

1 Pirminiai skaičiai

- 1.1. Raskite didžiausią bendrą daliklį $\text{dbd}(455, 1235)$.
- 1.2. Naudodami Eratosteno rėtį raskite visus pirminius skaičius mažesnius už 100.

1.3. Įrodykite, kad aritmetinėje progresijoje $6x - 1$ yra be galo daug pirminių skaičių.

1.4. Įrodykite, kad $\lim_{x \rightarrow \infty} \frac{\pi(x)}{x} = 0$.

1.5. Tarkime a, b, c, n yra sveikieji skaičiai. Įrodykite, kad

(a) jei $\text{dbd}(a, b) = 1$, $a \mid n$ ir $b \mid n$, tai $ab \mid n$.

(b) jei $a \mid bc$ ir $\text{dbd}(a, b) = 1$, tai $a \mid c$.

1.6. Tarkime a, b, c, d ir m yra sveikieji skaičiai. Įrodykite, kad

(a) jei $a \mid b$ ir $b \mid c$, tai $a \mid c$.

(b) jei $a \mid b$ ir $c \mid d$, tai $ac \mid bd$.

(c) jei $m \neq 0$, tai $a \mid b$ tada ir tik tada, kai $ma \mid mb$.

(d) jei $d \mid a$ ir $a \neq 0$, tai $|d| \leq |a|$.

1.7. Naudodami dalybos algoritmą, raskite tokius q ir r , kad $a = bq + r$ ir $0 \leq r < |b|$:

$$\begin{aligned} a &= 300, b = 17, \\ a &= 729, b = 31, \\ a &= 300, b = -17, \\ a &= 389, b = 4. \end{aligned}$$

1.8. Raskite skaičių 323 ir 437 didžiausią bendrą daliklį naudodami Euklido algoritmą.

1.9. (a) Tarkime, kad a, b ir n yra natūralieji skaičiai. Įrodykite, kad jei $a^n \mid b^n$, tai $a \mid b$.

(b) Tarkime, kad p yra pirminis skaičius, o a ir k yra natūralieji skaičiai. Įrodykite, kad jei $p \mid a^k$, tai $p^k \mid a^k$.

1.10. (a) Įrodykite, kad jei natūralusis skaičius n yra pilnas kvadratas, tai n negali būti užrašytas kaip $4k + 3$ ($k \in \mathbb{N}$).

(b) Įrodykite, kad joks sekos

$$11, 111, 1111, 11111, 111111, \dots$$

narys nėra pilnas kvadratas.

1.11. Įrodykite, kad natūralusis skaičius n yra pirminis skaičius tada ir tik tada, kai n nesidalija iš jokio pirminio skaičiaus mažesnio už \sqrt{n} .

1.12. Raskite 1000 dalybos iš 7 liekaną.

1.13. Raskite kiek yra skaičių, kurių

- vienas iš daliklių yra 3 ir vienas iš kartotinių yra 30?
- vienas iš daliklių yra 3 ir vienas iš kartotinių yra 31?

1.14. Raskite bent vieną skaičių, kuris yra 3, 4, 5 ir 6 kartotinis. Kiek tokių skaičių yra?

1.15. Kiek yra skaičių nuo 1 iki 1000, besidalijančių iš 13?

1.16. Įrodykite, kad bet kaip sudėliojus devynis skaitmenis $1, 2, \dots, 9$, gautas devynženklis skaičius dalinsis iš 9.

1.17. Įrašykite žvaigžducių vietoje tokius skaitmenis, kad skaičius $15 * * 15$ dalytųsi iš 99.

- 1.18. Tegu a yra b kartotinis. Ar tiesa, kad bet kuris a daliklis yra ir b daliklis? O atvirkščiai, ar bet kuris b daliklis yra ir a daliklis?
- 1.19. Ar skaičius, kurio skaitmenų suma lygi 5, gali dalintis iš 11?
- 1.20. Įrodykite, kad skaičiaus, kuris dalijasi iš 99, skaitmenų suma yra ne mažesnė už 18.
- 1.21. Raskite bent vieną n , kad intervale $[n, n+10]$ nebūtų nė vieno pirminio skaičiaus.
- 1.22. Duotas 100-ženklis skaičius a , kuris dalijasi iš 9. Žinome, kad b yra a skaitmenų suma, c yra b skaitmenų suma, d yra c skaitmenų suma. Kam lygus skaičius d ?
- 1.23. Nurodykite kokį nors skaičiaus $n = 27^{28} + 4$ daliklį skirtingą nuo 1 ir paties n .
- 1.24. Raskite visus n , su kuriais $n^2 + 1$ dalijasi iš $n + 1$.
- 1.25. Kokius skaičius galime išreikšti suma $8x + 5y$, kur $x, y \in \mathbb{Z}$?
- 1.26. Raskite visus sveikuosius n , su kuriais skaičius $\frac{n^3+3}{n^2+7}$ yra sveikasis.
- 1.27. Duota, kad $11|3x + 7y$ ir $11|2x + 5y$. Įrodykite, kad $121|x^2 + 3y^2$.
- 1.28. Samprotaudami panašiai kaip įrodyme, kad pirminių skaičių yra be galo daug, įrodykite, kad pirminių skaičių pavidalo $4k + 3$ yra be galo daug.
- 1.29. Raskite visus pirminius skaičius p ir q , tenkinančius $p|q + 6$ ir $q|p + 7$.
- 1.30. Įrodykite, kad $\underbrace{11 \cdots 1}_{3^n}$ dalijasi iš 3^n .
- 1.31. Tegu $n \geq 2$ natūralusis skaičius, kurio dalikliai yra $1 = d_1 < d_2 < \cdots < d_k = n$. Įrodykite, kad $d_1d_2 + d_2d_3 + \cdots + d_{k-1}d_k$ yra visuomet mažesnis už n^2 , ir raskite, kada jis yra n^2 daliklis.
- 1.32. Raskite didžiausią bendrąjį skaičių 1234 ir 5678 daliklį.
- 1.33. Raskite sveikuosius x, y , tenkinančius $182x + 413y = 7$.
- 1.34. Raskite tris skaičius, kurie neturi bendro daliklio, tačiau nėra tarpusavyje pirminiai imant po du.
- 1.35. Įrodykite, kad jei $\text{dbd}(a, b) = \text{mbk}(a, b)$, tai $a = b$.
- 1.36. Tegu $a|b$. Kam lygūs $\text{dbd}(a, b)$ ir $\text{mbk}(a, b)$?
- 1.37. Raskite $\text{dbd}(n, n + 1)$ ir $\text{mbk}(n, n + 1)$.
- 1.38. Tegu $(a, b) = 1$. Įrodykite, kad $(a + b, a - b)$ lygus 1 arba 2.
- 1.39. Ar teisingi šie teiginiai:
- (a) Jei $\text{dbd}(a, b) = \text{dbd}(a, c)$, tai $\text{mbk}(a, b) = \text{mbk}(a, c)$,
 - (b) Jei $(a, b) = (a, c)$, tai $(a^2, b^2) = (a^2, c^2)$,
 - (c) Jei $(a, b) = (b, c)$, tai $(a, b) = (a, b, c)$,
 - (d) $\text{mbk}(a^2, b^2) = \text{mbk}(a^2, ab, b^2)$,
 - (e) $(a, b, c) = ((a, b), (b, c))$?
- 1.40. Įrodykite, kad $(a, a + k)|k$.
- 1.41. Įrodykite, kad $\text{mbk}(a, b) \cdot \text{dbd}(a, b) = ab$.
- 1.42. Raskite visus trejetus a, b, c , kurie tenkina $(a, b, c) = 10$ ir $\text{mbk}(a, b, c) = 100$.

