DAUGAVPILS UNIVERSITĀTE
Dabaszinātņu un matemātikas fakultāte
Matemātikas katedra

Studiju kurss

SKAITĻU TEORIJA

2.lekcija

Docētājs: Dr. P. Daugulis

2012./2013.studiju gads

Saturs

Lekcijas mērķis:

- apgūt svarīgākās Eiklīda algoritma sekas,

Lekcijas kopsavilkums:

- no Eiklīda algoritma seko vairāki secinājumi par dalāmību u.c.

Svarīgākie jēdzieni: lineārā kombinācija ar veseliem koeficientiem, kopīgie daudzkārtņi, mazākais kopīgais daudzkārtnis (MKD).

Svarīgākie fakti un metodes: lineārās kombinācijas īpašība, Blankinšipa algoritms, MKD īpašības.

1. Eiklīda algoritma sekas un lietojumi

1.1. Dalāmības īpašības - Eiklīda algoritma sekas

1.1. teorēma. $x \in D(a,b) \implies x \mid LKD(a,b)$.

PIERĀDĪJUMS $D(a,b) = D(LKD(a,b))$. ■

1.1. piezīme. Seko, ka LKD ir "lielākais" kopīgais dalītājs divās nozīmēs: 1) pēc absolūtās vērtības un 2) dalāmības (eksistē ceļš Hasses grafā no LKD uz jebkuru pozitīvu dalītāju).

1.2. teorēma. (vienkāršākie secinājumi no Eiklīda algoritma)

1. $\forall\ a,b \in \mathbb{Z}, m \in \mathbb{N}:\ LKD(am,bm) = m \cdot LKD(a,b)$.
2. $\forall\ a,b \in \mathbb{Z}, \forall\ d \in D(a,b):$

$$LKD\left(\frac{a}{d},\frac{b}{d}\right) = \frac{LKD(a,b)}{d}.$$

3. $\forall\ a, b \in \mathbb{Z}$:

$$LKD\Big(\frac{a}{LKD(a,b)}, \frac{b}{LKD(a,b)}\Big) = 1.$$

4. $\forall\ a, b, c \in \mathbb{Z}$: $LKD(a,b) = 1 \implies LKD(ac,b) = LKD(c,b)$.

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

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 algoritmam ar sākuma datiem $\left[\frac{am}{bm}\right]$ pārveidojumi neatšķiras no Eiklīda algoritma ar sākuma datiem $\left[\frac{a}{b}\right]$- pirmajā gadījumā m var iznest kā reizinātāju.

Seko, ka $LKD(am, bm) = m \cdot LKD(a,b)$.

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

3. Iepriekšējā apgalvojuma speciālgadījums.

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

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

$$\begin{cases} d_1 \mid c \\ d_1 \mid b \end{cases} \Longrightarrow d_1 \mid \underbrace{LKD(b,c)}_{=d_2}.$$

$$\begin{cases} d_2 \mid ac \\ d_2 \mid b \end{cases} \Longrightarrow d_2 \mid \underbrace{LKD(ac,b)}_{=d_1} \Longrightarrow d_1 = d_2.$$

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

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

$$\Big(LKD(a,b) = d > 1 \ \vee \ LKD(a,c) = d > 1 \Big) \implies \left\{ \begin{array}{l} d \Big| a \\ d \Big| bc \end{array} \right. \implies$$

$LKD(a,bc) \neq 1.$ ■

1.1. piemērs.

1. $LKD(8,12) = 4 \cdot LKD(2,3) = 4.$
2. $LKD(8/2, 12/2) = \dfrac{LKD(8,12)}{2} = 4/2 = 2 = LKD(4,6).$
3. $LKD(8/4, 12/4) = \dfrac{LKD(8,12)}{4} = 4/4 = 1.$

4. $LKD(10,3) = LKD(2 \cdot 5, 3) = LKD(5,3) = 1.$
5. $2|7a \iff 2|a.$
6. $LKD(2,3a) = 1 \iff LKD(2,a) = 1.$

1.2. Lineārās kombinācijas īpašība

1.2.1. Teorija

1.3. 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. $\left\{ \begin{array}{l} d \big| xa \\ d \big| yb \end{array} \right. \Longrightarrow\ d \big| xa + yb \Longrightarrow\ xa + yb = d \cdot c.$

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

Apakšgadījums $b \nmid a$. Tiek dots algoritms koeficientu u un v atrašanai.

