DAUGAVPILS UNIVERSITĀTE
Dabaszinātņu un matemātikas fakultāte
Matemātikas katedra
Jauno matemātiķu skola

Studiju kurss

Veselo skaitļu teorija

4.lekcija

Docētājs: Dr. P. Daugulis

2009./2010.studiju gads

Saturs

Lekcijas kopsavilkums:

- apgūt veselo skaitļu salīdzināmības teorijas pamatus,
- apgūt atlikumu (modulārās) aritmētikas pamatus.

Svarīgākie jēdzieni: kongruence/salīdzināmība mod m, ekvivalences attiecība un ekvivalences klases.

Svarīgākie fakti un metodes: kongruences īpašības (ar fiksētu moduli, ar mainīgu moduli, aritmētiskās).

1. Kongruence, atlikumu klases un to īpašības

1.1. Kongruence

1.1.1. Definīcija

Fiksēsim $m \in \mathbb{Z}$. Teiksim, ka $a, b \in \mathbb{Z}$ ir *salīdzināmi* vai *kongruenti* pēc moduļa m $(\mathrm{mod}\ m)$ $\iff$ a un b dalījumā ar m dod vienādu atlikumu. Apzīmē ar pierakstu $a \equiv b(\mathrm{mod\ m})$.

1.1. piemērs. $2 \equiv 5(\mathrm{mod}\ 3)$, $4 \equiv -3(\mathrm{mod}\ 7)$,

1.1. teorēma. $a \equiv b(\mathrm{mod}\ m) \iff m|a-b.$

PIERĀDIJUMS

$$\begin{cases} a = q_1 m + r \\ b = q_2 m + r \end{cases} \Longrightarrow a - b = m(q_1 - q_2) \Longrightarrow m|a-b.$$

$$\begin{cases} a = q_1 m + r_1 \\ b = q_2 m + \underbrace{r_2}_{\neq r_1} \end{cases} \Longrightarrow a - b = m(q_1 - q_2) + \underbrace{(r_1 - r_2)}_{\neq 0}.$$

Pieņemsim, ka $r_1 > r_2$.

$$\begin{cases} 0 \leq r_1 \leq m-1 \\ 0 \leq r_2 \leq m-1 \end{cases} \Longrightarrow r' = r_1 - r_2 \leq m-1.$$

$\Longrightarrow atl(a-b, m) = r' \neq 0 \Longrightarrow m \nmid a-b.$ ■

1.1.2. Salīdzināmības mod m ekvivalences klases

Salīdzināmības attiecībai atbilstošā veselo skaitļu kopas sadalījuma apakškopas vai klases sauc par *atlikumu klasēm mod m*. Katrā atlikumu klasē ir visi veselie skaitļi, kas dalījumā ar m dod vienu un to pašu atlikumu.

1.2. piemērs. $m = 2$, $\mathbb{Z} = C_0 \bigcup C_1$, kur
C_0 ir 0 klase - pāra skaitļi, $2k$,

C_1 ir 1 klase - nepāra skaitļi, $2k+1$.

$m=3$, $\mathbb{Z}=C_0 \bigcup C_1 \bigcup C_2$, kur
C_0 ir 0 klase - skaitļi formā $3k$,
C_1 ir 1 klase - skaitļi formā $3k+1$,
C_2 ir 2 klase - skaitļi formā $3k+2$.

1.2. teorēma. Atlikumu klašu skaits mod m ir vienāds ar $|m|$.

PIERĀDĪJUMS Atlikums dalot ar m var būt vesels skaitlis robežās no 0 līdz $|m|-1$, tātad klašu skaits ir $|m|$.■

Jebkuru kopas $\mathbb{Z}$ apakškopu, kas satur tieši vienu elementu no katras atlikumu klases, sauksim par *pilnu atlikumu klašu pārstāvju kopu (PAK)*.

