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

Studiju kurss

Veselo skaitļu teorija

3.lekcija

Docētājs: Dr. P. Daugulis

2009./2010.studiju gads

Saturs

Lekcijas mērķis:

- apgūt pirmskaitļu īpašības un faktorizācijas teorēmu.

Lekcijas kopsavilkums:

- pirmskaitļiem piemīt vairākas raksturīgas īpašības,
- jebkuru naturālu skaitli var viennozīmīgi izteikt pirmskaitļu pakāpju reizinājuma formā,

- pirmskaitļu pakāpju reizinājuma formu var izmantot LKD un MKD atrašanai.

Svarīgākie jēdzieni: pirmskaitļa kārta,

Svarīgākie fakti un metodes: pirmskaitļu īpašības, pirmskaitļu tuksneši, Bertrana postulāts, Dirihlē teorēma par pirmskaitļiem aritmētiskajās progresijās, aritmētikas pamatteorēma, LKD un MKD atrašana izmantojot faktorizāciju.

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 $p|n$.

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

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

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

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 $D(n) \cap \mathbb{N}$, tajā ir vismaz trīs elementi - 1, $|n|$ un vismaz vēl viens.

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

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

3. $p|ab \ \wedge \ p \nmid a \implies LKD(a,p) = 1 \implies p|b$.

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

$p|n \implies n = pm$, kur $m \geq p$ (ja $m < p$, tad eksistē pirmskaitlis - m dalītājs, kas ir mazāks kā p un dala n).

$$\begin{cases} n = pm \\ m \geq p \end{cases} \implies n \geq p^2 \implies \sqrt{n} \geq p.$$

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. Papildinformācija par pirmskaitļiem

1.2. teorēma. (*pirmskaitļu tuksnešu eksistence*) $k \in \mathbb{N}\ \exists$ k skaitļi $\{N, N+1, ..., N+k-1\} \subseteq \mathbb{N}$ tādi, ka tie visi nav pirmskaitļi.

PIERĀDĪJUMS Definēsim $N = (k+1)! + 2$. Redzam, ka

$$N + i = (k+1)! + (i+2).$$

$i + 2 | N + i$, ja $0 \leq i \leq k-1 \implies N + i \notin \mathbb{P}$. Esam ieguvuši k pēc kārtas ejošu saliktu skaitļu virkni $N, ..., N + k - 1$.■

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

1.2. piezīme. Vai var samazināt N?

1.3. teorēma. (*Bertrana postulāts*)

$$\forall n > 1\ \exists p : n < p < 2n - 2.$$

1.4. teorēma. (*Dirihlē teorēma par pirmskaitļiem aritmētiskajās progresijās*) $LKD(a,d)=1 \implies$

$$\exists \text{ bezgalīgi daudz } p \in \mathbb{P} \text{ formā } p=a+nd, n \in \mathbb{Z}.$$

1.3. piemērs. $\exists$ bezgalīgi daudz pirmskaitļu formā $4n \pm 1$.

1.2. Aritmētikas pamatteorēma un tās sekas

1.2.1. Teorēma

1.5. teorēma. $\forall\, n \in \mathbb{N}\ \forall\, p \in \mathbb{P}\ \exists\, \alpha \in \mathbb{N} \cup \{0\}$, tāds ka

$$\begin{cases} p^{\alpha} | n \\ p^{\alpha+1} \nmid n \end{cases}$$

(skaitli α sauc 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. $ord_2(96) = 5$, $ord_2(15) = 0$.

1.6. teorēma. (*Aritmētikas pamatteorēma, viennozīmīgās faktorizācijas teorēma*) $\forall\ n \in \mathbb{N}$ ir viennozīmīgi izsakāms pirmskaitļu pakāpju reizinājuma formā

$$n = p_1^{\alpha_1} p_2^{\alpha_2} ... p_m^{\alpha_m},\ \text{kur}\ \ p_i \in \mathbb{P},\ p_1 < p_2 < ... < p_m,\ \alpha_i \in \mathbb{N}.$$

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

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

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

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

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.■

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

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

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

1.4. piezīme. Simboliski varam definēt

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

1.5. piezīme. Ja ir doti vairāki skaitļi, tad lietderīgi ir uzskatīt, ka

tiem atbilstošās pirmskaitļu kopas ir vienādas, papildinot tās, ja nepieciešams, piemēram:

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

1.7. 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:

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

1.2.2. LKD un MKD atrašana

1.8. teorēma. $a|b \iff \forall\, p \in \mathbb{P}$ izpildās nosacījums

$$ord_p(a) \leq ord_p(b).$$

PIERĀDĪJUMS

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

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

$$\forall\, p \in \mathbb{P}:\ p^{\alpha}|a \ \wedge\ a|b \implies p^{\alpha}|b \implies ord_p(a) \leq ord_p(b). \ \blacksquare$$

1.9. 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. $\blacksquare$

1.10. teorēma.

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

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

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

1.6. piemērs. $LKD(24,18) = LKD(2^3 3^1, 2^1 3^2) = 2^1 3^1 = 6.$
$MKD(24,18) = MKD(2^3 3^1, 2^1 3^2) = 2^3 3^2 = 72.$

2. 3.mājasdarbs

3.1 Pierādīt, ka eksistē bezgalīgi daudz pirmskaitļu formā $4n-1$.

3.2 Pierādīt, ka visiem $n \in \mathbb{N}, n > 1$ summa

$$1 + \frac{1}{2} + \frac{1}{3} + ... + \frac{1}{n} \notin \mathbb{N}.$$

3.2 Gada uzdevumi.

(a) Kāda ir 2 kārta skaitlim 2010! ?
(b) Ar kādu maksimālo 2010 pakāpi dalās 2010! ?

3.2 Dots $n = n = p_1^{\alpha_1}...p_m^{\alpha_m}$. Atrast

(a) n naturālo dalītāju skaitu,
(b) n naturālo dalītāju summu.

3.3 Atrast mazāko naturālo skaitli n, kas vienlaicīgi apmierina šādas trīs īpašības:

(a) $2n$ ir naturāla skaitļa kvadrāts,
(b) $3n$ ir naturāla skaitļa kubs (trešā pakāpe),
(c) $5n$ ir naturāla skaitļa piektā pakāpe.

3.4 Atrisināt veselos skaitļos vienādojumu

$$y^n = x^2 + x, \text{ kur } n \in \mathbb{N}, n > 1.$$

3.5 Cik ir skaitļu $n \in \mathbb{N}: \ 1 \leq n \leq 10^5$, tādu, ka n nav ne naturāla skaitļa kvadrāts, ne kubs, ne piektā pakāpe?

3.6 Atrast $MKD(10, 11, ..., 30)$.