Algoritms u un v atrašanai (*Blankinšipa algoritms*):

1. Izveidot matricu
$$\mathbf{M} = \left[\begin{array}{cc|c} 1 & 0 & a \\ 0 & 1 & b \end{array}\right] = [\mathbf{E}_2|\mathbf{k}], \text{ kur } \mathbf{k} = \left[\begin{array}{c} a \\ \hline b \end{array}\right].$$
2. Sākot ar $\mathbf{M}$ veikt REP3 atbilstoši Eiklīda algoritmam:
$$\left[\begin{array}{c|c|c} 1 & 0 & a \\ \hline 0 & 1 & b \end{array}\right] \overset{R_{21}(-q_1)}{\longrightarrow} \left[\begin{array}{c|c|c} 1 & -q_1 & r_1 \\ \hline 0 & 1 & b \end{array}\right] \overset{R_{12}(-q_2)}{\longrightarrow}$$
$$\left[\begin{array}{c|c|c} 1 & -q_1 & r_1 \\ \hline -q_2 & 1+q_1q_2 & r_2 \end{array}\right] \longrightarrow \ldots \longrightarrow \left[\begin{array}{c|c|c} u & v & d \\ \hline w & z & 0 \end{array}\right]$$
3. No matricas rindas, kura satur d pēdējā kolonnā, nolasīt u, v.

Algoritma pamatojums:

1. **M** tiek interpretēta LVS
$$\begin{cases} X_1 + & = a \\ & X_2 = b \end{cases}$$
paplašinātā matrica, kuras atrisinājums ir **k**,
2. veicot REP3 saskaņā ar Eiklīda algoritmu, tiek iegūta brīvo locekļu kolonna $\left[\begin{array}{c} d \\ \hline 0 \end{array}\right]$ vai $\left[\begin{array}{c} 0 \\ \hline d \end{array}\right]$,
3. REP3 saglabā LVS atrisinājumu $\begin{cases} X_1 = a \\ X_2 = b \end{cases} \Longrightarrow$ vienu matricas rindu var interpretēt kā vienādību $ua + vb = d$.

1.2. piemērs. Izteiksim 1 kā skaitļu 87 un 13 lineāru kombināciju ar veseliem koeficientiem:
$$\left[\begin{array}{c|c|c} 1 & 0 & 87 \\ \hline 0 & 1 & 13 \end{array}\right] \xrightarrow{R_{21}(-6)} \left[\begin{array}{c|c|c} 1 & -6 & 9 \\ \hline 0 & 1 & 13 \end{array}\right] \xrightarrow{R_{12}(-1)}$$
$$\left[\begin{array}{c|c|c} 1 & -6 & 9 \\ \hline -1 & 7 & 4 \end{array}\right] \xrightarrow{R_{21}(-2)} \left[\begin{array}{c|c|c} 3 & -20 & 1 \\ \hline -1 & 7 & 4 \end{array}\right].$$

1.3. Kopīgie daudzkārtņi

1.3.1. Definīcijas

$b \in \mathbb{Z}$ daudzkārtņu kopa - $M(b)$:

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

1.2. piezīme. $M(\pm 1) = \mathbb{Z}$.

$M(-b) = M(b)$.

$\forall\ b \in \mathbb{Z}, b \neq 0 :\ |M(b)| = \infty$. 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:

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

1.3. piemērs. $MKD(2, 3, 4) = 12$.

1.3.2. Īpašības

1.4. teorēma.

