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

Studiju kurss

Veselo skaitļu teorija

12.lekcija (papildmateriāls)

Docētājs: Dr. P. Daugulis

2009./2010.studiju gads

Saturs

1. Kvadrātiskās reciprocitātes teorēma

1.1. Gausa lemma un tās pielietojumi

1.1. piezīme. Parasti mēs strādājam ar invertējamu atlikumu klašu pārstāvjiem no kopas

$$\mathcal{C} = \{1, ..., p-1\}.$$

Tagad strādāsim ar citu kopu -

$$\mathcal{G} = \{-\frac{p-1}{2}, ..., -1, 1, ..., \frac{p-1}{2}\}.$$

Kopa $\mathcal{G}$ tiek iegūta no $\mathcal{C}$ atņemot p no $\mathcal{C}$ elementiem $\frac{p-1}{2}+1, ..., p-1$ (un nemainot elementus $1, ..., \frac{p-1}{2}$).

Redzam, ka $\mathcal{G} = \mathcal{P} \cup \mathcal{N}$, kur $\mathcal{P} = \{1, ..., \frac{p-1}{2}\}$,$\mathcal{N} = \{-1, ..., -\frac{p-1}{2}\}$.

Definēsim

$$t\mathcal{P} = \{u \in U_p | u = tx, \text{ kur } x \in \mathcal{P}\} = \{t, 2t, 3t, ..., \frac{p-1}{2} \cdot t\}.$$

Piemēram, $\mathcal{N} = (-1)\mathcal{P}$.

1.2. piezīme. Reizināšana ar $a \in \mathcal{U}_p$ ir permutācija $U_p \to U_p$, kuru var reprezentēt ar tās grafu Γ_a (virsotņu kopa - $\mathcal{G}$, šķautnes formā $x \to ax$). Grafam Γ_a piemīt šādas simetrijas:

- škautne $u \to v$ starp divām kopas $\mathcal{P}$ virsotnēm eksistē $\iff$ eksistē šķautne starp $\mathcal{N}$ virsotnēm $-u \to -v$ ($au = v \implies a(-u) = -v$);
- škautne $u \to -v$ no $\mathcal{P}$ virsotnes uz $\mathcal{N}$ virsotni eksistē $\iff$ eksistē šķautne no $\mathcal{N}$ virsotnes uz $\mathcal{P}$ virsotni $-u \to v$ ($au = -v \implies a(-u) = v$);

Tā kā $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$, tad jautājums par $\left(\frac{a}{p}\right)$ vērtību ir loģiski ekvivalents šādam jautājumam: kāds ir galapunkts maršrutam grafā Γ_a ar garumu $\frac{p-1}{2}$, kas sākas ar virsotni (klasi) 1 - 1 vai -1?

1.1. teorēma. (*Gausa lemma*) $p \in \mathbb{P}, p > 2$, $\gamma = |a\mathcal{P} \bigcap \mathcal{N}|$. Tad

$$\left(\frac{a}{p}\right) = (-1)^{\gamma}.$$

PIERĀDĪJUMS Fiksēsim $a \in \mathcal{U}_p$. Definēsim

$$\begin{cases} R = 1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2} = \prod_{t \in \mathcal{P}} t \\ R' = \prod_{t \in \mathcal{P}} (at) = \prod_{u \in a\mathcal{P}} u \end{cases} \Longrightarrow R' = a^{\frac{p-1}{2}} R$$

Sāksim pētīt klases formā at, kur $t \in \mathcal{P}$. Daži no šiem elementiem ir kopā $\mathcal{P}$, daži - kopā $\mathcal{N}$.

Izdaram šādus secinājumus:

- Ja $at \in \mathcal{P}$ kādam $t \in \mathcal{P}$, tad $-(at) \notin a\mathcal{P}$, jo pretējā gadījumā mēs iegūtu, ka $-at \equiv at'$ (mod p) un $t \equiv -t'$ (mod p), kas ir pretruna, jo klasēm t un t' ir vienādas zīmes.
- Ja $at \in \mathcal{N}$ kādam $t \in \mathcal{P}$, tad $-(at) \notin a\mathcal{P}$ tā paša iemesla dēļ.

