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

***Studiju kurss***

# Veselo skaitļu teorija

## 2.lekcija

***Docētājs: Dr. P. Daugulis***

***2009./2010.studiju gads***

# Saturs

**Lekcijas mērķis:**

- apgūt Eiklīda algoritmu un tā lietojumus.

**Lekcijas kopsavilkums:**

- var piedāvāt algoritmu, ar kura palīdzību var atrast divu skaitļu $LKD$ - Eiklīda algoritmu,
- analizējot Eiklīda algoritmu, var iegūt vairākus lietderīgus secinājumus par dalāmību, kopīgajiem daudzkārtņiem u.c.
- Eiklīda algoritma sekas var izmantot lineāru vienādojumu risināšanā.

**Svarīgākie jēdzieni:** kopīgie daudzkārtņi, mazākais kopīgais daudzkārtnis (MKD), lineārie Diofanta vienādojumi,

**Svarīgākie fakti un metodes:** Eiklīda algoritms, Eiklīda algoritma pareizības pierādījums, dalāmības īpašības, kas seko no Eiklīda algoritma, MKD īpašības, lineārās kombinācijas īpašība, homogēnu lineāru vienādojumu risināšana, nehomogēnu lineāru vienādojumu risināšana.

# 1. Eiklīda algoritms un tā sekas

## 1.1. Algoritms

### 1.1.1. Apraksts

Meklēsim naturālu skaitļu $a$ un $b$ LKD, $a > b$. Sākam ar pāri $(a, b)$.

Vispārējā ideja: ja ir dots skaitļu pāris $\{u, v\}$, kur $u > v$, tad pāriesim uz "mazāku" pāri $\{\underbrace{atl(u,v)}_{=u-qv}, v\}$ - abiem pāriem ir vienādas dalītāju kopas, un tāpēc arī LKD.

1. Dalām $a$ ar $b$:

$$\boxed{a = q_1 b + r_1}.$$

Pārejam uz pāri $(b, r_1)$. $LKD(a, b) = LKD(b, r_1)$. Ja $r_1 = 0$, tad apstājamies, ja nē, tad pārejam uz 2. soli.

2. Dalām $b$ ar $r_1$:

$$\boxed{b = q_2 r_1 + r_2}.$$

Pārejam uz pāri $(r_1, r_2)$. $LKD(b, r_1) = LKD(r_1, r_2)$. Ja $r_2 = 0$, tad apstājamies, ja nē, tad ejam uz 3. soli.

3. Dalām $r_1$ ar $r_2$:

$$\boxed{r_1 = q_3 r_2 + r_3}.$$

Pārejam uz pāri $(r_2, r_3)$. $LKD(r_1, r_2) = LKD(r_2, r_3)$. Ja $r_3 = 0$, tad apstājamies, ja nē, tad ejam uz 4. soli.

.....

i. Dalām $r_{i-2}$ ar $r_{i-1}$:

$$\boxed{r_{i-2} = q_i r_{i-1} + r_i}.$$

Pārejam uz pāri $(r_{i-1}, r_i)$. $LKD(r_{i-2}, r_{i-1}) = LKD(r_{i-1}, r_i)$. Ja $r_i = 0$, tad apstājamies, ja nē, tad ejam uz soli $i + 1$. soli.

.....

Virkne $r_1, r_2, ...$ ir stingri dilstoša, tāpēc šī algoritma realizācijā soļu skaits ir galīgs.

Ja ir veikti $n$ soļi, tad algoritma izpildes rezultātā tiek iegūta skaitļu pāru virkne

$$(a, b) \to (b, r_1) \to (r_1, r_2) \to ... \to (r_{n-1}, 0).$$

### 1.1.2. Algoritma pareizības pierādījums

**1.1. teorēma.** Pieņemsim, ka tiek realizēts Eiklīda algoritms ar sākuma datiem $(a, b)$, kur $a > b > 0$, $b \nmid a$, tiek veikti $n$ soļi, pēdējais nenulles atlikums ir $r_{n-1}$.

