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

Studiju kurss

Veselo skaitļu teorija

12.lekcija

Docētājs: Dr. P. Daugulis

2009./2010.studiju gads

Saturs

Lekcijas mērķis:

- apgūt modulāro vienādojumu un sistēmu risināšanu ar saliktiem moduļiem, apgūt kvadrātisko modulāro vienādojumu risināšanu.

Lekcijas kopsavilkums:

- vienādojumus mod p^α var risināt sākot ar mazām pakāpēm,
- vienādojumus ar saliktiem moduļiem var risināt izmantojot ĶAT,
- kvadrātiskus vienādojumus var risināt ar specifiskām metodēm.

Svarīgākie jēdzieni: kvadrātiskie un nekvadrātiskie atlikumu, augstāku pakāpju atlikumi, Ležandrs simbols.

Svarīgākie fakti un metodes: modulāro vienādojumu risināšanas algoritms mod p^α, modulāro vienādojumu mod p^α atrisināmības kritērijs, modulāro vienādojumu risināšanas algoritms ar saliktu moduli izmantojo ĶAT, kvadrātisko atlikumu īpašības, Eilera kritērijs, Ležandra simbola īpašības, kvadrātiskās reciprocitātes teorēmas formulējums.

1. Modulārie vienādojumi ar saliktu moduli

1.1. Modulārie vienādojumi ar pirmskaitļa pakāpes moduli

1.1. piezīme. Modulāros vienādojumus mod p^α risināsim izmantojot šādu zināmo faktu:

$$\begin{cases} a \equiv b \pmod{\mathrm{m}} \\ k|m \end{cases} \implies a \equiv b \pmod{k}.$$

Konkrētāk, risināsim modulāros vienādojumus sākot no mazām p pakāpēm: no sākuma mod p, pēc tam mod p^2 u.t.t.

1.2. piezīme. Algoritms vienādojuma $f(x) \equiv 0 \pmod{p^\alpha}$ risināšanai:

1. Atrisināsim vienādojumu

$$f(x) \equiv 0 \pmod{\mathrm{p}},$$

iegūsim atrisinājumu kopu S_1.

2. Katram $s \in S_1$ ievietosim $x = s + x'p$ vienādojumā

$$f(x) \equiv 0 \pmod{p^2},$$

atrisināsim iegūto vienādojumu attiecībā uz x', iegūsim atrisinājumu kopu S_2;

3. ...

1.1. piemērs. Atrisināsim vienādojumu $3x^2 + x - 1 \equiv 0 \pmod{27}$.

1. Jebkurš atrisinājums x apmierina vienādojumu

$$3x^2 + x - 1 \equiv 0 \pmod{3} \implies x \equiv 1 \pmod{3}.$$

2. Ievietosim iegūto atrisinājumu $x = 1 + 3x'$ vienādojumā

$$3x^2 + x - 1 \equiv 0 \pmod{9} \implies 3x' + 3 \equiv 0 \pmod{9}.$$

Izdalīsim visu ar 3 $\implies$ $x' + 1 \equiv 0 \pmod{3}$ $\implies$ $x' \equiv 2 \pmod{3}$. Tātad $x \equiv 1 + 3 \cdot 2 = 7 \pmod{9}$.

3. Ievietosim iegūto atrisinājumu $x = 7 + 9x''$ vienādojumā

$$3x^2 + x - 1 \equiv 0 \pmod{27}.$$

Iegūsim vienādojumu $9x'' + 18 \equiv 0 \pmod{27}$. Izdalīsim visu ar $9 \implies x'' + 2 \equiv 0 \pmod{3} \implies x'' \equiv 1 \pmod{3}$.

Atbilde ir $x \equiv 7 + 9 \cdot 1 = 16 \pmod{27}$.

1.1. teorēma. $f(s) \equiv 0 (\mathrm{mod}\ p^\alpha)$.

