TARTU RIIKLIK ÜLIKOOL

L. Kivistik, J. Gabovitš

ARVUTEOORIA

TARTU 1974

TARTU RIIKLIK ÜLIKOOL
Arvutusmatemaatika kateeder

L. Kivistik, J. Gabovitš

ARVUTEOORIA

Teine, ümbertöötatud trükk

TARTU 1974

Kinnitatud Matemaatikateaduskonna nõukogus
16. veebruaril 1973.a.

E E S S Õ N A

Käesolev õppevahend sisaldab kogu materjali, mis on ette nähtud riiklike ülikoolide arvuteooria programmis. Samal ajal on aga enamikke küsimusi käsitletud põhjalikumalt kui seda võimaldaks õppeplaanides arvuteooriale eraldatud loengutundide arv. Paragrahvid ja punktid, mis sisaldavad ainult programmivälist materjali, on märgitud tärniga. Tärniga on märgitud ka mõned raskemad harjutusülesanded.

Võrreldes esimese trükiga on uues, ümbertöötatud trükis tehtud rida täiendusi (näiteks lisatud III ja IX pt.), mis on peamiselt tingitud uue ametliku programmi kehtestamisest 1969. aastal. Ümbertöötamisel on parandatud esimeses trükis avastatud trükivead ja ebatäpsused ning märksa suurendatud harjutusülesannete arvu. Materjali esitamise järjekorda on kohati muudetud, endine kongruentse käsitlev peatükk on jaotatud kolmeks omaette peatükiks.

Täiendused ja parandused on tehtud L.Kivistiku poolt.

S I S S E J U H A T U S

Arvuteooria tekkis aritmeetika edasiarenemise tulemusena ja tema aineks oli esialgu naturaalarvude spetsiifiliste omaduste uurimine. Käesoleval ajal haarab arvuteooria märksa laiema probleemide hulga. Arvuteoorias käsitletakse mitte ainult naturaalarve, vaid paljudel juhtudel täisarvude ringi, ratsionaalarvude ja isegi reaalarvude ning kompleksarvude korpust.

Probleemid ja ülesanded, mis tekivad arvuteoorias, võib jaotada järgmisse nelja põhirühma.

1. Määramatute ehk diofantiliste võrrandite lahendamine. Diofantilisteks (kreeka matemaatiku Diophantose nime järgi , kes elas III saj.) nimetatakse täisarvuliste kordajatega algebralisi võrrandeid ja nende süsteeme, kus tundmatute arv on suurem võrrandite arvust. Selliste võrrandite lahendamise all mõistetakse tavaliselt kõigi täisarvuliste lahendite leidmist.

Lineaarsete ja teist järku diofantiliste võrrandite teooria on põhjalikult välja töötatud. Kõrgemat järku diofantiliste võrrandite lahendamiseks puudub aga üldine teooria. On teada vaid erivõtteid üksikute võrrandite lahendamiseks. Rida probleeme ootab veel lahendamist. Nii näiteks

pole teada, kas võrrand $x^4 + y^4 + z^4 = t^4$ on lahenduv. Samuti on tänapäevani lõpuni lahendamata kuulus Fermat' probleem võrrandi $x^n + y^n = z^n$ $(n \geqslant 3)$ lahenduvuse kohta jne.

2. Diofantiline lähendamine. Siia kuuluvad reaalarvude ratsionaalarvudega lähendamise küsimused (näiteks arvu π ratsionaalsete lähismurdude leidmine), samuti võrratuste lahendamine täisarvudes (näiteks võrratus $|\alpha x - y| < \frac{1}{x}$, kus α on antud irratsionaalarv). Efektiivseks meetodiks nende probleemide lahendamisel osutub ahelmurdude algoritm.

Diofantilise lähendamise alla kuulub ka transtsendentsete arvude teooria, mille tekkimine 19. sajandil on seotud transtsendentsete arvude olemasolu tõestamisega ja arvude e ja π transtsendentsuse näitamisega. Selle teooria edasises arengus on eriti suur nõukogude matemaatikute osa (A.O.Gelfond jt.).

3. Algarvude jaotus. Juba Eukleidesel leiame tõestuse selle kohta, et algarvude hulk on lõpmatu. 19. saj. tekkis probleem algarvude jaotumisest aritmeetilistes jadades. Vastuse sellele küsimusele andis L.Dirichlet' poolt tõestatud tähtis teoreem: iga aritmeetiline jada $\{an + b\}$, kus a ja b on ühistegurita arvud, sisaldab lõpmata palju algarve.

Rida algarvude jaotusega seotud küsimusi on tänapäevani veel lahendamata. Näiteks pole teada, kas algarve kujuga $2^p - 1$ on lõpmata palju (nn. Mersenne'i arvud). Puudub ka vastus analoogilisele küsimusele arvude kohta kujuga $n^2 + 1$ jne.

4. Aditiivsed probleemid. Need probleemid on seotud naturaalarvude (tavaliselt suurte arvude) lahutamisega kindlat tüüpi liidetavate summaks (näiteks naturaalarvude ruutude summaks, algarvude summaks jne.). Sealjuures püütakse kindlaks teha, milline on vähim vaadeldavat tüüpi liidetavate arv jne.

Kasutatavate meetodite poolest jaotatakse arvuteooria enamasti järgmisteks põhiharudeks (vt. näit. [2]).

1. Elementaarne arvuteooria. Siia kuuluvad loetletud põhiküsimustest ja probleemidest need, mis on lahendatavad peamiselt elementaarmatemaatika vahenditega, sealhulgas kongruentside teooria, mille loojaks oli saksa matemaatik C.F.Gauss (1777-1855), ahelmurdude teooria, mida arendasid L.Euler (1707-1783) ja prantsuse matemaatik J.Lagrange (1736-1813), ja paljud teised küsimused. Tuleb märkida, et arvuteooria meetodite elementaarsus ei tähenda veel nende lihtsust.

Arvuteooria elementaarsete meetodite loomisel on suuri teeneid väljapaistval vene matemaatikul P.L.Tšebõšovil (1821-1894), prantsuse matemaatikutel J.Liouville'il (1809--1882) ja C.Hermite'il (1822-1901), nõukogude matemaatikul L.G.Šnirelmanil (1905-1938) jt.

2. Analüütiline arvuteooria. Analüütiline arvuteooria kasutab matemaatilise analüüsi, reaal- ja kompleksmuutuja funktsioonide teooria, ridade teooria, tõenäosusteooria jt. matemaatika harude vahendeid. Arvuteooria selle haru loojaks on L.Euler. Suurt mõju analüütilise arvuteooria aren-

gule avaldasid C.F.Gaussi tööd.

Reaalarvude piirkonnas arendasid analüütilisi meetodeid saksa matemaatik L.Dirichlet (1805-1859) ja P.L.Tšebõšov, kompleksmuutuja funktsioonide teooriaga seotud analüütilist arvuteooriat arendas saksa matemaatik B.Riemann (1826-1866). Analüütilise arvuteooria edasiarendajatena tuleb veel märkida saksa matemaatikut H.Weyl'i (1885-1955), vene matemaatikut G.F.Voronoid (1868-1908), india matemaatikut S.Ramanudžani (1887-1920), inglise matemaatikuid G.Hardy't (1877--1947) ja J.Littlewoodi (sünd. 1885), saksa matemaatikut C.L.Siegelit. Võimsad analüütilised meetodid on välja töötanud nõukogude matemaatikud I.M.Vinogradov (sünd. 1891), A.O.Gelfond (1906-1968) ja J.V.Linnik (1915-1972).

3. Algebraline arvuteooria. See teooria, mis lähtub algebralise arvu mõistest, on loodud inglase J.Wallis'e (1616--1703), J.L.Lagrange'i ja L.Euleri poolt. Eriti tähtsad on siin saksa matemaatikute C.F.Gaussi, E.Kummeri (1810-1893), R.Dedekindi (1831-1916), L.Kroneckeri (1823-1891) ja väljapaistvate vene matemaatikute J.I.Zolotarjovi (1847-1878) ja G.F.Voronoi tööd. Kaasaegsetest välismaa matemaatikutest tuleb märkida H.Hasset ja C.L.Siegelit, nõukogude matemaatikutest N.G.Tšebotarjovi (1894-1947), B.V.Venkovi (sünd. 1900), I.R.Šafarevitšit (sünd. 1923).

4. Geomeetriline arvuteooria. Arvuteooria selles harus kasutatakse nn. ruumilisi võresid ehk täisarvuliste koordinaatidega punktide hulki. See teooria leiab rakendamist geomeetrias ja kristallograafias, arvuteoorias on ta seotud

täisarvuliste kordajatega ruutvormide teooriaga. Selle arvuteooria haru rajajateks on G.Minkovski (1864-1909), G.F.Voronoi ja F.Klein (1849-1925).

Käesolevas õppevahendis leiab vastavalt programmile käsitlemist peamiselt elementaarne arvuteooria. Mõningal määral kasutatakse ka analüütilise arvuteooria meetodeid.

I. TÄISARVUDE JAGUVUS

Käesolevas peatükis tähendagu sümbolid a, b, c, ..., x, y, ... täisarve. Nagu me varsti näeme, võime enamasti piirduda mittenegatiivsete täisarvudega, s.o. arvu null ja naturaalarvudega. Esitamata naturaalarvude aksiomaatilist definitsiooni, märgime, et naturaalarvud rahuldavad kaht järgmist põhilist aksioomi.*

Induktsiooniaksioom. Kui mingi naturaalarvude hulk sisaldab arvu 1 ja koos iga naturaalarvuga ka temale järgnevat naturaalarvu, siis ta sisaldab kõiki naturaalarve.

Archimedese aksioom. Iga kahe naturaalarvu a ja b jaoks eksisteerib kolmas naturaalarv c, nii et $bc > a$.

Induktsiooniaksioomist järeldub hästi tuntud täieliku induktsiooni printsiip.

§ 1. JAGAJA MÕISTE JA JAGUVUSE LIHTSAMAD OMADUSED

Olgu antud täisarvud a ja b. Kui leidub kolmas täisarv c, nii et $a = bc$, siis ütleme, et a jagub b-ga, ja kirjuta-

---

* Naturaalarvu mõiste range põhjendamine kuulub teoreetilise aritmeetika valdkonda. Naturaalarvude valla ja teiste arvuvaldade aksiomaatiline ülesehitus on esitatud näiteks raamatus J. H i o n. Elementaarmatemaatika kõrgemalt vaatekohalt, I. Algebra. TRÜ rotaprint, Tartu, 1962.

me $a \mid b$, ehk b on a jagaja ja märgime $b \mid a$. Siinjuures nimetame arvu b ka arvu a teguriks ja arvu a arvu b kordseks. Asjaolu, et d ei ole a jagaja, märgitakse tavaliselt nii: $d \nmid a$. Täisarvude jaguvusel on järgmised definitsioonist lihtsalt järelduvad omadused, mille kontrollimise jätame enamasti lugejale.*

Teoreem 1.1.

1° $a \mid a$ ja $a \mid 1$ iga a korral.

2° $0 \mid a$ iga a korral.

3° Kui $b \mid a$ ja $a \mid b$, siis $a = \pm b$.

4° Kui $a \mid b$ ja $b \mid c$, siis $a \mid c$.

5° Kui $a \mid c$, siis $ab \mid c$ iga b korral.

6° Kui $a \mid b$, siis $\pm a \mid (\pm b)$.

Märgime eriti, et omaduse 2° kohaselt $0 \mid 0$ ja et omadus 6° võimaldab jaguvusteoorias piirduda mittenegatiivsete täisarvudega.

Teoreem 1.2. Kui kehtib võrdus

$$c + d + \ldots + f = p + q + \ldots + s$$

ja kõigi liikmete kohta peale ühe on teada, et nad on arvu b kordsed, siis ka see ülejäänud üks on b kordne.

Teoreem 1.3. Kui a on b kordne ja $|a| < |b|$, siis $a = 0$.

Tõepoolest, kui $a = bc$, siis $|a| = |b| \cdot |c| < |b|$, millest $|c| < 1$. Et c on täisarv, siis $c = 0$.

Teoreem 1.4 (teoreem jäägiga jagamisest). Mistahes

---

*Selleks et hõlbustada viiteid eespool esitatud tulemustele, on siin ja edaspidi ka üsna lihtsaid omadusi nimetatud teoreemideks. Viimased on kõik nummerdatud.

täisarvude a ja $b \neq 0$ korral leidub parajasti üks täisarvude paar q, r, nii et

1) $0 \leq r < |b|$ ja 2) $a = qb + r$.

Siin nimetatakse a jagatavaks, b - jagajaks, q - mittetäielikuks jagatiseks, r - jäägiks.

Tõestus. 1) Eeldame algul, et $a > b > 0$. Vaatleme arvu b kordseid, s.o. arve 1b, 2b, 3b,... Archimedese aksioomi kohaselt leidub naturaalarv k, nii et $kb > a$. Järelikult leidub selline naturaalarv q, et

$$qb \leq a \quad \text{ja} \quad (q+1)b > a.$$

Tähistame $a - qb = r$; siis $r \geq 0$. Siit $a = qb + r$. Arvu q valiku tõttu

$$qb + b = (q+1)b > a = qb + r.$$

Seega $b > r$. Selle juhu jaoks on teoreem tõestatud.

2) Kui $a = b > 0$, siis $q = 1$, $r = 0$.

3) Kui $b > a > 0$, siis $q = 0$, $r = a$.

4) Kui $a < 0$, $b > 0$, siis on $-a > 0$ ja eelenva tõttu $-a = q_1 b + r_1$, $0 \leq r_1 < b$; siit

$$a = (-q_1)b - r_1.$$

Kui r_1 võrdub nulliga, siis teoreem on tõestatud. Kui aga $r_1 > 0$, siis tähistame

$$b - r_1 = r \quad \text{ja} \quad -q_1 - 1 = q.$$

Nüüd $0 < r < b$ ja $a = (q+1)b - b + r = qb + r$.

5) Kui $b < 0$, siis on $-b > 0$ ja seega $a = (-b)q + r$, $0 \leq r < |b|$, ehk $a = (-q)b + r$.

Tõestame lõpuks, et q ja r on üheselt määratud. Oletame, et

$$a = bq + r = bq_1 + r_1 ,$$

kus $0 \leq r < |b|$ ja $0 \leq r_1 < |b|$. Siis

$$b(q - q_1) = r_1 - r,$$

kusjuures $|r_1 - r| < |b|$. Et võrduse vasak pool jagub b-ga, siis teoreemide 1.2 ja 1.3 põhjal $|r_1 - r| = 0$ ehk $r_1 = r$. Seega ka $q_1 = q$.

Harjutusülesandeid.

1.1. Arv a = 42 157 andis jagamisel teatud positiivse arvuga b mittetäielikuks jagatiseks q = 231. Leida jagaja b ja jääk r.

1.2. Täisarvu a jagamisel 13-ga saadakse mittetäielik jagatis 17. Leida jagatava a suurim võimalik väärtus.

1.3. Tõestada, et kui viiekohaline arv jagub 41-ga, siis jaguvad 41-ga ka kõik arvud, mis saadakse antud arvust numbrite tsüklilise ümberpaigutuse teel.

1.4. Tõestada, et iga naturaalarvu n korral jagub korrutis $n(n+1)(2n+1)$ arvuga 6.

1.5. Tõestada, et $n(n^2+5)$ jagub arvuga 6.

1.6. Tõestada, et $n^5 - n$ jagub arvuga 30.

§ 2. SUURIM ÜHISTEGUR. EUKLEIDESE ALGORITM

Vaatleme vaid positiivseid arve ja nende positiivseid tegureid.

Arvude $a_1, a_2, \ldots, a_n$ ühisteguriks nimetatakse iga arvu b, millega jaguvad kõik need arvud. Arvudel $a_1, a_2, \ldots, a_n$ võib olla mitu ühistegurit, kuid ükski tegur ei saa olla suu-

rem kui $\min\{a_1, a_2, \ldots, a_n\}$. Kõige väiksem ühistegur on arv 1. Ühistegurite hulga suurimat elementi nimetatakse suurimaks ühisteguriks ja tähistatakse

$$d = (a_1, a_2, \ldots, a_n).$$

Arve, mille suurimaks ühisteguriks on arv 1, nimetatakse ühistegurita arvudeks. Märgime, et ühistegurita arvude hulga osahulgad võivad olla ühisteguriga. Nii on näiteks arvud 6, 10, 15 ühistegurita, kuid paarikaupa ühisteguriga.

Teoreem 1.5. Kui a on b kordne, siis a ja b ühistegurite hulk ühtib b tegurite hulgaga, kusjuures

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

Tõestus. Olgu $a = bk$. Siis a ja b iga ühistegur on ka b teguriks. Vastupidi, teoreemi 1.1 põhjal on arvu b iga tegur korrutise $bk = a$ teguriks. Seega a ja b ühistegurite hulk ühtib b tegurite hulgaga. Siis ühtivad ka nende hulkade suurimad elemendid.

Teoreem 1.6. Kui $a = bq + r$, siis a ja b ühistegurite hulk ühtib b ja r ühistegurite hulgaga ja

$$(a,b) = (b,r).$$

Tõestus. Teoreemi 1.2 kohaselt peab a ja b iga ühistegur olema arvu r teguriks, s.t. b ja r ühisteguriks. Vastupidi, b ja r iga ühistegur peab olema a teguriks, s.t. a ja b ühisteguriks. Ühtivad ka ühistegurite hulkade suurimad elemendid:

$$(a,b) = (b,r).$$

Edasi vaatleme Eukleidese algoritmi, mis seisneb järgne-

vas. Olgu a ja b täisarvud, kusjuures $b>0$. Teoreemi 1.4 kohaselt kirjutame välja võrdused

$$
\begin{aligned}
a &= bq_1 + r_1 && (0 < r_1 < b),\\
b &= r_1q_2 + r_2 && (0 < r_2 < r_1),\\
r_1 &= r_2q_3 + r_3 && (0 < r_3 < r_2),\\
&\dots\dots\dots\dots\dots\dots\dots\dots\\
r_{k-2} &= r_{k-1}q_k + r_k && (0 < r_k < r_{k-1}),\\
r_{k-1} &= r_kq_{k+1} && (r_{k+1} = 0).
\end{aligned}
\tag{1}
$$

Võrduste ahelik (1) lõpeb, kui mingi jääk $r_{k+1} = 0$. Nulliga võrduva jäägi tekkimine on sealjuures mõõdapäästematu, sest

$$b > r_1 > r_2 > r_3 > \dots \geqslant 0$$

ja seega ei saa jadas $b, r_1, r_2, \dots$ olla rohkem kui b elementi.

Märgime, et kuna $r_k < r_{k-1}$, siis $q_{k+1} \geqslant 2$.

Võrdustest (1) järeldub teoreemi 1.6 tõttu, et

$$(a,b) = (b,r_1) = (r_1,r_2) = \dots = (r_{k-1},r_k) = r_k,$$

kusjuures a ja b ühistegurite hulk ühtib r_k tegurite hulgaga. Saime järgmise tulemuse:

Teoreem 1.7. Arvude a ja b ühistegurite hulk ühtib Euklleidese algoritmi viimase nullist erineva jäägi r_k tegurite hulgaga ja

$$(a,b) = r_k.$$

Järeldus. $k|a$ ja $k|b$ parajasti siis, kui $k|(a,b)$, ehk teisiti: arvude a ja b ühistegurite hulk ühtib nende arvude suurima ühisteguri tegurite hulgaga.

Teoreem 1.8. Kehtib valem: $(am,bm) = (a,b)m$.

Tõestuseks tarvitseb kõik võrdused (1) arvuga m läbi

korrutada. Tulemus on samaväärne Eukleidese algoritmi rakendamisega arvudele am ja bm. Siis aga

$$(am,bm) = r_k m = (a,b)m.$$

Teoreem 1.9. Kui c on arvude a ja b mingi ühistegur, siis

$$\left(\frac{a}{c}, \frac{b}{c}\right) = \frac{(a,b)}{c}.$$

Tõestus. Eelmise teoreemi põhjal

$$(a,b) = \left(c\cdot\frac{a}{c},\ c\cdot\frac{b}{c}\right) = c\left(\frac{a}{c},\ \frac{b}{c}\right).$$

Järeldus. $\left(\frac{a}{(a,b)},\ \frac{b}{(a,b)}\right) = 1$, s.t. arvude jagamisel nende suurima ühisteguriga saame ühistegurita arvud.

