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

Studiju kurss

Veselo skaitļu teorija

11.lekcija

Docētājs: Dr. P. Daugulis

2008./2009.studiju gads

Saturs

1. Vienādojumu risināšana atlikumu gredzenos ar saliktu moduli

1.1. Vienādojumi atlikumu gredzenos ar pirmskaitļa pakāpes moduli

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

$$a \equiv b \pmod{\mathrm{m}} \wedge k|m \implies a \equiv b \pmod{k}.$$

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

1.2. piezīme. No iepriekšējās piezīmes seko 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 $x = s + px'$ 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

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

šim vienādojumam ir viens atrisinājums $x \equiv 1 \pmod{3}$.

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

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

Iegūsim vienādojumu $3x' + 3 \equiv 0 \pmod{9}$. Izdalīsim visu ar 3, iegūsim vienādojumu $x' + 1 \equiv 0 \pmod{3}$, kura atrisinājums ir $x' \equiv 2 \pmod{3}$. 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, iegūsim vienādojumu $x'' + 2 \equiv 0 \pmod{3}$, kura atrisinājums ir $x'' \equiv 1 \pmod{3}$.

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

1.2. Risināšanas vispārīgā shēma gadījumā ar saliktu moduli

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

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

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

Ja skaitlis a apmierina sistēmu $\implies m_i | f(a), \forall\, i \implies m | f(a) \iff f(a) \equiv 0 (\text{mod } m)$.

$f(b) \equiv 0 \pmod{\text{m}} \implies f(b) \equiv 0 \pmod{m_i}$ katram i, jo $m_i | m$, tātad b apmierina arī visu sistēmu. ■

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

1.4. piezīme. Iepriekšējā teorēma vedina uz šādu algoritmu vienādojuma $f(x) \equiv 0 \pmod{m}$ risināšanai ar saliktu moduli $m = p_1^{\alpha_1} ... p_l^{\alpha_l}$:

1. Atrisināt vienādojumu $f(x) \equiv 0$ pēc katras pirmskaitļa pakāpes $p_i^{\alpha_i}$. Šī soļa rezultātā tiek iegūtas atlikumu klašu kopas S_i, kur $S_i \subseteq \mathbb{Z}/p_i^{\alpha_i}\mathbb{Z}$ (*lokālie atrisinājumi*).
2. Mēģināt rekonstruēt sākotnējā vienādojuma globālos atrisinājumus no lokālajiem atrisinājumiem (mod $p_i^{\alpha_i}$): katram kopu tiešā reizinājuma $S_1 \times S_2 \times ... \times S_l$ elementam (virknei $(a_1, ..., a_l)$) mēģināt piekārtot atlikumu klases pēc moduļa m. Citiem vārdiem sakot, ja $a_i \in S_i$ ir atrisinājums vienādojumam

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

tad ir jāatrod visi veselie skaitļi x, kas visām iespējamajām

virknēm $(a_1, ..., a_l)$ apmierina sistēmu

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

1.3. Ķīniešu atlikumu teorēma un tās pastiprinājumi

1.3.1. Klasiskā divu vienādojumu teorēma

1.2. teorēma. (*Ķīniešu atlikumu teorēma - klasiskais variants*, 3.gs. AD) Ja $LKD(m_1, m_2) = 1$, tad vienādojumu sistēmai

$$\begin{cases} x \equiv a \pmod{m_1} \\ x \equiv b \pmod{m_2} \end{cases}$$

ir tieši viens atrisinājums pēc moduļa $m_1 m_2$.

PIERĀDĪJUMS Tā kā $LKD(m_1, m_2) = 1$, tad 1 un līdz ar to arī $a - b = (a - b) \cdot 1$ var tikt izteikts kā m_1 un m_2 lineāra kombinācija: eksistē veseli skaitļi u_1 un u_2 tādi, ka

$$a - b = u_1 m_1 + u_2 m_2.$$

Pārnesot dažus locekļus uz pretējāmu pusēm definēsim

$$\tilde{x} = a - u_1 m_1 = b + u_2 m_2.$$

Redzam, ka $\tilde{x}$ apmierina doto sistēmu, tātad tā klase mod $m_1 m_2$ arī apmierina sistēmu.