1. $f'(s) \not\equiv 0 (\mathrm{mod}\ p) \implies \exists$ tieši viens $t \in \mathbb{Z}_p$:

$$f(s + tp^\alpha) \equiv 0 (\mathrm{mod}\ p^{\alpha+1}).$$

2. $\begin{cases} f'(s) \equiv 0 (\mathrm{mod}\ p) \\ f(s) \equiv 0 (\mathrm{mod}\ p^{\alpha+1}) \end{cases} \implies f(s + tp^\alpha) \equiv 0 (\mathrm{mod}\ p^{\alpha+1}), \forall\ t \in \mathbb{Z}_p.$

3. $\begin{cases} f'(s) \equiv 0 (\mathrm{mod}\ p) \\ f(s) \not\equiv 0 (\mathrm{mod}\ p^{\alpha+1}) \end{cases} \implies f(s + tp^\alpha) \not\equiv 0 (\mathrm{mod}\ p^{\alpha+1}), \forall\ t \in \mathbb{Z}_p.$

1.2. Risināšanas vispārīgā shēma gadījumā ar saliktu moduli

1.2. teorēma. Ja $m = m_1 ... m_l$, kur $LKD(m_i, m_j) = 1$, $\forall i, j$, tad

$$f(x) \equiv 0 \pmod{\text{m}} \iff \begin{cases} f(x) \equiv 0 \pmod{m_1} \\ f(x) \equiv 0 \pmod{m_2} \\ ... \\ f(x) \equiv 0 \pmod{m_l}. \end{cases}$$

PIERĀDĪJUMS Saskaņā ar iepriekš pierādītu faktu sistēmas atrisinājumi veido klases mod $MKD(m_1, ..., m_l) = m$.

$a \in \mathbb{Z}$ apmierina sistēmu $\Longrightarrow$ $m_i | f(a), \forall\ i$ $\Longrightarrow$ $m | f(a)$ $\Longleftrightarrow$ $f(a) \equiv 0 (\text{mod } m)$.

$f(b) \equiv 0 \pmod{\text{m}}$ $\Longrightarrow$ $f(b) \equiv 0 \pmod{m_i} \forall\ i$, jo $m_i | m$ $\Longrightarrow$ b apmierina sistēmu. ■

1.3. piezīme. Speciālgadījumā iegūsim apgalvojumu, ja $m = p_1^{\alpha_1} ... p_l^{\alpha_l}$.

1.4. piezīme. Algoritms vienādojuma $f(x) \equiv 0 \pmod{m}$ risināšanai mod $m = p_1^{\alpha_1} ... p_l^{\alpha_l}$:

1. Atrisināt vienādojumu $f(x) \equiv 0 \bmod p_i^{\alpha_i}, \forall\ i$. Šī soļa rezultātā tiek iegūtas atlikumu klašu kopas S_i, kur $S_i \subseteq \mathbb{Z}_{p_i^{\alpha_i}}$ (*lokālie atrisinājumi*).

2. Rekonstruēt sākotnējā vienādojuma veselos (*globālos*) atrisinājumus no lokālajiem atrisinājumiem (mod $p_i^{\alpha_i}$) izmantojot ĶAT: $\forall$ atlikumu virknei no $(a_1, ..., a_l) \in S_1 \times S_2 \times ... \times S_l$ piekārtot atlikumu klases mod m. Citiem vārdiem sakot, ja $a_i \in S_i$ ir atrisinājums vienādojumam

$$f(x) \equiv 0 \pmod{p^{\alpha_i}},$$

tad ir jāatrod $\forall\ x \in \mathbb{Z}$, kas visām iespējamajām virknēm $(a_1, ..., a_l)$

apmierina sistēmu

$$\begin{cases} x \equiv a_1 \pmod{p_1^{\alpha_1}} \\ x \equiv a_2 \pmod{p_2^{\alpha_2}} \\ \dots \\ x \equiv a_l \pmod{p_l^{\alpha_l}}. \end{cases}$$

1.2. piemērs. Izmantojot ĶAT atrisināsim vienādojumu

$$x^2 \equiv 4 \pmod{30}.$$

Redzam, ka vienādojums ir ekvivalents sistēmai

$$\begin{cases} x^2 \equiv 4 \pmod 2 \\ x^2 \equiv 4 \pmod 3 \\ x^2 \equiv 4 \pmod 5. \end{cases} \Longrightarrow \begin{cases} x \equiv 0 \pmod 2 \\ x \in \{1,2\} \pmod 3 \\ x \in \{2,3\} \pmod 5 \end{cases}$$

Ir iespējams konstruēt 4 atlikumu klašu virknes:

$$(0,1,2), (0,1,3), (0,2,2), (0,2,3).$$

Katrai no šīm atlikumu klašu virknēm saskaņā ar ĶAT ir iespējams

piekārtot vienu atlikumu klasi mod 30, kas atrisina sākotnējo vienādojumu. Piemēram, virknei $(0, 1, 3)$ atbilst sistēmas

$$\begin{cases} x \equiv 0 \pmod 2 \\ x \equiv 1 \pmod 3 \\ x \equiv 3 \pmod 5 \end{cases}$$

atrisinājums $x \equiv 28 \pmod{30}$. Pārējie atrisinājumi ir $2, 8, 22 \pmod{30}$.

