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

Studiju kurss

Veselo skaitļu teorija

4.lekcija (datoriķiem)

Docētājs: Dr. P. Daugulis

2007./2008.studiju gads

Saturs

1. Atlikumu klases un to īpašības

1.1. Definīcija

Fiksēsim veselu skaitli m. Teiksim, ka divi veseli skaitļi a un b ir *salīdzināmi* vai *kongruenti* pēc moduļa m, apzīmē ar pierakstu

$$a \equiv b(\text{mod m}),$$

tad un tikai tad, ja $a - b$ dalās ar m vai, citos terminos, skaitļi a un b dalījumā ar m dod vienādu atlikumu.

1.1. piezīme. Tiek izmantoti arī šādi pieraksti:

$$a \equiv b(\text{m}), a \equiv b, \text{ mod m}.$$

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

1.1. teorēma. Abas salīdzināmības definīcijas ir loģiski ekvivalentas.

PIERĀDIJUMS

Ja $a = q_1 m + r$ un $b = q_2 m + r$, tad $a - b = m(q_1 - q_2)$ un tāpēc $m|a - b$.

Ja $a = q_1 m + r_1$ un $b = q_2 m + r_2$, kur $r_1 \neq r_2$, tad

$$a - b = m(q_1 - q_2) + (r_1 - r_2).$$

Redzam, ka $r_1 - r_2 \neq 0$, tāpēc, izdalot $r_1 - r_2$ ar m, iegūsim

$$r_1 - r_2 = q'm + r',$$

kur $r' \neq 0$. Tāpēc

$$a - b = m(q_1 - q_2 + q') + r'$$

un $m \nmid a - b$. ■

1.2. teorēma. Skaitļu salīdzināmībai pēc fiksēta moduļa m ir spēkā šādas īpašības:

1. katrs skaitlis a ir salīdzināms ar sevi - $a \equiv a$ (*refleksivitāte*),
2. ja $a \equiv b$, tad $b \equiv a$ (*simetrija*),
3. ja $a \equiv b$ un $b \equiv c$, tad $a \equiv c$ (*tranzitivitāte*).

PIERĀDĪUMS $m|a-a$.

Ja $m|a-b$, tad $a-b=qm$ un $b-a=(-q)m$, tāpēc $m|b-a$.

Ja $m|a-b$ un $m|b-c$, tad $a-b=qm$ un $b-c=q'm$. Saskaitot šīs vienādības, iegūsim $a-c=(q+q')m$, tāpēc $m|a-c$.

■

1.2. Atkārtojums - ekvivalences attiecība un tās īpašības, faktorkopa

1.2.1. Attiecības definīcija

Attiecība - īpašība, kas piemīt vai nepiemīt sakārtotai vienas vai vairāku kopu elementu virknei (var lietot arī terminu *attieksme*).

Binära attiecība - īpašība, kas piemīt vai nepiemīt kopas (vai divu dažādu kopu) sakārtotiem elementu pāriem. Parasti pēc noklusēšanas termins "attiecība" nozīmē "binära attiecība".

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

Tātad attiecība definē kādu apakškopu R kopā $A \times B$: ja $x\rho y$, tad $(x, y) \in R$, pretējā gadījumā - $(x, y) \notin R$.

Bināru attiecību starp kopu A un B elementiem var identificēt ar $A \times B$ apakškopu R.

Ja $A = B$, tad bināru attiecību sauc par bināru attiecību kopā A. Biežāk tiek izmantotas attiecības vienā kopā.

Attiecību ρ, kas atbilst apakškopai $R \subseteq A \times B$ apzīmēsim ar pierakstu $\rho = (A, B, R)$ $(\rho = (A, R))$.

Kopu R sauc par attiecības *grafiku*.

Strādājot ar konkrētām attiecībām, burta ρ vietā izmanto dažādus konkrētus atdalošos simbolus, piemēram

$$<, =, \equiv, |$$

un citus.

