

ARVUTEORIA

Kevad 2002

Loengukonspekt

Lektor: Valdis Laan

Sisukord

1. Jaguvus. Aritmeetika põhiteoreem	3
2. Algarvud	8
3. Kongruentsi mõiste ja lihtsamad omadused	12
4. Jäägiklassiringid	14
5. Arvuteoreetilisi funktsioone	16
6. Tundmatut sisaldavad kongruentsid. Hiina jäägiteoreem.	20
6.1. Ülesande püstitusest	20
6.2. Linearkongruentsid	20
6.3. Hiina jäägiteoreem	21
6.4. Kongruentsid algarvu astme järgi	23
6.5. Kongruentsid suvalise mooduli järgi	24
7. Algjuured	26
8. Lõplikud korpused	30
8.1. Lõplike korpuste ehitus	30
8.2. Aritmeetika lõplikes korpustes	33
8.3. Juurimine lõplikes korpustes	35
9. Ruutjäägid	37
10. Arvuvallad	43
10.1. Naturaalarvudelt täisarvudele	43
10.2. Täisarvudelt ratsionaalarvudele	44
10.3. Ratsionaalarvudelt reaalarvudele	45
10.3.1. Weierstrassi meetod	45
10.3.2. Dedekindi meetod	45
10.3.3. Cantori meetod	46
10.3.4. p -aadilised arvud	47
10.4. Reaalarvude valla laiendamine	50

1. Jaguvus. Aritmeetika põhiteoreem

Väga oluline koht arvuteoorias on jaguvuse mõistel. Sellega olete te tõenäoliselt juba kokku puutunud kursuses Algebra I või Algebra II. Meenutame siiski olulisemaid definitsioone (vt. ka [1], lk. 191–198).

Olgu $(R, +, \cdot)$ nullitegureita kommutatiivne ring. (Käesolevas kursuses peame *ringi* all silmas ühikelemendiga assotsiatiivset ringi.) Sellisel juhul võib kõnelda selle ringi elementide jaguvusest. Nimelt, öeldakse, et element $a \in R$ jagab elementi $b \in R$ (ja tähistatakse $a \mid b$), kui leidub selline element $c \in R$, et $ac = b$. Fakti, et $a \mid b$, võib tähistada ja väljendada väga mitmel erineval moel. Kõik järgnevad kirjutised ja väited tähendavad tegelikult ühte ja sedasama:

$$\begin{aligned} a \mid b &\equiv \text{element } a \text{ jagab elemeti } b \equiv b : a \equiv \text{element } b \text{ jagub elemendiga } a \\ &\equiv a \text{ on } b \text{ jagaja} \equiv a \text{ on } b \text{ tegur} \equiv b \text{ on } a \text{ kordne} \equiv (\exists c)(ac = b). \end{aligned}$$

Jaguvuse definitsioonist järeldub vahetult, et element on pööratav ringis R parajasti siis, kui ta jagab selle ringi ühikelementi. Ringi R pööratavad elemendid moodustavad korrutamise suhtes rühma, mida tähistatakse $U(R)$ ja mille elemente nimetatakse vahel ka *ühikuiks* (ingl. k. *unit*). Seega $U(R) = \{a \in R \mid (\exists c \in R)(ac = 1)\}$. Mittepööratavat elementi $p \in R$ nimetatakse *taandumatuks*, kui iga $a, b \in R$ korral võrdusest $p = ab$ järeldub, et kas a on pööratav või b on pööratav. Öeldakse, et elemendid $a, b \in R$ on *assotsieeritud* (tähistatakse $a \sim b$), kui $a = bu$, kus $u \in R$ on pööratav. Saab tõestada, et a ja b on assotsieeritud parajasti siis, kui $a \mid b$ ja $b \mid a$ (vt. [1], Lemma 6.12.2.).

Näide 1.1. Täisarvude ringis \mathbb{Z} on pööratavad elemendid vaid 1 ja -1 , s.t. $U(\mathbb{Z}) = \{1, -1\}$. Igal arvul $a \notin U(\mathbb{Z})$ on vähemalt 4 jagajat: $1, -1, a, -a$. Näiteks arvu 6 jagajad on $\pm 1, \pm 2, \pm 3$ ja ± 6 . Arvud a ja b on assotsieeritud, kui $a = \pm b$ ning ringi \mathbb{Z} taandumatud elemendid on algarvud ja nende vastandarvud.

Meenutame mõningaid jaguvusseose omadusi.

Lause 1.2. Jaguvusseosel nullitegureita kommutatiivses ringis R on järgmised omadused: iga $a, b, c \in R$ 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 $ac \mid bc$ (järelilikult ka $a \mid bc$).

Nullitegureita kommutatiivses ringis R võib kõnelda elementide suurimast ühistegurist ja vähimast ühiskordsest.

Definitsioon 1.3. Elementi $d \in R$ nimetatakse elementide $a, b \in R$ suurimaks ühisteguriks (tähistatakse $d = \text{SÜT}(a, b)$ ehk lühidalt $d = (a, b)$), kui

- (i) $d \mid a$ ja $d \mid b$;
- (ii) iga $c \in R$ korral, kui $c \mid a$ ja $c \mid b$, siis $c \mid d$.

Definitsioon 1.4. Elementi $m \in R$ nimetatakse elementide $a, b \in R$ vähimaks ühiskordseks (tähistatakse $m = \text{VÜK}(a, b)$ ehk $m = [a, b]$), kui

- (i) $a \mid m$ ja $b \mid m$;
- (ii) iga $c \in R$ 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) ja $u \in U(R)$, siis ka du on a ja b suurim ühistegur (vähim ühiskordne). Teiste sõnadega, suurim ühistegur ja vähim ühiskordne on määratud üheselt assotsieerituse täpsusega (täisarvude korral tähendab see siis märgi täpsust). Muuhulgas tähendab see seda, et mistahes suurimat ühistegurit või vähimat ühiskordset sisaldavate avaldiste võrdust tuleb tõlgendada assotsieerituse täpsusega.

Suurimal ühisteguril on järgmised omadused.

Lause 1.5. Iga $a, b, c \in R$ 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 $b = 0$;

$$4. (ca, cb) = c(a, b);$$

$$5. ((a, b), c) = (a, (b, c)).$$

On ringe, mille kahe elemendi SÜT ja VÜK ei eksisteeri. Täisarvude korral on siiski igal kahel arvul olemas täpselt kaks suurimat ühistegurit ja vähimat ühiskordset (v.a. juhul, kui mõlemad arvud on võrdsed nulliga).

Järgmine lause on lugejale kindlasti tuttav. Lühidalt öeldes väidab ta seda, et iga täisarvu võib jäägiga jagada iga naturaalarvuga. Märgime, et selle kursuse jooksul me loeme naturaalarvudeks arve $1, 2, 3, \dots$ (kuid mitte 0).

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

$$a = bq + r \quad \text{ja} \quad 0 \leq r < b.$$

TÕESTUS. Selliste q ja r leidumine on tõestatud raamatus [1], lauses 6.1.21. Näitame, et nad on üheselt määratud. Selleks oletame, et leiduvad täisarvud q_1, q_2, r_1, r_2 nii, et

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

Siis $b(q_1 - q_2) = r_2 - r_1$. Kuna $b \neq 0$, $|r_2 - r_1| < b$ ja $q_1 - q_2 \in \mathbb{Z}$, siis võrdusest $|r_2 - r_1| = |b||q_1 - q_2|$ järeldub, et $q_1 - q_2 = 0$ ja seega ka $r_2 - r_1 = 0$. See tähendab, et $q_1 = q_2$ ja $r_1 = r_2$. \square

Seega naturaalarv b jagab täisarvu a (ehk a jagub arvuga b) parajasti siis, kui arvu a jagamisel arvuga b tekkinud jääk on 0.

Lausest 1.6 järeldub muuhulgas, et ring \mathbb{Z} on nn. *Eukleidese ring* ja seega (nagu teada kursusest Algebra I või Algebra II), võib selles ringis kahe elemendi suurima ühisteguri leida *Eukleidese algoritmi* abil.

Algoritm ise töötab järgmiselt. Olgu eesmärgiks leida täisarvude a ja b suurim ühistegur. Üldsust kitsendamata võime eeldada, et $a \geq b > 0$ (sest $(a, b) = (|a|, |b|)$). Kõigepäält jagame arvu a jäägiga arvuga b :

$$a = bq_1 + r_1, \quad 0 \leq r_1 < b.$$

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 :

$$b = r_1q_2 + r_2, \quad 0 \leq r_2 < r_1.$$

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

$$r_1 = r_2q_3 + r_3, \quad 0 \leq r_3 < r_2.$$

Niimoodi jätkame senikaua kui saame mingil sammul jäägiks $r_{n+1} = 0$. Varem või hiljem peab see juhtuma, sest $b > r_1 > r_2 > \dots \geq 0$ ja ei leidu lõpmatuid kahanevaid naturaalarvujadaseid. Osutub, et 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.

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

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 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 sümbolikat ja lahendas mitme tundmatuga võrrandeid.

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

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

olemas täisarvuline lahend parajasti siis, kui $(a, b) \mid c$. Kui vähemalt üks arvudest a ja b ei ole 0 ning x_0, y_0 on selle võrrandi mingi (eri)lahend, siis kõik ülejäänud selle võrrandi lahendid x, y saadakse valemite

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

abil, andes muutujale t kõik täisarvulised väärtused.

TÕESTUS. Tõestame esimese väite.

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) põhjal ka $(a, b) \mid ax + by = c$.

PIISAVUS. See, et $(a, b) \mid c$, tähendab, et leidub selline $s \in \mathbb{Z}$, et $r_n s = c$. Olgu $(a, b) = r_n$ leitud Eukleidese algoritmi abil. Liikudes tabelis (1) alt üles, saame r_n avaldada a ja b kaudu:

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

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

Enne teise väite tõestamist märgime, et esimesest väitest saab teha järeldused 1.10, 1.11 ja 1.12

Oletame nüüd, et meile on teada võrrandi (2) mingi lahend x_0, y_0 . Kui x', y' on selle võrrandi mingi teine lahend, siis $ax_0 + by_0 = c = ax' + by'$, millest saame, 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 1.10 põhjal $(a', b') = (\frac{a}{d}, \frac{b}{d}) = 1$. Asendades a ja b ning jagades võrduse mõlemaid pooli arvuga d , saame

$$a'(x' - x_0) = b'(y_0 - y'). \quad (3)$$

Meil on olukord, kus $a' \mid b'(y_0 - y')$ ja $(a', b') = 1$. Kasutades järeldust 1.11 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 jagades arvuga a' , saame $x' - x_0 = b't$. Seega oleme saanud, et lahend x', y' avaldub kujul $x' = x_0 + b't = x_0 + \frac{b}{(a, b)}t$, $y' = y_0 - a't = y_0 - \frac{a}{(a, b)}t$.

Teisest küljest, on lihtne näha, et iga $t \in \mathbb{Z}$ korral sellised arvud rahuldavad võrrandit (2):

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

□

Märkus 1.8. Kirjutame korraks võrrandi (2) lahendeid paaridena $\langle x, y \rangle$. Vaatleme võrrandit $ax + by = c$ üle reaalarvude ning eeldame, et vähemalt üks arvudest a ja b ei ole 0. Siis lineaarvõrrandisüsteemide teooria põhjal on teada, et sellest võrrandist koosnevale süsteemile vastava homogeenise süsteemi $ax + by = 0$ lahendite fundamentaalsüsteem sisaldab ühe lahendi $\langle x_1, y_1 \rangle$ (selleks võib võtta näiteks paari $\langle x_1, y_1 \rangle = \left\langle \frac{b}{(a, b)}, -\frac{a}{(a, b)} \right\rangle \in \mathbb{R}^2$) ning süsteemi $ax + by = c$ kõigi reaalarvuliste lahendite hulk avaldub kujul $\langle x_0, y_0 \rangle + \{t \langle x_1, y_1 \rangle \mid t \in \mathbb{R}\} = \{\langle x_0 + tx_1, y_0 + ty_1 \rangle \mid t \in \mathbb{R}\}$, kus $\langle x_0, y_0 \rangle \in \mathbb{R}^2$ on selle võrrandi mingi erilahend (vt. [1], teoreem 5.5.3). Teoreem 1.7 ütleb, et kui vaadelda võrrandit $ax + by = c$ üle täisarvude, siis tema kõigi lahendite hulk avaldub sisuliselt samamoodi.

Näide 1.9. Lahendame diofantilise võrrandi

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

Selleks leiame Eukleidese algoritmi abil $(172, 20)$. Saame, et

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

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

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

Korrutades saadud seose 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

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

kus t on täisarv.

Leiame veel näiteks 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 $t = -99$. Seega antud võrrandil on vaid üks positiivne lahend $x = 500 + 5 \cdot (-99) = 5$, $y = -4250 - 43 \cdot (-99) = 7$.

Järeldus 1.10. Iga $a, b, d \in \mathbb{Z}$, $d \neq 0$, korral on võrdus $(a, b) = d$ samaväärne võrdusega $(\frac{a}{d}, \frac{b}{d}) = 1$.

TÕESTUS. Näitame, et esimesest võrdusest järeldub teine. Et d on a ja b jagaja, siis $\frac{a}{d}$ ja $\frac{b}{d}$ on täisarvud. Teoreemi 1.7 esimese väite põhjal leiduvad sellised täisarvud x ja y , et $ax + by = d$. Jagades selle võrduse pooli arvuga d saame, et $\frac{a}{d}x + \frac{b}{d}y = 1$, millest jällegi teoreemi 1.7 põhjal saame, et $(\frac{a}{d}, \frac{b}{d}) \mid 1$ ehk $(\frac{a}{d}, \frac{b}{d}) = 1$.

Oletame nüüd, et kehtib $(\frac{a}{d}, \frac{b}{d}) = 1$. Siis lause 1.5 osa 3. põhjal $d = d(\frac{a}{d}, \frac{b}{d}) = (a, b)$. \square

Järeldus 1.11. Kui $a \mid bc$ ja $(a, b) = 1$, $a, b, c \in \mathbb{Z}$, siis $a \mid c$.

TÕESTUS. Kuna $(a, b) = 1$, siis leiduvad sellised täisarvud x ja y , et $ax + by = 1$. Järelikult $axc + byc = c$. Et a jagab selle võrduse vasakut poolt, siis peab ta jagama ka paremat poolt, s.t. $a \mid c$. \square

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 1.12. Kui p on algarv ja $p \mid bc$, $b, c \in \mathbb{Z}$, 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 1.11 põhjal, et $p \mid c$. \square

Induktsiooniga saab nüüd lihtsalt tõestada järgmise väite.

Järeldus 1.13. Kui p on algarv ja $p \mid a_1 a_2 \dots a_n$, $a_1, a_2, \dots, a_n \in \mathbb{Z}$, siis leidub $k \in \{1, 2, \dots, n\}$, nii et $p \mid a_k$.

Kuna algarvu ainsad naturaalarvulised jagajad on 1 ja see arv ise, siis saame järgmise tulemuse.

Järeldus 1.14. Kui p, q_1, q_2, \dots, q_n on algarvud ja $p \mid q_1 q_2 \dots q_n$, siis leidub $k \in \{1, 2, \dots, n\}$, nii et $p = q_k$.

Näitena nende omaduste rakendamiseks vaatleme järgmist väidet, mille tõestas juba Pythagoras (569–500 e.m.a.).

Näide 1.15. $\sqrt{2}$ ei ole ratsionaalarv.

Oletame vastuväiteliselt, et $\sqrt{2}$ on ratsionaalarv, s.t. $\sqrt{2} = \frac{b}{a}$, kus a ja b on täisarvud ja $(a, b) = 1$. Ruutu võttes saame $b^2 = 2a^2$, seega $a \mid b^2$. Kui $a > 1$, siis järelduse 1.11 põhjal peaks $a \mid b$ ja järelikult $(a, b) = a > 1$, mis pole võimalik. Seega $a = 1$ ja järelikult $b^2 = 2$, mis on vastuolu, sest ühegi täisarvu ruut pole 2. Saadud vastuolu näitabki, et $\sqrt{2}$ ei saa olla ratsionaalarv.

Järgnevalt tõestame väite, millele tugineb suur osa naturaalarvude aritmeetikas tõestatavatest teoreemidest ja mis pärineb Eukleidese (u. 350 e.m.a.) "Elementide" IX raamatust.

Teoreem 1.16 (Aritmeetika põhiteoreem). Iga naturaalarv $n > 1$ esitub algarvude korrutisena ja see esitus on ühene tegurite järjekorra täpsuseni.

TÕESTUS. Näitame esiteks induktsiooniga, et iga naturaalarv $n > 1$ esitub algarvude korrutisena. Arvu $n = 2$ korral on väide ilmne. Oletame, et $n > 2$ ja iga naturaalarv $1 < m < n$ esitub 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 $1 < d < n$. Valime selliste naturaalarvude d hulgast välja vähima, olgu see p . Siis p on algarv. Tõepoolest, kui leiduks naturaalarv c nii, et $c \mid p$ ja $1 < c < p$, siis seostest $c \mid p$ ja $p \mid n$ järelduks, et $c \mid n$, mis aga on vastuolus arvu p valikuga. Seega $n = pm$, kus p on algarv ja $1 < m < n$. Induktsiooni eelduse põhjal avaldub m algarvude korrutisena ning järelikult ka n avaldub algarvude korrutisena.

Ühesuse näitamiseks oletame, et n esitub algarvude korrutisena kahel viisil:

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

kus (üldsust kitsendamata) $r \leq s$ ja algarvud p_i ja q_j on mittekahanevas järjekorras, s.t. $p_1 \leq p_2 \leq \dots \leq p_r$ ja $q_1 \leq q_2 \leq \dots \leq q_s$. Kuna $p_1 \mid q_1 q_2 \dots q_s$, siis järelduse 1.14 põhjal $p_1 = q_k$ mingi $k \in \{1, \dots, s\}$ korral; kuid siis $p_1 \geq q_1$. Samamoodi saame $q_1 \geq p_1$ ning seega $p_1 = q_1$. Taandades p_1 saame $p_2 p_3 \dots p_r = q_2 q_3 \dots q_s$. Korrates seda mõttekäiku saame $p_2 = q_2$ ja $p_3 p_4 \dots p_r = q_3 q_4 \dots q_s$. Kui $r < s$, siis niimoodi jätkates saame $1 = q_{r+1} q_{r+2} \dots q_s$, mis on aga võimatu, sest kõik $q_i > 1$. Seega $r = s$ ning $p_1 = q_1, p_2 = q_2, \dots, p_r = q_r$, mida oligi vaja näidata. \square

Märgime, et kuigi siin me andsime aritmeetika põhiteoreemi vahetuma tõestuse, on see teoreem tegelikult otseseks järelduseks teoreemile, mis väidab, et iga Eukleidese ring on faktoriaalne ([1], teoreem 6.13.4).

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 1.17. Iga naturaalarv $n > 1$ esitub üheselt kujul

$$n = p_1^{k_1} p_2^{k_2} \dots p_s^{k_s}, \quad (4)$$

kus $k_i > 0$, p_i on algarv iga $i = 1, 2, \dots, s$ korral ning $p_1 < p_2 < \dots < p_s$.

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

Näide 1.18. $180 = 2 \cdot 5 \cdot 2 \cdot 3 \cdot 3 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 = 2^2 \cdot 3^2 \cdot 5^1$, kus viimane korrutis on arvu 180 standardkuju.

