4 pratybos. Liekanų aritmetika

Paulius Drungilas

Turinys

Kaip skaičiuoti $a^b \pmod n$? Skaičių b užrašome dvejetainėje skaičiavimo sistemoje:

$$b = \alpha_0 + \alpha_1 2^1 + \alpha_2 2^2 + \cdots + \alpha_k 2^k, \quad \alpha_j \in \{0, 1\}.$$

(Pavyzdžiui, $11 = 1 + 2^1 + 2^3$, $27 = 1 + 2^1 + 2^3 + 2^4$.) Tada

$$a^n = a^{\alpha_0 + \alpha_1 2^1 + \alpha_2 2^2 + \cdots + \alpha_k 2^k} = a^{\alpha_0} \cdot a^{\alpha_1 2^1} \cdot a^{\alpha_2 2^2} \cdots a^{\alpha_k 2^k}.$$

Suskaičiuojame skaičių a^{2^j}, $0 \leqslant j \leqslant k$, dalybos iš n liekanas. Tai nėra taip sunku, kaip iš pirmo žvilgsnio gali atrodyti. Iš tikrųjų, jei radome skaičiaus a^{2^j} dalybos iš n liekaną r, tai skaičiaus $a^{2^{j+1}}$ dalybos iš n liekana sutaps su skaičiaus r^2 liekana, nes

$$a^{2^{j+1}} \equiv \left(a^{2^j}\right)^2 \pmod n.$$

1. **pavyzdys.** Rasime skaičiaus 7^{39} dalybos iš 41 liekaną.

Sprendimas. Skaičių 39 užrašome dvejetainėje skaičiavimo sistemoje:

$$39 = 1 + 2 + 2^2 + 2^5.$$

Tada

$$7^{39} \equiv 7^{1+2+2^2+2^5} \equiv 7^1 \cdot 7^2 \cdot 7^{2^2} \cdot 7^{2^5} \pmod{41}.$$

Skaičiuojame liekanas:

$$7^1 \equiv 7 \pmod{41},$$
$$7^2 \equiv 49 \equiv 8 \pmod{41},$$

$$7^{2^2} \equiv (7^{2^1})^2 \equiv 8^2 \equiv 64 \equiv 23 \,(\mathrm{mod}\ 41),$$
$$7^{2^3} \equiv (7^{2^2})^2 \equiv 23^2 \equiv 37 \equiv -4 \,(\mathrm{mod}\ 41),$$
$$7^{2^4} \equiv (7^{2^3})^2 \equiv (-4)^2 \equiv 16 \,(\mathrm{mod}\ 41),$$
$$7^{2^5} \equiv (7^{2^4})^2 \equiv 16^2 \equiv 10 \,(\mathrm{mod}\ 41).$$

Taigi

$$7^{39} \equiv 7 \cdot 8 \cdot 23 \cdot 10 \equiv 56 \cdot 230 \equiv 15 \cdot 25 \equiv 6 \,(\mathrm{mod}\ 41).$$

□

Oilerio funkcija. Tarkim, n – natūralusis skaičius, $n > 1$. Aibės

$$\{1, 2, \ldots, n-1\}$$

skaičių, tarpusavyje pirminių su n, skaičius žymimas $\varphi(n)$. Apibrėžkime $\varphi(1) = 1$. Taip apibrėžta funkcija

$$\varphi : \mathbb{N} \to \mathbb{N}$$

vadinama **Oilerio funkcija**. Pavyzdžiui, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, $\varphi(5) = 4$. Oilerio funkcija yra multiplikatyvi:

$$\mathrm{DBD}(m, n) = 1 \implies \varphi(mn) = \varphi(m) \cdot \varphi(n).$$

Pavyzdžiui, $\varphi(12) = \varphi(3 \cdot 4) = \varphi(3) \cdot \varphi(4) = 2 \cdot 2 = 4$.

Sakykime, kad natūraliojo skaičiaus n kanoninė išraiška yra

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}.$$

Tada

$$\varphi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right).$$

2. **pavyzdys.** Rasime $\varphi(360)$.

Sprendimas. Skaičiaus 360 kanoninė išraiška yra $360 = 2^3 \cdot 3^2 \cdot 5^1$, todėl

$$\varphi(360) = 360 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) = 96.$$

Taigi aibėje $\{1, 2, 3, \ldots, 359\}$ yra 96 skaičiai, tarpusavyje pirminiai su 360.

