DAUGAVPILS UNIVERSITĀTE
Dabaszinātņu un matemātikas fakultāte
Matemātikas katedra

Daugavpils Universitātes Jauno matemātiķu skola

Veselo skaitļu teorija - 1

Docētājs: Dr. P. Daugulis

2008./2009.studiju gads

Saturs

1. Skaitļu kopas

1.1. Naturālie skaitļi

Naturāls skaitlis - skaitlis, ko var iegūt dabiskā skaitīšanas ceļā

$$\{1, 2, 3...\}$$

Visu naturālo skaitļu kopu apzīmēsim ar $\mathbb{N}$.

Dabiskās darbības (*aritmētiskās operācijas*) ar naturālajiem skaitļiem -

saskaitīšana, atņemšana, reizināšana, dalīšana.

Naturālo skaitļu kopā var dabiski definēt sakārtojuma attiecību $<$. Teiksim, ka $x < y$, ja starpība $y - x$ ir definēta kā naturāls skaitlis.

Naturālā skaitļa ģeometriskā interpretācija - garums (piemēram, soļu skaits).

1.2. Naturālo skaitļu kopas paplašinājumi

Skaitlis 0 tiek definēts kā jebkuras starpības $n - n$ rezultāts, kur $n \in \mathbb{N}$.

Vesels skaitlis - divu naturālu skaitļu starpības rezultāts, piemēram

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

Veselos skaitļus iegūst no naturālajiem, pievienojot visas formālās starpības. Apzīmējums: ja $n \in \mathbb{N}$ un $n + x = 0$, tad x tiek apzīmēts kā $-n$. Visu veselo skaitļu kopu apzīmē ar $(\mathbb{Z}, +, \times)$.

Ievērosim, ka veselo skaitļu kopa ir slēgta attiecībā uz saskaitīšanu un atņemšanu - divu veselu skaitļu summa un starpība ir vesels skaitlis. Ievērosim arī to, ka veselo skaitļu kopa nav slēgta attiecībā uz dalīšanu ($\frac{1}{2} \notin \mathbb{Z}$).

Veselo skaitļu ģeometriskā interpretācija - orientētais garums, skaitļu ass punkti ar veselām koordinātēm.

Nākamais skaitļu kopas paplašināšanas solis - pievienot visus iespējamos dalījumus.

Racionāls skaitlis - formāls divu veselu skaitļu dalījums.Ja $m, n \in \mathbb{Z}$, $n \neq 0$ un $nx = m$, tad apzīmēsim x ar $\frac{m}{n}$. Visu racionālu skaitļu kopu apzīmē ar $\mathbb{Q}$.

2. Veselo skaitļu pamatīpašības

2.1. Kopteorētiskās pamatīpašības

2.1. teorēma. Jebkuriem veseliem skaitļiem x un y ir spēkā tieši viens no šādiem gadījumiem:

$$x = y, \; x < y \text{ vai } x > y.$$

2.2. teorēma. Attiecība $\leq$ ir *tranzitīva*: ja $x \leq y$ un $y \leq z$, tad $x \leq z$.

2.3. teorēma. (*Pilnīgā sakārtojums princips*) *Jebkura kopas* $\mathbb{N}$ *apakškopa satur vismazāko elementu.*

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

2.5. teorēma. Katram reālam skaitlim x eksistē viens un tikai viens

1. lielākais veselais skaitlis $[x]$(x veselā daļa jeb *grīda*, apzīmē arī kā $\lfloor x \rfloor$), kas nav lielāks par x,
2. mazākais veselais skaitlis $\lceil x \rceil$ (x *griesti*), kas nav mazāks par x.

(šai teorēmai ir uzskatāma ğeometriska interpretācija - katrs punkts uz reālo skaitļu taisnes atrodas starp diviem viennozīmīgi noteiktiem tuvākajiem punktiem ar veselām koordinātēm).

