# NMS SKAITĻU TEORIJA #2: MODULĀRĀ ARITMĒTIKA

Skaitļu teorijā daudzi rezultāti ir iegūstami galīgās atlikumu kopās. Tie izmanto kombinatoriskas metodes, jo bezgalīgi daudzo skaitļu vietā šķiro gadījumus. Piemēram, aplūkojot atlikumus, dalot ar 2, iegūstam divus gadījumus – pāra skaitlis un nepāra skaitlis, kur rezultāta paritātei vairs nevajag zināt pašu skaitli, bet tikai atlikumu.

Šādas idejas iespējams vispārināt arī atlikumiem, dalot ar lielākiem skaitļiem. Skaitļu teorijas algoritmus, kas uz skaitļiem raugās "ar atlikumu brillēm" sauc par *modulāro aritmētiku*. Šajā nodaļā aplūkosim sekojošas tēmas:

- Kongruenču klases, modulārā aritmētika.
- Dalāmības pazīmes ar $3, 9, 2^k, 5^k$ kongruenču klašu atrašanai.
- Mazā Fermā teorēma. Periodiskas decimāldaļas.
- Eilera funkcija un Eilera teorēma.
- Cikliski procesi . Periodiskas atlikumu virknes.
- Periodi un priekšperiodi virknēs.

## 2.1 Ievaduzdevums

**Uzdevums (Valsts4Posms-2012.P1):** Ar $S(x)$ apzīmēsim skaitļa $x$ ciparu summu. Aprēķināt $S(S(S(2012^{2012})))$.

**Risinājuma plāns:** Skaitlis $2012^{2012}$ ir ļoti liels; aprēķināt visus šos ciparus ir praktiski neiespējami. Toties skaitļa ciparu summa apmierina svarīgu invariantu (atlikums, dalot ar 9 saglabājas. Risinājuma pirmajā daļā meklēsim vienīgi skaitļu $S(S(S(2012^{2012})))$, $S(S(2012^{2012}))$, $S(2012^{2012})$ un $2012^{2012}$ atlikumu, dalot ar 9 (visiem tiem jābūt vienādiem). Risinājuma otrajā daļā noskaidrosim, kurš no skaitļiem ar atrasto atlikumu ir konkrēti $S(S(S(2012^{2012})))$ (novērtējot to ar nevienādībām).

**Apgalvojums 1:** Ja $n$ ir naturāls skaitlis, tad tā ciparu summa $S(n)$ un pats skaitlis $n$ dod vienādus atlikumus, dalot ar 9. (Šis apgalvojums pazīstams kā vispārināta dalāmības pazīme ar 9.)

**Pierādījums:** Skaitlis $n = \overline{c_1 c_2 \ldots c_{k-1} c_k}$, kur $c_i$ ir decimālcipari, ir pierakstāms kā polinoms, kur mainīgā vietā ir decimālsistēmas bāze $x = 10$:

$$n = c_1 \cdot 10^{k-1} + c_2 \cdot 10^{k-2} + \ldots + c_{k-1} \cdot 10^1 + c_k \cdot 10^0.$$

Ja aprēķinām ciparu summu $S(n) = c_1 + c_2 + \ldots + c_{k-1} + c_k$, tad tā atšķiras no $n$ ar to, ka saskaitāmo $c_i \cdot 10^{k-i}$ vietā ir saskaitāmie $c_i$. Piemēram, ja ceturtais cipars no skaitļa beigām jeb *tūkstošu cipars* ir $c_{k-3} = 7$, tad vērtības $7 \cdot 1000$ vietā pieskaitām vērtību 7.

Starpība abām vērtībām ir $c_i \cdot 10^{k-i} - c_i = c_i \cdot \overline{99\ldots99}$, kur cipars $c_i$ ir pareizināts ar skaitli kas sastāv no daudziem deviņniekiem. Šis skaitlis, acīmredzot dalās ar 9. Tāpēc atlikums, dalot ar 9 nemainās, ja skaitli $n$ aizstāj ar $S(n)$ jeb katru ciparu $c_i$ piesummē vienkārši, nevis reizina ar 10 pakāpi $c_i \cdot 10^{k-i}$. □

**Apgalvojums 2:** Pamatosim, ka $2012^{2012}$ dod atlikumu 7, dalot ar 9.

**Pierādījums:** Aplūkojot pakāpju $a^b$ atlikumus, dalot ar 9, ievērojam, ka tie atkarīgi vienīgi no $a$ atlikuma, dalot ar 9, jo reizinot (un kāpinot) skaitļus ar vienādiem atlikumiem, arī rezultāti dos vienādus atlikumus. Tātad $a^b$ atlikumi dalīšanā ar 9 atkārtojas ar ciklu 9, ja pakāpes bāze $a$ aug. Izsakām $(2012)^{2012} = (223 \cdot 9 + 5)^{2012}$. Tātad jāmeklē atlikums, dalot $5^{2012}$ ar 9.

Otrs novērojums – pakāpju $a^b$ atlikumi, dalot ar 9, cikliski atkārtojas ik pēc 6, ja kāpinātājs $b$ aug.

| $n$ | $5^n$ | Atlikums, dalot ar 9 |
|---|---|---|
| $5^0$ | 1 | 1 |
| $5^1$ | 5 | 5 |
| $5^2$ | 25 | 7 |
| $5^3$ | 125 | 8 |
| $5^4$ | 625 | 4 |
| $5^5$ | 3125 | 2 |
| $5^6$ | 15625 | 1 |

Vēl lielākām pakāpēm atlikumi, dalot ar 9 labajā kolonnā sāk atkārtoties: $5^7$ dod tādu pašu atlikumu kā $5^1$, $5^8$ dod tādu pašu atlikumu kā $5^2$, utt. Arī šīs tabulas aizpildīšanai var godīgi nekāpināt. Ja, teiksim, $5^2 = 25$ dod atlikumu 7, dalot ar 9, tad nākamā atlikuma iegūšanai pietiek ar 5 pareizināt nevis visu 25, bet gan tikai šo atlikumu 7 – rezultāts jeb atlikums skaitlim 35 būs tas pats, kas atlikums skaitlim 125.

Tā kā $5^6$ dod atlikumu 1, dalot ar 9, tad arī $(5^6)^{335} = 5^{2010}$ dod atlikumu 1.

Visbeidzot, $5^{2012} = 5^{2010} \cdot 5^2 = 1 \cdot 25$, kas dod atlikumu 7, dalot ar 9. □

**Secinājums:** Arī skaitlis $S(S(S(2012^{2012})))$ dod atlikumu 7, dalot ar 9. □. (Apvienojam Apgalvojumu 1 un Apgalvojumu 2.)

**Apgalvojums 3:** $S(S(S(2012^{2012}))) = 7$.

**Pierādījums:** Mums jāpārbauda, vai $S(S(S(2012^{2012})))$ nevar būt vienāds ar kādu citu skaitli, kas arī dod atlikumu 7, dalot ar 9. Mazākais šāds skaitlis ir $7 + 9 = 16$. Pamatosim nevienādības:

$$\begin{array}{ll} (1) & S(S(S(2012^{2012}))) < 16, \\ (2) & S(S(2012^{2012})) < 79, \\ (3) & S(2012^{2012}) < 799999999. \end{array}$$

Skaitlis 79 ir mazākais, kurš dod atlikumu 7 dalot ar 9, bet kura ciparu summa ir 16. Skaitlis 799999999 ir mazākais, kurš dod atlikumu 7 dalot ar 9, bet kura ciparu summa ir 79. Tāpēc $(3) \rightarrow (2) \rightarrow (1)$.

Pierādīsim pašu pēdējo no minētajām nevienādībām, novērtējot pašu skaitli $2012^{2012}$.

$$2012^{2012} < 2100^{2100} = ((2.1)^3)^{700} \cdot (1000)^{2100} = (9.261)^{700} \cdot (1000)^{2100} < 10^{700} \cdot 10^{6300} = 10^{7000}.$$

Iegūstam, ka skaitļa $2012^{2012}$ decimālpierakstā ir ne vairāk kā 7000 cipari. Pat ja tie visi būtu deviņnieki, tad to summa nepārsniedz 63000, kas ir mazāk nekā 799999999. Tātad nevienādība (3) ir pierādīta (un tātad arī nevienādības (2) un (1)). □

Var pārbaudīt iegūto rezultātu (skaitli 7) ar aprēķinu valodā Python:

```python
def S(num):
    return sum(int(digit) for digit in str(num))

S(S(S(2012**2012)))
```

## 2.2 Kongruenču klases

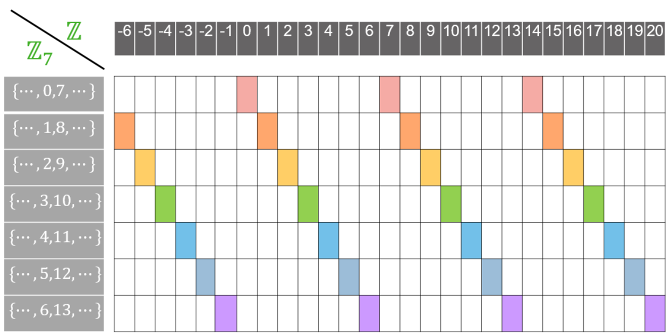
Viena mēneša ietvaros var ievērot, ka datumi $1, 8, 15, 22, 29$ nonāk tanī pašā nedēļas dienā – tādā ziņā tie ir ekvivalenti. Tāpat arī datumi $2, 9, 16, 23, 30$ visi nonāk (citā) nedēļas dienā utml. Vispārīgāk – visus veselos skaitļus (arī tos, kuri nevar būt kalendāra datumi) var sadalīt 7 ekvivalences klasēs.

