

*DAUGAVPILS UNIVERSITĀTE*  
*Dabaszinātņu un matemātikas fakultāte*  
*Matemātikas katedra*

DAUGAVPILS UNIVERSITĀTES  
JAUNO MATEMĀTIĶU SKOLA

Veselo skaitļu teorija - 2

*Docētājs: Dr. P. Daugulis*

*2008./2009.studiju gads*

# Saturs

<b>1. Eiklīda algoritms</b>	<b>3</b>
1.1. Eiklīda algoritma sākotnējā forma . . . . .	4
1.1.1. Eiklīda algoritma sākotnējās formas pamatojums	4
1.1.2. Algoritms . . . . .	5
1.2. Eiklīda algoritma mūsdienu forma . . . . .	8
1.2.1. Eiklīda algoritma mūsdienu formas pamatojums	8
1.2.2. Algoritms . . . . .	10
1.3. LKD kā vesela lineāra kombinācija . . . . .	12
<b>2. Eiklīda algoritma pielietojums vienādojumu risināšanā</b>	<b>15</b>

# 1. Eiklīda algoritms

Aprakstīsim divu naturālu skaitļu  $LKD$  atrašanas algoritmu, kas neizmanto sadalījumu pirmskaitļu pakāpju reizinājumā. Šo algoritms ir aprakstīts Eiklīda darbā "Elementi" ap 300 BC. Viens no senākajiem netriviālajiem algoritmiem.

Senajiem grieķiem nebija decimālā vai līdzvērtīga skaitļu pieraksta (tas parādījās tikai Agrajos Viduslaikos), ar kura palīdzību varētu ērti veikt dalīšanu, tāpēc  $LKD$  atrašanai viņi nevarēja izmantot vienzīmīgās faktorizācijas teorēmu (kas mūsdienu formā tika noformulēta tikai 18.gs). Šī iemesla dēļ tika piedāvāts cits algoritms, kas izmantotu tikai saskaitīšanu un atņemšanu.

## 1.1. Eiklīda algoritma sākotnējā forma

### 1.1.1. Eiklīda algoritma sākotnējās formas pamatojums

Eiklīda ideja: veikt vienkāršus pārveidojumus ar skaitļu pāriem, kas saglabā to  $LKD$  un samazina pašus skaitļus. Sākotnējais Eiklīda algoritms balstās uz šādu faktu.

**1.1. teorēma.**  $LKD(a, b) = LKD(b, a - b)$ .

PIERĀDĪJUMS Ja  $d \in D(a, b)$ , tad  $d|a$  un  $d|b$ . Seko, ka  $d|a - b$ , tātad  $d \in D(b, a - b)$ .

Ja  $d' \in D(b, a - b)$ , tad  $d'|a - b$  un  $d'|b$ . Seko, ka  $d'|(a - b) + b$  jeb  $d'|a$ , tātad  $d' \in D(a, b)$ .

Ja kopas  $D(a, b)$  un  $D(b, a - b)$  ir vienādas, tad ir vienādi arī to maksimālie elementi dalāmības attiecībā, tas ir

$$LKD(a, b) = LKD(a, b - a). \blacksquare$$

### 1.1.2. Algoritms

”Atkārtoti atņemam no lielākā skaitļa mazāko”. Ir uzdoti 2 pozitīvi skaitļi  $a$  un  $b$ ,  $a > b$  un  $b \nmid a$ . Definējam  $(a_0, b_0)$ :

$$\begin{cases} a_0 = a \\ b_0 = b \end{cases}$$

1. Definējam  $(a_1, b_1)$ :

$$\begin{cases} a_1 = \max(b_0, a_0 - b_0) \\ b_1 = \min(b_0, a_0 - b_0) \end{cases}$$

Ja  $a_1 = b_1$ , tad apstājamies, ja nē, tad ejam uz nākamo soli.

... ..

i. Definējam  $(a_i, b_i)$ :

$$\begin{cases} a_i = \max(b_{i-1}, a_{i-1} - b_{i-1}) \\ b_i = \min(b_{i-1}, a_{i-1} - b_{i-1}) \end{cases}$$

Ja  $a_i = b_i$ , tad apstājamies, ja nē, tad ejam uz nākamo soli.

... ..

Redzam, ka  $a_0 > a_1 > \dots > a_n > a_{n+1}$ , tāpēc algoritma izpilde apstāsies pēc galīga skaita soļu. Pēdējā solī izpildīsies vienādība

$$a_n = b_n.$$

**1.2. teorēma.** Pēdējā nenulles pāra  $(a_n, b_n)$  elementi Eiklīda algoritma realizācijā ar sākuma datiem  $(a, b)$  ir vienādi ar  $LKD(a, b)$ .

