

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

Studiju kurss

Veselo skaitļu teorija

9.lekcija

Docētājs: Dr. P. Daugulis

2008./2009.studiju gads

Saturs

1. Primitīvās saknes un indeksi	3
1.1. Primitīvās saknes (ģeneratori)	3
1.2. Invertējama elementa indekss (diskrētais logaritms) . .	17
2. 9.mājasdarbs	24
2.1. Obligātie uzdevumi	24
2.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi	25

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

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

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

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

un a kārtā 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 $g, g^2, \dots, g^{\varphi(m)}$ veido reducēto atlikumu klašu pārstāvju kopu.

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

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

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 apgalvo to, ka primitīvā sakne ir U_m kā grupas *generators* vai *veidotājelements*. 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.

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

- $m = 16, \emptyset$;
- $m = 17, \{3, 5, 6, 7, 10, 11, 12, 14\}$;
- $m = 18, \{5, 11\}$;
- $m = 19, \{2, 3, 10, 13, 14, 15\}$;
- $m = 20, \emptyset$;
- $m = 2007, \emptyset$;
- $m = 2008, \emptyset$;
- $m = 2009, \emptyset$.

1.2. teorēma.

1. Ja p ir pirmskaitlis, tad primitīvo sakņu mod p 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 kārtā 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 $h \equiv g^s \pmod{m}$ 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 dalās ar vismaz diviem nepāra pirmskaitļiem vai vienu nepāra pirmskaitli un 2^k , kur $k \geq 2$, tad pētot pirmskaitļa 2 kārtas skaitļos $L(m)$ un $\varphi(m)$, var redzēt, ka

$$L(m) < \varphi(m).$$

No pastiprinātās Eilera teorēmas seko, ka šajos gadījumos neviens $a \in U_m$ nevar ģenerēt visu U_m , jo $P_m(a) < \varphi(m)$.

Atlika apskatīt šādus gadījumus:

- $m = 2^\alpha$, kur $\alpha \geq 3$, ja $m \in \{2, 4\}$, tad var uzrādīt konkrētas primitīvās saknes;
- $m = p^\alpha$, 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 ja g ir primitīva sakne mod p , tad g vai $g + p$ ir primitīva sakne mod p^2 , tātad eksistē 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 $2p^\alpha$.



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

PIERĀDĪJUMS Izmantojot matemātisko indukciju ar parametru α , pierādīsim, ka $\forall a \in U_m$ izpildās

$$a^{2^{\alpha-2}} \equiv 1 \pmod{2^\alpha}.$$

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 kārtā nepārsniedz $2 = 2^{3-1}$.

Indukcijas solis Pieņemsim, ka

$$a^{2^{\alpha-2}} \equiv 1 \pmod{2^\alpha} \iff a^{2^{\alpha-2}} = 1 + 2^\alpha q.$$

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 $a^{2^{\alpha-1}} \equiv 1 \pmod{2^{\alpha+1}}$. ■

1.5. 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 Pieņemsim, ka g ir primitīva sakne mod p .

$$LKD(g, p) = 1 \implies LKD(g, p^2) = 1, \text{ tāpēc } g \in U_{p^2}.$$

Apzīmēsim $P_{p^2}(g)$ ar k . Ir zināms, ka $k | \varphi(p^2) = p(p-1)$.

$$g^k \equiv 1 \pmod{p^2} \implies g^k \equiv 1 \pmod{p} \implies p-1 | k.$$

$$k | p(p-1) \text{ un } p-1 | k \implies k = p(p-1) \text{ vai } k = p-1.$$

$k = p(p-1)$ Ja $k = p(p-1)$, tad g ir primitīva sakne mod p^2 , jo $P_{p^2}(g) = k = \varphi(p^2) = p(p-1)$.

$k = p - 1$ Definēsim $h = g + p$.

Tā kā $h \equiv g \pmod{p}$, tad ar tiem pašiem spriedumiem iegūstam, ka $P_{p^2}(h) \in \{p - 1, p(p - 1)\}$.

Pierādīsim, ka $P_{p^2}(h) \neq p - 1$, tas nozīmēs, ka h ir primitīva sakne mod p^2 .

Redzam, ka

$$\begin{aligned} h^{p-1} &= (g + p)^{p-1} = \\ g^{p-1} + (p-1)g^{p-2}p + \frac{(p-1)(p-2)}{2}g^{p-3}p^2 + \dots + p^{p-1} &= \\ \underbrace{g^{p-1}}_{\equiv 1 \pmod{p^2}} - g^{p-2}p + p^2(\dots) &\equiv \\ 1 - g^{p-2}p \pmod{p^2}. & \end{aligned}$$

$g \in U_{p^2} \implies g^{p-2}p \not\equiv 0 \pmod{p^2}$. Seko, ka $h^{p-1} \not\equiv 1 \pmod{p^2}$. ■

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 daļa $\varphi(m)$ un primitīvās saknes kārtā 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 $p_1^{\alpha_1} \cdots p_k^{\alpha_k}$.
2. (Ir nepieciešams zināt orientētu grafu definīciju) Konstruēsim orientētu grafu Γ ar šādām īpašībām:
 - Γ 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 daļa $\varphi(m)$, jo jebkura kāpināšana ir šādu kāpināšanu kompozīcija).

