DAUGAVPILS UNIVERSITĀTE
Dabaszinātņu un matemātikas fakultāte
Matemātikas katedra

Studiju kurss

Veselo skaitļu teorija

2.lekcija

Docētājs: Dr. P. Daugulis

2009./2010.studiju gads

Saturs

Lekcijas mērķis:

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

Lekcijas kopsavilkums:

- no Eiklīda algoritma seko vairāki secinājumi par dalāmību u.c.,
- katru veselu skaitli var viennozīmīgi izteikt pirmskaitļu pakāpju reizinājuma formā.

Svarīgākie jēdzieni: kopīgie daudzkārtņi, mazākais kopīgais daudzkārtnis (MKD), pirmskaitļa kārta.

Svarīgākie fakti un metodes: no Eiklīda algoritma izrietošās dalāmības īpašības, lineārās kombinācijas īpašība, paplašinātais Eiklīda algoritms, MKD īpašības, pirmskaitļu īpašības, Erastotena siets, viennozīmīgās faktorizācijas teorēma, LKD un MKD atrašana.

1. Eiklīda algoritma pielietojumi

1.1. Dalāmības īpašības

Bieži tiks izmantots šāds secinājums no Eiklīda algoritma:

$$D(a, b) = D(LKD(a, b)).$$

1.1. teorēma. (secinājumi no Eiklīda algoritma)

1. $\forall\, a, b \in \mathbb{Z}, m \in \mathbb{N}:\ LKD(am, bm) = m \cdot LKD(a, b).$
2. $\forall\, a, b \in \mathbb{Z}, d \in D(a, b):$
$$LKD\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{LKD(a, b)}{d}.$$
3. $\forall\, a, b \in \mathbb{Z}:$
$$LKD\left(\frac{a}{LKD(a, b)}, \frac{b}{LKD(a, b)}\right) = 1.$$
4. $\forall\, a, b, c \in \mathbb{Z}:\ LKD(a, b) = 1 \implies LKD(ac, b) = LKD(c, b).$

5. $\forall\, a, b, c \in \mathbb{Z}: \begin{cases} LKD(a,b) = 1 \\ a|bc \end{cases} \Longrightarrow a|c.$

6. $\forall\, a, b, c \in \mathbb{Z}:\; LKD(a,bc) = 1 \iff \begin{cases} LKD(a,b) = 1 \\ LKD(a,c) = 1. \end{cases}$

PIERĀDĪJUMS

1. Eiklīda algoritms ar sākuma datiem (am, bm) atšķiras no Eiklīda algoritma ar sākuma datiem (a, b) ar to, ka visas dalīšanas vienādības tiek reizinātas ar m.

2. $LKD(a,b) = LKD(\frac{a}{d} \cdot d, \frac{b}{d} \cdot d) = d \cdot LKD(\frac{a}{d}, \frac{b}{d})$.

3. Iepriekšējā apgalvojuma speciālgadījums.

4. Apzīmēsim $\begin{cases} d_1 = LKD(ac,b), \\ d_2 = LKD(c,b). \end{cases}$

$$\begin{cases} d_1|ac \\ d_1|b \Longrightarrow d_1|bc \end{cases} \Longrightarrow d_1|\underbrace{LKD(ac,bc)}_{=c}.$$

$$\left\{\begin{array}{l} d_1|c \\ d_1|b \end{array}\right. \implies d_1|\underbrace{LKD(b,c)}_{=d_2}.$$

$$\left\{\begin{array}{l} d_2|ac \\ d_2|b \end{array}\right. \implies d_2|\underbrace{LKD(ac,b)}_{=d_1} \implies d_1 = d_2.$$

5. $a|bc \implies LKD(a,bc) = a \underbrace{\implies}_{4.} LKD(a,c) = a \implies a|c.$

6. $\left\{\begin{array}{l} LKD(a,b) = 1 \\ LKD(a,c) = 1. \end{array}\right. \implies \underbrace{LKD(a,b)}_{=1} = LKD(a,bc) = 1.$

$\Big(LKD(a,b) = d > 1 \vee LKD(a,c) = d > 1\Big) \implies d|a \wedge d|bc \implies LKD(a,bc) \neq 1.$ ■

1.1. piemērs.

