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

Studiju kurss

Veselo skaitļu teorija

12.lekcija

Docētājs: Dr. P. Daugulis

2007./2008.studiju gads

Saturs

1. Vienādojumu risināšana atlikumu gredzenos - kvadrātiskie vienādojumi

1.1. Kvadrātiskie vienādojumi atlikumu gredzenos ar pirmskaitļa moduli

1.1.1. Pamatfakti

1.1. piezīme. Kvadrātisku vienādojumu

$$a_2x^2 + a_1x + a_0 \equiv 0 \pmod{\mathrm{p}}$$

ar lineāru substitūciju $x \to x' = x + c$ var reducēt uz vienādojumu formā

$$x'^2 \equiv a \pmod{\mathrm{p}}$$

Tiešām, pirmkārt, var izdalīt ar a_2 un iegūt vienādojumu

$$x^2 + rx + s \equiv 0 \pmod{\mathrm{p}}.$$

Otrkārt, 2 ir invertējams elements mod p, tāpēc

$$x^2+rx+s \equiv x^2+2\cdot\frac{r}{2}\cdot x+(\frac{r}{2})^2-(\frac{r}{2})^2+s \equiv (x+\frac{r}{2})^2-(\frac{r}{2})^2+s \pmod{\text{p}}.$$

Ja $x' \equiv x+\frac{r}{2}$, tad attiecībā uz x' iegūsim vienādojumu

$$x'^2 \equiv (\frac{r}{2})^2 - s \pmod{\text{p}}.$$

1.1. piemērs. Pārveidosim vienādojumu $x^2+x+1 \equiv 0 \pmod 5$:

$$x^2+x+1 \equiv x^2+2\cdot\frac{1}{2}\cdot x+1 \equiv x^2+2\cdot 3\cdot x+1 \equiv$$
$$x^2+2\cdot 3\cdot x+(3)^2-(3)^2+1 \equiv$$
$$(x+3)^2+2 \equiv 0 \pmod 5.$$

Veicot substitūciju $x \to x' = x+3$, attiecībā uz jauno nezināmo x' iegūsim vienādojumu $x'^2 \equiv 3 \pmod 5$.

Tālāk mēs pētīsim tikai šādus kvadrātiskus vienādojumus.

1.2. piezīme. Vienādojumam $x^2 \equiv a \pmod{p}$ atrisinājumu kopa var būt tukša. Piemērs - $x^2 \equiv 2 \pmod{5}$ (jo 2 ir primitīva sakne).

1.3. piezīme. Ja x_0 ir vienādojuma $x^2 \equiv a \pmod{p}$ atrisinājums, tad $-x_0$ arī ir atrisinājums. Ja $x_0 \equiv -x_0 \pmod{p}$ tad $p = 2$. Vairāk kā divi atrisinājumi nevar būt saskaņā ar Bezū teorēmu. Tātad šādam vienādojumam var būt nulle vai divi atrisinājumi, ja $p > 2$.

1.2. piemērs. Vienādojumam $x^2 \equiv 2 \pmod{7}$ atrisinājumi ir 3 un $-3 \equiv 4 \pmod{7}$.

Atlikumu klasi $a \not\equiv 0 \pmod{p}$ sauksim par *kvadrātisku atlikumu*, ja vienādojumam $x^2 \equiv a \pmod{p}$ ir atrisinājumi. Visu kvadrātisko atlikumu kopu mod m apzīmēsim ar Q_m.

1.4. piezīme. $Q_m = \{t^2 | t \in U_m\}$.

1.1. teorēma. Kopa Q_m apmierina šādas īpašības:

1. $1 \in Q_m$.
2. Ja $a \in Q_m$ un $b \in Q_m$, tad $ab \in Q_m$ (Q_m ir slēgta attiecībā uz reizināšanu).
3. Ja $a \in Q_m$, tad $a^{-1} \in Q_m$ (Q_m ir slēgta attiecībā uz inverso elementu iekļaušanu).

PIERĀDĪJUMS 1. $1^2 \equiv 1 \pmod{m}$.

2. Ja $x^2 \equiv a \pmod{m}$ un $y^2 \equiv b \pmod{m}$, tad $(xy)^2 \equiv ab \pmod{m}$ un tādējādi $ab \in Q_m$.

3. Ja $x^2 \equiv a \pmod{m}$, tad $(\frac{1}{x})^2 \equiv a^{-1} \pmod{m}$ un tādējādi $a^{-1} \in Q_m$. ■

1.5. piezīme. Grupu teorijas terminos iepriekšējā teorēma nozīmē to, ka Q_m ir U_m apakšgrupa.

