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

Studiju kurss

Veselo skaitļu teorija

3.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 $r_1 > r_2$.

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

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

1.1.2. Kongruences īpašības

1.2. teorēma. (*īpašības ar fiksētu moduli*)

1. $a = b \implies a \equiv b (\mathrm{mod}\ m),\ \forall\ m \in \mathbb{Z}.$
2. $m = \pm 1 \implies a \equiv b (\mathrm{mod}\ m), \forall\ a, b.$
3. $m = 0 \implies \Big(a \equiv b (\mathrm{mod}\ m) \iff a = b\Big),$
4. $a \equiv a (\mathrm{mod}\ m)$ (*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. piezīme. Teorēmas 1.apgalvojuma apgrieztā forma:

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

Šī forma ir lietderīga risinot vienādojumus veselos skaitļos.

1.3. teorēma. (*īpašības ar mainīgu moduli*)

1. $a \equiv b(\mathrm{mod}\ m) \iff a \equiv b(\mathrm{mod}\ (-m))$ (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. $\left\{ \begin{array}{l} d|a \\ d|b \\ d|m \end{array} \right. \implies \left(a \equiv b(\mathrm{mod}\ m) \implies \frac{a}{d} \equiv \frac{b}{d}\ (\mathrm{mod}\ \frac{m}{d}) \right)$ (abas kongruences puses un moduli var dalīt ar kopīgu dalītāju)
4. $m'|m \implies \left(a \equiv b(\mathrm{mod}\ m) \implies a \equiv b(\mathrm{mod}\ m') \right)$ (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. $a \equiv b(\mathrm{mod}\ m) \implies a - b = qm \implies ak - bk = q(mk) \implies$
$ak \equiv bk(\mathrm{mod}\ mk)$

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

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

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

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

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

1.2. piemērs.

1.4. teorēma. (*īpašības ar aritmētiskajām operācijām*)

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

PIERĀDĪJUMS

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

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

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

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

5. Seko no iepriekšējiem apgalvojumiem.

6. Seko no iepriekšējiem apgalvojumiem. ■

1.3. piemērs.

1.2. piezīme. Pierādītā teorēma kopā ar apgalvojumu -

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

- 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.

1.4. piemērs. Pierādīsim, ka vienādojumam $x^2 + y^2 = 4n + 3$ nav veselu atrisinājumu, pētot redukciju pēc mod 4.

1.2. Atlikumu klases

1.2.1. Attiecības

Binära attiecība - īpašība, kas piemīt vai nepiemīt kopas (vai divu dažādu kopu) sakārtotiem elementu pāriem.

Ja elementu pārim (x, y) piemīt šī īpašība, tad teiksim, ka tie ir saistīti ar attiecību (kuru apzīmēsim ar kādu atdalošo simbolu, piemēram ρ, $+$, $<$ u.c.) un pierakstīsim to formā $x\rho y$, pretējā gadījumā - $x \not\rho y$.

1.5. piemērs. Attiecību piemēri:

- reālo skaitļu sakārtojums $\rho = \leq$,
- veselo skaitļu dalāmības attiecība $\rho = |$.

Attiecību ρ sauksim par *refleksīvu*, ja $\forall\ a \in A:\ a\rho a$.

Attiecību ρ sauksim par *simetrisku*, ja $\forall\ a, b \in A$: $a\rho b \implies b\rho a$.

Attiecību sauc par *tranzitīvu*, ja $\forall\, a, b, c \in A$ (ne obligāti dažādiem): $a\rho b$ un $b\rho c \implies a\rho c$.

1.2.2. Ekvivalences attiecība un sadalījumi

Attiecību sauc par *ekvivalenci*, ja tā ir

1. refleksīva,
2. simetriska,
3. tranzitīva.

Klasiski ekvivalenču piemēri: skaitļu un, vispārīgāk, matemātisku objektu vienādība, ģeometrisku figūru līdzība.

Par kopas A *sadalījumu* sauc A apakškopu kopu $\aleph = \{A_\alpha\}_{\alpha\in I}$ ar šādām īpašībām:

- $A_\alpha \neq A_{\alpha'} \implies A_\alpha \bigcap A_{\alpha'} = \emptyset$,
- $\bigcup_{\alpha\in I} A_\alpha = A$.

Par sadalījuma $\aleph$ *projekcijas funkciju* vai *projekciju* sauksim funkciju

$$\pi_{\aleph} : A \to \aleph,$$

kas katram elementam a piekārto to $\aleph$ apakškopu, kuram tas pieder.

Kopu $\aleph$ var uzskatīt par kopas A vienkāršotu modeli. Šādu pāreju sauc par A *faktorizāciju*, $\aleph$ sauc par A *faktorkopu*.

1.5. teorēma.

1. $\forall$ kopas A sadalījumam var piekārtot A ekvivalenci, kuras ekvivalences klases ir A sadalījuma elementi.
2. $\forall$ kopas A ekvivalencei atbilstošās ekvivalences klases veido A sadalījumu.

PIERĀDĪJUMS

1. Dots kopas A sadalījums $A = \{A_\alpha\}_{\alpha \in I}$, definēsim tam atbilstošu ekvivalenci $\equiv$: $a \equiv b \iff a$ un b pieder vienai un tai pašai sadalījuma apakškopai A_x.

2. Dota ekvivalence $\equiv$, parādīsim, kā tai piekārtot A sadalījumu.

$\forall\ a \in A$ definēsim $A_a = \{x \in A | x \equiv a\}$ (elementa a ekvivalences klasi). $\forall\ a$ izpildās $a \in A_a \implies A_a \neq \emptyset$ un $\bigcup_{a \in A} A_a = A \implies \{A_a\}_{a \in A}$ ir kopas A pārklājums.

Var pierādīt, ka $A_a \neq A_b \implies A_a \cap A_b = \emptyset$. ■

2. 3.mājasdarbs

2.1. Obligātie uzdevumi

3.1 Atrodiet atlikumus pēc dotā moduļa:

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

3.2 Atrisiniet vienādojumus atlikumu klasēs:

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

3.3 Pierādiet, ka visiem naturāliem skaitļiem n izpildās

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

3.4 Pierādiet, ka vienādojumam

$$x^2 - 2 = 5y^2$$

nav veselu atrisinājumu. (*Norādījums: risiniet šo vienādojumu mod* 4 *vai mod* 5)

2.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi

3.5 $\{x_0, ..., x_{m-1}\} \subseteq \mathbb{Z}$ veido PAK mod m. Kādiem jābūt $a, b \in \mathbb{Z}$, lai $\{ax_0 + b, ..., ax_{m-1} + b\}$ arī veidotu PAK.

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

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