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

Studiju kurss

SKAITĻU TEORIJA

10.lekcija

Docētājs: Dr. P. Daugulis

2012./2013.studiju gads

Saturs

Lekcijas mērķis:

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

Lekcijas kopsavilkums:

- modulāros vienādojumus mod p^α var risināt pēctecīgi sākot no mazām p pakāpēm,
- vienādojumus ar saliktiem moduļiem var risināt izmantojot ĶAT,
- kvadrātiskus vienādojumus var risināt ar specifiskām metodēm.

Svarīgākie jēdzieni: modulāro sistēmu lokālie un globālie atrisinājumi, kvadrātiskie un nekvadrātiskie atlikumu, Ležandra simbols.

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

1. Modulārie vienādojumi ar saliktu moduli

1.1. Modulārie vienādojumi ar moduli p^α

Vienādojumus mod p^α var risināt ar pārskaitīšanu vai gudrāk, izmantojot zemāk aprakstīto metodi.

Vienādojumus mod p^α risināsim izmantojot šādu faktu:

$$a \equiv b(\text{mod } m) \implies a \equiv b \ (\text{mod } k), \forall \ k|m.$$

Speciālgadījumā:

$$f(x) \equiv 0(\text{mod } p^\alpha) \implies \begin{cases} f(x) \equiv 0(\text{mod } p) \\ f(x) \equiv 0(\text{mod } p^2) \\ \dots \\ f(x) \equiv 0(\text{mod } p^\alpha) \end{cases}$$

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

Algoritms

Pieņemsim, ka klase $[x]$ mod p^α ir vienādojuma $f(x) \equiv 0 (\text{mod } p^\alpha)$ atrisinājums.

Tad eksistē $[x]$ pārstāvis $\widetilde{x}$: $0 \leq \widetilde{x} \leq p^\alpha - 1$.

Izteiksim $\widetilde{x}$ p-adiskajā formā

$$\widetilde{x} = \overline{a_{\alpha-1}a_{\alpha-2}...a_1a_0}_p = a_{\alpha-1}p^{\alpha-1} + a_{\alpha-2}p^{\alpha-2} + ... + a_1p + a_0.$$

Meklēsim p-adiskos ciparus sākot no a_0.

1. $f(\widetilde{x}) \equiv 0(\text{mod } p) \implies f(a_0) \equiv 0(\text{mod } p)$, atrodam a_0.
2. $f(\widetilde{x}) \equiv 0(\text{mod } p^2) \implies f(a_1p + a_0) \equiv 0(\text{mod } p^2)$, atrodam a_1.
3. ...

1.1. piemērs. $3x^2 + x - 1 \equiv 0 \ (\text{mod } 27)$. $\widetilde{x} = \overline{a_2a_1a_0}_3$.

1. $3a_0^2 + a_0 - 1 \equiv 0 \ (\text{mod } 3) \implies a_0 \equiv 1 \ (\text{mod } 3) \implies \widetilde{x} = \overline{a_2a_11}_3$.

2. $3(a_1\cdot 3+1)^2+(a_1\cdot 3+1)-1\equiv 0 \pmod 9 \Longrightarrow a_1+1\equiv 0 \pmod 3$
$\Longrightarrow a_1\equiv 2 \pmod 3 \Longrightarrow \widetilde{x}=\overline{a_2 21}_3.$

3. $3(a_2\cdot 9+2\cdot 3+1)^2+(a_2\cdot 9+2\cdot 3+1)-1\equiv 0 \pmod{27} \Longrightarrow$
$3(a_2\cdot 9+7)^2+(a_2\cdot 9+7)-1\equiv 0 \pmod{27} \Longrightarrow$
$a_2-1\equiv 0 \pmod 3 \Longrightarrow a_2\equiv 1 \pmod 3 \Longrightarrow$
$\widetilde{x}=\overline{121}_3\equiv 16 (\mathrm{mod}\ 27).$

1.2. Modulāro sistēmu risināšana patvaļīgiem moduļiem

1.2.1. Vienādojumu sistēmas ekvivalentā sašķelšana

1. $\forall$ vienādojumam tiek piekārtota ekvivalenta sistēma pēc pirmskaitļu pakāpju moduļiem,
2. visi vienādojumu tiek apvienoti vienā *sašķeltajā sistēmā* $\widetilde{\Sigma}$.

1.2.2. Lokālie atrisinājumi

Dota modulāra vienādojumu sistēma Σ mod $m_1, ..., m_l$. Pieņemsim, ka pirmskaitļu kopa, kuras elementi dala vismaz vienu m_i ir $p_1, ..., p_l$.

