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

Studiju kurss

SKAITĻU TEORIJA

8.lekcija

Docētājs: Dr. P. Daugulis

2012./2013.studiju gads

Saturs

Lekcijas mērķis:

- apgūt atlikumu multiplikatīvo grupu ģeneratoru - *primitīvo saķņu* teorijas pamatus,
- apgūt atlikumu multiplikatīvās grupas struktūras pamatus necikliskos gadījumos.

Lekcijas kopsavilkums:

- var pētīt invertējamus atlikumus, kuru pakāpju kopa sakrīt ar visu invertējamo atlikumu kopu - *primitīvās saknes*,
- var pētīt atlikumu mulitplikatīvās grupas struktūru gadījumos, kad tā nav cikliska, un atrast ģenerējošās kopas.

Svarīgākie jēdzieni: uzlabotā Eilera funkcija, primitīvā sakne, atlikumu multiplikatīvo grupu ģenerējošās kopas, invertējama atlikuma indekss.

Svarīgākie fakti un metodes: pastiprinātā Eilera teorēma, multiplikatīvās kārtas īpašības, primitīvās saknes ģenerējošā īpašība, primitīvo sakņu eksistence, primitīvo sakņu meklēšanas algoritmi, indeksa īpašības, primitīvo sakņu un indeksu pielietojumi vienādojumu risināšanā, atlikumu mulitplikatīvās grupas struktūra mod 2^α gadījumā.

1. Multiplikatīvās kārtas īpašības

1.1. Eilera teorēmas pastiprinājums

1.1.1. Uzlabotā Eilera funkcija

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

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

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

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

1.1.2. Teorēma

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

PIERĀDĪJUMS
$LKD(a, m) = 1 \implies LKD(a, p_i^{\alpha_i}) = 1, \forall i.$

Pielietojot Eilera teorēmu mod $p_i^{\alpha_i}$, iegūsim

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

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

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

Saskaņā ar kongruences pamatīpašību

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

1.2. Atlikumu multiplikatīvās kārtas īpašības

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

1.2. teorēma.

1. $a^k \equiv 1 \pmod{m} \implies k \equiv 0 \pmod{P(a)}$.
2. $a^{k_1} \equiv a^{k_2} \pmod{m} \iff k_1 \equiv k_2 \pmod{P(a)}$.
3. $P(a) \mid L(m)$.

PIERĀDĪJUMS

1. Izdalīsim k ar $P(a)$:

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

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

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

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

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

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

3. Seko no pastiprinātās Eilera teorēmas un 1.:
$a^{L(m)} \equiv 1 \pmod{\text{m}} \Longrightarrow L(m) \equiv 0 (\text{mod } P(a)) \Longrightarrow P(a) \Big| L(m).\blacksquare$

1.2. piemērs. $m = 20$, $L(20) = 4$, $\varphi(20) = 8$.
$\mathcal{U}_{20} = \{1, 3, 7, 9, 11, 13, 17, 19\}$. $\forall\, a \in \mathcal{U}_{20}: \ P(a) \in \{1, 2, 4\}$.
Invertējamo elementu kvadrāti:
$1^2 \equiv 9^2 \equiv 11^2 \equiv 19^2 \equiv 1$
$3^2 \equiv 7^2 \equiv 13^2 \equiv 17^2 \equiv (-3)^2 \equiv 9$.
$\Longrightarrow$ $P(9) = P(11) = P(19) = 2$. Visu invertējamo elementu ceturtās pakāpes ir 1, jo $9^2 \equiv 1 \Longrightarrow$ elementiem, kuru kārta nav ne 1, ne 2, tā ir vienāda ar 4. Šie elementi ir $3, 7, 13, 17$.

2. Atlikumu multiplikatīvās grupas struktūra

2.1. Cikliskais gadījums - primitīvās saknes

2.1.1. Cikliska apakšgrupa

G - grupa multiplikatīvajā pierakstā, $a \in G$. Apzīmēsim ar $\langle a \rangle$ kopu $\{e, a^{\pm 1}, a^{\pm 2}, a^{\pm 3}, ...\}$ - *ciklisko apakšgrupu ar ģeneratoru* a.

