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

Studiju kurss

Veselo skaitļu teorija

3.lekcija

Docētājs: Dr. P. Daugulis

2007./2008.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 viennozīmīgās faktorizācijas teorēmu (kas mūsdienu formā tika noformulēta tikai 18.gs). Šī iemesla dēļ tika piedāvāts cits algoritms, kas izmantotu tikai 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 $d \in D(a,b)$ ($D(x,y)$ apzīmējam x un y dalītāju kopu), 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

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

1. Definējam

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

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

... ...

i. Definējam

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

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

... .

Redzam, ka $a_{n+1} < a_n$, 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

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

■

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 $b \nmid a$.

1. Dalām a ar b: $a = q_1 b + r_1$. Ja $r_1 = 0$, tad apstājamies, ja nē, tad pārejam uz soli 2.
2. Dalām b ar r_1: $b = q_2 r_1 + r_2$. Ja $r_2 = 0$, tad apstājamies, ja nē, tad ejam uz soli 3.
3. Dalām r_1 ar r_2: $r_1 = q_3 r_2 + r_3$. Ja $r_3 = 0$, tad apstājamies, ja nē, tad ejam uz soli 4.

....

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

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 Pieņemsim, ka Eiklīda algoritma realizācijas pēdējais solis ir solis ar numuru n. Izteiksim iegūtos atlikumus, izmantojot algoritma soļu rezultātus. Viegli redzēt, ka

$$r_1 = a - q_1 b, \tag{1}$$

$$r_2 = b - q_2 r_1, \tag{2}$$

$$..., \tag{3}$$

$$r_{n-3} = r_{n-1} - q_{n-1} r_{n-2}, \tag{4}$$

$$r_{n-2} = q_n r_{n-1}. \tag{5}$$

Pēctecīgi aplūkojot šīs vienādības sākot no pēdējās iegūstam, ka iegūstam, ka $r_{n-1}|r_{n-2}$, $r_{n-1}|r_{n-3}$, ..., $r_{n-1}|b$, $r_{n-1}|a$, tātad r_{n-1} ir skaitļu a un b kopīgais dalītājs. Vēl ir jāpierāda, ka r_{n-1} ir lielākais kopīgais dalītājs.

Ja skaitlis c ir patvaļīgs skaitļu a un b kopīgais dalītājs, tad

1. no vienādības $r_1 = a - q_1 b$ seko, ka $c|r_1$,
2. no vienādības $r_2 = b - q_2 r_1$ seko, ka $c|r_2$,

   ...,

n. no vienādības $r_{n-2} = q_n r_{n-1}$ seko, ka $c|r_{n-1}$.

Tātad $r_{n-1} = LKD(a, b)$.■

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. Eiklīda algoritma realizācija datorprogrammas veidā

Eiklīda algoritmu var realizēt

1. iteratīvi,
2. rekursīvi.

Eiklīda algoritma rekursīvas realizācijas piemērs:

$Euclid(a, b)$;
ja $b = 0$
tad izvadīt a;
pretējā gadījumā izvadīt $Euclid(b, Atlikums(a, b))$

1.4. LKD kā vesela lineāra kombinācija

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*.)

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.

■

1.3. 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. $1 = 9 - 2 \cdot 4 = (87 - 6 \cdot 13) - 2 \cdot (2 \cdot 13 - 1 \cdot 87) = 3 \cdot 87 - 20 \cdot 13.$

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

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

PIERĀDĪJUMS No sākuma pierādīsim, ka

$$LKD(b_1, b_2, ..., b_n) = LKD(LKD(b_1, b_2), b_3, ..., b_n).$$

Apzīmēsim $LKD(a_1, ..., a_n)$ ar d:

1. $d|LKD(a_1, a_2)$, jo $d|a_1$ un $d|a_2$,
2. ja $d'|LKD(a_1, a_2)$ un $d'|a_i$ visiem $i \in \{3, ..., n\}$, tad $d|a_1$ un $d|a_2$, tāpēc $d'|d$.

Pielietojot tikko pierādīto faktu vairākas reizes, iegūsim šādu secinājumu virkni:

1. $LKD(a_1, a_2)$ ir a_1 un a_2 vesela lineāra kombinācija,
2. $LKD(LKD(a_1, a_2), a_3) = LKD(a_1, a_2, a_3)$ ir $LKD(a_1, a_2)$ un a_3 lineāra kombinācija, un tāpēc arī a_1, a_2 un a_3 vesela lineāra kombinācija,

3. $LKD(LKD(a_1, a_2, a_3), a_4) = LKD(a_1, a_2, a_3, a_4)$ ir a_1,a_2, a_3 un a_4 vesela lineāra kombinācija.