Tātad $a\mathcal{P} = S_+ \cup S_-$, kur $S_+ \subseteq \mathcal{P}$, $S_- \subseteq \mathcal{N}$, $S_+ \cap S_- = \emptyset$.

$|a\mathcal{P}| = |\mathcal{P}| \implies (-1)S_- \cup S_+ = \mathcal{P} \implies$ kopa $a\mathcal{P}$ atšķiras no kopas $\mathcal{P}$ ar to, ka dažām klasēm ir mainīta zīme, šādu elementu skaits ir $|S_-| = |a\mathcal{P} \cap \mathcal{N}|$.

Redzam, ka

$$R' = \prod_{u \in a\mathcal{P}} u = (\prod_{v \in S_+} v) \cdot (\prod_{w \in S_-} w) =$$

$$(\prod_{v \in S_+} v) \cdot (\prod_{-w \in (-1)S_-} (-w)) = (\prod_{v \in S_+} v) \cdot (\prod_{z \in \mathcal{P} \setminus S_+} z) \cdot (-1)^{|S_-|} =$$

$$(\prod_{t \in \mathcal{P}} t) \cdot (-1)^{|a\mathcal{P} \cap \mathcal{N}|} = R \cdot (-1)^{|a\mathcal{P} \cap \mathcal{N}|}.$$

$$R' = a^{\frac{p-1}{2}} R = R \cdot (-1)^{\gamma} \implies a^{\frac{p-1}{2}} = \left(\frac{a}{p}\right) = (-1)^{\gamma}. \blacksquare$$

1.1. piemērs. Atradīsim $\left(\frac{3}{13}\right)$ izmantojot Gausa lemmu. Šajā gadījumā $\mathcal{P} = \{1, ..., 6\}$, $\mathcal{N} = \{-1, ..., -6\}$. Redzam, ka

$$3\mathcal{P} = \{3, 6, -4, -1, 2, 5\}.$$

Tādējādi $\left(\frac{3}{13}\right) = (-1)^2 = 1$. Var arī pārbaudīt, ka $3 \equiv 4^2 \equiv 9^2 \pmod{13}$.

1.2. teorēma. $p \in \mathbb{P}, p > 2$.

1. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$;
2. $2 \in Q_p \iff p^2 \equiv 1 \pmod{8}$.

PIERĀDĪJUMS

1. Izmantosim Gausa lemmu. Ir jāatrod, cik elementu ir kopā $2\mathcal{P} \cap \mathcal{N}$. Zinām, ka

$$2\mathcal{P} = \{2, 4, ..., p-1\}.$$

Redzam, ka daži pirmie kopas $2\mathcal{P}$ elementi ir kopā $\mathcal{P}$, bet sākot ar kādu elementu visi nākamie ir kopā $\mathcal{N}$.

Mazākais $k \in \mathcal{P}$, kuram $2k > \frac{p-1}{2}$ un tāpēc $2k \in \mathcal{N}$, ir vienāds ar $\lceil \frac{p-1}{4} \rceil$. Tātad

$$2\mathcal{P} \cap \mathcal{N} = \{2 \cdot \lceil \frac{p-1}{4} \rceil, 2 \cdot (\lceil \frac{p-1}{4} \rceil + 1), ..., 2 \cdot \frac{p-1}{2}\}$$

un

$$|2\mathcal{P} \cap \mathcal{N}| = \frac{p-1}{2} - \lceil \frac{p-1}{4} \rceil + 1.$$

Ja $p \equiv 1 \pmod 4$, tad

$$|2\mathcal{P} \cap \mathcal{N}| = \frac{p-1}{2} - (\frac{p-1}{4} + 1) + 1 = \frac{p-1}{4}.$$

Ja $p \equiv 3 \pmod 4$, tad

$$|2\mathcal{P} \cap \mathcal{N}| = \frac{p-1}{2} - \frac{p+1}{4} + 1 = \frac{p+1}{4}.$$

Mums ir svarīgi zināt $|2\mathcal{P} \cap \mathcal{N}| \pmod 2$.

Skaitļi $\frac{p-1}{4}$ un $\frac{p+1}{4}$ var būt gan 0, gan 1 $\pmod 2$. Piemēram, ja $p \equiv 1 \pmod 4$, tad $p = 4n+1$ un $\frac{p-1}{4} \equiv n \pmod 2$, bet mēs neko nezinām par $n \pmod 2$.

