DAUGAVPILS UNIVERSITĀTE
Dabaszinātņu un matemātikas fakultāte
Matemātikas katedra

Studiju kurss

SKAITĻU TEORIJA

3.lekcija

Docētājs: Dr. P. Daugulis

2012./2013.studiju gads

Saturs

Lekcijas mērķis:

- apgūt svarīgākās pirmskaitļu īpašības, veselo skaitļu viennozīmīgās faktorizācijas teorēmu un tās sekas.

Lekcijas kopsavilkums:

- katru veselu skaitli var viennozīmīgi izteikt pirmskaitļu pakāpju reizinājuma formā.

Svarīgākie jēdzieni: pirmskaitļa kārta.

Svarīgākie fakti un metodes: pirmskaitļu īpašības, Erastotena siets, viennozīmīgās faktorizācijas teorēma, LKD un MKD atrašana ar faktorizācijas metodi, saliktu skaitļu faktorizācijas metodes - naivā dalīšana un Fermā metode.

1. Pirmskaitļi un aritmētikas pamatteorēma

1.1. Pirmskaitļu īpašības

1.1.1. Pamatīpašības

$\mathbb{P} = \{2, 3, 5, 7, ...\}$ - visu (pozitīvo) pirmskaitļu kopa.

1.1. teorēma.

1. $\forall\ n \in \mathbb{Z}, |n| > 1\ \exists\ p \in \mathbb{P}$ tāds, ka $p \Big| n$.

2. $\forall\ n \in \mathbb{Z}\ \forall\ p \in \mathbb{P} : LKD(n, p) = 1\ \vee\ p \Big| n$.

3. $\forall\ a, b \in \mathbb{Z}\ \forall\ p \in \mathbb{P} : p \Big| ab \implies p \Big| a\ \vee\ p \Big| b$.

4. $n \notin \mathbb{P} \implies \exists\, p \in \mathbb{P} : \begin{cases} p \big| n \\ p \leq \sqrt{n}. \end{cases}$

5. (Eiklīds, ap 300BC) $\mathbb{P}$ ir bezgalīga kopa.

PIERĀDĪJUMS

1. Ja $|n| \in \mathbb{P}$, tad nekas nav jāpierāda.

Apskatīsim salikta skaitļa n pozitīvo dalītāju kopu D_{pos}, tajā ir vismaz trīs elementi - 1, $|n|$ un vismaz vēl viens.

Apzīmēsim $d = \min\Big(D_{pos} \setminus \{1\}\Big)$, $d > 1 \implies d \in \mathbb{P}$, jo pretējā gadījumā skaitlim n ir vēl mazāki pozitīvi dalītāji (d dalītāji), kas nav 1.

2. $LKD(n,p) \big| p \implies LKD(n,p) \in \{1, p\}$.

3. $\left\{ \begin{array}{l} p \Big| ab \\ p \nmid a \end{array} \right. \Longrightarrow LKD(a,p) = 1 \Longrightarrow p \Big| b.$

4. Pieņemsim, ka p ir mazākais pirmskaitlis, kas dala n (vismaz viens pirmskaitlis eksistē, jo n ir salikts). Pierādīsim, ka p apmierina apgalvojumu.

$$p|n \Longrightarrow \left\{ \begin{array}{l} n = pm \\ m \geq p \end{array} \right.$$ (ja $m < p$, tad $\exists$ pirmskaitlis - m dalītājs, kas ir mazāks kā p un dala n).

$$\left\{ \begin{array}{l} n = pm \\ m \geq p \end{array} \right. \Longrightarrow n \geq p^2 \Longrightarrow \sqrt{n} \geq p.$$

5. Pieņemsim pretējo - $\mathbb{P}$ ir galīga kopa $\{p_1, ..., p_n\}$.

Apskatīsim skaitli

$$N = p_1 p_2 ... p_n + 1.$$

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.

