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

Studiju kurss

Veselo skaitļu teorija

3.lekcija

Docētājs: Dr. P. Daugulis

2008./2009.studiju gads

Saturs

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 vienozīmīgās 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 $d \in D(b, a-b)$. Esam pierādījuši, ka $D(a,b) \subseteq D(b, a-b)$.

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

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 $a_0 > a_1 > ... > a_n > a_{n+1}$, 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

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

■

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

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

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

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

var aizstāt ar pārveidojumu

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

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 daudzkārtni - 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: $a = q_1 b + r_1$. Pārejam uz pāri (b, r_1). Ja $r_1 = 0$, tad apstājamies, ja nē, tad pārejam uz 2. soli.
2. Dalām b ar r_1: $b = q_2 r_1 + r_2$. Pārejam 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: $r_1 = q_3 r_2 + r_3$. Pārejam 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}: $r_{i-2} = q_i r_{i-1} + r_i$. Pārejam uz pāri (r_{i-1}, r_i). Ja $r_i = 0$, tad apstājamies, ja nē, tad ejam uz soli $i + 1$. soli.

Virkne $r_1, r_2, \ldots$ 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

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

■

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

1.3. piezīme. No teorēmas par divu skaitļu LKD kā lineāro kombināciju var secināt analoģisku rezultātu, ja LKD tiek pētīts vairāk kā diviem skaitļiem.

1.6. teorēma. (Patstāvīgais darbs) Jebkuriem naturāliem skaitļiem $a_1, ..., a_n$ eksistē veseli skaitļi $x_1, ..., x_n$ tādi, ka

$$LKD(a_1, ..., a_n) = x_1a_1 + ... + x_na_n = \sum_{i=1}^{n} x_ia_i.$$

2. Eiklīda algoritma pielietojumi

2.1. Eiklīda algoritma pielietojums racionālu skaitļu reprezentēšanā ar ķēžu daļu palīdzību

Par galīgai pozitīvu reālu skaitļu virknei $(a_1, ..., a_n, ...)$ atbilstošo *ķēžu daļu* sauksim skaitli

$$[a_1, a_2, ..., a_n, ...] = a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + ...}}}$$

Kēžu daļu sauksim par *veselu (naturālu) ķēžu daļu*, ja visi atbilstošās virknes elementi ir veseli (naturāli) skaitļi. Acīmredzami galīga vesela ķēžu daļa ir racionāls skaitlis. Redzam, ka

$$[a_1, a_2, ..., a_n] = a_1 + \frac{1}{[a_2, ..., a_n]}.$$

2.1. teorēma. Ja a un b ir naturāli skaitļi, tad

$$\frac{a}{b} = [q_1, ..., q_n],$$

kur $q_1, ..., q_n$ ir Eiklīda algoritma rezultātā iegūtie dalījumi.

PIERĀDĪJUMS Pārveidosim daļu $\frac{a}{b}$ izmantojot Eiklīda algoritma un ķēžu daļu apzīmējumus:

$$\frac{a}{b} = \frac{q_1 b + r_1}{b} = q_1 + \frac{r_1}{b} = q_1 + \frac{1}{\frac{b}{r_1}} = q_1 + \frac{1}{\frac{q_2 r_1 + r_2}{r_1}} = q_1 + \frac{1}{q_2 + \frac{r_2}{r_1}} = ...$$

Lai formāli pabeigtu pierādījumu, ir jāizmanto matemātiskās indukcijas metode ar parametru n - pieņemam, ka formula ir pareiza visiem pāriem (a, b), kuriem $n = i$ un pierādām, ka no tā seko formulas pareizība pāriem (a, b), kuriem $n = i + 1$.

■

2.1. piemērs. Izmantojot iepriekš iegūto rezultātu, iegūsim racionāla skaitļa $\frac{87}{13}$ pierakstu ķēžu daļas veidā:

$$\frac{87}{13} = 6 + \frac{1}{1 + \frac{1}{2 + \frac{1}{4}}} = [6, 1, 2, 4].$$

2.2. Eiklīda algoritma pielietojums vienādojumu risināšanā

Algebrisku vienādojumu

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

un jebkuru tam ekvivalentu vienādojumu sauksim 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

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

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

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

Apzīmēsim $LKD(a_1, ..., a_n)$ ar d.

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

2.2. 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,

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

kur $t \in \mathbb{Z}$. Beidzot iegūstam, ka

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

2.2. piemērs. Atradīsim visus atrisinājumus vienādojumam

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

Šajā gadījumā $d = 0$. 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.

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

PIERĀDĪJUMS $d|a_i$ visiem i, tāpēc

$$d| \underbrace{(a_1x_1 + ... + a_nx_n)}_{=c}$$

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

Pierādīsim implikāciju otrā virzienā. Ja $d|c$, tad eksistē veseli skaitļi $q, x'_1, ..., x'_n$ tādi, ka

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

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

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

un par veselu atrisinājumu var izvēlēties virkni

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

■

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

2.4. teorēma. Jebkurš Diofanta vienādojuma $ax+by = c, d|c$ atrisinājums ir izsakāms formā

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

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

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

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.

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 $y_0=ty'$.

2.4. 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

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

Neatrisināta problēma (Frobēniusa lineāro Diofanta vienādojumu problēma): doti naturāli skaitļi $\{a_1, ..., a_n\}$, kuriem $d = 1$, atrast mazāko naturālo skaitli $G(a_1, ..., a_n)$ tādu, ka katram $c \geq G(a_1, ..., a_n)$ vienādojumam $a_1x_1 + ... + a_nx_n = c$ ir nenegatīvi atrisinājumi. Pašlaik atrisināta tikai gadījumā, kad $n = 2$.

3. 3.mājasdarbs

1. Skaitļiem 2813 un 92 atrodiet LKD un MKD. LKD atrodiet izmantojot Eiklīda algoritmu. Izsakiet LKD kā doto skaitļu lineāru kombināciju.
2. Pierādiet, ka summa
$$\sum_{i=1}^{n} \frac{1}{i} = 1 + \frac{1}{2} + ... + \frac{1}{n}$$
nevienam $n > 1$ nav vesels skaitlis.
3. Atrodiet skaitļa 1048509/731623 pierakstu ķēžu daļas veidā.
4. Atrodiet visus veselos atrisinājumus šādiem vienādojumiem:
   a) $5x + 3y = 15$,
   b) $8x - 6y = 10$,
   c) $nx + (2n + 1)y = 2, n \in \mathbb{N}$.