1. $LKD(a, b) = r_{n-1}$ ($LKD$ ir vienāds ar pēdējo nenulles algoritmu).
2. $D(a, b) = D(r_{n-1})$ ($LKD$ ir "lielākais" 2 nozīmēs: parastajā un dalāmības nozīmē).

PIERĀDĪJUMS

Saskaņā ar iepriekšējo teorēmu

$$D(a,b) = D(b,r_1) = D(r_1,r_2) = ... = D(r_{n-1},0) = D(r_{n-1}).$$

un

$$LKD(a,b) = LKD(b,r_1) = LKD(r_1,r_2) = ...$$
$$= LKD(r_{n-2},r_{n-1}) = LKD(r_{n-1},0) = r_{n-1}.$$

■

**1.1. piemērs.** Atradīsim $LKD(87,13)$ izmantojot Eiklīda algoritmu.

1. $87 = 6 \cdot 13 + 9$, $(87,13) \to (13,9)$.
2. $13 = 1 \cdot 9 + 4$, $(13,9) \to (9,4)$.
3. $9 = 2 \cdot 4 + 1$, $(9,4) \to (4,1)$.
4. $4 = 4 \cdot 1$, $(4,1) \to (1,0)$.

Tātad $LKD(87,13) = 1$.

**1.1. piezīme.** Ņemot vērā īpašību $D(-a) = D(a)$, Eiklīda algoritmu var izmantot veselu, ne obligāti pozitīvu, skaitļu, $LKD$ atrašanai.

**1.2. teorēma.** $LKD(b_1, ..., b_{n-1}, b_n) = LKD(LKD(b_1, ..., b_{n-1}), b_n)$ (pietiek prast atrast divu skaitļu $LKD$).

## 1.2. Eiklīda algoritma lietojumi

### 1.2.1. Dalāmības īpašības

Bieži tiks izmantots šāds secinājums no Eiklīda algoritma:

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

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

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

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

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

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

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

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

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

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

6. $\begin{cases} LKD(a, b) = 1 \\ LKD(a, c) = 1. \end{cases} \Longrightarrow \underbrace{LKD(a, b)}_{=1} = LKD(a, bc) = 1.$

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

**1.2. 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. $LKD(2,3a)=1 \iff LKD(2,a)=1.$

### 1.2.2. Kopīgie daudzkārtņi

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

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

**1.2. 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 $M(b_1, ..., b_n)$.

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

**1.3. piemērs.** $MKD(2, 3, 4) = 12$.

**1.4. teorēma.**

1. $\forall\ a, b \subseteq \mathbb{Z} :\ \ M(a, b) = M\Big(MKD(a, b)\Big)$ ($MKD$ ir "mazākais" divās nozīmēs: parastajā un dalāmības nozīmē).
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.** $MKD(4,6) = \frac{4\cdot 6}{LKD(4,6)} = \frac{24}{2} = 12$.

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

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

### 1.2.3. Lineārās kombinācijas īpašība

**1.5. 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

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

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*). ■

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

- $9 = 87 - 6 \cdot 13$
- $4 = 13 - 1 \cdot 9 = 13 - 1 \cdot (87 - 6 \cdot 13) = 7 \cdot 13 - 1 \cdot 87$

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

# 2. Lineāri vienādojumi ar diviem nezināmajiem

## 2.1. Diofanta vienādojumi

Algebrisku vienādojumu

$$F(x_1, ..., x_n) = 0$$

sauksim par *Diofanta vienādojumu*, ja polinoma $F$ koeficienti un atrisinājumi ir kopā $\mathbb{Z}$. Diofants bija 3.gs grieķu matemātiķis.

Diofanta vienādojumu atrisinājumus ģeometriski var interpretēt kā punktus ar veselām Dekarta koordinātēm, kas apmierina doto vienādojumu.