**Apgalvojums:** Dots naturāls skaitlis $m$. Tad katru veselu skaitli $n$ var vienā vienīgā veidā izteikt $n = qm + r$, kur $q \in \mathbb{Z}$, bet $r \in \{0, \ldots, m-1\}$. Šajā izteiksmē $q$ ir (veselo skaitļu dalīšanas) dalījums, bet $r \in \{0, 1, \ldots, m-1\}$ ir *atlikums*.

**Definīcija:** Ja divi veseli skaitļi $n_1, n_2 \in \mathbb{Z}$ dod vienādus atlikumus, dalot ar $m$, tad sauksim tos par *kongruentiem* pēc $m$ moduļa. Pieraksts: $n_1 \equiv n_2 \pmod{m}$.

**Piemērs:** Kongruence pēc moduļa 7 sadala visus veselos skaitļus $n = 7$ klasēs. Katrā klasē ietilpst skaitļi, kas dod vienādus atlikumus pēc moduļa 7. Katru šādu klasi var aprakstīt šādi:

$$\{qk + r \mid q \in \mathbb{Z},\ r \in \{0, 1, \ldots, 6\}\}.$$



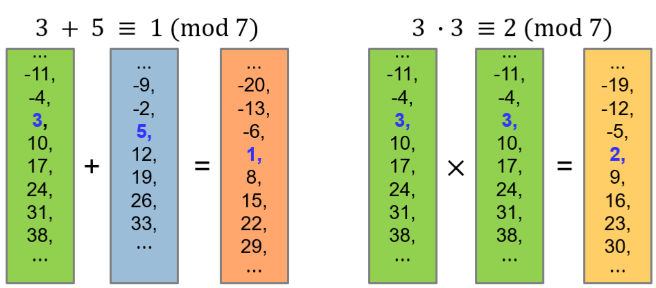

**Definīcija:** Dots vesels skaitlis $m > 1$. Ar $\mathbb{Z}_m$ apzīmēsim skaitļu kopu ar $m$ elementiem $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$, kurā var veikt saskaitīšanas, atņemšanas, reizināšanas un kāpināšanas darbības, kuru rezultāti ir atlikumi, dalot ar $m$.

**Piemērs:** $a + b$ šajā kopā dod rezultātu $c$, ja $c = (a + b) \bmod m$, kas ir atlikums, dalot $(a + b)$ ar $m$.

**Apgalvojums:** Veicot aritmētiskas darbības kopā $\mathbb{Z}_m$, skaitļu $a, b \in \mathbb{Z}_m$ vietā var izvēlēties jebkurus veselus skaitļus $a'$ un $b'$, kuri dod atlikumus attiecīgi $a$ un $b$, dalot ar $m$.

Šis apgalvojums ir spēkā, jo saskaitīšanas, atņemšanas un reizināšanas darbību atlikumu, dalot ar $m$, nosaka vienīgi operandu atlikumi, dalot ar $m$. Šajā zīmējumā parādīts, kā var saskaitīt un sareizināt kopā $\mathbb{Z}_7$. Saskaitāmo un reizinātāju 3 un 5 vietā var izvēlēties jebkuru pārstāvi no attiecīgās kongruenču klases.

Citiem vārdiem, modulārā aritmētika kongruences klašu kopā $\mathbb{Z}_7$ izkrāso visus skaitļus 7 krāsās. Un balstās uz faktu, ka saskaitot divus skaitļus ar noteiktu krāsu, rezultāta krāsa arī būs viennozīmīgi noteikta.



| | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 0 |
| 2 | 2 | 3 | 4 | 5 | 6 | 0 | 1 |
| 3 | 3 | 4 | 5 | 6 | 0 | 1 | 2 |
| 4 | 4 | 5 | 6 | 0 | 1 | 2 | 3 |
| 5 | 5 | 6 | 0 | 1 | 2 | 3 | 4 |
| 6 | 6 | 0 | 1 | 2 | 3 | 4 | 5 |

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 2 | 0 | 2 | 4 | 6 | 1 | 3 | 5 |
| 3 | 0 | 3 | 6 | 2 | 5 | 1 | 4 |
| 4 | 0 | 4 | 1 | 5 | 2 | 6 | 3 |
| 5 | 0 | 5 | 3 | 1 | 6 | 4 | 2 |
| 6 | 0 | 6 | 5 | 4 | 3 | 2 | 1 |

Fig. 1: Saskaitīšanas un reizināšanas tabulas 7 kongruenču klasēm no $\mathbb{Z}_7$.

### 2.2.1 Paritāte

Apakšgadījums kongruencēm pēc moduļa ir *paritāte*, kas visus veselos skaitļus iedala pāra skaitļos ($\equiv 0 \pmod 2$) un nepāra skaitļos ($\equiv 1 \pmod 2$).

```
p + p = p         p * p = p
p + n = n         p * n = p
n + p = n         n * p = p
n + n = p         n * n = n
```

Šajos apzīmējumos $\texttt{p} = [0]_2$ and $\texttt{n} = [1]_2$ ir abas ekvivalences klases pēc 2 moduļa.

### 2.2.2 Lietojums mūzikas teorijā

Modulāro aritmētiku var viegli iztēloties kā aritmētiku uz pulksteņa ciparnīcas. Piemēram, $14 \equiv 2 \pmod{12}$ (pulksten `2:00` un `14:00` uz ciparnīcas izskatās vienādi). Savukārt, pieskaitot 9 pie 22 (pēc 12 moduļa) iegūstam 7, jo $22 + 9 \equiv 7 \pmod{12}$. Ja kopš laika momenta `22:00` paiet 9 stundas, tad parasti saka, ka pulkstenis ir `7:00`, nevis `31:00`. Kaut arī `31:00` pauž to pašu informāciju.

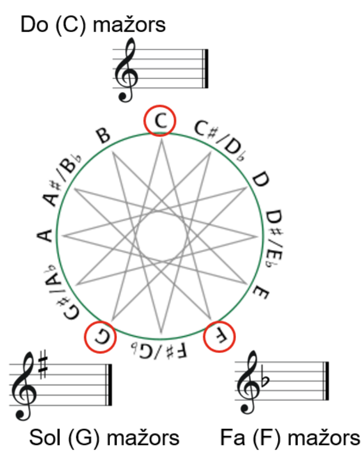



Fig. 2: “Kvintu aplis” zvaigznītes formā savieno “radniecīgus” nošu augstumus.

Līdzīgi "pulksteņa ciparnīcas aritmētikai" ir arī riņķošana pa nošu augstumiem, pārejot no vienas toņkārtas uz citu. Zīmējumā dots mūzikas teorijā pazīstamais *kvintu aplis*. Apļa augšā atrodas skaņa DO (jeb C), kuras mažora gammā nav nevienas alterācijas zīmes (diēza vai bemola). Pārlecot par kvintu (jeb 7 pustoņiem) uz priekšu, nonākam pie SOL (jeb G), kuras mažora gammā ir viens diēzs. Pēc sešiem pārlēcieniem par kvintu būsim nonākuši līdz FA diēzam (vienu pustoni uz augšu, salīdzinot ar C). Virzoties pretējā virzienā, gammai nāk klāt pa vienam bemolam. Pašu FA diēza mažoru var uzrakstīt divos veidos – vai nu kā FA diēza mažoru (kur sešas skaņas gammā ir paaugstinātas), vai arī kā SOL bemol minoru (kur sešas skaņas gammā ir pazeminātas).

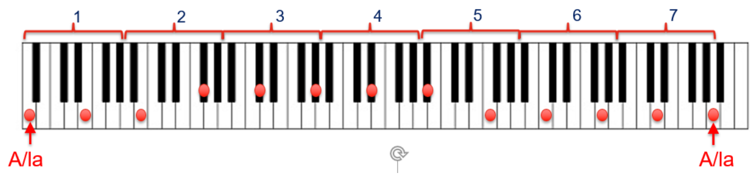



Fig. 3: Kvintu aplis uz klavierēm, aptver 7 oktāvas.