1.2. piemērs. Attiecību piemēri:

- reālu skaitļu vienādība $\rho =\!=$,
- reālo skaitļu sakārtojums $\rho =\!\leq$, jeb attiecība "mazāks vai vienāds",
- veselo skaitļu dalāmības attiecība $\rho = |$,
- kopu ietilpšanas attiecība $\rho =\!\subseteq$,
- apakšprogrammu izsaukšanas attiecība visu dotās programmas apakšprogrammu kopā,
- trijstūru līdzības attiecība.

1.2.2. Attiecību speciālgadījumi

Attiecību ρ sauksim par *refleksīvu*, ja katram $a \in A$ izpildās nosacījums $a\rho a$. Refleksīvu attiecību piemēri: skaitļu vienādība, ģeometrisku figūru vienādība un līdzība.

Attiecību ρ sauksim par *simetrisku*, ja jebkuriem diviem $a \in A$ un $b \in A$ izpildās šāds nosacījums: ja $a\rho b$, tad $b\rho a$. Simetrisku attiecību piemēri: skaitļu vienādība, figūru līdzība.

Attiecību sauc par *tranzitīvu*, ja jebkuriem trīs elementiem a, b un c (ne obligāti dažādiem) izpildās nosacījums: ja $a\rho b$ un $b\rho c$, tad $a\rho c$. Tranzitīvu attiecību piemēri: skaitļu attiecība "mazāks", skaitļu dalāmības attiecība, ģeometrisku figūru līdzības attiecība.

1.2.3. Ekvivalences attiecība un sadalījumi

Attiecību sauc par *ekvivalenci*, ja tā ir

1. refleksīva,
2. simetriska un
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:

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

Ievērosim, ka jebkurām divām sadalījuma apakškopām A_α un A_β vai nu $A_\alpha \bigcap A_\beta = \emptyset$, vai arī $A_\alpha = A_\beta$.

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. Pāreju no A uz $\aleph$ matemātikā izmanto bieži. Šādu pāreju sauc par A *faktorizāciju*, $\aleph$ sauc par A *faktorkopu*.

Katram $a \in A$ ir definēta tā iekļaušanas funkcija $i : \{a\} \to A$, kas objektam a piekārto viņu pašu kā A elementu.

1.3. teorēma. Jebkurai kopai A pastāv bijekcija starp ekvivalencēm, kas uzdotas kopā A un kopas A sadalījumiem.

PIERĀDĪJUMS Ja ir dots kopas A sadalījums $\aleph = \{A_\alpha\}_{\alpha \in I}$, tad definēsim tam atbilstošu ekvivalenci $\equiv_\aleph$ šādā veidā: $a \equiv_\aleph b$ tad un tikai tad, ja a un b pieder vienai un tai pašai sadalījuma $\aleph$ apakškopai A_β.

Pierādīsim, ka katram sadalījumam definētā attiecība tiešām ir ekvivalence:

1. refleksivitāte - katram a izpildās $a \in \pi_\aleph(i(a))$,
2. simetrija - ja $a \equiv_\aleph b$, tad $a \in A_\gamma$ un $b \in A_\gamma$ un $b \equiv_\aleph a$,
3. tranzitivitāte - ja $a \equiv_\aleph b$ un $b \equiv_\aleph c$, tad $\{a, b\} \in A_\gamma$ un $\{b, c\} \in A_\delta$, bet $A_\gamma \bigcap A_\delta = \emptyset$ vai $A_\gamma \bigcap A_\delta$, tātad $A_\gamma = A_\delta$ un $a \equiv_\aleph c$.

No otras puses, pieņemsim, ka ir dota ekvivalence $\equiv$ un parādīsim, ka šādai attiecībai vviennozīmīgi piekārtot kopas A sadalījumu.