1. Pārveidosim Σ ekvivalentajā sašķeltajā sistēmā $\widetilde{\Sigma}$,
2. pārkārtosim $\widetilde{\Sigma}$ formā $\Sigma_1 \wedge \Sigma_2 \wedge ... \wedge \Sigma_k$, kur Σ_i ir *lokālā apakšsistēma*, kas satur visus vienādojumus mod p_i^α, $\forall\ \alpha$.

Sistēmu Σ_i atrisinājumus sauc par *lokālajiem atrisinājumiem.*

1.2. piemērs. $x^2 \equiv 4 \pmod{30} \iff \begin{cases} x^2 \equiv 4 \pmod 2 \\ x^2 \equiv 4 \pmod 3 \\ x^2 \equiv 4 \pmod 5 \end{cases} \implies$

lokālie atrisinājumi: $\implies \begin{cases} [0] \in \mathbb{Z}/2, \\ \{[1],[2]\} \in \mathbb{Z}/3, \\ \{[2],[3]\} \in \mathbb{Z}/5. \end{cases}$

1.2.3. Globālie atrisinājumi

Katrai lokālo atrisinājumu virknei var piekārtot atrisinājumu mod m - *globālo atrisinājumu* izmantojot ĶAT.

Algoritms vienādojuma $f(x) \equiv 0(\mathbf{mod}\ m)$ risināšanai, $m = p_1^{\alpha_1} ... p_l^{\alpha_l}$**.**

1. Atrast vienādojuma $f(x) \equiv 0(\mathrm{mod}\ m)$ lokālos atrisinājumus mod $p_i^{\alpha_i}, \forall\ i$. Šī soļa rezultātā tiek iegūtas atlikumu klašu kopas

S_i, kur $S_i \subseteq \mathbb{Z}/p_i^{\alpha_i}$.

2. Rekonstruēt atrisinājumus mod m (*globālos*) atrisinājumus no lokālajiem atrisinājumiem (mod $p_i^{\alpha_i}$) izmantojot ĶAT: $\forall$ lokālo atrisinājumu virknei $(a_1, ..., a_l) \in S_1 \times S_2 \times ... \times S_l$ piekārtot atbilstošo globālo atlikumu klasi x mod m:

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

$\forall$ lokālo atrisinājumu virknei atbilst viens globālais atrisinājums, tie ir jāapvieno vienā atrisinājumu kopā.

1.3. piemērs. $x^2 \equiv 4 \pmod{30}$. No lokālajiem atrisinājumiem ir iespējams konstruēt 4 atlikumu klašu virknes:

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

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 $2, 8, 22 \pmod{30}$.

1.1. 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. Sašķeļam katru vienādojumu mod m_i ekvivalentā sašķeltajā sistēmā $\widetilde{\Sigma}_i$.
2. Apvienojam visus vienādojumus vienā sistēmā $\widetilde{\Sigma}$.
3. Sadalām $\widetilde{\Sigma}$ apakšsistēmās Σ_i, kas atbilst katra pirmskaitļa p_i pakāpēm.
4. Atrodam lokālos atrisinājumus - atlikumu virknes.

5. Iegūstam globālos atrisinājumus izmantojot ĶAT.

2. Kvadrātiskie modulārie vienādojumi

2.1. Kvadrātvienādojumi mod p

$p = 2 \Longrightarrow x^2 \equiv x (\mathrm{mod}\ p) \Longrightarrow$ kvadrātvienādojumi ir ekvivalenti lineārajiem vienādojumiem. Visur zemāk $p \in \mathbb{P}, p > 2$.

2.1.1. Pamatfakti

Pilnā kvadrāta atdalīšana

Kvadrātisku vienādojumu

$$\boldsymbol{a_2 x^2 + a_1 x + a_0 \equiv 0} (\mathrm{mod}\ \boldsymbol{p})$$

var reducēt uz vienādojumu formā

$$\boldsymbol{y^2 \equiv a (\mathrm{mod}\ p)}:$$

1. var izdalīt ar a_2 un iegūt vienādojumu

$$x^2 + rx + s \equiv 0 (\mathrm{mod}\ p),$$

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

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

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

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

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

$$x^2 + x + 1 \equiv x^2 + 2 \cdot \frac{1}{2} \cdot x + 1 \equiv x^2 + 2 \cdot 3 \cdot x + 1 \equiv$$

$$x^2 + 2 \cdot 3 \cdot x + (3)^2 - (3)^2 + 1 \equiv (\underbrace{x+3}_{=y})^2 + 2 \equiv 0 \pmod 5.$$

Tālāk mēs pētīsim tikai šādus kvadrātiskus vienādojumus.

Atrisinājumu skaits

- Vienādojumam $x^2 \equiv a(\text{mod p})$ atrisinājumu kopa var būt tukša.
- $x_0^2 \equiv a(\text{ mod } p) \implies (-x_0)^2 \equiv a(\text{mod } p)$.
  $p \neq 2 \implies x_0 \not\equiv -x_0(\text{mod } p)$.
- Vairāk kā divi atrisinājumi nevar būt saskaņā ar Lagranža teorēmu $\implies$ var būt nulle vai divi atrisinājumi, ja $p > 2$.