Kvintu aplis faktiski ir aritmētiska progresija ar diferenci 7 pustoņi pēc moduļa 12. Šajā progresijā apzīmējam skaņas augstumu A(la) ar 9, jo tas ir 9 pustoņus augstāk par C(do). Pēc divpadsmit soļiem virkne atgriežas sākumpunktā.

$$9,\ 4,\ 11,\ 6,\ 1,\ 8,\ 3,\ 10,\ 5,\ 0,\ 7,\ 2,\ 9 \pmod{12}$$

Mūzikā skaitlim 12 ir īpaša loma, jo oktāvu dala divpadsmit pustoņos. Savukārt skaitļu teorijas lietojumos modulārā aritmētika pēc 12 moduļa ir iespējama, bet bieži vien neērta, jo skaitļi, kuriem ir kopīgi dalītāji ar 12 (pāru skaitļi, 3 un 9) pēc šī moduļa uzvedas atšķirīgi no citiem skaitļiem. Minēto iemeslu dēļ matemātikā populārākā modulārā aritmētika ir $\pmod{p}$, kur $p$ ir jebkurš pirmskaitlis. Dažos gadījumos arī $\pmod{p^k}$ – kongruences pēc pirmskaitļu pakāpju moduļiem.

## 2.3 Kongruenču īpašības

**Apgalvojums:** Saskaitīšanas, atņemšanas un reizināšanas izteiksmēs veseliem skaitļiem rezultāta pēdējo ciparu nosaka izteiksmē ietilpstošo skaitļu pēdējie cipari.

**Piemērs:** Ar kādu ciparu beidzas $2022^{2022}$?

**Risinājums:** Saskaņā ar apgalvojumu, pietiek atrast izteiksmes $2^{2022}$ pēdējo ciparu. Izrakstot skaitļa 2 pakāpes $(1, 2, 4, 8, 16, 32, 64, \ldots)$ secinām, ka pakāpe vienmēr beidzas ar ciparu 4 tad, ja kāpinātājs dod atlikumu 2, dalot ar 4. (Piemēram, $2^2 = 4$, $2^6 = 64$, utt.) Tāpēc arī $2^{2022}$ beigsies ar ciparu 4.

### 2.3.1 Modulārā kāpināšana

Ja pakāpes bāze $a$ un kāpinātājs $k$ ir nelieli skaitļi tad pakāpes $a^k$ atlikumu dalot ar nelielu skaitli $m$, aprēķinus bieži var veikt uz papīra – pat ja skaitlis $a^k$ ir tik liels, lai to tieši izrēķināt nevarētu.

**Piemērs 1:** Atrast atlikumu, dalot $2^{1000}$ ar 17.

**Risinājums:** Ievērojam, ka $2^4 = 16 \equiv -1 \pmod{17}$. Tad $2^{1000} = (2^4)^{250} \equiv (-1)^{250} \equiv 1 \pmod{17}$.

**Piemērs 2:** Atrast atlikumu, dalot $10^6 = 1000000$ ar 7.

**Risinājums:** Pārveidojam šo pakāpi:

$$10 \cdot 10 \cdot 10 \cdot 10 \cdot 10 \cdot 10 \equiv (3 \cdot 3) \cdot (3 \cdot 3) \cdot (3 \cdot 3) \equiv 2 \cdot 2 \cdot 2 \equiv 1 \pmod{7}.$$

**Piemērs 3:** Atrast atlikumu, dalot $8^{1834}$ ar 7.

**Piemērs 4:** Atrast atlikumu, dalot $6^{2022}$ ar 7.

**Piemērs 5:** Zināms, ka skaitlis 1001 dalās ar 13. Atrast atlikumu, dalot $10^{100}$ ar 13.

Visos šajos piemēros pakāpes var pārveidot, izmantojot kāpināšanas identitātes, izrēķināt dažas apakšizteiksmes, aizstāt lielākus skaitļus ar kongruentiem, bet mazākiem skaitļiem.

Augstāk aprakstītās metodes noder, risinot nelielus piemērus uz papīra. Tomēr izrādās, ka arī visai lieliem skaitļiem kāpināšanu pēc moduļa var veikt efektīvi uz datora – un nepieciešamais darbību skaits ir nesalīdzināmi mazāks par to, kas būtu aprēķinot pašu pakāpi (nevis tās atlikumu) un arī nesalīdzināmi mazāks par to, kāds būtu, ja ar "godīgu ciklu" veiktu kāpināšanu – pat ar modulāro aritmētiku.

**Piemērs 6:** Aprēķināt $5118895664034934 1003^{48037453520941872361}$ pēc moduļa $15522299127691416427$.

```
>>> a = 51188956640349341003
>>> k = 48037453520941872361
>>> m = 15522299127691416427
>>> pow(a,k,m)
12880833635320190 64
>>> bin(k)
'0b101001101010100111010100010111011011000110000100111111010011101001'
```

Rezultātu $12880833635320190 64$ Python programma izrēķina acumirklī – tur nenotiek reizināšana $k = 48037453520941872361$ reizes (pat pēc $m$ moduļa). Tai vietā kāpinātāju $k$ pieraksta bināri - izsaka kā divnieka pakāpju summu; pēc tam skaitli $a$ atkārtoti kāpina kvadrātā, iegūstot $a^0, a^1, a^2, a^4, a^8, a^{16}, \ldots$. Un pēc tam sareizina tās pakāpes, kuras nepieciešamas, lai saliktu skaitli $k$.

Ja, piemēram, $k$ binārajā pierakstā ir 66 cipari (un 35 no tiem ir vieninieki), tad šādai kāpināšanai $a^k \pmod{m}$ vajag veikt tikai $66 - 1 + 35 = 100$ reizināšanas pēc moduļa $m$. Ievērosim, ka 100 reizināšanas darbības (pēc $m$ moduļa) ir liels uzlabojums, salīdzinot ar $\approx 48 \cdot 10^{18}$ jeb 48 kvintiljoniem reizināšanas darbību, kas prasītu ievērojamu laiku arī uz ļoti ātra datora.

### 2.3.2 Atņemšana kongruenču klasēs

Katram elementam no $\mathbb{Z}_m$ eksistē pretējais (saskaitot elementu ar tam pretējo, iegūstam 0).

$$\begin{array}{l}
-1 \equiv 6 \pmod{7} \\
-2 \equiv 5 \pmod{7} \\
-3 \equiv 4 \pmod{7} \\
-4 \equiv 3 \pmod{7} \\
-5 \equiv 2 \pmod{7} \\
-6 \equiv 1 \pmod{7}
\end{array}$$

Pretējā elementa eksistēšana nozīmē, ka kongruencei var abām pusēm pieskaitīt un atņemt tādu pašu kongruences klasi:

$$\text{Ja } x + a \equiv y + a \pmod{m}, \text{ tad } x \equiv y \pmod{m}.$$

No abām kongruences pusēm var atņemt to pašu skaitli, noīsinot abus saskaitāmos. Jebkuram naturālam modulim $m \in \mathbb{N}$ var šādi īsināt.

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 0 |
| 2 | 2 | 3 | 4 | 5 | 6 | 0 | 1 |
| 3 | 3 | 4 | 5 | 6 | 0 | 1 | 2 |
| 4 | 4 | 5 | 6 | 0 | 1 | 2 | 3 |
| 5 | 5 | 6 | 0 | 1 | 2 | 3 | 4 |
| 6 | 6 | 0 | 1 | 2 | 3 | 4 | 5 |

Saskaitīšanas tabula rāda, ka ikvienā rindiņā parādās visas iespējamās vērtības (tāpēc jebkura skaitļa pieskaitīšana pēc moduļa $m$ ir injektīva darbība – tā saglabā informāciju un tātad var atņemt to pašu konstanti no abām pusēm).

### 2.3.3 Dalīšana kongruenču klasēs

Vai no $ka \equiv kb \pmod{m}$ seko, ka $a \equiv b \pmod{m}$? Atbilde atkarīga no tā, vai reizināšana ar $k$ ir injektīva (t.i. "nesalipina" divus skaitļus) vai nē. Tikai injektīvām funkcijām eksistē inversās. Reizināšanas tabulai pēc pirmskaitļa moduļa reizināšana ir injektīva (reizināšanai eksistē inversā darbība). Vienīgais izņēmums ir reizināšana ar kongruenču klasi 0.

Savukārt reizināšanas tabula pēc salikta skaitļa satur tādas kongruenču klases (tostarp atšķirīgas no 0)), kuras reizinot var iegūt atkārtotas vērtības. Reizināšanas tabula (mod 6) ar izsvītrotiem $n$, kam $\gcd(n, 6) > 1$.

| | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 | 4 | 5 |
| 2 | 0 | 2 | 4 | 0 | 2 | 4 |
| 3 | 0 | 3 | 0 | 3 | 0 | 3 |
| 4 | 0 | 4 | 2 | 0 | 4 | 2 |
| 5 | 0 | 5 | 4 | 3 | 2 | 1 |

Piemēram kongruenču klasēm (pēc moduļa 6) ir dažas klases $(2, 3, 4)$, kuras atšķiras no 0, bet reizināšanas tabula satur atkārtotas rindas.

$$2 \cdot 3 \equiv 6 \equiv 0 \pmod{6}$$

Arī pēdējie cipari (atlikumi pēc 10) neveido injektīvu reizināšanas darbību. Piemēram, nevar viennozīmīgi atrisināt šādu kongruenču vienādojumu:

$$4x \equiv 2 \pmod{10}.$$

Eksistē divas saknes $x \equiv 3 \pmod{10}$ un $x \equiv 8 \pmod{10}$.