$N > p_i,\ \forall\ p_i \in \{p_1, ..., p_n\}$ - pretruna. ■

1.1. piezīme. No teorēmas 4.apgalvojuma seko, ka lai noteiktu, vai $n \in \mathbb{P}$, 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.

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

1.1.2. Erastotena siets

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

1. sarakstīsim virknē skaitļus $2, 3, ..., n$;
2. izsvītrojam visus pirmā virknes elementa (2) daudzkārtņus, paliek virkne $2, 3, 5, 7, ...,$ nobīdamies par vienu vienību pa labi - $2 \| 3, 5, 7, ...$;

3. izsvītrojam visus pirmā (neizsvītrotā) virknes elementa (3) daudzkārtņus, paliek virkne $2\|3, 5, 7, 11, 13, ...,$ nobīdamies par vienu vienību pa labi - $2, 3\|5, 7, ...;$

   ...

l. izsvītrojam visus pirmā (neizsvītrotā) virknes elementa p daudzkārtņus, ja $p \leq \sqrt{n}$, nobīdamies par vienu vienību pa labi;

... ...

1.2. 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 $2, 3, 5, 7, 11, 13, 17, 19, 23, 29.$

1.2. Aritmētikas pamatteorēma un tās sekas

1.2.1. Pirmskaitļa kārta

$p \in \mathbb{P}$, $n \in \mathbb{N}$. Par p kārtu attiecībā uz n ($ord_p(n)$) sauc maksimālo p pakāpi, kas dala n:

$$\alpha = ord_p(n) \iff \begin{cases} p^{\alpha} \mid n \\ p^{\alpha+1} \nmid n \end{cases}$$

$ord_p(n) \in \mathbb{N} \cap \{0\}$.

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

1.2.2. Teorēma

1.2. teorēma. (*Aritmētikas pamatteorēma, viennozīmīgās faktorizācijas teorēma*) $\forall\, n \in \mathbb{N}$, $n > 1$, ir viennozīmīgi izsakāms formā

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

kur $p_i \in \mathbb{P}$, $p_1 < p_2 < \ldots < p_m$, $\alpha_i \in \mathbb{N}$.

PIERĀDĪJUMS Atradīsim visus pirmskaitļus, kas dala n, sašķirosim tos pēc lieluma, iegūsim viennozīmīgi noteiktu kopu $P = \{p_1, \ldots, p_m\}$, kur $p_1 < p_2 < \ldots < p_m$.

$\forall\, p_i \in P$ atradīsim $ord_{p_i}(n) = \alpha_i > 0$. $\forall\, i$

$$p_i^{\alpha_i} \Big| n \implies n = p_i^{\alpha_i} q_i, \text{ kur } p_i \nmid q_i.$$

$$n = p_1^{\alpha_1} q_1 = p_2^{\alpha_2} q_2 \implies p_1^{\alpha_1} \Big| p_2^{\alpha_2} q_2 \implies p_1^{\alpha_1} \Big| q_2 \implies p_1^{\alpha_1} p_2^{\alpha_2} \Big| n.$$

Turpinot šādus spriedumus, iegūsim, ka

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

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

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

1.2. piezīme. Aritmētikas pamatteorēmu var vispārināt uz $\mathbb{Z}$: $\forall\, n \in \mathbb{Z}$ ir viennozīmīgi izsakāms formā

$$n = (-1)^{\epsilon} p_1^{\alpha_1} p_2^{\alpha_2} ... p_m^{\alpha_m}, \text{ kur } \varepsilon \in \{0, 1\}.$$

1.3. piezīme. Ja ir doti vairāki skaitļi, tad lietderīgi ir uzskatīt, ka tiem atbilstošās pirmskaitļu kopas ir vienādas, papildinot tās, ja nepieciešams, piemēram:

$$\begin{cases} 24 = 2^3 3^2 5^0 7^0, \\ 35 = 2^0 3^0 5^1 7^1. \end{cases}$$

1.3. teorēma.