PIERĀDĪJUMS Saskaņā ar pierādīto teorēmu

$$LKD(a, b) = LKD(a_1, b_1) = \dots = LKD(a_n, b_n) = a_n.$$

■

**1.1. piemērs.** Atradīsim  $LKD(12, 33)$ . Iegūsim šādu pāru virkni:

$$(33, 12) \rightarrow (21, 12) \rightarrow (12, 9) \rightarrow (9, 3) \rightarrow (6, 3) \rightarrow (3, 3).$$

Tātad  $LKD(12, 33) = 3$ .

## 1.2. Eiklīda algoritma mūsdienu forma

### 1.2.1. Eiklīda algoritma mūsdienu formas pamatojums

L.Eilers 18.gs ievēroja, ka pārveidojumu

$$(a, b) \rightarrow (b, a - b)$$

var aizstāt ar pārveidojumu

$$(a, b) \rightarrow (b, a - kb),$$

kur  $k \geq 1$ , jo  $LKD(a, b) = LKD(b, a - kb)$ . Tādējādi, lai padarītu algoritmu ātrāku, ir vēlams katrā solī  $k$  izvēlēties pēc iespējas lielāku.

Eiklīda algoritma mūsdienu formulējums atšķiras no sākotnējā ar to, ka katrā solī mēs atņemam no lielākā skaitļa maksimāli lielāko iespējamo mazākā skaitļa daudzkārti - tādu, lai pāri paliktu tikai atlikums, ko iegūst, izdalot lielāko skaitli ar mazāko. Citiem vārdiem sakot, mūsdienu formulējums balstās uz šādu faktu.



**1.3. teorēma.** Dots, ka  $a > b, b \nmid a$ . Apzīmēsim ar  $r$  atlikumu, ko iegūst, dalot  $a$  ar  $b$ . Ja  $r > 0$ , tad  $LKD(a, b) = LKD(b, r)$ .

PIERĀDĪJUMS Pieņemsim, ka  $a = qb + r, 0 < r < b$ .

Ja  $d \in D(a, b)$ , tad  $d|a$  un  $d|b$ . Seko, ka  $d|a - bq$ , tātad  $d|r$  un  $d \in D(b, r)$ . Esam pierādījuši, ka  $D(a, b) \subseteq D(b, r)$ .

Ja  $d' \in D(b, r)$   $d'|r$  un  $d'|b$ . Seko, ka  $d'|qb + r$  jeb  $d'|a$ , tātad  $d' \in D(a, b)$ . Esam pierādījuši, ka  $D(b, r) \subseteq D(a, b)$ , tātad  $D(a, b) = D(b, r)$ .

Ja kopas  $D(a, b)$  un  $D(b, r)$  ir vienādas, tad ir vienādi arī to maksimālie elementi dalāmības attiecībā, tātad

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



### 1.2.2. Algoritms

Ir uzdoti 2 pozitīvi skaitļi  $a$  un  $b$ ,  $a > b$  un  $b \nmid a$ . Sākam ar pāri  $(a, b)$ .

1. Dalām  $a$  ar  $b$ :  $a = q_1b + r_1$ . Pārejām uz pāri  $(b, r_1)$ . Ja  $r_1 = 0$ , tad apstājamies, ja nē, tad pārejām uz 2. soli.
2. Dalām  $b$  ar  $r_1$ :  $b = q_2r_1 + r_2$ . Pārejām uz pāri  $(r_1, r_2)$ . Ja  $r_2 = 0$ , tad apstājamies, ja nē, tad ejam uz 3. soli.
3. Dalām  $r_1$  ar  $r_2$ :  $r_1 = q_3r_2 + r_3$ . Pārejām uz pāri  $(r_2, r_3)$ . Ja  $r_3 = 0$ , tad apstājamies, ja nē, tad ejam uz 4. soli.

.....

- i. Dalām  $r_{i-2}$  ar  $r_{i-1}$ :  $r_{i-2} = q_i r_{i-1} + r_i$ . Pārejām uz pāri  $(r_{i-1}, r_i)$ . Ja  $r_i = 0$ , tad apstājamies, ja nē, tad ejam uz soli  $i + 1$ . soli.

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

**1.4. teorēma.** Pēdējais nenulles atlikums Eiklīda algoritma realizācijā ar sākuma datiem  $(a, b)$  ir vienāds ar  $LKD(a, b)$ .