Teoreem 1.10. Kui $(a,b) = 1$, siis $(ac,b) = (c,b)$.

Tõestus. Et $b \mid (ac,b)$, siis $bc \mid (ac,b)$. Kuna ka $ac \mid (ac,b)$, siis $c = (ac,bc) \mid (ac,b)$. Järelduse põhjal teoreemist 1.7 saame

$$(b,c) \mid (ac,b).$$

Vastupidi, $b \mid (b,c)$ ja $ac \mid (b,c)$; seega järelduse põhjal teoreemist 1.7 $(b,ac) \mid (b,c)$. Teoreemi 1.1 põhjal on siis

$$(ac,b) = (c,b).$$

Teoreem 1.11. Kui $(a,b) = 1$ ja $ac \mid b$, siis $c \mid b$.

Tõepoolest, eelmise teoreemi põhjal $(ac,b) = (c,b)$. Et aga $ac \mid b$, siis teoreemi 1.5 kohaselt $(ac,b) = b$ ja seega ka $(c,b) = b$, s.t. c on b kordne.

Teoreem 1.12. Kui $(a_i,b) = 1 \quad (i=1,\ldots,n)$, siis

$$(a_1a_2\ldots a_n,b) = 1.$$

Tõestus. Teoreemi 1.10 põhjal $(a_1a_2\ldots a_n,b) =$

$= (a_2 \ldots a_n, b) = \ldots = (a_n, b) = 1.$

Teoreem 1.13. Kui $(a_i, b_j) = 1$, kus $i=1,2,\ldots,m$ ja $j=1,2,\ldots,n$, siis

$$(a_1 a_2 \ldots a_m,\ b_1 b_2 \ldots b_n) = 1.$$

Teoreem 1.13 on järeldus teoreemidest 1.10 ja 1.12.

Rohkem kui kahe arvu

$$a_1,\ a_2,\ \ldots,\ a_n \qquad (n > 2)$$

suurima ühisteguri leidmine taandub arvupaaride ühistegurite leidmisele:

Teoreem 1.14. Olgu

$$(a_1, a_2) = d_1,\quad (d_1, a_3) = d_2, \ldots, (d_{n-2}, a_n) = d_{n-1}.$$

Siis

$$d_{n-1} = (a_1, a_2, \ldots, a_n).$$

Tõestus. Järelduse põhjal teoreemist 1.7 ühtib arvude a_1 ja a_2 ühistegurite hulk arvu d_1 tegurite hulgaga; arvude a_1, a_2, a_3 ühistegurite hulk ühtib seega d_1 ja a_3 ühistegurite hulgaga, s.o. d_2 tegurite hulgaga. Edasi, a_1, a_2, a_3, a_4 ühistegurite hulk ühtib d_2 ja a_4 tegurite hulgaga, s.o. d_3 tegurite hulgaga jne. Lõpuks saame, et arvude a_1, a_2, ..., a_n ühistegurite hulk ühtib d_{n-1} tegurite hulgaga. Nende hulkade suurimad elemendid on sealjuures võrdsed:

$$(a_1, a_2, \ldots, a_n) = d_{n-1}.$$

Teoreemi 1.14 võib esitada ka kujul

$$(a_1, a_2, \ldots, a_{n-1}, a_n) = ((a_1, a_2, \ldots, a_{n-1}), a_n).$$

Harjutusülesandeid.

1.7. Leida arvude järgmised suurimad ühistegurid:

a) (6188, 4709);

b) (81 719, 52 003);

c) (81 719, 52 003, 33 649);

d) (42 914, 66 397).

1.8. On antud a = 899 ja b = 493. Leida d = (a,b) ja määrata x ja y nii, et d = ax + by.

1.9. Tõestada teoreemide 1.8 ja 1.9 üldistused:

a) $(ma_1, ma_2, \ldots, ma_n) = m(a_1, a_2, \ldots, a_n)$;

b) $\left(\frac{a_1}{c}, \frac{a_2}{c}, \ldots, \frac{a_n}{c}\right) = \frac{(a_1, a_2, \ldots, a_n)}{c}$, kui c on arvude $a_1, a_2, \ldots, a_n$ mingi ühine tegur.

§ 3. VÄHIM ÜHISKORDNE

Olgu antud positiivsed täisarvud $a_1, a_2, \ldots, a_n$. Iga täisarvu, mis on kõikide nende arvude kordne, nimetatakse arvude $a_1, a_2, \ldots, a_n$ <u>ühiskordseks</u>. Üheks ühiskordseks on korrutis $a_1a_2\ldots a_n$. Kuid ka iga korrutis $ka_1a_2\ldots a_n$, kus k on täisarv, on nende arvude ühiskordne. Seega on arvude ühiskordseid lõpmata palju. Ühiskordseks on samuti arv 0. Järelikult eksisteerib väikim positiivne ühiskordne. Viimast nimetatakse arvude $a_1, a_2, \ldots, a_n$ <u>vähimaks ühiskordseks</u> ja märgitakse

$$m = [a_1, a_2, \ldots, a_n].$$

On selge, et $0 < m \leq a_1a_2\ldots a_n$.

<u>Teoreem 1.15.</u> Arvude iga ühiskordne jagub vähima ühiskordsega.

<u>Tõestus.</u> Olgu M arvude $a_1, a_2, \ldots, a_n$ mingi ühiskord-

ne. Siis teoreemi 1.4 kohaselt

$$M = mq + r, \quad 0 \leq r < m.$$

Viimasest võrdusest järeldub teoreemi 1.2 põhjal, et ka r peab olema nende arvude ühiskordne. Kuid $r < m$ ja m on arvude vähim ühiskordne. Järelikult $r = 0$ ja

$$M = mq.$$

Järeldus. Arvude a ja b ühiskordsete hulk $\{M\}$ ühtib arvu m kordsete hulgaga $\{mq\}$.

Teoreem 1.16. Olgu antud n arvu $a_1, a_2, \ldots, a_n$ ja olgu $m_1 = [a_1, a_2]$, $m_2 = [m_1, a_3]$, $\ldots$, $m_{n-1} = [m_{n-2}, a_n]$. Siis

$$m_{n-1} = [a_1, a_2, \ldots, a_n].$$

Tõestus. Järelduse põhjal teoreemist 1.15 ühtib a_1 ja a_2 ühiskordsete hulk arvu m_1 kordsete hulgaga. Samal põhjusel ühtib a_1, a_2 ja a_3 kordsete hulk m_1 ja a_3 ühiskordsete hulgaga, s.o. m_2 kordsete hulgaga. Edasi ühtib a_1, a_2, a_3 ja a_4 ühiskordsete hulk m_2 ja a_4 ühiskordsete hulgaga, s.o. m_3 kordsete hulgaga jne. Lõpuks ühtib $a_1, a_2, \ldots, a_n$ ühiskordsete hulk m_{n-1} kordsete hulgaga. Siis on aga võrdsed ka nende hulkade vähimad elemendid, s.o.

$$[a_1, a_2, \ldots, a_n] = m_{n-1}.$$

Teoreemi 1.16 võib esitada ka kujul

$$[a_1, a_2, \ldots, a_{n-1}, a_n] = [[a_1, a_2, \ldots, a_{n-1}], a_n].$$

Teoreem 1.17. Kehtivad järgmised valemid:

(1) $[a_1, a_2, \ldots, a_n](A_1, A_2, \ldots, A_n) = a_1a_2\ldots a_n$,

(2) $(a_1, a_2, \ldots, a_n)[A_1, A_2, \ldots, A_n] = a_1a_2\ldots a_n$,

kus

$$A_i = \frac{a_1 a_2 \dots a_n}{a_i} .$$

Tõestus. Tõestame seose (1). Selleks tähistame $A = a_1 a_2 \dots a_n$, $d = (A_1, A_2, \dots, A_n)$, $m = [a_1, a_2, \dots, a_n]$ ja $x = \frac{A}{d}$. Kuna

$$x = a_1 \frac{A_1}{d} = a_2 \frac{A_2}{d} = \dots = a_n \frac{A_n}{d}$$

ja $\frac{A_i}{d}$ $(i=1,2,\dots,n)$ on täisarv, siis iga i korral $x : a_i$ ja x on arvude $a_1, a_2, \dots, a_n$ ühiskordne ning jagub nende vähima ühiskordsega m, s.t.

$$\frac{A}{d} = x = mq.$$

Siis aga

$$\frac{A_1}{d} = \frac{m}{a_1} q, \ \dots, \ \frac{A_n}{d} = \frac{m}{a_n} q.$$

Kuna viimaste võrduste vasakud pooled on ühistegurita, paremal on aga ühine tegur q, siis $q = 1$. Seega $\frac{A}{d} = m$, mida oligi tarvis tõestada.

Näidata analoogiliselt seose (2) kehtivus!

Järeldus. Kehtib valem:

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

Tõestuseks tarvitseb võtta valemites (1) või (2) $n = 2$.

Et Eukleidese algoritmi abil on leitav iga kahe arvu suurim ühistegur, siis on seosest (3) leitav ka iga kahe arvu vähim ühiskordne.

Teoreem 1.18. Paarikaupa ühisjagajata arvude vähim ühiskordne võrdub nende arvude korrutisega, s.t. kui

$$(a_i, a_j) = 1, \quad i,j=1,2,\dots,n \ \text{ja} \ i \neq j,$$

siis

$$[a_1, a_2, \ldots, a_n] = a_1a_2\ldots a_n.$$

Tõestus. Kui n = 2, siis järeldub tõestus seosest (3). Üldjuhu

$$m_1 = [a_1, a_2] = a_1a_2 \quad , \quad (m_1, a_3) = 1,$$
$$m_2 = [m_1, a_3] = a_1a_2a_3 \quad , \quad (m_2, a_4) = 1,$$
$$m_3 = [m_2, a_4] = a_1a_2a_3a_4 \quad , \quad (m_3, a_5) = 1,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots,$$
$$m_{n-1} = a_1a_2\ldots a_n.$$

Järeldus. Kui c jagub arvudega $a_1, a_2, \ldots, a_n$ ja viimased on paarikaupa ühisjagajata, siis c jagub korrutisega $a_1a_2\ldots a_n$.

Tõepoolest, c on arvude $a_1, \ldots, a_n$ ühiskordne. Seega jagub ta vähima ühiskordsega $a_1a_2\ldots a_n$.

Harjutusülesandeid.

1.10. Leida arvude järgmised vähimad ühiskordsed:

a) [10 001, 8103];

b) [8407, 21 111];

c) [511, 803, 1095];

d) [391, 437, 299].

1.11. Tõestada seos:

$$[1,2,3,\ldots,2n] = [n+1, n+2, \ldots, 2n].$$

§ 4. ALGARVUD

1. Naturaalarvu vähim ühest erinev jagaja. Naturaalarvude hulgas on vaid arvul 1 üksainus positiivne jagaja, kõigil teistel naturaalarvudel on vähemalt kaks jagajat: arv 1 ja see arv ise. Naturaalarve, millel on parajasti kaks erinevat jagajat, nimetatakse algarvudeks. Naturaalarve, mis peale ühe ja iseendaga jagumise jaguvad veel vähemalt mingi kolmanda naturaalarvuga, nimetatakse kordarvudeks.

Kordarv a on iseloomustatud sellega, et leidub arv b, kus $1 < b < a$, nii et $a:b$. Algarve tähistame tavaliselt sümbolitega p ja q, kasutades vajaduse korral veel indekseid.

Teoreem 1.19. Ühest suurema naturaalarvu vähim ühest erinev jagaja on algarv.

Tõestus. Olgu arvu a vähim ühest erinev jagaja b $(1 < b \leq a)$,

$$a = bc.$$

Oletame, et b ei ole algarv. Siis on ta kordarv ja jagub mingi arvuga q,

$$b = qs, \quad 1 < q < b.$$

Seega

$$a = q(cs), \quad q < b.$$

Et aga b on vähim ühest erinev jagaja, siis oletus, et eksisteerib q, mis on nimetatud omadusega, ei pea paika.

Teoreem 1.20. Kordarvu a vähim ühest erinev jagaja ei ületa reaalarvu $\sqrt{a}$.

Tõestus. Olgu p vähim jagaja. Siis $a = pb$. Et p on vähim jagaja, siis

$$b \geq p.$$

Korrutame võrratust arvuga $a = pb$. Saame

$$ab \geq p^2 b,$$

millest

$$p \leq \sqrt{a}.$$

Teoreemi abil saab kindlaks teha, kas antud arv a on algarv või kordarv. Selleks tarvitseb proovida, kas arvul a leidub jagajaid $p \leq \sqrt{a}$. Kui leidub, siis a on kordarv, kui ei, siis algarv. Samaaegselt saab jagajad leida. Näiteks selleks, et teha kindlaks, kas 337 on algarv või kordarv, leiame kõigepealt, et $\sqrt{337} = 18,....$, ja seejärel kontrollime, kas 337 jagub algarvudega 2, 3, 5, 7, 11, 13, 17. Osutub, et ei jagu. Järelikult on 337 algarv.

2. <u>Algarvude hulga lõpmatus. Algarvude tabelid</u>.

<u>Teoreem 1.21</u>. Algarvude hulk on lõpmatu.

Vaatleme Eukleidese poolt umbes 2500 a. tagasi antud vastuväitelist tõestust.

Oletame, et algarve on lõplik hulk ja kirjutame nad kõik välja kasvavas järjekorras:

(1) $$p_1 = 2, \quad p_2 = 3, \quad p_3 = 5, \ \ldots, \ p_n.$$

Moodustame naturaalarvu

(2) $$a = p_1 p_2 \ldots p_n + 1.$$

Et p_n on suurim algarv ja $a > p_n$, siis a ei ole algarv. Seega peab a olema kordarv ja tal peab olema algarvulisi jagajaid. Seetõttu

$$a : p_i,$$

kus p_i on mingi algarv jadast (1). Et võrduse (2) vasak pool

ja esimene liidetav paremal jagub p_i-ga, siis peab jaguma p_i-ga ka teine liidetav, s.t. $1 \vdots p_i$. See on aga võimatu, sest $p_i > 1$. Vastuolu tuli oletusest, et algarve on lõplik hulk. Teoreem on tõestatud.

Järeldus. Arv kujul (2), kus p_1, p_2, ..., p_n on n esimest järjestikust algarvu, on kas algarv või tema väikim algarvuline jagaja on suurem kui p_n.

Praeguseni pole meetodit, mis lubaks iga antud arvu kohta praktiliselt öelda, kas ta on algarv või kordarv. Sellise meetodi leidmine on arvuteooria üks raskemaid probleeme ja tema lahendamine oleks tõeliseks suursündmuseks. Väiksemate arvude puhul saab kasutada proovimismeetodit, kusjuures proovimist hõlbustavad algarvude tabelid.

Selleks, et küsimust lahendada arvu N kohta, on vaja tabelit, mis haarab algarvud kuni reaalarvuni $\sqrt{N}$.

Käesolevaks ajaks on algarvude tabelid viidud üsna suurte arvudeni. Tuntuimad neist on ameeriklase D.N.Lehmeri poolt koostatud ja 1914.a. ilmunud tabelid, mis sisaldavad kõiki algarve kuni algarvuni 10 006 721. Märgime, et nimetatud tabelid ilmusid 1967. aastal trükist venekeelse väljaandena (Д.Н.Лемер. Таблицы простых чисел от 1 до 10 006 721). 1959.a. koostasid C.L.Baker ja F.J.Gruenberger algarvude tabeli, mis sisaldab kõiki algarve kuni arvuni

$$p_{6000000} = 104\ 395\ 301.$$

See tabel ei ole trükis avaldatud, vaid on paljundatud mikrofilmina.

Algarvude tabelite koostamiseks kasutatakse kuni tänа-

seni Eratosthenese poolt III sajandil e.m.a. väljatöötatud lihtsat meetodit (nn. Eratosthenese "sõel") või selle meetodi modifikatsioone. Vaatleme Eratosthenese meetodit arvu N mitte ületavate algarvude tabeli koostamiseks.

Kirjutame välja kõik naturaalarvud alates arvust 2 ja lõpetades arvuga N:

(3) 2, 3, 4, 5, 6, 7, 8, 9, ..., N.

Esimene arv 2 jagub ainult arvuga 1 ja iseendaga. Järelikult on 2 algarv. Kriipsutame jadas (3) läbi kõik arvu 2 kordsed peale arvu 2 enda. Pärast 2 on esimene läbikriipsutamata arv 3. See ei jagu 2-ga, sest muidu oleks ta läbi kriipsutatud. Järelikult 3 jagub vaid 1 ja iseendaga ja on seepärast algarv. Kriipsutame jadas läbi kõik arvu 3 kordsed peale 3, s.o. iga kolmanda arvu alates arvust 6. Sealjuures loendame ka juba läbikriipsutatud arve. Järgmine läbikriipsutamata arv on 5. Ta ei jagu algarvudega 2 ja 3 (muidu oleks ta läbi kriipsutatud). Järelikult jagub 5 vaid arvu 1 ja iseendaga ning on algarv. Nüüd kriipsutame läbi arvu 5 kordsed, s.o. iga viienda arvu alates arvust 10. Analoogiliselt toimime edasi. Lõpuks jadas läbikriipsutamata jäänud arvud ongi kõik algarvud vahemikust 1 kuni N.

Märgime, et kui on juba läbi kriipsutatud kõik algarvust p väiksemate algarvude kordsed, siis kõik allesjäänud arvud, mis on väiksemad kui p^2, on algarvud. Tõepoolest, iga kordarv a, mis on väiksem kui p^2, on juba läbi kriipsutatud, sest tal on algarvuline jagaja $q \leqslant \sqrt{a} < p$ ja q kordsed on kõik läbi kriipsutatud. Siit järelduvad järgmised tulemused.

Teoreem 1.22. Algarvude tabeli koostamisel Eratosthenese meetodil võib järjekordse algarvu p kordsete läbikriipsutamist alustada arvust p^2.

Teoreem 1.23. Arvu N mitte ületavate algarvude tabeli koostamine on lõpetatud, kui on läbi kriipsutatud arvu $\sqrt{N}$ mitte ületavate algarvude kõik kordsed.

Niisiis, algarvude tabeli koostamiseks näiteks 100 piires tuleb läbi kriipsutada arvude 2, 3, 5 ja 7 kordsed. Tabeli koostamiseks ei tarvitse välja kirjutada kõiki naturaalarve 2 kuni 100. Piisab kui joonestame järgmise tabeli:

	0	1	2	3	4	5	6	7	8	9
00	-	-	o	o	x	o	x	o	x	x
10	x	o	x	o	x	x	x	o	x	o
20	x	x	x	o	x	x	x	x	x	o
30	x	o	x	x	x	x	x	o	x	x
40	x	o	x	o	x	x	x	o	x	x
50	x	x	x	o	x	x	x	x	x	o
60	x	o	x	x	x	x	x	o	x	x
70	x	o	x	o	x	x	x	x	x	o
80	x	x	x	o	x	x	x	x	x	o
90	x	x	x	x	x	x	x	o	x	x

Igale ruudule vastab tabelis parajasti üks 100-st väiksem naturaalarv. Arvu läbikriipsutamist võib märkida ristikesega vastavas ruudus. 2 ja 5 kordsed võib läbi kriipsutada veergude kaupa. Tühjaks jäänud ruutudele vastavad nüüd algarvud. Tähistame need ruudud ringikestega.

3. Erikujulisi algarve. Peale suurte algarvude, mida võib leida koostatud algarvude tabelitest, on teada veel mõningaid erikujulisi algarve, mis asuvad kaugel väljaspool olemasolevate tabelite piire. Selliseid suuri algarve on leitud Mersenne'i arvude hulgast. Mersenne'i arvudeks - prantsuse matemaatiku M.Mersenne'i (1588-1648) nime järgi - nimetatakse arve

$$M_n = 2^n - 1.$$

Teoreem 1.24. Selleks, et Mersenne'i arv oleks algarv, on tarvilik (kuid mitte piisav), et astendaja n oleks algarv.

Tõepoolest, kui n on kordarv, n = mk, siis

$$M_n = 2^n - 1 = (2^m)^k - 1$$

jagub arvuga $2^m - 1 > 1$, s.t. M_n on siis kordarv. Tingimuse mittepiisavus järeldub näiteks sellest, et $M_{11} = 2047 = 23 \cdot 89$.