$$\begin{cases} n = p_1^{\alpha_1} ... p_m^{\alpha_m} \\ n' = p_1^{\beta_1} ... p_m^{\beta_m} \end{cases} \Longrightarrow \begin{cases} nn' = p_1^{\alpha_1+\beta_1} ... p_m^{\alpha_m+\beta_m} \\ \frac{n}{n'} = p_1^{\alpha_1-\beta_1} ... p_m^{\alpha_m-\beta_m} \\ n^k = p_1^{k\alpha_1} ... p_m^{k\alpha_m} \end{cases}$$

PIERĀDĪJUMS Izmantojam reizināšanas komutatīvo īpašību, piemēram:

$$nn' = (p_1^{\alpha_1} ... p_m^{\alpha_m})(p_1^{\beta_1} ... p_m^{\beta_m}) =$$
$$(p_1^{\alpha_1} p_1^{\beta_1}) ... (p_m^{\alpha_m} p_m^{\beta_m}) = p_1^{\alpha_1+\beta_1} ... p_m^{\alpha_m+\beta_m}. \blacksquare$$

1.2.3. LKD un MKD atrašana

1.4. teorēma. $a|b \iff \forall\, p \in \mathbb{P} : ord_p(a) \leq ord_p(b).$

PIERĀDĪJUMS

$$ord_p(a) \leq ord_p(b) \implies ord_p(b) - ord_p(a) \geq 0 \implies$$

$$\frac{b}{a} = \prod_{p \in \mathbb{P}} p^{ord_p(b) - ord_p(a)} \in \mathbb{N} \implies a|b.$$

$$\forall\, p \in \mathbb{P} : \left\{ \begin{array}{l} p^{\alpha}|a \\ a|b \end{array} \right. \implies p^{\alpha} \Big| b \implies ord_p(a) \leq ord_p(b). \blacksquare$$

1.5. teorēma. Dots, ka $b = p_1^{\beta_1} p_2^{\beta_2} ... p_m^{\beta_m}$, $\beta_i \geq 0$.

1. $a|b \iff a = \pm p_1^{\alpha_1} p_2^{\alpha_2} ... p_m^{\alpha_m}$, kur $\forall\, i\ 0 \leq \alpha_i \leq \beta_i$.
2. $b|c \iff c = \pm p_1^{\gamma_1} p_2^{\gamma_2} ... p_m^{\gamma_m} q$, kur $\forall\, i\ \beta_i \leq \gamma_i, q \in \mathbb{N}$.

PIERĀDĪJUMS Seko no iepriekšējās teorēmas. $\blacksquare$

1.6. teorēma.

$$\begin{cases} a = p_1^{\alpha_1}...p_m^{\alpha_m}, \\ b = p_1^{\beta_1}...p_m^{\beta_m} \end{cases} \Longrightarrow \begin{cases} LKD(a,b) = p_1^{\gamma_1}...p_m^{\gamma_m}, \gamma_i = \min(\alpha_i, \beta_i), \\ MKD(a,b) = p_1^{\delta_1}...p_m^{\delta_m}, \delta_i = \max(\alpha_i, \beta_i). \end{cases}$$

PIERĀDĪJUMS

1. Apzīmēsim $d = LKD(a,b)$. $\forall\ p_i \in \mathbb{P}$:

$$\begin{cases} ord_{p_i}(d) \leq ord_{p_i}(a) = \alpha_i \\ ord_{p_i}(d) \leq ord_{p_i}(b) = \beta_i \end{cases} \Longrightarrow ord_p(d) \leq \min(\alpha_i, \beta_i) = \gamma_i.$$

