Latvijas Universitāte
Fizikas un matemātikas fakultāte
Matemātiskās analīzes katedra

Jānis Buls

IEVADS SKAITĻU TEORIJĀ

Lekciju konspekts — 2007

Ievads

Vesels skaitlis, tāpat kā vienkāršākās ģeometriskās figūras, vēsturiski ir viens no pirmajiem jēdzieniem matemātikā. Jau senajā Grieķijā (VI gs. p. m. ē.) zināja vienādojuma $x^2 + y^2 = z^2$ atrisinājumus. Vācu matemātiķis Kārlis Fridrihs Gauss (XIX gs.) izstrādāja pamatmetodes kongruenču teorijā. Tās pamatrezultātus arī šodien izmanto gan algebrā, gan kriptogrāfijā. Skaitļu teorija kalpo par instrumentu rezultātu formulēšanai citās matemātikas nozarēs, tai skaitā arī algoritmu un varbūtību teorijā. Īpaša loma skaitļu teorijai ir dažādu pseidogadījumskaitļu ģeneratoru radīšanas procesā.

Sakarā ar e-pārvaldes un e-komercijas ieviešanu aktualizējas datu aizsardzības problēmas, kas būtiski balstās uz skaitļu teorijas atziņām. Tā rezultātā skaitļu teorija mūsdienās vairs nav tikai tīri teorētiska matemātikas disciplīna.

Kursa mērķis — iepazīstināt ar skaitļu teorijas pamatjēdzieniem un metodēm, kuras plaši lieto citās disciplīnās.

Apzīmējumi

$\neg$ — negācija,
$\vee$ — disjunkcija, $\wedge$ — konjunkcija,
$\Rightarrow$ — implikācija, $\Leftrightarrow$ — ekvivalence,
$\mathfrak{A} \sim a$ — izteikums $\mathfrak{A}$ ir aplams,
$\mathfrak{A} \sim p$ — izteikums $\mathfrak{A}$ ir patiess,
$\exists$ — eksistences kvantors, $\forall$ — universālkvantors,
$\exists! x\ P(x)$ — eksistē viens vienīgs tāds x, kam izpildās nosacījums $P(x)$,

$x \in X$ — elements x pieder kopai X jeb x ir kopas X elements,
$A \subseteq B$ — kopa A ir kopas B apakškopa,
$A \cup B$, $A \cap B$, $A \setminus B$ — kopu A un B apvienojums, šķēlums, starpība,
$\min K$ — kopas K minimālais elements,
$\max K$ — kopas K maksimālais elements,

$\rightleftharpoons$, $=\!\!:$ — vienādības saskaņā ar definīciju,
$\overline{1,n} \rightleftharpoons \{1,2,\ldots,n\}$; $\overline{k,n} \rightleftharpoons \{k,k+1,\ldots,n\}$, te $k \leq n$,
$\mathbb{Z}$ — veselo skaitļu kopa, $\mathbb{Z}_+ \rightleftharpoons \{x \,|\, x \in \mathbb{Z} \wedge x > 0\}$,
$\mathbb{N} \rightleftharpoons \mathbb{Z}_+ \cup \{0\}$, $\mathbb{N}_- \rightleftharpoons \mathbb{Z} \setminus \mathbb{Z}_+$,
$\mathbb{P}$ — visu pirmskaitļu kopa,
$\mathbb{Q}$ — racionālo skaitļu kopa,
$\mathbb{R}$ — reālo skaitļu kopa, $\mathbb{C}$ — komplekso skaitļu kopa,
$|K|$ — kopas K apjoms,
$\aleph_0$ — kopas $\mathbb{N}$ apjoms, $\mathfrak{c}$ — reālo skaitļu kopas $\mathbb{R}$ apjoms,

$\langle x,y\rangle \rightleftharpoons (x,y) \rightleftharpoons \{\{x\},\{x,y\}\}$,
$(x_1,x_2,\ldots,x_n) \rightleftharpoons ((x_1,x_2,\ldots,x_{n-1}),x_n)$,
$A_1 \times A_2 \times \ldots \times A_n \rightleftharpoons \{(x_1,x_2,\ldots,x_n) \,|\, \forall i \in \overline{1,n}\ (x_i \in A_i)\}$, A^n,
$f : x \mapsto y$, $f : X \multimap Y$, $X \overset{f}{\multimap} Y$,
$\mathrm{Dom}(f) \rightleftharpoons \{x \,|\, \exists y \in Y\ (f : x \mapsto y)\}$, $\mathrm{Ran}(f) \rightleftharpoons \{y \,|\, \exists x \in X\ (f : x \mapsto y)\}$,
$f : X \to Y$, $X \overset{f}{\to} Y$, $f : X \twoheadrightarrow Y$, $f : X \hookrightarrow Y$,
$\lfloor x \rfloor \rightleftharpoons \max\{t \,|\, t \leq x \ \wedge\ t \in \mathbb{Z}\}$,
$\{x\} \rightleftharpoons x - \lfloor x \rfloor$,

$\sum_{i=k}^{m} a_i \rightleftharpoons a_k + a_{k+1} + \ldots + a_m$,

$\prod_{i=k}^{m} a_i \rightleftharpoons a_k a_{k+1} \dots a_m,$

$a \diagdown b$ — skaitlis b ir skaitļa a daudzkārtnis,
$a \nmid b$ — skaitlis b nav skaitļa a daudzkārtnis,
$D(a_1, a_2, \dots, a_n) \rightleftharpoons \{q | \forall i \in \overline{1,n}\ q \diagdown a_i\}$,
$\mathrm{ld}(a_1, a_2, \dots, a_n) \rightleftharpoons \max D(a_1, a_2, \dots, a_n)$,
$\mathrm{md}(a_1, a_2, \dots, a_n)$ — skaitļu $a_1, a_2, \dots, a_n$ mazākais kopīgais dalāmais,
$[q_1; q_2, \dots, q_n]$ — galīga ķēžu daļa,
$[q_1; q_2, \dots, q_n, \dots]$ — bezgalīga ķēžu daļa,

$a \equiv b (\mathrm{mod}\ m)$ — skaitļi a un b ir kongruenti pēc moduļa m,
$[a] \rightleftharpoons \{b \mid a \equiv b (\mathrm{mod}\ m)\}$, izņemot 1. nodaļu,
$\mathbb{Z}_m \rightleftharpoons \{[0], [1], \dots, [m-1]\}$,
$\mathbb{Z}_m^* \rightleftharpoons \{\ [a] \mid \mathrm{ld}(a, m) = 1\ \wedge\ [a] \in \mathbb{Z}_m\}$,

$\square$ — pierādījuma sākums,
$\blacksquare$ — pierādījuma beigas;
$\Rightarrow$ — implikācijas zīmi pierādījuma sākumā mēs izmantojam, lai norādītu, ka tagad sākas teorēmas nepieciešamā nosacījuma pierādījums,
$\Leftarrow$ — šo zīmi pierādījumos mēs izmantojam, lai norādītu, ka tagad sākas teorēmas pietiekamā nosacījuma pierādījums.

1. Aritmētikas aksiomātika

Pamatjēdzieni un atvasināti jēdzieni. Dekarta reizinājums, attēlojums. Algebriska sistēma. Formālā aritmētika. Matemātiskās indukcijas metode. Vesela skaitļa daudzkārtņi.

Attīstītas teorijas pamatiezīme ir "spēles noteikumu" fiksēšana. Tāpēc rodas uzdevums veidot teoriju ar vislielāko rūpību un loģisko precizitāti. Tie apgalvojumi, kurus izmanto kaut kādā pierādījumā, arī paši prasa pierādījumu ar kādu agrāku apgalvojumu palīdzību, savukārt agrākie apgalvojumi arī jāpierāda, utt. Kurā vietā šai spriedumu ķēdei būs gals (precīzāk — sākums)? Tāda vispār nav. Kāda ir izeja no aprakstītā šķietami bezcerīgā stāvokļa? Matemātiķi šo "Gordija mezglu" nav atraisījuši, bet vienkārši pārcirtuši. Proti, kādā vietā spriedumu ķēdē daži apgalvojumi tiek akceptēti *bez pierādījuma*. Tos sauc par *aksiomām*.

Līdzīga situācija ir ar jēdzieniem. Katrā definīcijā jaunais jēdziens tiek konstruēts ar citu jēdzienu palīdzību. Tā rezultātā katra definīcija saistās ar citām, kuras definē tos jēdzienus, kas apskatāmajā definīcijā tiek uzskatīti par zināmiem. Piemēram, par taisnes nogriezni sauc taisnes daļu, kas atrodas starp diviem punktiem. Bet kā definēt jēdzienus "taisne" un "starp"? Tātad definīcijas veido tādu pašu bezgalīgu virkni kā pierādījumi. Tādēļ dažus jēdzienus izvēlas *bez definīcijas*. Tos sauc par *pamatjēdzieniem* jeb *sākotnējiem jēdzieniem*. Pārējos (definētos) jēdzienus sauc par *atvasinātiem jēdzieniem*. Pamatjēdzienu un aksiomu izvēles pamatotība daudzējādā ziņā ir ārpus matemātikas. Te jābalstās gan uz filozofiju, praksi, gan zinātnes metodoloģiju. Matemātikas sistematizācija deviņpadsmitā gadsimta beigu posmā ļāva secināt, ka viens no perspektīvākajiem pamatjēdzieniem matemātikā ir kopas jēdziens. To var izvēlēties par vienīgo pamatjēdzienu visā matemātikā.

Kopu $\{\{x\},\{x,y\}\}$ sauc par elementu $x \in X$ un $y \in Y$ *sakārtotu pāri* un lieto apzīmējumu (x,y) vai $\langle x,y\rangle$. Pāri $((x_1,x_2,\ldots,x_{n-1}),x_n)$, kur $\forall i \in \overline{1,n}$ $(x_i \in A_i)$ sauc par *n-dimensionālu kortežu* pār kopām $A_1,A_2,\ldots,A_n$. Turpmāk n-dimensionāla korteža apzīmēšanai lietosim pierakstu $(x_1,x_2,\ldots,x_n)$. Par kopu $A_1,A_2,\ldots,A_n$ *Dekarta reizinājumu* sauc visu n-dimensionālo kortežu kopu pār kopām $A_1,A_2,\ldots,A_n$, t.i.,

$$A_1 \times A_2 \times \ldots \times A_n \rightleftharpoons \{(x_1,x_2,\ldots,x_n) \,|\, \forall i \in \overline{1,n}\,(x_i \in A_i)\}.$$

Ja $A = A_1 = A_2 = \ldots = A_n$, tad lieto arī pierakstu $A^n \rightleftharpoons A_1 \times A_2 \times \ldots \times A_n$. Kopas $A_1 \times A_2 \times \ldots \times A_n$ apakškopu ϱ mēdz saukt arī par *n-vietīgu attieksmi*

(attiecību, predikātu), kas definēta kopā $A_1 \times A_2 \times \ldots \times A_n$.

Trijnieku $f = \langle X, Y, F \rangle$, kur $F \subseteq X \times Y$ sauc par *attēlojumu* jeb *funkciju*, ja visiem kopas F elementiem $(x, y), (x, z)$ ir spēkā vienādība $y = z$. Kopu X sauc par attēlojuma f *starta* jeb *izejas* kopu, Y — par *finiša* jeb *ieejas* kopu, F sauc par *grafiku*. Ja $(x, y) \in F$, tad lieto pierakstu $f(x) = y$ jeb $f : x \mapsto y$. Vispārīgs pieraksts $f : X \multimap Y$ (lieto arī pierakstu $X \overset{f}{\multimap} Y$) norāda, ka f ir attēlojums ar starta kopu X un finiša kopu Y.

Kopu

$$\mathrm{Dom}(f) \rightleftharpoons \{x \,|\, \exists y \in Y \; (f : x \mapsto y)\}$$

sauc par attēlojuma $f : X \multimap Y$ *definīcijas apgabalu*. Savukārt kopu

$$\mathrm{Ran}(f) \rightleftharpoons \{y \,|\, \exists x \in X \; (f : x \mapsto y)\}$$

sauc par attēlojuma f *vērtību apgabalu*. Attēlojumu $f : X \multimap Y$ sauc par *visur definētu attēlojumu*, ja $\mathrm{Dom}(f) = X$. Šai gadījumā mēdz lietot vienu no apzīmējumiem

$$f : X \to Y \quad \text{vai} \quad X \overset{f}{\to} Y.$$

Pretējā gadījumā attēlojumu $f : X \multimap Y$ sauc par *daļēji definētu,* proti, ja

$$\exists x \in X \; x \notin \mathrm{Dom}(f).$$

Visur definētu attēlojumu $g : X_1 \times X_2 \times \ldots \times X_n \to X_{n+1}$ sauc arī par *n-vietīgu algebrisku operāciju*.

Attēlojumu $f : X \multimap Y$ sauc par *sirjekciju* un lieto apzīmējumu $f : X \twoheadrightarrow Y$, ja $\mathrm{Ran}(f) = Y$. Attēlojumu f sauc par *injekciju* un lieto apzīmējumu $f : X \hookrightarrow Y$, ja dažādiem elementiem x_1, x_2 atbilst dažādi y_1, y_2, t.i.,

$$\forall (x_1, x_2) \in X^2 \; [x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)].$$

Ja algebriska operācija $h : X \to Y$ ir gan sirjekcija, gan injekcija, tad to sauc par *bijekciju*.

Trijnieku $\langle K, O, A \rangle$ sauc par *algebrisku sistēmu*, ja

(i) K ir netukša kopa,

(ii) O ir algebrisku operāciju $\circ_i : K^{k(i)} \to K$ kopa,

(iii) A ir dažādu attieksmju $\varrho_i \subseteq K^{m(i)}$ kopa.

Ja kopas O un A ir galīgas, un nerodas pārpratumi, piemēram,

$$O = \{\circ_1, \circ_2, \ldots, \circ_k\}, \quad A = \{\varrho_1, \varrho_2, \ldots, \varrho_m\},$$

tad $\langle K, O, A\rangle$ vietā lieto pierakstu

$$\langle K; \circ_1, \circ_2, \ldots, \circ_k; \varrho_1, \varrho_2, \ldots, \varrho_m\rangle.$$

Ja $O = \emptyset$, tad algebrisko sistēmu sauc par *modeli*, ja turpretī $A = \emptyset$, tad — par *algebru*. Šai situācijā $\langle K, O, A\rangle$ vietā attiecīgi lieto pierakstu $\langle K, A\rangle$ vai $\langle K, O\rangle$, vai arī attiecīgi $\langle K; \varrho_1, \varrho_2, \ldots, \varrho_m\rangle$ vai $\langle K; \circ_1, \circ_2, \ldots, \circ_k\rangle$.

Mēs nofiksēsim aritmētikas aksiomātiku. Algebrisku sistēmu

$$\langle \mathbb{N}; 0, s, +, \cdot; =, <\rangle$$

sauc par formālo aritmētiku, ja tā apmierina sekojošas aksiomas:

$\mathbb{N}1.$ $s(x) \neq 0$,

$\mathbb{N}2.$ $s(x) = s(y) \Rightarrow x = y$,

$\mathbb{N}3.$ $x + 0 = 0$,

$\mathbb{N}4.$ $x + s(y) = s(x + y)$,

$\mathbb{N}5.$ $x \cdot 0 = 0$,

$\mathbb{N}6.$ $x \cdot s(y) = (x \cdot y) + x$,

$\mathbb{N}7.$ $\neg(x < 0)$,

$\mathbb{N}8.$ $x < s(y) \Leftrightarrow x < y \vee x = y$,

$\mathbb{N}9.$ $F(0, \bar{z}) \wedge \forall y(F(y, \bar{z}) \Rightarrow F(s(y), \bar{z})) \Rightarrow F(x, \bar{z})$.

Te 0 — nullvietīga operācija; s — vienvietīga operācija; $+, \cdot$ — divvietīgas operācijas; $=, <$ — divvietīgas attiecības. Kaut arī attīstot formālu teoriju mēs abstrahējamies no konkrētas interpretācijas, mēs tomēr visu laiku ņemam vērā, ka šī algebriskā sistēma kalpo mums no skolas laikiem labi pazīstamo operāciju un attiecību aprakstam, proti,

- 0 apzīmē skaitli nulle,

- $+$ apzīmē saskaitīšanas operāciju,
- $\cdot$ apzīmē reizināšanas operāciju,
- $=$ apzīmē vienādību,
- $<$ apzīmē mazāks par.

Nedaudz neparasts ir apzīmējums $s(x)$, kas saturiski apzīmē operāciju $x+1$. Visbeidzot pēdējā aksioma $\mathbb{N}9$ patiesībā ir bezgala daudzas aksiomas. Te $F(x,\bar{z})$ ir klasiskās predikātu loģikas formula no mainīgajiem

$$x, z_1, z_2, \ldots, z_n.$$

$F(x,\bar{z})$ lietots kā saīsinājums pierakstam $F(x,z_1,z_2,\ldots,z_n)$. Šī aksioma $\mathbb{N}9$ katram konkrētam predikātam F saturīgi izsaka kādu apgalvojumu par naturāliem skaitļiem. Pašu aksiomu $\mathbb{N}9$ mēdz saukt par *matemātiskās indukcijas aksiomu (principu, metodi).*

Matemātiskās indukcijas aksioma ir svarīgākais instruments ar kā palīdzību elementārajā skaitļu teorijā pierāda dažnedažādus apgalvojumus, lemmas un teorēmas. Pielietojot matemātiskās indukcijas metodi, parasti visus spriedumus sadala 3 soļos:

1. solis — pārbauda izteikuma $F(0,\bar{z})$ patiesumu;
2. solis — pieņem, ka $F(x,\bar{z})$ ir patiess kādai patvaļīgi fiksētai vērtībai $x=y$ un, vadoties no šī pieņēmuma, pierāda, ka $F(x,\bar{z})$ ir patiess arī x vērtībai $y+1$;
3. solis — pamatojoties uz matemātiskās indukcijas metodi, secina, ka jebkuram naturālam skaitlim x izteikums $F(x,\bar{z})$ ir patiess.

1. soli parasti sauc par *indukcijas bāzi*, 2. soli — par *induktīvo pāreju.*
2. solī jāpierāda izteikums

$$\forall y \in \mathbb{N}\ (F(y,\bar{z}) \Rightarrow F(y+1,\bar{z})).$$

Tātad jāpierāda, ka patvaļīgam y izteikums $F(y+1,\bar{z})$ ir patiess, ja pieņem par dotu, ka patiess izteikums $F(y,\bar{z})$. Šai situācijā apgalvojumu $F(y,\bar{z})$ mēdz saukt par *induktīvo pieņēmumu.*

Nekas principiāli nemainās, ja kopas $\mathbb{N}$ vietā aplūko kopu

$$\mathbb{N}_- \rightleftharpoons \mathbb{Z} \setminus \mathbb{Z}_+.$$

Tagad matemātiskās indukcijas metode izskatās šādi

$$\frac{F(0,\bar{z}), \quad \forall y \in \mathbb{N}_- \ (F(y,\bar{z}) \Rightarrow F(y-1,\bar{z}))}{\forall x \in \mathbb{N}_- \ F(x,\bar{z})}$$

Parasti indukcijas bāze pierādāma samērā viegli, bieži vien pat triviāli. Grūtākā spriedumu daļa slēpjas induktīvajā pārejā.

Veselo skaitļu kopu var ieviest balstoties uz naturālo skaitļu kopu $\mathbb{N}$. Shēma ir sekojoša: vispirms kopā $\mathbb{N}^2$ definējam ekvivalences tipa predikātu, proti,

$$(a,b) \sim (x,y) \underset{\text{def}}{\Leftrightarrow} a-b = x-y \vee b-a = y-x.$$

Tā kā kopā $\mathbb{N}$ atņemšana ne vienmēr ir definēta, tad mums jābūt nedaudz uzmanīgiem. Šī iemesla dēļ mēs lietojam nosacījumu

$$a-b = x-y \vee b-a = y-x,$$

nevis nosacījumu $a-b=x-y$. Atzīmēsim, ja $a \geq b$, tad $(a,b) \sim (a-b,0)$; ja turpretī $b > a$, tad $(a,b) \sim (0,b-a)$.

Ekvivalences tipa predikāts $\sim$ kopā $\mathbb{N}^2$ definē klases

$$\begin{aligned} [a] &\rightleftharpoons \{(x,y) | (x,y) \sim (a,0)\}, \\ [-a] &\rightleftharpoons \{(x,y) | (x,y) \sim (0,a)\}. \end{aligned}$$

Tā rezultātā iegūstam faktorkopu

$$\mathbb{N}^2/\sim \ \rightleftharpoons \{[a] | a \in \mathbb{N}\} \cup \{[-a] | a \in \mathbb{N}\}.$$

Vēl tikai šai faktorkopā jānodefinē saskaitīšana, rezināšana un attiecība mazāks par, un tad jau gredzenu $\mathbb{N}^2/\sim$ ar precizitāti līdz izomorfismam var uzlūkot par veselo skaitļu gredzenu $\mathbb{Z}$.

Mūsu kursa uzdevums ir elementārā skaitļu teorija, nevis matemātikas pamati, tāpēc mēs jautājumam par aksiomātiku pieskārāmies tikai garāmejot.

Galvenajām skaitļu kopām, kuras matemātikā izmanto ļoti bieži, piešķirti patstāvīgi standartapzīmējumi (diemžēl sakarā ar teorētiskās datorzinātnes

strauju ienākšanu mūsdienu zinātnē daži apzīmējumi vairs nav interpretējami viennozīmīgi).

$$\begin{array}{rcl} \mathbb{Z} & — & \text{visu } \textit{veselo skaitļu} \text{ kopa,} \\ \mathbb{Z}_+ & \rightleftharpoons & \{x \,|\, x \in \mathbb{Z} \text{ un } x > 0\}, \\ \mathbb{N} & \rightleftharpoons & \mathbb{Z}_+ \cup \{0\}, \\ \mathbb{Q} & \rightleftharpoons & \left\{ \dfrac{x}{y} \,\middle|\, x \in \mathbb{Z} \text{ un } y \in \mathbb{Z}_+ \right\}, \\ \mathbb{R} & — & \text{visu } \textit{reālo skaitļu} \text{ kopa,} \\ \mathbb{C} & — & \text{visu } \textit{komplekso skaitļu} \text{ kopa,} \end{array}$$

Kā jau atzīmējām naturālo skaitļu kopā $\mathbb{N}$ ne vienmēr var veikt atņemšanas operāciju. Šī iemesla dēļ arī ieviesta veselo skaitļu kopa $\mathbb{Z}$. Taču veselo skaitļu kopā ne vienmēr var veikt dalīšanas operāciju, tāpēc ieviesta racionālo skaitļu kopa $\mathbb{Q}$.

Pirmajā tuvinājumā skaitļu teoriju var raksturot kā matemātikas disciplīnu, kas interesējas tikai par veseliem skaitļiem, racionālo skaitļu lauku jau atstājot citu matemātikas nozaru pārziņā, piemēram, algebras. Saprotams šis iedalījums ir nosacīts, taču tas zināmā mērā pamato, kāpēc tieši skaitļu teorija aplūko jautājumus, kas saistīti dalāmības problemātiku.

1.1. Definīcija. *Pieņemsim, ka a un b ir veseli skaitļi, piedevām $b \neq 0$. Skaitli b sauc par skaitļa a dalītāju, ja*

$$\exists q \in \mathbb{Z}\ a = bq.$$

Šai situācijā lieto apzīmējumu $b \smallsetminus a$, un skaitli a sauc par skaitļa b *daudzkārtni*. Skaitli q sauc par skaitļu a un b *dalījumu*. Gadījumā, ja b nav skaitļa a dalītājs, tad lietosim pierakstu $b \nmid a$.

1.2. Apgalvojums. *Ja $a \smallsetminus b$ un $b \smallsetminus c$, tad $a \smallsetminus c$.*

□ Saskaņā ar doto $a \smallsetminus b$ un $b \smallsetminus c$, tāpēc

$$\exists p \in \mathbb{Z}\ b = ap \qquad \text{un} \qquad \exists q \in \mathbb{Z}\ c = bq.$$

No šejienes

$$c = bq = (ap)q = a(pq).$$

Tā kā $pq \in \mathbb{Z}$, tad $a \smallsetminus c$. ■

1.3. Apgalvojums. *Pieņemsim, ka*

$$n + n_1 + n_2 + \ldots + n_s = m_1 + m_2 + \ldots + m_\sigma.$$

Ja $\forall i\ a \nmid n_i$ *un* $\forall j\ a \nmid m_j$, *tad* $a \nmid n$.

□ Saskaņā ar doto $\forall i\ a \nmid n_i$ un $\forall j\ a \nmid m_j$, tāpēc

$$\forall i \exists p_i \in \mathbb{Z}\ n_i = ap_i \qquad \text{un} \qquad \forall j \exists q_j \in \mathbb{Z}\ m_j = aq_j.$$

Rezultātā

$$\begin{aligned} n &= m_1 + m_2 + \ldots + m_\sigma - n_1 - n_2 - \ldots - n_s \\ &= aq_1 + aq_2 + \ldots + aq_\sigma - ap_1 - ap_2 - \ldots - ap_s \\ &= a(q_1 + q_2 + \ldots + q_\sigma - p_1 - p_2 - \ldots - p_s). \end{aligned}$$

Tā kā $q_1 + q_2 + \ldots + q_\sigma - p_1 - p_2 - \ldots - p_s \in \mathbb{Z}$, tad $a \nmid n$. ■

1.4. Vingrinājumi. *Pierādīt sekojošas dalāmības attieksmes īpašības!*

(i) $\forall a \in \mathbb{Z}\ (a \neq 0 \Rightarrow a \nmid 0)$;
(ii) $\forall a \in \mathbb{Z}\ \pm 1 \nmid a$;
(iii) dalāmības attieksme ir gan refleksīva, gan transitīva;
(iv) $\forall a \in \mathbb{Z}_+ \forall b \in \mathbb{Z}_+\ (a \nmid b \Rightarrow a \leq b)$;
(v) $a \nmid b \wedge b \nmid a \Rightarrow a = \pm b$;
(vi) $a \nmid b \wedge a \nmid c \Rightarrow a \nmid b \pm c$;
(vii) $a \nmid b \Rightarrow \forall x \in \mathbb{Z}\ a \nmid bx$;
(viii) $a \nmid b \wedge a \nmid c \Rightarrow \forall x \in \mathbb{Z} \forall y \in \mathbb{Z}\ a \nmid bx + cy$;
(ix) $a \nmid b \wedge x \nmid y \Rightarrow ax \nmid by$;
(x) $\forall a \in \mathbb{Z} \forall b \in \mathbb{Z} \forall x \in \mathbb{Z}\ (ax \nmid bx \Rightarrow a \nmid b)$.

Un tagad nodemonstrēsim kā izmantojama matemātiskās indukcijas metode elementārās skaitļu teorijas rezultātu pamatošanai.

1.5. Apgalvojums.

$$\forall a \in \mathbb{Z}\ \forall b \in \mathbb{Z}_+\ \exists q \in \mathbb{Z} \quad bq \leq a < b(q+1)$$

□ Pierādījumu sadalīsim divās daļās.

(i) Vispirms ar matemātiskās indukcijas palīdzību pierādīsim apgalvojumu

$$\forall a \in \mathbb{N}\, \forall b \in \mathbb{Z}_+\, \exists q \in \mathbb{Z} \quad bq \leq a < b(q+1). \tag{1}$$

Indukcijas bāze: ja $a = 0$, tad

$$b \cdot 0 \leq 0 < b(0+1).$$

No šejienes redzams, ka $q = 0$.

Induktīvā pāreja: pieņemam, ka apgalvojums (1) ir pareizs, ja $a = y$. Tas ir induktīvais pieņēmums. No šejienes, eksistē tāds vesels skaitlis q', ka

$$bq' \leq y < b(q'+1).$$

- Ja $y + 1 < b(q' + 1)$, tad mūsu rīcībā ir nevienādības

  $$bq' \leq y < y + 1 < b(q' + 1),$$

  un skaitļa q lomai varam ņemt q', t.i., $q = q'$.

- Pretējā gadījumā $b(q' + 1) \leq y + 1$. Tā kā $b \in \mathbb{Z}_+$, tad $b \geq 1$. No šejienes, ņemot vērā induktīvo pieņēmumu,

  $$y + 1 \leq y + b < b(q' + 1) + b = b(q' + 2).$$

  Esam konstatējuši, ka šai gadījumā

  $$b(q' + 1) \leq y + 1 < b(q' + 2).$$

  Tātad skaitļa q lomai varam ņemt $q' + 1$, t.i., $q = q' + 1$.

