***DAUGAVPILS UNIVERSITĀTE***
***Dabaszinātņu un matemātikas fakultāte***
***Matemātikas katedra***

# Daugavpils Universitātes Jauno matemātiķu skola

# Veselo skaitļu teorija - 3

***Docētājs: Dr. P. Daugulis***

***2008./2009.studiju gads***

# Saturs

# 1. Modulārā aritmētika - atlikumu klases un to īpašības

## 1.1. Motivācija

### 1.1.1. Pāra un nepāra skaitļi

**1.1. piemērs.** Vai var samainīt 35 latus izmantojot 10 "monētas" ar vērtībām $1, 3, 5$ lati?

Vai ir iespējams salikt mağisko kvadrātu no pirmajiem 16 pirmskaitļiem?

Uz papīra lapas ir uzrakstīti skaitļi $1, 2, ..., 2009$. Ir atļauts izvēlēties jebkurus divus skaitļus, nodzēst tos un to vietā uzrakstīt to starpības absolūto vērtību. Atļauts šādu darbību veikt vairākas reizes. Vai var panākt, ka beigās paliks 0? (nepāra skaitļu skaita paritāte)

Nepāra pakāpju virsotņu skaits grafā.

### 1.1.2. Atlikumu pētīšana

Fiksēsim veselu (parasti naturālu) skaitli $m$.
Pētīsim skaitļu atlikumus dalot ar $m$.

**1.2. piemērs.** Pierādīt, ka $n^2 + 1$ nedalās ar 3 nekādam $n \in \mathbb{Z}$.

## 1.2. Definīcijas

Fiksēsim veselu skaitli $m$. Teiksim, ka divi veseli skaitļi $a$ un $b$ ir *salīdzināmi* vai *kongruenti* pēc moduļa $m$, apzīmē ar pierakstu

$$a \equiv b(\text{mod m}),$$

tad un tikai tad, ja

- $a - b$ dalās ar $m$,
- citos terminos, skaitļi $a$ un $b$ dalījumā ar $m$ dod vienādu atlikumu.

**1.3. piemērs.** $2 \equiv 5(\text{mod } 3)$, $4 \equiv -3(\text{mod } 7)$,

## 1.3. Atlikumu un kongruences vienkāršākās īpašības

**1.1. teorēma.**

1. $a = b \implies a \equiv b \pmod{m}, \forall m,$
1' $\exists\, m : a \not\equiv b \pmod{m} \implies a \neq b,$
2. $a \equiv b \pmod{m} \iff b \equiv a \pmod{(-m)},$
3. $m = \pm 1 \implies a \equiv b \pmod{m},$
4. $m' | m \implies \Big( a \equiv b \pmod{m} \implies a \equiv b \pmod{m'} \Big),$
5. $a \equiv b \pmod{m}$ un $a \equiv b \pmod{m'} \implies a \equiv b \pmod{\text{MKD}(m,m')}.$

PIERĀDĪJUMS

1. acīmredzami;
1' no iepriekšējā;
2. ja $a \equiv b \pmod{m}$, tad $a - b = qm = (-q)(-m)$, un otrādi,
3. $a - b = (a - b) \cdot 1 = (b - a)(-1),$

4. ja $m|a-b$ un $m'|m$, tad saskaņā ar dalāmības tranzitivitāti $m'|a-b$,
5. katram pirmskaitlim $p$, kas piedalās $m$ un $m'$ faktorizācijās, $a-b$ dalās ar tā augstāko kārtu attiecībā uz $m$ vai $m'$, tā kā divu pirmskaitļu pakāpes ir savstarpēji pirmskaitļi, tad no tā, ka $a-b=q_1p_1^{\alpha_1}$ un $a-b=q_2p_2^{\alpha_2}$ ir seko, ka $p_1^{\alpha_1}p_2^{\alpha_2}|a-b$, turpinot šādu secinājumu virkni uz visiem pirmskaitļiem, iegūsim, ka $MKD(m,m')|a-b$.

■

**1.2. teorēma.**

1. $a\equiv b\ (\text{mod m}) \implies ak\equiv bk\ (\text{mod mk})$;
2. $d|a$, $d|b$ un $LKD(d,m)=1 \implies$
$$\left(a\equiv b\ (\text{mod m}) \implies \frac{a}{d}\equiv\frac{b}{d}\ (\text{mod m})\right);$$
3. $d|a$, $d|b$ un $d|m \implies$
$$\left(a\equiv b\ (\text{mod m}) \implies \frac{a}{d}\equiv\frac{b}{d}\ (\text{mod }\frac{m}{d})\right);$$

PIERĀDĪJUMS

1. Ja $a - b = mq$, tad $ak - bk = (mk)q$.

2. Tā kā $a = a_1 d$ un $b = b_1 d$, tad $a - b = (a_1 - b_1)d = q_3 m$. Tā kā $LKD(d, m) = 1$, tad $m | a_1 - b_1$, tātad $a_1 \equiv b_1 \pmod{\text{m}}$.

3. Šajā gadījumā ir dots, ka $a = dq_1$, $b = dq_2$ un $m = dq_3$. Ja $a - b = mq$, tad $dq_1 - dq_2 = dq_3 q$ un $q_1 - q_2 = q_3 q$. Seko, ka

$$q_1 \equiv q_2 (\text{mod } q_3).$$

■

## 1.4. Atlikumu un kongruences aritmētiskās īpašības

**1.3. teorēma.** Ja $a \equiv b \pmod{m}$ un $a' \equiv b' \pmod{m}$, tad

1. $a + a' \equiv b + b' \pmod{m}$;
2. $aa' \equiv bb' \pmod{m}$;
3. $a^n \equiv b^n \pmod{m}$.