Piemēram, ja $\frac{p-1}{4} \equiv 0 (\mathrm{mod}\ 2)$, tad

$$\frac{p-1}{4} = 2n' \iff p = 1 + 8n' \iff p \equiv 1 (\mathrm{mod}\ 8).$$

Tāpēc, lai atrastu $|2\mathcal{P} \cap \mathcal{N}| \pmod 2$, apskatīsim visus p atlikumus mod 8:

$$|2\mathcal{P} \cap \mathcal{N}| = \begin{cases} 0 \pmod 2, & \text{ja } p \equiv 1 \pmod 8, \\ 1 \pmod 2, & \text{ja } p \equiv 5 \pmod 8, \\ 1 \pmod 2, & \text{ja } p \equiv 3 \pmod 8, \\ 0 \pmod 2, & \text{ja } p \equiv 7 \pmod 8. \end{cases}$$

Var pārbaudīt, ka

$$|2\mathcal{P} \cap \mathcal{N}| \equiv \frac{(p-1)(p+1)}{8} \pmod 2.$$

2. Seko no iepriekšējā apgalvojuma. ■

1.2. Teorēma

1.3. teorēma. (*Ležandra simbola argumentu simetrijas (kvadrātiskās reciprocitātes) teorēma*) Dots, ka p un q ir nepāra pirmskaitļi.

1. Ja $p \not\equiv 3 \pmod 4$ vai $q \not\equiv 3 \pmod 4$, tad
$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right).$$

2. Ja $p \equiv q \equiv 3 \pmod 4$, tad
$$\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right).$$

Ekvivalents formulējums - $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$.

PIERĀDĪJUMS Izmantosim šādus apzīmējumus: $\mathcal{P} = \{1, 2, ..., \frac{p-1}{2}\}$, $\mathcal{N} = \{-1, -2, ..., -\frac{p-1}{2}\}$, $\mathcal{Q} = \{1, 2, ..., \frac{q-1}{2}\}$.

Saskaņā ar Gausa lemmu, $\left(\frac{q}{p}\right) = (-1)^{\gamma}$, kur $\gamma = |q\mathcal{P} \cap \mathcal{N}|$.

1.solis - γ interpretācija.
γ ir tādu $x \in \mathcal{P}$ skaits, kuriem $\exists\, n \in \mathcal{N} :\ qx \equiv n \pmod{\text{p}}$.

Tas ir ekvivalents nosacījumam, ka $\exists\ y \in \mathbb{Z} :\ \ qx - py \in \mathcal{N}$ un tātad

$$-\frac{p}{2} < qx - py < 0.$$

Katram x var būt ne vairāk kā viens y, jo pretējā gadījumā eksistē divi dažādi veseli y_1 un y_2 tādi, ka

$$-\frac{p}{2} < qx - py_1 < 0,$$

$$-\frac{p}{2} < qx - py_2 < 0.$$

Bet $|(qx - py_1) - (qx - py_2)| = |p(y_1 - y_2)| \geq p$.

Ja tāds y eksistē, tad pārveidojot nevienādības iegūsim

$$0 < \frac{qx}{p} < y < \frac{qx}{p} + \frac{1}{2}.$$

Tā kā $x \leq \frac{p-1}{2}$, tad

$$y < \frac{q(p-1)}{2p} + \frac{1}{2} < \frac{q+1}{2}.$$

Tātad $y \in \mathcal{Q} = \{1, 2, ..., \frac{q-1}{2}\}$. Esam pierādījuši, ka γ ir to veselu skaitļu pāru (x, y) skaits kopā $\mathcal{P} \times \mathcal{Q}$, kuri apmierina nosacījumu

$$-\frac{p}{2} < qx - py < 0.$$

2.solis - p un q maiņa. Mainot vietām p un q un izmantojot iepriekšējā soļa rezultātu, redzam, ka $\left(\frac{p}{q}\right) = (-1)^{\delta}$, kur δ ir to veselu skaitļu pāru (y, x) skaits kopā $\mathcal{Q} \times \mathcal{P}$, kas apmierina nevienādību

$$-\frac{q}{2} < py - qx < 0.$$

Reizinot visu ar $-$ zīmi un mainot nevienādības iegūsim ekvivalentu nosacījumu

$$0 < qx - py < \frac{q}{2}.$$

3.solis - iepriekšējo soļu rezultātu apvienošana un interpretēšana.

