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

Studiju kurss

Veselo skaitļu teorija

8.lekcija

Docētājs: Dr. P. Daugulis

2009./2010.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 vienkāršākā atlikuma multiplikatīvās kārtas īpašības.

Svarīgākie jēdzieni: atlikuma multiplikatīvā kārta, Eilera funkcija, vispārinātā Eilera funkcija.

Svarīgākie fakti un metodes: ciklisko apakšgrupu īpašības multiplikatīvajā grupā, Eilera funkcijas īpašības, Fermā teorēma, Eilera teorēma, Eilera teorēmas pastiprinājums, multiplikatīvās kārtas īpašības.

1. Ievads atlikumu multiplikatīvās grupas īpašībās

1.1. Pamatfakti

Agrāk tika pierādīts, ka

- multiplikatīvi invertējamo atlikumu klašu mod m kopa $\mathcal{U}_m$ ir grupa attiecībā uz atlikumu reizināšanu:
  1. $u, u' \in \mathcal{U}_m \implies uu' \in \mathcal{U}_m$,
  2. $1 \in \mathcal{U}_m$ - neitrālais elements,
  3. $u \in \mathcal{U}_m \implies \exists\, u^{-1} \in \mathcal{U}_m$- inversais elements,
- $|\mathcal{U}_m| = \varphi(m) \implies \mathcal{U}_m$ ir galīga grupa.
- $\mathcal{U}_m$ ir komutatīva grupa.
- tiek izmantots multiplikatīvais pieraksts (kaut arī grupa ir komutatīva).

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

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

PIERĀDĪJUMS

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

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

Vienkāršākās multiplikatīvās invertējamības sekas:

- invertējamos atlikumus var saīsināt kā reizinātājus:

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

- $a \in \mathcal{U}_m \implies \begin{cases} a^n a^{n'} \equiv a^{n+n'}(\text{mod } m) \\ (a^n)^{n'} \equiv a^{nn'}(\text{mod } m), \end{cases}$
- $a \in \mathcal{U}_m \implies (a^n)^{-1} = (a^{-1})^n.$

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

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

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

1.2. 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, kuram $a^k \equiv 1 (\text{mod } m)$ (*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

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

$$\begin{cases} 0 \leq x < m \\ LKD(x, m) = 1. \end{cases}$$

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 $\varphi(m)$.

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

1.3. teorēma.

1. $LKD(n, m) = 1 \implies \varphi(nm) = \varphi(n)\varphi(m)$ (Eilera funkcija ir *multiplikatīva*).
2. $m = p^\alpha \implies \varphi(m) = p^\alpha - p^{\alpha-1} = m(1 - \frac{1}{p})$.

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

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

PIERĀDĪJUMS

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

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

Sakārtosim skaitļus no 0 līdz $nm - 1$ matricā, kurā ir m rindas un n kolonnas šādā veidā:

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

Ievērosim šādus faktus:

- $\forall$ rinda veido PAK mod n (jo $\forall$ rindā ir n pēc kārtas ejoši skaitļi),
- $\forall$ kolonnā visi skaitļi ir kongruenti mod n,
- $\forall$ kolonna veido PAK mod m (jo $\forall$ kolonnā ir m skaitļi formā $a+nq$, kur $0 \leq q < m$): $a+nq_1 \equiv a+nq_2 (\text{mod m}) \iff$

$$nq_1 \equiv nq_2 (\text{mod m}) \iff$$

$$n^{-1}nq_1 \equiv n^{-1}nq_2 (\text{mod m}) \iff$$

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

Tātad

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

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

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

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

$$0 \leq k \leq p^{\alpha-1} - 1 \implies$$

neinvertējamu atlikumu a skaits ir

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

3. Vairākas reizes pielietosim multiplikatīvo īpašību:

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

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

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

1.2. piemērs. $\varphi(2007) = \varphi(3^2 \cdot 223) = (3^2 - 3^1) \cdot 222 = 6 \cdot 222 = 1332.$
$\varphi(2008) = \varphi(2^3 \cdot 251) = (2^3 - 2^2) \cdot 250 = 4 \cdot 250 = 1000.$
$\varphi(2009) = \varphi(7^2 \cdot 41) = (7^2 - 7)(41 - 1).$

1.3. Atlikuma multiplikatīvā kārta

1.3.1. Definīcija

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

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

1.3. 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

1.4. 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:

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

- 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

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

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

1.2. piezīme. Fermā teorēmu formulē arī šādos veidos:

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

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

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

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

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

1.3. piezīme. Fermā teorēma ir Eilera teorēmas speciālgadījums.