Niisiis M_4, M_6, M_8, M_9, ... on kordarvud. M_2, M_3, M_5, M_7, ... võivad olla algarvud ja esimesed neist ongi: $M_2 = 3$, $M_3 = 7$, $M_5 = 31$, $M_7 = 127$.

Tarviliku ja piisava tingimuse selleks, et Mersenne'i arv M_p oleks algarv, annab järgmine teoreem, mille tõestuse võib leida näiteks raamatust [9], lk. 43-46.

Teoreem 1.25. Arv $M_p = 2^p - 1$ on paaritu algarvu p korral algarv parajasti siis, kui rekurrentse jada

$$s_1 = 4, \quad s_2 = 14, \ldots, \quad s_k = s_{k-1}^2 - 2, \ldots$$

element s_{p-1} jagub arvuga M_p.

Tuginedes sellele teoreemile kontrolliti 1971. aastaks elektronarvutite abil läbi kõik 20 000-st väiksema indeksiga Mersenne'i arvud. Osutus, et nende hulgas on vaid 24 algarvu, mis saadakse järgmistel p väärtustel: 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4353, 4423, 9689, 9941, 11213, 19937. Neist viimane, $2^{19937} - 1 = 4315424797...0968041471$ koosneb 6002-st numbrist ja oli 1971. aastaks suurim teadaolev algarv (numbrite arvu saab lihtsalt leida kümnendlogaritmide abil:

$\log 2^{19937} = 19937 \cdot \log 2 = 19937 \cdot 0{,}30103 = 6001{,}6$).

Teiseks puudutame Fermat' algarve. Fermat' arvudeks - prantsuse matemaatiku Pierre Fermat' (1601-1665) nime järgi - nimetatakse arve kujul

$$F_k = 2^{2^k} + 1, \quad k \geqslant 0.$$

Fermat' arvude juurde jõuame, kui püüame leida tingimust, millise n korral $2^n + 1$ on algarv.

Teoreem 1.26. Arv $2^n + 1$ võib olla algarv vaid juhul, kui $n = 2^k$.

Tõestus. Kõigepealt märgime, et kui n on paaritu, jagub $2^n + 1$ alati kolmega:

$$2^n + 1 = (2+1)(2^{n-1} - 2^{n-2} + 2^{n-3} - \ldots + 1).$$

Niisiis juhul, kui $2^n + 1$ on algarv, on n paarisarv. Paarisarv võib aga olla vaid kujuga 2^k või $2^k q$, kus $k > 0$ ja q on ühest suurem paaritu naturaalarv, Kui $n = 2^k q$, siis lahutub $2^n + 1$ teguriteks:

$$2^n + 1 = 2^{2^k q} + 1 = \left(2^{2^k}\right)^q + 1 = A^q + 1 =$$

$$= (A+1)(A^{q-1} - A^{q-2} + A^{q-3} - \ldots + 1),$$

kus $A = 2^{2^k}$. Seega võib $2^n + 1$ olla algarv vaid juhul, kui $n = 2^k$.

Fermat pani tähele, et esimesed arvud $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65\,537$ on algarvud ja oletas, et kõik F_k on algarvud. See hüpotees püsis üle 100 aasta, sest juba järgmine Fermat' arv

$$F_5 = 2^{2^5} + 1 = 4\,296\,961\,297$$

on niivõrd suur, et tema alg- või kordarvulisust oli väga raske tõestada. Alles Euler leidis, et F_5 ei ole algarv, vaid avaldub algarvude 641 ja 6 700 417 korrutisena. Praeguseni pole teada ühtki Fermat' algarvu peale esimese viie. Mõnekümne kohta on teada, et nad on kordarvud. Tõestatud on see kõikide indeksite korral vahemikust 5 kuni 16, aga ka mõnede suuremate indeksite, näiteks 452 ja 1945 korral. Lahendamata on küsimus, kas Fermat' algarve on lõplik või lõpmatu hulk. Ka Fermat' arve on viimasel ajal hakatud uurima elektronarvutite abil. Fermat' arvude tegurite leidmine tugineb peamiselt järgmisele teoreemile.

Teoreem 1.27. Kui $k > 1$, siis F_k iga algarvuline tegur on kujuga

$$p = m \cdot 2^{k+2} + 1.$$

Näiteks on tõestatud, et arvu F_{1945} vähim jagaja on $p = 5 \cdot 2^{1947} + 1$.

Teoreemi 1.27 tõestuse võib leida raamatust [9], lk. 47.

Fermat' arvud esinevad ringjoone võrdseteks osadeks jaotamise probleemis. Nimelt tõestas Gauss, et sirkli ja joonlaua abil saab ringjoont jaotada n võrdseks osaks parajasti siis, kui $n = 2^k p_1 p_2 \ldots p_n$, kus $k \geqslant 0$ ja $p_1, p_2, \ldots, p_n$ on erinevad Fermat' algarvud.

Peale ebaõnnestunud funktsiooni $F_n = 2^{2^n} + 1$ on püütud leida ka teisi funktsioone, mis annaksid ainult algarve. Euler uuris sellest seisukohast polünoome. Ta leidis, et polünoomi

$$n^2 + n + 17$$

väärtusteks on algarvud, kui $n = 0,1,\ldots,16$. Analoogiliselt on polünoomi

$$2n^2 + 29$$

väärtused algarvud, kui $n = 0,1,\ldots,28$; polünoomi

$$n^2 + n + 41$$

väärtused on algarvud, kui $n = 0,1,\ldots,40$; polünoomi

$$n^2 - 79n + 1601$$

väärtused on algarvud, kui $n = 0,1,\ldots,79$. Tekib küsimus, kas ei leidu polünoomi, mille väärtused on iga täisarvulise n korral algarvud. Euler tõestas, et sellist polünoomi ei leidu. Nimelt kehtib järgmine teoreem.

Teoreem 1.28. Ühegi täisarvuliste kordajatega kõrgema kui nullastme polünoomi väärtused ei ole argumendi täisarvulistel väärtustel kõik algarvud.

Tõestus. Olgu

$$f(n) = a_0 + a_1 n + a_2 n^2 + \ldots + a_k n^k ,$$

kusjuures $f(c)$ olgu algarv:

$$f(c) = a_0 + a_1 c + a_2 c^2 + \ldots a_k c^k = p.$$

Arvutame

$$f(c+pt) = a_0 + a_1(c+pt) + a_2(c+pt)^2 + \ldots + a_k(c+pt)^k.$$

Olles avanud sulud ja võtnud kokku liikmed, kus puudub p, saame $f(c) = p$. Ülejäänud liikmed annavad p sulgude ette võtmisel sulgudes naturaalarvu

$$N = a_1 t + 2a_2 ct + a_2 pt^2 + \ldots = N_k(t),$$

s.o. t suhtes k-astme polünoomi väärtuse. Seega

$$f(c+pt) = p(1+N_k(t)).$$

Loeme t täisarvuliseks muutujaks. Et vasak pool ei ole konstant, siis $N_k(t)$ ei saa olla samaselt null. Seega on $N_k(t)$ kõikidel t väärtustel nullist erinev, välja arvatud lõplik arv võrrandi $N_k(t) = 0$ juuri, kui viimaste hulgas on täisarve. Tegur $1+N_k(t)$ on siis ühest erinev ja $f(c+pt)$ on kordarv. Niisiis, kui $f(c) = p$ on algarv, võib $f(c+pt)$ olla algarv vaid lõpliku arvu t väärtuste korral.

Väga oluline lahendamata probleem on sellise funktsiooni f(x) leidmine, mille väärtus kohal n võrduks n-nda algarvuga p_n ehk teiste sõnadega n-nda algarvu valemi leidmise probleem. Poola matemaatiku W.Sierpiński poolt on küll tõestatud, et leidub reaalarv α, nii et*

$$p_n = \left[\alpha \cdot 10^{2^n}\right] - 10^{2^n} \left[\alpha \cdot 10^{2^{n-1}}\right],$$

mis nagu lubaks p_n arvutada, kuid α täpne väärtus pole teada. On teada selle reaalarvu (arvatavasti irratsionaalarvu) mõned esimesed kohad (vt. [2], lk. 239). On teada ka teisi

---

* [a] tähistab arvu a täisosa.

analoogilisi valemeid, kuid need on sama laadi puudustega.

4. Algarvud aritmeetilistes jadades. Algarvud on peale arvu 2 kõik paaritud. Seega saab kõiki algarve, välja arvatud arv 2, esitada kujul 2n+1. Jada $\{2n+1\}$ saab aga jaotada osajadadeks $\{4n+1\}$ ja $\{4n-1\}$:

$$3, 7, 11, 15, \ldots, 4n - 1, \ldots ,$$

$$5, 9, 13, 17, \ldots, 4n + 1, \ldots$$

Seega peituvad kõik paaritud algarvud jadades $\{4n-1\}$ ja $\{4n+1\}$. Saab tõestada, et mõlemad osajadad sisaldavad lõpmata palju algarve. Tõestame näiteks järgmise teoreemi.

Teoreem 1.29. Jadas $\{4n-1\}$ on lõpmata palju algarve.

Tõestus. Oletame, et algarve kujuga 4n-1 on lõplik hulk. Olgu need

$$p_1, p_2, \ldots, p_k. \tag{4}$$

Moodustame naturaalarvu

$$4p_1p_2\ldots p_k - 1.$$

Et see arv on kujuga 4n-1 ja on suurem kõikidest sellekujulistest algarvudest, siis peab ta olema kordarv. Järelikult avaldub ta paaritute algarvude korrutisena

$$4p_1p_2\ldots p_k - 1 = q_1q_2\ldots q_m . \tag{5}$$

Algarvude $q_1, \ldots, q_m$ seas peab olema vähemalt üks kujuga 4n-1, sest vastasel juhul oleks nende korrutis kujuga 4n+1. Niisiis jagub võrduse (5) parem pool vähemalt ühega algarvudest (4). Siit järeldub, et ka arv 1 peab jaguma ühega nendest arvudest, mis on aga võimatu. Vastuolu tuli oletusest, et algarve kujuga 4n-1 on lõplik hulk.

Jada $\{2n+1\}$ võib jaotada ka kolmeks osajadaks: $\{6n-1\}$,

$\{6n+1\}, \{6n+3\}$. Viimane neist sisaldab vaid algarvu 3, osajada teised elemendid jaguvad sellega. Niisamuti võib väita, et kõik paaritud algarvud peituvad jadades $\{8n+1\}$, $\{8n+3\}$, $\{8n+5\}$, $\{8n+7\}$ või jadades, milles n kordaja on 10, 12, 14, ..., vabaliikmed aga nendest väiksemad paaritud naturaalarvud. Sealjuures ei huvita meid need osajadad, mille üldelemendis on muutuja n kordaja ja vabaliige ühisteguriga, sest need osajadad võivad sisaldada ülimalt üht algarvu.

Analoogiliselt võib uurida kõigi naturaalarvude jada osajadasid $\{3n+1\}$, $\{3n+2\}$; $\{5n+1\}$, $\{5n+2\}$, $\{5n+3\}$, $\{5n+4\}$ jne. 1837. aastal tõestas Dirichlet järgmise üldise teoreemi.

Teoreem 1.30. Kui $(a,b) = 1$, siis jada $\{an+b\}$ sisaldab lõpmata palju algarve.

Teoreemi tõestus on komplitseeritud, seda me siin ei esita.

Algarvudega, eriti nende jaotumisega seotud probleeme käsitleme veel X peatükis.

Harjutusülesandeid.

1.12. Leida n väärtused, mille korral arvud n, n+10 ja n+14 oleksid kõik algarvud.

1.13. Tõestada, et algarve kujul 3n+2 on lõpmata palju.

§ 5. ARVU LAHUTAMINE ALGTEGURITEKS

Arvu algteguriteks nimetatakse selle arvu algarvulisi jagajaid.

Teoreem 1.31. Erinevate algarvude p ja q korral $p \nmid q$.

Tõestus. Algarvu q positiivseks teguriks on vaid arvud 1 ja q. Et $p \neq 1$ ja $p \neq q$, siis $p \nmid q$.

Järeldus. Kui algarv q jagub algarvuga p, siis $q = p$.

Teoreem 1.32. Kui korrutis $a_1 a_2 \ldots a_n$ jagub algarvuga p, siis jagub selle algarvuga vähemalt üks tegur.

Tõestus. Kui oletada, et ükski tegur a_i ei jagu p-ga, siis $(a_i, p) = 1$ $(i = 1, 2, \ldots, n)$ ja teoreemi 1.12 põhjal ei jagu ka korrutis p-ga.

Märkus. Teoreem si kehti, kui jagaja on kordarv.

Teoreem 1.33. Iga ühest suuremat naturaalarvu saab lahutada algarvude korrutiseks parajasti ühel viisil (tegurite lahutusi, mis erinevad vaid tegurite järjekorra poolest, loetakse identseteks).

Tõestus. 1) Tõestame algul, et ühest suurema naturaalarvu a jaoks leidub vähemalt üks algteguriteks lahutus. Kui a on algarv, siis koosneb teguriteks lahutus ühest tegurist. Kui a ei ole algarv, siis $a = p_1 a_1$, kus p_1 on arvu a vähim algarvuline jagaja. Kui a_1 on algarv, siis algteguriteks lahutus on saadud. Kui a_1 ei ole algarv, siis

$$a_1 = p_2 a_2,$$

kus p_2 on arvu a_1 vähim algarvuline tegur. Kui a_2 on algarv, siis

$$a = p_1 p_2 a_2$$

ja algteguriteks lahutus on saadud. Kui a_2 ei ole algarv, siis

$$a_2 = p_3 a_3$$

jne. Protsess on lõplik, sest

$$a > a_1 > a_2 > \ldots > 1.$$

Lõpptulemusena saame

$$a = p_1 p_2 \cdots p_{k-1} p_k, \quad \text{kus} \quad p_k = a_{k-1}.$$

Siinjuures tegurid p_1, p_2, ..., p_k ei tarvitse olla kõik üksteisest erinevad.

2) Tõestame algteguriteks lahutuse ühesuse. Oletame, et leidub vähemalt kaks algteguriteks lahutust (teine võib olla saadud mingil teisel teel):

$$a = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_k \cdots q_m,$$

kus konkreetsuse mõttes olgu $k \leq m$. Võrduse parem pool jagub algarvuga q_1. Siis peab jaguma q_1-ga ka korrutis $p_1 p_2 \cdots p_k$. Eelmise teoreemi põhjal peab siis vähemalt üks tegur jaguma q_1-ga. Jagugu p_1 (tegurite numeratsioon on meie valida: siin ei pea tegurid olema kasvavas järjekorras). Et p_1 ja q_1 on algarvud, siis $p_1 = q_1$ (teoreemi 1.31 järeldus). Jagame võrduse p_1-ga läbi, saame

$$p_2 \cdots p_k = q_2 \cdots q_k \cdots q_m.$$

Rakendame endist mõttekäiku, võttes q_1 asemel q_2 jne. Lõpuks, kui $k < m$ saame, et

$$1 = q_{k+1} \cdots q_m.$$

Viimane võrdus on aga võimatu. Järelikult $k = m$. Tõestuse käigus saime, et

$$q_i = p_i, \quad i = 1, 2, \ldots, k.$$

Seega algteguriteks lahutus on ühene.

Teoreemi 1.33 nimetatakse aritmeetika põhiteoreemiks

või ka jaguvusteooria põhiteoreemiks.

Pärast põhiteoreemi tõestust võime kirjutada

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

kus $p_i \neq p_j$, kui $i \neq j$, ja α_i on iga i korral naturaalarv. Viimast kuju nimetatakse naturaalarvu kanooniliseks kujuks.

On koostatud spetsiaalseid tabeleid, mis lihtsustavad naturaalarvu teguriteks lahutamist. Nii koostas D.N.Lehmer 1909.a. tabeli, milles on toodud väikseimad algtegurid kõikide naturaalarvude jaoks, mis ei ületa 10 miljonit ning ei jagu ühegagi algarvudest 2, 3, 5 ja 7 (viimaste tegurite leidmine on ka ilma tabelita lihtne). Märgime, et õpiku [5] lõpus on esitatud analoogiline tabel kõikide 10 000-st väiksemate arvude jaoks.

Teoreem 1.34. Olgu naturaalarvu n kanooniline kuju järgmine:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}. \tag{1}$$

Selleks, et d oleks arvu a jagaja, on tarvilik ja piisav, et

$$d = p_1^{\beta_1} p_2^{\beta_2} \dots p_n^{\beta_n}, \tag{2}$$

kus $0 \leq \beta_i \leq \alpha_i$, $i = 1, 2, \dots, n$.

Tõestus. Tarvilikkus. Olgu $d \mid a$ ja $p \mid d$, kus p on algarv. Siis teoreemi 1.1 põhjal $p \mid a$. Jaguvusteooria põhiteoreemist järeldub, et p peab ühtima ühega algarvudest $p_1, p_2, \dots, p_n$. Niisiis ei saa d kanoonilises kujus olla ühtki arvudest $p_1, p_2, \dots, p_n$ erinevat algarvu. Seega d avaldub kujul (2), kus $\beta_i \geq 0$. Esitame a korrutisena $a = bd$ ja asendame viima-

see seoses a ja d nende kanooniliste teguriteks lahutustega (1) ja (2):

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n} = bp_1^{\beta_1} p_2^{\beta_2} \dots p_n^{\beta_n}.$$

Kui nüüd oletada, et mõne i korral $\beta_i > \alpha_i$, siis võrduse läbijagamisel teguriga $p_i^{\alpha_i}$ saaksime naturaalarvu $\frac{a}{p_i^{\alpha_i}}$ jaoks kaks teguriteks lahutust: üks ei sisalda p_i, teine sisaldab. Põhiteoreemi põhjal pole see võimalik. Seega $\beta_i \leq \alpha_i$.

Piisavus. Olgu arv d antud korrutisena (2). Näitame, et $d|a$. Selleks leiame jagatise

$$\frac{a}{d} = p_1^{\alpha_1 - \beta_1} \dots p_n^{\alpha_n - \beta_n}.$$

Eelduse põhjal on kõik astendajad mittenegatiivsed. Seega $\frac{a}{d}$ on naturaalarv ja teoreem on tõestatud.

Teoreemi põhjal võib välja kirjutada arvu a kõik jagajad. Näiteks arvu $600 = 2^3 \cdot 3 \cdot 5^2$ kõik jagajad on antud valemiga $d = 2^{\alpha} 3^{\beta} 5^{\gamma}$, kus $\alpha = 0, 1, 2, 3$; $\beta = 0, 1$; $\gamma = 0, 1, 2$. Teoreemi põhjal võib lihtsalt saada naturaalarvu a kõigi jagajate arvu $\tau(a)$:

$$\tau(a) = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_n + 1).$$

Nagu näha, ei sõltu jagajate arv teguritest $p_1, \dots, p_n$, vaid sõltub ainult nende astendajatest $\alpha_1, \dots, \alpha_n$.

Teoreemi järeldusena võib tuletada ka juba koolikursusest tuntud reeglid arvude suurima ühisteguri ja vähima ühiskordse arvutamiseks. Jäägu see lugejale.

Harjutusülesandeid.

1.14. Leida arvu 81 057 226 635 000 kanooniline kuju ja

jagajate arv.

1.15. Leida arvu 968 kõik jagajad.

1.16. On teada arvude a, b, ..., d kanoonilised kujud

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}, \quad \alpha_i \geqslant 0,$$
$$b = p_1^{\beta_1} p_2^{\beta_2} \dots p_n^{\beta_n}, \quad \beta_i \geqslant 0,$$
$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots,$$
$$d = p_1^{\delta_1} p_2^{\delta_2} \dots p_n^{\delta_n}, \quad \delta_i \geqslant 0.$$

Kirjutada välja nende arvude suurim ühistegur ja vähim ühiskordne.