Redzam, ka

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\gamma+\delta},$$

kur $\gamma+\delta$ ir to skaitļu pāru skaits kopā $\mathcal{P}\times\mathcal{Q}$, kas apmierina nosacījumu

$$-\frac{p}{2} < qx - py < 0 \text{ vai } 0 < qx - py < \frac{q}{2}.$$

Tā kā $qx-py \neq 0$, jo $LKD(p,q) = 1$, tad varam abus nosacījumus apvienot vienā:

$$-\frac{p}{2} < qx - py < \frac{q}{2}.$$

Ievērosim arī, ka pietiek zināt $\gamma + \delta \pmod 2$, jo tas ir kāpinātājs skaitlim -1.

4.solis - rezultāta interpretēšana Dekarta koordinātēs.

Apzīmēsim ar T taisnstūri ar virsotnēm

$$(1,1), (1, \frac{q-1}{2}), (\frac{p-1}{2}, 1), (\frac{p-1}{2}, \frac{q-1}{2}).$$

Skaitļu pāriem no kopas $\mathcal{P} \times \mathcal{Q}$ atbilst punkti ar veselām Dekarta koordinātēm, kas pieder T.

Nevienādības

$$-\frac{p}{2} < qx - py < \frac{q}{2}$$

atrisinājumi ir punkti ar veselām Dekarta koordinātēm, kas atrodas joslā J, ko ierobežo taisnes

$$-\frac{p}{2} = qx - py \text{ un } qx - py = \frac{q}{2}.$$

Skaitļu pāriem, kas apmierina šo nevienādību, atbilst punkti ar veselām Dekarta koordinātēm, kas atrodas figūrā $\mathrm{T} \cap \mathrm{J}$. Tādu punktu skaits ir vienāds ar $t - a - b$, kur

- t ir punktu ar veselām koordinātēm skaits taisnstūrī T,
- a ir punktu ar veselām koordinātēm skaits slēgtajā apgabalā virs taisnes $-\frac{p}{2} = qx - py$,
- b ir punktu ar veselām koordinātēm skaits slēgtajā apgabalā zem taisnes $qx - py = \frac{q}{2}$.

5.solis - punktu skaits taisnstūrī T.

Redzam, ka punktu ar veselām koordinātēm skaits t taisnstūrī T ir vienāds ar elementu skaitu kopā $\mathcal{P} \times \mathcal{Q}$, kas ir vienāds ar

$$|\mathcal{P}| \cdot |\mathcal{Q}| = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

6.solis - vienādības $a = b$ pierādīšana.

Taisnstūris T ir figūra, kura ir centrāli simetriska ar centru

$$C = (\frac{p+1}{4}, \frac{q+1}{4}).$$

Centrālā simetrija šajā gadījumā ir pārveidojums

$$(x, y) \to (x', y') = (\frac{p+1}{2} - x, \frac{q+1}{2} - y)$$

(trīs vienkāršāku pārveidojumu kompozīcija - paralēli pārnest par vektoru $-\overrightarrow{OC}$, reizināt ar -1, pārnest atpakaļ par vektoru $\overrightarrow{OC}$).

Var pārbaudīt, ka taisnes

$$-\frac{p}{2} = qx - py$$

un

$$qx - py = \frac{q}{2}$$

arī ir centrāli simetriskas attiecībā uz T centru - punkts (x, y) apmierina vienu no vienādojumiem tad un tikai tad, ja punkts (x', y') apmierina otru vienādojumu. Piemēram, ja (x, y) apmierina vienādojumu $-\frac{p}{2} = qx - py$, tad

$$qx' - py' = q\Big(\frac{p+1}{2} - x\Big) - p\Big(\frac{q+1}{2} - y\Big) =$$
$$(py - qx) + \frac{pq}{2} + \frac{q}{2} - \frac{pq}{2} - \frac{p}{2} =$$
$$\frac{p}{2} + \frac{q}{2} - \frac{p}{2} = \frac{q}{2}.$$

