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

Studiju kurss

SKAITĻU TEORIJA

7.lekcija

Docētājs: Dr. P. Daugulis

2013./2014.studiju gads

Saturs

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 kārta, 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}.
- $\underbrace{xx...x}_{n \text{ reizes}}$ apzīmē ar x^n.

Multiplikatīvo pierakstu izmanto skaitļu un atlikumu reizināšanā.

1.1.2. Atlikumu reizināšanas īpašības

1.1. teorēma.

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

$$\Big(xy \equiv 0(\text{mod } p)\Big) \implies \Big(x \equiv 0(\text{mod } p) \text{ vai } y \equiv 0(\text{mod } p)\Big).$$

(*nulles dalītāju neeksistence mod* p),

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

$$xz \equiv 1(\text{mod } p).$$

(*visu nenulles elementu invertējamība mod* p),

3. x ir invertējams attiecībā uz reizināšanu mod m $(\exists\, y:\ xy \equiv 1(\text{mod } m)) \iff LKD(x,m) = 1$ (*multiplikatīvi inversā elementa eksistences kritērijs*).

PIERĀDĪJUMS

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

$xy \equiv 0(\text{mod } p) \implies \Big(x \equiv 0(\text{mod } p) \text{ vai } y \equiv 0(\text{mod } p)\Big)$.

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

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

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

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

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

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. $x \equiv x'(\text{mod m}) \implies \exists\, k \in \mathbb{Z} : x + km = x' \implies$

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

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. $\mathcal{U}_p = \{[1], ..., [p-1]\}$, jo visi skaitļi kopā $\{1, ..., p-1\}$ 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 komutativitāte

Atlikumu reizināšana ir asociatīva un komutatīva.

Neitrālais elements

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

Invertējamība

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

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

1.3. piezīme.

Vienkāršākās multiplikatīvās invertējamības sekas:

- invertējamos atlikumus var saīsināt kā reizinātājus:

$$a \in \mathcal{U}_m \implies \Big(ab \equiv ac(\text{mod } m) \iff b \equiv c(\text{mod } m)\Big),$$

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

1.4. piezīme. Multiplikatīvi invertējamie atlikumi ir izvietoti simetriski attiecībā uz 0: $LKD(a, m) = 1 \iff LKD(m - a, m) = 1.$

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

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

PIERĀDĪJUMS

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

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

1.4. teorēma. $\left\{ \begin{array}{l} a \notin \mathcal{U}_m \\ b \in \mathbb{Z}_m \end{array} \right. \implies ab, ba \notin \mathcal{U}_m.$

PIERĀDĪJUMS

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

1.1.5. Multiplikatīvās cikliskās apakšgrupas

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

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

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

1.5. teorēma. $a \in \mathcal{U}_m$. Tad $\langle a \rangle = \{a, a^2, ..., \underbrace{a^k}_{\equiv 1}\}$, kur k ir mini-mālais naturālais skaitlis: $a^k \equiv 1 (\text{mod } m)$ (a *multiplikatīvā kārta*).

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

$$\exists\, i < j : \; a^i \equiv a^j (\text{mod } m) \implies a^{j-i} \equiv 1 (\text{mod } m) \implies$$

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

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

1.2. Eilera funkcija un tās īpašības

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

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

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

PIERĀDĪJUMS

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

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

$\forall$ vienādojumu sistēmai

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

saskaņā ar ĶAT $\exists$ tieši viens atrisinājums mod nm.

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

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

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

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

neinvertējamu atlikumu a skaits ir

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

3. Vairākas reizes pielietosim multiplikatīvo īpašību:

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

$$\left(p_1^{\alpha_1} - p_1^{\alpha_1-1}\right)\varphi(p_2^{\alpha_2})\varphi(p_3^{\alpha_3}...p_k^{\alpha_k}) = ... = \prod_{i=1}^{k}\left(p_i^{\alpha_i} - p_i^{\alpha_i-1}\right) =$$

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

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 kārta

1.3.1. Definīcija

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

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

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*)

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

PIERĀDĪJUMS Apskatīsim funkciju

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

$$f_a(x) = ax.$$

(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 sirjektīva.

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

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

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

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

- no vienas puses, pielietojot reizināšanas komutativitāti:

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

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

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

Tātad

$$a^{p-1}(z_1\cdot\ldots\cdot z_{p-1}) \equiv z_1\cdot\ldots\cdot z_{p-1}(\mathrm{mod}\ p) \Longrightarrow \boxed{a^{p-1}\equiv 1}\ (\mathrm{mod}\ p).\blacksquare$$

1.5. piemērs. $2^2 \equiv 1(\mathrm{mod}\ 3)$, $2^4 \equiv 1(\mathrm{mod}\ 5)$, $2^{10} \equiv 1(\mathrm{mod}\ 11)$.

1.5. piezīme. Fermā teorēmu formulē arī šādos veidos:

$$a^p \equiv a(\mathrm{mod}\ p)$$

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

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

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

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

1.6. piezīme. Fermā teorēma ir Eilera teorēmas speciālgadījums.

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

2. 7.mājasdarbs

2.1. Obligātie uzdevumi

7.1 Atrast multiplikatīvi invertējamos elementus mod m, ja a) $m = 15$, b) $m = 24$.

7.2 Izmantojot Fermā teorēmu, pierādīt, ka

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

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

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

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

(a) $m = 8$;

(b) $m = 10$;

(c) $m = 11$.

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

7.5 Atrast $\prod_{a=1}^{p-1} a = 1 \cdot 2 \cdot \ldots \cdot (p-1) (\text{mod } p)$.

2.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi

7.5 Pierādiet, ka ja p ir pirmskaitlis, tad

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

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

7.6 Pierādīt šādas Eilera funkcijas īpašības:

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

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

(c) m ir l dažādi nepāra pirmskaitļu dalītāji $\implies 2^l \Big| \varphi(m)$,

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

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