PIERĀDĪJUMS

1. $m|a-b$ un $m|a'-b' \implies m|(a-b)+(a'-b')$. Bet $(a-b)+(a'-b') = (a+a')-(b+b')$, tātad $m|(a+a')-(b+b')$.

2. Apskatīsim starpību $aa' - bb'$:

$$aa' - bb' = aa' - ab' + ab' - bb' = a(a'-b') + b'(a-b).$$

$m|a-b$ un $m|a'-b' \implies m|aa'-bb'$.

3. Seko no 2.apgalvojuma. ■

**1.4. piemērs.** Atrast atlikumu, ko iegūst, dalot $2009^{2009}$ ar 7.

**1.4. teorēma.** Ja $f(x)$ ir polinoms ar veseliem koeficientiem, tad katram $m \in \mathbb{Z}$ $a \equiv b \pmod{m} \implies f(a) \equiv f(b) \pmod{m}$.

PIERĀDĪJUMS Izmantosim matemātisko indukciju pēc polinoma pakāpes ■

**1.1. piezīme.** Pierādītā teorēma kopā apgalvojumu - ja eksistē $m$ tāds, ka izpildās nosacījums

$$a \not\equiv b \pmod{m} \implies a \neq b$$

- ir viens no veidiem kā pierādīt, ka vienādojumam vai vienādojumu sistēmai neeksistē atrisinājums veselos skaitļos:

1. meklējam risinājumus vienādojumam

   $$f(x) \equiv 0 (\mathrm{mod}\ m),$$

   ar nelielām vai īpaši izvēlētām $m$ vērtībām.

2. Ja ir iespējams atrast veselu skaitli $m$, tādu, ka vienādojumam $f(x) \equiv 0 \pmod{m}$ nav atrisinājumu, tad vienādojumam $f(x) = 0$ nav atrisinājumu.

Lai pierādītu, ka vienādojumam

$$f(x) \equiv 0 \pmod{\mathrm{m}}$$

nav atrisinājumu, pietiek apskatīt galīgu skaitu variantu -

$$0 \leq x \leq m - 1.$$

Diemžēl ne vienmēr šāds pierādījums ir iespējams - eksistē vienādojumi, kas ir atrisināmi pēc visiem moduļiem, bet nav atrisināmi veselos skaitļos.

**1.2. piezīme.** Pierādot, ka vienādojumam nav veselu atrisinājumu ar modulārās aritmētika palīdzību, ir svarīgi atrast labu moduli $m$. Var izmantot šādas idejas:

- pārbaudīt mazus pirmskaitļus,
- pārbaudīt koeficientu dalītājus (tad atbilstošie koeficienti būs 0).

**1.5. piemērs.** Pierādiet, ka vienādojumam $x^2 - 2 = 5y^2$ nav veselu atrisinājumu (mod 4 vai mod 5).

Pierādiet, ka vienādojumam $x^2 + y^2 = 4n + 3$ nav veselu atrisinājumu (mod 4).

# 1.5. Ekvivalence un atlikumu klases

## 1.5.1. Kongruences attiecība kā ekvivalence

**1.5. teorēma.** Skaitļu salīdzināmībai pēc fiksēta moduļa $m$ ir spēkā šādas īpašības:

1. katrs skaitlis $a$ ir salīdzināms ar sevi - $a \equiv a$ (*refleksivitāte*),
2. ja $a \equiv b$, tad $b \equiv a$ (*simetrija*),
3. ja $a \equiv b$ un $b \equiv c$, tad $a \equiv c$ (*tranzitivitāte*).

PIERĀDĪUMS

1. $m|a-a$.

2. $m|a-b \implies a-b=qm,\ b-a=(-q)m \implies m|b-a$.

3. Ja $m|a-b$ un $m|b-c$, tad $a-b=qm$ un $b-c=q'm$. Saskaitot šīs vienādības, iegūsim $a-c=(q+q')m$, tāpēc $m|a-c$. ■

**1.3. piezīme.** No šīs teorēmas seko, ka skaitļi dalās klasēs atkarībā no to atlikuma mod $m$.

### 1.5.2. Salīdzināmības pēc moduļa $m$ attiecības klases

Salīdzināmības attiecībai atbilstošā veselo skaitļu kopas sadalījuma apakškopas vai klases sauc par *atlikumu klasēm pēc moduļa* $m$.

Katrā atlikumu klasē ir visi veselie skaitļi, kas dalījumā ar $m$ dod vienu un to pašu atlikumu.

**1.6. piemērs.** Piemēram, ja $m = 2$, tad $\mathbb{Z} = C_0 \bigcup C_1$, kur $C_0$ ir 0 klase - pāra skaitļi un $C_1$ ir 1 klase - nepāra skaitļi.

Ja $m = 3$, tad $\mathbb{Z} = C_0 \bigcup C_1 \bigcup C_2$, kur $C_0$ ir 0 klase - skaitļi formā $3k$, $C_1$ ir 1 klase - skaitļi formā $3k + 1$, $C_2$ ir 2 klase - skaitļi formā $3k + 2$.

**1.6. teorēma.** Atlikumu klašu skaits pēc moduļa $m$ ir vienāds ar $|m|$.

PIERĀDĪJUMS Atlikums dalot ar $m$ var būt vesels skaitlis robežās no 0 līdz $|m| - 1$, tātad klašu skaits ir $|m|$.■

Jebkuru kopas $\mathbb{Z}$ apakškopu, kas satur tieši vienu elementu no katras atlikumu klases, sauksim par *klašu pārstāvju kopu*. Par *kanonisko klašu pārstāvju kopu sauksim kopu*

$$\{0, 1, ..., |m| - 1\}.$$

Ja $m$ ir nepāra skaitlis, tad var izmantot arī atlikumu klašu pārstāvju kopu, kas ir simetriska attiecībā uz 0:

$$\{-\frac{|m|-1}{2}, ... -1, 0, 1, ..., \frac{|m|-1}{2}\}, \text{ja m ir nepāra skaitlis.}$$

Skaitlim $n$ atlikumu klasi $\pi_m(n) = \overline{n}$ sauksim par $n$ *redukciju pēc moduļa* $m$.

