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

Studiju kurss

Veselo skaitļu teorija

1.lekcija

Docētājs: Dr. P. Daugulis

2009./2010.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, matemātiskās indukcijas 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 ($\mathbb{N}$) un to pamatīpašības:

- skaitļi, ko var iegūt dabiskā skaitīšanas ceļā $1, 2, 3...$;
- dabiskās darbības (*aritmētiskās operācijas*) ar naturālajiem skaitļiem - *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, $1 - 2 \notin \mathbb{N}$, $1/2 \notin \mathbb{N}$);
- naturālā skaitļa ģeometriskā interpretācija - garums (piemēram, soļu skaits).

Vēsturiski izmantojamo, "pieņemamo" skaitļu kopa tika paplašināta vairākos soļos (vairāku tūkstošu gadu periodā) saglabājot aritmētisko operāciju īpašības.

Veselie skaitļi ($\mathbb{Z}$) un to pamatīpašības:

- - 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 ($\frac{1}{2} \notin \mathbb{Z}$).
- Veselo skaitļu 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 dalījums $\frac{m}{n}$, kur $m, n \in \mathbb{Z}$, $n \neq 0$.

Algebriskie skaitļi $\overline{\mathbb{Q}}$ - reāla sakne algebriskam vienādojumam 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 $\leq$.

1.2. Kopteorētiskās pamatīpašības

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

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

1.3. teorēma. (*Matemātiskās indukcijas princips*) Pieņemsim, ka katram $n \in \mathbb{N}$ ir definēts apgalvojums $P(n)$ un ir spēkā šādi apgalvojumi:

1. $P(1)$ ir patiess,
2. ja $P(i)$ ir patiess, tad $P(i+1)$ ir patiess visiem $i \in \mathbb{N}$.

Tad visiem $n \in \mathbb{N}$ apgalvojums $P(n)$ ir patiess.

1.3. Aritmētiskās pamatīpašības

1.4. teorēma.

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. $\Big(a \neq 0 \ \wedge \ ab = ac\Big) \implies b = c$ (reizināšanas saīsināšanas īpašība).

1.4. Veselo skaitļu dalīšana ar atlikumu

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

$$b = qa + r$$

(q sauksim par *dalījumu*, r - par *atlikumu*, r apzīmē arī kā $atl(b, a)$).

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 $0 \leq r < |a|$. ■

2. Veselo skaitļu dalāmības attiecība

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 $\exists\, q \in \mathbb{Z}$:

$$b = qa.$$

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

$$b = qa + 0.$$

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 sauksim par *pāra skaitli*, ja $2 \nmid a$, tad a ir *nepāra skaitlis.*

Dalāmība definē attiecību $\rho = |$ kopā $\mathbb{Z}$.

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

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

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

PIERĀDĪJUMS

1. $a = 1 \cdot a.$

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

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

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

$$a|b + b'.$$

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

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

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 kopu apzīmēsim ar $D(b)$.

2.2. piezīme. $D(0) = \mathbb{Z}$.
$D(-b) = D(b)$.
$|D(b)| < \infty$, ja $b \neq 0$.
$D(b)$ maksimālais elements ir vienāds ar $|b|$, minimālais - ar $-|b|$.

Skaitli $p \in \mathbb{N}$ sauc par *pirmskaitli*, ja $D(p) \cap \mathbb{N} = \{1, p\}$ - tā vienīgie pozitīvie dalītāji ir 1 un 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.

$a \in \mathbb{Z}$ sauksim par kopas $\{b_1, ..., b_m\} \subseteq \mathbb{Z}$ *kopīgu dalītāju*, ja $\forall\ i$ $a|b_i$. $\{b_1, ..., b_m\}$ visu dalītāju kopu apzīmē ar $D(b_1, ..., b_m)$:

$$D(b_1, ..., b_m) = \bigcap_{i=1}^{m} D(b_i).$$

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

$$LKD(b_1, ..., b_n) = \max\Big(D(b_1, ..., b_n) \cap \mathbb{N}\Big) = \max\Big(D(b_1, ..., b_n)\Big).$$

$D(b_1, ..., b_n)$ un $LKD(b_1, ..., b_n)$ nav atkarīgi no elementu $b_1, ..., b_n$ kārtības, tas seko no šķēluma operācijas komutativitātes.

Skaitļu kopu $\{b_1, ..., b_n\}$ sauksim par *savstarpējiem pirmskaitļiem*, ja $LKD(b_1, ...b_n) = 1$. Tādējādi p ir pirmskaitlis tad un tikai tad, ja $LKD(p, m) = 1$ visiem $1 \leq m < p$.

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

2.2. teorēma.