(ii) Tagad ar matemātiskās indukcijas palīdzību pierādīsim apgalvojumu

$$\forall a \in \mathbb{N}_-\, \forall b \in \mathbb{Z}_+\, \exists q \in \mathbb{Z} \quad bq \leq a < b(q+1). \tag{2}$$

Indukcijas bāze, t.i., ja $a = 0$, jau pierādīta (i) daļā.

Induktīvā pāreja: pieņemam, ka apgalvojums (2) ir pareizs, ja $a = y$. Tas ir induktīvais pieņēmums. No šejienes, eksistē tāds vesels skaitlis q', ka

$$bq' \leq y < b(q'+1).$$

- Ja $bq' \leq y - 1$, tad mūsu rīcībā ir nevienādības

$$bq' \leq y - 1 < y < b(q' + 1),$$

un skaitļa q lomai varam ņemt q', t.i., $q = q'$.

- Pretējā gadījumā $y - 1 < bq'$. Tā kā $b \in \mathbb{Z}_+$, tad $b \geq 1$. No šejienes, ņemot vērā induktīvo pieņēmumu,

$$y - 1 \geq y - b \geq bq' - b = b(q' - 1).$$

Esam konstatējuši, ka šai gadījumā

$$b(q' - 1) \leq y - 1 < bq'.$$

Tātad skaitļa q lomai varam ņemt $q' - 1$, t.i., $q = q' - 1$. ■

2. Skaitļu kopīgie dalītāji un dalāmie.

Teorēma par dalīšanu ar atlikumu. Eiklīda algoritms. Skaitļu kopīgie dalītāji un dalāmie.

Vienošanās. *Turpmāk šī kursa ietvaros, ja tas netiks speciāli atrunāts, visi skaitļi ir veseli pozitīvi skaitļi. Turklāt vēl, mēs aplūkosim tikai skaitļu pozitīvos dalītājus.*

Šīs nodaļas pamatmērķis ir Eiklīda algoritms un tā lietojumi skaitļu kopīgo dalītāju atrašanai. Vispirms pievērsīsimies dalīšanai ar atlikumu.

2.1. Teorēma.

$$\forall a \in \mathbb{Z}\ \forall b\ \exists! q \in \mathbb{Z}\ \exists! r \in \mathbb{N}\ (a = bq + r \wedge r < b).$$

□ Vispirms pierādīsim eksistenci un tad unitāti.
Saskaņā ar apgalvojumu 1.5

$$\exists q \in \mathbb{Z}\ bq \leq a < b(q+1).$$

No šejienes izvēlamies $r \rightleftharpoons a - bq$. Esam ieguvuši vienādību $a = bq + r$.
Tā kā $bq \leq a < b(q+1)$, tad

$$\begin{array}{rrcl} & 0 = bq - bq \leq & a - bq & < b(q+1) - bq = b, \\ \text{t.i.,} & 0 \leq & r & < b. \end{array}$$

Atliek pierādīt unitāti. Ja nu eksistē vēl kādi citi $q' \in \mathbb{Z}$ un $r' \in \mathbb{N}$ tādi, ka

$$a = bq' + r' \wedge r' < b,$$

tad

$$\begin{array}{rcl} a & = & bq + r \\ a & = & bq' + r' \\ \hline 0 & = & b(q - q') + (r - r') \end{array}$$

un

$$\begin{array}{rcl} 0 \leq & r & < b \\ -b < & -r' & \leq 0 \\ \hline -b < & r - r' & < b. \end{array}$$

No apgalvojuma 1.3 seko, ka $b \nmid (r - r')$, taču intervālā $]-b; b[$ ir tikai viens skaitlis, kas dalās ar b. Tas ir skaitlis 0. Tātad $r - r' = 0$, t.i., $r = r'$.

Mēs iepriekš konstatējām, ka $0 = b(q - q') + (r - r')$. No šejienes (ja reiz $r = r'$) izriet, ka $0 = b(q - q')$. Tā kā $b \neq 0$, tad $q - q' = 0$, t.i., $q = q'$. Līdz ar to unitāte ir pierādīta. ■

2.2. Piemērs. $-7 = 3(-3) + 2$.

Šai piemērā $a = -7$, $b = 3$, $q = -3$ un $r = 2$.

2.3. Definīcija. *Pieņemsim, ka $a \in \mathbb{Z}$, $b \in \mathbb{Z}_+$ un $a = bq + r$, kur $r \in [0; b[$, tad skaitli q sauc par nepilno dalījumu, bet skaitli r — par atlikumu.*

2.4. Sekas. *Ja $a = bq + r$, $a, q \in \mathbb{Z}$, un $r = 0$, tad nepilnais dalījums ir vienāds ar dalījumu.*

2.5. Definīcija. *Skaitli q sauc par skaitļu $a_1, a_2, \ldots, a_n$ kopīgo dalītāju, ja $\forall i \in \overline{1,n}\ q \nmid a_i$.*

Lielāko no skaitļu $a_1, a_2, \ldots, a_n$ kopīgajiem dalītājiem sauc par skaitļu $a_1, a_2, \ldots, a_n$ *lielāko kopīgo dalītāju*. Skaitļu $a_1, a_2, \ldots, a_n$ lielākā kopīgā dalītāja apzīmēšanai lietosim pierakstu $\mathrm{ld}(a_1, a_2, \ldots, a_n)$.

Nedaudz formālāk to visu var paskaidrot šādi. Pieņemsim, ka

$$D(a_1, a_2, \ldots, a_n) \rightleftharpoons \{q | \forall i \in \overline{1,n}\ q \nmid a_i\},$$

tad

$$\mathrm{ld}(a_1, a_2, \ldots, a_n) = \max D(a_1, a_2, \ldots, a_n).$$

2.6. Definīcija. *Skaitļus $a_1, a_2, \ldots, a_n$ sauc par relatīviem pirmskaitļiem, ja $\mathrm{ld}(a_1, a_2, \ldots, a_n) = 1$. Ja*

$$\forall i \forall j\ (i \neq j \Rightarrow \mathrm{ld}(a_i, a_j) = 1),$$

tad skaitļus $a_1, a_2, \ldots, a_n$ sauc par savstarpējiem pirmskaitļiem.

2.7. Sekas. *Savstarpēji pirmskaitļi ir arī relatīvi pirmskaitļi.*

2.8. Sekas. *Skaitļu pārim jēdzieni "savstarpēji pirmskaitļi" un "relatīvi pirmskaitļi" sakrīt.*

2.9. Teorēma. *Ja a ir b daudzkārtnis, tad $D(a,b) = D(b)$.*

□ $\Rightarrow$ Pieņemsim, ka $q \in D(a,b)$, tad $q \setminus b$. Tas nozīmē, ka $q \in D(b)$. Esam parādījuši, ka $D(a,b) \subseteq D(b)$.

$\Leftarrow$ Pieņemsim, ka $q \in D(b)$, tad $q \setminus b$. Saskaņā ar doto a ir b daudzkārtnis, t.i., $b \setminus a$. Tagad, atsaucoties uz apgalvojumu 1.2, secināms: $q \setminus a$. Līdz ar to $q \in D(a,b)$. Esam pierādījuši, ka $D(b) \subseteq D(a,b)$. ■

2.10. Sekas. *Ja a ir b daudzkārtnis, tad* $\mathrm{ld}(a,b) = b$.

□ Tikko pierādījām, ka $D(a,b) = D(b)$, tāpēc

$$\mathrm{ld}(a,b) = \max D(a,b) = \max D(b) = b. \blacksquare$$

2.11. Teorēma. *Ja $a = bq + c$, tad $D(a,b) = D(b,c)$.*

□ $\Rightarrow$ Pieņemsim, ka $d \in D(a,b)$, tad $d \setminus a$ un $d \setminus b$. Saskaņā ar doto $c = bq - a$, tāpēc (apgalvojums 1.3) $d \setminus c$. Līdz ar to $d \in D(b,c)$. Esam parādījuši, ka $D(a,b) \subseteq D(b,c)$.

$\Leftarrow$ Pieņemsim, ka $d \in D(b,c)$, tad $d \setminus b$ un $d \setminus c$. Saskaņā ar doto $a = bq + c$, tāpēc (apgalvojums 1.3) $d \setminus a$. Līdz ar to $d \in D(a,b)$. Esam parādījuši, ka $D(b,c) \subseteq D(a,b)$. ■

2.12. Sekas. *Ja $a = bq + c$, tad* $\mathrm{ld}(a,b) = \mathrm{ld}(b,c)$.

□ Tikko pierādījām, ka $D(a,b) = D(b,c)$, tāpēc

$$\mathrm{ld}(a,b) = \max D(a,b) = \max D(b,c) = \mathrm{ld}(b,c). \blacksquare$$

Eiklīda algoritms. Pieņemsim, ka $r_0 \in \mathbb{Z}$, bet $r_1 \in \mathbb{Z}_+$.
(i) Skaitli r_0 izsaka formā

$$r_0 = r_1 q_1 + r_2, \qquad \text{kur} \qquad 0 \le r_2 < r_1.$$

Ja $r_2 = 0$, tad Eiklīda algoritms beidz darbu. Ja $r_2 \neq 0$, tad Eiklīda algoritms atkārto soli (i) par r_0 ņemot r_1, bet par r_1 ņemot r_2.

(ii) *Induktīvais solis.* Pieņemsim, ka iegūta vienādība

$$r_{n-1} = r_n q_n + r_{n+1}, \qquad \text{kur} \qquad 0 \leq r_{n+1} < r_n.$$

Ja $r_{n+1} = 0$, tad Eiklīda algoritms beidz darbu. Pretējā gadījumā, t.i., $r_{n+1} \neq 0$, Eiklīda algoritms atkārto soli (i) par r_0 ņemot r_n, bet par r_1 ņemot r_{n+1}.

2.13. Sekas. *Eiklīda algoritms vienmēr beidz darbu galīgā soļu skaitā.*

□ Saskaņā ar Eiklīda algoritmu iegūstam vienādības

$$\begin{aligned}
r_0 &= r_1 q_1 + r_2, && 0 \leq r_2 < r_1;\\
r_1 &= r_2 q_1 + r_3, && 0 \leq r_3 < r_2;\\
&\ldots\ldots\ldots\ldots\ldots\ldots\\
r_{i-1} &= r_i q_i + r_{i+1}, && 0 \leq r_{i+1} < r_i;\\
&\ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned}$$

Tā rezultātā

$$r_1 > r_2 > \ldots > r_{i+1} > \ldots \geq 0.$$

Esam ieguvuši dilstošu naturālo skaitļu virkni. Šādas virknes elementu skaits nepārsniedz skaitli $r_1 + 1$. Tātad Eiklīda algoritms nestrādās vairāk par r_1 soli. Tas arī nozīmē, ka Eiklīda algoritms beidz darbu galīgā soļu skaitā. ■

Mēs tikko pierādījām, ka katram skaitļu pārim $r_0 \in \mathbb{Z}$, $r_1 \in \mathbb{Z}_+$ eksistē tāds $n \in \mathbb{Z}_+$, ka izpildās vienādības

$$\begin{aligned}
r_0 &= r_1 q_1 + r_2, && 0 < r_2 < r_1;\\
r_1 &= r_2 q_1 + r_3, && 0 < r_3 < r_2;\\
&\ldots\ldots\ldots\ldots\ldots\ldots\\
r_{i-1} &= r_i q_i + r_{i+1}, && 0 < r_{i+1} < r_i;\\
&\ldots\ldots\ldots\ldots\ldots\ldots\\
r_{n-2} &= r_{n-1} q_{n-1} + r_n, && 0 < r_n < r_{n-1};\\
r_{n-1} &= r_n q_n + r_{n+1}, && 0 = r_{n+1} < r_n.
\end{aligned} \tag{3}$$

Tātad

$$r_{n-1} = r_n q_n. \tag{4}$$

2.14. Apgalvojums. $D(a,b) = D(\mathrm{ld}(a,b))$.

□ Izmantojam vienādības (3), r_0 lomai ņemot skaitli a, bet r_1 lomai — skaitli b. Tagad, balstoties uz teorēmu 2.11, iegūstam

$$\begin{aligned} D(a,b) &= D(r_0,r_1) = D(r_1,r_2) = D(r_2,r_3) = \dots \\ &= D(r_{i-1},r_i) = D(r_i,r_{i+1}) = \dots \\ &= D(r_{n-2},r_{n-1}) = D(r_{n-1},r_n). \end{aligned}$$

Visbeidzot, atsaucoties uz vienādību (4) un teorēmu 2.9, secināms

$$D(r_{n-1},r_n) = D(r_n).$$

No šejienes $D(a,b) = D(r_n)$, un tāpēc

$$\mathrm{ld}(a,b) = \max D(a,b) = \max D(r_n) = r_n. \tag{5}$$

Tas parāda, ka

$$D(\mathrm{ld}(a,b)) = D(r_n) = D(a,b). \blacksquare$$

2.15. Sekas. *Skaitļu a un b lielākais kopīgais dalītājs* $\mathrm{ld}(a,b)$ *ir vienāds ar pēdējo nenulles atlikumu Eiklīda algoritmā.*

□ Skatīt formulas (3) un (5) ■

2.16. Piemērs. Atrast $\mathrm{ld}(525, 231)$!

Risinājums. Izmantojam Eiklīda algoritmu:

$$\begin{array}{rrl} & 525 & : 231 = 2 \\ - & 462 & \\ \hline & 231 & : 63 = 3 \\ - & 189 & \\ \hline & 63 & : 42 = 1 \\ - & 42 & \\ \hline 42 : & 21 & = 2 \end{array}$$

Tā kā pēdējais nenulles atlikums ir 21, tad $\mathrm{ld}(525, 231) = 21$.

2.17. Apgalvojums. $\mathrm{ld}(am, bm) = m\,\mathrm{ld}(a,b)$.

□ Šī apgalvojuma pierādījums balstās uz Eiklīda algoritmu (skatīt vienādības (3)). Par r_0 ņemot a, bet par r_1 — b iegūst: $\mathrm{ld}(a,b) = r_n$. Ja vienādības $r_{i-1} = r_i q_i + r_{i+1}$ abas puses pareizina ar m, tad

$$r_{i-1}m = r_i m q_i + r_{i+1}m.$$

Tā kā $0 \leq r_{i+1} < r_i$, tad $0 \leq mr_{i+1} < mr_i$. Tas pamato sekojošas formulas

$$\begin{aligned}
r_0 m &= r_1 m q_1 + r_2 m, && 0 < r_2 m < r_1 m;\\
r_1 m &= r_2 m q_1 + r_3 m, && 0 < r_3 m < r_2 m;\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
r_{i-1} m &= r_i m q_i + r_{i+1} m, && 0 < r_{i+1} m < r_i m;\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
r_{n-2} m &= r_{n-1} m q_{n-1} + r_n m, && 0 < r_n m < r_{n-1} m;\\
r_{n-1} m &= r_n m q_n + r_{n+1} m, && 0 = r_{n+1} m < r_n m.
\end{aligned}$$

Saskaņā ar Eiklīda algoritmu tas nozīmē, ka $\mathrm{ld}(am, bm) = r_n m$.

Tā kā $r_n = \mathrm{ld}(a,b)$, tad

$$m\,\mathrm{ld}(a,b) = r_n m = \mathrm{ld}(am, bm). \blacksquare$$

2.18. Teorēma. *Ja* $\mathrm{ld}(a,b) = d$, *tad* $\exists x \in \mathbb{Z}\, \exists y \in \mathbb{Z} \quad ax + by = d$.

□ Pieņemsim, ka skaitļiem $r_0 \rightleftharpoons a$ un $r_1 \rightleftharpoons b$ pielietots Eiklīda algoritms un iegūtas izteiksmes (3), tad (sekas 2.15) $r_n = \mathrm{ld}(a,b)$.

Pievēršamies vēlreiz vienādībām (3). Te

$$\begin{aligned}
r_{n-2} &= r_{n-1} q_{n-1} + r_n, && 0 < r_n < r_{n-1};\\
r_{n-1} &= r_n q_n + r_{n+1}, && 0 = r_{n+1} < r_n.
\end{aligned}$$

Tas demonstrē, ka skaitļiem r_{n-2} un r_{n-1} pielietots Eiklīda algoritms, tāpēc

$$\mathrm{ld}(r_{n-2}, r_{n-1}) = r_n\,.$$

Savukārt no vienādības

$$r_{n-2} = r_{n-1} q_{n-1} + r_n$$

izriet, ka

$$r_n = r_{n-2} - r_{n-1} q_{n-1}\,.$$

Tā, rezultātā

$$\mathrm{ld}(r_{n-2}, r_{n-1}) = r_n = r_{n-2} - r_{n-1}q_{n-1}\,,$$

t.i.,

$$\exists x_{n-2} \in \mathbb{Z}\, \exists y_{n-2} \in \mathbb{Z} \quad r_{n-2}x_{n-2} + r_{n-1}y_{n-2} = \mathrm{ld}(r_{n-2}, r_{n-1})\,.$$

Dotajā gadījumā $x_{n-2} = 1$, $y_{n-2} = -q_{n-1}$.

Tālākie spriedumi induktīvi. Pieņemsim, ka

$$\exists x_i \in \mathbb{Z}\, \exists y_i \in \mathbb{Z} \quad r_i x_i + r_{i+1}y_i = \mathrm{ld}(r_i, r_{i+1})\,.$$

Saskaņā ar (3)

$$r_{i-1} = r_i q_i + r_{i+1}\,,$$

tāpēc (sekas 2.12)

$$\begin{aligned} \mathrm{ld}(r_{i-1}, r_i) &= \mathrm{ld}(r_i, r_{i+1}) \\ &= r_i x_i + r_{i+1}y_i \\ &= r_i x_i + (r_{i-1} - r_i q_i)y_i \\ &= r_{i-1}y_i + r_i(x_i - y_i q_i)\,. \end{aligned}$$

Esam parādījuši, ka

$$\exists x_{i-1} \in \mathbb{Z}\, \exists y_{i-1} \in \mathbb{Z} \quad r_{i-1}x_{i-1} + r_i y_{i-1} = \mathrm{ld}(r_{i-1}, r_i)\,.$$

Līdz ar to saskaņā ar indukcijas principu

$$\exists x_0 \in \mathbb{Z}\, \exists y_0 \in \mathbb{Z} \quad r_0 x_0 + r_1 y_0 = \mathrm{ld}(r_0, r_1)\,.$$

Tagad atliek tikai atcerēties, ka $r_0 = a$, $r_1 = b$ un $\mathrm{ld}(r_0, r_1) = d$, lai secinātu, ka

$$ax_0 + by_0 = d\,. \quad \blacksquare$$

2.19. Sekas.

$$\mathrm{ld}(a, b) = 1 \;\Leftrightarrow\; \exists x \in \mathbb{Z}\, \exists y \in \mathbb{Z} \quad ax + by = 1\,.$$

□ $\Rightarrow$ Nepieciešamais nosacījums ir nepastarpinātas sekas no tikko pierādītās teorēmas.

$\Leftarrow$ Pieņemsim, ka $\mathrm{ld}(a, b) = d$, tad $d \smallsetminus a$ un $d \smallsetminus b$. No šejienes

$$d \smallsetminus ax + by = 1\,.$$

Tas iespējams tikai tad, ja $d = 1$. ■

2.20. Apgalvojums. *Ja* $d \nmid a$ *un* $d \nmid b$, *tad*

$$\mathrm{ld}\Big(\frac{a}{d}, \frac{b}{d}\Big) = \frac{\mathrm{ld}(a,b)}{d}.$$

□ Saskaņā ar apgalvojumu 2.17

$$\mathrm{ld}(a,b) = \mathrm{ld}\Big(\frac{a}{d}\,d, \frac{b}{d}\,d\Big) = d\,\mathrm{ld}\Big(\frac{a}{d}, \frac{b}{d}\Big).$$

No šejienes pēc izdalīšanas ar skaitli d iegūstam apgalvojuma pierādījumu. ■

2.21. Apgalvojums. *Ja* $d \nmid a$ *un* $d \nmid b$, *tad* $d \nmid \mathrm{ld}(a,b)$.

□ Saskaņā ar apgalvojumu 2.14 $D(a,b) = D(\mathrm{ld}(a,b))$. Tā kā $d \in D(a,b)$, tad $d \in D(\mathrm{ld}(a,b))$, t.i., $d \nmid \mathrm{ld}(a,b)$. ■

2.22. Apgalvojums. *Ja* $\mathrm{ld}(d,b) = 1$, *tad* $\mathrm{ld}(ad,b) = \mathrm{ld}(a,b)$.

□ (i) Vispirms ievērojam, ka

$$\mathrm{ld}(ad,b) \nmid ad \quad \text{un} \quad \mathrm{ld}(ad,b) \nmid ab\,.$$

Saskaņā ar apgalvojumu 2.21

$$\mathrm{ld}(ad,b) \nmid \mathrm{ld}(ad,ab) = a\,\mathrm{ld}(d,b) = a\,.$$

Tā rezultātā

$$\mathrm{ld}(ad,b) \nmid a \quad \text{un} \quad \mathrm{ld}(ad,b) \nmid b\,.$$

Tas saskaņā ar apgalvojumu 2.21 ļauj secināt, ka $\mathrm{ld}(ad,b) \nmid \mathrm{ld}(a,b)$. No šejienes $\mathrm{ld}(ad,b) \le \mathrm{ld}(a,b)$.

(ii) Ievērojam, ka

$$\mathrm{ld}(a,b) \nmid ad \quad \text{un} \quad \mathrm{ld}(a,b) \nmid b\,,$$

tāpēc saskaņā ar apgalvojumu 2.21 $\mathrm{ld}(a,b) \nmid \mathrm{ld}(ad,b)$. No šejienes

$$\mathrm{ld}(a,b) \le \mathrm{ld}(ad,b).$$

Tagad ņemot vērā gan punktā (i), gan punktā (ii) pierādīto secināms: $\mathrm{ld}(ad,b) = \mathrm{ld}(a,b)$. ■

2.23. Apgalvojums. *Ja* $\mathrm{ld}(a,b)=1$ *un* $a \nmid bd$ *tad* $a \nmid d$.

□ Ņemot vērā sekas 2.10

$$\mathrm{ld}(a,bd)=a\,,$$

jo $a \nmid bd$. Tagad, atsaucoties uz apgalvojumu 2.22, secināms

$$\mathrm{ld}(a,d)=\mathrm{ld}(a,bd)=a\,.$$

Tātad $a \nmid d$. ■

2.24. Apgalvojums. *Ja* $\forall i \in \overline{1,m}\ \forall j \in \overline{1,n}\ \ \mathrm{ld}(a_i,b_j)=1$, *tad*

$$\mathrm{ld}(a_1a_2\ldots a_m, b_1b_2\ldots b_n)=1.$$

□ Mēs ņemam vērā apgalvojumu 2.22. Katram $j \in \overline{1,n}$

$$\mathrm{ld}(a_1a_2\ldots a_m,b_j)=\mathrm{ld}(a_2\ldots a_m,b_j)=\ldots=\mathrm{ld}(a_m,b_j)=1.$$

No šejienes

$$\begin{aligned}\mathrm{ld}(a_1a_2\ldots a_m,b_1b_2\ldots b_n) &= \mathrm{ld}(a_1a_2\ldots a_m,b_2\ldots b_n)\\ &= \ldots=\mathrm{ld}(a_1a_2\ldots a_m,b_n)=1\,.\ \blacksquare\end{aligned}$$

2.25. Definīcija. *Katru veselu pozitīvu skaitli, kas ir visu doto skaitļu daudzkārtnis sauc par šo skaitļu kopīgo dalāmo.*

2.26. Sekas. *Skaitļiem* $a_1,a_2,\ldots,a_n$ *eksistē kopīgais dalāmais.*

□ Reizinājums $a_1a_2\ldots a_n$ ir skaitļu $a_1,a_2,\ldots,a_n$ kopīgais dalāmais. ■

Mazāko no skaitļu $a_1,a_2,\ldots,a_n$ kopīgajiem dalāmajiem sauc par skaitļu $a_1,a_2,\ldots,a_n$ *mazāko kopīgo dalāmo.* Skaitļu $a_1,a_2,\ldots,a_n$ mazākā kopīgā dalāmā apzīmēšanai lietosim pierakstu $\mathrm{md}(a_1,a_2,\ldots,a_n)$.

2.27. Sekas. *Skaitļiem* $a_1,a_2,\ldots,a_n$ *eksistē mazākais kopīgais dalāmais.*

□ Reizinājums $a_1a_2\ldots a_n$ ir skaitļu $a_1,a_2,\ldots,a_n$ kopīgais dalāmais. Tagad atliek tikai pārbaudīt vai tikai kopā $\overline{1,a_1a_2\ldots a_n}$ neeksistē kāds par skaitli $a_1a_2\ldots a_n$ mazāks skaitļu $a_1,a_2,\ldots,a_n$ kopīgais dalāmais. ■

2.28. Apgalvojums. *Skaitlis m ir veselu pozitīvu skaitļu a un b kopīgais dalāmais tad un tikai tad, ja*

$$\exists t \in \mathbb{Z}_+ \;\; m = \frac{ab}{\mathrm{ld}(a,b)} t\,.$$

$\square$ $\Rightarrow$ Pieņemsim, ka m ir skaitļu a un b kopīgais dalāmis, tad $a \smallsetminus m$ un $b \smallsetminus m$. No šejienes eksistē tāds k, ka $m = ak$ un $\frac{m}{b} \in \mathbb{Z}_+$.

Pieņemsim, ka

$$\alpha \eqcirc \frac{a}{\mathrm{ld}(a,b)} \qquad \text{un} \qquad \beta \eqcirc \frac{b}{\mathrm{ld}(a,b)}\,,$$

tad $\mathrm{ld}(\alpha,\beta) = 1$. No šejienes

$$\frac{m}{b} = \frac{ak}{b} = \frac{\alpha\,\mathrm{ld}(a,b)\,k}{\beta\,\mathrm{ld}(a,b)} = \frac{\alpha k}{\beta}\,.$$

Tā kā $\frac{m}{b} \in \mathbb{Z}_+$, tad arī $\frac{\alpha k}{\beta} \in \mathbb{Z}_+$. Tas nozīmē, ka $\beta \smallsetminus \alpha k$. Tagad ņemam vērā, ka $\mathrm{ld}(\alpha,\beta) = 1$, tāpēc $\beta \smallsetminus k$. Tātad eksistē tāds $t \in \mathbb{Z}_+$, ka $k = \beta t$. Līdz ar to

$$\frac{m}{b} = \frac{\alpha k}{\beta} = \frac{\alpha\beta t}{\beta} = \alpha t.$$

No šejienes

$$m = \alpha b t = \frac{a}{\mathrm{ld}(a,b)}\, bt = \frac{ab}{\mathrm{ld}(a,b)}\, t.$$

$\Leftarrow$ Tā kā $\frac{b}{\mathrm{ld}(a,b)} \in \mathbb{Z}_+$, tad

$$a \smallsetminus \frac{ab}{\mathrm{ld}(a,b)}\, t = a\, \frac{b}{\mathrm{ld}(a,b)}\, t\,.$$

Līdzīgi

$$b \smallsetminus \frac{ab}{\mathrm{ld}(a,b)}\, t = b\, \frac{a}{\mathrm{ld}(a,b)}\, t\,,$$

jo $\frac{a}{\mathrm{ld}(a,b)} \in \mathbb{Z}_+$. $\blacksquare$

2.29. Sekas. $\qquad \mathrm{md}(a,b) = \dfrac{ab}{\mathrm{ld}(a,b)}\,.$

Brīdinājums. Vispārīgā gadījumā $\mathrm{md}(a,b,c) \neq \dfrac{abc}{\mathrm{ld}(a,b,c)}$.
Ja $a = 2, b = 3$ un $c = 6$, tad

$$\mathrm{md}(a,b,c) = \mathrm{md}(2,3,6) = 6 \neq 36 = \frac{2 \cdot 3 \cdot 6}{1} = \frac{abc}{\mathrm{ld}(a,b,c)} .$$

3. Pirmskaitļi.

Pirmskaitļi. Eratosfena siets. Kanoniskais sadalījums.

