ARVUTEOORIA

Kevad 2017

Loengukonspekt

Lektor: Aleksei Lissitsin

Konspekt: Valdis Laan ja Lauri Tart

Sisukord

1. Jaguvus. Aritmeetika põhiteoreem

1.1. Täisarvud

Käesoleva kursuse põhiliseks uurimisobjektiks on täisarvud ja nende omadused. Teatavasti on täisarvude hulk $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ järjestatud kommutatiivne ring, s.t., et sellel hulgal on defineeritud liitmistehe $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, korrutamistehe $\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ ning järjestusseos $\leqslant \subseteq \mathbb{Z} \times \mathbb{Z}$ nii, et

Z1. $(\forall a, b, c \in \mathbb{Z})((a + b) + c = a + (b + c))$ (liitmine on assotsiatiivne);

Z2. $(\exists 0 \in \mathbb{Z})(\forall a \in \mathbb{Z})(a + 0 = a = 0 + a)$ (leidub *nullelement*);

Z3. $(\forall a \in \mathbb{Z})(\exists(-a) \in \mathbb{Z})(a + (-a) = 0 = (-a) + a)$ (igal täisarvul leidub *vastandarv*);

Z4. $(\forall a, b \in \mathbb{Z})(a + b = b + a)$ (liitmine on kommutatiivne);

Z5. $(\forall a, b, c \in \mathbb{Z})((ab)c = a(bc))$ (korrutamine on assotsiatiivne);

Z6. $(\exists 1 \in \mathbb{Z})(\forall a \in \mathbb{Z})(a1 = a = 1a)$ (leidub *ühikelement*);

Z7. $(\forall a, b \in \mathbb{Z})(ab = ba)$ (korrutamine on kommutatiivne);

Z8. $(\forall a, b, c \in \mathbb{Z})(a(b + c) = ab + ac)$ (liitmine on korrutamise suhtes distributiivne);

Z9. $(\forall a, b, c \in \mathbb{Z})(a \leqslant b \Longrightarrow a + c \leqslant b + c)$ (järjestus on kooskõlas liitmisega);

Z10. $(\forall a, b, c \in \mathbb{Z})(a \leqslant b \wedge c \geqslant 0 \Longrightarrow ac \leqslant bc)$ (järjestus on kooskõlas mittenegatiivsete arvudega korrutamisega).

Lisaks nendele on täisarvude ringil veel teisigi omadusi. Näiteks

Z11. $(\forall a, b, c \in \mathbb{Z})(ac = bc \wedge c \neq 0 \Longrightarrow a = b)$;

Z12. $(\forall a, b \in \mathbb{Z})(ab = 0 \Longleftrightarrow a = 0 \vee b = 0)$;

Z13. $(\forall a, b \in \mathbb{Z})(ab = 1 \Longleftrightarrow a = b = 1 \wedge a = b = -1)$;

s.t. täisarvude ring on taandamisega, nullitegureita ning ainsad pööratavad elemendid on -1 ja 1.

Täisarvude hulk sisaldab naturaalarvude hulka $\mathbb{N} = \{1, 2, 3, \ldots\}$. Võib vaadelda kujutust $|\ | : \mathbb{Z} \to \mathbb{N} \cup \{0\}$, mis on defineeritud võrdusega

$$|a| = \begin{cases} a, & \text{kui } a \geqslant 0, \\ -a, & \text{kui } a < 0. \end{cases}$$

Mittenegatiivset täisarvu $|a|$ nimetatakse täisarvu a *absoluutväärtuseks*. Absoluutväärtuse tähtsamad omadused on järgmised:

ABS1. $(\forall a \in \mathbb{Z})(|a| = 0 \Longleftrightarrow a = 0)$;

ABS2. $(\forall a, b \in \mathbb{Z})(|ab| = |a||b|)$ (absoluutväärtus on kooskõlas korrutamisega);

ABS3. $(\forall a, b \in \mathbb{Z})(|a + b| \leqslant |a| + |b|)$ (kolmnurga võrratus).

1.2. Täisarvude jaguvus. Suurim ühistegur ja vähim ühiskordne

Väga oluline koht arvuteoorias on jaguvuse mõistel.

Definitsioon 1.1. Öeldakse, et täisarv a *jagab* täisarvu b (ja tähistatakse $a \mid b$), kui leidub selline täisarv c, et $ac = b$.

Fakti, et $a \mid b$, võib tähistada ja väljendada väga mitmel moel. Kõik järgnevad kirjutised ja väited tähendavad täisarvude a ja b korral ühte ja sedasama:

$$\begin{aligned} a \mid b \quad &\equiv \quad \text{arv } a \text{ jagab arvu } b \equiv b \vdots a \equiv \text{arv } b \text{ jagub arvuga } a \\ &\equiv \quad a \text{ on } b \text{ jagaja} \equiv a \text{ on } b \text{ tegur} \equiv b \text{ on } a \text{ kordne} \equiv (\exists c \in \mathbb{Z})(ac = b). \end{aligned}$$

Definitsioonist järelduvad lihtsalt mitmed jaguvusseose omadused.

Lause 1.2. *Täisarvude jaguvusseosel on järgmised omadused: iga $a, b, c \in \mathbb{Z}$ korral*

1. *kui* $a \mid b$ *ja* $b \mid c$, *siis* $a \mid c$ *(transitiivsus);*

2. *kui* $a \mid b$ *ja* $a \mid c$, *siis* $a \mid (b \pm c)$*;*

3. *kui* $a \mid b$, *siis* $ac \mid bc$ *(järelikult ka* $a \mid bc$*);*

4. $a \mid 1$ *parajasti siis, kui* $a \in \{-1, 1\}$.

Tõestus. Neljas väide järeldub omadusest Z13. Esimene väide kehtib sellepärast, et mistahes $a, b, c \in \mathbb{Z}$ korral

$$a|b \wedge b|c \underset{\text{Def. 1.1}}{\Longrightarrow} (\exists d, e \in \mathbb{Z})(ad = b \wedge be = c) \Longrightarrow c = be = (ad)e \underset{\text{Z5}}{=} a(de) \wedge de \in \mathbb{Z} \underset{\text{Def. 1.1}}{\Longrightarrow} a|c.$$

Ülejäänud kaks väidet saab tõestada analoogiliselt. □

Jaguvusseose abil saab defineerida täisarvude suurima ühisteguri ja vähima ühiskordse.

Definitsioon 1.3. Mittenegatiivset täisarvu d nimetatakse täisarvude a ja b *suurimaks ühisteguriks* (tähistatakse $d = \text{SÜT}(a, b)$ ehk lühidalt $d = (a, b)$, antud kursuses eelistame viimast tähistust), kui

(i) $d \mid a$ ja $d \mid b$;

(ii) iga täisarvu c korral, kui $c \mid a$ ja $c \mid b$, siis $c \mid d$.

Kui a ja b suurim ühistegur on 1, siis öeldakse tihti, et a ja b on *ühistegurita.*

Definitsioon 1.4. Mittenegatiivset täisarvu m nimetatakse täisarvude a ja b *vähimaks ühiskordseks* (tähistatakse $m = \text{VÜK}(a, b)$ ehk $m = [a, b]$), kui

(i) $a \mid m$ ja $b \mid m$;

(ii) iga täisarvu c korral, kui $a \mid c$ ja $b \mid c$, siis $m \mid c$.

Eelmises kahes definitsioonis nõuame mittenegatiivsust selleks, et nii suurim ühistegur kui ka vähim ühiskordne oleks üheselt määratud (tõepoolest, näiteks ka $-(a, b)$ rahuldab definitsiooni 1.3 tingimusi (i) ja (ii)). Mõnikord (nagu ka konspekti eelmiste aastate versioonides) mittenegatiivsust ei nõuta ja siis suurim ühistegur ja vähim üheskordne on defineeritud märgi täpsuseni.

Märkus. Üldiselt siin on tegemist vähima ülemise (*supremum*) ja suurima alumise (*infimum*) rajadega eeljärjestatud hulgal. Meenutame, et hulk X on *osaliselt järjestatud* relatsiooniga $\prec \subset X \times X$, kui $\prec$ on

(R) refleksiivne, s.t. $\forall x \in X \; x \prec x$,

(A) antisümeetriline, s.t. $\forall x, y \in X \; (x \prec y \wedge y \prec x) \implies x = y$,

(T) transitiivne, s.t. $\forall x, y, z \in X \; (x \prec y \wedge y \prec z) \implies x \prec z$.

Siis kahe elementide $a, b \in X$ vähim ülemine raja $\sup(a, b)$ on selline element $m \in X$, et

(i) $a \prec m$ ja $b \prec m$;

(ii) iga elemendi $c \in X$ korral, kui $a \prec c$ ja $b \prec c$, siis $m \prec c$.

Lihtne on näha, et osaliselt järjestatud hulgas kahe elemendi vähim ülemine raja (kui ta leidub) on üheselt määratud (on vaja lihtsalt kasutada antisümmeetrilisust). Osaliselt järjestatud hulga näited on hulk $\mathbb{Z}$ tavalise arvude järjestusega $\leq$ ja hulk $\mathbb{N}$ jaguvusseosega $|$.

Oletame nüüd, et relatsioon $\prec$ ei ole osaline järjestus vaid on ainult *eeljärjestus*, s.t. ta on refleksiivne ja transitiivne, kuid ei pruugi olla antisümmeetriline. Siis definitsiooni kohaselt võivad leiduda elemendid $x, y \in X$ nii, et $x \prec y$ ja $y \prec x$, kuid $x \neq y$. Eeljärjestatud hulga näide on hulk $\mathbb{Z}$ jaguvusseosega $|$.

Osutub aga, et iga eeljärjestatud hulk loomulikul viisil tekitab teatud osaliselt järjestatud hulka. Täpsemalt, kui defineerida relatsiooni $\sim$ nii, et

$$\forall x, y \in X \; x \sim y \overset{\text{def}}{\iff} x \prec y \wedge y \prec x,$$

siis $\sim$ osutub ekvivalentsusseoseks ning X esitub paarikaupa lõikumatute ekvivalentsklasside (nagu $\tilde{x} = \{y \in X : y \sim x\}$, $x \in X$) ühendina. Faktorhulgal ehk ekvivalentsklasside hulgal $X/_\sim = \{\tilde{x} : x \in X\}$ võib nüüd defineerida osalise järjestuse

$$\tilde{x} \prec \tilde{y} \overset{\text{def}}{\iff} \forall \xi \in \tilde{x} \; \forall \eta \in \tilde{y} \quad \xi \prec \eta \iff \exists \xi \in \tilde{x} \; \exists \eta \in \tilde{y} \quad \xi \prec \eta \iff x \prec y.$$

Nüüd on selge, et eeljärjestatud hulgas rahuldab element m tingimusi (i) ja (ii) üleval parajasti siis, kui $m \in \sup(\tilde{a}, \tilde{b})$, kusjuures ekvivalentsklass $\sup(\tilde{a}, \tilde{b})$ (kui ta eksisteerib) võib sisaldada ka mitu elementi.

Meie juhul (hulk $\mathbb{Z}$ eeljärjestatud jaguvusseosega $|$) täisarvule $a \in \mathbb{Z}$ vastav ekvivalentsklass on (reeglina kaheelemendiline) hulk $\{-a, a\}$. Kahe täisarvu vähima ühiskordse $[a, b]$ võiks seega samuti vaadata klassina $\sup(\tilde{a}, \tilde{b})$, mis võrdub $\{-m, m\}$ mingi $m \in \mathbb{Z}$ korral, aga see võib olla natuke tülikas. Seetõttu konspektis nimetame vähimaks ühiskordseks selle klassi mittenegatiivset elementi ehk $|m|$. Sama asi käib ka suurima ühisteguri kohta.

Suurimal ühisteguril on järgmised omadused.

Lause 1.5. *Iga $a, b, c \in \mathbb{Z}$ korral*

1. $(a, b) = |a|$ *parajasti siis, kui* $a \mid b$;
2. $(a, 0) = |a|$;
3. $(a, b) = 0$ *parajasti siis, kui* $a = 0$ *ja* $b = 0$;
4. $((a, b), c) = (a, (b, c))$.

Tõestus. Tõestame näitena esimese väite. Kui $a = (a, b)$, siis definitsiooni 1.3 tingimuse (i) põhjal $a \mid b$. Kui $-a = (a, b)$, siis samamoodi $a \mid (-a) \mid b$. Vastupidi, eeldame, et $a \mid b$. Kuna lisaks sellele $a \mid a$, siis a on a ja b ühine tegur. Oletame, et ka $c \mid a$ ja $c \mid b$. Siis ilmselt $c \mid a$, mis tähendab, et ka definitsiooni 1.3 tingimus (ii) on rahuldatud ning $|a|$ on tõesti a ja b suurim ühistegur. □

Järgmine lause on lugejale kindlasti tuttav. Lühidalt öeldes väidab ta seda, et iga täisarvu võib jäägiga jagada iga naturaalarvuga.

