

*DAUGAVPILS UNIVERSITĀTE*  
*Dabaszinātņu un matemātikas fakultāte*  
*Matemātikas katedra*  
*Bakalaura studiju programma "Matemātika"*

*Studiju kurss*

# SKAITĻU TEORIJA

## 7.lekcija

*Docētājs: Dr. P. Daugulis*

*2012./2013.studiju gads*

# Saturs

<b>1. Ievads atlikumu reizināšanas īpašībās</b>	<b>4</b>
1.1. Pamatfakti . . . . .	4
1.1.1. Grupas multiplikatīvais pieraksts . . . . .	4
1.1.2. Atlikumu reizināšanas īpašības . . . . .	5
1.1.3. Multiplikatīvi invertējamas atlikumu klases . . . . .	6
1.1.4. Multiplikatīvi invertējamie atlikumi kā grupa . . . . .	8
1.1.5. Multiplikatīvās cikliskās apakšgrupas . . . . .	10
1.2. Eilera funkcija un tās īpašības . . . . .	12
1.3. Atlikuma multiplikatīvā kārtā . . . . .	15
1.3.1. Definīcija . . . . .	15
1.3.2. Fermā un Eilera teorēmas . . . . .	15
<b>2. 6.mājasdarbs</b>	<b>19</b>
2.1. Obligātie uzdevumi . . . . .	19
2.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi	20

**Lekcijas mērķis:**

- apgūt atlikumu multiplikatīvo grupu pamatīpašības.

**Lekcijas kopsavilkums:**

- var noskaidrot invertējamo atlikumu skaita funkcijas  $\varphi(m)$  īpašības un atrašanas algoritmu,
- var noskaidrot vienkāršākās atlikumu multiplikatīvās kārtas īpašības.

**Svarīgākie jēdzieni:** atlikuma multiplikatīvā kārtā, Eilera funkcija.

**Svarīgākie fakti un metodes:** ciklisko apakšgrupu īpašības multiplikatīvajā grupā, Eilera funkcijas īpašības, Fermā teorēma, Eilera teorēma.

# 1. Ievads atlikumu reizināšanas īpašībās

## 1.1. Pamatfakti

### 1.1.1. Grupas multiplikatīvais pieraksts

Grupām vispārīgā gadījumā (ne obligāti komutatīvām) lieto *multiplikatīvo pierakstu* -

- par atdalošo simbolu izmanto  $\cdot$  vai neizmanto neko,
- neitrālo elementu apzīmē ar 1,
- $x$  inverso elementu  $x^{-1}$ .
- $\underbrace{xx\dots x}_{n \text{ reizes}}$  apzīmē ar  $x^n$ .

Multiplikatīvo pierakstu izmanto skaitļu un atlikumu reizināšanā.

## 1.1.2. Atlikumu reizināšanas īpašības

### 1.1. teorēma.

$$1. p \in \mathbb{P} \implies$$

$$\left( xy \equiv 0 \pmod{p} \right) \implies \left( x \equiv 0 \pmod{p} \text{ vai } y \equiv 0 \pmod{p} \right).$$

(nulle dalītāju neeksistence mod  $p$ ),

$$2. p \in \mathbb{P} \implies \forall x \in \mathbb{Z}/p, x \not\equiv 0 \pmod{p} \exists \text{ tieši viens } z \in \mathbb{Z}/p:$$

$$xz \equiv 1 \pmod{p}.$$

(visu nenulle elementu invertējamība mod  $p$ ),

$$3. x \text{ ir invertējams attiecībā uz reizināšanu mod } m$$

$(\exists y : xy \equiv 1 \pmod{m}) \iff LKD(x, m) = 1$  (multiplikatīvi inversā elementa eksistences kritērijs).