3.1. Definīcija. *Veselu pozitīvu skaitli a sauc par pirmskaitli, ja tā vienīgie dalītāji ir* 1 *un pats skaitlis a.*

3.2. Definīcija. *Veselu pozitīvu skaitli a sauc par saliktu skaitli, ja tā dalītāju skaits ir lielāks par* 2.

3.3. Apgalvojums. *Skaitļa a mazākais no* 1 *atšķirīgais dalītājs ir pirmskaitlis.*

□ Ja q ir mazākais no 1 atšķirīgais skaitļa a dalītājs un q ir salikts skaitlis, tad

$$\exists p \, (1 < p < q \ \wedge \ p \smallsetminus q) \, .$$

Esam ieguvuši, ka

$$p \smallsetminus q \qquad \text{un} \qquad q \smallsetminus a \, .$$

No šejienes $p \smallsetminus a$. Tātad q nav mazākais no 1 atšķirīgais skaitļa a dalītājs. Pretruna! ■

3.4. Apgalvojums. *Salikta skaitļa a mazākais no* 1 *atšķirīgais dalītājs nav lielāks par $\sqrt{a}$.*

□ Pieņemsim, ka q ir mazākais no 1 atšķirīgais saliktā skaitļa a dalītājs, tad $\exists p \ (qp = a)$. Tā kā a ir salikts skaitlis un q ir pirmskaitlis (skatīt iepriekšējo apgalvojumu), tad $q \neq a$, tāpēc $p \neq 1$. Ja reiz $p \neq 1$ un $p \smallsetminus a$, tad $p \geq q$, jo q ir mazākais no 1 atšķirīgais skaitļa a dalītājs. No šejienes

$$a = qp \geq qq = q^2$$

jeb

$$\sqrt{a}^{\,2} = a \geq q^2, \qquad \text{t.i.,} \qquad \sqrt{a} \geq q. \quad ■$$

3.5. Apgalvojums. *Pirmskaitļu ir bezgala daudz.*

□ Ja $p_1, p_2 \ldots, p_k$ ir visi iespējamie pirmskaitļi, tad pirmskaitlis p, kas dala summu

$$a \rightharpoonup p_1 p_2 \ldots p_k + 1$$

nesakrīt ne ar vienu no skaitļiem $p_1, p_2 \ldots, p_k$. Pretējā gadījumā $p \diagdown 1$ (skatīt apgalvojumu 1.3). Pretruna, jo mēs pieņēmām, ka citu pirmskaitļu kā $p_1, p_2 \ldots, p_k$ nav. ■

Turpmāk visu pirmskaitļu veidoto kopu apzīmēsim ar burtu $\mathbb{P}$.

Eratosfena siets — algoritms visu pirmskaitļu atrašanai, kas nepārsniedz doto skaitli n.

(i) Uzraksta visus skaitļus

$$2, 3, \ldots, n. \tag{6}$$

Šīs virknes (6) pirmais skaitlis 2 ir pirmskaitlis. Virknē (6) atstāj skaitli 2, bet pārejos skaitļa 2 daudzkārtņus izsvītro.

(ii) *Induktīvais solis.* Pieņemsim, ka virknē (6) atrasti pirmie k pirmskaitļi $p_1, p_2, \ldots, p_k$. Virknes (6) pirmais neizsvītrotais skaitlis p, kas atšķiras no visiem skaitļiem $p_1, p_2, \ldots, p_k$, ir pirmskaitlis, jo tas saskaņā ar konstrukciju nedalās ne ar vienu no skaitļiem $p_1, p_2, \ldots, p_k$.

Virknē (6) atstāj skaitli p, bet pārejos skaitļa p daudzkārtņus izsvītro.

(iii) Algoritmu turpina līdz atrasts tāds pirmskaitlis q, ka $q^2 > n$.

3.6. Sekas. *Rīkojoties ar Eratosfena sietu induktīvajā solī* (ii) *pirmais virknē* (6) *neizsvītrotais no p atšķirīgais pirmskaitļa p daudzkārtnis $a \geq p^2$.*

□ Pieņemsim, ka $p \diagdown a$ un $p < a < p^2$. Saskaņā ar apgalvojumu 3.4 salikta skaitļa a mazākais no 1 atšķirīgais dalītājs q nav lielāks par $\sqrt{a}$. Tātad

$$\exists q \, (1 < q < p \ \wedge \ q \diagdown a) \, .$$

Tā kā mazākais no 1 atšķirīgais skaitļa a dalītājs q ir pirmskaitlis (apgalvojums 3.3), tad skaitlis a izsvītrots kādā no iepriekšējiem soļiem. ■

3.7. Sekas. *Eratosfena siets korekti sastāda pirmskaitļu, kas nepārsniedz n, tabulu.*

□ Pieņemsim, ka a ir salikts skaitlis un $a \leq n$. Saskaņā ar apgalvojumu 3.4 tā mazākais dalītājs p nav lielāks par $\sqrt{a}$. Tātad a ir pirmskaitļa (apgalvojums 3.3) p daudzkārtnis un $p \leq \sqrt{a}$.

Ja $a \leq n$, tad $\sqrt{a} \leq \sqrt{n}$, tāpēc $p \leq \sqrt{n}$. Līdz ar to a izsvītrots no saraksta (6) kā pirmskaitļa $p \leq \sqrt{n}$ daudzkārtnis. ■

3.8. Apgalvojums. *Ja* $a \in \mathbb{Z}_+$ *un* $p \in \mathbb{P}$, *tad* $\mathrm{ld}(a,p) = 1$ *vai arī* $p \nmid a$.

□ Tā kā $\mathrm{ld}(a,p) \mid p \in \mathbb{P}$, tad

$$\mathrm{ld}(a,p) = 1 \qquad \text{vai arī} \qquad \mathrm{ld}(a,p) = p\,. \quad \blacksquare$$

3.9. Apgalvojums. *Ja* $p \mid \prod_{i=1}^{m} a_i$ *un* $p \in \mathbb{P}$, *tad*

$$\exists i \in \overline{1,m} \quad p \mid a_i\,.$$

□ Saskaņā ar apgalvojumu 3.8

$$\forall i \in \overline{1,m} \quad [\quad \mathrm{ld}(a_i,p) = 1 \quad \text{vai arī} \quad p \mid a_i \quad].$$

Ja $\forall i \in \overline{1,m}\ \mathrm{ld}(a,p) = 1$, tad ņemot vērā apgalvojumu 2.24 secināms:

$$\mathrm{ld}(\prod_{i=1}^{m} a_i, p) = 1.$$

Pretruna! Tātad kaut viens a_i dalās ar p. $\blacksquare$

3.10. Apgalvojums. *Katrs vesels skaitlis, kas lielāks par* 1, *ir vai nu pirmskaitlis, vai arī (ar precizitāti līdz reizinātāju secībai) vienā vienīgā veidā sadalās pirmskaitļu reizinājumā.*

□ Ja $a \in \mathbb{Z}_+$ un $a > 1$, tad ar p_1 apzīmējot no 1 atšķirīgo mazāko skaitļa a dalītāju, kas saskaņā ar apgalvojumu 3.3 ir pirmskaitlis, iegūst $a = p_1 a_1$.

Ja $a_1 > 1$, tad ar p_2 apzīmējot no 1 atšķirīgo mazāko skaitļa a_1 dalītāju, iegūst $a_1 = p_2 a_2$.

Šo procedūru turpina līdz iegūst $a_n = 1$. Skaitļa n eksistenci garantē fakts, ka

$$a > a_1 > a_2 > \ldots$$

ir dilstoša naturālo skaitļu virkne, un tāpēc tā nevar saturēt vairāk par a locekļiem, t.i., $n \leq a$.

Tā rezultātā

$$\begin{aligned} a &= p_1 a_1 \\ a_1 &= p_2 a_2 \\ a_2 &= p_3 a_3 \\ &\cdots \\ a_{n-2} &= p_{n-1} a_{n-1} \\ a_{n-1} &= p_n \end{aligned}$$

$$\begin{aligned} a a_1 a_2 \dots a_n &= (p_1 a_1)(p_2 a_2)(p_3 a_3) \dots (p_{n-1} a_{n-1}) p_n \\ a &= p_1 p_2 \dots p_n \end{aligned}$$

Tagad pievērsīsimies unitātei. Ja pieņem, ka

$$a = q_1 q_2 \dots q_k \,,$$

kur visi q_i ir pirmskaitļi, tad

$$p_1 p_2 \dots p_n = q_1 q_2 \dots q_k \,. \tag{7}$$

Tā kā $q_1 \setminus q_1 q_2 \dots q_k$, tad $q_1 \setminus p_1 p_2 \dots p_n$. Tas nozīmē (skatīt apgalvojumu 3.9), ka eksistē vismaz viens tāds p_i, ka $q_1 \setminus p_i$. Tā kā reizinātāju secība nav svarīga, tad var pieņemt, ka tieši p_1 dalās ar q_1. Ņemot vērā, ka p_1 ir pirmskaitlis, secināms: p_1 dalās ar 1, vai arī ar p_1, un tikai ar šiem skaitļiem; tāpēc $q_1 = p_1$. Vienādības (7) abas puses saīsinot ar $p_1 = q_1$ iegūst

$$p_2 \dots p_n = q_2 \dots q_k \,.$$

Šo procedūru var turpināt līdz kādā no vienādības (7) pusēm vairs nebūs reizinātāju atšķirīgu no 1. Konkrētības labad var pieņemt, ka $n \le k$, tad

$$1 = q_{n+1} q_{n+2} \dots q_k \,. \tag{8}$$

Tā kā vienādība (8) nevar būt spēkā, ja kaut vienam $j \in \overline{n+1, k}$ $q_j > 1$, tad tas nozīmē, ka $n = k$.

Līdz ar to pierādīts, ka $q_1 q_2 \dots q_k$ ar precizitāti līdz reizinātāju secībai ir tā pati izteiksme $p_1 p_2 \dots p_n$. ■

3.11. Definīcija. *Katru pirmskaitli p, kas dala skaitli a sauc par skaitļa a pirmreizinātāju.*

3.12. Definīcija. *Reizinājumu $p_1 p_2 \dots p_n$, sauc par skaitļa a sadalījumu pirmreizinātājos, ja*

$$\forall i \in \overline{1,n}\; p_i \in \mathbb{P} \;\wedge\; a = p_1 p_2 \dots p_n \,.$$

3.13. Definīcija. *Reizinājumu $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$, sauc par skaitļa a kanonisko sadalījumu, ja*

$$\begin{aligned} \forall i \in \overline{1,n}\,[p_i \in \mathbb{P} \;\wedge\; \alpha_i \in \mathbb{Z}_+ \quad &\wedge \quad \forall j \in \overline{1,n}\,(i \neq j \Rightarrow p_i \neq p_j)] \\ &\wedge \quad a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n} \,. \end{aligned}$$

3.14. Apgalvojums. *Katram veselamskaitlim, kas lielāks par 1, (ar precizitāti līdz reizinātāju secībai) eksistē viens vienīgs kanoniskais sadalījums.*

□ Saskaņā ar apgalvojumu 3.10 skaitlim a ar precizitāti līdz reizinātāju secībai eksistē viens vienīgs sadalījums pirmreizinātājos

$$a = q_1 q_2 \dots q_m \,. \tag{9}$$

Apzīmējot ar $p_1, p_2, \dots, p_n$ dažādos skaitļa a pirmreizinātājus un ar $\alpha_1, \alpha_2 \dots, \alpha_n$ — skaitu, cik katrs no reizinātājiem ieiet vienādībā (9), iegūst

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n} \,.$$

Ja $a = r_1^{\beta_1} r_2^{\beta_2} \dots r_k^{\beta_k}$ ir skaitļa a kanoniskais sadalījums, tad

$$a = \underbrace{r_1 r_1 \dots r_1}_{\beta_1 \text{ reizes}} \underbrace{r_2 r_2 \dots r_2}_{\beta_2 \text{ reizes}} \dots \underbrace{r_k r_k \dots r_k}_{\beta_k \text{ reizes}} \tag{10}$$

ir skaitļa a sadalījums pirmreizinātājos; un tā kā tas ar precizitāti līdz reizinātāju secībai ir viens vienīgs, tad tas nozīmē, ka

$$\{r_1, r_2, \dots, r_k\} = \{p_1, p_2 \dots, p_n\}$$

Ņemot vērā, ka visi r_i ir dažādi, tāpat arī visi p_j ir dažādi, secināms: $k = n$. Tā kā elementu r_i secība gan pierakstā (10), gan pierakstā $\{r_1, r_2, \dots, r_k\}$ nav svarīga, tad var pieņemt, ka $r_1 = p_1, r_2 = p_2, \dots, r_n = p_n$. Vēlreiz atsaucoties uz apgalvojumu 3.10 tagad secināms, ka $\beta_1 = \alpha_1, \beta_2 = \alpha_2, \dots, \beta_n = \alpha_n$. Līdz ar to esam pierādījuši, ka skaitlim a (ar precizitāti līdz reizinātāju secībai) eksistē viens vienīgs kanoniskais sadalījums. ■

3.15. Piemērs. *Skaitļa* 130 931 *kanoniskais sadalījums:*

$$130\,931 = 311 \cdot 421\,.$$

3.16. Apgalvojums. *Ja* $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$ *ir skaitļa* a *kanoniskais sadalījums, tad jebkurš skaitļa* a *dalītājs*

$$d = p_1^{\beta_1} p_2^{\beta_2} \dots p_n^{\beta_n}\,, \tag{11}$$

kur

$$0 \le \beta_1 \le \alpha_1, 0 \le \beta_2 \le \alpha_2, \dots, 0 \le \beta_n \le \alpha_n\,,$$

□ $\Rightarrow$ Ja $d \setminus a$, tad eksitē tāds vesels skaitlis q, ka $a = dq$. Tātad visi skaitļa d pirmreizinātāji ieiet skaitļa d kanoniskajā sadalījumā ar pakāpi ne lielāku, kā tie ieiet skaitļa a kanoniskajā sadalījumā. Tāpēc d ir izskatā (11).

$\Leftarrow$ Ja d ir izskatā (11), tad $d \setminus a$, jo

$$a : d = p_1^{\alpha_1-\beta_1} p_2^{\alpha_2-\beta_2} \dots p_n^{\alpha_n-\beta_n} \in \mathbb{Z}_+\,. \blacksquare$$

3.17. Piemērs. *Skaitļa* $60 = 2^2 \cdot 3 \cdot 5$ *dalītāji ir* $1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60$.

3.18. Apgalvojums. $\mathrm{ld}(a_1, a_2, \dots, a_n) = \prod\limits_i p_i^{\alpha_i}$,

kur p_i *ir skaitļu* $a_1, a_2 \dots, a_n$ *kopīgais pirmreizinātājs;* α_i *ir mazākā pakāpe ar kādu* p_i *ieiet skaitļu* $a_1, a_2 \dots, a_n$ *kanoniskajos sadalījumos.*

□ Ja $\forall j\ (d \setminus a_j)$, tad $\forall j \exists q_j\ (a_j = dq_j)$. Tas nozīmē, ka jebkurš skaitļa d pirmreizinātājs p_i ir arī katra skaitļa a_j pirmreizinātājs; tāpēc p_i ieiet skaitļa d kanoniskajā sadalījumā ar pakāpi, kas nepārsniedz mazāko no pakāpēm ar kādām p_i ieiet skaitļu a_j kanoniskajos sadalījumos.

No otras puses, ja:

(i) jebkurš skaitļa d pirmreizinātājs p_i ir arī katra skaitļa a_j pirmreizinātājs;

(ii) skaitlis p_i ieiet skaitļa d kanoniskajā sadalījumā ar pakāpi α_i, kas nepārsniedz mazāko no pakāpēm ar kādu p_i ieiet visu skaitļu a_j kanoniskajos sadalījumos, tad $\forall j\ (d \setminus a_j)$.

Tātad nosacījumi (i) un (ii) ir nepieciešami un pietiekami, lai d būtu skaitļu $a_1, a_2, \dots, a_n$ kopīgais dalītājs.

Pats lielākais no skaitļiem d ir tas, kura kanoniskajā sadalījumā katrs p_i ieiet ar vislielāko pakāpi, proti, pakāpi, kas ir vienāda ar mazāko no pakāpēm ar kādām p_i ieiet skaitļu a_j kanoniskajos sadalījumos. ■

3.19. Apgalvojums. *Skaitļu* $a_1, a_2, \ldots, a_n$ *kopīgo dalītāju kopa* $D(a_1, a_2, \ldots, a_n)$ *sakrīt ar skaitļa* $\mathrm{ld}(a_1, a_2, \ldots, a_n)$ *dalītāju kopu.*

□ Jāparāda, ka

$$\{d \mid \forall j \in \overline{1,n}\ (d \diagdown a_j)\} \quad = \quad \{\delta \mid \delta \diagdown \mathrm{ld}(a_1, a_2, \ldots, a_n)\}\,,$$

proti,

$$D(a_1, a_2, \ldots, a_n) = D(\mathrm{ld}(a_1, a_2, \ldots, a_n))\,.$$

Tā kā $\forall j \in \overline{1,n}\ \ \mathrm{ld}(a_1, a_2, \ldots, a_n) \diagdown a_j$, tad saskaņā ar apgalvojumu 1.2

$$\{\delta \mid \delta \diagdown \mathrm{ld}(a_1, a_2, \ldots, a_n)\} \subseteq \{d \mid \forall j \in \overline{1,n}\ (d \diagdown a_j)\}\,,$$

t.i.,

$$D(\mathrm{ld}(a_1, a_2, \ldots, a_n)) \subseteq D(a_1, a_2, \ldots, a_n)\,.$$

No otras puses, ja $\forall j \in \overline{1,n}\ (d \diagdown a_j)$, tad $\forall j \exists q_j\ (a_j = dq_j)$. Tas nozīmē, ka jebkurš skaitļa d pirmreizinātājs p_i ir arī katra skaitļa a_j pirmreizinātājs; tāpēc p_i ieiet skaitļa d kanoniskajā sadalījumā ar pakāpi, kas nepārsniedz mazāko no pakāpēm ar kādām p_i ieiet skaitļu a_j kanoniskajos sadalījumos.

Saskaņā ar apgalvojumu 3.18 skaitļa $\mathrm{ld}(a_1, a_2, \ldots, a_n)$ kanoniskais sadalījums

$$\mathrm{ld}(a_1, a_2, \ldots, a_n) = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$$

satur pirmreizinātāju p_i ar pakāpi α_i, kas ir tieši vienāda ar mazāko no pakāpēm ar kādu p_i ieiet skaitļu $a_1, a_2, \ldots, a_n$ kanoniskajos sadalījumos. Līdz ar to, ja

$$d = p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k}\,,$$

tad $\forall i\ \beta_i \leq \alpha_i$. Tātad

$$\{d \mid \forall j \in \overline{1,n}\ (d \diagdown a_j)\} \subseteq \{\delta \mid \delta \diagdown \mathrm{ld}(a_1, a_2, \ldots, a_n)\}\,,$$

t.i.,

$$D(a_1, a_2, \ldots, a_n) \subseteq D(\mathrm{ld}(a_1, a_2, \ldots, a_n))\,.$$

Visu savelkot kopā tagad varam secināt, ka

$$D(a_1, a_2, \ldots, a_n) = D(\mathrm{ld}(a_1, a_2, \ldots, a_n))\,. \blacksquare$$

3.20. Piemērs.

$$\begin{aligned} 6\,791\,400 &= 2^3 \cdot 3^2 \cdot 5^2 \cdot 7^3 \cdot 11\,, \\ 178\,500 &= 2^2 \cdot 3 \cdot 5^3 \cdot 7 \cdot 17\,, \\ 27\,720 &= 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11\,. \end{aligned}$$

No šejienes

$$\mathrm{ld}(6\,791\,400, 178\,500, 27\,720) = 2^2 \cdot 3 \cdot 5 \cdot 7 = 420\,.$$

3.21. Apgalvojums. *Ja* $\mathrm{ld}(a,b) = 1$ *un* $a \diagdown c$, $b \diagdown c$, *tad* $ab \diagdown c$.

□ Saskaņā ar doto $a \diagdown c$, tāpēc $\exists d\ (c = ad)$. Tagad atsaucoties uz apgalvojumu 2.23 secināms: $b \diagdown d$. Tātad $\exists \delta\ (d = b\delta)$. Līdz ar to

$$c = ad = a(b\delta) = (ab)\delta\,,$$

kas arī parāda, ka $ab \diagdown c$. ■

3.22. Apgalvojums. *Skaitļu* $a_1, a_2, \ldots, a_n$ *mazākais kopīgais dalāmais*

$$\mathrm{md}(a_1, a_2, \ldots, a_n) = \prod_i p_i^{\alpha_i}\,,$$

kur

p_i — *pirmreizinātājs vismaz vienam no skaitļiem* a_j*;*
α_i — *maksimālā pakāpe ar kādu* p_i *ieiet skaitļu* a_j *kanoniskajos sadalījumos.*

□ Ja m ir skaitļu $a_1, a_2, \ldots, a_n$ dalāmais, tad $\forall j \exists q_j\ (m = a_j q_j)$. Tas parāda, ka jebkura skaitļa a_j pirmreizinātājs p_i ir skaitļa m dalītājs. Šim dalītājam p_i skaitļa m kanoniskajā sadalījumā jāieiet ar pakāpi α_i ne mazāku par maksimālo no pakāpēm ar kādu p_i ieiet skaitļu a_j kanoniskajos sadalījumos (apgalvojums 3.16).

No otras puses, ja:

(i) jebkura skaitļa a_j pirmreizinātājs p_i ir arī skaitļa m pirmreizinātājs;

(ii) skaitlis p_i skaitļa m kanoniskajā sadalījumā ieiet ar pakāpi α_i ne mazāku par maksimālo no pakāpēm ar kādām p_i ieiet skaitļu a_j kanoniskajos sadalījumos, tad m ir skaitļu $a_1, a_2, \ldots, a_n$ kopīgais dalāmais.

Tātad nosacījumi (i) un (ii) ir nepieciešami un pietiekami, lai m būtu skaitļu $a_1, a_2, \ldots, a_n$ kopīgais dalāmais.

Pats mazākais no skaitļiem m ir tas, kura kanoniskajā sadalījumā katrs skaitļu a_j pirmreizinātājs p_i ieiet ar pakāpi α_i, kas ir tieši vienāda ar maksimālo no pakāpēm ar kādām p_i ieiet skaitļu a_j kanoniskajos sadalījumos. ■

3.23. Vingrinājums. *Ja* $\mathrm{ld}(a,b)=1$, *tad*

$$\forall m\in\mathbb{N}\forall n\in\mathbb{N}\ \mathrm{ld}(a^m,b^n)=1\,.$$

□ Skatīt apgalvojumu 2.24 ■

3.24. Apgalvojums. *Ja* $a_1,a_2,\ldots,a_n$ *ir savstarpēji pirmskaitļi, tad šo skaitļu mazākais kopīgais dalāmais*

$$\mathrm{md}(a_1,a_2,\ldots,a_n)=a_1a_2\ldots a_n\,.$$

□ (i) Vispirms parādīsim, ka

$$\forall k\in\overline{1,n}\ \mathrm{md}(a_1,a_2,\ldots,a_n)=a_1a_2\ldots a_kd_k\,.$$

Pierādījums induktīvs pa k.

Indukcijas bāze: tā kā $a_1\nmid\mathrm{md}(a_1,a_2,\ldots,a_n)$, tad eksistē tāds d_1, ka $\mathrm{md}(a_1,a_2,\ldots,a_n)=a_1d_1$.

Induktīvā pāreja: pieņemsim, ka $\mathrm{md}(a_1,a_2,\ldots,a_n)=a_1a_2\ldots a_{k-1}d_{k-1}$. Saskaņā ar 2.24

$$\mathrm{ld}(a_1a_2\ldots a_{k-1},a_k)=1\,.$$

Tā kā $a_k\nmid\mathrm{md}(a_1a_2\ldots a_n)=a_1a_2\ldots a_{k-1}d_{k-1}$ un $\mathrm{ld}(a_1a_2\ldots a_{k-1},a_k)=1$ (apgalvojums 2.24), tad $a_k\nmid d_k$ (apgalvojums 2.23). No šejienes, eksistē tāds d_k, ka $d_{k-1}=a_kd_k$. Tātad

$$\mathrm{md}(a_1,a_2,\ldots,a_n)=a_1a_2\ldots a_{k-1}a_kd_k\,.$$

Līdz ar to veikta induktīvā pāreja.

(ii) Mēs tikko pierādījām, ka

$$\mathrm{md}(a_1,a_2,\ldots,a_n)=a_1a_2\ldots a_nd_n\geq a_1a_2\ldots a_n\,.$$

Tagad ņemam vērā, ka $\forall i\ (a_i\nmid a_1a_2\ldots a_n)$, tāpēc

$$\mathrm{md}(a_1,a_2,\ldots,a_n)\leq a_1a_2\ldots a_n\,.$$

Tikko konstatētās nevienādības ļauj secināt, ka

$$\mathrm{md}(a_1,a_2,\ldots,a_n)=a_1a_2\ldots a_n\,.\ \blacksquare$$

3.25. Teorēma. *Skaitļu $a_1, a_2, \ldots, a_n$ kopīgo dalāmo kopa sakrīt ar šo skaitļu mazākā kopīgā dalāmām daudzkārtņu kopu.*

□ Ja m ir skaitļu $a_1, a_2, \ldots, a_n$ kopīgais dalāmais, tad $\forall i\ (a_i \diagdown m)$. Tātad katram a_i eksistē tāds q_i, ka $m = a_i q_i$. Tas parāda, ka katra skaitļa a_i jebkurš pirmreizinātājs p_j ir skaitļa m dalītājs. Šim dalītājam p_j skaitļa m kanoniskajā sadalījumā jāieiet ar pakāpi β_j ne mazāku par maksimālo no pakāpēm ar kādām p_j ieiet skaitļu a_i kanoniskajos sadalījumos. Tas nozīmē, ka

$$m = d \prod_j p_j^{\beta_j} ,$$

kur p_j ir pirmreizinātājs vismaz vienam no skaitļiem a_i, savukārt β_j ir pakāpe, kas nav mazāka par maksimālo no pakāpēm ar kādām p_j ieiet skaitļu a_i kanoniskajos sadalījumos.

Saskaņā ar apgalvojumu 3.22

$$\mathrm{md}(a_1, a_2, \ldots, a_n) = \prod_j p_j^{\alpha_j} ,$$

kur

p_j — pirmreizinātājs vismaz vienam no skaitļiem a_i;

α_j — maksimālā pakāpe ar kādu p_j ieiet skaitļu a_i kanoniskajos sadalījumos.

Tātad $\forall j\ \alpha_j \leq \beta_j$. No šejienes

$$m : \mathrm{md}(a_1, a_2, \ldots, a_n) = d \prod_j p_j^{\beta_j - \alpha_j} \in \mathbb{Z}_+ .$$

Līdz ar to $\mathrm{md}(a_1, a_2, \ldots, a_n) \diagdown m$, t.i., m ir $\mathrm{md}(a_1, a_2, \ldots, a_n)$ daudzkārtnis. ■

3.26. Piemērs. *Skaitļu*

$$\begin{aligned} 1\,800 &= 2^3 \cdot 3^2 \cdot 5^2 , \\ 3\,780 &= 2^2 \cdot 3^3 \cdot 5 \cdot 7 , \\ 8\,910 &= 2 \cdot 3^4 \cdot 5 \cdot 11 \end{aligned}$$

mazākais kopīgais dalāmais ir skaitlis

$$\mathrm{md}(1\,800, 3\,780, 8\,910) = 2^3 \cdot 3^4 \cdot 5^2 \cdot 7 \cdot 11 = 1\,247\,400 .$$

4. Ķēžu daļas.

Ķēžu daļas. Eilera algoritms. Rekurences vienādojumi.

4.1. Definīcija. *Vektoru pāri* $(q_1, q_2, \ldots, q_n)$, $(\delta_1, \delta_2, \ldots, \delta_n)$ *sauc par galīgu ķēžu daļu, ja:*

(i) $\forall i > 1\ q_i > 0$;

(ii)

$$\delta_i = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ddots + \cfrac{1}{q_{i-1} + \cfrac{1}{q_i}}}}.$$

q_i sauc par i–to *nepilno dalījumu*;

δ_i sauc par i–to *tuvinājuma daļu*.

Galīgas ķēžu daļas apzīmēšanai lieto pierakstu $[q_1; q_2, \ldots, q_n]$. Galīgu ķēžu daļu $[q_1; q_2, \ldots, q_n]$ sauc par skaitļa $\alpha \in \mathbb{R}$ *reprezentāciju*, ja $\alpha = \delta_n$. Šai gadījumā mēs arī teiksim, ka ķēžu daļa $[q_1; q_2, \ldots, q_n]$ reprezentē skaitli α.

4.2. Definīcija. *Virkņu pāri* $(q_i)_{i\in\mathbb{Z}_+}$, $(\delta_i)_{i\in\mathbb{Z}_+}$ *sauc par bezgalīgu ķēžu daļu, ja katram* i *vektoru pāris* $(q_1, q_2, \ldots, q_i)$, $(\delta_1, \delta_2, \ldots, \delta_i)$ *ir galīga ķēžu daļa.*

Bezgalīgas ķēžu daļas apzīmēšanai lieto pierakstu $[q_1; q_2, \ldots, q_n, \ldots]$. Bezgalīgu ķēžu daļu $[q_1; q_2, \ldots, q_n, \ldots]$ sauc par skaitļa $\alpha \in \mathbb{R}$ *reprezentāciju*, ja $\alpha = \lim\limits_{n\to\infty} \delta_n$. Šai gadījumā mēs arī teiksim, ka ķēžu daļa $[q_1; q_2, \ldots, q_n, \ldots]$ reprezentē skaitli α.