Lause 1.6. *Olgu a täisarv ja b naturaalarv. Siis leiduvad üheselt määratud täisarvud q (jagatis) ja r (jääk), nii et*

$$a = bq + r \quad ja \quad 0 \leqslant r < b.$$

Tõestus. Olgu antud $a \in \mathbb{Z}$ ja $b \in \mathbb{N}$. Vaatleme hulka

$$A = \{a - bx \mid x \in \mathbb{Z}, a - bx \geqslant 0\} \subseteq \mathbb{N} \cup \{0\}.$$

Paneme tähele, et $a + a^2 \geqslant 0$. Tõepoolest, $a \geqslant 0$ korral on see võrratus ilmne, $a \leqslant -1$ ehk $-a \geqslant 1$ korral $a^2 = (-a)^2 \geqslant -a$ omaduse Z10 põhjal ning $a^2 + a \geqslant 0$ omaduste Z9 ja Z3 põhjal. Järelikult $a - b(-a^2) = a + ba^2 \geqslant a + a^2 \geqslant 0$ ning seega $a - b(-a^2) \in A$. Kuna hulga $\mathbb{N} \cup \{0\}$ igas mittetühjas alamhulgas leidub vähim element, siis leidub ka hulga A vähim element $r = a - bq \in A$, kus $q \in \mathbb{Z}$. Näitame, et $r < b$. Selleks oletame vastuväiteliselt, et $r \geqslant b$. Siis $0 \leqslant r' = r - b = a - b(q + 1) \in A$ ja $r' < r$, mis on vastuolus r valikuga. Niiviisi oleme leidnud sellised $q, r \in \mathbb{Z}$, et $a = bq + r$ ja $0 \leqslant r < b$.

Näitame, et q ja r on üheselt määratud. Selleks oletame, et leiduvad täisarvud q_1, q_2, r_1, r_2 nii, et

$$a = bq_1 + r_1 = bq_2 + r_2 \quad \text{ja} \quad 0 \leqslant r_1, r_2 < b.$$

Siis $b(q_1 - q_2) = r_2 - r_1$. Kuna $b \geqslant 1$, $|r_2 - r_1| < b$ ja $q_1 - q_2 \in \mathbb{Z}$, siis võrdusest $|r_2 - r_1| = |b||q_1 - q_2| = b|q_1 - q_2|$ järeldub, et $q_1 - q_2 = 0$ ja seega ka $r_2 - r_1 = 0$. Sellega oleme näidanud, et $q_1 = q_2$ ja $r_1 = r_2$. □

Võrreldes lauset 1.6 definitsiooniga 1.1 võime öelda, et naturaalarv b jagab täisarvu a (ehk a jagub arvuga b) parajasti siis, kui arvu a jagamisel arvuga b tekkiv jääk on 0.

Lausest 1.6 järeldub muuhulgas, et kahe täisarvu suurima ühisteguri leidmiseks saab kasutada *Eukleidese algoritmi*. Eukleides (sündis u. 350. aastal e.m.a.) oli kreeka matemaatik, kes elas ja töötas Aleksandrias. Eukleidese algoritm sisaldub Eukleidese põhiteose "Elemendid" VII raamatus. Algoritm ise võis olla teada kuni 200 aastat enne Eukleidest.

See algoritm töötab järgmiselt. Olgu eesmärgiks leida täisarvude a ja b suurim ühistegur. Üldisust kitsendamata võime eeldada, et $a \geqslant b > 0$ (sest $(a, b) = (|a|, |b|)$, $(a, b) = (b, a)$ ja $b = 0$ korral on selge, millega (a, b) võrdub). Kõigepealt jagame arvu a jäägiga arvuga b:

$$a = bq_1 + r_1, \qquad 0 \leqslant r_1 < b.$$

Kui $r_1 = 0$, siis $b \mid a$ ja seega $(a, b) = b$. Kui $r_1 \neq 0$, siis jagame arvu b arvuga r_1:

$$b = r_1 q_2 + r_2, \qquad 0 \leqslant r_2 < r_1.$$

Kui $r_2 = 0$, siis lõpetame; vastasel juhul jagame arvu r_1 arvuga r_2:

$$r_1 = r_2 q_3 + r_3, \qquad 0 \leqslant r_3 < r_2.$$

Niimoodi jätkame senikaua kui saame mingil sammul jäägiks $r_{n+1} = 0$. Varem või hiljem peab see juhtuma, sest $b > r_1 > r_2 > \ldots \geqslant 0$ ja ei leidu lõpmatuid kahanevaid naturaalarvujadasid. Osutub, et a ja b suurimaks ühisteguriks on viimane nullist erinev jääk r_n (tõestuse võib leida raamatust [1], lk. 196–197). Algoritmi võib kokku võtta järgmise tabelina.

Eukleidese algoritm.

$$\begin{array}{rcll} a & = & bq_1 + r_1, & 0 < r_1 < b, \\ b & = & r_1q_2 + r_2, & 0 < r_2 < r_1, \\ r_1 & = & r_2q_3 + r_3, & 0 < r_3 < r_2, \\ & \dots & & \dots \\ r_{n-3} & = & r_{n-2}q_{n-1} + r_{n-1} & 0 < r_{n-1} < r_{n-2}, \\ r_{n-2} & = & r_{n-1}q_n + r_n & 0 < r_n < r_{n-1}, \\ r_{n-1} & = & r_nq_{n+1} + 0. & \end{array} \tag{1}$$

1.3. Võrrand $ax + by = c$

Paljudel arvuteooria probleemidel on järgmine kuju: kui f on täisarvuliste kordajatega (ühe- või mitmemuutuja) polünoom, siis kas võrrandil $f = 0$ on täisarvulisi lahendeid? Selliseid võrrandeid on hakatud kreeka matemaatiku Diophantose auks nimetama *diofantilisteks võrranditeks*. Diophantos elas 3. sajandil ja töötas Aleksandrias. Tema põhiteos oli "Aritmeetika", milles ta muuhulgas käsitles tehteid ratsionaalarvudega, kasutas algelist algebralist sümboolikat ja lahendas mitme tundmatuga võrrandeid.

Üheks lihtsamaks diofantiliseks võrrandiks on võrrand $ax + by = c$, kus a, b, c on täisarvud ja x, y tundmatud. Järgnevas anname tarviliku ja piisava tingimuse selle võrrandi lahenduvuseks ja eeskirja kõigi lahendite leidmiseks.

Teoreem 1.7. *Antud täisarvude a, b, c korral leidub diofantilisel võrrandil*

$$ax + by = c \tag{2}$$

täisarvuline lahend parajasti siis, kui $(a, b) \mid c$.

Tõestus. Tarvilikkus. Oletame, et leiduvad sellised täisarvud x_0 ja y_0, et $ax_0 + by_0 = c$. Kuna $(a, b) \mid a$ ja $(a, b) \mid b$, siis lause 1.2(2, 3) põhjal ka $(a, b) \mid ax_0 + by_0 = c$.
Piisavus. Olgu $(a, b) = r_n$ leitud Eukleidese algoritmi abil. Et $(a, b) \mid c$, siis leidub selline $s \in \mathbb{Z}$, et $r_ns = c$. Liikudes tabelis (1) alt üles, saame r_n avaldada a ja b kaudu:

$$r_n = r_{n-2} - r_{n-1}q_n = r_{n-2} - (r_{n-3} - r_{n-2}q_{n-1})q_n = (1 + q_{n-1}q_n)r_{n-2} - q_nr_{n-3} = \ldots = ax' + by',$$

kus $x', y' \in \mathbb{Z}$. Seega $a(x's) + b(y's) = (ax' + by')s = r_ns = c$, s.t. täisarvupaar $x's, y's$ on võrrandi (2) lahend. □

Teoreemist 1.7 saab teha mitmeid kasulikke järeldusi.

Järeldus 1.8 (Bézout' lemma)**.** *Nullist erinevate täisarvude a ja b jaoks leiduvad täisarvud x ja y nii, et*

$$ax + by = (a, b).$$

Järeldus 1.9. *Olgu $a, b, d \in \mathbb{Z}$ sellised, et $d \mid a,\ d \mid b$ ja $d \neq 0$. Siis võrdus $(a, b) = |d|$ on samaväärne võrdusega $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.*

Tõestus. Olgu $a, b, d \in \mathbb{Z}$ sellised, et $d \mid a,\ d \mid b$ ning $d \neq 0$ (siis muuhulgas $\frac{a}{d}$ ja $\frac{b}{d}$ on täisarvud). Tähistame $d' = (a, b)$. Definitsiooni 1.3 põhjal teame, et $d \mid d'$. Seega $d' = |d|$ parajasti siis, kui $d' \mid d$. Järelikult

$$d' = |d| \iff d' \mid d \underset{\text{Teor. 1.7}}{\iff} (\exists x_0, y_0 \in \mathbb{Z})(ax_0 + by_0 = d) \iff (\exists x_0, y_0 \in \mathbb{Z}) \left(\frac{a}{d}x_0 + \frac{b}{d}y_0 = 1\right)$$
$$\underset{\text{Teor. 1.7}}{\iff} \left(\frac{a}{d}, \frac{b}{d}\right) \mid 1 \underset{\text{Lause 1.2(4)}}{\iff} \left(\frac{a}{d}, \frac{b}{d}\right) = 1.$$

□

Järeldus 1.10 (Eukleidese lemma)**.** *Mistahes $a, b, c \in \mathbb{Z}$ korral, kui $a \mid bc$ ja $(a, b) = 1$, siis $a \mid c$.*

Tõestus. Kuna $(a, b) = 1$, siis leiduvad sellised täisarvud x_0 ja y_0, et $ax_0 + by_0 = 1$. Järelikult $ax_0c + by_0c = c$. Et a jagab selle võrduse vasakut poolt, siis peab ta jagama ka paremat poolt, s.t. $a \mid c$. □

Meenutame, et *algarvuks* nimetatakse naturaalarvu $p > 1$, mille ainsad naturaalarvulised jagajad on 1 ja p. Naturaalarvu, mis on suurem kui 1 ja mis pole algarv, nimetatakse *kordarvuks*.

Järeldus 1.11. *Mistahes $b, c \in \mathbb{Z}$ ja algarvu p korral, kui $p \mid bc$, siis kas $p \mid b$ või $p \mid c$.*

TÕESTUS. Algarvu p ainsad täisarvulised jagajad on ± 1 ja $\pm p$. Seega $(p,b) = p$ või $(p,b) = 1$. Esimesel juhul $p \mid b$. Teisel juhul saame järelduse 1.10 põhjal, et $p \mid c$. □

Järeldust 1.11 kasutades saab lihtsalt tõestada järgmise väite.

Järeldus 1.12. *Mistahes täisarvude $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ ja algarvu p korral, kui $p \mid a_1 a_2 \ldots a_n$, siis leidub selline $k \in \{1, 2, \ldots, n\}$, et $p \mid a_k$.*

Kuna ainus algarv, millega mingi algarv jagub, on see algarv ise, siis saame järgmise tulemuse.

Järeldus 1.13. *Kui $p, q_1, q_2, \ldots, q_n$ on algarvud ja $p \mid q_1 q_2 \ldots q_n$, siis leidub selline $k \in \{1, 2, \ldots, n\}$, et $p = q_k$.*

Näitena nende omaduste rakendamisest vaatleme järgmist väidet, mille tõestas juba kreeka matemaatik ja filosoof Pythagoras (569–500 e.m.a.).

Näide 1.14. $\sqrt{2}$ ei ole ratsionaalarv.

Oletame vastuväiteliselt, et leidub ratsionaalarv, mille ruut on 2, s.t. $2 = \left(\frac{b}{a}\right)^2$, kus a ja b on täisarvud ja $(a,b) = 1$. Siis $b^2 = 2a^2$ ning seega $a \mid b^2 = bb$. Järelduse 1.10 põhjal peaks $a \mid b$ ning järelikult $1 = (a,b) = |a|$ ja $b^2 = 2$, mis on vastuolu, sest ühegi täisarvu ruut pole 2. Saadud vastuolu näitabki, et $\sqrt{2}$ ei saa olla ratsionaalarv.

Lõpetuseks tõestame teoreemi, mis näitab, kuidas leida diofantilise võrrandi (2) kõik täisarvulised lahendid, kui on teada selle võrrandi üks (eri)lahend.

Teoreem 1.15. *Olgu a, b ja c täisarvud. Kui vähemalt üks arvudest a ja b ei ole 0 ning x_0, y_0 on võrrandi $ax+by = c$ mingi lahend, siis selle võrrandi kõik lahendid x, y saadakse valemite*

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

abil, andes muutujale t kõik täisarvulised väärtused.

TÕESTUS. Olgu meile teada võrrandi $ax + by = c$ mingi lahend x_0, y_0. Kui x', y' on selle võrrandi mingi teine lahend, siis $ax_0 + by_0 = c = ax' + by'$, millest järeldub, et $a(x' - x_0) = b(y_0 - y')$. Kui vähemalt üks arvudest a ja b ei ole 0, siis $(a,b) \neq 0$. Tähistades $d = (a,b)$, saame leida sellised täisarvud a' ja b', et $a = da'$ ja $b = db'$, kusjuures järelduse 1.9 põhjal $(a', b') = \left(\frac{a}{d}, \frac{b}{d}\right) = 1$. Järelikult $da'(x' - x_0) = db'(y_0 - y')$, millest arvu d taandamisel (täisarvude omadus Z11) saame

$$a'(x' - x_0) = b'(y_0 - y'). \tag{3}$$

Meil on olukord, kus $a' \mid b'(y_0 - y')$ ja $(a', b') = 1$. Kasutades järeldust 1.10 saame, et $a' \mid (y_0 - y')$, s.t. leidub selline $t \in \mathbb{Z}$, et $y_0 - y' = a't$. Asendades $y_0 - y'$ võrduses (3) ning taandades arvu a' (juhul kui $a \neq 0$), saame $x' - x_0 = b't$. Seega näeme, et lahend x', y' avaldub kujul

$$x' = x_0 + b't = x_0 + \frac{b}{(a,b)}t, \qquad y' = y_0 - a't = y_0 - \frac{a}{(a,b)}t.$$

Kui $a = 0$, kuid $b \neq 0$, siis toimime analoogiliselt lähtudes asjaolust, et $b' \mid a'(x' - x_0)$.