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

Lause 1.19. Olgu $m, n > 1$ naturaalarvud, $m = p_1^{k_1} \dots p_s^{k_s}$, $n = p_1^{l_1} \dots p_s^{l_s}$, kus p_1, \dots, p_s on paarikaupa erinevad algarvud ja $k_i \geq 0, l_i \geq 0, i = 1, \dots, s$. Siis

1. $m \mid n$ parajasti siis, kui $k_i \leq l_i, i = 1, \dots, s$;
2. $(m, n) = p_1^{u_1} \dots p_s^{u_s}$, kus $u_i = \min(k_i, l_i), i = 1, \dots, s$;
3. $[m, n] = p_1^{v_1} \dots p_s^{v_s}$, kus $v_i = \max(k_i, l_i), i = 1, \dots, s$.

TÕESTUS. 1. **TARVILIKKUS.** Olgu $m \mid n$. 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 $a = p_1^{j_1} \dots p_s^{j_s}$, kus $j_1, \dots, j_s \geq 0$. Järelikult

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

Aritmeetika põhiteoreemi põhjal $k_i + j_i = l_i$, millest järeldubki, et $k_i \leq l_i, i = 1, \dots, s$.

PIISAVUS. Olgu $k_i \leq l_i, i = 1, \dots, s$. Siis $m \left(p_1^{l_1-k_1} \dots p_s^{l_s-k_s} \right) = n$, ehk $m \mid n$.

2. Tähistame $d = p_1^{u_1} \dots p_s^{u_s}$. Kuna $u_i \leq k_i$ ja $u_i \leq l_i, i = 1, \dots, s$, siis väite 1 põhjal $d \mid m$ ja $d \mid n$. Oletame, et $c \mid m$ ja $c \mid n$, kusjuures $c = p_1^{j_1} \dots p_s^{j_s}$. Jällegi

väite 1 põhjal $j_i \leq k_i$ ning $j_i \leq l_i, i = 1, \dots, s$. Seega $j_i \leq \min(k_i, l_i) = u_i, i = 1, \dots, s$, millest järeldub, et $c \mid d$.

3. saab tõestada analoogiliselt. □

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

Lause 1.20. Mistahes naturaalarvude a ja b korral

$$(a, b) [a, b] = ab.$$

Näide 1.21. 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 1.19 saame, et $(m, n) = 2^0 \cdot 3^2 = 9$ ja $[m, n] = 2^2 \cdot 3^3 = 108$.

Tuleb märkida, et lause 1.19 omab tähtsust pigem teoreetilistes arutlustes, sest naturaalarvu algteguriks lahutamine on reeglina vga tmahukas. Suurima ühisteguri praktiliseks leidmiseks kasutatakse reeglina Eukleidese algoritmi.

2. Algarvud

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*.

Kuidas antud naturaalarvu korral teha kindlaks, 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 $b \leq c$, saame, et $b^2 \leq bc = a$ ja seega $b \leq \sqrt{a}$. Et $b > 1$, siis leidub arvul b vähemalt üks algtegur p . Siis $p \leq b \leq \sqrt{a}$, ning kuna $p \mid b$ ja $b \mid a$, siis $p \mid a$. Seega, kui a on kordarv, siis tal leidub selline algtegur, mis pole suurem kui \sqrt{a} . Ehk samaväärselt, kui ükski algarv $p \leq \sqrt{a}$ ei ole arvu a jagaja, siis a on algarv. Seega arvu a algarvulisuse kontrollimiseks piisab, kui kontrollime, kas ta jagub algarvudega $p \leq \sqrt{a}$.

Näide 2.1. Kas 101 on algarv?

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

Eespool nägime, et kui ükski algarv $p \leq \sqrt{a}$ 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, mõõdetakse [jada] teise arvu suuruse abil, see on viie abil, kolm mõõdab 15-t viis korda. Jälle, kui alustades viieteistkümnest ma jätan vahel kaks arvu, mis on paigutatud jadas tema järele, siis esimene arv on tema [s.o. arvu 21] 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 vahel jätta 4 paaritud arvu pärast 5-t, kuni tuleb see, mida 5 mõõta saab. Vahele jäetakse 4 paaritud 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 jätavad 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 jäetakse vahele veel kuus vahepäälset arvu, siis arvu, mis järgneb, seitsmendat arvu [21] saab mõõta seitsmega kolme suuruse abil; ja see kindel kord jätkub jada viimase arvuni."

Juba Eukleides leidis, et ei saa olla suurimat algarvu.

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

TÕESTUS. Olgu algarvud tähistatud $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, \dots$. Oletame vastuväiteliselt, et leidub suurim algarv p_n . Vaatleme naturaalarvu $a = p_1 p_2 \dots p_n + 1$. Et $a > 1$, siis peab leiduma algarv, mis arvu a jagab. Kuna

oletasime, et p_1, \dots, p_n on ainsad algarvud, siis peab leiduma selline $i \in \{1, \dots, n\}$, et $p_i \mid a$. Seega saame lause 1.2 põhjal, et $p_i \mid a - p_1 p_2 \dots p_n = 1$, mis on vastuolus sellega, et $p_i > 1$. \square

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 $4k + 2 = 2(2k + 1)$ on paarisarvud ja seega kordarvud. Paaritud arvud jagunevad kahte lõpmatusse jadasse: ühed, mis on kujul $4k + 1$, s.t.

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

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

$$3, 7, 11, 15, 19, 23, \dots$$

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 $mn = (4k + 1)(4l + 1) = 4(4kl + k + l) + 1$. \square

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

TÕESTUS. Oletame jällegi, et on vaid lõplik arv algarve kujul $4k + 3$. Olgu nad tähistatud q_1, \dots, q_n . Vaatleme naturaalarvu $a = 4q_1 q_2 \dots q_n - 1 = 4(q_1 q_2 \dots q_n - 1) + 3$. Olgu $a = r_1 r_2 \dots r_s$ 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, \dots, 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 $r_i \mid a - 4q_1 q_2 \dots q_n = -1$, vastuolu. \square

Tegelikult ka jadas $(4k + 1)_{k \in \mathbb{N} \cup \{0\}}$ on lõpmata palju algarve (vt. lause 9.8) ja veelgi enam, kehtib Dirichlet' poolt 1837. a. tõestatud teoreem algarvude kohta aritmeetilises jadas.

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

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

on lõpmata palju algarve.

Teisest küljest, ei ole ühtegi aritmeetilist jada $a, a + b, a + 2b, \dots = (a + kb)_{k \in \mathbb{N} \cup \{0\}}$, $a, b \in \mathbb{N}$, mis koosneks ainult algarvudest. Tõepoolest, 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 $a + (l + p)b = a + lb + pb = p(1 + b)$ on kordarv. Veelgi enam, iga $m \in \mathbb{N}$ korral $a + (l + mp)b = a + lb + mpb = p(1 + mb)$ on kordarv ja seega jada $(a + kb)_{k \in \mathbb{N} \cup \{0\}}$ sisaldab lõpmata palju kordarve.

On püstitatud hüpotees, et mistahes naturaalarvu n korral leidub aritmeetiline jada pikkusega n , mis koosneb algarvudest. Näiteks $n = 3$ ja $n = 4$ korral on sellisteks jadadeks 41, 47, 53 ja 251, 257, 263, 269.

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

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

Näiteks, kui tahame saada 4 järjestikust kordarvu, võime võtta

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

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 süiski otsima väga kaugel.

Teoreem 2.6 (Tšebõšev). *Kui $n > 3$ on naturaalarv, siis n ja $2n - 2$ vahel leidub vähemalt üks algarv.*

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

Teoreem 2.7. *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 Hadamard'il ja Vallé Poussinil teineteisest sõltumatult tõestada, et

$$\lim_{n \rightarrow \infty} \frac{\pi(n)}{n/\ln(n)} = 1.$$

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 2.8. *n . astme polünoomil üle nullitegureita kommutatiivse ringi ei ole selles ringis rohkem kui n juurt.*

Teoreem 2.9 (Euler). *Ühegi täisarvuliste kordajatega mittekonstantse polünoomi väärtused ei ole kõigi argumenti naturaalarvuliste väärtuste korral algarvud.*

TÕESTUS. Oletame vastuväiteliselt, et leidub mittekonstantne polünoom

$$f(x) = a_k x^k + a_{k-1} x^{k-1} + \dots + a_2 x^2 + a_1 x + a_0,$$

kus $a_0, \dots, a_k \in \mathbb{Z}$, mille väärtus iga naturaalarvu n korral on algarv. Siis muuhulgas $f(1) = a_k + \dots + a_0 = p$ on algarv. Kui $t \in \mathbb{N} \cup \{0\}$, siis kasutades Newtoni binoomvalemit saame

$$f(1+tp) = a_k(1+tp)^k + \dots + a_1(1+tp) + a_0 = (a_k + \dots + a_1 + a_0) + pg(t) = p + pg(t) = p(1+g(t)),$$

kus $g(t)$ on täisarvuliste kordajatega polünoom t suhtes. Järelikult $p \mid f(1+tp)$, millest eelduse tõttu saame, et $f(1+tp) = p$ iga $t \in \mathbb{N} \cup \{0\}$ korral. Seega mittekonstantsel polünoomil $f(x) - p$ on lõpmata palju täisarvulisi juuri, mis on vastuolus lausega 2.8 □

1947. a. tõestas Mills, et leidub selline positiivne reaalarv r , et avaldis $f(n) = \lfloor r^{3^n} \rfloor$, 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. Arvu r tegeliku väärtuse kohta pole aga midagi teada.

Üheks kuulsamaks algarvude kohta käivaks lahendamata probleemiks on Goldbachi (1690–1764) poolt kirjavaletuses Euleriga 1742. a. püstitatud hüpootees.

Probleem 2.10 (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 saab iga 5-st suurema paaritu arvu 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. Kõige enam on Goldbachi hüpoteesile tõestust otsides saavutanud vene matemaatik Vinogradov, kes 1937. a. näitas, et leidub selline naturaalarv N (kaks aastat hiljem leiti, et $N = \lfloor e^{e^{41,96}} \rfloor$), et kõik sellest suuremad paaritud arvud on esitatavad kolme algarvu summana. Sellest järeldub, et kõik piisavalt suured paarisarvud on esitatavad ülimalt 4 paaritu algarvu summana.

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

Teoreem 2.11 (Fermat' suur teoreem). *Kui $n > 3$ 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 üldjuhul 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

Kongruentsi mõiste võttis kasutusele Gauss (1777–1855) oma teoses “Disquisitiones Arithmeticae”, 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 $5 \mid 22 - 7 = 15$ 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 $0 \leq r < n$. 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 $a = q_1n + r$ ja $b = q_2n + r$, kus $0 \leq r < n$. Siis $b - a = (q_2n + r) - (q_1n + r) = (q_2 - q_1)n$, kust saame, et $n \mid b - a$ ehk $a \equiv b \pmod{n}$. \square

Lause 3.4. Täisarvude kongruentsusseos on ekvivalentsusseos.

TÕESTUS. Olgu $a, b, c \in \mathbb{Z}$ ja $n \in \mathbb{N}$.

Refleksiivsus. Kuna $a - a = 0$ ja $n \mid 0$, siis $a \equiv a \pmod{n}$.

Sümmeetrilisus. Kui $a \equiv b \pmod{n}$, ehk $n \mid b - a$, siis ka $n \mid a - b$, ehk $b \equiv a \pmod{n}$.

Transitiivsus. Oletame, et $a \equiv b \pmod{n}$ ja $b \equiv c \pmod{n}$. Siis $n \mid b - a$ ja $n \mid c - b$. Järelikult $n \mid (c - b) + (b - a) = c - a$, ehk $a \equiv c \pmod{n}$. \square

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

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

ja nimetame selliseid hulki jäägiklassideks mooduli n järgi. Kongruentsusseose refleksiivsuse tõttu $a \in \bar{a}$ iga täisarvu a korral.

Lause 3.5. 1. Iga $a, b \in \mathbb{Z}$ korral $\bar{a} = \bar{b}$ parajasti siis, kui $a \equiv b \pmod{n}$.

2. Mooduli n järgi leidub täpselt n erinevat jäägiklassi.

TÕESTUS. 1. **TARVILIKKUS.** Kui $\bar{a} = \bar{b}$, siis $b \in \bar{a}$ ja järelikult $a \equiv b \pmod{n}$.

PIISAVUS. Kui $a \equiv b \pmod{n}$, siis $b \in \bar{a}$. Mistahes täisarvu c korral, kui $c \in \bar{b}$, s.t. $b \equiv c \pmod{n}$, siis kongruentsusseose transitiivsuse tõttu ka $a \equiv c \pmod{n}$ ja $c \in \bar{a}$. Seega $\bar{b} \subseteq \bar{a}$. Analoogiliselt saab näidata, et $\bar{a} \subseteq \bar{b}$ ning järelikult $\bar{a} = \bar{b}$.

2. Vaatleme jäägiklasse $\bar{0}, \bar{1}, \dots, \overline{n-1}$ mooduli n järgi. Kui $a \in \mathbb{Z}$ ja a jagamisel arvuga n tekib jääk r , s.t. $a = nq + r$, $0 \leq r < n$, siis $a \equiv r \pmod{n}$ ning 1. põhjal $\bar{a} = \bar{r}$. Seega iga jäägiklass mooduli n järgi on võrdne ühega jäägiklassidest $\bar{0}, \bar{1}, \dots, \overline{n-1}$. Lause 3.3 tõttu iga $i, j \in \{0, 1, \dots, n-1\}$ 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) ja väite 1 tõttu siis ka $\bar{i} \neq \bar{j}$, s.t. jäägiklassid $\bar{0}, \bar{1}, \dots, \overline{n-1}$ on kõik erinevad. \square

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

Lause 3.6. 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 $a_1 a_2 \equiv b_1 b_2 \pmod{n}$. \square

Järeldus 3.7. Kui $f(x)$ on täisarvuliste kordajatega polünoom ning $a \equiv b \pmod{n}$, siis $f(a) \equiv f(b) \pmod{n}$.

TÕESTUS. Olgu $f(x) = a_k x^k + a_{k-1} x^{k-1} + \dots + a_1 x + a_0$, kus $a_0, \dots, a_k \in \mathbb{Z}$, ning olgu $a \equiv b \pmod{n}$. Kasutades lauset 3.6 saame, et iga $i = 1, \dots, k$ korral $a^i \equiv b^i \pmod{n}$. Kuna $a_i \equiv a_i \pmod{n}$, siis jällegi lauset 3.6 kasutades saame, et $a_i a^i \equiv a_i b^i \pmod{n}$ iga $i = 1, \dots, k$ korral. Siis aga ka

$$f(a) = a_k a^k + a_{k-1} a^{k-1} + \dots + a_1 a + a_0 \equiv a_k b^k + a_{k-1} b^{k-1} + \dots + a_1 b + a_0 = f(b) \pmod{n}.$$

□

Näide 3.8. Näitame, et polünoomil $x^2 - 117x + 31$ ei ole täisarvulisi juuri.

Vaatleme moodulit $n = 2$. Siis 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 3.7 põhjal kas $f(a) \equiv f(0) \pmod{2}$ või $f(a) \equiv f(1) \pmod{2}$. Kui $f(x) = a_k x^k + a_{k-1} x^{k-1} + \dots + a_1 x + a_0$, siis $f(0) = a_0$ ja $f(1) = a_k + a_{k-1} + \dots + a_1 + a_0$. Seega, 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 3.9. Iga täisarvu $k \neq 0$ korral $a \equiv b \pmod{n}$ parajasti siis, kui $ka \equiv kb \pmod{kn}$.

TÕESTUS. Olgu $k \neq 0$. Siis kasutades seda, et nullist erineva täisarvu võib taandada, saame

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

□

Lause 3.10. Kui $ka \equiv kb \pmod{n}$ ja $k \neq 0$, siis $a \equiv b \pmod{\frac{n}{(k,n)}}$.

TÕESTUS. Olgu $d = (k, n)$, $n = dn'$ ja $k = dk'$, siis järelduse 1.10 põhjal $(n', k') = 1$. Kuna $n \mid kb - ka$, siis leidub selline $x \in \mathbb{Z}$, et $nx = kb - ka$. Asendades n ja k saame, et $dn'x = dk'b - dk'a$. Kuna $k \neq 0$, siis ka $d \neq 0$ ja seega $n'x = k'b - k'a$. Sellest, et $n' \mid k'b - k'a = k'(b - a)$ ja $(n', k') = 1$, saame järelduse 1.11 põhjal, et $n' = \frac{n}{d} \mid b - a$, ehk $a \equiv b \pmod{\frac{n}{d}}$. □

Järeldus 3.11. Kui $ka \equiv kb \pmod{n}$, $k \neq 0$, ja $(k, n) = 1$, siis $a \equiv b \pmod{n}$.

Näide 3.12. Sellest, et $33 \equiv 15 \pmod{9}$ ja $(3, 9) = 3$, saame lause 3.10 põhjal, et $11 \equiv 5 \pmod{3}$. Sellest, et $-35 \equiv 45 \pmod{8}$ ja $(5, 8) = 1$, saame järelduse 3.11 põhjal, et $-7 \equiv 9 \pmod{8}$.

Näitena kongruentside lihtsamate omaduste rakendamiseks vaatame, kuidas nende abil põhjendada jaguvustunnuseid.

Lause 3.13. Olgu

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \dots + a_1 \cdot 10 + a_0 = \underline{a_k a_{k-1} \dots a_1 a_0},$$

kus $0 \leq a_i \leq 9$ (s.o. n on arv, mille kümnendnumbreiks on a_k, \dots, a_0). Siis

1. $3 \mid n \iff 3 \mid a_0 + a_1 + \dots + a_k$;
2. $9 \mid n \iff 9 \mid a_0 + a_1 + \dots + a_k$;
3. $11 \mid n \iff 11 \mid a_0 - a_1 + a_2 - \dots + (-1)^k a_k$.

TÕESTUS. Olgu $f(x) = a_k x^k + a_{k-1} x^{k-1} + \dots + a_1 x + a_0$. Siis $n = f(10)$.

2. Kuna $10 \equiv 1 \pmod{9}$, siis järelduse 3.7 põhjal $n = f(10) \equiv f(1) = a_0 + a_1 + \dots + a_k \pmod{9}$. Seega arvud n ja $a_0 + a_1 + \dots + a_k$ annavad 9-ga jagades sama jäägi, sääljuures n jagub 9-ga (s.o. annab jäägi 0) parajasti siis, kui $a_0 + a_1 + \dots + a_k$ jagub 9-ga.

Tunnuse 1. saab tõestada analoogiliselt.

3. Et $10 \equiv -1 \pmod{11}$, siis $n = f(10) \equiv f(-1) = a_0 - a_1 + a_2 - \dots + (-1)^k a_k \pmod{11}$, millest järeldubki, et n jagub 11-ga parajasti siis, kui $a_0 - a_1 + a_2 - \dots + (-1)^k a_k$ jagub 11-ga. □

4. Jäägiklassiringid

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

$$\mathbb{Z}_n = \{\bar{a} \mid a \in \mathbb{Z}\} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}.$$

Selle hulga saame muuta kommutatiivseks ringiks defineerides liitmise ja korrutamise võrdustega

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

iga $\bar{a}, \bar{b} \in \mathbb{Z}_n$ korral. Lausest 3.6 järeldub, et need definitsioonid on korrektsed, s.t. ei sõltu jäägiklasside esindajate valikust. Ringi definitsiooni tingimuste täidetuse järeldub täisarvude vastavatest omadustest. Ringi \mathbb{Z}_n nimetatakse *jäägiklassiringiks* mooduli n järgi. Jäägiklassiringi, mille iga nullist (s.o. jäägiklassist $\bar{0}$) erinev element on pööratav, nimetatakse *jäägiklassikorpuseks*.