1.5. piezīme. Līdzīgā veidā var risināt arī modulāru vienādojumu sistēmas

$$\begin{cases} f_1(x_1, ..., x_n) \equiv 0 (\text{mod } m_1) \\ ... \\ f_l(x_1, ..., x_n) \equiv 0 (\text{mod } m_l) \end{cases}$$

1. Sadalot moduļus $m_1, ..., m_l$ pirmskaitļu pakāpju reizinājumos, iegūt sistēmu ar, iespējams, lielāku vienādojumu skaitu, kas satur $\forall$ vienādojumu mod $\forall$ pirmskaitļa pakāpe.
2. Apvienot apakšsistēmās vienādojumus ar vienu pirmskaitļa pakāpi, iegūt lokālos atrisinājumus.

3. Izmantojot ĶAT iegūt globālos atrisinājumus.

2. Kvadrātiskie vienādojumi atlikumu gredzenos ar pirmskaitļa moduli

$p = 2 \implies x^2 \equiv x (\mathrm{mod}\ p) \implies$ kvadrātvienādojumi ir ekvivalenti lineārajiem vienādojumiem.

Visur zemāk $p \in \mathbb{P}, p > 2$.

2.1. Pamatfakti

2.1. piezīme. Kvadrātisku vienādojumu

$$a_2x^2 + a_1x + a_0 \equiv 0 \ (\mathrm{mod\ p})$$

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

formā

$$y^2 \equiv a \pmod{\mathrm{p}} :$$

1. var izdalīt ar a_2 un iegūt vienādojumu

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

2. $2 \in \mathcal{U}_p \implies$

$$x^2 + rx + s \equiv x^2 + 2 \cdot \left(\frac{r}{2}\right) \cdot x + \left(\frac{r}{2}\right)^2 - \left(\frac{r}{2}\right)^2 + s \equiv$$

$$(x + \frac{r}{2})^2 - \left(\frac{r}{2}\right)^2 + s \pmod{\mathrm{p}}.$$

$y \equiv x + \frac{r}{2} \implies$ attiecībā uz y iegūsim vienādojumu

$$y^2 \equiv \left(\frac{r}{2}\right)^2 - s \pmod{\mathrm{p}}.$$

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

Tālāk mēs pētīsim tikai šādus kvadrātiskus vienādojumus.

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

2.3. piezīme. $x_0^2 \equiv a(\text{ mod } p) \implies (-x_0)^2 \equiv a(\text{mod } p)$. $x_0 \equiv -x_0(\text{mod p}) \implies p = 2$. Vairāk kā divi atrisinājumi nevar būt saskaņā ar Lagranža teorēmu $\implies$ var būt nulle vai divi atrisinājumi, ja $p > 2$.

2.2. piemērs. $x^2 \equiv 2 \pmod 7$ atrisinājumi ir $\pm 3 \pmod 7$.

2.2. Kvadrātiskie un augstāku pakāpju atlikumi

Atlikumu klasi $a \in \mathcal{U}_m$ sauksim par *kvadrātisku atlikumu*, ja vienādojumam $x^2 \equiv a (\mathrm{mod}\ m)$ ir atrisinājumi. Visu kvadrātisko atlikumu kopu mod m $\{t^2 | t \in \mathcal{U}_m\}$ apzīmēsim ar $\mathcal{Q}_m$.

Atlikumu klasi $a \in \mathcal{U}_m$ sauksim par *n-tās pakāpes atlikumu*, ja vienādojumam $x^n \equiv a (\mathrm{mod}\ m)$ ir atrisinājumi. Visu n-tās pakāpes atlikumu kopu mod m apzīmēsim ar $\mathcal{Q}_{n,m}$.

2.1. teorēma. Kopa $\mathcal{Q}_m$ apmierina šādas īpašības:

1. $1 \in \mathcal{Q}_m$.
2. $\left\{ \begin{array}{l} a \in \mathcal{Q}_m \\ b \in \mathcal{Q}_m \end{array} \right. \Longrightarrow ab \in \mathcal{Q}_m$ ($\mathcal{Q}_m$ ir slēgta attiecībā uz reizināšanu).
3. $a \in \mathcal{Q}_m \Longrightarrow a^{-1} \in \mathcal{Q}_m$ ($\mathcal{Q}_m$ ir slēgta attiecībā uz inverso elementu iekļaušanu).