## 2.4 Mazā Fermā teorēma

**Teorēma:** Ja $p$ ir pirmskaitlis, tad katram $a$, kurš nedalās ar $p$ ir spēkā sakarība:

$$a^{p-1} \equiv 1 \pmod{p}$$

**Pierādījums:** Aplūkojam visus skaitļus $\{1, 2, \ldots, p-1\}$. Piereizinām tos visus ar $a$. Iegūsim $\{1 \cdot a, 2 \cdot a, \ldots, (p-1) \cdot a\}$.

Nav iespējams, ka diviem dažādiem $i, j \in \{1, 2, \ldots, p-1\}$ izpildās $i \cdot a \equiv j \cdot a \pmod{p}$. Citādi sanāktu, ka reizinājums $a(i-j)$ dalās ar $p$, kur $a$ nedalās ar $p$ un arī $(i-j) < p$. Tātad $p$ nebūtu pirmskaitlis – pretruna.

Tādēļ kopa $\{1 \cdot a, 2 \cdot a, \ldots, (p-1) \cdot a\}$ satur visas tās pašas kongruenču klases, ko $\{1, 2, \ldots, p-1\}$ (tikai, iespējams, citā secībā). Sareizinot visas šīs kongruenču klases, iegūsim

$$(p-1)!a^{p-1} \equiv (p-1)! \pmod{p}$$

Saīsinām abas kongruences puses ar faktoriālu (kurš nav kongruents ar 0, jo nevar dalīties ar $p$) un iegūstam teorēmas apgalvojumu:

$$a^{p-1} \equiv 1 \pmod{p}$$

**Sekas:** Jebkuram pirmskaitlim $p > 5$, skaitlis, kura decimālpieraksts sastāv no $p-1$ deviņniekiem dalās ar $p$.

**Piemērs:** Skaitlis no $40$ deviņniekiem $9999999999999999999999999999999999999999$ dalās ar $41$. (Faktiski, jau daudz īsāks skaitlis $99999$ dalās ar $41$, bet arī, uzrakstot šo piecu deviņnieku grupu astoņas reizes, iegūstam četrdesmit deviņniekus un arī tas dalās ar $41$. )

**Piemērs:** Pirmskaitlim $p = 7$ skaitlis $999999$ (skaitlis no $p - 1 = 6$ deviņniekiem) dalās ar $7$. (Un ar mazāku deviņnieku skaitu nepietiek.)

**Teorēma:** Ja $p$ ir nepāra pirmskaitlis un $a$ ir jebkurš skaitlis, kas nedalās ar $p$, tad

$$a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}.$$

**Pierādījums.** Zināms (M.Fermā teorēma), ka $a^p - 1$ dalās ar $p$, jeb

$$\left(a^{\frac{p-1}{2}}\right)^2 - 1 \equiv 0 \pmod{p}.$$
$$\left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \pmod{p}.$$

Ja reizinājums dalās ar $p$, tad viens no reizinātājiem dalās ar $p$. Tātad izteiksme $a^{\frac{p-1}{2}}$ ir kongruenta vai nu ar $+1$ vai ar $-1$ pēc $p$ moduļa.

**Piemērs:** Aplūkojam $p = 11$ un visas kongruenču klases pēc šī moduļa:

| $a$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| $a^5$ | 1 | 32 | 243 | 1024 | 3125 | 7776 | 16807 | 32768 | 59049 | 100000 |
| $a^5$ mod 11 | 1 | 10 | 1 | 1 | 1 | 10 | 10 | 10 | 1 | 10 |

### 2.4.1 M.Fermā teorēma un periodiskas decimāldaļas

Mazā Fermā teorēma nav tikai gari formulēts matemātikas rezultāts, kas lietojams īpašās situācijās. Tās izpausmes ir redzamas, piemēram, ikreiz, kad ar kalkulatoru dala divus veselus skaitļus.

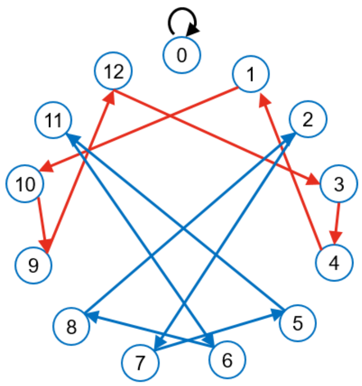
Vienkāršības dēļ aplūkosim daļas $1/p$, kur skaitli $1$ dala ar pirmskaitli $p$, bet atrastie daļu periodi der arī citām racionālām daļām ar to pašu saucēju.

Tabulā attēlots novērojums, ka $1/p$ bezgalīgās decimāldaļas perioda garums sakrīt ar mazāko $k$, kuram $10^k - 1$ (skaitlis, ko veido $k$ deviņnieki) dalās ar $p$. Un pēc Mazās Fermā teorēmas – vai nu $k = p - 1$, vai arī $k$ ir skaitļa $p - 1$ dalītājs.

| $p$ | Min.dalāmais formā $10^k - 1$ | $1/p$ kā decimāldaļa |
|---|---|---|
| 3 | $10^1 - 1 = 9$ | $1/3 = 0.(3) = 0.33\ldots$ |
| 7 | $10^6 - 1 = 999999$ | $1/7 = 0.(142857) = 0.142857142857\ldots$ |
| 11 | $10^2 - 1 = 99$ | $1/11 = 0.(09) = 0.0909\ldots$ |
| 13 | $10^6 - 1 = 999999$ | $1/13 = 0.(076923)$ |
| 17 | $10^{16} - 1$ | $1/17 = 0.(0588235294117647)$ |
| 19 | $10^{18} - 1$ | $1/19 = 0.(052631578947368421)$ |
| 23 | $10^{22} - 1$ | $1/23 = 0.(0434782608695652173913)$ |
| 29 | $10^{28} - 1$ | $1/29 = 0.(0344827586206896551724137931)$ |
| 31 | $10^{15} - 1$ | $1/31 = 0.(032258064516129)$ |
| 37 | $10^3 - 1 = 999$ | $1/37 = 0.(027) = 0.027027\ldots$ |
| 41 | $10^5 - 1 = 99999$ | $1/41 = 0.(02439)$ |
| 43 | $10^{21} - 1$ | $1/43 = 0.(023255813953488372093)$ |

Varam ar konkrētu piemēru aplūkot detalizēti, kā veidojas periodiski decimāldaļskaitļi.

**Piemērs:** Aprēķinām $1/13$, dalot stabiņā.




```
1:13=0.076923...
10
00
100
 91
  90
  78
  120
  117
    30
    26
     40
     39
      10
```

Aplūkojot šo dalīšanas algoritmu kā veselu skaitļu aritmētikas problēmu, rēķinām virkni ar atlikumiem:

$$x_n = \begin{cases} 1, & \text{if } n = 0, \\ (10 \cdot x_{n-1}) \mod 13, & \text{if } n > 0. \end{cases}$$

Pirmie šīs virknes locekļi:

$$1, 10, 9, 12, 3, 4, 1, \ldots$$

Tā kā ikviens no šīs virknes locekļiem viennozīmīgi atkarīgs no iepriekšējā (un iespējamo atlikumu ir tikai 12, jo dalīšanas rezultātā nevar rasties atlikums 0, bet var rasties citi atlikumi $\{1, \ldots, 12\}$).

Redzot, ka šīs virknes periods ir tieši seši locekļi, iegūstam, ka $x_{n+6} \equiv \left(10^6 \cdot x_n\right) \pmod{13}$. No šejienes iegūstam, ka $10^6 \equiv 1 \pmod{13}$.

Lai no periodiskas decimāldaļas atgrieztos pie racionālas daļas, aplūkojam sekojošu piemēru (kas ļaus konstruēt jebkuru periodisku daļskaitli ar periodu 6):

$$1 : 999999 = 0.000001000001000001000001\ldots = 0.(000001)$$

Par šo vienādību pārliecinās vai nu dalot stabiņā, vai arī summējot bezgalīgi dilstošu ģeometrisku progresiju, izmantojot formulu $b_1/(1-q)$, kur $b_1$ ir progresijas pirmais loceklis, bet $q$ ir tās kvocients.

$$0.(000001) = \frac{1}{10^6} + \frac{1}{10^12} + \frac{1}{10^18} + \frac{1}{10^24} + \ldots$$

$$S = \frac{b_1}{1-q} = \frac{\frac{1}{10^6}}{1 - \frac{1}{10^6}} = \frac{1}{10^6 - 1} = \frac{1}{999999}$$

Aplūkosim kādu citu periodisku daļskaitli ar periodu 6:

$$0.076923076923076923076923\ldots = 76923 \cdot 0.000001000001000001\ldots = \frac{76923}{999999}$$

Pēc noīsināšanās iegūstam, ka

$$\frac{76923}{999999} = \frac{1}{13}.$$

**Apgalvojums (Pazīme, ka n/p periodā ir k cipari):** Dots pirmskaitlis $p$ un $n$ nedalās ar $p$. Skaitlis $n/p$ ir periodiska daļa ar periodu $k$ tad un tikai tad, ja $k$ ir mazākais naturālais skaitlis, kam $10^k - 1$ dalās ar $p$.