- 1.43. Ar teisinga lygybė $\text{mbd}(a, b, c) \cdot \text{dbd}(a, b, c) = abc$?
- 1.44. Tegū a, b, c sveikieji. Įrodykite, kad lygtis $ax + by = c$ turi sveikųjų sprendinių tada ir tik tada, kai $(a, b) | c$.
- 1.45. Kiek yra sveikųjų skaičių $1 \leq n \leq 100$, kad
- (a) $\text{dbd}(n^2 + 1, n + 1) > 1$,
(b) $\text{dbd}(n^2 + 1, n + 2) > 1$?
- 1.46. Įrodykite, kad $a | bc$ tada ir tada, kai $\frac{a}{(a, b)} | c$.
- 1.47. 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?
- 1.48. Tegū $(a, b) = 1$. Įrodykite, kad $(a + b, a^2 - ab + b^2)$ lygus 1 arba 3.
- 1.49. Įrodykite, kad trupmena $\frac{21n+4}{14n+3}$ yra nesuprastinama su visomis natūraliosiomis n reikšmėmis.
- 1.50. Įrodykite, kad nėra tokių sveikųjų $a, b, n > 1$, su kuriais $(a^n - b^n) | (a^n + b^n)$.
- 1.51. Įrodykite, kad nėra tokių sveikųjų $a, b > 2$, su kuriais $2^b - 1 | 2^a + 1$.
- 1.52. Įrodykite, kad $(n! + 1, (n + 1)! + 1) = 1$, kai $n \in \mathbb{N}$.
- 1.53. Įrodykite, kad jei $(a, b) = 1$ ir p yra nelyginis pirminis, tai
- $$\left(a + b, \frac{a^p + b^p}{a + b} \right) = 1 \text{ arba } p.$$
- 1.54. Tegū k ir m , $k > m$, tokie natūralieji skaičiai, kad $km(k^2 - m^2)$ dalijasi iš $k^3 - m^3$. Įrodykite, kad $(k - m)^3 > 3km$.
- 1.55. Raskite visus skaičiaus 60 daliklius, besidalijančius iš trijų.
- 1.56. Su kuriomis natūraliosiomis n reikšmėmis skaičius $n^2 + 5n + 6$ pirminis?
- 1.57. Tegū $(a, b) = p$, kur p – pirminis. Kokias reikšmes gali įgyti
- (a) (a^2, b) ,
(b) (a^3, b) ,
(c) (a^3, b^2) ?
- 1.58. Tegū $(a^2, p) = p$ ir $(b, p^3) = p^2$, kur p – pirminis. Kokias reikšmes gali įgyti
- (a) $(a + b, p^4)$,
(b) (ab, p^4) ?
- 1.59. Su kuriomis $a, b > 1$ reikšmėmis $a - b | a + b$?
- 1.60. Tegū $(a, b) = 1$. Įrodykite, kad jei $a | c$ ir $b | c$, tai $ab | c$.
- 1.61. Įrodykite, kad skaičius turi nelyginį daliklių skaičių tada ir tik tada, kai jis yra sveikojo skaičiaus kvadratas.
- 1.62. Įrodykite, kad jei $(a, b) = 1$ ir ab kvadratas, tai ir a, b kvadratai.
- 1.63. Ar egzistuoja skaičius n , su kuriuo $3n$ turi 60 daliklių, o $7n$ turi 80 daliklių?
- 1.64. Raskite mažiausią sveikąjį skaičių turintį 75 daliklius ir besidalijantį iš 75.
- 1.65. Raskite mažiausią natūralųjį skaičių, kurio pusė yra sveikojo skaičiaus kvadratas, trečdalis yra sveikojo skaičiaus kubas, o penktadalis yra sveikojo skaičiaus penktasis laipsnis.

- 1.66. Su kuriomis n reikšmėmis $n|(n-1)!$?
- 1.67. Įrodykite, kad $\text{mbk}(a, b, c) \cdot \text{dbd}(ab, bc, ca) = abc$, kur $a, b, c \in \mathbb{N}$.
- 1.68. Įrodykite, kad $(ab, cd, ac + bd)|(ac, bd)$. Ar visuomet $(ac, bd)|(ab, cd, ac + bd)$?
- 1.69. Įrodykite, kad $n^4 + 4$ ir $n^4 + n^2 + 1$ yra sudėtiniai, kai $n > 1$.
- 1.70. Su kuriomis neneigiamomis n reikšmėmis vienu metu $2n + 1$ ir $3n + 1$ yra pilnieji kvadratai ir $5n + 3$ yra pirminis?
- 1.71. Kokius skaičius galima išreikšti kaip sumą dviejų ar daugiau iš eilės einančių natūraliųjų skaičių? Kokių nelyginių skaičių negalima išreikšti suma trijų ar daugiau iš eilės einančių natūraliųjų skaičių?
- 1.72. Raskite visas skirtingų sveikųjų skaičių aibes, susidedančias bent iš trijų elementų, kurių bet kurio elementų trejeto suma dalinasi iš kiekvieno to trejeto elemento.
- 1.73. Įrodykite, kad $\sum_{i=1}^n \frac{1}{n}$ nėra sveikasis su visomis $n > 1$ reikšmėmis.
- 1.74. Įrodykite, kad kiekvienas pirminis p dalo $\binom{p}{i}$, jei $0 < i < p$, kur $\binom{i}{p}$ yra binominis koeficientas. Ar teiginys teisingas sudėtiniam skaičiams?
- 1.75. Nagrinėdami seką $2^{2^1} + 1, 2^{2^2} + 1, 2^{2^3} + 1, \dots$, įrodykite, kad pirminių skaičių yra be galo daug.
- 1.76. Raskite visus skaičius n , kurių bet kurių dviejų daliklių nelygių nei 1 nei n skirtumas taip pat yra n daliklis.