Minimālais $n \in \mathbb{N}$: $a^n = e$ (ja $\exists$) - a *(multiplikatīvā) kārta* $P(a)$. $|\langle a \rangle| = P(a)$, $\langle a \rangle = \{a, a^2, ..., a^{k-1}, 1\}$.

Pirmais jautājums, ko var uzdot par atlikumu multiplikatīvās grupas struktūru - kādiem m grupa $\mathcal{U}_m$ ir cikliska - var tikt multiplikatīvi ģenerēta ar vienu elementu ?

2.1.2. Primitīvās saknes (ģeneratori)

$g \in \mathcal{U}_m$ sauksim par *primitīvu sakni*, ja

$$P_m(g) = \varphi(m).$$

Citiem vārdiem sakot, g kārta ir maksimāla. Primitīvo sakņu mod m kopa - $\mathcal{G}_m$.

2.1. teorēma. (ģenerējošā īpašība) $g \in \mathcal{G}_m \implies$ mod m klases $g, g^2, ..., g^{\varphi(m)}$ veido $\mathcal{U}_m$ klašu pārstāvju kopu.

PIERĀDĪJUMS
$P_m(g) = \varphi(m) \implies g, g^2, ..., g^{\varphi(m)}$ ir dažādi mod m.

$\forall\ g^i$ ir invertējamu klašu pārstāvji $\implies \langle g \rangle = \mathcal{U}_m$. ■

2.1. piezīme. Iepriekšējā teorēma nozīmē to, ka primitīvā sakne g ir $\mathcal{U}_m$ *ģenerators:* $\mathcal{U}_m = \langle g \rangle$ un $(\mathcal{U}_m, \cdot)$ ir cikliska grupa.

2.1. piemērs.

- $m = 2$, $\{1\}$;
- $m = 3$, $\{2\}$;
- $m = 4$, $\{3\}$;
- $m = 5$, $\{2, 3\}$;
- $m = 6$, $\{5\}$;
- $m = 7$, $\{3, 5\}$;
- $m = 8$, $\emptyset$;
- $m = 9$, $\{2, 5\}$;
- $m = 10$, $\{3, 7\}$;
- $m = 11$, $\{2, 6, 7, 8\}$;
- $m = 12$, $\emptyset$;
- $m = 13$, $\{2, 6, 7, 11\}$;
- $m = 14$, $\{3, 5\}$;
- $m = 15$, $\emptyset$;

- $m = 16$, $\emptyset$;
- $m = 17$, $\{3, 5, 6, 7, 10, 11, 12, 14\}$;
- $m = 18$, $\{5, 11\}$;
- $m = 19$, $\{2, 3, 10, 13, 14, 15\}$;
- $m = 20$, $\emptyset$;
- $m = 2008$, $\emptyset$;
- $m = 2009$, $\emptyset$.
- $m = 2010$, $\emptyset$.
- $m = 2011 \in \mathbb{P}$, $\{3, 7, 11, 12, 17, 18, 19, ..., 2002, 2006\}$, kopā 528 primitīvās saknes.
- $m = 2012$, $\emptyset$.
- $m = 2013$, $\emptyset$.

2.1.3. Primitīvo saknŗu eksistence

Kad nevar būt primitīvās saknes

2.2. teorēma. m dalās ar vismaz diviem nepāra pirmskaitļiem vai ar $4p$, kur p - nepāra pirmskaitlis $\Longrightarrow$ $\mathcal{G}_m = \varnothing$.

