ARVUTEOORIA

Kevad 2018

Loengukonspekt

Lektor: Lauri Tart

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

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:

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

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. 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 $c \mid d$.

Definitsioon 1.4. 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 $m \mid c$.

Lihtne on veenduda, et kui d on a ja b suurim ühistegur (vähim ühiskordne), siis ka $-d$ on a ja b suurim ühistegur (vähim ühiskordne) ja rohkem suurimaid ühistegureid (vähimaid ühiskordseid) arvudel a ja b ei ole. Teiste sõnadega, suurim ühistegur ja vähim ühiskordne on määratud üheselt märgi täpsusega. Muuhulgas tähendab see seda, et mistahes suurimat ühistegurit või vähimat ühiskordset sisaldavate avaldiste võrdust tuleb tõlgendada märgi täpsusega. Kui a ja b suurim ühistegur on 1, siis öeldakse tihti, et a ja b on *ühistegurita*.

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 $a \mid b$. 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.

$$\begin{array}{rcll} a & = & bq_1 + r_1, & 0 < r_1 < b, \\ b & = & r_1 q_2 + r_2, & 0 < r_2 < r_1, \\ r_1 & = & r_2 q_3 + r_3, & 0 < r_3 < r_2, \\ & \ldots & & \ldots \\ r_{n-3} & = & r_{n-2} q_{n-1} + r_{n-1} & 0 < r_{n-1} < r_{n-2}, \\ r_{n-2} & = & r_{n-1} q_n + r_n & 0 < r_n < r_{n-1}, \\ r_{n-1} & = & r_n q_{n+1} + 0. & \end{array} \tag{1}$$

Järeldus 1.7 (Bezout' lemma). *Olgu a ja b täisarvud. Siis leiduvad täisarvud x' ja y' nii, et $(a, b) = x'a + y'b$.*

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 1.8. *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. Järelduse 1.7 kohaselt leiduvad $x', y' \in \mathbb{Z}$ nii, et

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

Seega $a(x's) + b(y's) = (ax' + by')s = (a, b)\, s = c$, s.t. täisarvupaar $x's, y's$ on võrrandi (2) lahend. □

Teoreemist 1.8 saab teha mitmeid kasulikke järeldusi.

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

$$\begin{aligned} d' = d \quad &\iff \quad d' \mid d \underset{\text{Teor. 1.8}}{\iff} (\exists x_0, y_0 \in \mathbb{Z})(ax_0 + by_0 = d) \iff (\exists x_0, y_0 \in \mathbb{Z}) \left(\frac{a}{d}x_0 + \frac{b}{d}y_0 = 1\right) \\ &\underset{\text{Teor. 1.8}}{\iff} \left(\frac{a}{d}, \frac{b}{d}\right) \mid 1 \underset{\text{Lause 1.2(4)}}{\iff} \left(\frac{a}{d}, \frac{b}{d}\right) = 1. \end{aligned}$$

□

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 $p \mid a_1a_2 \ldots a_n$, 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 $p \mid q_1q_2 \ldots q_n$, 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 1.8 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. *$(cm, cn) = c(m, n)$ iga $c \in \mathbb{Z}$ korral;*
5. *$[cm, cn] = c\,[m, n]$ 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 8.10) 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

$$\pi(n) \approx \frac{n}{\ln(n)} \text{ , kui } n \to \infty, \qquad \text{ehk} \qquad \lim_{n\to\infty} \frac{\pi(n)}{n/\ln(n)} = 1.$$

Lisaks võib tähele panna, et $2n$-kohalisi algarve on suhteliselt umbes kaks korda vähem, kui n-kohalisi algarve, sest

$$\frac{\pi(10^{2n})/10^{2n}}{\pi(10^n)/10^n} \approx \frac{\frac{1}{\ln(10^{2n})}}{\frac{1}{\ln(10^n)}} = \frac{n \cdot \ln(10)}{2n \cdot \ln(10)} = \frac{1}{2}.$$

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 $f(n) = \left\lfloor \theta^{3^n} \right\rfloor$ 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.

Funktsioonide $\pi(n)$ ja p_n väärtusi ning mitmesuguseid algarve genereerivaid valemeid, funktsioone või seoseid on leitud ka varem ja hiljem, ning nende otsimist jätkatakse tänapäevalgi. Kahjuks on kõik need vähemalt seniajani praktiliseks kasutuseks täiesti ebasobivateks osutunud.

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:

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

Kui Goldbachi hüpotees peaks paika pidama, siis kehtiks ka nn. *nõrk Goldbachi hüpotees*: iga 5-st suurema paaritu arvu saab esitada kolme paaritu algarvu summana. Nimelt, kui n on 5-st suurem paaritu arv, siis $n-3$ on paarisarv ja suurem kui 2. Kui $n-3$ saaks esitada kahe paaritu algarvu summana, siis n oleks kolme paaritu algarvu summa. Sellest omakorda järeldub, et kõik piisavalt suured paarisarvud on esitatavad ülimalt 4 paaritu algarvu summana. Nõrga Goldbachi hüpoteesi kehtivuse tõestas 2013. aastal Peruu matemaatik Harald Helfgott (sünd. 1977).

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 2.12 (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*

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

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. □

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 1.8 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 1.8 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 1.8 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 $\{\overline{a} \in \mathbb{Z}_n \mid (a, n) = 1\} \subseteq U(\mathbb{Z}_n)$. □

Näide 4.11. 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 4.12. Tänu lausele 4.8 on rühm

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

isomorfne rühmaga

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

Lause 4.13. *Jäägiklassiring $\mathbb{Z}_n$ on korpus parajasti siis, kui n on algarv.*

Tõestus. Tarvilikkus. Oletame, et $\mathbb{Z}_n$ on korpus, kuid n ei ole algarv, s.t. leiduvad sellised $a, b \in \mathbb{N}$, $1 < a, b < n$, et $n = ab$. Siis $\overline{a} \cdot \overline{b} = \overline{n} = \overline{0}$, kuid $\overline{a} \neq \overline{0}$ ja $\overline{b} \neq \overline{0}$. Korpuse igal nullist erineval elemendil on olemas pöördelement. Korrutades võrduse $\overline{a} \cdot \overline{b} = \overline{0}$ mõlemad pooled elemendiga $\overline{a}^{-1}$ saame, et $\overline{b} = \overline{0}$, vastuolu. Seega n on algarv.
Piisavus. Olgu n algarv. Siis iga $a \in \mathbb{Z}$ korral kas $(a, n) = 1$ või $(a, n) = n$. Viimasel juhul $n \mid a$ ja $\overline{a} = \overline{0}$. Seega kui $\overline{a} \in \mathbb{Z}_n \setminus \left\{\overline{0}\right\}$, siis $(a, n) = 1$ ja $\overline{a} \in U(\mathbb{Z}_n)$. Kuna iga nullist erinev element on pööratav, siis $\mathbb{Z}_n$ on korpus. □

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.

□

5. Arvuteoreetilisi funktsioone

5.1. Euleri funktsioon

Üks tähtsam arvuteoreetiline funktsioon on Euleri funktsioon, mis loetleb, kui palju on antud naturaalarvust väiksemaid ja selle arvuga ühistegurita naturaalarve.

Definitsioon 5.1. *Euleri funktsioon* $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ defineeritakse võrdusega

$$\varphi(n) = |\{x \in \mathbb{N} \mid 1 \leqslant x \leqslant n, (x,n) = 1\}|.$$

Kui $n \geqslant 2$, siis $(n,n) = n > 1$. Seega kui $n \geqslant 2$, siis

$$\varphi(n) = |\{x \in \mathbb{N} \mid 1 \leqslant x < n, (x,n) = 1\}|.$$

Silmas pidades teoreemi 4.10 saame, et iga $n \geqslant 2$ korral

$$\varphi(n) = |U(\mathbb{Z}_n)|,$$

s.t. $\varphi(n)$ on jäägiklassiringi $\mathbb{Z}_n$ pööratavate elementide arv.

Näide 5.2. $\varphi(30) = 8$, sest naturaalarvude seas, mis pole suuremad kui 30, on 8 sellist, mis on 30-ga ühistegurita, nimelt $1, 7, 11, 13, 17, 19, 23$ ja 29.

Kui p on algarv, siis kõik temast väiksemad naturaalarvud on temaga ühistegurita ja ka vastupidi, kui naturaalarvul pole ühest suuremaid ühiseid tegureid temast väiksemate naturaalarvudega, siis on ta algarv. Seega kehtib järgmine väide.

Lause 5.3. *Naturaalarv p on algarv siis ja ainult siis, kui*

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

Teame, et mistahes naturaalarvu $n > 1$ saab esitada algarvude astmete korrutisena. Püüame leida valemi, mille abil saaks leida $\varphi(n)$, kui on teada arvu n standardkuju. Selleks leiame kõigepealt φ väärtuse algarvu astmetel.

Lause 5.4. *Kui p on algarv ja k naturaalarv, siis*

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

Tõestus. Iga $x \in \mathbb{N}$ korral on $(x, p^k) > 1$ parajasti siis, kui $p \mid x$. Arve x, mis jaguvad arvuga p, on hulgas $\{1, 2, \ldots, p^k\}$ p^{k-1} tükki: nimelt $p, 2p, 3p, \ldots, (p^{k-1})p$. Seega hulgas $\{1, 2, \ldots, p^k\}$ on täpselt $p^k - p^{k-1}$ arvu, mis on arvuga p^k ühistegurita. □

Näide 5.5. $\varphi(3^2) = 3^2 - 3^1 = 3^{2-1}(3-1) = 6$. Need kuus 9-st väiksemat ja temaga ühistegurita arvu on $1, 2, 4, 5, 7, 8$ (vt. ka näidet 4.11).

Lause 5.6. *Mistahes ringide $R_1, \ldots, R_s$ korral*

$$U(R_1 \times \ldots \times R_s) = U(R_1) \times \ldots \times U(R_s).$$

Selle võrduse vasakul poolel on rühm (vt. lauset 4.7) ja paremal poolel samuti: nimelt rühmade $U(R_1), \ldots, U(R_s)$ otsekorrutis, mis saadakse kui hulkade otsekorrutisel

$$U(R_1) \times \ldots \times U(R_s) = \{(u_1, \ldots, u_s) \mid u_i \in U(R_i)\}$$

defineeritakse korrutamine komponenthaaval.

Tõestus. Mistahes elementide $r_1 \in R_1, \ldots, r_s \in R_s$ korral

$$\begin{array}{ll}
 & (r_1, \ldots, r_s) \in U(R_1 \times \ldots \times R_s) \\
\iff & (\exists (r_1', \ldots, r_s') \in R_1 \times \ldots \times R_s)\,[(r_1, \ldots, r_s)(r_1', \ldots, r_s') = (r_1', \ldots, r_s')(r_1, \ldots, r_s) = (1, \ldots, 1)] \\
\iff & (\exists (r_1', \ldots, r_s') \in R_1 \times \ldots \times R_s)\left[(r_1 r_1', \ldots, r_s r_s') = (r_1' r_1, \ldots, r_s' r_s) = (1, \ldots, 1)\right] \\
\iff & (\exists (r_1', \ldots, r_s') \in R_1 \times \ldots \times R_s)(\forall i \in \{1, \ldots, s\})\left[r_i r_i' = r_i' r_i = 1\right] \\
\iff & (\forall i \in \{1, \ldots, s\})\,[r_i \in U(R_i)] \\
\iff & (r_1, \ldots, r_s) \in U(R_1) \times \ldots \times U(R_s).
\end{array}$$

□

Teoreem 5.7. *Kui $n_1, \ldots, n_s$ on paarikaupa ühistegurita naturaalarvud, siis*

$$\varphi(n_1 \ldots n_s) = \varphi(n_1) \ldots \varphi(n_s)$$

(Euleri funktsioon on nõrgalt multiplikatiivne).

TÕESTUS. Tähistame $n = n_1 \ldots n_s$. Kui $n = 1$, siis on väide ilmne. Olgu $n > 1$. Järelduse 4.9 ja lause 5.6 põhjal

$$\varphi(n) = |U(\mathbb{Z}_n)| = |U(\mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_s})| = |U(\mathbb{Z}_{n_1}) \times \ldots \times U(\mathbb{Z}_{n_s})| = |U(\mathbb{Z}_{n_1})| \cdot \ldots \cdot |U(\mathbb{Z}_{n_s})| = \varphi(n_1) \ldots \varphi(n_s).$$

□

Teoreem 5.8. *Kui $n > 1$ ja $n = p_1^{k_1} \ldots p_s^{k_s}$ on naturaalarvu n standardkuju, siis*

$$\varphi(n) = p_1^{k_1 - 1} \ldots p_s^{k_s - 1}(p_1 - 1) \ldots (p_s - 1).$$

TÕESTUS. Kuna $p_1, \ldots, p_s$ on paarikaupa erinevad algarvud, siis arvud $p_1^{k_1}, \ldots, p_s^{k_s}$ on paarikaupa ühistegurita ning seega teoreemist 5.7 ja lausest 5.4 järeldub, et

$$\varphi(n) = \varphi(p_1^{k_1}) \ldots \varphi(p_s^{k_s}) = p_1^{k_1 - 1}(p_1 - 1) \ldots p_s^{k_s - 1}(p_s - 1) = p_1^{k_1 - 1} \ldots p_s^{k_s - 1}(p_1 - 1) \ldots (p_s - 1).$$

□

Näide 5.9. $\varphi(360) = \varphi(2^3 \cdot 3^2 \cdot 5) = 2^{3-1} \cdot 3^{2-1} \cdot 5^{1-1}(2-1)(3-1)(5-1) = 4 \cdot 3 \cdot 2 \cdot 4 = 96$,
$\varphi(2012) = \varphi(2^2 \cdot 503) = 2 \cdot 502 = 1004$.

Lause 5.10. *Kui n ja d on naturaalarvud ning $d \mid n$, siis*

$$|\{x \in \mathbb{N} \mid 1 \leqslant x \leqslant n, (x, n) = d\}| = \varphi\left(\frac{n}{d}\right).$$

TÕESTUS. Tähistame $\{x \in \mathbb{N} \mid 1 \leqslant x \leqslant n, (x, n) = d\} = K$. Siis hulka K kuuluvad arvud peavad jaguma arvuga d. Seega hulka K kuuluvad sellised naturaalarvud $x = kd \in \left\{d, 2d, \ldots, \frac{n}{d}d\right\} = \left\{kd \mid k \in \mathbb{N}, 1 \leqslant k \leqslant \frac{n}{d}\right\}$, mis rahuldavad tingimust $(kd, n) = d$. Järeldusest 1.9 saame, et võrdus $(kd, n) = d$ on samaväärne võrdusega $(k, \frac{n}{d}) = 1$. Seega hulga K elemente on niipalju, kuipalju on naturaalarve k, $1 \leqslant k \leqslant \frac{n}{d}$, mille korral $\left(k, \frac{n}{d}\right) = 1$. See tähendab, et hulgas K on $\varphi\left(\frac{n}{d}\right)$ elementi. □

Teoreem 5.11 (Gauss). *Iga naturaalarvu n korral*

$$\sum_{d \mid n} \varphi(d) = n.$$

TÕESTUS. Olgu $1 = d_1, d_2, \ldots, d_s = n$ arvu n kõik naturaalarvulised jagajad. Tähistame

$$K_i = \{x \in \mathbb{N} \mid 1 \leqslant x \leqslant n, (x, n) = d_i\}.$$

Hulgad $K_1, \ldots, K_s$ on lõikumatud ja $\bigsqcup_{i=1}^{s} K_i = \{1, 2, \ldots, n\}$, sest iga $a \in \{1, 2, \ldots, n\}$ korral leidub selline i, et $(a, n) = d_i$. Kasutades seda, et $\{d_1, \ldots, d_s\} = \left\{\frac{n}{d_1}, \ldots, \frac{n}{d_s}\right\}$, ning lauset 5.10, saame

$$n = \left|\bigsqcup_{i=1}^{s} K_i\right| = \sum_{i=1}^{s} |K_i| = \sum_{i=1}^{s} \varphi\left(\frac{n}{d_i}\right) = \sum_{i=1}^{s} \varphi(d_i).$$

□

5.2. Euleri teoreem

Üks kasulikumaid Euleri funktsiooni rakendusi on järgmine tulemus, mida edaspidi kutsume Euleri teoreemiks.

Teoreem 5.12 (Euler). *Kui $a \in \mathbb{Z}$, $n \in \mathbb{N}$ ja $(a, n) = 1$, siis*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

TÕESTUS. Vaatleme jäägiklassiringi $\mathbb{Z}_n$ pööratavate elementide rühma $(U(\mathbb{Z}_n), \cdot)$. Et $(a, n) = 1$, siis teoreemi 4.10 põhjal $\overline{a} \in U(\mathbb{Z}_n)$. Olgu m elemendi $\overline{a}$ järk rühmas $U(\mathbb{Z}_n)$, s.t. tema poolt tekitatud alamrühma $\langle \overline{a} \rangle$ järk, s.o. vähim selline naturaalarv, et $\overline{a}^m = \overline{1}$ ([1], def. 6.3.6). Kuna lõpliku rühma elemendi järk jagab Lagrange'i teoreemi tõttu rühma järku, siis $m \mid |U(\mathbb{Z}_n)| = \varphi(n)$, s.t. leidub selline $k \in \mathbb{N}$, et $mk = \varphi(n)$. Seega rühmas $U(\mathbb{Z}_n)$

$$\overline{a^{\varphi(n)}} = \overline{a}^{\varphi(n)} = \overline{a}^{mk} = (\overline{a}^m)^k = \overline{1}^k = \overline{1}.$$

Järelikult lause 3.5 põhjal $a^{\varphi(n)} \equiv 1 \pmod{n}$. □

Euleri teoreem annab ühe võimaluse rühma $U(\mathbb{Z}_n)$ elemendi $\overline{a}$ pöördelemendi $\overline{a}^{-1}$ leidmiseks. Nimelt võrdusest $\overline{1} = \overline{a}^{\varphi(n)} = \overline{a} \cdot \overline{a}^{\varphi(n)-1}$ järeldub, et

$$\overline{a}^{-1} = \overline{a}^{\varphi(n)-1}. \tag{6}$$

Arvutuslikult on pöördelemendi leidmiseks siiski otstarbekam kasutada Eukleidese algoritmi.

Järeldusena Euleri teoreemist ja lausest 5.3 saame Fermat' väikese teoreemi.

Teoreem 5.13 (Fermat' väike teoreem). *Kui p on algarv ja a on täisarv, mis ei jagu arvuga p, siis*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Järeldus 5.14. *Kui p on algarv, siis iga täisarvu a korral*

$$a^p \equiv a \pmod{p}.$$

TÕESTUS. Kui $p \mid a$, siis $a^p \equiv 0 \equiv a \pmod{p}$. Kui $p \nmid a$, siis Fermat' väikse teoreemi tõttu $a^{p-1} \equiv 1 \pmod{p}$, millest järeldub, et $a^p \equiv a \pmod{p}$. □

Näide 5.15. Euleri teoreemi rakendusena leiame näiteks arvu 3^{256} kaks viimast numbrit.

Selleks tuleb leida jääk, mis tekib arvu 3^{256} jagamisel 100-ga, s.o. vähim mittenegatiivne täisarv, millega 3^{256} on kongruentne mooduli 100 järgi. Kuna $(3, 100) = 1$ ja $\varphi(100) = \varphi(2^2 \cdot 5^2) = 2 \cdot 5 \cdot 4 = 40$, siis Euleri teoreemi põhjal $3^{40} \equiv 1 \pmod{100}$. Et $256 = 6 \cdot 40 + 16$, siis

$$3^{256} = 3^{6 \cdot 40 + 16} = (3^{40})^6 \cdot 3^{16} \equiv 3^{16} \pmod{100}.$$

Seega jääb veel vaid leida, millega on 3^{16} kongruentne mooduli 100 järgi:

$$3^{16} = 81^4 \equiv (-19)^4 = 361^2 \equiv 61^2 \equiv 21 \pmod{100}.$$

Järelikult arv 3^{256} lõpeb numbritega 2 ja 1.

5.3. Möbiuse funktsioon

Möbiuse funktsioon on oma nime saanud saksa matemaatiku August Ferdinand Möbiuse (1790–1868) järgi, kes võttis selle funktsiooni kasutusele 1831. a.

Definitsioon 5.16. *Möbiuse funktsioon* $\mu : \mathbb{N} \to \mathbb{Z}$ defineeritakse võrdusega

$$\mu(n) = \begin{cases} 1, & \text{kui } n = 1, \\ 0, & \text{kui leidub algarv } p \text{ nii, et } p^2 \mid n, \\ (-1)^s, & \text{kui } n = p_1 \cdot \ldots \cdot p_s, \text{ kus } p_1, \ldots, p_s \text{ on paarikaupa erinevad algarvud.} \end{cases}$$

Teoreem 5.17. *Kui $n \in \mathbb{N}$, siis*

$$\sum_{d \mid n} \mu(d) = \left\lfloor \frac{1}{n} \right\rfloor = \begin{cases} 1, & \textit{kui } n = 1, \\ 0, & \textit{kui } n > 1. \end{cases}$$

TÕESTUS. Kui $n = 1$, siis on väide ilmne. Olgu $n > 1$ ja esitame ta standardkujul $n = p_1^{k_1} \dots p_s^{k_s}$. Summasse $\sum_{d|n} \mu(d)$ tulevad nullist erinevad liidetavad ainult $d = 1$ ja selliste jagajate d korral, mis on erinevate algarvude korrutised. Seega

$$\begin{aligned}\sum_{d|n} \mu(d) &= \mu(1) + \mu(p_1) + \ldots + \mu(p_s) + \mu(p_1p_2) + \ldots + \mu(p_{s-1}p_s) + \ldots + \mu(p_1p_2 \ldots p_s) \\ &= 1 + \binom{s}{1}(-1) + \binom{s}{2}(-1)^2 + \ldots + \binom{s}{s}(-1)^s = (1-1)^s = 0.\end{aligned}$$

□

Euleri ja Möbiuse funktsioon on seotud järgmise valemi abil.

Teoreem 5.18 (Möbiuse inversioonivalem). *Iga naturaalarvu n korral*

$$\varphi(n) = \sum_{d|n} \mu(d)\frac{n}{d}.$$

TÕESTUS. Euleri funktsiooni definitsiooni põhjal on ilmne, et

$$\varphi(n) = \sum_{k=1}^{n} \left\lfloor \frac{1}{(n,k)} \right\rfloor.$$

Kasutades teoreemi 5.17, kus n osas on võetud (n, k), saame

$$\varphi(n) = \sum_{k=1}^{n} \sum_{d|(n,k)} \mu(d) = \sum_{k=1}^{n} \sum_{\substack{d|n \\ d|k}} \mu(d).$$

Kui fikseerida arvu n jagaja d, siis tuleb arvu $\mu(d)$ liita iseendale niimitu korda, kuipalju on hulgas $\{1, 2, \ldots, n\}$ arvu d kordseid. Kuna neid on $\frac{n}{d}$ tükki, siis

$$\varphi(n) = \sum_{d|n} \sum_{i=1}^{\frac{n}{d}} \mu(d) = \sum_{d|n} \mu(d) \sum_{i=1}^{\frac{n}{d}} 1 = \sum_{d|n} \mu(d)\frac{n}{d}.$$

□

5.4. Teisi funktsioone

Definitsioon 5.19. Kui n on naturaalarv, siis tähistagu $\tau(n)$ arvu n kõigi naturaalarvuliste jagajate arvu ning $\sigma(n)$ arvu n kõigi naturaalarvuliste jagajate summat.

Näide 5.20. Kuna arvu 12 naturaalarvulisteks jagajateks on $1, 2, 3, 4, 6$ ja 12, siis $\tau(12) = 6$ ja $\sigma(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28$.

Kui on teada arvu n lahutus algtegureiks, siis järgmine teoreem annab lihtsa võimaluse funktsioonide τ ja σ arvutamiseks.

Teoreem 5.21. *Kui $n > 1$ ja $n = p_1^{k_1} p_2^{k_2} \dots p_s^{k_s}$ on arvu n standardkuju, siis*

1. $$\tau(n) = (k_1 + 1)(k_2 + 1) \dots (k_s + 1);$$

2. $$\sigma(n) = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{k_2+1} - 1}{p_2 - 1} \cdot \ldots \cdot \frac{p_s^{k_s+1} - 1}{p_s - 1}.$$

TÕESTUS. 1. Tänu lausele 1.21 on arvu n jagajaiks need ja ainult need arvud, millel on kuju $p_1^{l_1} \dots p_s^{l_s}$, kus $0 \leqslant l_i \leqslant k_i$, $i = 1, \dots, s$. Aritmeetika põhiteoreemi tõttu annavad erinevad astendajate komplektid $(l_1, \dots, l_s)$ erinevad n jagajad. Astendaja l_1 valikuks on $k_1 + 1$ võimalust, astendaja l_2 valikuks on $k_2 + 1$ võimalust jne. Seega on arvul n kokku $(k_1 + 1)(k_2 + 1) \dots (k_s + 1)$ erinevat jagajat.

2. Et leida $\sigma(n)$ väärtust, vaatleme korrutist

$$(1 + p_1 + p_1^2 + \dots + p_1^{k_1})(1 + p_2 + p_2^2 + \dots + p_2^{k_2}) \dots (1 + p_s + p_s^2 + \dots + p_s^{k_s}).$$

Kui sulud avada, siis saadavas summas esineb arvu n iga naturaalarvuline jagaja täpselt ühe korra, seega

$$\sigma(n) = (1 + p_1 + p_1^2 + \dots + p_1^{k_1}) \dots (1 + p_s + p_s^2 + \dots + p_s^{k_s}).$$

Kasutades geomeetrilise jada summa valemit saame, et iga $i = 1, \dots, s$ korral

$$1 + p_i + p_i^2 + \dots + p_i^{k_i} = \frac{p_i^{k_i+1} - 1}{p_i - 1},$$

millest järeldubki väide 2. □

Funktsiooniga σ on seotud huvitav lahendamata probleem. Naturaalarvu n nimetatakse *täiuslikuks*, kui $\sigma(n) = 2n$. Näiteks arvud 6 ja 28 on täiuslikud. Üldisemalt, kui $2^m - 1$ on algarv, siis $n = 2^{m-1}(2^m - 1)$ on täiuslik. Selle tõestas juba Eukleides. Euler näitas, et mistahes paarisarvuline täiuslik arv on sellisel kujul. Seega paarisarvuliste täiuslike arvude leidmise probleem taandub algarvude $2^m - 1$ otsimisele. Selliseid algarve nimetatakse *Mersenne'i algarvudeks*. Praeguse seisuga (veebruar 2018) on teada 50 Mersenne'i algarvu, neist suurim on $2^{77\,232\,917} - 1$, millel on 23 249 425 kümnendnumbrit. Otsingud jätkuvad (vt. ka http://www.mersenne.org). Lahendamata on probleemid: kas leidub lõpmata palju täiuslikke arve ja kas leidub mõni paaritu täiuslik arv.

6. Tundmatut sisaldavad kongruentsid. Hiina jäägiteoreem.

6.1. Ülesande püstitusest

Vaatleme tundmatut x sisaldavaid kongruentse kujul

$$f(x) \equiv 0 \pmod{n}, \tag{7}$$

kus

$$f(x) = a_m x^m + a_{m-1}x^{m-1} + \ldots + a_1 x + a_0 \tag{8}$$

on täisarvuliste kordajatega polünoom muutuja x suhtes ja $a_m \not\equiv 0 \pmod{n}$. Kui $m = 1$, siis kõneldakse lineaarkongruentsidest, kui $m = 2$, siis ruutkongruentsidest, jne. Ütleme, et täisarv x_0 on kongruentsi (7) *lahend*, kui $f(x_0) \equiv 0 \pmod{n}$. Kui mingi täisarv x_0 on kongruentsi (7) lahend, siis tänu järeldusele 3.8 on ka kõik arvuga x_0 mooduli n järgi kongruentsed arvud selle kongruentsi lahendid. Seepärast loeme kongruentsi (7) lahendiks tervet jäägiklassi $\overline{x_0} \in \mathbb{Z}_n$ ja lahendit märgime ka järgmiselt:

$$x \equiv x_0 \pmod{n}.$$

See, et $f(x_0) \equiv 0 \pmod{n}$ on lause 3.5 tõttu samaväärne sellega, et $\overline{f(x_0)} = \overline{0}$ ringis $\mathbb{Z}_n$. Arvestades seda, kuidas on defineeritud liitmine ja korrutamine jäägiklassiringis, on viimane samaväärne sellega, et $\overline{f}(\overline{x_0}) = \overline{0}$, kus

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

on polünoom kordajatega ringist $\mathbb{Z}_n$. Seega kongruentsi (7) lahendamine on samaväärne võrrandi

$$\overline{f}(x) = \overline{0} \tag{9}$$

lahendamisega jäägiklassiringis $\mathbb{Z}_n$.

Et mooduli n järgi on olemas täpselt n jäägiklassi, siis võrrandi (9) (ja seega ka kongruentsi (7)) lahendid saame kätte, kui lihtsalt proovime läbi kõik n jäägiklassi. Väikese mooduli n korral ei ole see liiga raske, kuid suure n korral on proovimismeetod arvutuslikult äärmiselt ebaefektiivne.

Näide 6.1. Lahendame proovimismeetodil kongruentsi

$$3x^4 + 2x^2 - 1 \equiv 0 \pmod{5}.$$

Proovime kõiki jäägiklasse $\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}$ mooduli 5 järgi:

$$\begin{aligned}
&\overline{3}\cdot\overline{0}^4 + \overline{2}\cdot\overline{0}^2 - \overline{1} = \overline{4} \neq \overline{0},\\
&\overline{3}\cdot\overline{1}^4 + \overline{2}\cdot\overline{1}^2 - \overline{1} = \overline{3} + \overline{2} - \overline{1} = \overline{4} \neq \overline{0},\\
&\overline{3}\cdot\overline{2}^4 + \overline{2}\cdot\overline{2}^2 - \overline{1} = \overline{3}\cdot\overline{1} + \overline{2}\cdot\overline{4} - \overline{1} = \overline{10} = \overline{0},\\
&\overline{3}\cdot\overline{3}^4 + \overline{2}\cdot\overline{3}^2 - \overline{1} = \overline{3}\cdot\overline{1} + \overline{2}\cdot\overline{4} - \overline{1} = \overline{10} = \overline{0},\\
&\overline{3}\cdot\overline{4}^4 + \overline{2}\cdot\overline{4}^2 - \overline{1} = \overline{3}\cdot\overline{1} + \overline{2}\cdot\overline{1} - \overline{1} = \overline{4} \neq \overline{0}.
\end{aligned}$$

Näeme, et antud kongruentsi lahendeiks on jäägiklassid $\overline{2}$ ja $\overline{3}$ mooduli 5 järgi, ehk pisut teistmoodi kirjapanduna võime lahendi esitada kujul $x \equiv 2 \pmod{5}$, $x \equiv 3 \pmod{5}$.

Märgime, et $\overline{f}(x_0)$ leidmiseks võib kasutada ka Horneri skeemi. Näiteks skeemi

	$\overline{3}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{-1}$
$\overline{2}$	$\overline{3}$	$\overline{0} + \overline{2}\cdot\overline{3} = \overline{1}$	$\overline{2} + \overline{2}\cdot\overline{1} = \overline{4}$	$\overline{0} + \overline{2}\cdot\overline{4} = \overline{3}$	$\overline{-1} + \overline{2}\cdot\overline{3} = \overline{0}$

abil näeme, et $\overline{2}$ on eespoolvaadeldud kongruentsi lahend.

6.2. Lineaarkongruentsid

Kõige lihtsamad kongruentsid on lineaarkongruentsid, need on kongruentsid kujul

$$ax \equiv b \pmod{n}, \tag{10}$$

kus $a \not\equiv 0 \pmod{n}$. Osutub, et sellel kongruentsil võib olla üks, mitu või mitte ühtegi lahendit.

Lause 6.2. *Lineaarkongruents (10) omab lahendit parajasti siis, kui* $(a,n) \mid b$. *Kui* $d = (a,n) \mid b$, *siis sellel kongruentsil on* d *lahendit. Need on*

$$\overline{x_0}, \overline{x_0 + n'}, \overline{x_0 + 2n'}, \ldots, \overline{x_0 + (d-1)n'}, \tag{11}$$

kus $n' = \frac{n}{(a,n)} = \frac{n}{d}$ *ja* $\overline{x_0} \in \mathbb{Z}_n$ *on selle kongruentsi mingi (eri)lahend.*

Tõestus. Olgu $d = (a,n)$, $n' = \frac{n}{d}$ ja $a' = \frac{a}{d}$. Kui $\overline{x_0}$ on lahend, siis leidub selline täisarv k, et $b = ax_0 + kn$. Kuna d jagab viimase võrduse paremat poolt, siis ka $d \mid b$. Vastupidi, oletame, et $d \mid b$ ning olgu $b = db'$, $b' \in \mathbb{Z}$. Teoreemi 1.8 põhjal leiduvad sellised täisarvud x_0' ja y_0', et $ax_0' + ny_0' = d$. Korrutame võrduse mõlemad pooled arvuga b'. Siis $a(x_0'b') + n(y_0'b') = b$. Võttes $x_0 = x_0'b'$ saame, et $ax_0 \equiv b \pmod{n}$. Sellega on näidatud, et kongruents (10) on lahenduv parajasti siis, kui $d \mid b$.

Oletame nüüd, et $d \mid b$, s.t. leidub selline $b' \in \mathbb{Z}$, et $db' = b$, ning olgu $\overline{x_0}$ kongruentsi (10) mingi lahend. Näitame, et jäägiklassid (11) on kongruentsi (10) lahendid. Tõepoolest, iga $k \in \{0, \ldots, d-1\}$ korral

$$a(x_0 + kn') = ax_0 + a'dkn' \equiv b + a'kn \equiv b \pmod{n}.$$

Näitame, et lahendid (11) on kõik erinevad. Selleks oletame vastuväiteliselt, et $\overline{x_0 + in'} = \overline{x_0 + jn'}$, $0 \leqslant i < j \leqslant d-1$, s.t. $x_0 + in' \equiv x_0 + jn' \pmod{n}$. Siis $n \mid (x_0 + jn') - (x_0 + in') = (j-i)n'$, mis aga pole võimalik, sest $0 < (j-i)n' < dn' = n$.

Lõpetuseks näitame, et kongruentsi (10) mistahes lahend $\overline{x_1}$ on võrdne ühega lahendeist (11). Sellest, et $ax_0 \equiv b \pmod{n}$ ja $ax_1 \equiv b \pmod{n}$, järeldub kongruentside vastavaid pooli lahutades, et $a(x_1 - x_0) \equiv 0 \pmod{n}$, mis tähendab, et $a(x_1 - x_0) = kn$ mingi $k \in \mathbb{Z}$ korral. Jagades viimase võrduse mõlemaid pooli arvuga d saame, et $a'(x_1 - x_0) = kn'$. Kuna järelduse 1.9 tõttu $(a', n') = 1$, siis järelduse 1.10 põhjal $n' \mid x_1 - x_0$, s.t. leidub selline $l \in \mathbb{Z}$, et $x_1 - x_0 = ln'$ ehk $x_1 = x_0 + ln'$. Lause 1.6 põhjal leiduvad selised $q, r \in \mathbb{Z}$, et $l = qd + r$ ja $0 \leqslant r < d$. Järelikult

$$x_1 = x_0 + (qd + r)n' = x_0 + qn + rn' \equiv x_0 + rn' \pmod{n},$$

mis tähendab, et $\overline{x_1}$ on võrdne ühega lahendeist (11). □

Märkus 6.3. Kongruentsi $a'x \equiv b' \pmod{n'}$ lahend on lause 3.10 tõttu ka kongruentsi $ax \equiv b \pmod{n}$ lahend. Seega kongruentsi $ax \equiv b \pmod{n}$ mingi erilahendi leidmiseks piisab leida kongruentsi $a'x \equiv b' \pmod{n'}$ mingi lahend.