### PIERĀDĪJUMS

$$1. p \in \mathbb{P} \implies \left( p|xy \implies p|x \text{ vai } p|y \right). \text{ Atlikumu klašu terminos:}$$

$$xy \equiv 0 \pmod{p} \implies \left( x \equiv 0 \pmod{p} \text{ vai } y \equiv 0 \pmod{p} \right).$$

2.  $p \in \mathbb{P} \implies (1 \leq x \leq p-1 \implies LKD(x, p) = 1) \implies$  saskaņā ar  $LKD$  lineārās kombinācijas īpašību  $\exists a, b \in \mathbb{Z} : ax + bp = 1 \implies$

$$ax + bp \equiv ax + b \cdot 0 \equiv \boxed{ax \equiv 1} \pmod{p}.$$

3.  $LKD(x, m) = 1 \implies \exists a, b \in \mathbb{Z} : ax + bm = 1 \implies$

$$ax + bm \equiv ax + b \cdot 0 \equiv ax \equiv 1 \pmod{m}.$$

Ja  $\exists y : xy \equiv 1 \pmod{m} \implies xy - 1 = mq$  un  $xy - mq = 1$ .  
 Reducējot mod  $d = LKD(x, m) \implies 0 \equiv 1 \pmod{d} \implies d = 1$ . ■

### 1.1.3. Multiplikatīvi invertējamas atlikumu klases

Par  $m \in \mathbb{N}$  Eilera funkciju  $\varphi(m)$  sauksim tādu  $x \in \mathbb{Z}$  skaitu, kuriem izpildās nosacījumi

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

**1.1. piezīme.**  $x \equiv x' \pmod{m} \implies \exists k \in \mathbb{Z} : x + km = x' \implies$

$$LKD(x, m) = LKD(x + km, m) = LKD(x', m),$$

tāpēc jebkurā PAK to skaitļu skaits, kas ir savstarpēji pirmskaitļi ar  $m$ , ir vienāds ar  $\varphi(m)$ .

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

Jebkuru multiplikatīvi invertējamu klašu mod  $m$  pārstāvju kopu sauksim par *invertējamu atlikumu mod  $m$  klašu kopu* ( $\mathcal{U}_m$ ).

**1.1. piemērs.**  $\mathcal{U}_p = \{[1], \dots, [p-1]\}$ , jo visi skaitļi kopā  $\{1, \dots, p-1\}$  ir savstarpēji pirmskaitļi ar  $p$  un  $LKD(0, p) = p$ .

$$\mathcal{U}_{15} = \{[1], [2], [4], [7], [8], [11], [13], [14]\}.$$

### 1.1.4. Multiplikatīvi invertējamie atlikumi kā grupa

**1.2. teorēma.**  $\forall m \in \mathbb{Z}$  ( $\mathcal{U}_m, \cdot$ ) ir galīga komutatīva grupa (*atlikumu multiplikatīvā grupa*).

#### PIERĀDĪJUMS

#### Slēgtums attiecībā uz reizināšanu

$$u, u' \in \mathcal{U}_m \implies (uu')^{-1} = u^{-1}u'^{-1} \implies uu' \in \mathcal{U}_m.$$

#### Asociativitāte un komutatīvitāte

Atlikumu reizināšana ir asociatīva un komutatīva.

#### Neitrālais elements

$1 \in \mathbb{Z}/m$  ir neitrālais elements.



## Invertējamība

$$\forall u \in \mathcal{U}_m \exists u^{-1} \in \mathcal{U}_m.$$

$$|\mathcal{U}_m| = \varphi(m) \implies \mathcal{U}_m \text{ ir galīga grupa. } \blacksquare$$

### 1.3. piezīme.

Vienkāršākās multiplikatīvās invertējamības sekas:

- invertējamos atlikumus var saīsināt kā reizinātājus:

$$a \in \mathcal{U}_m \implies \left( ab \equiv ac \pmod{m} \iff b \equiv c \pmod{m} \right),$$

