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

Studiju kurss

Veselo skaitļu teorija

10.lekcija

Docētājs: Dr. P. Daugulis

2009./2010.studiju gads

Saturs

Lekcijas mērķis:

- apgūt atlikumu multiplikatīvo grupu ģeneratoru - *primitīvo sakņu* teorijas pamatus.

Lekcijas kopsavilkums:

- var pētīt invertējamus atlikumus, kuru pakāpju kopa sakrīt ar visu invertējamo atlikumu kopu - *primitīvās saknes.*

Svarīgākie jēdzieni: primitīvā sakne, atlikumu multiplikatīvo grupu ģenerējošās kopas, invertējama atlikuma indekss,

Svarīgākie fakti un metodes: primitīvās saknes ģenerējošā īpašība, primitīvo sakņu eksistence un skaits dažādos gadījumos, primitīvo sakņu meklēšanas algoritmi, indeksa īpašības, primitīvo sakņu un indeksu pielietojumi vienādojumu risināšanā.

1. Primitīvās saknes un indeksi

1.1. Primitīvās saknes

1.1.1. Grupu ģeneratori

G - grupa. $g \in G$ sauc par G *ģeneratoru*, ja $\langle g \rangle = G$.
$\exists$ ģenerators $g \in G \implies G$ ir *cikliska grupa*.

1.1. piemērs. $G = (\mathbb{Z}_m, +)$, $g = 1$: $\langle 1 \rangle = G$.

Pētīsim ģeneratorus atlikumu multiplikatīvajās grupās.

1.1.2. Primitīvās saknes (ģeneratori)

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

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

Citiem vārdiem sakot, g kārta ir maksimāli iespējamā.

Apzīmēsim primitīvo sakņu mod m kopu ar $\mathcal{G}_m$.

Vēl viena interpretācija: $\nexists\ b \in \mathcal{U}_m$ un naturāls $l > 1$, $l|\varphi(m)$:

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

(no g "nevar izvilkt" nekādu sakni $b = \sqrt[l]{a}$). Pretējā gadījumā

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

$\Longrightarrow\ P(g) = \frac{\varphi(m)}{l} < \varphi(m).$

1.2. 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. $g \in \mathcal{G}_m \implies$ 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.

$LKD(g,m)=1 \implies \forall\, i:\ LKD(g^i,m)=1 \implies$ šīs pakāpes ir invertējamu klašu pārstāvji. ■

1.1. 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.

1.3. piemērs.

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

- $m = 11$, $\{2, 6, 7, 8\}$;
- $m = 12$, $\emptyset$;
- $m = 13$, $\{2, 6, 7, 11\}$;
- $m = 14$, $\{3, 5\}$;
- $m = 15$, $\emptyset$;
- $m = 16$, $\emptyset$;
- $m = 17$, $\{3, 5, 6, 7, 10, 11, 12, 14\}$;
- $m = 18$, $\{5, 11\}$;
- $m = 19$, $\{2, 3, 10, 13, 14, 15\}$;
- $m = 20$, $\emptyset$;
- $m = 2007$, $\emptyset$;
- $m = 2008$, $\emptyset$;
- $m = 2009$, $\emptyset$.
- $m = 2010$, $\emptyset$.
- $m = 2011 \in \mathbb{P}$, $\{3, 7, 11, 12, 17, 18, 19, ..., 2002, 2006\}$, kopā 528 primitīvās saknes.

1.1.3. Primitīvo sakņu skaits

Apzīmēsim ar $\psi(k)$ to $\mathcal{U}_m$ elemento skaitu, kuriem multiplikatīvā kārta ir vienāda ar k.

1.2. teorēma. $p \in \mathbb{P} \implies$

1. $\forall\ k \neq 0 :\ \psi(k) \in \{0, \varphi(k)\})$.
2. $k|p-1 \implies \psi(k) = \varphi(k)$.

PIERĀDĪJUMS Pielikumā.■

1.3. teorēma.

1. $p \in \mathbb{P} \implies |\mathcal{G}_m| = \varphi(\varphi(p)) = \varphi(p-1)$.
2. $\mathcal{G}_m \neq \emptyset \implies |\mathcal{G}_m| = \varphi(\varphi(m))$.

PIERĀDĪJUMS 1. Primitīvās saknes mod p ir elementi, kuriem kārta ir vienāda ar $\varphi(p) = p-1$. Šādu elementu skaits ir vienāds ar $\varphi(\varphi(p)) = \varphi(p-1)$.

2. $\exists\ g \in \mathcal{G}_m \implies \left(g^k \in \mathcal{G}_m \iff LKD(k, \varphi(m)) = 1 \right)$ saskaņā ar iepriekš pierādītu teorēmu par multiplikatīvās kārtas īpašībām. Šādu kāpinātāju k skaits ir $\varphi(\varphi(m)) \implies |\mathcal{G}_m| \geq \varphi(\varphi(m))$.