Teisest küljest, on lihtne kontrollida, et iga $t \in \mathbb{Z}$ korral sellised arvud rahuldavad võrrandit $ax + by = c$:

$$a\left(x_0 + \frac{b}{(a,b)}t\right) + b\left(y_0 - \frac{a}{(a,b)}t\right) = ax_0 + by_0 = c.$$

□

Märkus 1.16. Vaatleme võrrandit $ax+by = c$ üle reaalarvude ning kirjutame selle võrrandi reaalarvulisi lahendeid järjestatud paaridena $\langle x, y\rangle$. Eeldame, et vähemalt üks arvudest a ja b ei ole 0. Siis lineaaralgebrast on teada, et sellest ühest võrrandist koosnevale lineaarvõrrandisüsteemile vastava homogeense süsteemi $ax + by = 0$ lahendite fundamentaalsüsteem sisaldab ühe lahendi $\langle x_1, y_1\rangle$ (selleks võib võtta näiteks paari $\langle x_1, y_1\rangle = \left\langle \frac{b}{(a,b)}, -\frac{a}{(a,b)} \right\rangle \in \mathbb{R}^2$) ning süsteemi $ax + by = c$ kõigi reaalarvuliste lahendite hulk avaldub kujul

$$\langle x_0, y_0\rangle + \{t\langle x_1, y_1\rangle \mid t \in \mathbb{R}\} = \{\langle x_0 + tx_1, y_0 + ty_1\rangle \mid t \in \mathbb{R}\},$$

kus $\langle x_0, y_0\rangle \in \mathbb{R}^2$ on selle võrrandi mingi erilahend (vt. [1], teoreem 5.5.3). Teoreem 1.7 ütleb, et kui vaadelda võrrandit $ax + by = c$ üle täisarvude, siis tema kõigi lahendite hulk avaldub sisuliselt samasugusel kujul.

Näide 1.17. Lahendame diofantilise võrrandi

$$172x + 20y = 1000.$$

Selleks leiame Eukleidese algoritmi abil $(172, 20)$:

$$\begin{aligned} 172 &= 20 \cdot 8 + 12 \\ 20 &= 12 \cdot 1 + 8 \\ 12 &= 8 \cdot 1 + 4 \\ 8 &= 4 \cdot 2, \end{aligned}$$

kust näeme, et $(172, 20) = 4$. Kuna $4 \mid 1000$, siis võrrandil on lahend olemas. Avaldame nüüd arvu 4 arvude 172 ja 20 "lineaarkombinatsioonina":

$$4 = 12 - 8 = 12 - (20 - 12) = 2 \cdot 12 - 20 = 2 \cdot (172 - 20 \cdot 8) - 20 = 2 \cdot 172 + (-17) \cdot 20.$$

Korrutades saadud võrduse mõlemaid pooli arvuga 250, saame $1000 = 500 \cdot 172 + (-4250) \cdot 20$, seega $x_0 = 500, y_0 = -4250$ on antud võrrandi üheks lahendiks. Kõik ülejäänud täisarvulised lahendid saame arvutada valemeist

$$\begin{aligned} x &= 500 + \tfrac{20}{4}t = 500 + 5t, \\ y &= -4250 - \tfrac{172}{4}t = -4520 - 43t, \end{aligned}$$

kus t on täisarv.

Leiame veel näiteks selle võrrandi kõik positiivsed lahendid (s.t. lahendid, kus $x > 0$ ja $y > 0$). Positiivsete lahendite korral peab t rahuldama võrratusi $500 + 5t > 0$ ja $-4250 - 43t > 0$, ehk samaväärselt $-100 < t < -98\frac{36}{43}$. Ainus täisarv, mis neid tingimusi rahuldab, on $t = -99$. See tähendab, et antud võrrandil on vaid üks positiivne lahend $x = 500 + 5 \cdot (-99) = 5$, $y = -4520 - 43 \cdot (-99) = 7$.

1.4. Aritmeetika põhiteoreem

Järgnevalt tõestame väite, millele tugineb suur osa naturaalarvude aritmeetikas tõestatavatest teoreemidest ja mis pärineb Eukleidese "Elementide" IX raamatust.

Teoreem 1.18 (Aritmeetika põhiteoreem)**.** *Iga naturaalarvu $n > 1$ saab esitada algarvude korrutisena (s.t. leiduvad $r \in \mathbb{N}$ ja algarvud $p_1, \ldots, p_r$ nii, et $n = p_1 \ldots p_r$) ning see esitus on ühene tegurite järjekorra täpsuseni.*

Tõestus. Näitame esiteks matemaatilise induktsiooniga, et iga naturaalarvu $n > 1$ saab esitada algarvude korrutisena. Arvu $n = 2$ korral on väide ilmne. Oletame, et $n > 2$ ja iga naturaalarvu $1 < m < n$ saab esitada algarvude korrutisena. Naturaalarv n peab olema kas algarv või kordarv. Esimesel juhul pole midagi tõestada. Kui aga n on kordarv, siis leidub naturaalarv $d \mid n$, kusjuures $1 < d < n$. Olgu $n = da, a \in \mathbb{N}$; siis ka $1 < a < n$. Induktsiooni eelduse põhjal avalduvad d ja a algarvude korrutisena ning järelikult ka n avaldub algarvude korrutisena.

Ühesuse näitamiseks oletame, et n saab algarvude korrutisena esitada kahel viisil:

$$n = p_1 p_2 \ldots p_r = q_1 q_2 \ldots q_s,$$

kus (üldisust kitsendamata) $r \leqslant s$ ja algarvud p_i ja q_j on mittekahanevas järjekorras, s.t. $p_1 \leqslant p_2 \leqslant \ldots \leqslant p_r$ ja $q_1 \leqslant q_2 \leqslant \ldots \leqslant q_s$. Kuna $p_1 \mid q_1 q_2 \ldots q_s$, siis järelduse 1.13 põhjal $p_1 = q_k$ mingi $k \in \{1, \ldots, s\}$ korral; kuid siis $p_1 \geqslant q_1$. Samamoodi saame $q_1 \geqslant p_1$ ning kokkuvõttes $p_1 = q_1$. Arvu p_1 taandades saame $p_2 p_3 \ldots p_r = q_2 q_3 \ldots q_s$. Korrates seda mõttekäiku saame $p_2 = q_2$ ja $p_3 p_4 \ldots p_r = q_3 q_4 \ldots q_s$. Kui $r < s$, siis niimoodi jätkates jõuame võrduseni $1 = q_{r+1} q_{r+2} \ldots q_s$, mis on aga võimatu, sest $q_i > 1$ iga $i \in \{1, \ldots, s\}$ korral. Seega $r = s$ ning $p_1 = q_1$, $p_2 = q_2, \ldots, p_r = q_r$, mida oligi tarvis tõestada. □

Naturaalarvu esitust algarvude korrutisena nimetame tema *algtegureiks lahutuseks* ning selles lahutuses esinevaid algarve nimetame antud arvu *algtegureiks*. Sõltuvalt tegurite järjekorrast võib algtegureiks lahutusi olla mitu. Vahel on siiski otstarbekam kasutada arvu ühesemat esitust.

Järeldus 1.19. *Iga naturaalarvu $n > 1$ saab üheselt esitada kujul*

$$n = p_1^{k_1} p_2^{k_2} \ldots p_s^{k_s}, \tag{4}$$

kus $k_i \in \mathbb{N}$, p_i on algarv iga $i = 1, 2, \ldots, s$ korral ning $p_1 < p_2 < \ldots < p_s$.

Naturaalarvu n esitust kujul (4) nimetame selle arvu *standardkujuks*.

Näide 1.20. $180 = 2 \cdot 5 \cdot 2 \cdot 3 \cdot 3 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 = 2^2 \cdot 3^2 \cdot 5^1$, kus viimane korrutis on arvu 180 standardkuju.

Aritmeetika põhiteoreem annab veel ühe võimaluse SÜT ja VÜK arvutamiseks. Kui $m, n > 1$ on naturaalarvud ja $\{p_1, \ldots, p_s\}$ on nende arvude algtegurite hulkade ühend, siis võime need arvud esitada kujul $m = p_1^{k_1} \ldots p_s^{k_s}$, $n = p_1^{l_1} \ldots p_s^{l_s}$, kus $p_1, \ldots, p_s$ on paarikaupa erinevad algarvud ja $k_i \geqslant 0, l_i \geqslant 0$, $i = 1, \ldots, s$. (NB! Tegemist pole standardkujudega, sest astendajate hulgas võib olla nulle.)

Lause 1.21. *Olgu $m, n > 1$ naturaalarvud, $m = p_1^{k_1} \ldots p_s^{k_s}$, $n = p_1^{l_1} \ldots p_s^{l_s}$, kus $p_1, \ldots, p_s$ on paarikaupa erinevad algarvud ja $k_i \geqslant 0, l_i \geqslant 0$, $i = 1, \ldots, s$. Siis*

1. *$m \mid n$ parajasti siis, kui $k_i \leqslant l_i$ iga $i = 1, \ldots, s$ korral;*
2. *$(m, n) = p_1^{u_1} \ldots p_s^{u_s}$, kus $u_i = \min(k_i, l_i)$ iga $i = 1, \ldots, s$ korral;*
3. *$[m, n] = p_1^{v_1} \ldots p_s^{v_s}$, kus $v_i = \max(k_i, l_i)$ iga $i = 1, \ldots, s$ korral;*
4. *$(cm, cn) = |c| \cdot (m, n)$ iga $c \in \mathbb{Z}$ korral;*
5. *$[cm, cn] = |c| \cdot [m, n]$ iga $c \in \mathbb{Z}$ korral.*

Tõestus. 1. Tarvilikkus. Eeldame, et $m \mid n$. See tähendab, et leidub selline $a \in \mathbb{N}$, et $ma = n$. Kui $a = 1$, siis järeldub väide vahetult aritmeetika põhiteoreemist. Kui $a > 1$, siis tänu aritmeetika põhiteoreemile ei saa a algtegurite hulgas olla selliseid algarve, mis ei ole n algtegurid. Seega on a kujul $a = p_1^{j_1} \ldots p_s^{j_s}$, kus $j_1, \ldots, j_s \geqslant 0$. Järelikult

$$p_1^{k_1+j_1} \ldots p_s^{k_s+j_s} = \left(p_1^{k_1} \ldots p_s^{k_s}\right)\left(p_1^{j_1} \ldots p_s^{j_s}\right) = ma = n = p_1^{l_1} \ldots p_s^{l_s}.$$

Aritmeetika põhiteoreemi põhjal $k_i + j_i = l_i$, millest järeldubki, et $k_i \leqslant l_i$ iga $i = 1, \ldots, s$ korral.

Piisavus. Olgu $k_i \leqslant l_i$ iga $i = 1, \ldots, s$ korral. Siis $m\left(p_1^{l_1-k_1} \ldots p_s^{l_s-k_s}\right) = n$, ehk $m \mid n$.

2. Tähistame $d = p_1^{u_1} \ldots p_s^{u_s}$. Kuna $u_i \leqslant k_i$ ja $u_i \leqslant l_i$, $i = 1, \ldots, s$, siis väite 1 põhjal $d \mid m$ ja $d \mid n$. Oletame, et $c \mid m$ ja $c \mid n$, kusjuures $c = p_1^{j_1} \ldots p_s^{j_s}$. Jällegi väite 1 põhjal $j_i \leqslant k_i$ ning $j_i \leqslant l_i$, $i = 1, \ldots, s$. Seega $j_i \leqslant \min(k_i, l_i) = u_i$, $i = 1, \ldots, s$, millest järeldub, et $c \mid d$.

Väite 3 saab tõestada analoogiliselt. Väited 4 ja 5 järelduvad sellest, et $\min(j + k, j + l) = j + \min(k, l)$ ja $\max(j + k, j + l) = j + \max(k, l)$ mistahes mittenegatiivsete täisarvude j, k ja l korral. □

Tuleb märkida, et lause 1.21 omab tähtsust pigem teoreetilistes arutlustes, sest naturaalarvu algtegureiks lahutamine on enamasti väga töömahukas. Suurima ühisteguri praktiliseks leidmiseks kasutatakse reeglina Eukleidese algoritmi.

Kuna mistahes mittenegatiivsete täisarvude k ja l korral $\min(k, l) + \max(k, l) = k + l$, siis kehtib järgmine lause.

Lause 1.22. *Mistahes naturaalarvude m ja n korral*

$$(m, n)\,[m, n] = mn.$$

Näide 1.23. Olgu $m = 36$ ja $n = 27$. Lahutame nad algarvude astmete korrutiseks: $m = 2^2 \cdot 3^2$ ja $n = 2^0 \cdot 3^3$. Kasutades lauset 1.21 saame, et $(m, n) = 2^0 \cdot 3^2 = 9$ ja $[m, n] = 2^2 \cdot 3^3 = 108$.

Näide 1.24. Leiame $[172, 20]$. Näite 1.17 põhjal teame, et $(172, 20) = 4$. Järelikult

$$[172, 20] = \frac{172 \cdot 20}{(172, 20)} = \frac{172 \cdot 20}{4} = 43 \cdot 20 = 860.$$

2. Algarvud

2.1. Algarvulisuse kontrollimine

Meenutame veelkord, et naturaalarvu $p > 1$ nimetatakse *algarvuks*, kui tema ainsad naturaalarvulised jagajad on 1 ja p. Naturaalarvu, mis on suurem kui 1 ja mis pole algarv, nimetatakse *kordarvuks*. Kõigi algarvude hulka tähistame edaspidi sümboliga $\mathbb{P}$.