Edaspidises läheb vaja kahte lemmat.

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

TÕESTUS. Oletame, et $(n_1 \dots n_s, n) = d > 1$. Siis leidub selline algarv p , et $p \mid d$ ning seega $p \mid n_1 \dots n_s$ ja $p \mid n$. Järelduse 1.13 põhjal peab leiduma selline i , et $p \mid n_i$. Siis aga $p \mid (n_i, n)$, mis on vastuolus sellega, et $(n_i, n) = 1$. \square

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

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

Jäägiklassiringide uurimisel kasutame mõningaid ringide üldisi omadusi, andes ka nende omaduste tõestused üldjuhul. Seejuures rõhutame veelkord, et selles kursuses vaatleme vaid selliseid ringe, mis on assotsiatiivsed ja ühikelemendiga.

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

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

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

$$\begin{aligned}(r_1, \dots, r_s) + (r'_1, \dots, r'_s) &= (r_1 + r'_1, \dots, r_s + r'_s), \\ (r_1, \dots, r_s)(r'_1, \dots, r'_s) &= (r_1 r'_1, \dots, r_s r'_s).\end{aligned}$$

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

Teoreem 4.3. *Kui arvud $n_1, \dots, n_s \in \mathbb{N}$ on paarikaupa ühistegurita ja $n = n_1 \dots n_s$, siis ringid \mathbb{Z}_n ja $\mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_s}$ on isomorfsed.*

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

$$f(\bar{a}) = (\bar{a}_1, \dots, \bar{a}_s),$$

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

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

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

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

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

$$\begin{aligned}f(\bar{a} + \bar{b}) &= f(\overline{a + b}) = (\overline{a + b}_1, \dots, \overline{a + b}_s) = (\bar{a}_1 + \bar{b}_1, \dots, \bar{a}_s + \bar{b}_s) \\ &= (\bar{a}_1, \dots, \bar{a}_s) + (\bar{b}_1, \dots, \bar{b}_s) = f(\bar{a}) + f(\bar{b})\end{aligned}$$

ja analoogiliselt $f(\bar{a}\bar{b}) = f(\bar{a})f(\bar{b})$. Lisaks sellele $f(\bar{1}) = (\bar{1}_1, \dots, \bar{1}_s)$.

Seega f on ringide isomorfism. \square

Lause 4.4. Ringi R pööratavate elementide hulk $U(R)$ on rühm.

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. \square

Lause 4.5. Kui $f : R \rightarrow S$ on ringide R ja S isomorfism, siis $f(U(R)) = U(S)$. Seega $f|_{U(R)}$ 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 $ba = 1$, $a \in U(R)$ ja seega $u = f(a) \in f(U(R))$. Järelikult ka $U(S) \subseteq f(U(R))$. \square

Järeldus 4.6. Kui arvud $n_1, \dots, n_s \in \mathbb{N}$ on paarikaupa ühistegurita ja $n = n_1 \cdot \dots \cdot n_s$, siis rühmad $U(\mathbb{Z}_n)$ ja $U(\mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_s})$ on isomorfsed.

Leiame ringi \mathbb{Z}_n pööratavad elemendid.

Teoreem 4.7. Iga $n > 1$ korral

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

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

Näitame vastupidist sisalduvust. Olgu $(a, n) = 1$. Siis leiduvad sellised $k, l \in \mathbb{Z}$, et $ak + nl = 1$. Järelikult $\bar{1} = \overline{ak + nl} = \overline{ak} + \overline{nl} = \overline{ak} + \overline{0l} = \overline{ak}$. S.t. \bar{a} on pööratav ja seega $\{\bar{a} \in \mathbb{Z}_n \mid (a, n) = 1\} \subseteq U(\mathbb{Z}_n)$. \square

Näide 4.8. Ringi \mathbb{Z}_9 pööratavate elementide hulk

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

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

Lause 4.9. 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 $\overline{ab} = \bar{n} = \bar{0}$, kuid $\bar{a} \neq \bar{0}$ ja $\bar{b} \neq \bar{0}$. Korpuse igal nullist erineval elemendil on olemas pöördelement. Korrutades võrduse $\overline{ab} = \bar{0}$ mõlemad pooled elemendiga $\overline{a^{-1}}$ saame, et $\bar{b} = \bar{0}$, vastuolu. Seega n on algarv.

PHISAVUS. Olgu n algarv. Siis iga $a \in \mathbb{Z}$ korral kas $(a, n) = 1$ või $(a, n) = n$. Viimasel juhul $n \mid a$ ja $\bar{a} = \bar{0}$. Seega kui $\bar{a} \in \mathbb{Z}_n \setminus \{\bar{0}\}$, siis $(a, n) = 1$ ja $\bar{a} \in U(\mathbb{Z}_n)$. Kuna iga nullist erinev element on pööratav, siis \mathbb{Z}_n on korpus. \square

5. Arvuteoreetilisi funktsioone

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

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

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

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

Silmas pidades teoreemi 4.7 saame, et iga $n \geq 2$ korral

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

s.t. $\varphi(n)$ on ringi \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 ühiseid tegureid temast väiksemate naturaalarvudega, siis on ta algarv. Seega saame järgmise väite.

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 valemit, mille abil saaks leida $\varphi(n)$, kui on teada n esitus algarvude astmete korrutisena. Selleks leiame algul 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 $\{1, 2, \dots, p^k\}$ p^{k-1} tükki; nimelt $p, 2p, 3p, \dots, (p^{k-1})p$. Seega hulgas $\{1, 2, \dots, p^k\}$ on täpselt $p^k - p^{k-1}$ arvu, mis on arvuga p^k ühistegurita. \square

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 4.1).

Lause 5.6. *Mistahes ringide R_1, \dots, R_s korral*

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

Märkus 5.7. Selle võrduse vasakul poolel on rühm ja paremal poolel samuti: rühmade $U(R_1), \dots, U(R_s)$ otsekorrutis, mis saadakse kui hulkade otsekorrutisel

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

defineeritakse korrutamise komponenthaaval.

TÕESTUS. Mistahes elementide $r_1 \in R_1, \dots, r_s \in R_s$ korral

$$\begin{aligned} & (r_1, \dots, r_s) \in U(R_1 \times \dots \times R_s) \\ \iff & (\exists (r'_1, \dots, r'_s) \in R_1 \times \dots \times R_s) [(r_1, \dots, r_s)(r'_1, \dots, r'_s) = (r'_1, \dots, r'_s)(r_1, \dots, r_s) = (1, \dots, 1)] \\ \iff & (\exists (r'_1, \dots, r'_s) \in R_1 \times \dots \times R_s) [(r_1 r'_1, \dots, r_s r'_s) = (r'_1 r_1, \dots, r'_s r_s) = (1, \dots, 1)] \\ \iff & (\exists (r'_1, \dots, r'_s) \in R_1 \times \dots \times R_s) (\forall i \in \{1, \dots, s\}) [r_i r'_i = r'_i r_i = 1] \\ \iff & (\forall i \in \{1, \dots, s\}) [r_i \in U(R_i)] \\ \iff & (r_1, \dots, r_s) \in U(R_1) \times \dots \times U(R_s). \end{aligned}$$

\square

Teoreem 5.8. Kui n_1, \dots, n_s on paarikaupa ühistegurita naturaalarvud, siis

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

(Euleri funktsioon on nõrgalt multiplikatiivne).

TÕESTUS. Tähistame $n = n_1 \dots n_s$. Kasutades järeldust 4.6 ja lauset 5.6 saame, et

$$\begin{aligned} \varphi(n) &= |U(\mathbb{Z}_n)| = |U(\mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_s})| = |U(\mathbb{Z}_{n_1}) \times \dots \times U(\mathbb{Z}_{n_s})| \\ &= |U(\mathbb{Z}_{n_1})| \cdot \dots \cdot |U(\mathbb{Z}_{n_s})| = \varphi(n_1) \dots \varphi(n_s). \end{aligned}$$

□

Teoreem 5.9. Kui $n > 1$ ja $n = p_1^{k_1} \dots p_s^{k_s}$ on arvu n standardkuju, siis

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

TÕESTUS. Kuna p_1, \dots, p_s on paarikaupa erinevad algarvud, siis $p_1^{k_1}, \dots, p_s^{k_s}$ on paarikaupa ühistegurita ning seega teoreemist 5.8 ja lausest 5.4 järeldub, et

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

□

Näide 5.10. $\varphi(360) = \varphi(2^3 \cdot 3^2 \cdot 5) = 2^{3-1} \cdot 3^{2-1} \cdot 5^{1-1} (2-1)(3-1)(5-1) = 4 \cdot 3 \cdot 2 \cdot 4 = 96$,
 $\varphi(2002) = \varphi(2 \cdot 7 \cdot 11 \cdot 13) = 6 \cdot 10 \cdot 12 = 720$.

Toome ära veel mõned Euleri funktsiooni omadused.

Lause 5.11. Kui n ja d on naturaalarvud ning $d \mid n$, siis

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

TÕESTUS. Tähistame $\{x \in \mathbb{N} \mid 1 \leq x \leq n, (x, n) = d\} = K$. Siis hulka K kuuluvad arvud peavad jaguma arvuga d . Seega hulka K kuuluvad sellised naturaalarvud $x = kd \in \{d, 2d, \dots, \frac{n}{d}d\} = \{kd \mid k \in \mathbb{N}, 1 \leq k \leq \frac{n}{d}\}$, mis rahuldavad tingimust $(kd, n) = d$. Järeldusest 1.10 saame, et võrdus $(kd, n) = d$ on samaväärne võrdusega $(k, \frac{n}{d}) = 1$. Seega hulka K elemente on niipalju, kuipalju on naturaalarve k , $1 \leq k \leq \frac{n}{d}$, mille korral $(k, \frac{n}{d}) = 1$. Teiselt poolt aga vastavalt Euleri funktsiooni definitsioonile ka $\varphi\left(\frac{n}{d}\right) = |\{k \in \mathbb{N} \mid 1 \leq k \leq \frac{n}{d}, (k, \frac{n}{d}) = 1\}| = |K|$. □

Järgmist Euleri funktsiooni omadust märkas esimesena Gauss.

Teoreem 5.12 (Gauss). Iga naturaalarvu n korral

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

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

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

Hulgad K_1, \dots, K_s on lõikumatud ja $\bigsqcup_{i=1}^s K_i = \{1, 2, \dots, n\}$, sest iga $a \in \{1, 2, \dots, n\}$ korral leidub selline i , et $(a, n) = d_i$. Kasutades seda, et $\{d_1, \dots, d_s\} = \left\{\frac{n}{d_1}, \dots, \frac{n}{d_s}\right\}$ ja lauset 5.11, saame

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

□

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

Teoreem 5.13 (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 4.7 põhjal $\bar{a} \in U(\mathbb{Z}_n)$. Olgu m elemendi \bar{a} järk rühmas $U(\mathbb{Z}_n)$, s.t. tema poolt moodustatud alamrühma $\langle \bar{a} \rangle$ järk, s.o. vähim selline naturaalarv, et $\bar{a}^m = \bar{1}$ ([1], lk. 156, 164). 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 $U(\mathbb{Z}_n)$ saame, et

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

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

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

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

Jällegi, arvutuslikult on pöördelemendi leidmiseks otstarbekam kasutada Eukleidese algoritmi.

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

Teoreem 5.14 (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 5.15. *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 järeldeb, et $a^p \equiv a \pmod{p}$. □

Näide 5.16. Euleri teoreemi rakendusena leiame 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.

Järgnevalt vaatleme Möbiuse funktsiooni.

Definitsioon 5.17. *Möbiuse funktsioon $\mu: \mathbb{N} \rightarrow \mathbb{N}$ defineeritakse võrdusega*

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

Teoreem 5.18. *Kui $n \in \mathbb{N}$, siis*

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

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 $\sum_{d \mid n} \mu(d)$ tulevad nullist erinevad liidetavad ainult $d = 1$ ja selliste jagajate d korral, mis on erinevate algarvude korrutised. Seega

$$\begin{aligned} \sum_{d \mid n} \mu(d) &= \mu(1) + \mu(p_1) + \dots + \mu(p_s) + \mu(p_1 p_2) + \dots + \mu(p_{s-1} p_s) + \dots + \mu(p_1 p_2 \dots p_s) \\ &= 1 + \binom{s}{1}(-1) + \binom{s}{2}(-1)^2 + \dots + \binom{s}{s}(-1)^s = (1-1)^s = 0. \end{aligned}$$

□

Euleri ja Möbiuse funktsioon on seotud järgmise valemi abil.

Teoreem 5.19. Kui $n \in \mathbb{N}$, siis

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

TÕESTUS. Euleri funktsiooni definitsiooni põhjal on ilmne, et

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

Kasutades teoreemi 5.18, 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 $\{1, 2, \dots, n\}$ arvu d kordseid. Kuna neid on $\frac{n}{d}$ tükki, siis

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

□

Vaatleme veel mõningaid arvuteoreetilisi funktsioone.

Definitsioon 5.20. Kui n on naturaalarv, siis tähistagu $\tau(n)$ arvu n kõigi naturaalarvuliste jagajate arvu ning $\sigma(n)$ arvu n kõigi naturaalarvuliste jagajate summat.

Näide 5.21. 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 algteureiks lahutus, siis järgmine teoreem annab lihtsa võimaluse funktsioonide τ ja σ arvutamiseks.

Teoreem 5.22. 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.

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

TÕESTUS. 1. Tänu lausele 1.19 on arvu n jagajaiks need ja ainult need arvud, millel on kuju $p_1^{l_1} \dots p_s^{l_s}$, kus $0 \leq l_i \leq k_i$, $i = 1, \dots, s$. Aritmeetika põhiteoreemi tõttu annavad erinevad astendajate komplektid erinevad n jagajad. Astendaja l_1 valikuks on $k_1 + 1$ võimalust, astendaja l_2 valikuks on $k_2 + 1$ võimalust jne. Seega on arvu 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 (11. veebr. 2002) on teada 39 Mersenne'i algarvu, neist suurim on $2^{13466917} - 1$, millel on 4, 053 946 numbrit. 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

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

kus

$$f(x) = a_k x^k + a_{k-1} x^{k-1} + \dots + a_1 x + a_0 \quad (8)$$

on täisarvuliste kordajatega polünoom muutuja x suhtes ja $a_k \not\equiv 0 \pmod{n}$. Kui $k = 1$, siis kõneldakse lineaarkongruentsidest, kui $k = 2$, 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 3.7 ka kõik arvuga x_0 mooduli n järgi kongruentsed arvud on 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 3.3 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 $\overline{f(x_0)} = \overline{0}$, kus

$$\overline{f(x)} = \overline{a_k} x^k + \overline{a_{k-1}} x^{k-1} + \dots + \overline{a_1} x + \overline{a_0} \in \mathbb{Z}_n[x].$$

Seega kongruentsi (7) lahendamine on samaväärne võrrandi

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

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:

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

Seega antud kongruentsi lahendeiks on jäägiklassid $\overline{2}$ ja $\overline{3}$ mooduli 5 järgi, ehk pisut teistmoodi kirjutades 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

$$\begin{array}{r|rrrrr} \overline{3} & \overline{0} & \overline{2} & \overline{0} & \overline{-1} \\ \hline \overline{2} & \overline{3} & \overline{0 + 2 \cdot 3 = 1} & \overline{2 + 2 \cdot 1 = 4} & \overline{0 + 2 \cdot 4 = 3} & \overline{-1 + 2 \cdot 3 = 0} \end{array}$$

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

6.2. Lineaarkongruentsid

Kõige lihtsamad kongruentsid on lineaarkongruentsid, s.o. kongruentsid kujul

$$ax \equiv b \pmod{n}, \quad (10)$$

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 $(a, n) \mid b$, siis sellel kongruentsil on (a, n) lahendit. Need on

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

kus $n' = \frac{n}{(a, n)}$ ja $\overline{x_0}$ 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 1.7 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 $k \in \{0, \dots, d-1\}$, 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 $\overline{x_0 + in'} = \overline{x_0 + jn'}$, $0 \leq i < j \leq d-1$, 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 leidub selline $k \in \mathbb{Z}$, et $a(x_1 - x_0) = kn$. Jagades viimase võrduse mõlemad pooli arvuga d saame, et $a'(x_1 - x_0) = kn'$. Kuna järelduse 1.10 tõttu $(a', n') = 1$, siis järelduse 1.11 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 $0 \leq r < d$. Järelikult

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

ja seega $\overline{x_1}$ on võrdne ühega lahendeist (11). □

Märkus 6.3. Kongruentsi $a'x \equiv b' \pmod{n'}$ lahend on lause 3.9 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 lahendamiseks 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 mõlemad 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 $\overline{5}^{-1}$. Valemi (6) abil saame

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

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. Põhitulemus on järgmine.

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

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ \dots \\ x \equiv a_s \pmod{n_s} \end{cases} \quad (12)$$

on olemas ühene lahend mooduli n järgi.

Anname sellele teoreemile kaks tõestust.

TÕESTUS 1. Kui n_1, \dots, n_s paarikaupa ühistegurita, siis teoreemi 4.3 tõestuse põhjal kujutus $f : \mathbb{Z}_n \longrightarrow \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_s}$, $f(\overline{a}) = (\overline{a_1}, \dots, \overline{a_s})$, kus $\overline{a_i}$ on arvu a_i jäägiklass mooduli n_i järgi, on ringide isomorfism. Vaatleme elementi $((\overline{a_1})_1, \dots, (\overline{a_s})_s) \in \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_s}$ (siin $(\overline{a_i})_i$ on arvu a_i jäägiklass mooduli n_i järgi). Kujutuse f surjektivsusest järeldub, et leidub selline $a \in \mathbb{Z}$, et $f(\overline{a}) = ((\overline{a_1})_1, \dots, (\overline{a_s})_s)$. Teiselt poolt aga vastavalt f definitsioonile $f(\overline{a}) = (\overline{a_1}, \dots, \overline{a_s})$. Seega $(\overline{a_i})_i = \overline{a_i}$, $i = 1, \dots, s$. 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. $\bar{b}_i = (\bar{a}_i)_i$ ning $f(\bar{a}) = ((\bar{a}_1)_1, \dots, (\bar{a}_s)_s) = (\bar{b}_1, \dots, \bar{b}_s) = f(\bar{b})$. Kujutuse f injektiivsuse tõttu $\bar{a} = \bar{b}$, ehk $a \equiv b \pmod{n}$. \square

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

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

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

$$\bar{k}_i = \bar{m}_i^{-1} \in U(\mathbb{Z}_{n_i}),$$

s.t. sellise $k_i \in \mathbb{Z}$, et $\bar{k}_i \bar{m}_i = \bar{1}$, 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 $i = 1, \dots, s$ 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 $i = 1, \dots, s$ korral $x \equiv a_i \equiv y \pmod{n_i}$ ning kuna n_1, \dots, n_s on paarikaupa ühistegurita, siis lemma 4.2 põhjal $x \equiv y \pmod{n}$. \square

Näide 6.7. Lahendame kongruentside süsteemi

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

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

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

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 $\bar{k}_1 = \bar{m}_1^{-1} = \bar{1}^{-1} = \bar{1}$, ringis \mathbb{Z}_5 $\bar{k}_2 = \bar{m}_2^{-1} = \bar{1}^{-1} = \bar{1}$ ja ringis \mathbb{Z}_3 $\bar{k}_3 = \bar{m}_3^{-1} = \bar{2}^{-1} = \bar{2}$. Seega

$$x = 4 \cdot 1 \cdot 15 + 4 \cdot 1 \cdot 21 + 1 \cdot 2 \cdot 35 = 60 + 84 + 70 = 214$$

ja

$$x \equiv 4 \pmod{105}.$$

Näide 6.8. Lahendame järgmise ülesande, mis on pärit Hiinast, 7. sajandist.