$h \in \mathcal{G}_m \implies h \equiv g^s \pmod{\text{m}} \implies$ atkal $LKD(s, \varphi(m)) = 1 \implies$ jaunas primitīvas saknes mēs neatradīsim $\implies |\mathcal{G}_m| = \varphi(\varphi(m))$. ■

1.2. piezīme. $p = 11$, $2 \in \mathcal{G}_{11}$. 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 $\varphi(\varphi(11)) = 4$.

1.1.4. Primitīvo sakņu eksistence saliktiem moduļiem

1.4. teorēma. *m dalās ar vismaz diviem nepāra pirmskaitļiem* $\implies$

$$\mathcal{G}_m = \emptyset.$$

PIERĀDĪJUMS

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

$\Longrightarrow$

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

$\Longrightarrow$ saskaņā ar pastiprināto Eilera teorēmu $\forall\, a \in \mathcal{U}_m$: $P(a) < \varphi(m)$.

■

1.4. piemērs. $m = 15$, $L(m) = MKD(2,4) = 4 < 8 = \varphi(15)$.

1.5. teorēma. $\mathcal{G}_m \neq \emptyset \iff$

- $m \in \{2, 4\}$,
- $m = p^\alpha$, kur p ir nepāra pirmskaitlis,
- $m = 2p^\alpha$, kur p ir nepāra pirmskaitlis.

PIERĀDĪJUMS Saskaņā ar iepriekšējo teorēmu atliek apskatīt šādus gadījumus:

- $m \in \{2, 4\}$, var uzrādīt konkrētas primitīvās saknes;
- $m = 2^\alpha$, kur $\alpha \geq 3$;

- $m = p^\alpha$, kur p ir nepāra pirmskaitlis, $\alpha \geq 2$;
- $m = 2p^\alpha$, kur p ir nepāra pirmskaitlis, $\alpha \geq 1$.

Pierādījuma soļi:

- pierādām, ka primitīvās saknes neeksistē, ja $m = 2^\alpha$, kur $\alpha \geq 3$;
- 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 ja g ir primitīva sakne mod p^2, tad g ir primitīva sakne mod p^α, kur $\alpha \geq 3$, tātad eksistē 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 $2p^\alpha$, tātad eksistē primitīvas saknes mod $2p^\alpha$.

■

1.6. teorēma. Ja $m = 2^\alpha$, $\alpha \geq 3$, tad primitīvās saknes mod m neeksistē.

PIERĀDĪJUMS Izmantojot matemātisko indukciju ar parametru α, pierādīsim, ka $\forall a \in \mathcal{U}_m$ izpildās

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

No šī fakta seko, ka $P(a) \leq 2^{\alpha-2} < 2^{\alpha-1} = \varphi(m)$, tātad nekāds a nevar būt primitīva sakne.

Indukcijas bāze Ja $\alpha = 3$, tad var redzēt, ka visiem elementiem kārta nepārsniedz $2 = 2^{3-2}$.

Indukcijas solis Pieņemsim, ka

$$a^{2^{\alpha-2}} \equiv 1 (\mathrm{mod}\ 2^\alpha) \iff a^{2^{\alpha-2}} = 1 + 2^\alpha q.$$

Kāpinot kvadrātā iegūstam:

$$(a^{2^{\alpha-2}})^2 = a^{2^{\alpha-1}} = (1 + 2^\alpha q)^2 = 1 + 2^{\alpha+1} q + 2^{2\alpha} q^2.$$

Seko, ka $a^{2^{\alpha-1}} \equiv 1 (\mathrm{mod}\ 2^{\alpha+1})$. ■

1.7. teorēma. Dots, ka p ir nepāra pirmskaitlis. Ja g ir primitīva sakne mod p, tad g vai $g+p$ ir primitīva sakne mod p^2.

PIERĀDĪJUMS Pielikumā. ■

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 $\mathcal{U}_m$ 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 $|P_2| = \mathcal{U}_m$, tad 2 ir primitīva sakne, ja nē, tad ejam uz nākamo soli;
2. Atradīsim pakāpju kopu P_{k_1} mazākajai klasei $k_1 \in \mathcal{U}_m \backslash P_2$, ja $|P_{k_1}| = \mathcal{U}_m$, tad k_1 ir primitīva sakne, ja nē, tad ejam uz nākamo soli;

... ...

Algoritms Nr 2 (visu primitīvo saknu 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 $a \xrightarrow{p_i} b \iff a^{p_i} \equiv b \pmod{\text{m}}$.

   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.

1.5. piemērs. $p = 7$, $p = 11$.

1.1.5. Atlikumu multiplikatīvo grupu 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

$$a = g_1^{\alpha} g_2^{\alpha_2} ... g_r^{\alpha_r}.$$

1.6. piemērs. Atradīsim minimālu ģenerējošu kopu, ja $m = 12$. $\varphi(12) = 4$, tāpēc elementu kārtas ir skaitļa 4 dalītāji. $\mathcal{U}_{12} = \{1, 5, 7, 11\}$.