2.2. piemērs. $x^2 \equiv 2 \pmod 5$ - $\varnothing$ (jo 2 ir primitīva sakne).
$x^2 \equiv 2 \pmod 7$ atrisinājumi ir $\pm 3 \pmod 7$.

2.1.2. Kvadrātiskie atlikumi

$a \in \mathcal{U}_m$ - *kvadrātisks atlikums*, ja vienādojumam

$$x^2 \equiv a (\mathrm{mod}\ m)$$

ir atrisinājumi. Visu kvadrātisko atlikumu kopu mod m $\{t^2 \big| t \in \mathcal{U}_m\}$ apzīmēsim ar $\mathcal{Q}_m$.

2.1. teorēma. $g \in \mathcal{G}_m \neq \varnothing \implies$

1. $\mathcal{Q}_m = \langle g^2 \rangle$.
2. $|\mathcal{Q}_m| = \dfrac{\varphi(m)}{2}$.

PIERĀDĪJUMS

1. $n = 2n_1 \implies g^n \equiv (g^{n_1})^2 \in \mathcal{Q}_m$.

Otrādi, $a \in \mathcal{Q}_m \implies a \equiv b^2$.

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

2. $\varphi(m)$ ir pāra skaitlis. $\mathcal{Q}_m$ veido ģeneratora pāra pakāpes ar kāpinātājiem kopā $\{0, 2, ..., \varphi(m) - 2\}$. Šādu kāpinātāju skaits ir $\frac{\varphi(m)}{2} \Longrightarrow |\mathcal{Q}_m| = \frac{\varphi(m)}{2}$. ■

2.1. piezīme. Seko, ka primitīvās saknes g nepāra pakāpes veido nekvadrātisko atlikumu kopu.

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

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

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

Pieņemsim, ka

$$\begin{cases} 1 \leq u \leq \dfrac{p-1}{2} \\ 1 \leq v \leq \dfrac{p-1}{2} \\ u \neq v. \end{cases}$$

$$\begin{cases} u \neq v \\ u+v < p \end{cases} \Longrightarrow \begin{cases} u - v \not\equiv 0 (\text{mod } p) \\ u + v \not\equiv 0 (\text{mod } p) \end{cases} \Longrightarrow$$

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

Esam pierādījuši, ka $\{1^2, ..., \left(\dfrac{p-1}{2}\right)^2\}$ elementi pārstāv kvadrātiskus atlikumus un tie ir dažādi mod p.

Bet kvadrātisko atlikumu skaits ir vienāds ar $\dfrac{p-1}{2} \Longrightarrow$ šie skaitļi $\{1^2, ..., \left(\dfrac{p-1}{2}\right)^2\}$ pārstāv visus kvadrātiskos atlikumus. ■

2.1.3. Eilera kritērijs

2.3. teorēma. (*Eilera kritērijs*)

1. $a \in \mathcal{Q}_p \iff a^{\frac{p-1}{2}} \equiv 1 (\mathrm{mod}\ p)$.
2. $a \notin \mathcal{Q}_p \iff a^{\frac{p-1}{2}} \equiv -1 (\mathrm{mod}\ p)$.

PIERĀDĪJUMS $\forall\ a \in \mathcal{U}_p\ e = a^{\frac{p-1}{2}}$ saskaņā ar Eilera teorēmu apmierina vienādību $e^2 \equiv 1 (\mathrm{mod}\ p) \implies e \in \{1, -1\} (\mathrm{mod}\ p)$.

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

$a \notin \mathcal{Q}_p \implies a \equiv g^{2n+1} \implies a^{\frac{p-1}{2}} \equiv g^{(2n+1)\frac{p-1}{2}} \equiv g^{(p-1)n} g^{\frac{p-1}{2}} \equiv g^{\frac{p-1}{2}} \not\equiv 1 (\mathrm{mod}\ p)$, jo tas nozīmētu, ka $P(g) < p-1$ un tādējādi $g \notin \mathcal{G}_p$. Ir pierādīts, ka $a^{\frac{p-1}{2}} \equiv -1 (\mathrm{mod}\ p)$. ■

2.4. piemērs. $p = 7, \dfrac{p-1}{2} = 3.\ 1^3 \equiv 1, 2^3 \equiv 1, 3^3 \equiv -1, 4^3 \equiv 1, 5^3 \equiv -1, 6^3 \equiv -1\ (\mathrm{mod}\ 7). \implies \mathcal{Q}_7 = \{1, 2, 4\}$.

2.1.4. 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.

