

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

*Studiju kurss*

## Veselo skaitļu teorija

### 9.lekcija (datoriķiem)

*Docētājs: Dr. P. Daugulis*

*2008./2009.studiju gads*

# Saturs

|                                                                   |           |
|-------------------------------------------------------------------|-----------|
| <b>1. Vienādojumu risināšana atlikumu kopās ar saliktu moduli</b> | <b>3</b>  |
| 1.1. Risināšanas vispārīgā shēma gadījumā ar saliktu moduli       | 3         |
| 1.2. Ķīniešu atlikumu teorēma un tās pastiprinājumi . . .         | 6         |
| <b>2. 9.mājasdarbs</b>                                            | <b>23</b> |

# 1. Vienādojumu risināšana atlikumu kopās ar saliktu moduli

## 1.1. Risināšanas vispārīgā shēma gadījumā ar saliktu moduli

**1.1. teorēma.** Ja  $m = p_1^{\alpha_1} \dots p_l^{\alpha_l}$ , tad vienādojums

$$f(x) \equiv 0 \pmod{m}$$

ir ekvivalents sistēmai

$$\begin{cases} f(x) \equiv 0 \pmod{p_1^{\alpha_1}} \\ f(x) \equiv 0 \pmod{p_2^{\alpha_2}} \\ \dots \\ f_l(x) \equiv 0 \pmod{p_l^{\alpha_l}}. \end{cases}$$

PIERĀDĪJUMS Saskaņā ar iepriekš pierādītu faktu sistēmas atrisinājumi veido klases mod  $m = p_1^{\alpha_1} \dots p_l^{\alpha_l}$ . Ja skaitlis  $a$  apmierina

sistēmu, tad  $p_i^{\alpha_i} | f(a)$  katram  $i$ , tātad ir spēkā dalāmība  $m | f(a)$  un  $f(a) \equiv 0 \pmod{m}$ .

Ja vesels skaitlis  $b$  apmierina vienādojumu  $f(x) \equiv 0 \pmod{m}$ , tad tas apmierina vienādojumu  $f(x) \equiv 0 \pmod{p_i^{\alpha_i}}$  katram  $i$ , jo  $p_i^{\alpha_i} | m$ , tātad tas apmierina arī visu sistēmu.



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

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 ("salīmēt") sākotnējā vienādojuma globālos atrisinājumus no lokālajiem atrisinājumiem  $\pmod{p_i^{\alpha_i}}$ : katrai kopu virknei  $(a_1, \dots, a_l)$ , kur  $a_i \in S_i$ , 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 vesēlie skaitļi  $x$ , kas visām iespējamajām virknēm  $(a_1, \dots, a_l)$  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. Ķīniešu atlikumu teorēma un tās pastiprinājumi

**1.2. 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  $m_2 | q_1$  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  $m_1 m_2$ . ■

**1.2. 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

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

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

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

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

**PIERĀDĪJUMS** Ir vairāki pierādījuma veidi.

Pierādījums izmantojot matemātisko indukciju ar parametru  $s$ . Ja  $s = 2$ , tad ir pierādīts. Pieņemsim, ka apgalvojums ir spēkā, ja  $s = i$  un pierādīsim, ka apgalvojums ir spēkā ar  $s = i + 1$ . Apskatīsim



sistēmu

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \dots \\ x \equiv a_s \pmod{m_s} \\ x \equiv a_{s+1} \pmod{m_{s+1}} \end{cases}$$

Sistēma, kas satur pirmos  $s$  vienādojumus, saskaņā ar indukcija pieņēmumu ir ekvivalenta vienam vienādojumam

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

Tātad visa sistēma ir ekvivalenta divu vienādojumu sistēmai

$$\begin{cases} x \equiv c \pmod{m_1 \dots m_s} \\ x \equiv a_{s+1} \pmod{m_{s+1}}, \end{cases}$$

kas apmierina divu vienādojumu sistēmas ķīniešu atlikumu teorēmas nosacījumus. Tādējādi  $s + 1$  vienādojumu sistēmai eksistē viens atrisinājums mod  $m_1 \dots m_{s+1}$ .

Pierādījums izmantojot elementu invertējamību. Apzīmēsim ar  $M$  skaitli  $m_1 m_2 \dots m_s$ . 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

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

Redzam, ka  $D$  apmierina sistēmu, jo

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

kur  $i \neq j$ . Vienīgums  $\pmod{M}$  tiek pierādīts tāpat kā klasiskajā gadījumā. ■

**1.3. 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 diviem paņēmieniem, kas atbilst dotajiem pierādījumiem.

Matemātiskās indukcijas paņēmieni. 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

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

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

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

**1.3. 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  $2, 8, 22 \pmod{30}$ .

**1.4. 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  $\pmod{d}$ , 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. 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.

Vienīgums tiek pierādīts kā klasiskajā ķīniešu atlikumu teorēmā.



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

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

ir ekvivalenta vienam vienādojumam

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

**1.4. 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

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

**1.5. 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

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

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

PIERĀDĪJUMS Līdzīgi klasiskajam gadījumam.



**1.6. 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

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

### 1.5. 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. 9.mājasdarbs

9.1 Atrisiniet vienādojumu sistēmas

(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)

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

9.2 Atrisiniet vienādojumu sistēmas

(a)

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

(b)

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

9.3 Izmantojot ķīniešu atlikumu teorēmu atrisiniet vienādojumu

$$x^2 \equiv 19 \pmod{30}.$$

9.4 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?