Järeldus 6.4. *Kongruents (10) on üheselt lahenduv parajasti siis, kui* $(a,n) = 1$.

Näide 6.5. Lahendame kongruentsi $5x \equiv 3 \pmod{16}$.

Selle kongruentsi lahendamine on samaväärne võrrandi $\overline{5}x = \overline{3}$ lahendamisega ringis $\mathbb{Z}_{16}$. Kuna $(5,16) = 1$, siis $\overline{5} \in U(\mathbb{Z}_{16})$ ja seega saame x leida korrutades selle võrrandi mõlemaid pooli elemendiga $\overline{5}^{-1}$. Et rühma elemendi pöördelement on üheselt määratud, siis ka x on üheselt määratud (sedasama väidab meile ka järeldus 6.4). Leiame $\overline{5}^{-1}$ ringis $\mathbb{Z}_{16}$. Valemi (6) abil saame

$$\overline{5}^{-1} = \overline{5}^{\varphi(16)-1} = \overline{5}^7 = \left(\overline{5}^2\right)^3 \cdot \overline{5} = \overline{9}^3 \cdot \overline{5} = \overline{81} \cdot \overline{9} \cdot \overline{5} = \overline{9} \cdot \overline{5} = \overline{-3} = \overline{13}$$

ja seega

$$x = \overline{5}^{-1} \cdot \overline{3} = \overline{-3} \cdot \overline{3} = \overline{-9} = \overline{7}.$$

Kontrollime: $5 \cdot 7 \equiv 3 \pmod{16}$.

6.3. Hiina jäägiteoreem

Selles punktis vaatleme lineaarkongruentside süsteemide lahendamist. Selliseid süsteeme vaadeldi Hiinas juba 3. sajandil. Põhitulemus on järgmine.

Teoreem 6.6 (Hiina jäägiteoreem). *Olgu* $a_1, \ldots, a_s$ *täisarvud,* $n_1, \ldots, n_s$ *paarikaupa ühistegurita naturaalarvud ja* $n = n_1 \ldots n_s$. *Siis kongruentside süsteemil*

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ \ldots \\ x \equiv a_s \pmod{n_s} \end{cases} \tag{12}$$

on olemas ühene lahend mooduli n *järgi.*

Anname sellele teoreemile kaks erinevat tõestust.

TÕESTUS 1. Kui $n_1, \ldots, n_s$ on paarikaupa ühistegurita, siis teoreemi 4.5 tõestuse põhjal kujutus $f : \mathbb{Z}_n \longrightarrow \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_s}$, $f(\overline{b}) = \left(\overline{b}_1, \ldots, \overline{b}_s\right)$, kus $\overline{b}_i$ on arvu b jäägiklass mooduli n_i järgi, on ringide isomorfism. Vaatleme elementi $\left(\left(\overline{a_1}\right)_1, \ldots, \left(\overline{a_s}\right)_s\right) \in \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_s}$ (siin $\left(\overline{a_i}\right)_i$ on arvu a_i jäägiklass mooduli n_i järgi). Kujutuse f sürjektiivsusest järeldub, et leidub selline $a \in \mathbb{Z}$, et $f(\overline{a}) = \left(\left(\overline{a_1}\right)_1, \ldots, \left(\overline{a_s}\right)_s\right)$. Teiselt poolt aga vastavalt f definitsioonile $f(\overline{a}) = \left(\overline{a}_1, \ldots, \overline{a}_s\right)$. Seega $\left(\overline{a_i}\right)_i = \overline{a}_i, i = 1, \ldots, s$. See tähendab, et iga i korral $a \equiv a_i \pmod{n_i}$ ning järelikult $x = a$ ongi süsteemi (12) lahend.

Veendume, et see lahend on ühene mooduli n järgi. Olgu ka b süsteemi (12) lahend. Siis $b \equiv a_i \pmod{n_i}$ iga i korral, s.t. $\overline{b}_i = \left(\overline{a_i}\right)_i$ ning $f(\overline{a}) = \left(\left(\overline{a_1}\right)_1, \ldots, \left(\overline{a_s}\right)_s\right) = \left(\overline{b}_1, \ldots, \overline{b}_s\right) = f(\overline{b})$. Kujutuse f injektiivsuse tõttu $\overline{a} = \overline{b}$, ehk $a \equiv b \pmod{n}$. □

TÕESTUS 2. Leiame iga $i = 1, \ldots, s$ korral arvu

$$m_i = \frac{n}{n_i} = \prod_{j \neq i} n_j.$$

Kuna $(n_j, n_i) = 1$, kui $j \neq i$, siis lemma 4.1 põhjal ka $(m_i, n_i) = 1$. Seega $\overline{m_i} \in U(\mathbb{Z}_{n_i})$. Iga $i = 1, \ldots, s$ korral leiame elemendi $\overline{m_i}$ pöördelemendi ringis $\mathbb{Z}_{n_i}$

$$\overline{k_i} = \overline{m_i}^{-1} \in U(\mathbb{Z}_{n_i}),$$

s.t. sellise $k_i \in \mathbb{Z}$, et $\overline{k_i}\overline{m_i} = \overline{1}$ ehk $k_i m_i \equiv 1 \pmod{n_i}$. Tähistame

$$x = \sum_{j=1}^{s} a_j k_j m_j.$$

Siis $x = \sum_{j=1}^{s} a_j k_j m_j \equiv a_i k_i m_i \equiv a_i \pmod{n_i}$ iga $i = 1, \ldots, s$ korral, sest $j \neq i$ korral $n_i \mid m_j$. Seega x on süsteemi (12) lahend.

Kui ka y on süsteemi (12) lahend, siis iga $i = 1, \ldots, s$ korral $x \equiv a_i \equiv y \pmod{n_i}$ ning kuna $n_1, \ldots, n_s$ on paarikaupa ühistegurita, siis lemma 4.2 põhjal $x \equiv y \pmod{n}$. □

Näide 6.7. Lahendame lineaarkongruentside süsteemi

$$\begin{cases} 3x \equiv 4 \pmod{7} \\ 2x \equiv 1 \pmod{5} \\ x \equiv 4 \pmod{3}. \end{cases}$$

Selleks lahendame esialgu iga kongruentsi eraldi. Et ringis $\mathbb{Z}_7$ on $\overline{3}^{-1} = \overline{5}$, siis $x \equiv 5 \cdot 4 \equiv 6 \pmod{7}$. Kuna ringis $\mathbb{Z}_5$ on $\overline{2}^{-1} = \overline{3}$, siis $x \equiv 3 \cdot 1 = 3 \pmod{5}$. Lisaks sellele $x \equiv 4 \pmod{3}$ parajasti siis, kui $x \equiv 1 \pmod{3}$. Seega tuleb lahendada esialgsega samaväärne kongruentside süsteem

$$\begin{cases} x \equiv 6 \pmod{7} \\ x \equiv 3 \pmod{5} \\ x \equiv 1 \pmod{3}. \end{cases}$$

Selle süsteemi lahendi saame kätte Hiina jäägiteoreemi abil. Selleks tähistame $m_1 = 15$, $m_2 = 21$, $m_3 = 35$ ning leiame, et ringis $\mathbb{Z}_7$ $\overline{k_1} = \overline{m_1}^{-1} = \overline{1}^{-1} = \overline{1}$, ringis $\mathbb{Z}_5$ $\overline{k_2} = \overline{m_2}^{-1} = \overline{1}^{-1} = \overline{1}$ ja ringis $\mathbb{Z}_3$ $\overline{k_3} = \overline{m_3}^{-1} = \overline{2}^{-1} = \overline{2}$. Seega

$$x = 6 \cdot 1 \cdot 15 + 3 \cdot 1 \cdot 21 + 1 \cdot 2 \cdot 35 = 90 + 63 + 70 = 223$$

ja

$$x \equiv 13 \pmod{105}.$$

Näide 6.8. Lahendame järgmise ülesande, mis on pärit india matemaatikult Brahmaguptalt (598—668).

Kui võtta korvist mune 2, 3, 4, 5 või 6 kaupa, siis jääb lõpuks järgi vastavalt 1, 2, 3, 4 või 5 muna. Kui võtta korvist mune 7 kaupa, siis ei jää lõpuks ühtegi muna üle. Leida vähim võimalik munade arv korvis.

Kui otsitav munade arv tähistada tähega x, siis saame x leidmiseks järgmise kongruentside süsteemi:

$$\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{4} \\ x \equiv 4 \pmod{5} \\ x \equiv 5 \pmod{6} \\ x \equiv 0 \pmod{7}. \end{cases}$$

Lihtne on näha, et selle süsteemi kaks esimest kongruentsi on järelduseks ülejäänutest. Seetõttu on see süsteem samaväärne oma alamsüsteemiga

$$\begin{cases} x \equiv 3 \pmod 4 \\ x \equiv 5 \pmod 6 \\ x \equiv 4 \pmod 5 \\ x \equiv 0 \pmod 7. \end{cases}$$

Paneme tähele, et siin ei ole moodulid ühistegurita ning seega ei saa lahendada nii nagu eelmises ülesandes. Selle ülesande saab siiski lahendada kasutades järgmist meetodit (lahendame n.ö. järk-järgult). See seisneb selles, et iga järgmise kongruentsi lahendeid otsitakse vaid kõigist eelnevatest kongruentsidest koosneva osasüsteemi lahendite hulgast. Igal sammul tuleb siinjuures lahendada teatud lineaarkongruents. Selle lahendite puudumine toob kaasa kogu süsteemi mittelahenduvuse. Lineaarkongruentside lahendite olemasolu kõigil etappidel tagab süsteemi lahendi olemasolu. Vastus jääb mooduli järgi, mis on antud moodulite vähim ühiskordne.

Esimese kongruentsi lahendeiks on kõik täisarvud kujul $x = 4t + 3$, $t \in \mathbb{Z}$. Leiame nende hulgas need, mis rahuldavad ka teist kongruentsi. Asendades saame $4t+3 \equiv 5 \pmod 6$, kust $2t \equiv 1 \pmod 3$ ja seega $t \equiv 2 \pmod 3$. Niisiis $t = 3u + 2, u \in \mathbb{Z}$, ja $x = 12u + 11$. (Seega $x \equiv 11 \pmod{12}$ ja edasi võiks põhimõtteliselt kasutada Hiina jäägiteoreemi, kuid jätkame siin siiski sama meetodiga.) Otsime selliste arvude hulgast neid, mis rahuldavad ka kolmandat kongruentsi. Nende korral $12u+11 \equiv 4 \pmod 5$, kust saame $u \equiv -1 \pmod 5$. Seega $u = 5v-1, v \in \mathbb{Z}$, ja $x = 60v - 1$. Viimasesse kongruentsi asendades saame $60v - 1 \equiv 0 \pmod 7$ ehk $4v \equiv 1 \pmod 7$, kust $v \equiv 2 \pmod 7$. Seega $v = 7w + 2$, $w \in \mathbb{Z}$, ja $x = 420w + 119$. Järelikult vähim võimalik munade arv korvis on 119.

6.4. Kongruentsid algarvu astme järgi

Uurime, kuidas lahendada kongruentse

$$f(x) \equiv 0 \pmod{p^k}, \tag{13}$$

kus $f(x)$ on polünoom kujul (8), p on algarv ja k on naturaalarv. Oletame, et meil on mingil viisil (nt. proovimismeetodil, üldjuhul paremat meetodit polegi) leitud kongruentsi

$$f(x) \equiv 0 \pmod p \tag{14}$$

kõik lahendid. Kui $\overline{x_0} \in \mathbb{Z}_p$ on selle kongruentsi mingi lahend, siis iga täisarvu y korral $f(x_0 + py) \equiv f(x_0) \equiv 0 \pmod p$. Paneme tähele, et kongruentsi

$$f(x) \equiv 0 \pmod{p^2} \tag{15}$$

iga lahend on ka kongruentsi (14) lahend (kuid vastupidine üldjuhul ei kehti). Seetõttu tuleks kongruentsi (15) lahendite saamiseks eraldada kongruentsi (14) lahendite hulgast välja need, mis rahuldavad kongruentsi (15), s.t. kongruentsi (14) iga lahendi $\overline{x_0} = \{x_0 + py \mid y \in \mathbb{Z}\} \in \mathbb{Z}_p$ korral tuleks leida kõik sellised täisarvud y, mille korral $f(x_0 + py) \equiv 0 \pmod{p^2}$. Kuna Newtoni binoomvalemi põhjal

$$\begin{aligned} &f(x_0 + py) = a_m(x_0 + py)^m + a_{m-1}(x_0 + py)^{m-1} + \ldots + a_2(x_0 + py)^2 + a_1(x_0 + py) + a_0 \\ &\equiv a_m x_0^m + a_m \binom{m}{1} x_0^{m-1} py + a_{m-1} x_0^{m-1} + a_{m-1} \binom{m-1}{1} x_0^{m-2} py + \ldots + a_2 x_0^2 + a_2 \binom{2}{1} x_0 py + a_1 x_0 + a_1 py + a_0 \\ &= (a_m m x_0^{m-1} + a_{m-1}(m-1)x_0^{m-2} + \ldots + a_2 2x_0 + a_1)py + f(x_0) = f'(x_0)py + f(x_0) \pmod{p^2}, \end{aligned}$$

siis tuleks leida lineaarkongruentsi

$$f'(x_0)py + f(x_0) \equiv 0 \pmod{p^2}$$

(tundmatu y suhtes) lahendid. Kuna x_0 on kongruentsi (14) lahend ehk $p \mid f(x_0)$, siis lause 3.10 põhjal on viimane kongruents samaväärne kongruentsiga

$$f'(x_0)y + \frac{f(x_0)}{p} \equiv 0 \pmod p. \tag{16}$$

Kui kongruentsi (16) lahendiks on jäägiklass $\overline{y_0} \in \mathbb{Z}_p$, s.t. kõik täisarvud $y = y_0 + pz$, $z \in \mathbb{Z}$, siis kongruentsi (14) rahuldavatest arvudest $x_0 + py$ rahuldavad kongruentsi (15) arvud kujul $x = x_0 + p(y_0 + pz) = x_1 + p^2 z$, kus $x_1 = x_0 + py_0$ ja $z \in \mathbb{Z}$. Eraldame viimaste hulgast välja arvud, mis rahuldavad kongruentsi

$$f(x) \equiv 0 \pmod{p^3}.$$

Selleks tuleb leida kõik täisarvud z, mille korral $f(x_1+p^2z) \equiv 0 \pmod{p^3}$. Kasutades jällegi Newtoni binoomvalemit saame

$$\begin{aligned} f(x_1+p^2z) &= a_m(x_1+p^2z)^m + a_{m-1}(x_1+p^2z)^{m-1} + \ldots + a_2(x_1+p^2z)^2 + a_1(x_1+p^2z) + a_0 \\ &\equiv a_m x_1^m + a_m \binom{m}{1} x_1^{m-1} p^2 z + \ldots + a_2 x_1^2 + a_2 \binom{2}{1} x_1 p^2 z + a_1 x_1 + a_1 p^2 z + a_0 \\ &\equiv (a_m m x_1^{m-1} + \ldots + a_2 2x_1 + a_1) p^2 z + f(x_1) = f'(x_1)p^2 z + f(x_1) \pmod{p^3}. \end{aligned}$$

Kuna x_1 on kongruentsi (15) lahend, siis $p^2 \mid f(x_1)$ ja seega tuleb lahendada lineaarkongruents

$$f'(x_1)z + \frac{f(x_1)}{p^2} \equiv 0 \pmod{p}$$

tundmatu z suhtes. Analoogiliselt jätkame, kuni saame kätte kongruentsi (13) lahendid.

Näide 6.9. Lahendame kongruentsi

$$4x^3 + 7x^2 - 7x - 10 \equiv 0 \pmod{3^2}. \tag{17}$$

Selle kongruentsi lahendamiseks lahendame kõigepealt kongruentsi

$$4x^3 + 7x^2 - 7x - 10 \equiv 0 \pmod{3}$$

ehk

$$x^3 + x^2 - x - 1 \equiv 0 \pmod{3}.$$

Et järelduse 5.14 tõttu mistahes x korral $x^3 \equiv x \pmod{3}$, siis viimane kongruents on samaväärne kongruentsiga

$$x^2 - 1 \equiv 0 \pmod{3},$$

mille lahendeiks on $x_1 \equiv 1 \pmod{3}$ ja $x_2 \equiv 2 \equiv -1 \pmod{3}$. Seega peame kongruentsi (17) lahendamiseks vaatlema eraldi kahte juhtu.

Otsime kongruentsi (17) lahendit kujul $x = 1 + 3y$. Kuna polünoomi $f(x) = 4x^3 + 7x^2 - 7x - 10$ tuletis on $f'(x) = 12x^2 + 14x - 7$, $f(1) = -6$ ning $f'(1) = 19 \equiv 1 \pmod{3}$, siis tuleb lahendada lineaarkongruents

$$1 \cdot y + \frac{-6}{3} \equiv 0 \pmod{3}.$$

Selle kongruentsi ainus lahend on $y \equiv 2 \pmod{3}$ ehk arvud $y = 2 + 3z$, $z \in \mathbb{Z}$. Seega kongruentsi (17) lahendeiks on arvud $x = 1 + 3(2 + 3z) = 7 + 9z$, $z \in \mathbb{Z}$, ehk $x \equiv 7 \pmod{9}$.

Otsime nüüd kongruentsi (17) lahendit kujul $x = -1 + 3y$. Arvutades $f(-1) = 0$ ja $f'(-1) = -9 \equiv 0 \pmod{3}$ saame kongruentsi

$$0 \cdot y + \frac{0}{3} \equiv 0 \pmod{3},$$

mis on rahuldatud iga y korral, s.t. $y \equiv 0, 1, 2 \pmod{3}$. Järelikult kongruentsi (17) lahendeiks on veel $x \equiv 2 \pmod{9}$, $x \equiv 5 \pmod{9}$ ja $x \equiv 8 \pmod{9}$.

6.5. Kongruentsid suvalise mooduli järgi

Vaatleme kongruentsi $f(x) \equiv 0 \pmod{n}$ lahendamist üldjuhul. Olgu moodul $n = p_1^{k_1} \ldots p_s^{k_s}$ antud standardkujul. Järeldusest 4.3 tuleb välja, et selle kongruentsi saame asendada teatava kongruentside süsteemiga.

Lause 6.10. *Kongruents*

$$f(x) \equiv 0 \pmod{p_1^{k_1} \ldots p_s^{k_s}} \tag{18}$$

on samaväärne kongruentside süsteemiga

$$\begin{cases} f(x) \equiv 0 \pmod{p_1^{k_1}} \\ \ldots \\ f(x) \equiv 0 \pmod{p_s^{k_s}} \end{cases} \tag{19}$$

(s.t. neil on samad lahendid).

Oletame, et iga $i = 1, \ldots, s$ korral on leitud kongruentsi $f(x) \equiv 0 \pmod{p_i^{k_i}}$ mingi lahend a_i. Siis lineaarkongruentside süsteemi

$$\begin{cases} x \equiv a_1 \pmod{p_1^{k_1}} \\ \ldots \\ x \equiv a_s \pmod{p_s^{k_s}} \end{cases} \tag{20}$$

iga lahend on järelduse 3.8 põhjal ka süsteemi (19) lahend. Ka vastupidi, kui x_0 on süsteemi (19) lahend, siis ta on iga $i = 1, \ldots, s$ korral mooduli $p_i^{k_i}$ järgi kongruentne kongruentsi $f(x) \equiv 0 \pmod{p_i^{k_i}}$ lahendiga x_0, s.o. rahuldab süsteemi (20), kus $a_1 = \ldots = a_s = x_0$. Niisiis, kui me oskaksime lahendada kongruentse $f(x) \equiv 0 \pmod{p_i^{k_i}}$, siis süsteemi (19) (ja seega kongruentsi (18)) kõik lahendid saame, kui lahendame Hiina jäägiteoreemi abil kõikvõimalikud süsteemid (20), kus iga $i = 1, \ldots, s$ korral a_i on kongruentsi $f(x) \equiv 0 \pmod{p_i^{k_i}}$ mingi lahend. Kui r_i on kongruentsi $f(x) \equiv 0 \pmod{p_i^{k_i}}$ lahendite arv, siis selliseid süsteeme (ja seega ka kongruentsi (18) lahendeid) on $r_1 r_2 \ldots r_s$ tükki.

Näide 6.11. Lahendame kongruentsi

$$4x^3 + 7x^2 - 7x - 10 \equiv 0 \pmod{225}. \tag{21}$$

Kuna $225 = 3^2 \cdot 5^2$, siis taandub selle kongruentsi lahendamine kongruentside süsteemi

$$4x^3 + 7x^2 - 7x - 10 \equiv 0 \pmod{3^2} \tag{22}$$
$$4x^3 + 7x^2 - 7x - 10 \equiv 0 \pmod{5^2} \tag{23}$$

lahendamisele. Esimene neist kongruentsidest on lahendatud näites 6.9.

Asume kongruentsi (23) lahendama. Selleks lahendame esialgu kongruentsi

$$4x^3 + 7x^2 - 7x - 10 \equiv 0 \pmod{5}$$

ehk

$$-x^3 + 2x^2 - 2x \equiv 0 \pmod{5}.$$

Proovimise teel saame, et selle kongruentsi lahendeiks on $x \equiv 0 \pmod{5}$, $x \equiv 3 \pmod{5}$ ja $x \equiv 4 \pmod{5}$.

Arvestades, et $(4x^3 + 7x^2 - 7x - 10)' = 12x^2 + 14x - 7$, saame iga $x_0 \in \{0, 3, 4\}$ korral Horneri skeemi abil arvutada $f(x_0)$ ja $f'(x_0)$, need väärtused on järgneva tabeli vastavalt viiendas ja viimases veerus:

x_0	4	7	-7	-10	12	14	-7
0	4	7	-7	-10	12	14	-7
3	4	19	50	140	12	50	143
4	4	23	85	330	12	62	241

.

(Kuna kongruents $f'(x_0)y + \frac{f(x_0)}{5} \equiv 0 \pmod{5}$ tuleb lahendada mooduli 5 järgi, siis tegelikult võiksime kõik arvutused selle tabeli viimases kolmes veerus teha ka mooduli 5 järgi. Arvutused $f(x_0)$ leidmiseks võib aga teha mooduli 25 järgi.) Seega tuleb lahendada kongruentsid

$$-7y + \frac{-10}{5} \equiv 0 \pmod{5}, \quad 143y + \frac{140}{5} \equiv 0 \pmod{5} \quad \text{ja} \quad 241y + \frac{330}{5} \equiv 0 \pmod{5}$$

ehk

$$3y \equiv 2 \pmod{5}, \quad 3y \equiv 2 \pmod{5} \quad \text{ja} \quad y \equiv 4 \pmod{5}.$$

Nende kõigi lahendamisel saame $y \equiv 4 \pmod{5}$. Seega kongruentsi (23) lahendeiks on $x \equiv 0 + 5 \cdot 4 = 20 \pmod{25}$, $x \equiv 3 + 5 \cdot 4 = 23 \pmod{25}$ ja $x \equiv 4 + 5 \cdot 4 = 24 \pmod{25}$.

Saime, et kongruentsi (22) lahendeiks on $x \equiv 2, 5, 7, 8 \pmod{9}$ ja kongruentsi (23) lahendeiks $x \equiv 20, 23, 24 \pmod{25}$. Seega kongruentsil (21) on $4 \cdot 3 = 12$ lahendit. Need saame, kui Hiina jäägiteoreemi abil lahendame 12 lineaarkongruentside süsteemi

$$\begin{cases} x \equiv a_1 \pmod{9} \\ x \equiv a_2 \pmod{25}, \end{cases}$$

kus $a_1 \in \{2, 5, 7, 8\}$ ja $a_2 \in \{20, 23, 24\}$. Lahendame neist ühe:

$$\begin{cases} x \equiv 2 \pmod{9} \\ x \equiv -5 \pmod{25}. \end{cases}$$

Ringis $\mathbb{Z}_{25}$ $\overline{9}^{-1} = \overline{-11} = \overline{14}$ ja ringis $\mathbb{Z}_9$ $\overline{25}^{-1} = \overline{4}$. Seega kongruentsi (21) üheks lahendiks on

$$x = 2 \cdot 25 \cdot 4 + (-5) \cdot 9 \cdot 14 = -430$$

ehk $x \equiv 20 \pmod{225}$. Ülejäänud lahendite saamiseks tuleb x avaldises võtta 2 ja -5 asemel teised arvud a_1 ja a_2. Nii tehes saame lahendeiks $x \equiv 20, 23, 70, 74, 95, 98, 124, 149, 170, 173, 223, 224 \pmod{225}$.

7. Algjuured

7.1. Algjuure mõiste ja algjuurte olemasolu

Algjuurte defineerimiseks ja nende olulisuse mõistmiseks on meil vaja meelde tuletada järgmised rühmateooria põhimõisted.

Definitsioon 7.1. Lõpliku rühma G *järguks* nimetatakse tema elementide arvu $|G|$.

Kui G on lõplik rühm ja $a \in G$, siis kindlasti leidub elemendi a naturaalarvuliste astmete hulgas võrdseid. Olgu näiteks $a^k = a^l$, kus $k, l \in \mathbb{N}$ ja $k > l$. Korrutades selle võrduse mõlemaid pooli elemendiga $a^{-l} = (a^{-1})^l$ saame $a^{k-l} = a^0 = 1$, kusjuures $k - l \in \mathbb{N}$. Seega omab mõtet järgmine definitsioon.

Definitsioon 7.2. Vähimat naturaalarvu m, mille korral $a^m = 1$, kus 1 on rühma G ühikelement, nimetatakse elemendi a *järguks*. Elemendi g järku tähistatakse sümboliga $\operatorname{ord}(g)$ või $\operatorname{o}(g)$.

Lagrange'i teoreem ütleb, et lõpliku rühma elemendi järk on rühma järgu jagaja.

Definitsioon 7.3. Rühma nimetatakse *tsükliliseks*, kui temas leidub element, mille astmetena avalduvad kõik selle rühma elemendid. Sellist elementi nimetatakse tsüklilise rühma *moodustajaks* ehk *tekitajaks*.

Seega m-elemendiline rühm G on tsükliline, kui leidub selline element $a \in G$, et $G = \{a, a^2, \ldots, a^{m-1}, a^m = 1\}$, muuhulgas elemendi a järk on võrdne rühma G järguga. Asjaolu, et element $a \in G$ on rühma G moodustaja, väljendatakse võrduse $G = \langle a \rangle$ abil. Näiteks rühm $(\mathbb{Z}, +)$ on tsükliline rühm moodustajaga 1 või -1 ($\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$) ning $(\mathbb{Z}_m, +)$ on tsükliline rühm moodustajaga $\overline{1}$.

Selles paragrahvis uurime, millal on rühm $(U(\mathbb{Z}_n), \cdot)$ tsükliline, s.t. millal leidub selline element $\overline{a} \in U(\mathbb{Z}_n)$, mille järk on $\varphi(n) = |U(\mathbb{Z}_n)|$, ehk millal leidub element $\overline{a} \in U(\mathbb{Z}_n)$, mille astmetena avalduvad rühma $U(\mathbb{Z}_n)$ kõik elemendid.

Definitsioon 7.4. Täisarvu a nimetatakse *algjuureks* mooduli n järgi, kui $(U(\mathbb{Z}_n), \cdot)$ on tsükliline rühm moodustajaga $\overline{a}$, s.t. kui $U(\mathbb{Z}_n) = \left\{\overline{a}, \overline{a}^2, \ldots, \overline{a}^{\varphi(n)-1}, \overline{a}^{\varphi(n)} = \overline{1}\right\}$.

Samaväärselt võiks defineerida ka nii, et a on algjuur mooduli n järgi, kui $(a, n) = 1$ ja $\varphi(n)$ on vähim naturaalarv, mille korral $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Näide 7.5. Kui $n = 2$, siis $U(\mathbb{Z}_2) = \left\{\overline{1}\right\}$ on tsükliline rühm. Kui $n = 3$, siis $U(\mathbb{Z}_3) = \left\{\overline{1}, \overline{2}\right\} = \left\{\overline{2}, \overline{2}^2\right\}$ on tsükliline rühm moodustajaga $\overline{2}$, seega 2 on algjuur mooduli 3 järgi. Kui $n = 4$, siis $U(\mathbb{Z}_4) = \left\{\overline{1}, \overline{3}\right\} = \left\{\overline{3}, \overline{3}^2\right\}$ on tsükliline rühm moodustajaga $\overline{3}$, seega 3 on algjuur mooduli 4 järgi. Kui $n = 5$, siis $U(\mathbb{Z}_5) = \left\{\overline{1}, \overline{2}, \overline{3}, \overline{4}\right\} = \left\{\overline{2}, \overline{2}^2, \overline{2}^3, \overline{2}^4\right\} = \left\{\overline{3}, \overline{3}^2, \overline{3}^3, \overline{3}^4\right\}$ on tsükliline rühm, seega 2 ja 3 on algjuured mooduli 5 järgi. Kui $n = 8$, siis $U(\mathbb{Z}_8) = \left\{\overline{1}, \overline{3}, \overline{5}, \overline{7}\right\}$ ja $\overline{1}^2 = \overline{1}, \overline{3}^2 = \overline{1}, \overline{5}^2 = \overline{1}, \overline{7}^2 = \overline{1}$, seega ühegi $U(\mathbb{Z}_8)$ elemendi järk pole $4 = \varphi(8)$, järelikult $U(\mathbb{Z}_8)$ ei saa olla tsükliline rühm ning ei leidu ühtegi algjuurt mooduli 8 järgi.

Meie eesmärk on teha kindlaks, milliste moodulite järgi leidub algjuuri, ning anda eeskiri algjuurte konstrueerimiseks etteantud mooduli järgi. Selleks tõestame esialgu paar lihtsat abitulemust rühmade kohta.

Lemma 7.6. *Olgu G rühm, olgu elemendi $a \in G$ järk m ning olgu $l \in \mathbb{N}$. Siis $a^l = 1$ parajasti siis, kui $m \mid l$.*

Tõestus. Tarvilikkus. Olgu $a^l = 1$. Lause 1.6 põhjal leiduvad sellised $q, r \in \mathbb{Z}$, et $l = qm + r$ ja $0 \leqslant r < m$. Siis $1 = a^l = a^{qm+r} = (a^m)^q a^r = 1^q a^r = a^r$. Kuna m on vähim naturaalarv, mille korral $a^m = 1$, siis r ei saa olla naturaalarv, mis tähendab, et $r = 0$. Seega $l = qm$, ehk $m \mid l$.
Piisavus. Kui leidub selline $k \in \mathbb{N}$, et $mk = l$, siis $a^l = (a^m)^k = 1^k = 1$. □

Lemma 7.7. *Paarisarvulise järguga rühmas leidub element, mille järk on kaks.*

Tõestus. Kui rühmas G ei ole elementi, mille järk on kaks, s.t. iga elemendi $1 \neq a \in G$ korral $a^2 \neq 1$ ehk $a \neq a^{-1}$, siis kõik G ühikelemendist erinevad elemendid jagunevad lõikumatuteks paarideks $\left\{a, a^{-1}\right\}$. Seega G järk on paaritu arv. Järelikult kui G järk on paarisarv, siis peab leiduma vähemalt üks teist järku element. □

Lemma 7.8. *Paarisarvulise järguga tsüklilises rühmas on täpselt üks element, mille järk on kaks.*

TÕESTUS. Olgu $G = \langle a \rangle$ tsükliline rühm moodustajaga a ja $|G| = 2m$, kus $m \in \mathbb{N}$. Siis $a^{2m} = 1$ ja $G = \left\{1, a, a^2, \ldots, a^{2m-1}\right\}$. Järelikult $a^m \neq 1$ ja $(a^m)^2 = 1$, s.t. elemendi a^m järk on 2. Oletame, et ka elemendi a^l, kus $1 \leqslant l \leqslant 2m-1$, järk on 2, s.t. $a^{2l} = \left(a^l\right)^2 = 1$. Siis lemma 7.6 tõttu $2m \mid 2l$, ehk $m \mid l$. Kuna $m \leqslant l < 2m$ ja $m \mid l$, siis $m = l$ ja $a^m = a^l$. □

Näide 7.9. Näites 7.5 vaadeldud mittetsüklilises 4. järku rühmas $U(\mathbb{Z}_8)$ on kolm teist järku elementi: $\overline{3}, \overline{5}$ ja $\overline{7}$. Tsüklilises 4. järku rühmas $U(\mathbb{Z}_5)$ on aga täpselt üks teist järku element, see on $\overline{4}$.

Teoreemist 5.8 järeldub lihtsalt järgmine väide.

Lemma 7.10. *Iga naturaalarvu $n > 2$ korral on $\varphi(n)$ paarisarv.*

Pöördume tagasi küsimuse juurde, millal leidub mooduli n järgi algjuuri. Olgu $n = p_1^{k_1} \ldots p_s^{k_s}$, kus $p_1, \ldots, p_s$ on paarikaupa erinevad algarvud ja $k_1, \ldots, k_s \in \mathbb{N}$. Järelduse 4.9 ja lause 5.6 põhjal kehtib rühmade isomorfism

$$U(\mathbb{Z}_n) \cong U\left(\mathbb{Z}_{p_1^{k_1}} \times \ldots \times \mathbb{Z}_{p_s^{k_s}}\right) = U\left(\mathbb{Z}_{p_1^{k_1}}\right) \times \ldots \times U\left(\mathbb{Z}_{p_s^{k_s}}\right).$$

Oletame, et leiduvad erinevad $i, j \in \{1, \ldots, s\}$, nii et p_i ja p_j on paaritud algarvud. Üldisust kitsendamata eeldame, et $i = 1$ ja $j = 2$. Lemma 7.10 põhjal on $U\left(\mathbb{Z}_{p_1^{k_1}}\right)$ ja $U\left(\mathbb{Z}_{p_2^{k_2}}\right)$ paarisarvulist järku rühmad ning seega leiduvad lemma 7.7 põhjal teist järku elemendid $\overline{a} \in U\left(\mathbb{Z}_{p_1^{k_1}}\right)$ ja $\overline{b} \in U\left(\mathbb{Z}_{p_2^{k_2}}\right)$. Siis ka elemendid

$$\left(\overline{a}, \overline{1}, \overline{1}, \ldots, \overline{1}\right), \left(\overline{1}, \overline{b}, \overline{1}, \ldots, \overline{1}\right) \in U\left(\mathbb{Z}_{p_1^{k_1}}\right) \times \ldots \times U\left(\mathbb{Z}_{p_s^{k_s}}\right)$$

on teist järku. Lemma 7.8 põhjal rühm $U\left(\mathbb{Z}_{p_1^{k_1}}\right) \times \ldots \times U\left(\mathbb{Z}_{p_s^{k_s}}\right)$ ning järelikult ka sellega isomorfne rühm $U(\mathbb{Z}_n)$ ei saa olla tsükliline.

Oletame, et $n = 2^k p^l$, kus $p > 2$ on algarv ja $k \geqslant 2$. Siis jällegi rühmad $U\left(\mathbb{Z}_{2^k}\right)$ ja $U\left(\mathbb{Z}_{p^l}\right)$ on paarisarvulist järku, leiduvad teist järku elemendid $\overline{a} \in U\left(\mathbb{Z}_{2^k}\right)$ ja $\overline{b} \in U\left(\mathbb{Z}_{p^l}\right)$ ning seega ka elemendid $(\overline{a}, \overline{1}), (\overline{1}, \overline{b}) \in U\left(\mathbb{Z}_{2^k}\right) \times U\left(\mathbb{Z}_{p^l}\right)$ on teist järku, mistõttu $U(\mathbb{Z}_n)$ ei saa olla tsükliline.