II. A H E L M U R R U D

§ 1. LÕPLIKUD AHELMURRUD

Olgu antud täisarv a ja naturaalarv b. Rakendame neile Eukleidese algoritmi:

$$\frac{a}{b} = a_1 + \frac{r_1}{b} \quad \text{ehk} \quad \frac{a}{b} = a_1 + \frac{1}{\frac{b}{r_1}},$$

$$\frac{b}{r_1} = a_2 + \frac{r_2}{r_1} \quad \text{ehk} \quad \frac{b}{r_1} = a_2 + \frac{1}{\frac{r_1}{r_2}},$$

$$\frac{r_1}{r_2} = a_3 + \frac{r_3}{r_2} \quad \text{ehk} \quad \frac{r_1}{r_2} = a_3 + \frac{1}{\frac{r_2}{r_3}},$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots,$$

$$\frac{r_{n-3}}{r_{n-2}} = a_{n-1} + \frac{r_{n-1}}{r_{n-2}} \quad \text{ehk} \quad \frac{r_{n-3}}{r_{n-2}} = a_{n-1} + \frac{1}{\frac{r_{n-2}}{r_{n-1}}},$$

$$\frac{r_{n-2}}{r_{n-1}} = a_n.$$

Järkjärgulisel asendamisel leiame

$$\frac{a}{b} = a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \ddots + \cfrac{1}{a_n}}}}.$$

Saadud murdu nimetatakse ratsionaalarvu $\frac{a}{b}$ ahelmurruks. Seejuures a_1, a_2, ..., a_n kannavad ahelmurru elementide ehk mittetäielike jagatiste nimetust. Ahelmurru elemendid on naturaalarvud, välja arvatud a_1, mis võib olla ka 0 või negatiivne täisarv; viimane element $a_n > 1$ (miks?). Seega saame Eukleidese algoritmi abil iga ratsionaalarvu $\frac{a}{b}$ arendada lõplikuks ahelmurruks.

Ahelmurdu (1) tähistatakse sageli ka kompaktsemalt:

$$a_1 + 1/a_2 + 1/a_3 + \ldots + 1/a_n$$

ehk

$$a_1 + \frac{1}{a_2+} \frac{1}{a_3+} \ldots \frac{1}{a_{n-1}+} \frac{1}{a_n}$$

või

$$[a_1, a_2, \ldots, a_n].$$

Oma kursuses kasutame neist tähistustest esimest ja viimast. Kuigi viimane sümbol ühtib eelmises peatükis kasutatud vähima ühiskordse sümboliga, ei tekita see asjaolu segadust, sest korraga vähimast ühiskordsest ja ahelmurdudest juttu ei tule.

Eukleidese algoritm annab ratsionaalarvu $\frac{a}{b}$ jaoks vaid ühe ahelmurru, sest ta määrab mittetäielikud jagatised üheselt. Kuid on mõeldav, et mõnel teisel teel on saadud $\frac{a}{b}$ jaoks teine ahelmurd, mis erineb Eukleidese algoritmiga saadud murrust. Näitame aga, et sellist olukorda ei saa esineda, kui ahelmurru elemendid rahuldavad ülalpool märgitud tingimusi.

Teoreem 2.1. Iga ratsionaalarvu $\frac{a}{b}$ jaoks eksisteerib vaid üks ahelmurd kujul (1), kus elemendid $a_2, a_3, \ldots, a_n$ on naturaalarvud ja viimane element a_n on ühest suurem.

Tõestus. Oletame, et eksisteerib kaks märgitud omadusega ahelmurdu, s.t.

$$\frac{a}{b} = a_1 + \frac{1}{a_2} + \ldots + \frac{1}{a_n} = a_1' + \frac{1}{a_2'} + \ldots + \frac{1}{a_m'}, \tag{2}$$

kus $a_i \geqslant 1$, $a_j' \geqslant 1$, kui $i = 2, 3, \ldots, n-1$, $j = 2, 3, \ldots, n-1$, $a_n > 1$, $a_m' > 1$. Olgu $m \geqslant n$. Oletame, et a_k ja a_k' $(k \leqslant n)$ on esimesed üksteisest erinevad elemendid, s.t.

$$a_1 = a_1', \ldots, a_{k-1} = a_{k-1}', \quad a_k \neq a_k' \quad (1 \leqslant k \leqslant n).$$

Lahutame ahelmurdude võrduse (2) vastavatest pooltest võrdsed elemendid a_1 ja a_1'. Et saadavas võrduses murdude lugejad on võrdsed, siis on võrdsed ka nimetajad. Saame võrduse uute ahelmurdude vahel

$$a_2 + \frac{1}{a_3} + \ldots + \frac{1}{a_n} = a_2' + \frac{1}{a_3'} + \ldots + \frac{1}{a_m'}.$$

Viimase võrduse vastavatest pooltest lahutame jälle võrdsed arvud a_2 ja a_2' ning võrdsustame nimetajad.

Nii toimime seni, kuni jõuame võrduseni

$$\alpha_k = a_k + \frac{1}{a_{k+1}} + \ldots + \frac{1}{a_n} = a_k' + \frac{1}{a_{k+1}'} + \ldots + \frac{1}{a_m'}, \tag{3}$$

kus sümbolit α_k on kasutatud viimati saadud ratsionaalarvu tähistamiseks. Kui $k < n$, siis

$$a_{k+1} + \ldots + \frac{1}{a_n} > 1$$

ja seetõttu

$$0 < \frac{1}{a_{k+1}} + \ldots + \frac{1}{a_n} < 1.$$

Seega $a_k = [\alpha_k]$ (α_k täisosa). Kui aga $k = n$, siis $a_k = \alpha_k$ ja ikkagi $a_k = [\alpha_k]$. Täpselt samuti näeme, et $a'_k = [\alpha_k]$. Saadud tulemus on vastuolus oletusega, et $a_k \neq a'_k$. Seega $a_1 = a'_1$, ..., $a_n = a'_n$. Kirjutades välja võrduse (3) $k = n$ korral, saame

$$a_n = a'_n + \frac{1}{a'_{n+1}} + \ldots + \frac{1}{a'_m}, \quad \text{kus} \quad a_n = a'_n.$$

Viimane võrdus saab kehtida vaid siis, kui $n = m$. (Miks?) Seega on teoreem tõestatud.

Eukleidese algoritm annab viimaseks jagatiseks a_n alati ühest suurema naturaalarvu, samal ajal kui eelnevad mittetäielikud jagatised a_i ($i = 1, 2, \ldots, n-1$) võivad ka ühega võrduda. Mõnikord osutub kasulikuks ahelmurd, kus viimaseks elemendiks on 1. Sellise ahelmurru saamiseks esitatakse element a_n kujul $(a_n - 1) + \frac{1}{1}$, millega ahelmurru elementide arv suureneb ühe võrra. Seega saab ratsionaalarvu $\frac{a}{b}$ esitada nii paaris- kui ka paaritu arvu elementidega murruna. Kaob küll ahelmurruks arenduse ühesus, kuid viimane polegi tähtis. (Teha kindlaks, kus on teoreemi 2.1 tõestamise käigus kasutatud eeldust, et $a_n > 1$ ja $a'_m > 1$! Ühtlasi veenduda, et ei esine kolmandat võimalust $\frac{a}{b}$ esitamiseks ahelmurruna kujul (1), kus $a_i \geqslant 1$, $i = 2, 3, \ldots, n$).

Märgime, et kogu alljärgnev mõttekäik ja saadavad tulemused ei sõltu sellest, kas ahelmurru viimane element on 1 või mitte. Seepärast olgu edaspidi valemiga (1) antud $\frac{a}{b}$ ahelmurd ükskõik kummal kujul.

Ratsionaalarvu $\frac{a}{b}$ ahelmurruks arendamisel võime Eukleidese algoritmi rakendada järgmisel kompaktsel kujul (näites on $\frac{a}{b} = \frac{134}{51}$):

134	51	32	19	13	6	1
	2	1	1	1	2	6

.

Seega

$$\frac{134}{51} = 2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{6}}}}} =$$

$$= [2, 1, 1, 1, 2, 6] = [2, 1, 1, 1, 2, 5, 1].$$

Kui murru lugeja ja nimetaja on väikesed arvud, saab ahelmurruks arendada ka peast:

$$\frac{7}{5} = 1 + \frac{2}{5} = 1 + \cfrac{1}{2 + \frac{1}{2}}.$$

Sealjuures on otstarbekas vaadelda Eukleidese algoritmi kui täisosa väljaeraldamise meetodit.

Vastupidi, kui ahelmurd on teada, saab arvutada tema väärtuse

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} = 1 + \frac{1}{2} + \frac{4}{13} = 1 + \frac{13}{30} = \frac{43}{30}.$$

Allpool esitame mugava arvutusskeemi ahelmurru väärtuste leidmiseks. Nimetatud skeemi saamiseks toome sisse ahelmurru lähismurru mõiste ja tuletame rekurrentse seose lähismurdude arvutamiseks.

Ahelmurru (1) <u>lähismurdudeks</u> nimetatakse järgmisi ahelmurde:

$$a_1,\ a_1 + \frac{1}{a_2},\ a_1 + \cfrac{1}{a_2 + \frac{1}{a_3}},\ \ldots,\ a_1 + \frac{1}{a_2} + \ldots + \frac{1}{a_n}$$

või nende avaldisi hariliku murruna. Tähistame i-ndat lähismurdu $\frac{P_i}{Q_i}$. Siis

$$\frac{P_1}{Q_1} = \frac{a_1}{1},$$

$$\frac{P_2}{Q_2} = \frac{a_1a_2 + 1}{a_2},$$

$$\frac{P_3}{Q_3} = \frac{a_1a_2a_3 + a_1 + a_3}{a_2a_3 + 1} = \frac{P_2a_3 + P_1}{Q_2a_3 + Q_1}.$$

Üldiselt ei ole murruga veel tema lugeja ja nimetaja määratud, sest murd ei muutu laiendamisel ja taandamisel. Olgu aga P_i ja Q_i nii valitud, et nad võrduvad vastavalt paremal pool võrdusmärki olevate murdude lugejate ja nimetajatega. Kui arvutame järgmise lähismurru, siis saame

$$\frac{P_4}{Q_4} = \frac{P_3a_4 + P_2}{Q_3a_4 + Q_2}.$$

Tõestame täieliku induktsiooni meetodil, et üldiselt võib võtta

$$\begin{aligned} P_k &= P_{k-1}a_k + P_{k-2}, \\ Q_k &= Q_{k-1}a_k + Q_{k-2} \end{aligned} \qquad (k \geqslant 3).$$

Selleks oletame, et viimased valemid kehtivad, ja näitame, et nad jäävad kehtima ka siis, kui indeks k asendada (k+1)-ga. Kirjutame välja lähismurrud järjekorranumbritega k ja k+1:

$$\frac{P_k}{Q_k} = a_1 + \frac{1}{a_2} + \ldots + \frac{1}{a_k} = \frac{P_{k-1}a_k + P_{k-2}}{Q_{k-1}a_k + Q_{k-2}},$$

$$\frac{P_{k+1}}{Q_{k+1}} = a_1 + \frac{1}{a_2} + \ldots + \frac{1}{a_k} + \frac{1}{a_{k+1}}.$$

Selleks, et saada k-ndast lähismurrust lähismurdu järjekorranumbriga $k+1$, tarvitseb asendada a_k summaga $a_k + \frac{1}{a_{k+1}}$. Asendamise juures arvestame, et P_{k-1}, P_{k-2}, Q_{k-1} ja Q_{k-2} ei sisalda elementi a_k. Saame

$$\frac{P_{k+1}}{Q_{k+1}} = \frac{P_{k-1}(a_k + \frac{1}{a_{k+1}}) + P_{k-2}}{Q_{k-1}(a_k + \frac{1}{a_{k+1}}) + Q_{k-2}} = \frac{P_{k-1}(a_k a_{k+1}+1) + a_{k+1}P_{k-2}}{Q_{k-1}(a_k a_{k+1}+1) + a_{k+1}Q_{k-2}} =$$

$$= \frac{(P_{k-1}a_k+P_{k-2})a_{k+1} + P_{k-1}}{(Q_{k-1}a_k+Q_{k-2})a_{k+1} + Q_{k-1}} = \frac{P_k a_{k+1} + P_{k-1}}{Q_k a_{k+1} + Q_{k-1}} .$$

Seega

$$\text{(4)} \qquad \begin{aligned} P_{k+1} &= P_k a_{k+1} + P_{k-1} , \\ Q_{k+1} &= Q_k a_{k+1} + Q_{k-1} , \end{aligned}$$

mida oligi tarvis näidata.

Saadud rekurrentseid valemeid kasutatakse lähismurdude järkjärguliseks arvutamiseks. Selleks, et neid valemeid saaks rakendada alates indeksist 1, toome sisse suurused P_{-1}, Q_{-1}, P_0 ja Q_0, nii et

$$P_2 = a_1a_2 + 1 = P_1a_2 + P_0, \quad Q_2 = a_2 = Q_1a_2 + Q_0,$$

$$P_1 = a_1 = P_0a_1 + P_{-1}, \quad Q_1 = 1 = Q_0a_1 + Q_{-1}.$$

Siit

$$P_0 = 1, \quad P_{-1} = 0, \quad Q_0 = 0, \quad Q_{-1} = 1.$$

Arvestades seoseid (4), võib lähismurde arvutada järgmise skeemi järgi:

		a_1	a_2	a_3	...	a_n
0	1	P_1	P_2	P_3	...	P_n
1	0	Q_1	Q_2	Q_3	...	Q_n

Näide 1. Kasutades toodud arvutusskeemi, arvutame ahelmurru

$$[1, 2, 3, 4, 5, 6, 7] = 1 + \cfrac{1}{2+\cfrac{1}{3+\cfrac{1}{4+\cfrac{1}{5+\cfrac{1}{6+\cfrac{1}{7}}}}}}$$

kõik lähismurrud:

		1	2	3	4	5	6	7
0	1	1	3	10	43	225	1393	9976
1	0	1	2	7	30	157	972	6961

Seega

$$\frac{P_1}{Q_1} = 1, \quad \frac{P_2}{Q_2} = \frac{3}{2}, \quad \frac{P_3}{Q_3} = \frac{10}{7}, \quad \frac{P_4}{Q_4} = \frac{43}{30},$$

$$\frac{P_5}{Q_5} = \frac{225}{157}, \quad \frac{P_6}{Q_6} = \frac{1393}{972}, \quad \frac{P_7}{Q_7} = \frac{9976}{6961}.$$

Näide 2. Arvutame $\frac{171}{191}$ kõik lähismurrud:

171		191	171	20	11	9	2	1
		0	1	8	1	1	4	2
0	1	0	1	8	9	17	77	171
1	0	1	1	9	10	19	86	191

Seega

$\frac{171}{191} = [0,1,8,1,4,2]$ ja $\frac{P_1}{Q_1} = 0, \quad \frac{P_2}{Q_2} = 1, \quad \frac{P_3}{Q_3} = \frac{8}{9}, \quad \frac{P_4}{Q_4} = \frac{9}{10},$

$\frac{P_5}{Q_5} = \frac{17}{19}, \quad \frac{P_6}{Q_6} = \frac{77}{86}, \quad \frac{P_7}{Q_7} = \frac{171}{191}.$

Tõestame nüüd järgnevas olulise valemi.

Teoreem 2.2. Kahe järjestikuse lähismurru lugejate ja

nimetajate vahel kehtib seos

$$P_kQ_{k-1} - P_{k-1}Q_k = (-1)^k. \tag{5}$$

Tõestus. Kasutame täieliku induktsiooni meetodit. Kõigepealt veendume, et valem (5) kehtib, kui $k = 0$:

$$P_0Q_{-1} - P_{-1}Q_0 = 1\cdot 1 - 0\cdot 0 = 1 = (-1)^0.$$

Edasi oletame, et valem kehtib kuni indeksini k, ja näitame, et ta kehtib ka indeksi k+1 puhul. Tõepoolest,

$$P_{k+1}Q_k - P_kQ_{k+1} = (a_{k+1}P_k + P_{k-1})Q_k -$$

$$- P_k(a_{k+1}Q_k + Q_{k-1}) = P_{k-1}Q_k - P_kQ_{k-1} = -(-1)^k = (-1)^{k+1}.$$

Seega valem kehtib iga k korral.

Järeldus. Iga ahelmurru kõik lähismurrud on taandumatud.

Tõepoolest, kui $\frac{P_k}{Q_k}$ oleks taanduv, siis lugejal ja nimetajal oleks ühine jagaja. Siis peab aga jaguma ka võrduse

$$P_kQ_{k-1} - P_{k-1}Q_k = (-1)^k$$

parem pool selle jagajaga, mis on võimatu.

Niisiis,

$$(P_k, Q_k) = 1.$$

Ahelmurruks arendatav murd $\frac{a}{b}$ võib olla taanduv. Kui aga saadud ahelmurru väärtus arvutada rekurrentsete seoste (4) abil, siis saadav viimane lähismurd ehk murru $\frac{a}{b}$ väärtus $\frac{P_n}{Q_n}$ on taandumatu.

Harjutusülesandeid.

2.1. Arendada arv $\frac{170}{99}$ ahelmurruks, millel on

1) paarisarv elemente,

2) paaritu arv elemente.

2.2. Arendada ahelmurruks arv 2,3547 ja leida kõik lähismurrud.

2.3. Leida arv, mille ahelmurruks on

$$[0, 1, 2, 3, 4, 5, 6, 7, 8, 9].$$

2.4. Leida arv, mille ahelmurruks on

$$[1, 1, 1, 1, 1, 1, 1, 1].$$

Leida kõik lähismurrud. Kuidas muutuvad lähismurrud, kui sama arv on arendatud paaritu elementide arvuga ahelmurruks?

2.5. Tõestada, et kehtib järgmine valem:

$$P_{k+1}Q_{k-1} - P_{k-1}Q_{k+1} = (-1)^k a_{k+1}.$$

2.6. Olgu $[a_1, a_2, \ldots, a_n]$ lõplik ahelmurd. Tõestada, et $k \geqslant 2$ korral

$$\frac{P_k}{P_{k-1}} = [a_k, a_{k-1}, \ldots, a_1], \quad \frac{Q_k}{Q_{k-1}} = [a_k, \ldots, a_2].$$

§ 2. KAHE TUNDMATUGA LINEAARNE DIOFANTILINE VÕRRAND

Olgu antud kahe tundmatuga täisarvuliste kordajatega lineaarvõrrand

$$ax + by = c.$$

Sellist võrrandit nimetatakse <u>diofantiliseks võrrandiks</u>, kusjuures tema lahendamise all mõistetakse kõigi täisarvuliste komponentidega lahendite leidmist. Võrrandi kordajatel a ja b võib olla ühine tegur. Olgu

$$(a,b) = d > 1.$$

Siis $a = a_1 d$, $b = b_1 d$, kusjuures $(a_1, b_1) = 1$. Pärast asendamist saame võrrandi

$$a_1 dx + b_1 dy = c.$$

Et võrduse vasak pool jagub d-ga, siis selleks, et võrrand oleks täisarvudes lahenduv, peab d-ga jaguma ka parem pool, s.t. peab olema $d \mid c$. Niisiis juhul, kui $(a,b) \nmid c$, puuduvad võrrandil lahendid.

Edasi vaatleme juhtu, kus $(a,b) \mid c$. Siis $c = c_1 d$ ja pärast asendamist võrrandisse ning d-ga läbijagamist saame eelnevaga ekvivalentse võrrandi

$$a_1 x + b_1 y = c_1 ,$$

kus juba $(a_1, b_1) = 1$. Allpool näeme, et vaadeldaval juhul on võrrand lahenduv, s.t. tingimus $(a,b) \mid c$ on lahenduvuseks ka piisav. Selleks, et vabaneda kordajate indeksite kirjutamisest, vaatleme kohe algusest peale võrrandit

(1) $$ax + by = c, \quad \text{kus} \quad (a,b) = 1.$$

Võrrandi lahendi saamiseks arendame $\frac{a}{b}$ ahelmurruks ning leiame eelviimase lähismurru $\frac{P_{n-1}}{Q_{n-1}}$. Et $\frac{a}{b} = \frac{P_n}{Q_n}$ ja $(a,b) = 1$, siis $P_n = a$, $Q_n = b$. Asendame seoses

$$P_n Q_{n-1} - P_{n-1} Q_n = (-1)^n$$

P_n ja Q_n vastavalt väärtustega a ja b:

$$aQ_{n-1} - bP_{n-1} = (-1)^n.$$

Korrutame võrduse mõlemat poolt teguriga $(-1)^n c$. Saame seose

$$a\left[(-1)^n c Q_{n-1}\right] + b\left[(-1)^{n-1} c P_{n-1}\right] = c.$$

Siit näeme, et võrrandit (1) rahuldavad täisarvud

(2) $$x_0 = (-1)^n cQ_{n-1}, \quad y_0 = (-1)^{n-1} cP_{n-1}.$$

Märkus: Eelmises paragrahvis märkisime, et ratsionaalarvu $\frac{a}{b}$ saab arendada kaheks erinevaks ahelmurruks, kusjuures ühe ahelmurru elementide arv erineb teise omast ühe võrra. Seetõttu võime alati arendada $\frac{a}{b}$ paarisarvulise elementide arvuga ahelmurruks. Siis valemid (2) lihtsustuvad ja omandavad kuju

$$x_0 = cQ_{n-1}, \quad y_0 = -cP_{n-1}.$$

Viimane lahend ei ühti üldiselt lahendiga (2).