2 Lyginiai

- 2.1. Įrodykite, kad \mathbb{Z}_n yra grupė daugybos atžvilgiu.
- 2.2. Naudodami Euklido algoritimą, raskite tokius $x, y \in \mathbb{Z}$, kad $2261x + 1275y = 17$.
- 2.3. Įrodykite, kad binominis koeficientas

$$\frac{p!}{r!(p-r)!}$$

yra sveikasis skaičius.

- 2.4. Įrodykite, kad jei a ir b yra sveikieji skaičiai, ir p yra pirminis skaičius, tai $(a+b)^p \equiv a^p + b^p \pmod{p}$.
- 2.5. (a) Įrodykite, kad jei x, y yra lygties $ax + by = d$ sprendinys ($\text{dbd}(a, b) = d$), tai su visais $c \in \mathbb{Z}$

$$x' = x + c \cdot \frac{b}{d}, \quad y' = y - c \cdot \frac{a}{d}$$

taip pat yra lygties $ax + by = d$ sprendinys.

- (b) Raskite du skirtingus lygties $2261x + 1275y = 17$ sprendinius.
- (c) Įrodykite, kad visi sprendiniai yra (a) punkte nurodyto pavidalo.
- 2.6. Raskite visų liekanų modulių 7 aibę R , kurios elementai yra: (1) neneigiami, (2) nelyginiai, (3) lyginiai, (4) pirminiai.
- 2.7. Įrodykite dalybos iš 5, 9 ir 11 požymius.
- 2.8. (1998 Putnam) Dešimtainė sveikųjų skaičių seka apibrėžta taip: $a_1 = 0$, $a_2 = 1$, o a_{n+2} gaunamas „sulipinus“ a_{n+1} su a_n . Pavyzdžiui, $a_3 = 10$, $a_4 = 101$, $a_5 = 10110$ ir t. t.

- (a) Raskite tokį mažiausią sveikąjį skaičių $n > 1$, kad a_n dalytųsi iš 11.
- (b) Įrodykite, kad a_n dalijasi iš 11 tada ir tik tada, kai $n \equiv 1 \pmod{6}$.
- 2.9. Išspręskite lygtį $37x \equiv 1 \pmod{101}$.
- 2.10. Kokia yra 2 eilė modulių 17?
- 2.11. Įrodykite, kad jei p yra pirminis, tai \mathbb{Z}_p yra kūnas.
- 2.12. Raskite tokį $x \in \mathbb{Z}$, kad $x \equiv -4 \pmod{17}$ and $x \equiv 3 \pmod{23}$.
- 2.13. Įrodykite, kad jei $n > 4$ yra sudėtinis skaičius, tai
- $$(n-1)! \equiv 0 \pmod{n}.$$
- 2.14. Su kuriomis n reikšmėmis, $\varphi(n)$ yra nelyginis skaičius?
- 2.15. Raskite liekanas, gaunamas dalijant
- (a) $1 + 11 + 111 + 1111 + 11111$ iš 9,
- (b) $555 \cdot 777 + 666 \cdot 888$ iš 9,
- (c) 7^{777} iš 10.
- 2.16. Įrodykite, kad $ab + cd \equiv ad + bc \pmod{a - c}$.
- 2.17. Įrodykite, kad jei $a \equiv 1 \pmod{6}$, tai $a \equiv 1 \pmod{3}$. Ar teisingas atvirkščias teiginys?
- 2.18. Įrodykite, kad su visais n :
- (a) $2|n^2 - n$
- (b) $30|n^5 - n$
- (c) $42|n^7 - n$
- 2.19. Įrodykite, kad $n^2 + 2$ niekada nesidalina iš 4.
- 2.20. Įrodykite, kad jei $3|a^2 + b^2$, tai $3|a$ ir $3|b$.
- 2.21. Įrodykite, kad jei $a \equiv b \pmod{n}$, tai $\text{dbd}(a, n) = \text{dbd}(b, n)$.
- 2.22. Įrodykite dalumo požymius iš 3, 9 ir 11.
- 2.23. Įrodykite, kad skaičiaus ir jo skaitmenų sumos dalybos iš 9 liekanos sutampa.
- 2.24. Tegū n – nelyginis. Įrodykite, kad $8|n^2 - 1$.
- 2.25. Tegū n nesidalija nei iš dviejų nei iš trijų. Įrodykite, kad $24|n^2 - 1$.
- 2.26. Įrodykite, kad $10^n + 45n - 1$ dalijasi iš 27.
- 2.27. Įrodykite, kad $n^2 + 3n + 5$ nesidalija iš 121 su visomis n reikšmėmis.
- 2.28. Įrodykite, kad su visomis sveikomis n reikšmėmis skaičius $\frac{1}{5}n^5 + \frac{1}{3}n^3 + \frac{7}{15}n$ yra sveikasis.
- 2.29. Įrodykite, kad $6|a + b + c$ tada ir tik tada, kai $6|a^3 + b^3 + c^3$
- 2.30. Tegū q daugianaris su sveikaisiais koeficientais. Įrodykite, kad bet kokiems sveikiesiems x ir y teisinga $q(x) \equiv q(x + y) \pmod{y}$.
- 2.31. Ar egzistuoja daugianaris su sveikaisiais koeficientais, kurio visos reikšmės yra pirminiai skaičiai?
- 2.32. Raskite visus pirminius p ir q tenkinančius lygybę $p^2 - 2q^2 = 1$.