Lõpuks oletame, et $n = 2^k$, kus $k \geqslant 3$. Siis $U\left(\mathbb{Z}_{2^k}\right)$ sisaldab jälle kaks erinevat teist järku elementi (ja seega ei saa olla tsükliline). Nendeks teist järku elementideks on $\overline{2^{k-1}-1}$ ja $\overline{2^{k-1}+1}$. Tõepoolest, kuna $k \geqslant 3$, siis $1 < 2^{k-1} - 1 < 2^k$ ja $1 < 2^{k-1} + 1 < 2^k$, seega $\overline{2^{k-1}-1} \neq \overline{1} \neq \overline{2^{k-1}+1}$. Lisaks sellele

$$\left(2^{k-1} \pm 1\right)^2 = 2^{2k-2} \pm 2^k + 1 \equiv 1 \pmod{2^k},$$

s.t. need elemendid on teist järku. Ning kuna $k \geqslant 3$, siis $2 \not\equiv 0 \pmod{2^k}$ ja seetõttu $2^{k-1} - 1 \not\equiv 2^{k-1} + 1 \pmod{2^k}$, ehk $\overline{2^{k-1}-1} \neq \overline{2^{k-1}+1}$.

Seega kui n ei ole kujul $2, 4, p^k$ ega $2p^k$, kus $p > 2$ on algarv, siis mooduli n järgi ei saa leiduda algjuuri, s.t. me oleme tõestanud järgmise tulemuse.

Lause 7.11. *Kui mooduli n järgi leidub algjuuri, siis n on kujul $2, 4, p^k$ või $2p^k$, kus $p > 2$ on algarv.*

7.2. Algjuurte leidmine

Näitame nüüd, et kui arvul n on lauses 7.11 mainitud kuju, siis mooduli n järgi leidub algjuuri. Arvude 2 ja 4 korral oleme seda juba teinud näites 7.5. Järgmisena sammuna veendume, et iga algarvulise mooduli järgi leidub algjuuri.

Teoreem 7.12. *Kui p on algarv, siis jäägiklassikorpuse $\mathbb{Z}_p$ multiplikatiivne rühm $\mathbb{Z}_p^*$ on tsükliline.*

TÕESTUS. Tähistagu $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{\overline{0}\} = U(\mathbb{Z}_p)$ korpuse $\mathbb{Z}_p$ pööratavate elementide rühma. Olgu K_d rühma $\mathbb{Z}_p^*$ kõigi selliste elementide hulk, mille järk on d. Kuna $\mathbb{Z}_p^*$ iga elemendi järk on Lagrange'i teoreemi põhjal arvu $p-1 = |\mathbb{Z}_p^*|$ jagaja ning elemendi järk on üheselt määratud, siis $\mathbb{Z}_p^* = \bigsqcup_{d \mid p-1} K_d$. Gaussi teoreemi (teoreem 5.11) põhjal

$$\sum_{d \mid p-1} \varphi(d) = p - 1 = |\mathbb{Z}_p^*| = \sum_{d \mid p-1} |K_d|. \tag{24}$$

Näitame, et iga $d \mid p-1$ korral $|K_d| = \varphi(d)$, ehk et rühmas $\mathbb{Z}_p^*$ leidub täpselt $\varphi(d)$ elementi, mille järk on d.

Oletame, et antud $d \mid p-1$ korral $K_d \neq \emptyset$, s.t. et leidub d-ndat järku element $\overline{a}$, ning tõestame, et sellisel juhul

$$K_d = \{\overline{a}^k \mid 1 \leqslant k \leqslant d, (k,d) = 1\}. \tag{25}$$

Kuna $\overline{a}$ järk on d, siis elemendid $\overline{a}, \overline{a}^2, \ldots, \overline{a}^d$ on erinevad ning nad rahuldavad võrrandit

$$x^d - \overline{1} = \overline{0},$$

sest $(\overline{a}^k)^d = (\overline{a}^d)^k = \overline{1}^k = \overline{1}$ iga $k = 1, \ldots, d$ korral. Kuna d-nda astme polünoomil üle korpuse $\mathbb{Z}_p$ ei saa lause 2.9 põhjal olla rohkem kui d juurt korpuses $\mathbb{Z}_p$, siis $\overline{a}, \overline{a}^2, \ldots, \overline{a}^d$ on polünoomi $x^d - \overline{1}$ ainsad juured, järelikult iga element $\overline{b} \in K_d$ on võrdne ühega neist elementidest; olgu $\overline{b} = \overline{a}^k$. Oletame vastuväiteliselt, et $(k,d) = d' > 1$. Siis elemendi $\overline{b}$ järk oleks väiksem kui d, sest $\overline{b}^{\frac{d}{d'}} = \left(\overline{a}^k\right)^{\frac{d}{d'}} = \left(\overline{a}^d\right)^{\frac{k}{d'}} = \overline{1}$ ja $\frac{d}{d'} < d$. Sellega oleme tõestanud, et $K_d \subseteq \{\overline{a}^k \mid 1 \leqslant k \leqslant d, (k,d) = 1\}$. Oletame nüüd, et $1 \leqslant k \leqslant d$ ja $(k,d) = 1$. Olgu m elemendi $\overline{a}^k$ järk rühmas $\mathbb{Z}_p^*$. Kuna $(\overline{a}^k)^d = \overline{1}$, siis $m \leqslant d$. Lisaks sellele $\overline{a}^{km} = \left(\overline{a}^k\right)^m = \overline{1}$. Kuna $\overline{a}$ järk on d, siis lemma 7.6 põhjal $d \mid km$. Järelduse 1.10 tõttu peab $d \mid m$, mis koos võrratusega $m \leqslant d$ annab, et $m = d$, s.t. $\overline{a}^k \in K_d$. Sellega oleme tõestanud võrduse (24).

Niisiis iga $d \mid p-1$ korral kas $|K_d| = \varphi(d)$ või $K_d = \emptyset$. Tänu võrdusele (24) ei ole aga viimane võrdus võimalik. Seega iga $d \mid p-1$ korral on täpselt $\varphi(d)$ elementi, mille järk on d. Muuhulgas, kuna $p-1 \mid p-1$, siis leidub $\varphi(p-1)$ elementi, mille järk on $p-1$, teiste sõnadega: leidub $\varphi(p-1)$ rühma $\mathbb{Z}_p^*$ moodustajat. Kui $\overline{a}$ on mingi moodustaja, siis ülejäänud moodustajaiks on eespooltõestatu põhjal astmed $\overline{a}^k$, kus $1 \leqslant k < p-1$ ja $(k, p-1) = 1$. □

Järeldus 7.13. *Kui p on algarv, siis mooduli p järgi leidub $\varphi(p-1)$ algjuurt. Täpsemalt, kui a on mingi algjuur mooduli p järgi, siis kõik ülejäänud algjuured kuuluvad ühte hulkadest $\overline{a}^k$, kus $1 \leqslant k < p-1$ ja $(k, p-1) = 1$.*

Järgnevalt näitame, kuidas leida algjuurt mooduli p^2 järgi, kui on teada mingi algjuur mooduli p järgi.

Teoreem 7.14. *Olgu $p > 2$ algarv. Kui a on algjuur mooduli p järgi, siis arvudest a ja $a+p$ vähemalt üks on algjuur mooduli p^2 järgi.*

Tõestus. Olgu a algjuur mooduli p järgi. Siis $\overline{a} \in U(\mathbb{Z}_p)$, s.t. $p \nmid a$ ning $\overline{a}$ järk selles rühmas on $|U(\mathbb{Z}_p)| = \varphi(p) = p-1$. Kuna $p \nmid a$, siis ka $p \nmid a+p$ ja seega $\left(p^2, a\right) = 1 = \left(p^2, a+p\right)$, mis tähendab, et $\overline{a}, \overline{a+p} \in U(\mathbb{Z}_{p^2})$. Tuleb näidata, et kas $\overline{a}$ või $\overline{a+p}$ järk rühmas $U(\mathbb{Z}_{p^2})$ on $\left|U(\mathbb{Z}_{p^2})\right| = \varphi(p^2) = p(p-1)$. Olgu m elemendi $\overline{a}$ järk rühmas $U(\mathbb{Z}_{p^2})$. Siis $a^m \equiv 1 \pmod{p^2}$, järelikult ka $a^m \equiv 1 \pmod{p}$, s.t. $\overline{a}^m = \overline{1}$ rühmas $U(\mathbb{Z}_p)$. Seega lemma 7.6 põhjal $p-1 \mid m$. Lagrange'i teoreemi tõttu aga $m \mid p(p-1)$. Seega leiduvad sellised $u, v \in \mathbb{N}$, et $(p-1)u = m$ ja $mv = p(p-1)$. Järelikult $(p-1)uv = p(p-1)$, millest arvu $p-1$ taandamisel saame, et $uv = p$ ehk $u = p$ või $v = p$ (sest p on algarv). See tähendab, et kas $m = (p-1)p$ või $m = p-1$.

Kui a on algjuur mooduli p järgi, siis ka $a+p$ on algjuur mooduli p järgi, sest ringis $\mathbb{Z}_p$ on $\overline{a} = \overline{a+p}$. Seetõttu saame $\overline{a+p}$ jaoks läbi viia sama arutluse, mis $\overline{a}$ jaoks. See tähendab, et ka elemendi $\overline{a+p}$ järk rühmas $U(\mathbb{Z}_{p^2})$ on kas $(p-1)p$ või $p-1$. Oletame vastuväiteliselt, et nii $\overline{a}$ kui ka $\overline{a+p}$ järk rühmas $U(\mathbb{Z}_{p^2})$ on $p-1$, muuhulgas $a^{p-1} \equiv 1 \pmod{p^2}$ ja $(a+p)^{p-1} \equiv 1 \pmod{p^2}$. Newtoni binoomvalemi põhjal

$$1 \equiv (a+p)^{p-1} \equiv a^{p-1} + (p-1)a^{p-2}p \equiv 1 + (p-1)a^{p-2}p \pmod{p^2},$$

millest saame, et $(p-1)a^{p-2}p \equiv 0 \pmod{p^2}$. Lause 3.10 põhjal $(p-1)a^{p-2} \equiv 0 \pmod{p}$ ehk $p \mid (p-1)a^{p-2}$. Kuna $p \nmid p-1$ ja $p \nmid a$, siis oleme saanud vastuolu. Järelikult peab kas elemendi $\overline{a}$ või elemendi $\overline{a+p}$ järk rühmas $U(\mathbb{Z}_{p^2})$ olema $(p-1)p$, s.t. vähemalt üks arvudest a ja $a+p$ on algjuur mooduli p^2 järgi. □

Järeldus 7.15. *Kui $p > 2$ on algarv, a on algjuur mooduli p järgi, $b \in \{a, a+p\}$ ja $b^{p-1} \not\equiv 1 \pmod{p^2}$, siis b on algjuur mooduli p^2 järgi.*

Näide 7.16. Leiame mingi algjuure mooduli 25 järgi. Nagu näites 7.5 veendusime on üheks algjuureks mooduli 5 järgi arv 2. Järelduse 7.15 põhjal on algjuureks mooduli 25 järgi see arvudest 2 ja $2+5$, mille jäägiklassi järk rühmas $U(\mathbb{Z}_{5^2})$ ei ole $5-1 = 4$. Kuna $\overline{2}^4 = \overline{16} \neq \overline{1}$, siis üheks algjuureks mooduli 25 järgi on 2.

Selleks, et minna ruudult üle kõrgemaile p astmeile, vajame järgmist abitulemust.

Lemma 7.17. *Kui p on algarv ja $1 \leqslant k \leqslant p-1$ on naturaalarv, siis p jagab binoomkordajat $\binom{p}{k}$.*

Tõestus. Definitsiooni järgi

$$\binom{p}{k} = \frac{p(p-1)\dots(p-k+1)}{k!},$$

ehk $\binom{p}{k}k! = p(p-1)\dots(p-k+1)$. Kuna p jagab selle võrduse paremat poolt, siis peab ta jagama ka vasakut poolt. Et aga $p \nmid k!$, siis $p \mid \binom{p}{k}$. □

Teoreem 7.18. *Olgu $p > 2$ algarv. Siis iga algjuur mooduli p^2 järgi on ka algjuur mooduli p^k järgi, kus $k > 2$.*

Tõestus. Olgu a algjuur mooduli p^2 järgi. Tõestame induktsiooniga l järgi, et

$$\text{iga } l \in \mathbb{N} \text{ korral leidub } t_l \in \mathbb{Z} \text{ nii, et } a^{(p-1)p^{l-1}} = 1 + t_l p^l \text{ ja } p \nmid t_l. \tag{26}$$

Vaatleme kõigepealt juhtu $l = 1$. Kuna a on algjuur mooduli p^2 järgi, siis $\overline{a} \in U(\mathbb{Z}_{p^2})$ ja seega $p \nmid a$. Fermat' väikese teoreemi põhjal $a^{p-1} \equiv 1 \pmod p$. Järelikult leidub selline $t_1 \in \mathbb{Z}$, et $a^{p-1} = 1 + t_1 p$. Kui oletada, et $p \mid t_1$, siis $a^{p-1} \equiv 1 \pmod{p^2}$ ehk $\overline{a}^{p-1} = \overline{1}$ rühmas $U(\mathbb{Z}_{p^2})$, mis on vastuolus sellega, et a on algjuur mooduli p^2 järgi. Seega $p \nmid t_1$.

Oletame nüüd, et $l > 1$ ja $l-1$ korral leidub selline täisarv t_{l-1}, et $a^{(p-1)p^{l-2}} = 1 + t_{l-1}p^{l-1}$ ja $p \nmid t_{l-1}$. Siis

$$\begin{aligned}
a^{(p-1)p^{l-1}} &= \left(a^{(p-1)p^{l-2}}\right)^p = (1 + t_{l-1}p^{l-1})^p \\
&= 1 + \binom{p}{1}t_{l-1}p^{l-1} + \binom{p}{2}t_{l-1}^2\left(p^{l-1}\right)^2 + \dots + \binom{p}{p-1}t_{l-1}^{p-1}\left(p^{l-1}\right)^{p-1} + \binom{p}{p}t_{l-1}^p\left(p^{l-1}\right)^p \\
&= 1 + \left(t_{l-1} + \binom{p}{2}t_{l-1}^2 p^{2(l-1)-l} + \dots + \binom{p}{p-1}t_{l-1}^{p-1}p^{(p-1)(l-1)-l} + t_{l-1}^p p^{p(l-1)-l}\right)p^l \\
&= 1 + t_l p^l,
\end{aligned}$$

kus

$$t_l = t_{l-1} + \binom{p}{2}t_{l-1}^2 p^{2(l-1)-l} + \dots + \binom{p}{p-1}t_{l-1}^{p-1}p^{(p-1)(l-1)-l} + t_{l-1}^p p^{p(l-1)-l} \in \mathbb{Z}$$

ja p^l sulgude taha võtmisel oleme arvestanud, et iga $m \geqslant 2$ korral $m(l-1)-l = m(l-1)-l+1-1 = (m-1)(l-1)-1 \geqslant 0$. Kuna $p > 2$, siis $p(l-1) - l = (p-1)(l-1) - 1 \geqslant 1$ ja seega $p \mid t_{l-1}^p p^{p(l-1)-l}$. Lisaks sellele, lemma 7.17 tõttu $p \mid \sum_{i=2}^{p-1}\binom{p}{i}t_{l-1}^i p^{i(l-1)-l}$ ning seega

$$p \mid \sum_{i=2}^{p}\binom{p}{i}t_{l-1}^i p^{i(l-1)-l} = t_l - t_{l-1}.$$

Kui oletada, et $p \mid t_l$, siis ka $p \mid t_{l-1}$, mis ei ole aga induktsiooni eelduse tõttu võimalik. Seega $p \nmid t_l$ ja väide (26) on tõestatud.

Olgu m elemendi $\overline{a}$ järk rühmas $U(\mathbb{Z}_{p^k})$. Siis $\overline{a}^m = \overline{1}$ ehk $a^m \equiv 1 \pmod{p^k}$ ja $m \mid \left|U(\mathbb{Z}_{p^k})\right| = \varphi(p^k) = (p-1)p^{k-1}$. Tuleb näidata, et $m = (p-1)p^{k-1}$. Kuna $a^m \equiv 1 \pmod{p^k}$ ja $k > 2$, siis ka $a^m \equiv 1 \pmod{p^2}$, järelikult lemma 7.6 põhjal $(p-1)p \mid m$ (sest $\overline{a}$ järk rühmas $U(\mathbb{Z}_{p^2})$ on $(p-1)p$). Niisiis leiduvad sellised $u, v \in \mathbb{Z}$, et $mu = (p-1)p^{k-1}$ ja $(p-1)pv = m$ ning seega $(p-1)p^{k-1} = (p-1)pvu$. Taandades $(p-1)p$ saame $p^{k-2} = vu$. Seega $v = p^{r-2}$, kus $2 \leqslant r \leqslant k$, ning $m = (p-1)p^{r-1}$. Järelikult

$$1 + t_r p^r = a^{(p-1)p^{r-1}} = a^m \equiv 1 \pmod{p^k},$$

millest saame, et $t_r p^r \equiv 0 \pmod{p^k}$ ehk $p^k \mid t_r p^r$. Kuna $p \nmid t_r$ siis $p^k \mid p^r$ ehk $k \leqslant r$. Koos võrratusega $r \leqslant k$ annab see, et $r = k$ ja $m = (p-1)p^{k-1}$. □

Teoreem 7.19. *Kui a on algjuur mooduli p^k järgi, kus $p > 2$ on algarv, siis üheks algjuureks mooduli $2p^k$ järgi on paaritu arv arvudest a ja $a + p^k$.*

Tõestus. Kuna p^k on paaritu arv, siis täpselt üks arvudest a ja $a + p^k$ on paaritu. Oletame, et a on paaritu (juhul kui $a + p^k$ on paaritu, saab väite tõestada analoogiliselt). Kui a on algjuur mooduli p^k järgi, siis $\overline{a} \in U(\mathbb{Z}_{p^k})$, millest järeldub, et $(a, p^k) = 1$. Kuna a on paaritu, siis ka $(a, 2) = 1$ ja seega $(a, 2p^k) = 1$, s.t. $\overline{a} \in U(\mathbb{Z}_{2p^k})$. Sellest, et a on algjuur mooduli p^k järgi, järeldub, et elemendi $\overline{a}$ järk rühmas $U(\mathbb{Z}_{p^k})$ on $m = \left|U(\mathbb{Z}_{p^k})\right| = p^{k-1}(p-1)$. Olgu n elemendi $\overline{a}$ järk rühmas $U(\mathbb{Z}_{2p^k})$. Siis $n \mid \left|U(\mathbb{Z}_{2p^k})\right| = p^{k-1}(p-1) = m$, järelikult $n \leqslant m$. Teiselt poolt aga sellest, et $a^n \equiv 1 \pmod{2p^k}$ järeldub, et $a^n \equiv 1 \pmod{p^k}$ ja seega lemma 7.6 põhjal $m \leqslant n$. Oleme saanud võrduse $n = m$, mida oligi tarvis tõestada. □

Näide 7.20. Leiame mingi algjuure mooduli $2 \cdot 5^{2012}$ järgi. Näites 7.16 nägime, et 2 on algjuur mooduli 5^2 järgi. Teoreemi 7.18 põhjal on 2 algjuur ka mooduli 5^{2012} järgi. Teoreemile 7.19 tuginedes on üheks algjuureks mooduli $2 \cdot 5^{2012}$ järgi arv $2 + 5^{2012}$.

Tehtu võime kokku võtta järgmise teoreemina.

Teoreem 7.21. *Mooduli n järgi leidub algjuuri parajasti siis, kui n on kujul 2, 4, p^k või $2p^k$, kus $p > 2$ on algarv.*

Teoreemid 7.14, 7.18 ja 7.19 annavad lihtsa võimaluse algjuurte leidmiseks mooduli p^k või $2p^k$ järgi, kui teame mingit algjuurt mooduli p järgi. Algjuuri mooduli p järgi aitab leida järgmine lemma.

Lemma 7.22. *Olgu G lõplik rühm, mille järk $|G| = n = p_1^{k_1} \dots p_s^{k_s}$ on antud standardkujul. Iga $a \in G$ korral, $\langle a \rangle \neq G$ parajasti siis, kui leidub selline $i \in \{1, \dots, s\}$, et $a^{\frac{n}{p_i}} = 1$.*

Tõestus. Tarvilikkus. Oletame, et $\langle a \rangle \neq G$. Olgu m elemendi a järk. Siis $m \mid n$ ning seega $m = p_1^{l_1} \dots p_s^{l_s}$, kus iga $i \in \{1, \dots, s\}$ korral $0 \leqslant l_i \leqslant k_i$. Kuna $\langle a \rangle \neq G$, siis a järk on väiksem kui n. Seega peab leiduma selline i, et $l_i < k_i$. Sellisel juhul $m \mid \frac{n}{p_i}$ ja seega $a^{\frac{n}{p_i}} = 1$.
Piisavus. Kui $a^{\frac{n}{p_i}} = 1$, siis elemendi a järk on väiksem kui n ning järelikult $\langle a \rangle \neq G$. □

Järeldus 7.23. *Olgu G lõplik rühm, mille järk $|G| = n = p_1^{k_1} \dots p_s^{k_s}$ on antud standardkujul. Iga $a \in G$ korral, $\langle a \rangle = G$ parajasti siis, kui iga $i \in \{1, \dots, s\}$ korral $a^{\frac{n}{p_i}} \neq 1$.*

Järeldus 7.24. *Olgu $p > 2$ algarv. Siis a on algjuur mooduli p järgi parajasti siis, kui arvu $p - 1$ iga algteguri q korral $a^{\frac{p-1}{q}} \not\equiv 1 \pmod{p}$.*

Tõestus. Rakendame järeldust 7.23 juhul $G = U(\mathbb{Z}_p)$. □

Näide 7.25. Olgu $p = 13$. Kuna $p - 1 = 12 = 2^2 \cdot 3$, $2^6 = 64 \equiv -1 \not\equiv 1 \pmod{13}$ ja $2^4 = 16 \equiv 3 \not\equiv 1 \pmod{13}$, siis 2 on algjuur mooduli 13 järgi. Teoreemi 7.12 tõestuse põhjal on rühmal $U(\mathbb{Z}_{13})$ kokku $\varphi(12) = 4$ moodustajat ning nendeks on jäägiklassid $\overline{2}^k$, kus $1 \leqslant k \leqslant 12$ ja $(k, 12) = 1$, s.t. $\overline{2}^1 = \overline{2}$, $\overline{2}^5 = \overline{6}$, $\overline{2}^7 = \overline{11}$, $\overline{2}^{11} = \overline{7}$.

Lause 7.26. *Olgu n naturaalarv. Siis n-elemendilisel tsüklilisel rühmal on täpselt $\varphi(n)$ moodustajat.*

Tõestus. Olgu $G = \{1, a, a^2, \dots, a^{n-1}\}$ tsükliline rühm, kus $a^n = 1$. Esitame n standardkujul: $n = p_1^{k_1} \dots p_s^{k_s}$. Piisab näidata, et iga $k \in \{1, \dots, n\}$ korral $\langle a^k \rangle = G$ parajasti siis, kui $(k, n) = 1$. Selleks tõestame, et

$$\langle a^k \rangle \neq G \text{ parajasti siis, kui } (k, n) \neq 1.$$

Oletame esiteks, et $\langle a^k \rangle \neq G$. Lemma 7.22 põhjal leidub siis selline $i \in \{1, \dots, s\}$, et $\left(a^k\right)^{\frac{n}{p_i}} = 1$ rühmas G. Lemma 7.6 põhjal $n \mid \frac{kn}{p_i}$, s.t. leidub selline $u \in \mathbb{N}$, et $nu = \frac{kn}{p_i}$. Järelikult $up_i = k$, millest saame, et $p_i \mid k$. Seega $(k, n) \geqslant p_i > 1$. Vastupidi, oletame, et $(k, n) = d > 1$. Siis leidub selline $i \in \{1, \dots, s\}$, et $p_i \mid d$. Järelikult ka $p_i \mid k$. Olgu $k = p_i k'$, kus $k' \in \mathbb{N}$. Siis

$$\left(a^k\right)^{\frac{n}{p_i}} = a^{k'n} = (a^n)^{k'} = 1$$

ning lemma 7.22 põhjal $\langle a^k \rangle \neq G$. □

Rakendades lauset 7.26 rühmale $U(\mathbb{Z}_n)$ saame järgmise tulemuse.

Teoreem 7.27. *Kui mooduli n järgi leidub algjuuri, siis on neid täpselt $\varphi(\varphi(n))$ tükki.*

7.3. Indeksid

Algjuurte olemasolul on võimalik arvutusi, sealhulgas kongruentside lahendamist mooduli n järgi lihtsustada nn. indeksarvutuse abil. Põhimõtteliselt on indeksite näol tegemist logaritmidega jäägiklassiringides. Eelnevast teame, et kui mooduli n järgi leidub algjuur a, siis

$$\{\overline{b} \in \mathbb{Z}_n \mid (b,n)=1\} = U(\mathbb{Z}_n) = \{\overline{a}, \overline{a}^2, \ldots, \overline{a}^{\varphi(n)} = \overline{1}\}.$$

Seetõttu omab mõtet järgmine definitsioon:

Definitsioon 7.28. Olgu a algjuur mooduli n järgi ja b selline täisarv, et $(b,n)=1$. Siis arvu b *indeksiks* alusel a mooduli n järgi nimetatakse vähimat võimalikku positiivset astendajat k, mille korral

$$b \equiv a^k \pmod{n}.$$

Arvu b indeksit tähistatakse $k = \operatorname{ind}_a b$ või $k = \operatorname{ind} b$, kui algjuur a on kontekstist leitav.

Edaspidi eeldame vaikimisi, et mooduli n järgi leidub algjuuri ja et kirjutis $\operatorname{ind}_a b$ sisaldab endas eeldust $(b,n)=1$.

Näide 7.29. Näite 7.25 põhjal on arv 2 algjuur mooduli 13 järgi ja arvutades saame, et

$$2^1 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 8, 2^4 \equiv 3, 2^5 \equiv 6, 2^6 \equiv 12, 2^7 \equiv 11, 2^8 \equiv 9, 2^9 \equiv 5, 2^{10} \equiv 10, 2^{11} \equiv 7, 2^{12} \equiv 1 \pmod{13}.$$

Järelikult $\operatorname{ind}_2 1 = 12$, $\operatorname{ind}_2 2 = 1$, $\operatorname{ind}_2 3 = 4$, $\operatorname{ind}_2 4 = 2$, $\operatorname{ind}_2 5 = 9$, $\operatorname{ind}_2 6 = 5$, $\operatorname{ind}_2 7 = 11$, $\operatorname{ind}_2 8 = 3$, $\operatorname{ind}_2 9 = 8$, $\operatorname{ind}_2 10 = 10$, $\operatorname{ind}_2 11 = 7$, $\operatorname{ind}_2 12 = 6$. Saadud tulemused võime kokku võtta alljärgneva tabeliga, kus esimeses reas on indekseeritava arvu viimane kümnendnumber ja esimeses veerus kümneliste number.

	0	1	2	3	4	5	6	7	8	9
0		12	1	4	2	9	5	11	3	8
1	10	7	6							

Paljude moodulite jaoks on sellised *indeksite tabelid* juba välja arvutatud (vt. näiteks [3], lk. 330–335).

Lause 7.30. *Kongruents*

$$b \equiv c \pmod{n} \tag{27}$$

on samaväärne kongruentsiga

$$\operatorname{ind}_a b \equiv \operatorname{ind}_a c \pmod{\varphi(n)}. \tag{28}$$

Tõestus. Olgu $b \equiv c \pmod{n}$. Kuna $c \equiv b \equiv a^{\operatorname{ind}_a b} \pmod{n}$, siis $\operatorname{ind}_a c \le \operatorname{ind}_a b$. Analoogiliselt $\operatorname{ind}_a b \le \operatorname{ind}_a c$ ja $\operatorname{ind}_a b = \operatorname{ind}_a c$, mistõttu ka $\operatorname{ind}_a b \equiv \operatorname{ind}_a c \pmod{\varphi(n)}$. Teisipidi, olgu $\operatorname{ind}_a b \equiv \operatorname{ind}_a c \pmod{\varphi(n)}$ ja üldisust kitsendamata $\operatorname{ind}_a b \ge \operatorname{ind}_a c$. Siis $\varphi(n) \mid \operatorname{ind}_a b - \operatorname{ind}_a c$. Kuna a on algjuur, siis $\overline{a}$ järk on $\varphi(n)$ ja lemma 7.6 tõttu $a^{\operatorname{ind}_a b - \operatorname{ind}_a c} \equiv 1 \pmod{n}$. Korrutades tulemust kongruentsiga $a^{\operatorname{ind}_a c} \equiv a^{\operatorname{ind}_a c} \pmod{n}$, saamegi, et $b \equiv a^{\operatorname{ind}_a b} \equiv a^{\operatorname{ind}_a c} \equiv c \pmod{n}$. □

Üleminekut kongruentsilt (27) kongruentsile (28) nimetatakse *indekseerimiseks* ja vastupidist sammu *potentseerimiseks*. Paneme siinkohal tähele, et lause 7.30 tõestuse kohaselt on kongruents (28) hoopiski võrdus. Tegelikult kehtib järgmine, üldisem väide, kus kongruents ei taandu enam võrdusele.

Lemma 7.31. *Olgu a algjuur mooduli n järgi ja $s,t \in \mathbb{N}$. Siis $a^s \equiv a^t \pmod{n}$ parajasti siis, kui $s \equiv t \pmod{\varphi(n)}$.*

Tõestus. Tõestuse piisavuse osa on identne lause 7.30 tõestuse vastava osaga. Tarvilikkuse tõestamiseks oletame üldisust kitsendamata, et $0 \le s \le t$. Kuna $\varphi(n) \ge 1$, siis $\varphi(n)\cdot s - s \ge 0$ ja Euleri teoreemi (teoreem 5.12) põhjal

$$a^{\varphi(n)\cdot s - s} \cdot a^s = a^{\varphi(n)\cdot s - s + s} = \left(a^{\varphi(n)}\right)^s \equiv 1^s = 1 \pmod{n}.$$

Seetõttu saame kongruentsi $a^s \equiv a^t \pmod{n}$ mõlemat poolt arvuga $a^{\varphi(n)\cdot s - s}$ läbi korrutades, et

$$a^{t-s} = a^{t-s}\cdot 1^s \equiv a^{t-s}\cdot\left(a^{\varphi(n)}\right)^s = a^t \cdot a^{\varphi(n)\cdot s - s} \equiv a^s \cdot a^{\varphi(n)\cdot s - s} \equiv 1 \pmod{n}.$$

Lemma 7.6 kohaselt jagab elemendi $\overline{a}$ järk (mis on $\varphi(n)$, sest a on algjuur) astendajat $t-s$. Teisisõnu, $\varphi(n) \mid t-s$ ehk $s \equiv t \pmod{\varphi(n)}$, mida oligi tarvis tõestada. □

Indeksitel on mitmeid logaritmidega sarnaseid omadusi, kus algjuur a on logaritmi aluse rollis.

Teoreem 7.32. *Olgu a, α algjuured mooduli n järgi, $l \in \mathbb{N}$ ja $b, c, d \in \mathbb{Z}$ sellised, et $(b, n) = 1 = (c, n)$ ja $d \mid b$. Siis*

1. $1 \leq \operatorname{ind}_a b \leq \varphi(n)$, $a^{\operatorname{ind}_a b} \equiv b \pmod{n}$;
2. $\operatorname{ind}_a 1 = \varphi(n) \equiv 0 \pmod{\varphi(n)}$, $\operatorname{ind}_a a = 1$;
3. $\operatorname{ind}_a(bc) \equiv \operatorname{ind}_a(b) + \operatorname{ind}_a(c) \pmod{\varphi(n)}$;
4. $\operatorname{ind}_a b^l \equiv l \cdot \operatorname{ind}_a b \pmod{\varphi(n)}$;
5. $\operatorname{ind}_a \left(\frac{b}{d}\right) \equiv \operatorname{ind}_a b - \operatorname{ind}_a d \pmod{\varphi(n)}$;
6. $\operatorname{ind}_\alpha b \equiv \operatorname{ind}_a b \cdot \operatorname{ind}_\alpha a \pmod{\varphi(n)}$;
7. $\operatorname{ind}_a \alpha \cdot \operatorname{ind}_\alpha a \equiv 1 \pmod{\varphi(n)}$.

TÕESTUS. Omadused 1. ja 2. järelduvad vahetult indeksi definitsioonist. Omadus 6. on omaduse 7. erijuht, kus $b = \alpha$. Omadused 3.-5. ja 7. tõestatakse ühe ja sama skeemi abil, mistõttu põhjendame siinkohal ära vaid ühe neist ja jätame ülejäänud lugejale kontrollimiseks.

5. Kuna $(b, n) = 1$ ja $d \mid b$, siis ka $(d, n) = 1$ ehk $\overline{d} \in U(\mathbb{Z}_n)$. Paneme nüüd tähele, et $\frac{b}{d} \equiv be \pmod{n}$, kus $de \equiv 1 \pmod{n}$, st. $\overline{e} = \overline{d}^{-1}$. Tõepoolest, lause 3.7 ja järelduse 3.11 põhjal on kongruents $\frac{b}{d} \equiv be \pmod{n}$ samaväärne samaselt tõese kongruentsiga $b = \frac{b}{d} \cdot d \equiv be \cdot d \equiv b \cdot 1 = b \pmod{n}$. Lemma 7.31 tõttu saame kirjutada, et

$$a^{\operatorname{ind}_a\left(\frac{b}{d}\right)} = a^{\operatorname{ind}_a be} \equiv be \equiv a^{\operatorname{ind}_a b} \cdot a^{\operatorname{ind}_a e} = a^{\operatorname{ind}_a b + \operatorname{ind}_a e} \pmod{n}.$$

Lemma 7.31 abil indekseerides nüüd $\operatorname{ind}_a \left(\frac{b}{d}\right) \equiv \operatorname{ind}_a b + \operatorname{ind}_a e \pmod{\varphi(n)}$. Tõestuse lõpetamiseks piisab näitamisest, et $\operatorname{ind}_a e \equiv -\operatorname{ind}_a d \pmod{\varphi(n)}$. Selleks paneme tähele, et omaduse 2. ning lemmade 7.6 ja 7.31 tõttu

$$a^{\operatorname{ind}_a d + \operatorname{ind}_a e} = a^{\operatorname{ind}_a de} \equiv de \equiv 1 = a^{\varphi(n)} \pmod{n}.$$

Uuesti lemmat 7.31 kasutades saame, et $\operatorname{ind}_a d + \operatorname{ind}_a e \equiv \varphi(n) \pmod{\varphi(n)}$ ehk tõepoolest $\operatorname{ind}_a e \equiv -\operatorname{ind}_a d \pmod{\varphi(n)}$. □

Indeksid võimaldavad meil lahendada lineaarkongruentse kujul

$$sx^m \equiv t \pmod{n}, \quad s, t \in \mathbb{Z}, \tag{29}$$

sest indekseerimisel saame me lemma 7.31 ja teoreemi 7.32 abil samaväärse lineaarkongruentsi

$$\operatorname{ind}_a s + m \cdot \operatorname{ind}_a x \equiv \operatorname{ind}_a t \pmod{\varphi(n)}. \tag{30}$$

Lineaarkongruentse oskame me aga lause 6.2 abil lihtsasti lahendada. Kuna lineaarkongruentsid kujul (29) on teisendatavad kujule

$$x^m \equiv u \pmod{n'},$$

kus n' on n jagaja, siis osutub otstarbekaks järgmine lahenduvuskriteerium.