Eilera algoritms. Dots reāls skaitlis α.

Algoritma sākums. Definējam $\alpha_1 \rightleftharpoons \alpha$ Aprēķinam $q_1 \rightleftharpoons \lfloor \alpha_1 \rfloor$.

(i) Ja $\{\alpha_1\} = 0$, tad algoritms beidz darbu;

(ii) ja $\{\alpha_1\} \neq 0$, tad aprēķinam $\alpha_2 \rightleftharpoons \dfrac{1}{\{\alpha_1\}}$, un tālāk algoritms turpina darbu saskaņā ar induktīvo soli.

Induktīvais solis. Dots reāls skaitlis α_n. Aprēķinam $q_n \rightleftharpoons \lfloor \alpha_n \rfloor$.

(i) Ja $\{\alpha_n\} = 0$, tad algoritms beidz darbu;

(ii) ja $\{\alpha_n\} \neq 0$, tad aprēķinam $\alpha_{n+1} \rightleftharpoons \dfrac{1}{\{\alpha_n\}}$, un tālāk algoritms turpina darbu saskaņā ar induktīvo soli.

Tā rezultātā katram reālam skaitlim α Eilera algoritms, ja tas ir beidzis darbu, tad ir uzģenerējis divas galīgas virknes:

$$q_1, q_2, \ldots, q_n;$$
$$\alpha_1, \alpha_2, \ldots, \alpha_n.$$

Pretējā gadījumā Eilera algoritms ģenerē divas bezgalīgas virknes:

$$q_1, q_2, \ldots, q_n, \ldots$$
$$\alpha_1, \alpha_2, \ldots, \alpha_n, \ldots$$

Atzīmēsim, ka Eilera algoritms var arī nebūt algoritms šī vārda precīzā nozīmē, piemēram, ja skaitlis α nav efektīvi uzdots.

4.3. Apgalvojums. *Ja q_i skaitlim α ģenerēti saskaņā ar Eilera algoritmu un $\{\alpha_n\} \neq 0$, tad*

$$[q_1; q_2, \ldots, q_n, \alpha_{n+1}]$$

ir skaitļa α reprezentācija.

□ Pierādījums induktīvs pa n.

Indukcijas bāze. Pieņemsim, ka $\{\alpha_1\} \neq 0$, tad $q_1 = \lfloor \alpha_1 \rfloor$ un $\alpha_2 = \dfrac{1}{\{\alpha_1\}}$. No šejienes ķēžu daļai $[q_1; \alpha_2]$ tuvinājuma daļa

$$\delta_2 = q_1 + \frac{1}{\alpha_2} = \lfloor \alpha_1 \rfloor + \{\alpha_1\} = \alpha_1 = \alpha\,.$$

Induktīvā pāreja. Pieņemsim, ka $\{\alpha_n\} \neq 0$, tad arī $\{\alpha_{n-1}\} \neq 0$. Saskaņā ar indukcijas pieņēmumu ķēžu daļas $[q_1; q_2, \ldots, q_{n-1}, \alpha_n]$ tuvinājuma daļa

$$q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ddots + \cfrac{1}{q_{n-1} + \cfrac{1}{\alpha_n}}}} = \alpha\,.$$

Mums jāparāda, ka

$$q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ddots + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n + \cfrac{1}{\alpha_{n+1}}}}}} = \alpha\,.$$

Ņemot vērā induktīvo pieņēmumu, tas nozīmē, ka mums pietiek pierādīt vienādību $\alpha_n = q_n + \dfrac{1}{\alpha_{n+1}}$.

Saskaņā ar Eilera algoritmu $q_n = \lfloor \alpha_n \rfloor$ un $\alpha_{n+1} = \dfrac{1}{\{\alpha_n\}}$. No šejienes

$$q_n + \frac{1}{\alpha_{n+1}} = \lfloor \alpha_n \rfloor + \{\alpha_n\} = \alpha_n\,.$$

Līdz ar to veikta induktīvā pāreja. ■

4.4. Apgalvojums. *Ja q_i skaitlim α ģenerēti saskaņā ar Eilera algoritmu un $\{\alpha_n\} = 0$, tad*

$$[q_1; q_2, \ldots, q_n]$$

ir skaitļa α reprezentācija.

□ Ja reiz $\{\alpha_n\} = 0$, tad $\{\alpha_{n-1}\} \neq 0$. Saskaņā ar apgalvojumu 4.3

$$q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ddots + \cfrac{1}{q_{n-1} + \cfrac{1}{\alpha_n}}}} = \alpha\,.$$

Tagad pievēršanies Eilera algoritmam:

$$q_n = \lfloor \alpha_n \rfloor = \lfloor \alpha_n \rfloor + 0 = \lfloor \alpha_n \rfloor + \{\alpha_n\} = \alpha_n\,.$$

Tātad

$$\alpha = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{}{\ddots + \cfrac{1}{q_{n-1} + \cfrac{1}{\alpha_n}}}}}$$

$$= q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{}{\ddots + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}}}.$$

Tas arī nozīmē, ka ķēžu daļa $[q_1; q_2, \ldots, q_n]$ reprezentē skaitli α. ■

4.5. Apgalvojums. *Pieņemsim, ka* $\alpha \in \mathbb{Q}$.
(i) *Izvēlas* $r_0 \in \mathbb{Z}$ *un* $r_1 \in \mathbb{Z}_+$ *tā, lai* $\mathrm{ld}(r_0, r_1) = 1$ *un* $\alpha = \frac{r_0}{r_1}$.
(ii) *Skaitļu pārim* r_0, r_1 *pielieto Eiklīda algoritmu:*

$$\begin{aligned}
r_0 &= r_1 q_1' + r_2, & 0 < r_2 < r_1;\\
r_1 &= r_2 q_1' + r_3, & 0 < r_3 < r_2;\\
&\ldots\ldots\ldots\ldots\ldots\ldots \\
r_{i-1} &= r_i q_i' + r_{i+1}, & 0 < r_{i+1} < r_i;\\
&\ldots\ldots\ldots\ldots\ldots\ldots \\
r_{n-2} &= r_{n-1} q_{n-1}' + r_n, & 0 < r_n < r_{n-1};\\
r_{n-1} &= r_n q_n' + r_{n+1}, & 0 = r_{n+1} < r_n.
\end{aligned}$$

Ja q_i *skaitlim* α *ģenerēti saskaņā ar Eilera algoritmu, tad* $\forall i\ (q_i' = q_i)$ *un* $\{\alpha_n\} = 0$.

□ Pieņemsim, ka saskaņā ar Eilera algoritmu iegūti skaitļi

$$q_1, q_2, \ldots, q_k, \ldots$$
$$\alpha_1, \alpha_2, \ldots, \alpha_k, \ldots$$

Šobrīd mēs nezinam, vai šīs virknes ir galīgas, vai bezgalīgas, tāpēc pagaidām šo faktu nefiksēsim.

Tālākais pierādījums induktīvs.

Indukcijas bāze.

$$r_0 = r_1 q_1' + r_2 \qquad \text{un} \qquad 0 \leq r_2 < r_1 \,.$$

Saskaņā ar r_1 izvēli $r_1 \neq 0$, tāpēc

$$\frac{r_0}{r_1} = q_1' + \frac{r_2}{r_1} \,.$$

Tā kā $\dfrac{r_0}{r_1} = \alpha = \alpha_1$ un $0 \leq r_2 < r_1$, tad

$$\lfloor \alpha_1 \rfloor = q_1' \qquad \text{un} \qquad \{\alpha_1\} = \frac{r_2}{r_1} \,.$$

Līdz ar to $q_1' = q_1$ un $\{\alpha_1\} = 0 \Leftrightarrow r_2 = 0$. Tas nozīmē, ka Eilera algoritms šai brīdī beidz darbu tad un tikai tad, ja Eiklīda algoritms beidz darbu.

Indukcijas solis. Mēs pieņemam, ka

$$q_1' = q_1, q_2' = q_2, \ldots, q_{i-1}' = q_{i-1};$$

$$\alpha_1 = \frac{r_0}{r_1}, \alpha_2 = \frac{r_1}{r_2}, \ldots, \alpha_{i-1} = \frac{r_{i-2}}{r_{i-1}};$$

$$\{\alpha_1\} = \frac{r_2}{r_1}, \{\alpha_2\} = \frac{r_3}{r_2}, \ldots, \{\alpha_{i-1}\} = \frac{r_i}{r_{i-1}}$$

un $\{\alpha_{i-1}\} = 0 \Leftrightarrow r_i = 0$, proti, mēs pieņemam, ka Eilera algoritms šai brīdī beidz darbu tad un tikai tad, ja Eiklīda algoritms beidz darbu.

Saskaņā ar Eiklīda algoritmu

$$r_{i-1} = r_i q_i' + r_{i+1} \qquad \text{un} \qquad 0 \leq r_{i+1} < r_i \,.$$

Tā kā $r_i \neq 0$, tad

$$\frac{r_{i-1}}{r_i} = q_i' + \frac{r_{i+1}}{r_i}$$

un

$$\frac{r_{i-1}}{r_i} = \frac{1}{\{\alpha_{i-1}\}} = \alpha_i \,.$$

Tā rezultātā

$$\lfloor \alpha_i \rfloor = q_i' \qquad \text{un} \qquad \{\alpha_i\} = \frac{r_{i+1}}{r_i}\,.$$

Tas ļauj secināt, ka $q_i' = q_i$ un $\{\alpha_i\} = 0 \Leftrightarrow r_{i+1} = 0$. Tas nozīmē, ka Eilera algoritms šai brīdī beidz darbu tad un tikai tad, ja Eiklīda algoritms beidz darbu. Līdz ar to pilnībā veikta induktīvā pāreja. ■

4.6. Teorēma. *Eilera algoritms skaitlim α beidz darbu galīgā soļu skaitā tad un tikai tad, ja $\alpha \in \mathbb{Q}$.*

□ $\Rightarrow$ Ja Eilera algoritms beidz darbu galīgā soļu skaitā, tad eksistē tāds α_n, ka $\{\alpha_n\} = 0$. Saskaņā ar apgalvojumu 4.4 ķēžu daļa $[q_1; q_2, \ldots, q_n]$ ir skaitļa α reprezentācija, proti,

$$\alpha = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ddots + \cfrac{1}{q_{n-1} + \cfrac{1}{q_n}}}} \in \mathbb{Q}\,.$$

$\Leftarrow$ Ja $\alpha \in \mathbb{Q}$, tad saskaņā ar apgalvojumu 4.5 Eilera algoritmu var reducēt uz Eiklīda algoritmu. Tā kā Eiklīda algoritms beidz darbu galīgā soļu skaitā, tad arī Eilera algoritms beidz darbu galīgā soļu skaitā. ■

Rekurences virknes. Katrai reālo skaitļu virknei $(q_n)_{n\in\mathbb{Z}_+}$ definēsim virkņu pāri $(P_n)_{n\in\mathbb{N}}$, $(Q_n)_{n\in\mathbb{N}}$:

$$\begin{aligned} &P_0 \rightleftharpoons 1, \quad P_1 \rightleftharpoons q_1, \quad P_n \rightleftharpoons q_n P_{n-1} + P_{n-2};\\ &Q_0 \rightleftharpoons 0, \quad Q_1 \rightleftharpoons 1, \quad Q_n \rightleftharpoons q_n Q_{n-1} + Q_{n-2}\,. \end{aligned}$$

4.7. Definīcija. *Virknes (P_n), (Q_n) sauc par virknes (q_n) rekurences virknēm.*

4.8. Lemma. *Pieņemsim, ka (P_n), (Q_n) ir virknes (q_n) rekurences virknes, bet (P_n'), (Q_n') ir virknes (q_n') rekurences virknes. Ja $q_n' = q_{n+1}$, tad*

$$\begin{cases} P_{n+1} &= Q_n' + q_1 P_n'\,,\\ Q_{n+1} &= P_n'\,. \end{cases}$$

□ Pierādījums induktīvs pa n.

Indukcijas bāze.

(i) Saskaņā ar virkņu $(P_n), (Q_n)$ un $(P'_n), (Q'_n)$ definīciju

$$P_1 = q_1;\ P'_0 = 1 \quad \text{un} \quad Q'_0 = 0\,,$$

tāpēc

$$Q'_0 + q_1 P'_0 = q_1 = P_1\,.$$

Savukārt

$$Q_1 = 1 \quad \text{un} \quad P'_0 = 1, \quad \text{tāpēc} \quad P'_0 = Q_1\,.$$

(ii) Saskaņā ar virkņu $(P_n), (Q_n)$ un $(P'_n), (Q'_n)$ definīciju

$$\begin{aligned} P_2 = q_2 P_1 + P_0 &= q_2 q_1 + 1; \\ Q'_1 + q_1 P'_1 &= 1 + q_1 q_2\,, \end{aligned}$$

tāpēc

$$Q'_1 + q_1 P'_1 = P_2\,.$$

Savukārt

$$\begin{aligned} Q_2 = q_2 Q_1 + Q_0 &= q_2; \\ P'_1 &= q_2\,, \end{aligned}$$

tāpēc $P'_1 = Q_2$.

Induktīvā pāreja.

$$\begin{aligned} P_{n+1} &= q_{n+1} P_n + P_{n-1} \\ &= q_{n+1}(Q'_{n-1} + q_1 P'_{n-1}) + Q'_{n-2} + q_1 P'_{n-2} \\ &= q'_n(Q'_{n-1} + q_1 P'_{n-1}) + Q'_{n-2} + q_1 P'_{n-2} \\ &= q'_n Q'_{n-1} + Q'_{n-2} + q_1(q'_n P'_{n-1} + P'_{n-2}) \\ &= Q'_n + q_1 P'_n\,; \end{aligned}$$

$$\begin{aligned} Q_{n+1} &= q_{n+1} Q_n + Q_{n-1} \\ &= q'_n P'_{n-1} + P'_{n-2} = P'_n\,. \blacksquare \end{aligned}$$

4.9. Lemma. *Katrai ķēžu daļai* $[q_1; q_2, \ldots, q_n, \ldots]$ *tuvinājuma daļa*

$$\delta_n = \frac{P_n}{Q_n}\,.$$

□ Pierādījums induktīvs pa n.
Indukcijas bāze.

$$\delta_1 = q_1 = \frac{q_1}{1} = \frac{P_1}{Q_1}\,.$$

Induktīvā pāreja.

Pieņemsim, ka jebkurai ķēžu daļai $\delta_n = \dfrac{P_n}{Q_n}$. Tātad arī ķēžu daļai $[q_1'; q_2', \ldots, q_n', \ldots]$ ir spēkā vienādība $\delta_n' = \dfrac{P_n'}{Q_n'}$.

Izvēlamies $q_i' \rightleftharpoons q_{i+1}$. Šai situācijā

$$\begin{aligned}
\delta_{n+1} &= q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \ddots + \cfrac{1}{q_n + \cfrac{1}{q_{n+1}}}}} \\
&= q_1 + \cfrac{1}{q_1' + \cfrac{1}{q_2' + \ddots + \cfrac{1}{q_{n-1}' + \cfrac{1}{q_n'}}}} \\
&= q_1 + \frac{1}{\delta_n'} \\
&= q_1 + \frac{Q_n'}{P_n'} = \frac{q_1 P_n' + Q_n'}{P_n'} = \frac{P_n}{Q_n}\,.
\end{aligned}$$

Pēdējā vienādība iegūta balstoties uz lemmu 4.8 ■

4.10. Piemērs. *Skaitļa* $\alpha = \dfrac{105}{38}$ *izvirzījums ķēžu daļā.*

Risinājums. Izmantojam Eiklīda algoritmu:

$$
\begin{array}{rrrr}
 & & 105 & :38=2 \\
 & - & 76 & \\
\hline
 & 38 & :29 & =1 \\
 - & 29 & & \\
\hline
 & 29 & :9 & =3 \\
 - & 27 & & \\
\hline
 & 9 & :2 & =4 \\
 - & 8 & & \\
\hline
 & 2 & :1 & =2
\end{array}
$$

Tagad varam sastādīt tabulu:

q_i		2	1	3	4	2
P_i	1	2	3	11	47	105
Q_i	0	1	1	4	17	38

Tā rezultātā ķēžu daļa $[2;1,3,4,2]$ reprezentē skaitli $\dfrac{105}{38}$.

4.11. Apgalvojums. *Ja*
(i) $[q_1;q_2,\ldots,q_n,\ldots]$ *ir ķēžu daļa;*
(ii) δ_n — *n–tā tuvinājuma daļa;*
(iii) $(P_n),(Q_n)$ — *šīs ķēžu daļas rekurences virknes, tad*

$$\text{(i)} \qquad P_nQ_{n-1}-Q_nP_{n-1}=(-1)^n\,,$$
$$\text{(ii)} \qquad \delta_n-\delta_{n-1}=\frac{(-1)^n}{Q_nQ_{n-1}}\,.$$

□ (i) Pierādījums induktīvs pa n.
Indukcijas bāze.

$$\begin{aligned}
P_1Q_0-Q_1P_0 &= 1\cdot 0-1\cdot 1=(-1)^1\,;\\
P_2Q_1-Q_2P_1 &= (q_2P_1+P_0)\cdot 1-(q_2Q_1+Q_0)q_1\\
&= (q_2q_1+1)-(q_2\cdot 1+0)q_1\\
&= 1=(-1)^2\,.
\end{aligned}$$

Induktīvā pāreja.

$$\begin{aligned} P_nQ_{n-1} - Q_nP_{n-1} &= (q_nP_{n-1} + P_{n-2})Q_{n-1} - (q_nQ_{n-1} + Q_{n-2})P_{n-1} \\ &= q_n(P_{n-1}Q_{n-1} - Q_{n-1}P_{n-1}) \\ &+ P_{n-2}Q_{n-1} - Q_{n-2}P_{n-1} \\ &= -(P_{n-1}Q_{n-2} - Q_{n-1}P_{n-2}) \\ &= -(-1)^{n-1} = (-1)^n\,. \end{aligned}$$

(ii)

$$\begin{aligned} \delta_n - \delta_{n-1} &= \frac{P_n}{Q_n} - \frac{P_{n-1}}{Q_{n-1}} \\ &= \frac{P_nQ_{n-1} - Q_nP_{n-1}}{Q_nQ_{n-1}} = \frac{(-1)^n}{Q_nQ_{n-1}}\,. \blacksquare \end{aligned}$$

4.12. Apgalvojums. *Ja* $[q_1; q_2, \ldots, q_n, \alpha_{n+1}]$ *ir skaitļa* α *reprezentācija ķēžu daļā ar Eilera algoritmu, tad*

$$\begin{aligned} &\text{(i)} && (s \in \overline{1,n} \Rightarrow Q_{s-1} \le Q_s) \ \wedge \ (2 < s \le n \Rightarrow Q_{s-1} < Q_s)\,, \\ &\text{(ii)} && s \in \overline{2,n} \Rightarrow \delta_{s-1} < \alpha < \delta_s \ \vee \ \delta_{s-1} > \alpha > \delta_s\,, \\ &\text{(iii)} && 1 < s \le n \Rightarrow |\alpha - \delta_s| < \frac{1}{(s-1)^2}\,. \end{aligned}$$

□ (i) Pierādījums induktīvs pa s.
Indukcijas bāze.

$$\begin{aligned} &Q_0 = 0,\ Q_1 = 1, Q_2 = q_2 \cdot 1 + 0 \ge 1 = Q_1\,, \\ &Q_3 = q_3Q_2 + Q_1 \ge Q_2 + Q_1 > Q_2\,. \end{aligned}$$

Induktīvā pāreja.

$$Q_s = q_sQ_{s-1} + Q_{s-2} \ge Q_{s-1} + Q_{s-2} > Q_{s-1}\,.$$

(ii) Apskatīsim ķēžu daļu $[q_1; q_2, \ldots, q_s, \alpha_{s+1}]$, un atbilstošās rekurenču virknes $(P_i^s), (Q_i^s)$. Atzīmēsim, ja $i \le s$, tad

$$P_i^s = P_i^n =_7 P_i \qquad \text{un} \qquad Q_i^s = Q_i^n =_7 Q_i\,.$$

No šejienes

$$\alpha = \frac{P_{s+1}^s}{Q_{s+1}^s} = \frac{\alpha_{s+1}P_s + P_{s-1}}{\alpha_{s+1}Q_s + Q_{s-1}}$$

un

$$\begin{aligned}
\alpha - \delta_s &= \frac{\alpha_{s+1}P_s + P_{s-1}}{\alpha_{s+1}Q_s + Q_{s-1}} - \frac{P_s}{Q_s} \\
&= \frac{(\alpha_{s+1}P_s + P_{s-1})Q_s - P_s(\alpha_{s+1}Q_s + Q_{s-1})}{(\alpha_{s+1}Q_s + Q_{s-1})Q_s} \\
&= \frac{\alpha_{s+1}P_sQ_s + P_{s-1}Q_s - \alpha_{s+1}P_sQ_s - P_sQ_{s-1}}{(\alpha_{s+1}Q_s + Q_{s-1})Q_s} \\
&= \frac{-(P_sQ_{s-1} - Q_sP_{s-1})}{(\alpha_{s+1}Q_s + Q_{s-1})Q_s} \\
&= \frac{-(-1)^s}{(\alpha_{s+1}Q_s + Q_{s-1})Q_s} = \frac{(-1)^{s-1}}{(\alpha_{s+1}Q_s + Q_{s-1})Q_s}\,. \qquad (12)
\end{aligned}$$

Tā kā

$$\alpha_{s+1} = \frac{1}{\{\alpha_s\}} > 1\,,$$

tad

$$(\alpha_{s+1}Q_s + Q_{s-1})Q_s > Q_s^2 > 0\,. \qquad (13)$$

Tātad $\alpha - \delta_s = (-1)^{s-1}a_s$, kur $a_s > 0$. Tas nozīmē, ka

$$\begin{gathered}
(\alpha - \delta_s > 0 \ \wedge \ \alpha - \delta_{s-1} < 0) \ \vee \ (\alpha - \delta_s < 0 \ \wedge \ \alpha - \delta_{s-1} > 0)\,, \\
\delta_s < \alpha < \delta_{s-1} \ \vee \ \delta_{s-1} < \alpha < \delta_s\,.
\end{gathered}$$

(iii) Ņemot vērā (12) un (13)

$$|\alpha - \delta_s| < \frac{1}{Q_s^2}\,.$$

Savukārt no (i) izriet, ka

$$Q_s > Q_{s-1} > \ldots > Q_2 \geq 1\,,$$

t.i., $Q_s \geq s - 1$. Tātad

$$|\alpha - \delta_s| < \frac{1}{(s-1)^2}\,. \quad \blacksquare$$

4.13. Teorēma. *Ja bezgalīga ķēžu daļa* $[q_1; q_2, \ldots, q_n, \ldots]$ *skaitlim* $\alpha \notin \mathbb{Q}$ *iegūta ar Eilera algoritmu, tad šī ķēžu daļa reprezentē skaitli* α*.*

□

$$\lim_{s\to\infty} |\alpha - \delta_s| \leq \lim_{s\to\infty} \frac{1}{(s-1)^2} = 0\,.$$

Tātad $\lim\limits_{s\to\infty} \delta_s = \alpha$. ■

Pasaulslavena problēma. Pieņemsim, ka $[q_1; q_2, \ldots, q_n, \ldots]$ skaitlim $\sqrt[3]{2}$ iegūta ar Eilera algoritmu. Vai virkne (q_n) ir ierobežota?

5. Funkcijas.

Populārākās skaitļu teorijā lietotās funkcijas. Multiplikatīvas funkcijas. Mebiusa un Eilera funkcijas.

5.1. Apgalvojums. *Kāpinātājs ar kādu dotais pirmskaitlis p ieiet skaitļa $n!$ kanoniskajā sadalījumā ir vienāds ar*

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \dots \tag{14}$$

□ Vispirms atzīmēsim, ka rinda (14) īstenībā ir galīga summa, jo $\left\lfloor \frac{n}{p^m} \right\rfloor = 0$ tiklīdz $n < p^m$. Ja

$$p < 2p < \dots < kp \leq n < (k+1)p\,,$$

tad

$$k \leq \frac{n}{p} < k+1\,.$$

No šejienes $k = \left\lfloor \frac{n}{p} \right\rfloor$. Tātad ir tieši k tādu skaitļu starp 1 un n, kas dalās ar p. Līdzīgi, ir tieši $\left\lfloor \frac{n}{p^2} \right\rfloor$ tādu skaitļu starp 1 un n, kas dalās p^2. Vispārīgā gadījumā tas nozīmē, ka ir tieši $\left\lfloor \frac{n}{p^s} \right\rfloor$ tādu skaitļu starp 1 un n, kas dalās ar p^s.

Tā kā $n! = 1 \cdot 2 \cdot \ldots \cdot n$, tad katram $a \in \overline{1,n}$ jāatrod tāds m, ka

$$p^m \setminus a \ \wedge \ p^{m+1} \nmid a\,;$$

un summāciju jāveic pa visiem $a \in \overline{1,n}$, t.i., jāatrod

$$\sum_{a=1}^{n} \max\{m \mid p^m \setminus a\}\,.$$

Ja

$$1 \leq a \leq n \ \wedge \ p^m \setminus a \ \wedge \ p^{m+1} \nmid a\,,$$

tad skaitlis a summā (14) ieskaitīts tieši m reizes, proti:

1) a ir starp tiem $\left\lfloor \frac{n}{p} \right\rfloor$ skaitļiem, kas dalās ar p;

2) a ir starp tiem $\left\lfloor \frac{n}{p^2} \right\rfloor$ skaitļiem, kas dalās ar p^2;

. . . . . .

m) a ir starp tiem $\left\lfloor \frac{n}{p^m} \right\rfloor$ skaitļiem, kas dalās ar p^m;

bet

m+1) a nav starp tiem $\left\lfloor \frac{n}{p^{m+1}} \right\rfloor$ skaitļiem, kas dalās ar p^{m+1}.

Līdz ar to skaitlis a summā (14) ieskaitīts tieši m reizes; un tāds pats spriedums ir spēkā par jebkuru skaitli $a \in \overline{1,n}$. Tāpēc

$$\sum_{a=1}^{n} \max\{m \,|\, p^m \nmid a\} = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \ldots \quad \blacksquare$$

5.2. Piemērs. *Kāpinātājs ar kādu skaitlis* 3 *ieiet skaitļa* 367! *kanoniskajā sadalījumā ir*

$$\left\lfloor \frac{367}{3} \right\rfloor + \left\lfloor \frac{367}{9} \right\rfloor + \left\lfloor \frac{367}{27} \right\rfloor + \left\lfloor \frac{367}{81} \right\rfloor + \left\lfloor \frac{367}{243} \right\rfloor$$

$$= \quad 122 + 40 + 13 + 4 + 1 = 180\,.$$

Multiplikatīvas funkcijas.

5.3. Definīcija. *Funkciju*

$$\theta \;:\; \mathbb{Z}_+ \;\to\; \mathbb{C}$$

sauc par multiplikatīvu funkciju, ja:
(i) $\exists a\ \theta(a) \neq 0$,
(ii) $\mathrm{ld}(a_1, a_2) = 1 \;\Rightarrow\; \theta(a_1 a_2) = \theta(a_1)\theta(a_2)$.

5.4. Piemērs. $\forall s \in \mathbb{C}\ \theta(a) \rightleftharpoons a^s$ *ir multiplikatīva funkcija.*
(i) $1^s = 1 \neq 0$;
(ii) $(a_1 a_2)^s = a_1^s a_2^s$.