Pieņemsim, ka divi skaitļi $\tilde{x_1}$ un $\tilde{x_2}$ apmierina sistēmu, tad

$$\tilde{x_1} - \tilde{x_2} = m_1 q_1 = m_2 q_2,$$

kur $m_2 | q_1$ un $m_1 | q_2$, tātad $\tilde{x_1} - \tilde{x_2} \equiv 0 \pmod{m_1 m_2}$. Ir pierādīts, ka atrisinājumi veido vienu klasi mod $m_1 m_2$. ■

1.5. piezīme. Ķīniešu atlikumu teorēmas cits formulējums: sistēma

$$\begin{cases} x \equiv a \pmod{m_1} \\ x \equiv b \pmod{m_2} \end{cases}$$

ir ekvivalenta vienam vienādojumam

$$x \equiv c \pmod{m_1 m_2}.$$

1.2. piemērs. Atrisināsim sistēmu

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

Redzam, ka $3 - 2 = 1 = 2 \cdot 3 - 1 \cdot 5$, tātad

$$x \equiv 3 + 1 \cdot 5 = 2 + 2 \cdot 3 = 8 \pmod{15}.$$

1.3.2. Vairāku vienādojumu teorēma

1.3. teorēma. (*Ķīniešu atlikumu teorēma - modernais variants*) Ja $LKD(m_i, m_j) = 1$ visiem pāriem i, j, tad vienādojumu sistēmai

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \ldots \\ x \equiv a_s \pmod{m_s} \end{cases}$$

ir tieši viens atrisinājums pēc moduļa $m_1 m_2 \ldots m_s$.

PIERĀDĪJUMS Ir vairāki pierādījuma veidi.

Pierādījums izmantojot matemātisko indukciju ar parametru s.

Indukcijas bāze Ja $s = 2$, tad ir pierādīts - klasiskā ķīniešu teorēma.

Indukcijas solis Pieņemsim, ka apgalvojums ir spēkā, ja $s = n$ un pierādīsim, ka apgalvojums ir spēkā ar $s = n + 1$. Apskatīsim sistēmu

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \dots \\ x \equiv a_n \pmod{m_n} \\ x \equiv a_{n+1} \pmod{m_{n+1}} \end{cases}$$

Sistēma, kas satur pirmos n vienādojumus, saskaņā ar indukcijas pieņēmumu ir ekvivalenta vienam vienādojumam

$$x \equiv c \pmod{m_1 \dots m_n}.$$

Tātad visa sistēma ir ekvivalenta divu vienādojumu sistēmai

$$\begin{cases} x \equiv c \pmod{m_1 ... m_n} \\ x \equiv a_{n+1} \pmod{m_{n+1}}, \end{cases}$$

kas apmierina divu vienādojumu sistēmas ķīniešu atlikumu teorēmas nosacījumus:

$$LKD(m_1 ... m_n, m_{n+1}) = 1.$$

Tādējādi saskaņā ar klasisko ķīniešu atlikumu teorēmu $n+1$ vienādojumu sistēmai eksistē viens atrisinājums mod $m_1 ... m_{n+1}$.

Pierādījums izmantojot Eilera teorēmu.

Apzīmēsim $m_1 ... m_s$ ar M. Apskatīsim veselu skaitli

$$C = a_1 \left(\frac{M}{m_1}\right)^{\varphi(M)} + a_2 \left(\frac{M}{m_2}\right)^{\varphi(M)} + ... + a_s \left(\frac{M}{m_s}\right)^{\varphi(M)} = \sum_{i=1}^{s} a_i \left(\frac{M}{m_i}\right)^{\varphi(M)}.$$

Redzam, ka C apmierina sistēmu, jo

$$a_i\left(\frac{M}{m_i}\right)^{\varphi(M)} \equiv \begin{cases} a_i \pmod{\text{i}}, \\ 0 \pmod{\text{j}}, \end{cases}$$

kur $i \neq j$. Vienīgums (mod M) tiek pierādīts tāpat kā klasiskajā gadījumā. Kāpinātāju $\varphi(M)$ var aizvietot ar $MKD(\varphi(m_1), ..., \varphi(m_s))$.

Pierādījums izmantojot elementu invertējamību.

Katram i definēsim t_i šādi:

$$\frac{M}{m_i} \cdot t_i \equiv 1 \pmod{m_i}.$$

Tas ir iespējams, jo visi skaitļi m_j, $i \neq j$ ir invertējami mod m_i. Apskatīsim veselu skaitli

$$D = a_1\left(\frac{M}{m_1}\right) \cdot t_1 + a_2\left(\frac{M}{m_2}\right) \cdot t_2 + ... + a_s\left(\frac{M}{m_s}\right) \cdot t_s = \sum_{i=1}^{s} a_i\left(\frac{M}{m_i}\right) \cdot t_i.$$