## 1.6. Operācijas ar atlikumu klasēm

Fiksēsim skaitli $m$. Par divu atlikumu klašu (pēc moduļa $m$) $C$ un $C'$ summu $C + C'$, sauksim klasi $\pi_m(a + a')$, kur $a \in C$ un $a' \in C'$.

Par divu atlikumu klašu $C$ un $C'$ reizinājumu $CC'$, sauksim klasi $\pi_m(aa')$, kur $a \in C$ un $a' \in C'$.

Atlikumu klašu pārstāvju kopu pēc moduļa $m$ ir pieņemts izvēlēties kā $\{\overline{0}, ..., \overline{m-1}\}$.

**1.7. piemērs.** Atlikumu klases pēc moduļa 5 var identificēt ar kopu $\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$.

Redzam, ka pēc moduļa 5 izpildās šādas vienādības:

$2 + 3 \equiv 0$, $2 \cdot 3 \equiv 1$,

$3 + 3 \equiv 1$, $3 \cdot 3 \equiv 4$. u.t.t.

**1.4. piezīme.** Par atlikumu klašu kopu var domāt kā par veselo skaitļu kopu, kas ir "uztīta" uz riņķa līnijas. Atbilstoši var interpretēt operācijas ar atlikumu klasēm.

**1.7. teorēma.** Katram $m$ un visiem veseliem skaitļiem $a$ un $b$ ir spēkā sakarības

$$\pi_m(a+b) = \pi_m(a) + \pi_m(b)$$

un

$$\pi_m(ab) = \pi_m(a)\pi_m(b).$$

PIERĀDĪJUMS Ja $a = q_1 m + r_1$ un $b = q_2 m + r_2$, tad

$$a + b = (q_1 + q_2)m + (r_1 + r_2)$$

un

$$ab = q_1 q_2 m^2 + (q_1 + q_2)m + r_1 r_2,$$

tātad $a + b \equiv r_1 + r_2$ un $ab \equiv r_1 r_2$. Tā kā $\pi_m(a) \equiv r_1$ un $\pi_m(b) \equiv r_2$, tad apgalvojums ir pierādīts.■

# 1.7. Atlikumu aritmētikas pielietojumi

## 1.7.1. Pozicionālais pieraksts

Senajos laikos cilvēki izmantoja primitīvu skaitļu pierakstu, kas pēc būtības ir līdzīgs svītriņu vilkšanai (*nepozicionālās sistēmas*), piemēram:

- viena svītriņa - vieninieks vai viens objekts,
- pārsvītrota svītriņa (X) - desmitnieks vai desmit objekti,
- īpaši simboli (hieroglifiskajās sistēmās), kas apzīmē 100 u.t.t.
- burti (alfabētiskās sistēmas senajā Grieķijā un Izraēlā)

Šādā pierakstā simbola vietai nav lielas nozīmes. Parasti simboli tika sakārtoti noteiktā kārtībā, piemēram, lielākā svara simboli atradās pieraksta sākumā.

Problēmas - ar šādu pierakstu grūti veikt aritmētiskās operācijas.

Būtiskas izmaiņas notika tad, kad cilvēki sāka pierakstīt skaitļus tā, lai simbola atrašanās vietai būtu lielāka nozīme - *pozicionālajās sistēmās*. Tāds pieraksts tika ieviests Indijā ap 500 AD. Viduslaikos tas tika pārņemts Eiropā un tiek izmantots līdz pat mūsu dienām.

**1.8. teorēma.** Ja $m > 1$ ir vesels skaitlis, tad jebkurš naturāls skaitlis $n$ ir viennozīmīgi izsakāms formā

$$n = \sum_{i=0}^{k} a_i m^i,$$

kur $a_k \neq 0$ un katram $i$ izpildās nosacījums $0 \leq a_i < m$.

PIERĀDĪJUMS Aprakstīsim algoritmu, ar kura palīdzību var atrast skaitļus $a_i$:

1. Izdalīsim $n$ ar $m$:
$$n = q_1 m + a_0;$$
2. Izdalīsim $q_1$ ar $m$:
$$q_1 = q_2 m + a_1,$$

ievērosim, ka

$$n = q_1 m + a_0 = (q_2 m + a_1)m + a_0 = q_2 m^2 + a_1 m + a_0;$$

3. Izdalīsim $q_2$ ar $m$:

$$q_2 = q_3 m + a_2,$$

ievērosim, ka

$$n = q_2 m^2 + a_1 m + a_0 =$$
$$(q_3 m + a_2)m^2 + a_1 m + a_0 =$$
$$q_3 m^3 + a_2 m^2 + a_1 m + a_0;$$

... ...

Algoritms tiek uzskatīts par pabeigtu, kad kārtējais dalījums ir vienāds ar 0 - pēdējais nenulles atlikums ir $a_k$.

Ievērosim, ka algoritma izpilde vienmēr apstājas, jo dalījumu virkne $q_1, q_2, ...$ ir stingri dilstoša.

Algoritma izpildes rezultātā iegūsim skaitļu virkni $(a_0, a_1, ..., a_k)$, kas apmierina vienādību

$$n = a_k m^k + a_{k-1} m^{k-1} + ... + a_2 m^2 + a_1 m + a_0,$$

tātad skaitļu virkne, kas ir deklarēta teorēmas apgalvojumā, eksistē.