□

3. **pastaba.** Jei p – pirminis skaičius, tai visi aibės $\{1, 2, \ldots, p-1\}$ skaičiai yra tarpusavyje pirminiai su p, todėl $\varphi(p) = p - 1$.

Kaip skaičiuoti $a^b \,(\mathbf{mod}\ n)$, kai $b \geqslant \varphi(n)$? Sakykime, kad $b \geqslant \varphi(n)$. Skaičiuojant $a^b \,(\mathrm{mod}\ n)$ praverčia tokia teorema:

4. **teorema** (Oilerio teorema)**.** *Tegu* $n \in \mathbb{N},\ n > 1$, *ir* $(a, n) = 1$. *Tada*

$$a^{\varphi(n)} \equiv 1 \,(mod\ n)\,.$$

Padalijame skaičių b iš skaičiaus $\varphi(n)$ su liekana:

$$b = \varphi(n) \cdot m + r, \quad 0 \leqslant r < \varphi(n).$$

Remiantis Oilerio teorema,

$$a^b \equiv a^{\varphi(n)\cdot m + r} \equiv a^{\varphi(n)\cdot m} \cdot a^r \equiv (a^{\varphi(n)})^m \cdot a^r \equiv a^r \,(\mathrm{mod}\ n)\,.$$

5. **pavyzdys.** Rasime $3^{201} \,(\mathrm{mod}\ 38)$.

Sprendimas. Suskaičiuojame:

$$\varphi(38) = \varphi(2 \cdot 19) = \varphi(2) \cdot \varphi(19) = 18.$$

Tada skaičių 201 padalijame su liekana iš $\varphi(38) = 18$:

$$201 = 18 \cdot 11 + 3.$$

Kadangi $(3, 38) = 1$, tai, remiantis Oilerio teorema, $3^{18} \equiv 1 \,(\mathrm{mod}\ 38)$, todėl

$$3^{201} \equiv 3^{18\cdot 11 + 3} \equiv (3^{18})^{11} \cdot 3^3 \equiv (1)^{11} \cdot 3^3 \equiv 27 \,(\mathrm{mod}\ 38).$$

□

Likinių klasės. Fiksuokime natūralųjį skaičių n. Bet kuriam sveikajam skaičiui k apibrėžkime aibę

$$\overline{k} = \{a + nt \mid t \in \mathbb{Z}\},$$

kuri sudaryta iš tų sveikųjų skaičių, kurių dalybos iš n liekana sutampa su skaičiaus k dalybos iš n liekana. Ši aibė vadinama **likinių klase moduliu** n. Likinių klasę nusako bet kuris jos elementas, t. y., jei $a \in \overline{k}$, tai $\overline{a} = \overline{k}$, nes a ir k. Visų likinių klasių moduliu n aibė žymima $\mathbb{Z}_n$. Apibrėžkime sudėties ir daugybos operacijas aibėje $\mathbb{Z}_n$:

$$\overline{k} + \overline{l} := \overline{k + l},$$

$$\overline{k} \cdot \overline{l} := \overline{k \cdot l}.$$

Pavyzdžiui, liekanų klasių moduliu 5 aibė yra $\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$. Tada $\overline{3} + \overline{4} = \overline{3 + 4} = \overline{7} = \overline{2}$, nes skaičių 7 ir 2 dalybos iš 5 liekanos sutampa. $\overline{3} \cdot \overline{4} = \overline{3 \cdot 4} = \overline{12} = \overline{2}$, nes skaičių 12 ir 2 dalybos iš 5 liekanos sutampa.

Pažymėkime

$$U_n = \{\overline{a} \in \mathbb{Z}_n \,|\, (a,n) = 1\}.$$

Elementas $\overline{a}$, $a \in \{1, 2, \ldots, n-1\}$, priklauso aibei U_n tada ir tik tada, kai $(a,n) = 1$. Todėl aibė U_n turi lygiai $\varphi(n)$ elementų. Pavyzdžiui, aibė $U_{10} = \{\overline{1}, \overline{3}, \overline{7}, \overline{9}\}$ turi lygiai $\varphi(10) = 4$ elementus.

6. **pavyzdys.** Įrodysime, kad aibė U_n liekanų klasių daugybos atžvilgiu sudaro grupę.

Įrodymas. Jei $\overline{a}, \overline{b} \in U_n$, tai $(a,n) = (b,n) = 1$, todėl $(ab,n) = 1$. Vadinasi, $\overline{ab} \in U_n$. Taigi liekanų klasių daugyba yra operacija aibėje U_n.