Redzam, ka D apmierina sistēmu, jo

$$a_i\left(\frac{M}{m_i}\right)\cdot t_i \equiv \begin{cases} a_i \pmod{\text{i}}, \\ 0 \pmod{\text{j}}, \end{cases}$$

kur $i \neq j$. Vienīgums (mod M) tiek pierādīts tāpat kā klasiskajā gadījumā. ■

1.6. piezīme. Iepriekšējās teorēmas cits formulējums: sistēma

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \ldots \\ x \equiv a_s \pmod{m_s} \end{cases}$$

ir ekvivalenta vienam vienādojumam

$$x \equiv c \pmod{m_1 m_2 \ldots m_s}.$$

1.3. piemērs. Atrisināsim sistēmu

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 5 \pmod 7 \end{cases}$$

ar trīs paņēmieniem, kas atbilst trīs dotajiem pierādījumiem.

Matemātiskās indukcijas paņēmiens. Zinām, ka pirmo divu vienādojumu atrisinājums ir $x \equiv 8 \pmod{15}$, tāpēc sistēma ir ekvivalenta divu vienādojumu sistēmai

$$\begin{cases} x \equiv 8 \pmod{15} \\ x \equiv 5 \pmod 7. \end{cases}$$

Redzam, ka $8 - 5 = 3 = 3 \cdot 15 - 6 \cdot 7$, tāpēc

$$x \equiv 8 - 3 \cdot 15 = 5 - 6 \cdot 7 = -37 \equiv 68 \pmod{105}.$$

Eilera teorēmas paņēmiens. Redzam, ka $M = 105$, $\varphi(M) = 48$, $MKD(\varphi(3), \varphi(5), \varphi(7)) = 12$. Atrodam C:

$$C = 2 \cdot (5 \cdot 7)^{12} + 3 \cdot (3 \cdot 7)^{12} + 5 \cdot (3 \cdot 5)^{12} \equiv$$
$$35 + 63 + 75 \equiv 68 \pmod{105}.$$

Invertējamo elementu paņēmiens. Redzam, ka

$$t_1 = 35^{-1} \equiv 2^{-1} \equiv 2 \pmod 3,$$
$$t_2 = 21^{-1} \equiv 1^{-1} \equiv 1 \pmod 5,$$
$$t_3 = 15^{-1} \equiv 1^{-1} \equiv 1 \pmod 7.$$

Tādējādi

$$D = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 5 \cdot 15 \cdot 1 = 278 \equiv 68 \pmod{105}.$$

1.4. piemērs. Izmantojot ķīniešu atlikumu teorēmu atrisināsim vienādojumu

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

Redzam, ka vienādojums ir ekvivalents sistēmai

$$\begin{cases} x^2 \equiv 4 \pmod{2} \\ x^2 \equiv 4 \pmod{3} \\ x^2 \equiv 4 \pmod{5}. \end{cases}$$

Pirmā vienādojuma atrisinājums ir $0 \pmod{2}$, otrā vienādojuma atrisinājumu kopa ir $\{1, 2\} \pmod{3}$, trešā vienādojuma atrisinājumu kopa ir $\{2, 3\} \pmod{5}$. 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 ķīniešu atlikumu teorēmu ir iespējams piekārtot vienu atlikumu klasi mod 30, kas atrisi-

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

1.3.3. Pastiprinātā divu vienādojumu teorēma

1.7. piezīme. Ja ir dota sistēma

$$\begin{cases} x \equiv a \pmod{m_1} \\ x \equiv b \pmod{m_2}, \end{cases}$$

kurai $LKD(m_1, m_2) = d > 1$, tad viens acīmredzams šķērslis atrisinājumu eksistencei ir šāds: ja $a \not\equiv b \pmod{\text{d}}$, tad reducējot abus

vienādojumus mod d, iegūsim pretrunu. Izrādās, ka tas ir vienīgais šķērslis.

1.4. teorēma. (*divu vienādojumu pastiprinātā ķīniešu atlikumu teorēma, 7.gs. AD*) Apzīmēsim $LKD(m_1, m_2)$ ar d.

1. $a \not\equiv b \pmod{d} \implies$ sistēmai

$$\begin{cases} x \equiv a \pmod{m_1} \\ x \equiv b \pmod{m_2} \end{cases}$$

nav atrisinājumu.

2. $a \equiv b \pmod{d} \implies$ sistēmai ir tieši viens atrisinājums mod $MKD(m_1, m_2)$.

PIERĀDĪJUMS

1. $d|m_1 \wedge d|m_2 \implies x$ apmierina arī sistēmu

$$\begin{cases} x \equiv a \pmod{d} \\ x \equiv b \pmod{d}, \end{cases}$$

no kuras seko, ka $a \equiv b \pmod{d}$.