1.2. teorēma. Ja kopā U_m, $m > 2$, eksistē primitīvā sakne g, tad g^2 ir kopas Q_m ģenerators - katram $a \in Q_m$ eksistē naturāls k tāds, ka $a \equiv (g^2)^k \pmod{m}$

PIERĀDĪJUMS Ja $n = 2n_1$ ir pāra skaitlis, tad $g^n \equiv (g^{n_1})^2 \in Q_m$, tātad g kāpināts pāra pakāpē pieder Q_m. Otrādi, ja $a \in Q_m$, tad $a \equiv b^2$ un tāpēc $a \equiv (g^l)^2 \equiv g^{2l} \pmod{m}$. ■

1.6. piezīme. Ja $p > 2$, tad $\varphi(p) = p - 1$ ir pāra skaitlis. U_p veido ģeneratora pāra pakāpes ar kāpinātājiem kopā $\{0, ..., p-2\}$. Šādu kāpinātāju skaits ir $\frac{p-1}{2}$, tāpēc $|Q_p| = \frac{p-1}{2}$.

1.7. piezīme. Vēl daži secinājumi no iepriekšējās teorēmas:

1. Primitīvās saknes g nepāra pakāpes ģenerē nekvadrātisko atlikumu kopu.
2. Kvadrātiska atlikuma un nekvadrātiska atlikuma reizinājums ir nekvadrātisks atlikums.
3. Divu nekvadrātisku atlikumu reizinājums ir kvadrātisks atlikums.

1.1.2. Eilera kritērijs

1.3. teorēma. (*Eilera kritērijs*)

1. a ir kvadrātisks atlikumus tad un tikai tad, ja
$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$
2. a ir nekvadrātisks atlikumus tad un tikai tad, ja
$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

PIERĀDĪJUMS Katram $a \in U_p$ elements $e = a^{\frac{p-1}{2}}$ saskaņā ar Eilera teorēmu apmierina vienādību $e^2 \equiv 1 \pmod{p}$, tāpēc tas ir vienādojuma
$$x^2 - 1 \equiv (x-1)(x+1) \equiv 0 \pmod{p}$$
atrisinājums, tātad $a^{\frac{p-1}{2}} \in \{1, -1\} \pmod{p}$.

Ja $a \in Q_p$, tad $a \equiv g^{2n} \pmod{p}$, tātad $a^{\frac{p-1}{2}} \equiv (g^{p-1})^n \equiv 1 \pmod{p}$.

Ja a ir nekvadrātisks atlikums, tad $a \equiv g^{2n+1}$ un

$$a^{\frac{p-1}{2}} \equiv g^{(2n+1)\frac{p-1}{2}} \equiv g^{(p-1)n} g^{\frac{p-1}{2}} \equiv g^{\frac{p-1}{2}} \not\equiv 1 \pmod{\text{p}},$$

jo tas nozīmētu, ka g kārta ir mazāka kā $p-1$ un tādējādi g nav primitīva sakne. Ir pierādīts, ka $a^{\frac{p-1}{2}} \equiv -1 \pmod{\text{p}}$. ■

1.3. piemērs. Apskatīsim gadījumu $p = 7$, $\frac{p-1}{2} = 3$. Apskatīsim nenulles atlikumu kubus:

$$1^3 \equiv 1, 2^3 \equiv 1, 3^3 \equiv -1, 4^3 \equiv 1, 5^3 \equiv -1, 6^3 \equiv -1 \pmod{7}.$$

Redzam, ka kvadrātiskie atlikumi ir $1, 2, 4$.

Apskatīsim gadījumu $p = 11$, $\frac{p-1}{2} = 5$. Apskatīsim nenulles atlikumu piektās pakāpes:

$$1^5 \equiv 1, 2^5 \equiv -1, 3^5 \equiv 1,$$
$$4^5 \equiv 1, 5^5 \equiv 1, 6^5 \equiv -1,$$
$$7^5 \equiv -1, 8^5 \equiv -1, 9^5 \equiv 1,$$
$$11^5 \equiv -1 \pmod{11}.$$

Redzam, ka kvadrātiskie atlikumi ir $1, 3, 4, 5, 9$.

1.4. teorēma. Skaitļi $1^2, 2^2, ..., (\frac{p-1}{2})^2$ veido kvadrātisko atlikumu klašu pārstāvju kopu mod p.

