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

*Studiju kurss*

# Veselo skaitļu teorija

## 9.lekcija

*Docētājs: Dr. P. Daugulis*

*2007./2008.studiju gads*

# Saturs

**1. Primitīvās saknes un indeksi** **3**

1.1. Primitīvās saknes (ģeneratori) . . . . . 3

1.2. Invertējama elementa indekss (diskrētais logaritms) . . 13

**2. 9.mājasdarbs** **20**

# 1. Primitīvās saknes un indeksi

## 1.1. Primitīvās saknes (ģeneratori)

Elementu $a \in U_m$ sauksim par *primitīvu sakni* , ja

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

Citiem vārdiem sakot, neeksistē nekāda cita invertējama klase $b$ un naturāls $l > 1$, $l|\varphi(m)$ tādi, ka

$$b^l \equiv a \pmod{\text{m}}$$

(no $a$ nevar izvilkt nekādu sakni $b = \sqrt[l]{a}$). Tas ir tāpēc, ka pretējā gadījumā mēs iegūtu, ka

$$a^{\frac{\varphi(m)}{l}} \equiv b^{l \cdot \frac{\varphi(m)}{l}} \equiv b^{\varphi(m)} \equiv 1 \pmod{\text{m}}$$

un $a$ kārta būtu vienāda ar $\frac{\varphi(m)}{l} < \varphi(m)$.

**1.1. piemērs.** $2 \equiv 3^2 \pmod 7$, tāpēc var uzskatīt, ka $\sqrt{2} \equiv 3 \pmod 7$. Neeksistē klase $x$ tāda, ka $x^k \equiv 3 \pmod 7$, ja $k \geq 2$ un $k|6$.

**1.1. teorēma.** Ja $g$ ir primitīva sakne pēc moduļa $m$, tad klases $g, g^2, ..., g^{\varphi(m)}$ veido reducēto atlikumu klašu pārstāvju kopu.

PIERĀDĪJUMS Tā kā $P_m(g) = \varphi(m)$, tad visas pakāpes

$$g, g^2, ..., g^{\varphi(m)}$$

ir dažādas pēc moduļa $m$. Tā kā $LKD(g, m) = 1$, tad katram $i$ izpildās $LKD(g^i, m) = 1$, tāpēc šīs pakāpes ir invertējamu klašu pārstāvji. ■

**1.1. piezīme.** Iepriekšējā teorēma grupu teorijas terminos apgalvoto, ka primitīvā sakne ir $U_m$ kā grupas ģenerators. Tajos gadījumos, kad atlikumu gredzenā eksistē primitīvā sakne, tā multiplikatīvā grupa $U_m$ ir cikliska.

Par primitīvajām saknēm var domāt divējādi:

- kā par elementiem, no kuriem nevar izvilkt sakni (analītiskā pieeja),
- kā par multiplikatīvās grupas ģeneratoriem (algebriskā pieeja).

**1.2. piemērs.**

- $m = 2$, $\{1\}$;
- $m = 3$, $\{2\}$;
- $m = 4$, $\{3\}$;
- $m = 5$, $\{2, 3\}$;
- $m = 6$, $\{5\}$;
- $m = 7$, $\{3, 5\}$;

- $m = 8$, $\emptyset$;
- $m = 9$, $\{2, 5\}$;
- $m = 10$, $\{3, 7\}$;
- $m = 11$, $\{2, 6, 7, 8\}$;
- $m = 12$, $\emptyset$;
- $m = 13$, $\{2, 6, 7, 11\}$;
- $m = 14$, $\{3, 5\}$;
- $m = 15$, $\emptyset$;
- $m = 16$, $\emptyset$;
- $m = 17$, $\{3, 5, 6, 7, 10, 11, 12, 14\}$;
- $m = 18$, $\{5, 11\}$;
- $m = 19$, $\{2, 3, 10, 13, 14, 15\}$;
- $m = 20$, $\emptyset$;
- $m = 2007$, $\emptyset$;
- $m = 2008$, $\emptyset$.