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. Leidke 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 kõigest 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 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 on 119.

6.4. Kongruentsid algarvu astme järgi

Uurime, kuidas lahendada kongruentse

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

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

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

kõik lahendid. Kui $\bar{x}_0 \in \mathbb{Z}_p$ on selle kongruentsi mingi lahend, siis iga täisarvu y korral $f(x_0 + py) \equiv 0 \pmod{p}$. Paneme tähele, et kongruentsi

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

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 $\bar{x}_0 = \{x_0 + py \mid y \in \mathbb{Z}\} \in \mathbb{Z}_p$ korral tuleks leida kõik sellised täisarvud y , mille korral $f(x_0 + py) \equiv 0 \pmod{p^2}$. Kuna Newtoni binoomvalemi põhjal

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

kus $f(x_0) = pm$, $m \in \mathbb{Z}$ (sest $f(x_0) \equiv 0 \pmod{p}$), siis tuleks leida lineaarkongruentsi

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

(muutuja y suhtes), mis on lause 3.9 põhjal samaväärne kongruentsiga

$$f'(x_0) y + m \equiv 0 \pmod{p},$$

lahendid.

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

Näide 6.9. Lahendame kongruentsi

$$4x^3 + 7x^2 - 7x - 10 \equiv 0 \pmod{3^2}. \quad (16)$$

Selle kongruentsi lahendamiseks lahendame kõigepäält kongruentsi

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

ehk

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

Et järelduse 5.15 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 $x_2 \equiv 2 \equiv -1 \pmod{3}$.

Otsime kongruentsi (16) lahendit kujul $x = 1 + 3y$. Asendades kongruentsi (16) saame

$$4(1 + 3y)^3 + 7(1 + 3y)^2 - 7(1 + 3y) - 10 \equiv 0 \pmod{9}$$

ehk

$$4 + 4 \cdot 3 \cdot 3y + 7 + 7 \cdot 2 \cdot 3y - 7 - 7 \cdot 3y - 10 \equiv 0 \pmod{9}.$$

Seega lahendada tuleb lineaarkongruents

$$21y \equiv 6 \pmod{9}$$

ehk

$$7y \equiv 2 \pmod{3},$$

kust saame, et $y \equiv 2 \pmod{3}$. Seega $x = 1 + 3 \cdot 2 = 7$, s.t. $x \equiv 7 \pmod{9}$ on kongruentsi (16) lahend.

Otsime nüüd kongruentsi (16) lahendit kujul $x = -1 + 3y$. Asendades kongruentsi (16) saame

$$4(-1 + 3y)^3 + 7(-1 + 3y)^2 - 7(-1 + 3y) - 10 \equiv 0 \pmod{9}$$

ehk

$$-4 + 4 \cdot 3 \cdot 3y + 7 - 7 \cdot 2 \cdot 3y + 7 - 7 \cdot 3y - 10 \equiv 0 \pmod{9}.$$

Viimasest saame kongruentsi $0 \equiv 0 \pmod{9}$, mis on rahuldatud iga y korral, s.t. $y \equiv 0, 1, 2 \pmod{3}$. Seega kongruentsi (16) 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 (7) lahendamist üldjuhul. Olgu moodul $n = p_1^{k_1} \dots p_s^{k_s}$ antud standardkujul. Asendame selle kongruentsi teatava kongruentside süsteemiga.

Lause 6.10. *Kongruents*

$$f(x) \equiv 0 \pmod{p_1^{k_1} \dots p_s^{k_s}} \tag{17}$$

on samaväärne kongruentside süsteemiga

$$\begin{cases} f(x) \equiv 0 \pmod{p_1^{k_1}} \\ \dots \\ f(x) \equiv 0 \pmod{p_s^{k_s}} \end{cases} \tag{18}$$

(s.t. neil on samad lahendid).

TÕESTUS. Kui $f(x_0) \equiv 0 \pmod{p_1^{k_1} \dots p_s^{k_s}}$, siis $p_1^{k_1} \dots p_s^{k_s} \mid f(x_0)$. Kuid siis ka iga $i = 1, \dots, s$ korral $p_i^{k_i} \mid f(x_0)$, ehk $f(x_0) \equiv 0 \pmod{p_i^{k_i}}$. Seega kongruentsi (17) iga lahend on ka süsteemi (18) lahend.

Näitame vastupidist. Oletame, et x_0 rahuldab süsteemi (18), s.t. iga $i = 1, \dots, s$ korral $p_i^{k_i} \mid f(x_0)$. Kuna iga $i \neq j$ korral $(p_i^{k_i}, p_j^{k_j}) = 1$, siis lemma 4.2 põhjal ka $p_1^{k_1} \dots p_s^{k_s} \mid f(x_0)$, ehk $f(x_0) \equiv 0 \pmod{p_1^{k_1} \dots p_s^{k_s}}$. \square

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

$$\begin{cases} x \equiv x_1 \pmod{p_1^{k_1}} \\ \dots \\ x \equiv x_s \pmod{p_s^{k_s}} \end{cases} \tag{19}$$

iga lahend on ka süsteemi (18) lahend. Ka vastupidi, kui x_0 on süsteemi (18) lahend, siis ta peab iga $i = 1, \dots, s$ korral mooduli $p_i^{k_i}$ järgi olema kongruentne kongruentsi $f(x) \equiv 0 \pmod{p_i^{k_i}}$ mingi lahendiga x_i . Niisiis, kui me oskaksime lahendada kongruentse $f(x) \equiv 0 \pmod{p_i^{k_i}}$, siis süsteemi (18) (ja seega kongruentsi (17)) kõik lahendid saame, kui lahendame Hiina jäägiteoreemi abil kõikvõimalikud süsteemid (19), kus iga $i = 1, \dots, s$ korral x_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 (17)) lahendeid on $r_1 r_2 \dots r_s$ tükki.

Näide 6.11. Lahendame kongruentsi

$$4x^3 + 7x^2 - 7x - 10 \equiv 0 \pmod{225}. \quad (20)$$

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

$$4x^3 + 7x^2 - 7x - 10 \equiv 0 \pmod{3^2} \quad (21)$$

$$4x^3 + 7x^2 - 7x - 10 \equiv 0 \pmod{5^2} \quad (22)$$

lahendamisele. Esimene neist kongruentsidest on lahendatud näites 6.9.

Asume kongruentsi (22) 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 $x \equiv 4 \pmod{5}$.

Otsime kongruentsi (22) lahendit kujul $x = 5y$. Asendades kongruentsi (22) saame

$$4(5y)^3 + 7(5y)^2 - 7(5y) - 10 \equiv 0 \pmod{25}$$

ehk $-10y - 10 \equiv 0 \pmod{25}$. Seega $2y \equiv -2 \pmod{5}$, s.t. $y \equiv 4 \pmod{5}$, ning $x \equiv 20 \pmod{25}$ on kongruentsi (22) lahend.

Otsime kongruentsi (22) lahendit kujul $x = 3 + 5y$. Asendades kongruentsi (22) saame

$$4(3 + 5y)^3 + 7(3 + 5y)^2 - 7(3 + 5y) - 10 \equiv 0 \pmod{25}$$

ehk

$$4 \cdot 3^3 + 4 \cdot 3 \cdot 3^2 \cdot 5y + 7 \cdot 3^2 + 7 \cdot 2 \cdot 3 \cdot 5y - 7 \cdot 3 - 7 \cdot 5y - 10 \equiv 0 \pmod{25}.$$

Seega lahendada tuleb lineaarkongruents $-10y - 10 \equiv 0 \pmod{25}$ ehk jällegi $y \equiv 4 \pmod{5}$. Seega $x \equiv 23 \pmod{25}$ on kongruentsi (22) lahend.

Otsime kongruentsi (22) lahendit kujul $x = 4 + 5y$. Asendades kongruentsi (22) saame

$$4(4 + 5y)^3 + 7(4 + 5y)^2 - 7(4 + 5y) - 10 \equiv 0 \pmod{25}$$

ehk

$$4 \cdot 4^3 + 4 \cdot 3 \cdot 4^2 \cdot 5y + 7 \cdot 4^2 + 7 \cdot 2 \cdot 4 \cdot 5y - 7 \cdot 4 - 7 \cdot 5y - 10 \equiv 0 \pmod{25}.$$

Seega lahendada tuleb lineaarkongruents $5y + 5 \equiv 0 \pmod{25}$ ehk $y \equiv 4 \pmod{5}$. Seega $x \equiv 24 \pmod{25}$ on kongruentsi (22) lahend.

Saime, et kongruentsi (21) lahendeiks on $x \equiv 2, 5, 7, 8 \pmod{9}$ ja kongruentsi (22) lahendeiks $x \equiv 20, 23, 24 \pmod{25}$. Seega kongruentsil (20) on 12 lahendit. Need saame, kui Hiina jäägiteoreemi abil lahendame 12 lineaarkongruentside süsteemi. 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 (20) 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. Nii tehes saame lahendeiks $x \equiv 20, 23, 70, 74, 95, 98, 124, 149, 170, 173, 223, 224 \pmod{225}$.

7. Alguured

Meenutame, et lõpliku rühma *järguks* nimetatakse tema elementide arvu. Kui G on lõplik rühm ja $a \in G$, siis elemendi a *järguks* nimetatakse vähimat astendajat $k \in \mathbb{N}$, mille korral $a^k = 1$, kus 1 on selle rühma ühikelement. Lagrange'i teoreemi põhjal on lõpliku rühma elemendi järk rühma järgu jagaja. Rühma nimetatakse *tsükliliseks*, kui leidub selline element, mille astmetena avalduvad kõik selle rühma elemendid. Sellist elementi nimetatakse tsüklilise rühma *moodustajaks*.

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

Definitsioon 7.1. Täisarvu a nimetatakse *alguureks* mooduli n järgi, kui \bar{a} on rühma $U(\mathbb{Z}_n)$ moodustaja, s.t. kui $U(\mathbb{Z}_n) = \{\bar{a}, \bar{a}^2, \dots, \bar{a}^{\varphi(n)-1}, \bar{a}^{\varphi(n)} = \bar{1}\}$.

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 7.2. Kui $n = 2$, siis $U(\mathbb{Z}_2) = \{\bar{1}\}$ on tsükliline rühm. Kui $n = 3$, siis $U(\mathbb{Z}_3) = \{\bar{1}, \bar{2}\} = \{\bar{2}, \bar{2}^2\}$ on tsükliline rühm moodustajaga $\bar{2}$, seega 2 on algjuur mooduli 3 järgi. Kui $n = 4$, siis $U(\mathbb{Z}_4) = \{\bar{1}, \bar{3}\} = \{\bar{3}, \bar{3}^2\}$ on tsükliline rühm moodustajaga $\bar{3}$, seega 3 on algjuur mooduli 4 järgi. Kui $n = 5$, siis $U(\mathbb{Z}_5) = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\} = \{\bar{2}, \bar{2}^2, \bar{2}^3, \bar{2}^4\} = \{\bar{3}, \bar{3}^2, \bar{3}^3, \bar{3}^4\}$ on tsükliline rühm, seega 2 ja 3 on algjuured mooduli 5 järgi. Kui $n = 8$, siis $U(\mathbb{Z}_8) = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ ja $\bar{1}^2 = \bar{1}, \bar{3}^2 = \bar{1}, \bar{5}^2 = \bar{1}, \bar{7}^2 = \bar{1}$, 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. Selleks tõestame esialgu paar abitulemust rühmade kohta.

Lemma 7.3. Olgu G rühm, $a \in G$, olgu elemendi a 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 $0 \leq r < m$. 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 $r = 0$. Seega $l = qm$, ehk $m \mid l$.

PIISAVUS. Kui leidub selline $k \in \mathbb{N}$, et $mk = l$, siis $a^l = (a^m)^k = 1$. □

Lemma 7.4. Paarisarvulise järguga rühmas leidub element, mille järk on kaks.

TÕESTUS. Olgu rühma G järk paarisarv. Kui rühmas G ei ole elementi, mille järk on kaks, s.t. ühegi elemendi $1 \neq a \in G$ korral $a^2 \neq 1$ ehk $a \neq a^{-1}$, siis kõik G ühikelemendid erinevad elemendid jagunevad lõikumatuks paarideks $\{a, a^{-1}\}$. Seega G järk on paaritu arv, vastuolu. Järelikult kui G järk on paarisarv, siis peab leiduma vähemalt üks teist järku element. □

Lemma 7.5. 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 $G = \{1, a, a^2, \dots, a^{2m-1}\}$. 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 $1 \leq l \leq 2m - 1$, järk on 2, s.t. $(a^l)^2 = a^{2l} = 1$. Siis lemma 7.3 tõttu $2m \mid 2l$, ehk $m \mid l$. Kuna $m \leq l < 2m$ ja $m \mid l$, siis $m = l$ ja $a^m = a^l$. □

Teoreemist 5.9 järgneb lihtsalt järgmine väide.

Lemma 7.6. Mistahes naturaalarvu $n > 2$ korral on $\varphi(n)$ paarisarv.

Pöördume tagasi küsimuse juurde, millal leidub mooduli n järgi algjuuri.

Olgu $n = p_1^{k_1} \dots p_s^{k_s}$ arvu $n > 1$ standardkuju. Järelduse 4.6 ja lause 5.6 põhjal kehtib rühmade isomorfism

$$U(\mathbb{Z}_n) \cong U(\mathbb{Z}_{p_1^{k_1}}) \times \dots \times U(\mathbb{Z}_{p_s^{k_s}}).$$

Oletame, et leiduvad erinevad $i, j \in \{1, \dots, s\}$, nii et p_i ja p_j on paaritud algarvud. Üldsust kitsendamata eeldame, et $i = 1$ ja $j = 2$. Järelikult lemma 7.6 põhjal on $U(\mathbb{Z}_{p_1^{k_1}})$ ja $U(\mathbb{Z}_{p_2^{k_2}})$ paarisarvulist järku rühmad ning

seega leiduvad lemma 7.4 põhjal teist järku elemendid $\bar{a} \in U(\mathbb{Z}_{p_1^{k_1}})$ ja $\bar{b} \in U(\mathbb{Z}_{p_2^{k_2}})$. Siis ka elemendid $(\bar{a}, \bar{1}, \bar{1}, \dots, \bar{1})$, $(\bar{1}, \bar{b}, \bar{1}, \dots, \bar{1}) \in U(\mathbb{Z}_{p_1^{k_1}}) \times \dots \times U(\mathbb{Z}_{p_s^{k_s}})$ on teist järku ja seega lemma 7.5 põhjal rühm $U(\mathbb{Z}_n)$ ei saa olla tsükliline.

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

Lõpuks oletame, et $n = 2^k$, kus $k \geq 3$. Siis $U(\mathbb{Z}_{2^k})$ 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 $k \geq 3$, siis $1 < 2^{k-1} - 1 < 2^k$ ja $1 < 2^{k-1} + 1 < 2^k$, seega $\overline{2^{k-1} - 1} \neq \overline{2^{k-1} + 1}$. Lisaks sellele

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

s.t. need elemendid on teist järku. Ning kuna $k \geq 3$, siis $2 \not\equiv 0 \pmod{2^k}$ ning seetõttu $\overline{2^{k-1} - 1} \not\equiv \overline{2^{k-1} + 1} \pmod{2^k}$, 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 7.7. *Kui mooduli n järgi leidub algjuuri, siis n on kujul $2, 4, p^k$ või $2p^k$, kus $p > 2$ on algarv.*

Näitame nüüd, et kui arvul n on eespoolmainitud kuju, siis mooduli n järgi leidub algjuuri.

Esimese asjana peaksime näitama, et jäägiklassikorpuse \mathbb{Z}_p multiplikatiivne rühm $U(\mathbb{Z}_p)$ on tsükliline. Osutub, et selline omadus on mitte ainult jäägiklassikorpustel, vaid ka kõigil teistel lõplikel korpustel.

Teoreem 7.8. *Iga lõpliku (kommutatiivse¹) 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 $K^* = \sqcup_{d|q-1} K_d$. Gaussi teoreemi (teoreem 5.12) põhjal

$$\sum_{d|q-1} \varphi(d) = q - 1 = |K^*| = \sum_{d|q-1} |K_d|. \quad (23)$$

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

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

$$K_d = \{a^k \mid 1 \leq k \leq d, (k, d) = 1\}. \quad (24)$$

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

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

sest $(a^k)^d = (a^d)^k = \mathbf{1}$ iga $k = 1, \dots, d$ korral. Kuna d . astme polünoomil üle korpuse K ei saa lause 2.8 põhjal olla rohkem kui d juurt korpuses K , siis a, a^2, \dots, 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 $b^{\frac{d}{d'}} = (a^k)^{\frac{d}{d'}} = (a^d)^{\frac{k}{d'}} = \mathbf{1}$ ja $\frac{d}{d'} < d$. Sellega oleme tõestanud, et $K_d \subseteq \{a^k \mid 1 \leq k \leq d, (k, d) = 1\}$. Oletame nüüd, et $1 \leq k \leq d$, $(k, d) = 1$ ja elemendi a^k järk on $m \leq d$. Siis $a^{mk} = (a^k)^m = \mathbf{1}$. Kuna a järk on d , siis lemma 7.3 põhjal $d | mk$. Seega järelduse 1.11 põhjal $d | m$, mis koos võrratusega $m \leq d$ annab, et $m = d$, s.t. $a^k \in K_d$. Sellega oleme tõestanud võrduse (24).

Niisiis iga $d | q - 1$ korral kas $|K_d| = \varphi(d)$ või $K_d = \emptyset$. Tänu võrdusele (23) ei ole aga viimane võrdus võimalik. Seega iga $d | q - 1$ korral on täpselt $\varphi(d)$ elementi, mille järk on d . Muuhulgas, kuna $q - 1 | q - 1$, siis leidub $\varphi(q - 1)$ elementi, mille järk on $q - 1$, s.o. leidub $\varphi(q - 1)$ rühma K^* moodustajat. Kui a on mingi moodustaja, siis ülejäänud moodustajaiks on eespooltõestatu põhjal astmed a^k , kus $1 \leq k \leq q - 1$ ja $(k, q - 1) = 1$. \square

Järeldus 7.9. *Kui p on algarv, siis mooduli p järgi leidub algjuuri.*

TÕESTUS. Teoreemi 7.8 põhjal leidub $\varphi(p - 1) \geq 1$ rühma $\mathbb{Z}_p^* = U(\mathbb{Z}_p)$ moodustajat. \square

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

¹ Iga lõplik korpus on Wedderburni teoreemi (vt. [11], teoreem 1.3.10) tõttu kommutatiivne.