(Asociatyvumas) Akivaizdu, kad bet kuriems $\overline{a}, \overline{b}, \overline{c} \in U_n$ teisinga lygybė

$$\overline{a} \cdot (\overline{b} \cdot \overline{c}) = (\overline{a} \cdot \overline{b}) \cdot \overline{c}.$$

(Neutralusis elementas) Liekanų klasė $\overline{1} \in U_n$ yra neutralus elementas, nes

$$\overline{a} \cdot \overline{1} = \overline{a}.$$

(Atvirkštinis elementas) Tegu $\overline{a} \in U_n$. Kadangi $(a,n) = 1$, tai egzistuoja tokie skaičiai $x, y \in \mathbb{Z}$, kad

$$ax + ny = 1.$$

Iš čia gauname, kad $(x,n) = 1$, todėl $\overline{x} \in U_n$. Tada

$$\overline{a} \cdot \overline{x} = \overline{ax} = \overline{ax + ny} = \overline{1},$$

todėl $\overline{a}^{-1} = \overline{x}$. □

7. **pavyzdys.** Įrodysime, kad grupė U_{13} yra ciklinė, o grupė U_{16} – nėra.

Įrodymas. Baigtinė grupė yra ciklinė tada ir tik tada, kai egzistuoja jos elementas, kurio eilė lygi tos grupės elementų skaičiui.

Nagrinėkime grupę U_{13}. Tegu $\overline{2} \in U_{13}$. Grupė U_{13} turi $\varphi(13) = 12$ elementų. Įrodysime, kad elemento $\overline{2}$ eilė yra 12, todėl U_{13} bus ciklinė grupė. Kadangi $(2,13) = 1$, tai pagal Oilerio teoremą $2^{\varphi(13)} \equiv 2^{12} \equiv 1 \,(\mathrm{mod}\, 13)$, todėl $\overline{2}^{12} = \overline{1}$. Todėl elemento $\overline{2}$ eilė yra skaičiaus 12 daliklis. Patikriname

visus skaičiaus 12 daliklius:

$$\overline{2}^1 = \overline{2} \neq \overline{1},$$
$$\overline{2}^2 = \overline{4} \neq \overline{1},$$
$$\overline{2}^3 = \overline{8} \neq \overline{1},$$
$$\overline{2}^4 = \overline{3} \neq \overline{1},$$
$$\overline{2}^6 = \overline{12} \neq \overline{1}.$$

Todėl skaičius 12 yra mažiausias natūralusis skaičius, kuriuo pakėlus elementą $\overline{2}$ gauname $\overline{1}$. Taigi elemento $\overline{2}$ eilė yra 12 ir grupė U_{13} yra ciklinė:

$$U_{13} = \left\{\overline{2}, \overline{2}^2, \overline{2}^3, \ldots, \overline{2}^{11}, \overline{2}^{12} = 1\right\}.$$

Nagrinėkime grupę U_{16}. Ši grupė turi $\varphi(16) = 8$ elementus, todėl pakanka įrodyti, kad nėra elemento, kurio eilė lygi 8. Iš tikrųjų,

$$U_{16} = \left\{\overline{1}, \overline{3}, \overline{5}, \overline{7}, \overline{9}, \overline{11}, \overline{13}, \overline{15}\right\}.$$

Tikriname:

$$\overline{1}^{\,1} = \overline{1},$$
$$\overline{3}^{\,4} = \overline{1},$$
$$\overline{5}^{\,4} = \overline{1},$$
$$\overline{7}^{\,2} = \overline{1},$$
$$\overline{9}^{\,2} = \overline{9-16}^{\,2} = \overline{-7}^{\,2} = \overline{1},$$
$$\overline{11}^{\,4} = \overline{11-16}^{\,4} = \overline{-5}^{\,4} = \overline{1},$$
$$\overline{13}^{\,4} = \overline{13-16}^{\,4} = \overline{-3}^{\,4} = \overline{1},$$
$$\overline{15}^{\,2} = \overline{15-16}^{\,2} = \overline{-1}^{\,2} = \overline{1}.$$

Iš čia matome, kad kiekvieno grupės elemento eilė mažesnė už 8, todėl grupė U_{16} nėra ciklinė. □

8. **pastaba.** Yra žinoma, jog grupė U_n yra ciklinė tada ir tik tada, kai skaičius n turi pavidalą 2, 4, p^a arba $2p^a$, kur p – nelyginis pirminis skaičius.