Ņemot vērā centrālo simetriju redzam, ka katram punktam ar veselām koordinātēm taisntūrī T virs taisnes

$$-\frac{p}{2} = qx - py$$

atbilst simetriskais punkts zem taisnes

$$qx - py = \frac{q}{2},$$

tātad šādu punktu skaits ir vienāds un iegūstam, ka

$$a = b.$$

7.solis - lieluma $t-a-b$ paritāte un noslēgums. Tā kā $a = b$, tad

$$t - a - b = t - 2a \equiv t \pmod 2.$$

Redzam, ka $\gamma + \delta \equiv t \pmod 2$ $\Longrightarrow$

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\gamma+\delta} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.\blacksquare$$

2. Kvadrātiskie vienādojumi saliktiem moduļiem

2.1. Pirmskaitļu pakāpju moduļi

2.1. teorēma. $p > 2$ ir pirmskaitlis.

$$a \in Q_{p^\alpha} \iff a \in Q_p.$$

PIERĀDĪJUMS
No iepriekš dotām teorēmām seko šādi fakti:

- $\mathcal{G}_{p^\alpha} \neq \emptyset$.
- $\mathcal{Q}_{p^\alpha} = \langle g^2 \rangle$.

$$g \in \mathcal{G}_{p^\alpha} \implies g \in \mathcal{G}_p \implies \mathcal{Q}_p = \langle g^2 \rangle.$$

$$a \in Q_{p^\alpha} \iff a \equiv g^{2n} (\text{mod } p^\alpha) \implies$$
$$a \equiv g^{2n} (\text{mod } p) \iff a \in Q_p.$$

Pierādīsim, ka $a \in Q_p \implies a \in Q_{p^\alpha}$ izmantojot vienkāršotu matemātisko indukciju - pierādīsim, ka

$$\forall \beta \geq 1, a \in Q_{p^\beta} \implies a \in Q_{p^{\beta+1}}.$$

Ja $a \in Q_{p^\beta}$, tad vienādojumam

$$x^2 \equiv a (\text{mod } p^\beta)$$

eksistē atrisinājums $x = x_1 + p^\beta x_2$, kur $x_1 \not\equiv 0 (\text{mod } p^\beta)$.

Ievietosim to vienādojumā

$$x^2 \equiv a (\text{mod } p^{\beta+1}).$$

Iegūsim, ka

$$(x_1 + p^\beta x_2)^2 \equiv a (\text{mod } p^{\beta+1}) \iff \underbrace{(x_1^2 - a)}_{\equiv 0 (\text{mod } p^\beta)} + 2p^\beta x_1 x_2 \equiv 0 (\text{mod } p^{\beta+1})$$

$$\Longleftrightarrow \quad \frac{(x_1^2 - a)}{p^\beta} + 2x_1x_2 \equiv 0(\text{mod } p).$$

Redzam, ka pēdējam vienādojumam ir atrisinājums attiecībā uz x_2:

$$x_2 \equiv -\frac{(x_1^2 - a)}{2x_1p^\beta}(\text{mod } p).\blacksquare$$

2.1. piemērs. $Q_7 = \{1, 2, 4\}$.

$$Q_{49} = \{1, 2, 4, 8, 9, 11, 15, 16, 18, 22, 23, 25, 29, 30, 32, 36, 37, 39, 43, 44, 46\}.$$

Redzam, ka

$$\begin{aligned} Q_{49} = \{\underline{1}, 8, 15, 22, 29, 36, 43\} \cup \\ \{\underline{2}, 9, 16, 23, 30, 37, 44\} \cup \\ \{\underline{4}, 11, 18, 25, 32, 39, 46\} = \\ \pi_{49,7}^{-1}(1) \cup \pi_{49,7}^{-1}(2) \cup \pi_{49,7}^{-1}(4). \end{aligned}$$

2.2. teorēma.

1. $a \in Q_2 \Longleftrightarrow a \equiv 1(\text{mod } 2)$.

2. $a \in Q_4 \iff a \equiv 1 (\mathrm{mod}\ 4)$.

3. $\alpha \geq 3 \implies a \in Q_{2^\alpha} \iff a \equiv 1 (\mathrm{mod}\ 8)$.

PIERĀDĪJUMS

1., 2. Tieša pārbaude.