Teoreem 7.10. Olgu p 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 $\bar{a} \in U(\mathbb{Z}_p)$, s.t. $p \nmid a$ ning \bar{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 $(p^2, a) = 1 = (p^2, a + p)$, mis tähendab, et $\bar{a}, \overline{a + p} \in U(\mathbb{Z}_{p^2})$. Tuleb näidata, et kas \bar{a} või $\overline{a + p}$ järk rühmas $U(\mathbb{Z}_{p^2})$ on $|U(\mathbb{Z}_{p^2})| = \varphi(p^2) = p(p - 1)$. Olgu m elemendi \bar{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. $\bar{a}^m = \bar{1}$ rühmas $U(\mathbb{Z}_p)$. Seega lemma 7.3 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 $p - 1$ taandamisel saame, et $uv = p$ ehk $u = p$ või $v = p$ (sest p on algarv). Seega 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 $\bar{a} = \overline{a + p}$. Seetõttu saame $\overline{a + p}$ jaoks läbi viia sama arutelu, mis \bar{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, et nii \bar{a} kui ka $\overline{a + p}$ järk rühmas $U(\mathbb{Z}_{p^2})$ on $p - 1$, s.t. $a^{p-1} \equiv 1 \pmod{p^2}$ ja $(a + p)^{p-1} \equiv 1 \pmod{p^2}$. Kasutades Newtoni binoomvalemit saame siis, et

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

millest saame, et $(p - 1)a^{p-2}p \equiv 0 \pmod{p^2}$. Lause 3.9 põhjal $(p - 1)a^{p-2} \equiv 0 \pmod{p}$ ehk $p \mid (p - 1)a^{p-2}$. Kuna p on algarv, siis $(p, p - 1) = 1$ ning järelikult $p \mid a$, vastuolu. Seega peab kas elemendi \bar{a} või $\overline{a + p}$ 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. \square

Järeldus 7.11. Kui p 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 7.12. Leiame mingi algjuure mooduli 25 järgi. Nagu eespool nägime on üheks algjuureks mooduli 5 järgi arv 2. Järelduse 7.11 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 $\bar{7}^2 = \overline{49} = \overline{-1}$, siis $\bar{7}^4 = \overline{-1}^2 = \bar{1}$, s.t. elemendi $\bar{7}$ järk rühmas $U(\mathbb{Z}_{5^2})$ on 4. Seega algjuureks mooduli 25 järgi peab olema 2.

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

Lemma 7.13. Kui p on algarv ja $1 \leq k \leq p - 1$ on naturaalarv, siis p jagab binoomkordajat $\binom{p}{k}$.

TÕESTUS. Definiitsiooni 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 $p \mid \binom{p}{k}$. \square

Teoreem 7.14. 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

$$\text{iga } l \in \mathbb{N} \text{ korral leidub } t_l \in \mathbb{Z} \text{ nii, et } a^{(p-1)p^{l-1}} = 1 + t_l p^l \text{ ja } p \nmid t_l. \quad (25)$$

Vaatleme kõigepäält juhtu $l = 1$. Kuna a on algjuur mooduli p^2 järgi, siis $\bar{a} \in U(\mathbb{Z}_{p^2})$ ja seega $p \nmid a$. Fermat' väikse 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 $\bar{a}^{p-1} = \bar{1}$ 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

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

kus $t_l = t_{l-1} + \binom{p}{2} t_{l-1}^2 p^{2(l-1)-l} + \dots + \binom{p}{p-1} t_{l-1}^{p-1} p^{(p-1)(l-1)-l} + t_{l-1}^p p^{p(l-1)-l}$ ja p^l sulgude taha võtmisel oleme arvestanud, et iga $m \geq 2$ korral $m(l-1) - l = m(l-1) - l + 1 - 1 = (m-1)(l-1) - 1 \geq 0$. Kuna $p > 2$, siis $p(l-1) - l = (p-1)(l-1) - 1 \geq 1$ ja seega $p \mid t_{l-1}^p p^{p(l-1)-l}$. Lisaks sellele, lemma 7.13 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 (25) on tõestatud.

Olgu m elemendi \bar{a} järk rühmas $U(\mathbb{Z}_{p^k})$. Siis $\bar{a}^m = \bar{1}$ ehk $a^m \equiv 1 \pmod{p^k}$ ja $m \mid |U(\mathbb{Z}_{p^k})| = \varphi(p^k) = (p-1)p^{k-1}$. Tuleb näidata, et $m = (p-1)p^{k-1}$. Kuna $a^m \equiv 1 \pmod{p^k}$, siis ka $a^m \equiv 1 \pmod{p}$, järelikult lemma 7.3 põhjal $p-1 \mid m$ (sest \bar{a} järk rühmas $U(\mathbb{Z}_p)$ on $p-1$). Niisiis leiduvad sellised $u, v \in \mathbb{Z}$, et $mu = (p-1)p^{k-1}$ ja $(p-1)v = m$ ning seega $(p-1)p^{k-1} = (p-1)vu$. Taandades $p-1$ saame, et $p^{k-1} = vu$. Seega $v = p^{r-1}$, kus $1 \leq r \leq k$, 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 $k \leq r$. Teisest küljest aga $r \leq k$. Seega kokkuvõttes $r = k$ ja $m = (p-1)p^{k-1}$. \square

Teoreem 7.15. *Kui a on algjuur mooduli p^k järgi, kus $p > 2$ on algarv, siis algjuureks mooduli $2p^k$ järgi on paaritu arv arvudest a ja $a + p^k$.*

TÕESTUS. Kuna p^k on paaritu arv, siis üks arvudest a ja $a + p^k$ peab olema 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 $\bar{a} \in U(\mathbb{Z}_{p^k})$, millest järeldub, et $(a, p^k) = 1$. Kuna a on paaritu, siis ka $(a, 2) = 1$ ja seega $(a, 2p^k) = 1$, s.t. $\bar{a} \in U(\mathbb{Z}_{2p^k})$. Sellest, et a on algjuur mooduli p^k järgi, järeldub, et elemendi \bar{a} järk rühmas $U(\mathbb{Z}_{p^k})$ on $m = |U(\mathbb{Z}_{p^k})| = p^{k-1}(p-1)$. Olgu n elemendi \bar{a} järk rühmas $U(\mathbb{Z}_{2p^k})$. Siis $n \mid |U(\mathbb{Z}_{2p^k})| = p^{k-1}(p-1) = |U(\mathbb{Z}_{p^k})| = m$, järelikult $n \leq m$. Teiselt poolt aga sellest, et $a^n \equiv 1 \pmod{2p^k}$ järeldub, et $a^n \equiv 1 \pmod{p^k}$ ja seega lemma 7.3 põhjal $m \leq n$. Oleme saanud, et $n = m$, mida oligi tarvis tõestada. \square

Tehtu võime kokku võtta järgmise teoreemina.

Teoreem 7.16. *Mooduli n järgi leidub algjuuri parajasti siis, kui n on kujul $2, 4, p^k$ või $2p^k$, kus $p > 2$ on algarv.*

Teoreemid 7.10, 7.14 ja 7.15 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.

Olgu G rühm ning $|G| = p_1^{k_1} \dots p_s^{k_s} = n$, kus p_1, \dots, p_s on paarikaupa erinevad algarvud.

Lemma 7.17. *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 $0 \leq l_i \leq k_i$. 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 lemma 7.3 põhjal a järk on väiksem kui n ning järelikult $\langle a \rangle \neq G$. \square

Järeldus 7.18. *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 7.19. *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 7.18 juhul $G = U(\mathbb{Z}_p)$. \square

Näide 7.20. 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.

Teoreem 7.21. *Kui mooduli n järgi leidub algjuuri, siis on nende arv $\varphi(\varphi(n))$.*

TÕESTUS. Olgu a algjuur mooduli n järgi. Siis $U(\mathbb{Z}_n) = \{\bar{1}, \bar{a}, \bar{a}^2, \dots, \bar{a}^{\varphi(n)-1}\}$. Olgu $|U(\mathbb{Z}_n)| = \varphi(n) = p_1^{k_1} \dots p_s^{k_s}$, kus p_1, \dots, p_s on paarikaupa erinevad algarvud. Näitame, et $a^k, 1 \leq k \leq \varphi(n) - 1$, on algjuur parajasti siis, kui $(k, \varphi(n)) = 1$ (sellest järeldubki, et algjuurte arv on $\varphi(\varphi(n))$). Selleks näitame, et

$$\langle \bar{a}^k \rangle \neq U(\mathbb{Z}_n) \text{ parajasti siis, kui } (k, \varphi(n)) \neq 1.$$

Oletame, et $\langle \bar{a}^k \rangle \neq U(\mathbb{Z}_n)$. Lemma 7.17 põhjal leidub siis selline p_i , et $(\bar{a}^k)^{\frac{\varphi(n)}{p_i}} = \bar{1}$ rühmas $U(\mathbb{Z}_n)$. Lemma 7.3 põhjal $\varphi(n) \mid \frac{k\varphi(n)}{p_i}$, s.t. leidub selline $u \in \mathbb{N}$, et $\varphi(n)u = \frac{k\varphi(n)}{p_i}$. Järelikult $up_i = k$, millest saame, et $p_i \mid k$. Seega $(k, \varphi(n)) \geq p_i > 1$. Vastupidi, oletame, et $(k, \varphi(n)) = d > 1$. Siis leidub selline p_i , et $p_i \mid d$. Järelikult ka $p_i \mid k$. Olgu $k = p_i k'$. Siis $(\bar{a}^k)^{\frac{\varphi(n)}{p_i}} = \bar{a}^{k'\varphi(n)} = \bar{1}$ ning lemma 7.17 põhjal $\langle \bar{a}^k \rangle \neq U(\mathbb{Z}_n)$. \square

8. Lõplikud korpused

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

8.1. 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

$$ma = \underbrace{a + a + \dots + a}_m \text{ liidetavat}$$

$0a = \mathbf{0}$ ning $(-m)a = -(ma)$. Lihtne on näha, et nii defineeritud korpuse elemendi kordsete 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 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 $\text{char}K = p$. Definiitsioonist järeldub, et kui $\text{char}K = p$, 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 8.1. *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 $(k\mathbf{1}) \cdot (l\mathbf{1}) = (kl)\mathbf{1} = p\mathbf{1} = \mathbf{0}$. Korrutades seda võrdust elemendiga $(k\mathbf{1})^{-1}$ saame vastuolu $l\mathbf{1} = \mathbf{0}$. Seega p on algarv. \square

Definiitsioon 8.2. Kui korpus K on korpuse L alamkorpus, siis öeldakse, et korpus L on korpuse K *laiend*.

Lause 8.3. *Korpuse iga laiendi karakteristika on võrdne selle korpuse karakteristikaga.*

TÕESTUS. Olgu L korpuse K laiend ja $\text{char}K = p$. 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 ka tema järk rühmas $(L, +)$ on p ja seega $\text{char}L = p$. \square

Teoreem 8.4. *Lõpliku korpuse elementide arv on algarvu aste.*

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

$$P = \{\mathbf{1}, \mathbf{1} + \mathbf{1}, \mathbf{1} + \mathbf{1} + \mathbf{1}, \dots, (p-1)\mathbf{1}, p\mathbf{1} = \mathbf{0}\} = \{m\mathbf{1} \mid m \in \mathbb{Z}\} \subseteq K.$$

Kuna mistahes $k, l \in \{1, \dots, p\}$ 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 $\bar{u} = \bar{k}^{-1}$ korpuses \mathbb{Z}_p), siis P on korpuse K alamkorpus. Korpus P on isomorfne korpusega \mathbb{Z}_p , kusjuures isomorfismi realiseerib kujutus $f : P \rightarrow \mathbb{Z}_p$,

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

Korpust K võib vaadelda (lõpliku) vektorruumina üle korpuse P : liitmine on korpuse K liitmine ning vektori $a \in K$ ja skalaari $k\mathbf{1} \in P$ korrutise defineerime võrdusega

$$(k\mathbf{1})a = ka.$$

Selles, et tõesti kõik vektorruumi aksioomid on täidetud, pole raske veenduda.

On hästi teada, et igas lõplikumõõtmelises vektorruumis on olemas baas ([1], teoreem 3.2.3). Olgu e_1, \dots, e_n baas vektorruumis K üle korpuse P . Siis iga $a \in K$ esitub üheselt lineaarkombinatsioonina $a = \alpha_1 e_1 + \dots + \alpha_n e_n$, kus $\alpha_1, \dots, \alpha_n \in P$. Selliseid lineaarkombinatsioone on p^n tükki. Seega $|K| = p^n$. \square

Selle teoreemi tõestuse käigus näitasime, et kehtib järgmine väide.

Järeldus 8.5. Kui korpuse K karakteristika on p , siis see korpus sisaldab jäägiklassikorpusega \mathbb{Z}_p isomorfse alamkorpuse.

Edasises läheb meil vaja järgmisi abitulemusi.

Lemma 8.6. Kui 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 7.13 põhjal mistahes i , $1 \leq i \leq p - 1$, korral $p \mid \binom{p}{i}$, s.t. leidub $k_i \in \mathbb{N}$ nii, et $k_i p = \binom{p}{i}$. Järelikult iga i , $1 \leq i \leq p - 1$, 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 $(a + b)^p = a^p + b^p$, s.t. kehtib induktsiooni alus.

Oletame nüüd, et $(a + b)^{p^k} = a^{p^k} + b^{p^k}$. Siis 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 8.7. Kui K on lõplik korpus ning $|K| = q$, siis iga $a \in K^* = K \setminus \{0\}$ korral $a^{q-1} = 1$.

TÕESTUS. Olgu m elemendi a järk korpuse K multiplikatiivses rühmas K^* . Siis $m \mid q - 1 = |K^*|$. Olgu $mk = q - 1$. Siis $a^{q-1} = a^{mk} = (a^m)^k = 1$. □

Teoreemi 7.8 põhjal on lõpliku korpuse multiplikatiivne rühm tsükliline. Selle rühma moodustajaid nimetatakse korpuse *primitiivseteks elementideks*. (Näiteks korpuse \mathbb{Z}_p primitiivsed elemendid on algjuured mooduli p järgi.) Olgu L korpuse K laiend, kusjuures $|K| = q$ ja $|L| = q^m$, $m \in \mathbb{N}$. Kui $b \in L$, siis elemente

$$b, b^q, b^{q^2}, \dots, b^{q^{m-1}}$$

nimetatakse elemendi b *kaaselementideks* korpuse K suhtes.

Lause 8.8. Elemendi $b \in L^*$ kaaselementidel q^m -elemendilise korpuse L q -elemendilise alamkorpuse K suhtes on sama järk rühmas L^* .

TÕESTUS. Olgu $b, b^q, b^{q^2}, \dots, b^{q^{m-1}}$ elemendi $b \in L^*$ kaaselemendid alamkorpuse K suhtes. Olgu a korpuse L primitiivne element. Siis leidub selline k , et $b = a^k$. Saab tõestada, et kui G on s . järku tsükliline rühm moodustajaga g , siis elemendi g^k järk on $\frac{s}{(k, s)}$. Kuna iga $l \in \{0, \dots, m - 1\}$ korral $(q^l, q^m - 1) = 1$, siis elemendi $b^{q^l} = a^{kq^l}$ järk on $\frac{q^m - 1}{(kq^l, q^m - 1)} = \frac{q^m - 1}{(k, q^m - 1)}$ ja seega ei sõltu l -st. □

Järeldus 8.9. Kui a on korpuse L primitiivne element, siis tema kaaselemendid mistahes alamkorpuse suhtes on samuti primitiivsed.

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 pääideaali tähistame $\langle p(x) \rangle$. Seega

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

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

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

Muuhulgas $[0] = \langle p(x) \rangle = [p(x)]$. Tihti kõrvalklassid samastatakse nende esindajatega ja kirjutatakse $[f(x)]$ asemel lihtsalt $f(x)$. Saab näidata, et

$$[f(x)] = [g(x)] \iff f(x) - g(x) \in \langle p(x) \rangle \iff p(x) \mid f(x) - g(x). \quad (26)$$

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 $K[x]$ faktoringiks ideaali $\langle p(x) \rangle$ järgi (vt. [1], lk. 169) ja tähistatakse $K[x]/\langle p(x) \rangle = \{[f(x)] \mid f(x) \in K[x]\}$.

Mittekonstantset polünoomi $p(x)$ nimetatakse *taandumatuks*, kui ta ei esitu mittekonstantsete polünoomide korrutisena, s.t. kui võrdusest $p(x) = f(x)g(x)$ järeldub, et kas polünoom $f(x)$ on konstantne või $g(x)$ on konstantne.

Järgmised kaks väidet on tõestatud raamatus [1], lk 217–219.

Lause 8.10. *Olgu K kommutatiivne korpus ja $p(x) \in K[x]$ taandumatu polünoom, mille aste $d \geq 2$. Siis faktoring $L = K[x]/\langle p(x) \rangle$ on korpus, mis sisaldab korpusega K isomorfset alamkorpust ning milles polünoomil $p(x)$ on olemas juur. Seejuures kui $|K| = p^m$, siis $|L| = p^{md}$.*

Olgu

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

ringi $K[x]$ faktoringi ideaali $\langle p(x) \rangle$ järgi. 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

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

Näitame, et $\{[f(x)] \mid f(x) \in K[x]\} \subseteq \{[f(x)] \mid f(x) \in K[x], \deg f(x) < d\}$. Vöttes $g(x) \in K[x]$ võime selle polünoomi jagada jäägiga polünoomiga $p(x)$, s.t. leida $q(x), r(x) \in K[x]$, nii et

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

Järelikult $[g(x)] = [p(x)][q(x)] + [r(x)] = [0][q(x)] + [r(x)] = [r(x)] \in \{[f(x)] \mid f(x) \in K[x], \deg f(x) < d\}$. Vastupidine sisalduvus on ilmne. Seega iga kõrvalklassi esindajaks saab valida sellise polünoomi, mille aste on väiksem kui d :

$$L = \{[k_{d-1}x^{d-1} + \dots + k_1x + k_0] \mid k_0, \dots, k_{d-1} \in K\}. \quad (27)$$

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 $\deg g < d$, 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 (26) põhjal $[f(x)] \neq [g(x)]$. Sellega oleme tõestanud, et $|L| = p^{md}$.

Teoreem 8.11. *Olgu $f(x) \in K[x]$ polünoom kordajatega kommutatiivsest korpusest K ning olgu $f(x)$ aste $n \geq 1$. Siis leidub korpuse K selline laiend L , milles polünoomil $f(x)$ on n juurt.*

Kui need juured on $a_1, \dots, a_n \in L$, siis $f(x)$ lahutub lineaartegurite korrutiseks üle korpuse L :

$$f(x) = b(x - a_1) \dots (x - a_n), \quad \text{kus } b \in K \text{ on } x^n \text{ kordaja polünoomis } f(x).$$

Definitsioon 8.12. Korpuse K laiendit L nimetatakse polünoomi $f(x) \in K[x]$ lahutuskorpuseks, kui $f(x)$ lahutub lineaartegurite korrutiseks üle L ,

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

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

Teoreem 8.11 ütleb, et igal mittekonstantsel polünoomil üle kommutatiivse korpuse on lahutuskorpus olemas. Veelgi enam, kehtib järgmine teoreem, mida me siinkohla ei tõesta (vt. [12], lk. 343–350).

Teoreem 8.13. *Polünoomi lahutuskorpus on isomorfismi täpsuseni üheselt määratud.*

Teoreem 8.4 väitis, et lõpliku korpuse elementide arv on algarvu aste. Järgnevalt veendume, et kehtib ka selle teoreemi pöördteoreem.

Teoreem 8.14. *Iga algarvu p ja naturaalarvu n korral leidub korpus, milles on p^n elementi. See korpus on isomorfismi täpsuseni üheselt määratud.*

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 korpuse L karakteristik on 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 $k \geq 2$ ja $g(x) \in L[x]$. Siis korrutise tuletise reegli põhjal

$$(x^q - x)' = k(x - a)^{k-1}g(x) + (x - a)^k g'(x) = (x - a) [k(x - a)^{k-2}g(x) + (x - a)^{k-1}g'(x)].$$

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, s.t. 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 8.6 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 $a = -a$. Kui aga $p > 2$, siis

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

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.