### 2.4.2 Vingrinājumi par Mazo Fermā teorēmu

**Piemērs:** Pārveidot sekojošu periodisku decimāldaļskaitli par racionālu daļu: $0.(20221115)$.

**Piemērs:** Uzrakstīt tādu $1/p$ ($p$ ir pirmskaitlis), kura decimālpierakstā ir periods tieši no $4$ cipariem.

**Piemērs:** Kāds ir mazākais naturālu skaitļu kopas izmērs, lai no šīs kopas noteikti varētu izvēlēties tādus $a, b$ kuru piekto pakāpju starpība $a^5 - b^5$ dalītos ar $11$?

## 2.5 Pretrunas moduļa metode

Pretrunas moduļa metode parāda, ka vienādojumam nav atrisinājumu veselos skaitļos (jo vienādojuma kreisā puse ir kongruenta ar citiem atlikumiem nekā labā puse, tātad tās nevar būt vienādas). Lietojot pretrunas moduli, svarīgi ievērot šādas vadlīnijas:

- Izvēlamies tikai pirmskaitļus vai to pakāpes.
- Ja vesela izteiksme satur mainīgos arī kāpinātājos, tad var iznākt, ka pretruna parādās tikai moduļiem $m$, kas satur dažādus pirmreizinātājus. Tomēr šo pretrunu var iegūt arī aplūkojot tikai pirmskaitļa pakāpes.
- Sākam ar maziem moduļiem $2, 3, 4, 5, 7, 8, 9, 11, \ldots$.
- Izvēlamies moduļus, kas ir vienādojuma koeficientu dalītāji, samazinot vienādojuma locekļu skaitu.
- Vienādojumos, kuros figurē skaitļu k-tās pakāpes, aplūkojam moduļus $k^2$ un visus pirmskaitļus, kas izsakāmi formā $mk + 1$.

**Piemēri:** Pierādīt, ka sekojošiem vienādojumiem nav atrisinājumu veselos skaitļos:

**(A)** $y^2 - 5x^2 = 6$,

**(B)** $15x^2 - 7y^2 = 9$,

**(C)** $x^2 - 2y^2 + 8z = 9$,

**(D)** $x^3 + y^3 + z^3 = 1969^2$.

## 2.6 Eilera teorēma

Ja $n$ nav pirmskaitlis, tad arī iespējama Mazajai Fermā teorēmai līdzīga analīze, ko drīz aplūkosim. Vispirms definējam jaunu funkciju.

**Definīcija:** Funkciju $\varphi(n)$ no naturāliem skaitļiem uz naturālām vērtībām saucam par *Eilera funkciju*, ja tā saskaita, cik ir tādu naturālu skaitļu $j$ intervālā $[1; n]$, kas ir savstarpēji pirmskaitļi ar $n$.

Ja zināms skaitļa sadalījums pirmreizinātājos, Eilera funkcijas aprēķināšana ir vienkārša.

**Apgalvojums:** Ja $n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$ ir skaitļa $n$ sadalījums pirmskaitļa pakāpju reizinājumā (sadalījums pirmreizinātājos), tad Eilera funkcija:

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_m}\right).$$

Šo apgalvojumu pamatosim nodaļā *Multiplikatīvas funkcijas*. Pagaidām pieņemsim bez pierādījuma šo formulu, kas $\varphi(n)$ atrod, izmantojot $n$ pirmreizinātājus.

**Apgalvojums:** Par Eilera funkciju ir spēkā šādi apgalvojumi:

- Ja $p$ ir pirmskaitlis, tad $\varphi(p) = p - 1$.

- Ja $p^k$ ir pirmskaitļa pakāpe, tad $\varphi(p^k) = p^k - p^{k-1}$.

**Piemērs:** Ja $m = 70 = 2 \cdot 5 \cdot 7$, tad $\varphi(70) = 70 \cdot \frac{1}{2} \cdot \frac{4}{5} \cdot \frac{6}{7} = 24$.

**Piemērs:** Ja $m = 144 = 2^4 \cdot 3^2$. Iegūstam, ka $\varphi(144) = 144 \cdot \frac{1}{2} \cdot \frac{2}{3} = 48$.

**Piemērs:** Ja $m = 2022 = 2^1 \cdot 3^1 \cdot 337^1$. Iegūstam, ka $\varphi(2022) = 2022 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{336}{337} = (2-1)(3-1)(337-1) = 672$.

**Teorēma:** Ja $a$ un $n$ ir savstarpēji pirmskaitļi, tad

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

**Pierādījums:** Līdzīgi kā Mazajai Fermā teorēmai – izraksta visas kongruenču klases:

$$S = \{b_1, \ldots, b_{\varphi(n)}\}, \text{kam } \gcd(b_i, n) = 1.$$

Pēc tam reizina tās visas ar kongruenču klasi $a$. Pārliecinās, ka šī reizināšana ir injektīva, tātad tas ir kopas $S$ bijektīvs attēlojums pašai par sevi. Sareizinot visas kongruenču klases abās vienādībās, iegūsim

$$\prod_{i=1}^{\varphi(n)} b_i \equiv \prod_{i=1}^{\varphi(n)} (a \cdot b_i) \pmod{n}.$$

Pēc noīsināšanas ar visu kongruenču klašu reizinājumu, iegūstam Eilera teorēmas identitāti. □

**Piemērs.** $\varphi(10) = 4$, tādēļ katram no skaitļiem $1, 3, 7, 9$ ir spēkā sakarība $a^4 \equiv 1 \pmod{10}$. Teiksim, skaitļa 3 pakāpes ir $1, 3, 9, 27, 81, \ldots$. Iegūstam, ka $3^4$ beidzas ar to pašu ciparu, ar ko $3^0 = 1$.

Protams, cikls var iestāties arī ātrāk. Piemēram, kāpinot skaitļus, kuri beidzas ar ciparu 1, periods (pēdējā cipara atkārtošanās) vienāds ar 1. Bet tas nemaina faktu, ka $a^4 \equiv 1 \pmod{10}$. Pēdējā cipara periods var būt 1, 2 vai 4 (jo Eilera teorēma neapgalvo, ka $\varphi(n)$ būs **mazākais** kāpinātājs $k$, kuram $a^k$ ir kontruents ar 1. Toties Eilera teorēma apgalvo, ka mazākajam periodam ir jābūt $\varphi(n)$ dalītājam.

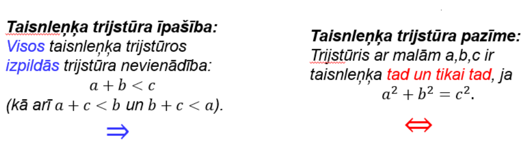
**Piemērs:** Zināms, ka $\varphi(100) = \varphi(25) \cdot \varphi(4) = (25-5)(4-2) = 40$. Iedomāsimies, ka $a$ ir skaitlis, kas nedalās ne ar 2, ne ar 5, turklāt $k$ ir mazākais naturālais skaitlis, kuram $a^k$ beidzas ar cipariem "`01`" . Kāda noteikti nevar būt $k$ vērtība?

Atbilžu varianti: **(A)** 5, **(B)** 10, **(C)** 15, **(D)** 20.

## 2.7 Dalāmības pazīmes

### 2.7.1 Kas ir pazīmes?

Matemātikā, medicīnā un citās jomās par *pazīmēm* sauc nosacījumus, kas ir nepieciešami un pietiekami kādam apgalvojumam (*necessary and sufficient conditions*). Tās atšķiramas no *īpašībām* (*necessary conditions*), kas ir nepieciešamas, bet var nebūt pietiekamas.




Pazīmes darbojas abos virzienos, tādēļ tās viegli lietot, lai "pārtulkotu" kādu apgalvojumu citā formā. Ģeometrijā sakarības starp malām vai leņķiem var norādīt uz kādas figūras speciālu īpašību. Arī skaitļu teorijā šāda tulkošana ir noderīga.

| Aprakstošs/kvalitatīvs apgalvojums | Ekvivalents/kvantitatīvs apgalvojums |
|---|---|
| Skaitlis $n$ ir pāra skaitlis | Var izteikt $n = 2k$ |
| Skaitlis $n$ ir nepāra skaitlis | Var izteikt $n = 2k + 1$ |
| Skaitlis $n$ nedalās ar 3 | $n \equiv \pm 1 \pmod 3$ |
| $n$ pieraksts beidzas ar 37 | $n \equiv 37 \pmod 1)00$ |
| $n$ pieraksts ir $\overline{abcabc}$ | $n = 1001 \cdot \overline{abc}$ |
| $a$ un $b$ nav savstarpēji pirmskaitļi | LKD$(a, b) > 1$ |
| Skaitlis $n$ ir pilns kvadrāts | Var izteikt $n = k^2$ |
| Skaitlis $x$ ir racionāls | $x = \frac{p}{q}$ |
| Skaitlis $x$ ir galīga decimāldaļa | $x = \frac{p}{2^m \cdot 5^n}$ |
| Skaitlis $n$ dalās ar 9 | $n$ ciparu summa dalās ar 9 |

### 2.7.2 Dalāmības pazīmes ar 2 un 5 pakāpēm

*Dalāmības pazīme* (*divisibility rule*) ir kāds paņēmiens, kas ļauj noskaidrot skaitļa $n$ dalāmību ar kādu nelielu skaitli $m$. Parasti dalāmības pazīme dod atbildi par dalāmību ātrāk nekā pilnvērtīga $n$ dalīšana ar $m$, piemēram, stabiņā.