- $a \in \mathcal{U}_m \implies (a^n)^{-1} = (a^{-1})^n.$

**1.3. teorēma.**  $m = p_1^{\alpha_1} \dots p_n^{\alpha_n}$ ,  $d \mid m$ . Tad

$$a \in \mathcal{U}_m \iff a \in \mathcal{U}_d, \forall d \geq 2.$$

## PIERĀDĪJUMS

$$a \in \mathcal{U}_m \iff LKD(a, m) = 1 \implies LKD(a, d) = 1 \forall d|m, d \geq 2 \\ \implies a \in \mathcal{U}_d.$$

$$a \in \mathcal{U}_d, \forall d \geq 2 \implies LKD(a, d) = 1 \implies LKD(a, m) = 1 \implies \\ a \in \mathcal{U}_m. \blacksquare$$

**1.4. teorēma.**  $\begin{cases} a \notin \mathcal{U}_m \\ b \in \mathbb{Z}_m \end{cases} \implies ab, ba \notin \mathcal{U}_m.$

PIERĀDĪJUMS

$$ab \in \mathcal{U}_m \implies \exists x \in \mathbb{Z}_m : (ab)x = 1 \implies a(bx) = 1 \implies a \in \mathcal{U}_m \\ \text{- pretruna. } \blacksquare$$

### 1.1.5. Multiplikatīvās cikliskās apakšgrupas

Atlikuma  $a \in \mathcal{U}_m$  cikliskā apakšgrupa

$$\langle a \rangle = \{a^n\}_{n \in \mathbb{Z}} = \{1, a, a^2, \dots, a^{-1}, a^{-2}, \dots\}.$$

**1.2. piemērs.**  $m = 13$ .  $\langle 2 \rangle = \mathcal{U}_{13}$ .

**1.5. teorēma.**  $a \in \mathcal{U}_m$ . Tad  $\langle a \rangle = \{a, a^2, \dots, \underbrace{a^k}_{\equiv 1}\}$ , kur  $k$  ir minimālais naturālais skaitlis:  $a^k \equiv 1 \pmod{m}$  ( $a$  multiplikatīvā kārtā).

PIERĀDĪJUMS Virknē  $(a, a^2, a^3 \dots)$  elementi pēc galīga skaita soļu veikšanas atkārtosies:

$$\exists i < j : a^i \equiv a^j \pmod{m} \implies a^{j-i} \equiv 1 \pmod{m} \implies$$

$$\exists \text{ minimālais naturālais } k : a^k \equiv 1 \pmod{m} \implies$$

$$a^n \equiv a^{atl(n,k)} \pmod{m}. \blacksquare$$

## 1.2. Eilera funkcija un tās īpašības

Atšķirībā no aditīvās grupas, pat  $|\mathcal{U}_m| = \varphi(m)$  nav viegli atrodamas.

### 1.6. teorēma.

1.  $LKD(n, m) = 1 \implies \varphi(nm) = \varphi(n)\varphi(m)$  (Eilera funkcija ir multiplikatīva).

2.  $m = p^\alpha \implies \varphi(m) = p^\alpha - p^{\alpha-1} = m\left(1 - \frac{1}{p}\right)$ .

3.  $m = p_1^{\alpha_1} \dots p_k^{\alpha_k} = \prod_{i=1}^k p_i^{\alpha_i} \implies$

$$\varphi(m) = \prod_{i=1}^k \left(p_i^{\alpha_i} - p_i^{\alpha_i-1}\right) = m \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right).$$

### PIERĀDĪJUMS

1. Jāskaita, cik no skaitļiem  $\{0, \dots, nm-1\}$  ir savstarpēji pirmskaitļi ar  $nm$ .

$$LKD(x, nm) = 1 \iff \begin{cases} LKD(x, n) = 1 \\ LKD(x, m) = 1. \end{cases}$$

∀ vienādojumu sistēmai

$$\begin{cases} x \equiv a \pmod{n}, \text{ kur } a \in \mathcal{U}_n \\ x \equiv b \pmod{m}, \text{ kur } b \in \mathcal{U}_m \end{cases}$$

saskaņā ar KĀT ∃ tieši viens atrisinājums mod  $nm$ .

