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

Studiju kurss

SKAITĻU TEORIJA

4.lekcija

Docētājs: Dr. P. Daugulis

2012./2013.studiju gads

Saturs

Lekcijas mērķis:

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

Lekcijas kopsavilkums:

- kopā $\mathbb{Z}$ var definēt kongruences mod m jēdzienu - salīdzināt skaitļus atkarībā no to atlikuma dalot ar m,
- kongruence mod m inducē $\mathbb{Z}$ sadalījumu *atlikumu klasēs*,
- atlikumu klašu kopā var definēt operācijas, kas ir līdzīgas veselo skaitļu aritmētiskajām operācijām.

Svarīgākie jēdzieni: kongruence/salīdzināmība mod m, atlikumu klase mod m, pilna un kanoniska atlikumu klašu pārstāvju kopa, redukcija mod m, operācijas ar atlikumu klasēm.

Svarīgākie fakti un metodes: kongruences īpašības (ar fiksētu moduli, ar mainīgu moduli, aritmētiskās), atlikumu klašu operāciju definīcijas un īpašības, atlikumu lietojumi vienādojumu risināšanā, dalāmības pazīmju atrašana.

1. Veselo skaitļu kongruence, atlikumu klases un to īpašības

1.1. Veselo skaitļu kongruence mod m

1.1.1. Definīcija

Fiksēsim $m \in \mathbb{Z}$. Teiksim, ka $a, b \in \mathbb{Z}$ ir *salīdzināmi* vai *kongruenti* attiecībā uz dalīšanu ar m (mod m, apzīmē kā $a \equiv b (\text{mod m})$) tad un tikai tad, ja a un b dalījumā ar m dod vienādus atlikumus:

$$atl(a, m) = atl(b, m).$$

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

1.1. teorēma.

$$\boldsymbol{a \equiv b} (\text{mod } \boldsymbol{m}) \iff \boldsymbol{m} \mid \boldsymbol{a - b}.$$

PIERĀDIJUMS

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

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

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. piezīme. Svarīgs speciālgadījums: $a \equiv 0 (\mathrm{mod}\ m) \iff m \Big| a.$

1.1.2. Kongruences īpašības

Īpašības ar fiksētu moduli

1.2. teorēma.

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

PIERĀDĪJUMS

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

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

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

4. $m \Big| a-a.$

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

6.
$$\begin{cases} m \Big| a-b \\ m \Big| b-c \end{cases} \implies \begin{cases} a-b=qm \\ b-c=q'm \end{cases}$$

Saskaitot šīs vienādības, iegūsim $a-c=(q+q')m$, tāpēc $m \Big| a-c$. ■

1.2. piezīme. Teorēmas 1.apgalvojuma apgrieztā forma (M-īpašība):

$$\Big(\exists\, \boldsymbol{m} \in \mathbb{Z} : \ \boldsymbol{a} \not\equiv \boldsymbol{b} (\mathrm{mod}\ \boldsymbol{m})\Big) \implies \boldsymbol{a} \neq \boldsymbol{b}.$$

Īpašības ar mainīgu moduli

1.3. teorēma.

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. $m' \Big| m \implies \left(a \equiv b(\mathrm{mod}\ m) \implies a \equiv b(\mathrm{mod}\ m') \right)$ (kongruenci var pārnest uz moduļa dalītājiem).
5. $\left\{ \begin{array}{l} a \equiv b(\mathrm{mod}\ m_1) \\ a \equiv b(\mathrm{mod}\ m_2) \\ \ldots \\ a \equiv b(\mathrm{mod}\ m_s) \end{array} \right. \iff a \equiv b(\mathrm{mod}\ MKD(m_1, ..., m_s))$ (skaitļi

ir kongruenti pēc vairākiem moduļiem $\Longleftrightarrow$ tie ir kongruenti pēc moduļu MKD).

PIERĀDĪJUMS

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

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

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

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

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

5. $$\begin{cases} a \equiv b(\text{mod } m_1) \\ a \equiv b(\text{mod } m_2) \\ \dots \\ a \equiv b(\text{mod } m_s) \end{cases} \Longleftrightarrow \begin{cases} m_1 | a-b \\ m_2 | a-b \\ \dots \\ m_s | a-b \end{cases} \Longleftrightarrow$$

$$MKD(m_1, ..., m_s) \Big| a-b \Longleftrightarrow a \equiv b(\text{mod } MKD(m_1, ..., m_s)). \blacksquare$$

Īpašības ar aritmētiskajām operācijām

1.4. teorēma.

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

PIERĀDĪJUMS

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

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

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

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

5.,6. Seko no iepriekšējiem apgalvojumiem. ■

1.2. Atlikumu klases

1.2.1. Attiecības un ekvivalences

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

1.2. piemērs. Attiecību piemēri:

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

Attiecību ρ sauksim par *ekvivalenci*, ja tā ir

1. *refleksīva*- $\forall\ a \in A:\ a\rho a$,
2. *simetriska*- $\forall\ a, b \in A$: $a\rho b \implies b\rho a$,
3. *tranzitīva*- $\forall\ a, b, c \in A$ (ne obligāti dažādiem): $a\rho b$ un $b\rho c \implies a\rho c$.