PIERĀDĪJUMS

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

2. $\left\{ \begin{array}{l} x^2 \equiv a \pmod{\text{m}} \\ y^2 \equiv b \pmod{\text{m}} \end{array} \right. \Longrightarrow (xy)^2 \equiv ab \pmod{\text{m}} \Longrightarrow ab \in \mathcal{Q}_m.$

3. $x^2 \equiv a \pmod{\text{m}} \Longrightarrow (x^{-1})^2 \equiv a^{-1} \pmod{\text{m}} \Longrightarrow a^{-1} \in \mathcal{Q}_m.$

■

2.4. piezīme. Grupu teorijas terminos iepriekšējā teorēma nozīmē to, ka $\mathcal{Q}_m$ ir $\mathcal{U}_m$ apakšgrupa. Tas pats apgalvojums ir spēkā kopai $\mathcal{Q}_{n,m}$.

2.2. teorēma. $g \in \mathcal{G}_m \neq \emptyset \Longrightarrow \mathcal{Q}_m = \langle g^2 \rangle$ - $\forall\ a \in \mathcal{Q}_m \exists\ k \in \mathbb{N}$: $a \equiv (g^2)^k \pmod{\text{m}}$.

PIERĀDĪJUMS

$n = 2n_1 \Longrightarrow g^n \equiv (g^{n_1})^2 \in \mathcal{Q}_m \Longrightarrow g$ kāpināts jebkurā pāra pakāpē pieder $\mathcal{Q}_m$.

Otrādi, $a \in \mathcal{Q}_m \implies a \equiv b^2$.
$g \in \mathcal{G}_m \implies \exists\, l\colon\ b \equiv g^l (\mathrm{mod}\ m)$ un tāpēc

$$a \equiv (g^l)^2 \equiv g^{2l}\ (\mathrm{mod\ m}).\blacksquare$$

2.5. piezīme. $p > 2 \implies \varphi(p) = p - 1$ ir pāra skaitlis. $\mathcal{Q}_p$ veido ģeneratora pāra pakāpes ar kāpinātājiem kopā $\{0, ..., p-2\}$. Šādu kāpinātāju skaits ir $\frac{p-1}{2} \implies |\mathcal{Q}_p| = \frac{p-1}{2}$.

2.6. piezīme. Vēl daži secinājumi no iepriekšējās teorēmas:

1. Primitīvās saknes g nepāra pakāpes veido nekvadrātisko atlikumu kopu.
2. $\left\{ \begin{array}{l} a \in \mathcal{Q}_m \\ z \notin \mathcal{Q}_m \end{array} \right. \implies az \notin \mathcal{Q}_m.$
3. $\left\{ \begin{array}{l} t \notin \mathcal{Q}_m \\ z \notin \mathcal{Q}_m \end{array} \right. \implies tz \in \mathcal{Q}_m.$

2.3. piemērs. $p = 7,\ \mathcal{Q}_7 = \{1, 2, 4\}$.

2.3. Eilera kritērijs

2.3. teorēma. (*Eilera kritērijs*)

1. $a \in \mathcal{Q}_p \iff a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.
2. $a \notin \mathcal{Q}_p \iff a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

PIERĀDĪJUMS $\forall\ a \in \mathcal{U}_p\ e = a^{\frac{p-1}{2}}$ saskaņā ar Eilera teorēmu apmierina vienādību $e^2 \equiv 1 \pmod{p} \implies e$ ir vienādojuma

$$x^2 - 1 \equiv (x-1)(x+1) \equiv 0 \pmod{p}$$

atrisinājums $\implies e = a^{\frac{p-1}{2}} \in \{1, -1\} \pmod{p}$.

$$a \in \mathcal{Q}_p \implies a \equiv g^{2n} \pmod{p} \implies a^{\frac{p-1}{2}} \equiv (g^{p-1})^n \equiv 1 \pmod{p}.$$

$$a \notin \mathcal{Q}_p \implies a \equiv g^{2n+1} \text{ un}$$

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

jo tas nozīmētu, ka g kārta ir mazāka kā $p-1$ un tādējādi $g \notin \mathcal{G}_p$. Ir pierādīts, ka $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. ■

2.4. piemērs. $p = 7$, $\frac{p-1}{2} = 3$. 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 $1, 2, 4$.

2.4. teorēma. Skaitļi $1^2, 2^2, ..., (\frac{p-1}{2})^2$ veido $\mathcal{Q}_p$ pārstāvju kopu.