5.5. Apgalvojums. *Ja* θ *ir multiplikatīva funkcija, tad* $\theta(1) = 1$.

□ Tā kā θ ir multiplikatīva funkcija, tad eksistē tāds a, ka $\theta(a) \neq 0$.

$$\theta(a) = \theta(a \cdot 1) = \theta(a)\theta(1) \, .$$

No šejienes pēc saīsināšanas ar $\theta(a)$ iegūstam $1 = \theta(1)$. ■

5.6. Apgalvojums. *Ja θ ir multiplikatīva funkcija un visiem indeksiem i, j izpildās nosacījums*

$$i \neq i \;\Rightarrow\; \mathrm{ld}(a_i, a_j) = 1 \, ,$$

tad

$$\theta\left(\prod_{i=1}^{k} a_i\right) = \prod_{i=1}^{k} \theta(a_i) \, .$$

□ Pierādījums induktīvs pa k.
Indukcijas bāze.
Saskaņā ar doto θ ir multiplikatīva funkcija, tāpēc

$$\theta\left(\prod_{i=1}^{2} a_i\right) = \theta(a_1 a_2) = \theta(a_1)\theta(a_2) = \prod_{i=1}^{2} \theta(a_i) \, .$$

Induktīvā pāreja.

$$\begin{aligned} \theta\left(\prod_{i=1}^{k} a_i\right) &= \theta\left(\left(\prod_{i=1}^{k-1} a_i\right) a_k\right) = \theta\left(\prod_{i=1}^{k-1} a_i\right) \, \theta(a_k) \\ &= \left(\prod_{i=1}^{k-1} \theta(a_i)\right) \, \theta(a_k) = \prod_{i=1}^{k} \theta(a_i) \, . \blacksquare \end{aligned}$$

5.7. Sekas. *Ja θ ir multiplikatīva funkcija un $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ ir skaitļa a kanoniskais sadalījums, tad*

$$\theta(a) = \theta(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}) = \theta(p_1^{\alpha_1}) \, \theta(p_2^{\alpha_2}) \dots \theta(p_k^{\alpha_k}) \, .$$

□ Sekas no apgalvojuma 5.6 ■

5.8. Teorēma. *Nosacījumi:*

(i) $\theta(1) \rightleftharpoons 1$;
(ii) $\forall p \in \mathbb{P}\ \forall \alpha \in \mathbb{Z}_+\ \exists! c \in \mathbb{C}\ \theta(p^\alpha) \rightleftharpoons c$;
(iii) $i \neq j \Rightarrow p_i \neq p_j$;
(iv) $\forall k \in \mathbb{Z}_+\ \forall i \in \overline{1,k}\ [p_i \in \mathbb{P}\ \wedge\ \alpha_i \in \mathbb{Z}_+\ \Rightarrow \theta\left(\prod_{i=1}^{k} p_i^{\alpha_i}\right) \rightleftharpoons \prod_{i=1}^{k} \theta(p_i^{\alpha_i})]$
viennozīmīgi definē multiplikatīvu funkciju θ.

□ Nosacījums (i) nodrošina, ka $\exists a\ \theta(a) \neq 0$. Savukārt nosacījums (ii) nodrošina, ka θ definēta visām pirmskaitļu pakāpēm. Ja a nav viena pirmskaitļa pakāpe, tad $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$, kur $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ ir skaitļa a kanoniskais sadalījums un $k > 1$. Šai gadījumā funkciju θ definē nosacījums (iv). Tā kā katram skaitlim ar precizitāti līdz reizinātāju secībai eksistē viens vienīgs kanoniskais sadalījums, tad nosacījums (iv) funkciju θ definē viennozīmīgi.

Atliek pārliecināties, ka funkcija θ apmierina nosacījumu

$$\mathrm{ld}(a_1, a_2) = 1 \ \Rightarrow\ \theta(a_1 a_2) = \theta(a_1)\theta(a_2)\,.$$

Pieņemsim, ka

$$\begin{aligned} a_1 &= p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}, \\ a_2 &= q_1^{\beta_1} q_2^{\beta_2} \dots q_n^{\beta_n} \end{aligned}$$

ir attiecīgi skaitļu a_1 un a_2 kanoniskie sadalījumi. Ja $\mathrm{ld}(a_1, a_2) = 1$, tad visi p_i atšķiras no visiem q_j. Līdz ar to

$$p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} q_1^{\beta_1} q_2^{\beta_2} \dots q_n^{\beta_n}$$

ir skaitļa $a_1 a_2$ kanoniskais sadalījums. No šejienes

$$\begin{aligned} \theta(a_1 a_2) &= \theta(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} q_1^{\beta_1} q_2^{\beta_2} \dots q_n^{\beta_n}) \\ &= \theta(p_1^{\alpha_1})\theta(p_2^{\alpha_2}) \dots \theta(p_k^{\alpha_k})\theta(q_1^{\beta_1})\theta(q_2^{\beta_2}) \dots \theta(q_n^{\beta_n}) \\ &= \theta(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k})\theta(q_1^{\beta_1} q_2^{\beta_2} \dots q_n^{\beta_n}) \\ &= \theta(a_1)\theta(a_2)\,. \blacksquare \end{aligned}$$

Šī teorēma parāda, ka multiplikatīva funkcija θ ir viennozīmīgi definēta, ja $\forall p \in \mathbb{P}\ \forall \alpha \in \mathbb{Z}_+\ \exists! c \in \mathbb{C}\ \theta(p^\alpha) \rightleftharpoons c$.

5.9. Piemērs. *Nosacījums*

$$\forall p \in \mathbb{P}\ \forall \alpha \in \mathbb{Z}_+ \quad \theta\ :\ p^\alpha \mapsto 2$$

definē multiplikatīvu funkciju.

Šai gadījumā, ja $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ ir skaitļa a kanoniskais sadalījums, tad $\theta(a) = 2^k$. Pirmajiem 12 pozitīvajiem naturālajiem skaitļiem multiplikatīvās funkcijas θ vērtības ir šādas:

$\theta(1) = 1,$	$\theta(2) = 2,$	$\theta(3) = 2,$
$\theta(4) = \theta(2^2) = 2,$	$\theta(5) = 2,$	$\theta(6) = \theta(2 \cdot 3) = 2^2 = 4,$
$\theta(7) = 2,$	$\theta(8) = \theta(2^3) = 2,$	$\theta(9) = \theta(3^2) = 2,$
$\theta(10) = \theta(2 \cdot 5) = 2^2 = 4,$	$\theta(11) = 2,$	$\theta(12) = \theta(2^2 \cdot 3) = 2^2 = 4\,.$

5.10. Apgalvojums. *Multiplikatīvu funkciju reizinājums ir multiplikatīva funkcija.*

□ Pierādījums induktīvs pa k, kur k reizinātāju skaits.

Indukcijas bāze.

Pieņemsim, ka $\theta(a) = \theta_1(a)\theta_2(a)$, kur θ_1, θ_2 ir multiplikatīvas funkcijas, tad

$$\theta(1) = \theta_1(1)\theta_2(1) = 1 \cdot 1 = 1.$$

Ja $\mathrm{ld}(ab) = 1$, tad

$$\begin{aligned} \theta(ab) &= \theta_1(ab)\theta_2(ab) \\ &= \theta_1(a)\theta_1(b)\ \theta_2(a)\theta_2(b) \\ &= (\theta_1(a)\theta_2(a))\ (\theta_1(b)\theta_2(b)) \\ &= \theta(a)\theta(b). \end{aligned}$$

Induktīvā pāreja nesatur nekādas jaunas idejas, tāpēc šo pierādījuma daļu atstājam lasītājam kā vingrinājumu. ■

5.11. Teorēma. *Ja θ ir multiplikatīva funkcija, $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ ir skaitļa a kanoniskais sadalījums, tad*

$$\sum_{d \backslash a} \theta(d) = \prod_{i=1}^{k} \sum_{j=0}^{\alpha_i} \theta(p_i^j)\,.$$

$$\square \qquad \prod_{i=1}^{k}\sum_{j=0}^{\alpha_i}\theta(p_i^j) = \sum_{\beta_1}^{\alpha_1}\dots\sum_{\beta_k=0}^{\alpha_k}\theta(p_1^{\beta_1})\dots\theta(p_k^{\beta_k})$$

$$= \sum_{\substack{0\le\beta_1\le\alpha_1\\ \dots\dots\dots\dots\\ 0\le\beta_k\le\alpha_k}} \theta(p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k})\,.$$

Tagad atsaucoties uz apgalvojumu 3.16 secināms, ka

$$\sum_{\substack{0\le\beta_1\le\alpha_1\\ \dots\dots\dots\dots\\ 0\le\beta_k\le\alpha_k}} \theta(p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}) = \sum_{d\backslash a}\theta(d)\,. \qquad \blacksquare$$

5.12. Apgalvojums. *Ja $p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}$ ir skaitļa a kanoniskais sadalījums, tad šī skaitļa dalītāju skaits*

$$\tau(a) = \prod_{i=1}^{k}(1+\alpha_i)\,.$$

$\square$ Atceramies (piemērs 5.4), ka funkcija $\theta(a) = a^s$ ir multiplikatīva funkcija. Tā ir multiplikatīva funkcija arī, ja $s = 0$. Šai situācijā $\forall a\ \theta(a) = a^0 = 1$.

Tagad atsaucoties uz teorēmu 5.11 iegūstam

$$\sum_{d\backslash a}\theta(d) = \prod_{i=1}^{k}\sum_{j=0}^{\alpha_i}\theta(p_i^j) = \prod_{i=1}^{k}(1+\alpha_i)\,.$$

No otras puses

$$\sum_{d\backslash a}\theta(d) = \sum_{d\backslash a}1 = \tau(a)\,. \qquad \blacksquare$$

5.13. Piemērs.

$$\tau(720) = \tau(2^4\cdot 3^2\cdot 5) = (4+1)(2+1)(1+1) = 30\,.$$

5.14. Apgalvojums. *Funkcija τ ir multiplikatīva funkcija, kas pilnībā definējama ar nosacījumu*

$$\forall p \in \mathbb{P}\ \forall \alpha \in \mathbb{Z}_+ \quad \tau(p^\alpha) = \alpha + 1\,.$$

□ Ņemot vērā teorēmu 5.8 mums faktiski ir jāpārbauda tikai šīs teorēmas nosacījums (iv). Saskaņā ar apgalvojumu 5.12

$$\tau(\prod_{i=1}^{k} p_i^{\alpha_i}) = \prod_{i=1}^{k}(1+\alpha_i) = \prod_{i=1}^{k}\tau(p_i^{\alpha_i})\,. \quad \blacksquare$$

5.15. Apgalvojums. *Ja $p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}$ ir skaitļa a kanoniskais sadalījums, tad šī skaitļa dalītāju summa*

$$S(a) = \prod_{i=1}^{k}\frac{p_i^{\alpha_i+1}-1}{p_i-1}\,.$$

□ Pierādījums kopē apgalvojuma 5.12 pierādījumu. Atceramies (piemērs 5.4), ka funkcija $\theta(a) = a^s$ ir multiplikatīva funkcija. Tā ir multiplikatīva funkcija arī, ja $s = 1$. Šai situācijā $\forall a\ \theta(a) = a^1 = a$.

Tagad atsaucoties uz teorēmu 5.11 iegūstam

$$\sum_{d\backslash a}\theta(d) \;=\; \prod_{i=1}^{k}\sum_{j=0}^{\alpha_i}\theta(p_i^j) = \prod_{i=1}^{k}\sum_{j=0}^{\alpha_i}p_i^j = \prod_{i=1}^{k}\frac{p_i^{\alpha_i+1}-1}{p_i-1}\,.$$

No otras puses

$$\sum_{d\backslash a}\theta(d) = \sum_{d\backslash a} d = S(a)\,. \quad \blacksquare$$

5.16. Piemērs.

$$\begin{aligned} S(720) &= S(2^4\cdot 3^2\cdot 5) = \frac{2^5-1}{2-1}\cdot\frac{3^3-1}{3-1}\cdot\frac{5^2-1}{5-1} \\ &= \frac{32-1}{1}\cdot\frac{27-1}{2}\cdot\frac{25-1}{4} = 31\cdot 13\cdot 6 = 2418\,. \end{aligned}$$

5.17. Apgalvojums. *Funkcija S ir multiplikatīva funkcija, kas pilnībā definējama ar nosacījumu*

$$\forall p \in \mathbb{P}\ \forall \alpha \in \mathbb{Z}_+ \quad S(p^\alpha) = \frac{p^{\alpha+1}-1}{p-1}\,.$$

□ Pierādījums kopē apgalvojuma 5.14 pierādījumu. Ņemot vērā teorēmu 5.8 mums faktiski ir jāpārbauda tikai šīs teorēmas nosacījums (iv). Saskaņā ar apgalvojumu 5.15

$$S(\prod_{i=1}^{k} p_i^{\alpha_i}) = \prod_{i=1}^{k} \frac{p_i^{\alpha_i+1}-1}{p_i-1} = \prod_{i=1}^{k} S(p_i^{\alpha_i})\,. \quad \blacksquare$$

5.18. Definīcija. *Multiplikatīvu funkciju*

$$\mu \,:\, \mathbb{Z}_+ \,\to\, \mathbb{Z}$$

sauc par Mēbiusa funkciju, ja

$$\begin{array}{ll} \text{(i)} & \forall p \in \mathbb{P} \quad \mu(p) \neq -1; \\ \text{(ii)} & \forall p \in \mathbb{P}\ \forall \alpha \in \mathbb{Z}_+ \quad [\alpha > 1 \Rightarrow \mu(p^\alpha) \neq 0]\,. \end{array}$$

5.19. Piemērs.

$$\begin{array}{ccc} \mu(1)=1, & \mu(2)=-1, & \mu(3)=-1, \\ \mu(4)=0, & \mu(5)=-1, & \mu(6)=1, \\ \mu(7)=-1, & \mu(8)=0, & \mu(9)=0, \\ \mu(10)=1, & \mu(11)=1, & \mu(12)=0\,. \end{array}$$

5.20. Sekas. *Ja skaitļa $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ kanoniskajā sadalījumā kaut viens kāpinātājs $\alpha > 1$, t.i., ja a dalās ar no skaitļa 1 atšķirīgu kavadrātu, tad $\mu(a) = 0$.*

□ Pieņemsim, ka $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ ir skaitļa a kanoniskais sadalījums un $\alpha_s > 1$, kur $0 < s \leq k$, tad

$$\begin{aligned} \mu(a) &= \mu(\prod_{i=1}^{k} p_i^{\alpha_i}) = \prod_{i=1}^{k} \mu(p_i^{\alpha_i}) \\ &= \mu(p_s^{\alpha_s}) \prod_{\substack{i=1 \\ i\neq s}}^{k} \mu(p_i^{\alpha_i}) = 0 \cdot \prod_{\substack{i=1 \\ i\neq s}}^{k} \mu(p_i^{\alpha_i}) = 0\,. \quad \blacksquare \end{aligned}$$

5.21. Sekas. *Ja skaitļa a kanoniskais sadalījums ir $p_1 p_2 \dots p_k$, tad*

$$\mu(a) = (-1)^k.$$

5.22. Teorēma. *Ja θ — multiplikatīva funkcija un $p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}$ ir skaitļa a kanoniskais sadalījums, tad*

$$\sum_{d\backslash a}\mu(d)\theta(d)=\prod_{i=1}^{k}(1-\theta(p_i))\,.$$

□ Vispirms ievērojam, ka funkcija

$$\nu(a)\rightleftharpoons\mu(a)\theta(a)$$

ir multiplikatīva funkcija, jo ir multiplikatīvu funkciju reizinājums (apgalvojums 5.10). Tālāk balstamies uz teorēmu 5.11. Ja $p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}$ ir skaitļa a kanoniskais sadalījums, tad

$$\sum_{d\backslash a}\nu(d)=\prod_{i=1}^{k}\sum_{j=0}^{\alpha_i}\nu(p_i^j)\,.$$

Tagad ņemam vērā Mēbiusa funkcijas īpašības.

(i) $\forall p\in\mathbb{P}\quad \nu(p)=\mu(p)\theta(p)=-\theta(p)$;

(ii) $\forall p\in\mathbb{P}\;\forall\alpha\in\mathbb{Z}_+\quad \nu(p^{\alpha+1})=\mu(p^{\alpha+1})\theta(p^{\alpha+1})=0\cdot\theta(p^{\alpha+1})=0\,.$

No šejienes

$$\prod_{i=1}^{k}\sum_{j=0}^{\alpha_i}\nu(p_i^j)\;=\;\prod_{i=1}^{k}(1+\nu(p_i))=\prod_{i=1}^{k}(1-\theta(p_i))\,.$$

Tātad

$$\sum_{d\backslash a}\mu(d)\theta(d)=\sum_{d\backslash a}\nu(d)=\prod_{i=1}^{k}\sum_{j=0}^{\alpha_i}\nu(p_i^j)=\prod_{i=1}^{k}(1-\theta(p_i))\,.\;\blacksquare$$

5.23. Sekas.

$$\sum_{d\backslash a}\mu(d)=\begin{cases}0, & \text{ja}\quad a>1,\\ 1, & \text{ja}\quad a=1.\end{cases}$$

□ Ņemot teorēmā 5.22 funkciju θ identiski vienādu ar 1 iegūst pierādījumu. ■

5.24. Sekas.

$$\sum_{d\searrow a}\frac{\mu(d)}{d}=\begin{cases}\prod\limits_{i=1}^{k}(1-\frac{1}{p_i}), & \text{ja} \quad a>1,\\ 1, & \text{ja} \quad a=1.\end{cases}$$

□ Ņemot teorēmā 5.22 funkciju $\theta=a^{-1}=\dfrac{1}{a}$ iegūst pierādījumu. ■

5.25. Teorēma. *Ja*

$$\begin{aligned}&\text{(i)} && (\delta_1,\delta_2\ldots,\delta_n)\in\mathbb{Z}_+;\\ &\text{(ii)} && (c_1,c_2,\ldots,c_n)\in\mathbb{C};\\ &\text{(iii)} && S=\sum_{\substack{i\\ \delta_i=1}}c_i;\\ &\text{(iii)} && S_d=\sum_{\substack{j\\ d\searrow\delta_j}}c_j\,,\end{aligned}$$

tad

$$S=\sum_d\mu(d)S_d\,.$$

□ Vispirms mēs ņemsim vērā sekas 5.23.

$$S \;=\; \sum_{\substack{i\\ \delta_i=1}}c_i \overset{5.23}{=} \sum_{\substack{i\\ \delta_i=1}}c_i\sum_{\substack{d\\ d\searrow\delta_i}}\mu(d) \overset{5.23}{=} \sum_i c_i\sum_{\substack{d\\ d\searrow\delta_i}}\mu(d)=\sum_i\sum_{\substack{d\\ d\searrow\delta_i}}c_i\mu(d)\,.$$

Tas nozīmē, ka tiek pārskatīti visi pāri (i,d) un summā tiek iekļauti tikai tie locekļi, kas apmierina nosacījumu $d\searrow\delta_i$. Tātad

$$\begin{aligned}S \;&=\; \sum_i\sum_{\substack{d\\ d\searrow\delta_i}}c_i\mu(d)=\sum_{\substack{(i,d)\\ d\searrow\delta_i}}c_i\mu(d)=\sum_d\sum_{\substack{i\\ d\searrow\delta_i}}c_i\mu(d)\\ &=\; \sum_d\mu(d)\sum_{\substack{i\\ d\searrow\delta_i}}c_i=\sum_d\mu(d)S_d\,. \quad ■\end{aligned}$$

5.26. Piemērs. *Pieņemsim, ka*

(i) $(\delta_1, \delta_2, \delta_3) = (1, 6, 1)$,
(ii) $(c_1, c_2, c_3) = (2, 3, 2)$,
tad

$$\begin{array}{ll} S = 2 + 2 = 4, & \\ S_1 = 2 + 3 + 2 = 7, & S_2 = 3, \\ S_3 = 3, & S_4 = 0, \\ S_5 = 0, & S_6 = 3; \end{array}$$

$$\begin{aligned} \sum_d \mu(d) S_d &= \mu(1)S_1 + \mu(2)S_2 + \mu(3)S_3 + \mu(4)S_4 + \mu(5)S_5 + \mu(6)S_6 \\ &= 7 - 3 - 3 + 0 + 0 + 3 = 4 = S\,. \end{aligned}$$

5.27. Definīcija. *Funkciju* $\varphi : \mathbb{Z}_+ \to \mathbb{Z}_+$ *sauc par Eilera funkciju, ja*

$$\varphi(a) \rightleftharpoons |\{x \in \mathbb{N} \mid x < a \ \wedge \ \mathrm{ld}(x, a) = 1\}|\,.$$

5.28. Piemērs.

$$\begin{array}{lll} \varphi(1) = 1, & \text{jo} & \mathrm{ld}(0, 1) = 1; \\ \varphi(2) = 1, & \text{jo} & \mathrm{ld}(1, 2) = 1, \\ & \text{bet} & \mathrm{ld}(0, 2) = 2; \\ \varphi(3) = 2, & \text{jo} & \mathrm{ld}(1, 3) = \mathrm{ld}(2, 3) = 1, \\ & \text{bet} & \mathrm{ld}(0, 3) = 3; \\ \varphi(4) = 2, & \text{jo} & \mathrm{ld}(1, 4) = \mathrm{ld}(3, 4) = 1, \\ & \text{bet} & \mathrm{ld}(0, 4) = 3, \mathrm{ld}(2, 4) = 2; \\ \varphi(5) = 4, & \text{jo} & \mathrm{ld}(1, 5) = \mathrm{ld}(2, 5) = \mathrm{ld}(3, 5) = \mathrm{ld}(4, 5) = 1, \\ & \text{bet} & \mathrm{ld}(0, 5) = 5; \\ \varphi(6) = 2, & \text{jo} & \mathrm{ld}(1, 6) = \mathrm{ld}(5, 6) = 1, \\ & \text{bet} & \mathrm{ld}(0, 6) = 6, \mathrm{ld}(2, 6) = 2, \mathrm{ld}(3, 6) = 3, \mathrm{ld}(4, 6) = 2\,. \end{array}$$

5.29. Teorēma. *Ja* $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ *ir skaitļa* a *kanoniskais sadalījums, tad*

$$\varphi(a) = a \prod_{i=1}^{k} (1 - \frac{1}{p_i}) = \prod_{i=1}^{k} (p_i^{\alpha_i} - p_i^{\alpha_i - 1})\,.$$

Speciālā gadījumā, ja $p \in \mathbb{P}$ *un* $\alpha \in \mathbb{Z}_+$,

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$$

un

$$\varphi(p) = p - 1\,.$$

□ Pierādījums balstās uz teorēmu 5.25. Izvēlamies
(i) $(\delta_1, \delta_2 \ldots, \delta_a) \rightleftharpoons (\mathrm{ld}(1,a), \mathrm{ld}(2,a), \ldots, \mathrm{ld}(a-1,a), \mathrm{ld}(a,a))$;
(ii) $(c_1, c_2, \ldots, c_a) = (1, 1, \ldots, 1)$,
tad

$$\begin{aligned} S &= \sum_{\substack{i \\ \delta_i = 1}} c_i = \sum_{\substack{i \in \mathbb{Z}_+ \ \wedge \ i \le a \\ \mathrm{ld}(i,a) = 1}} 1 = \varphi(a)\,, \\ S_d &= \sum_{\substack{j \\ d \smallsetminus \delta_j}} c_j = \sum_{\substack{j \in \mathbb{Z}_+ \ \wedge \ j \le a \\ d \smallsetminus \mathrm{ld}(j,a)}} 1 = \sum_{\substack{j \in \mathbb{Z}_+ \ \wedge \ j \le a \\ d \smallsetminus j \ \wedge d \smallsetminus a}} 1\,. \end{aligned}$$

Tagad izanalizēsim, kādus skaitļus dala skaitlis d.

$$\begin{aligned} j = d &\ \Rightarrow \ d \smallsetminus j \ \wedge \ c_j = 1, \\ j = 2d &\ \Rightarrow \ d \smallsetminus j \ \wedge \ c_j = 1, \\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot & \\ j = sd = a &\ \Rightarrow \ d \smallsetminus j \ \wedge \ c_j = 1\,. \end{aligned}$$

No šejienes

$$\sum_{\substack{j \in \mathbb{Z}_+ \ \wedge \ j \le a \\ d \smallsetminus j \ \wedge d \smallsetminus a}} 1 \ = \ \left\{ \begin{array}{lll} 0, & \text{ja} & d \nmid a; \\ s, & \text{ja} & d \smallsetminus a \end{array} \right\} = \left\{ \begin{array}{lll} 0, & \text{ja} & d \nmid a; \\ \dfrac{a}{d}, & \text{ja} & d \smallsetminus a\,. \end{array} \right.$$

Saskaņā ar teorēmu 5.25

$$S \ = \ \sum_d \mu(d) S_d = \sum_{d \backslash a} \mu(d) \frac{a}{d} = a \sum_{d \backslash a} \frac{\mu(d)}{d}$$

Visbeidzot atsaucoties uz sekām 5.24 secināms

$$a\sum_{d\backslash a}\frac{\mu(d)}{d}=a\begin{cases}\displaystyle\prod_{i=1}^{k}(1-\frac{1}{p_i}), & \text{ja} \quad a>1;\\ \\ 1, & \text{ja} \quad a=1\,.\end{cases}$$

Tātad, ja skaitļa a kanoniskais sadalījums ir $p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}$, tad

$$\varphi(a)=a\prod_{i=1}^{k}(1-\frac{1}{p_i})=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k}\prod_{i=1}^{k}(1-\frac{1}{p_i})=\prod_{i=1}^{k}(p_i^{\alpha_i}-p_i^{\alpha_i-1})\,.\ \blacksquare$$

5.30. Piemēri.

$$\begin{aligned}\text{(i)}\qquad 60 &= 4\cdot 15=2^2\cdot 3\cdot 5\,;\\ \varphi(60) &= 60(1-\frac{1}{2})(1-\frac{1}{3})(1-\frac{1}{5})\\ &= 60\cdot\frac{1}{2}\cdot\frac{2}{3}\cdot\frac{4}{5}=16\,;\end{aligned}$$

$$\begin{aligned}\text{(ii)}\qquad 81 &= 9\cdot 9=3^4\,;\\ \varphi(81) &= 3^4-3^3=81-27=54\,;\end{aligned}$$

$$\begin{aligned}\text{(iii)}\qquad 19 &\ \text{ir} \quad \text{pirmskaitlis, tāpēc}\\ \varphi(19) &= 19-1=18\,.\end{aligned}$$

5.31. Apgalvojums. *Eilera funkcija φ ir multiplikatīva funkcija, kas pilnībā definējama ar nosacījumu*

$$\forall p\in\mathbb{P}\ \forall\alpha\in\mathbb{Z}_+\quad \varphi(p^\alpha)=p^\alpha-p^{\alpha-1}\,.$$

□ Pierādījums kopē apgalvojuma 5.14 pierādījumu. Ņemot vērā teorēmu 5.8 mums faktiski ir jāpārbauda tikai šīs teorēmas nosacījums (iv). Saskaņā ar teorēmu 5.29

$$\varphi(\prod_{i=1}^{k}p_i^{\alpha_i})=\prod_{i=1}^{k}(p_i^{\alpha_i}-p_i^{\alpha_i-1})=\prod_{i=1}^{k}\varphi(p_i^{\alpha_i})\,.\quad\blacksquare$$

5.32. Apgalvojums.

$$\sum_{d \backslash a} \varphi(d) = a\,.$$

□ Ja $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ ir skaitļa a kanoniskais sadalījums, tad saskaņā ar teorēmu 5.11

$$\begin{aligned}
\sum_{d \backslash a} \varphi(d) &= \prod_{i+1}^{k} \sum_{j=0}^{\alpha_i} \varphi(p_i^j) = \prod_{i=1}^{k} [1 + \sum_{j=1}^{\alpha_i} (p_i^j - p_i^{j-1})] \\
&= \prod_{i=1}^{k} [1 + (p_i - 1) + (p_i^2 - p_i) + (p_i^3 - p_i^2) + \dots + (p_i^{\alpha_i} - p_i^{\alpha_i - 1})] \\
&= \prod_{i=1}^{k} p_i^{\alpha_i} = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} = a\,. \quad \blacksquare
\end{aligned}$$

5.33. Piemērs. *Ja $a = 12$, tad*

$$\begin{aligned}
\sum_{d \backslash 12} \varphi(d) &= \varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(6) + \varphi(12) \\
&= 1 + 1 + 2 + 2 + 2 + 12(1 - \frac{1}{2})(1 - \frac{1}{3}) \\
&= 8 + 12 \cdot \frac{1}{2} \cdot \frac{2}{3} = 8 + 4 = 12\,.
\end{aligned}$$

Saprotams, ja ņemam vērā tikko pierādīto apgalvojumu 5.32, tad nekādi aprēķini nav vajadzīgi.

6. Kongruences.

Kongruences, to veidotie gredzeni.