1.3. piemērs. 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:

- $A_\alpha \neq A_{\alpha'} \implies A_\alpha \bigcap A_{\alpha'} = \varnothing$,
- $\bigcup\limits_{\alpha \in I} A_\alpha = A$.

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.

1.2.2. Kongruences mod m ekvivalences klases

Kongruences attiecība ir ekvivalence, 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.

Citiem vārdiem sakot, mod m kongruences klasi veido visi $x \in \mathbb{Z}$:

$$x \equiv a(\text{mod } m), \text{ kur } a \text{ ir fiksēts.}$$

1.4. piemērs. $m = 2$, $\mathbb{Z} = C_0 \bigcup C_1$, kur
C_0 ir 0 klase - pāra skaitļi, $2k$, $x \equiv 0(\text{mod } 2)$.
C_1 ir 1 klase - nepāra skaitļi, $2k+1$, $x \equiv 1(\text{mod } 2)$.

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

1.3. piezīme. Atlikumu klases $x \equiv a(\text{mod } m)$ elementi veido uz abām pusēm bezgalīgu aritmētisku progresiju ar vienu elementu a un diferenci m:

$$..., a-2m, a-m, a, a+m, a+2m, a+3m, ..., a+qm, ...$$

1.6. teorēma. $m \in \mathbb{Z}\backslash\{0\}$. Atlikumu klašu skaits mod m ir vienāds ar $|m|$.

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

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

1.5. piemērs. $m = 2$ - $\{0, 1\}$, $\{2, -3\}$. $m = 5$ - $\{-2, -1, 0, 1, 2\}$, $\{5, 11, 17, 23, 29\}$.

Par *kanonisko klašu pārstāvju kopu* sauksim minimālo nenegatīvo atlikumu klašu pārstāvju kopu

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

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

$$\left\{-\frac{|m|-1}{2}, ... -1, 0, 1, ..., \frac{|m|-1}{2}\right\}.$$

n atlikuma klasi mod m apzīmē kā $[n]$, n, $\overline{n}$ vai $m\mathbb{Z}+r$.

1.2.3. Operācijas ar atlikumu klasēm un to īpašības

$m \in \mathbb{Z}$ - fiksēts. Atlikumu klašu mod m $[a]$ un $[b]$

- summa $[a] + [b] := [a + b]$,
- reizinājumu $[a][b] := [ab]$.

1.6. piemērs. $[2] + [3] = [2 + 3] = [5] = [0](\text{mod } 5)$,
$[2] \cdot [3] = [2 \cdot 3] = [6] = [1](\text{mod } 5)$.

1.7. teorēma. (*atlikumu operāciju pamatīpašības*)

1. Atlikuma klašu operācijas ir definētas korekti - nav atkarīgas no pārstāvju izvēles.
2. $[a] + [b] = [b] + [a]$ (saskaitīšanas komutativitāte).
3. $[a][b] = [b][a]$ (reizināšanas komutativitāte).
4. $([a] + [b]) + [c] = [a] + ([b] + [c])$ (saskaitīšanas asociativitāte).
5. $([a][b])[c] = [a]([b][c])$ (reizināšanas asociativitāte).
6. $[a]([b] + [c]) = [a][b] + [a][c]$ (distributivitāte).

7. $[0] + [a] = [a] + [0] = [a]$ (saskaitīšanas neitrālā elementa eksistence).

8. $[1] \cdot [a] = [a]$ (reizināšanas neitrālā elementa eksistence).

PIERĀDĪJUMS

1. Jāpierāda, ka

$$\begin{cases} [a] = [a'] \\ [b] = [b'] \end{cases} \Longrightarrow [a+b] = [a'+b'].$$

$$\begin{cases} a \equiv a' (\text{mod } m) \\ b \equiv b' (\text{mod } m) \end{cases} \Longrightarrow a + b \equiv a' + b' (\text{mod } m).$$

2., 3. Seko no klašu operāciju definīcijām.

4.-10. Seko no aritmētisko operāciju īpašībām. ■

Atlikumu kopu mod m ar tajā uzdotām saskaitīšanas un reizināšanas operācijām sauc par *atlikumu gredzenu mod m* $(\mathbb{Z}/m, +, \cdot)$.

Tādējādi kongruenci

$$a \equiv b \pmod{m}$$

var domāt arī kā atlikumu klašu vienādību

$$[a] = [b].$$

Parasti mēs tā arī domāsim.

1.4. piezīme. Par atlikumu klašu kopu var domāt kā par veselo skaitļu kopu, kas ir "uztīta" uz riņķa līnijas. Atbilstoši var interpretēt operācijas ar atlikumu klasēm.