**1.2. teorēma.**

1. Ja $m = p$ ir pirmskaitlis, tad primitīvo sakņu skaits ir vienāds ar $\varphi(p-1)$.
2. Ja eksistē primitīva sakne pēc moduļa $m$, tad primitīvo sakņu skaits pēc moduļa $m$ ir vienāds ar $\varphi(\varphi(m))$.

PIERĀDĪJUMS 1. Primitīvās saknes pēc moduļa $p$ ir elementi, kuriem kārta ir vienāda ar $\varphi(p) = p-1$. Saskaņā ar iepriekšējo teorēmu, šādu elementu skaits ir vienāds ar $\varphi(p) = p-1$.

2. Ja eksistē primitīva sakne $g \in U_m$, tad tās pakāpe $g^k$ ir primitīva sakne tad un tikai tad, ja $LKD(k, \varphi(m)) = 1$ saskaņā ar iepriekš pierādītu teorēmu. Šādu kāpinātāju skaits ir $\varphi(\varphi(m))$. Esam pierādījuši, ka primitīvo sakņu skaits nav mazāks kā $\varphi(\varphi(m))$. Ja $h$ ir primitīva sakne, tad $h \equiv g^s \pmod{\text{m}}$ un atkal ir jābūt spēkā vienādībai $LKD(s, \varphi(m)) = 1$, tāpēc jaunas primitīvas saknes mēs neatradīsim. ■

**1.2. piezīme.** Ja $p = 11$, tad viena primitīvā sakne ir 2. Pārējās primitīvās saknes ir $2^3 \equiv 8$, $2^7 \equiv 7$, $2^9 \equiv 6$ (kāpinātajiem jābūt savstarpējiem pirmskaitļiem ar $\varphi(11) = 10$). Primitīvo sakņu skaits ir $\varphi(\varphi(11)) = 4$.

**1.3. teorēma.** Grupā $U_m$ eksistē primitīva sakne tad un tikai tad, ja $m \in \{2, 4\}$, $m = p^\alpha$ vai $m = 2p^\alpha$, kur $p$ ir nepāra pirmskaitlis.

PIERĀDĪJUMS Ja $m \in \{2, 4\}$, tad var uzrādīt konkrētas primitīvās saknes. Pierādījums sastāv no šādiem soļiem:

1. pierādām, ka primitīvās saknes eksistē, ja $m = p^\alpha$,
2. pierādām, ka primitīvās saknes eksistē, ja $m = 2p^\alpha$,
3. pierādām, ka primitīvās saknes neeksistē, ja $m = 2^\beta$, $\beta \geq 3$,
4. pierādām, ka primitīvās saknes neeksistē, ja $m = m_1 m_2$, kur $m_i \geq 4$ un $LKD(m_1, m_2) = 1$ (šis solis izslēdz gadījumus $m = 2^\gamma p^\alpha$, $\gamma \geq 2$ un $p_1^{\alpha_1} p_2^{\alpha_2} | m$, $p, p_i$ - nepāra pirmskaitļi).

■

**1.3. 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.

**1.4. piezīme.** Aprakstīsim naivos algoritmus primitīvo sakņu atrašanai (ja $m$ nav pārāk liels). Atcerēsimies, ka $U_m$ elementu kārtas dala $\varphi(m)$ un primitīvās saknes kārta ir vienāda ar $\varphi(m)$.

Algoritms Nr 1 (vienas primitīvās saknes atrašana):

1. Atradīsim klases 2 pakāpju kopu $P_2$, ja $|P_2| = U_m$, tad 2 ir primitīva sakne, ja nē, tad ejam uz nākamo soli;
2. Atradīsim pakāpju kopu $P_{k_1}$ mazākajai klasei $k_1$, kas nepieder $P_2$, ja $|P_{k_1}| = U_m$, tad $k_1$ ir primitīva sakne, ja nē, tad ejam uz nākamo soli;

... ...