Pierādīsim šādas skaitļu virknes $(a_0, a_1, ..., a_k)$ vienīgumu. Pieņemsim, ka eksistē divi izvirzījumi

$$n = a_k m^k + a_{k-1} m^{k-1} + ... + a_2 m^2 + a_1 m + a_0 = b_k m^k + b_{k-1} m^{k-1} + ... + b_2 m^2 + b_1 m + b_0$$

un sāksim salīdzināt skaitļus $a_i$ un $b_i$ sākot no $i = 0$:

1. Reducēsim $n$ pēc moduļa $m$: $n \equiv a_0 \equiv b_0 \pmod{m}$, tāpēc

$$a_0 = b_0,$$

2. Reducēsim $\frac{n-a_0}{m}$ pēc moduļa $m$:

$$\frac{n-a_0}{m} = a_k m^{k-1} + ... + a_2 m + a_1 \equiv a_1 \equiv$$
$$b_k m^{k-1} + ... + b_2 m + b_1 \equiv b_1 \pmod{\text{m}},$$

tāpēc

$$a_1 = b_1,$$

3. Reducēsim $\frac{n-a_0-a_1 m}{m^2}$ pēc moduļa $m$:

$$\frac{n-a_0-a_1 m}{m^2} = a_k m^{k-2} + ... + a_3 m + a_2 \equiv a_2 \equiv$$
$$b_k m^{k-2} + ... + b_3 m + b_2 \equiv b_2 \pmod{\text{m}},$$

tāpēc

$$a_2 = b_2,$$

■

**1.5. piezīme.** Skaitļa izvirzījumu $m$ pakāpju lineārās kombinācijas veidā sauksim par skaitļa *m-āro pozicionālo pierakstu* (vai par *m-adisko pierakstu*) un apzīmēsim ar $\overline{a_k a_{k-1} \ldots a_0}_m$ vai kādā vienkāršākā veidā, ja nav riska pārprast pierakstu. Pēc noklusēšanas pieņemsim $\overline{a_k a_{k-1} \ldots a_0} = \overline{a_k a_{k-1} \ldots a_0}_{10}$. Skaitli $m$ sauksim par pieraksta *bāzi*.

**1.6. piezīme.** Mūsdienās cilvēki gandrīz vienmēr strādā ar decimālo pierakstu ($m = 10$), arī ciparu skaits ir saskaņots ar šo $m$ vērtību.

Plašāk pielietotie pieraksti datorzinātnēs un datortehnoloģijās -

- $m = 2$ - *binārais* pieraksts, simbolus $0, 1$ sauc par *bitiem*,
- $m = 8$ - *oktālais* pieraksts,
- $m = 16$ (ar cipariem 0,1,2,3,4,5,6,7,8,9,$A = 10$,$B = 11$,$C = 12$,$D = 13$,$E = 14$,$F = 15$) - *heksadecimālais* pieraksts.

**1.7. piezīme.** No binārā pieraksta seko šāds neacīmredzams fakts - katru naturālu skaitli var viennozīmīgi izteikt kā 2 pakāpju summu.

**1.8. piezīme.** Algoritms skaitļa $n$ pārveidošanai no decimālās sistēmas uz $m$-āro sistēmu:

1. izdalīt $n$ ar $m$: $n \to (q_1, a_0)$, kur $n = q_1 m + a_0$, ja $q_1 \neq 0$, tad iet tālāk;
2. izdalīt $q_1$ ar $m$: $(q_1, a_0) \to (q_2, a_1)$, kur $q_1 = q_2 m + a_1$, ja $q_2 \neq 0$, tad iet tālāk;
3. izdalīt $q_2$ ar $m$: $(q_2, a_1) \to (q_3, a_2)$, kur $q_2 = q_3 m + a_2$, ja $q_3 \neq 0$, tad iet tālāk;

... izdalīt ...

k+1. Uzrakstīt simbolus pareizā kārtībā - $\overline{a_k a_{k-1} \ldots a_0}_m$;

k+2. Veikt pārbaudi: $a_k m^k + a_{k-1} m^{k-1} + \ldots + a_0 \stackrel{?}{=} n$.

**1.8. piemērs.** Pārveidosim skaitli 2007 5-ārajā pierakstā:

1. $2007 = 401 \cdot 5 + 2 \rightarrow a_0 = 2, q_1 = 401$;
2. $401 = 80 \cdot 5 + 1 \rightarrow a_1 = 1, q_2 = 80$;
3. $80 = 16 \cdot 5 + 0 \rightarrow a_2 = 0, q_3 = 16$;
4. $16 = 3 \cdot 5 + 1 \rightarrow a_3 = 1, q_4 = 3$;
5. $3 = 0 \cdot 5 + 3 \rightarrow a_4 = 3, q_5 = 0$;
6. Pierakstām rezultātu $2007 = \overline{31012}_5$;
7. Veicam pārbaudi: $3 \cdot 5^4 + 1 \cdot 5^3 + 0 \cdot 5^2 + 1 \cdot 5^1 + 2 = 1875 + 125 + 5 + 2 = 2007$.

**1.9. piezīme.** Algoritms skaitļa $n$ pārveidošanai no $m$-ārās sistēmas uz decimālo sistēmu:

1. Ja ir dots skaitlis $n = \overline{a_k a_{k-1} ... a_0}_m$, aprēķināt decimālajā pierakstā summu

$$n = a_k m^k + a_{k-1} m^{k-1} + ... + a_0.$$

**1.9. piemērs.** Ja skaitlis 7-ārajā pierakstā ir $\overline{3621}_7$, tad decimālajā pierakstā tas ir $3 \cdot 7^3 + 6 \cdot 7^2 + 6 \cdot 7^1 + 1 = 1338$.