PIERĀDĪJUMS Katrs no šiem skaitļiem acīmredzami ir kvadrātisks atlikums. Pierādīsim, ka tie ir dažādi mod p. Pieņemsim, ka

$$1 \leq u \leq \frac{p-1}{2}, 1 \leq v \leq \frac{p-1}{2} \text{ un } u \neq v.$$

Redzam, ka

$$u^2 - v^2 \equiv (u-v)(u+v) \pmod{\text{p}},$$

bet

$$u - v \not\equiv 0 \pmod{\text{p}} \text{ un } u + v \not\equiv 0 \pmod{\text{p}}, \text{ jo } u + v < p.$$

Tādējādi $u^2 - v^2 \not\equiv 0 \pmod{\text{p}}$ un $u^2 \not\equiv v^2 \pmod{\text{p}}$. Esam pierādījuši, ka visi kopas $\{1^2, ..., (\frac{p-1}{2})^2\}$ elementi pārstāv kvadrātiskus atlikumus un tie ir dažādi mod p. Bet kvadrātisko atlikumu skaits ir vienāds ar $\frac{p-1}{2}$. Tātad šie skaitļi pārstāv visus kvadrātiskos atlikumus. ■

1.4. piemērs. Ja $p = 7$, tad skaitļi $1, 4, 9$ pārstāv kvadrātiskos atlikumus.

1.1.3. Ležandra simbols

Eilera kritērijs un atlikumu reizināšanas īpašības attiecībā uz kvadrātiskumu vedina uz ideju attēlot U_p uz kopu $\{1, -1\}$ tā, lai šis attēlojums kalpotu par kvadrātiskuma indikatoru.

Par *Ležandra simbolu* sauksim funkciju $U_p \to \{1, -1\}$, kas ir definēta šādi:

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} = \begin{cases} 1, & \text{ja } a \text{ ir kvadrātisks atlikums mod p,} \\ -1, & \text{ja } a \text{ ir nekvadrātisks atlikums mod p.} \end{cases}$$

Ležandra simbola definīciju var paplašināt uz visu kopu $\mathbb{Z}/p\mathbb{Z}$ definējot $\left(\frac{0}{p}\right) = 0$.

1.5. teorēma. Pieņemsim, ka $p > 2$ ir pirmskaitlis.

1. Ja $a \equiv a'$ (mod p), tad $\left(\frac{a}{p}\right) = \left(\frac{a'}{p}\right)$ (modulārā īpašība).
2. Ja g ir primitīva sakne mod p, tad $\left(\frac{g^k}{p}\right) = (-1)^k$.
3. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ (multiplikatīvā īpašība).
4. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

PIERĀDĪJUMS 3. Ja $a \equiv g^k$ (mod p) un $b \equiv g^l$ (mod p), tad

$$\left(\frac{ab}{p}\right) = \left(\frac{g^k g^l}{p}\right) = \left(\frac{g^{k+l}}{p}\right) = (-1)^{k+l} = (-1)^k(-1)^l = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

■

1.8. piezīme. Multiplikatīvā īpašība grupu teorijas terminos nozīmē to, ka Ležandra simbols ir grupu homomorfizms $(U_p, \cdot) \to (\{1, -1\}, \cdot)$. Multiplikatīvā īpašība nozīmē arī to, ka pietiek zināt lielumus $\left(\frac{q}{p}\right)$, kur p un q ir pirmskaitļi.

1.5. piemērs.

$$\left(\frac{24}{43}\right) = \left(\frac{2^3 \cdot 3}{43}\right) = \left(\frac{2}{43}\right)^3 \left(\frac{3}{43}\right) = \left(\frac{2}{43}\right)\left(\frac{3}{43}\right)$$

1.1.4. Gausa lemma un tās pielietojumi

1.9. piezīme. Parasti mēs strādājam ar atlikumu klašu pārstāvjiem no kopas

$$\mathcal{C} = \{0, 1, ..., p-1\}.$$

Tagad strādāsim ar citu atlikumu klašu pārstāvju 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 $\frac{p-1}{2}+1, ..., p-1$. 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, $\mathcal{N} = (-1)\mathcal{P}$.

1.10. piezīme. Reizināšana ar $a \in U_p$ ir bijektīva funkcija $U_p \to U_p$, 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 tad un tikai ja eksistē šķautne starp $\mathcal{N}$ virsotnēm $-u \to -v$ (ja $au = v$, tad $a(-u) = -v$);
- škautne $u \to -v$ no $\mathcal{P}$ virsotnes uz $\mathcal{N}$ virsotni eksistē tad un tikai ja eksistē šķautne no $\mathcal{N}$ virsotnes uz $\mathcal{P}$ virsotni $-u \to v$ (ja $au = -v$, tad $a(-u) = v$);

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?