Aplūkosim tās dalāmības pazīmes, kuras pārveido $n$ par kādu daudz mazāku skaitli $f(n)$, kas dod tādu pašu atlikumu, dalot ar $m$ kā sākotnējais skaitlis $n$. Tādēļ dalāmības pazīmes ne tikai paātrina aprēķinus, bet ļauj labāk saprast skaitļa decimālpierakstu.

**Teorēma (dalāmība ar 2 pakāpēm):** Jebkuram naturālam skaitlim $n$ ir spēkā sekojoši apgalvojumi:

- $n$ dalās ar 2 tad un tikai tad, ja $n$ pēdējais cipars dalās ar 2 .
- $n$ dalās ar 2 tad un tikai tad, ja $n$ pēdējie divi cipari (kā skaitlis) dalās ar 4 ($n$ beidzas ar $00, 04, 08, 12, \ldots, 96$).
- $n$ dalās ar 8 tad un tikai tad, ja $n$ pēdējie trīs cipari (kā skaitlis) dalās ar 8 ($n$ beidzas ar $000, 008, 016, \ldots, 992$).

**Teorēma (dalāmība ar 5 pakāpēm):** Jebkuram naturālam skaitlim $n$ ir spēkā sekojoši apgalvojumi:

- Skaitlis dalās ar 5 tad un tikai tad, ja tā pēdējais cipars dalās ar 5 (beidzas ar ciparu 0 vai 5).
- Skaitlis dalās ar 25 tad un tikai tad, ja tā pēdējo divu ciparu veidotais skaitlis dalās ar 25 (beidzas ar $00, 25, 50, 75$).
- Skaitlis dalās ar 125 tad un tikai tad, ja tā pēdējo trīs ciparu veidotais skaitlis dalās ar 125 (beidzas ar $000, 125, 250, 375, 500, 625, 750, 875$).

Visas šīs dalāmības pazīmes var vispārināt arī tiem gadījumiem, ja skaitlis $n$ nedalās ar pārbaudāmo skaitli. Piemēram, var iegūt šādu apgalvojumu:

**Sekas:** Jebkuram naturālam skaitlim $n$ ir spēkā sekojošs apgalvojums: $n$ dod tādu pašu atlikumu dalot ar 4 (vai ar 25) kādu dod tā pēdējie divi cipari. Citiem vārdiem, ja $n = \overline{d_k d_{k-1} \ldots d_1 d_0}$, kur $d_i$ ir skaitļa $n$ decimālpieraksta cipari, tad

$$n \equiv \overline{d_1 d_0} \pmod 4$$
$$n \equiv \overline{d_1 d_0} \pmod{25}$$

Iemesls, kādēļ drīkst atmest visus pārējos ciparus ir tas, ka pilni simti (arī tūkstoši, desmittūkstoši utt.) dalās ar 4 un ar 25 bez atlikuma. Tie neizmaina $n$ kongruences klasi.

Minētos rezultātus var vispārināt arī dažiem citiem skaitļiem (piemēram, atrodot dalāmības pazīmi ar $10, 20, 40, 50$ utt.).

Tabulā redzamas visas iespējamās kombinācijas ar skaitļu 2 un 5 pakāpēm un to reizinājumiem. Izceltajās tabulas šūnās ierakstīti skaitļi $(16, 80, 400, 2000, 10000, 5000, 2500, 1250, 625)$, kuru dalāmības noskaidrošanai pietiek aplūkot skaitļa $n$ pēdējos 4 ciparus. Visus desmittūkstošu (un vēl vecākus) ciparus var atmest, jo 10000 dalās ar visiem nosauktajiem skaitļiem.

| | | | | | |
|---|---|---|---|---|---|
| 1 | 2 | 4 | 8 | 16 | 32 |
| 5 | 10 | 20 | 40 | 80 | 160 |
| 25 | 50 | 100 | 200 | 400 | 800 |
| 125 | 250 | 500 | 1000 | 2000 | 4000 |
| 625 | 1250 | 2500 | 5000 | 10000 | 20000 |
| 3125 | 6250 | 12500 | 25000 | 50000 | 100000 |

Runājot par dalāmības pazīmēm, skaitļi $k = 2^m 5^n$ ieņem īpašu vietu. Katram no tiem eksistē mazākā desmitnieka pakāpe, kas dalās ar $k$. Dalāmības pazīme var atmest ciparus, kuru pozīcija (vieta decimālpierakstā no labās puses) ir lielāka par $\max(m, n)$.

### 2.7.3 Dalāmības pazīmes ar 3, 9

**Teorēma:** Ar $S(n)$ apzīmējam skaitļa $n$ ciparu summu. Tad $S(n) \equiv n \pmod 9$.

**Pierādījums:** Sākotnējais skaitlis ir

$$n = \overline{d_k d_{k-1} d_{k-2} \ldots d_2 d_1 d_0} == d_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + d_1 \cdot 10 + d_0$$

Šeit $d_i$ apzīmē ciparus. Ja šo skaitli aizstāj ar $S(n) = d_k + d_{k-1} + \ldots + d_1 + d_0$, tad reizinātājs pie jebkura cipara $d_j$ bija $10^j$, bet kļuva 1. No viena decimālpieraksta ir samazinājums par šādu lielumu:

$$\left(10^j d_j - d_j\right) = \underbrace{\overline{9999\ldots9999}}_{j \text{ deviņnieki}}$$

Skaitlim samazinoties par $(10^j - 1)d_j$, atlikums, dalot ar 9, nemainās.

**Sekas:** Katram naturālam skaitlim ir spēkā kongruence $n \equiv S(n) \pmod 3$.

**Sekas:** Skaitlis $n$ dalās ar 9 (vai ar 3) tad un tikai tad, ja ciparu summa $S(n)$ dalās ar 9 (vai ar 3).

---

**Note:** Citu skaitļu, izņemot 3 un 9) ar līdzīgu dalāmības pazīmi nav. Šeit izmantojam faktu, ka veselie skaitļi $9, 99, 999, ldots$ visi dalītos ar $3$ vai ar $9$.

---

### 2.7.4 Dalāmības pazīmes ar 11 kā arī 7 un 13

Naturāla skaitļa decimālpieraksts ir $n = \overline{d_{2k-1} d_{2k-1} d_{2k-2} \ldots d_2 d_1 d_0}$. (Ja skaitlī ir nepāra skaits ciparu, tad tam priekšā pieraksta nulli tā, lai ciparu skaits būtu tieši $2k$.) Apzīmējam atsevišķi pāru un nepāru ciparu summas šajā skaitlī.

$$S_0(n) = \sum_{j=0}^{k-1} d_{2j} = d_0 + d_2 + d_4 + \ldots + d_{2k-2}$$

$$S_1(n) = \sum_{j=0}^{k-1} d_{2j+1} = d_1 + d_3 + d_5 + \ldots + d_{2k-1}$$

Tātad $S_0(n)$ apzīmē skaitļa $n$ vienu ciparu plus simtu ciparu plus desmittūkstošu ciparu, utt. Savukārt $S_1(n)$ apzīmē skaitļa $n$ desmitu ciparu plus tūkstošu ciparu plus simttūkstošu ciparu, utt.

**Teorēma:** Katram naturālam $n$, $S_0(n) - S_1(n) \equiv n \pmod{11}$.

**Pierādījums:** Sākotnējais skaitlis ir

$$n = \overline{d_{2k-1}d_{2k-1}d_{2k-2}\ldots d_2d_1d_0} =$$
$$= d_{2k-1}10^{2k-1}a_{2k-2}10^{2k-2} + \ldots + d_2 10^2 + d_1 10^1 + d_0.$$

Visas pāra pakāpes $10^{2j}$ dod atlikumu 1, dalot ar 11, bet visas nepāra pakāpes $10^{2j+1}$ dod atlikumu $-1$, dalot ar 11. Tas seko no fakta, ka $10 \equiv (-1) \pmod{11}$.