Näitame, et lahendeid on lõpmata palju ja nad avalduvad kõik ühe erilahendi kaudu. Olgu arvupaar x_0, y_0 võrrandi (1) erilahend (ükskõik, kas äsja leitud lahend või mingi teine), s.t. kehtigu samasus

(3) $$ax_0 + by_0 = c.$$

Oletame, et leidub veel teisi lahendeid. Tähistame mistahes lahendi x, y. Siis kehtib ka samasus

(4) $$ax + by = c.$$

Lahutades võrdusest (4) võrduse (3) saame

$$a(x-x_0) + b(y-y_0) = 0$$

ehk

$$a(x-x_0) = b(y_0 - y).$$

Viimase võrduse parem pool jagub b-ga, järelikult peab jaguma ka vasak. Et aga (a,b) = 1, siis peab b-ga jaguma $x-x_0$, s.t.

$$x - x_0 = bt \quad \text{ehk} \quad x = x_0 + bt,$$

kus t on mingi täisarv. Asendamisel saame

$$abt = b(y_0 - y),$$

millest

$$y = y_0 - at.$$

Näitame, et

$$x = x_0 + bt,$$

$$y = y_0 - at \tag{5}$$

on võrrandi (1) lahend iga t korral. Tõepoolest,

$$ax + by = a(x_0 + bt) + b(y_0 - at) = ax_0 + by_0 = c.$$

Niisiis juhul, kui (a,b) = 1, on diofantilisel võrrandil ax + by = c lõpmata palju lahendeid, mis avalduvad valemitega (5), kus t on suvaline täisarv ja x_0, y_0 - mistahes erilahend.

Näide. Lahendame võrrandi 29x + 41y = 35.

Arendame $\frac{29}{41}$ ahelmurruks ja leiame eelviimase lähismurru (arvutuste õigsuse kontrollimiseks arvutame ka viimase lähismurru, mis peab võrduma $\frac{29}{41}$).

29		41	29	12	5	2	1
		0	1	2	2	2	2
0	1	0	1	2	5	12	29
1	0	1	1	3	7	17	41

Seega $P_5 = 12$, $Q_5 = 17$, $n = 6$ ja üheks erilahendiks on

$$x_0 = (-1)^6 \cdot 35 \cdot 17 = 595,$$

$$y_0 = (-1)^5 \cdot 35 \cdot 12 = -420.$$

Üldlahend avaldub aga järgmiselt:

$$x = 595 + 41\,t,$$

$$y = -420 - 29\,t.$$

Saadud üldlahendi kuju on ebasobiv, sest vabaliikmed on absoluutväärtuselt liialt suured. Selleks et vähemalt üht vabaliiget vähendada, eraldame 595-st 41 teatud kordse (jagame 595 41-ga nii, et saaksime absoluutväärtuselt vähima positiivse või negatiivse jäägi):

$$595 = 41 \cdot 14 + 21.$$

Seega

$$x = 21 + 41 \cdot 14 + 41\,t = 21 + 41(14+t) = 21 + 41\,u,$$

kus $u = 14 + t$. Nüüd

$$y = -420 - 29(u-14) = -420 - 29\,u + 406 = -14 - 29\,u.$$

Kui võrrandi kordajad on väikesed, saab erilahendi leida ka lihtsa proovimise teel. Näiteks võrrandi

$$5x - 11y = 7$$

lahendamiseks võib x avaldada y kaudu:

$$x = \frac{11y + 7}{5}$$

ja teha kindlaks, millise väärtuse peaks andma y-le, et 11y + 7 jaguks 5-ga. Ilmselt sobib $y_0 = 3$. Siis aga $x_0 = 8$. Seega erilahendiks on $x_0 = 8$, $y_0 = 3$ ja üldlahendiks

$$x = 8 - 11\,t,$$

$$y = 3 - 5\,t.$$

Lõpuks märgime, et lihtne meetod lineaarse üldkujulise diofantilise võrrandisüsteemi lahendamiseks on esitatud R.Kulmeti artiklis "Diofantiliste võrrandisüsteemide lahendamine" kogumikus "Matemaatika ja kaasaeg", XVIII, 1972, lk. 23-30.

Harjutusülesandeid.

2.7. Lahendada diofantilised võrrandid

a) $97x + 35y = 3189$,

b) $30x + 57y = 66$.

2.8. Lasteaiale osteti kaht liiki pildiraamatuid. Ühed maksid 23 kop. tükk, teised 38 kop. Kui palju osteti kumbagi liiki raamatuid, kui kokku maksti 13 rbl. 59 kop?

2.9. Leida võrrandi

$$25x + 18y = 2423$$

positiivsed täisarvulised lahendid.

2.10. 523 m pikkuse tsentraalküttesüsteemi soojustrassi rajamiseks on kasutada 30 12 m pikkust ja 70 7 m pikkust toru. Millised võimalused on torude valikuks, kui tahetakse läbi saada torusid tükeldamata? Kui palju tuleb võtta kumbagi liiki torusid juhul, kui tahetakse säilitada võimalikult palju pikemaid torusid?

§ 3. IRRATSIONAALARVU AHELMURD

Näitame, et suvalist reaalarvu α saab arendada ahelmurruks. Piirdume juhuga, kus α on irratsionaalarv, sest ratsionaalarvu ahelmurruks arendamist me juba käsitlesime.

Olgu $a_1 = [\alpha]$, s.o. suurim täisarv, mis ei ületa α. Siis

$$\alpha = a_1 + \frac{1}{\alpha_2}, \quad \text{kus} \quad \alpha_2 > 1.$$

α_2 on irratsionaalarv, sest juhul, kui α_2 oleks ratsionaalarv, oleks seda ka α. Edasi olgu $a_2 = [\alpha_2]$. Siis

$$\alpha_2 = a_2 + \frac{1}{\alpha_3}, \quad \text{kus } \alpha_3 > 1.$$

Analoogiliselt leiame

$$\alpha_3 = a_3 + \frac{1}{\alpha_4}, \quad \text{kus } \alpha_4 > 1 \text{ jne.}$$

Üldiselt

$$\alpha_n = a_n + \frac{1}{\alpha_{n+1}},$$

kus $a_n = [\alpha_n]$ ja α_{n+1} on ühest suurem irratsionaalarv.

Vaadeldav protsess ei ole irratsionaalse α korral lõplik. Kui katkestame täisosade väljaeraldamise n-ndal sammul, siis saame ahelmurru

$$(1) \quad \alpha = a_1 + 1/a_2 + 1/a_3 + \ldots + 1/a_n + 1/\alpha_{n+1}.$$

Siin a_1 on täisarv, a_2, a_3, ..., a_n on naturaalarvud, α_{n+1} on ühest suurem irratsionaalarv.

Ahelmurdu, mille element a_1 on täisarv, elemendid a_k ($k = 2,3,\ldots$) aga naturaalarvud, nimetame regulaarseks. Ahelmurd (1) pole regulaarne, sest α_{n+1} ei ole naturaalarv. Jätkates aga täisosade väljaeraldamise protsessi piiramatult, s.t. lastes $n \to \infty$, saame lõpmatu regulaarse ahelmurru

$$(2) \quad a_1 + 1/a_2 + 1/a_3 + \ldots + 1/a_n + \ldots$$

Lõpmatute ahelmurdude korral kasutame analoogilisi kompaktsemaid tähistusi nagu lõplike ahelmurdude puhul.

Enne kui kirjutada, et ahelmurd (2) võrdub α-ga, tuleb defineerida lõpmatu ahelmurru väärtus ja näidata, et antud juhul see väärtus võrdub α-ga. Vaatleme esialgu mistahes lõpmatut ahelmurdu kujul (2), kus a_1 on täisarv ja

$a_i \geqslant 1$, kui $i \geqslant 2$, eeldamata, et see ahelmurd on saadud antud reaalarvust α ülalkirjeldatud täisosade väljaeraldamise protsessi tulemusena. Võtame lõplike ahelmurdude jada

$$(3)\quad \frac{P_1}{Q_1} = a_1,\ \frac{P_2}{Q_2} = a_1 + \frac{1}{a_2},\ \frac{P_3}{Q_3} = a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3}},\ \ldots,$$

$$\frac{P_n}{Q_n} = a_1 + 1/a_2 + 1/a_3 + \ldots + 1/a_n,\ \ldots,$$

mida nimetame ahelmurru (2) lähismurdude jadaks. Lõpmatut ahelmurdu (2) nimetatakse koonduvaks, kui eksisteerib lõplik piirväärtus

$$\lim_{n\to\infty} \frac{P_n}{Q_n}.$$

Viimast piirväärtust nimetatakse lõpmatu ahelmurru (2) väärtuseks.

Teoreem 2.3. Iga lõpmatu ahelmurd koondub teatud reaalarvuks.

Tõestus. Tõestame, et lähismurdude jada on fundamentaaljada, s.t.

$$(4)\quad \lim_{n\to\infty}\left(\frac{P_n}{Q_n} - \frac{P_{n+m}}{Q_{n+m}}\right) = 0 \quad \text{iga} \quad m \geqslant 1 \quad \text{puhul.}$$

Kuna lähismurrud (3) on lõplikud ahelmurrud ja igale ahelmurrule jadas (3) eelnevaid ahelmurde võib lugeda tema lähismurdudeks, siis kehtivad §-s 1 leitud seosed. Eriti on

$$P_{n+1}Q_n - P_nQ_{n+1} = (-1)^{n+1},$$

millest

$$\frac{P_n}{Q_n} - \frac{P_{n+1}}{Q_{n+1}} = \frac{(-1)^n}{Q_nQ_{n+1}}.$$

Et $Q_{n+1} = Q_n a_{n+1} + Q_{n-1}$ ja $Q_1 = 1$, $Q_2 = a_2 \geqslant 1$, $Q_3 \geqslant Q_2 + Q_1 \geqslant 2$, $Q_4 \geqslant Q_3 + Q_2 \geqslant 3$, $Q_5 \geqslant Q_4 + Q_3 \geqslant 5$, siis alates n väärtusest 6 on kindlasti* $Q_n > n$. Niisiis saame $n \geqslant 5$ korral

$$\left|\frac{P_n}{Q_n} - \frac{P_{n+m}}{Q_{n+m}}\right| \leqslant \left|\frac{P_n}{Q_n} - \frac{P_{n+1}}{Q_{n+1}}\right| + \ldots + \left|\frac{P_{n+m-1}}{Q_{n+m-1}} - \frac{P_{n+m}}{Q_{n+m}}\right| =$$

$$= \sum_{k=0}^{m-1} \frac{1}{Q_{n+k}Q_{n+k+1}} < \sum_{k=0}^{m-1} \frac{1}{(n+k)(n+k+1)} = \frac{m}{n(n+m)},$$

millest järeldubki võrdus (4). Et reaalarvude hulgas iga fundamentaaljada koondub, siis leidub reaalarv β, nii et

$$\lim_{n\to\infty} \frac{P_n}{Q_n} = \beta,$$

millega teoreem on tõestatud.

Edasi tõestame järgmise teoreemi.

Teoreem 2.4. Kui ahelmurd (2) on saadud irratsionaalarvust α täisosade väljaeraldamise protsessi piiramatul jätkamisel (nagu on kirjeldatud käesoleva punkti alguses), siis tema väärtus on α.

Tõestus. Seosest (1) näeme, et α erineb lähismurrust $\frac{P_{n+1}}{Q_{n+1}}$ ainult selle poolest, et a_{n+1} on asendunud α_{n+1}-ga. Et

$$\frac{P_{n+1}}{Q_{n+1}} = \frac{P_n a_{n+1} + P_{n-1}}{Q_n a_{n+1} + Q_{n-1}},$$

---

* Tegelikult võib väita, et $Q_n \geqslant u_n$, kus u_n on Fibonacci jada n-es element. Fibonacci jada on defineeritud rekurrentselt valemiga $u_n = u_{n-1} + u_{n-2}$, $u_0 = u_1 = 1$.

siis

$$\alpha = \frac{P_n \alpha_{n+1} + P_{n-1}}{Q_n \alpha_{n+1} + Q_{n-1}}. \tag{5}$$

Leiame vahe $\frac{P_n}{Q_n} - \alpha$:

$$\frac{P_n}{Q_n} - \alpha = \frac{P_n}{Q_n} - \frac{P_n \alpha_{n+1} + P_{n-1}}{Q_n \alpha_{n+1} + Q_{n-1}} = \frac{P_n Q_{n-1} - P_{n-1} Q_n}{Q_n (Q_n \alpha_{n+1} + Q_{n-1})} =$$

$$= \frac{(-1)^n}{Q_n (Q_n \alpha_{n+1} + Q_{n-1})}.$$

Et $\alpha_{n+1} > 1$, siis $\lim\limits_{n \to \infty} (Q_n \alpha_{n+1} + Q_{n-1}) = +\infty$ ja seega

$$\lim_{n \to \infty} \frac{P_n}{Q_n} = \alpha, \tag{6}$$

mida oligi tarvis tõestada.

Tõestame lõpuks, et iga irratsionaalarvu jaoks eksisteerib vaid üks lõpmatu ahelmurd.

Teoreem 2.5. Kui kaks lõpmatut ahelmurdu kujul (2), kus $a_i \geqslant 1$ $(i = 2,3,4,\ldots)$, on võrdsed, siis on võrdsed nende ahelmurdude kõik elemendid.

Tõestus. Oletame, et leidub kaks lõpmatut ahelmurdu, mille väärtused on võrdsed, s.t.

$$a_1 + \frac{1}{a_2} + \frac{1}{a_3} + \ldots = a'_1 + \frac{1}{a'_2} + \frac{1}{a'_3} + \ldots, \tag{7}$$

kuid mis erinevad vähemalt ühe elemendi poolest. Olgu k elementide esimene indeks, mille korral $a_k \neq a'_k$, s.t.

$$a_1 = a'_1, \ \ldots, \ a_{k-1} = a'_{k-1}, \ a_k \neq a'_k.$$

Tähistame

$$\alpha_k = a_k + \frac{1}{a_{k+1}} + \ldots, \ \alpha'_k = a'_k + \frac{1}{a'_{k+1}} + \ldots \tag{8}$$

Et $a_{k+1} \geqslant 1,\ a_{k+2} \geqslant 1,\ \ldots,\ a'_{k+1} \geqslant 1,\ a'_{k+2} \geqslant 1,\ \ldots,$

siis

$$1/a_{k+1} + \ldots < 1, \quad 1/a'_{k+1} + \ldots < 1$$

ja seega

$$a_k = [\alpha_k], \quad a'_k = [\alpha'_k].$$

Kuna iga lõpmatu ahelmurd koondub, siis seoste (8) tõttu on α_k ja α'_k teatud irratsionaalarvud ning võrduse (7) võib kirjutada kujul

$$\begin{aligned} &a_1 + 1/a_2 + \ldots + 1/a_{k-1} + 1/\alpha_k = \\ &= a'_1 + 1/a'_2 + \ldots + 1/a'_{k-1} + 1/\alpha'_k . \end{aligned} \tag{9}$$

Et $a_1 = a'_1, \ldots, a_{k-1} = a'_{k-1}$, siis toimime samuti nagu teoreemi 2.1 tõestamisel: lahutame võrduse (9) pooltest vastavalt võrdsed elemendid a_1, a'_1 ja võrdsustame saadavas võrduses murdude nimetajad (arvestame, et mõlema murru lugejad võrduvad ühega). Sellist protsessi korrates jõuame võrduseni $\alpha_k = \alpha'_k$. Siis aga

$$a_k = [\alpha_k] = [\alpha'_k] = a'_k ,$$

mis on vastuolus oletusega, et $a_k \neq a'_k$. Saadud vastuolu tõestabki teoreemi.

Esitame näite irratsionaalarvu ahelmurruks arendamise kohta.

Näide. Arendame ahelmurruks $\alpha = \sqrt{7}$.

Täisosade järkjärgulisel väljaeraldamisel saame

$$\alpha = \sqrt{7} = 2 + \frac{1}{\alpha_2}, \quad \alpha_2 = \frac{1}{\sqrt{7} - 2} = \frac{\sqrt{7} + 2}{3} = 1 + \frac{1}{\alpha_3} ,$$

$$\alpha_3 = \frac{3}{\sqrt{7}-1} = \frac{\sqrt{7}+1}{2} = 1 + \frac{1}{\alpha_4},$$

$$\alpha_4 = \frac{2}{\sqrt{7}-1} = \frac{\sqrt{7}+1}{3} = 1 + \frac{1}{\alpha_5}, \quad \alpha_5 = \frac{3}{\sqrt{7}-2} = \sqrt{7}+2 =$$

$$= 4 + \frac{1}{\alpha_6}, \quad \alpha_6 = \frac{1}{\sqrt{7}-2} = \alpha_2.$$

Seega $\alpha_7 = \alpha_3, \alpha_8 = \alpha_4$ jne. Siit järeldub ka vaadeldavate täisosade võrdus. Saame nn. perioodilise ahelmurru

$$\sqrt{7} = [2,1,1,1,4,1,1,1,4,\ldots].$$

Viimast perioodilist ahelmurdu märgime lühemalt järgmiselt:

$$[2,(1,1,1,4)].$$

Põhjalikumalt käsitleme perioodilisi ahelmurde paragrahvis 5.

Käesoleva paragrahvi lõpus märgime, et arvu π ahelmurru esimesed elemendid on järgmised:

$$\pi = [3,7,15,1,292,1,1,1,2,1,3,1,14,2,1,\ldots],$$

arvu e ahelmurruks on aga

$$e = [2,1,2,1,1,4,1,1,6,1,1,8,1,\ldots],$$

s.t.

$a_1 = 2$, $a_2 = 1$, $a_{3n} = 2n$, $a_{3n+1} = a_{3n+2} = 1$ $(n=1,2,3,\ldots)$.

Valemite tuletuse arvu e ahelmurru elementide jaoks võib leida näiteks õpikust [1], lk. 221-223. Arvu e ahelmurd on leitud Euleri poolt.

Harjutusülesandeid.

2.11. Arendada ahelmurruks irratsionaalarvud

a) $\sqrt{3}$, b) $\sqrt{13}$, c) $\sqrt{31}$, d) $\frac{\sqrt{5}+2}{3}$, e) $\frac{\sqrt{13}-7}{6}$.

2.12. Leida irratsionaalarvu $\sqrt[3]{3}$ ahelmurru mõned elemendid.

§ 4. REAALARVU RATSIONAALSED LÄHENDID

1. Reaalarvu lähendamine ahelmurru lähismurdudega. Eelmise paragrahvi seosest (6) järeldub, et iga reaalarvu α võib tema ahelmurru lähismurdudega kuitahes hästi lähendada. Käesolevas punktis uurime sellise lähendamise viga ja jada $\left\{\frac{P_n}{Q_n}\right\}$ elementide arvule α lähenemise iseloomu.