- 2.33. Raskite visas natūraliąsias n reikšmes, su kuriomis reiškinys $36^n + 24^n - 7^n - 5^n$ dalijasi iš 899 be liekanos.
- 2.34. Kiek skaitmenų turi skaičius $1010 \cdots 101$, jeigu jis dalijasi iš 9999?
- 2.35. Raskite visus pirminius skaičius p , su kuriais $11 + p^2$ turi ne daugiau nei 11 daliklių.
- 2.36. Raskite tokius penkis skaičius a_1, \dots, a_5 , kad kiekvienas sveikasis x tenkintų bent vieną iš lyginių $x \equiv a_1 \pmod{2}$, $x \equiv a_2 \pmod{3}$, $x \equiv a_3 \pmod{4}$, $x \equiv a_4 \pmod{6}$, $x \equiv a_5 \pmod{12}$.
- 2.37. Raskite visus natūraliųjų skaičių trejetus a, b, c tenkinančius $a \equiv b \pmod{c}$, $b \equiv c \pmod{a}$, $c \equiv a \pmod{b}$.
- 2.38. Raskite, kokią liekaną gausime dalindami 3^{33} iš 13, 7^{77} iš 17, 9^{99} iš 19.
- 2.39. Raskite $11^{11^{11}}$ dalybos iš 15 liekaną.
- 2.40. Kodėl keldami laipsniais skaičius, kurie nėra tarpusavyje pirminiai su n , niekada negausime liekanos 1 moduliui n ?
- 2.41. Įrodykite, kad $n^{13} - n$ visuomet dalinasi iš 2, 3, 5, 7 ir 13.
- 2.42. Įrodykite, kad jei a ir b tarpusavyje pirminiai su 91, tai $91 | a^{12} - b^{12}$.
- 2.43. Tegu p, q skirtingi pirminiai. Įrodykite, kad $pq | n^{pq} - n^p - n^q + n$ su visais $n \in \mathbb{N}$.
- 2.44. Įrodykite, kad su visomis n reikšmėmis $3^{2n+1} + 2^{n+2}$ dalijasi iš 7.
- 2.45. Kiek yra skaičių mažesnių už ab ir tarpusavyje pirminių su a , kur a ir b natūralieji? Atsakymą užrašykite naudodami φ funkciją.
- 2.46. Įrodykite, kad visų skaičių mažesnių už n ir tarpusavyje pirminių su n suma lygi $n\varphi(n)/2$.
- 2.47. Tegu p ir q pirminiai nedalantys a . Įrodykite, kad jei $q - 1 | p - 1$, tai $a^{p-1} \equiv 1 \pmod{pq}$.
- 2.48. Tegu p – pirminis. Įrodykite, kad jei $a^p \equiv b^p \pmod{p}$, tai $a^p \equiv b^p \pmod{p^2}$.
- 2.49. Tegu a, b, c sveikieji skaičiai ir $a + b + c = 0$. Ar gali $a^{47} + b^{47} + c^{47}$ būti pirminis?
- 2.50. Įrodykite, kad kiekvienam pirminiam p , išskyrus 2 ir 5, egzistuoja be galo daug pavidalo $11 \dots 11$ skaičių, besidalijančių iš p .
- 2.51. Įrodykite, kad kiekvienas n turi kartotinį m , kurio skaitmenys yra tik 1 arba 0. Ar teiginys išlieka teisingas, jei m skaitmenimis gali būti tik 1 ir 2?
- 2.52. Kada $\varphi(ab) = a\varphi(b)$? Kada $\varphi(ab) = \varphi(b)$? Kada $\varphi(2n) > \varphi(n)$?
- 2.53. Įrodykite, kad egzistuoja be galo daug tokių natūraliųjų skaičių n , kad $2003^n - 1$ dalijasi iš n be liekanos.
- 2.54. Iš sekos $a_1 = 3$, $a_{n+1} = 3^{a_n}$ gauta seka $\{b_n\}$ kur b_i lygus a_i dalybos iš 100 liekanai. Ar seka b_i periodinė?
- 2.55. Įrodykite, kad jei $n\varphi(n) = m\varphi(m)$, tai $n = m$.
- 2.56. Ant lentos užrašytas natūralusis skaičius. Prie jo dešinės galime prirašyti bet koki skaitmenį išskyrus 9. Įrodykite, kad kaip berašinėtume, ilgainiui gausime sudėtinį skaičių.

- 2.57. Tegū a_1, a_2, \dots, a_m natūralieji skaičiai, $m \geq 2$. Įrodykite, kad egzistuoja be galo daug natūraliųjų n , su kuriais $a_1 1^n + a_2 2^n + \dots + a_m m^n$ yra sudėtinis.
- 2.58. Įrodykite, kad seka $1^1, 2^2, 3^3, \dots$ yra periodinė modulių p .
- 2.59. Raskite visus dauginarius $q(x)$ su sveikais koeficientais, tenkinančius $q(n) | 2^n - 1$ su visais $n \in \mathbb{N}$.
- 2.60. Raskite sveikuosius skaičius, kurie yra tarpusavyje pirminiai su visais sekos $a_n = 2^n + 3^n + 6^n - 1$ nariais.
- 2.61. Tegū $n \geq 2$ – natūralusis skaičius ir $n | 3^n + 4^n$. Įrodykite, kad $7 | n$.
- 2.62. Išspręskite lyginių sistemą:
- $$\begin{cases} r \equiv 0 \pmod{5}, \\ r \equiv 4 \pmod{7}, \\ r \equiv 3 \pmod{11}; \end{cases} \quad \text{ir} \quad \begin{cases} 3r \equiv 1 \pmod{5}, \\ 3r \equiv 1 \pmod{7}, \\ 3r \equiv 1 \pmod{11}. \end{cases}$$
- 2.63. Kam lygūs du paskutiniai 3^{400} skaitmenys?
- 2.64. Kokią liekaną gausime dalindami skaičių $123456789101112 \dots 20082009$ iš 450?
- 2.65. Ar egzistuoja x , tenkinantis lyginius $x \equiv 29 \pmod{52}$ ir $x \equiv 19 \pmod{72}$?
- 2.66. Sekdami funkcijos φ multiplikatyvumo įrodymą, parodykite, kad $\varphi(24) = \varphi(3)\varphi(8)$. Raskite visas liekanas tarpusavyje pirmines su 24, visas poras liekanų, tarpusavyje pirminių su 3 ir 8 bei atitikmenį tarp jų (t.y. kuri pora, kuriai liekanai priskiriama).
- 2.67. Užbaikite funkcijos φ multiplikatyvumo įrodymą. Parodykite, kad bet kuriam skaičiui priskiriama pora (y_i, y'_j) tenkins $(y_i, m) = 1$ ir $(y'_j, n) = 1$, bei bet kuriai porai priskiriamas skaičius x_i tenkins $(x_i, mn) = 1$.
- 2.68. Raskite mažiausiąjį natūralųjį a , kad $5x^{13} + 13x^5 + 9ax$ dalintųsi iš 65 su visomis natūraliomis x reikšmėmis.
- 2.69. Įrodykite, kad nepaisant to, jog $561 = 3 \cdot 11 \cdot 17$ yra sudėtinis, jam vistiek "galioja mažoji Ferma teorema", t.y. kiekvienam a teisinga $a^{561} \equiv a \pmod{561}$. (Tokie skaičiai yra vadinami *pseudopirminiais*).
- 2.70. Įrodykite, kad egzistuoja dešimt iš eilės einančių skaičių, kurie turi bent po 100 skirtingų pirminių daliklių.
- 2.71. Tegū $(a, b) = 1$ ir $c > 0$. Įrodykite, kad egzistuoja x tenkinantis $(a + bx, c) = 1$. (Užuomina: išskaidykite c pirminiais dauginamaisiais).
- 2.72. Tegū a, b, c trys skirtingi sveikieji skaičiai. Įrodykite, kad egzistuoja be galo skaičių n , su kuriais $(a + n, b + n) = (a + n, c + n) = (b + n, c + n) = 1$.
- 2.73. Ar egzistuoja toks natūralusis a , kad skaičiai $a, 2a, 3a, \dots, 1997a$ būtų natūraliųjų skaičių laipsniai?
- 2.74. Tegū $\psi(n)$ žymi skaičių $\{1, 2, \dots, n\}$ mažiausią bendrą kartotinį. Įrodykite, kad kiekvienam a egzistuoja b , toks kad $\psi(a + 1) = \psi(a + 2) = \dots = \psi(a + b)$.
- 2.75. Įrodykite, kad bet kurioje didėjančioje begalinėje aritmetinėje progresijoje galime rasti kiek norima daug iš eilės einančių sudėtinių skaičių.
- 2.76. Įrodykite, kad kiekvienam $n \in \mathbb{N}$ egzistuoja tokie didesni už vieneta tarpusavyje pirminiai skaičiai k_1, k_2, \dots, k_n , kad $k_1 k_2 \dots k_n - 1$ išsi-skaido kaip dviejų paeiliui einančių natūraliųjų skaičių sandauga.