Teoreem 7.33. *Olgu a algjuur mooduli n järgi ja olgu $b \in \mathbb{Z}$ selline, et $(b, n) = 1$. Tähistame $d = (m, \varphi(n))$. Kongruents $x^m \equiv b \pmod{n}$ on lahenduv siis ja ainult siis, kui*

$$b^{\varphi(n)/d} \equiv 1 \pmod{n}.$$

Juhul, kui kongruents $x^m \equiv b \pmod{n}$ on lahenduv, on tal täpselt d erinevat lahendit.

TÕESTUS. Indekseerides saame, et kongruents $b^{\varphi(n)/d} \equiv 1 \pmod{n}$ on lahenduv parajasti siis, kui

$$\varphi(n)/d \cdot \operatorname{ind}_a b \equiv \operatorname{ind}_a 1 = \varphi(n) \equiv 0 \pmod{\varphi(n)}.$$

Viimane kongruents kehtib parajasti siis, kui $d \mid \operatorname{ind}_a b$. Lause 6.2 kohaselt on selline jaguvusseos samaväärne lineaarkongruentsi $m \cdot \operatorname{ind}_a x \equiv \operatorname{ind}_a b \pmod{\varphi(n)}$ lahenduvusega tundmatu $\operatorname{ind}_a x$ suhtes, mis tagasi potentseerides tähendabki kongruentsi

$$x^m \equiv a^{\operatorname{ind}_a x^m} \equiv a^{m \cdot \operatorname{ind}_a x} \equiv a^{\operatorname{ind}_a b} \equiv b \pmod{n}$$

lahenduvust.

Oletame viimaks, et kongruents $x^m \equiv c$ on lahenduv. Eelneva põhjal on kõik selle kongruentsi lahendid vastavuses lineaarkongruentsi $m \cdot \operatorname{ind}_a x \equiv \operatorname{ind}_a b \pmod{\varphi(n)}$ lahenditega, mida on lause 6.2 põhjal $(m, \varphi(n)) = d$ tükki. □

Järeldus 7.34 (Euler). *Olgu p algarv, $b \in \mathbb{Z}$, $(b,p)=1$ ja $d=(m,p-1)$. Siis kongruents $x^m \equiv b \pmod p$ on lahenduv parajasti siis, kui*

$$b^{(p-1)/d} \equiv 1 \pmod p.$$

Näide 7.35. Lahendame kongruentsi

$$5 \cdot x^{2013} \equiv 12 \pmod{13}.$$

On lihtne näha, et $5 \cdot 8 = 40 \equiv 1 \pmod{13}$, ehk $\overline{5}^{-1} = \overline{8}$, seega võime antud kongruentsi teisendada kujule

$$x^{2013} \equiv 8 \cdot 12 \equiv 5 \pmod{13}.$$

Kuna $\varphi(13)=12$, siis

$$5^{12/(2013,12)} = 5^{12/3} = 5^4 = 25^2 \equiv (-1)^2 = 1 \pmod{13}.$$

Järelikult teoreemi 7.33 põhjal on kongruents $x^{2013} \equiv 5 \pmod{13}$ lahenduv ja tal on $(2013, \varphi(13)) = (2013,12) = 3$ erinevat lahendit. Leiame need. Indekseerides saame, et $2013 \cdot \operatorname{ind} x \equiv \operatorname{ind} 5 \pmod{12}$, mis näites 7.29 koostatud indeksite tabeli põhjal on samaväärne lineaarkongruentsiga

$$2013 \cdot \operatorname{ind} x \equiv 9 \pmod{12}.$$

Jagades selle kongruentsi mõlemad pooled ja mooduli läbi arvuga 3 (seda lubab meil teha lause 3.10) on tulemuseks, et $3 \cdot \operatorname{ind} x \equiv 671 \cdot \operatorname{ind} x \equiv 3 \pmod 4$. Kuna $\overline{3} \in U(\mathbb{Z}_4)$, siis $\operatorname{ind} x \equiv 1 \pmod 4$. Tänu teoreemi 7.32 omadusele 1. saame, et $\operatorname{ind} x = 1, 5, 9$, sest need on ainsad täisarvud vahemikust $[1, \varphi(13) = 12]$, mis rahuldavad seost $\operatorname{ind} x \equiv 1 \pmod 4$. Näites 7.29 leitud tabelit tagurpidi kasutades saamegi vastuse, milleks on $x \equiv 2, 6, 5 \pmod{13}$.
Kontroll: astendades $2^{2013} = 2^{167 \cdot 12+9} = (2^{12})^{167} \cdot 2^9 \equiv 1 \cdot (2^4)^2 \cdot 2 = 16^2 \cdot 2 \equiv 3^2 \cdot 2 = 18 \equiv 5 \pmod{13}$,

$$5^{2013} = 5^{167 \cdot 12+9} = (5^{12})^{167} \cdot 5^9 \equiv 1 \cdot (5^2)^4 \cdot 5 = 25^4 \cdot 5 \equiv (-1)^4 \cdot 5 = 5 \pmod{13},$$

$$6^{2013} = 6^{167 \cdot 12+9} = (6^{12})^{167} \cdot 6^9 \equiv 1 \cdot (6^2)^4 \cdot 6 = 36^4 \cdot 65 \equiv (10^2)^2 \cdot 6 \equiv (-4)^2 \cdot 6 = 16 \cdot 6 \equiv 3 \cdot 6 = 18 \equiv 5 \pmod{13}.$$

Järelikult $5 \cdot 2^{2013} \equiv 5 \cdot 5^{2013} \equiv 5 \cdot 6^{2013} \equiv 5^2 = 25 \equiv 12 \pmod{13}$.

Peale kongruentside lahendamise saab indekseid ja nende tabeleid kasutada algjuurte ning pööratavate elementide järkude leidmisel. Täpsemalt, alltoodud teoreem võimaldab meil indeksite tabelite abil lahendada järgmisi ülesandeid

- leida pööratava elemendi järk rühmas $U(\mathbb{Z}_n)$,
- leida kõik algjuured mooduli n järgi,
- leida kõik fikseeritud järku elemendid rühmas $U(\mathbb{Z}_n)$,
- jaotada kõik rühma $U(\mathbb{Z}_n)$ elemendid klassidesse vastavalt järgule.

Teoreem 7.36. *Olgu a algjuur mooduli n järgi ja $b \in \mathbb{Z}$ selline, et $(b,n)=1$. Siis*

1. *elemendi $\overline{b}$ järk rühmas $U(\mathbb{Z}_n)$ on $\frac{\varphi(n)}{(\operatorname{ind}_a b, \varphi(n))}$,*
2. *b on algjuur mooduli n järgi parajasti siis, kui $(\operatorname{ind}_a b, \varphi(n)) = 1$,*
3. *kui $m \mid \varphi(n)$, siis rühma $U(\mathbb{Z}_n)$ m. järku elemendid on need ja ainult need jäägiklassid $\overline{b}$, mille korral*

$$(\operatorname{ind}_a b, \varphi(n)) = \frac{\varphi(n)}{m}.$$

Tõestus. 1. Tähistame edaspidi $d = (\operatorname{ind}_a b, \varphi(n))$, $\varphi' = \frac{\varphi(n)}{d}$ ja $\operatorname{ind}' = \frac{\operatorname{ind}_a b}{d}$. Paneme muuseas tähele, et järelduse 1.9 põhjal $(\varphi', \operatorname{ind}') = 1$. Olgu m elemendi $\overline{b}$ järk rühmas $U(\mathbb{Z}_n)$. Kuna a on algjuur, siis $a^{\varphi(n)} \equiv 1 \pmod n$ ja

$$b^{\varphi'} \equiv (a^{\operatorname{ind}_a b})^{\varphi'} = a^{\operatorname{ind}_a b \cdot \varphi'} = a^{\operatorname{ind}' \cdot d \cdot \varphi'} = a^{\operatorname{ind}' \cdot \varphi(n)} = (a^{\varphi(n)})^{\operatorname{ind}'} \equiv 1 \pmod n,$$

järelikult lemma 7.6 tõttu $m \mid \varphi'$. Teisipidi, elemendi järgu definitsioonist $b^m \equiv 1 \pmod n$, seega

$$1 \equiv b^m \equiv (a^{\operatorname{ind}_a b})^m = a^{m \cdot \operatorname{ind}_a b}.$$

Kasutades uuesti asjaolu, et $\overline{a}$ järk on $\varphi(n)$, ja lemmat 7.6, saame nüüd, et $\varphi(n) \mid m \cdot \operatorname{ind}_a b$ ehk

$$m \cdot \operatorname{ind}' \cdot d \equiv 0 \pmod{\varphi' \cdot d}.$$

Jagades viimase kongruentsi läbi teguriga $d \neq 0$, on tulemuseks $m \cdot \operatorname{ind}' \equiv 0 \pmod{\varphi'}$. Teisisõnu, $\varphi' \mid m \cdot \operatorname{ind}'$, mis Eukleidese lemma tõttu annab meile, et $\varphi' \mid m$. Kokkuvõttes oleme näidanud, et m ja φ' on positiivsed, teineteist jagavad täisarvud, mis saab kehtida vaid juhul, kui $m = \varphi' = \frac{\varphi(n)}{(\operatorname{ind}_a b, \varphi(n))}$.

2. Kuna algjuureks olek on samaväärne $\varphi(n)$. järku elemendiks olemisega, siis osa 1. põhjal on b algjuur parajasti siis, kui $\varphi(n) = \frac{\varphi(n)}{(\operatorname{ind}_a b, \varphi(n))}$. Viimane seos kehtib ilmselt parajasti siis, kui $(\operatorname{ind}_a b, \varphi(n)) = 1$.

3. Eelduse kohaselt $m \mid \varphi(n)$ ja 1. osa põhjal $m = \frac{\varphi(n)}{(\operatorname{ind}_a b, \varphi(n))}$, järelikult $(\operatorname{ind}_a b, \varphi(n)) = \frac{\varphi(n)}{m}$. □

Näide 7.37. Leiame elemendi $\overline{17}$ järgu jäägiklassiringis $\mathbb{Z}_{19}$, kõik algjuured mooduli 19 järgi ja kõik ringi $\mathbb{Z}_{19}$ kolmandat järku elemendid. Algjuure 2 jaoks on indeksite tabel järgmine ([3], lk. 330):

	0	1	2	3	4	5	6	7	8	9
0		18	1	13	2	16	14	6	3	8
1	17	12	15	5	7	11	4	10	9	

Elemendi $\overline{17}$ järk on seetõttu $\frac{\varphi(19)}{(\operatorname{ind}_2 17, \varphi(19))} = \frac{18}{(10,18)} = \frac{18}{2} = 9$. Algjuurte leidmiseks tuleb meil võtta sellised indeksid vahemikust $[1, 18]$, mille suurim ühistegur arvuga $\varphi(19) = 18$ on 1. Nendeks on $1, 5, 7, 11, 13$ ja 17, millele indeksite tabelis vastavad arvud $2, 13, 14, 15, 3$ ja 10. Kolmandat järku elemendid on need jäägiklassid $\overline{b}$, mille korral $(\operatorname{ind}_2 b, \varphi(19)) = \frac{\varphi(19)}{3} = \frac{18}{3} = 6$. Sellisteks indeksiteks on parajasti need arvud vahemikust $[1, 18]$, mille suurim ühistegur arvuga 18 on 6, ehk 6 ja 12. Neile kahele indeksile vastavad tabelis arvud 7 ja 11. Viimane tulemus on muuseas kooskõlas teoreemi 7.12 tõestusega, mille kohaselt peab leiduma $\varphi(3) = 2$ kolmandat järku elementi.

8. Ruutjäägid

8.1. Legendre'i sümbol ja selle lihtsamad omadused

Olgu $p > 2$ algarv. Selles peatükis huvitab meid, millistel jäägiklassikorpuse $\mathbb{Z}_p$ elementidel on olemas ruutjuur, s.t. millised korpuse $\mathbb{Z}_p$ elemendid on mingi teise elemendi ruudud. Oletame, et mingil elemendil $\overline{a} \in \mathbb{Z}_p^*$ on olemas ruutjuur, s.t. leidub selline $\overline{b} \in \mathbb{Z}_p^*$, et

$$\overline{b}^2 = \overline{a}.$$

Siis ka $\overline{-b}$ on elemendi $\overline{a}$ ruutjuur, sest $\overline{-b}^2 = \overline{b}^2 = \overline{a}$. Kui oletada, et $\overline{-b} = \overline{b}$, siis $\overline{2b} = \overline{0}$, millest $p > 2$ tõttu järeldub, et $\overline{b} = \overline{0}$, mis aga pole võimalik. Seega $\overline{b}$ ja $\overline{-b}$ on erinevad elemendi $\overline{a}$ ruutjuured. Lause 2.9 põhjal on teise astme polünoomil $x^2 - \overline{a}$ üle korpuse $\mathbb{Z}_p$ ülimalt 2 juurt, s.t. elemendil $\overline{a}$ teisi ruutjuuri pole. Seega, kui elemendil $\overline{a}$ leidub ruutjuur, siis on neid ruutjuuri täpselt kaks tükki ja nad on teineteise vastandelemendid.

Kõik ruutjuurt omavad elemendid rühmas $\mathbb{Z}_p^*$ saab leida, kui arvutada hulga $\left\{\overline{1}, \overline{2}, \ldots, \overline{\frac{p-1}{2}}\right\}$ kõigi elementide ruudud (sest ülejäänud jäägiklassid on sellesse hulka kuuluvate jäägiklasside vastandelemendid). Seetõttu on ruutjuur olemas ülimalt $\frac{p-1}{2}$ elemendil, milleks ongi needsamad eelnevalt välja arvutatud ruudud. Põhimõtteliselt võiksid mõned neist ruutudest korpuses $\mathbb{Z}_p$ kokku langeda, millisel juhul oleks meil vähem kui $\frac{p-1}{2}$ ruutjuurt omavat elementi, aga tänu järeldusele 8.6 seda tegelikult kunagi ei juhtu. (Alternatiivselt, kuna $(2, p-1) = 2$, siis teoreemi 10.19 põhjal on ruutjuur olemas $\frac{p-1}{2}$ nullist erineval elemendil, s.o. täpselt pooltel $\mathbb{Z}_p^*$ elementidel.) Kui aga tahame teada, kas mingil konkreetsel elemendil on olemas ruutjuur ning p on suur, siis on kõigi ruutude väljaarvutamine ebaotstarbekas. Osutub, et leidub palju paremaid viise.

Definitsioon 8.1. Olgu $p > 2$ algarv ja a selline täisarv, et $p \nmid a$. Täisarvu a nimetatakse *ruutjäägiks* (*mitteruutjäägiks*) mooduli p järgi, kui element $\overline{a}$ omab (ei oma) ruutjuurt korpuses $\mathbb{Z}_p$.

Niisiis a on ruutjääk mooduli p järgi, kui $p \nmid a$ ja ruutkongruents

$$x^2 \equiv a \pmod{p}$$

on lahenduv.

Näide 8.2. Korpuses $\mathbb{Z}_{11}$ on ruutjuur olemas elementidel $\overline{1} = \overline{1}^2 = \overline{10}^2$, $\overline{4} = \overline{2}^2 = \overline{9}^2$, $\overline{9} = \overline{3}^2 = \overline{8}^2$, $\overline{5} = \overline{4}^2 = \overline{7}^2$ ja $\overline{3} = \overline{5}^2 = \overline{6}^2$. Seega ruutjäägid mooduli 11 järgi on $1, 3, 4, 5, 9$ ning mitteruutjäägid on $2, 6, 7, 8, 10$.

Definitsioon 8.3. Olgu a täisarv ja $p > 2$ algarv. *Legendre'i*[1] *sümbol* $\left(\frac{a}{p}\right)$ defineeritakse järgmiselt

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{kui } p \mid a; \\ 1, & \text{kui } a \text{ on ruutjääk mooduli } p \text{ järgi;} \\ -1, & \text{kui } a \text{ on mitteruutjääk mooduli } p \text{ järgi.} \end{cases}$$

(Seda sümbolit loetakse "a p suhtes".)

Näites 8.2 saadud tulemuse võib Legendre'i sümboli abil kirja panna järgmiselt:

$$\left(\frac{1}{11}\right) = \left(\frac{3}{11}\right) = \left(\frac{4}{11}\right) = \left(\frac{5}{11}\right) = \left(\frac{9}{11}\right) = 1,$$
$$\left(\frac{2}{11}\right) = \left(\frac{6}{11}\right) = \left(\frac{7}{11}\right) = \left(\frac{8}{11}\right) = \left(\frac{10}{11}\right) = -1.$$

Vahetult definitsioonist järeldub järgmine Legendre'i sümboli omadus.

Lemma 8.4. *Mistahes täisarvude a, b ning algarvu $p > 2$ korral, kui $a \equiv b \pmod{p}$, siis $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.*

Lemma 8.5. *Kui c on algjuur mooduli $p > 2$ järgi, siis iga $k \in \mathbb{N}$ korral*

$$\left(\frac{c^k}{p}\right) = (-1)^k.$$

[1] Prantsuse matemaatiku Adrien–Marie Legendre'i (1752-–1833) järgi.

Tõestus. Olgu c algjuur mooduli p järgi, s.t. $\mathbb{Z}_p^* = \left\{\overline{c}, \overline{c}^2, \ldots, \overline{c}^{p-1} = \overline{1}\right\}$. Kui $k \in \{1, \ldots, p-1\}$ on paarisarv, siis elemendi $\overline{c}^k$ ruutjuureks on $\overline{c}^{\frac{k}{2}}$. Et täpselt pooled arvudest $1, \ldots, p-1$ on paarisarvud ja kõik neile vastavad astmed c^k on c algjuureks oleku tõttu erinevad, siis omavad ruutjuurt vähemalt $\frac{p-1}{2}$ elementi. Käesoleva peatüki sissejuhatuse kohasel on selliseid elemente aga ülimalt $\frac{p-1}{2}$, mistõttu neid peab olema täpselt $\frac{p-1}{2}$. Järelikult ülejäänud elemendid kujul c^k, kus $1 \leq k \leq p-1$ on paaritu, ei oma ruutjuurt. Kokkuvõttes saamegi, et ruutjuurt omavad parajasti need elemendid $\overline{c}^k$, kus $k \in \{1, \ldots, p-1\}$ on paaris.

Kui aga k on suvaline naturaalarv, siis leiduvad $q, r \in \mathbb{N}$ nii, et $k = (p-1)q + r$ ja $1 \leqslant r \leqslant p-1$. Siis $c^k \equiv \left(c^{p-1}\right)^q \cdot c^r \equiv c^r \pmod{p}$ ja

$$\left(\frac{c^k}{p}\right) = \left(\frac{c^r}{p}\right) = (-1)^r = (-1)^k,$$

sest $p-1$ on paarisarv ning k ja r on sama paarsusega. □

Eelneva lemma tõestuses tegime tegelikult kindlaks ruutjääkide arvu mooduli p järgi.

Järeldus 8.6. *Algarvulise mooduli $p > 2$ järgi leidub $\frac{p-1}{2}$ ruutjääki ja $\frac{p-1}{2}$ mitteruutjääki.*

Lause 8.7 (Euleri kriteerium). *Iga täisarvu a ja algarvu $p > 2$ korral*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Tõestus. Kui $p \mid a$, siis $\left(\frac{a}{p}\right) = 0 \equiv a^{\frac{p-1}{2}} \pmod{p}$. Oletame, et $p \nmid a$ ja $\overline{a} = \overline{c}^k$, kus $\mathbb{Z}_p^* = \left\{\overline{c}, \overline{c}^2, \ldots, \overline{c}^{p-1} = \overline{1}\right\}$. Siis $\left(c^{\frac{p-1}{2}}\right)^2 = c^{p-1} \equiv 1 \pmod{p}$. Järelikult $\overline{c}^{\frac{p-1}{2}}$ on polünoomi $x^2 - \overline{1} \in \mathbb{Z}_p[x]$ juur ning seega kas $c^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ või $c^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, sest teisi juuri kui $\overline{1}$ ja $\overline{-1}$ sellel polünoomil ei ole. Kuna $\overline{c}$ on rühma $\mathbb{Z}_p^*$ moodustaja, siis esimene võimalus langeb ära ja seega

$$\left(\frac{a}{p}\right) = \left(\frac{c^k}{p}\right) = (-1)^k \equiv \left(c^{\frac{p-1}{2}}\right)^k = \left(c^k\right)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

□

Kuigi Euleri kriteeriumi abil saab põhimõtteliselt iga täisarvu korral kindlaks teha, kas ta on ruutjääk või mitte, ei ole see siiski sobiv suurte algarvude p korral. Õnneks on Legendre'i sümbolil terve rida omadusi, mis lihtsustavad tema väärtuse arvutamist.

Lause 8.8. *Iga algarvu $p > 2$ korral on Legendre'i sümbolil järgmised omadused.*

1. *Iga $a, b \in \mathbb{Z}$ korral*
$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$
2. *Iga $a, b \in \mathbb{Z}$, $p \nmid b$, korral*
$$\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right).$$
3. *Kehtib $\left(\frac{1}{p}\right) = 1$ ja*
$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \textit{kui } p \equiv 1 \pmod{4}; \\ -1, & \textit{kui } p \equiv 3 \pmod{4}. \end{cases}$$

Tõestus. 1. Euleri kriteeriumi kasutades saame, et

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p},$$

kust soovitud võrdus järeldub tänu sellele, et $p > 2$ ning viimase kongruentsi kummalgi poolel on kas $0, 1$ või -1.
2. Kui $p \nmid b$, siis vastavalt definitsioonile 8.3 $\left(\frac{b^2}{p}\right) = 1$ ning seega tõestuse esimese osa põhjal

$$\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b^2}{p}\right) = \left(\frac{a}{p}\right).$$

3. Võrdus $\left(\frac{1}{p}\right) = 1$ kehtib sellepärast, et $\overline{1}^2 = \overline{1}$ korpuses $\mathbb{Z}_p$. Teine võrdus järeldub Euleri kriteeriumist võttes $a = -1$ või järgmise peatüki järeldusest 10.21, sest $\frac{p-1}{2}$ on paarisarv parajasti siis kui $p-1$ jagub neljaga ehk $p \equiv 1 \pmod 4$. □

Näide 8.9. Teeme kindlaks, kas kongruents $x^2 \equiv 29 \pmod{17}$ on lahenduv. Selleks leiame Legendre'i sümboli $\left(\frac{29}{17}\right)$ väärtuse. Kuna $29 \equiv 12 \pmod{17}$, siis

$$\left(\frac{29}{17}\right) = \left(\frac{12}{17}\right) = \left(\frac{3 \cdot 2^2}{17}\right) = \left(\frac{3}{17}\right).$$

Viimase sümboli arvutamiseks kasutame Euleri kriteeriumi. Et

$$\left(\frac{3}{17}\right) \equiv 3^{\frac{17-1}{2}} = 3^8 = 27 \cdot 27 \cdot 9 \equiv 10 \cdot 10 \cdot 9 \equiv 10 \cdot 5 \equiv -1 \pmod{17},$$

siis $\left(\frac{3}{17}\right) = -1$ ja seega ka $\left(\frac{29}{17}\right) = -1$, mis tähendab, et kongruentsil $x^2 \equiv 29 \pmod{17}$ ei ole lahendit.

Väikse kõrvalepõikena kasutame lauset 8.8 selleks, et näidata teatud kujul algarvude hulga lõpmatust (vt. ka teoreemi 2.4).

Lause 8.10. *On lõpmata palju algarve kujul* $4k+1$.

Tõestus. Oletame, et on ainult lõplik arv selliseid algarve; tähistame nad $p_1, p_2, \ldots, p_n$. Vaatleme naturaalarvu $a = (2p_1p_2 \ldots p_n)^2 + 1$. On selge, et a on paaritu, seega peab leiduma mingi paaritu algarv p, nii et $p \mid a$, ehk $(2p_1p_2 \ldots p_n)^2 \equiv -1 \pmod p$. See tähendab, et -1 on ruutjääk mooduli p järgi, ehk $\left(\frac{-1}{p}\right) = 1$. Lause 8.8 põhjal $\left(\frac{-1}{p}\right) = 1$ parajasti siis, kui $p = 4k+1$, kus $k \in \mathbb{N}$. Järelikult p on üks algarvudest $p_1, \ldots, p_n$. Seega $p \mid a - (2p_1p_2 \ldots p_n)^2 = 1$, vastuolu. □

Teeme nüüd kindlaks, millal on arv 2 ruutjääk mooduli p järgi.

Teoreem 8.11. *Iga algarvu* $p > 2$ *korral*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & \textit{kui } p \equiv \pm 1 \pmod 8; \\ -1, & \textit{kui } p \equiv \pm 3 \pmod 8. \end{cases}$$

Tõestus. Vaatleme järgmist $\frac{p-1}{2}$ kongruentsist koosnevat süsteemi:

$$\begin{array}{rcll} p-1 & \equiv & 1(-1)^1 & \pmod p \\ 2 & \equiv & 2(-1)^2 & \pmod p \\ p-3 & \equiv & 3(-1)^3 & \pmod p \\ 4 & \equiv & 4(-1)^4 & \pmod p \\ & \ldots & & \\ r & \equiv & \frac{p-1}{2}(-1)^{\frac{p-1}{2}} & \pmod p, \end{array}$$

kus r on kas $p - \frac{p-1}{2}$ (juhul kui $\frac{p-1}{2}$ on paaritu arv) või $\frac{p-1}{2}$ (kui $\frac{p-1}{2}$ on paarisarv). Korrutades nende kongruentside vastavad pooled, saame, et

$$2 \cdot 4 \cdot 6 \cdot \ldots \cdot (p-1) \equiv \left(\frac{p-1}{2}\right)!(-1)^{1+2+\ldots+\frac{p-1}{2}} \pmod p.$$

Kõik tegurid selle kongruentsi vasakul poolel on paarisarvud ja $\left(1 + \frac{p-1}{2}\right)\frac{p-1}{4} = \frac{p^2-1}{8}$, järelikult

$$2^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)! \equiv \left(\frac{p-1}{2}\right)!(-1)^{\frac{p^2-1}{8}} \pmod p.$$

Kuna $\left(\frac{p-1}{2}\right)! \not\equiv 0 \pmod p$, siis

$$2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}} \pmod p.$$

Euleri kriteeriumi põhjal $2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right) \pmod p$, millest järeldubki väide, sest kuna kongruentsi $\left(\frac{2}{p}\right) \equiv (-1)^{\frac{p^2-1}{8}} \pmod p$ mõlemal poolel on kas 1 või -1, $p > 2$ ning $1 \not\equiv -1 \pmod p$, siis viimase kongruentsi mõlemal poolel peavad olema võrdsed arvud. □

8.2. Gaussi ruutvastavusseadus

Gaussi poolt 1796. a. tõestatud teoreem ruutjääkide kohta kuulub arvuteooria kõige ilusamate ja sügavamate tulemuste hulka. Aastaks 2013 oli trükis avaldatud vähemalt 246 erinevat tõestust [13], millest 8 autoriks on Gauss ise. Selle teoreemi tõestamiseks vajame järgmist, samuti Gaussi nime kandvat abitulemust.

Teoreem 8.12 (Gaussi lemma). *Olgu $p > 2$ paaritu algarv, a täisarv ja $(a, p) = 1$. Siis*

$$\left(\frac{a}{p}\right) = (-1)^n,$$

kus n on hulga $A = \left\{a, 2a, 3a, \ldots, \frac{p-1}{2} \cdot a\right\}$ selliste elementide arv, mis annavad arvuga p jagamisel jäägi $r > \frac{p}{2}$.

Tõestus. Paneme kõigepealt tähele, et kuna $(a, p) = 1$, siis Eukleidese lemma (lemma 1.10) põhjal ei saa ükski hulka A kuuluvate erinevate täisarvude paar olla kongruentne mooduli p järgi. Samamoodi ei ole ükski neist kongruentne nulliga mooduli p järgi. Olgu $r_1, r_2, \ldots, r_n$ sellised jäägid, mis tekivad hulga A elementide jagamisel arvuga p ja mis rahuldavad tingimust $\frac{p}{2} < r_i < p$, ning $s_1, s_2 \ldots, s_m$ niisugused jäägid, mille korral $0 < s_j < \frac{p}{2}$. Siis $m + n = \frac{p-1}{2}$ ja

$$0 < p - r_1, p - r_2 \ldots, p - r_n, s_1, s_2, \ldots, s_m < \frac{p}{2}.$$

Nüüd veendume, et tegelikult on arvud $p - r_1, p - r_2, \ldots, p - r_n, s_1, s_2 \ldots, s_m$ kõik erinevad. Kuna $(a, p) = 1$, siis jällegi Eukleidese lemma tõttu ei ole võimalik, et $r_i = r_j$ või $s_i = s_j$, kui $i \neq j$. Järele jääb võimalus, et leiduvad sellised indeksid i ja j, mille korral

$$p - r_i = s_j \quad \text{ehk} \quad r_i + s_j = p.$$

Olgu jääkidele r_i ja s_j vastavad hulga A elemendid ua ja va, st. $1 \leq u, v \leq \frac{p-1}{2}$ on täisarvud ning $r_i \equiv ua \pmod{p}$ ja $s_j \equiv va \pmod{p}$. Siis

$$(u + v)a \equiv r_i + s_j = p \pmod{p}.$$

Uuesti Eukleidese lemmat kasutades saame siit, et $p \mid u + v$ ehk $u + v \equiv 0 \pmod{p}$. See ei ole aga võimalik, sest $2 \leq u + v \leq 2 \cdot \frac{p-1}{2} = p - 1$.

Seega oleme me näidanud, et $\{p - r_1, p - r_2, \ldots, p - r_n, s_1, s_2, \ldots, s_m\} = \left\{1, 2, \ldots, \frac{p-1}{2}\right\}$. Järelikult

$$\begin{aligned}
\left(\frac{p-1}{2}\right)! &= (p - r_1) \cdot (p - r_2) \cdot \ldots \cdot (p - r_n) \cdot s_1 \cdot s_2 \cdot \ldots \cdot s_m \\
&\equiv (-r_1) \cdot (-r_2) \cdot \ldots \cdot (-r_n) \cdot s_1 \cdot s_2 \cdot \ldots \cdot s_m \pmod{p} \\
&= (-1)^n r_1 \cdot r_2 \cdot \ldots \cdot r_n \cdot s_1 \cdot s_2 \cdot \ldots \cdot s_m \pmod{p}.
\end{aligned}$$

Samas defineerisime me jäägid $r_1, r_2, \ldots, r_n, s_1, s_2, s_m$ selliselt, et nad on mooduli p järgi mingis järjekorras kongruentsed arvudega $a, 2a, 3a, \ldots, \frac{p-1}{2} \cdot a$, st. $r_1 \cdot r_2 \cdot \ldots \cdot r_n \cdot s_1 \cdot s_2 \cdot \ldots \cdot s_m \equiv a \cdot 2a \cdot 3a \cdot \ldots \cdot \frac{p-1}{2} \cdot a$. Seetõttu

$$\begin{aligned}
\left(\frac{p-1}{2}\right)! &\equiv (-1)^n \cdot r_1 \cdot r_2 \cdot \ldots \cdot r_n \cdot s_1 \cdot s_2 \cdot \ldots \cdot s_m \pmod{p} \\
&\equiv (-1)^n \cdot a \cdot 2a \cdot 3a \cdot \ldots \cdot \frac{p-1}{2} \cdot a \pmod{p} \\
&= \left(\frac{p-1}{2}\right)! \cdot (-1)^n \cdot a^{\frac{p-1}{2}} \pmod{p}.
\end{aligned}$$

Kuna $\left(\frac{p-1}{2}\right)! \not\equiv 0 \pmod{p}$, siis võime temaga taandada ja saada $1 \equiv (-1)^n \cdot a^{\frac{p-1}{2}} \pmod{p}$. Selle ekvivalentsi mõlemaid pooli arvuga $(-1)^n$ korrutades on tulemuseks $(-1)^n \equiv a^{\frac{p-1}{2}} \pmod{p}$. Euleri kriteerium (lause 8.7) annab meile nüüd, et

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv (-1)^n \pmod{p}.$$

Eelduse kohaselt $p > 2$, seega $1 \not\equiv -1 \pmod{p}$ ja kongruentsi mõlemad pooled peavad olema võrdsed, ehk tõepoolest

$$\left(\frac{a}{p}\right) = (-1)^n \pmod{p}.$$

□

Selleks, et Gaussi lemmat saaks rakendada ruutvastavusseaduse tõestamiseks, on vaja veel ühte abitulemust.