Vaatleme kõigepealt, kuidas toimub lähismurdude jada $\left\{\frac{P_n}{Q_n}\right\}$ elementide lähenemine arvule α. Selleks lähtume teoreemi 2.4 tõestamisel saadud seosest

$$\alpha - \frac{P_n}{Q_n} = \frac{(-1)^{n+1}}{Q_n(Q_n\alpha_{n+1} + Q_{n-1})}. \tag{1}$$

Võrduse (1) paremal poolel esineva murru nimetaja on positiivne, lugeja aga paaritu n korral positiivne, paarisarvulise n korral negatiivne. Seetõttu juhul, kui n on paaritu arv, on $\alpha > \frac{P_n}{Q_n}$, paarisarvulise n korral aga $\alpha < \frac{P_n}{Q_n}$. Seega

$$\frac{P_{2k+1}}{Q_{2k+1}} < \alpha < \frac{P_{2m}}{Q_{2m}}. \tag{2}$$

Näitame, et sealjuures

$$\left|\frac{P_n}{Q_n} - \alpha\right| < \left|\frac{P_{n-1}}{Q_{n-1}} - \alpha\right|.$$

Selleks lähtume α avaldisest (§ 1, valem (5))

$$\alpha = \frac{\alpha_{n+1} P_n + P_{n-1}}{\alpha_{n+1} Q_n + Q_{n-1}},$$

millest avaldame α_{n+1}:

$$\alpha_{n+1} = \frac{P_{n-1} - \alpha Q_{n-1}}{\alpha Q_n - P_n} = \frac{Q_{n-1}\left(\frac{P_{n-1}}{Q_{n-1}} - \alpha\right)}{Q_n\left(\alpha - \frac{P_n}{Q_n}\right)}.$$

Siit

$$\left|\frac{P_{n-1}}{Q_{n-1}} - \alpha\right| = \alpha_{n+1}\frac{Q_n}{Q_{n-1}}\left|\alpha - \frac{P_n}{Q_n}\right| > \left|\alpha - \frac{P_n}{Q_n}\right|,$$

sest

$$\alpha_{n+1} > 1 \quad \text{ja} \quad Q_n \geqslant Q_{n-1}, \text{ kui } n \geqslant 2.$$

Niisiis

$$(3) \qquad \left|\frac{P_{n+1}}{Q_{n+1}} - \alpha\right| < \left|\frac{P_n}{Q_n} - \alpha\right| < \left|\frac{P_{n-1}}{Q_{n-1}} - \alpha\right|.$$

Arvestades võrratusi (2) ja (3) võime kirjutada

$$\frac{P_1}{Q_1} < \frac{P_3}{Q_3} < \frac{P_5}{Q_5} < \ldots < \alpha < \ldots < \frac{P_6}{Q_6} < \frac{P_4}{Q_4} < \frac{P_2}{Q_2}.$$

Edasi hindame viga, mis tekib α lähendamisel ratsionaalarvudega $\frac{P_n}{Q_n}$. Valemist (1) saadav täpne hinnang

$$(4) \qquad \left|\alpha - \frac{P_n}{Q_n}\right| = \frac{1}{Q_n(\alpha_{n+1} Q_n + Q_{n-1})}$$

ei ole otseselt kasutatav, sest ta sisaldab tundmatut suurust α_{n+1}. Paneme aga tähele, et

$$\alpha_{n+1} = a_{n+1} + \frac{1}{\alpha_{n+2}} > a_{n+1}.$$

Seega

$$Q_n(\alpha_{n+1} Q_n + Q_{n-1}) > Q_n(a_{n+1} Q_n + Q_{n-1}) = Q_n Q_{n+1},$$

mistôttu

(5) $$\left|\frac{P_n}{Q_n} - \alpha\right| < \frac{1}{Q_n Q_{n+1}} .$$

Seos (4) võimaldab hinnata ka vea alammäära. Hinnangu saamiseks arvestame, et

$$\alpha_{n+1} = a_{n+1} + \frac{1}{\alpha_{n+2}} < a_{n+1} + 1$$

ja

$$\alpha_{n+1} Q_n + Q_{n-1} < (a_{n+1} + 1)Q_n + Q_{n-1} = Q_{n+1} + Q_n .$$

Seega

(6) $$\left|\frac{P_n}{Q_n} - \alpha\right| > \frac{1}{Q_n(Q_{n+1} + Q_n)} .$$

Näeme, et vea ülemine ja alumine tôke erinevad suhteliselt vähe. Seepärast annab valem (5) väga täpse hinnangu.

Näide 1. Leiame arvu π môned esimesed lähismurrud ja hindame nende erinevust arvust π:

		3	7	15	1	292	1	...
0	1	3	22	333	355	103993	104348	...
1	0	1	7	106	113	33102	33215	...

Valem (5) annab

$$\left|\pi - \frac{22}{7}\right| < \frac{1}{7 \cdot 106} < \frac{1}{700} , \quad \left|\pi - \frac{333}{106}\right| < \frac{1}{106 \cdot 113} < 0{,}0001 ,$$

$$\left|\pi - \frac{355}{113}\right| < \frac{1}{113 \cdot 33102} < 0{,}000\ 000\ 27.$$

Eriti mugavaks lähendiks arvule π on neljas lähismurd $\frac{P_4}{Q_4} = \frac{355}{113}$, mis suhteliselt väikese nimetaja puhul annab suure täpsuse. Viimane on tingitud sellest, et ahelmurru järgmine element $a_5 = 292$ on võrdlemisi suur ja selletôttu ka

valemis (5) esinev nimetaja Q_5 on võrreldes eelneva nimetajaga $Q_4 = 113$ järsult kasvanud. Märgime, et π ja $\frac{355}{133}$ tegelik erinevus on 0,00000025... ; niisiis valemi (5) abil saadav veahinnang peaaegu ühtib tegeliku veaga.

Kuna $Q_{n+1} \geqslant Q_n$, siis valemist (5) järeldub hinnang

$$(7) \qquad \left| \alpha - \frac{P_n}{Q_n} \right| < \frac{1}{Q_n^2} \qquad (n \geqslant 1).$$

Siit omakorda järeldub, et ahelmurru lähismurrud on arvule üldiselt märksa paremad lähendid kui lõplikud kümnendmurrud, mis saadakse arvu kümnendmurruks arendamise protsessis. Tõepoolest, kui c_1, c_2, ... on arvu α kümnendnumbrid pärast koma ja $c_0 = [\alpha]$, s.t.

$$\alpha = c_0 + \frac{c_1}{10} + \frac{c_2}{10^2} + \dots ,$$

siis võttes α lähendiks kümnendmurru

$$c_0 + \frac{c_1}{10} + \dots + \frac{c_n}{10^n} = \frac{a}{10^n} ,$$

saame vea hinnanguks

$$\left| \alpha - \frac{a}{10^n} \right| = \frac{c_{n+1}}{10^{n+1}} + \frac{c_{n+2}}{10^{n+2}} + \dots \leqslant$$

$$\leqslant \frac{9}{10^{n+1}} + \frac{9}{10^{n+2}} + \dots = \frac{1}{10^n} ,$$

kusjuures seda hinnangut üldiselt parandada ei saa. Tähistanud $10^n = b$, võime kirjutada

$$(8) \qquad \left| \alpha - \frac{a}{b} \right| \leqslant \frac{1}{b} .$$

Võrreldes hinnanguid (7) ja (8) näeme, et reaalarvu lähendamisel ahelmurru lähismurdudega ei ületa viga ratsionaalse lähendi nimetaja pöördväärtuse ruutu, lähendamisel kümnend-

murdudega võib aga viga ulatuda kümnendmurru nimetaja pöördväärtuseni. Seepärast võib esimesel juhul rääkida teist järku lähendamisest, teisel juhul vaid esimest järku lähendamisest.

Näide 2. Võrdleme irratsionaalarvu $\sqrt{2} = 1{,}4142\ldots$ ahelmurru lähismurde selle arvu kümnendmurdudega $1{,}4 = \frac{14}{10} = \frac{7}{5}$; $1{,}41 = \frac{141}{100}$; $1{,}414 = \frac{1414}{1000} = \frac{707}{500}$; ...

Arvu $\sqrt{2}$ ahelmurruks on $[1, (2)]$. Leiame mõned lähismurrud:

		1	2	2	2	2	2	2 ...
0	1	1	3	7	17	41	99	
11	0	1	2	5	12	29	70	169

Lähismurd $\frac{P_2}{Q_2} = \frac{7}{5}$ ühtib kümnendlähismurruga 1,4. Lähismurrud

$$\frac{P_4}{Q_4} = \frac{17}{12}, \quad \frac{P_5}{Q_5} = \frac{41}{29}, \quad \frac{P_6}{Q_6} = \frac{99}{70}$$

on aga kõik paremad lähendid kui kümnendlähismurd $1{,}41 = \frac{141}{100}$, kuigi nende nimetajad on väiksemad kui viimase nimetaja 100. Kui $\left|\sqrt{2} - \frac{141}{100}\right| = 0{,}0042\ldots$, siis 100-le lähedase nimetajaga lähismurru $\frac{P_6}{Q_6}$ vea hindamine annab:

$$\left|\sqrt{2} - \frac{99}{70}\right| < \frac{1}{70 \cdot 169} < 0{,}000085.$$

Analoogiline on olukord järgnevate lähismurdude korral.

Järgmine teoreem näitab, et ratsionaalmurd, mis teatud mõttes küllalt hästi aproksimeerib reaalarvu, ühtib tingimata selle reaalarvu ahelmurru ühe lähismurruga. See teoreem leiab kasutamist Pelli võrrandi lahendusvalemite tuletamisel (§5, punkt 3).

Teoreem 2.6. Kui täisarvude a ja b ($b > 0$, $(a,b) = 1$) korral on täidetud tingimus

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{2b^2},$$

siis $\frac{a}{b}$ on reaalarvu α ahelmurru üks lähismurde.

Tõestus. Eeldame, et $\alpha \neq \frac{a}{b}$, sest vastasel juhul oleks väide triviaalne. Arendame ratsionaalarvu $\frac{a}{b}$ ahelmurruks,

$$\frac{a}{b} = [a_1, a_2, \ldots, a_k] = \frac{P_k}{Q_k},$$

võttes k paarisarvu, kui $\alpha - \frac{a}{b} < 0$, ja k paaritu, kui $\alpha - \frac{a}{b} > 0$. Siis

$$\alpha - \frac{a}{b} = \alpha - \frac{P_k}{Q_k} = (-1)^{k-1}\left|\alpha - \frac{P_k}{Q_k}\right| = (-1)^{k-1}\left|\alpha - \frac{a}{b}\right|.$$

Moodustame arvu ω nii, et

$$\alpha = \frac{P_k\omega + P_{k-1}}{Q_k\omega + Q_{k-1}}.$$

Selleks tarvitseb võtta

$$\omega = \frac{P_{k-1} - \alpha Q_{k-1}}{\alpha Q_k - P_k}. \tag{9}$$

Siis

$$\omega + \frac{Q_{k-1}}{Q_k} = \frac{P_{k-1} - \alpha Q_{k-1}}{\alpha Q_k - P_k} + \frac{Q_{k-1}}{Q_k} = \frac{P_{k-1}Q_k - P_kQ_{k-1}}{Q_k(\alpha Q_k - P_k)} =$$

$$= \frac{(-1)^{k+1}}{Q_k(\alpha Q_k - P_k)} = \frac{1}{Q_k^2\left|\alpha - \frac{P_k}{Q_k}\right|} = \frac{1}{b^2\left|\alpha - \frac{a}{b}\right|} > 2,$$

millest saame, et

$$\omega > 2 - \frac{Q_{k-1}}{Q_k} \geqslant 1.$$

Olgu ω arendatud ahelmurruks

$$\omega = [a_{k+1}, a_{k+2}, \ldots].$$

Et $\omega > 1$, siis $a_{k+1} \geqslant 1$ ja avaldis $[a_1, a_2, \ldots, a_k, a_{k+1}, a_{k+2}, \ldots] = \beta$ kujutab endast regulaarset ahelmurdu, mille väärtus on mingi reaalarv β. Arvu β võib esitada ka mitteregulaarse lõpliku ahelmurruna

$$\beta = [a_1, a_2, \ldots, a_k, \omega],$$

mistõttu eelmise paragrahvi valemi (5) kohaselt

$$\beta = \frac{P_k\omega + P_{k-1}}{Q_k\omega + Q_{k-1}}.$$

Asendanud siia ω avaldise (9), saame lihtsustamisel, et $\beta = \alpha$. Seega on ratsionaalarv

$$[a_1, a_2, \ldots, a_k] = \frac{a}{b}$$

reaalarvu α lähismurd.

2.* <u>Reaalarvu lähendamine ratsionaalarvude lõpmatu jadaga</u>. Valemist (7) järeldub, et iga irratsionaalarvu jaoks eksisteerib lõpmata palju ratsionaalarve $\frac{a}{b}$, mis rahuldavad tingimust

(10) $$\left|\alpha - \frac{a}{b}\right| < \frac{1}{b^2},$$

kusjuures murruks $\frac{a}{b}$ sobib arvu α ahelmurru iga lähismurd. Tekib küsimus, kas võib võrratuse (10) paremal poolel esineva murru lugeja 1 asendada arvuga $c < 1$, nii et ka võrratust

(11) $$\left|\alpha - \frac{a}{b}\right| < \frac{c}{b^2}$$

rahuldab iga irratsionaalarvu α korral lõpmata palju ratsionaalarve. Osutub, et see on võimalik, kusjuures vähimaks selliseks arvuks on

$$c = \frac{1}{\sqrt{5}} = 0{,}4472 \ldots$$

Teoreem 2.7. Iga irratsionaalarvu α jaoks eksisteerib lõpmata palju ratsionaalarve $\frac{a}{b}$, mille korral

$$(12) \qquad \left|\alpha - \frac{a}{b}\right| < \frac{1}{\sqrt{5}\, b^2} .$$

Teoreemi tõestuse võib leida näiteks õpikust [1], lk. 233-234. Tõestamiseks näidatakse, et arvu α ahelmurru igast kolmest järjestikusest lähismurrust $\frac{P_{n-1}}{Q_{n-1}}, \frac{P_n}{Q_n}, \frac{P_{n+1}}{Q_{n+1}}$ vähemalt üks sobib arvuks $\frac{a}{b}$.

Edasi saab tõestada, et konstanti c võrratuses (11) ei saa enam vähendada: väiksema c korral leidub α, mille jaoks saab eksisteerida veel vaid lõplik hulk ratsionaalarve, mis seda võrratust rahuldavad. Kehtib nimelt järgmine teoreem.

Teoreem 2.8. Iga positiivse reaalarvu $c < \frac{1}{\sqrt{5}}$ ja arvu $\alpha = \frac{1+\sqrt{5}}{2}$ jaoks eksisteerib vaid lõplik hulk ratsionaalarve $\frac{a}{b}$ (või ei eksisteeri ühtki), mille korral

$$(13) \qquad \left|\alpha - \frac{a}{b}\right| < \frac{c}{b^2} .$$

Tõestus. Oletame, et $\alpha = \frac{1+\sqrt{5}}{2}$ ja $c < \frac{1}{\sqrt{5}}$ korral leidub lõpmatu hulk ratsionaalarve $\frac{a}{b}$, mis rahuldavad võrratust (13). Siis iga sellise ratsionaalarvu korral on rahuldatud võrratused

$$\alpha - \frac{c}{b^2} < \frac{a}{b} < \alpha + \frac{c}{b^2} ,$$

millest pärast α asendamist ja b-ga korrutamist saame:

$$\frac{\sqrt{5}}{2} b - \frac{c}{b} < a - \frac{b}{2} < \frac{\sqrt{5}}{2} b + \frac{c}{b} .$$

Siit saame ruutu tõstmisel:

$$\frac{c^2}{b^2} - \sqrt{5}c < a^2 - ab - b^2 < \frac{c^2}{b^2} + \sqrt{5}c.$$

Kuna $0 < \sqrt{5}c < 1$, siis küllalt suure b korral

$$-1 < a^2 - ab - b^2 < 1$$

ja järelikult $a^2 - ab - b^2 = 0$, sest $a^2 - ab - b^2$ on täisarv. Siis aga $\frac{a}{b} = \frac{1 \pm \sqrt{5}}{2}$, mis pole täisarvuliste a ja b korral võimalik. Saadud vastuolu näitab, et võrratus (13) võib kehtida vaid lõpliku arvu ratsionaalarvude $\frac{a}{b}$ korral.

Teoreemist 2.8 järeldub, et kui antud $\alpha = \frac{1 + \sqrt{5}}{2}$ korral võtta c küllalt väike, siis pole võrratus (13) täidetud enam ühegi ratsionaalarvu $\frac{a}{b}$ korral, s.t. küllalt väikese positiivse reaalarvu c puhul kehtib iga ratsionaalarvu $\frac{a}{b}$ korral võrratus

$$\left|\alpha - \frac{a}{b}\right| \geqslant \frac{c}{b^2}.$$

3.* Reaalarvu parimad ratsionaalsed lähendid. Ratsionaalarvu $\frac{a}{b}$ $(b > 0)$ nimetatakse reaalarvu α parimaks lähendiks, kui ei eksisteeri ühtki naturaalarvust b väiksema või temaga võrdse positiivse nimetajaga ratsionaalarvu $\frac{x}{y}$, mis erineks α-st vähem kui erineb $\frac{a}{b}$. Seega on $\frac{a}{b}$ reaalarvu α parimaks lähendiks parajasti siis, kui iga teise ratsionaalarvu $\frac{x}{y}$ korral, mis rahuldab võrratust

$$\left|\alpha - \frac{x}{y}\right| < \left|\alpha - \frac{a}{b}\right|,$$

on $y > b$. Geomeetriliselt tähendab see seda, et kui võtta arvteljel punkt α ja vahemik $(\alpha - \left|\frac{a}{b} - \alpha\right|, \alpha + \left|\frac{a}{b} - \alpha\right|)$, kus $\frac{a}{b}$ on α parim lähend, siis kõigi selles vahemikus asu-

vate ratsionaalmurdude nimetajad on suuremad kui b. Tõestame järgmise teoreemi.

Teoreem 2.9. Reaalarvu α ahelmurru iga lähismurd $\frac{P_n}{Q_n}$ $(n \geqslant 2)$ on arvu α parimaks lähendiks.

Tõestus. Võtame mistahes ratsionaalarvu $\frac{x}{y}$, mis erineb α-st vähem kui $\frac{P_n}{Q_n}$, s.t. ratsionaalarvu, mille korral $\left|\frac{x}{y} - \alpha\right| < \left|\frac{P_n}{Q_n} - \alpha\right|$. Tarvitseb näidata, et siis $y > Q_n$. Eelduse kohaselt

$$\left|\frac{x}{y} - \alpha\right| < \left|\frac{P_n}{Q_n} - \alpha\right| < \left|\frac{P_{n-1}}{Q_{n-1}} - \alpha\right|.$$

Et $\frac{x}{y}$ asub vahemikus $\left(\frac{P_{n-1}}{Q_{n-1}}, \frac{P_n}{Q_n}\right)$, siis $\left|\frac{P_n}{Q_n} - \frac{P_{n-1}}{Q_{n-1}}\right| > \left|\frac{P_{n-1}}{Q_{n-1}} - \frac{x}{y}\right| = \frac{|yP_{n-1} - xQ_{n-1}|}{Q_{n-1}y}$ ehk $\frac{1}{Q_n Q_{n-1}} > \frac{|yP_{n-1} - xQ_{n-1}|}{Q_{n-1}y}$.

Siit

$$\frac{y}{Q_n} > |yP_{n-1} - xQ_{n-1}| \neq 0.$$

Kui oleks $yP_{n-1} - xQ_{n-1} = 0$, siis $\frac{x}{y} = \frac{P_{n-1}}{Q_{n-1}}$. Viimane võrdus pole aga võimalik, sest $\frac{P_{n-1}}{Q_{n-1}}$ asub α-st kaugemal kui $\frac{P_n}{Q_n}$. Et $|yP_{n-1} - xQ_{n-1}|$ on naturaalarv, siis ongi $y > Q_n$.

Lähismurdude vahel kehtib seos

$$\frac{P_{n+1}}{Q_{n+1}} = \frac{P_n a_{n+1} + P_{n-1}}{Q_n a_{n+1} + Q_{n-1}}, \text{ kus } a_{n+1} \geqslant 1. \tag{14}$$

Kui $a_{n+1} > 1$, siis saab rääkida veel nn. vahepealsetest murdudest

$$\frac{P_n k + P_{n-1}}{Q_n k + Q_{n-1}}, \quad k = 1, 2, \ldots, a_{n+1} - 1.$$

Märgime tõestuseta, et ka mõningad ahelmurru vahepealsed murrud osutuvad selleks ahelmurruks arendatud reaalarvu parimateks lähenditeks ja tema parimateks lähenditeks saavad olla vaid murrud (14) (vt. [1, 5]).