- 2.77. Sveikųjų skaičių gardelės plokštumoje tašką vadinsime nematomu, jei jį ir koordinačių pradžios tašką jungiančiai atkarpai priklauso dar bent vienas gardelės taškas. Įrodykite, kad kiekvienam n atsiras kvadratas, kurio kraštinės ilgis n ir kurio visi viduje esantys taškai yra nematomi.
- 2.78. Natūralųjų skaičių n vadinsime *neįtikėtiniu*, jei pavyks rasti tris natūraliuosius skaičius a, b, c , tenkinančius $n = (b, c)(a, bc) + (c, a)(b, ca) + (a, b)(c, ab)$. Įrodykite, kad egzistuoja 2011 iš eilės einančių neįtikėtinų skaičių.
- 2.79. Įrodykite, kad egzistuoja tokia natūraliųjų skaičių seka $\{a_n\}$, kad su bet kuriuo k sekoje $\{k + a_n\}$ yra tik baigtinis skaičius pirminių.
- 2.80. Tegų $P(x)$ daugianaris su sveikaisiais koeficientais. Tegų aibė $\{a_0, a_1, \dots, a_k\}$, tokia, kad su kiekviena x reikšme $P(x)$ dalijasi bent iš vieno tos aibės elemento. Įrodykite, kad tuomet $P(x)$ visada dalinsis iš kažkurio vieno tos aibės elemento.
- 2.81. Įrodykite, kad kiekvieniems tarpusavyje pirminiems a ir b egzistuoja tokie natūralieji m ir n , kad $a|m, b|n$, bet $a \nmid n, b \nmid m$, ir tenkinantys
- $$m|n^2 + n \text{ ir } n|m^2 + m.$$
- 2.82. Raskite visų tarpusavyje pirminių su 8 liekanų modulių 8 eiles.
- 2.83. Įrodykite, kad liekanos ir jos atvirkštinės liekanos eilės sutampa.
- 2.84. Kodėl visos liekanos modulių sudėtinio skaičiaus nesudaro grupės?
- 2.85. Kam lygi visų liekanų modulių n suma? Kam lygi visų tarpusavyje pirminių su n liekanų suma?
- 2.86. Tegų liekanos a modulių p eilė lygi d . Parodykite, kad jei $a^r \equiv a^s \pmod{p}$, tai $r \equiv s \pmod{d}$.
- 2.87. Kiek šaknų modulių pirminio p turi daugianaris $x^2 - 1$? Kam jos lygios?
- 2.88. Tegų liekanos a eilė modulių pirminio p yra $2k$. Ar būtinai tuomet $a^k \equiv -1 \pmod{p}$?
- 2.89. Kiek šaknų modulių 6 turi daugianaris $x^2 + x$? Pasirinkę šaknį 2 sekite teiginio apie šaknų skaičių modulių p įrodymą. Kuri jo vieta neteisinga modulių sudėtinio skaičiaus?
- 2.90. Įrodykite Vilsono (*Wilson*) teoremą: jei p pirminis, tai visų tarpusavyje pirminių su p liekanų sandauga yra lygi -1 , arba kitaip:
- $$(p-1)! \equiv -1 \pmod{p}.$$
- (Užuomina: nagrinėkite viena kitai atvirkštinių liekanų poras)
- 2.91. Parodykite, kad $61! + 1 \equiv 63! + 1 \equiv 0 \pmod{71}$.
- 2.92. Kiek šaknų daugianaris $x^2 - x$ turės modulių sudėtinio n ?
- 2.93. Įrodykite, kad jei $p \equiv 3 \pmod{4}$, tai $\frac{p-1}{2}! \equiv \pm 1 \pmod{p}$.
- 2.94. Tegų p – pirminis. Įrodykite, kad $\binom{p-1}{k} \equiv (-1)^k \pmod{p}$, su visomis k reikšmėmis $0 \leq k \leq p-1$.
- 2.95. Pažymėkime a_1, a_2, \dots, a_{p-1} visas liekanas modulių p , tarpusavyje pirmines su p . Sumaišykime jas bet kaip ir pažymėkime b_1, b_2, \dots, b_{p-1} . Ar gali taip atsitikti, kad sudauginę $a_1 b_1, a_2 b_2, \dots, a_{p-1} b_{p-1}$ gausime skirtingas liekanas?
- 2.96. Įrodykite, kad $(p-1)! \equiv p-1 \pmod{1+2+\dots+(p-1)}$.

2.97. Įrodykite, kad jei $\text{dbd}(a, b) = 1$, tai

$$\text{dbd}(a^n - b^n, a^m - b^m) = a^{\text{dbd}(n,m)} - b^{\text{dbd}(n,m)}.$$

2.98. Įrodykite, kad jei n ir a natūralieji, tai $n | \varphi(a^n - 1)$.

2.99. Įrodykite, kad jei pirminis p dalo 2^{2^n} , tai $p \equiv 1 \pmod{2^{n+1}}$.