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

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

PIERĀDĪJUMS Fiksēsim $a \in U_p$. Definēsim

$$R = 1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2} = \prod_{t \in \mathcal{P}} t$$

un

$$R' = \prod_{t \in \mathcal{P}} (at) = \prod_{u \in a\mathcal{P}} u.$$

Redzam, ka $R' = a^{\frac{p-1}{2}} R$.

Sāksim pētīt klases formā at, kur $t \in \mathcal{P}$. Daži no šiem elementiem ir kopā $\mathcal{P}$, daži - kopā $\mathcal{N}$. Veicam 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 pretuna, 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 $S_+ \subseteq \mathcal{P}$, $S_- \subseteq \mathcal{N}$, $S_+ \cap S_- = \emptyset$.

Ievērosim, ka $|a\mathcal{P}| = |\mathcal{P}|$, tāpēc $(-1)S_- \cup S_+ = \mathcal{P}$, tātad 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

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

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

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

Tā kā $R' = a^{\frac{p-1}{2}} R = R \cdot (-1)^{\gamma}$, tad

$$a^{\frac{p-1}{2}} = \left(\frac{a}{p}\right) = (-1)^{\gamma}.$$

■

1.6. 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 $3 \equiv 4^2 \equiv 9^2 \pmod{13}$.

1.7. teorēma. Ja $p > 2$ ir pirmskaitlis, tad

1. $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$;
2. $2 \in Q_p$ tad un tikai tad, ja $p^2 \equiv 1 \pmod 8$.

PIERĀDĪJUMS 1. Izmantosim Gausa lemmu. Ir jāatrod, cik elementu ir kopā $2\mathcal{P} \cap \mathcal{N}$. Zināms, 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 $n \pmod 2$.

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. ■

1.1.5. Kvadrātiskās reciprocitātes teorēma un tās pielietojumi

1.8. 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 veselu skaitļu $x \in \mathcal{P}$ skaits, kuriem eksistē vesels $n \in \mathcal{N}$ tāds, ka $qx \equiv n \pmod{p}$. Tas ir ekvivalents nosacījumam, ka eksistē vesels skaitlis y tāds, ka $qx - py \in \mathcal{N}$ un tātad

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

Katram x var būt ne vairāk kā viens y. 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 $\gamma + \delta \equiv t \pmod 2$, tātad

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

■

1.11. piezīme. Kvadrātiskās reciprocitātes teorēma ļauj būtiski paātrināt Ležandra simbola aprēķināšanu, vairākkārtīgi izmantojot Ležandra simbolu maiņas un īpašības (modularitāti, multiplikativitāti).

1.7. piemērs. Noteiksim, vai eksistē atrisinājumi vienādojumam

$$x^2 \equiv 37 \pmod{73}.$$

Redzam, ka

$$\left(\frac{37}{73}\right) = \left(\frac{73}{37}\right) = \left(\frac{36}{37}\right) = \left(\frac{2}{37}\right)^2 \left(\frac{3}{37}\right)^2 = 1,$$

tāpēc eksistē divi atrisinājumi.

Noteiksim, vai eksistē atrisinājumi vienādojumam

$$x^2 \equiv 31 \pmod{73}.$$

Redzam, ka

$$\left(\frac{31}{73}\right) = \left(\frac{73}{31}\right) = \left(\frac{11}{31}\right) = -\left(\frac{31}{11}\right) = -\left(\frac{9}{11}\right) = -\left(\frac{3}{11}\right)^2 = -1,$$

tāpēc atrisinājumi neeksistē.

2. 12.mājasdarbs

12.1 Nosakiet, vai ir atrisināmi vienādojumi

(a) $x^2 \equiv 7 \pmod{17}$,
(b) $x^2 \equiv 989 \pmod{1987}$,
(c) $x^2 \equiv 2008 \pmod{2007}$,
(d) $x^2 \equiv 2007 \pmod{2008}$.

12.2 Nosakiet, vai ir atrisināmi vienādojumi

(a) $x^4 \equiv 5 \pmod{13}$,
(b) $x^6 \equiv 10 \pmod{23}$.

12.3 Pierādiet, ka vienādojums

$$(x^2 - 2)(x^2 - 3)(x^2 - 6) \equiv 0 \pmod{p}$$

ir atrisināms katram pirmskaitlim p.

12.4 Nosakiet, kādiem pirmskaitļiem ir atrisināms vienādojums

$$x^2 \equiv 3 \pmod{p}.$$

(Norādījums - mod 12)