3. Detalizēts pierādījums netiks dots. Viens ceļš - no sākuma pierādīt, ka $\mathcal{U}_{2^\alpha}$ ģenerējošā kopa ir $\{5, -1\}$. ■

2.2. piemērs. $Q_{32} = \pi_{32,8}^{-1}(1) = \{1, 9, 17, 25\}$.

2.2. Patvaļīgi moduļi

2.3. teorēma. Dots, ka $m = m_1 m_2 ... m_l$, kur $LKD(m_i, m_j) = 1$. Tad

$$a \in Q_m \iff a \in Q_{m_i}, \forall i.$$

PIERĀDĪJUMS

$a \in Q_m \implies \exists x \in \mathbb{Z} : x^2 \equiv a(\text{mod } m) \implies x^2 \equiv a(\text{mod } m_i), \forall i.$
Tas seko no tā, ka $m_i | m$. Papildus tam $a \in U_m \implies a \in U_{m_i}$.

$a \in Q_{m_i}, \forall i \implies \forall i \exists x_i : x_i^2 \equiv a(\text{mod } m_i).$

Saskaņā ar ķīniešu atlikumu teorēmu sistēmai

$$\begin{cases} x \equiv x_1(\text{mod } m_1) \\ \dots \\ x \equiv x_l(\text{mod } m_l) \end{cases}$$

eksistē atrisinājumu klase x mod m.

Seko, ka x apmierina sistēmu

$$\begin{cases} x^2 \equiv a(\text{mod } m_1) \\ \dots \\ x^2 \equiv a(\text{mod } m_l) \end{cases} \iff x^2 \equiv a(\text{mod } m).$$

Tas seko no iepriekš pierādītas teorēmas. ■

2.1. piezīme. Speciālgadījumā iegūsim šādu apgalvojumu:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_l^{\alpha_l} \implies \left(a \in Q_m \iff a \in Q_{p_i^{\alpha_i}}, \forall i. \right)$$

2.4. teorēma. Dots, ka $m = p_1^{\alpha_l} p_2^{\alpha_2} ... p_l^{\alpha_l}$.

$$a \in Q_m \iff$$

1. $a \in Q_{p_i}, \forall i, p_i > 2.$
2. $$ord_2(m) \leq 2 \implies a \equiv 1 (\text{mod } 4) \wedge$$
$$ord_2(m) > 2 \implies a \equiv 1 (\text{mod } 8).$$

2.3. piemērs. Atradīsim Q_{72}. $72 = 2^3 3^2$. Seko, ka

$$a \in Q_{72} \iff a \equiv 1 (\text{mod } 3) \wedge a \equiv 1 (\text{mod } 8).$$

Sistēmas

$$\begin{cases} a \equiv 1 (\text{mod } 3) \\ a \equiv 1 (\text{mod } 8) \end{cases}$$

atrisinājums ir $a \equiv 1(\text{mod } 24)$. Seko, ka

$$Q_{72} = \pi_{72,24}^{-1}(1) = \{1, 25, 49\}.$$

3. Augstāku pakāpju atlikumi

3.1. teorēma. $p \in \mathbb{P}$, $n \geq 2$, $d = LKD(n, p-1)$, $a \not\equiv 0(\text{mod } p)$, $g \in \mathcal{G}_p$.

1. $a \in \mathcal{Q}_{n,p} \iff \mathsf{ind}_g(a) \equiv 0(\text{mod } d)$.
2. $\mathsf{ind}_g(a) \equiv 0(\text{mod } d) \iff a^{\frac{p-1}{d}} \equiv 1(\text{mod } p)$.
3. $a \in \mathcal{Q}_{n,p} \implies$ vienādojumam
$$x^n \equiv a(\text{mod } p)$$
ir d dažādi atrisinājumi mod p;
4. $|\mathcal{Q}_{n,p}| = \frac{p-1}{d}$.

