenų suma dalijasi iš 3.

Įrodymas: Išskleidę skaičių $\overline{a_1a_2...a_n}$ gauname $a_1 \cdot 10^{n-1} + a_2 \cdot 10^{n-2} + ... + a_{n-1} \cdot 10 + a_n \equiv a_1 + a_2 + ... + a_{n-1} + a_n \pmod{3}$, kadangi $10^k \equiv 1^k = 1 \pmod{3}$. Vadinasi jeigu skaitmenų suma dalinsis iš 3, tai tada ir skaičius dalinsis iš 3 (nes liekanos lygios dalijant iš 3).

3 Požymis. Skaičius dalijasi iš 4, jeigu skaičius sudarytas iš dviejų paskutinių skaitmenų $\overline{a_{n-1}a_n}$ dalijasi iš 4.

4 Požymis. Skaičius dalijasi iš 5, jeigu jo paskutinis skaitmuo dalijasi iš 5.

5 Požymis. Skaičius dalijasi iš 8, jeigu skaičius sudarytas iš trijų paskutinių skaitmenų $\overline{a_{n-2}a_{n-1}a_n}$ dalijasi iš 8.

6 Požymis. Skaičius dalijasi iš 9, jeigu jo skaitmenų suma dalijasi iš 9.

7 Požymis. Skaičius dalijasi iš 11, jeigu jo alternuojanti skaitmenų suma $a_1 - a_2 + a_3 - a_4 + ... \pm a_n$ dalijasi iš 11.

Įrodymas: Kadangi $10^k \equiv (-1)^k \pmod{11}$, tai tada skaičius $\overline{a_1a_2...a_n} = a_1 \cdot 10^{n-1} + a_2 \cdot 10^{n-2} + ... + a_{n-1} \cdot 10 + a_n \equiv (-1)^{n-1} \cdot a_1 + (-1)^{n-2} \cdot a_2 + ... - a_{n-1} + a_n \pmod{11}$.

1 Pavyzdys Tegul $a > b > c$ yra natūralieji skaičiai. Jų liekanos dalijant iš 11 yra atitinkamai 2,7 ir 9. Raskite $(a + b + c)(a - b)(b - c) \bmod 11$.

Sprendimas: Kadangi $a \equiv 2 \pmod{11}$, $b \equiv 7 \pmod{11}$ ir $c \equiv 9 \pmod{11}$, tai tada $(a+b+c)(a-b)(b-c) \equiv (2+7+9) \cdot (2-7) \cdot (7-9) \equiv 18 \cdot (-5) \cdot (-2) = 180 \equiv 4 \pmod{11}$.

2 Pavyzdys Įrašykite, vietoj žvaigždučių tokius skaitmenis, kad 15**15 dalintųsi iš 99.

Sprendimas: Pažymėkime praleistus skaitmenis a ir b atitinkamai. Kadangi skaičius dalijasi iš 99, tai jis dalinsis iš 9 ir iš 11. Pritaikome dalumo požymius ir gauname, jog $9 \mid 1{+}5{+}a{+}b{+}1{+}5 \implies 9 \mid 3{+}a{+}b$ ir $11 \mid 1{-}5{+}a{-}b{+}1{-}5 \implies 11 \mid a{-}b{-}8$. Ranka patikrinę visus atvejus gauname, jog $a = 6, b = 9$.

3 Pavyzdys Įrodykite, jog $n^k \equiv n \pmod 3$ galioja bet kokiam nelyginiam k.

Įrodymas: Ir vėl pasinaudosime įrodymu su atvejais. Kadangi dalijam iš trijų tai galim turėti 3 liekanas (0,1,2).
1 atvejis: $x \equiv 0 \pmod 3 \implies x^k \equiv 0^k = 0 \equiv x \pmod 3$.
2 atvejis: $x \equiv 1 \pmod 3 \implies x^k \equiv 1^k = 1 \equiv x \pmod 3$.
3 atvejis: $x \equiv 2 \equiv -1 \pmod 3 \implies x^k \equiv (-1)^k = -1 \equiv x \pmod 3$, nes k yra nelyginis.

Toks išskaidymas atvejais ir nagrinėjimas skirtingomis liekanomis yra labai naudingas ir dažnai pasitaikantis uždavinių sprendimo būdas (pvz. VU MIF 2024 10kl. U4)

Apačioje pateikti keli skirtingi būdai kuriais galima surasti skaičiaus liekaną dalijant iš kito skaičiaus. Priklausomai nuo užduoties naudoti reikia skirtingą būdą, todėl vertėtų visus juos žinoti.

4 Pavyzdys Raskite, kokią liekaną gauname 2^{1000} dalindami iš 11.

Sprendimas: Uždavinį galima išspręsti keliais būdais, tačiau pasinaudokime tuo, kad $2^5 = 32 \equiv -1 \pmod{11}$. Tada $2^{1000} = (2^5)^{200} \equiv (-1)^{200} = 1 \pmod{11}$.