2.2. Aritmētiskās pamatīpašības

2.6. teorēma. Ir spēkā šādi apgalvojumi:

1. divu veselu skaitļu summa un reizinājums ir vesels skaitlis (veselo skaitļu kopa ir slēgta attiecībā uz saskaitīšanu un reizināšanu),
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. ja $a+x = a$, tad $x = 0$ (saskaitīšanas neitrālā elementa vienīgums),
8. $a \cdot 1 = a$ (reizināšanas neitrālā elementa eksistence),
9. ja $ax = a$, tad $x = 1$ (reizināšanas neitrālā elementa vienīgums),
10. $a(b + c) = ab + ac$ (distributativitātes likums),
11. ja $ab = 0$, tad $a = 0$ vai $b = 0$ (nulles dalītāju neeksistence),

12. ja $a \neq 0$ un $ab = ac$, tad $b = c$ (reizināšanas saīsināšanas īpašība).

Par vesela skaitļa a *daudzkārtni* sauksim jebkuru skaitli qa, kur $q \in \mathbb{Z}$.

Skaitļa a daudzkārtņu ir bezgalīgi daudz. Tos var intetpretēt ģeometriski.

3. Veselo skaitļu dalīšana ar atlikumu

3.1. teorēma. (*Par veselu skaitļu dalīšanu ar atlikumu*) Katram veselam skaitlim $a \neq 0$ un katram veselam skaitlim b eksistē viens un tikai viens veselu skaitļu pāris (q, r) tāds, ka

$$0 \leq r < |a|$$

un ir spēkā vienādība

$$b = qa + r$$

(q sauksim par *dalījumu*, r - par *atlikumu*).

PIERĀDĪJUMS

Ģeometriskais pierādījums. Atzīmēsim uz taisnes ar Dekarta koordinātēm visus a daudzkārtņus - punktus, kurus koordinātes ir vienādas ar ka, kur $k \in \mathbb{Z}$.

Jebkurš vesels skaitlis b ir viennozīmīgi izsakāms formā

$$b = qa + r,$$

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

4. Veselo skaitļu dalāmība

4.1. Dalāmības pamatīpašības

Atsevišķi pētīsim gadījumu $r = 0$.

Teiksim, ka vesels skaitlis a *dala* veselu skaitli b vai, ka b *dalās ar* a (apzīmē ar pierakstu $a|b$) tad un tikai tad, ja eksistē vesels skaitlis q tāds, ka

$$b = qa$$

(atlikums ir vienāds ar 0). Ja a nedala b, tad šo faktu apzīmē ar pierakstu $a \nmid b$.

Ja $a|b$, tad b ir a daudzkārtnis.

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

4.1. teorēma. Dalāmībai naturālo skaitļu kopā piemīt šādas īpašības:

1. *refleksivitāte* - katrs naturāls skaitlis dala pats sevi - $a|a$;
2. *antisimetrija* - ja $a|b$ un $b|a$, tad $a = b$;
3. *tranzitivitāte* - ja $a|b$ un $b|c$, tad $a|c$;
4. ja $a|b$, tad $a \leq b$.

PIERĀDĪJUMS

1. $a = 1 \cdot a$.

2. Ja $a|b$ un $b|a$, tad $b = qa$ un $a = q'b$, tātad $b = qa = (qq')b$ un $qq' = 1$, tāpēc $a = b$.

3. Ja $a|b$ un $b|c$, tad $b = qa$ un $c = q'b$, tātad $c = q'b = (q'q)a$ un $a|c$.

4. Ja $a|b$, tad $b = qa$, tātad $\frac{b}{a} = q \geq 1$ un $b \geq a$.

■

4.1. piezīme. Veseliem skaitļiem a, b ir spēkā šāds apgalvojums: ja $a|b$ un $b|a$, tad $a = \pm b$.

4.1. piemērs. Jebkurš skaitlis dala skaitli 0, skaitlis 0 nedala nevienu citu skaitli, izņemot 0, skaitļi 1 un -1 dala visus veselos skaitļus, skaitļi 1 un -1 dalās tikai ar 1 un -1.