Ja $\exists\ p_j \in \mathbb{P}: \quad ord_{p_j}(d) < \gamma_j \Longrightarrow$ d nav $LKD(a,b)$ - to var palielināt līdz lielākam a un b kopīgam dalītājam

$$\widetilde{d} = p_1^{\gamma_1}...p_j^{\gamma_j}...p_m^{\gamma_m}.$$

2. Apzīmēsim $c = MKD(a,b)$. $\forall\ p \in \mathbb{P}$:

$$\begin{cases} ord_p(d) \geq ord_p(a) \\ ord_p(d) \geq ord_p(b) \end{cases} \Longrightarrow ord_p(d) \geq \max(ord_p(a), ord_p(b)).$$

Ja $\exists\ p_j \in \mathbb{P} :\ ord_{p_j}(d) > \delta_j \implies d$ nav $MKD(a,b)$ - to var samazināt līdz mazākam a un b kopīgam daudzkārtnim

$$\widehat{d} = p_1^{\delta_1} ... p_j^{\delta_j} ... p_m^{\delta_m} .\blacksquare$$

1.3. Vienkāršākās faktorizācijas metodes

1.3.1. Dalīšana ar maziem pirmskaitļiem - naivā dalīšanas metode

Var pārbaudīt, vai n dalās ar pirmskaitļiem, kas nepārsniedz $\sqrt{n}$, sākot no maziem pirmskaitļiem $(2, 3, 5, 7, ...)$. Ja n nedalās ne ar vienu pirmskaitli $p \leq \sqrt{n}$, tad n ir pirmskaitlis.

1.3.2. Fermā metode

Naivā dalīšanas metode nav laba, ja n nedalās ar maziem pirmskaitļiem, piemēram, $n = pq$, kur p, q lieli un tuvi pirmskaitļi.

n - nepāra skaitlis, $n = uv$, $u > v$.

1.7. teorēma. n - nepāra skaitlis, $n = uv$, $u > v$. Tad

$$n = a^2 - b^2, \text{ kur } \begin{cases} a = \dfrac{u+v}{2}, \\ b = \dfrac{u-v}{2}. \end{cases}$$

PIERĀDĪJUMS Tieša pārbaude:

$$\left(\frac{u+v}{2}\right)^2 - \left(\frac{u-v}{2}\right)^2 = \frac{u^2+2uv+v^2-u^2+2uv-v^2}{4} = uv.$$

Algoritms:

1. definēt $a := \lceil \sqrt{n} \rceil$,
2. noteikt, vai $a^2 - n$ ir vesela skaitļa kvadrāts (jo $a^2 - n = b^2 \iff n = a^2 - b^2$), ja nē, tad definēt $a := a + 1$, iet uz 2).

2. 2.mājasdarbs

2.1. Obligātie uzdevumi

2.1 (a) Atrast $ord_2(20!)$.
(b) Ar cik nullēm beidzas skaitlis $25! = 1 \cdot 2 \cdot ... \cdot 25$? (*Norādījums: ja skaitlis beidzas ar k nullēm, tad tas dalās ar* $10^k = 2^k 5^k$).

2.2 Sadalīt pirmskaitļu pakāpju reizinājumā

(a) 107053455600000;
(b) 74649551 (*Norādījums: Fermā metode*);
(c) 82861.

2.3 Atrast skaitļu a un b LKD un MKD izmantojot faktorizācijas metodi.

(a) $a = 72$, $b = 702$;
(b) $a = 3240$, $b = 11088$.

2.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi

2.4 Ir zināms skaitļa $n \in \mathbb{N}$ sadalījums pirmskaitļu pakāpju reizinājumā: $n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_m^{\alpha_m}$. Atrodiet n dažādo pozitīvo dalītāju skaitu $\nu(n)$. (*Norādījums: ja* $x \Big| n$, *tad* $ord_p(x) \leq ord_p(n)$).

2.5 (Putnam Competition, 2009) Pierādīt, ka jebkuru racionālu skaitli var izteikt kā pirmskaitļu faktoriālu reizinājumu dalījumu, piemēram, $\frac{4}{3} = \frac{(2!)^3}{3!}$.