**1.10. piezīme.** Algoritms skaitļa $n$ pārveidošanai no $m_1$-ārās sistēmas uz $m_2$-āro sistēmu:

1. Pārveidot skaitli $n$ no $m_1$-ārā pieraksta uz decimālo pierakstu,
2. Pārveidot skaitli $n$ no decimālā pieraksta uz $m_2$-āro pierakstu.

**1.10. piemērs.** Pārveidosim skaitli $\overline{3621}_7$ uz heksadecimālo pierakstu:

$$\overline{3621}_7 \to 1338 \to \overline{53A}_{16}$$

**1.11. piezīme.** Pozicionālās sistēmas plusi:

- simbolu ekonomija,
- ērti veikt aritmētiskās operācijas - algoritmi visiem ir zināmi, tos var vispārināt no $m = 10$ uz jebkuru $m$ vērtību.

**1.9. teorēma.**

1. Maksimālais naturālais skaitlis, ko var ierakstīt $m$-ārajā sistēmā ar $k$ simboliem ir vienāds ar $m^{k+1} - 1$.
2. Lai skaitli $n$ ierakstītu $m$-ārajā sistēmā, ir nepieciešami

$$k_n = [\log_m n] + 1$$

simboli.

PIERĀDĪJUMS 1. Lielākais skaitlis ar $k$ simboliem $m$-ārajā pierakstā ir

$$\overline{(m-1)(m-1)...(m-1)}_m = (m-1)(1 + m + ... + m^k) = (m-1)\frac{m^{k+1} - 1}{m-1} = m^{k+1} - 1.$$

2. $n = m^{\log_m n}$, tāpēc

$$m^{[\log_m n]} \leq n < m^{[\log_m n]+1}.$$

$m$-ārajā pierakstā skaitlis $m^{[\log_m n]}$ ir $1\underbrace{000...000}_{[\log_m n] \text{ reizes}}$ ($[\log_m n]+1$ cipari) un $m^{[\log_m n]+1}$ ir $1\underbrace{000...000}_{[\log_m n]+1 \text{ reizes}}$ ($[\log_m n]+2$ cipari). Redzam, ka skaitli $n$ var pierakstīt ar $[\log_m n]+1$ ciparіem. ■

### 1.7.2. Aritmētisko operāciju pārbaude

Aritmētisko operāciju rezultātu pareizības pārbaudē var izmantot vienu no modulārās aritmētikas īpašībām:

$$a = b \implies a \equiv b \pmod{\mathrm{m}} \forall m.$$

Pretējais apgalvojums:

$$\exists m : a \not\equiv b \pmod{\mathrm{m}} \implies a \neq b.$$

Pārbaudes algoritms:

1. Atrodam operācijas rezultātu $c = a \star b$,
2. Atrodam $c' = a \star b \pmod{\mathrm{m}}$ un $c'' = c \pmod{\mathrm{m}}$),
3. Ja $c' \neq c''$, tad konstatējam kļūdu.

### 1.7.3. Dalāmības pazīmes

*Dalāmības ar $m$ pazīme* - īpašība, kas piemīt $m$ daudzkārtņu cipariem (parasti 10-ārajā pierakstā).

Šajā sadaļā pieņemam, ka

$$n = \overline{a_k a_{k-1} ... a_0} = a_k \cdot 10^k + ... + a_1 \cdot 10 + a_0.$$

Dalāmība ar 2 un vispārināšana uz $2^l$

Tā kā $10^l = 2^l \cdot 5^l \equiv 0 \pmod 2$, ja $l \geq 1$, tad

$$n \equiv a \cdot 0 + a_{k-1} \cdot 0 + ... + a_0 \equiv a_0 \pmod 2.$$

*Dalāmības pazīme ar 2:*

$$2|n \iff 2|a_0$$

(ja $n$ pēdējais cipars dalās ar 2 - pieder kopai $\{0, 2, 4, 6, 8\}$).

Tā kā $10^j = 2^j \cdot 5^j \equiv 0 \pmod{2^l}$, ja $j \geq l$, tad

$n \equiv a_{l-1} \cdot 10^{l-1} + a_{l-1} \cdot 1 + ... + a_0 = \overline{a_{l-1}a_{l-2}...a_0} \pmod{2^l}$.

*Dalāmības pazīme ar* $2^l$:

$$2^l | n \iff 2^l | \overline{a_{l-1}a_{l-2}...a_0}$$

(ja pēdējo $l$ ciparu veidotais skaitlis dalās ar $2^l$).

Dalāmība ar 3

Tā kā $10^l \equiv 1 \pmod{3}$, tad

$n \equiv a_k \cdot 1 + a_{k-1} \cdot 1 + ... + a_0 \equiv a_k + a_{k-1} + ... + a_0 \pmod{3}$.

*Dalāmības pazīme ar* 3:

$$3 | n \iff 3 | a_k + a_{k-1} + ... + a_0$$

(ja $n$ ciparu summa dalās ar 3).

Dalāmība ar 5 un vispārināšana uz $5^k$

Tā kā $10^j = 2^j \cdot 5^j \equiv 0 \pmod{5^l}$, ja $j \geq l$, tad

$$n \equiv a_{l-1} \cdot 10^{l-1} + a_{l-1} \cdot 1 + ... + a_0 = \overline{a_{l-1}a_{l-2}...a_0} \pmod{5^l}.$$

*Dalāmības pazīme ar* $5^l$:

$$5^l | n \iff 5^l | \overline{a_{l-1}a_{l-2}...a_0}$$

(ja pēdējo $l$ ciparu veidotais skaitlis dalās ar $5^l$).