PIERĀDĪJUMS Saskaņā ar iepriekšējo teorēmu

$$\begin{aligned} LKD(a, b) &= LKD(b, r_1) = LKD(r_1, r_2) = \dots \\ &= LKD(r_{n-2}, r_{n-1}) = r_{n-1}. \end{aligned}$$



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

1.  $87 = 6 \cdot 13 + 9,$
2.  $13 = 1 \cdot 9 + 4,$
3.  $9 = 2 \cdot 4 + 1,$
4.  $4 = 4 \cdot 1.$

Tātad  $LKD(87, 13) = 1.$

### 1.3. LKD kā vesela lineāra kombinācija

**1.1. piezīme.** Ja  $t = xa + yb$ , tad  $LKD(a, b)|t$ , jo  $LKD(a, b)|a$  un  $LKD(a, b)|b$ . Seko, ka visiem  $x, y$  izpildās

$$xa + yb = LKD(a, b) \cdot c.$$

Var uzdot jautājumu - kādi veseli skaitļi ir izsakāmi formā

$$xa + yb?$$

**1.5. teorēma.** Katram naturālu skaitļu pārim  $(a, b)$  eksistē veselu skaitļu pāris  $(x, y)$  tāds, ka

$$LKD(a, b) = xa + yb$$

( $LKD(a, b)$  ir  $a$  un  $b$  lineāra kombinācija ar veseliem koeficientiem - Bezū vienādība.)

PIERĀDĪJUMS Realizēsīm skaitļiem  $a$  un  $b$  Eiklīda algoritmu. Pēctecīgi apskatīsim dalīšanas vienādības:

1. no vienādības  $r_1 = a - q_1 b$  seko, ka  $r_1$  ir  $a$  un  $b$  lineāra kombinācija,
2. no vienādības  $r_2 = b - q_2 r_1$  seko, ka  $r_2$  ir  $b$  un  $r_1$  un tādējādi arī  $b$  un  $a$  lineāra kombinācija,
- ...
- n-1. no vienādības  $r_{n-1} = r_{n-3} - q_{n-1} r_{n-2}$  seko, ka  $r_{n-1}$  ir  $r_{n-3}$  un  $r_{n-2}$  un tādējādi arī  $b$  un  $a$  lineāra kombinācija.



**1.2. piezīme.** No teorēmas seko, ka formā  $xa + by$  ir izsakāmi tikai  $LKD(a, b)$  daudzkārtņi.

**1.3. piemērs.** Atradīsim lineāro kombināciju skaitļiem 87 un 13:

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

**1.6. teorēma.** Jebkuriem naturāliem skaitļiem  $a_1, \dots, a_n$  eksistē veseli skaitļi  $x_1, \dots, x_n$  tādi, ka

$$LKD(a_1, \dots, a_n) = x_1 a_1 + \dots + x_n a_n = \sum_{i=1}^n x_i a_i.$$

## 2. Eiklīda algoritma pielietojums vienādojumu risināšanā

Algebrisku vienādojumu

$$F(x_1, \dots, x_n) = 0$$

un jebkuru tam ekvivalentu vienādojumu saucim par *Diofanta vienādojumu*, ja polinoma  $F$  koeficienti ir veseli skaitļi un atrisinājumi tiek meklēti kopā  $\mathbb{Z}$ . Diofants bija 3.gs grieķu matemātiķis, kurš atrisināja vairākus šī tipa vienādojumus un uzrakstīja liela apjoma darbu par šo tēmu.

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

Attiecībā uz Diofanta vienādojumiem var risināt vismaz šādas problēmas:

1. noteikt, vai dotajam vienādojumam eksistē vismaz viens vesels atrisinājums, konstruktīvi vai nekonstruktīvi,
2. atrast visus dotā vienādojuma veselos atrisinājumus, vairāk vai mazāk konstruktīvi un/vai aprakstoši,
3. saskaitīt atrisinājumus ar dotiem ierobežojumiem (kādā apgabalā).

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

$$a_1x_1 + \dots + a_nx_n = c$$

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



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  $x = \frac{b}{a}$  tad un tikai tad, ja  $a|b$ .

Tālāk šajā sadaļā risināsim lineāros Diofanta vienādojumus ar vismaz diviem nezināmajiem

$$a_1x_1 + \dots + a_nx_n = c.$$

Apzīmēsim  $LKD(a_1, \dots, a_n)$  ar  $d$ .