1. $LKD(8,12) = 4 \cdot LKD(2,3) = 4.$
2. $LKD(8/2, 12/2) = \frac{LKD(8,12)}{2} = 4/2 = 2 = LKD(4,6).$
3. $LKD(8/4, 12/4) = \frac{LKD(8,12)}{4} = 4/4 = 1.$
4. $LKD(10,3) = LKD(2 \cdot 5, 3) = LKD(5,3) = 1.$
5. $2|7a \implies 2|a.$
6. $LKD(2,3a) = 1 \iff LKD(2,a) = 1.$

1.2. Lineārās kombinācijas īpašība

1.2. teorēma.

1. $\forall\ a,b,x,y \subseteq \mathbb{Z}\ \exists\ c \in \mathbb{Z}:$
$$xa + yb = LKD(a,b) \cdot c.$$
2. $\forall\ a,b \subseteq \mathbb{Z}\ \exists\ u,v \subseteq \mathbb{Z}:$
$$LKD(a,b) = ua + vb.$$
($LKD(a,b)$ ir a un b lineāra kombinācija ar veseliem koeficientiem - Bezū vienādība.)

PIERĀDĪJUMS Apzīmēsim $LKD(a,b)$ ar d.

1. $d|xa \ \wedge \ d|yb \implies d|xa+yb \implies xa+yb = d\cdot c.$

2. $b|a \implies LKD(a,b) = b = 0\cdot a + 1\cdot b.$

Pieņemsim, ka $b \nmid a$, $a > b$. Realizēsim Eiklīda algoritmu ar sākuma datiem (a,b) un iegūsim vienādību sistēmu

$$\begin{cases} a = q_1 b + r_1 \\ b = q_2 r_1 + r_2 \\ r_1 = q_3 r_2 + r_3 \\ \ldots \\ r_{n-3} = q_{n-1} r_{n-2} + r_{n-1} \\ r_{n-2} = q_n r_{n-1}. \end{cases}$$

Sākot no pirmās vienādības, izteiksim pēctecīgi $r_1, r_2, ..., r_{n-1}$ kā a un b lineāru kombināciju ar veseliem koeficientiem (*paplašinātais Eiklīda algoritms*). ■

1.2. piemērs. Izteiksim 1 kā skaitļu 87 un 13 lineāru kombināciju ar veseliem koeficientiem:

- $9 = 87 - 6 \cdot 13$
- $4 = 13 - 1 \cdot 9 = 13 - 1 \cdot (87 - 6 \cdot 13) = 7 \cdot 13 - 1 \cdot 87$
- $1 = 9 - 2 \cdot 4 = (87 - 6 \cdot 13) - 2 \cdot (2 \cdot 13 - 1 \cdot 87) = 3 \cdot 87 - 20 \cdot 13.$

1.3. Kopīgie daudzkārtņi

$b \in \mathbb{Z}$ daudzkārtņu kopu apzīmēsim ar $M(b)$:

$$a \in M(b) \iff a = qb, \text{ kur } q \in \mathbb{Z}.$$

1.1. piezīme. $M(\pm 1) = \mathbb{Z}$.
$M(-b) = M(b)$.
$\forall\, b \in \mathbb{Z}\ |M(b)| = \infty$. Eksistē minimālais pozitīvais elements.
$M(b)$ minimālais pozitīvais elements ir vienāds ar $|b|$.

$c \in \mathbb{Z}$ sauksim par kopas $\{b_1, ..., b_n\} \subseteq \mathbb{Z}$ *kopīgu daudzkārtni*, ja $\forall\ i\ b_i|c$. Apzīmēsim $\{b_1, ..., b_n\}$ daudzkārtņu kopu ar $M(b_1, ..., b_n)$:

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

Mazāko pozitīvo $M(b_1, ..., b_n)$ elementu sauc par *mazāko kopīgo daudzkārtni*, apzīmē ar MKD:

$$MKD(b_1, ..., b_n) = \min(M(b_1, ..., b_n) \cap \mathbb{N}).$$

1.3. piemērs. $MKD(2, 3, 4) = 12$.

1.3. teorēma.

1. $\forall\ a, b \subseteq \mathbb{Z}:\ M(a, b) = M(MKD(a, b))$.
2. $\forall\ a, b \subseteq \mathbb{Z}:\ MKD(a, b) = \frac{|a||b|}{LKD(a,b)}$.