Dalāmība ar 6

$6 = 2 \cdot 3$ un $LKD(2,3) = 1$, tāpēc $6|n$ tad un tikai tad, ja $2|n$ un $3|n$.

*Dalāmības pazīme ar* 6: $6|n$ tad un tikai tad, ja $n$ pēdējais cipars ir pāra skaitlis un $n$ ciparu summa dalās ar 3.

Dalāmība ar 11

Tā kā $10 \equiv -1 \pmod{11}$, tad

$$10^{2j} \equiv (-1)^{2j} \equiv 1 \pmod{11}$$

un

$$10^{2j+1} \equiv (-1)^{2j+1} \equiv -1 \pmod{11}.$$

Redzam, ka

$$n \equiv a_k(-1)^k + ... + a_2 - a_1 + a_0 \pmod{11}.$$

*Dalāmības pazīme ar* 11:

$$11|n \iff 11|a_0 - a_1 + a_2 + ... + a_k(-1)^k$$

(ja $n$ ciparu alternējoša summa dalās ar 11).

# 2. Atlikumu gredzena īpašības

Atlikumu mod $m$ kopu ar saskaitīšanas un reizināšanas operācijām (*atlikumu gredzenu mod $m$ apzīmēsim ar $\mathbb{Z}_m$*).

## 2.1. Pamatfakti

**2.1. teorēma.** Atlikumu gredzenā $\mathbb{Z}_m$ ir spēkā šādas īpašības:

1. katram $x \in \mathbb{Z}_m$ eksistē viens un tikai viens $y \in \mathbb{Z}_m$ tāds, ka
$$x + y \equiv 0(\text{mod m})$$
(*aditīvi inversā elementa eksistence un viennozīmīgums*),
2. ja $p$ ir pirmskaitlis, tad
$$xy \equiv 0(\text{mod p}) \implies x \equiv 0(\text{mod p}) \text{ vai } y \equiv 0(\text{mod p})$$
(*nulles dalītāju neeksistence*),

3. ja $p$ ir pirmskaitlis, tad katram $x \in \mathbb{Z}_p$ tādam, ka
$$x \not\equiv 0(\text{mod p})$$
eksistē viens un tikai viens $z \in \mathbb{Z}_p$, kas apmierina vienādību
$$xz \equiv 1(\text{mod p}),$$
4. ja $m$ nav pirmskaitlis, tad eksistē nenulles elementi $x$ un $y$ tādi, ka
$$xy \equiv 0(\text{mod m}),$$
5. $x$ ir invertējams attiecībā uz reizināšanu pēc moduļa $m$ (eksistē viens un tikai viens $y$ tāds, ka $xy \equiv 1(\text{mod m})$) tad un tikai tad, ja $LKD(x, m) = 1$ (*multiplikatīvi inversā elementa eksistence*).

PIERĀDĪJUMS

1. Katram $x \in \mathbb{Z}$ eksistē $y \in \mathbb{Z}$, tāds, ka $x + y = m \implies$
$$x + y \equiv (\text{mod } m).$$

$x + y_1 \equiv x + y_2 \equiv 0(\text{mod m}) \implies y_1 \equiv y_2(\text{mod m}).$

2. Ja $p$ ir pirmskaitlis, tad no tā, ka $p|xy$ seko, ka $p|x$ vai $p|y$. Pārtulkojot to atlikumu klašu terminos: ja $xy \equiv 0(\text{mod p})$, tad $x \equiv 0(\text{mod p})$ vai $y \equiv 0(\text{mod p})$.

3. Ja $p$ ir pirmskaitlis, tad jebkurš vesels skaitlis $x$ robežās no 1 līdz $p-1$ un $p$ ir savstarpēji pirmskaitļi - $LKD(x,p) = 1$, tātad saskaņā ar $LKD$ lineārās kombinācijas īpašību eksistē veseli skaitļi $a$ un $b$ tādi, ka $ax + bp = 1$ un, tādējādi

$$ax + bp \equiv ax + b \cdot 0 \equiv 1(\text{mod p}),$$

tas nozīmē, ka skaitļa $a$ klase reizinājumā ar $x$ dod klasi 1,

4. Ja $m$ nav pirmskaitlis, tad eksistē vismaz divi skaitļi $a > 1$ un $b > 1$, tādi, ka $ab = m$, no kurienes seko, ka

$$ab \equiv m \equiv 0(\text{mod m}).$$

5. Ja $LKD(x,m)=1$, tad eksistē skaitļi $a$ un $b$ tādi, ka

$$ax+bm=1$$

un reducējot abas puses pēc moduļa $m$, iegūsim, ka

$$ax+bm\equiv ax+b\cdot 0\equiv ax\equiv 1(\text{mod m}).$$

Ja eksistē divas klases $y_1$ un $y_2$ tādas, ka

$$xy_1\equiv xy_2\equiv 1(\text{mod m}),$$

tad

$$x(y_1-y_2)\equiv 0(\text{mod m}).$$

Reizinot abas puses ar $y_1$ vai $y_2$, iegūsim $y_1-y_2\equiv 0(\text{mod m})$, tātad $y_1\equiv y_2(\text{mod m})$. Ja eksistē $y$ tāds, ka $xy\equiv 1(\text{mod m})$, tad $xy-1=mq$ un $xy-mq=1$. Reducējot pēc moduļa $d=LKD(x,m)$, iegūsim $0\equiv 1(\text{mod d})$, tātad $d=1$.

■

## 2.2. Eilera funkcija un tās īpašības

Par naturāla skaitļa $n$ *Eilera funkciju* $\varphi(n)$ sauksim tādu veselu skaitļu $x$ skaitu, kuriem izpildās nosacījumi

- $0 \leq x < n$,
- $LKD(x, n) = 1$.