Attiecībā uz Diofanta vienādojumiem un to sistēmām var risināt vismaz šādas problēmas:

1. noteikt, vai dotajam vienādojumam eksistē vismaz viens vesels atrisinājums,
2. atrast visus dotā vienādojuma veselos atrisinājumus.

Par *lineāru Diofanta vienādojumu* sauksim Diofanta vienādojumu, kuram $F$ ir lineārs (pirmās pakāpes) polinoms. Lineārus Diofanta vienādojumus tradicionāli pieraksta formā

$$a_1x_1 + ... + a_nx_n = c.$$

Ja $c = 0$, tad vienādojumu sauksim par homogēnu.

**2.1. piemērs.** Pats vienkāršākais gadījums - lineārie Diofanta vienādojumi ar vienu nezināmo. Lineārie vienādojumi ar vienu nezināmo ir vienkārši - Diofanta vienādojumam

$$ax = b, a \neq 0$$

ir viens atrisinājums $x = \frac{b}{a} \iff a|b.$

Diofanta vienādojumu vienkāršākie ekvivalentie pārveidojumi:

- pieskaitīt abām vienādojuma pusēm veselu skaitli,
- reizināt vienādojuma koeficientus ar veselu skaitli $\neq 0$,
- dalīt vienādojuma koeficientus ar to kopīgu dalītāju.

## 2.2. Lineāri vienādojumi ar diviem nezināmiem

### 2.2.1. Homogēni vienādojumi

**2.1. teorēma.** Jebkurš vienādojuma

$$ax + by = 0$$

vesels atrisinājums ir izsakāms formā

$$\begin{cases} x = \frac{b}{d}t \\ y = -\frac{a}{d}t. \end{cases}$$

PIERĀDĪJUMS

$ax = -by \iff \frac{a}{d}x = -\frac{b}{d}y$ (dalām kreiso vienādojumu ar koeficientu kopīgu dalītāju).

$$\left\{ \begin{array}{l} LKD(\frac{a}{d}, \frac{b}{d}) = 1 \\ \frac{a}{d}x = -\frac{b}{d}y \end{array} \right. \Longrightarrow \left\{ \begin{array}{l} LKD(\frac{a}{d}, \frac{b}{d}) = 1 \\ \frac{b}{d} | \frac{a}{d}x \end{array} \right. \Longrightarrow \frac{b}{d}|x \Longrightarrow$$

$$x = \frac{b}{d}t, \text{ kur } t \in \mathbb{Z} \Longrightarrow y = -\frac{a}{d}t. \blacksquare$$

**2.2. piemērs.** Atradīsim visus atrisinājumus vienādojumam

$$4x + 6y = 0.$$

$d = 2$. Jebkurš skaitļu pāris $(3t, -2t), t \in \mathbb{Z}$ ir atrisinājums.

Atradīsim visus atrisinājumus vienādojumam

$$12x - 24y = 0.$$

$d = 12$. Jebkurš skaitļu pāris $(2t, t), t \in \mathbb{Z}$ ir atrisinājums.

### 2.2.2. Nehomogēni vienādojumi

**2.2. teorēma.** Diofanta vienādojumam

$$ax + by = c$$

$\exists$ vesels atrisinājums $(x_0, y_0) \iff d|c.$

PIERĀDĪJUMS

$d|a \ \wedge \ d|b \implies d|(ax+by) \ \forall \ x, y \in \mathbb{Z}. \ ax+by = c \implies d|c.$

Pierādīsim implikāciju otrā virzienā. $d|c \implies \exists \ q, x', y' \in \mathbb{Z}$:

$$c = qd = q\underbrace{(ax' + by')}_{=d}$$

($d$ var izteikt kā kopas $\{a, b\}$ elementu veselu lineāru kombināciju ar koeficientiem $x', y'$).