Lause 8.13. *Olgu $p > 2$ paaritu algarv, a paaritu täisarv ja $(a, p) = 1$. Siis*

$$\left(\frac{a}{p}\right) = (-1)^{\sum\limits_{k=1}^{\frac{p-1}{2}} \lfloor ka/p \rfloor}.$$

TÕESTUS. Kuna eeldused on siin kitsamad, kui Gaussi lemmal, siis võime kasutada seal sissetoodud tähiseid $A = \left\{a, 2a, 3a, \ldots, \frac{p-1}{2} \cdot a\right\}$, r_i ja s_i. Jagades hulga A elemendid järgemööda arvuga p, on tulemuseks võrdused

$$ka = q_k p + t_k, \quad 1 \le t_k \le p-1, \quad 1 \le k \le \frac{p-1}{2}.$$

Eelneva tähistuse kohaselt juhul $\frac{p}{2} < t_k < p$ leidub selline indeks i, et $t_k = r_i$, ja juhul $0 < t_k < \frac{p}{2}$ leidub niisugune indeks j, et $t_k = s_j$. Järelikult kõiki jäägiga jagamisel tekkinud võrdusi kokku liites saame, et

$$\sum_{k=1}^{\frac{p-1}{2}} ka = \sum_{k=1}^{\frac{p-1}{2}} q_k p + \sum_{i=1}^{n} r_i + \sum_{j=1}^{m} s_j.$$

Gaussi lemma tõestuse põhjal $\left\{1, 2, \ldots, \frac{p-1}{2}\right\} = \{p - r_1, p - r_2, \ldots, p - r_n, s_1, s_2, \ldots, s_m\}$. Seega

$$\sum_{k=1}^{\frac{p-1}{2}} k = \sum_{i=1}^{n} (p - r_i) + \sum_{j=1}^{m} s_j.$$

Nende kahe summa omavahelisel lahutamisel tekib võrdus

$$(a-1) \sum_{k=1}^{\frac{p-1}{2}} k = p \cdot \left(\sum_{k=1}^{\frac{p-1}{2}} q_k - n \right) + 2 \sum_{i=1}^{n} r_i.$$

Kuna arvud p ja a on mõlemad paaritud, siis $p \equiv a \equiv 1 \pmod 2$ ja järelikult omandab eelnev võrdus mooduli 2 järgi kuju

$$0 \cdot \sum_{k=1}^{\frac{p-1}{2}} k \equiv 1 \cdot \left(\sum_{k=1}^{\frac{p-1}{2}} q_k - n \right) \pmod 2.$$

Viimane kongruents on samaväärne kongruentsiga

$$n \equiv \sum_{k=1}^{\frac{p-1}{2}} q_k \pmod 2.$$

Nüüd jääb ainult tähele panna, et $q_k = \lfloor \frac{ka}{p} \rfloor$ ja Gaussi lemma põhjal

$$\left(\frac{a}{p}\right) = (-1)^n = (-1)^{\sum\limits_{k=1}^{\frac{p-1}{2}} \lfloor ka/p \rfloor}.$$

□

Teoreem 8.14 (Ruutvastavusseadus). *Kui $p > 2$ ja $q > 2$ on erinevad algarvud, siis*

$$\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{q}{p}\right) = \begin{cases} -\left(\frac{q}{p}\right), & \textit{kui } p \equiv q \equiv 3 \pmod 4; \\ \left(\frac{q}{p}\right), & \textit{ülejäänud juhtudel.} \end{cases}$$

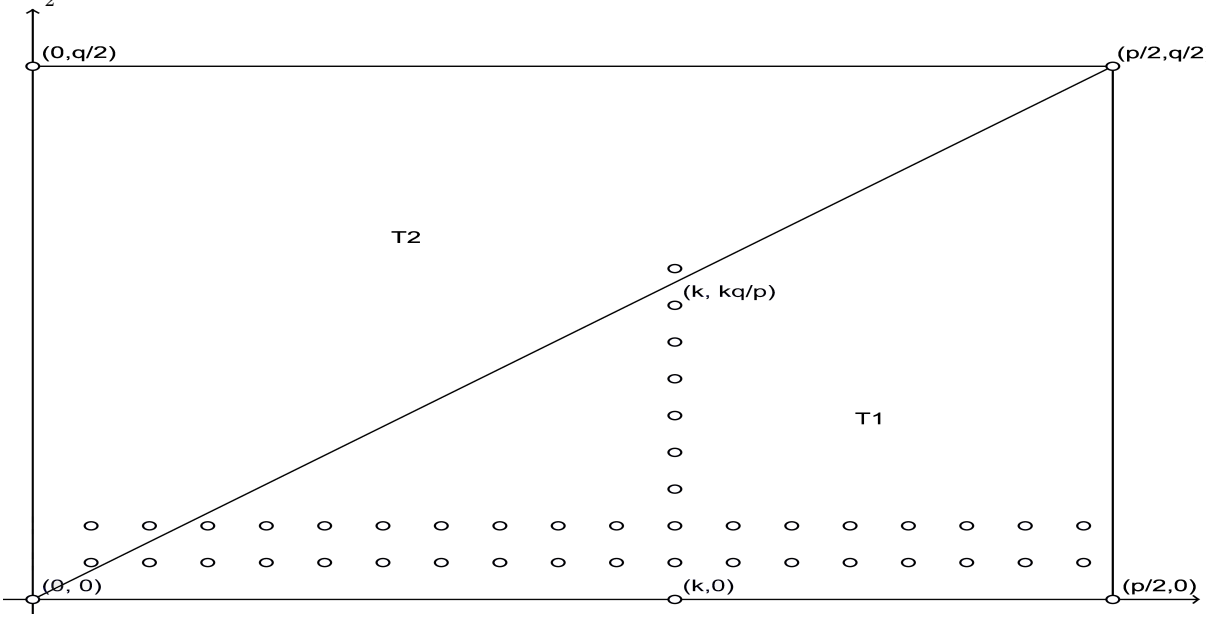
TÕESTUS. Tõestame ainult esimese võrduse kehtivuse, sest on lihtne veenduda, et

$$(-1)^{\frac{(p-1)(q-1)}{4}} = \begin{cases} -1, & \text{kui } p \equiv q \equiv 3 \pmod 4; \\ 1, & \text{ülejäänud juhtudel.} \end{cases}$$

Selleks vaatleme tasandil asetsevat ristkülikut, mille tippude koordinaadid on $(0,0), (\frac{p}{2},0), (0,\frac{q}{2})$ ja $(\frac{p}{2},\frac{q}{2})$. Olgu R tasandi see osa, mis asub antud ristküliku sisemuses, s.t.

$$R = \left\{(x,y) \in \mathbb{R}^2 \mid 0 < x < \frac{p}{2}, 0 < y < \frac{q}{2}\right\}.$$

Ruutvastavusseaduse tõestamiseks leiame hulka R jäävate täisarvuliste koordinaatidega punktide (edaspidi nimetame neid *võrepunktideks*) arvu kahel eri viisil. Kuna p ja q on paaritud arvud, siis hulka R kuuluvate võrepunktide hulk koosneb punktidest (m,n), kus $m,n \in \mathbb{Z}$ ning $1 \le m \le \frac{p-1}{2}$ ja $1 \le n \le \frac{q-1}{2}$. Ilmselt on selliseid punkte kokku $\frac{p-1}{2} \cdot \frac{q-1}{2}$ tükki.



Ristküliku R diagonaal D rahuldab võrrandit $y = \frac{q}{p} \cdot x$, mis on samaväärne võrrandiga $py = qx$. Kuna $(p,q) = 1$, siis iga võrrandi $py = qx$ täisarvuline lahend rahuldab seoseid $p \mid x$ ja $q \mid y$. Samas me teame, et hulga R sisemuses asuvate võrepunktide (x,y) korral $1 \le x \le \frac{p-1}{2} < p$ ja $1 \le y \le \frac{q-1}{2} < q$, mistõttu ilmselt $p \nmid x$ ja $q \nmid y$. Seega ei saa ükski hulga R sisemusse kuuluv võrepunkt asuda diagonaalil D. Tähistame sümbolitega T_1 ja T_2 hulga R need osad, mis jäävad diagonaalist D vastavalt allapoole ja ülespoole. Kuna diagonaalil võrepunkte ei ole, siis on hulka R kuuluvate võrepunktide arv võrdne hulkadesse T_1 ja T_2 kuuluvate võrepunktide arvude summaga.

Kui fikseerida $1 \le x \le \frac{p-1}{2}$, siis vahemikku $1 \le y \le \frac{qx}{p}$ jäävaid täisarve on kokku $\left\lfloor \frac{qx}{p} \right\rfloor$ tükki. Järelikult on diagonaali D ja fikseeritud punkti $(x,0)$ vahel täpselt $\left\lfloor \frac{qx}{p} \right\rfloor$ võrepunkti, mistõttu hulka T_1 kuulub kokku $\sum\limits_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{qk}{p} \right\rfloor$ võrepunkti. Samasugune arutelu punktide $(0,y)$ ja hulga T_2 jaoks annab viimasesse kuuluvate võrepunktide arvuks $\sum\limits_{l=1}^{\frac{q-1}{2}} \left\lfloor \frac{pl}{q} \right\rfloor$. Kokkuvõttes oleme saanud hulka R kuuluvaid võrepunkte loendades, et

$$\frac{p-1}{2} \cdot \frac{q-1}{2} = \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{qk}{p} \right\rfloor + \sum_{l=1}^{\frac{q-1}{2}} \left\lfloor \frac{pl}{q} \right\rfloor.$$

Kuna $(p,q) = 1$ ning p ja q on mõlemad paaritud arvud, siis võime kasutada lauset 8.13 ja leida, et

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\sum\limits_{k=1}^{\frac{p-1}{2}} \lfloor kq/p \rfloor} \cdot (-1)^{\sum\limits_{l=1}^{\frac{q-1}{2}} \lfloor lp/q \rfloor} = (-1)^{\sum\limits_{k=1}^{\frac{p-1}{2}} \lfloor kq/p \rfloor + \sum\limits_{l=1}^{\frac{q-1}{2}} \lfloor lp/q \rfloor} = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

Lõpptulemusena saame lause 8.8 punktide 2. ja 3. kohaselt, et $\left(\frac{q}{p}\right)^2 = \left(\frac{1 \cdot q^2}{p}\right) = \left(\frac{1}{p}\right) = 1$, mistõttu tõepoolest

$$\left(\frac{p}{q}\right) = \left(\frac{p}{q}\right)\left(\frac{q}{p}\right)^2 = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \left(\frac{q}{p}\right) = (-1)^{\frac{(q-1)(p-1)}{4}} \left(\frac{q}{p}\right).$$

□

Näide 8.15. Teeme kindlaks, kas algarv 7411 on ruutjääk algarvulise mooduli 9283 järgi.

Selleks arvutame

$$\begin{aligned}\left(\frac{7411}{9283}\right) &= (-1)^{\frac{9282}{2}\cdot\frac{7410}{2}}\left(\frac{9283}{7411}\right) = (-1)^{4641\cdot 3705}\left(\frac{9283}{7411}\right) = -\left(\frac{9283}{7411}\right) = -\left(\frac{1872}{7411}\right)\\ &= -\left(\frac{\left(2^2\right)^2}{7411}\right)\left(\frac{3^2}{7411}\right)\left(\frac{13}{7411}\right) = -\left(\frac{13}{7411}\right) = -(-1)^{6\cdot 3705}\left(\frac{7411}{13}\right) = -\left(\frac{7411}{13}\right) = -\left(\frac{1}{13}\right) = -1.\end{aligned}$$

Seega 7411 on mitteruutjääk mooduli 9283 järgi.

8.3. Jacobi sümbol

Legendre'i sümboli üldistuseks on saksa matemaatiku Carl Gustav Jacob Jacobi (1804–1851) poolt kasutusele võetud sümbol.

Definitsioon 8.16. Olgu a täisarv ja n paaritu naturaalarv. Olgu $n = p_1p_2\dots p_s$, kus $p_1, p_2, \dots, p_s$ on algarvud (nende hulgas võib olla võrdseid). *Jacobi sümbol* $\left(\frac{a}{n}\right)$ defineeritakse Legendre'i sümbolite abil järgmiselt:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\dots\left(\frac{a}{p_s}\right).$$

Definitsiooni 8.1 loomulikul viisil üldistades öeldakse, et täisarv a on *ruutjääk* naturaalarvulise mooduli n järgi, kui kongruents $x^2 \equiv a \pmod{n}$ on lahenduv. Märgime, et sellise sõnastuse järgi muutub ka null ehk jäägiklass $\overline{n}$ ruutjäägiks, kuigi definitsioon 8.1 jättis selle juhu vaatluse alt välja.

Märkus 8.17. Kui n on kordarv ja $\left(\frac{a}{n}\right) = 1$, siis see ei tähenda veel, et a on ruutjääk mooduli n järgi. Näiteks $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1$, kuid ei leidu sellist täisarvu x, et $x^2 \equiv 2 \pmod{15}$, sest kui ta leiduks, siis oleks ka $x^2 \equiv 2 \pmod{3}$.

Küll aga sellest, et $\left(\frac{a}{n}\right) = -1$ järeldub, et a on mitteruutjääk mooduli n järgi, sest siis vähemalt ühe p_i korral $\left(\frac{a}{p_i}\right) = -1$ ja kui vastuväiteliselt oletada, et leidub selline $x \in \mathbb{Z}$, et $x^2 \equiv a \pmod{n}$, siis ka $x^2 \equiv a \pmod{p_i}$, mida ei saa olla.

Jacobi sümboli omadused on üsna sarnased Legendre'i sümboli omadustega.

Lause 8.18. *Jacobi sümbolil on järgmised omadused.*

1. *Iga $a, b \in \mathbb{Z}$ ja paaritu naturaalarvu n korral, kui $a \equiv b \pmod{n}$, siis $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.*
2. *Iga $a, b \in \mathbb{Z}$ ja paaritu naturaalarvu n korral*
$$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right).$$
3. *Iga $a, b \in \mathbb{Z}$ ja paaritu naturaalarvu n korral, kui $(b, n) = 1$, siis*
$$\left(\frac{ab^2}{n}\right) = \left(\frac{a}{n}\right).$$
4. *Iga $a \in \mathbb{Z}$ ja mistahes paaritute naturaalarvude n ja m korral*
$$\left(\frac{a}{nm}\right) = \left(\frac{a}{n}\right)\left(\frac{a}{m}\right).$$

Tõestus. Kolm esimest omadust järelduvad vahetult Legendre'i sümboli vastavatest omadustest ning kolmas järeldub Jacobi sümboli definitsioonist. □

Lemma 8.19. *Kui k ja l on paaritud naturaalarvud, siis*

1. $(kl-1)/2 \equiv (k-1)/2 + (l-1)/2 \pmod{2}$;
2. $(k^2l^2-1)/8 \equiv (k^2-1)/8 + (l^2-1)/8 \pmod{2}$.

TÕESTUS. 1. Kuna $(k-1)(l-1) \equiv 0 \pmod 4$, siis $kl-1 \equiv (k-1)+(l-1) \pmod 4$. Väide järeldub nüüd lausest 3.10, sest viimase kongruentsi mõlemal poolel on paarisarvud.

2. osa saab tõestada analoogiliselt. □

Lemma 8.20. *Kui $k_1, k_2, \ldots, k_s$ on paaritud naturaalarvud, siis*

1. $\sum_{i=1}^{s}(k_i-1)/2 \equiv (k_1k_2\ldots k_s-1)/2 \pmod 2$;
2. $\sum_{i=1}^{s}(k_i^2-1)/8 \equiv (k_1^2k_2^2\ldots k_s^2-1)/8 \pmod 2$.

TÕESTUS. Tõestame väite 1 induktsiooniga s järgi (väite 2 saab tõestada analoogiliselt). Kui $s=1$, siis on väide ilmne. Kui $s=2$, siis kasutame eelmist lemmat. Olgu $s>2$ ja oletame, et väide kehtib, kui arve on vähem kui s. Siis kasutades eelmist lemmat saame

$$\frac{k_1-1}{2}+\ldots+\frac{k_{s-1}-1}{2}+\frac{k_s-1}{2} \equiv \frac{k_1\ldots k_{s-1}-1}{2}+\frac{k_s-1}{2} \equiv \frac{k_1\ldots k_{s-1}k_s-1}{2} \pmod 2.$$

□

Üldistame nüüd teoreemid 8.11 ja 8.14 Jacobi sümbolite jaoks.

Lause 8.21. *Mistahes paaritute naturaalarvude n ja m korral*

1. $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}} = \begin{cases} 1, & kui\ \ n \equiv 1 \pmod 4; \\ -1, & kui\ \ n \equiv 3 \pmod 4; \end{cases}$
2. $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}} = \begin{cases} 1, & kui\ n \equiv \pm 1 \pmod 8; \\ -1, & kui\ n \equiv \pm 3 \pmod 8; \end{cases}$
3. $\left(\frac{m}{n}\right) = (-1)^{\frac{(m-1)(n-1)}{4}}\left(\frac{n}{m}\right) = \begin{cases} -\left(\frac{n}{m}\right), & kui\ m \equiv n \equiv 3 \pmod 4; \\ \left(\frac{n}{m}\right), & ülejäänud\ juhtudel. \end{cases}$

TÕESTUS. Olgu $n = p_1p_2\ldots p_s$ ja $m = q_1q_2\ldots q_r$, kus $p_1, \ldots, p_s$ ja $q_1, \ldots, q_r$ on algarvud.
1. Tänu lemmale 8.20 $\sum_{i=1}^{s}(p_i-1)/2 \equiv (p_1p_2\ldots p_s-1)/2 = (n-1)/2 \pmod 2$ ning seetõttu kasutades lauset 8.8 saame

$$\left(\frac{-1}{n}\right) = \left(\frac{-1}{p_1}\right)\ldots\left(\frac{-1}{p_s}\right) = (-1)^{\frac{p_1-1}{2}}\ldots(-1)^{\frac{p_s-1}{2}} = (-1)^{\sum_{i=1}^{s}\frac{p_i-1}{2}} = (-1)^{\frac{n-1}{2}}.$$

2. Tänu lemmale 8.20 $\sum_{i=1}^{s}(p_i^2-1)/8 \equiv (p_1^2p_2^2\ldots p_s^2-1)/8 = (n^2-1)/8 \pmod 2$ ning seetõttu teoreemi 8.11 põhjal

$$\left(\frac{2}{n}\right) = \left(\frac{2}{p_1}\right)\ldots\left(\frac{2}{p_s}\right) = (-1)^{\frac{p_1^2-1}{8}}\ldots(-1)^{\frac{p_s^2-1}{8}} = (-1)^{\sum_{i=1}^{s}\frac{p_i^2-1}{8}} = (-1)^{\frac{n^2-1}{8}}.$$

3. Kui leiduvad sellised i ja j, et $p_i = q_j$, siis vastavalt Legendre'i sümboli definitsioonile $\left(\frac{p_i}{q_j}\right) = \left(\frac{q_j}{p_i}\right) = 0$ ning tõestatava võrduse mõlemal poolel on 0. Eeldame nüüd, et selliseid võrdseid algarve ei leidu. Rakendades veelkord lemmat 8.20 saame

$$\sum_{i=1}^{r}\sum_{j=1}^{s}\frac{q_i-1}{2}\cdot\frac{p_j-1}{2} = \left(\sum_{i=1}^{r}\frac{q_i-1}{2}\right)\left(\sum_{j=1}^{s}\frac{p_j-1}{2}\right) \equiv \frac{m-1}{2}\cdot\frac{n-1}{2} \pmod 2.$$

Kasutades ruutvastavusseadust ja seda, et $\left(\frac{q_i}{p_j}\right)^2 = 1$, saame siis

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = \prod_{i=1}^{r}\prod_{j=1}^{s}\left(\frac{q_i}{p_j}\right)\left(\frac{p_j}{q_i}\right) = \prod_{i=1}^{r}\prod_{j=1}^{s}(-1)^{\frac{q_i-1}{2}\cdot\frac{p_j-1}{2}} = (-1)^{\sum_{i=1}^{r}\sum_{j=1}^{s}\frac{q_i-1}{2}\cdot\frac{p_j-1}{2}} = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}}.$$

□

Näide 8.22. Leiame Legendre'i sümboli $\left(\frac{7411}{9283}\right)$ (vt. näidet 8.15) väärtuse ilma arvu 1872 tegureiks lahutamata (välja arvatud 2 astmete eraldamine). Kasutades lauset 8.21 saame

$$\left(\frac{7411}{9283}\right) = -\left(\frac{1872}{7411}\right) = -\left(\frac{16}{7411}\right)\left(\frac{117}{7411}\right) = -\left(\frac{7411}{117}\right) = -\left(\frac{40}{117}\right)$$
$$= -\left(\frac{2}{117}\right)\left(\frac{5}{117}\right) = \left(\frac{5}{117}\right) = \left(\frac{117}{5}\right) = \left(\frac{2}{5}\right) = -1.$$

9. Arvuteooria krüptograafias

Käesolevas peatükis anname põgusa ülevaate mõnedest tuntumatest arvuteoorial põhinevatest krüptograafilisest algoritmidest. Krüptograafia ehk teadus salakirjutamisest on arvuteooria suuremaid praktilisi kasutusvaldkondi ja mõjutab otseselt 21. sajandi igapäevaelu tänu elektroonilise side (e-post, mobiilside), panganduse (pangaautomaadid, krediitkaardid, internetipangad) ja arvutustehnika (digitaalallkiri, andmete krüpteerimine, kasutajatunnused ja paroolid) laialdasele levikule.

9.1. Algarvulisuse testimine

Teises peatükis me juba nägime, et üks võrdlemisi keeruline probleem on selle kindlakstegemine, kas mingi etteantud arv on alg- või kordarv. Aritmeetika põhiteoreemi tõttu on see küsimus oluline osa arvu algteguriteks lahutamisel, lisaks vajavad mitmed krüptosüsteemid sisendina suuri algarve. Edaspidises vaatleme paari lihtsamat algoritmi algarvulisuse kindlakstegemiseks.

9.1.1. Fermat' algarvulisuse test

Fermat' väikese teoreemi 5.13 põhjal kehtib iga algarvu p ja täisarvu a (kui $(a,p)=1$) korral kongruents $a^{p-1} \equiv 1 \pmod{p}$. Kuna arvutused käivad siin mooduli p järgi, siis võib võtta $1 \le a \le p-1$, mis muuseas garanteerib, et $(a,p)=1$. Seega etteantud arvu n korral saab algarvulisust kontrollida sel viisil, et anname arvule a suvalisi väärtusi vahemikust $[2, n-1]$ ja kontrollime, kas

$$a^{n-1} \equiv 1 \pmod{n}.$$

Definitsioon 9.1. Täisarvu a nimetatakse naturaalarvu n kordarvulisuse *Fermat' tunnistajaks*, kui $n \nmid a$ ja $a^{n-1} \not\equiv 1 \pmod{n}$. Juhul, kui $a^{n-1} \equiv 1 \pmod{n}$, aga n on kordarv, nimetatakse arvu a *Fermat' valetajaks* (siis muuseas alati $(a,n)=1$)). Kui n kordarvulisus ei ole teada, siis kasutatakse valetaja asemel terminit *Fermat' mittetunnistaja*.

Eelnevast on selge, et kasvõi ühe Fermat' tunnistaja leidmine näitab, et n on kordarv. Kui oleme uurinud mitmeid arve a lõigust $[2, n-1]$ ja alati $a^{n-1} \equiv 1 \pmod{n}$, siis n on *tõenäoliselt* algarv.

Kahjuks on Fermat' testil üks suur viga: nimelt on olemas lõpmata palju selliseid kordarve n, mille korral $a^{n-1} \equiv 1 \pmod{n}$ kõigi $1 < a < n$, $(a,n)=1$ korral. Niisuguseid arve nimetatakse *Carmichaeli arvudeks*.[2] Kui me rakendame Fermat' testi mõnele Carmichaeli arvule, siis ainus võimalus, et $a^{n-1} \not\equiv 1 \pmod{n}$, on juht $(a,n)>1$. See on aga eritingimus Carmichaeli arvude jaoks, mida Fermat' test otseselt ei kontrolli. Muuseas on Carmichaeli arvud kõik paaritud, sest kui $n \ge 4$ on paarisarv, siis $(n-1,n)=1$ ja $(n-1)^{n-1} \equiv -1 \not\equiv 1 \pmod{n}$.

Carmichaeli arve on õnneks siiski suhteliselt vähe. Veelgi enam, mitte-Carmichaeli arvudel on suhteliselt palju Fermat' tunnistajaid.

Lause 9.2. *Olgu n on kordarv, mis ei ole Carmichaeli arv. Siis* vähemalt pooled *arvudest $1 < a < n$ on Fermat' tunnistajad.*

See tõke ei pruugi alati piisav olla, mistõttu Fermat' testi rakendatakse tavaliselt kombinatsioonis teiste testidega.

Näide 9.3. Uurime Fermat' testi abil, kas arvud 559, 561 ja 563 on algarvud. Selleks kontrollime, kas 2, 10, 29, 50, 100, 199, 254, 334, 421 on Fermat' tunnistajad või mitte. Arvutustulemused on kokku võetud järgmisesse tabelisse:

n	2^{n-1}	10^{n-1}	29^{n-1}	50^{n-1}	100^{n-1}	199^{n-1}	254^{n-1}	334^{n-1}	421^{n-1}
559	441	365	183	259	183	365	207	365	532
561	1	1	1	1	1	1	1	1	1
563	1	1	1	1	1	1	1	1	1

Järelikult ütleb Fermat' test meile kohe, et $559 = 13 \cdot 43$ on kordarv, 561 ja 563 aga tõenäoliselt algarvud. Viimane on tõepoolest algarv, aga $561 = 3 \cdot 11 \cdot 17$ on tegelikult vähim Carmichaeli arv. Kui me oleks testinud näiteks $252^{560} \equiv 375 \pmod{561}$, siis oleks viimase kordarvuks olek välja tulnud ($(252, 561) = 3$).

[2] Ameerika matemaatiku Robert Daniel Carmichaeli (1879–1967) järgi.

9.1.2. Miller-Rabini algarvulisuse test

Üks laialdaselt kasutatav algarvulisuse test, mis elimineerib Fermat' testi nõrkuse Carmichaeli arvude suhtes, on *Miller-Rabini*[3] test. Meetod ise toetub järgmisele Fermat' väikese teoreemi järeldusele.

Lause 9.4. *Olgu $p > 2$ algarv, a täisarv ja $p \nmid a$. Esitame paarisarvu $p-1$ kujul $p-1 = 2^s \cdot t$, kus $s \geq 1$ ja t on paaritu arv. Siis kas $a^t \equiv 1 \pmod{p}$ või leidub $0 \leq r < s$ nii, et $a^{2^r \cdot t} \equiv -1 \pmod{p}$.*

Tõestus. Fermat' väikesest teoreemist $a^{p-1} \equiv 1 \pmod{p}$. Lause 2.9 tõttu on polünoomil $x^2 - 1$ täpselt kaks juurt mooduli p järgi, nimelt 1 ja -1. Seega ruutjuur arvust 1 mooduli p järgi saab olla ainult 1 või -1. Võtame järjest ruutjuurt arvust a^{p-1} nii kaua, kuni kas tulemuseks on -1 või ruutjuurt enam võtta ei saa, sest oleme jõudnud kongruentsini $a^t \equiv \pm 1 \pmod{p}$. Viimasel juhul väide kehtib, esimesel juhul aga $-1 \equiv a^{\frac{p-1}{2^x}} = a^{2^{s-x} \cdot t} \pmod{p}$, kus $1 \leq x \leq s$ on ruutjuure võtmise kordade arv. Siis $0 \leq r = s - x \leq s - 1$ ja $a^{2^r \cdot t} \equiv -1 \pmod{p}$, mida oligi tarvis tõestada. □

Definitsioon 9.5. Olgu n paaritu naturaalarv ja a täisarv, kusjuures $(a, n) = 1$ ja $n - 1 = 2^s \cdot t$, kus t on paaritu arv. Arvu a nimetatakse naturaalarvu n kordarvulisuse *Miller-Rabini tunnistajaks* (mõnikord lihtsalt *tugevaks tunnistajaks*), kui

1. $a^t \not\equiv 1 \pmod{n}$,
2. $a^{2^i \cdot t} \not\equiv -1 \pmod{n}$ iga $i = 0, 1, \ldots, s-1$ korral.

Juhul, kui n on kordarv, aga vähemalt üks neist kongruentsidest kehtib, nimetatakse arvu a *Miller-Rabini valetajaks* (või *tugevaks valetajaks*). Jälle, kui ei ole teada, kas n on kordarv, siis valetaja asemel öeldakse, et arv a on *Miller-Rabini mittetunnistaja* (või *tugev mittetunnistaja*).

Nagu varemgi, kasvõi ühe Miller-Rabini tunnistaja olemasolu ütleb, et tegu on kordarvuga. Seega algarvulisuse testimiseks anname arvule a erinevaid täisarvulisi väärtusi lõigust $[2, n-1]$. Kui n on paarisarv või $(a, n) > 1$, siis on n ilmselt kordarv. Vastasel korral avaldame n kujul $n - 1 = 2^s \cdot t$ ja leiame järjest

$$a^t, \quad (a^t)^2 = a^{2t}, \quad ((a^t)^2)^2 = a^{2^2 t}, \quad \ldots, \quad (((a^t)^2)\ldots)^2 = a^{2^{s-1} t} \pmod{n}.$$

Kui $a^t \not\equiv 1 \pmod{n}$ ja $a^{2^i t} \not\equiv -1 \pmod{n}$, $0 \leq i \leq s-1$, siis a on Miller-Rabini tunnistaja ja n on kordarv. Vastasel korral, testides mitmete erinevate a väärtustega, on n tõenäoliselt algarv.

Miller-Rabini testi eelis Fermat' testi ees seisneb selles, et tema jaoks ei ole olemas Carmichaeli arvude analooge. Veelgi enam, kehtib järgmine väide, mida me siinkohal ei tõesta.

Lause 9.6. *Olgu n paaritu kordarv. Siis vähemalt 75% täisarvudest $1 < a < n$ on arvu n jaoks Miller-Rabini tunnistajad.*

Seetõttu Rabin-Milleri testi korduval kasutamisel erinevate a väärtuste jaoks kasvab Miller-Rabini tunnistajate (kui need on olemas) leidmise tõenäosus tunduvalt kiiremini, kui Fermat' tunnistajate leidmise tõenäosus.

Näide 9.7. Kontrollime Rabin-Milleri testi abil, kas arvud 551, 553, 557, 559, 561 ja 563 on algarvud. Selleks uurime, kas 2 on Rabin-Milleri tunnistaja. Ilmselt on kõik testitavad arvud paaritud ja $(2, 551) = (2, 553) = (2, 557) = (2, 559) = (2, 561) = (2, 563) = 1$. Nüüd teisendame $551 - 1$, $553 - 1$, $557 - 1$, $559 - 1$, $561 - 1$ ja $563 - 1$ kujule

$$550 = 2 \cdot 275, \ 552 = 2^3 \cdot 69, \ 556 = 2^2 \cdot 139, \ 558 = 2 \cdot 279, \ 560 = 2^4 \cdot 35, \ 562 = 2 \cdot 281.$$

Tähistame $t_1 = 275$, $t_2 = 69$, $t_3 = 139$, $t_4 = 279$, $t_5 = 35$, $t_6 = 281$, $s_1 = s_4 = s_6 = 1$, $s_2 = 3$, $s_3 = 2$ ja $s_5 = 4$, kasutades eelnevalt sissetoodud tähistust $n - 1 = 2^s \cdot t$. Edasised arvutustulemused on kokku võetud järgmisesse tabelisse:

n	2^{t_i}	2^{2t_i}	2^{4t_i}	2^{8t_i}
551	184			
553	526	176	8	
557	118	-1		
559	151			
561	263	166	67	1
563	-1			

Seega Rabin-Milleri test näitab, et 551, 553, 559 ja 561 on kordarvud, 557 ja 563 võivad aga olla algarvud. Me võime testi korrata erinevate a väärtustega (näiteks $a = 10, 29, 50, 100, 199, 254, 334, 421$), aga kuna 557 ja 563 on tõepoolest algarvud, siis on tulemus alati -1. Muuseas tuvastati Carmichaeli arv 561 kohe $a = 2$ korral kordarvuna ära.

[3] Ameerika arvutiteadlase Gary Lee Milleri ja juudi arvutiteadlase Michael Oser Rabini järgi.

9.2. Algteguriteks lahutamine

Aritmeetika põhiteoreemi kohaselt saab kõiki naturaalarve esitada algarvude korrutistena sisuliselt ühelainsal viisil. Selle esituse praktiline leidmine on aga hoopis keerulisem. Näiteks aastatel 2007-2009 kulus järgmise 232-kohalise arvu tegurdamiseks üle 2000 tingliku arvutiaasta:

$$
\begin{aligned}
&1230186684530117755130494958384962720772853569595334792197322452151726400507263657518745202199786469\\
&3899564749427740638459251925573263034537315482685079170261221429134616704292143116022212404792747377\\
&9408066535141959745985690214341 3\\
&=\\
&3347807169895689878604416984821269081770479498371376856891243138898288379387800228761471165253174308\\
&7737814467999489\\
&\times\\
&3674604366679959042824463379962795263227915816434308764267603228381573966651127923337341714339681027\\
&0092798736308917.
\end{aligned}
$$

9.2.1. RSA krüptosüsteem

RSA[4] on asümmeetriline avaliku võtme krüptosüsteem. Asümmeetriline tähendab siin seda, et kodeerimine ja dekodeerimine toimuvad erinevate võtmetega. Muuhulgas kasutab RSA krüptosüsteemi Eesti ID-kaart, millele on talletatud digiallkirjastamisel kasutatavad avalik ja salajane võti. Asümmeetria tõttu saab viimaseid kasutada ka tekstide kodeerimiseks, aga see ei ole eriti otstarbekas ega levinud.

RSA algoritm töötab järgmise skeemi alusel. Kodeerimiseks/dekodeerimiseks on vajalikud avalik ja salajane võti. Kuna iga digitaalset suurust saab esitada naturaalarvuna, siis need ongi lihtsalt kaks naturaalarvu(paari). Võtmete leidmiseks kasutatakse järgmist skeemi:

- valime kaks algarvu p ja q (siin on kasulikud algarvulisuse testid), mis praktilistel kaalutlustel peaksid olema umbkaudu samas suurusjärgus;
- arvutame *mooduli* $n = pq$;
- leiame $\varphi(n) = (p-1)(q-1)$;
- valime sellise *avaliku astendaja* $1 < e < \varphi(n)$, et $(e, \varphi(n)) = 1$;
- leiame *salajase astendaja* $1 < d < \varphi(n)$ nii, et $\overline{d}_{\varphi(n)} = (\overline{e}_{\varphi(n)})^{-1}$, st. $ed \equiv 1 \pmod{\varphi(n)}$.

Avalik võti on arvupaar (n, e) ja *salajane võti* on arvupaar (n, d). Kuna d arvutati $\varphi(n)$, p ja q abil, siis tuleb ka viimased salajas hoida. Avalik võti tehakse kõigile järgmistes protsessides osalejatele teatavaks, salajane võti peab jääma ainult kodeerija enda teada.

RSA abil sõnumi S kodeerimine käib järgmiselt. Esiteks teisendame sõnumi S naturaalarvuks s (iga digitaalne suurus on bitijada, mis on sisuliselt mingi naturaalarvu esitus kahendsüsteemi arvuna), kusjuures peavad kehtima tingimused $0 \leq s < n$ ja $(s, n) = 1$. Kui sõnum on liiga pikk ($s \geq n$), siis võib ta osadeks jagada ja need eraldi kodeerida. Praktikas seda tegelikult mitmetel põhjustel siiski ei tehta ja sõnumid ongi üldjuhul moodulist väiksemad. Tingimuse $(s, n) = 1$ täitmiseks on erinevaid meetodeid, mis muuseas elimineerivad mõned RSA nõrkused nagu juhusliku komponendi puudumine, semantiline ebaturvalisus, jagatud avalik võti jne. Siinkohal me neid täpsemalt ei vaatle, aga oluline on, et kõik osapooled teaksid ja kasutaksid ühte ja sama meetodit.

Seejärel kodeeritakse sõnum s salasõnumiks

$$c \equiv s^e \pmod{n}.$$

Mooduli järgi astendamine ei ole väga arvutusmahukas operatsioon, mistõttu see tehe on mõistliku aja jooksul sooritatav. Dekodeerimiseks leitakse lihtsalt

$$c^d \equiv s^{de} \equiv s^1 = s \pmod{n}.$$

Viimane võrdus kehtib tänu lemmale 7.31, sest $de \equiv 1 \pmod{\varphi(n)}$.

Asümmetria tõttu saab skeemi kasutada ka tagurpidi ja teisendada sõnumit järgnevalt:

$$s \mapsto s^d \mapsto (s^d)^e \equiv s \pmod{n}.$$

[4] Ameerika arvutiteadlaste Ronald Linn Rivesti ja Leonard Adlemani ning juudi arvutiteadlase Adi Shamiri järgi.

Erinevus seisneb siin selles, et esimesena vaadeldud meetod on sõnumi s vaid salajase võtme (n, d) omajale loetavale kujule c teisendamine (salakirja saatmine või andmete kodeerimine). Teine meetod on aga põhimõtteliselt digiallkirjastamine, kus s on allkirjastatav tekst ja c juba allkirjastatud dokument.

RSA murdmiseks on vajalik leida sõnum s, kui on teada salasõnum

$$c \equiv s^e \pmod{n},$$

moodul n ja avalik astendaja e, aga ei ole teada salajast astendajat d. Sisuliselt on tegu e-nda juure leidmisega jäägiklassist $\bar{c} \in U(\mathbb{Z}_n)$. Praktikas on seni kõige efektiivsemaks osutunud meetodiks mooduli $n = pq$ tegurdamine ja selle abil salajase astendaja d arvutamine. Kuna mittekvantarvutite jaoks ei ole tänaseni olemas kiiret algteguriteks lahutamise algoritmi, siis see meetod ei ole eriti efektiivne. Samas ei ole keegi suutnud tõestada ei seda, et RSA murdmine on samaväärne suvaliste naturaalarvude algteguriteks lahutamisega (tegelikult arvatakse, et RSA murdmine peaks olema lihtsam), ega ka seda, et algteguriteks lahutamine on kuidagi olemuslikult arvutusmahukas operatsioon. Lihtsalt hetkel olemasolevad algoritmid ei võimalda meil praktikas kumbagi eriti kiiresti teha.

Näide 9.8. Olgu meil teada allkirjastatud tekst 081820090969, avalik võti $(2419, 19)$ ja sõnumite teisendamise skeem, kus igale neljakohalisele numbrile *abcd* vastavad *ab*.-s ja *cd*.-s täht 26-tähelises ladina tähestikus ning 00 tähistab sõnadevahelist tühikut. Tuvastame digiallkirja, jagades teksti kõigepealt blokkidesse 0818, 2009 ja 0969. Seejärel arvutame

$$818^{19} \equiv 1209 \pmod{2419}, \quad 2009^{19} \equiv 820 \pmod{2419}, \quad 969^{19} \equiv 1405 \pmod{2419}.$$

Astendamisel on otstarbekas kasutada skeemi $s^{19} = s^{16} \cdot s^2 \cdot s$ ning leida järjest s^2, s^4, s^8 ja s^{16}. Seega dekodeeritud sõnum on 120908201405, mis teiseneb tagasi kujule $12 \mapsto L$, $9 \mapsto I$, $8 \mapsto H$, $20 \mapsto T$, $14 \mapsto N$ ja $5 \mapsto E$. Algtekst oli järelikult LIHTNE ja kui me juba varem teadsime, et ta pidigi olema LIHTNE, siis ka korrektselt allkirjastatud.