1.3. Atlikumu un to aritmētikas lietojumi

1.3.1. Periodiskie procesi

Atlikumu ideju izmanto laika mērīšanā:

- nedēļas dienas - kongruence mod 7,
- diennakts laiks - kongruence mod 24,

- gadalaiki - kongruence mod 4.

1.3.2. M-īpašības lietojumi

$$\Big(\exists\, \boldsymbol{m} \in \mathbb{Z} :\ \boldsymbol{a} \not\equiv \boldsymbol{b}\ (\mathrm{mod\ m})\Big) \implies \boldsymbol{a} \neq \boldsymbol{b}.$$

Aritmētisko operāciju pārbaude

Pārbaudes algoritms:

1. Atrodam operācijas rezultātu $c = a \star b$,
2. Atrodam $c' \equiv a \star b (\mathrm{mod}\ m)$ un $c'' \equiv c (\mathrm{mod}\ m)$,
3. Ja $c' \not\equiv c'' (\mathrm{mod}\ m)$, tad konstatējam kļūdu.

Vienādojumu neatrisināmības pierādīšana

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

- Ja ir iespējams atrast $m \in \mathbb{Z}$: vienādojumam $f(x) \equiv 0 (\mathrm{mod}\ m)$ nav atrisinājumu, tad vienādojumam $f(x) = 0$ nav atrisinājumu.
- Lai pierādītu, ka vienādojumam $f(x) \equiv 0 (\mathrm{mod}\ m)$ nav atrisinājumu, pietiek apskatīt galīgu skaitu variantu -

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

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

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

1.3.3. Dalāmības pazīmes

Dalāmības ar m pazīme - īpašība, kas ļauj pārbaudīt dalāmību ātrāk nekā izdalot, piemēram, īpašība, kas piemīt m daudzkārtņu cipariem (parasti decimālajā pierakstā).

Šajā sadaļā pieņemam, ka

$$n = \overline{a_k a_{k-1} ... a_0} = a_k \cdot 10^k + ... + a_1 \cdot 10 + a_0.$$

Lai atrastu dalāmības pazīmi ar m, ir lietderīgi izteikt n decimālajā pierakstā kā 10 pakāpju lineāru kombināciju un apskatīt $n (\text{mod } m)$:

$$n = \overline{a_k a_{k-1} ... a_0} = a_k \cdot 10^k + ... + a_1 \cdot 10 + a_0 (\text{mod } m).$$

Dalāmība ar 3 un 9

$m \in \{3, 9\}$.

$10^l \equiv 1 (\text{mod } m) \implies$

$n \equiv a_k \cdot 1 + a_{k-1} \cdot 1 + ... + a_0 \equiv a_k + a_{k-1} + ... + a_0 \text{ (mod m)}.$

Dalāmības pazīme ar m:

$$m|n \iff m\Big|a_k + a_{k-1} + ... + a_0.$$

(ja n ciparu summa dalās ar m).

2. 3.mājasdarbs

2.1. Obligātie uzdevumi

3.1 Atrast atlikumus pēc dotā moduļa:
(a) $2012 + 2013 + 2014 \pmod 8$,
(b) $2012 \cdot 2013 \cdot 2014 \pmod{11}$,
(c) $10! \pmod 7$,
(d) $2013^{2013} \pmod{13}$.

3.2 Atrast skaitļa $2011^{2012^{2013}}$ pēdējo ciparu.

3.3 Atrast saskaitīšanas un reizināšanas tabulas gredzeniem $\mathbb{Z}/7$ un $\mathbb{Z}/8$. Uzrādīt visus elementus, kuriem eksistē multiplikatīvi inversie elementi.

3.4 Atrisināt vienādojumus atlikumu klasēs:
(a) $x^3 + x + 1 \equiv 0 \pmod 7$,
(b) $x^5 \equiv 1 \pmod{11}$.

3.5 Pierādīt, ka vienādojumiem nav atrisinājumu veselos skaitļos.
(a) $x^2 - 2 = 5y^2$ (*Norādījums: mod* 4 *vai mod* 5),
(b) $x^4 + y^4 - z^4 = 2012$.

2.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi

3.6 $n \in \mathbb{N}$, skaitļa n^2 decimālajā pierakstā viens cipars ir 2, bet pārējie ir 1. Pierādīt, ka $11 \mid n$.

3.7 $\{x_0, ..., x_{m-1}\} \subseteq \mathbb{Z}$ veido PAK mod m. Kādiem jābūt $a, b \in \mathbb{Z}$, lai $\{ax_0 + b, ..., ax_{m-1} + b\}$ arī veidotu PAK.

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

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

3.9 Atrast ērtas dalāmības pazīmes ar $7, 11, 13$.

3.10 $f(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0$, $n > 0$, $a_n \neq 0$, $\forall\, i\ a_i \in \mathbb{Z}$ - nekonstants polinoms ar veseliem koeficientiem. Pierādīt, ka bezgalīgi daudziem $n \in \mathbb{Z}$ $f(n)$ ir salikts skaitlis.