Kuidas antud naturaalarvu korral kindlaks teha, kas ta on algarv või kordarv? Kõige lihtsam viis on jagada seda arvu kõigi talle eelnevate naturaalarvudega. Kui ta ühegagi neist (välja arvatud 1) ei jagu, siis on ta algarv, vastasel juhul kordarv. Kuigi see meetod on lihtne, ei kõlba ta praktikas kasutamiseks arvutuste liiga suure mahu tõttu.

Arvutuste mahtu saab veidi vähendada, kui paneme tähele järgmist kordarvude omadust. Olgu $a > 1$ kordarv, s.t. $a = bc$, kus $1 < b, c < a$. Eeldades, et näiteks $b \leqslant c$, saame, et $b^2 \leqslant bc = a$ ja seega $b \leqslant \sqrt{a}$. Et $b > 1$, siis leidub arvul b vähemalt üks algtegur p. Siis $p \leqslant b \leqslant \sqrt{a}$, ning kuna $p \mid b$ ja $b \mid a$, siis $p \mid a$. Niisiis, kui a on kordarv, siis tal leidub selline algtegur, mis pole suurem kui $\sqrt{a}$. Ehk samaväärselt: kui ükski algarv $p \leqslant \sqrt{a}$ ei ole arvu a jagaja, siis a on algarv. Niisiis arvu a algarvulisuse kontrollimiseks piisab, kui kontrollime, kas ta jagub algarvudega $p \leqslant \sqrt{a}$.

Näide 2.1. Kas 101 on algarv?

Et $10 < \sqrt{101} < 11$, siis tuleb kontrollida jaguvust algarvudega 2, 3, 5 ja 7. Kuna 101 ühegagi neist ei jagu, siis on ta algarv.

Eespool nägime, et kui ükski algarv $p \leqslant \sqrt{a}$ ei ole arvu a jagaja, siis a on algarv. Sellel faktil põhineb kreeka matemaatiku Eratosthenese (276–194 e.m.a.) poolt välja töötatud meetod mingist fikseeritud naturaalarvust n mittesuuremate algarvude leidmiseks, mida nimetatakse *"Eratosthenese sõelaks"*. Alljärgnev kirjeldus on pärit Boethiuse (u. 480–524 m.a.j.) raamatust "Aritmeetika alustest".

"Nende arvude [algarvude] genereerimine ja leidmine on võetud uurimusest, mida Eratosthenes, muuhulgas, nimetas "sõelaks", sest kui kõik paaritud arvud on pandud keskele kokku, siis kunsti abil, mida me tahame edasi anda, sõelutakse teiste hulgast välja iga arv, mis on kas esimest või kolmandat liiki [s.t. on algarv]. Olgu kõik paaritud arvud alates kolmest paigutatud mistahes pikkusega järjestatud ritta: 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31, 33, 35, 37, 39, 41, 43, 45, 47. Nende arvude sellise jada korral peame vaatama, mis on esimene arv, mida saab mõõta esimene arv reas. Siis ta järgmisena mõõdab arvu, mis on kahe arvu kaugusel esimesest ja selleks, et mõõta arvu tolle mõõdetud arvu järel, peab veel kaks arvu vahele jätma ning samamoodi edasi, kui need kaks arvu on vahele jäetud, siis arv, mida jälle kord mõõdetakse, on mõõdetud esimese arvu poolt; niimoodi iga mõõdetava arvu ja eelmise mõõdetud arvu vahel on kaks ja nii jätkatakse esimesest arvust lõpmatuseni.

Kuid las ma teen seda mitte üldisel ja segasel moel. Esimene arv mõõdab oma suurusega seda, mis paikneb kahe arvu järel pärast teda ennast. Nii kolm, jättes kaks arvu vahele, see on 5 ja 7, mõõdab üheksat ja mõõdab teda iseenda suurusega, see on kolm korda. Kolm korda kolm mõõdab üheksat. Kui pärast üheksat jätan vahele kaks arvu, siis saan arvu, mis tuleb nende järel ja on mõõdetud esimese paaritu arvu poolt teise paaritu arvu suuruse abil, see on viie abil. Nii et kui pärast 9-t me jätame vahele 2 arvu, see on 11 ja 13, siis kolmandat arvu, 15-t, mõõdetakse [jada] teise arvu suuruse abil, see on viie abil, kolm mõõdab 15-t viis korda. Jälle, kui alustades viieteistkümnest ma jätan vahele kaks arvu, mis on paigutatud jadas tema järele, siis esimene arv on tema [s.o. arvu 3] mõõt jada kolmanda paaritu arvu abil. Kui pärast 15-t ma jätan vahele 17 ja 19, siis ma jõuan 21-ni, mis on mõõdetud arvu kolm poolt seitse korda. Arvust 21 on kolm seitsmendikosa, ja tehes seda lõpmatult, ma leian, et jada esimene arv, kui jadas kaks arvu järjest vahel jätta, suudab mõõta kõiki järgnevaid arve, ja seda järjest selle jada paaritute arvude suuruste abil.

Kui arvu viis korral, mis asub jadas teisel kohal, tahaks keegi leida esimese ja järgnevad arvud, millele 5 on mõõduks, tuleks vahele jätta 4 paaritut arvu pärast 5-t, kuni tuleb see, mida 5 mõõta saab. Vahele jäetakse 4 paaritut arvu, see on 7, 9, 11 ja 13. Pärast neid on 15, mida viis mõõdab esimese paaritu arvu suurusega, see on kolmega. 5 mõõdab 15-t kolm korda. Kui seejärel jäetakse vahele neli arvu, siis seda, mis asetseb nende järel, mõõdab jada teine arv, see on 5, oma suurusega. Nii pärast 15-t, kui arvud 17, 19, 21 ja 23 jätad vahele, siis pärast neid leiame 25, mida viis mõõdab iseenda suurusega. Viis korrutades viiega kasvab 25-ni. Kui pärast seda jäetakse vahele järgmised neli arvu, säilitades sellega sellesama jada konstantsuse, siis arvu, mis järgneb, mõõdab viis jada kolmanda arvu, see on seitsme, suurusega; ja see protsess on lõpmatu.

Kui kolmas arv, millega saab mõõta, on välja otsitud, ja kuus kohta on vahele jäetud, siis jõuab järjestus seitsmenda arvuni, seda saab mõõta esimese arvu, see on kolme, suurusega; ja pärast seda arvu, kui kuus arvu paned vahele, siis arvu, mille jada siis annab, saab mõõta viiega, jada teise arvuga, ja see mõõdab 15-t kolm korda. Kui siis jäetaks vahele veel kuus vahepealset arvu, siis arvu, mis järgneb, seitsmendat arvu [21] saab mõõta seitsmega kolme suuruse abil; ja see kindel kord jätkub jada viimase arvuni."

Juba Eukleides oma "Elementides" näitas, et ei saa olla suurimat algarvu.

Teoreem 2.2 (Eukleides)**.** *Algarvude hulk on lõpmatu.*

TÕESTUS. Olgu algarvud tähistatud $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, \ldots$. Oletame vastuväiteliselt, et leidub suurim algarv p_n. Vaatleme naturaalarvu $a = p_1 p_2 \ldots p_n + 1$. Et $a > 1$, siis peab leiduma algarv, mis arvu a jagab. Kuna oletasime, et $p_1, \ldots, p_n$ on ainsad algarvud, siis peab leiduma selline $i \in \{1, \ldots, n\}$, et $p_i \mid a$. Lause 1.2 põhjal saame, et $p_i \mid a - p_1 p_2 \ldots p_n = 1$, mis on vastuolus sellega, et $p_i > 1$. □

2.2. Algarvud ja aritmeetilised jadad

Lause 1.6 tõttu võib iga naturaalarvu esitada üheselt kas kujul $4k$, $4k+1$, $4k+2$ või $4k+3$, kus $k \in \mathbb{N} \cup \{0\}$, sõltuvalt sellest, millise jäägi annab see naturaalarv jagamisel 4-ga. On selge, et arvud $4k$ ja $4k+2 = 2(2k+1)$, $k \in \mathbb{N}$, on paarisarvud ja seega kordarvud. Paaritud arvud jagunevad kahte lõpmatusse jadasse: ühed, mis on kujul $4k+1$, s.t.

$$1, 5, 9, 13, 17, 21, \ldots$$

ja teised, mis on kujul $4k+3$, s.t.

$$3, 7, 11, 15, 19, 23, \ldots .$$

Mõlemas jadas on nii alg- kui kordarve. Osutub, et analoogiliselt eelmise teoreemiga, saab tõestada, et teine jada sisaldab lõpmata palju algarve. Selleks tõestame enne ühe tillukese lemma.

Lemma 2.3. *Kui kaks naturaalarvu on kujul $4k+1$, siis nende korrutis on samal kujul.*

TÕESTUS. Olgu $m = 4k+1$ ja $n = 4l+1$, $k, l \in \mathbb{N} \cup \{0\}$. Siis $mn = (4k+1)(4l+1) = 4(4kl + k + l) + 1$. □

Teoreem 2.4. *On lõpmata palju algarve kujul $4k+3$.*

TÕESTUS. Oletame jällegi vastuväiteliselt, et on vaid lõplik arv algarve kujul $4k+3$. Olgu nad tähistatud $q_1, \ldots, q_n$. Vaatleme naturaalarvu $a = 4q_1 q_2 \ldots q_n - 1 = 4(q_1 q_2 \ldots q_n - 1) + 3$. Olgu $a = r_1 r_2 \ldots r_s$ arvu a lahutus algtegureiks. Kuna a on paaritu arv, siis ükski r_i ei ole 2. Seega iga r_i on kas kujul $4k+1$ või $4k+3$. Lemma 2.3 tõttu peab vähemalt üks tegureist $r_1, \ldots, r_s$ olema kujul $4k+3$. Olgu $r_i = 4k+3, k \in \mathbb{N} \cup \{0\}$. Siis peab leiduma selline j, et $r_i = q_j > 1$. Järelikult $r_i \mid a - 4q_1 q_2 \ldots q_n = -1$, vastuolu. □

Tegelikult on ka jadas $(4k+1)_{k \in \mathbb{N} \cup \{0\}}$ lõpmata palju algarve (vt. lauset **??**) ja veelgi enam, kehtib saksa matemaatiku Dirichlet' (1805–1859) poolt 1837. a. tõestatud teoreem algarvude kohta aritmeetilises jadas, mida me siinkohal ei tõesta.

Teoreem 2.5 (Dirichlet)**.** *Kui a ja b on naturaalarvud ja $(a, b) = 1$, siis aritmeetilises jadas*

$$a, a+b, a+2b, a+3b, \ldots$$

on lõpmata palju algarve.

Lihtne on tõestada järgmist tulemust.

Lause 2.6. *Igas aritmeetilises jadas on lõpmata palju kordarve.*

TÕESTUS. Vaatleme aritmeetilist jada $a, a+b, a+2b, \ldots = (a+kb)_{k \in \mathbb{N} \cup \{0\}}$, $a, b \in \mathbb{N}$. Kui kõik selle jada liikmed on kordarvud, siis on väide ilmne. Kui aga leidub $l \in \mathbb{N} \cup \{0\}$ nii, et $a + lb = p$, kus p on algarv, siis iga $m \in \mathbb{N}$ korral on $a + (l + mp)b = a + lb + mpb = p(1 + mb)$ kordarv ja seega jada $(a+kb)_{k \in \mathbb{N} \cup \{0\}}$ sisaldab lõpmata palju kordarve. □

2004. aastal õnnestus briti matemaatikul Ben Greenil (sünd. 1977) ja austraalia matemaatikul Terence Taol (sünd. 1975) tõestada, et iga naturaalarvu n korral leidub aritmeetiline jada pikkusega n, mis koosneb algarvudest. Näiteks $n = 3$ ja $n = 4$ korral on sellisteks jadadeks $3, 5, 7$ ja $251, 257, 263, 269$.

2.3. Algarvude jaotus

Et algarvude hulk on lõpmatu, oleks huvitav teada, kuidas nad paiknevad teiste naturaalarvude seas. Järjestikuste algarvude vahe võib olla väike, nagu näiteks paaride 11 ja 13, 17 ja 19 või 1 000 000 000 061 ja 1 000 000 000 063 korral. Selliseid järjestikuste algarvude p ja $p+2$ paare nimetatakse *algarvukaksikuiks*. Kas selliseid paare on lõpmata palju või mitte, ei ole teada.

Samas võivad kaks järjestikust algarvu olla teineteisest kuitahes kaugel. Täpsemalt, iga naturaalarvu n korral leidub n järjestikust kordarvu. Nendeks on näiteks

$$(n+1)!+2, (n+1)!+3, \ldots, (n+1)!+(n+1).$$

Kui tahame saada näiteks nelja järjestikust kordarvu, võime võtta

$$\begin{array}{lcll} 5!+2 & = & 122 & = & 2 \cdot 61 \\ 5!+3 & = & 123 & = & 3 \cdot 41 \\ 5!+4 & = & 124 & = & 4 \cdot 31 \\ 5!+5 & = & 125 & = & 5 \cdot 25. \end{array}$$

Loomulikult on ka väiksemate järjestikuste kordarvude nelikuid, nt. $24, 25, 26, 27$ või $32, 33, 34, 35$.

