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

Studiju kurss

SKAITĻU TEORIJA

1.lekcija

Docētājs: Dr. P. Daugulis

2012./2013.studiju gads

Saturs

Lekcijas mērķis:

- apgūt veselo skaitļu dalāmības pamatus,
- apgūt Eiklīda algoritmu lielākā kopīgā dalītāja atrašanai.

Lekcijas kopsavilkums:

- veselo skaitļu kopā var definēt un pētīt dalāmības attiecību,
- eksistē algoritms (Eiklīda algoritms), ar kuru var atrast skaitļu lielāko kopīgo dalītāju.

Svarīgākie jēdzieni: naturālie skaitļi, veselie skaitļi, dalāmība, kopīgie dalītāji, pirmskaitlis, salikts skaitlis, lielākais kopīgais dalītājs, savstarpējie pirmskaitļi.

Svarīgākie fakti un metodes: pilnīgā sakārtojuma princips, maksimālā elementa princips, aritmētiskās pamatīpašības, veselo skaitļu dalīšana ar atlikumu, dalāmības īpašības, LKD pamatīpašības, Eiklīda algoritms.

1. Veselo skaitļu pamatīpašības

1.1. Skaitļu kopas

1.1.1. Naturālie un veselie skaitļi

Naturālie skaitļi ($\mathbb{N}$):

- skaitļi, ko var iegūt dabiskā skaitīšanas ceļā $1, 2, 3...$;
- dabiskās *aritmētiskās operācijas* - *saskaitīšana*, *atņemšana*, *reizināšana*, *dalīšana;*
- naturālo skaitļu kopā var dabiski definēt sakārtojuma attiecību $<$: $x < y$, ja starpība $y - x$ ir definēta kā naturāls skaitlis;
- problēma - naturālo skaitļu kopa *nav slēgta* attiecībā uz atņemšanu un dalīšanu (piemēram, $1 - 2 \notin \mathbb{N}$, $1/2 \notin \mathbb{N}$);
- ģeometriskā interpretācija - garums (piemēram, soļu skaits).

Laika gaitā izmantojamo, "pieņemamo" skaitļu kopa tika paplašināta vairākos soļos (vairāku tūkstošu gadu periodā) saglabājot arit-

mētisko operāciju īpašības.

Veselie skaitļi ($\mathbb{Z}$):

- - divu naturālu skaitļu starpības rezultāts, piemēram

$$-1 = 2 - 3, 0 = 3 - 3.$$

  Veselos skaitļus iegūst no naturālajiem, pievienojot visas formālās starpības.

- $\mathbb{Z}$ ir slēgta attiecībā uz saskaitīšanu un atņemšanu - divu veselu skaitļu summa un starpība ir vesels skaitlis. $\mathbb{Z}$ nav slēgta attiecībā uz dalīšanu ($\frac{1}{2} \notin \mathbb{Z}$).
- ģeometriskā interpretācija - orientētais garums, skaitļu ass punkti ar veselām koordinātēm.

1.1.2. Veselo skaitļu kopas paplašinājumi

Racionālie skaitļi $\mathbb{Q}$ - formāls divu veselu skaitļu pāris - dalījums $\frac{m}{n}$, kur $m, n \in \mathbb{Z}$, $n \neq 0$.

Algebriskie skaitļi $\overline{\mathbb{Q}}$ - reālas saknes algebriskiem vienādojumiem ar racionāliem koeficientiem, piemēram, $\sqrt{2}$ ir sakne vienādojumam

$$x^2 = 2.$$

Reālie skaitļi $\mathbb{R}$ - algebrisko skaitļu kopas paplašināšana pievienojot visas konverģējošu racionālu vai algebrisku skaitļu virkņu robežas.

Reālos skaitļus var interpretēt kā punktus uz taisnes.

Reālo skaitļu kopā var arī dabiskā veidā vispārināt naturālo skaitļu sakārtojuma attiecību $\leq$.

Pastāv kopu iekļaušanas $\mathbb{N} \subsetneq \mathbb{Z} \subsetneq \mathbb{Q} \subsetneq \overline{\mathbb{Q}} \subsetneq \mathbb{R} \subsetneq \mathbb{C}$.