Par *kanonisko klašu pārstāvju kopu sauksim kopu*

$$\{0,1,...,|m|-1\}.$$

Ja m ir nepāra skaitlis, tad var izmantot arī atlikumu klašu pārstāvju kopu, kas ir simetriska attiecībā uz 0:

$$\{-\frac{|m|-1}{2}, \ldots -1, 0, 1, \ldots, \frac{|m|-1}{2}\}, \text{ja m ir nepāra skaitlis.}$$

Skaitlim n atlikumu klasi $\pi_m(n) = \overline{n} = [n]$ sauksim par n *redukciju mod* m. Strādājot ar atlikumu klasēm parasti ekonomijas nolūkā $[n]$ raksta kā n.

1.1.3. Kongruences īpašības ar fiksētu moduli

1.3. teorēma.

1. $a = b \implies a \equiv b (\text{mod } m), \ \forall\, m \in \mathbb{Z}.$
1' $\exists\, m \in \mathbb{Z} : \ a \not\equiv b (\text{mod } m) \implies a \neq b.$
2. $m = \pm 1 \implies a \equiv b (\text{mod } m), \forall\, a, b.$
3. $m = 0 \implies \Big(a \equiv b (\text{mod } m) \iff a = b\Big),$
4. $a \equiv a (\text{mod } m)$ (*refleksivitāte*),

5. $a \equiv b(\text{mod } m) \implies b \equiv a(\text{mod } m)$ (*simetrija*),

6. $\begin{cases} a \equiv b(\text{mod } m) \\ b \equiv c(\text{mod } m) \end{cases} \implies a \equiv c(\text{mod } m)$ (*tranzitivitāte*).

7. $\begin{cases} d|a \\ d|b \\ LKD(d,m) = 1 \end{cases} \implies \left(a \equiv b(\text{mod } m) \implies \frac{a}{d} \equiv \frac{b}{d} \text{ (mod m)}\right)$

PIERĀDĪJUMS

1. $a - b = 0$, $m|0$.

2. $\pm 1|a - b$.

3. $0|a - b \iff a - b = 0$.

4. $m|a - a$.

5. $m|a - b \implies a - b = qm$ un $b - a = (-q)m \implies m|b - a$.

6.
$$\begin{cases} m|a-b \\ m|b-c \end{cases} \Longrightarrow \begin{cases} a-b=qm \\ b-c=q'm \end{cases}$$
Saskaitot šīs vienādības, iegūsim $a-c=(q+q')m$, tāpēc $m|a-c$.

7. Pieņemsim, ka $a=da'$, $b=db'$.
$a \equiv b(\text{mod } m) \Longrightarrow a-b=qm \Longrightarrow d(a'-b')=qm \Longrightarrow$

$$\begin{cases} m|d(a'-b') \\ LKD(d,m)=1 \end{cases} \Longrightarrow m|a'-b' \Longrightarrow a' \equiv b'(\text{mod } m).\blacksquare$$

1.1.4. Kongruences īpašības ar mainīgu moduli

1.4. teorēma.

1. $a \equiv b(\text{mod } m) \iff a \equiv b(\text{mod } (-m))$ (var mainīt moduļa zīmi).

2. $a \equiv b(\mathrm{mod}\ m) \implies ak \equiv bk(\mathrm{mod}\ mk), \forall\ k \in \mathbb{Z}$ (modulārās vienādības abas puses un moduli var reizināt ar vienu un to pašu skaitli).

3. $\left\{ \begin{array}{l} d|a \\ d|b \\ d|m \end{array} \right. \implies \Big(a \equiv b(\mathrm{mod}\ m) \implies \frac{a}{d} \equiv \frac{b}{d}\ (\mathrm{mod}\ \frac{m}{d}) \Big)$ (abas kongruences puses un moduli var dalīt ar kopīgu dalītāju)

4. $m'|m \implies \Big(a \equiv b(\mathrm{mod}\ m) \implies a \equiv b(\mathrm{mod}\ m') \Big)$ (var pārnest kongruenci uz moduļa dalītājiem).