PIERĀDĪJUMS

1. $a \in \mathcal{Q}_{n,p} \iff \exists y \in \mathbb{Z}$ tāds, ka

$$\begin{cases} x \equiv g^y (\mathrm{mod}\ p) \\ x^n \equiv g^{ny} \equiv g^{\mathsf{ind}_g}(a) (\mathrm{mod}\ p) \end{cases}$$

$$\iff ny \equiv \mathsf{ind}_g(a) (\mathrm{mod}\ p-1).$$

Lineārajai kongruencei ir atrisinājums $\iff$

$$\mathsf{ind}_g(a) \equiv 0 (\mathrm{mod}\ d)$$

2. $\mathsf{ind}_g(a) \equiv 0 (\mathrm{mod}\ d) \implies \exists x : x^n \equiv a (\mathrm{mod}\ p) \implies$

$$a^{\frac{p-1}{d}} \equiv x^{n\frac{p-1}{d}} \equiv (x^{p-1})^{\frac{n}{d}} \equiv 1 (\mathrm{mod}\ p).$$

Apzīmēsim $\mathsf{ind}_g(a)$ ar t. Tad

$$a^{\frac{p-1}{d}} \equiv g^{t\frac{p-1}{d}} \equiv 1 (\mathrm{mod}\ p) \implies t\frac{p-1}{d} \equiv 0 (\mathrm{mod}\ p-1).$$

$LKD(\frac{p-1}{d}, p-1) = 1$, tāpēc var dalīt abas puses ar $\frac{p-1}{d}$. Seko, ka

$$t \equiv 0 (\mathrm{mod}\ p-1) \implies t \equiv 0 (\mathrm{mod}\ d).$$

3. Ja

$$\mathsf{ind}_g(a) \equiv 0(\text{mod } d),$$

tad lineārajai kongruencei

$$ny \equiv \mathsf{ind}_g(a)(\text{mod } p-1)$$

ir d dažādi atrisinājumi mod p - tas seko no lineārā vienādojuma atrisinājumu īpašībām (jāizmanto inversā relatīvā redukcija no $\frac{p-1}{d}$ uz $p-1$.

4. $a \in \mathcal{Q}_{n,p} \iff \iff \mathsf{ind}_g(a) \equiv 0(\text{mod } d)$. ind_g pieņem visas vērtības mod $p-1$ un vienādojumam

$$z \equiv 0(\text{mod } d)$$

ir $\frac{p-1}{d}$ atrisinājumi formā

$$0, 0+d, 0+2d, ..., 0+\frac{p-1}{d}-1.$$

Tādējādi eksistē tieši $\frac{p-1}{d}$ n-tās pakāpes atlikumi.

$$g^0, g^d, ..., g^{d\cdot(\frac{p-1}{d}-1)}. \blacksquare$$

3.1. piemērs. $p = 11$.

$n = 2$. $Q_{2,11} = \{1, 3, 4, 5, 9\}$. $|Q_{2,11}| = 5 = \frac{11-1}{LKD(2,10)} = 5$.

$n = 3$. $Q_{3,11} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. $|Q_{3,11}| = 10 = \frac{11-1}{LKD(3,10)} = 10$.

$n = 4$. $Q_{4,11} = \{1, 3, 4, 5, 9\}$. $|Q_{4,11}| = 5 = \frac{11-1}{LKD(4,10)} = 5$.

$n = 5$. $Q_{5,11} = \{1, 10\}$. $|Q_{5,11}| = 5 = \frac{11-1}{LKD(5,10)} = 2$.

$n = 6$. $Q_{6,11} = \{1, 3, 4, 5, 9\}$. $|Q_{6,11}| = 5 = \frac{11-1}{LKD(6,10)} = 5$.

4. 12.mājasdarbs

12.7 Atrisināt vienādojumus

(a) $x^2 \equiv 11 (\mathrm{mod}\ 625)$;
(b) $x^2 \equiv 9 (\mathrm{mod}\ 32)$;
(c) $x^2 \equiv 3 (\mathrm{mod}\ 7^5)$.

12.8 Atrisināt vienādojumus

(a) $x^2 \equiv 13 (\mathrm{mod}\ 108)$;
(b) $x^2 \equiv 79 (\mathrm{mod}\ 210)$.
(c) $x^2 \equiv 37 (\mathrm{mod}\ 441)$.

12.9 Atrast

(a) Q_{144},
(b) Q_{168},
(c) Q_{264}.

12.10 Atrast

(a) $Q_{3,13}$,
(b) $Q_{4,13}$,
(c) $Q_{6,19}$.