1.2. $\mathbb{N}$ un $\mathbb{Z}$ pamatīpašības

1.1. teorēma. ($\mathbb{N}$ *pilnīgā sakārtojums princips)* $\forall$ $\mathbb{N}$ *apakškopa satur vismazāko elementu.*

1.2. teorēma. ($\mathbb{N}$ *maksimālā elementa princips*) $\forall$ $\mathbb{N}$ apakškopa, kas ir ierobežota no augšas, satur maksimālo elementu.

1.3. teorēma. ($\mathbb{Z}$ aritmētiskās pamatīpašības)

1. divu veselu skaitļu summa un reizinājums ir vesels skaitlis,
2. $a + b = b + a$ (saskaitīšanas komutativitātes likums),
3. $ab = ba$ (reizināšanas komutativitātes likums),
4. $(a + b) + c = a + (b + c)$ (saskaitīšanas asociativitātes likums),
5. $(ab)c = a(bc)$ (reizināšanas asociativitātes likums),
6. $a + 0 = a$ (saskaitīšanas neitrālā elementa eksistence),
7. $a+x = a \implies x = 0$ (saskaitīšanas neitrālā elementa vienīgums),
8. $a \cdot 1 = a$ (reizināšanas neitrālā elementa eksistence),

9. $ax = a \implies x = 1$ (reizināšanas neitrālā elementa vienīgums),
10. $a(b + c) = ab + ac$ (distributivitātes likums),
11. $ab = 0 \implies a = 0 \ \vee \ b = 0$ (nulles dalītāju neeksistence),
12. $\left\{ \begin{array}{l} a \neq 0 \\ ab = ac \end{array} \right. \implies b = c$ (reizināšanas saīsināšanas īpašība).

1.3. Veselo skaitļu dalīšana ar atlikumu

1.4. teorēma. $\forall\ a \in \mathbb{Z}$, $a \neq 0$ un $\forall\ b \in \mathbb{Z}$ $\exists$ tieši viens veselu skaitļu pāris $(q, r) \in \mathbb{Z}^2$, kur $0 \leq r < |a|$, tāds, ka

$$\boldsymbol{b = qa + r.}$$

(q - dalījums, r - atlikums).

PIERĀDĪJUMS

Atzīmēsim uz taisnes ar Dekarta koordinātēm visus punktus, kuru koordinātes ir vienādas ar ka, kur $k \in \mathbb{Z}$.

$\forall\ b \in \mathbb{Z}$ ir viennozīmīgi izsakāms formā

$$b = qa + r,$$

kur qa ir pirmais atzīmētais punkts pa kreisi no b un $0 \leq r < |a|$. ■

1.1. piezīme. Seko, ka ir korekti definēta *pilnās redukcijas* vai atlikuma funkcija

$$\rho_a(b) = atl(b, a) = b - qa = r.$$

2. Veselo skaitļu dalāmība

2.1. Dalāmības pamatīpašības

$a \in \mathbb{Z}$ *dala* $b \in \mathbb{Z}$ vai, b *dalās ar* a $(a|b)$ tad un tikai tad, ja $\exists\, q \in \mathbb{Z}$:

$$\boldsymbol{b = qa.}$$

Citiem vārdiem sakot, atlikums dalot b ar a ir vienāds ar 0:

$$\boldsymbol{b = qa + 0.}$$

Ja $a|b$, tad b sauc par a *daudzkārtni.*

Ja a nedala b, tad to apzīmē ar pierakstu $a \nmid b$.

Svarīgs speciālgadījums: ja $2|a$, tad a - *pāra skaitlis*, ja $2 \nmid a$, tad a - *nepāra skaitlis.*

2.1. piemērs. $\forall\ a:\ \ a|0.\ \ 0|a \implies a = 0.$ ± 1 dala visus veselos skaitļus, ± 1 dalās tikai ar ± 1.