PIERĀDĪJUMS Ideja: pierādīt, ka šajos gadījumos $L(m) < \varphi(m)$ $\Longrightarrow$ $\forall\, a \in \mathcal{U}_m\ P(a) \leq L(m) < \varphi(m)$.

m dalās ar vismaz diviem nepāra pirmskaitļiem p un q: $m = p^\alpha q^\beta n$ $\Longrightarrow$

$$L(m) = MKD\Big(p^\alpha(p-1), q^\beta(q-1), \varphi(n)\Big) < p^\alpha(p-1)q^\beta(q-1)\varphi(n) = \varphi(m)$$

($<$ tāpēc, ka $2 \Big| LKD(p-1, q-1)$).

m dalās ar $4p^\beta$: $m = 2^\alpha p^\beta n$ $\Longrightarrow$

$$L(m) = MKD\Big(2^{\alpha-1}, p^\beta(p-1), \varphi(n)\Big) < 2^{\alpha-1}p^\beta(p-1)\varphi(n) = \varphi(m).\blacksquare$$

Kad var būt primitīvās saknes

Seko, ka primitīvās saknes mod m var eksistēt (un, tādējādi, multiplikatīvā grupa $\mathcal{U}_m$ var būt cikliska) šādos gadījumos:

- $m = 2^\alpha$ vai $m = p^\alpha$, kur p - nepāra pirmskaitlis,
- $m = 2p^\alpha$, kur p - nepāra pirmskaitlis.

2.3. teorēma. $\mathcal{G}_m \neq \varnothing \iff$

- $m \in \{2, 4\}$ (citu 2 pakāpju nav),
- $m = p^\alpha$, kur p ir nepāra pirmskaitlis, $\alpha \geq 1$,
- $m = 2p^\alpha$, kur p ir nepāra pirmskaitlis, $\alpha \geq 1$.

PIERĀDĪJUMS
Pierādījuma soļi:

- pierādām, ka primitīvās saknes neeksistē, ja $m = 2^\alpha$, kur $\alpha \geq 3$,
- pierādām, ka primitīvās saknes $\exists$, ja p ir nepāra pirmskaitlis,

- pierādām, ka
  $\Big(g$ ir primitīva sakne mod $p\Big) \implies \Big(g$ vai $g+p$ ir primitīva sakne mod $p^2\Big) \implies \exists$ primitīvas saknes mod p^2,
- pierādām, ka
  $\Big(g$ ir primitīva sakne mod $p^2\Big) \implies \Big(g$ ir primitīva sakne mod p^α, kur $\alpha \geq 3\Big)$ - $\exists$ primitīvas sakne mod p^α, kur $\alpha \geq 3$;
- pierādām, ka ja g ir primitīva sakne mod p^α, $\alpha \geq 1$, tad g vai $g+p^\alpha$ ir primitīva sakne mod $2p^\alpha$ - $\exists$ primitīvas saknes mod $2p^\alpha$.

2.2. piezīme. Primitīvo sakņu atrašana dotajam p ir grūts uzdevums. Ātri algoritmi nav zināmi un nav pietiekoši daudz likumsakarību.

Artina hipotēze (saīsinātā formā): 2 ir primitīva sakne bezgalīgi daudziem pirmskaitļiem.

Ne par vienu pirmskaitli nav zināms, vai tas ir primitīvā sakne bezgalīgi daudziem pirmskaitļiem.

2.3. piezīme. Aprakstīsim naivu algoritmu primitīvo sakņu atrašanai (ja m nav pārāk liels). Atcerēsimies, ka $\mathcal{U}_m$ elementu kārtas dala $\varphi(m)$ un primitīvās saknes kārta ir vienāda ar $\varphi(m)$.

Algoritms (visu primitīvo sakņu atrašana):

1. Atradīsim $\varphi(m)$ sadalījumu pirmskaitļu pakāpju reizinājumā $p_1^{\alpha_1} ... p_k^{\alpha}$.
2. (Ir nepieciešams zināt orientētu grafu definīciju) Konstruēsim orientētu grafu Γ ar šādām īpašībām:
   - Γ virsotņu kopa ir $\mathcal{U}_m$,
   - $\exists$ šķautne $a \xrightarrow{p_i} b \iff a^{p_i} \equiv b \pmod{m}$.

   Tādējādi šajā grafā šķautnes nozīmē kāpināšanu pirmskaitļu pakāpēs. (Mūs interesē $\mathcal{U}_m$ struktūra attiecībā uz elementu kāpināšanu dažādās pakāpēs. Lai to labāk saskatītu, mēs vizualizēsim tikai kāpināšanu pirmskaitļu pakāpēs, kas dala $\varphi(m)$, jo jebkura interesanta kāpināšana ir šādu kāpināšanu kompozīcija).