6.1. Definīcija. *Ja* $(a,b) \in \mathbb{Z}^2$, $m \in \mathbb{Z}_+$ *un*

$$\begin{aligned} a &= mt_1 + q_1\,, \\ b &= mt_2 + q_2\,, \end{aligned}$$

t_1, t_2 *ir attiecīgi skaitļu* a, m *un* b, m *nepilnie dalījumi,*

$$q_1 = q_2\,,$$

tad skaitļus a *un* b *sauc par kongruentiem pēc moduļa* m*.*

Šai situācijā lieto pierakstu

$$a \equiv b (\mathrm{mod}\ m)\,;$$

un saka: skaitlis a kongruents b pēc moduļa m. Skaitli m sauc par *moduli.*

6.2. Apgalvojums.

$$a \equiv b (\mathrm{mod}\ m) \Leftrightarrow m \diagdown a - b\,.$$

$\square \Rightarrow$ Pieņemsim, ka $a \equiv b (\mathrm{mod}\ m)$, tad

$$\begin{aligned} a &= mt_1 + q_1\,, \\ b &= mt_2 + q_2\,, \end{aligned}$$

kur t_1, t_2 ir attiecīgi skaitļu a, m un b, m nepilnie dalījumi un

$$q_1 = q_2\,.$$

No šejienes

$$\begin{aligned} a - b &= mt_1 + q_1 - mt_2 - q_2 \\ &= mt_1 + q_2 - mt_2 - q_2 \\ &= mt_1 - mt_2 = m(t_1 - t_2)\,. \end{aligned}$$

Tas arī nozīmē, ka $m \setminus a - b$, jo $t_1 - t_2 \in \mathbb{Z}$.

$\Leftarrow$ Pieņemsim, ka $m \setminus a - b$ un

$$\begin{aligned} a &= mt_1 + q_1\,, \\ b &= mt_2 + q_2\,, \end{aligned}$$

kur t_1, t_2 ir attiecīgi skaitļu a, m un b, m nepilnie dalījumi, tad

$$\begin{aligned} a - b &= mt_1 + q_1 - mt_2 - q_2 \\ &= m(t_1 - t_2) + (q_1 - q_2)\,. \end{aligned}$$

Saskaņā ar doto $m \setminus a - b$, tāpēc (apgalvojums 1.3) $m \setminus q_1 - q_2$. Tā kā t_1 un t_2 ir nepilnie dalījumi, tad

$$\begin{array}{rcl} 0 \leq & q_1 & < m \\ -m < & -q_2 & \leq 0 \\ \hline -m < & q_1 - q_2 & < m. \end{array}$$

Intervālā $]-m; m[$ ir tikai viens skaitlis, kas dalās ar m. Tas ir skaitlis 0. Tātad $q_1 - q_2 = 0$, t.i., $q_1 = q_2$. Līdz ar to pierādīts, ka $a \equiv b (\mathrm{mod}\ m)$. ■

6.3. Apgalvojums.

$$a \equiv b (\mathrm{mod}\ m) \Leftrightarrow \exists t \in \mathbb{Z}\ (a = b + mt)\,.$$

$\square \Rightarrow$ Pieņemsim, ka $a \equiv b (\mathrm{mod}\ m)$, tad

$$\begin{aligned} a &= mt_1 + q_1\,, \\ b &= mt_2 + q_2\,, \end{aligned}$$

kur t_1, t_2 ir attiecīgi skaitļu a, m un b, m nepilnie dalījumi un

$$q_1 = q_2\,.$$

No šejienes

$$\begin{aligned} a &= mt_1 + q_1 = mt_1 + q_2 \\ &= mt_1 + q_2 + mt_2 - mt_2 \\ &= mt_2 + q_2 + mt_1 - mt_2 \\ &= b + m(t_1 - t_2) \\ &= b + mt\,, \end{aligned}$$

kur $t \rightleftharpoons t_1 - t_2 \in \mathbb{Z}$.

$\Leftarrow$ Pieņemsim, ka $a = b + mt$, tad $a - b = mt$. Tas nozīmē, ka $m \setminus a - b$. Saskaņā ar tikko pierādīto apgalvojumu 6.2 $a \equiv b (\mathrm{mod}\ m)$. ■

Tikko pierādītie apgalvojumi ir ekvivalenti skaitļu a un b kongruences pēc moduļa m definīcijai. Tas nozīmē, ka katru no šiem apgalvojumiem var pieņemt arī par definīciju skaitļu a un b kongruencei pēc moduļa m.

6.4. Definīcija. *Pieņemsim, ka E ir kopā K visur definēta divvietīga attiecība. Attiecību E sauc par:*
(i) *refleksīvu, ja* $E(x,x) \sim p$;
(ii) *simetrisku, ja* $E(x,y) \sim p \Rightarrow E(y,x) \sim p$;
(iii) *transitīvu, ja* $E(x,y) \sim p \wedge E(y,z) \sim p \Rightarrow E(x,z) \sim p$.

Kopā K visur definētu attiecību E sauc par *ekvivalences tipa predikātu*, ja tā ir gan refleksīva, gan simetriska, gan transitīva.

6.5. Apgalvojums. *Skaitļu a un b kongruence pēc moduļa m kopā $\mathbb{Z}$ ir ekvivalences tipa predikāts.*

□ Attiecības $\equiv$ refleksivitāte un simetriskums nepastarpināti izriet no definīcijas. Atliek pierādīt transitivitāti. Pieņemsim, ka

$$a \equiv b (\mathrm{mod\ m}) \qquad \text{un} \qquad b \equiv c (\mathrm{mod\ m})\,,$$

tad

$$\exists t_1 \in \mathbb{Z}\ (a = b + mt_1) \qquad \text{un} \qquad \exists t_2 \in \mathbb{Z}\ (b = c + mt_2).$$

No šejienes

$$\begin{aligned} a &= b + mt_1 = c + mt_2 + mt_1 \\ &= c + m(t_1 + t_2)\,. \end{aligned}$$

Tātad $a \equiv c (\mathrm{mod\ m})$, t.i., transitivitāte ir pierādīta.

Līdz ar to parādīts, ka skaitļu a un b kongruence pēc moduļa m kopā $\mathbb{Z}$ ir ekvivalences tipa predikāts. ■

Ja reiz $\equiv$ ir ekvivalences tipa predikāts, tad ekvivalences klases

$$[a] \rightleftharpoons \{b \mid a \equiv b (\mathrm{mod}\ m)\},$$

veido kopas $\mathbb{Z}$ sadalījumu, proti,

$$\text{(i)} \quad [a] \neq [b] \Rightarrow [a] \cap [b] = \emptyset,$$
$$\text{(ii)} \quad \sum_{i=0}^{m-1} [i] = \mathbb{Z}\,.$$

Izmantojot šīs ekvivalences klases definējam faktorkopu

$$\mathbb{Z}_m \rightleftharpoons \{[0], [1], \ldots, [m-1]\}\,.$$

Ekvivalences klasi $[a]$ sauc par skaitļa *a rezidiju.*

6.6. Apgalvojums. *Ja* $\forall i \in \overline{1,n} \quad a_i \equiv b_i (\mathrm{mod}\ m)$*, tad*

$$\sum_{i=1}^{n} a_i \equiv \sum_{i=1}^{n} b_i (\mathrm{mod}\ m)\,.$$

□ Saskaņā ar apgalvojumu 6.3

$$\forall i \in \overline{1,n}\, \exists t_i \in \mathbb{Z} \quad a_i = b_i + t_i\,,$$

tāpēc

$$\sum_{i=1}^{n} a_i = \sum_{i=1}^{n} b_i + m \sum_{i=1}^{n} t_i\,.$$

Tas demonstrē, ka

$$\sum_{i=1}^{n} a_i \equiv \sum_{i=1}^{n} b_i (\mathrm{mod}\ m)\,. \blacksquare$$

Tagad atkārtosim dažus algebras jēdzienus.

6.7. Definīcija. *Visur definētu attēlojumu* $f : X^n \to X$ *sauc par algebrisku n–vietīgu operāciju.*

6.8. Definīcija. *Kortežu* $\langle A, O \rangle$ *sauc par algebru, ja*

(i) A *— netukša kopa,*

(ii) O *ir algebrisku operāciju* $\circ_i : A^{k(i)} \to A$ *kopa.*

Ja kopa O ir galīga, un nerodas pārpratumi, piemēram,

$$O = \{\circ_1, \circ_2, \ldots, \circ_n\},$$

tad $\langle A, O\rangle$ vietā lieto pierakstu

$$\langle A, \circ_1, \circ_2, \ldots, \circ_n\rangle.$$

6.9. Definīcija. *Algebru $\langle G, \circ\rangle$ sauc par* grupoīdu*, ja $\circ$ ir divvietīga algebriska operācija.*

Kā tas parasti pieņemts, arī mēs šai situācijā, teiksim: kopu G sauc par grupoīdu, ja tajā definēta divvietīga operācija $G \times G \overset{\circ}{\to} G$. Šāda izteiksmes forma ir vispārpieņemta, ja definē algebru.

6.10. Definīcija. *Grupoīdu G sauc par komutatīvu grupoīdu, ja tajā izpildās aksioma*

$$xy = yx\,.$$

Kā parasti šādās situācijās operācijas simbols un universālkvantori netiek lietoti, bez tam klusu ciešot pieņemts, ka $(x, y) \in G^2$.

6.11. Definīcija. *Grupoīdu G sauc par pusgrupu, ja tajā izpildās aksioma*

$$(xy)z = x(yz)\,.$$

Pusgrupas G elementu λ sauc par *neitrālo* elementu, ja visiem kopas G elementiem x izpildās nosacījums

$$\lambda x = x = x\lambda\,.$$

Dažkārt neitrālo elementu sauc par *vienības* elementu vai *nulli*. Pusgrupu ar neitrālo elementu sauc par *monoīdu*.

Monoīda elementu y sauc par elementa x *duālo* elementu, ja $xy = \lambda = yx$. Dažkārt duālo elementu sauc par *apgriezto* vai *pretējo* elementu.

6.12. Definīcija. *Monoīdu G sauc par grupu, ja*

$$\forall x \exists y \;\; xy = \lambda = yx\,.$$

6.13. Apgalvojums. *Algebra*

$$\langle \mathbb{Z}_m, + \rangle,$$

kur $[a] + [b] \rightleftharpoons [a + b]$, *ir komutatīva grupa.*

□ (i) Apgalvojums 6.6 parāda, ka saskaitīšana kopā $\mathbb{Z}_m$ definēta korekti, proti, ja $[a] = [a']$ un $[b] = [b']$, tad $[a + b] = [a' + b']$.

Tagad mēs pārbaudīsim visas komutatīvās grupas aksiomas.

(ii) Operācija + kopā $\mathbb{Z}_m$ ir asociatīva. Tiešām

$$\begin{aligned} [a] + ([b] + [c]) &= [a] + [b + c] = [a + (b + c)] \\ &= [(a + b) + c] = [a + b] + [c] = ([a] + [b]) + [c]\,. \end{aligned}$$

(iii) Klase $[0]$ ir neitrālais elements. Tiešām

$$[0] + [a] = [0 + a] = [a] = [a + 0] = [a] + [0]\,.$$

(iv) Elementa $[a]$ pretējais elements ir $[-a]$. Tiešām

$$[-a] + [a] = [-a + a] = [0] = [a - a] = [a + (-a)] = [a] + [-a]\,.$$

(v) Operācija + kopā $\mathbb{Z}_m$ ir komutatīva. Tiešām

$$[a] + [b] = [a + b] = [b + a] = [b] + [a]\,. \quad \blacksquare$$

6.14. Apgalvojums. *Ja* $\forall i \in \overline{1,n} \quad a_i \equiv b_i (\mathrm{mod}\ m)$, *tad*

$$\prod_{i=1}^{n} a_i \equiv \prod_{i=1}^{n} b_i (\mathrm{mod}\ m)\,.$$

□ Saskaņā ar apgalvojumu 6.3

$$\forall i \in \overline{1,n}\, \exists t_i \in \mathbb{Z} \quad a_i = b_i + t_i\,,$$

tāpēc

$$\begin{aligned} a_1 a_2 &= (b_1 + m t_1)(b_2 + m t_2) \\ &= b_1 b_2 + m(b_1 t_1 + t_1 b_2 + m t_1 t_2)\,. \end{aligned}$$

Tas demonstrē, ka $a_1 a_2 \equiv b_1 b_2 (\mathrm{mod}\ m)$.

Tālākais pierādījums induktīvs pieņemot, ka

$$\prod_{i=1}^{k} a_i \equiv \prod_{i=1}^{k} b_i (\mathrm{mod}\ m)\,.$$

$$\prod_{i=1}^{k+1} a_i = (\prod_{i=1}^{k} a_i)a_{k+1} \equiv (\prod_{i=1}^{k} b_i)b_{k+1} = \prod_{i=1}^{k+1} b_i\,. \quad \blacksquare$$

6.15. Apgalvojums. *Algebra*

$$\langle \mathbb{Z}_m, \cdot \rangle,$$

kur $[a] \cdot [b] \rightleftharpoons [ab]$*, ir komutatīvs monoīds.*

□ (i) Apgalvojums 6.14 parāda, ka reizināšana kopā $\mathbb{Z}_m$ definēta korekti, proti, ja $[a] = [a']$ un $[b] = [b']$, tad $[ab] = [a'b']$.

Tagad mēs pārbaudīsim visas komutatīvā monoīda aksiomas.

(ii) Operācija $\cdot$ kopā $\mathbb{Z}_m$ ir asociatīva. Tiešām

$$\begin{aligned} [a] \cdot ([b] \cdot [c]) &= [a] \cdot [bc] = [a(bc)] \\ &= [(ab)c] = [ab] \cdot [c] = ([a] \cdot [b]) \cdot [c]\,. \end{aligned}$$

(iii) Klase [1] ir neitrālais elements. Tiešām

$$[1] \cdot [a] = [1a] = [a] = [a1] = [a] \cdot [1]\,.$$

(iv) Operācija $\cdot$ kopā $\mathbb{Z}_m$ ir komutatīva. Tiešām

$$[a] \cdot [b] = [ab] = [ba] = [b] \cdot [a]\,. \quad \blacksquare$$

Kā tas tradicionāli pieņemts (ja neradīsies pārpratumi) mēs reizināšanas zīmi $\cdot$ izlaidīsim, proti, $[a][b] \rightleftharpoons [a] \cdot [b]$.

6.16. Definīcija. *Algebru* $\langle A, +, \cdot \rangle$ *sauc par komutatīvu gredzenu, ja*

- *tajā izpildās aksioma* $x(y + z) = xy + xz$*,*
- $\langle A, + \rangle$ *ir komutatīva grupa,*
- $\langle A, \cdot \rangle$ *ir komutatīvs monoīds.*

6.17. Sekas. *Algebra*

$$\langle \mathbb{Z}_m, +, \cdot \rangle,$$

ir komutatīvs gredzens.

□ Ņemot vērā apgalvojumus 6.13 un 6.15, vienīgais, ko vēl mums ir jāpierāda ir distributīvais likums.

$$\begin{aligned} [a]([b]+[c]) &= [a][b+c] = [a(b+c)] \\ &= [ab+ac] = [ab]+[ac] = [a][b]+[a][c]\,. \end{aligned}$$ ■

6.18. Definīcija. *Gredzena elementus a un b sauc par nulles dalītājiem, ja*
(i) $a \neq 0 \neq b$;
(ii) $ab = 0$.

6.19. Apgalvojums. *Ja a ir gredzena G nulles dalītājs, tad šim elementam neeksistē apgrieztais elements.*

□ Pieņemsim, ka a ir gredzena G nulles dalītājs, kuram eksistē apgrieztais elements, proti, $\exists a' \in G\ a'a = 1 = aa'$. Tā kā a ir nulles dalītājs, tad $\exists b \in G\ (b \neq 0\ \wedge\ ab = 0)$. No šejienes

$$b = 1b = a'ab = a'0 = 0\,.$$

Pretruna, jo $b \neq 0$. ■

6.20. Piemērs. *Gredzenā $\mathbb{Z}_6$*

$$[2][3] = [6] = [0]\,.$$

Tātad gredzenā $\mathbb{Z}_6$ gan skaitļa 2, gan skaitļa 3 rezidijs ir nulles dalītājs.

Līdz ar to gredzenā $\mathbb{Z}_m$ ne vienmēr iespējama dalīšana. Nākošais apgalvojums parāda, ka dažos gadījumos tomēr dalīšana ir iespējama.

6.21. Apgalvojums. *Ja*

$$\begin{aligned} &\text{(i)} && a \equiv b \mod m, \\ &\text{(ii)} && d \smallsetminus a\ \wedge\ d \smallsetminus b, \\ &\text{(iii)} && \mathrm{ld}(d, m) = 1, \end{aligned}$$

tad

$$\frac{a}{d} \equiv \frac{b}{d} \mod m\,.$$

□ (i) Saskaņā ar doto $a \equiv b (\mathrm{mod}\ m)$, tāpēc (apgalvojums 6.2) $m \diagdown a - b$.
(ii) Saskaņā ar doto $d \diagdown a \ \wedge \ d \diagdown b$, tāpēc

$$\exists \alpha \ (a = \alpha d) \ \wedge \ \exists \beta \ (b = \beta d).$$

No šejienes

$$a - b = \alpha d - \beta d = (\alpha - \beta) d \, .$$

Tātad $d \diagdown a - b$.
(iii) Tā kā $\mathrm{ld}(d, m) = 1$ un $m \diagdown (\alpha - \beta) d$, tad (apgalvojums 2.23) $m \diagdown \alpha - \beta$. Līdz ar to

$$\frac{a}{d} = \alpha \equiv \beta = \frac{b}{d} \mod m \, . \quad \blacksquare$$

6.22. Apgalvojums. *Ja* $a \equiv b (\mathrm{mod}\ m)$, *tad* $ak \equiv bk (\mathrm{mod}\ m)$.

□ Ja reiz $a \equiv b (\mathrm{mod}\ m)$, tad $m \diagdown a - b$. No šejienes $m \diagdown (a - b) k = ak - bk$, t.i., $ak \equiv bk (\mathrm{mod}\ m)$. ■

6.23. Apgalvojums. *Ja*

$$\begin{array}{ll} \text{(i)} & a \equiv b \mod m, \\ \text{(ii)} & d \diagdown a \ \wedge \ d \diagdown b \ \wedge \ d \diagdown m, \end{array}$$

tad

$$\frac{a}{d} \equiv \frac{b}{d} \mod \frac{m}{d} \, .$$

□ Saskaņā ar doto $d \diagdown a \ \wedge \ d \diagdown b \ \wedge \ d \diagdown m$, tāpēc

$$\exists \alpha \ (a = \alpha d) \ \wedge \ \exists \beta \ (b = \beta d) \ \wedge \ \exists \mu \ (m = \mu d),$$

turklāt vēl $a \equiv b \mod m$, tādēļ $\exists t \ a = b + mt$. No šejienes

$$\alpha d = \beta d + \mu d t \, .$$

Tā kā $d \neq 0$, tad

$$\alpha = \beta + \mu t \, ,$$

t.i.,

$$\alpha \equiv \beta \mod \mu$$

jeb

$$\frac{a}{d} \equiv \frac{b}{d} \mod \frac{m}{d} \, . \quad \blacksquare$$

6.24. Lemma. *Ja* $\forall i \in \overline{1,n}\ (a_i \setminus m)$, *tad* $\mathrm{md}(a_1, a_2, \ldots, a_n) \setminus m$.

□ Pieņemsim, ka skaitļu $a_1, a_2, \ldots, a_n$ mazākā kopīgā dalāmā $\mathrm{md}(a_1, a_2, \ldots, a_n)$ kanoniskais sadalījums ir $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$. Saskaņā ar apgalvojumu 3.22 katram i eksistē tāds j, ka $p_i^{\alpha_i} \setminus a_j$. Tā rezultātā $p_i^{\alpha_i} \setminus m$. Tas ļauj secināt, ka skaitļa m kanoniskais sadalījums satur reizinātāju $p_i^{\beta_i}$ ar pakāpi $\beta_i \geq \alpha_i$.

No šejienes

$$\mathrm{md}(a_1, a_2, \ldots, a_n) = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k} \setminus m\,. \quad \blacksquare$$

6.25. Teorēma. *Ja* $\forall i \in \overline{1,n}\ a \equiv b (\mathrm{mod}\ m_i)$, *tad*

$$a \equiv b (\mathrm{mod}\ \mathrm{md}(m_1, m_2, \ldots, m_n))\,.$$

□ Saskaņā ar doto $\forall i \in \overline{1,n}\ (m_i \setminus a - b)$, tāpēc (lemma 6.24)

$$\mathrm{md}(m_1, m_2, \ldots, m_n) \setminus a - b.$$

No šejienes $a \equiv b (\mathrm{mod}\ \mathrm{md}(m_1, m_2, \ldots, m_n))\,.$ ■

6.26. Apgalvojums. *Ja*

$$\begin{array}{ll} \text{(i)} & a \equiv b \mod m, \\ \text{(ii)} & d \setminus m, \end{array}$$

tad

$$a \equiv b \mod d\,.$$

□ Saskaņā ar doto $m \setminus a - b$. No šejienes: tā kā $d \setminus m$, tad $d \setminus a - b$, t.i, $a \equiv b (\mathrm{mod}\ d)$. ■

6.27. Apgalvojums. *Ja*

$$\begin{array}{ll} \text{(i)} & a \equiv b \mod m, \\ \text{(ii)} & d \setminus m, \\ \text{(iii)} & d \setminus b\,, \end{array}$$

tad

$$d \setminus a\,.$$

□ Saskaņā ar doto $\exists t\ a = b + mt$. No šejienes: tā kā $d \diagdown m$ un $d \diagdown b$, tad $d \diagdown a$. ■

6.28. Apgalvojums. *Ja*

$$a \equiv b \mod m\,,$$

tad

$$\mathrm{ld}(a, m) = \mathrm{ld}(b, m)\,.$$

□ Saskaņā ar doto $\exists t\ a = b + mt$. No šejienes (sekas 2.12)

$$\mathrm{ld}(a, m) = \mathrm{ld}(b, m)\,. \blacksquare$$

7. Pilnas un reducētas atlikumu sistēmas.

Pilnas un reducētas atlikumu sistēmas. Eilera un Fermā teorēma. Publiskā kriptosistēma RSA.

Vispirms atgādināsim divas definīcijas no iepriekšējās nodaļas.

$$\begin{aligned} [a] &\rightleftharpoons \{b \mid a \equiv b (\mathrm{mod}\ m)\}, \\ \mathbb{Z}_m &\rightleftharpoons \{[0], [1], \ldots, [m-1]\}. \end{aligned}$$

7.1. Definīcija. *Skaitli*

$$\min_{x \in \mathbb{N}} [a]$$

sauc par rezidija $[a]$ *mzāko nenegatīvo atlikumu.*

7.2. Definīcija. *Skaitli*

$$(\mathrm{sgn} x) \min_{x \in [a]} |x|$$

sauc par rezidija $[a]$ *mazāko atlikumu pēc absolūtās vērtības.*

Te sgn$x$ ir *signum* no x, proti, reāla argumenta funkcija

$$\mathrm{sgn} x \quad \rightleftharpoons \quad \begin{cases} -1, & \text{ja} \quad x < 0, \\ 0, & \text{ja} \quad x = 0, \\ 1, & \text{ja} \quad x > 0. \end{cases}$$

7.3. Sekas. *Ja* r *— rezidija* $[a]$ *mazākais nenegatīvais atlikums, bet* ρ *— šī paša rezidija mazākais atlikums pēc absolūtās vērtības, tad izpildās šādi nosacījumi:*

$$\begin{aligned} &\text{(i)} && r < \frac{m}{2} \Rightarrow \rho = r, \\ &\text{(ii)} && r > \frac{m}{2} \Rightarrow \rho = m - r, \\ &\text{(iii)} && r = \frac{m}{2} \Rightarrow \rho \in \{\frac{m}{2}, -\frac{m}{2}\}. \end{aligned}$$

□ Skaitlim r tuvākais negatīvais rezidija $[a]$ elements ir skaitlis $r - m$. Atliek noskaidrot, kas mazāks: r vai $|r - m|$. Tas arī ir skaitlis ρ.

(i) Ja $r < \frac{m}{2}$, tad

$$r - m < \frac{m}{2} - m = -\frac{m}{2}.$$

No šejienes $|r - m| > \frac{m}{2}$. Tātad $\rho = r$.

(ii) Ja $r > \frac{m}{2}$, tad

$$r - m > \frac{m}{2} - m = -\frac{m}{2}.$$

No šejienes $|r - m| < \frac{m}{2}$. Tātad $\rho = |r - m| = m - r$.

(iii) Ja $r = \frac{m}{2}$, tad $r - \frac{m}{2} = -\frac{m}{2}$, tāpēc $\rho \in \{\frac{m}{2}, -\frac{m}{2}\}$. ■

7.4. Definīcija. *Skaitļus $x_1, x_2, \ldots, x_m$ sauc par pilnu atlikumu sistēmu pēc moduļa m, ja elementi x_i pieder dažādiem rezidijiem.*

7.5. Sekas. *Skaitļi $0, 1, \ldots, m - 1$ sastāda pilnu atlikumu saistēmu pēc moduļa m un tie ir mazākie nenegatīvie atlikumi.*

7.6. Sekas. *Ja m ir nepāra skaitlis, tad skaitļi*

$$-\frac{m-1}{2}, \ldots, -1, 0, 1, \ldots, \frac{m-1}{2}$$

sastāda pilnu atlikumu saistēmu pēc moduļa m un tie ir mazākie atlikumi pēc absolūtās vērtības.

□ Skatīt sekas 7.3 ■

7.7. Sekas. *Ja m ir pāra skaitlis, tad gan skaitļi*

$$-\frac{m}{2} + 1, \ldots, -1, 0, 1, \ldots, \frac{m}{2},$$

gan

$$-\frac{m}{2}, \ldots, -1, 0, 1, \ldots, \frac{m}{2} - 1$$

sastāda pilnu atlikumu saistēmu pēc moduļa m un tie ir mazākie atlikumi pēc absolūtās vērtības.

□ Skatīt sekas 7.3 ■

7.8. Sekas. *Ja skaitļu $x_1, x_2, \ldots, x_m$ vidū nav pēc moduļa m kongruentu skaitļu, tad šie skaitļi sastāda pilnu atlikumu sistēmu pēc moduļa m.*

7.9. Teorēma. *Ja* $\mathrm{ld}(a, m) = 1$, $b \in \mathbb{Z}$ *un*

$$x_1, x_2, \ldots, x_m$$

ir pilna atlikumu sistēma pēc moduļa m, tad arī

$$y_1, y_2, \ldots, y_m,$$

kur

$$y_i = ax_i + b,$$

ir pilna atlikumu sistēma pēc moduļa m.

□ Pieņemsim, ka

$$y_i \equiv y_j \mod m,$$

tad

$$ax_i + b \equiv ax_j + b \mod m,$$

un tāpēc

$$ax_i \equiv ax_j \mod m.$$

Tā kā $\mathrm{ld}(a, m) = 1$, tad ņemot vērā apgalvojumu 6.21, secināms

$$x_i \equiv x_j.$$

Tas iespējams tikai tad, ja $i = j$. ■

7.10. Apgalvojums. *Ja $p \in \mathbb{P}$, tad gredzens $\langle \mathbb{Z}_p, +, \cdot \rangle$ ir lauks.*

□ Mēs jau zinām (sekas 6.17), ka $\langle \mathbb{Z}_p, +, \cdot \rangle$ ir komutatīvs gredzens. Atliek parādīt, ja $[x] \neq [0]$, tad eksistē tāds $y \in \mathbb{Z}$, ka $[x][y] = [1]$.

Ja reiz $[x] \neq [0]$, tad $\mathrm{ld}(x, p) = 1$. Ņemam skaitļus

$$0, 1, \ldots, p - 1\,.$$

Šie skaitļi sastāda pilnu atlikumu sistēmu pēc moduļa p, tāpēc (teorēma 7.9) arī skaitļi

$$x \cdot 0, x \cdot 1, x \cdot 2, \ldots, x(p - 1)$$

sastāda pilnu atlikumu sistēmu pēc moduļa p. Tas nozīmē: eksistē tāds y, ka $xy \in [1]$. ■

7.11. Definīcija. *Skaitļus*

$$x_1, x_2, \ldots, x_n$$

sauc par reducētu atlikumu sistēmu pēc moduļa m, ja:

(i) elementi x_i pieder dažādiem rezidijiem,
(ii) $\mathrm{ld}(x_i, m) = 1$,
(iii) saraksts $x_1, x_2, \ldots, x_n$ ir maksimāls pēc skaita šādā nozīmē:

ja sarakstam $x_1, x_2, \ldots, x_n$ pievieno kādu elementu x_{n+1}, tad saraksts

$$x_1, x_2, \ldots, x_n, x_{n+1}$$

neapmierina vismaz vienu no nosacījumiem (i) vai (ii).

7.12. Apgalvojums. *Katra reducēta atlikumu sistēma pēc moduļa m satur tieši $\varphi(m)$ elementus.*

□ Apgalvojums 6.28 ļauj secināt, ka elementu x_i izvēle reducētās atlikumu sistēmas sastādīšanai nav atkarīga no konkrēta elementa, bet tikai no rezidija. Tātad sastādot reducēto atlikumu sistēmu pēc moduļa m var aprobežoties ar skaitļiem

$$0, 1, \ldots, m-1.$$

Starp šiem skaitļiem ir tieši $\varphi(m)$ elementu, kas apmierina definīcijas 7.11 nosacījumu (ii). ■

7.13. Sekas. *Ja visi skaitļi*

$$x_1, x_2, \ldots, x_n$$

ir no dažādiem rezidijiem, $n = \varphi(m)$ un

$$\forall i \in \overline{1,n} \quad \mathrm{ld}(x_i, m) = 1\,,$$

tad šie skaitļi

$$x_1, x_2, \ldots, x_n$$

sastāda reducētu atlikumu sistēmu pēc moduļa m.