Järgmine teoreem ütleb, et naturaalarvule n järgnevat algarvu ei pea siiski väga kaugelt otsima.

Teoreem 2.7 (Tšebõšov)**.** *Kui $n > 3$ on naturaalarv, siis n ja $2n-2$ vahel leidub vähemalt üks algarv.*

Selle teoreemi tõestas esimesena 1850. a. vene matemaatik Pafnuti Tšebõšov (1821–1894). Hüpoteesina sõnastas selle väite 1845. a. prantsuse matemaatik Joseph Bertrand (1822–1900) ning seetõttu kutsutakse seda väidet vahel ka Bertrand'i postulaadiks. Tegelikult kehtib isegi tugevam väide.

Teoreem 2.8. *Kui $n > 5$ on naturaalarv, siis n ja $2n$ vahel leidub vähemalt kaks erinevat algarvu.*

Veel on loomulik küsida, et kui palju on antud naturaalarvust väiksemaid algarve. Naturaalarvu n korral olgu $\pi(n)$ kõigi arvust n väiksemate algarvude arv. Täpset valemit $\pi(n)$ arvutamiseks pole. Mitmed matemaatikud leidsid proovides, et suurte naturaalarvude korral on $\pi(n)$ ligikaudu võrdne avaldisega $n/\ln(n)$. Ja tõepoolest, 1896. aastal õnnestus prantsuse matemaatikuil Jacques Hadamard'il (1865–1963) ja Charles de la Vallé Poussinil (1866–1962) teineteisest sõltumatult tõestada, et

$$\pi(n) \sim \frac{n}{\ln(n)} \text{ protsessis } n \to \infty \quad \text{ehk} \quad \lim_{n\to\infty} \frac{\pi(n)}{n/\ln(n)} = 1.$$

Paneme tähele, et sellest järeldub, et $\pi(2n)$ on asümptootiliselt 2 korda suurem kui $\pi(n)$, sest

$$\frac{\pi(2n)}{\pi(n)} \sim \frac{2n}{\ln(2n)} \cdot \frac{\ln(n)}{n} = \frac{2\ln(n)}{\ln(2n)} = \frac{2\ln(n)}{\ln(2)+\ln(n)} \sim 2 \quad \text{protsessis } n \to \infty.$$

Sajandeid on matemaatikud otsinud valemit, mille järgi saaks välja arvutada kõik algarvud. Kui see ei õnnestu, siis vähemalt leida selline funktsioon, mille määramispiirkond oleks naturaalarvude hulk ja muutumispiirkond oleks algarvude hulga mingi alamhulk. Keskajal oli laialt levinud arvamus, et ruutfunktsioon

$$f(n) = n^2 + n + 41$$

omandab vaid algarvulisi väärtusi. Tegelikult see muidugi nii ei ole, sest $n = 40$ ja $n = 41$ korral saame vastavalt $f(40) = 40 \cdot 41 + 41 = 41^2$ ja $f(41) = 41 \cdot 42 + 41 = 41 \cdot 43$. Järgmine väärtus $f(42) = 1747$ osutub jälle algarvuks. Pole teada, kas funktsioonil f on lõpmata palju algarvulisi väärtusi.

See, et $n = 40$ ja $n = 41$ korral saime kordarvud, polnud sugugi juhuslik. Kehtib üldisem teoreem, mille tõestamisel kasutame järgmist fakti (vt. [1], lause 7.1.9.).

Lause 2.9. *n-nda astme ühemuutuja polünoomil üle nullitegureita kommutatiivse ringi ei ole selles ringis rohkem kui n juurt.*

Teoreem 2.10 (Euler)**.** *Ühegi täisarvuliste kordajatega mittekonstantse ühemuutuja polünoomi väärtused ei ole kõigi muutuja naturaalarvuliste väärtuste korral algarvud.*

Tõestus. Oletame vastuväiteliselt, et leidub mittekonstantne polünoom

$$f(x) = a_m x^m + a_{m-1}x^{m-1} + \ldots + a_2 x^2 + a_1 x + a_0,$$

kus $a_0, \ldots, a_m \in \mathbb{Z}$, mille väärtus iga naturaalarvu n korral on algarv. Siis muuhulgas $f(1) = a_m + \ldots + a_0 = p$ on algarv. Kui $t \in \mathbb{N}$, siis kasutades Newtoni binoomvalemit saame

$$f(1+tp) = a_m(1+tp)^m + \ldots + a_1(1+tp) + a_0 = (a_m + \ldots + a_1 + a_0) + pg(t) = p + pg(t) = p(1+g(t)),$$

kus $g(x)$ on täisarvuliste kordajatega polünoom muutuja x suhtes. Järelikult $p \mid f(1+tp)$, millest eelduse tõttu saame, et $f(1+tp) = p$ iga $t \in \mathbb{N}$ korral. Seega täisarvuliste kordajatega mittekonstantsel polünoomil $f(x) - p$ on lõpmata palju täisarvulisi juuri, mis on vastuolus lausega 2.9. □

1947. a. tõestas William H. Mills, et leidub selline positiivne reaalarv $\theta = 1{,}3063\ldots$ (nn. *Millsi konstant*), et avaldise $f(n) = \lfloor \theta^{3^n} \rfloor$ väärtus, kus $\lfloor t \rfloor$ tähistab reaalarvu t *alumist täisosa*, s.t. suurimat täisarvu, mis ei ole suurem kui x, on algarv iga $n \in \mathbb{N}$ korral. Funktsiooni $f : \mathbb{N} \to \mathbb{N}$ esimesed väärtused on $2, 11, 1361, 2\,521\,008\,887, \ldots$. Ei ole teada, kas θ on ratsionaalarv. Kahjuks ei ole funktsioonist f praktilist kasu, sest θ täpse väärtuse leidmiseks peaks eelnevalt teadma funktsiooni f kõiki väärtusi. Samuti on funktsiooni f muutumispiirkond algarvude hulga väga väike alamhulk.

Veel ühe "looduses esineva" viisi genereerida algarve leidis 2008. a. Eric S. Rowland. Ta näitas, et rekurentse seosega

$$\begin{aligned} a_1 &= 7, \\ a_n &= a_{n-1} + (n, a_{n-1}),\ n > 1, \end{aligned}$$

defineeritud jada sisaldab ainult algarve ja ühtesid.

2.4. Aditiivseid probleeme

Üheks kuulsamaks algarvude kohta käivaks lahendamata probleemiks on preisi matemaatiku Christian Goldbachi (1690–1764) poolt kirjavahetuses šveitsi matemaatiku Leonhard Euleriga (1707–1783) aastal 1742 püstitatud hüpotees.

Hüpotees 2.11 (Goldbach)**.** *Iga positiivne paarisarv on esitatav summana $a + b$, kus nii a kui ka b on kas algarv või* 1*.*

Või natuke üldisemalt: kas iga 2-st suurem paarisarv on esitatav kahe algarvu summana? On lihtne näha, et väikeste paarisarvude korral see tõesti nii on:

$$\begin{aligned} 2 &= 1+1 \\ 4 &= 2+2 = 1+3 \\ 6 &= 3+3 = 1+5 \\ 8 &= 3+5 = 1+7 \\ 10 &= 3+7 = 5+5 \\ 12 &= 5+7 = 1+11 \\ 14 &= 3+11 = 7+7 = 1+13 \\ 16 &= 3+13 = 5+11 \\ 18 &= 5+13 = 7+11 = 1+17 \\ 20 &= 3+17 = 7+13 = 1+19. \end{aligned}$$

Goldbachi hüpoteesist järelduks nõrk Goldbachi hüpotees: iga 7-st suurema paaritu arvu saab esitada kolme paaritu algarvu summana. Nimelt, kui n on 7-st suurem paaritu arv, siis $n-3$ on paarisarv ja suurem kui 4. Kui $n-3$ saaks esitada kahe paaritu algarvu summana, siis n oleks kolme paaritu algarvu summa. Üheks märkimisväärsemaks Goldbachi hüpoteesiga seotud tulemuseks oli vene matemaatiku Ivan Vinogradovi (1891–1983) teoreem 1937. aastast, kus ta tõestas, et leidub naturaalarv N (kaks aastat hiljem leiti, et $N = \left\lfloor e^{e^{e^{41,96}}} \right\rfloor$; aastal 2002 tõestati, et piisab arvust $N = \lfloor e^{3100} \rfloor \approx 2 \cdot 10^{1346}$), millest suuremad paaritud arvud on esitatavad kolme algarvu summana. Nõrka Goldbachi hüpoteesi täielikult lahendas 2013. aastal Peruu matemaatik Harald Helfgott (sünd. 1977).

Teoreem 2.12. *Iga 7-st suurema paaritu arvu saab esitada kolme paaritu algarvu summana.*

Sellest tulemusest järeldub ka, et kõik 10-st suuremad paarisarvud on esitatavad ülimalt 4 paaritu algarvu summana.

Goldbachi probleem kuulub arvuteooria valdkonda, mida nimetatakse *aditiivseks* (s.o. liitmisega seotud) *arvuteooriaks.* Veel tuntum kui Goldbachi probleem on aga järgmine aditiivse arvuteooria tulemus.

Teoreem 2.13 (Fermat' suur teoreem)**.** *Kui $n \geqslant 3$ on naturaalarv, siis võrrandil*

$$x^n + y^n = z^n \tag{5}$$

ei ole mittetriviaalseid ratsionaalarvulisi lahendeid.

Triviaalseks loetakse lahendit, mille vähemalt üks komponent on 0.

Sellise hüpoteesi püstitas juba 1630. aastate lõpus prantsuse matemaatik Pierre de Fermat (1601–1665). Ta ise andis selle väite tõestuse juhul, kui $n = 4$. Kolme aastasaja kestel näitasid paljud matemaatikud Fermat' teoreemi tõestust otsides, et võrrandil (5) ei ole lahendeid ikka suuremate ja suuremate astendajate korral. Korrektne tõestus üldjuhu jaoks õnnestus aga leida alles möödunud sajandi lõpul. 23. juunil 1993. aastal teatas inglise matemaatik Andrew Wiles (sünd. 1953) Cambridge'is peetud loengus, et on tõestanud Fermat' teoreemi. Tõestamiseks kasutas ta algebralise geomeetria vahendeid, muuhulgas elliptilisi kõveraid ja modulaarseid vorme. See tõestus, mille ta välja pakkus, oli küll pisut vigane, kuid ta suutis need vead parandada ning lõplikult ilmus tema töö ajakirja *Annals of Mathematics* 1995. a. mainumbris.

3. Kongruentsi mõiste ja lihtsamad omadused

3.1. Kongruentsi mõiste

Kongruentsi mõiste võttis kasutusele saksa matemaatik Carl Friedrich Gauss (1777–1855) oma teoses "Disquisitiones Arithmeticae"(kirjutatud 1798, ilmunud 1801), mis pani aluse kaasaegsele arvuteooriale.

Definitsioon 3.1. Olgu $a, b \in \mathbb{Z}$ ja $n \in \mathbb{N}$. Öeldakse, et a ja b on *kongruentsed* mooduli n järgi (ja kirjutatakse $a \equiv b \pmod{n}$), kui $n \mid b - a$, s.t. kui leidub selline $k \in \mathbb{Z}$, et $b = a + kn$ ehk $a = b + (-k)n$.

Näide 3.2. $7 \equiv 22 \pmod{5}$, sest $5 \mid 15 = 22 - 7$ ehk $22 = 7 + 3 \cdot 5$.

Kuna mooduli 1 järgi on kõik täisarvud paarikaupa kongruentsed, siis see juhtum ei paku meile huvi. Edaspidises eeldame kongruentsidest kõneldes, et moodul n on vähemalt 2.

Lause 3.3. *Mistahes täisarvude a ja b korral $a \equiv b \pmod{n}$ parajasti siis, kui a ja b annavad arvuga n jäägiga jagamisel sama jäägi.*

Tõestus. Tarvilikkus. Olgu $a \equiv b \pmod{n}$, s.t. leidugu selline $k \in \mathbb{Z}$, et $b = a + kn$. Jagades a arvuga n, saame mingi jäägi r: $a = qn + r$, kus $0 \leqslant r < n$. Järelikult $b = a + kn = (qn + r) + kn = (q + k)n + r$, mis tähendabki, et b annab arvuga n jagades sama jäägi r, mis a.
Piisavus. Oletame, et $a = q_1 n + r$ ja $b = q_2 n + r$, kus $0 \leqslant r < n$. Siis $b - a = (q_2 n + r) - (q_1 n + r) = (q_2 - q_1)n$, kust saame, et $n \mid b - a$ ehk $a \equiv b \pmod{n}$. □

3.2. Jäägiklassid

Lausest 3.3 järeldub vahetult järgmine kongruentsusseose omadus.

Lause 3.4. *Täisarvude kongruentsusseos on ekvivalentsusseos.*

Tähistame sümboliga $\overline{a}$ kõigi selliste täisarvude hulga, mis on kongruentsed täisarvuga a mooduli n järgi, s.o.

$$\overline{a} = \{b \in \mathbb{Z} \mid a \equiv b \pmod{n}\} = \{a + kn \mid k \in \mathbb{Z}\},$$

ja nimetame selliseid hulki *jäägiklassideks* mooduli n järgi. Kongruentsusseose refleksiivsuse tõttu $a \in \overline{a}$.