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

1.5. piezīme. Fermā un Eilera teorēmu pielietojums - *ātrā kāpināšana:* $a \not\equiv 0(\text{mod p}) \implies a^b \equiv a^{b(\text{mod } p-1)}(\text{mod p})$.

1.3.3. Eilera teorēmas pastiprinājums

$m = p_1^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$. Definēsim *vispārināto Eilera funkciju* $L(m)$:

$$L(m) = MKD\Big(\varphi(p_1^{\alpha_1}), ..., \varphi(p_k^{\alpha_k})\Big) =$$

$$= MKD\Big(p_1^{\alpha_1 - 1}(p_1 - 1), ..., p_k^{\alpha_k - 1}(p_k - 1)\Big).$$

1.5. piemērs. $\varphi(30) = 8$, $L(30) = 4$.
$\varphi(1365) = 576$, $L(1365) = 12$.

1.6. teorēma. $LKD(a, m) = 1 \implies a^{L(m)} \equiv 1 (\text{mod } m)$.

PIERĀDĪJUMS
$LKD(a, m) = 1 \implies LKD(a, p_i^{\alpha_i}) = 1, \forall i$. Pielietojot Eilera teorēmu mod $p_i^{\alpha_i}$, iegūsim kongruences

$$a^{\varphi(p_i^{\alpha_i})} = a^{p_i^{\alpha_i - 1}(p_i - 1)} \equiv 1 (\text{mod } p_i^{\alpha_i}), \forall i.$$

Definēsim $\gamma_i = \frac{L(m)}{\varphi(p_i^{\alpha_i})} \in \mathbb{N}, \forall i \implies$

$$a^{\varphi(p_i^{\alpha_i})\gamma_i} \equiv a^{L(m)} \equiv 1 (\text{mod } p_i^{\alpha_i}), \forall i.$$

Saskaņā ar ĶAT:

$$\begin{cases} a^{L(m)} \equiv 1 (\text{mod } p_1^{\alpha_1}) \\ \dots \\ a^{L(m)} \equiv 1 (\text{mod } p_k^{\alpha_k}) \end{cases} \Longrightarrow a^{L(m)} \equiv 1 (\text{mod } \underbrace{p_1^{\alpha_1} \dots p_k^{\alpha_k}}_{=m}). \blacksquare$$

1.3.4. Atlikumu multiplikatīvās kārtas īpašības

m - fiksēts, apzīmēsim $P_m(a) = P(a)$.

1.7. teorēma.

1. $a^k \equiv 1 \text{ (mod m)} \Longrightarrow k \equiv 0 (\text{mod } P(a))$.
2. $P(a) | L(m)$.

PIERĀDĪJUMS

1. Izdalīsim k ar $P(a)$:

$$k = qP(a) + r, \text{ kur } 0 \leq r < P(a) \Longrightarrow$$

$$a^k \equiv a^{qP(a)+r} \equiv (a^{P(a)})^q a^r \equiv a^r \equiv 1 \text{ (mod m)}.$$

$r \neq 0 \implies a^r \not\equiv 1$ (mod m), jo $r < P(a)$ un $P(a)$ ir a kārta. Iegūta pretruna $\implies r = 0$ un $k \equiv 0 (\text{mod } P(a))$.

2. Seko no pastiprinātās Eilera teorēmas un 1.:
$a^{L(m)} \equiv 1$ (mod m) $\implies L(m) \equiv 0 (\text{mod } P(a)) \implies P(a)|L(m)$.■

1.6. piemērs. Atlikumu kārtas var būt tikai $L(m)$ dalītāji. $m = 20$, $L(20) = 4$, $\varphi(20) = 8$. $\mathcal{U}_{20} = \{1, 3, 7, 9, 11, 13, 17, 19\}$.

$\forall\ a \in \mathcal{U}_{20} :\ P(a) \in \{1, 2, 4, 8\}$.