Algoritms Nr 2 (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 $\Gamma$ ar šādām īpašībām: $\Gamma$ virsotņu kopa ir $U_m$, šķautne $a \xrightarrow{p_i} b$ ir tad un tikai tad, ja $a^{p_i} \equiv b \pmod{m}$. Citiem vārdiem sakot, zīmēsim orientētu šķautni ar indeksu $p_i$ no

$a$ uz $b$ tad un tikai tad, ja $a^{p_i} \equiv b \pmod{m}$. Tādējādi šajā grafā šķautnes nozīmē kāpināšanu pirmskaitļu pakāpēs. (Mūs interesē $U_m$ struktūra attiecībā uz elementu kāpināšanu dažādās pakāpēs. Lai to labāk saskatītu, mēs vizualizēsim tikai kāpināšanu pirmskaitļu pakāpēs, kas dala $\varphi(m)$, jo jebkura kāpināšana ir šādu kāpināšanu kompozīcija).

3. $U_m$ primitīvās saknes ir grafa $\Gamma$ *avots*: virsotnes, kurām nav ieejošo šķautņu.

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

**1.3. piemērs.** Atradīsim minimālu ģenerējošu kopu, ja $m = 12$. $\varphi(12) = 4$, tāpēc elementu kārtas ir skaitļa 4 dalītāji. $U_{12} = \{1, 5, 7, 11\}$. Redzam, ka $5^2 \equiv 1 \pmod{12}$, $7^2 \equiv 1 \pmod{12}$, $5 \cdot 7 \equiv -1 \equiv 11 \pmod{12}$. Kopa $\{5, 7\}$ ir minimāla ģenerējoša kopa mod 12.

Atradīsim minimālu ģenerējošu kopu, ja $m = 20$. $\varphi(20) = 8$, tāpēc elementu kārtas ir skaitļa 8 dalītāji. $U_{20} = \{1, 3, 7, 9, 11, 13, 17, 19\}$. Redzam, ka $3^2 \equiv 9$ ( mod 20), $3^3 \equiv 7$ (mod 20), $11^2 \equiv 1$ (mod 12), $3 \cdot 11 \equiv 13$ ( mod 20), $3^2 \cdot 11 \equiv 19$ (mod 20), $3^3 \cdot 11 \equiv 17$ (mod 2o). Kopa $\{3, 11\}$ ir minimāla ģenerējoša kopa mod 20.

## 1.2. Invertējama elementa indekss (diskrētais logaritms)

Dots, ka $a \in U_m$ un $b \in U_m$. Teiksim, ka $s$ ir $b$ *indekss ar bāzi* $a$ *pēc moduļa* $m$, ja

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

Apzīmēsim ar $\mathsf{ind}_a(b)$ vai $\mathsf{ind}(b)$. Par indeksu var domāt kā par "logaritmu pie bāzes $a$", tāpēc to sauc arī par *diskrēto logaritmu*. Ievērosim, ka

- pagaidām indekss ir noteikts ar precizitāti līdz $\varphi(m)$ daudzkārtnim, tāpēc ka
$$a^{s+k\varphi(m)} \equiv a^s (a^{\varphi(m)})^k \equiv b \pmod{\mathrm{m}};$$
- dabiski ir definēt $\mathsf{ind}_a(1) \equiv 0 \pmod{\varphi(m)}$;
- $\mathsf{ind}_a(a) \equiv 1 \pmod{\varphi(m)}$.