4.2. teorēma.

1. Ja veseliem skaitļiem $a, b_1, ..., b_n$ izpildās nosacījumi
$$a|b_1,\ a|b_2,\ ...,\ a|b_n,$$
tad
$$a|(b_1 + ... + b_n).$$
2. ja $a|b$, tad katram $c \in \mathbb{Z}$ izpildās $a|bc$.
3. ja $a|b$ un $c|d$, tad $ac|bd$.

PIERĀDĪJUMS

1. Ja $a|b_1$, $a|b_2$, ..., $a|b_n$, tad $b_i = q_i a$ katram i, tātad

$$\sum_{i=1}^{n} b_i = a \sum_{i=1}^{n} q_i = aq,$$

kur q ir vesels skaitlis.

2. Ja $a|b$, tad $b = qa$ un $bc = (qc)a$.
3. Ja $a|b$, tad $b = q_1 a$. Ja $c|d$, tad $d = q_2 c$. Tādējādi

$$bd = (q_1 a)(q_2 c) = (q_1 q_2)(ac).$$

■

4.2. piemērs. Dots, ka $3|n$ un $3|m$. Pierādīt, ka $3|n^3 + nm + 5m$.
Dots, ka $3|n - m$ un $5|n + m$. Pierādīt, ka $15|n^2 - m^2$.

4.2. Pirmskaitļi un to pamatīpašības

Naturālu skaitli sauksim par *pirmskaitli*, ja tas ir naturāls skaitlis, kuram ir tieši divi dažādi naturāli dalītāji.

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

Naturāls skaitlis ir vai nu 1, vai pirmskaitlis vai salikts skaitlis.

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

4.3. teorēma. Katram saliktam naturālam skaitlim ir vismaz viens dalītājs, kas ir pirmskaitlis.

PIERĀDĪJUMS Apskatīsim salikta skaitļa a dalītāju kopu, tajā ir vismaz trīs elementi - 1, a un vismaz vēl viens. Apskatīsim mazāko no dalītājiem b, kas nav 1. b obligāti ir pirmskaitlis, jo pretējā gadījumā skaitlim a ir vēl mazāki dalītāji (b dalītāji), kas nav 1.■

4.4. teorēma. (Eiklīds, Senā Grieķija, ap 300BC) Pirmskaitļu kopa ir bezgalīga.

PIERĀDĪJUMS Pieņemsim pretējo. Pieņemsim, ka pirmskaitļu kopa ir galīga kopa $p_1, ..., p_n$. Apskatīsim skaitli

$$N = p_1 p_2 ... p_n + 1. \tag{1}$$

N ir vai nu 1, vai pirmskaitlis, vai salikts skaitlis. Dalot N ar katru no skaitļiem p_i, atlikumā iegūsim 1, tātad N ir pirmskaitlis. N ir lielāks nekā jebkurš kopas $\{p_1, ..., p_n\}$ elements, tātad ir iegūta pretruna.■

4.5. teorēma. Ja pirmskaitlis p dala naturālu skaitļu reizinājumu ab, tad tas dala vai nu a vai b.

PIERĀDĪJUMS Ja $p|ab$, tad $ab = pc$, kur $c \in \mathbb{N}$. Tātad

$$a = p \cdot \tfrac{c}{b}$$

un

$$b = p \cdot \tfrac{c}{a}.$$

Pieņemsim, ka p nedala b. Tā kā p un b nav kopīgu reizinātāju, izņemot 1, tad $\frac{c}{b}$ ir vesels skaitlis (p nevar saīsināt saucēju), tāpēc $p|a$. Līdzīgā veidā pierāda, ka, ja $p \nmid a$, tad $p|b$.■

4.4. piemērs. Dots, ka p un q ir dažādi pirmskaitļi. Cik ir dažādu naturālu dalītāju skaitļiem pq, p^3q, p^3q^2, $p^\alpha q^\beta$?