2.1. teorēma. (dalāmības īpašības kopā $\mathbb{Z}$)

1. $\forall a:\ a|a$ (*refleksivitāte*).
2. $\forall\ a,b,c: \begin{cases} a|b \\ b|c \end{cases} \implies a|c$ (*tranzitivitāte*).
3. $\forall a,b: \begin{cases} a|b \\ b|a \end{cases} \iff |a| = |b|.$
4. $\forall\ a,b,b \neq 0:\ a|b \implies |a| \leq |b|.$
5. $\forall\ a,b,b': \begin{cases} a|b \\ a|b' \end{cases} \implies a|(b+b').$
6. $\forall\ a,b,c:\ a|b \implies a|bc.$
7. $\forall\ a,b,c,d: \begin{cases} a|b \\ c|d \end{cases} \implies ac|bd.$

PIERĀDĪJUMS

1. $a = 1 \cdot a.$

2. $\left\{ \begin{array}{l} a|b \\ b|c \end{array} \right. \Longrightarrow \left\{ \begin{array}{l} b = qa \\ c = q'b \end{array} \right. \Longrightarrow c = q'b = (q'q)a \Longrightarrow a|c.$

3. $\left\{ \begin{array}{l} a|b \\ b|a \end{array} \right. \Longrightarrow \left\{ \begin{array}{l} b = qa \\ a = q'b \end{array} \right. \Longrightarrow b = qa = (qq')b \Longrightarrow$

$$qq' = 1 \Longrightarrow q = \pm 1 \Longrightarrow a = \pm b.$$

4. $a|b \Longrightarrow b = qa \Longrightarrow |b| = |q||a| \Longrightarrow \dfrac{|b|}{|a|} = |q| \geq 1 \Longrightarrow$

$|b| \geq |a|.$

5. $\left\{ \begin{array}{l} a|b \\ a|b' \end{array} \right. \Longrightarrow \left\{ \begin{array}{l} b = qa \\ b' = q'a \end{array} \right. \Longrightarrow b+b' = qa+q'a = (q+q')a \Longrightarrow$

$$a \Big| b + b'.$$

6. $a|b \implies b = qa \implies bc = (qc)a.$

7.
$$\left\{ \begin{array}{l} a|b \\ c|d \end{array} \right. \implies \left\{ \begin{array}{l} b = q_1 a \\ d = q_2 c \end{array} \right. \implies bd = (q_1 a)(q_2 c) = (q_1 q_2)(ac). \blacksquare$$

2.1. piezīme. Naturālo skaitļu dalāmības attiecību var attēlot ar *Hasses grafu*, kas tiek definēts šādi:

- virsotnes ir naturālie skaitļi,
- divas virsotnes a un b ir savienotas ar šķautni $a \leftarrow b$, ja $a|b$ un neeksistē skaitlis $c, a < c < b$ tāds, ka $a|c$ un $c|b$.

2.2. Kopīgie dalītāji

Skaitļa $b \in \mathbb{Z}$ dalītāju kopa - $D(b)$.

2.2.1. Dalītāju īpašības

2.2. teorēma.

1. $D(0) = \mathbb{Z}$.
2. $D(-b) = D(b)$.
3. $b \neq 0 \implies |D(b)| < \infty$.
4. $D(b)$ maksimālais elements ir vienāds ar $|b|$, minimālais - ar $-|b|$.

PIERĀDĪJUMS

1.$\forall\ x \in \mathbb{Z}$: $x|0$.

2. $x|b \iff x|(-b)$.

3.,4. $\left\{ \begin{array}{l} x|b \\ b \neq 0 \end{array} \right. \implies \left\{ \begin{array}{l} b = qx \\ q \neq 0, x \neq 0 \end{array} \right. \implies x = \frac{b}{q} \implies |x| \leq |b|.$

■

2.2.2. Pirmskaitļi

Skaitli $p \in \mathbb{N}$ sauc par *pirmskaitli*, tā vienīgie pozitīvie dalītāji ir 1 un p. Visu pirmskaitļu kopu apzīmē ar $\mathbb{P}$.

Naturālu skaitli, kas nav pirmskaitlis un nav vienāds ar 1, sauc par *saliktu skaitli*.

2.2. piemērs. $2, 3, 5, 7, 11, 13$ ir pirmskaitļi. $4 = 2 \times 2$ nav pirmskaitlis.

2.2.3. Kopīgie dalītāji

$a \in \mathbb{Z}$ ir kopas $\{b_1, ..., b_m\} \subseteq \mathbb{Z}$ *kopīgs dalītājs*, ja $\forall\ i\ a|b_i$.