Tāpēc skaitlim $n$ spēkā šāda kongruence:

$$d_{2k-1}10^{2k-1} + a_{2k-2}10^{2k-2} + \ldots + d_2 10^2 + d_1 10^1 + d_0 \equiv$$
$$\equiv d_{2k-1} \cdot (-1) + d_{2k-2} \cdot 1 + \ldots + d_2 \cdot 1 + d_1 \cdot (-1) + d_0 \cdot 1 \equiv$$
$$\equiv (d_{2k-2} + d_{2k-4} + \ldots + d_2 + d_0) + (d_{2k-1} + d_{2k-3} + \ldots + d_3 + d_1) \equiv$$
$$\equiv S_0(n) - S_1(n) \pmod{11}.$$

**Sekas:** Skaitlis dalās ar 11 tad un tikai tad, ja tā ciparu summa, kas atrodas pāra pozīcijās, mīnus ciparu summa, kas atrodas nepāra pozīcijās, dalās ar 11.

**Teorēma:** Dots naturāls skaitlis $n \in \mathbb{N}$; $n = \overline{d_{3k-1}d_{3k-2}d_{3k-3}\ldots d_2d_1d_0}$. Grupējam tā ciparus pa trīs, skaitot no labās puses, un izveidojam summu ar mainītām zīmēm $1, -1, 1, -1, \ldots$.

$$S_3(n) = \overline{d_2d_1d_0} - \overline{d_5d_4d_3} + \overline{d_8d_7d_6} - \ldots + (-1)^k\overline{d_{3k-1}d_{3k-2}d_{3k-3}}.$$

Skaitlis $S_3(n)$ apmierina kongruences $S_3(n) \equiv n \pmod{m}$, kur $m = 7, 11, 13$ vai $m = 1001$.

**Piemērs:** $n = 62510448$. Papildinām to līdz deviņiem cipariem: $n = (062)(510)(448)$. Iegūstam $S_3(62510448) = 448 - 510 + 062 = 0$. Tā kā 0 dalās ar jebko, tad $n = 62510448$ dalās ar 7, 11, 13 un arī 1001.

**Piemērs:** $n = 729183$. Iegūstam $S_3(n) = 183 - 729 = -546$. Tā kā $S_3(n) = -546$ dalās ar 7 un 13, tad arī 729183 dalās ar 7 un 13 (bet ne ar 11).

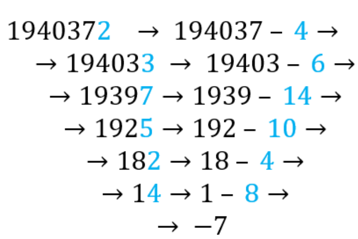
### 2.7.5 Citas dalāmības pazīmes

Ir virkne tādu dalāmības pazīmju, kas ļauj pārbaudīt dalāmību ar kādu skaitli :math;` m` , bet lieto tādus pārveidojumus, kas nesaglabā kongruenci pēc $m$ moduļa. Sk. apkopojumu http://www.savory.de/maths1.htm.

**Teorēma:** Naturāls skaitlis $n$ dalās ar 7 tad un tikai tad, ja nosvītrojot pēdējo ciparu, divkāršojot to un atņemot no "saīsinātā" skaitļa, rezultāts dalās ar 7. Citiem vārdiem, ja $n = 10a + b$, kur $b$ ir skaitļa pēdējais cipars, tad

$$7 \mid 10a + b \ \leftrightarrow \ 7 \mid a - 2b.$$

Attēlā redzama dalāmības pazīmes ar 7 lietošana lielam skaitlim:



### 2.7.6 Vingrinājumi dalāmības pazīmēm

**Piemērs:** Atrast $S_0(n)$ un $S_1(n)$ dotajiem skaitļiem; pārbaudīt to dalāmību ar $11$.

- $n = 1331$.
- $n = 14641$.
- $n = 1001$.
- $n = 979$.
- $n = 16808$.

**Definīcija:** Skaitļa decimālpierakstu sauc par *palindromu*, ja ciparu virkne ir identiska, to lasot no abiem galiem. Piemēram, $44$ un $131$ ir palindromi, bet $1431$ nav, jo, lasot no otra gala, veidojas cits skaitlis $1341$.

**Piemērs:** Vai piecciparu palindroms var būt pirmskaitlis? Vai sešciparu palindroms var būt pirmskaitlis?

**Risinājums:** Tā kā palindromā pastāv simetrija starp cipariem, kuri ir vienādi tālu no sākuma un beigām, tad (izņemot skaitli 11) nebūs palindromu-pirmskaitļu, kuros ir pāru skaits ciparu. Tas seko no dalāmības pazīmes ar 11. Savukārt piecciparu palindromus atras nav grūti – jau $10001$, $10101$, $10201$ ir salikti skaitļi. Bet jau $10301$ ir pirmskaitlis.

**Piemērs:** Autobusa biļetei ir sešciparu numurs no $000000$ līdz $999999$. Kādu biļešu ir vairāk: tādu, kuru numuru pirmo trīs ciparu summa ir vienāda ar pēdējo trīs ciparu summu, vai tādu, kuru numurs dalās ar $11$?

**Piemērs:** Pēc kārtas izrakstīti visu naturālo skaitļu (no 1 līdz 2016) kubu decimālpierakstu cipari:

$$1827641252163435127291000\ldots 8193540096$$

(Pēdējie cipari apzīmē to, ka $2016^3 = 8193540096$.) Atrast atlikumu, šo garo skaitli dalot ar $9$.

**Piemērs:** Pamatot sekojošu dalāmības pazīmi ar $13$: "Skaitlis dalās ar $13$ tad un tikai tad, ja šim skaitlim nosvītrojot pēdējo ciparu, četrkāršojot to un pieskaitot "saīsinātajam" skaitlim, iegūtais rezultāts dalās ar $13$. Citiem vārdiem, ja $n = 10a + b$, kur $b$ ir skaitļa pēdējais cipars, tad

$$13 \mid 10a + b \;\leftrightarrow\; 13 \mid a + 4b.$$

Vai skaitļa $n = 10a+b$ aizstāšana ar $n' = a+4b$ saglabā skaitļa kongruences klasi? Citiem vārdiem, vai $n \equiv n' \pmod{13}$?

## 2.8 Periodiski procesi

Ja kādā sistēmā ir galīgs skaits stāvokļu un katru nākamo stāvokli viennozīmīgi nosaka viens vai daži iepriekšējie stāvokļi. tad sistēmas stāvokļi pēc kāda laika sāk periodiski atkārtoties.

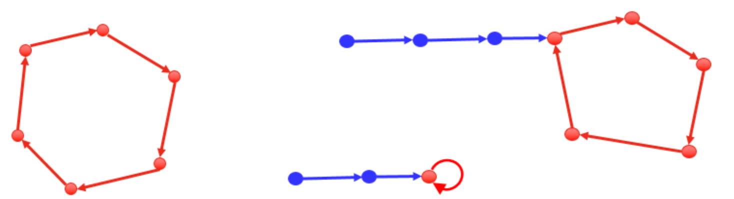
**Piemēri:**

- Naturālu skaitļu aritmētisku progresiju atlikumi $(\mathrm{mod}\ m)$.
- Naturālu skaitļu ģeometrisku progresiju atlikumi $(\mathrm{mod}\ m)$.
- Fibonači virknes locekļu atlikumi (piemēram, pēdējie 2 cipari Fibonači virknes locekļiem).
- Ciparu virkne aiz komata skaitļa $\frac{P}{Q}$ decimālpierakstā.

Visi šie procesi ir periodiski. Dažreiz virkne ir *tīri periodiska* (periods sākas jau no paša sākuma), citreiz virknei ir priekšperiods (*prefix*) un tā kļūst periodiska sākot ar kādu vietu, bezgalīgi atkārtojot vienu un to pašu periodu (*repetend*). Sk. https://bit.ly/3tHRQBv

### 2.8.1 Kādos gadījumos rodas priekšperiods

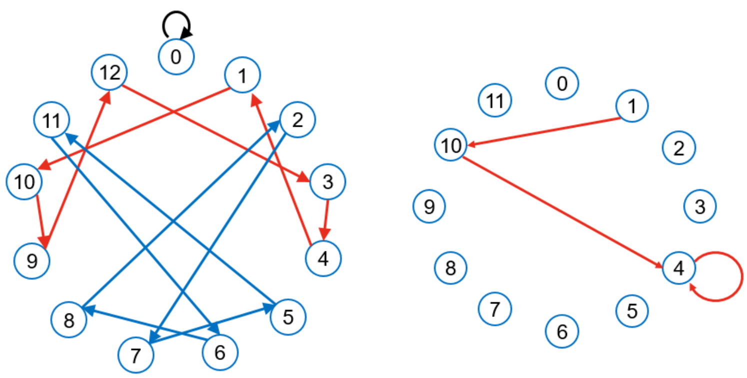
Attēlā redzami trīs grafi ar stāvokļu pārejas bultiņām. Pirmajam no tiem nav priekšperioda (visas bultiņas ir sarkanas), pārējiem diviem ir priekšperiods (aiz zilajām bultiņām seko sarkanā bultiņa - stabils/bezgalīgs periods).



