***DAUGAVPILS UNIVERSITĀTE***
***Dabaszinātņu un matemātikas fakultāte***
***Matemātikas katedra***

# Daugavpils Universitātes Jauno matemātiķu skola

## Veselo skaitļu teorija - 4

***Docētājs: Dr. P. Daugulis***

***2008./2009.studiju gads***

# Saturs

# 1. Ķīniešu atlikumu teorēma un tās pastiprinājumi

## 1.1. Klasiskā divu vienādojumu teorēma

**1.1. teorēma.** (*Ķīniešu atlikumu teorēma - klasiskais variants*, Sun Tzi, 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 $q_1 | m_2$ un $q_2 | m_1$, tātad $\tilde{x_1} - \tilde{x_2} \equiv 0 \pmod{m_1 m_2}$. Ir pierādīts, ka atrisinājumi veido vienu klasi mod $m_1 m_2$. ■

**1.1. 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

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

**1.1. 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

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

## 1.2. Vairāku vienādojumu teorēma

**1.2. 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 $m_1 m_2 ... m_s$.

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

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

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

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

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 $m_1 ... m_{n+1}$.

■

**1.2. piezīme.** Iepriekšējās teorēmas cits formulējums: sistēma

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

ir ekvivalenta vienam vienādojumam

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

**1.2. 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

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

## 1.3. Pastiprinātā divu vienādojumu teorēma

**1.3. 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 $a \not\equiv b \pmod{d}$, tad reducējot abus vienādojumus (mod d), iegūsim pretrunu. Izrādās, ka tas ir vienīgais šķērslis.

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

1. Ja $a \not\equiv b \pmod{d}$, tad sistēmai

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

nav atrisinājumu.

2. Ja $a \equiv b \pmod{d}$, tad dotajai vienādojumu sistēmai ir tieši viens atrisinājums pēc moduļa $MKD(m_1, m_2)$.

PIERĀDĪJUMS

1. Tā kā $d|m_1$ un $d|m_2$, tad $x$ 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 $q_1 | m_2'$ un $q_2 | m_1'$, 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 $m_1 m_2$. ■

**1.4. 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

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

**1.3. 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

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

## 1.4. 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

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

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

■

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

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

ir ekvivalenta vienam vienādojumam

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

**1.4. 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

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