... ...

n-1. $LKD(LKD(a_1, ..., a_{n-1}), a_n)$ ir $LKD(a_1, .., .a_{n-1})$ un a_n vesela lineāra kombinācija, un tāpēc visu skaitļu a_i vesela lineāra kombinācija.

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

2.1. Eiklīda reprezentācija

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

$$[a_1, a_2, ..., a_n, ...] = a_1 + \cfrac{1}{a_2 + \frac{1}{a_3 + \frac{1}{a_4 + \cdots}}} \tag{6}$$

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

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

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. Papildus fakti par ķēžu daļām (Patstāvīgais darbs)

2.2. teorēma. Jebkurš pozitīvs racionāls skaitlis var tikt izteikts galīgas naturālas ķēžu daļas veidā tieši divos veidos.

PIERĀDĪJUMS Ja ir dots racionāls nevesels skaitlis $\frac{a}{b}$, tad to var viennozīmīgi izteikt formā $q_1 + \frac{r_1}{b}$. Turpinot šo spriedumu, var secināt, ka skaitlim $\frac{a}{b}$ atbilstošajā Eiklīda reprezentācijā $[q_1, ..., q_n]$ visi elementi, izņemot, iespējams, pēdējo (q_n) ir noteikti viennozīmīgi. Veselu skaitli q_n var izteikt divos veidos kā ķēžu daļu:

$$q_n = q_n \text{ vai } q_n = (q_n - 1) + \frac{1}{1}.$$

Tādējādi skaitli $\frac{a}{b}$ arī var izteikt divos veidos

$$\frac{a}{b} = [q_1, ..., q_n] = [a_1, ..., q_n - 1, 1].$$

■

Ja skaitļu virkne $(q_1, ..., q_n, ...)$ ir bezgalīga, tad atbilstošo ķēžu daļu definē vienādu ar $\lim_{n\to\infty}[q_1, ..., q_n]$.

2.3. teorēma. Katru iracionālu pozitīvu skaitli var viennozīmīgi izteikt bezgalīgas naturālas ķēžu daļas veidā. Ja naturāla ķēžu daļa ir bezgalīga, tā ir vienāda ar iracionālu skaitli.

PIERĀDĪUMS Aprakstīsim algoritmu, ar kuru pozitīvam iracionālam skaitlim x var atrast atbilstošo ķēžu daļu $[x_1, x_2, ...]$. Acīmredzami $x_1 = [x]$. Redzam, ka

$$x - x_1 = \frac{1}{[x_2, x_3, ...]},$$

tāpēc

$$x_2 = [\frac{1}{x - x_1}].$$

Apzīmēsim x ar y_1 un $\frac{1}{x-x_1}$ ar y_2. Redzam, ka

$$y_2 - x_2 = \frac{1}{[x_3, x_4, ...]}$$

tāpēc

$$x_3 = [\frac{1}{y_2 - x_2}].$$

Turpinot veikt šādus spriedumus, iegūsim divas rekurentas skaitļu virknes:

$$\begin{cases} y_n = \frac{1}{y_{n-1} - x_{n-1}} \\ x_n = [y_n] \end{cases}$$

Ar šīs sistēmas palīdzību var atrast x ķēžu daļu. ■

2.2. piemērs. Atradīsim skaitļa $e = 2.718281828459045235360...$ dažus pirmos ķēžu daļas elementus:

$$e = [2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 10, 1, 1, ...].$$

2.4. teorēma. Bezgalīga ķēžu daļa $x = [x_1, x_2, ...]$ ir periodiska tad un tikai tad, ja x ir iracionāls atrisinājums kvadrātvienādojumam ar veseliem koeficientiem.

3. Eiklīda algoritma pielietojums vienādojumu risināšanā

Algebrisku vienādojumu

$$F(x_1, ..., x_n) = 0 \tag{7}$$

un jebkuru tam ekvivalentu vienādojumu sauksim par *Diofanta vienādojumu*, ja polinoma F koeficienti ir veseli skaitļi. Diofanta vienādojumi parasti tiek risināti veselo skaitļu kopā. 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

$$a_1x_1 + ... + a_nx_n = c \tag{8}$$

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 $a_1x_1 + ... + a_nx_n = c$, kur vismaz vienam i $a_i \neq 0$. Apzīmēsim $LKD(a_1, ..., a_n)$ ar d.

Izdarīsim šādu novērojumu: dalot Diofanta vienādojuma katru koeficientu ar to kopīgo dalītāju, vienādojuma atrisinājumu kopa nemainās.