Ležandra simbols - funkcija $\mathcal{U}_p \to \{1,-1\}$:

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

2.4. teorēma. $p \in \mathbb{P}$.

1. $a \equiv a' (\mathrm{mod}\ p) \implies \left(\frac{a}{p}\right) = \left(\frac{a'}{p}\right)$ (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).

PIERĀDĪJUMS

1. Seko no Ležandra simbola definīcijas.

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

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

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

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

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

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

2.1.5. Kvadrātiskās reciprocitātes teorēma un tās pielietojumi

2.5. teorēma. (*Ležandra simbola argumentu simetrijas - kvadrātiskās reciprocitātes teorēma*) p un q - nepāra pirmskaitļi.

1. $\Big(p \not\equiv 3 \pmod 4 \text{ vai } q \not\equiv 3 \pmod 4\Big) \implies \left(\frac{q}{p}\right) = \left(\frac{p}{q}\right).$

2. $\Big(p \equiv q \equiv 3 \pmod 4\Big) \implies \left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right).$

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

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

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

tāpēc eksistē divi atrisinājumi.

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

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

tāpēc atrisinājumi neeksistē.

2.2. Salikti moduļi

2.6. teorēma.

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_l^{\alpha_l} \implies \left(a \in \mathcal{Q}_m \iff a \in \mathcal{Q}_{p_i^{\alpha_i}}, \forall i.\right)$$

PIERĀDĪJUMS

$a \in \mathcal{Q}_m \implies \exists\, x \in \mathbb{Z} : x^2 \equiv a (\mathrm{mod}\ m) \implies x^2 \equiv a (\mathrm{mod}\ p_i^{\alpha_i}), \forall i.$

Papildus tam $a \in \mathcal{U}_m \implies a \in \mathcal{U}_{m_i}$.

Otrā virzienā - $a \in \mathcal{Q}_{p_i^{\alpha_i}}, \forall\, i \implies \forall\, i\ \exists\, x_i \in \mathbb{Z} : x_i^2 \equiv a (\mathrm{mod}\ p_i^{\alpha_i})$.

Saskaņā ar ĶAT sistēmai

$$\begin{cases} x \equiv x_1 (\mathrm{mod}\ p_1^{\alpha_1}) \\ \ldots \\ x \equiv x_l (\mathrm{mod}\ p_l^{\alpha_l}) \end{cases}$$

eksistē atrisinājumu klase x mod m.

Seko, ka x apmierina sistēmu

$$\begin{cases} x^2 \equiv a (\mathrm{mod}\ p_1^{\alpha_1}) \\ \ldots \\ x^2 \equiv a (\mathrm{mod}\ p_l^{\alpha_l}) \end{cases} \iff x^2 \equiv a (\mathrm{mod}\ m). \blacksquare$$

2.7. piemērs. Atradīsim $\mathcal{Q}_{72}$. $72 = 2^3 3^2 \implies a \in \mathcal{Q}_{72}. \iff$
$\begin{cases} a \equiv 1 (\mathrm{mod}\ 3) \\ a \equiv 1 (\mathrm{mod}\ 8) \end{cases} \iff a \equiv 1 (\mathrm{mod}\ 24) \implies \mathcal{Q}_{72} = \{1, 25, 49\}.$

3. 10.mājasdarbs

3.1. Obligātie uzdevumi

10.1 Atrisināt vienādojumus

(a) $x^3 - x - 1 \equiv 0 (\mathrm{mod}\ 125)$;
(b) $2011x^2 + 2012x + 2013 \equiv 0 (\mathrm{mod}\ 64)$;
(c) $x^4 + x^2 + x + 3 \equiv 0 (\mathrm{mod}\ 81)$.

10.2 Atrisināt vienādojumus

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

10.3 Atrisināt vienādojumu sistēmu

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

10.4 Atrast

(a) $\mathcal{Q}_{17}$,
(b) Q_{27},

(c) Q_{168}.

10.5 Nosakiet, vai ir atrisināmi vienādojumi

(a) $x^2 \equiv 989 \pmod{1987}$,
(b) $x^2 \equiv 2012 \pmod{2011}$,
(c) $x^2 \equiv 2011 \pmod{2012}$.

10.6 Nosakiet, vai ir atrisināms vienādojums $x^4 \equiv 5 \pmod{13}$.

3.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi

10.7 Nosakiet, kādiem pirmskaitļiem p ir atrisināms vienādojums

$$x^2 \equiv 3 (\mathrm{mod}\ p).$$

10.8 Pierādiet, ka vienādojums

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

ir atrisināms katram pirmskaitlim p.

10.9 Pierādīt, ka $a \in \mathcal{Q}_{2^\alpha}$, $\alpha \geq 3 \iff a \equiv 1 (\mathrm{mod}\ 8)$.