Vajadus reaalarvu parimate lähendite leidmiseks võib tekkida mitmetel juhtudel. Mainime näiteks hammasülekande projekteerimist. Kahe hammasseostusega ratta pöörlemise nurkkiirused on pöördvõrdelised hammaste arvuga. Hammaste arv hammasrattas saab aga olla vaid täisarv, kusjuures hammasrattaid ei saa valmistada väga suure hammaste arvuga. Seega hammasrataste pöörlemise nurkkiiruste suhe on mitte väga suure lugeja ja nimetajaga ratsionaalarv. Kui nõutakse kahe võlli ühendamist hammasratta abil nii, et nende nurkkiiruste suhe oleks α, siis juhul, kui α on irratsionaalne (või on väga suure nimetajaga ratsionaalarv), ei ole nurkkiiruste suhe täpselt realiseeritav ja tuleb leppida α ratsionaalse lähendiga, mille nimetaja ei ole eriti suur. Sellise probleemi ees seisis muide 17. sajandi väljapaistev mehaanik, füüsik ja matemaatik C. Huygens (1629-1695) päikesesüsteemi mudeli konstrueerimisel, kui oli tarvis realiseerida planeetide tiirlemisperioodide tegelikke suhteid hammasratasülekannete abil. Huygens kasutaski nimetatud suhetele sobivate parimate lähendite saamiseks ahelmurdude lähismurde.

Harjutusülesandeid.

2.13. Leida arvu e ahelmurru lähismurd, mille nimetaja ei ületa 100 ja erineb sealjuures arvust e kõige vähem.

Hinnata lähendi täpsust.

2.14. Leida arvu $\sqrt{13}$ ahelmurru esimene lähismurd, mis erineb antud arvust vähem kui 10^{-5}.

2.15. Leida arvu $\sqrt{7}$ vähima nimetajaga parim ratsionaalne lähend, mis erineb sellest arvust vähem kui 10^{-4}.

2.16. Kontrollida teoreemi 2.6 abil, kas $\frac{38}{17}$ on irratsionaalarvu $\sqrt{5}$ ahelmurru üks lähismurde.

§ 5. REAALSED RUUTIRRATSIONAALID

1. Ruutirratsionaal ja perioodiline ahelmurd. Reaalseks ruutirratsionaaliks nimetatakse täisarvuliste kordajatega ruutvõrrandi reaalset lahendit, mis ei ole ratsionaalarv. Seega avaldub reaalne ruutirratsionaal kujul

$$\frac{A+\sqrt{D}}{B},$$

kus A, B, D on täisarvud, $D > 0$ ja D ei ole täisruut. Esitatud ruutirratsionaaliga ühist ruutvõrrandit rahuldab tema kaasirratsionaal

$$\frac{A-\sqrt{D}}{B}.$$

Ruutirratsionaalid on tihedalt seotud perioodiliste ahelmurdudega. Ahelmurdu nimetatakse perioodiliseks, kui teatud kohast alates tema elemendid hakkavad korduma, s.t. kui ta avaldub kujul

$$[a_1, a_2, \ldots, a_{i-1}, a_i, \ldots, a_{i+k-1}, a_i, \ldots, a_{i+k-1}, \ldots].$$

Viimast ahelmurdu tähistame lühidalt järgmiselt:

$$[a_1, a_2, \ldots, a_{i-1}, (a_i, \ldots, a_{i+k-1})].$$

Kui $i = 1$, siis nimetatakse perioodilist ahelmurdu puhtperi-

oodiliseks, kui $i > 1$, siis segaperioodiliseks.

Kirjutame irratsionaalarvu α kujul

$$\alpha = a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots + \cfrac{1}{a_{i+k-1} + \cfrac{1}{\alpha_{i+k}}}}}.$$

Kui osutub, et $\alpha_{i+k} = \alpha_i$, siis ahelmurd on perioodiline, kusjuures $\alpha = [a_1, \ldots, a_{i-1}, (a_i, \ldots, a_{i+k-1})]$. Tõepoolest,

$$\alpha_i = a_i + \cfrac{1}{a_{i+1} + \ddots + \cfrac{1}{a_{i+k-1} + \cfrac{1}{\alpha_i}}}.$$

Viimase nimetaja ahelmurruks arendamisel saame jälle sama tulemuse. On selge ka vastupidine: kui ahelmurd on perioodiline, siis mingist indeksist alates

$$\alpha_{i+k} = \alpha_i ,$$

kus k on kindel naturaalarv (perioodi pikkus), i võib aga teatud indeksist alates omandada kõiki väärtusi.

Teoreem 2.10. Reaalarv α, mis annab arendamisel perioodilise ahelmurru, on ruutirratsionaal.

Tõestus. Kasutame seost $\alpha_{i+k} = \alpha_i$ ja esitame α kahel kujul:

$$\alpha = [a_1, a_2, \ldots, a_{i-1}, \alpha_i] = \frac{P_{i-1}\alpha_i + P_{i-2}}{Q_{i-1}\alpha_i + Q_{i-2}} ,$$

$$\alpha = [a_1, a_2, \ldots, a_{i+k-1}, \alpha_i] = \frac{P_{i+k-1}\alpha_i + P_{i+k-2}}{Q_{i+k-1}\alpha_i + Q_{i+k-2}} .$$

Avaldame kummastki seosest α_i:

$$\alpha_i = \frac{P_{i-2} - \alpha Q_{i-2}}{Q_{i-1}\alpha - P_{i-1}} = \frac{P_{i+k-2} - \alpha Q_{i+k-2}}{Q_{i+k-1}\alpha - P_{i+k-1}} .$$

Seega rahuldab α järgmist täisarvuliste kordajatega ruutvõrrandit :

$$(Q_{i-1}Q_{i+k-2} - Q_{i-2}Q_{i+k-1})\alpha^2 + (Q_{i+k-1}P_{i-2} + Q_{i-2}P_{i+k-1} -$$

$$- P_{i+k-2}Q_{i-1} - P_{i-1}Q_{i+k-2})\alpha + P_{i+k-2}P_{i-1} - P_{i+k-1}P_{i-2} = 0.$$

Teoreem on tõestatud.

Näide 1. Leida ruutirratsionaal, mis avaldub järgmise perioodilise ahelmurruna: $\alpha = [4,(1,3,1,8)]$. Siin $\alpha_2 = \alpha_6$. Seega i = 2, i+k = 6. Esitame α α_2 ja α_6 kaudu:

$$\alpha = \frac{P_1\alpha_2 + P_0}{Q_1\alpha_2 + Q_0} = \frac{P_5\alpha_6 + P_4}{Q_5\alpha_6 + Q_4} .$$

Arvutame P_i, Q_i:

		4	1	3	1	8
0	1	4	5	19	24	211
1	0	1	1	4	5	44

Seega

$$\alpha = \frac{4\alpha_2 + 1}{\alpha_2} = \frac{211\alpha_6 + 24}{44\alpha_6 + 5},$$

millest

$$\alpha_2 = \frac{1}{\alpha - 4} = \frac{24 - 5\alpha}{44\alpha - 211} = \alpha_6,$$

$$44\alpha - 211 = 24\alpha - 96 - 5\alpha^2 + 20\alpha,$$

$$5\alpha^2 = 115,$$

$$\alpha = \sqrt{23}.$$

(Miks on $\alpha = \sqrt{23}$, mitte aga $-\sqrt{23}$?)

Muidugi võib leitud P_m ja Q_m asendada kohe teoreemi tõestamisel saadud ruutvõrrandisse. Viimast on aga raske meeles pidada.

Kehtib ka tõestatud teoreemi pöördteoreem:

Teoreem 2.11 (Lagrange). Iga ruutirratsionaal avaldub perioodilise ahelmurruna.

Tõestus (vrd.[10]). Olgu α ruutirratsionaal, s.t. täisarvuliste kordajatega ruutvõrrandi

$$b_1x^2 - 2c_1x + d_1 = 0 \tag{1}$$

irratsionaalne lahend (alati võib saavutada, et lineaarliikme kordaja $2c_1$ on paarisarv; seepärast eeldame, et ka c_1 on täisarv). Leiame võrrandid järjestikuste α_i-de arvutamiseks. Kõigepealt

$$\alpha = a_1 + \frac{1}{\alpha_2} \qquad (\alpha_2 > 1), \tag{2}$$

mistõttu kehtib samasus

$$b_1(a_1 + \frac{1}{\alpha_2})^2 - 2c_1(a_1 + \frac{1}{\alpha_2}) + d_1 = 0$$

ehk

$$(b_1a_1^2 - 2c_1a_1 + d_1)\alpha_2^2 - 2(c_1 - b_1a_1)\alpha_2 + b_1 = 0.$$

Näeme, et α_2 rahuldab ruutvõrrandit

$$b_2x^2 - 2c_2x + d_2 = 0, \tag{3}$$

kus b_2, c_2 ja d_2 on samuti täisarvud nagu võrrandi (1) kordajad, kusjuures

$$\begin{aligned} b_2 &= b_1a_1^2 - 2c_1a_1 + d_1, \\ c_2 &= c_1 - b_1a_1, \\ d_2 &= b_1. \end{aligned} \tag{4}$$

Sama tüüpi ruutvõrrandid saame $\alpha_3, \ldots, \alpha_i, \alpha_{i+1}, \ldots$ jaoks. Kui $\alpha_i = a_i + \frac{1}{\alpha_{i+1}}$ rahuldab ruutvõrrandit

(5) $$b_i x^2 - 2c_i x + d_i = 0,$$

siis α_{i+1} rahuldab võrrandit

$$b_{i+1}x^2 - 2c_{i+1}x + d_{i+1} = 0,$$

kus

(6) $$b_{i+1} = b_i a_i^2 - 2c_i a_i + d_i,$$

(7) $$c_{i+1} = c_i - b_i a_i,$$

(8) $$d_{i+1} = b_i.$$

Siinjuures b_{i+1}, c_{i+1}, d_{i+1} on täisarvud. Kõikide võrrandite diskriminandid ühtivad, sest

$$D_{i+1} = c_{i+1}^2 - b_{i+1}d_{i+1} = (c_i - b_i a_i)^2 -$$

$$- b_i(b_i a_i^2 - 2c_i a_i + d_i) = c_i^2 - b_i d_i = D_i.$$

Niisiis $D_{i+1} = D_i = \ldots = D_1 = c_1^2 - b_1 d_1 = D$.

Vaatleme lõpmatut kordajate jada

(9) $$b_2, b_3, b_4, b_5, \ldots$$

Tõestame, et siin on lõpmata palju naaberelemente, mis on vastandmärkidega. Oletame vastupidi, et selliseid elemente on lõplik hulk. Siis alates teatud kohast on jada (9) elemendid kõik ühe ja sama märgiga. Olgu $b_i > 0$, kui $i \geqslant k$. Siis seose (8) tõttu on positiivsed kõik kordajad d_i alates kordajast $d_{k+1} = b_k$. Teiselt poolt näitab valem (7), et siis

(10) $$c_k > c_{k+1} > c_{k+2} > \ldots ,$$

sest $a_i > 0$. Et kõik c_i on täisarvud, siis teatud kohast alates on kõik c_i negatiivsed. Seega alates teatud indeksist

kehtivad võrratused

$$b_i > 0, \quad c_i < 0, \quad d_i > 0.$$

Et $\alpha_i > 0$, siis peab kehtima võrratus

$$b_i \alpha_i^2 - 2c_i \alpha_i + d_i > 0.$$

Tulemus on vastuolus eeldusega, et α_i on võrrandi (5) lahend. Analoogilisele vastuolule jõuame, kui oletame, et jadas (9) on teatud indeksist i alates kõik $b_i < 0$. Ilmne on ka, et üksk̈i $b_i \neq 0$. Seega on jadas (9) lõpmata palju vastandmärgilisi naaberelemente. Olgu b_m ja b_{m+1} vastandmärgilised. Ruutvõrrandi, mida rahuldab α_{m+1}, võib seose (8) tõttu esitada kujul

(11) $$b_{m+1}x^2 - 2c_{m+1}x + b_m = 0.$$

Nagu äsja tõestasime, on selliseid võrrandeid, kus esimene ja viimane kordaja on vastandmärgilised, lõpmata palju. Igal sellisel võrrandil (11) on üks positiivne ja üks negatiivne lahend. Positiivseks lahendiks on α_{m+1} (miks?). Näitame, et võrrandite (11) seas on erinevaid vaid lõplik hulk. Lähtume diskriminandist, mis on kõigil võrranditel sama:

$$c_{m+1}^2 - b_{m+1}b_m = D > 0.$$

Et $b_m b_{m+1} < 0$, siis $c_{m+1}^2 < D$ ehk $|c_{m+1}| < \sqrt{D}$. Samuti on $|b_{m+1}b_m| < D$. Täisarve, mis rahuldavad viimaseid võrratusi, on lõplik hulk. Järelikult lõpmata paljude võrrandite (11) hulgas on erinevaid vaid lõplik hulk. Olgu kaheks ühtivaks võrrandiks võrrandid

$$b_{\lambda+1}x^2 - 2c_{\lambda+1}x + b = 0$$

ja

$$b_{\mu+1}x^2 - 2c_{\mu+1}x + b = 0.$$

Nende ainsad positiivsed lahendid peavad ühtima: $\alpha_{\lambda+1} = \alpha_{\mu+1}$. See aga tähendab, et α on perioodiline.

2.* Puhtperioodilised ahelmurrud. Selgitame, missugused ruutirratsionaalid annavad arendamisel puhtperioodilise ahelmurru. Vastuse sellele küsimusele annab järgmine teoreem.

Teoreem 2.12. Ruutirratsionaali

$$\alpha = \frac{A + \sqrt{D}}{B}$$

ahelmurd on puhtperioodiline parajasti siis, kui $\alpha > 1$ ja kaasirratsionaal

$$\overline{\alpha} = \frac{A - \sqrt{D}}{B}$$

rahuldab tingimust $-1 < \overline{\alpha} < 0$.

Tõestus. Tarvilikkus. Olgu α puhtperioodilise ahelmurru väärtus, s.t. teatud indeksi $k \geqslant 2$ korral $\alpha_k = \alpha$. Siis $a_1 = a_k \geqslant 1$, millest järeldub omakorda, et $\alpha > 1$. Seostest

$$\alpha = \frac{P_{k-1}\alpha_k + P_{k-2}}{Q_{k-1}\alpha_k + Q_{k-2}}, \quad \alpha_k = \alpha$$

saame, et α rahuldab samasust

$$Q_{k-1}\alpha^2 + (Q_{k-2} - P_{k-1})\alpha - P_{k-2} = 0.$$

Arvutades ruutpolünoomi

$$f(x) = Q_{k-1}x^2 + (Q_{k-2} - P_{k-1})x - P_{k-2}$$

väärtused kohal 0 ja -1 saame $f(0) = -P_{k-2} < 0$ ja $f(-1) = (Q_{k-1} - Q_{k-2}) + (P_{k-1} - P_{k-2}) > 0$, millest nähtub, et polünoomi teine juur $\overline{\alpha}$ rahuldab võrratust $-1 < \overline{\alpha} < 0$.

Piisavus. Olgu $\alpha = \frac{A + \sqrt{D}}{B} > 1$ ja $-1 < \overline{\alpha} = \frac{A - \sqrt{D}}{B} < 0$.

Nagu nähtus teoreemi 2.11 tõestamisel, on kõik irratsionaalarvud α_n samuti ruutirratsionaalid, kusjuures ruutvõrranditel, mida nad rahuldavad, on ühine diskriminant D. Niisiis

$$\alpha_n = \frac{A_n + \sqrt{D}}{B_n}, \quad \bar{\alpha}_n = \frac{A_n - \sqrt{D}}{B_n},$$

kus A_n, B_n on täisarvud. Tõestame täieliku induktsiooni meetodil, et iga $n \geqslant 1$ korral

(12) $$-1 < \bar{\alpha}_n < 0.$$

Tingimus on täidetud eelduse kohaselt, kui n = 1, sest $\alpha_1 = \alpha$. Oletame, et võrratus (12) kehtib mingi $n \geqslant 1$ korral ja näitame, et ta kehtib siis indeksi n+1 korral. Kuna $\alpha_n = a_n + \frac{1}{\alpha_{n+1}}$, siis kaasirratsionaalide vahel kehtib seos $\bar{\alpha}_n = a_n + \frac{1}{\bar{\alpha}_{n+1}}$ (kontrollida!), millest $\bar{\alpha}_{n+1} = \frac{1}{\bar{\alpha}_n - a_n}$. Et $a_n \geqslant 1$ ja $-1 < \bar{\alpha}_n < 0$, siis saamegi võrratused $-1 < \bar{\alpha}_{n+1} < 0$. Lagrange'i teoreemi kohaselt eksisteerivad i ja k nii, et $\alpha_{i+k} = \alpha_i$ ja järelikult $\bar{\alpha}_{i+k} = \bar{\alpha}_i$. Näitame, et siit järeldub võrdus $\alpha_{k+1} = \alpha_1 = \alpha$, mis tähendabki, et α on puhtperioodiline. Seosest $\alpha_{i-1} = a_{i-1} + \frac{1}{\alpha_i}$ saame

$$\bar{\alpha}_{i-1} = a_{i-1} + \frac{1}{\bar{\alpha}_i}, \quad -\frac{1}{\bar{\alpha}_i} = a_{i-1} + (-\bar{\alpha}_{i-1}).$$

Et $0 < -\bar{\alpha}_{i-1} < 1$, siis $a_{i-1} = \left[-\frac{1}{\bar{\alpha}_i}\right]$ (täisosa). Analoogiliselt seosest

$$\bar{\alpha}_{k+i-1} = a_{k+i-1} + \frac{1}{\bar{\alpha}_{i+k}}$$

saame

$$a_{i+k-1} = \left[-\frac{1}{\bar{\alpha}_{i+k}}\right]$$

ja et $\overline{\alpha}_{i+k} = \overline{\alpha}_i$, siis $a_{i+k-1} = a_{i-1}$. Et võrduste

$$\overline{\alpha}_{i-1} = a_{i-1} + \frac{1}{\overline{\alpha}_i}, \quad \overline{\alpha}_{i+k-1} = a_{i+k-1} + \frac{1}{\overline{\alpha}_{i+k}}$$

paremad pooled on võrdsed, siis on $\overline{\alpha}_{i+k-1} = \overline{\alpha}_{i-1}$ ja $\alpha_{i+k-1} = \alpha_{i-1}$. Tõestasime, et võrdusest $\alpha_{i+k} = \alpha_i$ järeldub võrdus $\alpha_{i+k-1} = \alpha_{i-1}$. Tõestatu põhjal järeldub siit võrdus $\alpha_{k+i-2} = \alpha_{i-2}$ jne., kuni jõuamegi võrduseni $\alpha_{k+1} = \alpha_1 = \alpha$.

Järeldus. Ühegi ruutirratsionaali $\sqrt{D}$ $(D > 1)$ ahelmurd ei ole puhtperioodiline.

Tõepoolest, $-\sqrt{D} < -1$.

Näide 2. Ruutirratsionaali $\alpha = \frac{2+\sqrt{7}}{3}$ ahelmurd on puhtperioodiline, sest $\alpha > 1$ ja $\overline{\alpha} = \frac{2-\sqrt{7}}{3}$ asub vahemikus $(-1, 0)$. Ahelmurruks arendamisel saamegi

$$\frac{2+\sqrt{7}}{3} = [(1, 1, 1, 4)].$$

Teoreem 2.13. Olgu D mitteruutarv ja $\sqrt{D} > B > 0$. Siis ruutirratsionaali $\frac{\sqrt{D}}{B}$ ahelmurruks on

$$\frac{\sqrt{D}}{B} = [a_1, (a_2, \ldots, a_{k-1}, 2a_1)].$$

Tõestus. Vaatleme ruutirratsionaali $\alpha = a_1 + \frac{\sqrt{D}}{B}$, kus $a_1 = \left[\frac{\sqrt{D}}{B}\right]$. Et $\frac{\sqrt{D}}{B} > 1$, siis $\alpha > 1$ ja $\overline{\alpha} = a_1 - \frac{\sqrt{D}}{B}$ asub vahemikus $(-1, 0)$. Seega on α ahelmurd puhtperioodiline. Et $[\alpha] = \left[a_1 + \frac{\sqrt{D}}{B}\right] = 2a_1$, siis

$$a_1 + \frac{\sqrt{D}}{B} = [2a_1, a_2, \ldots, a_{k-1}, 2a_1, a_2, \ldots, a_{k-1}, 2a_1, \ldots],$$

millest

$$\frac{\sqrt{D}}{B} = [a_1, (a_2, a_3, \ldots, a_{k-1}, 2a_1)].$$

Näiteks on

$$\sqrt{13} = [3, (1, 1, 1, 1, 6)],$$

$$\sqrt{43} = [6, (1, 1, 3, 1, 5, 1, 3, 1, 1, 12)],$$

$$\frac{\sqrt{5}}{2} = [1, (8, 2)] \quad \text{(kontrollida!)}.$$

Märgime tõestuseta, et ruutirratsionaali $\frac{\sqrt{D}}{B}$ korral alati

$$a_{k-1} = a_2,$$

$$a_{k-2} = a_3,$$

$$\ldots\ldots\ldots$$

(vt. [7], lk. 336).