$a$  un  $b$  var ņemt neatkarīgi vienu no otra  $\implies$  šādu sistēmu skaits ir  $\varphi(n)\varphi(m)$ . ■

2. Visu atlikumu mod  $m = p^\alpha$  skaits ir vienāds ar  $p^\alpha$ . Atņemsim atlikumus, kas nav invertējami.

$$\left( LKD(p^\alpha, a) \neq 1 \iff p|a \right) \implies$$

$$a = p \cdot k, \text{ kur } 0 \leq p \cdot k < p^\alpha \implies 0 \leq k < p^{\alpha-1} \implies$$

neinvertējamu atlikumu  $a$  skaits ir

$$\left| \{0, p, \dots, p^{\alpha-1} - 1\} \right| = p^{\alpha-1} \implies \varphi(m) = p^{\alpha} - p^{\alpha-1}.$$

3. Vairākas reizes pielietosim multiplikatīvo īpašību:

$$\begin{aligned} \varphi(m) &= \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2} \dots p_k^{\alpha_k}) = (p_1^{\alpha_1} - p_1^{\alpha_1-1})\varphi(p_2^{\alpha_2} \dots p_k^{\alpha_k}) = \dots \\ &= (p_1^{\alpha_1} - p_1^{\alpha_1-1})\varphi(p_2^{\alpha_2})\varphi(p_3^{\alpha_3} \dots p_k^{\alpha_k}) = \dots = \prod_{i=1}^k (p_i^{\alpha_i} - p_i^{\alpha_i-1}) = \\ &= \prod_{i=1}^k p_i^{\alpha_i} \left(1 - \frac{1}{p_i}\right) = \prod_{i=1}^k p_i^{\alpha_i} \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right) = m \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right). \blacksquare \end{aligned}$$

**1.3. piemērs.**  $\varphi(2012) = \varphi(2^2 \cdot 503) = (2^2 - 2)(503 - 1) = 1004$ .  
 $\varphi(2013) = \varphi(3 \cdot 11 \cdot 61) = 2 \cdot 10 \cdot 60 = 1200$ .

## 1.3. Atlikuma multiplikatīvā kārtā

### 1.3.1. Definīcija

$a \in \mathcal{U}_m$  multiplikatīvā kārtā ( $P_m(a)$  vai  $P(a)$ ): mazākais  $k \in \mathbb{N}$ :

$$a^k \equiv 1 \pmod{m}.$$

**1.4. piemērs.**  $P(1) = 1$ . Atradīsim kāpinātājus, ar kuriem invertējamie elementi ir kongruenti ar 1 mod 5 un 7.

### 1.3.2. Fermā un Eilera teorēmas

### 1.7. teorēma. (*Fermā Mazā teorēma*)

$$\begin{cases} p \in \mathbb{P} \\ a \not\equiv 0 \pmod{p} \end{cases} \implies a^{p-1} \equiv 1 \pmod{p}.$$

PIERĀDĪJUMS Apskatīsim funkciju

$$f_a : \mathcal{U}_p \rightarrow \mathcal{U}_p,$$

$$f_a(x) = ax.$$

(Apskatīsim piemērus mod 5,  $a = 2$ , un 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  $x_1 \equiv x_2 \implies f_a$  ir injektīva;
- sirjektivitāte -  $\forall y \in \mathcal{U}_p : y \equiv a(a^{-1}y) \equiv f_a(a^{-1}y) \implies f_a$  ir sirjektivā.