□ Pierādījums nepastarpināti seko no definīcijas 7.11 un apgalvojuma 7.12. ■

7.14. Sekas. *Kopas*

$$\mathbb{Z}_m^* \rightleftharpoons \{\, [a] \mid \mathrm{ld}(a,m) = 1 \ \wedge\ [a] \in \mathbb{Z}_m\}$$

elementu skaits $|\mathbb{Z}_m^*| = \varphi(m)$.

□ Ja $x_1, x_2, \ldots, x_n$ ir reducēta atlikumu sistēma pēc moduļa m, tad

$$\{[x_1], [x_2], \ldots, [x_n]\} \subseteq \mathbb{Z}_m^*\,.$$

Tā kā saraksts $x_1, x_2, \ldots, x_n$ pēc skaita ir maksimāls, tad

$$\{[x_1], [x_2], \ldots, [x_n]\} = \mathbb{Z}_m^*\,.$$

Saskaņā ar apgalvojumu 7.12 $n = \varphi(m)$. ■

7.15. Teorēma. *Ja* $\mathrm{ld}(a,m) = 1$ *un*

$$x_1, x_2, \ldots, x_n$$

ir reducēta atlikumu sistēma pēc moduļa m*, tad arī*

$$y_1, y_2, \ldots, y_m,$$

kur

$$y_i = ax_i,$$

ir reducēta atlikumu sistēma pēc moduļa m.

□ Tā kā skaitļu

$$y_1, y_2, \ldots, y_m$$

ir tik pat daudz, cik skaitļu

$$x_1, x_2, \ldots, x_n,$$

tad (sekas 7.13) atliek pārbaudīt tikai definīcijas 7.11 nosacījumus (i) un (ii).

(i) Tā kā $\mathrm{ld}(a,m) = 1$, tad ņemot vērā teorēmu 7.9, secināms: visi elementi y_i pieder dažādiem rezidijiem.

(ii) Tagad mēs ņemam vērā ne tikai nosacījumu $\mathrm{ld}(a,m) = 1$, bet arī nosacījumu $\forall i \in \overline{1,n}\quad \mathrm{ld}(x_i,m) = 1$. No šejienes atsaucoties uz apgalvojumu 2.22, secināms

$$\mathrm{ld}(y_i,m) = \mathrm{ld}(ax_i,m) = \mathrm{ld}(x_i,m) = 1\,. \quad ■$$

7.16. Teorēma (Eilers). *Ja* $m > 1$ *un* $\operatorname{ld}(a, m) = 1$, *tad*

$$a^{\varphi(m)} \equiv 1 \mod m\,.$$

□ Pieņemsim, ka

$$x_1, x_2, \ldots, x_n,$$

ir reducēta atlikumu sistēma pēc moduļa m, tad

$$ax_1, ax_2, \ldots, ax_n,$$

arī ir reducēta atlikumu sistēma pēc moduļa m. Tā rezultātā

$$\forall i\ \exists! j \quad x_i \equiv ax_j \mod m\,.$$

Tā kā $\langle \mathbb{Z}_m, \cdot \rangle$, kur $[a] \cdot [b] \rightleftharpoons [ab]$, ir komutatīvs monoīds, tad

$$a^n \prod_{i=1}^{n} x_j = \prod_{j=1}^{n} ax_j \equiv \prod_{i=1}^{n} x_i \mod m\,.$$

Tagad ņemam vērā, ka $\forall i \in \overline{1, n} \quad \operatorname{ld}(x_i, m) = 1$, tāpēc (apgalvojums 6.21)

$$a^n \equiv 1 \mod m\,.$$

Visbeidzot atzīmēsim, ka $n = \varphi(m)$. ■

7.17. Teorēma (Fermā). *Ja* $p \in \mathbb{P}$ *un* $p \nmid a \in \mathbb{Z}_+$, *tad*

$$a^{p-1} \equiv 1 \mod p\,.$$

□ Eilera teorēmā izvēlamies $m \rightleftharpoons p$. Visbeidzot ņemam vērā, ka $\varphi(p) = p - 1$ un $\operatorname{ld}(a, p) = 1$, jo $p \nmid a$. Tā rezultātā

$$a^{p-1} = a^{\varphi(p)} \equiv 1 \mod p\,. \quad ■$$

7.18. Sekas.

$$\forall p \in \mathbb{P}\ \forall a \in \mathbb{Z}_+ \quad a^p \equiv a \mod p\,.$$

□ (i) Ja $p \nmid a$, tad saskaņā ar Fermā teorēmu

$$a^{p-1} \equiv 1 \mod p\,.$$

Tagad ņemam vērā, ka $\langle \mathbb{Z}_m, \cdot \rangle$ ir monoīds, tāpēc

$$a^p = a \cdot a^{p-1} \equiv a \cdot 1 = a \mod p\,.$$

(ii) Ja turpretī $p \nmid a$, tad

$$\exists b \in \mathbb{Z}\ (a = bp),$$

tāpēc $a \in [p] = [0]$. Bez tam

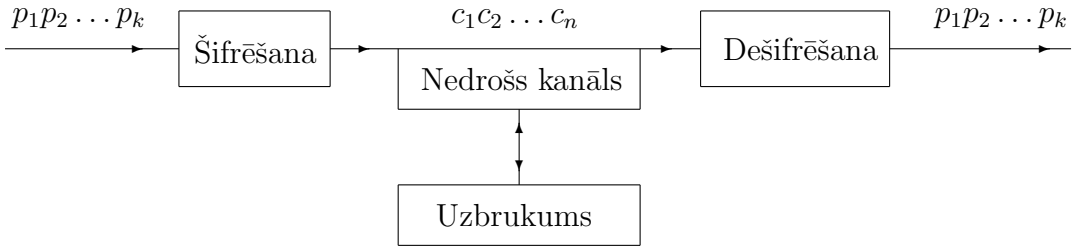
$$a^p = (bp)^p = (b^p p^{p-1})p \in [p] = [0]\,.$$

Tātad $a^p \equiv 0 \equiv a (\mathrm{mod} p)$. ■

Publiskā kriptosistēma RSA. Kriptogrāfija analizē legālās un nelegālās pasaules mijiedarbību informācijas jomā. Mēs apskatīsim tikai vienu šīs nozares aspektu, proti, Alise vēlas nosūtīt konfidenciālu ziņojumu Bucim. Ziņojuma sūtīšanai viņa izmantos e-pastu, taču Oskars ir profesionāls hakeris, un viņš šo ziņojumu var pārtvert. Ko darīt Alisei un Bucim, ja viņi nevēlas, lai Oskars varētu lasīt vēstules?

Alise ar Buci vienojas par vēstuļu šifrēšanu. Tagad Oskars gan spēs pārtvert sūtījumus, taču negūs nekādu labumu no tā (ilustrāciju skatīt 1. zīm.). Turpmākajam mēs vienosimies simbolu virkni $p_1 p_1 \ldots p_k$ saukt par *pamattekstu*, $c_1 c_2 \ldots c_n$ — par *kriptotekstu*.

Brīdinājums. Mēs analizējam tikai situāciju, kad Oskars var lasīt ziņojumus, taču nevar aizvietot īstos ziņojumus ar viltus ziņojumiem.



1. zīm. Konfidenciālas informācijas sūtīšana pa nedrošu kanālu.

RSA kriptosistēmas apraksts. Bucis izvēlas divus lielus pirmskaitļus

$$p \qquad \text{un} \qquad q.$$

Viņš aprēķina

$$m \rightharpoonup pq \qquad \text{un} \qquad \varphi(m).$$

Dotajā gadījumā $\varphi(m) = (p-1)(q-1)$. Visbeidzot Bucis izvēlas pietiekoši lielu skaitli

$$e \qquad \text{tā, lai} \qquad \mathrm{ld}(\varphi(m), e) = 1.$$

Tā kā komunikācijas kanāls ir nedrošs, tad Alisei Bucis nosūta tikai skaitļus m un e. Šie skaitļi ir publiskā atslēga. Skaitļi p, q un $\varphi(m)$ ir jāpatur slepenībā.

Brīdinājums. Bucim ir jābūt pārliecinātam, ka Alise tiešām saņems šos skaitļus. Pretējā gadījumā jāmeklē drošāks veids, kā šos skaitļus nosūtīt Alisei. Piemēram, šos skaitļus var publicēt kādā avīzē, teiksim, kā sludinājumu vai reklāmas pielikumu.

Šī kriptosistēma paredz, ka pamatteksts ir veseli nenegatīvi skaitļi. Tātad Alisei nāksies latviešu valodā uzrakstīto tekstu

$$t_1 t_2 \dots t_s$$

pārveidot par pamattekstu

$$p_1 p_2 \dots p_k \,.$$

Arī par šo procedūru Bucis ar Alisi var vienoties publiskajā telpā, teiksim, Bucis nosūta Alisei šādu tabulu

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	a	ā	b	c	č	d	e	ē	f	g	ğ	h	i	ī	j	k
1	A	Ā	B	C	Č	D	E	Ē	F	G	Ģ	H	I	Ī	J	K
2	ķ	l	ļ	m	n	ņ	o	p	r	s	š	t	u	ū	v	z
3	Ķ	L	Ļ	M	N	Ņ	O	P	R	S	Š	T	U	Ū	V	Z
4	ž	q	x	y	w	†	@	#	$	%	&	{	}	_	*	§
5	Ž	Q	X	Y	W	!	,	.	?	:	;	”	’	‘	∼	\
6	0	1	2	3	4	5	6	7	8	9	—	/	+	=	-	
7	|	<	>	(	)	[	]	“	–	×	∂	$\int$	$\sum$	$\prod$	•	·

ar paskaidrojumu:

— Katru tabulas elementu a_{ij} jāaizstāj ar 7 simbolu virkni

$$i_1 i_2 i_3 j_1 j_2 j_3 j_4$$

saskaņā ar doto tabulu:

i	$\mapsto$	$i_1 i_2 i_3$	j	$\mapsto$	$j_1 j_2 j_3 j_4$	j	$\mapsto$	$j_1 j_2 j_3 j_4$
0	$\mapsto$	000	0	$\mapsto$	0000	8	$\mapsto$	1000
1	$\mapsto$	001	1	$\mapsto$	0001	9	$\mapsto$	1001
2	$\mapsto$	010	2	$\mapsto$	0010	A	$\mapsto$	1010
3	$\mapsto$	011	3	$\mapsto$	0011	B	$\mapsto$	1011
4	$\mapsto$	100	4	$\mapsto$	0100	C	$\mapsto$	1100
5	$\mapsto$	101	5	$\mapsto$	0101	D	$\mapsto$	1101
6	$\mapsto$	110	6	$\mapsto$	0110	E	$\mapsto$	1110
7	$\mapsto$	111	7	$\mapsto$	0111	F	$\mapsto$	1111

Tā burts Ū jāaizstāj ar virkni 0111101. Vizuāli tas izskatās šādi:

$$\bar{\text{U}} \quad \mapsto \quad \text{3D} \quad \mapsto \quad 011\,1101\,.$$

3D norāda, ka Ū atrodas tabulas rindiņā ar pazīmi 3 un stabiņā ar pazīmi D. Pēc šādas vienošanās Alise tekstu

$$t_1 t_2 \ldots t_s$$

pārveidos par nuļļu un vieninieku virkni

$$t'_1 t'_2 \ldots t'_\sigma\,. \tag{15}$$

Uzskatāmības labad sāksim ar tekstu

Buci, es tevi mīlu! Rīt tiksimies Dzegužkalnā. Čau!

Lai nepjuktu, Alise vispirms sastāda tabulu

B	0010010	v	0101110	t	0100110		1100110	ā	0000001
u	0101100	i	0001100		1101111	D	0010101	.	1010111
c	0000011		1101111	t	0100110	z	0101111		1100110
i	0001100	m	0100011	i	0001100	e	0000110	Č	0010100
,	1010110	ī	0001101	k	0001111	g	0001001	a	0000000
	1101111	l	0100001	s	0101001	u	0101100	u	0101100
e	0000110	u	0101100	i	0001100	ž	1000000	!	1010101
s	0101001	!	1010101	m	0100011	k	0001111		
	1101111		1101111	i	0001100	a	0000000		
t	0101011	R	0111000	e	0000110	l	0100001		
e	0000110	ī	0001101	s	0101001	n	0100100		

Konkrētajā gadījumā Alise iegūst virkni

0010010 0101100 0000011 0001100 1010110 1101111 0000110 0101001
1101111 0101011 0000110 0101110 0001100 1101111 0100011 0001101
0100001 0101100 1010101 1101111 0111000 0001101 0100110 1101111
0100110 0001100 0001111 0101001 0001100 0100011 0001100 0000110
0101001 1100110 0010101 0101111 0000110 0001001 0101100 1000000
0001111 0000000 0100001 0100100 0000001 1010111 1100110 0010100
0000000 0101100 1010101

Tas vēl nav pamatteksts.

Lai iegūtu pamattekstu Alise aprēķina $\nu \rightleftharpoons \lfloor \log_2 m \rfloor$ un virkni (15) sadala blokos

$$\begin{aligned} p'_1 &\rightleftharpoons t'_1 t'_2 \dots t'_\nu, \\ p'_2 &\rightleftharpoons t'_{\nu+1} t'_{\nu+2} \dots t'_{2\nu}, \\ &\cdots \\ p'_k &\rightleftharpoons t'_{(k-1)\nu+1} t'_{(k-1)\nu+2} \dots t'_{k\nu}\,; \end{aligned}$$

te $k = \lceil \frac{\sigma}{\nu} \rceil$.

Saprotams rodas jautājums:

— Ko darīt, ja $k < \frac{\sigma}{\nu}$?

Lai nerastos problēmas Alise ar Buci vienojas, ka simbolu † lietos tikai vienā nozīmē, proti, šis simbols norādīs ziņojuma beigas. Tas nozīmē, ka Alise, lai nosūtītu vēstuli ar tekstu

Buci, es tevi mīlu! Rīt tiksimies Dzegužkalnā. Čau!

sūtīs ziņojumu

Buci, es tevi mīlu! Rīt tiksimies Dzegužkalnā. Čau!†

Un Alise iegūst virkni

0010010 0101100 0000011 0001100 1010110 1101111 0000110 0101001
1101111 0101011 0000110 0101110 0001100 1101111 0100011 0001101
0100001 0101100 1010101 1101111 0111000 0001101 0100110 1101111
0100110 0001100 0001111 0101001 0001100 0100011 0001100 0000110
0101001 1100110 0010101 0101111 0000110 0001001 0101100 1000000
0001111 0000000 0100001 0100100 0000001 1010111 1100110 0010100
0000000 0101100 1010101 1000101

Dotajā piemērā $t'_3 = 1$ un $\sigma = 364$.

Taču problēma paliek:

— Ko darīt, ja $k < \frac{\sigma}{\nu}$?

Tagad Alise var rīkoties vienkārši. Viņa virkni (15) patvaļīgi papildina ar nullēm un vieniniekiem līdz iegūst virkni

$$t'_1 t'_2 \dots t'_\sigma t'_{\sigma+1} \dots t'_{k\nu} .$$

Visbeidzot Alise katram blokam p'_i atmet sākotnējās nulles un iegūst skaitli p_i, kas reprezentēts 2–ku sistēmā. Tā, ja

$$p'_i = 00 \dots 01 t'_\tau t'_{\tau+1} \dots t'_{k\nu} ,$$

tad

$$p_i \rightleftharpoons 1 t'_\tau t'_{\tau+1} \dots t'_{k\nu} .$$

Saprotams, ja $p'_i = 00 \dots 0$, tad $p_i \rightleftharpoons 0$. Šādi iegūtie skaitļi

$$p_1 p_2 \dots p_k$$

ir kriptosistēmas RSA pamatteksts.

Tālāk Alise izmanto Buča atsūtīto skaitli e un aprēķina $c_i \in \overline{0, m-1}$ tā, lai

$$c_i \equiv p_i^e \mod m .$$

Savukārt Bucis saņēmis kriptotekstu

$$c_1 c_2 \dots c_k$$

(mūsu gadījumā kriptoteksta garums sakrīt ar pamatteksta garumu) veic šādus aprēķinus. Vispirms Bucis atrisina kongruenci

$$ex \equiv 1 \mod m$$

un izvēlas atrisinājumu $d \in \overline{0, \varphi(m)-1}$. Pēc tam Bucis izmanto skaitli d un aprēķina $d_i \in \overline{0, m-1}$ tā, lai

$$d_i \equiv c_i^d \mod m .$$

7.19. Teorēma. $d_i = p_i$.

□ Tā kā

$$ed \equiv 1 \mod \varphi(m)\,,$$

tad eksistē tāds vesels skaitlis $\varkappa$, ka $ed = 1 + \varkappa\varphi(m)$.

(i) Ja $\mathrm{ld}(p_i, m) = 1$, tad saskaņā ar Eilera teorēmu

$$\begin{aligned} d_i &\equiv c_i^d \mod m \\ &\equiv (p_i^e)^d \mod m \\ &\equiv p_i^{1 + \varkappa\varphi(m)} \mod m \\ &\equiv p_i \left(p_i^{\varphi(m)}\right)^{\varkappa} \mod m \\ &\equiv p_i 1^{\varkappa} \equiv p_i \mod m\,. \end{aligned}$$

(ii) Ja $\mathrm{ld}(p_i, m) \neq 1$, tad $p \diagdown p_i$ vai arī $q \diagdown p_i$, jo $m = pq$.

a) Ja $p_i = 0$, tad

$$d_i \equiv c_i^d \equiv (p_i^e)^d = (0^e)^d = 0 = p_i \mod m.$$

Turpmākajā pierādījumā uzskatīsim, ka $p_i \neq 0$.

b) Ja $p \diagdown p_i$, tad $q \nmid p_i$, jo $0 < p_i < m = pq$, tāpēc $\exists a \exists \alpha\ p_i = ap^{\alpha}$ un $\mathrm{ld}(a, m) = 1$. No šejienes

$$\begin{aligned} d_i &\equiv c_i^d \equiv (p_i^e)^d \mod m \\ &\equiv p_i^{1 + \varkappa\varphi(m)} \mod m \\ &= (ap^{\alpha})^{1 + \varkappa\varphi(m)} \\ &\equiv a\left(p^{1 + \varkappa\varphi(m)}\right)^{\alpha} \mod m\,. \end{aligned}$$

Tā kā $p \equiv p (\mathrm{mod}\, p)$, tad

$$p^{1 + \varkappa\varphi(m)} \equiv p \mod p\,.$$

Savukārt $\varphi(m) = (p-1)(q-1)$ un $q \nmid p$, tāpēc saskaņā ar Fermā teorēmu

$$\begin{aligned} p^{1+\varkappa\varphi(m)} &= p\, p^{\varkappa(p-1)(q-1)} \\ &= p\, \left(p^{q-1}\right)^{\varkappa(p-1)} \\ &\equiv p\, 1^{\varkappa(p-1)} \equiv p \mod q\,. \end{aligned}$$

Tagad, atsaucoties uz teorēmu 6.25, secināms:

$$p^{1+\varkappa\varphi(m)} \equiv p \mod pq\,.$$

Līdz ar to

$$\begin{aligned} d_i &\equiv a\left(p^{1+\varkappa\varphi(m)}\right)^{\alpha} \mod m \\ &\equiv ap^{\alpha} = p_i \mod m\,. \end{aligned}$$

c) Ja $q \smallsetminus p_i$, tad pierādījums faktiski kopē punktā b) apskatīto pierādījumu, tāpēc šī gadījuma pierādījumu atstājam kā vingrinājumu lasītājam.

Tātad $d_i \equiv p_i (\mathrm{mod}\ m)$, turklāt vēl $0 \leq d_i < m$ un $0 \leq p_i < m$. Tas nozīmē, ka $d_i = p_i$. ■

Mēs tikko parādījām, kā Bucis var iegūt pamattekstu. Tālākais jau ir tikai pacietība, lai Bucis varētu izlasīt, ko īsti atsūtījusi Alise.

Mūsdienās kriptosistēma RSA tiek uzskatīta par nedrošu, ja $m < 2^{40}$, taču, ja $p > 2^{600}$ un $q > 2^{1000}$, tad RSA tiek uzskatīta par drošu. Atzīmēsim, ka vēl joprojām nav pārliecinošu teorētisku argumentu, kas dotu atbildi uz jautājumu:

— Vai kriptosistēma RSA ir droša?

8. Kongruenču vienādojumi.

Kongruenču vienādojumi. Pirmās pakāpes kondruenču vienādojumu atrisināšana un ķēžu daļas.

Vienošanās. *Turpmāk ar terminu kongruence mēs sapratīsim izteiksmi*

$$p(x) \equiv 0 \mod m\,,$$

kur

$$p(x) = \sum_{k=0}^{n} a_k x^k\,.$$

8.1. Definīcija. *Ja $m \nmid a_n$, tad skaitli n sauc par polinoma $p(x)$ kongruences pakāpi.*

8.2. Definīcija. *Atrisināt kongruenci nozīmē atrast visas tās $a \in \mathbb{Z}$ vērtības, kas apmierina doto kongruenci, proti skaitļi $p(a)$ un 0 ir kongruenti pēc moduļa m.*

Šai situācijā mēs teiksim arī, ka vērtībai a ir spēkā kongruence $p(x) \equiv 0(\mathrm{mod}\ m)$. Divas kongruences, kuras apmierina vienas un tās pašas mainīgā x vērtības, sauc par *ekvivalentām kongruencēm.*

8.3. Apgalvojums. *Ja kongruenci $p(x) \equiv 0(\mathrm{mod}\ m)$ apmierina vērtība $x_0 \in \mathbb{Z}$, tad šo kongruenci apmierina jebkurš $a \in [x_0]$.*

□ Algebra

$$\langle \mathbb{Z}_m, +, \cdot \rangle,$$

ir komutatīvs gredzens (sekas 6.17). No šejienes, ja

$$x_0 \equiv a \mod m,$$

tad

$$\begin{aligned}
&\text{(i)} && x_0^k \equiv a^k \mod m,\\
&\text{(ii)} && a_k x_0^k \equiv a_k a^k \mod m,\\
&\text{(iii)} && \sum_{k=0}^{n} a_k x_0^k \equiv \sum_{k=0}^{n} a_k a^k \mod m\,. \qquad \blacksquare
\end{aligned}$$

Šis apgalvojums motivē sekojošo definīciju.

8.4. Definīcija. *Ja kongruenci* $p(x) \equiv 0(\mathrm{mod}\ m)$ *apmierina vērtība* x_0*, tad visu rezidiju* $[x_0]$ *sauc par kongruences* $p(x) \equiv 0(\mathrm{mod}\ m)$ *vienu atrisinājumu.*

8.5. Sekas. *Kongruences* $p(x) \equiv 0(\mathrm{mod}\ m)$ *atrisinājumu skaits ir galīgs. Atrisinājumi ir kopas* $\mathbb{Z}_m$ *apakškopa.*

Parasti uzskata, ka kongruence ir atrisināta, ja uzskaitīti visu atrisinājumu $[a]$ pārstāvji a. Vienmēr cenšas sniegt rezidija $[a]$ mazāko nenegatīvo atlikumu, vai arī — rezidija $[a]$ mazāko atlikumu pēc absolūtās vērtības.

8.6. Piemērs.

$$x^5 + x + 1 \equiv 0 \mod 7\,.$$

Vienkāršākā kongruences risināšanas metode ir visu rezidiju pārbaude. Šī piemēra ietvaros pieņemsim, ka $p(x) \leftharpoondown x^5 + x + 1$, tad

(i) $p(0) = 1 \not\equiv 0 \mod 7$.

(ii) $p(1) = 3 \not\equiv 0 \mod 7$.

(iii) $p(2) = 32 + 2 + 1 = 35 \equiv 0 \mod 7$.

(iv) $p(3) = 81 \cdot 3 + 3 + 1 = 243 + 4 = 247$.

$$\begin{array}{r|l} 247 & 7 \\ \hline 37 & 35 \\ \hline 2 & \end{array}$$

Tātad $247 \equiv 2 \not\equiv 0 \mod 7$.

(v) $p(4) = 4^5 + 4 + 1 = 1024 + 5 = 1029$.

$$\begin{array}{r|l} 1029 & 7 \\ \hline 3 & 147 \\ \hline 42 & \\ \hline 0 & \end{array}$$

Tātad $1029 \equiv 0 \mod 7$.

(vi) $p(5) = 5^5 + 5 + 1 = 125 \cdot 25 + 6$

$$\begin{array}{cccc} & 1 & 2 & 5 \\ & & 2 & 5 \\ \hline & 6 & 2 & 5 \\ 2 & 5 & 0 & \\ \hline 3 & 1 & 2 & 5 \end{array}$$

No šejienes $p(5) = 3125 + 6 = 3131.$

$$\begin{array}{cccccccc} 3 & \underline{1} & \underline{3} & 1 & : & 7 & = & 447 \\ & 3 & 3 & & & & & \\ \hline & & 5 & 1 & & & & \\ & & \underline{5} & \underline{1} & & & & \\ & & & 2 & & & & \end{array}$$

Tātad $3131 \equiv 2 \not\equiv 0 \mod 7.$

(vii) $p(6) = 6^5 + 6 + 1 = 36 \cdot 6 \cdot 36 + 7 = 216 \cdot 36 + 7$

$$\begin{array}{cccc} & 3 & 1 & 6 \\ & & 3 & 6 \\ \hline 1 & 2 & 9 & 6 \\ 6 & 4 & 8 & \\ \hline 7 & 7 & 7 & 6 \end{array}$$

No šejienes $p(6) = 7776 + 7 = 7783.$

$$\begin{array}{cccccccc} \underline{7} & \underline{7} & \underline{8} & \underline{3} & : & 7 & = & 1111 \\ & & 1 & 3 & & & & \\ \hline & & & 6 & & & & \end{array}$$

Tātad $7783 \equiv 6 \not\equiv 0 \mod 7.$

Atbilde: $x \equiv 2 \mod 7$ vai $x \equiv 4 \mod 7.$

Kā redzams, šāda kongruences risināšanas metode, kaut arī potenciālā nozīmē ir realizējama, prasa nogurdinoši lielus aprēķinus. Saprotams ar kalkulatoru to visu veikt ir ērtāk, ar datoru — vēl ērtāk (ja jums ir gatava programma, kas veic visas nepieciešamās darbības). Taču lieliem moduļiem m šāda kongruences atrisināšans metode ir neracionāla. Tas pamato nepieciešamību pēc teorijas izstrādes, vismaz vienkāršākajās situācijās.

8.7. Definīcija. *Kongruenci*

$$a_1 x + a_0 \equiv 0 \mod m$$

sauc par pirmās pakāpes kongruenci jeb lineāru kongruenci.

8.8. Apgalvojums. *Pirmās pakāpes kongruence*

$$a_1x + a_0 \equiv 0 \mod m$$

ekvivalenti pārveidojama izskatā

$$ax \equiv b \mod m.$$

□
$$\begin{aligned} a_1x + a_0 &\equiv 0 \mod m, \\ a_1x &\equiv -a_0 \mod m. \end{aligned}$$

Šajā situācijā $a = a_1$ un $b = -a_0$. ■

8.9. Apgalvojums. *Ja* $\mathrm{ld}(a, m) = 1$*, tad pirmās pakāpes kongruencei*

$$ax \equiv b \mod m$$

eksistē tieši viens atrisinājums.

□ Ja $x_1, x_2, \ldots, x_m$ ir pilna atlikumu sistēma pēc moduļa m, tad (teorēma 7.9) arī

$$ax_1, ax_2, \ldots, ax_m$$

ir pillna atlikumu sistēma pēc moduļa m. Tātad tieši vienai vērtībai x_i ir spēkā kongruence

$$ax_i \equiv b \mod m\,. \quad ■$$

8.10. Apgalvojums. *Ja* $\mathrm{ld}(a, m) = d$ *un* $d \nmid b$*, tad kongruencei*

$$ax \equiv b \mod m$$

atrisinājums neeksistē.