$\{b_1, ..., b_m\}$ visu kopīgo dalītāju kopu apzīmē ar $D(b_1, ..., b_m)$.

Kopas $D(b_1, ..., b_n)$ maksimālo (pozitīvo) elementu sauc par *lielāko kopīgo dalītāju* un apzīmē ar $LKD(b_1, ..., b_n)$.

$D(b_1, ..., b_n)$ un $LKD(b_1, ..., b_n)$ nav atkarīgi no elementu $b_1, ..., b_n$ kārtības.

$\{b_1, ..., b_n\}$ - *savstarpēji pirmskaitļi*, ja $LKD(b_1, ..., b_n) = 1$.

2.3. piemērs. $LKD(2, 4) = 2$. $LKD(12, 18) = 6$.

2.3. teorēma.

1. $\forall\, b \in \mathbb{Z}:\ LKD(b) = LKD(b, 0) = |b|$.
2. $\forall\, a, b \in \mathbb{Z}:\ a|b \implies \begin{cases} D(a, b) = D(a) \\ LKD(a, b) = |a|. \end{cases}$
3. $\forall\, a, b, k \in \mathbb{Z}: \begin{cases} D(a, b) = D(a - kb, b), \\ LKD(a, b) = LKD(a - kb, b). \end{cases}$

PIERĀDĪJUMS

1. $D(b, 0) = D(b) \cap D(0) = D(b) \cap \mathbb{Z} = D(b) \implies$

$$LKD(b, 0) = LKD(b) = |b|.$$

2. $a|b \implies \Big(x|a \implies x|b\Big) \implies D(a) \subseteq D(b) \implies$

$$D(a,b) = D(a) \cap D(b) = D(a) \implies LKD(a,b) = |a|.$$

3. $x \in D(a,b) \implies \begin{cases} x|a \\ x|b \end{cases} \implies x|a - kb \implies$

$x \in D(a - kb, b) \implies \boxed{D(a,b) \subseteq D(a - kb, b).}$

$x \in D(a - kb, b) \implies \begin{cases} x|a - kb \\ x|b \end{cases} \implies x|(a - kb) + kb \implies$

$x|a \implies x \in D(a,b) \implies \boxed{D(a - kb, b) \subseteq D(a,b)} \implies$

$$\boxed{D(a,b) = D(a - kb, b).}$$

$D(a,b) = D(a - kb, b) \implies LKD(a,b) = LKD(a - kb, b)$ ■

2.2. piezīme. Teorēmas 3.apgalvojums norāda uz to, ka meklējot $LKD(a,b)$ var aizvietot a ar *redukciju* $a - kb = atl(a,b) = \rho_b(a)$ (tā, lai $a - kb$ ir minimāls un nenegatīvs).

2.3. piezīme. Pārveidojumu $(a, b) \to (a - kb, b)$ ērti ir uzdot kolonnu formā

$$\left[\begin{array}{c} b \\ \hline a \end{array}\right] \to \left[\begin{array}{c} b \\ \hline a - kb \end{array}\right]$$

un interpretēt kā REP3 $R_{12}(-k) = \underbrace{R_{12}(-1)...R_{12}(-1)}_{k \text{ reizes}} = R_{12}(-1)^k$.

2.3. Eiklīda algoritms (divu skaitļu LKD atrašanai)

2.3.1. Algoritms

Meklēsim naturālu skaitļu a un b LKD, $a > b$. Sākam ar pāri (a, b) vai kolonnas matricu $\left[\begin{array}{c} a \\ \hline b \end{array}\right]$.

Vispārīgās idejas:

- ja ir dots skaitļu pāris $\{a, b\}$, kur $a > b$, tad pārejot uz "mazāku" pāri - veicot redukciju

$$\begin{bmatrix} a \\ b \end{bmatrix} \to \begin{bmatrix} atl(a,b) \\ b \end{bmatrix}$$

dalītāju kopas, un tāpēc arī LKD saglabāsies,

- šādu soli var atkārtot vairākas reizes, kamēr iegūsim mazus skaitļus.