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

Ühesuse näitamiseks paneme tähele, et mistahes q -elemendiline korpuse L' korral on lemma 8.7 tõttu kõik tema elemendid polünoomi $x^q - x \in \mathbb{Z}_p[x]$ juured. Kuna sellel polünoomil ei saa olla üle q juure, siis on L selle polünoomi lahutuskorpus. Kuna polünoomi mistahes kaks lahutuskorpus on isomorfsed, siis on ka korpus L' isomorfnine korpusele L . \square

Korpus, milles on $q = p^n$ elementi, tähistatakse tihti kas \mathbb{F}_q või $\text{GF}(q)$ ($\text{GF} = \text{Galois field}$). Sellise korpuse konstrueerimiseks võime kasutada lauset 8.10. Võtame näiteks korpuse \mathbb{Z}_p , leiame mingi n . astme taandumatu polünoomi üle \mathbb{Z}_p ning moodustame faktoringi $\mathbb{Z}_p[x]/\langle p(x) \rangle$. Tulemus on p^n -elemendiline korpus, mis tänu teoreemile 8.14 ongi \mathbb{F}_q .

8.2. Aritmeetika lõplikes korpustes

Lõpliku korpuse elementide esitamiseks on mitmeid võimalusi. Üks viis on kasutada faktoringi $\mathbb{F}_q[x]/\langle p(x) \rangle$, 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 8.15. Vaatleme lõplikku korpust \mathbb{F}_{16} kui korpuse $\mathbb{F}_2 = \mathbb{Z}_2 = \{0, 1\}$ ($\bar{0}$ ja $\bar{1}$ asemel kirjutame 0 ja 1) 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, need on

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

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

Kuna polünoomi $p(x)$ aste on 4, siis lause 8.10 põhjal

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

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

$$\begin{array}{ll} \text{konstantsed} & 0, 1, \\ \text{lineaarsed} & a, a + 1, \\ \text{ruutpolünoomid} & a^2, a^2 + 1, a^2 + a, a^2 + a + 1 \\ \text{kuuppolünoomid} & a^3, a^3 + 1, a^3 + a, a^3 + a^2, a^3 + a + 1, \\ & a^3 + a^2 + 1, a^3 + a^2 + a, a^3 + a^2 + a + 1. \end{array}$$

Sellisel kujul elementide liitmine on lihtne, sest see on lihtsalt polünoomide liitmine. Ent 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

$$\begin{aligned} a^{15} &= (a^5)^3 = (a \cdot a^4)^3 = (a \cdot (a + 1))^3 = a^3(a + 1)^3 = a^3 \cdot (a^3 + a^2 + a + 1) \\ &= a^6 + a^5 + a^4 + a^3 = (a^3 + a^2) + (a^2 + a) + (a + 1) + a^3 = 1, \end{aligned}$$

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 7.18 põhjal on a rühma \mathbb{F}_{16}^* moodustaja. Seega

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

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

Need kaks esitust saab omavahel siduda, kui arutada välja tabel, mis näitab, kuidas element a^k esitub ülimalt kolmanda astme polünoomina a suhtes. Kasutades seost $a^4 = 1 + a$ 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 $a_3a^3 + a_2a^2 + a_1a + a_0$ asemel kirjutame $a_3a_2a_1a_0$.

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]).

8.3. Juurimine lõplikes korpustes

Definitsioon 8.16. Olgu K (suvaline) korpus ja $b \in K$. Elementi $a \in K$ nimetatakse n . astme juureks elemendist b , kui $a^n = b$. n . astme juurt korpuse K ühikelemendist $\mathbf{1}$ nimetatakse n . astme ühejuureks .

Lause 8.17. Kommutatiivse korpuse K kõigi n . astme ühejuurte hulk H_n on rühma K^* alamrühm.

TÕESTUS. Olgu

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

ning olgu $a_1, a_2 \in H_n$, s.t. $a_1^n = \mathbf{1}$ ja $a_2^n = \mathbf{1}$. Siis ka $(a_1 a_2)^n = a_1^n a_2^n = \mathbf{1}$. Kui $a \in H_n$, s.t. $a^n = \mathbf{1}$, siis ka $(a^{-1})^n = (a^n)^{-1} = \mathbf{1}^{-1} = \mathbf{1}$. Seega H_n on rühma K^* alamrühm. \square

Kuna n . astme ühejuured on polünoomi $x^n - \mathbf{1} \in K[x]$ juured, siis lause 2.8 tõttu ei saa neid olla rohkem kui n tükki. On tuntud fakt, et kompleksarvude korpuses \mathbb{C} on n . astme ühejuurt ja ühejuurte rühm on tsükliline, kuid iga korpuse korral see nii ei ole.

Definitsioon 8.18. Kui n . astme ühejuuri korpuses K on n tükki ning kõik nad on esitatavad n . astme ühejuure ξ astmetena (s.t. kui H_n on n . järku rühm ja ξ on rühma H_n moodustaja), siis ühejuurt ξ nimetatakse *primitiivseks* n . astme ühejuureks.

Teoreem 8.19. Olgu $n \geq 2$ naturaalarv ja a korpuse \mathbb{F}_q primitiivne element, s.t. $\mathbb{F}_q^* = \{a, a^2, \dots, a^{q-2}, a^{q-1} = \mathbf{1}\}$. Siis

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

TÕESTUS. 1. Olgu a^k n . astme ühejuur. Siis $a^{kn} = \mathbf{1}$, ning kuna elemendi a järk rühmas K^* on $q-1$, siis lemma 7.3 põhjal $q-1 \mid kn$. Vastupidi, oletame, et leidub täisarv u , nii et $(q-1)u = kn$. Kuna $a \in K^*$, siis lemma 8.7 põhjal $(a^k)^n = a^{(q-1)u} = (a^{q-1})^u = \mathbf{1}$, s.t. a^k on n . 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 $k \in \{1, \dots, q-1\}$ korral, $q-1 \mid kn$ (s.t. $md \mid kn'd$) parajasti siis, kui $m \mid k$. Selliseid astendajaid $k \in \{1, \dots, q-1\}$, mida m jagab, on d tükki: $m, 2m, \dots, dm = q-1$. Seega on olemas täpselt d n . astme ühejuurt,

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

ning kõik ühejuured avalduvad ühejuure a^m astmetena.

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

4. Vaatleme kõrvalklasse alamrühma H_n järgi, s.t hulki

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

$c \in K^*$. Need kõrvalklassid ei lõiku ning kõigi kõrvalklasside võimsused on võrdsed, s.t. iga $c \in K^*$ korral $|cH_n| = |H_n|$ ([1], lk. 155-156). Kõrvalklasside arv on seega $\frac{|K^*|}{|H_n|} = \frac{q-1}{d} = m$. Näitame, et elemendid kuuluvad samasse kõrvalklassi parajasti siis, kui nende n . 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 . astmed on võrdsed kõrvalklassi esindaja c n . astmega (s.t. kõik kõrvalklassi cH_n elemendid on n . astme juurteks elemendist c^n). Vastupidi, oletame, et $c_1^n = c_2^n$. Siis $(c_2^{-1} c_1)^n = (c_2^{-1})^n c_1^n = (c_2^n)^{-1} c_1^n = \mathbf{1}$, 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 . astme juured.) \square

Järeldus 8.20. Kui $(n, q-1) = 1$, siis $\mathbf{1}$ on ainus n . astme ühejuur korpuses \mathbb{F}_q .

Järeldus 8.21. 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 -1 on täpselt 4. astme primitiivsed ühejuured. Olgu ξ ruutjuur elemendist -1 , s.t. $\xi^2 = -1$. Siis $\xi, \xi^2 = -1, \xi^3 = -\xi, \xi^4 = 1$ on neli erinevat 4. astme ühejuurt ning seega ξ on primitiivne 4. astme ühejuur. Vastupidi, olgu ξ primitiivne 4. astme ühejuur. Siis $\xi^4 = 1$, järelikult $\xi^4 - 1 = (\xi^2 + 1)(\xi^2 - 1) = 0$. Kuna ξ on primitiivne 4. astme ühejuur, siis ei ole võimalik, et $\xi^2 = 1$, sest siis me saaksime ξ astmetena kätte vaid kaks 4. astme ühejuurt (ξ ise ja 1). Seega, kuna korpus ei sisalda nullitegureid, peab $\xi^2 + 1 = 0$, ehk $\xi^2 = -1$. Sellega oleme näidanud, et ruutjuured elemendist -1 on parajasti 4. astme primitiivsed ühejuured. Teoreemi 8.19 põhjal leidub korpus K primitiivseid 4. astme ühejuuri parajasti siis, kui $4 \mid q - 1$ ehk $q \equiv 1 \pmod{4}$. \square

Märkus 8.22. Kui $q = 2^l$, siis $1 = -1$ ja seega -1 omab ruutjuurt.

Näide 8.23. Korpus \mathbb{Z}_{13} on ruutjuurteks elemendist $\overline{-1}$ elemendid $\overline{5}$ ja $\overline{8}$. Korpus \mathbb{Z}_7 aga elemendil $\overline{-1}$ ruutjuurt ei ole, sest $7 \equiv 3 \pmod{4}$.

Näide 8.24. Vaatleme korpust \mathbb{F}_{16} näitest 8.15. Kuna $(2, 15) = 1$, siis 1 on ainus 2. astme ühejuur korpus \mathbb{F}_{16} . Kuna $(3, 15) = 3$, siis kolmanda astme ühejuuri korpus \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 .

9. Ruutjäägid

Olgu $p > 2$ algarv. Selles paragrahvis huvitab meid, millistel jäägiklassikorpuse \mathbb{Z}_p elementidel on olemas ruutjuur, s.t millised korpuse \mathbb{Z}_p elemendid on mingi teise elemendi ruudud. Kuna $(2, p-1) = 2$, siis teoreemi 8.19 põhjal on ruutjuur olemas $\frac{p-1}{2}$ nullist erineval elemendil, s.o täpselt pooltel \mathbb{Z}_p^* elementidel. Oletame, et mingil elemendil $\bar{a} \in \mathbb{Z}_p^*$ on olemas ruutjuur, s.t. leidub selline $\bar{b} \in \mathbb{Z}_p^*$, et $\bar{b}^2 = \bar{a}$. Siis ka $\overline{\bar{b}}$ on elemendi \bar{a} ruutjuur, sest $\overline{\bar{b}^2} = \overline{\bar{a}} = \bar{a}$. Kui oletada, et $\overline{\bar{b}} = \bar{b}$, siis $\overline{\bar{b}} = \bar{b}$, millest $p > 2$ tõttu järeldub, et $\bar{b} = \bar{0}$, mis aga pole võimalik. Seega \bar{b} ja $\overline{\bar{b}}$ on erinevad elemendi \bar{a} ruutjuured. Nüüd teise astme polünoomil $x^2 - \bar{a}$ üle korpuse \mathbb{Z}_p on lause 2.8 põhjal ülimalt 2 juurt, s.t. elemendil \bar{a} teisi ruutjuuri pole. Seega, kui elemendil \bar{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 $\{\bar{1}, \bar{2}, \dots, \frac{p-1}{2}\}$ kõigi elementide ruudud (sest ülejäänud jäägiklassid on sellesse hulka kuuluvate jäägiklasside vastandelemendid). Kui aga tahame teada, kas mingil konkreetsel elemendil on olemas ruutjuur ning p on suur, siis on selline lähenemine liiga ebaotstarbekas. Osutub, et leidub palju paremaid viise.

Definitsioon 9.1. Olgu $p > 2$ algarv ja a selline täisarv, et $p \nmid a$. Täisarvu a nimetatakse *ruutjäägiks* (*mitterruutjäägiks*) mooduli p järgi, kui element \bar{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. Eelneva põhjal peab mooduli p järgi olema $\frac{p-1}{2}$ ruutjääki ja $\frac{p-1}{2}$ mitterruutjääki.

Näide 9.2. Korpuses \mathbb{Z}_{11} on ruutjuur olemas elementidel $\bar{1} = \bar{1}^2 = \bar{10}^2$, $\bar{4} = \bar{2}^2 = \bar{9}^2$, $\bar{9} = \bar{3}^2 = \bar{8}^2$, $\bar{5} = \bar{4}^2 = \bar{7}^2$ ja $\bar{3} = \bar{5}^2 = \bar{6}^2$. Seega ruutjäägid mooduli 11 järgi on 1, 3, 4, 5, 9 ning mitterruutjäägid on 2, 6, 7, 8, 10.

Definitsioon 9.3. Olgu a täisarv ja $p > 2$ algarv. *Legendre'i sümbol* $\left(\frac{a}{p}\right)$ defineeritakse järgmiselt

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

(Seda sümbolit loetakse “ a p suhtes”.)

Seega eelmises näites saadud tulemuse võib Legendre'i sümboli abil kirja panna järgmiselt:

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

Olgu $\mathbb{Z}_p^* = \{\bar{c}, \bar{c}^2, \dots, \bar{c}^{p-1} = \bar{1}\}$. Kui k on paarisarv, siis elemendi \bar{c}^k ruutjuureks on $\bar{c}^{\frac{k}{2}}$. Et täpselt pooled arvudest $1, \dots, p-1$ on paarisarvud ja eelneva põhjal ruutjuurt omab samuti täpselt $\frac{p-1}{2}$ elementi, siis saame, et ruutjuurt omavad parajasti need elemendid \bar{c}^k , kus k on paaris.

Lemma 9.4. *Kui c on algjuur mooduli p järgi, siis iga $k \in \mathbb{N}$ korral*

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

Lause 9.5 (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 $\bar{a} = \bar{c}^k$, kus $\mathbb{Z}_p^* = \{\bar{c}, \bar{c}^2, \dots, \bar{c}^{p-1} = \bar{1}\}$. Siis $\left(c^{\frac{p-1}{2}}\right)^2 = c^{p-1} \equiv 1 \pmod{p}$. Järelikult $c^{\frac{p-1}{2}}$ on polünoomi $x^2 - \bar{1} \in \mathbb{Z}_p[x]$ 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 $\bar{1}$ ja $\overline{-1}$ sellel polünoomil pole. Kuna \bar{c} on rühma \mathbb{Z}_p^* moodustaja, siis esimene võimalus langeb ära ja seega

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

□

Kuigi Euleri kriteeriumi abil saab põhimõtteliselt iga arvu korral kindlaks teha, kas ta on ruutjäak, ei ole ta siiski sobiv suurte algarvude p korral. Õnneks on Legendre'i sümbolil terve rida omadusi, mis lihtsustavad arvutamist.

Lause 9.6. Iga algarvu $p > 2$ korral on Legendre'i sümbolil järgmised omadused.

1. Iga $a, b \in \mathbb{Z}$ korral, kui $a \equiv b \pmod{p}$, siis $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

2. Iga $a, b \in \mathbb{Z}$ korral

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

3. Iga $a, b \in \mathbb{Z}$, $p \nmid b$, korral

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

4. Kehtib $\left(\frac{1}{p}\right) = 1$ ja

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \text{kui } p \equiv 1 \pmod{4} \\ -1, & \text{kui } p \equiv 3 \pmod{4}. \end{cases}$$

TÕESTUS. 1. järeldub vahetult Legendre'i sümboli definitsioonist.

2. Kui $p \mid a$ või $p \mid b$, siis on väide ilmne. Oletame, et $p \nmid a$ ja $p \nmid b$. Olgu $\mathbb{Z}_p^* = \{\bar{c}, \bar{c}^2, \dots, \bar{c}^{p-1} = \bar{1}\}$, $\bar{a} = \bar{c}^k$ ja $\bar{b} = \bar{c}^l$. Siis väite 1 ja lemma 9.4 põhjal

$$\left(\frac{ab}{p}\right) = \left(\frac{c^{k+l}}{p}\right) = (-1)^{k+l} = (-1)^k (-1)^l = \left(\frac{c^k}{p}\right) \left(\frac{c^l}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right).$$

3. Kui $p \nmid b$, siis vastavalt definitsioonile 9.3 $\left(\frac{b^2}{p}\right) = 1$ ning seega osa 2. põhjal

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

4. Võrdus $\left(\frac{1}{p}\right) = 1$ kehtib selletõttu, et $\bar{1}^2 = \bar{1}$ korpusel \mathbb{Z}_p . Teine võrdus järeldub Euleri kriteeriumist võttes $a = -1$ või järeldusest 8.21, sest $\frac{p-1}{2}$ on paarisarv parajasti siis kui $p - 1$ jagub neljaga ehk $p \equiv 1 \pmod{4}$. □

Näide 9.7. Teeme kindlaks, kas kongruents $x^2 \equiv -38 \pmod{13}$ on lahenduv. Selleks tuleks leida Legendre'i sümboli $\left(\frac{-38}{13}\right)$ väärtus. Kuna $38 \equiv 12 \pmod{13}$ ja $(-1)^{\frac{13-1}{2}} = 1$, siis saame, et

$$\left(\frac{-38}{13}\right) = \left(\frac{-1}{13}\right) \left(\frac{38}{13}\right) = \left(\frac{12}{13}\right) = \left(\frac{3 \cdot 2^2}{13}\right) = \left(\frac{3}{13}\right).$$

Viimase sümboli arvutamiseks kasutame Euleri kriteeriumi. Et

$$\left(\frac{3}{13}\right) \equiv 3^{\frac{13-1}{2}} = 3^6 = 27^2 \equiv 1 \pmod{13},$$

siis $\left(\frac{3}{13}\right) = 1$ ja seega ka $\left(\frac{-38}{13}\right) = 1$, s.t. kongruentsil $x^2 \equiv -38 \pmod{13}$ on lahend olemas.

Väikse kõrvalepõikena kasutame lauset 9.6 selleks, et näidata teatud kujul algarvude hulga lõpmatust.

Lause 9.8. On lõpmata palju algarve kujul $4k + 1$.

TÕESTUS. Oletame, et on ainult lõplik arv selliseid algarve; tähistame nad p_1, p_2, \dots, p_n . Vaatleme naturaalarvu $a = (2p_1 p_2 \dots p_n)^2 + 1$. On selge, et a on paaritu, seega peab leiduma mingi paaritu algarv p , nii et $p \mid a$, ehk $(2p_1 p_2 \dots p_n)^2 \equiv -1 \pmod{p}$. See tähendab, et -1 on ruutjäak mooduli p järgi, ehk $\left(\frac{-1}{p}\right) = 1$. Lause 9.6 põhjal $\left(\frac{-1}{p}\right) = 1$ parajasti siis, kui $p = 4k + 1$, $k \in \mathbb{N}$. Seega p on üks algarvudest p_1, \dots, p_n . Järelikult $p \mid a - (2p_1 p_2 \dots p_n)^2 = 1$, vastuolu. \square

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

Teoreem 9.9. Iga algarvu $p > 2$ korral

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

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

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

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

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

Kõik tegurid selle kongruentsi vasakul poolel on paarisarvud

ja $(1 + \frac{p-1}{2}) \frac{p-1}{4} = \frac{p^2-1}{8}$, 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 $(\frac{p-1}{2})! \not\equiv 0 \pmod{p}$, 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 0, 1 või -1 ja $p > 2$ ning $1 \not\equiv -1 \pmod{p}$ ja loomulikult ka $1 \not\equiv 0 \not\equiv -1 \pmod{p}$, siis viimase kongruentsi mõlemal poolel peavad olema võrdsed arvud. \square

Lemma 9.10. 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. \square

Järeldus 9.11. Kui $n > 1$ ja a on ühistegurita täisarvud, siis $U(\mathbb{Z}_n) = \bar{a} \cdot U(\mathbb{Z}_n)$. Teiste sõnadega, kui $a_1, a_2, \dots, a_{\varphi(n)}$ on kõik naturaalarvud, mis on väiksemad kui n ja on arvuga n ühistegurita, siis

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

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

Järeldus 9.12. Kui q on algarv ja $q \nmid a$, siis $\mathbb{Z}_p^* = \bar{a} \cdot \mathbb{Z}_p^*$, s.t. arvud $a, 2a, \dots, (q-1)a$ on mooduli q järgi kongruentsed arvudega $1, 2, \dots, q-1$ mingis järjekorras.

