DAUGAVPILS UNIVERSITĀTE
Dabaszinātņu un matemātikas fakultāte
Matemātikas katedra

Studiju kurss

Veselo skaitļu teorija

2.lekcija

Docētājs: Dr. P. Daugulis

2008./2009.studiju gads

Saturs

1. Pirmskaitļu īpašības

1.1. 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

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

un

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

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 $p|b$.■

1.2. teorēma. (*pirmskaitļu tuksnešu eksistence*) Katram naturālam k eksistē k skaitļi $N, N+1, ..., N+k-1$ tādi, ka tie visi nav pirmskaitļi.

PIERĀDĪJUMS Definēsim $N = (k+1)! + 2$. Redzam, ka $N + i = (k+1)! + (i+2)$ un $N + k - 1 = (k+1)! + (k+1)$. Skaitlis $N + i$ dalās ar $i+2$, tātad tas nav pirmskaitlis. Esam ieguvušu k pēc kārtas ejošu saliktu skaitļu virkni $N, ..., N + k - 1$.■

1.1. piemērs. Ja $k = 10$, tad $N = 11! + 2 = 39916802$.

1.3. teorēma. Ja n ir salikts skaitlis, tad eksistē pirmskaitlis $p \leq \sqrt{n}$ tāds ka $p|n$.

PIERĀDĪJUMS Pieņemsim, ka p ir mazākais pirmskaitlis, kas dala n (vismaz viens pirmskaitlis eksistē, jo n ir salikts). Tā kā $p|n$, tad $n = pm$, kur $m \geq p$ (ja $m < p$, tad eksistē pirmskaitlis, kas ir mazāks kā p un dala n). Ja $p > \sqrt{n}$, tad $p^2 > n$. Tā ir pretruna, jo

$$p^2 \leq pm = n.$$

■

1.1. piezīme. No šīs teorēmas seko šāds fakts: lai noteiktu, vai n ir pirmskaitlis, pietiek pārbaudīt, vai n dalās ar pirmskaitļiem, kas nepārsniedz $\sqrt{n}$. Ja n nedalās ne ar vienu pirmskaitli $p \leq \sqrt{n}$, tad n ir pirmskaitlis.

1.2. piemērs. Lai noteiktu, vai 43 ir pirmskaitlis, ir jāpārbauda, vai 43 dalās ar $2, 3, 5$.

Lai atrastu visus pirmskaitļus intervālā $[2, n]$, var izmantot vienkāršu rekursīvu algoritmu, ko sauc par *Erastotena sietu*:

1. atradīsim visus pirmskaitļus intervālā $[2, [\sqrt{n}]]$, apzīmēsim šo pirmskaitļu kopu ar P,
2. katram pirmskaitlim $p \in P$ izsvītrosim no intervāla $[2, n]$ veselo skaitļu kopas visus tā daudzkārtņus $pd, d \in \mathbb{N}, d \geq 2$,
3. izvadīsim neizsvītrotos skaitļus kā pirmskaitļus intervālā $[2, n]$.

Ievērosim, ka 1.solī mums ir jāzina visi pirmskaitļi intervālā $[2, [\sqrt{n}]]$. Tos var atrast, realizējot šo pašu algoritmu ar mazāku n vērtību. To var būt nepieciešams darīt vairākas reizes, kamēr pirmskaitļu kopa ir zināma. Tādus algoritmus sauc par *rekursīviem algoritmiem*.

1.3. piemērs. Atradīsim pirmskaitļus, kas ir mazāki kā 30. Ir jāizsvītro skaitļu $2, 3, 5$ daudzkārtņi

$$4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 9, 15, 21, 27, 25.$$

Pāri paliek

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29.$$

1.4. 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.■

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

Divas vienkārši formulējamas neatrisinātas problēmas.

Dvīņu pirmskaitļu problēma: vai pirmskaitļu pāru $(p, p+2)$ kopa ir bezgalīga?

Goldbaha problēma(> 200 gadi): vai katru pāra skaitli, kas ir lielāks kā 2 var izteikt divu pirmskaitļu summas veidā?

2. Aritmētikas pamatteorēma

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

$$n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_m^{\alpha_m}, \tag{1}$$

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.■

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

2.1. piezīme. Aritmētikas pamatteorēmu bieži interpretē šādā veidā. Par katru naturālu skaitli n var domāt kā par funkciju f_n no pirmskaitļu kopas uz nenegatīvo veselo skaitļu kopu, kas katram pirmskaitlim piekārto kāpinātāju, ar kādu šī pirmskaitļa pakāpe dala doto skaitli: ja $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_m^{\alpha_m}$, tad $f_n(p_i) = \alpha_i$.

2.2. piezīme. Aritmētikas pamatteorēmu var vispārināt uz visu veselo skaitļu kopu $\mathbb{Z}$: jebkurš vesels skaitlis n ir viennozīmīgi izsakāms formā

$$n = (-1)^{\epsilon} p_1^{\alpha_1} p_2^{\alpha_2} ... p_m^{\alpha_m},$$

kur $\varepsilon \in \{0, 1\}$.