3. $\mathcal{U}_m$ primitīvās saknes ir grafa Γ *avots*: virsotnes, kurām nav ieejošo šķautņu.
4. Lietderīgi ir pakāpeniski palielināt šķautņu skaitu - zīmēt apakšgrafus katram $\varphi(m)$ pirmskaitļa dalītājam un pakāpeniski samazināt avotu.

2.1.4. Invertējama elementa indekss (diskrētais logaritms)

$a, b \in \mathcal{U}_m$. s ir b *indekss ar bāzi* a *mod* m ($\mathsf{ind}_a(b)$ *vai* $\mathsf{ind}(b)$), ja

$$a^s \equiv b \pmod{\mathrm{m}}.$$

Ievērosim, ka indekss ir noteikts ar precizitāti mod $\varphi(m)$, tāpēc ka

$$a^{s+k\varphi(m)} \equiv a^s (a^{\varphi(m)})^k \equiv b \pmod{\mathrm{m}}.$$

2.2. piemērs. $p = 5$, $\mathsf{ind}_3(4) = \mathsf{ind}_2(4) = 2$, $\mathsf{ind}_3(2) = \mathsf{ind}_2(3) = 3$.

2.4. teorēma. $g \in \mathcal{G}_m \implies$

1. $\forall\ a \in \mathcal{U}_m\ \exists$ indekss pie bāzes g;
2. visas a indeksa vērtības ir kongruentas mod $\varphi(m)$.
3. $\mathsf{ind}_g : \mathcal{U}_m \to \mathbb{Z}\Big/\varphi(m)$ ir bijektīva funkcija;
4. $\mathsf{ind}_g(ab) \equiv \mathsf{ind}_g(a) + \mathsf{ind}_g(b) \pmod{\varphi(m)}$.

PIERĀDĪJUMS

1. $g \in \mathcal{G}_m \implies \forall\ a \in \mathcal{U}_m$: $a \equiv g^s \pmod{\text{m}} \implies$ indekss eksistē.

2. $g \in \mathcal{G}_m \implies g$ pakāpes ar kāpinātājiem $1, 2, ..., \varphi(m)$ ir dažādas un $g^{\varphi(m)} \equiv 1 \pmod{\text{m}}$.

$g^{s_1} \equiv g^{s_2} \pmod{\text{m}} \implies g^{s_1 - s_2} \equiv 1 \pmod{\text{m}} \implies s_1 - s_2 \equiv 0 \pmod{\varphi(m)}$.

3. Injektivitāte

$\mathsf{ind}_g(a_1) \equiv \mathsf{ind}_g(a_2) \pmod{\varphi(m)} \implies$

$\mathsf{ind}_g(a_1) = \mathsf{ind}_g(a_2) + \varphi(m) \cdot l \implies a_1 \equiv a_2 (g^{\varphi(m)})^l \pmod{\text{m}}$ un $a_1 \equiv a_2 \pmod{\text{m}} \implies \mathsf{ind}_g$ ir injektīva funkcija.

Sirjektivitāte $g \in \mathcal{G}_m \implies \forall\ k\ \exists\ a \in \mathcal{U}_m : \quad a \equiv g^k \pmod{\mathrm{m}}$
$\implies \mathsf{ind}_g$ ir sirjektīva funkcija.

4. $g^{\mathsf{ind}_g(ab)} \equiv ab \equiv g^{\mathsf{ind}_g(a)} g^{\mathsf{ind}_g(b)} \equiv g^{\mathsf{ind}_g(a)+\mathsf{ind}_g(b)} \pmod{\mathrm{m}}$. ■

2.4. piezīme. Elementu reizināšanu grupā $\mathcal{U}_m$ var aizvietot ar to indeksu saskaitīšanu mod $\varphi(m)$, ja $\mathcal{G}_m \neq \varnothing$, saskaņā ar šādu algoritmu:

$$ab \equiv g^{\mathsf{ind}_g(a)} \cdot g^{\mathsf{ind}_g(b)} = g^{\mathsf{ind}_g(a)+\mathsf{ind}_g(b)}$$