Lause 3.5. *Iga $a, b \in \mathbb{Z}$ korral $\overline{a} = \overline{b}$ parajasti siis, kui $a \equiv b \pmod{n}$.*

Tõestus. Tarvilikkus. Kui $\overline{a} = \overline{b}$, siis $b \in \overline{a}$ ja järelikult $a \equiv b \pmod{n}$.
Piisavus. Kui $a \equiv b \pmod{n}$, siis $b \in \overline{a}$. Iga $c \in \mathbb{Z}$ korral, kui $c \in \overline{b}$, s.t. $b \equiv c \pmod{n}$, siis kongruentsusseose transitiivsuse tõttu ka $a \equiv c \pmod{n}$ ja $c \in \overline{a}$. Seega $\overline{b} \subseteq \overline{a}$. Analoogiliselt kehtib $\overline{a} \subseteq \overline{b}$ ning järelikult $\overline{a} = \overline{b}$. □

Lause 3.6. *Mooduli n järgi leidub täpselt n erinevat jäägiklassi.*

Tõestus. Vaatleme jäägiklasse $\overline{0}, \overline{1}, \ldots, \overline{n-1}$ mooduli n järgi. Kui $a \in \mathbb{Z}$ ja a jagamisel arvuga n tekib jääk r, s.t. $a = nq + r$, $0 \leqslant r < n$, siis $a \equiv r \pmod{n}$ ning lause 3.5 põhjal $\overline{a} = \overline{r}$. Seega iga jäägiklass mooduli n järgi on võrdne ühega jäägiklassidest $\overline{0}, \overline{1}, \ldots, \overline{n-1}$. Lause 3.3 tõttu iga $i, j \in \{0, 1, \ldots, n-1\}$ korral, kui $i \neq j$, siis $i \not\equiv j \pmod{n}$ (sest i ja j annavad arvuga n jagades erinevad jäägid i ja j) ning lause 3.5 tõttu siis ka $\overline{i} \neq \overline{j}$, s.t. jäägiklassid $\overline{0}, \overline{1}, \ldots, \overline{n-1}$ on kõik erinevad. □

3.3. Konguentsusseose omadused

Kongruentsusseost võib vaadelda kui võrdusseose üldistust: kui täisarvud on võrdsed, siis on nad kongruentsed, kuid mitte tingimata vastupidi. Sellegipoolest on kongruentsidel mitmed võrdustega sarnased omadused. Näiteks võib kongruentside vastavaid pooli omavahel liita ja korrutada.

Lause 3.7. *Kui $a_1 \equiv b_1 \pmod{n}$ ja $a_2 \equiv b_2 \pmod{n}$, siis $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$ ja $a_1 a_2 \equiv b_1 b_2 \pmod{n}$.*

Tõestus. Oletame, et $n \mid b_1 - a_1$ ja $n \mid b_2 - a_2$. Siis $n \mid (b_1 - a_1) + (b_2 - a_2) = (b_1 + b_2) - (a_1 + a_2)$, s.t. $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$. Et $b_1 b_2 - a_1 a_2 = b_1(b_2 - a_2) + a_2(b_1 - a_1)$, siis $n \mid b_1 b_2 - a_1 a_2$ ning järelikult $a_1 a_2 \equiv b_1 b_2 \pmod{n}$. □

Järeldus 3.8. *Kui $f(x)$ on täisarvuliste kordajatega polünoom ning $a \equiv b \pmod{n}$, siis $f(a) \equiv f(b) \pmod{n}$.*

TÕESTUS. Olgu $f(x) = a_m x^m + a_{m-1}x^{m-1} + \ldots + a_1 x + a_0$, kus $a_0, \ldots, a_m \in \mathbb{Z}$, ning olgu $a \equiv b \pmod{n}$. Kasutades lauset 3.7 saame, et iga $i = 1, \ldots, m$ korral $a^i \equiv b^i \pmod{n}$. Kuna $a_i \equiv a_i \pmod{n}$, siis jällegi lauset 3.7 kasutades saame, et $a_i a^i \equiv a_i b^i \pmod{n}$ iga $i = 1, \ldots, m$ korral. Siis aga ka

$$f(a) = a_m a^m + a_{m-1}a^{m-1} + \ldots + a_1 a + a_0 \equiv a_m b^m + a_{m-1}b^{m-1} + \ldots + a_1 b + a_0 = f(b) \pmod{n}.$$

□

Näide 3.9. Näitame, et polünoomil $x^2 - 117x + 31$ ei ole täisarvulisi juuri.

Vaatleme moodulit $n = 2$. Iga täisarvu a korral kas $a \equiv 0 \pmod 2$ või $a \equiv 1 \pmod 2$ ja seega, kui $f(x)$ on täisarvuliste kordajatega polünoom, siis järelduse 3.8 põhjal kas $f(a) \equiv f(0) \pmod 2$ või $f(a) \equiv f(1) \pmod 2$. Kui $f(x) = a_m x^m + a_{m-1}x^{m-1} + \ldots + a_1 x + a_0$, siis $f(0) = a_0$ ja $f(1) = a_m + a_{m-1} + \ldots + a_1 + a_0$. Järelikult, kui $f(x) \in \mathbb{Z}[x]$ ning $f(0)$ ja $f(1)$ on mõlemad paaritud arvud (s.o. kongruentsed 1-ga mooduli 2 järgi), siis polünoomil $f(x)$ ei ole täisarvulisi juuri, sest kui $a \in \mathbb{Z}$ oleks polünoomi $f(x)$ juur, siis oleks $f(a) = 0 \equiv 0 \pmod 2$.

Et 31 ja $1 - 117 + 31$ on paaritud arvud, siis polünoomil $x^2 - 117x + 31$ ei saa olla täisarvulisi juuri. Samamoodi ei saa täisarvulisi juuri olla ka näiteks polünoomidel $2x^2 - 2x + 1$ ja $3x^3 + 2x^2 + x + 3$.

Tõestame veel mõned kongruentsusseose omadused.

Lause 3.10. *Iga täisarvu $k \neq 0$ korral $a \equiv b \pmod{n}$ parajasti siis, kui $ka \equiv kb \pmod{kn}$.*

TÕESTUS. Olgu $k \neq 0$. Kasutades seda, et nullist erineva täisarvu võib võrduse mõlemalt poolelt taandada, saame

$$\begin{aligned} a \equiv b \pmod{n} &\iff n \mid b - a \iff (\exists c \in \mathbb{Z})(nc = b - a) \\ &\iff (\exists c \in \mathbb{Z})((kn)c = kb - ka) \iff kn \mid kb - ka \iff ka \equiv kb \pmod{kn}. \end{aligned}$$

□

Lause 3.11. *Kui $ka \equiv kb \pmod{n}$, siis $a \equiv b \pmod{\frac{n}{(k,n)}}$.*

TÕESTUS. Kui $d = (k, n)$, $n = dn'$ ja $k = dk'$, siis järelduse 1.9 põhjal $(n', k') = 1$. Kuna $n \mid kb - ka$, siis leidub selline $c \in \mathbb{Z}$, et $nc = kb - ka$. Asendades viimases võrduses n ja k saame võrduse $dn'c = dk'b - dk'a$. Et $n \neq 0$, siis ka $d \neq 0$ ning järelikult $n'c = k'b - k'a$. Sellest, et $n' \mid k'b - k'a = k'(b - a)$ ja $(n', k') = 1$, saame järeldust 1.10 kasutades, et $n' = \frac{n}{d} \mid b - a$, ehk $a \equiv b \pmod{\frac{n}{d}}$. □

Järeldus 3.12. *Kui $ka \equiv kb \pmod{n}$ ja $(k, n) = 1$, siis $a \equiv b \pmod{n}$.*

Näide 3.13. Sellest, et $33 \equiv 15 \pmod 9$ ja $(3, 9) = 3$, saame lause 3.11 põhjal, et $11 \equiv 5 \pmod 3$. Sellest, et $-35 \equiv 45 \pmod 8$ ja $(5, 8) = 1$, saame järelduse 3.12 põhjal, et $-7 \equiv 9 \pmod 8$.

3.4. Jaguvustunnused

Näitena kongruentsusseose omaduste rakendamisest vaatame, kuidas nende abil tuletada jaguvustunnuseid.

Lause 3.14. *Olgu*

$$n = a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + \ldots + a_1 \cdot 10 + a_0 = \underline{a_m a_{m-1} \ldots a_1 a_0}_{10},$$

kus $0 \leqslant a_i \leqslant 9$ ja $a_m \neq 0$ (s.o. n on arv, mille kümnendnumbreiks on $a_m, \ldots, a_0$). Siis

1. $3 \mid n \iff 3 \mid a_0 + a_1 + \ldots + a_m$;
2. $9 \mid n \iff 9 \mid a_0 + a_1 + \ldots + a_m$;
3. $11 \mid n \iff 11 \mid a_0 - a_1 + a_2 - \ldots + (-1)^m a_m$.

TÕESTUS. Vaatleme polünoomi $f(x) = a_m x^m + a_{m-1}x^{m-1} + \ldots + a_1 x + a_0$. Siis $n = f(10)$.
2. Kuna $10 \equiv 1 \pmod 9$, siis järelduse 3.8 põhjal $n = f(10) \equiv f(1) = a_0 + a_1 + \ldots + a_m \pmod 9$. Seega arvud n ja $a_0 + a_1 + \ldots + a_m$ annavad 9-ga jagades sama jäägi, muuhulgas n jagub 9-ga (s.o. annab jäägi 0) parajasti siis, kui $a_0 + a_1 + \ldots + a_m$ jagub 9-ga. Tunnuse 1 saab tõestada analoogiliselt.
3. Et $10 \equiv -1 \pmod{11}$, siis $n = f(10) \equiv f(-1) = a_0 - a_1 + a_2 - \ldots + (-1)^m a_m \pmod{11}$, millest järeldubki, et n jagub 11-ga parajasti siis, kui $a_0 - a_1 + a_2 - \ldots + (-1)^m a_m$ jagub 11-ga. □

Näide 3.15. Kuna $f(8) \equiv f(1) \pmod 7$, siis $7 \mid n \iff 7 \mid a_0 + a_1 + \ldots + a_m$, kui $n = \underline{a_m a_{m-1} \ldots a_1 a_0}_8$. Kuna $1000 \equiv -1 \pmod 7$, siis $7 \mid n \iff 7 \mid a_0 - a_1 + a_2 - \ldots + (-1)^m a_m$, kui $n = \underline{a_m a_{m-1} \ldots a_1 a_0}_{1000}$.

4. Jäägiklassiringid

4.1. Jäägiklassiringid ja nende otsekorrutised

Tähistame kõigi jäägiklasside hulka (mooduli $n > 1$ järgi) sümboliga $\mathbb{Z}_n$, s.t.

$$\mathbb{Z}_n = \{\overline{a} \mid a \in \mathbb{Z}\} = \left\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\right\}.$$

Selle hulga saame muuta kommutatiivseks ringiks (s.t. hulgaks, millel on defineeritud liitmis- ja korrutamistehe nii, et selle hulga elemendid rahuldavad tingimusi Z1–Z8) defineerides liitmise ja korrutamise võrdustega

$$\begin{aligned} \overline{a} + \overline{b} &= \overline{a+b}, \\ \overline{a}\overline{b} &= \overline{ab}, \end{aligned}$$

iga $\overline{a}, \overline{b} \in \mathbb{Z}_n$ korral. Lausest 3.7 järeldub, et need definitsioonid on korrektsed, s.t. ei sõltu jäägiklasside esindajate valikust. Ringi definitsiooni tingimuste täidetus järeldub täisarvude vastavatest omadustest. Ringi $\mathbb{Z}_n$ nimetatakse *jäägiklassiringiks* mooduli n järgi.

Edaspidises läheb vaja kahte lemmat.

Lemma 4.1. *Kui arvud $n_1, \ldots, n_s, n \in \mathbb{N}$ on sellised, et iga $i = 1, \ldots, s$ korral $(n_i, n) = 1$, siis $(n_1 \ldots n_s, n) = 1$.*

TÕESTUS. Oletame, et $(n_1 \ldots n_s, n) = d > 1$. Siis leidub selline algarv p, et $p \mid d$ ning seega $p \mid n_1 \ldots n_s$ ja $p \mid n$. Järelduse 1.12 põhjal peab leiduma selline i, et $p \mid n_i$. Siis aga $p \mid (n_i, n)$, mis on vastuolus sellega, et $(n_i, n) = 1$. □

Lemma 4.2. *Kui arvud $n_1, \ldots, n_s, a \in \mathbb{N}$ on sellised, et iga $i = 1, \ldots, s$ korral $n_i \mid a$ ja iga $i, j \in \{1, \ldots, s\}$, $i \neq j$, korral $(n_i, n_j) = 1$, siis $n_1 \ldots n_s \mid a$.*

TÕESTUS. Tõestame selle väite induktsiooniga s järgi. Kui $s = 1$, siis on kõik korras. Oletame nüüd, et $s > 1$ ning et $s - 1$ korral väide kehtib. Siis $n_1 \ldots n_{s-1} \mid a$. Lemma 4.1 põhjal $(n_1 \ldots n_{s-1}, n_s) = 1$. Järelikult teoreemi 1.7 põhjal leiduvad sellised täisarvud x ja y, et $n_1 \ldots n_{s-1}x + n_s y = 1$. Korrutades viimase võrduse mõlemaid pooli arvuga a saame $n_1 \ldots n_{s-1}ax + n_s ay = a$. Näeme, et $n_1 \ldots n_s$ jagab selle võrduse vasakut poolt ja seega peab jagama ka paremat poolt ehk arvu a. □

Viimasest lemmast saame teha ühe kasuliku järelduse.