5. $\left\{ \begin{array}{l} a \equiv b(\mathrm{mod}\ m) \\ a \equiv b(\mathrm{mod}\ m') \end{array} \right. \iff a \equiv b(\mathrm{mod}\ MKD(m, m'))$ (ja skaitļi ir kongruenti pēc vairākiem moduļiem, tad tie ir kongruenti arī pēc moduļu MKD).

PIERĀDĪJUMS

1. $a \equiv b(\mathrm{mod}\ m) \iff a - b = qm = (-q)(-m) \iff$
$a \equiv b(\mathrm{mod}\ -m)$.

2. $a \equiv b(\text{mod } m) \implies a - b = qm \implies ak - bk = q(mk) \implies$
$ak \equiv bk(\text{mod } mk)$

3. Definēsim $\begin{cases} a = da' \\ b = db' \\ m = dm'. \end{cases}$

$a \equiv b(\text{mod } m) \implies a - b = qm \implies da' - db' = q(dm') \implies$
$a' = b' = qm' \implies a' \equiv b'(\text{mod } m').$

4. $\begin{cases} a \equiv b(\text{mod } m) \\ m'|m \end{cases} \implies \begin{cases} a - b = qm \\ m = q'm' \end{cases} \implies a - b = qq'm'$
$\implies a \equiv b(\text{mod } m').$

5. $\begin{cases} a \equiv b(\text{mod } m) \\ a \equiv b(\text{mod } m') \end{cases} \iff \begin{cases} m|a - b \\ m'|a - b \end{cases} \iff$
$MKD(m, m')|a - b \iff a \equiv b(\text{mod } MKD(m, m')).$ ■

1.1.5. Kongruences īpašības ar aritmētiskajām operācijām

1.5. teorēma.

1. $a \equiv b (\mathrm{mod}\ m) \iff a + c \equiv b + c (\mathrm{mod}\ m), \forall\ c \in \mathbb{Z}.$
2. $a \equiv b (\mathrm{mod}\ m) \implies ac \equiv bc (\mathrm{mod}\ m), \forall\ c \in \mathbb{Z}.$
3. $\left\{ \begin{array}{l} a \equiv b (\mathrm{mod}\ m) \\ a' \equiv b' (\mathrm{mod}\ m) \end{array} \right. \implies a + a' \equiv b + b' (\mathrm{mod}\ m)$
4. $\left\{ \begin{array}{l} a \equiv b (\mathrm{mod}\ m) \\ a' \equiv b' (\mathrm{mod}\ m) \end{array} \right. \implies aa' \equiv bb' (\mathrm{mod}\ m)$
5. $a \equiv b (\mathrm{mod}\ m) \implies a^n \equiv b^n (\mathrm{mod}\ m), \forall\ n \in \mathbb{N}.$
6. $a \equiv b (\mathrm{mod}\ m) \implies f(a) \equiv f(b) (\mathrm{mod}\ m), \forall\ f \in \mathbb{Z}[X].$

PIERĀDĪJUMS

1. $a - b = qm \iff (a + c) - (b + c) = qm.$

2. $a - b = qm \implies ac - bc = (qc)m \iff ac \equiv bc (\mathrm{mod}\ m).$

3. $\left\{ \begin{array}{l} m|a-b \\ m|a'-b' \end{array} \right. \Longrightarrow m|(a+a')-(b+b') \Longrightarrow$
$a+a' \equiv b+b' (\text{mod } m)$.

4. $\left\{ \begin{array}{l} m|a-b \\ m|a'-b' \end{array} \right. \Longrightarrow m|b'(a+a')-a(b+b') \Longrightarrow$
$m|aa'-bb' \Longrightarrow aa' \equiv bb' (\text{mod } m)$.

5. Seko no iepriekšējiem apgalvojumiem.

6. Seko no iepriekšējiem apgalvojumiem. ■

1.1. piezīme. Ja ir jāatrod $f(x_1, ..., x_n)(\text{mod } m)$, tad visus argumentus var aizvietot ar to atlikumiem mod m vai citiem kongruentiem skaitļiem.