2. Tā kā $LKD(m_1, m_2) = d$ un $d|a-b$, tad $a-b = q \cdot d$ var tikt izteikts kā m_1 un m_2 lineāra kombinācija: eksistē veseli skaitļi u_1 un u_2 tādi, ka

$$a - b = u_1 m_1 + u_2 m_2.$$

Definēsim $\tilde{x} = a - u_1 m_1 = b + u_2 m_2$. Redzam, ka $\tilde{x}$ apmierina doto sistēmu, tātad tā klase mod $MKD(m_1 m_2)$ arī apmierina sistēmu.

Pieņemsim, ka divi skaitļi $\tilde{x_1}$ un $\tilde{x_2}$ apmierina sistēmu. Pieņemsim, ka $m_1 = m_1' d$ un $m_2 = m_2' d$, kur $LKD(m_1', m_2') = 1$. Atcerēsimies arī, ka $MKD(m_1, m_1) = \frac{m_1 m_2}{d}$.

Redzam, ka

$$\tilde{x_1} - \tilde{x_2} = m_1 q_1 = m_1' d q_1 = m_2 q_2 = m_2' d q_2.$$

Izdalot abas puses ar d, iegūsim vienādību

$$m_1' q_1 = m_2' q_2.$$

Seko, ka $m_2' | q_1$ un $m_1' | q_2$, tātad

$$\tilde{x_1} - \tilde{x_2} = m_1' d m_2' q' \equiv 0 \pmod{MKD(m_1, m_2)}.$$

Ir pierādīts, ka atrisinājumi veido vienu klasi mod $m_1 m_2$. ■

1.8. piezīme. Iepriekšējās teorēmas cits formulējums: ja $a \equiv b \pmod{\text{d}}$, tad sistēma

$$\begin{cases} x \equiv a \pmod{m_1} \\ x \equiv b \pmod{m_2} \end{cases}$$

ir ekvivalenta vienam vienādojumam

$$x \equiv c \pmod{MKD(m_1, m_2)}.$$

1.5. piemērs. Atrisināsim sistēmu

$$\begin{cases} x \equiv 2 \pmod{6} \\ x \equiv 4 \pmod{20}. \end{cases}$$

Redzam, ka $LKD(6,20) = 2$ un $2 \equiv 4 \pmod 2$, tātad sistēmai ir atrisinājumi. Redzam, ka $4 - 2 = 2 = 1 \cdot 20 - 3 \cdot 6$, tātad

$$x \equiv 4 - 1 \cdot 20 = 2 - 3 \cdot 6 = -16 \equiv 44 \pmod{60}.$$

1.3.4. Pastiprinātā vairāku vienādojumu teorēma

1.5. teorēma. Apzīmēsim $LKD(m_i, m_j)$ ar d_{ij}.

1. Ja $a_i \not\equiv a_j \pmod{d_{ij}}$ vismaz vienam pārim i, j, tad sistēmai

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \dots \\ x \equiv a_s \pmod{m_s} \end{cases}$$

nav atrisinājumu.

2. Ja $a_i \equiv a_j \pmod{d_{ij}}$ visiem pāriem i, j, tad vienādojumu sistēmai

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \ldots \\ x \equiv a_s \pmod{m_s} \end{cases}$$

ir tieši viens atrisinājums pēc moduļa $MKD(m_1, m_2, ..., m_s)$.

PIERĀDĪJUMS

1. Tā kā $d_{ij}|m_i$ un $d_{ij}|m_j$, tad x apmierina arī sistēmu

$$\begin{cases} x \equiv a_i \pmod{d_{ij}} \\ x \equiv a_j \pmod{d_{ij}}, \end{cases}$$

no kuras seko, ka $a_i \equiv a_j \pmod{d_{ij}}$.

2. Pierādīsim šo apgalvojumu izmantojot matemātisko indukciju ar parametru s.

Indukcijas bāze Ja $s = 2$, tad tas ir pierādīts iepriekšējā teorēmā.