$5^2 \equiv 1$ (mod 12), $7^2 \equiv 1$ (mod 12), $5 \cdot 7 \equiv -1 \equiv 11$ (mod 12). $\{5, 7\}$ ir minimāla ģenerējoša kopa mod 12.

Atradīsim minimālu ģenerējošu kopu, ja $m = 20$. $\varphi(20) = 8$, tāpēc elementu kārtas ir skaitļa 8 dalītāji. $\mathcal{U}_{20} = \{1, 3, 7, 9, 11, 13, 17, 19\}$.

$3^2 \equiv 9$ (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 20). $\{3, 11\}$ ir minimāla ģenerējoša kopa mod 20.

1.2. Invertējama elementa indekss (diskrētais logaritms)

1.2.1. Definīcija

$a, b \in \mathcal{U}_m$. Teiksim, ka s ir b *indekss ar bāzi* a *mod* m, ja

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

Apzīmēsim s 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 $\mathsf{ind}_a(1) \equiv 0 \pmod{\varphi(m)}$;

- $\mathsf{ind}_a(a) \equiv 1 \pmod{\varphi(m)}$.

1.7. piemērs.

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

1.2.2. Īpašības

1.8. 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 $\varphi(m)$.

PIERĀDĪJUMS

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

2. Ja g ir primitīva sakne, tad visas g pakāpes ar kāpinātājiem $1, 2, ..., \varphi(m)$ ir dažādas un $g^{\varphi(m)} \equiv 1 \pmod{m}$.

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

Iepriekšējā teorēma apgalvoto, ka ir korekti definēta funkcija

$$\mathsf{ind}_g : \mathcal{U}_m \to \mathbb{Z}_{\varphi(m)},$$

kas $\forall$ invertējamam elementam mod m piekārto tā indeksu mod $\varphi(m)$, ja g ir primitīva sakne.

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

1. $\mathsf{ind}_g : \mathcal{U}_m \to \mathbb{Z}_{\varphi(m)}$ 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 $h \in \mathcal{G}_m$.

PIERĀDĪJUMS

1. Injektivitāte

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 ind_g ir injektīva funkcija.

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

2.

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

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

3.,4. - pierāda līdzīgi kā 2.

5.

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

■

1.5. piezīme. Pierādītā teorēma nozīmē to, ka funkcija ind_g ir bijektīvs grupu homomorfisms (izomorfisms) no $(\mathcal{U}_m, \cdot)$ uz $(\mathbb{Z}_{\varphi(m)}, +)$.

Tātad elementu reizināšanu grupā $\mathcal{U}_m$ var aizvietot ar to indeksu saskaitīšanu mod $\varphi(m)$, ja tajā eksistē primitīva sakne, saskaņā ar šādu algoritmu:

1. kopā $\mathcal{U}_m$ 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 $ab \equiv g^s \pmod{\mathrm{m}}$.

1.6. 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 (mod m),
2. atrast a indeksu pie bāzes g, apzīmēsim to ar α,
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.

1.7. piezīme. Aprakstīto algoritmu var vispārināt, ja grupa $\mathcal{U}_m$ nav cikliska:

1. atrast $\mathcal{U}_m$ minimālu ģenerējošu kopu $\{g_1, ..., g_r\}$,
2. izteikt a formā $a \equiv g_1^{\alpha_1} g_2^{\alpha_2} ... g_r^{\alpha_r}$;
3. pieņemt, ka $x \equiv g_1^{y_1} g_2^{y_2} ... g_r^{y_r} \pmod{\text{m}}$, citiem vārdiem sakot, veikt nezināmo substitūciju $x \to (y_1, ..., y_r)$,
4. izteikt vienādojuma abas puses kā g_i pakāpju reizinājumus;
5. atrisināt iegūto vienādojumu attiecībā uz $y_1, ..., y_r$.

2. 10.mājasdarbs

2.1. Obligātie uzdevumi

10.1 Atrodiet kādu primitīvu sakni mod 23.

10.2 Izmantojot tikai pamatfaktus un aprēķinus, pierādiet, ka primitīvās saknes neeksistē, ja

(a) $m = 8$;
(b) $m = 21$.

Katrā no šiem gadījumiem atrodiet grupas $(\mathcal{U}_m, \cdot)$ minimālo ģenerējošo kopu.

10.3 Atrisiniet šādus vienādojumus:

(a) $x^6 \equiv 4 \pmod{23}$;
(b) $x^2y^3 \equiv 5 \pmod{11}$;
(c) $x^6 \equiv 3 \pmod{40}$.

(*Norādījums: izmantojiet primitīvās saknes un minimālās ģenerējošās kopas*)

2.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi

10.4 Pierādiet, ka

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

10.5 Pierādiet, ka ja $p \neq 3$ ir pirmskaitlis, tad visu primitīvo saķņu mod p reizinājums ir kongruents ar $1 (\text{mod } p)$.

10.6 Atrodiet primitīvo saķņu mod p summu mod $p \in \mathbb{P}$.