5 Pavyzdys Raskite $3^{17} \bmod 100$.

Sprendimas: $3^{17} = (3^4)^4 \cdot 3 \equiv (-19)^4 \cdot 3 \equiv (19^2)^2 \cdot 3 = 361^2 \cdot 3 \equiv (-39)^2 \cdot 3 \equiv 21 \cdot 3 = 63 \pmod{100}$.

6 Pavyzdys Raskite paskutinį skaičiaus 7^{2024} skaitmenį.

Sprendimas: Rasti paskutinį skaičiaus skaitmenį yra tas pats, kaip surasti to skaičiaus liekaną dalinant iš 10 (tą nesunku pastebėti pasinaudojus skaičiaus išskleidimu, kurį naudojame, kad įrodytume skaičių dalumo požymius). Pradėkime užrašydami keletą pirmų septyneto laipsnių mod 10:
$7^1 = 7 \pmod{10}$
$7^2 = 49 \equiv 9 \pmod{10}$
$7^3 = 7 \cdot 7^2 \equiv 7 \cdot 9 = 63 \equiv 3 \pmod{10}$
$7^4 = 7 \cdot 7^3 \equiv 21 \equiv 1 \pmod{10}$
Toliau tęsdami gauname:

$7^5 \equiv 7 \pmod{10}$
$7^6 \equiv 9 \pmod{10}$
$7^7 \equiv 3 \pmod{10}$
$7^8 \equiv 1 \pmod{10}$
Nesunku pastebėti, jog septyneto laipsnių liekanos kartojas periodiškai (kas keturis), kadangi $4 \mid 2024$, tai vadinasi $7^{2024} \equiv 7^4 \equiv 1 \pmod{10}$.

5.2 Uždaviniai

1. Įrodykite, kad $a \equiv 0 \pmod{m} \iff m \mid a$.
2. Įrodykite, kad $a + n \equiv a \equiv a - n \pmod{n}$.
3. Raskite liekanas gaunamas dalijant a) $1 + 11 + 111 + 1111 + 11111$ iš 9; b) $555 \cdot 777 + 666 \cdot 888$ iš 9; c) 3^{99} iš 2,3,4,5,6 ir 7; d) 7^{777} iš 10; e) 3^{302} iš 28 f) $3^{2017} + 4^{2017}$ mod 5 g) 8^{88} mod 100.
4. Tegul $17! = 355687ab8096000$, kur a, b yra nežinomi skaitmenys. Raskite a ir b nenaudodami skaičiuotuvų.
5. Įrodykite, kad $ab + cd \equiv ad + bc \pmod{a - c}$.
6. Įrodykite, kad $3 \mid 4^n - 1$, visiems natūraliesiems n.
7. Įrodykite, kad $n^3 - n$ dalijasi iš 6 su visomis sveikosiomis n reikšmėmis.
8. Duoti $a, b, c, d \in \mathbb{N}$, kurie tenkina: $a+b+c+d = 2017$. Įrodykite, kad $a+b+c+d$ yra visada nelyginis.
9. Tegul a ir b yra natūralieji skaičiai, o r yra nenulinė liekana, kai b dalijamas iš a. Įrodykite, jog $-b$ dalijant iš a liekana yra $a - r$.
10. Duoti sveikieji skaičiai a, b, c, kurie tenkina: $a + b + c = 0$. Įrodyti, kad $6 \mid a^{2017} + b^{2017} + c^{2017}$.
11. Įrodykite, kad bet kokiam natūraliajam n galioja: $n^5 \equiv n \pmod{10}$.
12. Įrodykite, kad jei $n \mid a^2 + b^2$, tai $n \mid a$ ir $n \mid b$, kai a) $n = 3$; b) $n = 7$.
13. Duotas nelyginis natūralusis n. Įrodyti, kad $n^2 \equiv 1 \pmod{8}$.
14. Skaičius a nesidalija iš 2 ir 3. Įrodyti, kad $a^2 \equiv 1 \pmod{24}$.
15. Įrodykite, kad skaičiaus ir jo skaitmenų sumos dalybos iš 9 liekanos sutampa.
16. Įrodykite, kad dviejų nelyginių skaičių kvadratų suma negali būti kvadratas.

17. Raskite visus pirminius p ir q tenkinančius lygybę: $p^2 - 2q^2 = 1$.

18. Įrodykite, kad $n^2 + 3n + 5$ nesidalija iš 121 su visomis sveikomis n reikšmėmis.

19. Įrodykite, kad jei $a \equiv b \pmod{n}$, tai tada $\mathrm{dbd}(a, n) = \mathrm{dbd}(b, n)$.

20. [LKMMO 2002] Įrodykite, kad $10^n + 45n - 1 \equiv 0 \pmod{27}$.

21. [VU MIF 2024] Su kuriuo natūraliuoju n natūraliųjų skaičių nuo 1 iki n sumos paskutiniai keturi skaitmenys yra 2024?