Katram $a \in A$ definēsim $A_a = \{x \in A | x \equiv a\}$. Katram a izpildās $a \equiv a$, tātad $A_a \neq \emptyset$ un $\bigcup_{a \in A} A_a = A$.

Pierādīsim vēl, ka ja $A_a \neq A_b$, tad $A_a \bigcap A_b = \emptyset$. Ja $A_a \bigcap A_b \neq \emptyset$, tad eksistē $c \in A$ tāds, ka $c \in A_a$ un $c \in A_b$, no kā seko, ka $c \equiv a$,

$c \equiv b$ un tāpēc $a \equiv b$.

Pieņemsim, ka eksistē $x \in A_a$ tāds, ka $x \notin A_b$, tad iegūstam, ka $x \equiv a$ un $x \not\equiv b$. Tā kā $a \equiv b$, tad no attiecības tranzitivitātes seko, ka $x \equiv b$, kas ir pretruna.

Līdzīgā veidā iegūsim pretrunu, ja pieņemsim, ka eksistē $x \in A_b$ tāds, ka $x \notin A_a$.■

Par elementam $a \in A$ atbilstošo *ekvivalences klasi* (vai vienkārši *klasi*) attiecībā uz ekvivalences attiecību $\equiv$ ar projekcijas funkciju π sauksim A apakškopu $\pi(a)$ - visu to A elementu kopu, kas ir salīdzināmi ar a.

1.3. Salīdzināmības pēc moduļa m attiecības klases

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

1.3. piemērs. Piemēram, ja $m = 2$, tad $\mathbb{Z} = C_0 \bigcup C_1$, kur C_0 ir 0 klase - pāra skaitļi un C_1 ir 1 klase - nepāra skaitļi.

Ja $m = 3$, tad $\mathbb{Z} = C_0 \bigcup C_1 \bigcup C_2$, 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 $3k + 2$.

1.4. teorēma. Atlikumu klašu skaits pēc moduļa 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 *klašu pārstāvju kopu*. 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:

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

Atlikuma klasi pēc moduļa m, kas atbilst skaitlim r, bieži apzīmē kā $m\mathbb{Z} + r$. Tādējādi var domāt, ka

$$\mathbb{Z}/m\mathbb{Z} = \{m\mathbb{Z}, m\mathbb{Z} + 1, ..., m\mathbb{Z} + (m-1)\}.$$

Atlikumu klašu sadalījums (faktorkopa) pēc moduļa m, kuru parasti

apzīmē ar pierakstu $\mathbb{Z}/m\mathbb{Z}$ definē sirjektīvu funkciju - dabisko projekciju

$$\pi_m : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z},$$

kas katram skaitlim piekārto to atlikumu klasi, kurai tas pieder. Skaitlim n atlikumu klasi $\pi_m(n) = \overline{n}$ sauksim par n *redukciju pēc moduļa* m.

1.5. teorēma.

1. ja $a = b$, tad jebkuram m izpildās $a \equiv b$ (mod m),
2. $a \equiv b$ (mod m) tad un tikai tad, ja $b \equiv a$ (mod (-m)),
3. ja $m = \pm 1$, tad jebkuriem diviem skaitļiem a un b izpildās $a \equiv b$ (mod m),
4. ja $m = 0$, tad $a \equiv b$ (mod m) tad un tikai tad, ja $a = b$,
5. ja $m'|m$, tad no tā, ka $a \equiv b$ (mod m) seko $a \equiv b$ (mod m'),
6. ja $a \equiv b$ (mod m) un $a \equiv b$ (mod m'), tad $a \equiv b$ (mod MKD(m,m'))

PIERĀDĪJUMS

1. acīmredzami;
2. ja $a \equiv b$ (mod m), tad $a - b = qm = (-q)(-m)$, un otrādi,
3. $a - b = (a - b) \cdot 1 = (b - a)(-1)$,
4. tā kā ar nulli nedalās nekāds nenulles skaitlis, tad $0|a-b$ nozīmē, ka $a = b = 0$,
5. ja $m|a - b$ un $m'|m$, tad saskaņā ar dalāmības tranzitivitāti $m'|a - b$,