Järeldus 4.3. *Olgu a täisarv ja olgu naturaalarv $n = p_1^{k_1} \ldots p_s^{k_s} > 1$ antud standardkujul. Siis $n \mid a$ parajasti siis, kui $p_i^{k_i} \mid a$ iga $i \in \{1, \ldots, s\}$ korral.*

TÕESTUS. Tarvilikkus on ilmne. Piisavus järeldub lemmast 4.2, sest $i \neq j$ korral $\left(p_i^{k_i}, p_j^{k_j}\right) = 1$. □

Näide 4.4. Teeme kindlaks, kas arv $n = 1234567887654321$ jagub 99-ga.

Kuna $99 = 3^2 \cdot 11$, siis tänu järeldusele 4.3 piisab, kui kontrollida n jagumist 9 ja 11-ga. Et arvu n ristsumma (kõigi numbrite summa) $2(1+2+\ldots+8) = 2 \cdot 4 \cdot 9 = 72$ jagub 9-ga ja arv $1-2+3-4+5-6+7-8+8-7+6-5+4-3+2-1 = 0$ jagub 11-ga, siis lause 3.14 ja järelduse 4.3 põhjal n jagub 99-ga.

Jäägiklassiringide uurimisel kasutame mõningaid ringide üldisi omadusi, andes ka nende omaduste tõestused üldjuhul.

Meenutame, kuidas defineeritakse ringide $R_1, \ldots, R_s$ otsekorrutis $R_1 \times \ldots \times R_s$. Nimelt võetakse hulkade $R_1, \ldots, R_s$ otsekorrutis

$$R_1 \times \ldots \times R_s = \{(r_1, \ldots, r_s) \mid r_i \in R_i\}$$

ja defineeritakse sellel hulgal tehted komponentide kaupa, s.t.

$$\begin{aligned} (r_1, \ldots, r_s) + (r_1', \ldots, r_s') &= (r_1 + r_1', \ldots, r_s + r_s'), \\ (r_1, \ldots, r_s)(r_1', \ldots, r_s') &= (r_1 r_1', \ldots, r_s r_s'). \end{aligned}$$

Tulemuseks on ring, mille nullelemendiks on $(0, \ldots, 0)$, kus elemendi $(r_1, \ldots, r_s)$ vastandelemendiks on element $(-r_1, \ldots, -r_s)$ ning ühikelemendiks on $(1, \ldots, 1)$.

Teoreem 4.5. *Kui arvud $n_1, \ldots, n_s \in \mathbb{N}$ on paarikaupa ühistegurita ja $n = n_1 \ldots n_s$, siis ringid $\mathbb{Z}_n$ ja $\mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_s}$ on isomorfsed.*

TÕESTUS. Defineerime kujutuse $f : \mathbb{Z}_n \longrightarrow \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_s}$ järgmiselt:

$$f(\overline{a}) = (\overline{a}_1, \ldots, \overline{a}_s)\,,$$

mistahes $\overline{a} \in \mathbb{Z}_n$ korral, kus $\overline{a}_i$ on arvu a jäägiklass mooduli n_i järgi.

Veendume, et f on korrektselt defineeritud. Selleks oletame, et $\overline{a} = \overline{b}$, s.t. $n \mid b - a$. Et $n_i \mid n$, $i = 1, \ldots, s$, siis jaguvusseose transitiivsuse tõttu $n_i \mid b - a$, s.t. $\overline{a}_i = \overline{b}_i$ ja $(\overline{a}_1, \ldots, \overline{a}_s) = (\overline{b}_1, \ldots, \overline{b}_s)$.

Näitame, et f on injektiivne. Selleks oletame, et $f(\overline{a}) = f(\overline{b})$, see tähendab, et $(\overline{a}_1, \ldots, \overline{a}_s) = \left(\overline{b}_1, \ldots, \overline{b}_s\right)$. Siis $\overline{a}_i = \overline{b}_i$, millest järeldub, et $n_i \mid b - a$ iga $i = 1, \ldots, s$ korral. Et arvud $n_1, \ldots, n_s$ on paarikaupa ühistegurita, siis lemma 4.2 põhjal $n \mid b - a$ ehk $\overline{a} = \overline{b}$.

Sellest, et f on injektiivne ja $|\mathbb{Z}_n| = n = n_1 \ldots n_s = |\mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_s}|$, järeldub, et f on sürjektiivne.

Arvestades, et tehted ringide otsekorrutisel on defineeritud komponenthaaval, saame, et

$$\begin{aligned} f(\overline{a} + \overline{b}) &= f(\overline{a+b}) = \left(\overline{a+b}_1, \ldots, \overline{a+b}_s\right) = \left(\overline{a}_1 + \overline{b}_1, \ldots, \overline{a}_s + \overline{b}_s\right) \\ &= (\overline{a}_1, \ldots, \overline{a}_s) + \left(\overline{b}_1, \ldots, \overline{b}_s\right) = f\left(\overline{a}\right) + f\left(\overline{b}\right) \end{aligned}$$

ja analoogiliselt $f\left(\overline{a}\overline{b}\right) = f\left(\overline{a}\right) f\left(\overline{b}\right)$. Lisaks sellele $f(\overline{1}) = (\overline{1}_1, \ldots, \overline{1}_s)$.

Seega f on ringide isomorfism. □

Näide 4.6. Teoreemi 4.5 põhjal $\mathbb{Z}_{12} \cong \mathbb{Z}_4 \times \mathbb{Z}_3$. Üheks isomorfismiks $f : \mathbb{Z}_{12} \to \mathbb{Z}_4 \times \mathbb{Z}_3$ on kujutus, mis on defineeritud tabeliga

a	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$	$\overline{10}$	$\overline{11}$
$f(a)$	$(\overline{0},\overline{0})$	$(\overline{1},\overline{1})$	$(\overline{2},\overline{2})$	$(\overline{3},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{1},\overline{2})$	$(\overline{2},\overline{0})$	$(\overline{3},\overline{1})$	$(\overline{0},\overline{2})$	$(\overline{1},\overline{0})$	$(\overline{2},\overline{1})$	$(\overline{3},\overline{2})$

4.2. Jäägiklassiringi pööratavad elemendid

Ringi elementi nimetatakse *pööratavaks*, kui tal leidub korrutamise suhtes pöördelement. Kui $ax = xa = 1$ ringis R, siis elemente a ja x nimetatakse teineteise *pöördelementideks* ja tihti kirjutatakse $x = a^{-1}$ (või $a = x^{-1}$). Ringi R kõigi pööratavate elementide hulka tähistatakse $U(R)$, vahel ka R^*. Niisiis

$$U(R) = \{a \in R \mid (\exists x \in R)(ax = xa = 1)\}.$$

Kui $U(R) = R \setminus \{0\}$, siis ringi R nimetatakse *korpuseks*. Seega *jäägiklassikorpus* on jäägiklassiring, mille iga nullelemendist (s.o. jäägiklassist $\overline{0}$) erinev element on pööratav.

Lause 4.7. *Ringi R pööratavate elementide hulk $U(R)$ on rühm korrutamise suhtes.*

TÕESTUS. Olgu $a, b \in U(R)$. Siis leiduvad sellised $x, y \in R$, et $ax = xa = 1$ ja $by = yb = 1$. Järelikult $(ab)(yx) = a(by)x = ax = 1$ ja $(yx)(ab) = y(xa)b = yb = 1$, s.t. $ab \in U(R)$. Seega korrutamine on algebraline tehe hulgal $U(R)$. Korrutamine on assotsiatiivne kogu ringil, seega ka hulgal $U(R)$. Lisaks sellele $1 \in U(R)$ ja $U(R)$ iga elemendi pöördelement on samuti pööratav. □

Lause 4.8. *Kui $f : R \to S$ on ringide R ja S isomorfism, siis $f(U(R)) = U(S)$. Seega kujutus $U(R) \to U(S)$, $a \mapsto f(a)$ on rühmade isomorfism.*

TÕESTUS. Olgu $a \in U(R)$, s.t. leidub $x \in R$, nii et $ax = xa = 1$. Näitame, et $f(a) \in U(S)$. Tõepoolest, $f(a)f(x) = f(ax) = f(1) = 1$ ja analoogiliselt $f(x)f(a) = 1$. Seega $f(U(R)) \subseteq U(S)$.

Olgu nüüd $u \in U(S)$, s.t. leidub $v \in S$ nii, et $uv = vu = 1$. Kujutuse f sürjektiivsuse tõttu leiduvad $a, b \in R$ nii, et $f(a) = u$ ja $f(b) = v$. Seega $f(1) = 1 = uv = f(a)f(b) = f(ab)$. Kujutuse f injektiivsusest järeldub, et $ab = 1$. Analoogiliselt $ba = 1$, mis tähendab, et $a \in U(R)$ ja seega $u = f(a) \in f(U(R))$. Järelikult ka $U(S) \subseteq f(U(R))$. □

Teoreemist 4.5 ja lausest 4.8 saame järgmise väite.

Järeldus 4.9. *Kui arvud $n_1, \ldots, n_s \in \mathbb{N}$ on paarikaupa ühistegurita ja $n = n_1 \ldots n_s$, siis rühmad $U(\mathbb{Z}_n)$ ja $U(\mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_s})$ on isomorfsed.*

Leiame ringi $\mathbb{Z}_n$ pööratavad elemendid.

Teoreem 4.10. *Iga $n > 1$ korral*

$$U(\mathbb{Z}_n) = \{\overline{a} \in \mathbb{Z}_n \mid (a, n) = 1\}.$$

Tõestus. Olgu $\overline{a} \in \mathbb{Z}_n$ pööratav, s.t. leidugu selline $\overline{b}$, et $\overline{1} = \overline{a} \cdot \overline{b} = \overline{ab}$. Lause 3.5 põhjal tähendab see seda, et $ab \equiv 1 \pmod{n}$. Järelikult leidub selline $k \in \mathbb{Z}$, et $ab = 1 + kn$ ehk $ab - kn = 1$. Teoreemi 1.7 tõttu siis $(a, n) = 1$. Seega $U(\mathbb{Z}_n) \subseteq \{\overline{a} \in \mathbb{Z}_n \mid (a, n) = 1\}$.

Tõestame vastupidise sisalduvuse. Olgu $(a, n) = 1$. Siis teoreemi 1.7 põhjal leiduvad sellised $x, y \in \mathbb{Z}$, et $ax + ny = 1$. Järelikult

$$\overline{1} = \overline{ax + ny} = \overline{ax} + \overline{ny} = \overline{a} \cdot \overline{x} + \overline{0} \cdot \overline{y} = \overline{a} \cdot \overline{x}.$$

See tähendab, et $\overline{a}$ on pööratav ja seega $\{\overline{a} \in \mathbb{Z}_n \mid (a, n) = 1\} \subseteq U(\mathbb{Z}_n)$. □

Järeldus 4.11. *Jäägiklassiring $\mathbb{Z}_n$ on korpus parajasti siis, kui n on algarv.*

Näide 4.12. Ringi $\mathbb{Z}_9$ pööratavate elementide hulk

$$U(\mathbb{Z}_9) = \{\overline{a} \in \mathbb{Z}_9 \mid (a, 9) = 1\} = \left\{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}\right\}.$$

Seejuures $\overline{1}^{-1} = \overline{1}$, $\overline{2}^{-1} = \overline{5}$ (ja seega $\overline{5}^{-1} = \overline{2}$), $\overline{4}^{-1} = \overline{7}$ ja $\overline{8}^{-1} = \overline{8}$.

Näide 4.13. Tänu lausele 4.8 on rühm

$$U(\mathbb{Z}_{12}) = \{\overline{1}, \overline{5}, \overline{7}, \overline{11}\}$$

isomorfne rühmaga

$$U(\mathbb{Z}_4 \times \mathbb{Z}_3) = \{(\overline{1}, \overline{1}), (\overline{1}, \overline{2}), (\overline{3}, \overline{1}), (\overline{3}, \overline{2})\}.$$

Definitsioon 4.14. *Ringi R elementi $r \neq 0$ nimetatakse* nulliteguriks*, kui leidub teine selle ringi element $s \neq 0$ nii, et $rs = 0$.*

Lause 4.15. *Jäägiklassiringi $\mathbb{Z}_n$ iga element on kas $\overline{0}$, pööratav või nullitegur.*

Tõestus. Ilmselt väide kehtib, kui jäägiklassiring $\mathbb{Z}_n$ sisaldab vaid nullelementi ja pööratavaid elemente (sel juhul on meil tegu jäägiklassikorpusega). Oletame nüüd, et jäägiklassiringis $\mathbb{Z}_n$ leidub nullist erinevaid mittepööratavaid elemente. Fikseerime vabalt ühe sellise, näiteks $\overline{a} \in \mathbb{Z}_n$. Tõestuse lõpetamiseks piisab, kui me näitame, et $\overline{a}$ on nullitegur. Kuna $\overline{a}$ ei ole pööratav, siis teoreemi 4.10 põhjal $(a, n) > 1$ (juht $(a, n) = 0$ ei ole võimalik, sest $n > 0$). Tähistame $d = (a, n)$, $n' = \frac{n}{d}$ ja $a' = \frac{a}{d}$. Paneme tähele, et $d > 1$ tõttu $1 \leq n' < n$. Järelikult $\overline{n'} \neq \overline{0}$. Samas

$$\overline{a} \cdot \overline{n'} = \overline{a'd} \cdot \overline{n'} = \overline{a'} \cdot \overline{dn'} = \overline{a'} \cdot \overline{n} = \overline{a'} \cdot \overline{0} = \overline{0},$$

ehk $\overline{a}$ on tõepoolest nullitegur.