**2.1. piezīme.** No iepriekšējās teorēmas seko, ka to atlikuma klašu skaits pēc moduļa $m$, kurām eksistē multiplikatīvi inversais elements, ir vienāds ar $\varphi(m)$. Šādas atlikumu klases sauksim par *invertējamām pēc moduļa* $m$.

Jebkuru šādu klašu pārstāvju kopu sauksim par *reducētu atlikumu klašu kopu pēc moduļa* $m$. Kopas $\mathbb{Z}_m$ multiplikatīvi invertējamo elementu kopu apzīmēsim ar $(\mathbb{Z}_m)^\times$ vai $U_m$.

**2.1. piemērs.** $\varphi(p) = p - 1$, jo visi skaitļi kopā $\{1, ..., p-1\}$ ir savstarpēji pirmskaitļi ar $p$ un $LKD(0, p) = p$.

$\varphi(4) = |\{1, 3\}| = 2$.

$3^{-1} \equiv 3.$
$\varphi(6) = |\{1, 5\}| = 2.$
$5^{-1} \equiv 5.$
$\varphi(8) = |\{1, 3, 5, 7\}| = 4.$
$3^{-1} \equiv 3.\ 5^{-1} \equiv 5.\ 7^{-1} \equiv 7.$
$\varphi(9) = |\{1, 2, 4, 5, 7, 8\}| = 6.$
$2^{-1} \equiv 5.\ 5^{-1} \equiv 2.\ 4^{-1} \equiv 7.\ 7^{-1} \equiv 4.\ 8^{-1} \equiv 8.$

**2.2. piezīme.** No iepriekš pierādītas teorēmas seko, ka to atlikuma klašu skaits pēc moduļa $m$, kurām eksistē multiplikatīvi inversais elements, ir vienāds ar $\varphi(m)$.

**2.3. piezīme.** Ja $m \equiv m'(\text{mod n})$, tad

$$LKD(m, n) = LKD(m + nq, n) = LKD(m', n),$$

tāpēc jebkurā atlikumu klašu pārstāvju kopā to skaitļu skaits, kas ir savstarpēji pirmskaitļi ar $n$, ir vienāds ar $\varphi(n)$.

**2.2. teorēma.** Eilera funkcijai piemīt šādas īpašības:

1. Eilera funkcija $\varphi : \mathbb{N} \to \mathbb{N}$ nav ne injektīva, ne sirjektīva,
2. ja $LKD(n, m) = 1$, tad
$$\varphi(nm) = \varphi(n)\varphi(m)$$
(Eilera funkcija ir *multiplikatīva*),
3. $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$,
4. ja $n = p_1^{\alpha_1} ... p_k^{\alpha_k} = \prod_{i=1}^{k} p_i^{\alpha_i}$, tad
$$\varphi(n) = \prod_{i=1}^{k}(p_i^{\alpha_i} - p_i^{\alpha_i - 1}) = n\prod_{i=1}^{k}(1 - \frac{1}{p_i}),$$

PIERĀDĪJUMS

1. Eilera funkcija nav injektīva, jo $\varphi^{-1}(2) = \{3, 4, 6\}$. Eilera funkcija nav sirjektīva, jo $\varphi^{-1}(3) = \emptyset$.

2. Pieņemsim, ka $n$ un $m$ ir savstarpēji pirmskaitļi. Sakārtosim skaitļus no 0 līdz $nm-1$ matricā, kurā ir $m$ rindas un $n$ kolonnas šādā

veidā:

$$\begin{bmatrix} 0 & 1 & ... & n-1 \\ n & n+1 & ... & 2n-1 \\ ... & ... & ... & ... \\ n(m-1) & n(m-1)+1 & ... & nm-1 \end{bmatrix}$$

Skaitīsim, cik šajā matricā ir skaitļu, kas ir savstarpēji pirmskaitļi ar $nm$.

Ievērosim šādus faktus:

- katra rinda veido atlikumu klašu pārstāvju kopu pēc moduļa $n$ (jo katrā rindā ir $n$ pēc kārtas ejoši skaitļi),
- katrā kolonnā visi skaitļi ir kongruenti pēc moduļa $n$,
- katra kolonna veido atlikumu klašu pārstāvju kopu pēc moduļa $m$ (jo katrā kolonnā ir $m$ skaitļi formā $a + nq$, kur $0 \leq q < m$),

pēc algebriskiem pārveidojumiem redzam, ka

$$\begin{aligned} a + nq_1 \equiv a + nq_2 (\text{mod m}) &\iff \\ nq_1 \equiv nq_2 (\text{mod m}) &\iff \\ n^{-1}nq_1 \equiv n^{-1}nq_2 (\text{mod m}) &\iff \\ q_1 \equiv q_2 (\text{mod m}). & \end{aligned}$$

Ievērosim, ka

$$LKD(x, nm) = 1 \iff LKD(x, n) = 1 \text{ un } LKD(x, m) = 1.$$

Tātad ir spēkā šādi fakti:

- skaitļi $x$, kuriem $LKD(x, nm) = 1$, var atrasties tikai tajās kolonnās, kurās $LKD(x, n) = 1$, tādu kolonnu skaits ir $\varphi(n)$,
- katrā kolonnā, kur $LKD(x, n) = 1$, to skaitļu skaits, kuriem $LKD(x, m) = 1$, ir vienāds ar $\varphi(m)$.

Tādējādi $\varphi(nm) = \varphi(n)\varphi(m)$.