1.2. piezīme. Pierādītā teorēma kopā ar apgalvojumu -

$$\exists\, m: \ a \not\equiv b \ (\text{mod m}) \Longrightarrow a \neq b$$

- ir viens no veidiem kā pierādīt, ka vienādojumam vai vienādojumu sistēmai neeksistē atrisinājums veselos skaitļos.

Ja ir iespējams atrast $m \in \mathbb{Z}$: vienādojumam $f(x) \equiv 0 \pmod{m}$ nav atrisinājumu, tad vienādojumam $f(x) = 0$ nav atrisinājumu.

Teorēma apgalvo, ka, lai pierādītu, ka vienādojumam

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

nav atrisinājumu, pietiek apskatīt galīgu skaitu variantu -

$$0 \leq x \leq m - 1.$$

Diemžēl ne vienmēr šāds pierādījums ir iespējams - eksistē Diofanta vienādojumi, kas ir atrisināmi pēc visiem moduļiem, bet nav atrisināmi veselos skaitļos.

1.3. piemērs. Pierādīsim, ka vienādojumam $x^2 - 2 = 5y^2$ nav veselu atrisinājumu, pētot redukciju mod 2,3,4,....

1.1.6. Ķīniešu atlikumu teorēma

1.6. teorēma. *(Ķīniešu atlikumu teorēma (ĶAT)- klasiskais variants) Ja* $LKD(m_1, m_2) = 1$, *tad vienādojumu sistēmai*

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

ir tieši viens atrisinājums mod $m_1 m_2$.

PIERĀDĪJUMS $LKD(m_1, m_2) = 1 \implies$ 1 un līdz ar to arī $a - b = (a - b) \cdot 1$ 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 $m_1 m_2$. ■

1.3. piezīme. ĶAT cits formulējums: sistēma

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

ir ekvivalenta vienam vienādojumam

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

1.4. 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

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

1.7. teorēma. $LKD(m_i, m_j) = 1, \forall\ i, j \implies$ 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 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

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

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

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

kas apmierina divu vienādojumu sistēmas ĶAT nosacījumus:

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

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

1.4. piezīme. Iepriekšējās teorēmas cits formulējums: 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

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

1.5. 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

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

1.5. 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.

1.8. teorēma. (*divu vienādojumu pastiprinātā ĶAT*) 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 $\Longrightarrow$ klase mod $MKD(m_1 m_2)$ arī apmierina sistēmu. ■

1.6. piezīme. 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

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

1.6. 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

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

2. 4.mājasdarbs

2.1. Obligātie uzdevumi

4.1 Atrodiet atlikumus pēc dotā moduļa:

a) $10!(\text{mod } 7)$,
b) $100^{100}(\text{mod } 13)$,

4.2 $p \in \mathbb{P}$. Pierādīt, ka

(a) $p \equiv \pm 1(\text{mod } 6)$,
(b) $p^2 \equiv 1(\text{mod } 24)$.

4.3 Atrisiniet vienādojumus atlikumu klasēs:

a) $x^3 + x + 1 \equiv 0(\text{mod } 7)$,
b) $x^3 + y^2 \equiv 2(\text{mod } 5)$.

4.4 Pierādīt, ka dotajiem vienādojumiem nav atrisinājumu veselos skaitļos.

(a) $2x^2 - 3y^2 = 9$,
(b) $x^3 - 2y^3 = 14$,

(c) $x^3 + y^3 + z^3 = 2011$.

4.5 Pierādiet, ka visiem naturāliem skaitļiem n izpildās

$$1 + 2^{2^n} + 2^{2^{n+1}} \equiv 0 (\text{mod } 7).$$

2.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi

4.6 $\{x_0, ..., x_{m-1}\} \subseteq \mathbb{Z}$ veido PAK mod m. Kādiem jābūt $a, b \in \mathbb{Z}$, lai $\{ax_0 + b, ..., ax_{m-1} + b\}$ arī veidotu PAK.

4.7 Dots $p \in \mathbb{P}$. Ar ko var būt kongruents p

(a) mod 3,
(b) mod 6,
(c) mod 10,
(d) mod 12.