□ Pievērsīsimies apgalvojumam 6.27: ja

$$\begin{aligned} &\text{(i)} && a \equiv \beta \mod m, \\ &\text{(ii)} && d \setminus m, \\ &\text{(iii)} && d \setminus \alpha\,, \end{aligned}$$

tad

$$d \setminus \beta\,.$$

Saskaņā ar doto $\mathrm{ld}(a, m) = d$. Tas nozīmē, ka $d \setminus a$ un $d \setminus m$. Līdz ar to, ja x_0 ir kongruences

$$ax \equiv b \mod m$$

atrisinājums, tad $d \setminus b$. ■

8.11. Apgalvojums. *Ja* $\mathrm{ld}(a,m)=d$ *un* $d \setminus b$, *tad kongruencei*

$$ax \equiv b \mod m$$

eksistē tieši d *atrisinājumi.*

□ Pievērsīsimies apgalvojumam 6.23: ja

$$\begin{array}{ll} \text{(i)} & \alpha \equiv \beta \mod m, \\ \text{(ii)} & d \setminus \alpha \ \wedge \ d \setminus \beta \ \wedge \ d \setminus m, \end{array}$$

tad

$$\frac{\alpha}{d} \equiv \frac{\beta}{d} \mod \frac{m}{d}\,.$$

Tātad, ja x_0 ir kongruences

$$ax \equiv b \mod m$$

atrisinājums, tad x_0 ir arī kongruences

$$a_1 x \equiv b_1 \mod m_1$$

atrisinājums, kur

$$a_1 = \frac{a}{d}, \quad b_1 = \frac{b}{d}, \quad m_1 = \frac{m}{d}.$$

Saskaņā ar apgalvojumu 8.9 šai kongruencei eksistē tieši viens atrisinājums $[x_1] \in \mathbb{Z}_{m_1}$. Tas ļauj secināt, ka

$$x_1, x_1 + m_1, x_1 + 2m_1, \ldots, x_1 + (d-1)m_1$$

ir kongruences

$$ax \equiv b \mod m$$

atrisinājumi. Šie atrisinājumi pēc moduļa m nav kongruenti. Līdz ar to kongruencei

$$ax \equiv b \mod m$$

kopā $\mathbb{Z}_m$ ir d dažādi atrisinājumi. ■

8.12. Teorēma. *Ja* $\mathrm{ld}(a,m)=d$ *un* $d\nmid b$, *tad kongruencei*

$$ax \equiv b \mod m$$

atrisinājums neeksistē. Ja turpretī $d \mid b$, *tad kongruencei*

$$ax \equiv b \mod m$$

eksistē tieši d *atrisinājumi.*

□ Pierādījums nepastarpināti seko no apgalvojumiem 8.10 un 8.11 ■

8.13. Lemma. *Ja* $[a] \in \mathbb{Z}_m^*$ *un* $[b] \in \mathbb{Z}_m^*$, *tad* $[a][b] \in \mathbb{Z}_m^*$.

□ Atgādināsim kopas $\mathbb{Z}_m^*$ definīciju.

$$\mathbb{Z}_m^* \rightleftharpoons \{\, [a] \mid \mathrm{ld}(a,m)=1 \ \wedge\ [a] \in \mathbb{Z}_m \}\,.$$

Saskaņā ar doto

$$\mathrm{ld}(a,m) = 1 = \mathrm{ld}(b,m)\,.$$

No šejienes (apgalvojums 2.24) $\mathrm{ld}(ab,m)=1$. Tātad $[ab] \in \mathbb{Z}_m^*$. Tā kā $[a][b]=[ab]$, tad $[a][b] \in \mathbb{Z}_m^*$. ■

8.14. Lemma. *Elements* $[a] \in \mathbb{Z}_m^*$ *tad un tikai tad, ja*

$$\exists x_0 \in \mathbb{Z} \quad [ax_0] = [1]\,.$$

□ $\Rightarrow$ Pieņemsim, ka $[a] \in \mathbb{Z}_m^*$, tad $\mathrm{ld}(a,m)=1$, tāpēc (apgalvojums 8.9) kongruencei

$$ax \equiv 1 \mod m \tag{16}$$

eksistē atrisinājums. No šejienes, ja x_0 ir šīs kongruences atrisinājums, tad $[ax_0]=[1]$.

$\Leftarrow$ Pieņemsim, ka $[ax_0]=[1]$. Tas nozīmē, ka x_0 ir kongruences (16) atrisinājums. Ja šai kongruencei eksistē atrisnājums, tad (teorēma 8.12)

$$\mathrm{ld}(a,m) \mid 1\,.$$

Tas iespējams tikai tad, ja $\mathrm{ld}(a,m)=1$. Tātad $[a] \in \mathbb{Z}_m^*$. ■

8.15. Teorēma. *Algebra $\langle \mathbb{Z}_m^*, \cdot \rangle$ ir komutatīva grupa.*

□ (i) Lemma 8.13 parāda, ka reizināšanas operācija neizved ārpus kopas $\mathbb{Z}_m^*$. Tā kā $\mathbb{Z}_m^* \subseteq \mathbb{Z}_m$, tad skaidrs, ka reiznāšana kopā $\mathbb{Z}_m^*$ definēta korekti, jo kopā $\mathbb{Z}_m$ tā ir definēta korekti (apgalvojums 6.14).

Tagad mēs pārbaudīsim visas komutatīvās grupas aksiomas.

(ii) Tā kā $\mathbb{Z}_m^* \subseteq \mathbb{Z}_m$ un reizināšas operācija $\cdot$ kopā $\mathbb{Z}_m$ ir gan asociatīva, gan komutatīva, tad arī kopā $\mathbb{Z}_m^*$ tā ir gan asociatīva, gan komutatīva. Tas nozīmē, ka algebra $\langle \mathbb{Z}_m^*, \cdot \rangle$ ir komutatīva pusgrupa.

(iii) Ņemam vērā, ka $\mathrm{ld}(1, m) = 1$, tāpēc $[1] \in \mathbb{Z}_m^*$. Klase $[1]$ ir monoīda $\langle \mathbb{Z}_m, \cdot \rangle$ neitrālais elements. Tā kā $\mathbb{Z}_m^* \subseteq \mathbb{Z}_m$, tad $[1]$ ir arī pusgrupas $\langle \mathbb{Z}_m^*, \cdot \rangle$ neitrālais elements.

(iv) Lemma 8.14 ļauj secināt, ka katram kopas $\mathbb{Z}_m^*$ elementam $[a]$ eksistē apgrieztais elements $[a]^{-1} \in \mathbb{Z}_m^*$, proti, eksistē tāds elements $[a]^{-1} \in \mathbb{Z}_m^*$, ka $[a][a]^{-1} = [1]$. ■

8.16. Definīcija. *Komutatīvo grupu $\langle \mathbb{Z}_m^*, \cdot \rangle$ sauc par gredzena $\langle \mathbb{Z}_m, +, \cdot \rangle$ multiplikatīvo grupu.*

Parasti gan šo terminoloģiju vienkāršo un saka:

— $\mathbb{Z}_m^*$ ir gredzena $\mathbb{Z}_m$ multiplikatīvā grupa.

Lineāras kongruences risināšanas metode. Pieņemsim, ka dota kongruence

$$ax \equiv b \mod m\,.$$

(i) Vispirms aprēķinam $d \rightleftharpoons \mathrm{ld}(a, m)$. Pārbaudam, vai $d \diagdown b$?

(a) Ja $d \nmid b$, tad kongruencei

$$ax \equiv b \mod m$$

atrisinājums neeksistē.

(b) Ja $d \diagdown b$, tad aprēķinam

$$\alpha \rightleftharpoons \frac{a}{d}\,, \qquad \beta \rightleftharpoons \frac{b}{m}\,, \qquad \mu \rightleftharpoons \frac{m}{d}\,.$$

(ii) Risinam kongruenci

$$\alpha x \equiv \beta \mod \mu\,.$$

(a) Skaitli $\frac{\mu}{\alpha}$ izvirzam ķēžu daļā, proti, atrodam skaitļa $\frac{\mu}{\alpha}$ ķēžu daļu

$$[q_1; q_2, \ldots, q_n] .$$

(b) Saskaņā ar rekurences formulām

$$P_0 = 1, \quad P_1 = q_1, \quad P_{i+1} = q_{i+1}P_i + P_{i-1}$$

nosakām P_{n-1}.

(c) Aprēķinam skaitli $(-1)^{n-1}P_{n-1}b$. Nosakam skaitļu $(-1)^{n-1}P_{n-1}b$ un μ dalījuma atlikumu, proti, atrodam tādu $x_0 \in \overline{0, \mu - 1}$, ka

$$x_0 \equiv (-1)^{n-1}P_{n-1}b \mod \mu.$$

(d) Skaitļi

$$x_0, x_0 + \mu, x_1 + 2\mu, \ldots, x_1 + (d-1)\mu$$

ir kongruences

$$ax \equiv b \mod m \tag{17}$$

atrisinājums.

Tagad parādīsim, ka šī metode tiešām dod kongruences (17) atrisinājumu.

8.17. Apgalvojums. *Ja*

$$\mathrm{ld}(a, m) = 1 \qquad \text{un} \qquad [q_1; q_2, \ldots, q_n]$$

ir skaitļa $\frac{m}{a}$ *izvirzījums ķēžu daļā, tad rezidijs*

$$[(-1)^{n-1}P_{n-1}b]$$

ir kongruences (17) *atrisinājums.*

□ (i) Mēs esam parādījuši (apgalvojums 4.11), ka

$$P_nQ_{n-1} - Q_nP_{n-1} = (-1)^n. \tag{18}$$

Tas nozīmē, ka $\mathrm{ld}(P_n, Q_n)$=1.

Tiešām, pieņemsim, ka $d \diagdown P_n$ un $d \diagdown Q_n$, tad

$$d \diagdown P_nQ_{n-1} - Q_nP_{n-1} = (-1)^n.$$

Tas ir iespējams tikai vienā gadījumā, proti, ja $d = 1$.

(ii) Mēs esam parādījuši (lemma 4.9, apgalvojums 4.4), ka

$$\frac{P_n}{Q_n} = \delta_n = \frac{a}{m}\,.$$

(iii) Tā kā

$$\mathrm{ld}(a, m) = 1 = \mathrm{ld}(P_n, Q_n)$$

un

$$\frac{m}{a} = \frac{P_n}{Q_n}\,,$$

tad $m = P_n$ un $a = Q_n$. No šejienes, ņemot vērā (18),

$$mQ_{n-1} - aP_{n-1} = (-1)^n$$

jeb

$$\begin{aligned} -aP_{n-1} &\equiv (-1)^n \mod m\,, \\ (-a)P_{n-1}(-1)^n b &\equiv (-1)^n(-1)^n b \mod m\,, \\ a((-1)^{n-1}P_{n-1}b) &\equiv b \mod m\,. \end{aligned}$$

Tas ļauj secināt, ka rezidijs $[(-1)^{n-1}P_{n-1}b]$ ir kongruences

$$ax \equiv b \mod m$$

vienīgais (apgalvojums 8.9) atrisinājums. ■

8.18. Piemēri. (i) *Atrisināt kongruenci*

$$41x \equiv 9 \mod 52\,! \tag{19}$$

Risinājums. Izmantojam Eiklīda algoritmu:

$$\begin{array}{rrl} & 52 & :41 = 1 \\ - & 41 & \\ \hline & 41 & :11 = 3 \\ - & 33 & \\ \hline & 11 & :8 = 1 \\ - & 8 & \\ \hline & 8 & :3 = 2 \\ - & 6 & \\ \hline & 3 & :2 = 1 \\ - & 2 & \\ \hline & 2 & :1 = 2 \end{array}$$

Tā kā pēdējais nenulles atlikums ir 1, tad $\mathrm{ld}(41, 52) = 1$. Tas nozīmē, ka kongruencei (19) eksistē tieši viens atrisinājums.

Tagad varam sastādīt tabulu:

i	0	1	2	3	4	5	6
q_i		1	3	1	2	1	2
P_i	1	1	4	5	14	19	52

Tā rezultātā ķēžu daļa $[1; 3, 1, 2, 1, 2]$ reprezentē skaitli $\dfrac{52}{41}$,

$$n = 6 \qquad \text{un} \qquad P_{n-1} = 19\,.$$

Līdz ar to kongruences (19) atrisinājums

$$\begin{aligned} x &\equiv (-1)^{n-1} P_{n-1} b \mod m \\ &= (-1)^5 19 \cdot 9 = -171 \equiv -15 \mod 52\,. \end{aligned}$$

Atbilde: $x \equiv -15 \mod 52$.

(ii) Atrisināt kongruenci

$$627x \equiv 173 \mod 722\,! \tag{20}$$

Risinājums. Izmantojam Eiklīda algoritmu:

$$\begin{array}{rrrl} & & 722 & : 627 = 1 \\ & - & 627 & \\ \hline & & 627 & : 95 = 6 \\ & - & 570 & \\ \hline & & 95 & : 57 = 1 \\ & - & 57 & \\ \hline & & 57 & : 38 = 1 \\ - & & 38 & \\ \hline & & 38 & :19 = 2 \end{array}$$

Pēdējais nenulles atlikums ir 19, tāpēc $\mathrm{ld}(627, 722) = 19$. Tā kā 19 nedala 173, tad tas nozīmē, ka kongruencei (20) atrisinājums neeksistē.

(iii) Atrisināt kongruenci

$$432x \equiv 84 \mod 678\,! \tag{21}$$

Risinājums. Izmantojam Eiklīda algoritmu:

$$
\begin{array}{rrrl}
 & & 678 & :432 = 1 \\
 & - & 432 & \\
\hline
 & 432 & :246 & = 1 \\
 - & 246 & & \\
\hline
 & 246 & :186 & = 1 \\
 - & 186 & & \\
\hline
 & 186 & :60 & = 3 \\
 - & 180 & & \\
\hline
 & 60 & :6 & = 10
\end{array}
$$

Pēdējais nenulles atlikums ir 6, tāpēc $\mathrm{ld}(432, 678) = 6$. Tā kā 6 dala 84, tad tas nozīmē, ka kongruencei (21) ir 6 atrisinājumi. Tagad risinām kongruenci

$$\frac{432}{6}x \equiv \frac{84}{6} \mod \frac{678}{6},$$

t.i.,

$$72x \equiv 14 \mod 113. \tag{22}$$

Tagad sastādam tabulu

i	0	1	2	3	4	5
q_i		1	1	1	3	10
P_i	1	1	2	3	11	113

Tā rezultātā ķēžu daļa $[1; 1, 1, 3, 10]$ reprezentē skaitli $\frac{113}{72}$,

$$n = 5 \qquad \text{un} \qquad P_{n-1} = 11.$$

Līdz ar to kongruences (22) atrisinājums

$$\begin{aligned} x &\equiv (-1)^{n-1} P_{n-1} b \mod m \\ &= (-1)^4 11 \cdot 14 = -154 \equiv 41 \mod 113. \end{aligned}$$

Atbilde:

$x_1 \equiv -298 \mod 678$, $x_2 \equiv -185 \mod 678$, $x_3 \equiv -72 \mod 678$,
$x_4 \equiv 41 \mod 678$, $x_5 \equiv 154 \mod 678$, $x_6 \equiv 267 \mod 678$.

9. Kongruenču sistēmas.

Kongruenču sistēmas un ķīnišu teorēma par atlikumiem. Vilsona teorēma.

9.1. Teorēma. *Kongruenču sistēmas*

$$i \begin{cases} 1 \\ \\ k \end{cases} x \equiv b_i \mod m_i\,, \tag{23}$$

kur

$$\forall i\ \forall j\ (i \neq j \Rightarrow \mathrm{ld}(m_i, m_j) = 1)\,,$$

atrisinājums

$$x_0 \equiv \sum_{i=1}^{k} a_i a_i' b_i \mod m\,;$$

te

$$m = m_1 m_2 \ldots m_k\,, \qquad a_i = m : m_i$$

un a_i' *ir kongruences*

$$a_i y_i \equiv 1 \mod m_i \tag{24}$$

atrisinājums.

□ (i) Ievērojam, ka

$$\forall i\ \mathrm{ld}(a_i, m_i) = 1\,,$$

tāpēc katram i kongruencei (25) eksistē tieši viens atrisinājums.

(ii) Tagad ņemam vērā, ka $m \equiv 0 (\mathrm{mod}\ m_i)$ un $\forall j \neq i\ a_j \equiv 0 (\mathrm{mod}\ m_i)$, tāpēc

$$\begin{aligned} x_0 &\equiv a_i a_i' b_i \mod m_i \\ &\equiv b_i \mod m_i\,. \end{aligned}$$

Līdz ar to x_0 ir sistēmas (23) viens no atrisinājumiem.

(iii) Pieņemsim, ka x_1 ir sistēmas (23) atrisinājums, tad katram i

$$\begin{aligned} x_1 &\equiv b_i \mod m_i \\ &\equiv x_0 \mod m_i\,. \end{aligned}$$

No šejienes (teorēma 6.25)

$$x_1 \equiv x_0 \mod \mathrm{md}(\mathrm{m}_1, \mathrm{m}_2, \ldots, \mathrm{m}_\mathrm{k}) .$$

Mūsu gadījumā

$$\mathrm{md}(m_1, m_2, \ldots, m_k) = m_1 m_2 \ldots m_k = m.$$

Līdz ar to kopā $\mathbb{Z}_m$ elementi $[x_0]$ un $[x_1]$ sakrīt, t.i., $[x_0] = [x_1]$. ■

9.2. Teorēma (Ķīniešu teorēma par atlikumiem). *Ja*

$$m_1, m_2, \ldots, m_k$$

ir savstarpēji pirmskaitļi un

$$0 \leq b_1 < m_1, 0 \leq b_2 < m_2, \ldots, 0 \leq b_k < m_k$$

veseli nenegatīvi skaitļi, tad eksistē tāds vesels skaitlis a, ko dalot ar m_i atlikumā iegūst b_i.

□ Iepriekšējās teorēmas pārformulējums. ■

9.3. Apgalvojums. *Ja $m_1, m_2, \ldots, m_k$ ir savstarpēji pirmskaitļi un B_i ir kopa, kas sastāda pilnu atlikumu sistēmu pēc moduļa m_i, tad*

$$B \leftrightharpoons \{x \,|\, x = \sum_{i=1}^{k} a_i a_i' b_i \ \wedge \ b_i \in B_i\}$$

ir pilna atlikumu sistēma pēc moduļa $m = m_1 m_2 \ldots m_k$; te $a_i = m : m_i$ un a_i' ir kongruences

$$a_i y_i \equiv 1 \mod m_i$$

atrisinājums.

□ Pieņemsim, ka $x \equiv x' (\mathrm{mod}\ m)$ un $x, x' \in B$, tad

$$x = \sum_{i=1}^{k} a_i a_i' b_i, \qquad x' = \sum_{i=1}^{k} a_i a_i' b_i'$$

un $b_i, b_i' \in B_i$. No šejienes (teorēma 9.1)

$$\forall i \ (x \equiv b_i \mod m_i \ \wedge \ x' \equiv b_i' \mod m_i).$$

Saskaņā ar pieņēmumu $x \equiv x' (\mathrm{mod}\ m)$, tāpēc (apgalvojums 6.26)

$$x \equiv x' \mod m_i.$$

Tas nozīmē, ka

$$\forall i \ (b_i \equiv b_i' \mod m_i).$$

Tā kā $b_i, b_i' \in B_i$ un kopa B_i nesatur pēc moduļa m_i kongruentus elementus, tad secināms, ka $b_i = b_i'$.

Līdz ar to, ja $(b_1, b_2, \ldots, b_k) \neq (b_1', b_2', \ldots, b_k')$, tad $x \not\equiv x' \mod m$. Šāda tipa kortežu skaits ir m, tāpēc kopas B elementi sastāda pilnu atlikumu sistēmu pēc moduļa m. ■

9.4. Piemērs. *Atrisināt kongruenču sistēmu*

$$\begin{cases} x \equiv 3 \mod 4, \\ x \equiv 6 \mod 15, \\ x \equiv 9 \mod 49. \end{cases}$$

Atrisinājums. $m = 4 \cdot 15 \cdot 49 = 2940.$

$$\begin{aligned} a_1 = m : m_1 &= 2940 : 4 = 735, \\ a_2 = m : m_2 &= 2940 : 15 = 196, \\ a_3 = m : m_3 &= 2940 : 49 = 60. \end{aligned}$$

Tagad mums jārisina kongruences

$$\begin{aligned} a_1 y_1 &\equiv 1 \mod m_1, \\ a_2 y_2 &\equiv 1 \mod m_2, \\ a_3 y_3 &\equiv 1 \mod m_3. \end{aligned}$$

t.i.,

$$\begin{aligned} 735 y_1 &\equiv 1 \mod 4, \\ 196 y_2 &\equiv 1 \mod 15, \\ 60 y_3 &\equiv 1 \mod 49; \end{aligned}$$

$$\begin{aligned} 3y_1 &\equiv 1 \mod 4, \\ y_2 &\equiv 1 \mod 15, \\ 11y_3 &\equiv 1 \mod 49. \end{aligned}$$

Pirmo kongruenci vienkāršāk atrisināt ar pilnu pārlasi: $y_1 = -1$.

Trešās kongruences risināšanai izmantosim Eiklīda algoritmu:

$$\begin{array}{rrl} & 49 & : 11 = 4 \\ - & 44 & \\ \hline & 11 & : 5 = 2 \\ - & 10 & \\ \hline & 5 & : 1 = 5 \end{array}$$

Pēdējais nenulles atlikums ir 1, tāpēc $\mathrm{ld}(49, 11) = 1$. Tas nozīmē, ka kongruencei

$$11y_3 \equiv 1 \mod 49 \tag{25}$$

eksistē tieši viens atrisinājums.

Tagad sastādam tabulu

i	0	1	2	3
q_i		4	2	5
P_i	1	4	9	49

Tā rezultātā ķēžu daļa $[4; 2, 5]$ reprezentē skaitli $\dfrac{49}{11}$,

$$n = 3 \qquad \text{un} \qquad P_{n-1} = 9\,.$$

Līdz ar to kongruences (25) atrisinājums

$$\begin{aligned} y_3 &\equiv (-1)^{n-1} P_{n-1} b \mod 49 \\ &= (-1)^2 9 \cdot 1 \equiv 9 \mod 49\,. \end{aligned}$$

Tagad iegūstam kongruenču sistēmas atrisinājumu

$$\begin{aligned} x &\equiv a_1 a_1' b_1 + a_2 a_2' b_2 + a_3 a_3' b_3 \mod m \\ &\equiv 735 \cdot (-1) \cdot 3 + 196 \cdot 1 \cdot 6 + 60 \cdot 9 \cdot 9 \mod 2940 \\ &\equiv -2205 + 1176 + 4860 \mod 2940 \\ &\equiv 3831 \equiv 891 \mod 2940\,. \end{aligned}$$

Atbilde: $x \equiv 891 \mod 2940$.

9.5. Apgalvojums. *Kongruence*

$$p(x) \rightharpoonup \sum_{k=0}^{n} a_k x^k \equiv 0 \mod p\,, \qquad p \in \mathbb{P}\,, \tag{26}$$

ekvivalenta kongruencei, kuras pakāpe nav lielāka par $p-1$.

□ Mēs ņemam vērā, ka

$$p(x) = (x^p - x)q(x) + r(x),$$

kur polinoma $r(x)$ pakāpe ir mazāka par p. Savukārt (sekas 7.18)

$$x^p - x \equiv 0 \mod p\,. \quad \blacksquare$$

9.6. Lemma. *Jebkuram skaitļu kortežam* $(x_1, x_2, \ldots, x_n)$ *eksistē tādi koeficienti* $b_0, b_1, \ldots, b_n$, *ka*

$$\sum_{k=0}^{n} a_k x^k = b_0 + \sum_{k=1}^{n} b_k \prod_{i=1}^{k} (x - x_i).$$

Turklāt, ja $a_0, a_1, \ldots, a_n$ *un* $x_1, x_2, \ldots, x_n$ *ir veseli skaitļi, tad* $b_0, b_1, \ldots, b_n$ *arī ir veseli skaitļi.*

□ Ņemam vērā, ka pēc iekavu atvēršanas iegūstam izteiksmi

$$\prod_{i=1}^{k} (x - x_i) = x^k + \sum_{i=0}^{k-1} c_{ki} x^i\,.$$

Tātad, jābūt spēkā vienādībai

$$\begin{aligned} \sum_{k=0}^{n} a_k x^k &= b_0 + \sum_{k=1}^{n} b_k \prod_{i=1}^{k} (x - x_i) \\ &= b_0 + \sum_{k=1}^{n} b_k \prod_{i=1}^{k} (x^k + \sum_{i=0}^{k-1} c_{ki} x^i). \end{aligned}$$

No šejienes

$$\begin{aligned}
a_n &= b_n, \\
a_{n-1} &= b_n c_{nn-1} + b_{n-1}\,, \\
&\ldots\ldots\ldots\ldots\ldots \\
a_{n-i} &= b_n c_{nn-i} + b_{n-1}c_{n-1n-i} + \ldots + b_{n-i+1}c_{n-i+1n-i} + b_{n-i}\,, \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
a_0 &= b_n c_{n0} + b_{n-1}c_{n-10} + \ldots + b_1 c_{10} + b_0\,.
\end{aligned}$$

Tas nozīmē, ka

$$\forall i \in \overline{1,n} \quad b_{n-i} = a_{n-i} - \sum_{j=0}^{i-1} b_{n-j}c_{n-jn-i}. \quad \blacksquare$$

9.7. Apgalvojums. *Ja kongruencei* (26) *eksistē vairāk par* n *atrisinājumiem, tad* p *dala visus koeficientus* a_k.

□ Pieņemsim, ka

$$x_0, x_1, \ldots, x_n$$

ir kongruences (26) atrisinājumi, tad (lemma 9.6)

$$0 \equiv p(x_1) = \sum_{k=0}^{n} a_k x_1^k = b_0 + \sum_{k=1}^{n} b_k \prod_{i=1}^{k}(x_1 - x_i) = b_0 \mod p\,.$$

Līdzīgi

$$\begin{aligned}
0 \equiv p(x_2) = \sum_{k=0}^{n} a_k x_2^k &= b_0 + \sum_{k=1}^{n} b_k \prod_{i=1}^{k}(x_2 - x_i) \\
&= b_0 + b_1(x_2 - x_1) \\
&\equiv b_1(x_2 - x_1) \mod p\,.
\end{aligned}$$

Mēs varam pieņemt, ka $\forall i \;\; 0 \le x_i < p$ (apgalvojums 8.3), tad

$$\forall i \forall j \;\; |x_i - x_j| < p\,.$$

Tā kā $p \nmid b_1(x_2 - x_1)$ un $p \nmid (x_2 - x_1)$, tad $p \nmid b_1$.

Tālākie spriedumi induktīvi:

$$0 \equiv p(x_{s+1}) = \sum_{k=0}^{n} a_k x_{s+1}^k = b_0 + \sum_{k=1}^{n} b_k \prod_{i=1}^{k} (x_{s+1} - x_i)$$
$$\equiv b_s \prod_{i=1}^{s} (x_{s+1} - x_i) \mod p\,.$$

Tā kā

$$p \nmid b_s \prod_{i=1}^{s} (x_{s+1} - x_i)$$

un

$$\forall i \in \overline{1,s} \quad p \nmid (x_{s+1} - x_i), \qquad \text{tad} \qquad p \nmid b_s\,.$$

Visbeidzot

$$0 \equiv p(x_0) = \sum_{k=0}^{n} a_k x_0^k = b_0 + \sum_{k=1}^{n} b_k \prod_{i=1}^{k} (x_0 - x_i)$$
$$\equiv b_n \prod_{i=1}^{n} (x_0 - x_i) \mod p\,.$$

Tā kā

$$p \nmid b_n \prod_{i=1}^{n} (x_0 - x_i)$$

un

$$\forall i \in \overline{1,n} \quad p \nmid (x_0 - x_i),$$

tad $p \nmid b_n$. ■

9.8. Teorēma (Vilsons). *Ja* $p \in \mathbb{P}$, *tad*

$$(p-1)! + 1 \equiv 0 \mod p.$$

□ Ja $p = 2$, tad

$$(p-1)! + 1 = 1 + 1 \equiv 0 \mod 2\,.$$

Ja $p > 2$, tad apskatam kongruenci

$$\prod_{a=1}^{p-1}(x-a) - (x^{p-1}-1) \equiv 0 \mod p\,.$$

Šīs kongruences pakāpe nepārsniedz skaitli $p-2$, un tai ir $p-1$ atrisinājums, proti, ja $p \nmid a$, tad saskaņā ar Fermā mazo teorēmu (teorēma 7.17)

$$a^{p-1} \equiv 1 \mod p\,.$$

Līdz ar to, ņemot vērā apgalvojumu 9.7, secināms: skaitlis p dala brīvo locekli, t.i., $p \setminus (p-1)! + 1$. Iegūts

$$(p-1)! + 1 \equiv 0 \mod p\,. \quad \blacksquare$$