3. Ja $n = p^\alpha$, tad $LKD(n, m) \neq 1$ tad un tikai tad, ja $p|m$, tātad $m = p \cdot k$, kur $0 \leq p \cdot k < p^\alpha$. Redzam, ka $0 \leq k < p^{\alpha-1}$, tātad tādu skaitļu $m$ skaits ir $|\{0, p, ..., p^{\alpha-1} - 1\}| = p^{\alpha-1}$. Esam ieguvuši, ka $\varphi(n) = p^\alpha - p^{\alpha-1}$.

4. Rezultāts seko no iepriekšējiem teorēmas apgalvojumiem un algebriskiem pārveidojumiem. Sadalīsim $n$ pirmskaitļu pakāpju reizinājumā

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

Ievērosim, ka dažādu pirmskaitļu pakāpes ir savstarpēji pirmskaitļi.

Vairākas reizes pielietosim multiplikatīvo īpašību:

$$\varphi(n) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}...p_k^{\alpha_k}) = (p_1^{\alpha_1} - p_1^{\alpha_1-1})\varphi(p_2^{\alpha_2}...p_k^{\alpha_k}) = ...$$

$$(p_1^{\alpha_1} - p_1^{\alpha_1-1})\varphi(p_2^{\alpha_2})\varphi(p_3^{\alpha_3}...p_k^{\alpha_k}) = ... =$$

$$\prod_{i=1}^{k}(p_i^{\alpha_i} - p_i^{\alpha_i-1}) = \prod_{i=1}^{k} p_i^{\alpha_i}(1 - \frac{1}{p_i}) =$$

$$\prod_{i=1}^{k} p_i^{\alpha_i} \prod_{i=1}^{k}(1 - \frac{1}{p_i}) = n\prod_{i=1}^{k}(1 - \frac{1}{p_i})$$

■

**2.2. piemērs.** $\varphi(2007) = \varphi(3^2 \cdot 223) = (3^2 - 3^1) \cdot 222 = 6 \cdot 222 = 1332.$

$\varphi(2008) = \varphi(2^3 \cdot 251) = (2^3 - 2^2) \cdot 250 = 4 \cdot 250 = 1000.$ $\varphi(1000) = 400$, $\varphi(400) = 160$, ... $\varphi(160) = 64$,

## 2.3. Fermā un Eilera teorēmas

**2.3. piemērs.** Atradīsim kāpinātājus, ar kuriem invertējamie elementi ir kongruenti ar 1 gredzenos $GF(5)$, $GF(7)$.

**2.3. teorēma.** (*Fermā Mazā teorēma*) Ja $p$ ir pirmskaitlis un

$$a \not\equiv 0(\text{mod p}),$$

tad

$$a^{p-1} \equiv 1(\text{mod p})$$

PIERĀDĪJUMS Apskatīsim funkciju

$$f_a : U_p \to U_p,$$

kas tiek definēta šādi:

$$f_a(x) = ax.$$

Apskatīsim piemērus gredzenos $GF(5)$ ($a = 2$) un $GF(7)$ ($a = 2$ vai $a = 3$).

Pierādīsim, ka $f_a$ ir bijektīva funkcija:

- injektivitāte - $f_a(x_1) = f_a(x_2) \implies ax_1 \equiv ax_2$, reizinot abas puses ar $a^{-1}$, iegūsim $x_1 \equiv x_2$, tātad $f_a$ ir injektīva;
- sirjektivitāte - $\forall y \in U_p$ izpildās

$$y \equiv a(a^{-1}y) \equiv f_a(a^{-1}y),$$

tātad $f_a$ ir sirjektīva.

Tā kā $f_a$ ir bijektīva funkcija, tad reizinot ar $a$ kopas $U_p$ dažādos elementus sakārtotus kādā noteiktā kārtībā $(z_1, ..., z_{p-1})$, iegūsim tos pašus elementus citā kārtībā.

Apskatīsim reizinājumu $(az_1)(az_2) \cdot ... \cdot (az_{p-1})$ divos veidos:

- no vienas puses, pielietojot reizināšanas komutativitāti, tas ir vienāds ar

$$a^{p-1}(z_1 \cdot ... \cdot z_{p-1}),$$

- no otras puses, tas ir vienāds ar elementu $z_i$ reizinājumu kādā citā kārtībā un, pielietojot vēlreiz atlikumu klašu reizināšanas

komutativitātes īpašību, redzam, ka tas ir vienāds ar

$$z_1 \cdot ... \cdot z_{p-1}.$$

Tātad

$$a^{p-1}(z_1 \cdot ... \cdot z_{p-1}) \equiv z_1 \cdot ... \cdot z_{p-1}(\text{mod p})$$

un

$$a^{p-1} \equiv 1(\text{mod p}).$$

■

**2.4. piemērs.** $2^2 \equiv 1(\text{mod } 3)$, $2^4 \equiv 1(\text{mod } 5)$, $2^{10} \equiv 1(\text{mod } 11)$, $88^{88} \equiv 1(\text{mod } 89)$.

**2.4. teorēma.** (*Eilera teorēma*) Ja $LKD(a,m)=1$, tad

$$a^{\varphi(m)} \equiv 1(\text{mod m}).$$

PIERĀDĪJUMS Līdzīgs Fermā teorēmas pierādījumam. ■

**2.4. piezīme.** Ievērosim, ka Fermā teorēma ir Eilera teorēmas speciālgadījums.

**2.5. piezīme.** Dažreiz Fermā teorēmu formulē arī veidā

$$a^p \equiv a(\text{mod p}) \text{ vai } a^{-1} \equiv a^{p-2}(\text{mod p}).$$

**2.6. piezīme.** Fermā un Eilera teorēmu pielietojums - *ātrā kāpināšana*, ja $a \not\equiv 0(\text{mod p})$, tad :

$$a^b \equiv a^{b(\text{mod } p-1)}(\text{mod p}).$$