6. katram pirmskaitlim p, kas piedalās m un m' faktorizācijās, $a-b$ dalās ar tā augstāko kārtu attiecībā uz m vai m', tā kā divu pirmskaitļu pakāpes ir savstarpēji pirmskaitļi, tad no tā, ka $a-b=q_1p_1^{\alpha_1}$ un $a-b=q_2p_2^{\alpha_2}$ ir seko, ka $p_1^{\alpha_1}p_2^{\alpha_2}|a-b$, turpinot šādu secinājumu virkni uz visiem pirmskaitļiem, iegūsim, ka $MKD(m,m')|a-b$.

■

1.2. piezīme. Teorēmas 1.apgalvojuma apgrieztā forma: ja eksistē vesels skaitlis m tāds, ka $a \not\equiv b \pmod{m}$, tad $a \neq b$. Šī forma ir lietderīga risinot vienādojumus veselos skaitļos.

2. Operācijas ar atlikumu klasēm

2.1. Aritmētiskās operācijas un salīdzināmība pēc moduļa m

2.1. teorēma. Ja $a \equiv b \pmod{m}$ un $a' \equiv b' \pmod{m}$, tad

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

un

$$aa' \equiv bb' \pmod{m}.$$

PIERĀDĪJUMS Saskaitīšana. Ja $m|a-b$ un $m|a'-b'$, tad $m|(a-b)+(a'-b')$. Bet $(a-b)+(a'-b') = (a+a')-(b+b')$, tātad $m|(a+a')-(b+b')$.

Reizināšana. Apskatīsim starpību $aa' - bb'$:

$$aa' - bb' = aa' - ab' + ab' - bb' = a(a'-b') + b'(a-b).$$

Tā kā $m|a-b$ un $m|a'-b'$, tad $m|aa'-bb'$.■

2.2. teorēma. Ja $f(x)$ ir polinoms ar veseliem koeficientiem, tad katram $m \in \mathbb{Z}$ no $a \equiv b \pmod{m}$ seko

$$f(a) \equiv f(b) \pmod{m}.$$

PIERĀDĪJUMS Izmantosim matemātisko indukciju pēc polinoma pakāpes n. Ja $n = 0$, tad polinoms ir konstante un nekas nav jāpierāda.

Pieņemsim, ka teorēma ir pierādīta polinomiem ar pakāpi i un pierādīsim, ka tad tā ir patiesa polinomiem ar pakāpi $i+1$. Ja $a \equiv b$, tad

$$a^{i+1} = a^i a \equiv b^i b = b^{i+1}.$$

Jebkuram c izpildās arī $ca^{i+1} \equiv cb^{i+1}$. Pieņemsim, ka $f(x) = cx^{i+1} + g(x)$, kur $g(x)$ ir polinoms ar pakāpi i. Redzam, ka

$$f(a) = ca^{i+1} + g(a) \equiv cb^{i+1} + g(b),$$

jo pirmie un otrie locekļi ir pa pāriem salīdzināmi: $ca^{i+1} \equiv cb^{i+1}$ (tika pierādīts) un $g(a) \equiv g(b)$ (pēc indukcijas pieņēmuma). ■

2.1. piezīme. Pierādītā teorēma kopā ar 1.5.teorēmas 1.punkta kontrapozitīvo apgalvojumu (ja eksistē m tāds, ka izpildās nosacījums $a \not\equiv b \pmod{m}$, tad $a \neq b$) ir viens no vienkāršākajiem un efektīvākajiem veidiem kā pierādīt, ka vienādojumam vai vienādojumu sistēmai neeksistē atrisinājums veselos skaitļos - ja ir iespējams atrast veselu skaitli m, tādu, ka 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.