PIERĀDĪJUMS Pieņemsim, ka $a > 0$, $b > 0$. Apzīmēsim $d = LKD(a, b)$, $a = da'$, $b = db'$, $LKD(a', b') = 1$.

$$c \in M(a, b) \Longrightarrow \begin{cases} a|c \\ b|c \end{cases} \Longrightarrow \begin{cases} c = aq \\ c = aq = bq_1 \end{cases} \Longrightarrow$$

$$\frac{c}{b} = \frac{aq}{b} = \frac{(da')q}{(db')} = \frac{a'q}{b'} \in \mathbb{Z} \Longrightarrow b'|q \Longrightarrow q = b't \Longrightarrow$$

$$c = b\frac{a'q}{b'} = \frac{ba'b't}{b'} = \frac{a'bd}{d}t = \frac{ab}{d}t.$$

Mazākā pozitīvā c vērtība tiks pieņemta, kad $t = 1$. Tātad

$$MKD(a,b) = \frac{ab}{LKD(a,b)}.$$

Redzam, ka $\forall\ c \in M(a,b)\ MKD(a,b)|c.$ ■

1.4. piemērs. $MKD(4,6) = \frac{4 \cdot 6}{LKD(4,6)} = \frac{24}{2} = 12.$

2. Pirmskaitļi un aritmētikas pamatteorēma

2.1. Pirmskaitļu īpašības

2.1.1. Pamatīpašības

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

2.1. 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 ir lielāks nekā jebkurš kopas $\{p_1, ..., p_n\}$ elements, tātad ir iegūta pretruna. ■

2.1. 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.

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

2.1.2. 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;

... ...

2.2. 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 $2, 3, 5, 7, 11, 13, 17, 19, 23, 29$.

2.2. Aritmētikas pamatteorēma un tās sekas

2.2.1. Teorēma

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

$$p^{\alpha} | n \text{ un } p^{\alpha+1} \nmid n$$

(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.■

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

2.3. teorēma. (*Aritmētikas pamatteorēma, viennozīmīgās faktorizā-cijas 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.■

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

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

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

2.3. piezīme. Simboliski varam definēt

$$n = \prod_p p^{\alpha_n}, \text{ kur } \alpha_n \geq 0,$$

$$0 = \prod_p p^{+\infty}, 1 = \prod_p p^0.$$

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

$$24 = 2^3 3^2 5^0 7^0, 35 = 2^0 3^0 5^1 7^1.$$

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

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

PIERĀDĪJUMS Izmantojam reizināšanas komutatīvo īpašību, piemēram:

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

2.2.2. LKD un MKD atrašana

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

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

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

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

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

2.6. 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. ■

2.7. teorēma. Dots, ka

$$a = p_1^{\alpha_1} ... p_m^{\beta_m},$$

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

Tad

1. $LKD(a, b) = p_1^{\gamma_1} ... p_m^{\gamma_m}$, kur $\gamma_i = \min(\alpha_i, \beta_i)$.
2. $MKD(a, b) = p_1^{\delta_1} ... p_m^{\delta_m}$, kur $\delta_i = \max(\alpha_i, \beta_i)$.

PIERĀDĪJUMS

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

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

$\exists\, p_j \in \mathbb{P}:\ ord_{p_j}(d) < \gamma_j \Longrightarrow d$ 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 $c = MKD(a, b)$. $\forall\, p \in \mathbb{P}$:

$$\left\{\begin{array}{l} ord_p(d) \geq ord_p(a) \\ ord_p(d) \geq ord_p(b) \end{array}\right. \implies ord_p(d) \geq \max(ord_p(a), ord_p(b)).$$

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

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

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

3. 2.mājasdarbs

3.1. Obligātie uzdevumi

2.1 Atrodiet $ord_2(20!)$.

2.2 Sadalīt pirmskaitļu pakāpju reizinājumā

(a) 10705345560000,
(b) 82861.

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

2.4 Atrodiet visus $n \in \mathbb{N}$, kuriem $2^n + 2$ ir naturāla skaitļa kvadrāts. (*Norādījums: ja n ir naturāla skaitļa kvadrāts, tad $ord_2(n)$ ir pāra skaitlis*).

2.5 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 $x|n$, tad $ord_p(x) \leq ord_p(n)$*).

3.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi

2.6 Kuras no dotajām vienādībam ir patiesas?

(a) $LKD(LKD(a, b), LKD(a, c)) = LKD(LKD(a, b), c)$,

(b) $LMKD(LKD(a, b), MKD(a, c)) = MKD(LKD(a, b), c)$,

(c) $LKD(a, b)LKD(c, d) = LKD(ac, ad, bc, bd)$,

(d) $MKD(ab, ac, bc)LKD(a, b, c) = abc$.