Indukcijas solis Pieņemsim, ka apgalvojums ir spēkā, ja $s = n$ un pierādīsim, ka apgalvojums ir spēkā ar $s = n+1$. Apskatīsim sistēmu

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \dots \\ x \equiv a_n \pmod{m_n} \\ x \equiv a_{n+1} \pmod{m_{n+1}} \end{cases}$$

Sistēma, kas satur pirmos n vienādojumus, saskaņā ar indukcijas pieņēmumu ir ekvivalenta vienam vienādojumam

$$x \equiv c \pmod{MKD(m_1, ..., m_n)}.$$

Tātad visa sistēma ir ekvivalenta divu vienādojumu sistēmai

$$\begin{cases} x \equiv c \pmod{MKD(m_1, ..., m_n)} \\ x \equiv a_{n+1} \pmod{m_{n+1}}, \end{cases}$$

kas apmierina divu vienādojumu sistēmas pastiprinātās ķīniešu atlikumu teorēmas nosacījumus. Tādējādi $n+1$ vienādojumu sistēmai eksistē viens atrisinājums mod $MKD(m_1, ..., m_{s+1})$. ■

1.9. piezīme. Iepriekšējās teorēmas cits formulējums: ja izpildās visi nosacījumi $a_i \equiv a_j \pmod{d_{ij}}$, tad sistēma

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ ... \\ x \equiv a_s \pmod{m_s} \end{cases}$$

ir ekvivalenta vienam vienādojumam

$$x \equiv c \pmod{MKD(m_1 m_2 ... m_s)}.$$

1.6. piemērs. Atrisināsim sistēmu

$$\begin{cases} x \equiv 4 \pmod 6 \\ x \equiv 2 \pmod{10} \\ x \equiv 7 \pmod{105}. \end{cases}$$

No sākuma atrisināsim sistēmu, kas satur pirmos divus vienādojumus:

$$\begin{cases} x \equiv 4 \pmod 6 \\ x \equiv 2 \pmod{10}. \end{cases}$$

Redzam, ka atrisinājumi eksistē. $4 - 2 = 2 = 2 \cdot 6 - 1 \cdot 10$, tātad atrisinājums ir klase

$$x \equiv 4 - 2 \cdot 6 = -8 \equiv 22 \pmod{30}.$$

Iegūsim mazāku sistēmu

$$\begin{cases} x \equiv 22 \pmod{30} \\ x \equiv 7 \pmod{105}. \end{cases}$$

Redzam, ka $LKD(30, 105) = 15$ un $22 \equiv 7 \pmod{15}$, tātad atrisinājumi

eksistē. Ievērosim, ka $MKD(30, 105) = 210$. $22 - 7 = 15 = (-3) \cdot 30 + 1 \cdot 105$, tāpēc

$$x \equiv 22 + 3 \cdot 30 = 112 \pmod{210}.$$

2. 11.mājasdarbs

11.1 Atrisiniet vienādojumus

(a) $x^3 - x - 1 \equiv 0 (\text{mod } 125)$;

(b) $2007x^2 + 2008x + 2009 \equiv 0 (\text{mod } 64)$;

(c) $x^4 + x^2 + x + 3 \equiv 0 (\text{mod } 81)$.

11.2 Atrisiniet vienādojumu sistēmas

(a)

$$\begin{cases} x \equiv 4 \ (\text{mod } 7) \\ x \equiv 5 \ (\text{mod } 11) \end{cases}$$

(b)

$$\begin{cases} x \equiv 3 \ (\text{mod } 8) \\ x \equiv 2 \ (\text{mod } 9) \end{cases}$$

(c)

$$\begin{cases} x \equiv 10 \ (\text{mod } 12) \\ x \equiv 16 \ (\text{mod } 18) \end{cases}$$

11.3 Atrisiniet vienādojumu sistēmas

(a)

$$\begin{cases} x \equiv 2 \pmod 5 \\ x \equiv 3 \pmod 7 \\ x \equiv 4 \pmod{11} \end{cases}$$

(b)

$$\begin{cases} x \equiv 1 \pmod 8 \\ x \equiv 9 \pmod{20} \\ x \equiv 4 \pmod{15} \end{cases}$$

11.4 Izmantojot ķīniešu atlikumu teorēmu atrisiniet vienādojumus

(a) $x^2 \equiv 19 \pmod{30}$;

(b) $x^3 + x + 2 \equiv 0 \pmod{36}$.

11.5 Studentiem ir trīs dažādi studiju kursi - A,B un C. Semestra pirmajā nedēļā pirmdien notiek nodarbība kursā A, otrdien - kursā B, trešdien - kursā C. Starp divām kursa A nodarbībām ir divas brīvas dienas, starp divām kursa B nodarbībām ir trīs brīvas dienas, starp divām kursa C nodarbībām ir četras brīvas

dienas (nodarbības notiek bez brīvdienām). Nodarbības tiek atceltas, ja vienā dienā iekrīt visas trīs nodarbības. Kad pirmo reizi tiks atceltas nodarbības?