3. U_m primitīvās saknes ir grafa Γ avots: virsotnes, kurām nav ieejošo šķautņu.

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

Var pierādīt, ka katram m grupā U_m eksistē elementi g_1, \dots, g_r tādi, ka katrs $a \in U_m$ ir noteiktā nozīmē viennozīmīgi izsakāms formā

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

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 $3^2 \equiv 9 \pmod{20}$, $3^3 \equiv 7 \pmod{20}$, $11^2 \equiv 1 \pmod{12}$,

$3 \cdot 11 \equiv 13 \pmod{20}$, $3^2 \cdot 11 \equiv 19 \pmod{20}$, $3^3 \cdot 11 \equiv 17 \pmod{20}$.
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

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

Apzīmēsim ar $\text{ind}_a(b)$ vai $\text{ind}(b)$.

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 $\varphi(m)$ daudzskaitnim, tāpēc ka

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

- dabiski ir definēt $\text{ind}_a(1) \equiv 0 \pmod{\varphi(m)}$;
- $\text{ind}_a(a) \equiv 1 \pmod{\varphi(m)}$.

1.4. piemērs.

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

1.6. 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 $1, 2, \dots, \varphi(m)$ ir dažādas un $g^{\varphi(m)} \equiv 1 \pmod{m}$. Redzam, ka

$$g^{s_1} \equiv g^{s_2} \pmod{m} \implies g^{s_1 - s_2} \equiv 1 \pmod{m},$$

, tāpēc $s_1 - s_2 \equiv 0 \pmod{\varphi(m)}$. ■

Iepriekšējā teorēma apgalvoto, ka ir korekti definēta funkcija

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

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

1.7. teorēma. Ja g ir primitīva sakne mod m , tad

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

PIERĀDĪJUMS

1. Injektivitāte

Ja $\text{ind}_g(a_1) \equiv \text{ind}_g(a_2) \pmod{\varphi(m)}$, tad

$$\text{ind}_g(a_1) = \text{ind}_g(a_2) + \varphi(m) \cdot l$$

un

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

un $a_1 \equiv a_2 \pmod{m}$, tātad ind_g ir injektīva funkcija.

Sirjektivitāte Tā kā g ir primitīva sakne, tad katram k eksistē $a \in U_m$ tāds, ka $a \equiv g^k \pmod{m}$, tātad ind_g ir sirjektivā funkcija.

2.

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

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

3.,4. - pierāda līdzīgi kā 2.

5.

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



1.6. piezīme. Pierādītā teorēma nozīmē to, ka funkcija 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 elementu reizināšanu grupā U_m var aizvietot ar to indeksu saskaitīšanu mod $\varphi(m)$, ja tajā eksistē primitīva sakne, saskaņā ar šādu algoritmu:

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

Ievērosim, ka šis algoritms ir analogisks 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 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

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

saskaņā ar šādu algoritmu:

1. atrast primitīvu sakni $g \pmod{m}$,
2. atrast a indeksu pie bāzes g , apzīmēsim to ar α ,
3. pieņemt, ka $x \equiv g^y \pmod{m}$, citiem vārdiem sakot, veikt nezināmo substitūciju $x \rightarrow y$,
4. izteikt vienādojuma abas puses kā g pakāpes, iegūt vienādojumu

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

5. atrisināt vienādojumu

$$ky \equiv \alpha \pmod{\varphi(m)}$$

attiecībā uz y .

1.8. piezīme. Aprakstīto algoritmu var vispārināt, ja grupa U_m nav cikliska:

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

2. 9.mājasdarbs

2.1. Obligātie uzdevumi

9.1 Atrodiet kādu primitīvu sakni mod 23.

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

(a) $m = 8$;

(b) $m = 21$.

Katrā no šiem gadījumiem atrodiet grupas (U_m, \cdot) minimālo ģenerējošo kopu.

9.3 Atrisīniet šādus vienādojumus:

(a) $x^6 \equiv 4 \pmod{23}$;

(b) $x^7 \equiv 9 \pmod{18}$;

(c) $x^2 y^3 \equiv 5 \pmod{11}$;

(d) $x^6 \equiv 3 \pmod{40}$.

(Norādījums: izmantojiet primitīvās saknes un minimālās ģenerējošās kopas)

2.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi

9.4 Pierādiet, ka

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

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

9.5 Pierādiet, ka ja $p \neq 3$ ir pirmskaitlis, tad visu primitīvo sakņu mod p reizinājums ir kongruents ar $1 \pmod{p}$.

9.6 Atrodiet primitīvo sakņu mod p summu mod p , ja p ir pirmskaitlis.