Eiklīda algoritms

- Sākot ar pāri (a, b) vai kolonnas matricu $\begin{bmatrix} a \\ b \end{bmatrix}$ veicam pilno redukciju virkni - reducējam lielāko skaitli ar mazāko, kamēr kārtējais redukcijas rezultāts nav 0.
- Ja ir veikti n soļi, tad algoritma izpildes rezultātā tiek iegūta skaitļu pāru/kolonnu virkne

$$\begin{bmatrix} a \\ b \end{bmatrix}, \begin{bmatrix} r_1 \\ b \end{bmatrix}, \begin{bmatrix} r_1 \\ r_2 \end{bmatrix}, ..., \begin{bmatrix} r_{n-1} \\ 0 \end{bmatrix}.$$

- Virkne $r_1, r_2, ...$ ir stingri dilstoša, tāpēc šī algoritma realizācijā soļu skaits ir galīgs.

2.3.2. Algoritma pareizības pierādījums

2.4. teorēma. Pieņemsim, ka tiek realizēts Eiklīda algoritms ar sākuma datiem (a, b), kur $a > b > 0$, $b \nmid a$, tiek veikti n soļi, pēdējais nenulles atlikums ir r_{n-1}.

1. $D(a, b) = D(r_{n-1})$.
2. $LKD(a, b) = r_{n-1}$.

PIERĀDĪJUMS

$$D(a, b) = D(b, r_1) = D(r_1, r_2) = ... = D(r_{n-1}, 0) = D(r_{n-1}).$$

un

$$LKD(a, b) = LKD(b, r_1) = ... = LKD(r_{n-1}, 0) = r_{n-1}.\blacksquare$$

2.4. piemērs. Atradīsim $LKD(87, 13)$ izmantojot Eiklīda algoritmu.

1. $87 = 6 \cdot 13 + 9$, $\left[\frac{87}{13}\right] \to \left[\frac{9}{13}\right]$.

2. $13 = 1 \cdot 9 + 4$, $\left[\frac{9}{13}\right] \to \left[\frac{9}{4}\right]$.

3. $9 = 2 \cdot 4 + 1$, $\left[\frac{9}{4}\right] \to \left[\frac{1}{4}\right]$.

4. $4 = 4 \cdot 1$, $\left[\frac{1}{4}\right] \to \left[\frac{1}{0}\right]$.

$\Longrightarrow$ $LKD(87, 13) = 1$.

2.4. piezīme. Ņemot vērā īpašību $D(-a) = D(a)$, Eiklīda algoritmu var izmantot veselu, ne obligāti pozitīvu, skaitļu LKD atrašanai.

2.5. piezīme. Eiklīda algoritmu var veikt arī "lēnāk" - veicot reducijas, kas ir ne obligāti pilnas.

3. 1.mājasdarbs

3.1. Obligātie uzdevumi

1.1 Izdalīt ar atlikumu dotos veselo skaitļu pārus:

(a) 324 ar -19,
(b) 293742983472983 ar 3792.

1.2 Atrast

(a) visus naturālos skaitļus, kas dala 168,
(b) visus naturālos skaitļus intervālā $[500, 1000]$, kas dalās ar 168.

1.3 Atrast

(a) visus pirmskaitļus starp 100 un 200,
(b) visus veselus skaitļus starp 100 un 200, kas ir ne vairāk kā divu pirmskaitļu pakāpju reizinājumi (piemēram, $100 = 2^2 5^2$).

1.4 Dots, ka $5|3a + 2b$ un $5|a - 3b$. Pierādīt, ka $5|9a - b$.

1.5 Atrast LKD izmantojot Eiklīda algoritmu.
(a) $LKD(2813, 92)$,
(b) $LKD(377, 233)$,
(c) $LKD(39n + 29, 24n + 18)$, $\forall\, n \in \mathbb{Z}$.

3.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi

1.6 Ar kādām $n \in \mathbb{N}$ vērtībām dotās daļas ir saīsināmas?
(a) $\dfrac{n^2 + n + 1}{n^2 + 1}$,
(b) $\dfrac{n^2 + 2n - 2}{n^2 + n + 1}$.

1.7 Pierādīt: ja $LKD(m, n) = 1$, tad $LKD(m+n, m^2+n^2) \in \{1, 2\}$.