2.5. piezīme. Izmantojot diskrētos logaritmus, var risināt vienādojumus atlikumu kopās, kuros ir iesaistīta tikai reizināšana, piemēram,

$$x^k \equiv a \pmod{\mathrm{m}}$$

saskaņā ar šādu algoritmu:

1. atrast $g \in \mathcal{G}_m$,
2. atrast $\mathsf{ind}_g(a) = \alpha$,
3. pieņemot $x \equiv g^y \pmod{\mathrm{m}}$ veikt nezināmo substitūciju $x \to y$,

4. izteikt vienādojuma abas puses kā g pakāpes, iegūt vienādojumu

$$g^{ky} \equiv g^{\alpha} \pmod{\mathrm{m}},$$

5. atrisināt vienādojumu $ky \equiv \alpha \pmod{\varphi(m)}$ attiecībā uz y.

2.2. Necikliskais gadījums - ģenerējošās kopas

Primitīvās saknes jēdzienu var vispārināt. Ja grupa $\mathcal{U}_m$ nav cikliska, tad var meklēt minimālo tās elementu kopu $\Gamma = \{g_1, ..., g_r\}$ ar šādu īpašību: $\forall\, a \in \mathcal{U}_n$ var izteikt kā Γ elementu pakāpju reizinājumu. Šādu kopu sauc par $\mathcal{U}_m$ *ģenerējošu kopu*.

Var pierādīt, ka $\forall\, m$ grupā $\mathcal{U}_m$ $\exists$ elementi $g_1, ..., g_r$ tādi, ka $\forall\, a \in \mathcal{U}_m$ ir noteiktā nozīmē viennozīmīgi izsakāms formā

$$a \equiv g_1^{\alpha_1} g_2^{\alpha_2} ... g_r^{\alpha_r} \pmod{m}.$$

2.3. piemērs. $m = 12$. $L(12) = 2$, tāpēc elementu kārtas ir 1 vai 2. $\mathcal{U}_{12} = \{1, 5, 7, 11\}$. $\{5, 7\}$ ir minimāla ģenerējoša kopa mod 12.

2.2.1. $m = 2^\alpha$ - ģenerējošais pāris

$\mathcal{U}_{2^\alpha}$, kur $\alpha \geq 3$, var ģenerēt ar diviem elementiem.

2.5. teorēma. $\alpha \geq 3$, $m = 2^\alpha$. $\mathcal{U}_{2^\alpha} = \langle -1, 3 \rangle = \{\pm 3^\beta\}_{0 \leq \beta < 2^{\alpha-2}}$.

PIERĀDĪJUMS ■

3. 7.mājasdarbs

3.1. Obligātie uzdevumi

7.1 Atrast $\varphi(m)/L(m)$, ja

(a) $m = 2012$;
(b) $m = 8636355$.

7.2 Atrisināt vienādojumus

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

7.3 Izmantojot tikai pamatfaktus un aprēķinus, pierādiet, ka primitīvās saknes neeksistē

(a) mod 16;
(b) mod 30.

7.4 Atrodiet kādu primitīvu sakni

(a) mod 17,
(b) mod 23,

(c) mod 27.

7.5 Atrisiniet vienādojumus:

(a) $x^6 \equiv 4 \pmod{17}$;
(b) $x^2 y^3 \equiv 5 \pmod{11}$.

(*Norādījums: izmantojiet primitīvās saknes*)

3.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi

7.6 Pierādiet, ka

(a) 5 ir primitīva sakne mod $m = 2 \cdot 3^k$, $\forall\ k \geq 1$;
(b) 3 ir primitīva sakne mod $m = 2 \cdot 7^k$, $\forall\ k \geq 1$.

7.7 Pierādiet, ka $p \in \mathbb{P}, p \neq 3 \implies \prod\limits_{g \in \mathcal{G}_p} g \equiv 1 (\mathrm{mod}\ p)$.

7.8 Atrodiet primitīvo saknu mod p summu mod $p \in \mathbb{P}$.