Kodeerimisel on otstarbekas leida $c \equiv s^d \pmod{pq}$ mõlema algteguri järgi eraldi ($c_p = s^d \pmod{p}$ ja $c_q = s^d \pmod{q}$) ning kasutada Hiina jäägiteoreemi c leidmiseks mooduli $n = pq$ järgi.

9.3. Diskreetne logaritm

Diskreetne logaritm on eelnevalt juba käsitletud indeksi mõiste üldistus suvalistele lõplikele rühmadele. Täpsemalt, kui G on lõplik rühm ja $a, g \in G$, siis arv k on *diskreetne logaritm* alusel g elemendist a kui

$$g^k = a.$$

Paneme tähele, et üldiselt ei ole siin vajalik, et rühm G koosneks jäägiklassidest, g oleks tema moodustaja või isegi seda, et G oleks tsükliline. Praktikas on ühed populaarsemad rühmad siiski jäägiklassikorpuste multiplikatiivsed rühmad $\mathbb{Z}_p^*$, kus p on algarv.

9.3.1. Diffie-Hellmani võtmevahetus

Diffie-Hellmani[5] võtmevahetus on meetod salajase informatsiooni (üldiselt on selleks mingi krüptosüsteemi salajased võtmed või nende osad) jagamiseks üle ebaturvalise kanali (näiteks avalik internet).
Skeem iseenesest on järgmine:

- valime lõpliku tsüklilise rühma G ja selle moodustaja g (sageli $G = \mathbb{Z}_p^*$ ja g on algjuur mooduli p järgi);
- osapool A valib juhusliku naturaalarvu k ja saadab teisele osapoolele B elemendi g^k;
- osapool B valib samuti juhusliku naturaalarvu l ja saadab A-le tagasi g^l;
- A arvutab $(g^l)^k$, B aga $(g^k)^l$;
- kuna mistahes rühmas $(g^l)^k = g^{kl} = (g^k)^l$, siis on mõlemal osapoolel nüüd *jagatud saladus* g^{kl}.

Põhimõtteliselt võib kolmas (pahatahtlik) osaline E eelnevat protsessi pealt kuulata ja teada saada elemendid g^k ning g^l. Kuna esimene samm tehakse tavaliselt ära tunduvalt varem ja samuti võib-olla mitteturvalises keskkonnas, siis võib E teada ka rühma G ja tema moodustajat g. Teadaoleva informatsiooni kohta võib seetõttu koostada järgmise tabeli:

[5] Ameerika arvutiteadlaste Whitfield Diffie ja Martin Edward Hellmani järgi.

Osapool	G	g	k	l	g^k	g^l	g^{kl}
A	+	+	+	−	+	+	+
B	+	+	−	+	+	+	+
E	+	+	−	−	+	+	−

Diffie-Hellmani võtmevahetuse murdmiseks oleks vaja lahendada järgmine ülesanne: teades tsüklilise rühma G moodustajat g ning elemente g^k ja g^l, leida element g^{kl}. Seni on kõige efektiivsemaks lahendusmeetodiks osutunud diskreetsete logaritmide $k = \log_g g^k$ ja $l = \log_g g^l$ leidmine, mille abil saab otse arvutada g^{kl}.

Samamoodi, nagu ei ole teada efektiivseid algoritme naturaalarvude tegurdamiseks mittekvantarvutitel, ei ole neid olemas ka diskreetsete logaritmide leidmiseks. See ei ole jälle matemaatiline fakt, st. ei ole tõestatud selliste algoritmide olemasolu võimatust, neid lihtsalt ei ole suudetud välja mõelda. Nagu RSA puhulgi, ei ole ka Diffie-Hellmani võtmevahetuse jaoks otseselt tõestatud ei seda, et diskreetsete logaritmide leidmine on tarvilik (kuigi erinevalt RSA-st on siin olemas mitmed tulemused erijuhtude jaoks) ega seda, et diskreetsete logaritmide leidmine on juba oma olemuselt arvutuslikult keeruline.

Näide 9.9. Liisi ja Robert tahavad salakirjade saatmiseks omale ühist võtit, aga Robert on ajutiselt Soome kolinud. Nad ei oska hinnata, kuivõrd turvaline on nende võrguühendus. Oma elukohtade pealtkuulamatuse suhtes on nad aga kindlad ja seega otsustavad kasutada Diffie-Hellmani võtmevahetust. Kui Robert viimast korda Eestis käis, leppisid nad kokku, et kasutavad rühma $\mathbb{Z}_{19}^*$ ja algjuurt $g = 2$. (Kuna moodul 19 on väike, saab kasutada indeksite tabelit, aga praktikas töötab Diffie-Hellmani võtmevahetus vaid siis, kui indeksite tabeli koostamine on raske, sest indeksite tabel koosnebki diskreetsetest logaritmidest). Alati võib aga kasutada lemmast 7.31 tulenevat fakti, et $2^{x+18y} \equiv 2^x \pmod{19}$ iga $x, y \in \mathbb{Z}$ korral. Liisi läheb koju, valib juhuslikult arvu $k = 29$, arvutab

$$2^{29} \equiv 2^{11} \equiv 15 \pmod{19}$$

ja saadab Robertile arvu 15. Robert valib $l = 32$, leiab

$$2^{32} \equiv 2^{14} \equiv 6 \pmod{19}$$

ning saadab Liisile tagasi 6. Liisi arvutab

$$6^{29} \equiv 6^{11} = (2^{14})^{11} = 2^{154} \equiv 2^{10} = 17,$$

Robert aga

$$15^{32} \equiv 15^{14} \equiv (2^{11})^{14} = 2^{154} \equiv 2^{10} \equiv 17.$$

Nende ühiseks saladuseks ongi arv 17.

10. Lõplikud korpused*

Selles peatükis uurime lõplikke korpusi. Nagu mainitud, on Wedderburni teoreemi põhjal kõik lõplikud korpused kommutatiivsed. Kõige lihtsamaks näiteks lõplikest korpustest on meile hästituntud jäägiklassikorpused $\mathbb{Z}_p$, kuid osutub, et on ka teisi lõplikke korpusi.

10.1. Lõplike korpuste ehitus

Olgu K lõplik korpus ühikelemendiga $\mathbf{1}$ ja nullelemendiga $\mathbf{0}$. Edaspidises kasutame mistahes naturaalarvu m ja elemendi $a \in K$ korral tähistusi

$$ma = \underbrace{a + a + \ldots + a}_{m \text{ liidetavat}},$$

$0a = \mathbf{0}$ ning $(-m)a = -(ma)$. Lihtne on kontrollida, et nii defineeritud korpuse elemendi täisarvkordsete jaoks kehtivad järgmised omadused:

- $(\forall m, k \in \mathbb{Z})(\forall a \in K)((m+k)a = ma + ka)$;
- $(\forall m, k \in \mathbb{Z})(\forall a \in K)((mk)a = m(ka))$;
- $(\forall m \in \mathbb{Z})(\forall a, b \in K)(m(a+b) = ma + mb)$;
- $(\forall m \in \mathbb{Z})(\forall a, b \in K)(m(ab) = (ma)b)$;
- $(\forall m, k \in \mathbb{Z})(\forall a, b \in K)((ma)(kb) = (mk)(ab))$.

Kuna hulk K on lõplik, siis $(K, +)$ on lõplik rühm ja seega peavad kõik tema elemendid olema lõplikku järku. Olgu p ühikelemendi $\mathbf{1} \in K$ järk aditiivses rühmas $(K, +)$, s.t. vähim selline naturaalarv p, et $p\mathbf{1} = \mathbf{0}$. Siis öeldakse, et korpuse K *karakteristika* on p ja tähistatakse $\mathrm{char}K = p$. Definitsioonist järeldub, et kui $\mathrm{char}K = p$, siis iga $a \in K$ korral $pa = \mathbf{0}$, sest

$$pa = p(\mathbf{1} \cdot a) = (p\mathbf{1})a = \mathbf{0}a = \mathbf{0}.$$

Lause 10.1. *Lõpliku korpuse karakteristika on algarv.*

Tõestus. Olgu p elemendi $\mathbf{1} \in K$ järk rühmas $(K, +)$. Näitame, et p on algarv. Selleks oletame vastuväiteliselt, et $p = kl$, kus $1 < k, l < p$. Siis $k\mathbf{1} \neq \mathbf{0}$ ja $l\mathbf{1} \neq \mathbf{0}$, kuid $(k\mathbf{1}) \cdot (l\mathbf{1}) = (kl)(\mathbf{1} \cdot \mathbf{1}) = (kl)\mathbf{1} = p\mathbf{1} = \mathbf{0}$. Korrutades selle võrduse pooli elemendiga $(k\mathbf{1})^{-1}$ saame vastuolu $l\mathbf{1} = \mathbf{0}$. Seega p on algarv. □

Definitsioon 10.2. Kui korpus K on korpuse L alamkorpus, siis öeldakse, et korpus L on korpuse K *laiend*.

Lause 10.3. *Korpuse iga laiendi karakteristika on võrdne selle korpuse karakteristikaga.*

Tõestus. Olgu L korpuse K laiend ja $\mathrm{char}K = p$. Siis K kui korpuse L alamkorpus peab sisaldama korpuse L ühikelemendi $\mathbf{1}$, mis on seega ka K ühikelemendiks. Kuna elemendi $\mathbf{1}$ järk rühmas $(K, +)$ on p, siis tema järk rühmas $(L, +)$ on samuti p ja seega $\mathrm{char}L = p$. □

Lause 10.4. *Korpuse K iga laiendit L võib vaadelda vektorruumina üle korpuse K. Kui L on lõplik ja $|K| = q$, siis $|L| = q^m$, kus $m \in \mathbb{N}$.*

Tõestus. Vaatleme hulka L vektorruumina, kus liitmine on korpuse L liitmine ning vektori $a \in L$ ja skalaari $\alpha \in K$ korrutis on defineeritud kui nende elementide korrutis αa korpuses L. Vektorruumi aksioomide täidetus järeldub kohe korrutamise assotsiatiivsusest ja distributiivsuse seadustest korpuses L. Kui L on lõplik, siis on ta lõplikumõõtmeline vektorruum üle korpuse K ning seega, nagu hästi teada, omab lõplikku baasi ([1], teoreem 3.2.3). Olgu $e_1, \ldots, e_m$ baas vektorruumis L üle korpuse K. Siis iga $a \in L$ esitub üheselt lineaarkombinatsioonina $a = \alpha_1 e_1 + \ldots + \alpha_m e_m$, kus $\alpha_1, \ldots, \alpha_m \in K$. Et iga kordaja α_i valikuks on q võimalust, siis selliseid lineaarkombinatsioone on q^m tükki, s.t. $|L| = q^m$. □

Teoreem 10.5. *Lõpliku korpuse elementide arv on algarvu aste.*

Tõestus. Olgu K lõplik korpus, mille karakteristika on p. Vaatleme hulka

$$P = \{\mathbf{1}, \mathbf{1}+\mathbf{1}, \mathbf{1}+\mathbf{1}+\mathbf{1}, \ldots, (p-1)\mathbf{1}, p\mathbf{1} = \mathbf{0}\} \subseteq K.$$

Iga täisarvu m korral leiduvad $q, r \in \mathbb{Z}$ nii, et $m = pq + r$ ja $0 \leqslant r < p$. Seega $m\mathbf{1} = (pq)\mathbf{1} + r\mathbf{1} = q(p\mathbf{1}) + r\mathbf{1} = r\mathbf{1}$ ja $P = \{m\mathbf{1} \mid m \in \mathbb{Z}\}$. Kuna mistahes $k, l \in \{1, \ldots, p\}$ korral $k\mathbf{1} + l\mathbf{1} = (k+l)\mathbf{1} \in P$, $-(k\mathbf{1}) = (p-k)\mathbf{1} \in P$, $(k\mathbf{1}) \cdot (l\mathbf{1}) = (kl)\mathbf{1} \in P$ ja kui $k \neq p$, siis $(k\mathbf{1})^{-1} = u\mathbf{1} \in P$, kus $ku \equiv 1 \pmod{p}$ (ehk $\overline{u} = \overline{k}^{-1}$ korpuses $\mathbb{Z}_p$), siis P on korpuse K alamkorpus. Märgime, et korpus P on isomorfne korpusega $\mathbb{Z}_p$, kusjuures isomorfismi realiseerib kujutus $f : P \longrightarrow \mathbb{Z}_p$,

$$f(k\mathbf{1}) = \overline{k}.$$

Lause 10.4 põhjal leidub selline naturaalarv n, et $|K| = p^n$. □

Selle teoreemi tõestuse käigus näitasime, et kehtib järgmine väide.

Järeldus 10.6. *Kui korpuse K karakteristika on p, siis see korpus sisaldab jäägiklassikorpusega $\mathbb{Z}_p$ isomorfse alamkorpuse.*

Edasises läheb meil vaja järgmisi abitulemusi.

Lemma 10.7. *Kui kommutatiivse korpuse K karakteristika on p, siis iga $a, b \in K$ ja $n \in \mathbb{N}$ korral*

$$(a+b)^{p^n} = a^{p^n} + b^{p^n}.$$

Tõestus. Tõestame väite induktsiooniga n järgi. Olgu $n = 1$. Kuna K on kommutatiivne, siis $(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^{p-i} b^i$. Lemma 7.17 põhjal $p \mid \binom{p}{i}$ iga $i \in \{1, \ldots, p-1\}$ korral, s.t. leidub selline $k_i \in \mathbb{N}$, et $k_i p = \binom{p}{i}$. Järelikult iga $i \in \{1, \ldots, p-1\}$ korral

$$\binom{p}{i} a^{p-i} b^i = (k_i p)(a^{p-i} b^i) = k_i(p(a^{p-i} b^i)) = k_i \mathbf{0} = \mathbf{0},$$

seega $(a+b)^p = a^p + b^p$ ning induktsiooni alus on tõestatud.

Oletame nüüd, et $(a+b)^{p^k} = a^{p^k} + b^{p^k}$. Kasutades äsjatõestatut saame

$$(a+b)^{p^{k+1}} = \left((a+b)^{p^k}\right)^p = \left(a^{p^k} + b^{p^k}\right)^p = \left(a^{p^k}\right)^p + \left(b^{p^k}\right)^p = a^{p^{k+1}} + b^{p^{k+1}}.$$

□

Järgmise lemma üheks erijuhuks on Fermat' väike teoreem.

Lemma 10.8. *Kui K on lõplik korpus ning $|K| = q$, siis iga $a \in K^* = K \setminus \{\mathbf{0}\}$ korral $a^{q-1} = \mathbf{1}$.*

Tõestus. Olgu m elemendi a järk korpuse K multiplikatiivses rühmas K^*. Siis $m \mid q-1 = |K^*|$ ehk $mk = q-1$ mingi naturaalarvu k korral. Järelikult $a^{q-1} = a^{mk} = (a^m)^k = \mathbf{1}$. □

Olgu K kommutatiivne korpus ja vaatleme polünoomide ringi $K[x]$. Kui $p(x) \in K[x]$ on mingi polünoom üle korpuse K, siis selle polünoomi poolt tekitatud peaideaal

$$p(x)K[x] = \{p(x)h(x) \mid h(x) \in K[x]\}$$

koosneb kõigist polünoomidest ringis $K[x]$, mis jaguvad polünoomiga $p(x)$. Kõrvalklass esindajaga $f(x) \in K[x]$ ideaali $p(x)K[x]$ järgi on hulk

$$[f(x)] = f(x) + p(x)K[x] = \{f(x) + p(x)h(x) \mid h(x) \in K[x]\}.$$

Saab näidata, et

$$[f(x)] = [g(x)] \iff f(x) - g(x) \in p(x)K[x] \iff p(x) \mid f(x) - g(x). \tag{31}$$

(On lihtne aru saada, et kõrvalklassid on ekvivalentsiklassid "kongruentsusseose" järgi hulgal $K[x]$, kus polünoome $f(x)$ ja $g(x)$ loetakse "kongruentseiks", kui $p(x) \mid f(x) - g(x)$.) Sellest järeldub muuhulgas, et $[0] = [p(x)]$. Kui kõrvalklasside hulgal defineerida tehted esindajate abil, s.t.

$$\begin{aligned} [f(x)] + [g(x)] &= [f(x) + g(x)], \\ [f(x)] \cdot [g(x)] &= [f(x)g(x)], \end{aligned}$$

saame ringi, mida nimetatakse ringi $K[x]$ *faktorringiks* ideaali $p(x)K[x]$ järgi (vt. [1], def. 6.5.11) ning mida tähistatakse $K[x]/p(x)K[x] = \{[f(x)] \mid f(x) \in K[x]\}$.

Mittekonstantset polünoomi $p(x) \in K[x]$ nimetatakse *taandumatuks*, kui teda ei saa esitada kahe mittekonstantse polünoomi korrutisena, s.t. kui võrdusest $p(x) = f(x)g(x)$ järeldub, et kas polünoom $f(x)$ on konstantne või $g(x)$ on konstantne.

Lause 10.9. *Olgu K kommutatiivne korpus ja $p(x) \in K[x]$ taandumatu polünoom, mille aste $d \geqslant 2$. Siis faktorring $L = K[x]/p(x)K[x]$ on korpus, mis sisaldab korpusega K isomorfset alamkorpust ning milles polünoomil $p(x)$ on olemas juur. Seejuures kui $|K| = p^m$, siis $|L| = p^{md}$.*

Tõestus. Olgu

$$L = K[x]/p(x)K[x] = \{[f(x)] \mid f(x) \in K[x]\}$$

ringi $K[x]$ faktorring ideaali $p(x)K[x]$ järgi. Esimene väide on tõestatud raamatus [1] lausena 7.3.1. Meenutame, et elemendi $[0] \neq [f(x)] \in L$ pööratavus järeldub sellest, et $p(x)$ ei jaga polünoomi $f(x)$ ja $p(x)$ on taandumatu (seega $(p(x), f(x)) = 1$), korpusega K isomorfseks alamkorpuseks korpuses L on konstantsete polünoomide kõrvalklasside hulk $K' = \{[k] \mid k \in K\}$ ning polünoomi $p(x)$ üheks juureks korpuses L on lineaarpolünoomi x kõrvalklass $[x]$ (s.t. $p([x]) = [0]$).

Näitame veel, et korpuses L on p^{md} elementi. Selleks tõestame, et

$$K[x]/p(x)K[x] = \{[f(x)] \mid f(x) \in K[x], \deg f(x) < d\}.$$

Tuleb veenduda, et

$$\{[f(x)] \mid f(x) \in K[x]\} \subseteq \{[f(x)] \mid f(x) \in K[x], \deg f(x) < d\}$$

(vastupidine sisalduvus on ilmne). Võttes $g(x) \in K[x]$ võime selle polünoomi jagada jäägiga polünoomiga $p(x)$, s.t. leida sellised $q(x), r(x) \in K[x]$, et

$$g(x) = p(x)q(x) + r(x) \quad \text{ja} \quad \deg r(x) < \deg p(x) = d.$$

Järelikult

$$[g(x)] = [p(x)][q(x)] + [r(x)] = [0][q(x)] + [r(x)] = [r(x)] \in \{[f(x)] \mid f(x) \in K[x], \deg f(x) < d\}.$$

Seega iga kõrvalklassi esindajaks saab valida sellise polünoomi, mille aste on väiksem kui d:

$$L = \{[k_{d-1}x^{d-1} + \ldots + k_1x + k_0] \mid k_0, \ldots, k_{d-1} \in K\}. \tag{32}$$

Erinevaid selliseid polünoome on $|K|^d$ tükki ning erinevatele sellistele polünoomidele vastavad erinevad kõrvalklassid, sest kui $f(x), g(x) \in K[x]$, $f(x) \neq g(x), \deg f(x) < d$ ja $\deg g(x) < d$, siis $f(x) - g(x) \neq 0$, $\deg(f(x) - g(x)) < d$, mistõttu $p(x)$ ei jaga polünoomi $f(x) - g(x)$ ja seega (31) põhjal $[f(x)] \neq [g(x)]$. Sellega oleme tõestanud, et $|L| = |K|^d = p^{md}$. □

Lauset 10.9 kasutades saab tõestada järgmise teoreemi.

Teoreem 10.10 ([1], teoreem 7.3.3). *Olgu $f(x) \in K[x]$ polünoom kordajatega kommutatiivsest korpusest K ning olgu $f(x)$ aste $n \geqslant 1$. Siis leidub korpuse K selline laiend L, milles polünoomil $f(x)$ on n juurt.*

Kui need teoreemis 10.10 mainitud juured on $a_1, \ldots, a_n \in L$, siis $f(x)$ lahutub lineaartegurite korrutiseks üle korpuse L: $f(x) = b(x - a_1) \ldots (x - a_n)$, kus $b \in K$ on x^n kordaja polünoomis $f(x)$.

Definitsioon 10.11. Korpuse K laiendit L nimetatakse polünoomi $f(x) \in K[x]$ *lahutuskorpuseks*, kui $f(x)$ lahutub lineaartegurite korrutiseks üle L,

$$f(x) = b(x - a_1) \ldots (x - a_n),$$

kus $a_1, \ldots, a_n, b \in L$, ning L on korpuse K vähim laiend, mis sisaldab elemendid $a_1, \ldots, a_n$. Kui K on lõplik, siis ka $f(x)$ lahutuskorpus L on lõplik.

Teoreemist 10.10 järeldub, et igal mittekonstantsel polünoomil üle kommutatiivse korpuse on lahutuskorpus olemas. Veelgi enam, kehtib järgmine teoreem, mida me siinkohal ei tõesta (vt. [12], lk. 343–350).

Teoreem 10.12. *Polünoomi lahutuskorpus on isomorfismi täpsuseni üheselt määratud.*

Teoreem 10.5 väitis, et lõpliku korpuse elementide arv on algarvu aste. Järgnevalt veendume, et kehtib ka selle teoreemi pöördteoreem.

Teoreem 10.13. *Iga algarvu p ja naturaalarvu n korral leidub korpus, milles on p^n elementi.*

Tõestus. Olgu $q = p^n$. Vaatleme polünoomi $x^q - x \in \mathbb{Z}_p[x]$. Olgu L polünoomi $x^q - x$ lahutuskorpus ning olgu

$$x^q - x = (x - a_1) \dots (x - a_q),$$

kus $a_1, \dots, a_q \in L$. Kuna $\mathbb{Z}_p \subseteq L$ on alamkorpus, siis lause 10.3 põhjal on korpuse L karakteristika p, s.t. $p\mathbf{1} = \mathbf{0}$ ja seega ka $q\mathbf{1} = \mathbf{0}$. Järelikult $(x^q - x)' = (q\mathbf{1})x^{q-1} - \mathbf{1} = -\mathbf{1} \in L[x]$ ning seega polünoomi $x^q - x$ ja tema tuletise suurim ühistegur ringis $L[x]$ on

$$((x^q - x), (x^q - x)') = ((x^q - x), -\mathbf{1}) = \mathbf{1}.$$

Näitame, et sellest järeldub, et polünoomil $x^q - x$ ei ole kordseid juuri. Oletame vastuväiteliselt, et $a \in L$ on polünoomi $x^q - x$ kordne juur, s.t. $x^q - x = (x - a)^k g(x)$, kus $k \geqslant 2$ ja $g(x) \in L[x]$. Siis korrutise tuletise leidmise reegli põhjal

$$(x^q - x)' = (k\mathbf{1})(x - a)^{k-1} g(x) + (x - a)^k g'(x) = (x - a)\left((k\mathbf{1})(x - a)^{k-2} g(x) + (x - a)^{k-1} g'(x)\right).$$

Seega $(x - a) \mid ((x^q - x), (x^q - x)') = \mathbf{1}$ ringis $L[x]$, vastuolu. Järelikult tõesti polünoomil $x^q - x$ pole kordseid juuri, mis tähendab, et elemendid $a_1, \dots, a_q$ on erinevad.

Vaatleme q-elemendilist alamhulka

$$K = \{a_1, \dots, a_q\} = \{a \in L \mid a^q = a\} \subseteq L.$$

Näitame, et K on korpuse L alamkorpus. Selleks näitame, et K on kinnine tehete suhtes. Olgu $a, b \in K$, s.t. $a^q = a$ ja $b^q = b$. Lemma 10.7 põhjal

$$(a + b)^q = (a + b)^{p^n} = a^{p^n} + b^{p^n} = a^q + b^q = a + b,$$

s.t. $a + b \in K$. Kui $p = 2$, siis $a + a = \mathbf{0}$ ehk $-a = a \in K$. Kui aga $p > 2$, siis

$$(-a)^q = ((-\mathbf{1})a)^q = (-\mathbf{1})^q a^q = (-\mathbf{1})\, a = -a,$$

s.t. $-a \in K$. Korrutamise kommutatiivsuse tõttu ka

$$(ab)^q = a^q b^q = ab,$$

s.t. $ab \in K$. Olgu $a \neq \mathbf{0}$. Siis

$$(a^{-1})^q = (a^q)^{-1} = a^{-1},$$

s.t. $a^{-1} \in K$. Seega K on alamkorpus. Lisaks sellele $\mathbb{Z}_p \subseteq K$, sest iga $\overline{c} \in \mathbb{Z}_p$ korral $\overline{c}^{p^n} = (\overline{c}^p)^{p^{n-1}} = \overline{c}^{p^{n-1}} = \ldots = \overline{c}$.

Kuna L on vähim korpus, mis sisaldab $\mathbb{Z}_p$ ja elemendid $a_1, \dots, a_q$, siis $L = K$, järelikult $|L| = |K| = q$. □

Saab näidata, et korpus, milles on p^n elementi, on isomorfismi täpsuseni üheselt määratud.

Korpust, milles on $q = p^n$ elementi, tähistatakse tihti kas $\mathbb{F}_q$ või $\mathrm{GF}(q)$ (GF=*Galois field*, prantsuse matemaatiku Évariste Galois' (1811–1832) järgi). Sellise korpuse konstrueerimiseks on otstarbekas kasutada lauset 10.9. Võtame näiteks korpuse $\mathbb{Z}_p$, leiame mingi n-nda astme taandumatu polünoomi üle $\mathbb{Z}_p$ ning moodustame faktorringi $\mathbb{Z}_p[x]/p(x)\mathbb{Z}_p[x]$. Tulemus on p^n-elemendiline korpus, mis tänu teoreemile 10.13 ongi $\mathbb{F}_q$.

Viimaks tõestame, et tegelikult kehtib teoreem 7.12 mitte ainult jäägiklassikorpustes $\mathbb{Z}_p$, vaid ka mistahes lõplikes korpustes.

Teoreem 10.14. *Iga lõpliku (kommutatiivse[6]) korpuse multiplikatiivne rühm on tsükliline.*

Tõestus. Olgu K lõplik korpus ühikelemendiga $\mathbf{1}$ ja nullelemendiga $\mathbf{0}$, $|K| = q$, ja tähistagu $K^* = K \setminus \{\mathbf{0}\} = U(K)$ selle korpuse multiplikatiivset rühma, s.t. nullist erinevate elementide hulka korrutamise suhtes. Olgu K_d rühma K^* kõigi selliste elementide hulk, mille järk on d. Kuna K^* iga elemendi järk on Lagrange'i teoreemi põhjal arvu $q - 1 = |K^*|$ jagaja ning elemendi järk on üheselt määratud, siis $K^* = \bigsqcup_{d|q-1} K_d$. Gaussi teoreemi (teoreem 5.11) põhjal

$$\sum_{d|q-1} \varphi(d) = q - 1 = |K^*| = \sum_{d|q-1} |K_d|. \tag{33}$$

[6]Iga lõplik korpus on Wedderburni teoreemi (vt. [11], teoreem 1.3.10) tõttu kommutatiivne.

Näitame, et iga $d \mid q-1$ korral $|K_d| = \varphi(d)$, ehk et rühmas K^* leidub täpselt $\varphi(d)$ elementi, mille järk on d.

Oletame, et antud $d \mid q-1$ korral $K_d \neq \emptyset$, s.t. et leidub d-ndat järku element a, ning tõestame, et sellisel juhul

$$K_d = \{a^k \mid 1 \leqslant k \leqslant d, (k,d) = 1\}. \tag{34}$$

Kuna a järk on d, siis elemendid $a, a^2, \ldots, a^d$ on erinevad ning nad rahuldavad võrrandit

$$x^d - \mathbf{1} = \mathbf{0},$$

sest $(a^k)^d = (a^d)^k = \mathbf{1}^k = \mathbf{1}$ iga $k = 1, \ldots, d$ korral. Kuna d-nda astme polünoomil üle korpuse K ei saa lause 2.9 põhjal olla rohkem kui d juurt korpuses K, siis $a, a^2, \ldots, a^d$ on polünoomi $x^d - \mathbf{1}$ ainsad juured, järelikult iga element $b \in K_d$ on võrdne ühega neist elementidest; olgu $b = a^k$. Oletame vastuväiteliselt, et $(k,d) = d' > 1$. Siis elemendi b järk oleks väiksem kui d, sest $b^{\frac{d}{d'}} = \left(a^k\right)^{\frac{d}{d'}} = \left(a^d\right)^{\frac{k}{d'}} = \mathbf{1}$ ja $\frac{d}{d'} < d$. Sellega oleme tõestanud, et $K_d \subseteq \{a^k \mid 1 \leqslant k \leqslant d, (k,d) = 1\}$. Oletame nüüd, et $1 \leqslant k \leqslant d$ ja $(k,d) = 1$. Olgu m elemendi a^k järk rühmas K^*. Kuna $(a^k)^d = \mathbf{1}$, siis $m \leqslant d$. Lisaks sellele $a^{km} = \left(a^k\right)^m = \mathbf{1}$. Kuna a järk on d, siis lemma 7.6 põhjal $d \mid km$. Järelduse 1.10 tõttu peab $d \mid m$, mis koos võrratusega $m \leqslant d$ annab, et $m = d$, s.t. $a^k \in K_d$. Sellega oleme tõestanud võrduse (34).

Niisiis iga $d \mid q-1$ korral kas $|K_d| = \varphi(d)$ või $K_d = \emptyset$. Tänu võrdusele (33) ei ole aga viimane võrdus võimalik. Seega iga $d \mid q-1$ korral on täpselt $\varphi(d)$ elementi, mille järk on d. Muuhulgas, kuna $q-1 \mid q-1$, siis leidub $\varphi(q-1)$ elementi, mille järk on $q-1$, teiste sõnadega: leidub $\varphi(q-1)$ rühma K^* moodustajat. Kui a on mingi moodustaja, siis ülejäänud moodustajaiks on eespooltõestatu põhjal astmed a^k, kus $1 \leqslant k \leqslant q-1$ ja $(k, q-1) = 1$. □

Lõpliku korpuse multiplikatiivse rühma moodustajaid nimetatakse selle korpuse *primitiivseteks elementideks*. (Niisiis korpuse $\mathbb{Z}_p$ primitiivsed elemendid on algjuured mooduli p järgi.)

10.2. Aritmeetika lõplikes korpustes

Lõpliku korpuse elementide esitamiseks on mitmeid võimalusi. Üks viis on kasutada faktorringi $\mathbb{F}_q[x]/p(x)\mathbb{F}_q[x]$, kus $p(x)$ on taandumatu polünoom üle $\mathbb{F}_q$. Teine võimalus on kasutada fakti, et rühm $\mathbb{F}_q^*$ on tsükliline ja seega tema elemendid on esitatavad moodustaja (primitiivse elemendi) astmetena. On selge, et liita on lihtsam elemente, mis on esitatud polünoomidena ning korrutada on lihtsam rühma moodustaja astmeid. Osutub, et neid kahte viisi saab omavahel kombineerida, mis annab võimaluse aritmeetiliste tehete efektiivseks sooritamiseks lõplikus korpuses.

Näide 10.15. Vaatleme lõplikku korpust $\mathbb{F}_{16}$ kui korpuse $\mathbb{F}_2 = \mathbb{Z}_2 = \{0,1\}$ ($\overline{0}$ ja $\overline{1}$ asemel kirjutame 0 ja1) laiendit.

Näitame, et polünoom $p(x) = x^4 + x + 1$ on taandumatu üle $\mathbb{F}_2$. Selleks paneme tähele, et kui $p(x)$ oleks taanduv, siis ta peaks omama kas lineaar- või ruuttegurit. Kuna $p(0) \neq 0$ ja $p(1) \neq 0$, siis polünoomil $p(x)$ pole lineaartegureid. Veendumaks, et polünoom $p(x)$ ei jagu ühegi ruutpolünoomiga, märgime, et üle $\mathbb{F}_2$ on täpselt neli erinevat ruutpolünoomi

$$x^2, x^2+1, x^2+x, x^2+x+1$$

ning vahetu kontroll näitab, et neid polünoome omavahel korrutades me ei saa polünoomi $p(x)$.

Kuna polünoomi $p(x)$ aste on 4, siis lause 10.9 põhjal

$$\mathbb{F}_2[x]/(x^4+x+1)\mathbb{F}_2[x] = \mathbb{F}_{16}.$$

Tähistame $a = [x]$ ning samastame kõrvlaklassid [0] ja [1] esindajatega 0 ja 1. Kui vaatleme polünoomile $p(x)$ vastavat polünoomi $\tilde{p}(y) = y^4 + y + 1 \in \mathbb{F}_{16}[y]$, siis a on polünoomi $\tilde{p}(y)$ juur, sest

$$\tilde{p}(a) = a^4 + a + 1 = [x]^4 + [x] + [1] = [x^4 + x + 1] = [0].$$

Tänu võrdusele (32) võib korpuse $\mathbb{F}_{16}$ elemente esitada kui ülimalt kolmanda astme polünoome a suhtes:

konstantsed	$0, 1,$
lineaarsed	$a, a+1,$
ruutpolünoomid	$a^2, a^2+1, a^2+a, a^2+a+1$
kuuppolünoomid	$a^3, a^3+1, a^3+a, a^3+a^2, a^3+a+1,$
	$a^3+a^2+1, a^3+a^2+a, a^3+a^2+a+1.$

Sellisel kujul elementide liitmine on lihtne, sest see on lihtsalt polünoomide liitmine. Korrutamine nõuab taandamist "mooduli $p(x)$ järgi", s.o. jäägiga jagamist polünoomiga x^4+x+1, kuid võib kasutada ka seost $a^4+a+1=0$ ehk $a^4 = a+1$. Näiteks

$$\begin{aligned} a^{14} &= (a^4)^3a^2 = (a+1)^3a^2 = (a^3+a^2+a+1)a^2 = a^5+a^4+a^3+a^2 \\ &= (a+1)a + a + 1 + a^3 + a^2 = a^2 + a + a + 1 + a^3 + a^2 = a^3 + 1. \end{aligned}$$

Kuna $a \neq 0$, siis $a \in \mathbb{F}_{16}^*$, ning kuna $a^3 \neq 1$ ja $a^5 = a^2 + a \neq 1$, siis järelduse 7.23 põhjal on a rühma $\mathbb{F}_{16}^*$ moodustaja. Seega

$$\mathbb{F}_{16} = \{0, 1, a, a^2, \ldots, a^{14}\}.$$

Sellisel viisil esitatud elementide korrutamine on lihtne, kuid liitmine on tülikas.