Ja ir dots viens vienādojums ar vairākiem nezināmiem, tad var cerēt, ka tam (vismaz dažos gadījumos) eksistē daudz atrisinājumu.

3.1. 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,

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

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

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

Otrs pierādījums (patstāvīgais darbs). Pieņemsim, ka ir zināmi a un b sadalījumi pirmskaitļu pakāpju reizinājumā:

$$a = p_1^{\alpha_1}...p_n^{\alpha_n}, b = p_1^{\beta_1}...p_n^{\beta_n}.$$

Meklēsim arī x un y pirmskaitļu pakāpju reizinājumu veidā:

$$x = p_1^{\gamma_1}...p_n^{\gamma_n}q, y = -p_1^{\delta_1}...p_n^{\delta_n}r.$$

Salīdzinot pirmskaitļu pakāpes vienādojuma abās pusēs, iegūsim šādus nenegatīvus atrisinājumus kāpinātājiem γ_i un δ_i:

$$\gamma_i = (\beta_i - min(\alpha_i, \beta_i)) + \eta_i, \delta_i = (\alpha_i - min(\alpha_i, \beta_i)) + \eta_i,$$

kur $\eta_i \geq 0$. Attiecībā uz x un y šie atrisinājumi dod sagaidāmo atbildi.
■

3.1. 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.

3.2. 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 $d|(a_1x_1 + ... + a_nx_n)$ 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

$$c = qd = q(a_1x_1' + ... + a_nx_n')$$

(d var izteikt kā kopas $\{a_1, ..., a_n\}$ elementu veselu lineāru kombināciju). Redzam, ka $c = q(a_1x_1' + ... + a_nx_n')$ un par veselu atrisinājumu var izvēlēties virkni

$$x_1 = qx_1', ..., x_n = qx_n'.$$

■

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

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

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

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 $(\frac{b}{d}t, -\frac{a}{d}t)$. ■

3.3. 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 $\{(-4 + 3t, 4 - 2t) | t \in \mathbb{Z}\}$.

3.4. teorēma. (Patstāvīgais darbs) Ja $a_1, ..., a_n$ ir pozitīvi, $d = 1$ un

$$b \geq (a_n - 1) \sum_{i=1}^{n-1} a_i,$$

tad vienādojumam $a_1x_1 + ... + a_nx_n = b$ eksistē nenegatīvs atrisinājums.
PIERĀDĪJUMS Pieņemsim, ka veselu skaitļu virkne $\{y_1, ..., y_n\}$ apmierina vienādojumu $a_1y_1 + ... + a_ny_n = b$.

Izdalīsim katru no skaitļiem $y_i, 1 \leq i < n$ ar a_n:

$$y_i = q_ia_n + r_i,$$

kur $0 \leq r_i \leq a_n - 1$. Redzam, ka
$b = a_1y_1 + ... + a_{n-1}y_{n-1} + a_ny_n = a_1(q_1a_n + r_1) + ... + a_{n-1}(q_{n-1}a_n + r_{n-1}) + a_ny_n = a_1r_1 + ... + a_{n-1}r_{n-1} + a_n(y_n + a_1q_1 + ... + a_{n-1}q_{n-1})$.

Apzīmēsim $y_n + a_1q_1 + ... + a_{n-1}q_{n-1}$ ar r_n.

Redzam, ka

$$b = a_1r_1 + ... + a_nr_n \leq (a_n - 1)(a_1 + ... + a_{n-1}) + a_nr_n.$$

Ja $b \geq (a_n - 1)(a_1 + ... + a_{n-1})$ tad $a_nr_n \geq 0$ un $r_n \geq 0$. Esam ieguvuši nenegatīvu atrisinājumu $(r_1, ..., r_n)$.■

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 $n = 2$.

4. 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 $LKD(b_1, ..., b_n)$ ir mazākais naturālais skaitlis, ko var izteikt kā naturālo skaitļu $b_1, ..., b_n$ lineāru kombināciju ar veseliem koeficientiem.
3. Pierādiet, ka summa

   $$\sum_{i=1}^{n} \frac{1}{i} = 1 + \frac{1}{2} + ... + \frac{1}{n}$$

   nevienam $n > 1$ nav vesels skaitlis.
4. Atrodiet skaitļa 1048509/731623 pierakstu ķēžu daļas veidā.
5. Atrodiet visus veselos atrisinājumus šādiem vienādojumiem:
   a) $5x + 3y = 15$,
   b) $8x - 6y = 10$,
   c) $nx + (2n+1)y = 2, n \in \mathbb{N}$.