2.100. Raskite mažiausią n , su kuriuo $2^{2005} | 17^n - 1$.

2.101. Įrodykite, kad multiplikatyvi liekanų grupė moduliui pq izomorfiška multiplikatyvių grupių moduliui p ir q sandaugai. Apibendrinkite šį rezultatą bet kuriai multiplikatyviai grupei moduliui n .

2.102. Įrodykite, kad n nedalo $2^n - 1$, kur $n > 1$ natūralusis skaičius.

2.103. Raskite visus pirminius p, q su kuriais $p^2 + 1 | 2003^q + 1$ ir $q^2 + 1 | 2003^p + 1$.

2.104. Raskite visus pirminius p, q, r , su kuriais

$$p | q^r + 1, q | r^p + 1, r | p^q + 1.$$

2.105. Raskite visus pirminius p ir q , su kuriais $pq | 2^p + 2^q$.

2.106. Įrodykite, kad $3^n - 2^n$ nesidalija iš n .

2.107. Raskite liekanų grupės moduliui 11 generatorius.

2.108. Ar liekanų grupė moduliui 8 ciklinė?

2.109. Tegu p – nelyginis pirminis skaičius. Įrodykite, kad a yra liekanų mod p generatorius tada ir tik tada, kai $a^{\frac{p-1}{q}} \not\equiv 1 \pmod{p}$ su visais pirminiais $p - 1$ dalikliais q .

2.110. Įrodykite, kad liekanų grupė moduliui pirminio p turi $\varphi(p - 1)$ generatorių.

2.111. Įrodykite, kad generatoriaus atvirkštinis irgi yra generatorius. Remdamiesi tuo parodykite, kad visų grupės moduliui pirminio $p > 3$ generatorių sandauga yra lygi 1.

2.112. Parodykite, kad jei g ir g' yra multiplikatyvios grupės moduliui p generatoriai, tai gg' nėra generatorius.

2.113. Išspręskite lygtį $x^{17} \equiv 1 \pmod{19}$.

2.114. Parodykite, kad 2 – liekanų grupės moduliui 29 generatorius. Parodę išspręskite lygtis:

(a) $x^7 \equiv 1 \pmod{29}$,

(b) $x^6 + x^5 + \dots + x + 1 \equiv 0 \pmod{29}$.

2.115. Tegu p – pirminis, o k bet koks skaičius, tarpusavyje pirminis su $p - 1$. Įrodykite, kad keldami skirtingas liekanas laipsniu k gausime taip pat skirtingas liekanas. Parodykite, kaip iš to gauti, jog lygtis $x^k = a \pmod{p}$ turi tik vieną sprendinį moduliui p .

2.116. Įrodykite, kad $1^k + 2^k + \dots + (p - 1)^k \equiv 0 \pmod{p}$, jei $p - 1$ nedalo k ir $\equiv -1 \pmod{p}$, jei $p - 1$ dalo k .

2.117. Tegu g grupės moduliui p generatorius. Ar būtinai ir $-g$ generatorius?

2.118. Tegu $p = 2^n + 1, n \geq 2$ – pirminis skaičius. Įrodykite, kad 3 yra grupės moduliui p generatorius:

a) Tegu g vienas iš grupės moduliui p generatorių. Parodykite, kad visi nelyginiai g laipsniai taip pat bus generatoriais.

b) Parodykite, kad jei 3 nėra generatorius, tai $-3 \equiv a^2 \pmod{p}$ su kažkokiu a .

- c) Tegū $2u \equiv a - 1 \pmod{p}$. Parodykite, kad u yra trečios eilės elementas.
d) Gaukite prieštarą.
- 2.119. Įrodykite, kad jei a yra trečios eilės elementas moduliu pirminio $p > 3$, tai $a + 1$ yra šeštos eilės elementas mod p .
- 2.120. Įrodykite, kad liekanų grupė modulių pq , kur p ir q skirtingi pirminiai skaičiai, nėra ciklinė.
- 2.121. Įrodykite, kad lygtis $x^{37} \equiv y^3 + 11 \pmod{p}$ turi sprendinių su visais pirminiais $p \leq 100$.
- 2.122. Įrodykite, kad multiplikatyvioji grupė modulių p^n , kur $p > 2$ pirminis, yra ciklinė:
- (a) Įrodykite, kad jei $a \equiv b \pmod{p^n}$, tai $a^p \equiv b^p \pmod{p^{n+1}}$
(b) Įrodykite, kad jei $n \geq 2$ ir $p \neq 2$, tai visiems a teisinga $(1 + ap)^{p^{n-2}} \equiv 1 + ap^{n-1} \pmod{p^n}$.
(c) Įrodykite, kad jei $p \neq 2$ ir $p \nmid a$, tai liekanos $(1 + ap)$ eilė modulių p^n lygi p^{n-1} .
(d) Parodykite, kad egzistuoja ciklinės grupės modulių p generatorius g , tenkinantis $g^{p-1} \not\equiv 1 \pmod{p^2}$.
(e) Parodykite, kad taip parinktas g yra grupės p^n generatorius su visomis $n \geq 1$ reikšmėmis.
- 2.123. Įrodykite, kad visų mažesnių už n ir tarpusavyje pirminių su n natūraliųjų skaičių kubų suma dalijasi iš n .

3 Kvadratinio apverčiamumo dėsnis

- 3.1. Raskite visas kvadratinės liekanas modulių 11.
- 3.2. Pasinaudodami Gauso lema raskite $\left(\frac{7}{13}\right)$.
- 3.3. Parodykite, kad lygtis $x^2 \equiv a \pmod{p}$ turi $1 + \left(\frac{a}{p}\right)$ sprendinių.
- 3.4. Įrodykite, kad iš visų nelygių nuliui liekanų modulių pirminio p , pusė yra kvadratinės ir pusė nekvadratinės.
- 3.5. Kiek sprendinių turi lygtys
(a) $x^2 \equiv -1 \pmod{59}$,
(b) $x^2 \equiv -1 \pmod{244}$,
(c) $x^2 \equiv -1 \pmod{3599}$?
(Atkreipkite dėmesį, kad 244 ir 3599 nėra pirminiai!)
- 3.6. Įrodykite, kad kvadratinių liekanų sandauga lygsta 1 modulių p , kai $p \equiv 3 \pmod{4}$, ir -1 , kai $p \equiv 1 \pmod{4}$.
- 3.7. Įrodykite, kad $1^2 3^2 5^2 \dots (p-2)^2 \equiv (-1)^{(p+1)/2} \pmod{p}$.
- 3.8. Tegū $p \equiv 5 \pmod{8}$, ir $a^2 \equiv -1 \pmod{p}$. Naudodamiesi lygybe $a^{(p-1)/2} \equiv \left(\frac{a}{p}\right) \pmod{p}$ nustatykite, ar a bus kvadratinė liekana modulių p .
- 3.9. Tegū q mažiausias natūralusis skaičius, kuris nėra kvadratinė liekana modulių p . Parodykite, kad q turi būti pirminis.
- 3.10. Ar egzistuoja nors vienas sveikųjų skaičių kvadratas, užsirašantis kaip $55k - 1$?