**1.4. piemērs.**

- $p = 5$, $\mathsf{ind}_3(4) = \mathsf{ind}_2(4) = 2$, $\mathsf{ind}_3(2) = \mathsf{ind}_2(3) = 3$;

- $p = 7$, $\mathsf{ind}_3(2) = \mathsf{ind}_4(2) = \mathsf{ind}_2(4) = \mathsf{ind}_5(4) = 2$, $\mathsf{ind}_3(6) = \mathsf{ind}_5(6) = 3$, $\mathsf{ind}_5(2) = \mathsf{ind}_3(4) = 4$, $\mathsf{ind}_3(5) = \mathsf{ind}_5(3) = 5$;

**1.4. teorēma.** Ja $g$ ir primitīva sakne pēc moduļa $m$, tad

1. katram $a \in U_m$ eksistē indekss pie bāzes $g$;
2. visas iespējamās $a$ indeksa vērtības pieder vienai atlikumu klasei pēc moduļa $\varphi(m)$,

PIERĀDĪJUMS 1. Ja $g$ ir primitīva sakne, tad katrs $a \in U_m$ ir izsakāms formā $a \equiv g^s \pmod{m}$, tāpēc indekss eksistē.

2. Ja $g$ ir primitīva sakne, tad visas tās pakāpes ar kāpinātājiem $0, 1, ..., \varphi(m)$ ir dažādas un $g^{\varphi(m)} \equiv 1 \pmod{m}$. Ja $g^{s_1} \equiv g^{s_2} \pmod{m}$, tad $g^{s_1 - s_2} \equiv 1 \pmod{m}$, tāpēc $s_1 - s_2 \equiv 0 \pmod{\varphi(m)}$. ■

Iepriekšējā teorēma apgalvoto, ka ir korekti definēta funkcija

$$\mathsf{ind}_g : U_m \to \mathbb{Z}/\varphi(m)\mathbb{Z},$$

kas katram invertējamam elementa piekārto tās indeksu pēc moduļa $\varphi(m)$, ja $g$ ir primitīva sakne.

**1.5. teorēma.** Ja $g$ ir primitīva sakne pēc moduļa $m$, tad

1. $\mathsf{ind}_g \pmod{\varphi(m)}$ ir bijektīva funkcija;
2. $\mathsf{ind}_g(ab) \equiv \mathsf{ind}_g(a) + \mathsf{ind}_g(b) \pmod{\varphi(m)}$;
3. $\mathsf{ind}_g(a^k) \equiv k \cdot \mathsf{ind}_g(a) \pmod{\varphi(m)}$;
4. $\mathsf{ind}_g(\frac{a}{b}) \equiv \mathsf{ind}_g(a) - \mathsf{ind}_g(b) \pmod{\varphi(m)}$;
5. $\mathsf{ind}_g(a) \equiv \mathsf{ind}_g(h) \cdot \mathsf{ind}_h(a) \pmod{\varphi(m)}$, kur $h$ arī ir primitīva sakne pēc moduļa $m$;

PIERĀDĪJUMS 1. Ja $\mathsf{ind}_g(a_1) \equiv \mathsf{ind}_g(a_2) \pmod{\varphi(m)}$, tad

$$\mathsf{ind}_g(a_1) = \mathsf{ind}_g(a_1) + \varphi(m) \cdot l$$

un

$$a_1 \equiv a_2(g^{\varphi(m)})^l \pmod{\mathrm{m}}$$

un $a_1 \equiv a_2 \pmod{\mathrm{m}}$, tātad $\mathsf{ind}_g$ ir injektīva funkcija. Tā kā $g$ ir primitīva sakne, tad katram $k$ eksistē $a \in U_m$ tāds, ka $a \equiv g^k \pmod{\mathrm{m}}$, tātad $\mathsf{ind}_g$ ir sirjektīva funkcija.

2.

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

tāpēc $\mathsf{ind}_g(ab) \equiv \mathsf{ind}_g(a) + \mathsf{ind}_g(b) \pmod{\varphi(m)}$.

3.,4. - pierāda līdzīgi kā 2.