Järgmine, Gaussi poolt 1796. a. tõestatud teoreem kuulub arvuteooria kõige ilusamate ja sügavamate tulemuste hulka. Trükkis on avaldatud vähemalt 150 erinevat tõestust, Gauss ise andis vähemalt 8 erinevat tõestust.

Teoreem 9.13 (Ruutvastavussäämus). Kui $p > 2$ ja $q > 2$ on erinevad algarvud, siis

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

TÖESTUS. 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 8.19 põhjal leidub selles korpuses q . 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 $1, 2, \dots, q-1$, siis ka $q-k$ omandab samad väärtused, lauset 9.6, ning seda, et $\xi^{q-k} = \xi^{-k}$, 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 9.12 saame, et kui k omandab kõik väärtused $1, 2, \dots, q-1$, siis iga fikseeritud $j \in \{1, \dots, q-1\}$ korral

ka jk omandab samad väärtused mooduli q järgi. Seega arvestades, et kui $jk = uq + v$, kus $0 < v < q$, siis $\left(\frac{jk}{q}\right) \xi^{-jk} = \left(\frac{uq+v}{q}\right) \xi^{-uq-v} = \left(\frac{v}{q}\right) \xi^{-v}$, saame, et

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

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

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

Teisest küljest, kasutades lemmat 8.6, 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

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

Seega oleme saanud, et

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

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 viimast võrdust 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

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

□

Näide 9.14. Teeme kindlaks, kas algarv 7411 on ruutjäak algarvulise mooduli 9283 järgi.

Kuna $7411 \equiv 3 \pmod{4}$ ja $9283 \equiv 3 \pmod{4}$ ning $13 \equiv 1 \pmod{4}$, siis

$$\left(\frac{7411}{9283}\right) = -\left(\frac{9283}{7411}\right) = -\left(\frac{1872}{7411}\right) = -\left(\frac{(2^2)^2}{7411}\right) \left(\frac{3^2}{7411}\right) \left(\frac{13}{7411}\right) = -\left(\frac{13}{7411}\right) = -\left(\frac{7411}{13}\right) = -\left(\frac{1}{13}\right) = -1.$$

Seega 7411 on mitteruutjäak mooduli 9283 järgi.

Legendre'i sümboli üldistuseks on saksa matemaatiku Jacobi (1804–1851) poolt sisse toodud sümbol.

Definitsioon 9.15. Olgu a täisarv ja n paaritu naturaalarv. Olgu $n = p_1 p_2 \dots p_s$, 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 9.1 loomulikul viisil üldistades öeldakse, et täisarv a on *ruutjäak* naturaalarvulise mooduli n järgi, kui kongruents $x^2 \equiv a \pmod{n}$ on lahenduv.

Märkus 9.16. Kui n on kordarv ja $\left(\frac{a}{n}\right) = 1$, siis see ei tähenda veel, et a on ruutjäak 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 mitteruutjäak 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 $x^2 \equiv a \pmod{p_i}$, mis oleks vastuolu.

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

Lause 9.17. *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 $a \in \mathbb{Z}$ ja paaritute naturaalarvude n ja m korral

$$\left(\frac{a}{nm}\right) = \left(\frac{a}{n}\right) \left(\frac{a}{m}\right).$$

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

Lemma 9.18. *Kui k ja l on paaritud naturaalarvud, siis*

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

TÕESTUS. 1. Kuna $(k-1)(l-1) \equiv 0 \pmod{4}$, siis $kl-1 \equiv (k-1) + (l-1) \pmod{4}$. Väide jäeldub nüüd lausest 3.9, sest viimase kongruentsi mõlemal poolel on paarisarvud.

2. saab tõestada analoogiliselt. □

Lemma 9.19. *Kui k_1, k_2, \dots, k_s on paaritud naturaalarvud, siis*

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

TÕESTUS. Tõestame väite 1. induksiooniga 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

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

□

Üldistame nüüd teoreemid 9.9 ja 9.13 Jacobi sümbolite jaoks.

Lause 9.20. *Mistahes paaritute naturaalarvude n ja m korral*

1. $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$;
2. $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$;
3. $\left(\frac{m}{n}\right) = (-1)^{\frac{(m-1)(n-1)}{4}} \left(\frac{n}{m}\right)$.

TÕESTUS. Olgu $n = p_1 p_2 \dots p_s$ ja $m = q_1 q_2 \dots q_r$, kus p_1, \dots, p_s ja q_1, \dots, q_r on algarvud.

1. Tänu lemmale 9.19 $\sum_{i=1}^s (p_i - 1)/2 \equiv (p_1 p_2 \dots p_s - 1)/2 = (n - 1)/2 \pmod{2}$ ning seetõttu kasutades lauset 9.6 saame

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

2. Tänu lemmale 9.19 $\sum_{i=1}^s (p_i^2 - 1)/8 \equiv (p_1^2 p_2^2 \dots p_s^2 - 1)/8 = (n^2 - 1)/8 \pmod{2}$ ning seetõttu kasutades teoreemi 9.9 saame

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

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 seega on tõestatava võrduse mõlemal poolel 0. Eeldame nüüd, et selliseid võrdseid algarve ei leidu. Rakendades veelkord lemmat 9.19 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 ruutvastavussäadust ja seda, et $\left(\frac{q_i}{p_j}\right)^2 = 1$, saame siis

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

□

Näide 9.21. Leiame Legendre'i $\left(\frac{7411}{9283}\right)$ sümboli väärtuse ilma arvu 1872 teguriteks lahutamata (välja arvatud 2 astmete eraldamine). Kasutades lauset 9.20 saame

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

10. Arvuvaldad

Selles paragrahvis 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.

10.1. Naturaalarvudelt täisarvudele

Naturaalarvude hulk \mathbb{N} on kinnine liitmise suhtes, kuid kahe naturaalarvu vahe ei pruugi olla naturaalarv. Vähiim 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, et kasutades algebralisi konstruktsioone saab lähtudes poolrühmast $(\mathbb{N}, +)$ konstrueerida rühma $(\mathbb{Z}, +)$, kusjuures $\mathbb{N} \subset \mathbb{Z}$. Vastava väite tõestame tegelikult tunduvalt üldisemal juhul.

Definitsioon 10.1. Olgu $(S, +)$ kommutatiivne poolrühm. Öeldakse, et S on *taandamisega* poolrühm, kui iga $x, y, z \in S$ korral

$$x + y = x + z \implies y = z.$$

Poolrühm $(\mathbb{N}, +)$ on üheks taandamisega poolrühma näiteks.

Teoreem 10.2. Iga kommutatiivse taandamisega poolrühma saab sisestada rühma.

TÕESTUS. Olgu $(S, +)$ kommutatiivne taandamisega poolrühm. Näitame, et leidub rühm G , mis sisaldab poolrühmaga S isomorfset alampoolrühma. Selleks defineerime hulga S otseruudul $S^2 = S \times S$ binaarse seose \sim järgmiselt:

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

mistahes $(x, y), (u, v) \in S^2$ 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

$$G = (S \times S) / \sim = \{(x, y) / \sim \mid x, y \in S\},$$

kus $(x, y) / \sim$ tähistab paari $(x, y) \in S \times S$ ekvivalentsiklassi seose \sim järgi. Näitame, et G osutub rühmaks, kui defineerida hulgal G liitmine \oplus reeglina

$$(x, y) / \sim \oplus (u, v) / \sim = (x + u, y + v) / \sim.$$

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 seda, et poolrühmal S defineeritud liitmine on kommutatiivne, saame, et $x + u + y' + v' = y + v + x' + u'$ ehk $(x + u, y + v) \sim (x' + u', y' + v')$. Seega tõesti liitmise tulemus ei sõltu ekvivalentsiklassi esindajate valikust.

Kuna

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

siis liitmistehe \oplus on kommutatiivne. Analoogiliselt järeldub sellest, et liitmine poolrühmal S on assotsiatiivne, see, et ka tehe \oplus on assotsiatiivne hulgal G . Fikseerime mingi elemendi $z \in S$. Siis nullelemendiks on klass $(z, z) / \sim$. Tõepoolest, iga $(x, y) \in S^2$ korral $(z, z) / \sim \oplus (x, y) / \sim = (z + x, z + y) / \sim = (x, y) / \sim$, sest $z + x + y = z + y + x$. Elemendi $(x, y) / \sim \in G$ vastandelemendiks on $(y, x) / \sim$, sest $(x, y) / \sim \oplus (y, x) / \sim = (x + y, y + x) / \sim = (z, z) / \sim$, kuna $x + y + z = y + x + z$. Seega G on tõesti rühm.

Näitame, et poolrühm $(S, +)$ on isomorfne rühma (G, \oplus) mingi alampoolrühmaga.

Fikseerime mingi elemendi $y \in S$. Vaatleme hulka $S' = \{(x + y, y) / \sim \mid x \in S\} \subseteq G$. Kuna iga $x, x' \in S$ korral $(x + y, y) / \sim \oplus (x' + y, y) / \sim = (x + y + x' + y, y + y) / \sim = (x + x' + y, y) / \sim \in S'$, siis S' on rühma G alampoolrühm.

Defineerime kujutuse $\varphi : S \rightarrow S'$ järgmiselt: iga $x \in S$ korral

$$\varphi(x) = (x + y, y) / \sim.$$

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

$$\begin{aligned} \varphi(x + x') &= (x + x' + y, y) / \sim = (x + x' + y + y, y + y) / \sim \\ &= (x + y, y) / \sim \oplus (x' + y, y) / \sim = \varphi(x) \oplus \varphi(x'), \end{aligned}$$

siis φ on poolrühmade homomorfism.

Seega φ on bijektiivne homomorfism ehk isomorfism ja $S \cong S' = \varphi(S) \subseteq G$, kus S' on rühma G alampoolrühm. \square

Definitsioon 10.3. Rühma (G, \oplus) nimetatakse poolrühma $(S, +)$ vahede rühmaks.

Konstrueerides poolrühma $(\mathbb{N}, +)$ vahede rühma saame rühma, mis on isomorfne rühmaga $(\mathbb{Z}, +)$.

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

Lause 10.4. Kommutatiivse taandamisega poolrühma $(S, +)$ vahede rühma (G, \oplus) vähim alamrühm, mis sisaldab poolrühma S alampoolrühmana, on G ise.

TÕESTUS. Kasutame teoreemi 10.2 tähistusi. Olgu G' rühma (G, \oplus) vähim alamrühm, mis sisaldab poolrühma $S \cong S'$ alampoolrühmana. Olgu $(u, v)/\sim \in G'$ suvaline element. Kuna $S' \subseteq G'$, siis $(u + y, y)/\sim, (v + y, y)/\sim \in G'$. Et G' on alamrühm, siis on ta kinnine vastandelemendi võtmise ja liitmise suhtes, järelikult $(y, v + y)/\sim \in G'$ ning

$$(u + y, y)/\sim \oplus (y, v + y)/\sim = (u + y + y, y + v + y)/\sim = (u, v)/\sim \in G'.$$

Seega $G = G'$. □

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 10.5. Kui $(S, +)$ on kommutatiivne taandamisega poolrühm, siis iga rühm H , mis sisaldab poolrühma S alampoolrühmana ja mille vähim poolrühma S alampoolrühmana sisaldav alamrühm on see rühm ise, on isomorfne poolrühma S vahede rühmaga.

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

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

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. Fikseerime $z \in S$. Et mistahes $x \in S$ korral $x = (x + z) - z$, siis $S \subseteq H'$ ja et S on rühma H alampoolrühm, siis on ta ka rühma H' alampoolrühm. Kuna rühma H vähim poolrühma S alampoolrühmana sisaldav alamrühm on H ise, siis $H' = H$.

Defineerime kujutuse $\varphi : H \rightarrow G$ nii, et

$$\varphi(x - y) = (x, y)/\sim$$

iga $x, y \in S$ korral. Veendume, et φ definitsioon on korrektne. Selleks oletame, et $x - y = x' - y', x, y, x', y' \in S$. Siis $x + y' = y + x'$ ning järelikult $(x, y) \sim (x', y')$. Seega φ on defineeritud korrektselt. On selge, et φ on sürjekttiivne. Näitame, et ta on ka injekttiivne. Selleks oletame, et $(x, y) \sim (x', y'), x, y, x', y' \in S$. Siis vastavalt seose \sim definitsioonile $x + y' = y + x'$ ja järelikult $x - y = x' - y'$ rühmas H . Seega φ on injekttiivne. Lõpuks, kuna mistahes $x, y, u, v \in S$ korral

$$\varphi((x - y) + (u - v)) = \varphi((x + u) - (y + v)) = (x + u, y + v)/\sim = (x, y)/\sim \oplus (u, v)/\sim = \varphi(x - y) \oplus \varphi(u - v),$$

siis φ on rühmade homomorfism. Seega φ on isomorfism ning rühmad G ja H on isomorfne. □

Arvestades lauset 10.1 võime väita, et täisarvude rühm $(\mathbb{Z}, +)$ on vähim poolrühma $(\mathbb{N}, +)$ alampoolrühmana sisaldav \mathbb{Z} alamrühm ja ta on isomorfismi täpsuseni üheselt määratud.

10.2. 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} . Iga ratsionaalarvu võib esitada kahe täisarvu jagatisena. Osutub, et analoogilise konstruktsiooni saab jällegi läbi viia üldisemal juhul.

Teoreem 10.6. Iga kommutatiivse nullitegurita ringi R saab sisestada mingisse korpuse K .

Selle teoreemi tõestuse võib leida raamatust [1], lk. 199–200. 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} .

Analoogiliselt vahede rühma juhuga saab näidata, et ringi R jagatiste korpust K on korpuse K vähim alamkorpust, mis sisaldab ringi R alamringina. Veelgi enam, korpust, mille vähim ringi R sisaldav alamkorpust on see korpust ise, on isomorfismi täpsuseni üheselt määratud. Seda arvestades võib öelda, et ratsionaalarvude korpust \mathbb{Q} on vähim ringi \mathbb{Z} alamringina sisaldav korpust \mathbb{Q} alamkorpust ja ta on isomorfismi täpsuseni üheselt määratud.

10.3. Ratsionaalarvudelt reaalarvudele

Definitsioon 10.7. Hulka $(K, +, \cdot, \leq)$, kus $+$ ja \cdot on kahekohalised algebralised tehted ja \leq on binaarne seos hulgal K nimetatakse *reaalarvude hulgaks*, kui

R1. $(K, +, \cdot)$ on korpus;

R2. \leq on lineaarne järjestusseos hulgal K (s.t. selline järjestusseos, et mistahes $\alpha, \beta \in K$ korral kas $\alpha \leq \beta$ või $\beta \leq \alpha$) ning mistahes $\alpha, \beta, \gamma, \delta \in K, \delta > 0$, korral

$$\alpha < \beta \implies \alpha + \gamma < \beta + \gamma \text{ ja } \alpha\delta < \beta\delta;$$

R3. (täielikkuse aksioom) hulga K igal mittetühjal alt tõkestatud alamhulgal on olemas alumine raja hulgas K .

Märkus 10.8. Aksioomis **R2.** kasutatakse seost $<$, mis defineeritakse mistahes järjestusseose \leq korral järgmiselt:

$$\alpha < \beta \iff \alpha \leq \beta \text{ ja } \alpha \neq \beta.$$

10.3.1. 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 . järku *kümnendlähendiks*. Kui reaalarvu α märk on pluss (miinus) ja täisarvude $a_n, n \in \mathbb{N}$, 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 $a_k = b_k, k = 0, 1, \dots, N$, 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 $\alpha < \beta$. Lugeses $\alpha \leq \beta$ kui $\alpha = \beta$ või $\alpha < \beta$ saame lineaarse järjestusseose \leq .

Öeldakse, et täisarvude jada $(x_k)_{k \in \mathbb{N}}$ *stabiliseerub* arvuks m , kui leidub selline indeks N , et iga $k \geq N$ 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 . veerg stabiliseerub arvuks a_i iga $i \in \mathbb{N} \cup \{0\}$ korral. Kui $\alpha > 0$ ja $\beta > 0$, siis kümnendmurdudest $\underline{\alpha}_k + \underline{\beta}_k, \underline{\alpha}_k - \underline{\beta}_k, (\underline{\alpha}_k \underline{\beta}_k)_k$ ja $\left(\frac{\alpha_k}{\beta_k}\right)_k$ 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 $\alpha \leq 0$ ja $\beta \leq 0$, siis $\alpha + \beta = -(|\alpha| + |\beta|)$; kui α ja β on erinevate märkidega, siis $\alpha + \beta = \pm(|\alpha| - |\beta|)$, kus märgiks võetakse liidetavaist absoluutväärtuselt suurema märk. Mistahes α, β korral loetakse $\alpha - \beta = \alpha + (-\beta)$ jne. Saab näidata, et lõpmatute kümnendmurdude hulk koos temal defineeritud tehetega $+$ ja \cdot ning järjestusega \leq rahuldab aksioome R1.–R3.

10.3.2. Dedekindi meetod

Definitsioon 10.9. *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 seega ka kogu lõike. Seega edaspidises võime Dedekindi lõike samastada tema parempoolse hulga 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 α, β, \dots parempoolseid hulki ja nimetame Dedekindi lõikeid *reaalarvudeks*. Kõigi Dedekindi lõigete hulga tähistame \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 $\bar{\alpha}$ on olemas suurim element. Hulga \mathbb{Q} saab sisestada hulka \mathbb{R} kujutuse $f : \mathbb{Q} \rightarrow \mathbb{R}, f(a) = \underline{a}$, abil. Mitte kõik lõiked ei ole ratsionaalsed. Näiteks saab näidata, et $\sqrt{2}$, ehk täpsemalt öeldes lõige $\alpha = \{a \in \mathbb{Q} \mid a > 0, a^2 > 2\}$ ei ole ratsionaalne.

Lõigete (parempoolsete hulkade) järjestuse defineerime järgmiselt:

$$\alpha \leq \beta \iff \beta \subseteq \alpha.$$

Lihtne on veenduda, et \leq on osalise järjestuse seos hulgal \mathbb{R} . Veelgi enam, see seos on ka lineaarne järjestusseos ja rahuldab aksiomi R3.

Mistahes kahe lõike $\alpha, \beta \in \mathbb{R}$ summa ja vahe defineerime võrdusega

$$\alpha \pm \beta = \{a \pm b \mid a \in \alpha, b \in \beta\}.$$

Kui $\alpha, \beta \geq 0 (= \underline{0})$, 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 $\alpha \geq 0$ ja $\beta \geq 0$ vahena: $\gamma = \alpha - \beta$. Lõigete $\gamma = \alpha - \beta$ ja $\gamma' = \alpha' - \beta'$, kus ka $\alpha', \beta' \geq 0$, korrutise defineerime võrdusega

$$\gamma \cdot \gamma' = (\alpha - \beta) \cdot (\alpha' - \beta') = \alpha \cdot \alpha' + \beta \cdot \beta' - \alpha \cdot \beta' - \beta \cdot \alpha'.$$

Saab näidata, et defineeritud tehete suhtes osutub hulk \mathbb{R} korpuseks ja et järjestus \leq on kooskõlas liitmise ja korrutamiselega.