Šiek tiek kriptografijos. Sakykime, kad du asmenys nori susirašinėti taip, kad siunčiamo teksto niekas negalėtų perskaityti (žinoma, visada yra tikimybė, kad ir labai maža, jog pašalinis asmuo atspės jūsų kodavimo sistemą). Šie du asmenys sugalvoja skaičius p, q, $n = p \cdot q$, E, D, tenkinančius tokias sąlygas:

1) p ir q – skirtingi pirminiai skaičiai. Tada $\varphi(n) = (p-1)(q-1)$;
2) E yra tarpusavyje pirminis su $\varphi(n)$;
3) $E \cdot D \equiv 1 \,(\mathrm{mod}\ \varphi(n))$, t. y. D yra lyginio $Ex \equiv 1 \,(\mathrm{mod}\ \varphi(n))$ sprendinys.

Tada pranešimo dalys, abiem asmenim žinomu būdu, koduojamos kaip žiedo $\mathbb{Z}_n$ elementai. Tegu $x \in \mathbb{Z}_n$. Siuntėjas apskaičiuoja elementą

$$y = e(x), \quad y = x^E$$

ir siunčia jį gavėjui. Funkcija $e(x) = x^E$ vadinama užkodavimo funkcija. Gavėjas iš elemento y ir žinomų skaičių p, q, $n = p \cdot q$, E, D atkoduoja elementą $x = d(y)$:

$$x = y^D.$$

Funkcija $d(y) = y^D$ vadinama iškodavimo funkcija. Iš tikrųjų, kadangi

$$E \cdot D \equiv 1 \,(\mathrm{mod}\ \varphi(n)),$$

tai $E \cdot D = \varphi(n) \cdot m + 1$. Remiantis Oilerio teorema, $x^{\varphi(n)} = \overline{1}$, todėl

$$y^D = x^{E \cdot D} = x^{\varphi(n) \cdot m + 1} = (x^{\varphi(n)})^m \cdot x = (\overline{1})^m \cdot x = x.$$

9. **pavyzdys.** Žinodami skaičius $n = 667 = 23 \cdot 29$, $E = 19$, užkoduosime žiedo $\mathbb{Z}_{667}$ elementą $\overline{93}$ ir atkoduosime elementą $\overline{413}$.

Sprendimas. Kadangi $667 = 23 \cdot 29$, tai

$$\varphi(667) = \varphi(23 \cdot 29) = 22 \cdot 28 = 616.$$

Lyginio

$$Ex \equiv 1 \,(\mathrm{mod}\ 616)$$

sprendinys yra lyginys $x \equiv 227 \,(\mathrm{mod}\ 616)$, todėl $D = 227$ (skaičius D randamas nevienareikšmiškai; parenkame patį mažiausią teigiamą). Taigi koduodami elementą $\overline{93}$, gauname elementą

$$e(\overline{93}) = \overline{93}^{19} = \overline{323}.$$

Iškoduodami elementą $\overline{413}$ gauname elementą

$$d(\overline{413}) = \overline{413}^{227} = \overline{459}.$$

Patikrinkime: $d(\overline{323}) = \overline{323}^{227} = \overline{93}$ ir $e(\overline{459}) = \overline{459}^{19} = \overline{413}$. □

Kaip gauti dalumo požymį? Tegu n ir N – natūralieji skaičiai. Sakykime, kad skaičiaus N užrašas dešimtainėje skaičiavimo sistemoje yra $\overline{a_k a_{k-1} \dots a_2 a_1 a_0}$, t. y.

$$N = a_0 + a_1 \cdot 10^1 + a_2 \cdot 10^2 + \dots + a_k \cdot 10^k.$$

Skaičiaus 10^j, $j = 0, 1, 2, \dots$, dalybos iš n liekaną pažymėkime r_j:

$$10^j \equiv r_j \,(\text{mod } n).$$

Tada

$$N \equiv a_0 + a_1 \cdot r_1 + a_2 \cdot r_2 + \dots + a_k \cdot r_k \,(\text{mod } n).$$

Be to, liekanų seka r_0, r_1, r_2, r_3, … yra **periodinė**.

10. **pavyzdys.** Rasime skaičių 2422, 31256 ir 431564755125214119 dalybos iš 7 liekanas.