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

Pieņemsim, ka

$$\begin{cases} 1 \le u \le \frac{p-1}{2} \\ 1 \le v \le \frac{p-1}{2} \\ u \ne v. \end{cases}$$

$$\begin{cases} u \ne v \\ u + v < p \end{cases} \Longrightarrow \begin{cases} u - v \not\equiv 0 \pmod{p} \\ u + v \not\equiv 0 \pmod{p} \end{cases} \Longrightarrow$$

$$u^2 - v^2 = (u-v)(u+v) \not\equiv 0 \pmod{\text{p}} \implies u^2 \not\equiv v^2 \pmod{\text{p}}.$$

Esam pierādījuši, ka $\{1^2, ..., (\frac{p-1}{2})^2\}$ 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. ■

2.5. piemērs. $p = 7$, $\mathcal{Q}_7 = \{1, 4, 9\}$.

2.4. Ležandra simbols

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

Par *Ležandra simbolu* sauksim funkciju $\mathcal{U}_p \to \{1, -1\}$:

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} = \begin{cases} 1, & \text{ja } a \in \mathcal{Q}_p \\ -1, & \text{ja } a \notin \mathcal{Q}_p. \end{cases}$$

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

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

1. $a \equiv a' \pmod{p} \implies \left(\frac{a}{p}\right) = \left(\frac{a'}{p}\right)$ (modulārā īpašība).
2. $g \in \mathcal{G}_p \implies \left(\frac{g^k}{p}\right) = (-1)^k$.
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

1. Seko no Ležandra simbola definīcijas.

2. $a \in Q_p \iff a \equiv g^{2n} (\mathrm{mod}\ p) \implies \left(\frac{g^{2n}}{p}\right) = 1 = (-1)^{2n}$.

$a \notin Q_p \iff a \equiv g^{2n+1} (\mathrm{mod}\ p) \implies \left(\frac{g^{2n+1}}{p}\right) = (-1) = (-1)^{2n+1}$.

3. $\begin{cases} a \equiv g^k \ (\mathrm{mod\ p}) \\ b \equiv g^l \ (\mathrm{mod\ p}) \end{cases} \implies$

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

2.7. piezīme. Multiplikatīvā īpašība nozīmē to, ka pietiek zināt lielumus $\left(\frac{q}{p}\right)$, kur p un q ir pirmskaitļi.

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

2.5. Kvadrātiskās reciprocitātes teorēma un tās pielietojumi

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

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

2.7. piemērs. Noteiksim, vai eksistē atrisinājumi vienādojumam
$$x^2 \equiv 37 \pmod{73}.$$
$$\left(\frac{37}{73}\right) = \left(\frac{73}{37}\right) = \left(\frac{36}{37}\right) = \left(\frac{2}{37}\right)^2\left(\frac{3}{37}\right)^2 = 1,$$

tāpēc eksistē divi atrisinājumi.

Noteiksim, vai eksistē atrisinājumi vienādojumam

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

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

tāpēc atrisinājumi neeksistē.

3. 12.mājasdarbs

3.1. Obligātie uzdevumi

12.1 Atrisināt vienādojumus

(a) $x^3 - x - 1 \equiv 0 (\mathrm{mod}\ 125)$;
(b) $2007x^2 + 2008x + 2009 \equiv 0 (\mathrm{mod}\ 64)$;
(c) $x^4 + x^2 + x + 3 \equiv 0 (\mathrm{mod}\ 81)$.

12.2 Atrisināt vienādojumus

(a) $x^2 \equiv 19\ (\mathrm{mod}\ 30)$;
(b) $x^3 + x + 2 \equiv 0\ (\mathrm{mod}\ 36)$.

12.3 Atrisināt vienādojumu sistēmu

$$\begin{cases} 2x^2 + 3y^2 \equiv 3 (\mathrm{mod}\ 15) \\ 3x^2 - 4y^3 \equiv 2 (\mathrm{mod}\ 15). \end{cases}$$

12.4 Nosakiet, vai ir atrisināmi vienādojumi

(a) $x^2 \equiv 7\ (\mathrm{mod}\ 17)$,
(b) $x^2 \equiv 989\ (\mathrm{mod}\ 1987)$,

(c) $x^2 \equiv 2008 \pmod{2007}$,
(d) $x^2 \equiv 2007 \pmod{2008}$.

12.5 Nosakiet, vai ir atrisināmi vienādojumi

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

12.6 Nosakiet, kādiem pirmskaitļiem ir atrisināms vienādojums

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

(Norādījums - mod 12)

3.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi

12.7 Pierādiet, ka vienādojums

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

ir atrisināms katram pirmskaitlim p.