Redzam, ka

$$c = q(ax' + by') = a(qx') + b(qy')$$

un par veselu atrisinājumu var izvēlēties virkni

$$x = qx', y = qy'.\blacksquare$$

**2.3. piemērs.** Vienādojumam $4x + 6y = 5$ nevar būt veselu atrisinājumu, jo $2 \nmid 5$.

**2.3. teorēma.** Jebkurš vienādojuma

$$ax + by = c, \text{ kur } d|c,$$

atrisinājums ir izsakāms formā

$$\begin{cases} x = x_0 + \frac{b}{d}t \\ y = y_0 - \frac{a}{d}t \end{cases}$$

kur $(x_0, y_0)$ ir patvaļīgs fiksēts atrisinājums un $t \in \mathbb{Z}$.

PIERĀDĪJUMS Jebkurš veselu skaitļu pāris

$$(x_0 + \tfrac{b}{d}t, y_0 - \tfrac{a}{d}t)$$

ir nehomogēnā vienādojuma atrisinājums, jo

$$a(x_0 + \tfrac{b}{d}t) + b(y_0 - \tfrac{a}{d}t) = (ax_0 + by_0) + (a\tfrac{b}{d}t + b(-\tfrac{a}{d}t)) = c + 0 = c$$

No otras puses, ja skaitļu pāris $(x, y)$ ir nehomogēnā vienādojuma atrisinājums, tad

$$a(x - x_0) + b(y - y_0) = (ax + by) - (ax_0 + by_0) = c - c = 0,$$

tāpēc $(x - x_0, y - y_0)$ ir homogēnā vienādojuma atrisinājums un ir izsakāms formā $(\frac{b}{d}t, -\frac{a}{d}t)$. ■

**2.1. piezīme.** Nehomogēnā vienādojuma atrisinājumu $(x_0, y_0)$ var atrast izmantojot $LKD$ lineārās kombinācijas īpašību šādā veidā.

$$\begin{cases} d = LKD(a, b) \\ d|c \end{cases} \Longrightarrow \begin{cases} d = x'a + y'b \\ c = td \end{cases} \Longrightarrow$$

$$c = td = t\underbrace{(x'a + y'b)}_{=d} = a(tx') + b(ty'),$$

tāpēc veselu skaitļu pāris $(tx', ty')$ ir vienādojuma

$$ax + by = c$$

atrisinājums.

**2.4. piemērs.** Atradīsim visus atrisinājumus vienādojumam

$$4x + 6y = 8.$$

$d = 2 = (-1) \cdot 4 + 1 \cdot 6$, tāpēc skaitļu pāris

$$(x_0, y_0) = (-4, 4)$$

ir vienādojuma atrisinājums. Homogēnā vienādojuma atrisinājums ir jebkurš skaitļu pāris $(3t, -2t)$. Atrisinājumu kopa ir

$$\{(-4 + 3t, 4 - 2t) | t \in \mathbb{Z}\}.$$

## 2.3. Lineāri vienādojumi ar trīs nezināmajiem

Lineāru vienādojumu

$$a_1x + a_2y + a_3z = c$$

var risināt saskaņā ar šādu algoritmu:

1. Izteikt $a_1x + a_2y$ formā $du$, kur $d = LKD(a_1, a_2)$, $u$ - jauns nezināmais.
2. Atrisināt vienādojumu $du + a_3z = c$ attiecībā uz $u$ un $z$:
$$\begin{cases} u = u't + u_0 \\ z = z't + z_0. \end{cases}$$
3. Atrisināt vienādojumu $a_1x + a_2y = du$ attiecībā uz $x$ un $y$.

# 3. 2.mājasdarbs

2.1 Realizēt Eiklīda algoritmu skaitļiem 1326 un 4290. Atrast $LKD$, $MKD$, izteikt $LKD$ kā lineāru kombināciju.

2.2 Atrisināt vienādojumus veselos skaitļos:

(a) $7x + 9y = 11$,
(b) $12x - 16y = 24$,
(c) $3x - 4y + 5z = 7$.

2.3 Ar kādām parametra $c$ vērtībām vienādojumam

$$2x + 3y = c$$

ir 7 vai 8 pozitīvi atrisinājumi?