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

PIERĀDĪJUMS Uzskatīsim, ka $\forall$ skaitļi ir pozitīvi. Apzīmēsim $d = LKD(a, b)$, tad $\begin{cases} a = da' \\ b = db' \\ LKD(a', b') = 1. \end{cases}$

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

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

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

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

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

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

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

1.3. piezīme. No teorēmas 1.apgalvojuma seko šāds praktiski svarīgs

secinājums

$$\begin{cases} a|n \\ b|n \end{cases} \iff MKD(a,b)\Big|n.$$

1.4. Vairāku skaitļu LKD un MKD

1.5. teorēma.

1. $LKD(b_1,...,b_{n-1},b_n) = LKD(LKD(b_1,...,b_{n-1}),b_n)$.
2. $MKD(b_1,...,b_{n-1},b_n) = MKD(MKD(b_1,...,b_{n-1}),b_n)$.

(pietiek prast atrast divu skaitļu LKD un MKD).

PIERĀDĪJUMS (Patstāvīgi) Izmantosim matemātisko indukciju ar parametru n:

1) apgalvojums ir patiess, ja $n \in \{1,2\}$,

2) pieņemsim, ka apgalvojums

$$\begin{cases} D(b_1,...,b_m) = D(LKD(b_1,...,b_m)) \\ LKD(b_1,...,b_m) = LKD(LKD(b_1,...,b_{m-1}),b_m) \end{cases}$$

ir patiess visām virknēm ar garumu $m \leq n-1$ un pierādīsim, ka tad apgalvojums ir patiess visām virknēm ar garumu $m = n$.

$$D(b_1, ..., b_n) = D(b_1) \cap ... \cap D(b_{n-1}) \cap D(b_n) =$$
$$\Big(D(b_1) \cap ... \cap D(b_{n-1})\Big) \cap D(b_n) = D(b_1, ..., b_{n-1}) \cap D(b_n) =$$
$$D(LKD(b_1, ..., b_{n-1})) \cap D(b_n) = D(LKD(b_1, ..., b_{n-1}), b_n) =$$
$$D(LKD(LKD(b_1, ..., b_{n-1}), b_n)) = D(LKD(b_1, ..., b_n))$$

$$\Longrightarrow \; LKD(b_1, ..., b_n) = LKD(LKD(b_1, ..., b_{n-1}), b_n).$$

Līdzīgā veidā pierāda apgalvojumu par MKD:

$$M(b_1, ..., b_n) = M(b_1) \cap ... \cap M(b_{n-1}) \cap M(b_n) =$$
$$\Big(M(b_1) \cap ... \cap M(b_{n-1})\Big) \cap M(b_n) = M(b_1, ..., b_{n-1}) \cap M(b_n) =$$
$$M(MKD(b_1, ..., b_{n-1})) \cap M(b_n) = M(MKD(b_1, ..., b_{n-1}), b_n).$$

$$\Longrightarrow \quad MKD(b_1, ..., b_n) = MKD(MKD(b_1, ..., b_{n-1}), b_n).$$

1.5. piemērs. $LKD(21, 12, 121) = LKD(LKD(21, 12), 121) = LKD(3, 121) = 1.$

2. 2.mājasdarbs

2.1. Obligātie uzdevumi

2.1 Izteikt 1 kā skaitļu a un b lineāru kombināciju ar veseliem koeficientiem.

(a) $a = 17$, $b = 19$;
(b) $a = 610$, $b = 987$.

2.2 Atrast skaitļu a un b LKD un MKD izmantojot Eiklīda algoritmu.

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

2.3 Izteikt 1 kā skaitļu a_i lineāru kombināciju ar veseliem koeficientiem.

(a) $a_1 = 17$, $a_2 = 19$, $a_3 = 3$;
(b) $a_1 = 15$, $a_2 = 21$, $a_3 = 35$.
(c) $a_1 = 105$, $a_2 = 165$, $a_3 = 231$, $a_4 = 385$.

2.2. Paaugstinātas grūtības un pētnieciska rakstura uzdevumi

2.4 Kuras no dotajām vienādībam ir patiesas?

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

(b) $LKD\Big(LKD(a,b), MKD(a,c)\Big) = MKD\Big(LKD(a,b), c\Big)$,

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

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