2.3. piezīme. Simboliski varam definēt

$$n = \prod_p p^{\alpha_n},$$

kur $\alpha_n \geq 0$,

$$0 = \prod_p p^{+\infty}$$

un

$$1 = \prod_p p^0.$$

2.2. 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. ■

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 $D(b_1, ..., b_m)$. Acīmredzami

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

3.1. piezīme. Ievērosim, ka netukšas skaitļu kopas kopīgo dalītāju kopa ir galīga.

Naturāla skaitļa n naturālo dalītāju skaitu apzīmēsim ar $\nu(n)$, to summu apzīmēsim ar $\sigma(n)$.

3.1. piemērs. $D(12, 16, 20) = \{2, 4\}$, $\nu(10) = 4$, $\nu(2007) = 6$, $\nu(2008) = 8$, $\sigma(10) = 18$, $\sigma(2007) = 2912$, $\sigma(2008) = 3780$.

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 $a'|a$.

3.2. 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 $1 \leq m < p$.

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 $M(b_1, ..., b_n)$. Acīmredzami

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

3.2. 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 $c|c'$.

3.3. piemērs. $MKD(12, 18) = 36$.

3.1. teorēma. Ja $b = p_1^{\beta_1} p_2^{\beta_2} ... p_m^{\beta_m}$ un $a|b$, tad

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

kur katram i izpildās $\alpha_i \leq \beta_i$.

PIERĀDĪJUMS Skaitlim a ir viennozīmīgi noteikts tā sadalījums pirmskaitļu pakāpju reizinājumā.

Izmantosim dalāmības attiecības tranzitivitāti:

- neviens pirmskaitlis, kas nedala b, nevar būt šajā sadalījumā ar pozitīvu pakāpi (ja $p|a$ un $a|b$, tad jābūt $p|b$).
- ja pirmskaitlis p_i dala b, tad tā kārta attiecībā uz a nevar būt lielāka nekā tā kārta attiecībā uz b (ja $p^\alpha|a$ un $a|b$, tad jābūt $p^\alpha|b$).

■

3.2. teorēma. Ja $b = p_1^{\beta_1} p_2^{\beta_2} ... p_m^{\beta_m}$ un $b|c$, tad

$$c = p_1^{\gamma_1} p_2^{\gamma_2} ... p_m^{\gamma_m} q,$$

kur katram i izpildās $\beta_i \leq \gamma_i$ un q ir naturāls skaitlis.

PIERĀDĪJUMS Pierāda līdzīgi iepriekšējai teorēmai.■

3.3. 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

$$\lambda_i = \max(\alpha_i, \beta_i).$$

■

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

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

3.4. teorēma. $LKD(a,b)$ ir lielākais (parastajā salīdzinājumā) a un b kopīgais dalītājs.

PIERĀDĪJUMS Izmantosim dalītāju sadalījumu pirmskaitļu pakāpju reizinājumā. Ja $e > LKD(a,b)$ un $e|a$, $e|b$, tad vismaz vienam

pirmskaitlim p_i e sadalījumā kāpinātājs pārsniedz kāpinātāju LKD sadalījumā, tāpēc e nevar būt a un b kopīgais dalītājs.■

4. LKD un MKD īpašības

4.1. teorēma. Visiem naturāliem skaitļiem ir spēkā šādi fakti:

1. $LKD(a,b) = LKD(b,a)$,
2. $LKD(ac,bc) = c \cdot LKD(a,b)$,
3. $LKD(a,b) \cdot MKD(a,b) = ab$ (speciālgadījums - ja $LKD(a,b)=1$, tad $MKD(a,b) = ab$).

PIERĀDĪJUMS Visus apgalvojumus pierāda pētot kārtas katram pirmskaitlim.

1. Seko no fakta $\min(x,y) = \min(y,x)$ - katram pirmskaitlim minimālā kārta nav atkarīga no kārtības, kādā tiek pētītas kārtas.

2. Pieņemsim, ka $ord_p(a) = \alpha$, $ord_p(b) = \beta$, $ord_p(c) = \gamma$. Redzam, ka

$$\min(\alpha + \gamma, \beta + \gamma) = \min(\alpha, \beta) + \gamma.$$

3. Pieņemsim, ka $ord_p(a) = \alpha$, $ord_p(b) = \beta$. Redzam, ka

$$\min(\alpha, \beta) + \max(\alpha, \beta) = \alpha + \beta.$$

4.1. piemērs. $LKD(12, 30) = 6 \cdot LKD(2, 5) = 6$. $LKD(12, 30) \cdot MKD(12, 30) = 6 \cdot 60 = 360$.

5. 2.mājasdarbs

1. Atrodiet $ord_2(20!)$
2. Ar cik nullēm beidzas skaitlis 25! ? (*Norādījums: ja skaitlis beidzas ar k nullēm, tad tas dalās ar* $10^k = 2^k 5^k$)
3. Atrodiet visus naturālus skaitļus n, kuriem $2^n + 2$ ir naturāla skaitļa kvadrāts. (*Norādījums: ja n ir naturāla skaitļa kvadrāts, tad* $ord_2(n)$ *ir pāra skaitlis*)
4. Ir zināms skaitļa n sadalījums pirmskaitļu pakāpju reizinājumā: $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_m^{\alpha_m}$. Atrodiet skaitļa n dažādo pozitīvo dalītāju skaitu $\nu(n)$. (*Norādījums: ja* $x|n$, *tad* $ord_p(x) \leq ord_p(n)$)