Sprendimas. Iš pradžių randame skaičių 10^j, $j = 0, 1, 2, \dots$, dalybos iš 7 liekanas r_j. Skaičiuojame tol, kol liekanos pradeda kartotis:

$$r_0 \equiv 1 \,(\text{mod } 7), \quad r_1 \equiv 10^1 \equiv 3 \,(\text{mod } 7), \quad r_2 \equiv 10^2 \equiv 3^2 \equiv 2 \,(\text{mod } 7),$$

$$r_3 \equiv 10^3 \equiv 10^2 \cdot 10 \equiv 2 \cdot 10 \equiv 6 \,(\text{mod } 7),$$

$$r_4 \equiv 10^4 \equiv 10^3 \cdot 10 \equiv 6 \cdot 10 \equiv 4 \,(\text{mod } 7),$$

$$r_5 \equiv 10^5 \equiv 10^4 \cdot 10 \equiv 4 \cdot 10 \equiv 5 \,(\text{mod } 7),$$

$$r_6 \equiv 10^6 \equiv 10^5 \cdot 10 \equiv 5 \cdot 10 \equiv 1 \,(\text{mod } 7).$$

Gavome $r_0 = r_6$, todėl liekanos toliau kartosis periodiškai (periodas lygus 6). Dabar galime suskaičiuoti duotų skaičių dalybos iš 7 liekanas:

$$2422 \equiv 2r_0 + 2r_1 + 4r_2 + 2r_3 \equiv 2 \cdot 1 + 2 \cdot 3 + 4 \cdot 2 + 2 \cdot 6 \equiv 0 \,(\text{mod } 7),$$

$$31256 \equiv 6r_0 + 5r_1 + 2r_2 + 1r_3 + 3r_4 \equiv 6 \cdot 1 + 5 \cdot 3 + 2 \cdot 2 + 1 \cdot 6 + 3 \cdot 4 \equiv 1 \,(\text{mod } 7),$$

$$431564755125214119 \equiv 9r_0 + 1r_1 + 1r_2 + 4r_3 + 1r_4 + 2r_5 + 5r_6 + 2r_7 + 1r_8 +$$

$$+ 5r_9 + 5r_{10} + 7r_{11} + 4r_{12} + 6r_{13} + 5r_{14} + 1r_{15} + 3r_{16} + 4r_{17} \equiv$$

$$\equiv 9 \cdot 1 + 1 \cdot 3 + 1 \cdot 2 + 4 \cdot 6 + 1 \cdot 4 + 2 \cdot 5 + 5 \cdot 1 + 2 \cdot 3 + 1 \cdot 2 +$$

$$+ 5 \cdot 6 + 5 \cdot 4 + 7 \cdot 5 + 4 \cdot 1 + 6 \cdot 3 + 5 \cdot 2 + 1 \cdot 6 + 3 \cdot 4 + 4 \cdot 5 \equiv 3 \,(\text{mod } 7).$$

□

Uždaviniai.

1. **uždavinys** (*)**.** Apskaičiuokite:
a) $8^{38} \pmod{43}$;
b) $13^{69} \pmod{71}$;
c) $120^{87} \pmod{59}$;
d) $137^{87} \pmod{67}$.
Ats.: a) 4; b) 11; c) 58; d) 45.

2. **uždavinys** (*)**.** Oilerio teoremos pagalba, apskaičiuokite:
a) $3^{403} \pmod{100}$; b) $7^{4427} \pmod{100}$; c) $11^{922} \pmod{100}$.
Ats.:
a) $27 \pmod{100}$; b) $43 \pmod{100}$; c) $21 \pmod{100}$.

3. **uždavinys** (*)**.** Raskite skaičiaus 103^{123} a) paskutinį skaitmenį; b) paskutinius du skaitmenis.
Ats.: a) 7; b) 27.

4. **uždavinys.** Sudarykite dalumo iš 11 požymį ir jo pagalba suskaičiuokite skaičiaus a) 1523; b) 25331; c) 51245583 dalybos iš 11 liekaną.
Ats.: a) 5; b) 9; c) 4.

5. **uždavinys.** Sudarykite dalumo iš 13 požymį ir jo pagalba suskaičiuokite skaičiaus a) 1523; b) 25331; c) 51245583 dalybos iš 13 liekaną.
Ats.: a) 2; b) 7; c) 12.