Šie attēli ilustrē racionālu skaitļu izteikšanu bezgalīgu decimāldaļu veidā:

$$\frac{7}{13} = 0.(538461) = 0.538461538461538461\ldots$$
$$\frac{7}{12} = 0.58(3)\ldots = 0.58333\ldots$$
$$\frac{2020}{5125} = 0.39414634414634\ldots$$

Dalot ar 13 nav priekšperioda (skaitlis ir tīri periodisks ar sešu ciparu periodu). Dalot ar 12 ir divu ciparu priekšperiods un tad periods no viena cipara. Dalot ar $5125 = 125 \cdot 41$ ir trīs ciparu priekšperiods un tad piecu ciparu periods.




Kāpēc veselu skaitļu dalīšana var noved pie šiem atšķirīgajiem gadījumiem? Aplūkojam dalīšanu stabiņā kā stāvokļu pārejas starp atlikumiem.

Dalot ar 13 stāvokļu pārejas veido parastu, "tīru" ciklu. Savukārt, dalot ar 12, atlikumam 4 "iedur" divas bultiņas. Ja $10a \equiv 4 \pmod{12}$, tad iespējamas divas situācijas: vai nu $a = 4$, vai arī $a = 10$.

**Jautājumi par periodiskām virknēm** Katrai no virknēm noteikt, vai tā ir tīri periodiska vai arī periodiska no kādas vietas (un ja ir, tad atrast tās periodu un arī priekšperiodu).

- **(A)** Virknes $1$; $1+2$; $1+2+3$; $1+2+3+4$; ... pēdējais cipars?
- **(B)** Katram naturālam $n$ definējam $b_n$, kas ir virknes $n!$ pēdējais nenulles cipars.
- **(C)** Fibonači skaitļu virknes $F(n)$ pēdējie divi cipari (Fibonači skaitļa atlikums, dalot ar 100).
- **(D)** Virkne, kas satur locekli $+1$, ja $\sin\left(\frac{13\pi n}{7}\right) > 1$, bet $-1$ pretējā gadījumā. Šeit $n \in \mathbb{N}$ ir patvaļīgs naturāls skaitlis.
- **(E)** Atlikums, dalot $a^n$ ar $b$, kur $a, b$ ir abi naturāli.
- **(F)** Pēdējie 4 cipari $5^n$ pierakstā?
- **(G)** Skaitļa $\sin\left(\frac{n}{10}\right)$, $n \in \mathbb{N}$ zīme?

**(H)** $n$-tais cipars aiz komata skaitļa $7/13$ decimālpierakstā?

**Risinājumi:**

**(A)** Virkne ir periodiska – periods ir 20.

**(B)** Faktoriālam katru nākamo elementu viennozīmīgi nosaka iepriekšējais, Tomēr pēdējais nenulles cipars viennozīmīgi neizriet no iepriekšējā faktoriāla pēdējā nenulles cipara. (Tas gan **nav** pierādījums, ka virkne nav periodiska, bet tajā neizpildās nepieciešamais periodiskuma nosacījums).

**(C)** Fibonači skaitļa pēdējie divi cipari viennozīmīgi nenosaka nākamā locekļa pēdējos divus ciparus. Bet Fibonači skaitļu pārītis nosaka. Tādēļ ir periodiska.

**(D)** Ja $n$ pārlec $14$ vienības uz priekšu, tad sinusa zīme (un arī vērtība) nemainās.

**Piemērs:** Vai eksistē Fibonači skaitlis, kura decimālpieraksts beidzas ar divām nullēm?

**Piemērs:** Cik ir tādu $n$, kam $5^n \equiv 25 \pmod{10000}$ ?

**Piemērs:** Cik ir tādu $n$, kam $17^n \equiv 1 \pmod{100000}$? Citiem vārdiem, $17^n$ decimālpieraksts beidzas ar cipariem `00001`.

**Ieteikumi:** Visos gadījumos jānoskaidro, vai process, kurš ieciklojas, ir viennozīmīgi apvēršams.

Salīdzinām, teiksim $7/41$ decimālpierakstu ar $712$ decimālpierakstu. Pirmajam no skaitļiem nav pusperioda, tas uzreiz aiz komata sāk 5 ciparu periodu. Savukārt, dalot ar 12, rodas pusperiods.

## 2.9 Uzdevumi

**1.jautājums (BW.2018.18):** Dots tāds naturāls skaitlis $n \geq 3$, ka $4n+1$ ir pirmskaitlis. Pierādiet, ka $n^{2n}-1$ dalās ar $4n+1$.

**Atrisinājums:** No Fermā teorēmas tieši seko, ka $n^{4n}-1$ dalās ar $4n+1$. Jo $n^{p-1} \equiv 1 \pmod{p}$.

Bet par kongruenču klasi $n^{2n}$ ir divas iespējas. Ja šīs klases kvadrāts ir 1, tad pati klase varētu būt gan $+1$, gan arī $-1$.

**2.jautājums (BW.2016.1):** Atrast visus pirmskaitļu pārus $(p, q)$, kuriem

$$p^3 - q^5 = (p+q)^2.$$

**Atrisinājums:** Izrakstām iespējamās starpības $p^3 - q^5$ un meklēsim tajā pilnus kvadrātus. Šai izteiksmei jābūt nenegatīvai, lai tā būtu vienāda ar $(p+q)^2$.

| $p=$ | 2 | 3 | 5 | 7 | 11 | 13 | 17 | 19 |
|---|---|---|---|---|---|---|---|---|
| $q=2$ | – | – | 93 | 311 | 1299 | 2165 | 4881 | 6827 |
| $q=3$ | – | – | – | 100 | 1088 | 1954 | 4670 | 6616 |
| $q=5$ | – | – | – | – | – | – | 1788 | 3734 |

Aplūkojam atlikumu pārīšus (pēc 3 moduļa)

| $p$ | $q$ | $p^3$ | $q^5$ | $(p+q)^2$ | $p^3 - q^5 \equiv (p+q)^2$ |
|---|---|---|---|---|---|
| $\equiv 0$ | $\equiv 0$ | $\equiv 0$ | $\equiv 0$ | $\equiv 0$ | `true` |
| $\equiv 0$ | $\equiv 1$ | $\equiv 0$ | $\equiv 1$ | $\equiv 1$ | `false` |
| $\equiv 0$ | $\equiv 2$ | $\equiv 0$ | $\equiv 2$ | $\equiv 1$ | `true` |
| $\equiv 1$ | $\equiv 0$ | $\equiv 1$ | $\equiv 0$ | $\equiv 1$ | `true` |
| $\equiv 1$ | $\equiv 1$ | $\equiv 1$ | $\equiv 1$ | $\equiv 1$ | `false` |
| $\equiv 1$ | $\equiv 2$ | $\equiv 1$ | $\equiv 2$ | $\equiv 0$ | `false` |
| $\equiv 2$ | $\equiv 0$ | $\equiv 2$ | $\equiv 0$ | $\equiv 1$ | `false` |
| $\equiv 2$ | $\equiv 1$ | $\equiv 2$ | $\equiv 1$ | $\equiv 0$ | `false` |
| $\equiv 2$ | $\equiv 2$ | $\equiv 2$ | $\equiv 2$ | $\equiv 1$ | `false` |

Pārliecināmies, ka skaitlim $p$ vai $q$ ir jādalās ar 3; tātad kāds no tiem ir vienāds ar 3 (jo ir pirmskaitlis). Pārskatot nedaudzos gadījumus ar pirmskaitli 3, iegūsim, ka $(p, q) = (7, 3)$ ir vienīgais atrisinājums.

**3.jautājums (BWTST.2018.13):** Vai eksistē tāds pirmskaitlis $q$, ka nevienam pirmskaitlim $p$ skaitlis

$$\sqrt[3]{p^2 + q}$$

nav naturāls?

**Atrisinājums:** Ja $q = 2$, tad nesanāk, jo $5^2 + 2 = 3^3$ ir pilns kubs.

Ja $q = 3$, tad sanāk. Pierādījuma shēma – "pretrunas modulis" Atrodam tādu $m$, ka $p^2$ dod nelielu atlikumu skaitu, dalot ar $m$. Tad arī $p^2 + 3$ dod nedaudzus, paredzamus atlikumus. Vienlaikus var panākt, ka šādi atlikumi ir neiespējami naturāla skaitļa kubam $a^3$.

Nepāru skaitļu pilniem kvadrātiem ir izdevīgi aplūkot atlikumus, dalot ar 8 –- tas arī būs mūsu pretrunas modulis.

Ievērojam, ka jebkurš nepāru skaitļu kvadrāts $n^2$ dod atlikumu 1, dalot ar 8. (Lai par to pārliecinātos, apzīmējam $n = 2k + 1$. Tad $(2k + 1)^2 = 4k^2 + 4k + 1 = 4k(k + 1) + 1$. Tieši viens no $k, k + 1$ ir pāru skaitlis, tātad reizinājums $4k(k + 1)$ dalās ar 8.)

Esam pārbaudījuši, ka $\sqrt[3]{p^2 + 3}$ nav vesels skaitlis, jo vai nu $p^2 + 3 = 7$ (ja $p = 2$), vai arī $p^2 + 3$ dod atlikumu 4, dalot ar 8 Tas nav iespējams, jo visu pāru skaitļu kubi dalās ar 8.