- 3.11. Įrodykite, kad jei pirminis $p \equiv 3 \pmod{4}$, tai iš $p|a^2 + b^2$ seka $p^2|a^2 + b^2$.
- 3.12. Įrodykite, kad jei $19a^2 \equiv b^2 \pmod{7}$, tai $19a^2 \equiv b^2 \pmod{7^2}$.
- 3.13. Parodykite, kad lygtis $x^2 \equiv a \pmod{p^n}$ turi $1 + \left(\frac{a}{p}\right)$ sprendinių su visomis $n > 0$ reikšmėmis.
- 3.14. Parodykite, kad lygtis $x^2 \equiv a \pmod{n}$ turi $\prod_{p|m} \left(1 + \left(\frac{a}{p}\right)\right)$ sprendinių (dauginama pagal visus pirminius, dalijančius m).
- 3.15. Tegu q mažiausias natūralusis skaičius, kuris nėra kvadratinė liekana moduli p . Parodykite, kad $q < \sqrt{p} + 1$.
- 3.16. Įrodykite, kad, kaip ir įprastai, kvadratinė lygtis $ax^2 + bx + c \pmod{p}$, $a \neq 0, p \neq 2$ turės sprendinių tada ir tik tada, kai diskriminantas $b^2 - 4ac$ bus kvadratinė liekana (įskaitant nulį) moduli p .
- 3.17. Raskite mažiausią pirminį, kuris dalo daugianarį $n^2 + 5n + 23$.
- 3.18. Tegu p – pirminis. Įrodykite, kad
- $$\left(\frac{1 \cdot 2}{p}\right) + \left(\frac{2 \cdot 3}{p}\right) + \dots + \left(\frac{(p-2)(p-1)}{p}\right) = -1.$$
- 3.19. Ar $2^{41} - 1$ dalijasi iš 83?
- 3.20. Skaičius N lygus pirmųjų $n \geq 2$ pirminių skaičių sandaugai. Įrodykite, kad nei vienas iš skaičių $N - 1$ ir $N + 1$ nėra natūraliojo skaičiaus kvadratas.
- 3.21. Pasinaudoję lygybe $x^4 + 4 = ((x + 1)^2 + 1)((x - 1)^2 + 1)$ parodykite, kad -4 bus *bikvadratinė* liekana mod p tada ir tik tada, kai $p \equiv 1 \pmod{4}$. (a yra bikvadratinė liekana, jei egzistuoja sprendinys $x^4 \equiv a \pmod{p}$).
- 3.22. Raskite visus pirminius p , su kuriais lygtis $x^2 + y^2 = 2003 + pz$ turi sveikųjų sprendinių.
- 3.23. Raskite $\left(\frac{79}{101}\right)$ ir $\left(\frac{41}{61}\right)$.
- 3.24. Nustatykite, moduli kurių pirminių, 6 yra kvadratinė liekana.
- 3.25. Įrodykite, kad jei pirminis $p > 3$ dalo skaičių $a^2 + 12$, tai tuomet $p \equiv 2 \pmod{3}$. Kokie pirminiai p dalo $a^2 + 5$?
- 3.26. Tegu pirminis $p = 4n + 1$. Įrodykite, kad visi n dalikliai yra kvadratinės liekanos moduli p .
- 3.27. Įrodykite, kad pirminiai daugianario $x^4 - x^2 + 1$ dalikliai lygsta 1 mod 12. (Skaičių vadiname daugianario P dalikliu, jei egzistuoja a su kuriuo $P(a)$ dalijasi iš to skaičiaus).
- 3.28. Įrodykite, kad visi pirminiai yra daugianario $x^6 - 11x^4 + 36x^2 - 36$ dalikliai.
- 3.29. Tegu p ir q du pirminiai skaičiai, tenkinantys $p = q + 2$. Įrodykite, kad $p|(a^2 - q)$ su koku nors sveikuoju a tada ir tik tada, kai $q|(b^2 - q)$ su koku nors sveikuoju b .
- 3.30. Jei a nėra kvadratinė liekana moduli p ir q , ar lygtis $x^2 \equiv a \pmod{pq}$ turės sprendinių?
- 3.31. Įrodykite, kad $x^2 - 2$ niekada nesidalija iš $2y^2 + 3$.

- 3.32. Įrodykite, kad jei x nesidalija iš 3, tai $4x^2 + 3$ dalijasi iš bent vieno pirminio $p = 12k + 7$.
- 3.33. Įrodykite, kad su visais pirminiais p lygtis $x^4 \equiv 16 \pmod{p}$ turi sprendinį.
- 3.34. Tegu pirminis $p \equiv 3 \pmod{4}$, ir $q = 2p + 1$ taip pat pirminis. Įrodykite, kad $q | 2^p - 1$.
- 3.35. Tegu $p = 4^n + 1$ pirminis. Įrodykite, kad 3 nėra kvadratinė liekana moduliu p .
- 3.36. Žinoma, kad jei pirminis $p \equiv 1 \pmod{4}$, tai jis užrašomas kaip dviejų kvadratų suma $p = a^2 + b^2$. Tegu a – nelyginis dėmuo. Įrodykite:
- $\left(\frac{a}{p}\right) = 1$;
 - $\left(\frac{a+b}{p}\right) = (-1)^{\frac{(a+b)^2-1}{8}}$;
 - $(a+b)^2 \equiv 2ab \pmod{p}$;
 - $(a+b)^{\frac{p-1}{2}} \equiv (2ab)^{\frac{p-1}{4}} \pmod{p}$.
 - Tegu f toks, kad $b \equiv af \pmod{p}$. Įrodykite, kad $f^2 \equiv -1 \pmod{p}$ ir kad $2^{\frac{p-1}{4}} \equiv f^{ab/2} \pmod{p}$.
 - Įrodykite, kad 2 yra bikvadratinė liekana moduliu p tada ir tik tada, kai p užrašomas kaip $A^2 + 64B^2$.
- 3.37. Tegu $p = 2^{2^n} + 1$ pirminis. Įrodykite, kad jei $n > 1$, tai 3, 5 ir 7 yra ciklinės grupės moduliu p generatoriai.
- 3.38. Tegu $k = 2^{2^n} + 1$, kur $n > 0$. Įrodykite, kad k yra pirminis tada ir tik tada, kai $k | 3^{(k-1)/2} + 1$.
- 3.39. Įrodykite, kad $2^n + 1$ nesidalija iš pirminių $p = 8k + 7$.
- 3.40. Įrodykite, kad jei p yra pirminis, tai $A = 7p + 3^p - 4$ nėra pilnas kvadratas.
- 3.41. Tegu $S(n)$ skaičiaus n skaitmenų suma. Raskite mažiausią galimą $S(m)$ reikšmę, jei m dalijasi iš 2003.