$f_a$  ir bijektīva funkcija  $\implies$  reizinot ar  $a$  kopas  $\mathcal{U}_p$  dažādos elementus sakārtotus kādā noteiktā kārtībā  $(z_1, \dots, z_{p-1})$ , iegūsim virkni

$$(f_a(z_1), \dots, f_a(z_{p-1})) = (az_1, \dots, az_{p-1}),$$

kuru veido tie paši  $\mathcal{U}_p$  elementi, iespējams, citā kārtībā.

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

- no vienas puses, pielietojot reizināšanas komutativitāti:

$$(az_1)(az_2) \cdot \dots \cdot (az_{p-1}) = a^{p-1}(z_1 \cdot \dots \cdot z_{p-1}),$$



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

$$(az_1)(az_2) \cdot \dots \cdot (az_{p-1}) = z_1 \cdot \dots \cdot z_{p-1}.$$

Tātad

$$a^{p-1}(z_1 \cdot \dots \cdot z_{p-1}) \equiv z_1 \cdot \dots \cdot z_{p-1} \pmod{p} \implies \boxed{a^{p-1} \equiv 1} \pmod{p}. \blacksquare$$

**1.5. piemērs.**  $2^2 \equiv 1 \pmod{3}$ ,  $2^4 \equiv 1 \pmod{5}$ ,  $2^{10} \equiv 1 \pmod{11}$ .

**1.4. piezīme.** Fermā teorēmu formulē arī šādos veidos:

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

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

**1.8. teorēma.** (*Eilera teorēma*)  $LKD(a, m) = 1 \implies$

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

PIERĀDĪJUMS Līdzīgs Fermā teorēmas pierādījumam, ievērojot, ka  $LKD(a, m) = 1 \iff a \in \mathcal{U}_m$  un  $|\mathcal{U}_m| = \varphi(m)$ . ■

**1.5. piezīme.** Fermā teorēma ir Eilera teorēmas speciālgadījums.

**1.6. piezīme.** No Eilera teorēmas seko, ka  $\forall a \in \mathcal{U}_m: P_m(a) \leq \varphi(m)$ .

## 2. 6.mājasdarbs

### 2.1. Obligātie uzdevumi

6.1 Atrisināt vienādojumu  $\varphi(x) = 18$  naturālos skaitļos.

6.2 Izmantojot Fermā teorēmu, pierādīt, ka

(a)  $55^{66} \equiv 1 \pmod{67}$ .

(b)  $\forall p \in \mathbb{P} \forall a, b \in \mathbb{Z}$  izpildās

$$(a + b)^p \equiv a^p + b^p \pmod{p}.$$

6.3 Dots, ka  $a \in \mathcal{U}_m$ . Pierādīt, ka  $P_m(a) = P_m(a^{-1})$ .

6.4 Atrast elementu skaitus ar visām kārtām, kas dala  $\varphi(m)$ , ja

(a)  $m = 8$ ;

(b)  $m = 10$ ;

(c)  $m = 11$  .

6.5 Atrast  $\prod_{a=1}^{p-1} a = 1 \cdot 2 \cdot \dots \cdot (p-1) \pmod{p}$ .

## 2.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi

6.5 Pierādiet, ka ja  $p$  ir pirmskaitlis, tad

$$(a) 1^2 \cdot 3^2 \cdot \dots \cdot (p-2)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p};$$

$$(b) 2^2 \cdot 4^2 \cdot \dots \cdot (p-1)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}.$$

6.6 Pierādīt šādas Eilera funkcijas īpašības:

$$(a) \varphi(mn) = \frac{\varphi(m)\varphi(n)d}{\varphi(d)}, \text{ kur } d = LKD(m, n),$$

$$(b) m|n \implies \varphi(m) \mid \varphi(n),$$

$$(c) m \text{ ir } l \text{ dažādi nepāra pirmskaitļu dalītāji} \implies 2^l \mid \varphi(m),$$

$$(d) \sum_{t|m, t>0} \varphi(t) = m,$$

$$(e) \varphi(n^m) = n^{m-1}\varphi(n), \text{ ja } m \geq 1.$$