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

2.2. Operācijas ar atlikumu klasēm un to īpašības

Fiksēsim skaitli m. Par divu atlikumu klašu (pēc moduļa m) C un C' summu $C+C'$, sauksim klasi $\pi_m(a+a')$, kur $a \in C$ un $a' \in C'$. Par divu atlikumu klašu C un C' reizinājumu CC', sauksim klasi $\pi_m(aa')$, kur $a \in C$ un $a' \in C'$.

2.3. teorēma.

1. Atlikuma klašu operācijas ir definētas korekti - nav atkarīgas no pārstāvju izvēles,
2. $C + C' = C' + C$
3. $CC' = C'C$
4. $(C + C') + C'' = C + (C' + C'')$,
5. $(CC')C'' = C(C'C'')$,
6. $C(C' + C'') = CC' + CC''$,
7. $0 + C = C + 0 = C$,
8. $1 \cdot C = C$.

PIERĀDĪJUMS Korektums seko no iepriekš pierādītās 2.1.teorēmas. Pārējie teorēmas punkti seko no saskaitīšanas un reizināšanas īpašībām. ■

Atlikumu kopu pēc moduļa m ar tajā uzdotām saskaitīšanas un reizināšanas operācijām sauksim par *atlikumu gredzenu pēc moduļa* m un parasti arī apzīmē ar pierakstu $\mathbb{Z}/m\mathbb{Z}$, aprēķinos parasti pieņem, ka $m > 0$. Atlikumu klašu vienādību apzīmēsim ar simbolu $\equiv$.

Atlikumu klašu pārstāvju kopu pēc moduļa m ir pieņemts izvēlēties kā $\{\overline{0}, ..., \overline{m-1}\}$.

2.2. piemērs. Atlikumu klases pēc moduļa 5 var identificēt ar kopu $\{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$.

Redzam, ka pēc moduļa 5 izpildās šādas vienādības:

$2 + 3 \equiv 0$, $2 \cdot 3 \equiv 1$,

$3 + 3 \equiv 1$, $3 \cdot 3 \equiv 4$. u.t.t.

2.4. teorēma. Katram m un visiem veseliem skaitļiem a un b ir spēkā sakarības $\pi_m(a+b) = \pi_m(a) + \pi_m(b)$ un $\pi_m(ab) = \pi_m(a)\pi_m(b)$.

PIERĀDĪJUMS Ja $a = q_1 m + r_1$ un $b = q_2 m + r_2$, tad

$$a + b = (q_1 + q_2)m + (r_1 + r_2)$$

un

$$ab = q_1 q_2 m^2 + (q_1 + q_2)m + r_1 r_2,$$

tātad $a + b \equiv r_1 + r_2$ un $ab \equiv r_1 r_2$. Tā kā $\pi_m(a) \equiv r_1$ un $\pi_m(b) \equiv r_2$, tad apgalvojums ir pierādīts.■

3. 4.mājasdarbs

1. Atrodiet atlikumus pēc dotā moduļa:
   a) $10!(\text{mod } 7)$,
   b) $100^{100}(\text{mod } 13)$,
2. Atrodiet saskaitīšanas un reizināšanas tabulas atlikumu klasēm pēc moduļa 7 un 8. Uzrādiet visus elementus, kuriem eksistē multiplikatīvi inversie elementi.
3. Atrisiniet vienādojumus atlikumu klasēs:
   a) $x^3 + x + 1 \equiv (\text{mod } 7)$,
   b) $x^3 + y^2 \equiv 2(\text{mod } 5)$.
4. Pierādiet, ka visiem naturāliem skaitļiem n izpildās
$$1 + 2^{2^n} + 2^{2^{n+1}} \equiv 0(\text{mod } 7).$$
5. Pierādiet, ka vienādojumam
$$x^2 - 2 = 5y^2$$
nav veselu atrisinājumu.