4.5. piemērs. Vai tiesa, ka

1. ja $3|n$ un $4|n$, tad $12|n$;
2. ja $6|n$ un $4|n$, tad $24|n$.

5. Aritmētikas pamatteorēma un tās pielietojumi

5.1. Pirmskaitļa kārta

5.1. teorēma. Katram naturālam n un katram pirmskaitlim p eksistē nenegatīvs vesels skaitlis α, tāds ka $p^{\alpha}|n$ un $p^{\alpha+1} \nmid n$ (skaitli α sauksim par p *kārtu* skaitlī n, apzīmē ar $ord_p(n)$).

PIERĀDĪJUMS Dalīsim n ar 1, p, p^2,... tik ilgi, kamēr dalījumā iegūsim nenulles atlikumu.■

5.1. piemērs. $ord_2(96) = 5$,$ord_2(15) = 0$.

5.2. teorēma. Ja $n|m$, tad katram pirmskaitlim p

$$ord_p(n) \leq ord_p(m).$$

PIERĀDĪJUMS Ja $p^\alpha|n$ un $n|m$, tad no dalāmības tranzitivitātes seko, ka $p^\alpha|m$. Seko, ka $\alpha \leq ord_p(m)$. Ja $\alpha = ord_p(n)$, tad iegūstam teorēmas apgalvojumu.

5.2. Pamatteorēma

5.3. teorēma. (*Aritmētikas pamatteorēma, viennozīmīgās faktorizācijas teorēma*) Jebkurš naturāls skaitlis n ir viennozīmīgi izsakāms pirmskaitļu pakāpju reizinājuma formā

$$n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_m^{\alpha_m},$$

kur katram i skaitlis p_i ir pirmskaitlis, $p_1 < p_2 < ... < p_m$, skaitļi $\alpha_1, ..., \alpha_m$ ir naturāli.

PIERĀDĪJUMS Skaitlim n atradīsim visus pirmskaitļus, kas to dala, sašķirosim tos pēc lieluma, iegūsim kopu $P = \{p_1, ..., p_m\}$.

Katram pirmskaitlim $p_i \in P$ atradīsim tā kārtu $\alpha_i > 0$. Ievērosim, ka katram i izpildās vienādība

$$n = p_i^{\alpha_i} q_i,$$

kur $q_i \nmid p_i$, tātad q_i ir visu pārējo pirmskaitļu pakāpju reizinājums. Tādējādi $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_m^{\alpha_m}$.

Viennozīmīgums seko no tā, ka kopa P un pirmskaitļu kārtas α_i ir noteiktas viennozīmīgi.■

5.2. piemērs. $2520 = 2^3 3^2 5^1 7^1$.

5.4. teorēma. Ja $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_m^{\alpha_m}$ un $n' = p_1^{\beta_1} p_2^{\beta_2} ... p_m^{\beta_m}$, tad

1. $nn' = p_1^{\alpha_1+\beta_1} p_2^{\alpha_2+\beta_2} ... p_m^{\alpha_m+\beta_m}$,
2. $\frac{n}{n'} = p_1^{\alpha_1-\beta_1} p_2^{\alpha_2-\beta_2} ... p_m^{\alpha_m-\beta_m}$,
3. $n^k = p_1^{k\alpha_1} p_2^{k\alpha_2} ... p_m^{k\alpha_m}$.

PIERĀDĪJUMS Izmantojam reizināšanas komutatīvo īpašību. ■

5.3. LKD un MKD

Skaitli a sauksim par skaitļu kopas $\{b_1, ..., b_m\}$ *kopīgu dalītāju*, ja katram i izpildās nosacījums $a|b_i$. Apzīmēsim kopas $b_1, ..., b_m$ dalītāju kopu ar $D(b_1, ..., b_m)$.