Izdarīsim šādu novērojumu: dalot Diofanta vienādojuma katru koeficientu ar to kopīgo dalītāju, vienādojuma atrisinājumu kopa nemainās. To var redzēt, salīdzinot atrisinājumu kopas.

**2.1. teorēma.** Jebkurš homogēnā Diofanta vienādojuma

$$ax + by = 0$$

vesels atrisinājums ir izsakāms formā

$$x = \frac{b}{d}t,$$

$$y = -\frac{a}{d}t,$$

PIERĀDĪJUMS Vienādojumi

$$ax = -by$$

un

$$\frac{a}{d}x = -\frac{b}{d}y$$

ir ekvivalenti.

Pēdējā vienādojumā koeficienti pie  $x$  un  $y$  ir savstarpēji pirmskaitļi, tāpēc  $x$  dalās ar  $\frac{b}{d}$  (jo  $\frac{a}{d}$  un  $\frac{b}{d}$  nav kopīgu reizinātāju, kas ir lielāki kā 1), citiem vārdiem sakot,

$$x = \frac{b}{d}t, \text{ kur } t \in \mathbb{Z}.$$

Beidzot iegūstam, ka

$$y = -\frac{a}{d}t.$$

**2.1. piemērs.** Atradīsim visus atrisinājumus vienādojumam

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

Šajā gadījumā  $d = 2$ . Saskaņā ar teorēmu jebkurš skaitļu pāris  $(3t, -2t)$ ,  $t \in \mathbb{Z}$  ir atrisinājums.

Atradīsim visus atrisinājumus vienādojumam

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

Šajā gadījumā  $d = 12$ . Saskaņā ar teorēmu jebkurš skaitļu pāris  $(2t, t)$ ,  $t \in \mathbb{Z}$  ir atrisinājums.

**2.2. teorēma.** Diofanta vienādojumam  $a_1x_1 + \dots + a_nx_n = c$  vesels atrisinājums eksistē tad un tikai tad, ja  $d|c$ .

PIERĀDĪJUMS

$\implies$

$d|a_i$  visiem  $i$ , tātad

$$d \mid \underbrace{(a_1x_1 + \dots + a_nx_n)}_{=c}$$

visiem veseliem  $x_1, \dots, x_n$ . Esam pierādījuši, ka ja vienādojumam  $a_1x_1 + \dots + a_nx_n = c$  ir vesels atrisinājums, tad  $d|c$ .

$\Leftarrow$

Ja  $d|c$ , tad eksistē veseli skaitļi  $q, x'_1, \dots, x'_n$  tādi, ka

$$c = qd = q \underbrace{(a_1x'_1 + \dots + a_nx'_n)}_{=d}$$

( $d$  var izteikt kā kopas  $\{a_1, \dots, a_n\}$  elementu veselu lineāru kombināciju ar koeficientiem  $x'_i$ ). Redzam, ka

$$c = q(a_1x'_1 + \dots + a_nx'_n) = a_1(qx'_1) + a_2(qx'_2) + \dots + a_n(qx'_n)$$

un par veselu atrisinājumu var izvēlēties virkni

$$x_1 = qx'_1, \dots, x_n = qx'_n.$$



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

**2.3. teorēma.** Jebkurš Diofanta vienādojuma  $ax + by = c$ ,  $d|c$  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

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

ir nehomogēnā vienādojuma atrisinājums, jo

$$\begin{aligned} a\left(x_0 + \frac{b}{d}t\right) + b\left(y_0 - \frac{a}{d}t\right) &= \\ \left(ax_0 + by_0\right) + \left(a\frac{b}{d}t + b\left(-\frac{a}{d}t\right)\right) &= \\ c + 0 &= c \end{aligned}$$

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.

Ja

$$ax_0 + by_0 = c$$

un  $d|c$ , tad  $c = td$ .  $d$  var izteikt  $a$  un  $b$  veselas lineāras kombinācijas veidā:

$$d = x'a + y'b$$

Redzam, ka

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

tāpēc varam ņemt  $x_0 = tx'$  un  $y_0 = ty'$ .

**2.3. piemērs.** Atradīsim visus atrisinājumus vienādojumam

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

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

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

ir vienādojuma atrisinājums. Homogēnā vienādojuma atrisinājums ir jebkurš skaitļu pāris formā  $(3t, -2t)$ . Saskaņā ar teorēmu vienādojuma atrisinājumu kopa ir  $\{(-4 + 3t, 4 - 2t) | t \in \mathbb{Z}\}$ .