6. **uždavinys** (*)**.** Grupėje U_n, kai $2 \leqslant n \leqslant 15$, raskite didžiausios eilės elementą. Kurios iš šių grupių yra ciklinės?
Ats.:

n	$\overline{a}$	$\overline{a}$ eilė	$\lvert U_n \rvert$	ar ciklinė
2	$\overline{1}$	1	1	taip
3	$\overline{2}$	2	2	taip
4	$\overline{3}$	2	2	taip
5	$\overline{2}$	4	4	taip
6	$\overline{5}$	2	2	taip
7	$\overline{3}$	6	6	taip
8	$\overline{3}$	2	4	ne
9	$\overline{2}$	6	6	taip
10	$\overline{3}$	4	4	taip
11	$\overline{2}$	10	10	taip
12	$\overline{5}$	2	4	ne
13	$\overline{2}$	12	12	taip
14	$\overline{3}$	6	6	taip
15	$\overline{2}$	4	8	ne

Antrame stulpelyje parašytas grupės U_n maksimalios eilės elementas, o trečiame – šio elemento eilė. Ketvirtame stulpelyje $\lvert U_n \rvert$ žymi grupės U_n elementų skaičių.

7. **uždavinys** (*)**.** Užkoduokite ir iškoduokite aibės $\mathbb{Z}_n$ elementus a, b, c, kai

a) $n = 7 \cdot 13$, $E = 11$, $\varphi(7 \cdot 13) = 72$, $a = \overline{22}$, $b = \overline{41}$, $c = \overline{68}$;
b) $n = 11 \cdot 19$, $E = 13$, $\varphi(11 \cdot 19) = 180$, $a = \overline{21}$, $b = \overline{41}$, $c = \overline{68}$;
c) $n = 17 \cdot 23$, $E = 9$, $\varphi(17 \cdot 23) = 352$, $a = \overline{21}$, $b = \overline{41}$, $c = \overline{67}$;
d) $n = 31 \cdot 43$, $E = 11$, $\varphi(31 \cdot 43) = 1260$, $a = \overline{21}$, $b = \overline{41}$, $c = \overline{67}$;
e) $n = 47 \cdot 61$, $E = 53$, $\varphi(47 \cdot 61) = 2760$, $a = \overline{21}$, $b = \overline{41}$, $c = \overline{67}$.

Ats.:

a) $D = 59$, $e(\overline{22}) = \overline{29}$, $e(\overline{41}) = \overline{20}$, $e(\overline{68}) = \overline{87}$,
$d(\overline{22}) = \overline{29}$, $d(\overline{41}) = \overline{20}$, $d(\overline{68}) = \overline{87}$;
b) $D = 97$, $e(\overline{21}) = \overline{98}$, $e(\overline{41}) = \overline{204}$, $e(\overline{68}) = \overline{30}$,
$d(\overline{21}) = \overline{109}$, $d(\overline{41}) = \overline{2}$, $d(\overline{68}) = \overline{106}$;
c) $D = 313$, $e(\overline{21}) = \overline{293}$, $e(\overline{41}) = \overline{265}$, $e(\overline{67}) = \overline{339}$,
$d(\overline{21}) = \overline{106}$, $d(\overline{41}) = \overline{95}$, $d(\overline{67}) = \overline{152}$;
d) $D = 1031$, $e(\overline{21}) = \overline{508}$, $e(\overline{41}) = \overline{360}$, $e(\overline{67}) = \overline{831}$,
$d(\overline{21}) = \overline{570}$, $d(\overline{41}) = \overline{391}$, $d(\overline{67}) = \overline{490}$;
e) $D = 677$, $e(\overline{21}) = \overline{883}$, $e(\overline{41}) = \overline{2675}$, $e(\overline{67}) = \overline{2658}$,
$d(\overline{21}) = \overline{1249}$, $d(\overline{41}) = \overline{1674}$, $d(\overline{67}) = \overline{2654}$.

8. **uždavinys.** Tegu a, r, s ir t – sveikieji skaičiai. Įrodykite, kad skaičius $\mathrm{DBD}(a^2+t, sa+r)$ yra skaičiaus r^2+ts^2 daliklis.

9. **uždavinys.** Tegu p – pirminis skaičius, $p = 2k+1$. Įrodykite, kad $(k!)^2 + (-1)^k \equiv 0 \,(\mathrm{mod}\ p)$.

10. **uždavinys.** Tegu $n \in \mathbb{N}$. Kokias liekanas galima gauti dalijant skaičių $7^n + 11^n$ iš 19?
Ats.: 1, 2 ir 18.