Invertējamo elementu kvadrāti:

$1^2 \equiv 9^2 \equiv 11^2 \equiv 19^2 \equiv 1$

$3^2 \equiv 7^2 \equiv 13^2 \equiv 17^2 \equiv (-3)^2 \equiv 9$.

$\implies P(9) = P(11) = P(19) = 2$. Visu invertējamo elementu ceturtās pakāpes ir 1, jo $9^2 \equiv 1$. Tātad tiem elementiem, kuru kārta nav ne 1, ne 2, tā ir vienāda ar 4. Šie elementi ir $3, 7, 13, 17$.

1.8. teorēma.

1. $a^{k_1} \equiv a^{k_2} \pmod{m} \iff k_1 \equiv k_2 \pmod{P(a)}$.

2. $\forall\, a \in \mathcal{U}_m : \; P(a^k) = \frac{P(a)}{LKD(k,P(a))}$.

PIERĀDĪJUMS

1. $a^{k_1} \equiv a^{k_2} \pmod{m} \Longrightarrow a^{k_1-k_2} \equiv 1 \pmod{m} \Longrightarrow$
$P(a)|k_1 - k_2 \Longrightarrow k_1 \equiv k_2 \pmod{P(a)}$.

$k_1 \equiv k_2 \pmod{P(a)} \Longrightarrow k_1 = k_2 + qP(a) \Longrightarrow$

$$a^{k_1} \equiv a^{k_2+qP(a)} \equiv a^{k_2}(a^{P(a)})^q \equiv a^{k_2} \pmod{m}.$$

2. Apzīmēsim $\begin{cases} d = LKD(k, P(a)) \\ P(a) = P'd \\ k = k'd \end{cases}$, $LKD(k', P') = 1$.

$(a^k)^l \equiv a^{kl} \equiv 1 \pmod{m} \iff kl \equiv 0 \pmod{P(a)} \iff$

$$kl = P(a)q \iff k'l = P'q \implies \begin{cases} P'|k'l \\ LKD(k', P') = 1 \end{cases} \implies$$

$P'|l \implies$ minimālā l vērtība ir $P' \implies P(a^k) = P' = \frac{P(a)}{LKD(k,P(a))}$.

■

1.6. piezīme. Seko, ka dažādo a pakāpju skaits ir vienāds ar $P(a)$.

1.7. piemērs. $p = 7$. $P(3) = 6$ un $P(3^5) = 6$. $P(3^2) = \frac{6}{LKD(2,6)} = 3$, $P(3^3) = \frac{6}{LKD(3,6)} = 2$.

2. 8.mājasdarbs

2.1. Obligātie uzdevumi

8.1 Atrisināt vienādojumus.

(a) $\varphi(x) = 18$.
(b) $\varphi(x) = \frac{x}{3}$.

8.2 Izmantojot Fermā teorēmu, pierādīt, ka

(a) $66^{66} \equiv 1 (\text{mod } 67)$.
(b) $\forall\, p \in \mathbb{P}\ \forall\, a, b \in \mathbb{Z}$ izpildās

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

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

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

(a) $m = 8$;
(b) $m = 10$;
(c) $m = 11$.

8.5 Atrisināt vienādojumus

(a) $x^3 \equiv 1 (\mathrm{mod}\ 7)$;
(b) $x^3 \equiv 1 (\mathrm{mod}\ 11)$;
(c) $x^7 \equiv 1 (\mathrm{mod}\ 13)$.

8.6 Atrast $\varphi(m)/L(m)$, ja
(a) $m = 2009$;
(b) $m = 8636355$.

2.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi

8.7 Definēsim *Karmaikla (Carmichael) funkciju* $\lambda(m)$:

$$\lambda(m) = \begin{cases} L(m), & \text{ja } m \not\equiv 0 (\mathrm{mod}\ 8), \\ \frac{L(m)}{2}, & \text{ja } m \equiv 0 (\mathrm{mod}\ 8). \end{cases}$$

Pierādīt, ka $\forall\ a \in \mathcal{U}_m :\ a^{\lambda(m)} \equiv 1 (\mathrm{mod}\ m)$.

8.8 Pierādiet, ka ja p ir pirmskaitlis, tad
(a) $1^2 \cdot 3^2 \cdot \ldots \cdot (p-2)^2 \equiv (-1)^{\frac{p+1}{2}} (\mathrm{mod}\ p)$;

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