5.1. piezīme. Ievērosim, ka jebkuras skaitļu kopas kopīgo dalītāju kopa ir galīga.

5.3. piemērs. $D(12, 16, 20) = \{2, 4\}$.

Par kopas $\{b_1, ..., b_m\}$ *lielāko kopīgo dalītāju (LKD)* sauksim to kopīgo dalītāju, kurš dalās ar jebkuru šīs kopas kopīgo dalītāju. Citiem vārdiem sakot, a ir lielākais kopīgais dalītājs, ja

1. katram i izpildās $a|b_i$,
2. ja a' ir tāds, ja katram i izpildās $a'|b_i$, tad $a'|a$.

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

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 $1 \leq m < p$.

5.2. piezīme. Ja $LKD(a, b) = 1$ un $a|n$, $b|n$, tad $ab|n$.
Ja $a|bn$, tad $a|n$.

Skaitli c sauksim par skaitļu kopas $\{b_1, ..., b_m\}$ *kopīgu daudzkārtni*, ja katram i izpildās nosacījums $b_i|c$. Apzīmēsim kopas $b_1, ..., b_m$ daudzkārtņu kopu ar $M(b_1, ..., b_n)$.

5.3. piezīme. Ievērosim, ka skaitļu kopas kopīgo daudzkārtņu kopa ir bezgalīga. $M(2) = \{n|n = 2m, m \in \mathbb{Z}\}$.

Par kopas $\{b_1, ..., b_m\}$ *mazāko kopīgo daudzkārtni (MKD)* sauksim to kopīgo daudzkārtni, kurš dala jebkuru šīs kopas kopīgo daudzkārtni. Citiem vārdiem sakot, c ir mazākais kopīgais daudzkārtnis, ja

1. katram i izpildās $b_i|c$,
2. ja c' ir tāds, ja katram i izpildās $b_i|c'$, tad $c|c'$.

5.5. piemērs. $MKD(12, 18) = 36$.

5.6. piemērs. Apskatīsim vairākus piemērus ar LKD un MKD un atrašanu zinot skaitļu faktorizāciju.

5.5. teorēma. Jebkuriem diviem naturāliem skaitļiem a un b eksistē $LKD(a, b)$ un $MKD(a, b)$.

PIERĀDĪJUMS Konstruktīvi pierādīsim apgalvojumu par LKD. Pieņemsim, ka

$$a = p_1^{\alpha_1} p_2^{\alpha_2} ... p_m^{\alpha_m}$$

un

$$b = p_1^{\beta_1} p_2^{\beta_2} ... p_m^{\beta_m}.$$

Uzskatīsim, ka pirmskaitļu kopas abu skaitļu sadalījumos ir vienādas. Nepieciešamības gadījumā kāpinātājus ņemsim vienādus ar 0.

Katram i definēsim

$$\delta_i = \min(\alpha_i, \beta_i).$$

Pierādīsim, ka
$$LKD(a,b) = d = p_1^{\delta_1} p_2^{\delta_2} ... p_m^{\delta_m}.$$

Redzam, ka $d|a$ un $d|b$, jo katra pirmskaitļa kārta attiecībā uz d nepārsniedz tā kārtu attiecībā uz a un b.

Ja kāds skaitlis d' dala a un b, tad tas dala arī d, jo katra pirmskaitļa kārta attiecībā uz d' nevar būt lielāka kā kārta attiecībā uz d.

Līdzīgā veidā pierāda, ka
$$MKD(a,b) = p_1^{\lambda_1} p_2^{\lambda_2} ... p_m^{\lambda_m},$$
kur katram i definēsim
$$\lambda_i = \max(\alpha_i, \beta_i).$$
■

5.4. piezīme. Šo teorēmu var vispārināt uz gadījumu, kad ir jāatrod vairāk nekā divu skaitļu LKD un MKD.

5.7. piemērs. $LKD(24, 18) = LKD(2^3 3^1, 2^1 3^2) = 2^1 3^1 = 6.$