4 Grandininės trupmenos

4.1. Raskite grandininę trupmeną kiekvienam iš šių skaičių:

a) $\frac{5}{12}$ b) $\frac{5}{3}$ c) $\frac{33}{23}$ d) $\frac{37}{31}$

4.2. Apskaičiuokite grandininę trupmeną atitinkantį skaičių:

a) [2, 3, 2] b) [1, 4, 6, 4] c) [2, 3, 2, 3] d) [9, 12, 21, 2]

4.3. Raskite iracionalių skaičių grandinines trupmenas:

a) $\sqrt{3}$ b) $\sqrt{5}$ c) $\sqrt{6}$

4.4. Tarkime a ir b yra tarpusavyje pirminiai natūralieji skaičiai. Užrašykite

$$\frac{2a^2b + a^2 + ab + 2a + 1}{2ab + a + 2}$$

grandinine trupmena.

4.5. Duota, kad $x = [2, 2, 2, \dots]$. Įrodykite, kad

$$p_k = \left(1 + \frac{3\sqrt{2}}{4}\right) (1 + \sqrt{2})^k + \left(1 - \frac{3\sqrt{2}}{4}\right) (1 - \sqrt{2})^k,$$

$$q_k = \left(1 + \frac{3\sqrt{2}}{4}\right) (1 + \sqrt{2})^{k-1} + \left(1 - \frac{3\sqrt{2}}{4}\right) (1 - \sqrt{2})^{k-1};$$

b) $x = 1 + \sqrt{2}$.

- 4.6. Tarkime c_n yra skaičiaus $[a_0, a_1, \dots, a_n]$ n -toji konvergentė ir $a_0 > 0$. Įrodykite, kad
- $$[a_n, a_{n-1}, \dots, a_1, a_0] = \frac{p_n}{p_{n-1}} \quad \text{ir} \quad [a_n, a_{n-1}, \dots, a_2, a_0] = \frac{q_n}{q_{n-1}}$$
- 4.7. Raskite natūralųjį skaičių, kurį galima užrašyti 3 skirtingai būdais dviejų kvadratų suma.
- 4.8. Tarkime, kad p yra pirminis skaičius. Įrodykite, kad $p \equiv 1, 3 \pmod{8}$ tada ir tik tada, kai $p = a^2 + 2b^2$.
- 4.9. Įrodykite, kad tarp 4 iš eilės einančių skaičių, bent vieno negalima užrašyti 2 kvadratų suma.
- 4.10. Atspėkite (ir patikrinkite) mažiausią lygties $x^2 - 2y^2 = 1$ sprendinį, iš kurio gaukite dar bent tris sprendinius.
- 4.11. Ar lygtis $x^2 - dy^2 = -1$ visuomet turės sprendinių, kai d bekvadratis?
- 4.12. Ar lygtis $x^2 - dy^2 = k$ visuomet turės sprendinių, kai d bekvadratis?
- 4.13. Tegū (x_0, y_0) lygties $x^2 - dy^2 = 1$ sprendinys, o (a, b) – lygties $x^2 - dy^2 = k$ sprendinys (d bekvadratis). Kaip iš jų gauti dar vieną lygties $x^2 - dy^2 = k$ sprendinį?
- 4.14. Įrodykite, kad jei lygtis $x^2 - dy^2 = k$, kur d bekvadratis, turi bent vieną sprendinį, tai jų turi be galo daug.
- 4.15. Įrodykite, kad pirmų n skaičių suma be galo dažnai dažnai būna pilnas kvadratas. Raskite pirmas 6 tokias n reikšmes
- 4.16. Įrodykite, kad su begalo daug n reikšmių $n^2 + (n+1)^2$ yra pilnas kvadratas.
- 4.17. Sugalvokite kaip išskleisti duotą skaičių tęstine trupmena ir pasinaudoję skleidiniu raskite lygties $x^2 - 7y^2 = 1$ mažiausiąjį sprendinį.
- 4.18. 1657m. išspręsti lygtį $x^2 - 61y^2 = 1$ buvo nemenkas iššūkis Europos matematikams (tarp jų ir pačiam P. Ferma). Ar pajėgsite rasti nors vieną sprendinį?
- 4.19. Įrodykite, kad jei (x_1, y_1) ir (x_2, y_2) yra, atitinkamai, lygčių
- $$x^2 - dy^2 = a \quad \text{ir} \quad x^2 - dy^2 = b$$
- sprendiniai, tai
- $$(x_3, y_3) = (x_1, y_1) \cdot (x_2, y_2) = (x_1x_2 + dy_1y_2, x_1y_2 + x_2y_1)$$
- yra lygties $x^2 - dy^2 = ab$ sprendinys.
- 4.20. Įrodykite, kad $x^2 + xy - y^2 = 1$ turi be galo daug sprendinių ir raskite bent 2 teigiamus sprendinius.
- 4.21. Raskite visus lygčių sprendinius:
- $x^2 - 4y^2 = 45$,
 - $x^2 - y^2 = 6$,
 - $x^2 - 9y^2 = 7$.
- 4.22. Raskite lygties $x^2 = x + 2$ sveikuosius sprendinius.
- 4.23. Raskite lygties $x^2 + y^2 = 100$ sveikuosius sprendinius.
- 4.24. Raskite lygties $x^2 = 100 + y^2$ sveikuosius sprendinius.
- 4.25. Raskite lygties $xy = x + y$ sveikuosius sprendinius.
- 4.26. Raskite lygties $x^2 = 3y - 1$ sveikuosius sprendinius.

- 4.27. Raskite lygties $x^2 = 2^n - 1$ sveikuosius sprendinius.
- 4.28. Raskite lygties $x^2 + y^2 = 4z + 3$ sveikuosius sprendinius.
- 4.29. Raskite lygties $x^2 + 2x = 4y + 2$ sveikuosius sprendinius.
- 4.30. Raskite lygties $x^2 + y^2 = 2x + 3y + 4$ sveikuosius sprendinius.
- 4.31. Raskite lygties $2 + x^2 + x^3 = 6^n$ sveikuosius sprendinius