5.

$$a \equiv g^{\mathsf{ind}_g(a)} \equiv h^{\mathsf{ind}_h(a)} \equiv (g^{\mathsf{ind}_g(h)})^{\mathsf{ind}_h(a)} \equiv g^{\mathsf{ind}_g(h)\cdot\mathsf{ind}_h(a)} \pmod{\mathrm{m}},$$

■

**1.6. piezīme.** Pierādītā teorēma nozīmē to, ka funkcija $\mathsf{ind}_g$ ir bijektīvs (savstarpēji viennozīmīgs) grupu homomorfizms no $(U_m, \cdot)$ uz $(\mathbb{Z}/\varphi(m)\mathbb{Z}, +)$. Šādus homomorfizmus sauc par *grupu izomorfizmiem*. Ja grupas ir izomorfas, tad var uzskatīt, ka tās atšķiras tikai ar elementu un operāciju apzīmējumiem. Tātad reizināšanu grupā $U_m$ var aizvietot ar saskaitīšanu pēc moduļa $\varphi(m)$, ja tajā eksistē primitīva sakne, saskaņā ar šādu algoritmu:

1. kopā $U_m$ atradīsim primitīvu sakni;
2. atradīsim elementu $a$ un $b$ indeksus $\mathsf{ind}_g(a)$ un $\mathsf{ind}_g(b)$;
3. atradīsim $s = \mathsf{ind}_g(a) + \mathsf{ind}_g(b) \pmod{\varphi(m)}$;
4. atradīsim $ab \equiv g^s \pmod{\text{m}}$.

Ievērosim, ka šis algoritms ir analoģisks reizināšanai ar parasto logaritmu izmantošanu: $ab = \exp(\ln(a) + \ln(b))$.

Ievērosim, ka no teorēmas seko, ka ir definēta funkcijas, ka ir inversa attiecībā uz $\mathsf{ind}_g$ (*diskrētā eksponente*), kas arī ir bijektīva.

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

vienādojumus, kas ir izsakāmi formā

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

saskaņā ar šādu algoritmu:

1. atrast primitīvu sakni $g \pmod{\mathrm{m}}$,
2. atrast $a$ indeksu pie bāzes $g$, apzīmēsim to ar $\alpha$,
3. pieņemt, ka $x \equiv g^y \pmod{\mathrm{m}}$, citiem vārdiem sakot, 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. 9.mājasdarbs

1. Par pirmskaitļa $p$ *indeksu matricu* sauc tabulu, kurā rindas tiek indeksētas ar visiem nenulles atlikumiem $a_i$ pēc moduļa $p$, kolonnas tiek indeksētas ar primitīvajām saknēm $g_j$ pēc moduļa $p$ un katrā rūtiņā, kas atbilst pārim $(a, g)$, tiek ierakstīts $\mathsf{ind}_g(a) \pmod{\varphi(p)}$. Sastādīt indeksu matricu pirmskaitlim 7.
2. Atrodiet viena argumenta kvadrātisku polinomu, kas ir sadalāms mod 2, bet nav sadalāms mod 3.
3. Atrisiniet vienādojumus:
   (a) $8x^2 + 2008 \equiv 0 \pmod 3$;
   (b) $x^3 - 2007x^2 + 2x + 1 \equiv 0 \pmod 7$;
4. Izmantojot Gausa metodi atrisiniet lineāru vienādojumu sistēmas
   (a)
$$\begin{cases} x_1 + 2x_2 + x_3 \equiv 1 \pmod 3 \\ x_2 + 2x_3 + x_4 \equiv 2 \pmod 3 \end{cases},$$

(b)

$$\begin{cases} x_1 - x_2 + x_3 \equiv 4 \pmod 5 \\ x_2 - x_3 + x_1 \equiv 3 \pmod 5 \\ x_3 - x_1 + x_2 \equiv 3 \pmod 5 \end{cases}.$$

5. Atrisiniet vienādojumus pēctecīgi risinot tos pēc mazu pirmskaitļa pakāpju moduļiem:
   (a) $x^6 + x^4 + x + 1 \equiv 0 \pmod 8$,
   (b) $x^7 + x^5 - x^3 + x - 1 \equiv 0 \pmod 9$.