10.3.3. Cantori meetod

Definitsioon 10.10. Ratsionaalarvujada (a_i) nimetatakse *fundamentaaljadaks* ehk *Cauchy jadaks*, kui iga ratsionaalarvu $\varepsilon > 0$ korral leidub selline indeks N , et iga $i, j \geq N$ 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 $i \geq N$ 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, nt. $\sqrt{2}$ lähismurdude jada $a_0 = 1; a_1 = 1,4; a_2 = 1,41; a_3 = 1,414; a_4 = 1,4142; \dots$.

Definitsioon 10.11. Ratsionaalselt nulliks koonduvat jada, s.t. sellist jada (a_i) , et iga $\varepsilon > 0$ korral leidub N nii, et iga $i \geq N$ korral $|a_i| < \varepsilon$, nimetatakse *nulljadaks*.

Olgu $F(\mathbb{Q})$ kõigi ratsionaalarvuliste Cauchy jadade hulk. Defineerime hulgal $F(\mathbb{Q})$ seose \sim järgmiselt:

$$(a_i) \sim (b_i) \iff (a_i - b_i) \text{ on nulljada.}$$

Saab näidata, et \sim on ekvivalentsusseos. Tähistame faktorhulga selle seose järgi

$$\mathbb{R} = F(\mathbb{Q})/\sim = \{(a_i)/\sim \mid (a_i) \in F(\mathbb{Q})\}$$

ning nimetame selle hulga elemente *reaalarvudeks*. Defineerime sellel hulgal liitmise ja korrutamise võrdustega

$$(a_i)/\sim + (b_i)/\sim = (a_i + b_i)/\sim, \tag{28}$$

$$(a_i)/\sim \cdot (b_i)/\sim = (a_i \cdot b_i)/\sim. \tag{29}$$

Saab näidata, et ka summa ja korrutis on Cauchy jasad ning et $(F(\mathbb{Q})/\sim, +, \cdot)$ on korpus. Nullelemendiks selles korpuses on ekvivalentsiklass, mis koosneb kõigist nulljadadest.

\mathbb{Q} saab sisestada alamkorpuseks korpusesse $F(\mathbb{Q})/\sim$ kujutuse $f : \mathbb{Q} \rightarrow F(\mathbb{Q})/\sim, f(a) = (a, a, a, \dots)/\sim$ 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 $(a_i)/\sim$ nimetame *positiivseks (negatiivseks)* kui (a_i) on positiivne (negatiivne). Iga reaalarv on kas positiivne, negatiivne või null. Defineerime hulgal $F(\mathbb{Q})/\sim$ seose \leq järgmiselt:

$$\alpha \leq \beta \iff \alpha = \beta \text{ või } \beta - \alpha \text{ on positiivne.}$$

Seos \leq osutub lineaarseks järjestusseoseks ning saab näidata, et kehtivad aksioomid R2 ja R3.

Osutub, et aksioomid R1.–R3. kirjeldavad üheselt ära reaalarvude hulga.

Teoreem 10.12 ([9]. , lk 50–51] Iga järjestatud korpus K , mis rahuldab aksioome R1.–R3., on isomorfnega $F(\mathbb{Q})/\sim$.

10.3.4. p -aadilised arvud

Definitsioon 10.13. Norm korpusel $(K, +, \cdot)$ on kujutus $\| \cdot \|$, mis igale elemendile $x \in K$ säeb vastavusse mitte-negatiivse reaalarvu $\|x\|$ nii, et

N1. $\|x\| = 0$ siis ja ainult siis, kui $x = 0$;

N2. $\|xy\| = \|x\| \|y\|$;

N3. $\|x + y\| \leq \|x\| + \|y\|$.

Näiteks on normiks ratsionaalarvude korpusel absoluutvääratus. Osutub, et ratsionaalarvude korpusel saab defineerida ka teisi põnevaid norme.

Olgu p algarv. Iga täisarvu $a \neq 0$ korral olgu $\text{ord}_p a$ algarvu p kõrgeim aste, mis jagab arvu a . Näiteks $\text{ord}_5 35 = 1$, $\text{ord}_5(-250) = 3$, $\text{ord}_2 96 = 5$, $\text{ord}_2 97 = 0$. Loeme, et $\text{ord}_p 0 = \infty$. Paneme tähele, et $\text{ord}_p(a_1 a_2) = \text{ord}_p a_1 + \text{ord}_p a_2$. Mistahes ratsionaalarvu $x = \frac{a}{b}$ jaoks, kus $a, b \in \mathbb{Z}$, $(a, b) = 1$, defineerime $\text{ord}_p x = \text{ord}_p a - \text{ord}_p b$. See definitsioon sõltub vaid ratsionaalarvust x , mitte sellest, milliste täisarvude jagatisena x on esitatud, sest kui $x = \frac{ac}{bc}$, $c \in \mathbb{Z}$, siis $\text{ord}_p(ac) - \text{ord}_p(bc) = \text{ord}_p a - \text{ord}_p b$.

Defineerime kujutuse $| \cdot |_p : \mathbb{Q} \rightarrow \mathbb{Q}$ järgmiselt:

$$|x|_p = \begin{cases} \frac{1}{p^{\text{ord}_p x}}, & \text{kui } x \neq 0; \\ 0, & \text{kui } x = 0. \end{cases}$$

Ekh teisiti: kui esitame ratsionaalarvu $x \neq 0$ kujul $x = p^m \frac{a}{b}$, kus $m \in \mathbb{Z}$ ja $(ab, p) = 1$, siis $|x|_p = \frac{1}{p^m}$.

Lause 10.14. Kujutus $| \cdot |_p$ 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 $\text{ord}_p(x + y) = \text{ord}_p(ad + bc) - \text{ord}_p b - \text{ord}_p d$. Algarvu p kõrgeim aste, mis jagab kahe arvu summat ei ole väiksem kui vähim algarvu p kõrgemaist astmeist, mis jagavad liidetavaid. Seega

$$\begin{aligned} \text{ord}_p(x + y) &= \text{ord}_p(ad + bc) - \text{ord}_p(b) - \text{ord}_p(d) \geq \min(\text{ord}_p ad, \text{ord}_p bc) - \text{ord}_p b - \text{ord}_p d \\ &= \min(\text{ord}_p a + \text{ord}_p d, \text{ord}_p b + \text{ord}_p c) - \text{ord}_p b - \text{ord}_p d \\ &= \min(\text{ord}_p a - \text{ord}_p b, \text{ord}_p c - \text{ord}_p d) = \min(\text{ord}_p x, \text{ord}_p y). \end{aligned}$$

Järelikult $|x + y|_p = p^{-\text{ord}_p(x+y)} \leq \max(p^{-\text{ord}_p x}, p^{-\text{ord}_p y}) = \max(|x|_p, |y|_p)$ ning viimane on $\leq |x|_p + |y|_p$. \square

Definitsioon 10.15. Normi $| \cdot |_p$ nimetatakse p -aadiliseks normiks.

Tegelikult tõestasime me tugevama võrratuse, kui oli nõutud normi definitsiooni tingimuses N3. See võrratus võetakse järgmise definitsiooni aluseks.

Definitsioon 10.16. Normi $\| \cdot \|$ korpusel K nimetatakse *mittearhimeediliseks*, kui iga $x, y \in K$ korral

$$\|x + y\| \leq \max(\|x\|, \|y\|). \quad (30)$$

Normi, mis ei ole mittearhimeediline, nimetatakse *arhimeediliseks*.

Seega p -aadiline norm $|\cdot|_p$ on mitteamineediline ja absoluutväärtus $|\cdot|$ on arhimeediline norm korpusel \mathbb{Q} .

Asendades definitsioonides 10.10 ja 10.11 absoluutväärtuse normiga $|\cdot|_p$, saab defineerida Cauchy jadad, koonduvuse ja nulljadad normi $|\cdot|_p$ suhtes.

Normil $|\cdot|_p$ on mitmeid huvitavaid omadusi. Näiteks jada $1, p, p^2, p^3, \dots$ koondub nulliks selle normi järgi. Tõepoolest, iga $\varepsilon > 0$ korral leidub selline N , et iga $i > N$ korral $|p^i|_p = \frac{1}{p^i} < \varepsilon$. Või siis näiteks kui vaatleme kera keskpunktiga $a \in \mathbb{Q}$ ja raadiusega $r \in \mathbb{Q}^+$, $D(a, r) = \{x \in \mathbb{Q} \mid |x - a|_p \leq r\}$, 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. $|x - a|_p \leq r$, siis

$$|x - b|_p = |(x - a) + (a - b)|_p \leq \max(|x - a|_p, |a - b|_p) \leq r,$$

järelikult $x \in D(b, r)$. Vastupidise sisalduvuse saab tõestada analoogiliselt.

Norme $\|\cdot\|$ ja $\|\cdot\|'$ nimetatakse *ekvivalentseteks*, kui jada on Cauchy jada normi $\|\cdot\|$ suhtes parajasti siis, kui ta on Cauchy jada normi $\|\cdot\|'$ suhtes.

Näiteks, kui normi $|\cdot|_p$ definitsioonis kirjutada $\left(\frac{1}{p}\right)^{\text{ord}_p x}$ asemel $\alpha^{\text{ord}_p x}$, kus $0 < \alpha < 1$, siis saaksime normi, mis on ekvivalentne normiga $|\cdot|_p$. Samuti normid $|\cdot|^\alpha$, $0 < \alpha < 1$, on ekvivalentsed absoluutväärtusega.

Triviaalse normi all korpusel K peame silmas sellist normi $\|\cdot\|$, mille korral $\|0\| = 0$ ning iga $x \neq 0$ korral $\|x\| = 1$.

Kehtib järgmine teoreem ([10], lk. 3–5).

Teoreem 10.17 (Ostrowski). *Iga mittetriviaalne norm korpusel \mathbb{Q} on ekvivalentne kas absoluutväärtusega või mingi p -aadilise normiga $|\cdot|_p$, 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 $|\cdot|_p$ suhtes). Defineerime hulgal $F_p(\mathbb{Q})$ seose \sim järgmiselt:

$$(a_i) \sim (b_i) \iff (a_i - b_i) \text{ on nulljada normi } |\cdot|_p \text{ suhtes.}$$

Jällegi \sim on ekvivalentsusseos. Tähistame faktorhulga selle seose järgi

$$\mathbb{Q}_p = F_p(\mathbb{Q})/\sim = \left\{ (a_i)/\sim \mid (a_i) \text{ on Cauchy jada normi } |\cdot|_p \text{ suhtes} \right\}.$$

Hulgal \mathbb{Q}_p defineerime liitmise ja korrutamise jälle võrdustega (28) ja (29) 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 $x = x'$. Jada (0) ekvivalentsiklassi tähistame lihtsalt 0 . Korpus \mathbb{Q} on isomorfnne korpuse \mathbb{Q}_p alamkorpusega, mis koosneb kõigist ekvivalentsiklassidest $(x)/\sim$, $x \in \mathbb{Q}$.

Ekvivalentsiklassi $a = (a_i)/\sim$ normiks $|a|_p$ loeme $\lim_{i \rightarrow \infty} |a_i|_p$. 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 10.18 ([10], lk. 11–12) *Igal ekvivalentsiklassil $a \in \mathbb{Q}_p$, mille korral $|a|_p \leq 1$, on täpselt üks esindaja (a_i) , kus $a_i \in \mathbb{Z}$, mis rahuldab tingimusi*

1. $0 \leq a_i < p^i$ 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 $|a|_p \leq 1$. 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 $|a'|_p \leq 1$. 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.

$$a'_i = b_0 + b_1 p + b_2 p^2 + \dots + b_{i-1} p^{i-1},$$

kus $b_j \in \{0, 1, \dots, p-1\}$. Tingimus $a'_i \equiv a'_{i+1} \pmod{p^i}$ tähendab seda, et

$$a'_{i+1} = b_0 + b_1 p + b_2 p^2 + \dots + b_{i-1} p^{i-1} + b_i p^i,$$

kus $b_i \in \mathbb{Z}$. Kuna $0 \leq a'_{i+1} < p^{i+1}$, siis $0 \leq b_i < p$. Järelikult iga i korral $a_i = a'_i p^{-m} = b_0 p^{-m} + \dots + b_{i-1} p^{i-1-m}$. Jada (a_i) , mis esindab arvu a , võib seega esitada kujul

$$a = \frac{b_0}{p^m} + \frac{b_1}{p^{m-1}} + \dots + \frac{b_{m-1}}{p} + b_m + b_{m+1}p + b_{m+2}p^2 + \dots \quad (31)$$

(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, \dots , kusjuures teatud kohast vasakul pool on neid lõplik arv ja paremal pool lõpmata palju. Võrdluseks: reaalarvu $b_0 b_1 \dots b_{m-1} b_m, b_{m+1} b_{m+2} \dots$ võib esitada kujul

$$\frac{b_0}{(10^{-1})^m} + \frac{b_1}{(10^{-1})^{m-1}} + \dots + \frac{b_{m-1}}{(10^{-1})^1} + b_m + b_{m+1}10^{-1} + b_{m+2}(10^{-1})^2 + \dots$$

p -aadiliste arvudega saab teha tehteid üsna analoogiliselt kümnendmurdudega. Toome siin mõned näited korpus \mathbb{Q}_7 (erinevalt kümnendmurdudest liigutakse laenamisele, korrutamisel jne. vasakult paremale):

$$\begin{array}{r} 3+6 \times 7+2 \times 7^2 + \dots \\ \times 4+5 \times 7+1 \times 7^2 + \dots \\ \hline 5+4 \times 7+4 \times 7^2 + \dots \\ \quad 1 \times 7+4 \times 7^2 + \dots \\ \hline \quad \quad 3 \times 7^2 + \dots \\ \hline 5+5 \times 5+4 \times 7^2 + \dots \end{array} \quad \begin{array}{r} 2 \times 7^{-1} + 0 \times 7^0 + 3 \times 7^1 + \dots \\ -4 \times 7^{-1} + 6 \times 7^0 + 5 \times 7^1 + \dots \\ \hline 5 \times 7^{-1} + 0 \times 7^0 + 4 \times 7^1 + \dots \end{array}$$

$$\begin{array}{r} 1+2 \times 7+4 \times 7^2 + \dots \\ \hline 1+6 \times 7+1 \times 7^2 + \dots \\ \quad 3 \times 7+2 \times 7^2 + \dots \\ \quad \hline \quad 3 \times 7+5 \times 7^2 + \dots \\ \quad \quad 4 \times 7^2 + \dots \\ \quad \quad \hline \quad \quad 4 \times 7^2 + \dots \end{array} \left| \begin{array}{r} 3+5 \times 7+1 \times 7^2 + \dots \\ \hline 5+1 \times 7+6 \times 7^2 + \dots \end{array} \right.$$

Lemma 10.19. Olgu K korpus ja $\| \cdot \|$ norm korpusel K . Kui $q \in K$ ja $\|q\| < 1$, siis

$$1 + q + q^2 + \dots = \frac{1}{1-q}. \quad (32)$$

Lisaks eespoolmainituile on p -aadilistel arvudel ja reaalarvudel teisigi sarnaseid omadusi.

Teoreem 10.20. p -aadiline arv $a = \sum_{i=-m}^{\infty} a_i p^i \in \mathbb{Q}_p$ on ratsionaalarv parajasti siis, kui tema numbrite jada (a_i) on mingist kohast alates perioodiline.

Näide 10.21. 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 (32) 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 $\frac{11}{8}$ esitada 3-aadilisena. Selleks esitame 11 ja 8 3-aadilisel kujul: $11 = 2 + 0 \cdot 3 + 1 \cdot 3^2$ ja $8 = 2 + 2 \cdot 3$. $\frac{11}{8}$ on siis nende jagatis:

$$\begin{array}{r} 2 + 0 \times 3 + 1 \times 3^2 \\ 2 + 2 \times 3 \\ \hline 1 \times 3 \\ \hline 1 \times 3 + 2 \times 3^2 + 1 \times 3^3 \\ \quad 1 \times 3^2 + 1 \times 3^3 + 2 \times 3^4 + 2 \times 3^5 + \dots \\ \quad \hline \quad 1 \times 3^2 + 1 \times 3^3 + 2 \times 3^4 \\ \quad \quad 2 \times 3^3 + 0 \times 3^4 + 2 \times 3^5 + \dots \\ \quad \quad \hline \quad \quad 2 \times 3^3 + 2 \times 3^4 \\ \quad \quad \quad \hline \quad \quad \quad 1 \times 3^4 + 1 \times 3^5 + \dots \end{array} \left| \begin{array}{r} 2 + 2 \times 3 \\ \hline 1 + 2 \times 3 + 2 \times 3^2 + 1 \times 3^3 + \dots \end{array} \right.$$

10.4. 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 $ax = b$. 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 alamkorpuseks sisaldavaid pärisalamkorpuseid, üle mille võrrand $x^2 + 1 = 0$ oleks lahenduv. Veelgi enam, kehtib järgmine teoreem.

Teoreem 10.22. *Kompleksarvude korpust \mathbb{C} on isomorfismi täpsuseni ainus minimaalne korpust, mis sisaldab alamkorpuseks 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 algebralsed võrrandid (selle kohta öeldakse ka, et korpust \mathbb{C} on *algebraliselt kinnine*).

Teoreem 10.23 (Algebra põhiteoreem.). *Igal mittekonstantsel polünoomil üle korpuse \mathbb{C} on olemas juur selles korpuses.*

Indeks

- algarv, 8
 - Mersenne'i, 19
- algarvukaksikud, 9
- algjuur, 26
- algtegueriks lahutus, 6
- assotsieeritud elemendid, 3

- Cauchy jada, 46

- Dedekindi lõige, 45

- Eratosthenese sõel, 8
- Eukleidese algoritm, 4
- Euleri funktsioon, 16
- Euleri kriteerium, 37

- faktoring, 32

- Gaussi ruutvastavussäädu, 39
- Goldbachi probleem, 10

- jäägiklass, 12
- jäägiklassikorpust, 14
- jäägiklassiring, 14
- Jacobi sümbol, 41
- jagaja, 3
- jagajate arv, 19
- jagajate summa, 19
- jagamine, 3
- jagatiste korpust, 44

- kaaselemendid, 31
- kongruents
 - lineaar-, 20
 - ruut-, 20, 37
 - tundmatut sisaldav, 20
- kongruentsi lahend, 20
- kongruentsus, 12
- kordne, 3
- korpuse
 - elemendi juur, 35
 - karakteristika, 30
 - laiend, 30
 - multiplikatiivne rühm, 27
 - primitiivne element, 31

- lõplik korpust, 30
- Legendre'i sümbol, 37

- Möbiuse funktsioon, 18
- mitteruutjääk, 37
- moodul, 12

- naturaalarvu standardkuju, 7
- norm, 47
 - p -aadiline, 47
 - arhimeediline, 47
 - mittearhimeediline, 47
- nulljada, 46

- p -aadiline arv, 48
- pööratavate elementide rühm, 3
- polünoomi lahutuskorpust, 32

- reaalarvude hulk, 45
- ruutjääk, 37, 41

- suurim ühistegur, 3

- täisosa
 - alumine, 10
- täiuslik arv, 19
- taandamisega poolrühm, 43
- taandumatu element, 3
- tegur, 3
- teoreem
 - algebra põhi-, 50
 - aritmeetika põhi-, 6
 - Dirichlet', 9
 - Euleri, 17
 - Fermat' suur, 11
 - Fermat' väike, 18
 - Gaussi, 17
 - Hiina jäägi-, 21
 - Tšebõševi, 9

- vahede rühm, 44
- vahim ühiskordne, 3

- ühejuur, 35
 - primitiivne, 35