□

Indeks

Kirjandus

[1] M. Kilp, *Algebra I*, Eesti Matemaatika Selts, Tartu, 2005.

[2] L. Kivistik, J. Gabovitš, *Arvuteooria*, Tartu, 1974.

[3] E. Redi, *Arvuteooria*, Avita, Tallinn, 1998.

[4] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer Verlag, second edition, 1990.

[5] D. Burton, *Elementary Number Theory*, Brown, 1989.

[6] G. H. Hardy, E. M. Wright, *An Introduction to the Theory of Numbers*, fifth edition, Clarendon Press, Oxford, 1979.

[7] M. Edwards, *Fermat's Last Theorem*, Springer-Verlag, 1977.

[8] N. Koblitz, *A Course in Number Theory and Cryptography*, Springer-Verlag, 1987.

[9] H.-D. Ebbinghaus, H. Hermes, F. Hirzebruch, M. Koecher, K. Mainzer, J. Neukirch, A. Prestel, R. Remmert, *Numbers*, Springer-Verlag, 1990.

[10] N. Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, Springer-Verlag, 1997.

[11] M. Kilp, *Algebra II*, Tartu, 1998.

[12] G. Kangro, *Kõrgem algebra II*, Eesti Riiklik Kirjastus, Tartu, 1950.

[13] Р. Лидл, Г. Нидеррайтер, *Конечные поля I, II*, Мир, Москва, 1988.

[14] R. Lidl, H. Niederreiter, *Finite Fields*, second edition, Cambridge University Press, 1997.

[15] I. Niven, H. S. Zuckerman, H. L. Montgomery, *An Introduction to the Theory of Numbers*, fifth edition, Wiley, 1991.

[16] V. Shoup, *A Computational Introduction to Number Theory and Algebra*, Cambridge University Press, 2005, http://www.shoup.net/ntb/ .

Lisa 1

Abstraktse algebra põhimõisteid

Definitsioon. Olgu A mittetühi hulk ja $n \in \mathbb{N} \cup \{0\}$. Kujutust $\omega : A^n \to A$ nimetatakse *n-kohaliseks algebraliseks tehteks* hulgal A.

Definitsioon. *Rühmaks* nimetatakse hulka A, millel on defineeritud üks kahekohaline tehe $*$ (tähistame $*(a,b) = a * b$), nii et

G1. $(\forall a, b, c \in A)((a * b) * c = a * (b * c))$ (assotsiatiivsus);

G2. $(\exists e \in A)(\forall a \in A)(a * e = e * a = a)$ (leidub *ühikelement*);

G3. $(\forall a \in A)(\exists a^{-1} \in A)(a * a^{-1} = a^{-1} * a = e)$ (igal elemendil leidub *pöördelement*).

Öeldakse, et A on rühm tehte $*$ suhtes ja kirjutatakse $(A, *)$.

Kui hulgal A on defineeritud kahekohaline tehe, mis on assotsiatiivne, siis A on *poolrühm*. Kui poolrühmas leidub ühikelement, siis teda nimetatakse *monoidiks*.

Kahekohaline tehe $*$ hulgal A on *kommutatiivne*, kui kehtib samasus

COMM. $(\forall a, b \in A)(a * b = b * a)$.

Rühma, mille tehe on kommutatiivne, nimetatakse *kommutatiivseks* ehk *Abeli rühmaks*.

Tihti tähistatakse Abeli rühma tehet märgiga "+" ja nimetatakse liitmiseks. Sellisel juhul võtavad Abeli rühma aksioomid järgmise kuju:

AG1. $(\forall a, b, c \in A)((a + b) + c = a + (b + c))$ (assotsiatiivsus);

AG2. $(\exists 0 \in A)(\forall a \in A)(a + 0 = a)$ (leidub *nullelement*);

AG3. $(\forall a \in A)(\exists -a \in A)(a + (-a) = 0)$ (igal elemendil leidub *vastandelement*);

AG4. $(\forall a, b \in A)(a + b = b + a)$ (kommutatiivsus).

Definitsioon. *Ringiks* nimetatakse hulka R, millel on defineeritud kaks kahekohalist tehet, $+$ (liitmine) ja $\cdot$ (korrutamine), nii et

R1. $(R, +)$ on Abeli rühm;

R2. $(R, \cdot)$ on monoid;

R3. $(\forall a, b, c \in R)(a \cdot (b + c) = a \cdot b + a \cdot c$ ja $(a + b) \cdot c = a \cdot c + b \cdot c)$ (distributiivsus).

(Tihti defineeritakse ringid ilma nõudeta R2. Sellisel juhul kutsutakse meie poolt vaadeldavaid ringe assotsiatiivseteks ühikelemendiga ringideks.) (Kui mingis algebralises struktuuris kõneldakse korrutamistehtest $\cdot$, siis enamasti jäetakse tehtemärk ära ning kirjutatakse $a \cdot b$ asemel lihtsalt ab.)

Definitsioon. Ringi $(R, +, \cdot)$ nimetatakse *korpuseks*, kui igal nullist erineval elemendil on olemas pöördelement. Sel juhul $(R \setminus \{0\}, \cdot)$ on rühm.

Ringi (korpust) nimetatakse *kommutatiivseks*, kui tema korrutamine on kommutatiivne.

Ringi R nullist erinevat elementi a nimetatakse *nulliteguriks*, kui leidub selline nullist erinev element $b \in R$, et $ab = 0$.

Lause. Korpuses ei ole nullitegureid.

Definitsioon. *Vektorruumiks* üle korpuse K nimetatakse mittetühja hulka V, millel on defineeritud üks kahekohaline tehe $+$ (liitmine) ning iga $k \in K$ ja $a \in V$ korral on defineeritud korrutis $ka \in V$, nii et

VS1. $(V, +)$ on Abeli rühm;

VS2. $(\forall a, b \in V)(\forall k \in K)(k(a + b) = ka + kb)$;

VS3. $(\forall a \in V)(\forall k, l \in K)((k + l)a = ka + la)$;

VS4. $(\forall a \in V)(\forall k, l \in K)((kl)a = k(la))$;

VS5. $(\forall a \in V)(1a = a)$.

Vektorruumi V elemente kutsutakse *vektoriteks* ning korpuse K elemente *skalaarideks*.

Definitsioon. Olgu G_1 ja G_2 rühmad. Kujutust $\varphi : G_1 \to G_2$ nimetatakse (rühmade) *homomorfismiks*, kui

HG. $(\forall a, b \in G_1)(\varphi(ab) = \varphi(a)\varphi(b))$. (korrutamise säilitamine)

Definitsioon. Olgu R_1 ja R_2 ringid ühikelementidega 1 ja $1'$, vastavalt. Kujutust $\varphi : R_1 \to R_2$ nimetatakse (ringide) *homomorfismiks*, kui

HR1. $(\forall a, b \in R_1)(\varphi(a + b) = \varphi(a) + \varphi(b))$; (liitmise säilitamine)

HR2. $(\forall a, b \in R_1)(\varphi(ab) = \varphi(a)\varphi(b))$; (korrutamise säilitamine)

HR3. $\varphi(1) = 1'$. (ühikelemendi säilitamine)

Definitsioon. Olgu V_1 ja V_2 vektorruumid üle korpuse K. Kujutust $\varphi : V_1 \to V_2$ nimetatakse (vektorruumide) *homomorfismiks* ehk *lineaarkujutuseks*, kui

HVS1. $(\forall a, b \in V_1)(\varphi(a + b) = \varphi(a) + \varphi(b))$; (liitmise säilitamine)

HVS2. $(\forall a \in V_1)(\forall k \in K)(\varphi(ka) = k\varphi(a))$. (skalaariga korrutamise säilitamine)

Algebraliste struktuuride *isomorfismiks* nimetatakse nende bijektiivset homomorfismi. Kui leidub isomorfism ühest algebralisest struktuurist teise, siis neid struktuure nimetatakse *isomorfseteks*. Korpusi loetakse isomorfseteks, kui nad on isomorfsed kui ringid.

Definitsioon. Olgu $(G, \cdot)$ rühm. Mittetühja hulka $H \subseteq G$ nimetatakse rühma G *alamrühmaks*, kui

SG1. $(\forall a, b \in H)(ab \in H)$; (kinnisus korrutamise suhtes)

SG2. $(\forall a \in H)(a^{-1} \in H)$. (kinnisus pöördelemendi võtmise suhtes)

Kui a on rühma G mingi fikseeritud element, siis hulk $\langle a \rangle = \{\ldots, a^{-2}, a^{-1}, 1 = a^0, a, a^2, \ldots\} \subseteq G$ on rühma G alamrühm. Seda alamrühma nimetatakse *elemendi a poolt moodustatud (tekitatud) alamrühmaks*. Kui see rühm on lõpmatu, siis öeldakse, et element a on *lõpmatut järku*. Kui aga see rühm on lõplik, siis leidub selline naturaalarv m, et $\langle a \rangle = \{a, a^2, \ldots, a^{m-1}, a^m = 1\}$. Kui m on vähim sellise omadusega naturaalarv, siis öeldakse, et elemendi a *järk* rühmas G on m ning tähistatakse $\mathrm{ord}_G(a) = m$. Kui rühm G on moodustatud ühe elemendi poolt, s.t. kui $G = \langle a \rangle$, siis öeldakse, et rühm G on *tsükliline*.

Lõpliku rühma *järguks* nimetatakse tema elementide arvu. Seega elemendi järk on tema poolt moodustatud alamrühma järk.

Lagrange'i teoreem. Lõpliku rühma mistahes alamrühma järk on selle rühma järgu jagaja. Muuhulgas lõpliku rühma iga elemendi järk on selle rühma järgu jagaja.

Definitsioon. Olgu $(R, +, \cdot)$ ring ühikelemendiga 1. Mittetühja alamhulka $R' \subseteq R$ nimetatakse ringi R *alamringiks*, kui

SR1. $(\forall a, b \in R')(a + b \in R')$; (kinnisus liitmise suhtes)

SR2. $(\forall a \in R')(-a \in R')$; (kinnisus vastandelemendi võtmise suhtes)

SR3. $(\forall a, b \in R')(ab \in R')$; (kinnisus korrutamise suhtes)

SR4. $1 \in R'$. (kinnisus ühikelemendi suhtes)

Definitsioon. Olgu $(K, +, \cdot)$ korpus. Mittetühja alamhulka $K' \subseteq K$ nimetatakse korpuse K *alamkorpuseks*, kui

SF1. $(\forall a, b \in K')(a + b \in K')$; (kinnisus liitmise suhtes)

SF2. $(\forall a \in K')(-a \in K')$; (kinnisus vastandelemendi võtmise suhtes)

SF3. $(\forall a, b \in K')(ab \in K')$; (kinnisus korrutamise suhtes)

SF4. $(\forall a \in K' \setminus \{0\})(a^{-1} \in K')$. (kinnisus pöördelemendi võtmise suhtes)

Definitsioon. Olgu V vektorruum. Mittetühja alamhulka $U \subseteq V$ nimetatakse vektorruumi V *alamruumiks*, kui

SVS1. $(\forall a, b \in U)(a + b \in U)$; (kinnisus liitmise suhtes)

SVS2. $(\forall a \in U)(\forall k \in K)(ka \in U)$. (kinnisus skalaariga korrutamise suhtes)

Definitsioon. Rühma G alamrühma N nimetatakse *normaalseks alamrühmaks* ehk *normaaljagajaks*, kui

NSG. $(\forall a \in G)(\forall b \in N)(a^{-1}ba \in N)$.

Kommutatiivses rühmas on iga alamrühm normaalne.

Olgu N rühma G normaaljagaja. Alamhulki $aN = \{ab \mid b \in N\}$, kus $a \in G$, nimetatakse *kõrvalklassideks* normaaljagaja N järgi. Tähistame kõigi kõrvalklasside hulga $\{aN \mid a \in G\} = G/N$ ning defineerime sellel hulgal korrutamistehte võrdusega

$$(a_1N)(a_2N) = a_1a_2N.$$

Saab näidata, et G/N on rühm selle tehte suhtes. Seda rühma G/N nimetatakse rühma G *faktorrühmaks* normaaljagaja N järgi.

Definitsioon. Ringi R mittetühja alamhulka I nimetatakse *ideaaliks*, kui

I1. $(\forall a, b \in I)(a + b \in I)$;

I2. $(\forall a \in R)(\forall i \in I)(ai, ia \in I)$.

Olgu I ringi R ideaal. Alamhulki $a + I = \{a + i \mid i \in I\}$, kus $a \in R$, nimetatakse *kõrvalklassideks* ideaali I järgi. Lihtne on näha, et iga $a, b \in \mathbb{R}$ korral $a + I = b + I$ parajasti siis, kui $a - b \in I$. Tähistame kõigi kõrvalklasside hulga $\{a + I \mid a \in R\} = R/I$ ning defineerime sellel hulgal korrutamis- ja liitmistehte võrdustega

$$(a_1 + I) + (a_2 + I) = (a_1 + a_2) + I;$$
$$(a_1 + I)(a_2 + I) = (a_1a_2) + I.$$

Saab näidata, et R/I on ring nende tehete suhtes. Seda ringi R/I nimetatakse ringi R *faktorringiks* ideaali I järgi.