Need kaks esitust saab omavahel siduda, kui arvutada välja tabel, mis näitab, kuidas element a^k esitub ülimalt kolmanda astme polünoomina a suhtes. Kasutades seost $a^4 = a + 1$ saame

$$\begin{aligned}
&a^4 = a + 1,\\
&a^5 = a \cdot a^4 = a(a + 1) = a^2 + a,\\
&a^6 = a \cdot a^5 = a^3 + a^2,\\
&a^7 = a \cdot a^6 = a^4 + a^3 = a^3 + a + 1
\end{aligned}$$

ja nii edasi. Tulemused võtame kokku alljärgneva tabelina, kus elemendi a^k asemel kirjutame lihtsalt k ning polünoomi $k_3a^3 + k_2a^2 + k_1a + k_0$ asemel kirjutame tema kordajate jada $k_3k_2k_1k_0$.

0	0001
1	0010
2	0100
3	1000
4	0011
5	0110
6	1100
7	1011
8	0101
9	1010
10	0111
11	1110
12	1111
13	1101
14	1001

Selle tabeli ning seose $a^{15} = 1$ abil võime nüüd näiteks arvutada

$$(a^8 + a^4 + 1)(a^3 + a) = (0101 + 0011 + 0001)(1000 + 0010) = (0111)(1010) = a^{10} \cdot a^9 = a^{19} = a^4 = a + 1.$$

Seega arvutamiseks (liitmiseks ja korrutamiseks) lõplikus korpuses on kasulik teada tema multiplikatiivse rühma moodustajat koos mingi taandumatu polünoomiga, mille juureks ta on. Üldjuhul pole taandumatu polünoomi leidmine lihtne. Siiski on paljude konkreetsete korpuste jaoks leitud taandumatud polünoomid ja tabelid (vt. nt. [13]).

10.3. Juurimine lõplikes korpustes

Definitsioon 10.16. Olgu K (suvaline) korpus ja $b \in K$. Elementi $a \in K$ nimetatakse *n-nda astme juureks* elemendist b, kui $a^n = b$. n-nda astme juurt korpuse K ühikelemendist $\mathbf{1}$ nimetatakse *n-nda astme ühejuureks*.

Lause 10.17. *Kommutatiivse korpuse K kõigi n-nda astme ühejuurte hulk H_n on rühma K^* alamrühm.*

Tõestus. Tähistame

$$H_n = \{a \in K^* \mid a^n = \mathbf{1}\}$$

ning olgu $a, b \in H_n$, s.t. $a^n = \mathbf{1}$ ja $b^n = \mathbf{1}$. Siis ka $(ab)^n = a^n b^n = \mathbf{1}$. Kui $a \in H_n$, s.t. $a^n = \mathbf{1}$, siis ka $\left(a^{-1}\right)^n = (a^n)^{-1} = \mathbf{1}^{-1} = \mathbf{1}$. Seega H_n on rühma K^* alamrühm. □

Kuna n-nda astme ühejuured on polünoomi $x^n - \mathbf{1} \in K[x]$ juured, siis lause 2.9 tõttu ei saa neid olla rohkem kui n tükki. On tuntud fakt, et kompleksarvude korpuses $\mathbb{C}$ on n-nda astme ühejuuri täpselt n tükki ja ühejuurte rühm on tsükliline, kuid iga korpuse korral see nii ei ole. Näiteks korpustes $\mathbb{R}$ ja $\mathbb{Z}_3$ on ühikelement ainus 3. astme ühejuur.

Definitsioon 10.18. Kui n-nda astme ühejuuri kommutatiivses korpuses K on n tükki ning kõik nad on esitatavad n-nda astme ühejuure ξ astmetena (s.t. kui H_n on n-ndat järku rühm ja ξ on rühma H_n moodustaja), siis ühejuurt ξ nimetatakse *primitiivseks n-nda astme ühejuureks.*

Teoreem 10.19. *Olgu $n \geqslant 2$ naturaalarv ja a korpuse $\mathbb{F}_q$ primitiivne element, s.t. $\mathbb{F}_q^* = \{a, a^2, \ldots, a^{q-2}, a^{q-1} = \mathbf{1}\}$. Siis*

1. *iga $k \in \{1, \ldots, q-1\}$ korral, a^k on n-nda astme ühejuur parajasti siis, kui $q-1 \mid kn$;*
2. *n-nda astme ühejuuri on $(n, q-1)$ tükki;*
3. *korpuses $\mathbb{F}_q$ leidub primitiivne n-nda astme ühejuur parajasti siis, kui $n \mid q-1$;*
4. *$\mathbb{F}_q^*$ elemente, mis omavad n-nda astme juurt, on $\frac{q-1}{(n,q-1)}$ tükki.*

TÕESTUS. 1. Olgu a^k n-nda astme ühejuur. Siis $a^{kn} = \mathbf{1}$, ning kuna elemendi a järk rühmas $\mathbb{F}_q^*$ on $q-1$, siis lemma 7.6 põhjal $q-1 \mid kn$. Vastupidi, oletame, et leidub täisarv u, nii et $(q-1)\,u = kn$. Kuna $a \in \mathbb{F}_q^*$, siis lemma 10.8 põhjal $\left(a^k\right)^n = a^{(q-1)u} = \left(a^{q-1}\right)^u = \mathbf{1}$, s.t. a^k on n-nda astme ühejuur.

2. Tähistame $d = (q-1, n)$. Siis leiduvad sellised $m, n' \in \mathbb{N}$, et $q-1 = md$ ja $n = n'd$, kusjuures $(m, n') = 1$. Järelikult, iga $k \in \{1, \ldots, q-1\}$ korral, $q-1 \mid kn$ (s.t. $md \mid kn'd$) parajasti siis, kui $m \mid k$. Selliseid astendajaid $k \in \{1, \ldots, q-1\}$, mida m jagab, on d tükki: $m, 2m, \ldots, dm = q-1$. Seega on olemas täpselt d n-nda astme ühejuurt,

$$H_n = \{a^m, a^{2m}, \ldots, a^{(d-1)m}, a^{dm} = \mathbf{1}\} = \langle a^m \rangle,$$

ning kõik ühejuured avalduvad ühejuure a^m astmetena.

3. Osa 2 põhjal on H_n d-ndat järku tsükliline rühm moodustajaga a^m. On selge, et primitiivne ühejuur leidub parajasti siis, kui $d = (n, q-1) = n$, mis on samaväärne sellega, et $n \mid q-1$. Primitiivseks n-nda astme ühejuureks on sel juhul a^m.

4. Vaatleme kõrvalklasse rühma $\mathbb{F}_q^*$ alamrühma H_n järgi, s.t. hulki

$$cH_n = \{cb \mid b \in H_n\} = \{ca^{im} \mid i \in \{1, \ldots, d\}\},$$

$c \in \mathbb{F}_q^*$. Need kõrvalklassid ei lõiku ning kõigi kõrvalklasside võimsused on võrdsed, s.t. iga $c \in \mathbb{F}_q^*$ korral $|cH_n| = |H_n|$ ([1], lemma 6.1.1 ja lemma 6.1.3). Kõrvalklasside arv on seega $\frac{\left|\mathbb{F}_q^*\right|}{|H_n|} = \frac{q-1}{d} = m$. Näitame, et elemendid kuuluvad samasse kõrvalklassi parajasti siis, kui nende n-ndad astmed on võrdsed. Olgu $cb \in cH_n$, $b \in H_n$. Siis $(cb)^n = c^n b^n = c^n \mathbf{1} = c^n$, seega kõrvalklassi cH_n kõigi elementide n-ndad astmed on võrdsed kõrvalklassi esindaja c n-nda astmega (s.t. kõik kõrvalklassi cH_n elemendid on n-nda astme juurteks elemendist c^n). Vastupidi, oletame, et $c_1^n = c_2^n$. Siis $\left(c_2^{-1}c_1\right)^n = \left(c_2^{-1}\right)^n c_1^n = \left(c_2^n\right)^{-1} c_1^n = \mathbf{1}$, seega $c_2^{-1}c_1 \in H_n$. Järelikult $c_1 = c_2 c_2^{-1} c_1 \in c_2 H_n$. Seega $c_1 H_n \subseteq c_2 H_n$. Analoogiliselt $c_2 H_n \subseteq c_1 H_n$ ning kokkuvõttes $c_1 H_n = c_2 H_n$. (Seega erinevatesse kõrvalklassidesse kuuluvad elemendid on erinevate elementide n-nda astme juured.) □

Järeldus 10.20. *Kui $(n, q-1) = 1$, siis $\mathbf{1}$ on ainus n-nda astme ühejuur korpuses $\mathbb{F}_q$.*

Järeldus 10.21. *Element $-\mathbf{1} \in \mathbb{F}_q$, kus q on paaritu arv, omab ruutjuurt korpuses $\mathbb{F}_q$ parajasti siis, kui $q \equiv 1 \pmod 4$.*

TÕESTUS. Näitame, et ruutjuured elemendist $-\mathbf{1}$ on täpselt 4. astme primitiivsed ühejuured. Olgu ξ ruutjuur elemendist $-\mathbf{1}$, s.t. $\xi^2 = -\mathbf{1}$. Siis $\xi, \xi^2 = -\mathbf{1}, \xi^3 = -\xi, \xi^4 = \mathbf{1}$ on neli erinevat 4. astme ühejuurt ning seega ξ on primitiivne 4. astme ühejuur. Vastupidi, olgu ξ primitiivne 4. astme ühejuur. Siis $\xi^4 = \mathbf{1}$, järelikult $\xi^4 - \mathbf{1} = (\xi^2 + \mathbf{1})(\xi^2 - \mathbf{1}) = \mathbf{0}$. Kuna ξ on primitiivne 4. astme ühejuur, siis ei ole võimalik, et $\xi^2 = \mathbf{1}$, sest siis me saaksime ξ astmetena kätte vaid kaks 4. astme ühejuurt (ξ ise ja $\mathbf{1}$). Seega, kuna korpus ei sisalda nullitegureid, peab $\xi^2 + \mathbf{1} = \mathbf{0}$, ehk $\xi^2 = -\mathbf{1}$. Sellega oleme näidanud, et ruutjuured elemendist $-\mathbf{1}$ on parajasti 4. astme primitiivsed ühejuured. Teoreemi 10.19 põhjal leidub korpuses K primitiivseid 4. astme ühejuuri parajasti siis, kui $4 \mid q-1$ ehk $q \equiv 1 \pmod 4$. □

Märkus 10.22. Kui $q = 2^l$, siis $\mathbf{1} = -\mathbf{1}$ ja seega $-\mathbf{1}$ omab ruutjuurt korpuses $\mathbb{F}_q$.

Näide 10.23. Korpuses $\mathbb{Z}_{13}$ on ruutjuurteks elemendist $\overline{-1}$ elemendid $\overline{5}$ ja $\overline{8}$. Korpuses $\mathbb{Z}_7$ aga elemendil $\overline{-1}$ ruutjuurt ei ole, sest $7 \equiv 3 \pmod 4$.

Näide 10.24. Vaatleme korpust $\mathbb{F}_{16}$ näitest 10.15. Kuna $(2, 15) = 1$, siis $\mathbf{1}$ on ainus teise astme ühejuur korpuses $\mathbb{F}_{16}$. Primitiivseid teise astme ühejuuri selles korpuses ei ole. Kuna $(3, 15) = 3$, siis kolmanda astme ühejuuri korpuses $\mathbb{F}_{16}$ on 3 tükki, need on a^5, a^{10} ja $a^{15} = 1$ ehk $a^2 + a$, $a^2 + a + 1$ ja 1, kusjuures kaks esimest neist on primitiivsed.

Näide 10.25. Vaatleme korpust $\mathbb{F}_{13} = \mathbb{Z}_{13}$. Näite 7.25 põhjal teame, $\mathbb{Z}_{13}^* = \langle\overline{2}\rangle$. Järelikult $H_3 = \{\overline{2}^4, \overline{2}^8, \overline{2}^{12}\} = \{\overline{3}, \overline{9}, \overline{1}\}$. Kõrvalklasse alamrühma H_3 järgi on 4 tükki:

$$\begin{aligned}
\overline{1}H_3 &= H_3 = \{\overline{3}, \overline{9}, \overline{1}\} = \overline{3}H_3 = \overline{9}H_3,\\
\overline{2}H_3 &= \{\overline{6}, \overline{5}, \overline{2}\} = \overline{6}H_3 = \overline{5}H_3,\\
\overline{4}H_3 &= \{\overline{12}, \overline{10}, \overline{4}\} = \overline{12}H_3 = \overline{10}H_3,\\
\overline{7}H_3 &= \{\overline{8}, \overline{11}, \overline{7}\} = \overline{8}H_3 = \overline{11}H_3.
\end{aligned}$$

Seega elemente, mis omavad 3. astme juurt on $\frac{12}{(3,12)} = 4$ tükki ning need on $\overline{1}^3 = \overline{1}, \overline{2}^3 = \overline{8}, \overline{4}^3 = \overline{12}, \overline{7}^3 = \overline{5}$.

10.4. Gaussi ruutvastavusseadus

Lõplike korpuste abil on võimalik Gaussi ruutvastavusseadust mõnevõrra efektiivsemalt tõestada. Selleks vajame me ainult järgmist abitulemust.

Lemma 10.26. *Kui G on rühm ja $a \in G$, siis $G = aG$, kus $aG = \{ag \mid g \in G\}$.*

TÕESTUS. Kui $g \in G$, siis $g = (aa^{-1})g = a(a^{-1}g) \in aG$, seega $G \subseteq aG$. Vastupidine sisalduvus on ilmne. □

Järeldus 10.27. *Kui $n > 1$ ja a on ühistegurita täisarvud, siis $U(\mathbb{Z}_n) = \overline{a} \cdot U(\mathbb{Z}_n)$. Teiste sõnadega, kui arvud $a_1, a_2, \ldots, a_{\varphi(n)}$ on kõik naturaalarvud, mis on väiksemad kui n ja on arvuga n ühistegurita, siis*

$$aa_1, aa_2, \ldots, aa_{\varphi(n)}$$

on mooduli n järgi kongruentsed arvudega $a_1, a_2, \ldots, a_{\varphi(n)}$ mingis järjekorras.

Järeldus 10.28. *Kui q on algarv ja $q \nmid a$, siis $\mathbb{Z}_q^* = \overline{a} \cdot \mathbb{Z}_q^*$, s.t. arvud $a, 2a, \ldots, (q-1)a$ on mooduli q järgi kongruentsed arvudega $1, 2, \ldots, q-1$ mingis järjekorras.*

Teoreem 10.29 (Ruutvastavusseadus). *Kui $p > 2$ ja $q > 2$ on erinevad algarvud, siis*

$$\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{q}{p}\right) = \begin{cases} -\left(\frac{q}{p}\right), & \text{kui } p \equiv q \equiv 3 \pmod 4;\\ \left(\frac{q}{p}\right), & \text{ülejäänud juhtudel.}\end{cases}$$

TÕESTUS. Olgu n selline naturaalarv, et $p^n \equiv 1 \pmod q$ (näiteks võib Fermat' väikse teoreemi tõttu võtta $n = q-1$). Vaatleme p^n-elemendilist korpust $\mathbb{F}_{p^n}$. Siis $q \mid p^n - 1$ ja teoreemi 10.19 põhjal leidub selles korpuses q-nda astme primitiivne ühejuur; tähistame ta tähega ξ. Siis muuhulgas $\xi^q = \mathbf{1}$, kus $\mathbf{1}$ on korpuse $\mathbb{F}_{p^n}$ ühikelement. Defineerime summa

$$G = \sum_{j=1}^{q-1} \left(\frac{j}{q}\right) \xi^j \in \mathbb{F}_{p^n}.$$

Näitame, et $G^2 = (-1)^{\frac{q-1}{2}} q\mathbf{1}$ (s.t. et G^2 on kas $q\mathbf{1}$ või $-q\mathbf{1}$, sõltuvalt sellest, kas $\frac{q-1}{2}$ on paaris või paaritu). Kasutades seda, et kui k omandab väärtused $1, 2, \ldots, q-1$, siis ka $q-k$ omandab samad väärtused, seda, et $\xi^{q-k} = \xi^{-k}$, ning lauset 8.8, saame, et

$$\begin{aligned}
G^2 = G \cdot G &= \left(\sum_{j=1}^{q-1} \left(\frac{j}{q}\right) \xi^j\right) \left(\sum_{k=1}^{q-1} \left(\frac{q-k}{q}\right) \xi^{q-k}\right) = \sum_{j=1}^{q-1} \left(\frac{j}{q}\right) \xi^j \left(\sum_{k=1}^{q-1} \left(\frac{-k}{q}\right) \xi^{-k}\right)\\
&= \left(\frac{-1}{q}\right) \sum_{j=1}^{q-1} \left(\frac{j}{q}\right) \xi^j \left(\sum_{k=1}^{q-1} \left(\frac{k}{q}\right) \xi^{-k}\right) = (-1)^{\frac{q-1}{2}} \sum_{j=1}^{q-1} \left(\frac{j}{q}\right) \xi^j \left(\sum_{k=1}^{q-1} \left(\frac{k}{q}\right) \xi^{-k}\right).
\end{aligned}$$

Kasutades järeldust 10.28 saame, et kui k omandab kõik väärtused $1, 2, \ldots, q-1$, siis iga fikseeritud $j \in \{1, \ldots, q-1\}$ korral ka jk omandab samad väärtused mooduli q järgi. Seega arvestades, et kui $jk = uq + v$, kus $0 < v < q$, siis $\left(\frac{v}{q}\right) \xi^{-v} = \left(\frac{uq+v}{q}\right) \xi^{-uq-v} = \left(\frac{jk}{q}\right) \xi^{-jk}$, saame, et

$$\begin{aligned}
G^2 &= (-1)^{\frac{q-1}{2}} \sum_{j=1}^{q-1} \left(\frac{j}{q}\right) \xi^j \left(\sum_{k=1}^{q-1} \left(\frac{jk}{q}\right) \xi^{-jk}\right) = (-1)^{\frac{q-1}{2}} \sum_{j=1}^{q-1} \sum_{k=1}^{q-1} \left(\frac{j^2k}{q}\right) \xi^{j(1-k)} = (-1)^{\frac{q-1}{2}} \sum_{k=1}^{q-1} \left(\frac{k}{q}\right) \left(\sum_{j=1}^{q-1} \xi^{j(1-k)}\right)\\
&= (-1)^{\frac{q-1}{2}} \left(\sum_{k=1}^{q-1} \left(\frac{k}{q}\right) \left(\sum_{j=0}^{q-1} \xi^{j(1-k)}\right) - \sum_{k=1}^{q-1} \left(\frac{k}{q}\right) \mathbf{1}\right) = (-1)^{\frac{q-1}{2}} \sum_{k=1}^{q-1} \left(\frac{k}{q}\right) \left(\sum_{j=0}^{q-1} \xi^{j(1-k)}\right),
\end{aligned}$$

sest mooduli q järgi on ruutjääke ja mitteruutjääke hulgas $\{1,\dots,q-1\}$ ühepalju ja seega $\sum_{k=1}^{q-1}\left(\frac{k}{q}\right)=0$. Siis

$$\left(\mathbf{1}-\xi^{1-k}\right)\sum_{j=0}^{q-1}\xi^{j(1-k)}=\sum_{j=0}^{q-1}\xi^{j(1-k)}-\sum_{j=0}^{q-1}\xi^{(j+1)(1-k)}=\sum_{j=0}^{q-1}\xi^{j(1-k)}-\sum_{j=1}^{q}\xi^{j(1-k)}=\xi^0-\xi^{q(1-k)}=\mathbf{1}-\mathbf{1}=\mathbf{0}.$$

Et $k\in\{2,\dots,q-1\}$ korral $\mathbf{1}-\xi^{1-k}\neq\mathbf{0}$ ja korpuses pole nullitegureid, siis iga $k=2,\dots,q-1$ korral peab $\sum_{j=0}^{q-1}\xi^{j(1-k)}=\mathbf{0}$. Järelikult

$$G^2=(-1)^{\frac{q-1}{2}}\left(\frac{1}{q}\right)\left(\sum_{j=0}^{q-1}\xi^0\right)=(-1)^{\frac{q-1}{2}}\left(\frac{1}{q}\right)q\mathbf{1}=(-1)^{\frac{q-1}{2}}q\mathbf{1}.$$

Kasutades saadud võrdust, Euleri kriteeriumi ja seda, et korpuse $\mathbb{F}_{p^n}$ karakteristika on p, saame, et

$$G^p=\left(G^2\right)^{\frac{p-1}{2}}G=\left((-1)^{\frac{q-1}{2}}q\mathbf{1}\right)^{\frac{p-1}{2}}G=(-1)^{\frac{q-1}{2}\cdot\frac{p-1}{2}}q^{\frac{p-1}{2}}\mathbf{1}\cdot G=(-1)^{\frac{(p-1)(q-1)}{4}}\left(\frac{q}{p}\right)G.$$

Teisest küljest, kasutades lemmat 10.7, seda, et p on paaritu, ning seda, et kui j omandab väärtused $1,2,\dots,q-1$, siis ka pj omandab need väärtused mooduli q järgi, saame, et

$$\begin{aligned}G^p&=\left(\sum_{j=1}^{q-1}\left(\frac{j}{q}\right)\xi^j\right)^p=\sum_{j=1}^{q-1}\left(\frac{j}{q}\right)^p\xi^{pj}=\sum_{j=1}^{q-1}\left(\frac{j}{q}\right)\xi^{pj}=\sum_{j=1}^{q-1}\left(\frac{p^2j}{q}\right)\xi^{pj}\\&=\sum_{j=1}^{q-1}\left(\frac{p}{q}\right)\left(\frac{pj}{q}\right)\xi^{pj}=\left(\frac{p}{q}\right)\sum_{j=1}^{q-1}\left(\frac{pj}{q}\right)\xi^{pj}=\left(\frac{p}{q}\right)\sum_{j=1}^{q-1}\left(\frac{j}{q}\right)\xi^{j}=\left(\frac{p}{q}\right)G.\end{aligned}$$

Seega oleme saanud, et

$$\left(\frac{p}{q}\right)G=(-1)^{\frac{(p-1)(q-1)}{4}}\left(\frac{q}{p}\right)G. \tag{35}$$

Kuna $G^2=q\mathbf{1}$ või $G^2=-(q\mathbf{1})$ ja korpuse $\mathbb{F}_{p^n}$ karakteristika $p\neq q$, siis $G\neq\mathbf{0}$. Korrutades võrduse (35) pooli elemendiga $G^{-1}\in\mathbb{F}_{p^n}$, saame, et

$$\left(\frac{p}{q}\right)\mathbf{1}=(-1)^{\frac{(p-1)(q-1)}{4}}\left(\frac{q}{p}\right)\mathbf{1}.$$

Et korpuse $\mathbb{F}_{p^n}$ karakteristika p on suurem kui 2, siis saame sellest võrdusest, et

$$\left(\frac{p}{q}\right)=(-1)^{\frac{(p-1)(q-1)}{4}}\left(\frac{q}{p}\right).$$

□

11. Arvuvallad*

Selles peatükis uurime, kuidas saab naturaalarvudest lähtudes loomulikul viisil konstrueerida täisarvud, täisarvudest lähtudes ratsionaalarvud, ning veendume, et ratsionaalarvude üldistusena võib lisaks reaalarvudele vaadelda ka veel hoopis teistsuguseid arvuhulki.

11.1. Naturaalarvudelt täisarvudele

Naturaalarvude hulk $\mathbb{N}$ on kinnine liitmise suhtes, kuid kahe naturaalarvu vahe ei pruugi olla naturaalarv. Vähim hulk, mis sisaldab $\mathbb{N}$ ja on kinnine lahutamise suhtes, on täisarvude hulk $\mathbb{Z}$. Iga täisarvu võib esitada (kuigi mitte üheselt) kahe naturaalarvu vahena. Järgnevas näitame, kuidas kasutades algebralisi konstruktsioone saab lähtudes kommutatiivsest taandamisega (s.t. võrdusest $x+y = x+z$, $x, y, z \in \mathbb{N}$, järeldub võrdus $y = z$) poolrühmast $(\mathbb{N}, +)$ konstrueerida rühma $(\mathbb{Z}, +)$, kusjuures $\mathbb{N} \subset \mathbb{Z}$.

Teoreem 11.1. *Poolrühma $(\mathbb{N}, +)$ saab sisestada rühma.*

Tõestus. Defineerime hulga $\mathbb{N}$ otseruudul $\mathbb{N}^2 = \mathbb{N} \times \mathbb{N}$ binaarse seose $\sim$ järgmiselt:

$$(x, y) \sim (u, v) \Longleftrightarrow x + v = y + u,$$

mistahes $(x, y), (u, v) \in \mathbb{N}^2$ korral. Näitame, et $\sim$ on ekvivalentsusseos.
Refleksiivsus. Et $x + y = y + x$, siis $(x, y) \sim (x, y)$.
Sümmeetrilisus. Kui $(x, y) \sim (u, v)$, siis $x + v = y + u$, järelikult $u + y = v + x$, s.t. $(u, v) \sim (x, y)$.
Transitiivsus. Olgu $(x, y) \sim (u, v)$ ja $(u, v) \sim (w, z)$. Siis $x + v = y + u$ ja $u + z = v + w$. Nendest võrdustest järeldub, et $x + v + z = y + u + z = y + v + w$. Taandades v saame, et $x + z = y + w$ ehk $(x, y) \sim (w, z)$.

Tähistame faktorhulga seose $\sim$ järgi

$$\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/\sim = \{[(x, y)] \mid x, y \in \mathbb{N}\},$$

kus $[(x, y)]$ tähistab paari $(x, y) \in \mathbb{N} \times \mathbb{N}$ ekvivalentsiklassi seose $\sim$ järgi. Näitame, et $\mathbb{Z}$ osutub rühmaks, kui defineerida hulgal $\mathbb{Z}$ liitmistehe $\oplus$ reegliga

$$[(x, y)] \oplus [(u, v)] = [(x + u, y + v)].$$

Kontrollime, kas see definitsioon on korrektne. Selleks oletame, et $(x, y) \sim (x', y')$ ja $(u, v) \sim (u', v')$, s.t. $x + y' = y + x'$ ja $u + v' = v + u'$. Liites nende võrduste vastavad pooled ja kasutades naturaalarvude liitmise kommutatiivsust saame võrduse $x + u + y' + v' = y + v + x' + u'$, s.t. $(x + u, y + v) \sim (x' + u', y' + v')$. Seega tõesti liitmise tulemus ei sõltu liidetavate ekvivalentsiklasside esindajate valikust.

Kuna

$$[(x, y)] \oplus [(u, v)] = [(x + u, y + v)] = [(u + x, v + y)] = [(u, v)] \oplus [(x, y)],$$

siis liitmistehe $\oplus$ on kommutatiivne. Analoogiliselt järeldub naturaalarvude liitmise assotsiatiivsusest see, et ka tehe $\oplus$ on assotsiatiivne hulgal $\mathbb{Z}$. Nullelemendiks tehte $\oplus$ suhtes on klass $[(1, 1)]$. Tõepoolest, iga $(x, y) \in \mathbb{N}^2$ korral $[(1, 1)] \oplus [(x, y)] = [(1 + x, 1 + y)] = [(x, y)]$, sest $1 + x + y = 1 + y + x$. Elemendi $[(x, y)] \in \mathbb{Z}$ vastandelemendiks on $[(y, x)]$, sest $[(x, y)] \oplus [(y, x)] = [(x + y, y + x)] = [(1, 1)]$, kuna $x + y + 1 = y + x + 1$. Seega $\mathbb{Z}$ on tõesti rühm.

Näitame, et poolrühm $(\mathbb{N}, +)$ on isomorfne rühma $(\mathbb{Z}, \oplus)$ mingi alampoolrühmaga. Vaatleme hulka

$$\mathbb{N}' = \{[(x + 1, 1)] \mid x \in \mathbb{N}\} \subseteq \mathbb{Z}.$$

Kuna iga $x, x' \in \mathbb{N}$ korral

$$[(x + 1, 1)] \oplus [(x' + 1, 1)] = [(x + 1 + x' + 1, 1 + 1)] = [(x + x' + 1, 1)] \in \mathbb{N}',$$

siis $\mathbb{N}'$ on rühma $\mathbb{Z}$ alampoolrühm.

Defineerime kujutuse $\varphi : \mathbb{N} \longrightarrow \mathbb{N}'$ järgmiselt: iga $x \in \mathbb{N}$ korral

$$\varphi(x) = [(x + 1, 1)].$$

On selge, et φ on pealekujutus. Näitame, et φ on üksühene. Selleks oletame, et $\varphi(x) = \varphi(x')$ ehk $(x + 1, 1) \sim (x' + 1, 1)$. Siis $x + 1 + 1 = 1 + x' + 1$. Taandades 2 saame võrduse $x = x'$. Seega φ on üksühene. Kuna

$$\begin{aligned}\varphi(x + x') &= [(x + x' + 1, 1)] = [(x + x' + 1 + 1, 1 + 1)] \\ &= [(x + 1, 1)] \oplus [(x' + 1, 1)] = \varphi(x) \oplus \varphi(x'),\end{aligned}$$

siis φ on poolrühmade homomorfism.

Seega φ on bijektiivne homomorfism ehk isomorfism ja $\mathbb{N} \cong \mathbb{N}' = \varphi(\mathbb{N}) \subseteq \mathbb{Z}$, kus $\mathbb{N}'$ on rühma $\mathbb{Z}$ alampoolrühm. □

Hulga $\mathbb{Z}$ elemente nimetame *täisarvudeks*. Edaspidises samastame elemendi $[(x+1,1)] \in \mathbb{N}'$ naturaalarvuga x ja kirjutame tehtemärgi $\oplus$ asemel lihtsalt $+$. Nagu igas rühmas, on ka rühma $(\mathbb{Z},+)$ nullelement ning elemendi $[(x,y)]$ vastandelement üheselt määratud ning me tähistame neid vastavalt sümboliga 0 ja $-[(x,y)]$. Tähistades $-\mathbb{N} = \{-[(x+1,1)] \mid x \in \mathbb{N}\} = \{-x \mid x \in \mathbb{N}\}$ võime kirjutada $\mathbb{Z} = -\mathbb{N} \cup \{0\} \cup \mathbb{N}$. Tõepoolest, sõltuvalt sellest, kas $x > y$, $x = y$ või $x < y$ kuulub element $[(x,y)]$ kas hulka $\mathbb{N}$, $\{0\}$ või $-\mathbb{N}$.

Märkus 11.2. Samasuguse konstruktsiooni nagu teoreemis 11.1 saab läbi teha suvalise kommutatiivse taandamisega poolrühma $(S,+)$ korral. Tekkivat rühma nimetatakse poolrühma $(S,+)$ *vahede rühmaks*. Seega $(\mathbb{Z},+)$ on poolrühma $(\mathbb{N},+)$ vahede rühm.

Nägime, et poolrühma $(\mathbb{N},+)$ saab sisestada rühma $(\mathbb{Z},+)$. Kuid äkki on rühmal $\mathbb{Z}$ mõni pärisalamrühm, mis samuti sisaldab poolrühma $(\mathbb{N},+)$ alampoolrühmana? Järgmine lause ütleb, et rühm $\mathbb{Z}$ siiski ei sisalda liigseid elemente.

Lause 11.3. *Rühma $(\mathbb{Z},+)$ vähim alamrühm, mis sisaldab poolrühma $\mathbb{N}$ alampoolrühmana, on $\mathbb{Z}$ ise.*

Tõestus. Olgu $\mathbb{Z}'$ rühma $(\mathbb{Z},+)$ vähim alamrühm, mis sisaldab poolrühma $\mathbb{N}' \cong \mathbb{N}$ alampoolrühmana. Olgu $[(u,v)] \in \mathbb{Z}$ suvaline element. Kuna $\mathbb{N}' \subseteq \mathbb{Z}'$, siis $[(u+1,1)], [(v+1,1)] \in \mathbb{Z}'$. Et $\mathbb{Z}'$ on alamrühm, siis on ta kinnine vastandelemendi võtmise ja liitmise suhtes, järelikult $[(1,v+1)] \in \mathbb{Z}'$ ning

$$[(u,v)] = [(u+1+1, 1+v+1)] = [(u+1,1)] + [(1,v+1)] \in \mathbb{Z}'.$$

Seega $\mathbb{Z} = \mathbb{Z}'$. □

Tekib veel küsimus, kas lisaks rühmale $(\mathbb{Z},+)$ on veel teisi rühmi, mis sisaldavad poolrühma $(\mathbb{N},+)$ alampoolrühmana ja millel pole sama omadusega pärisalampoolrühmi. Osutub, et nii see siiski pole.

Lause 11.4. *Iga kommutatiivne rühm H, mis sisaldab poolrühma $(\mathbb{N},+)$ alampoolrühmana ja mille vähim poolrühma $\mathbb{N}$ alampoolrühmana sisaldav alamrühm on see rühm H ise, on isomorfne rühmaga $(\mathbb{Z},+)$.*

Tõestus. Vaatleme sellist rühma $(H,+)$ ja tema alamhulka

$$H' = \{x - y \mid x, y \in \mathbb{N}\} \subseteq H,$$

kus vahe $x-y$ defineeritakse võrdusega $x-y = x+(-y)$. Kuna mistahes $x-y, x'-y' \in H'$ korral $(x-y)+(x'-y') = (x+x') - (y+y') \in H'$ ja $-(x-y) = y - x \in H'$, siis H' on rühma H alamrühm. Et mistahes $x \in \mathbb{N}$ korral $x = (x+x) - x$, siis $\mathbb{N} \subseteq H'$ ja et $\mathbb{N}$ on rühma H alampoolrühm, siis on ta ka rühma H' alampoolrühm. Kuna rühma H vähim poolrühma $\mathbb{N}$ alampoolrühmana sisaldav alamrühm on H ise, siis $H' = H$.

Defineerime kujutuse $\varphi : H \longrightarrow \mathbb{Z}$ eeskirjaga

$$\varphi(x-y) = [(x,y)],$$

$x, y \in \mathbb{N}$. Kuna mistahes $x, y, x', y' \in \mathbb{N}$ korral

$$x - y = x' - y' \Longleftrightarrow x + y' = y + x' \Longleftrightarrow (x,y) \sim (x',y') \Longleftrightarrow [(x,y)] = [(x',y')],$$

siis φ on korrektselt defineeritud ja injektiivne. On selge, et φ on sürjektiivne. Lõpuks, kuna mistahes $x, y, u, v \in \mathbb{N}$ korral

$$\varphi((x-y)+(u-v)) = \varphi((x+u)-(y+v)) = [(x+u, y+v)] = [(x,y)] + [(u,v)] = \varphi(x-y) + \varphi(u-v),$$

siis φ on rühmade homomorfism. Seega φ on isomorfism ning rühmad $(\mathbb{Z},+)$ ja $(H,+)$ on isomorfsed. □

Arvestades lauseid 11.3 ja 11.4 võime väita, et täisarvude rühm $(\mathbb{Z},+)$ on vähim poolrühma $(\mathbb{N},+)$ alampoolrühmana sisaldav $\mathbb{Z}$ alamrühm ja ta on isomorfismi täpsuseni üheselt määratud.

11.2. Täisarvudelt ratsionaalarvudele

Täisarvude hulk $\mathbb{Z}$ on kinnine liitmise, lahutamise ja korrutamise suhtes, kuid kahe täisarvu jagatis ei pruugi olla täisarv. Vähim hulk, mis sisaldab $\mathbb{Z}$ ja on kinnine nullist erinevate elementidega jagamise suhtes, on ratsionaalarvude hulk $\mathbb{Q}$. Täpsemalt öeldes, lähtudes ringist $\mathbb{Z}$ saab konstrueerida korpuse $\mathbb{Q}$, mis sisaldab ringi $\mathbb{Z}$ alamringina. Selleks defineeritakse hulgal $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ ekvivalentsiseos $\sim$ nii, et

$$(a, b) \sim (c, d) \iff ad = bc,$$

tähistatakse

$$\mathbb{Q} = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) / \sim$$

ja $\frac{a}{b} = [(a, b)]$ ning defineeritakse hulgal $\mathbb{Q}$ liitmis- ja korrutamistehe sobival viisil. Jällegi osutub, et analoogilise konstruktsiooni saab läbi viia üldisemal juhul.

