DAUGAVPILS UNIVERSITĀTE
Dabaszinātņu un matemātikas fakultāte
Matemātikas katedra

Studiju kurss

Veselo skaitļu teorija

5.lekcija

Docētājs: Dr. P. Daugulis

2009./2010.studiju gads

Saturs

Lekcijas mērķis:

- apgūt "ķīniešu atlikumu teorēmu" un tās vispārinājumus,
- apgūt atlikumu gredzenu algebrisko īpašību pamatfaktus.

Lekcijas kopsavilkums:

- ir iespējams atrisināt vienkāršas vienādojumu sistēmas atlikumu klasēs.

Svarīgākie jēdzieni:

Svarīgākie fakti un metodes: klasiskā ķīniešu atlikumu teorēma (ĶAT), ĶAT ar vairākiem vienādojumiem, pastiprinātās ĶAT.

1. Ķīniešu atlikumu teorēma un tās pastiprinājumi

1.1. Klasiskās teorēmas

1.1.1. Divu vienādojumu teorēma

1.1. teorēma. (*Ķīniešu atlikumu teorēma (ĶAT)- klasiskais variants*) $LKD(m_1, m_2) = 1 \implies \forall\, a, b \in \mathbb{Z}\ \exists$ tieši viena klase $c (\mathrm{mod}\ m_1 m_2)$:

$$\begin{cases} x \equiv a\ (\mathrm{mod}\ m_1) \\ x \equiv b\ (\mathrm{mod}\ m_2) \end{cases} \iff x \equiv c\ (\mathrm{mod}\ m_1 m_2)$$

PIERĀDĪJUMS $LKD(m_1, m_2) = 1 \implies a - b = (a - b) \cdot 1$ var tikt izteikts kā m_1 un m_2 lineāra kombinācija: $\exists\, u_1, u_2 \in \mathbb{Z}$:

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

Pārnesot dažus locekļus uz pretējām 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

$$\begin{cases} \tilde{x_1} - \tilde{x_2} = m_1 q_1 \\ \tilde{x_1} - \tilde{x_2} = m_2 q_2 \end{cases} \Longrightarrow m_1 q_1 = m_2 q_2.$$

$$\begin{cases} m_1 | m_2 q_2 \\ LKD(m_1, m_2) = 1 \end{cases} \Longrightarrow m_1 | q_2 \Longrightarrow \tilde{x_1} - \tilde{x_2} = m_1 m_2 q'$$

$\Longrightarrow \tilde{x_1} - \tilde{x_2} \equiv 0 \pmod{m_1 m_2}$ Ir pierādīts, ka atrisinājumi veido vienu klasi mod $m_1 m_2$. ■

1.1. 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

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

1.1.2. Vairāku vienādojumu teorēma

1.2. teorēma. $LKD(m_i, m_j) = 1, \forall\ i, j \implies \forall\ a_1, ..., a_s \in \mathbb{Z}\ \exists$ tieši viena klase $c \pmod{m_1 ... m_s}$:

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

PIERĀDĪJUMS Izmantosim indukciju ar parametru s.

Indukcijas bāze Ja $s = 2$, tad ir pierādīts - ĶAT.

Indukcijas solis Pieņemsim, ka apgalvojums ir spēkā, ja $s = n$ un

pierādīsim, ka apgalvojums ir spēkā ar $s = n+1$. Apskatīsim sistēmu

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

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

$$x \equiv c_n \pmod{m_1...m_n}.$$

Tātad visa sistēma ir ekvivalenta divu vienādojumu sistēmai

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

kas apmierina divu vienādojumu sistēmas ĶAT nosacījumus:

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

Tādējādi saskaņā ar ĶAT $n+1$ vienādojumu sistēmai eksistē viens atrisinājums c mod $m_1...m_{n+1}$.■

1.2. piemērs. Atrisināsim sistēmu

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

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

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

1.2. Pastiprinātās teorēmas

1.2.1. Pastiprinātā divu vienādojumu teorēma

1.1. piezīme. Ja ir dota sistēma

$$\begin{cases} x \equiv a \pmod{m_1} \\ x \equiv b \pmod{m_2}, \end{cases} \quad \text{kur } LKD(m_1, m_2) = d > 1,$$

tad viens acīmredzams šķērslis atrisinājumu eksistencei ir šāds: ja $a \not\equiv b \pmod{d}$, tad reducējot abus vienādojumus mod d, iegūsim pretrunu. Izrādās, ka tas ir vienīgais šķērslis.

1.3. teorēma. (*divu vienādojumu pastiprinātā ĶAT, 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. $\begin{cases} d|m_1 \\ d|m_2 \end{cases} \implies x$ apmierina sistēmu $\begin{cases} x \equiv a \pmod{d} \\ x \equiv b \pmod{d}, \end{cases} \implies$

$$a \equiv b \pmod{d}.$$

2. $\begin{cases} LKD(m_1, m_2) = d \\ d|a-b \end{cases} \implies a - b = q \cdot d$ var tikt izteikts kā m_1 un m_2 lineāra kombinācija: $\exists\, u_1, u_2 \in \mathbb{Z}$:

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

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

Pieņemsim, ka $\tilde{x_1}, \tilde{x_2} \in \mathbb{Z}$ apmierina sistēmu, $m_1 = m_1' d$ un $m_2 = m_2' d$, kur $LKD(m_1', m_2') = 1$. Atcerēsimies arī, ka

$$MKD(m_1, m_1) = \frac{m_1 m_2}{d} = m_1' m_2' d.$$

Redzam, ka

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

Tāpat kā ĶAT seko, ka $m_2' | q_1$ un $m_1' | q_2$, tātad

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

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

1.3. 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

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

1.2.2. Pastiprinātā vairāku vienādojumu teorēma

1.4. 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 $a_i \equiv a_j \pmod{d_{ij}}$ $\forall$ i, j, tad vienādojumu sistēmai

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

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

PIERĀDĪJUMS Līdzīgs klasiskajam gadījumam.
■

1.4. 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. 5.mājasdarbs

2.1. Obligātie uzdevumi

5.1 Atrisiniet vienādojumu sistēmas izmantojot ķīniešu atlikumu teorēmas

(a) $\begin{cases} x \equiv 4 \pmod 7 \\ x \equiv 5 \pmod{11} \end{cases}$

(b) $\begin{cases} x \equiv 3 \pmod 8 \\ x \equiv 2 \pmod 9 \end{cases}$

(c) $\begin{cases} x \equiv 10 \pmod{12} \\ x \equiv 16 \pmod{18} \end{cases}$

5.2 Atrisiniet vienādojumu sistēmas

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

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

5.3 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?

2.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi

5.4 Izstrādājiet metodi, ar kuras palīdzību var atrisināt ĶAT atbilstošās vienādojumu sistēmas neizmantojot indukciju.