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

$$D(a,b) = D(a-kb,b) \text{ un } LKD(a,b) = LKD(a-kb,b).$$

PIERĀDĪJUMS

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

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. $x \in D(a,b) \implies \Big(x|a \ \wedge\ x|b\Big) \implies x|a-kb \implies$

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

$$x \in D(a-kb,b) \Longrightarrow \Big(x|a-kb \ \wedge \ x|b\Big) \Longrightarrow x|(a-kb)+kb \Longrightarrow$$

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

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

$$D(a,b) = D(a-kb,b) \Longrightarrow LKD(a,b) = LKD(a-kb,b) \ \blacksquare$$

2.3. Eiklīda algoritms

2.3.1. Algoritms

Meklēsim naturālu skaitļu a un b LKD, $a > b$. Sākam ar pāri (a,b).

Vispārējā ideja: ja ir dots skaitļu pāris $\{u,v\}$, kur $u > v$, tad pāriesim uz "mazāku" pāri $\{\underbrace{atl(u,v)}_{=u-qv}, v\}$ - abiem pāriem ir vienādas

dalītāju kopas, un tāpēc arī LKD.

1. Dalām a ar b:
$$\boxed{a = q_1 b + r_1}.$$
Pārejam uz pāri (b, r_1). $LKD(a, b) = LKD(b, r_1)$. Ja $r_1 = 0$, tad apstājamies, ja nē, tad pārejam uz 2. soli.

2. Dalām b ar r_1:
$$\boxed{b = q_2 r_1 + r_2}.$$
Pārejam uz pāri (r_1, r_2). $LKD(b, r_1) = LKD(r_1, r_2)$. Ja $r_2 = 0$, tad apstājamies, ja nē, tad ejam uz 3. soli.

3. Dalām r_1 ar r_2:
$$\boxed{r_1 = q_3 r_2 + r_3}.$$
Pārejam uz pāri (r_2, r_3). $LKD(r_1, r_2) = LKD(r_2, r_3)$. Ja $r_3 = 0$, tad apstājamies, ja nē, tad ejam uz 4. soli.

.....

i. Dalām r_{i-2} ar r_{i-1}:

$$\boxed{r_{i-2} = q_i r_{i-1} + r_i}.$$

Pārejam uz pāri (r_{i-1}, r_i). $LKD(r_{i-2}, r_{i-1}) = LKD(r_{i-1}, r_i)$. Ja $r_i = 0$, tad apstājamies, ja nē, tad ejam uz soli $i+1$. soli.

.....

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

Ja ir veikti n soļi, tad algoritma izpildes rezultātā tiek iegūta skaitļu pāru virkne

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

2.3.2. Algoritma pareizības pierādījums

2.3. 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
Saskaņā ar iepriekšējo teorēmu

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

un

$$LKD(a,b) = LKD(b,r_1) = LKD(r_1,r_2) = ...$$
$$= LKD(r_{n-2},r_{n-1}) = LKD(r_{n-1},0) = r_{n-1}.$$

■

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

1. $87 = 6 \cdot 13 + 9$, $(87,13) \to (13,9)$.
2. $13 = 1 \cdot 9 + 4$, $(13,9) \to (9,4)$.
3. $9 = 2 \cdot 4 + 1$, $(9,4) \to (4,1)$.
4. $4 = 4 \cdot 1$, $(4,1) \to (1,0)$.

Tātad $LKD(87, 13) = 1$.

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

2.4. teorēma. $LKD(b_1, ..., b_{n-1}, b_n) = LKD(LKD(b_1, ..., b_{n-1}), b_n)$ (pietiek prast atrast divu skaitļu LKD).

PIERĀDĪJUMS

$$D(b_1, ..., b_n) = D(b_1) \cap ... \cap D(b_{n-1}) \cap D(b_n) =$$
$$\Big(D(b_1) \cap ... \cap D(b_{n-1})\Big) \cap D(b_n) = D(b_1, ..., b_{n-1}) \cap D(b_n) =$$
$$D(LKD(b_1, ..., b_{n-1})) \cap D(b_n).$$

$\Longrightarrow$

$$LKD(b_1, ..., b_n) = \max(D(b_1, ..., b_n)) =$$
$$\max(D(LKD(b_1, ..., b_{n-1})) \cap D(b_n)) =$$
$$LKD(LKD(b_1, ..., b_{n-1}), b_n).\blacksquare$$

3. 1.mājasdarbs

3.1. Obligātie uzdevumi

1.1 Izdaliet ar atlikumu dotos veselo skaitļu pārus:
   (a) 324 ar -19,
   (b) 293742983472983 ar 3792.

1.2 Atrodiet visus naturālos skaitļus, kas dala 168.

1.3 Atrodiet visus pirmskaitļus, kas ir mazāki kā 100.

1.4 Dots, ka $7|3a+2b$ un $7|a-3b$. Pierādīt, ka $7|9a-2b$.

1.5 Atrodiet $LKD(2813, 92)$ izmantojot Eiklīda algoritmu.

3.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi

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

(b) $\frac{n^2+2n-2}{n^2+n+1}$.

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