Teoreem 11.5. *Iga kommutatiivse nullitegureita ringi R saab sisestada mingisse korpusse K.*

Selle teoreemi tõestuse võib leida raamatust [1] (paragrahv 6.14). Sellist korpust K nimetatakse ringi R *jagatiste korpuseks*. Lihtne on veenduda, et konstrueerides ringi $\mathbb{Z}$ jagatiste korpuse saame korpuse, mis on isomorfne ratsionaalarvude korpusega $\mathbb{Q}$.

11.3. Ratsionaalarvudelt reaalarvudele

Definitsioon 11.6. Nelikut $(K, +, \cdot, \leqslant)$, kus K on mittetühi hulk, $+$ ja $\cdot$ on kahekohalised algebralised tehted hulgal K ja $\leqslant$ on binaarne seos hulgal K nimetatakse *reaalarvude hulgaks*, kui

R1. $(K, +, \cdot)$ on kommutatiivne korpus;

R2. $\leqslant$ on lineaarne järjestusseos hulgal K (s.t. selline järjestusseos, et iga $\alpha, \beta \in K$ korral kas $\alpha \leqslant \beta$ või $\beta \leqslant \alpha$) ning iga $\alpha, \beta, \gamma, \delta \in K, \delta \geqslant \mathbf{0}$, korral

$$\alpha \leqslant \beta \Longrightarrow \alpha + \gamma \leqslant \beta + \gamma \ \text{ ja } \ \alpha\delta \leqslant \beta\delta;$$

R3. (täielikkuse aksioom) hulga K igal mittetühjal alt tõkestatud alamhulgal on olemas alumine raja hulgas K.

11.3.1. Weierstrassi meetod

Weierstrassi teooria järgi on *reaalarv* lõpmatu kümnendmurd pluss- või miinusmärgiga:

$$\pm a_0, a_1 a_2 \dots a_n \dots,$$

kus a_0 on mittenegatiivne täisarv ja iga $a_n, n \in \mathbb{N}$, on üks numbreist $0, 1, \dots, 9$. Seejuures lõpmatu kümnendmurd perioodiga 9, s.o. kümnendmurd $a_0, a_1 a_2 \dots a_n(9)$, kus $a_n \neq 9$, loetakse võrdseks lõpmatu kümnendmurruga $a_0, a_1 a_2 \dots a_{n-1}(a_n + 1)000 \dots$ (juhul $n = 0$ kümnendmurruga $(a_0 + 1), 000 \dots$). Arve $\underline{\alpha_n} = a_0, a_1 a_2 \dots a_n$ ja $\overline{\alpha_n} = a_0, a_1 a_2 \dots a_n + 10^{-n}$ nimetatakse vastavalt reaalarvu $\alpha = a_0, a_1 a_2 \dots a_n \dots$ *alumiseks* ja *ülemiseks* n-ndat *järku kümnendlähendiks*. Kui reaalarvu α märk on pluss (miinus) ja täisarvude $a_n, n \in \mathbb{N} \cup \{0\}$, seas on vähemalt üks nullist erinev, siis öeldakse, et α on *positiivne* (*negatiivne*). Arvu $\alpha = \pm a_0, a_1 a_2 \dots a_n \dots$ *absoluutväärtuseks* nimetatakse arvu $a_0, a_1 a_2 \dots a_n \dots$ ning seda tähistatakse $|\alpha|$.

Olgu $\alpha = a_0, a_1 a_2 \dots a_n \dots$ ja $\beta = b_0, b_1 b_2 \dots b_n \dots$. Loeme, et $\alpha < \beta$, kui kas $a_0 < b_0$ või leidub selline $N \in \mathbb{N} \cup \{0\}$, et $a_k = b_k$ iga $k \in \{0, 1, \dots, N\}$ korral, kuid $a_{N+1} < b_{N+1}$. Lisaks sellele loeme, et iga negatiivne arv ja 0 on väiksem igast positiivsest arvust ning kui α ja β on negatiivsed ja $|\beta| < |\alpha|$, siis $\alpha < \beta$. Lugedes $\alpha \leqslant \beta$ kui $\alpha = \beta$ või $\alpha < \beta$ saame lineaarse järjestusseose $\leqslant$.

Öeldakse, et täisarvude jada $(x_k)_{k \in \mathbb{N}}$ *stabiliseerub* arvuks m, kui leidub selline indeks N, et iga $k \geqslant N$ korral $x_k = m$. Öeldakse, et lõpmatute kümnendmurdude jada $(\alpha^k)_{k \in \mathbb{N}} = (a_0^k, a_1^k a_2^k \dots a_n^k \dots)_{k \in \mathbb{N}}$ *stabiliseerub* arvuks $\alpha = a_0, a_1 a_2 \dots a_n \dots$, kui lõpmatu maatriksi $(a_i^{(k)})$ (i on siin veerunumber, k reanumber) i-s veerg stabiliseerub arvuks a_i iga $i \in \mathbb{N} \cup \{0\}$ korral. Kui $\alpha > 0$ ja $\beta > 0$, siis kümnendmurdudest $\underline{a_k} + \underline{b_k}, \underline{a_k} - \underline{b_k}, (\underline{a_k} \underline{b_k})_k$ ja $\left(\frac{a_k}{\underline{b_k}}\right)_k$ moodustatud jadad stabiliseeruvad arvudeks, mida nimetatakse vastavalt reaalarvude α ja β *summaks* $\alpha + \beta$, *vaheks* $\alpha - \beta$, *korrutiseks* $\alpha\beta$ ning *jagatiseks* $\frac{\alpha}{\beta}$. Neid definitsioone saab laiendada ka suvalise märgiga reaalarvude jaoks. Näiteks, kui $\alpha \leqslant 0$ ja $\beta \leqslant 0$, siis $\alpha + \beta = -(|\alpha| + |\beta|)$, kui α ja β on erinevate märkidega, siis $\alpha + \beta = \pm\Big||\alpha| - |\beta|\Big|$, kus märgiks võetakse liidetavaist absoluutväärtuselt suurema märk. Mistahes α, β korral loetakse $\alpha - \beta = \alpha + (-\beta)$ jne. Saab näidata, et lõpmatute kümnendmurdude hulk koos sellel defineeritud tehetega $+$ ja $\cdot$ ning järjestusega $\leqslant$ rahuldab aksioome R1–R3.

11.3.2. Dedekindi meetod

Definitsioon 11.7. *Dedekindi lõige* on järjestatud paar (α, β), mis koosneb kahest hulgast, $\alpha \subset \mathbb{Q}$ ("vasakpoolne" ehk "alumine" hulk) ja $\beta \subset \mathbb{Q}$ ("parempoolne" ehk "ülemine" hulk), mis rahuldavad järgmisi tingimusi:

D1. iga ratsionaalarv kuulub ühte hulkadest α ja β;

D2. $\alpha \neq \emptyset$ ja $\beta \neq \emptyset$;

D3. α iga element on väiksem β igast elemendist;

D4. hulgas β pole vähimat elementi.

Kumbki hulkadest α ja β määrab üheselt ära teise ja sellega ka kogu lõike. Seega edaspidises võime Dedekindi lõike samastada tema parempoolse hulgaga β, millel on järgmised omadused:

D1′. $\beta \neq \emptyset$ ja tema täiend $\overline{\beta} = \mathbb{Q} \setminus \beta \neq \emptyset$;

D2′. kui $b \in \beta, b' \in \mathbb{Q}$ ja $b < b'$, siis $b' \in \beta$;

D3′. hulgas β pole vähimat elementi.

Edasises tähistame kreeka tähtedega $\alpha, \beta, \ldots$ parempoolseid hulki ja nimetame Dedekindi lõikeid *reaalarvudeks*. Kõigi Dedekindi lõigete hulga tähistame sümboliga $\mathbb{R}$.

Iga ratsionaalarv a määrab ära lõike $\underline{a} = \{b \in \mathbb{Q} \mid a < b\}$, mida nimetame *ratsionaalseks*. Lõige α on ratsionaalne siis ja ainult siis, kui hulga α täiendil $\overline{\alpha}$ on olemas suurim element. Hulga $\mathbb{Q}$ saab sisestada hulka $\mathbb{R}$ kujutuse $f : \mathbb{Q} \longrightarrow \mathbb{R}$, $f(a) = \underline{a}$, abil. Mitte kõik lõiked ei ole ratsionaalsed. Näiteks saab näidata, et $\sqrt{2}$, ehk täpsemalt öeldes lõige $\alpha = \left\{a \in \mathbb{Q} \mid a > 0, a^2 > 2\right\}$, ei ole ratsionaalne.

Lõigete (parempoolsete hulkade) järjestuse defineerime järgmiselt:

$$\alpha \leqslant \beta \Longleftrightarrow \beta \subseteq \alpha.$$

Lihtne on veenduda, et $\leqslant$ on osalise järjestuse seos hulgal $\mathbb{R}$. Veelgi enam, see seos on ka lineaarne järjestusseos ja rahuldab aksioomi R3.

Mistahes kahe lõike $\alpha, \beta \in \mathbb{R}$ summa defineerime võrdusega

$$\alpha + \beta = \{a + b \mid a \in \alpha, b \in \beta\}.$$

Sellise liitmise suhtes osutub nullelemendiks ratsionaalne lõige $\underline{0} = \{b \in \mathbb{Q} \mid 0 < b\}$. Lõike $\alpha \in \mathbb{R}$ vastandelement defineeritakse võrdusega

$$-\alpha = \{-a \mid a \in \overline{\alpha},\ \ a \text{ ei ole } \overline{\alpha} \text{ suurim element}\}$$

ja lõigete $\alpha, \beta \in \mathbb{R}$ vahe võrdusega $\alpha - \beta = \alpha + (-\beta)$. Kui $\alpha, \beta \geqslant \underline{0}$, siis defineerime nende lõigete korrutise võrdusega

$$\alpha \cdot \beta = \{ab \mid a \in \alpha, b \in \beta\}.$$

Mistahes lõike γ saab esitada kahe mittenegatiivse lõike $\alpha \geqslant \underline{0}$ ja $\beta \geqslant \underline{0}$ vahena: $\gamma = \alpha - \beta$. Lõigete $\gamma = \alpha - \beta$ ja $\gamma' = \alpha' - \beta'$, kus ka $\alpha', \beta' \geqslant \underline{0}$, korrutise defineerime võrdusega

$$\gamma \cdot \gamma' = (\alpha - \beta) \cdot (\alpha' - \beta') = \alpha \cdot \alpha' + \beta \cdot \beta' - \alpha \cdot \beta' - \beta \cdot \alpha'.$$

Sellise korrutamise suhtes osutub ühikelemendiks lõige $\underline{1}$. Lõike $\alpha > \underline{0}$ pöördelemendi defineerime võrdusega

$$\alpha^{-1} = \{a^{-1} \mid a \in \overline{\alpha}, a > 0,\ \ a \text{ ei ole } \overline{\alpha} \text{ suurim element}\}$$

ja lõike $\alpha < \underline{0}$ pöördelemendi võrdusega $\alpha^{-1} = -(-\alpha^{-1})$. Saab näidata, et defineeritud tehete suhtes osutub hulk $\mathbb{R}$ korpuseks ja et järjestus $\leqslant$ on kooskõlas liitmise ja korrutamisega.

11.3.3. Cantori meetod

Definitsioon 11.8. Ratsionaalarvujada (a_i) nimetatakse *fundamentaaljadaks* ehk *Cauchy jadaks*, kui iga ratsionaalarvu $\varepsilon > 0$ korral leidub selline indeks N, et iga $i, j \geqslant N$ korral $|a_i - a_j| < \varepsilon$.

Öeldakse, et ratsionaalarvujada (a_i) on *ratsionaalselt koonduv*, kui leidub selline ratsionaalarv a, et iga ratsionaalarvu $\varepsilon > 0$ korral leidub selline indeks N, et iga $i \geqslant N$ korral $|a_i - a| < \varepsilon$. Sellisel juhul on a üheselt määratud ja kirjutatakse $a = \lim a_i$.

Iga ratsionaalselt koonduv jada on Cauchy jada. Samas leidub Cauchy jadasid, mis ei koondu ratsionaalselt, näiteks $\sqrt{2}$ lähismurdude jada $a_0 = 1$; $a_1 = 1,4$; $a_2 = 1,41$; $a_3 = 1,414$; $a_4 = 1,4142$; ....

Definitsioon 11.9. Ratsionaalselt nulliks koonduvat jada, s.t. sellist jada (a_i), et iga $\varepsilon > 0$ korral leidub N nii, et iga $i \geqslant N$ korral $|a_i| < \varepsilon$, nimetatakse *nulljadaks*.

Olgu $F(\mathbb{Q})$ kõigi ratsionaalarvuliste Cauchy jadade hulk. Defineerime hulgal $F(\mathbb{Q})$ seose $\sim$ järgmiselt:

$$(a_i) \sim (b_i) \Longleftrightarrow (a_i - b_i) \text{ on nulljada.}$$

Saab näidata, et $\sim$ on ekvivalentsusseos. Tähistame faktorhulga selle seose järgi

$$\mathbb{R} = F(\mathbb{Q})/\sim = \{[(a_i)] \mid (a_i) \in F(\mathbb{Q})\},$$

kus $[(a_i)]$ on jada (a_i) ekvivalentsiklass seose $\sim$ järgi. Hulga $\mathbb{R}$ elemente nimetame *reaalarvudeks*. Defineerime sellel hulgal liitmise ja korrutamise võrdustega

$$[(a_i)] + [(b_i)] = [(a_i + b_i)], \tag{36}$$
$$[(a_i)] \cdot [(b_i)] = [(a_i \cdot b_i)]. \tag{37}$$

Saab näidata, et Cauchy jadade summa ja korrutis on ka Cauchy jadad ning et $(F(\mathbb{Q})/\sim, +, \cdot)$ on korpus. Nullelemendiks selles korpuses on ekvivalentsiklass, mis koosneb kõigist nulljadadest.

Ratsionaalarvude korpuse $\mathbb{Q}$ saab sisestada alamkorpusena korpusse $F(\mathbb{Q})/\sim$ kujutuse $f : \mathbb{Q} \longrightarrow F(\mathbb{Q})/\sim$, $f(a) = [(a, a, a, \ldots)]$ abil.

Ratsionaalsete elementidega Cauchy jada nimetatakse *positiivseks* (*negatiivseks*), kui leidub selline ratsionaalarv $\varepsilon > 0\,(\varepsilon < 0)$, et alates mingist kohast on kõik selle jada elemendid suuremad (väiksemad) kui ε. Iga ratsionaalsete elementidega Cauchy jada on kas positiivne, negatiivne või nulljada. Kui jada on positiivne (negatiivne), siis ka mistahes temaga ekvivalentne jada on positiivne (negatiivne). Reaalarvu $[(a_i)]$ nimetame *positiivseks* (*negatiivseks*) kui jada (a_i) on positiivne (negatiivne). Iga reaalarv on kas positiivne, negatiivne või null. Defineerime hulgal $F(\mathbb{Q})/\sim$ seose $\leqslant$ järgmiselt:

$$\alpha \leqslant \beta \Longleftrightarrow \alpha = \beta \text{ või } \beta - \alpha \text{ on positiivne.}$$

Seos $\leqslant$ osutub lineaarseks järjestusseoseks ning saab näidata, et kehtivad aksioomid R2 ja R3.

Osutub, et aksioomid R1–R3 kirjeldavad üheselt ära reaalarvude hulga.

Teoreem 11.10 ([9], lk. 50–51). *Iga järjestatud korpus K, mis rahuldab aksioome R1–R3, on isomorfne korpusega $F(\mathbb{Q})/\sim$.*

11.3.4. p-aadilised arvud

Definitsioon 11.11. *Norm* korpusel $(K, +, \cdot)$ on kujutus $\| \ \|$, mis igale elemendile $x \in K$ säeb vastavusse mittenegatiivse reaalarvu $\|x\|$ nii, et

N1. $\|x\| = 0$ siis ja ainult siis, kui $x = 0$;

N2. $\|xy\| = \|x\| \, \|y\|$;

N3. $\|x + y\| \leqslant \|x\| + \|y\|$.

Näiteks on normiks ratsionaalarvude korpusel absoluutväärtus. Osutub, et ratsionaalarvude korpusel saab defineerida ka teisi põnevaid norme.

Olgu p algarv. Iga täisarvu $a \neq 0$ korral olgu $\operatorname{ord}_p a$ algarvu p kõrgeim aste, mis jagab arvu a. Näiteks $\operatorname{ord}_5 35 = 1$, $\operatorname{ord}_5(-250) = 3$, $\operatorname{ord}_2 96 = 5$, $\operatorname{ord}_2 97 = 0$. Loeme, et $\operatorname{ord}_p 0 = \infty$. Paneme tähele, et $\operatorname{ord}_p(a_1 a_2) = \operatorname{ord}_p a_1 + \operatorname{ord}_p a_2$. Mistahes ratsionaalarvu $x = \frac{a}{b}$ jaoks, kus $a, b \in \mathbb{Z}$, $b \neq 0$, defineerime

$$\operatorname{ord}_p x = \operatorname{ord}_p a - \operatorname{ord}_p b.$$

Kui $\frac{a}{b} = \frac{c}{d}$ ehk $ad = bc$, $a, b, c, d \in \mathbb{Z}$, $b, d \neq 0$, siis $\operatorname{ord}_p a + \operatorname{ord}_p d = \operatorname{ord}_p b + \operatorname{ord}_p c$ ja seega $\operatorname{ord}_p a - \operatorname{ord}_p b = \operatorname{ord}_p c - \operatorname{ord}_p d$, mis tähendab, et antud definitsioon ei sõltu sellest, milliste täisarvude jagatisena ratsionaalarv x on esitatud.

Defineerime kujutuse $|\ |_p : \mathbb{Q} \longrightarrow \mathbb{Q}$ järgmiselt:

$$|x|_p = \begin{cases} \frac{1}{p^{\operatorname{ord}_p x}}, & \text{kui } x \neq 0; \\ 0, & \text{kui } x = 0. \end{cases}$$

Ehk teisiti: kui esitame ratsionaalarvu $x \neq 0$ kujul $x = p^m \frac{a}{b}$, kus $m \in \mathbb{Z}$ ja $(ab, p) = 1$, s.t. $m = \operatorname{ord}_p x$, siis $|x|_p = p^{-m} = p^{-\operatorname{ord}_p x}$.

Lause 11.12. *Kujutus* $|\ |_p$ *on norm korpusel* $\mathbb{Q}$.

Tõestus. Omaduste N1 ja N2 kontroll on lihtne. Näitame, et kehtib tingimus N3. Kui $x = 0$ või $y = 0$ või $x + y = 0$, siis on tõestus triviaalne. Seega võime eeldada, et x, y ja $x + y$ on nullist erinevad. Olgu $x = \frac{a}{b}$ ja $y = \frac{c}{d}$. Siis $x + y = \frac{ad+bc}{bd}$ ja $\operatorname{ord}_p(x+y) = \operatorname{ord}_p(ad+bc) - \operatorname{ord}_p b - \operatorname{ord}_p d$. Algarvu p kõrgeim aste, mis jagab kahe täisarvu summat ei ole väiksem kui vähim algarvu p kõrgemaist astmeist, mis jagavad liidetavaid. Seega

$$\begin{aligned} \operatorname{ord}_p(x+y) &= \operatorname{ord}_p(ad+bc) - \operatorname{ord}_p(b) - \operatorname{ord}_p(d) \geqslant \min(\operatorname{ord}_p ad, \operatorname{ord}_p bc) - \operatorname{ord}_p b - \operatorname{ord}_p d \\ &= \min(\operatorname{ord}_p a + \operatorname{ord}_p d, \operatorname{ord}_p b + \operatorname{ord}_p c) - \operatorname{ord}_p b - \operatorname{ord}_p d \\ &= \min(\operatorname{ord}_p a - \operatorname{ord}_p b, \operatorname{ord}_p c - \operatorname{ord}_p d) = \min(\operatorname{ord}_p x, \operatorname{ord}_p y). \end{aligned}$$

Järelikult

$$|x+y|_p = p^{-\operatorname{ord}_p(x+y)} \leqslant \max(p^{-\operatorname{ord}_p x}, p^{-\operatorname{ord}_p y}) = \max(|x|_p, |y|_p)$$

ning viimane on $\leqslant |x|_p + |y|_p$. □

Definitsioon 11.13. Normi $|\ |_p$ nimetatakse *p-aadiliseks normiks.*

Tegelikult tõestasime me tugevama võrratuse, kui oli nõutud normi definitsiooni tingimuses N3. See võrratus võetakse järgmise definitsiooni aluseks.

Definitsioon 11.14. Normi $\|\ \|$ korpusel K nimetatakse *mittearhimeediliseks*, kui iga $x, y \in K$ korral

$$\|x+y\| \leqslant \max(\|x\|, \|y\|). \tag{38}$$

Normi, mis ei ole mittearhimeediline, nimetatakse *arhimeediliseks.*

Seega p-aadiline norm $|\ |_p$ on mittearhimeediline ja absoluutväärtus $|\ |$ on arhimeediline norm korpusel $\mathbb{Q}$.

Asendades definitsioonides 11.8 ja 11.9 absoluutväärtuse normiga $|\ |_p$, saab defineerida Cauchy jadad, koonduvuse ja nulljadad normi $|\ |_p$ suhtes.

Normil $|\ |_p$ on mitmeid huvitavaid omadusi. Näiteks jada $1, p, p^2, p^3, \ldots$ koondub nulliks selle normi järgi. Tõepoolest, iga $\varepsilon > 0$ korral leidub selline N, et iga $i > N$ korral $\left|p^i\right|_p = \frac{1}{p^i} < \varepsilon$. Või siis näiteks kui vaatleme kera keskpunktiga $a \in \mathbb{Q}$ ja raadiusega $r \in \mathbb{Q}^+$, $D(a,r) = \left\{x \in \mathbb{Q} \mid |x-a|_p \leqslant r\right\}$, siis osutub, et mistahes $b \in D(a,r)$ korral $D(a,r) = D(b,r)$, s.t. selle kera iga punkt on keskpunkt! Tõepoolest, kui $x \in D(a,r)$, s.t. $|x-a|_p \leqslant r$, siis

$$|x-b|_p = |(x-a)+(a-b)|_p \leqslant \max(|x-a|_p, |a-b|_p) \leqslant r,$$

järelikult $x \in D(b,r)$. Vastupidise sisalduvuse saab tõestada analoogiliselt.

Norme $\|\ \|$ ja $\|\ \|'$ nimetatakse *ekvivalentseteks*, kui jada on Cauchy jada normi $\|\ \|$ suhtes parajasti siis, kui ta on Cauchy jada normi $\|\ \|'$ suhtes.

Näiteks, kui normi $|\ |_p$ definitsioonis kirjutada $\left(\frac{1}{p}\right)^{\mathrm{ord}_p\, x}$ asemel $\alpha^{\mathrm{ord}_p\, x}$, kus $0 < \alpha < 1$, siis saaksime normi, mis on ekvivalentne normiga $|\ |_p$. Samuti normid $|\ |^\alpha$, $0 < \alpha < 1$, on ekvivalentsed absoluutväärtusega.

Triviaalse normi all korpusel K peame silmas sellist normi $\|\ \|$, mille korral $\|0\| = 0$ ning iga $x \neq 0$ korral $\|x\| = 1$.

Kehtib järgmine teoreem ([10], lk. 3–5).

Teoreem 11.15 (Ostrowski). *Iga mittetriviaalne norm korpusel $\mathbb{Q}$ on ekvivalentne kas absoluutväärtusega või mingi p-aadilise normiga $|\ |_p$, kus p on algarv.*

Edasises olgu p fikseeritud algarv. Teeme läbi samasuguse konstruktsiooni nagu Cantori meetodi korral, ainult selle vahega, et absoluutväärtuse asemel kasutame p-aadilist normi.

Olgu $F_p(\mathbb{Q})$ kõigi selliste ratsionaalarvujadade (a_i) hulk, et iga $\varepsilon > 0$ korral leidub selline $N \in \mathbb{N}$, et $|a_i - a_j|_p < \varepsilon$, kui $i, j > N$ (s.t. $F_p(\mathbb{Q})$ on Cauchy jadade hulk normi $|\ |_p$ suhtes). Defineerime hulgal $F_p(\mathbb{Q})$ seose $\sim$ järgmiselt:

$$(a_i) \sim (b_i) \Longleftrightarrow (a_i - b_i) \text{ on nulljada normi } |\ |_p \text{ suhtes.}$$

Jällegi $\sim$ on ekvivalentsusseos. Tähistame faktorhulga selle seose järgi

$$\mathbb{Q}_p = F_p(\mathbb{Q})/\sim = \left\{ [(a_i)] \mid (a_i) \text{ on Cauchy jada normi } |\ |_p \text{ suhtes} \right\}.$$

Hulgal $\mathbb{Q}_p$ defineerime liitmise ja korrutamise jälle võrdustega (36) ja (37) ning hulk $\mathbb{Q}_p$ osutub nende tehete suhtes korpuseks. Selle korpuse elemente nimetame *p-aadilisteks arvudeks.*

Iga $x \in \mathbb{Q}$ korral tähistagu (x) Cauchy jada, mille kõik komponendid on võrdsed arvuga x. On ilmne, et $(x) \sim (x')$ siis ja ainult siis, kui $x = x'$. Korpus $\mathbb{Q}$ on isomorfne korpuse $\mathbb{Q}_p$ alamkorpusega, mis koosneb kõigist ekvivalentsiklassidest $[(x)]$, $x \in \mathbb{Q}$.

Ekvivalentsiklassi $a = [(a_i)]$ normiks $|a|_p$ loeme piirväärtust $\lim_{i\to\infty} |a_i|_p$. Saab näidata, et see piirväärtus eksisteerib. Osutub, et nii defineerides saame tõepoolest normi korpusel $\mathbb{Q}_p$, s.t. on rahuldatud aksioomid N1–N3.

Teoreem 11.16 ([10], lk. 11–12). *Igal ekvivalentsiklassil $a \in \mathbb{Q}_p$, mille korral $|a|_p \leqslant 1$, on täpselt üks esindaja (a_i), kus $a_i \in \mathbb{Z}$ iga naturaalarvu i korral, mis rahuldab tingimusi*

1. $0 \leqslant a_i < p^i$ *iga* $i \in \mathbb{N}$ *korral;*
2. $a_i \equiv a_{i+1} \pmod{p^i}$ *iga* $i \in \mathbb{N}$ *korral.*

Oletame, et p-aadiline arv a ei rahulda võrratust $|a|_p \leqslant 1$. Olgu $|a|_p = p^m$, $m \in \mathbb{N}$. Korrutades arvu a arvuga p^m, saame p-aadilise arvu $a' = ap^m$, mis rahuldab tingimust $|a'|_p \leqslant 1$. Tõepoolest, $|a'|_p = |ap^m|_p = |a|_p\,|p^m|_p = p^m \frac{1}{p^m} = 1$. Kui klassi a' tingimusi 1 ja 2 rahuldavaks esindajaks on jada (a'_i), siis klassi $a = a'p^{-m}$ esindajaks on jada (a_i), kus $a_i = a'_i p^{-m}$.

Esitame nüüd iga a'_i kui p-ndsüsteemi arvu, s.t.

$$a'_i = b_0 + b_1 p + b_2 p^2 + \ldots + b_{i-1} p^{i-1},$$

kus $b_j \in \{0, 1, \ldots, p-1\}$. Tingimus $a'_i \equiv a'_{i+1} \pmod{p^i}$ tähendab seda, et

$$a'_{i+1} = b_0 + b_1 p + b_2 p^2 + \ldots + b_{i-1} p^{i-1} + b_i p^i,$$

kus $b_i \in \mathbb{Z}$. Kuna $0 \leqslant a'_{i+1} < p^{i+1}$, siis $0 \leqslant b_i < p$. Järelikult iga i korral $a_i = a'_i p^{-m} = b_0 p^{-m} + \ldots + b_{i-1} p^{i-1-m}$. Jada (a_i), mis esindab arvu a, võib seega esitada kujul

$$a = \frac{b_0}{p^m} + \frac{b_1}{p^{m-1}} + \ldots + \frac{b_{m-1}}{p} + b_m + b_{m+1} p + b_{m+2} p^2 + \ldots. \tag{39}$$

(Jada (a_i) on selle võrduse paremal poolel oleva lõpmatu summa osasummade jada.) Saadud p-aadilise arvu esitus on teatud määral sarnane reaalarvu esitusega lõpmatu kümnendmurruna: p-aadilisel arvul on ka lõpmata palju numbreid $b_0, b_1, b_2, \ldots$, kusjuures teatud kohast vasakul pool on neid lõplik arv ja paremal pool lõpmata palju. Võrdluseks: reaalarvu $b_0 b_1 \ldots b_{m-1} b_m, b_{m+1} b_{m+2} \ldots$ võib esitada kujul

$$\frac{b_0}{(10^{-1})^m} + \frac{b_1}{(10^{-1})^{m-1}} + \ldots + \frac{b_{m-1}}{(10^{-1})^1} + b_m + b_{m+1} 10^{-1} + b_{m+2} \left(10^{-1}\right)^2 + \ldots.$$

p-aadiliste arvudega saab teha tehteid üsna analoogiliselt kümnendmurdudega. Toome siin mõned näited korrutamise, lahutamise ja jagamise kohta korpuses $\mathbb{Q}_7$ (erinevalt kümnendmurdudest liigutakse laenamisel, korrutamisel jne. vasakult paremale):

$$\begin{array}{r} 3{+}6\cdot 7{+}2\cdot 7^2+\dots \\ \times\underline{4{+}5\cdot 7{+}1\cdot 7^2+\dots} \\ 5{+}4\cdot 7{+}4\cdot 7^2+\dots \\ 1\cdot 7{+}4\cdot 7^2+\dots \\ \underline{3\cdot 7^2+\dots} \\ 5{+}5\cdot 7{+}4\cdot 7^2+\dots \end{array} \qquad \begin{array}{r} 2\cdot 7^{-1}+0\cdot 7^0+3\cdot 7^1+\dots \\ -\underline{4\cdot 7^{-1}+6\cdot 7^0+5\cdot 7^1+\dots} \\ 5\cdot 7^{-1}+0\cdot 7^0+4\cdot 7^1+\dots \end{array}$$

$$\begin{array}{r|l} 1{+}2\cdot 7{+}4\cdot 7^2+\dots & \underline{3+5\cdot 7{+}1\cdot 7^2+\dots} \\ \underline{1{+}6\cdot 7{+}1\cdot 7^2+\dots} & 5+1\cdot 7{+}6\cdot 7^2+\dots \\ 3\cdot 7{+}2\cdot 7^2+\dots & \\ \underline{3\cdot 7{+}5\cdot 7^2+\dots} & \\ 4\cdot 7^2+\dots & \\ \underline{4\cdot 7^2+\dots} & \end{array}$$

Lemma 11.17. *Olgu K korpus ja $\|\ \|$ norm korpusel K. Kui $q\in K$ ja $\|q\|<1$, siis*

$$1+q+q^2+\dots=\frac{1}{1-q}. \tag{40}$$

Lisaks eespoolmainituile on p-aadilistel arvudel ja reaalarvudel teisigi sarnaseid omadusi.

Teoreem 11.18. *p-aadiline arv $a=\sum_{i=-m}^{\infty}a_ip^i\in\mathbb{Q}_p$ on ratsionaalarv parajasti siis, kui tema numbrite jada (a_i) on mingist kohast alates perioodiline.*

Näide 11.19. Esitame 3-aadilise arvu

$$a=1+2\cdot 3+2\cdot 3^2+3^3+2\cdot 3^4+3^5+2\cdot 3^6+3^7+\dots=1+2\cdot 3+(2\cdot 3^2+3^3)$$

ratsionaalarvuna. Kasutades valemit (40) saame, et

$$a=1+2\cdot 3+\frac{2\cdot 3^2+3^3}{1-3^2}=7+\frac{45}{-8}=\frac{11}{8}.$$

Püüame ka, vastupidi, esitada ratsionaalarvu $\frac{11}{8}$ 3-aadilisena. Selleks esitame arvud 11 ja 8 3-aadilisel kujul: $11=2+0\cdot 3+1\cdot 3^2$ ja $8=2+2\cdot 3$. Arv $\frac{11}{8}$ on siis nende jagatis:

$$\begin{array}{r|l} 2+0\cdot 3+1\cdot 3^2 & \underline{2+2\cdot 3} \\ \underline{2+2\cdot 3} & 1+2\cdot 3+2\cdot 3^2+1\cdot 3^3+\cdots \\ 1\cdot 3 & \\ \underline{1\cdot 3+2\cdot 3^2+1\cdot 3^3} & \\ 1\cdot 3^2+1\cdot 3^3+2\cdot 3^4+2\cdot 3^5+\cdots & \\ \underline{1\cdot 3^2+1\cdot 3^3+2\cdot 3^4} & \\ 2\cdot 3^3+0\cdot 3^4+2\cdot 3^5+\cdots & \\ \underline{2\cdot 3^3+2\cdot 3^4} & \\ 1\cdot 3^4+1\cdot 3^5+\cdots & \end{array}$$

11.4. Reaalarvude valla laiendamine

Üleminekul naturaalarvude hulgalt täisarvude hulgale me täiendasime hulka $\mathbb{N}$ nii, et osutuks võimalikuks võrrandite $a+x=b$ lahendamine. Minnes täisarvudelt üle ratsionaalarvudele konstrueerisime sellised objektid, mille abil saab lahendada täisarvuliste kordajatega võrrandeid $ax=b$, kus $a\neq 0$. Kui vaatleme reaalarvude hulka, siis paneme tähele, et ka üle selle hulga leidub algebralisi võrrandeid (s.t. võrrandeid kujul $f(x)=0$, kus $f(x)$ on reaalarvuliste kordajatega polünoom), mis pole lahenduvad. Üheks lihtsamaks selliseks võrrandiks on võrrand $x^2+1=0$. Nagu algebra põhikursuses näidatud, saab konstrueerida kompleksarvude korpuse $\mathbb{C}$, mis sisaldab reaalarvude korpust ja üle mille see võrrand on lahenduv (lahendiks on imaginaarühik i). Seejuures "$\mathbb{C}$ ei sisalda

midagi liigset", s.t. korpusel $\mathbb{C}$ ei ole reaalarvude korpust alamkorpusena sisaldavaid pärisalamkorpusi, üle mille võrrand $x^2 + 1 = 0$ oleks lahenduv. Veelgi enam, kehtib järgmine teoreem.

Teoreem 11.20. *Kompleksarvude korpus $\mathbb{C}$ on isomorfismi täpsuseni ainus minimaalne korpus, mis sisaldab alamkorpusena reaalarvude korpust ja üle mille võrrand $x^2 + 1 = 0$ on lahenduv.*

Tuleb aga välja, et üle kompleksarvude korpuse ei ole mitte ainult võrrand $x^2 + 1 = 0$ lahenduv, vaid tegelikult on lahenduvad juba kõik algebralised võrrandid (selle kohta öeldakse ka, et korpus $\mathbb{C}$ on *algebraliselt kinnine*).

Teoreem 11.21 (Algebra põhiteoreem). *Igal mittekonstantsel polünoomil üle korpuse $\mathbb{C}$ on olemas juur selles korpuses.*

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] F. Lemmermeyer, *Proofs of the Quadratic Reciprocity Law*, `http://www.rzuser.uni-heidelberg.de/~hb3/fchrono.html` .

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

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

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

[17] 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.