3.* Pelli võrrand. Vaatleme diofantilise võrrandi

(13) $$x^2 - Dy^2 = 1$$

lahendamist. Euler nimetas seda võrrandit mingi arusaamatuse tõttu J.Pelli (1610-1685) nime järgi Pelli võrrandiks. See nimetus kandus Euleri töödest edasi ja on kirjanduses kasutusel senini. On selgunud, (vt. [1],lk. 314), et J.Pell ei tegelnud üldse võrrandiga (13), esimesena aga leidis üldise lahendusmeetodi P.Fermat. Seepärast oleks õigem nimetada võrrandit (13) Fermat' võrrandiks. Jääme siiski kirjanduses üldiselt kasutatava nimetuse juurde.

Kui $D < 0$ või $D = d^2$, siis on võrrandi (13) lahendamine triviaalne. Eeldame seepärast, et võrrandis (13) on D positiivne täisarv ja $\sqrt{D}$ irratsionaalarv. Olgu arvupaar (x_0, y_0) võrrandi (13) lahend. Võime piirduda positiivsete lahenditega, sest kui (x_0, y_0) on lahend, siis on seda ka $(\pm x_0, \pm y_0)$. Märgime veel, et x_0, y_0 on seose

(14) $$x_o^2 - Dy_o^2 = 1$$

tõttu ühistegurita. Kirjutame samasuse (14) kujul

$$(x_o - y_o\sqrt{D})(x_o + y_o\sqrt{D}) = 1$$

ehk

$$\frac{x_o}{y_o} - \sqrt{D} = \frac{1}{y_o^2\left(\frac{x_o}{y_o} + \sqrt{D}\right)} .$$

Kuna siit järeldub, et $\frac{x_o}{y_o} > \sqrt{D} > 1$, siis

$$\frac{x_o}{y_o} + \sqrt{D} > 2\sqrt{D} > 2.$$

Viimast võrratust arvestades saame, et

$$0 < \frac{x_o}{y_o} - \sqrt{D} < \frac{1}{2y_o^2} .$$

Teoreemi 2.6 kohaselt peab siis $\frac{x_o}{y_o}$ olema ruutirratsionaali $\sqrt{D}$ ahelmurru üks lähismurdudest $\frac{P_n}{Q_n}$, kusjuures $x_o = P_n$, $y_o = Q_n$. Et $\frac{x_o}{y_o} > \sqrt{D}$, siis indeks n peab olema paarisarv. Niisiis tuleb Pelli võrrandi kõiki lahendeid otsida vaid $\sqrt{D}$ ahelmurru paarisarvulise indeksiga lähismurdude lugejate ja (vastavate) nimetajate hulgast.

Edasi uurime, millised lähismurrud võivad anda võrrandi lahendi ja teeme kindlaks, kas Pelli võrrand on lahenduv iga D korral.

Avaldame D suuruste P_n ja Q_n kaudu:

(15) $$\sqrt{D} = \frac{P_n\alpha_{n+1} + P_{n-1}}{Q_n\alpha_{n+1} + Q_{n-1}} .$$

Siit

$$\alpha_{n+1} = \frac{Q_{n-1}\sqrt{D} - P_{n-1}}{P_n - Q_n\sqrt{D}} = \frac{(Q_{n-1}\sqrt{D} - P_{n-1})(P_n + Q_n\sqrt{D})}{P_n^2 - Q_n^2 D}$$

ehk arvestades, et n on paarisarv,

(16) $$\alpha_{n+1} = \frac{b + \sqrt{D}}{P_n^2 - Q_n^2 D},$$

kus $b = Q_{n-1}Q_n D - P_{n-1}P_n$ on täisarv.

Näitame, et $b > 0$. Selleks lähtume seosest

(17) $$b + \sqrt{D} = (Q_{n-1}\sqrt{D} - P_{n-1})(P_n + Q_n\sqrt{D}).$$

Et n on paarisarv, siis $\frac{P_{n-1}}{Q_{n-1}} < \sqrt{D} < \frac{P_n}{Q_n}$ ja eelmise paragrahvi valemist (6) (lk. 61) saame hinnangu

$$\sqrt{D} - \frac{P_{n-1}}{Q_{n-1}} = \left|\sqrt{D} - \frac{P_{n-1}}{Q_{n-1}}\right| > \frac{1}{2Q_{n-1}Q_n},$$

millest

$$Q_{n-1}\sqrt{D} - P_{n-1} > \frac{1}{2Q_n}$$

ja seose (17) tõttu

$$b + \sqrt{D} > \frac{1}{2Q_n}(P_n + Q_n\sqrt{D}) = \frac{1}{2}\left(\frac{P_n}{Q_n} + \sqrt{D}\right) > \sqrt{D}.$$

Seega tõepoolest $b > 0$.

Murru (16) nimetaja $P_n^2 - DQ_n^2$ võrdub võrrandi (13) vasaku poolega, kus $x = P_n$ ja $y = Q_n$. Täisarvude paar (P_n, Q_n) on seega võrrandi (13) lahendiks parajasti siis, kui

(18) $$\alpha_{n+1} = b + \sqrt{D}.$$

Et seose (15) tõttu

$$\sqrt{D} = [a_1, a_2, \ldots, a_n, \alpha_{n+1}],$$

siis võib avaldise (18) esitada kujul

$$\alpha_{n+1} = b + \sqrt{D} = [b+a_1, a_2, \ldots, a_n, \alpha_{n+1}] =$$

$$= [b+a_1, a_2, \ldots, a_n, b+a_1, a_2, \ldots, a_n, \ldots].$$

Kuna $b + a_1 > 0$, siis on α_{n+1} regulaarne puhtperioodiline ahelmurd ja teoreemi 2.12 kohaselt

$$-1 < \overline{\alpha}_{n+1} = b - \sqrt{D} < 0.$$

Siit $\sqrt{D} - 1 < b < \sqrt{D}$, mistõttu $b = [\sqrt{D}] = a_1$. Niisiis on arvupaar (P_n, Q_n) võrrandi (13) lahend parajasti siis, kui $\sqrt{D}$ avaldub perioodilise ahelmurruna kujul

$$\sqrt{D} = [a_1, (a_2, \ldots, a_n, 2a_1)], \tag{19}$$

kus perioodi pikkus n on paarisarv. Kujul (19) avaldub aga teoreemi 2.13 põhjal $\sqrt{D}$ iga positiivse täisarvu D korral, mis ei ole täisruut. Juhul kui irratsionaalarvu $\sqrt{D}$ ahelmurru perioodi pikkus n on paarisarv, on võrrandil (13) kindlasti lahend $x_0 = P_n$, $y_0 = Q_n$, kus n on perioodi eelviimase elemendi indeks. Kui aga $\sqrt{D}$ ahelmurru perioodi pikkus on paaritu arv k, siis võib $\sqrt{D}$ avaldada ikkagi kujul (19), kus n on paarisarv, kui vaid ühendada kaks perioodi:

$$\sqrt{D} = [a_1, (a_2, a_3, \ldots, a_k, 2a_1, a_2, a_3, \ldots, a_k, 2a_1)] =$$

$$= [a_1, (a_2, a_3, \ldots, a_n', 2a_1)], \quad n = 2k.$$

Seega on võrrand (13) lahenduv ka juhul, kui $\sqrt{D}$ ahelmurru vähima perioodi pikkus on paaritu arv k, kuid sel juhul on lahendiks arvupaar (P_{2k}, Q_{2k}). Kummalgi juhul saame niiviisi vähimad positiivsed lahendid. Ülejäänud lahendid saadakse, kui peatuda mingi teise perioodi eelviimasel elemendil ja arvutada vastava lähismurru lugeja ja nimetaja. Seega on võrrandi (13) kõik lahendid antud arvupaaridega

$$(P_k, Q_k), (P_{2k}, Q_{2k}), (P_{3k}, Q_{3k}), (P_{4k}, Q_{4k}), \ldots,$$

kui $\sqrt{D}$ ahelmurru vähima perioodi pikkus k on paarisarv, ja

arvupaaridega

$$(P_{2k}, Q_{2k}), (P_{4k}, Q_{4k}), (P_{6k}, Q_{6k}), \ldots,$$

kui $\sqrt{D}$ ahelmurru vähima perioodi pikkus k on paaritu arv.

Näide 4. Lahendame võrrandi $x^2 - 2y^2 = 1$.

Kuna $\sqrt{2} = [1,(2)]$, s.t. vähima perioodi pikkus $k = 1$ on paaritu, siis lahenditeks on arvupaarid (P_2, Q_2), (P_4, Q_4), (P_6, Q_6), ..., s.o. (3, 2), (17, 12), (99, 70), ...

Harjutusülesandeid.

2.17. Leida ruutirratsionaalid, mille ahelmurrud on järgmised:

a) $[(1)]$, b) $[-1,(1, 2)]$,

c) $[(18, 2, 3, 3, 2)]$, d) $[0,(2, 1, 1, 2, 10)]$,

e) $[7,(1, 1, 4, 1, 1, 14)]$, f) $[9,(1, 18)]$.

2.18. Kasutades teoreemi 2.12 teha kindlaks, kas järgmiste ruutirratsionaalide ahelmurrud on puhtperioodilised või mitte:

a) $\frac{2 + \sqrt{3}}{4}$, b) $\frac{1 + \sqrt{13}}{3}$.

2.19. Teades, et $\frac{2 + \sqrt{7}}{3} = [(1, 1, 1, 4)]$, kirjutada välja järgmiste ruutirratsionaalide ahelmurrud:

a) $\frac{8 + \sqrt{7}}{3}$, b) $\frac{-1 + \sqrt{7}}{3}$, c) $\frac{-4 + \sqrt{7}}{3}$.

2.20. Teades, et $\frac{\sqrt{11}}{3} = [1,(9, 2)]$, kirjutada välja ruutirratsionaalide

$$\frac{-3 + \sqrt{11}}{3} \text{ ja } \frac{3 + \sqrt{11}}{3} \text{ ahelmurrud.}$$

2.21. Lahendada järgmised Pelli võrrandid:

a) $x^2 - 3y^2 = 1$,

b) $x^2 - 32y^2 = 1$,

c) $x^2 - 13y^2 = 1$,

d) $x^2 - 89y^2 = 1$,

e) $x^2 - 98y^2 = 1$.

III. ALGEBRALISED JA TRANSTSENDENTSED ARVUD

Def. mid

§ 1. ALGEBRALISTE ARVUDE KORPUS

Kompleksarvu (sealhulgas reaalarvu) α nimetatakse algebraliseks arvuks, kui ta on mingi täisarvuliste kordajatega mitte-nullpolünoomi

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$$

juur, s.t. kui $f(\alpha) = 0$. Kui α on täisarvuliste kordajatega n-astme polünoomi juur, kuid ei ole ühegi madalama astmega täisarvuliste kordajatega mitte-nullpolünoomi juur, siis arvu α nimetatakse n-astme algebraliseks arvuks.

Antud definitsiooni kohaselt on ratsionaalarvud esimese astme algebralised arvud, ruutirratsionaalid aga teise astme algebralised arvud. Kolmanda astme algebralisi arve nimetatakse sageli kuupirratsionaalideks (näiteks $\sqrt[3]{2}$).

On ilmne, et algebralise arvu definitsioonis võib lubada ka $f(x)$ kordajate ratsionaalarvulisust - defineeritavate arvude klass sellest ei muutu.

Tõestame järgmise omaduse.

Teoreem 3.1. Kui n-astme algebraline arv α on ratsionaalsete kordajatega n-astme polünoomi $f(x)$ juur, siis $f(x)$ on taandumatu üle ratsionaalarvude korpuse.

Tõestus. Kui oletada, et $f(x)$ on taanduv üle ratsio-

naalarvude korpuse, siis $f(x) = g(x)h(x)$, kus $g(x)$ ja $h(x)$ on mõlemad ratsionaalsete kordajatega madalama kui n-astme polünoomid. Siis aga $0 = f(\alpha) = g(\alpha)h(\alpha)$ ja seega kas $g(\alpha) = 0$ või $h(\alpha) = 0$. See on aga vastuolus n-astme algebralise arvu definitsiooniga.

Kui n-astme $(n \geqslant 1)$ algebraline arv α_1 on ratsionaalsete kordajatega n-astme n o r m e e r i t u d polünoomi*)

$$f(x) = x^n + b_1x^{n-1} + \ldots + b_n$$

juur, siis polünoomi $f(x)$ nimetatakse arvu α_1 <u>minimaalpolünoomiks</u>, selle polünoomi ülejäänud juuri $\alpha_2, \alpha_3, \ldots, \alpha_n$ aga arvu α_1 <u>kaasarvudeks</u>.

Teoreemist 3.1 järeldub, et arvu minimaalpolünoom on taandumatu üle ratsionaalarvude korpuse.

<u>Teoreem 3.2</u>. Kui α ja β on algebralised arvud, siis $\alpha+\beta$, $\alpha-\beta$, $\alpha\beta$ ja juhul, kui $\beta \neq 0$, ka $\frac{\alpha}{\beta}$, on algebralised arvud; teisiti: kõigi algebraliste arvude hulk on korpus.

<u>Tõestus</u>. Olgu $\alpha_1 = \alpha$ n-astme algebraline arv ja $\beta_1 = \beta$ m-astme algebraline arv. Olgu $f(x)$ ja $g(x)$ nende arvude vastavad minimaalpolünoomid, $\alpha_2, \ldots, \alpha_n$ ja $\beta_2, \ldots, \beta_m$ aga vastavad kaasarvud. Siis Vieta valemite kohaselt

$$f(x) = x^n - \sigma_1x^{n-1} + \sigma_2x^{n-2} - \ldots + (-1)^n\sigma_n,$$

$$g(x) = x^m - \tau_1x^{m-1} + \tau_2x^{m-2} - \ldots + (-1)^m\tau_m,$$

*) Normeeritud polünoomiks nimetame polünoomi, mille pealiikme kordaja on 1.

kus σ_k (k=1,2,...,n) on sümmeetrilised põhipolünoomid polünoomi f(x) juurtest $\alpha_1, \alpha_2, \ldots, \alpha_n$ ja τ_l (l=1,2,...,m) on sümmeetrilised põhipolünoomid polünoomi g(x) juurtest $\beta_1, \beta_2, \ldots, \beta_m$. Kuna f(x) ja g(x) kordajad on eelduse kohaselt ratsionaalarvud, siis on seda ka põhipolünoomide väärtused σ_k ja τ_l.

Moodustame nm-astme polünoomi

$$F(x) = \prod_{i=1}^{n} \prod_{j=1}^{m} (x - (\alpha_i + \beta_j)) =$$

$$= (x - \alpha_1 - \beta_1)(x - \alpha_1 - \beta_2)\ldots(x - \alpha_1 - \beta_m) \cdot$$

$$\cdot (x - \alpha_2 - \beta_1)(x - \alpha_2 - \beta_2)\ldots(x - \alpha_2 - \beta_m) \cdot$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\cdot (x - \alpha_n - \beta_1)(x - \alpha_n - \beta_2)\ldots(x - \alpha_n - \beta_m) =$$

$$= x^{nm} - (m\sigma_1 + n\tau_1)x^{nm-1} + \ldots$$

On lihtne kontrollida, et funktsioon

$$F(x) \equiv F(x; \alpha_1, \alpha_2, \ldots, \alpha_n, \beta_1, \beta_2, \ldots, \beta_m)$$

on nii argumentide süsteemi $\alpha_1, \alpha_2, \ldots, \alpha_n$ kui ka argumentide süsteemi $\beta_1, \beta_2, \ldots, \beta_m$ suhtes sümmeetriline polünoom. Kasutame järgmist teoreemi (vt. А.Г. К у р о ш. Курс высшей алгебры, изд. 2 и 3, 1950, 1952, § 37), mis on kõrgema algebra kursusest tuttava sümmeetriliste polünoomide põhiteoreemi üldistuseks:

kui $G(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m)$ on kahe argumentide süsteemi $\alpha_1, \ldots, \alpha_n$ ja $\beta_1, \ldots, \beta_m$ suhtes sümmeetriline polünoom üle korpuse K, siis

$G(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m) = \phi(\sigma_1, \ldots, \sigma_n, \tau_1, \ldots, \tau_m)$, kus $\phi(\sigma_1, \ldots, \sigma_n, \tau_1, \ldots, \tau_m)$ on polünoom kordajatega korpusest K, $\sigma_1, \ldots, \sigma_n$ ja $\tau_1, \ldots, \tau_m$ on aga eespool defineeritud sümmeetrilised põhipolünoomid.

Võttes polünoomiks $G(\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m)$ polünoomi $F(x; \alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_m)$ ja korpuseks K ratsionaalarvude korpuse ning arvestades, et $\sigma_1, \ldots, \sigma_n$ ja $\tau_1, \ldots, \tau_m$ on ratsionaalsed, järeldame, et polünoomi $F(x)$ kordajad on ratsionaalsed. See tähendab, et $\alpha_i + \beta_j$, sealhulgas ka $\alpha + \beta$ on algebraline arv, mille aste ei ületa nm.

Analoogiliselt saab tõestada, et korrutis $\alpha\beta$ on algebraline arv. Selleks tarvitseb vaadelda polünoomi

$$F(x) = \prod_{i=1}^{n} \prod_{j=1}^{m} (x - \alpha_i \beta_j),$$

mille üheks juureks on $\alpha_1 \beta_1 = \alpha\beta$.

Kuna β on polünoomi $g(x)$ juur, siis $-\beta$ ja $\frac{1}{\beta}$ (kui $\beta \neq 0$) on vastavalt ratsionaalsete kordajatega polünoomide $g(-x)$ ja $x^m g(\frac{1}{x})$ juured. See tähendab, et ka $-\beta$ ja $\frac{1}{\beta}$ on algebralised arvud.

Et $\alpha - \beta = \alpha + (-\beta)$ ja $\frac{\alpha}{\beta} = \alpha \cdot \frac{1}{\beta}$, siis eeltõestatu põhjal on ka vahe ja jagatis algebralised arvud.

Järeldus. Reaalsete algebraliste arvude hulk on korpus.

Tõepoolest, aritmeetilised tehted ei vii välja reaalarvude korpusest.

Märgime tõestuseta ära (kompleksete) algebraliste arvude korpuse järgmise tähelepanuväärse omaduse.

Teoreem 3.3. Kui $\beta_0, \beta_1, \ldots, \beta_n$ on algebralised arvud, siis polünoomi

$$\beta_0 x^n + \beta_1 x^{n-1} + \ldots + \beta_n$$

iga juur α (kompleksarvude korpusest) on algebraline arv; teisiti: algebraliste arvude korpus on algebraliselt kinnine.

On selge, et r e a a l s e t e algebraliste arvude korpus pole algebraliselt kinnine (miks?).

Teoreemidest 3.2 ja 3.3 järeldub, et iga arv, mis on saadud algebralistest arvudest lõpliku arvu aritmeetiliste tehete ja juurimiste tulemusena, on algebraline arv. Nii näiteks on algebralised arvud

$$2 + \sqrt[3]{3 + \sqrt{2}} \quad \text{ja} \quad \frac{2 - i\sqrt[3]{2}}{\sqrt{\sqrt{5} + \sqrt[3]{7} + \sqrt[7]{5}}} + \sqrt[9]{10},$$

kus i on imaginaarühik. Radikaalide abil ei saa aga esitada kõiki algebralisi arve, sest teatavasti mitte kõigi kõrgema kui neljanda astme polünoomide juured ei ole avaldatavad radikaalide abil polünoomi kordajatest.

Peatume lühidalt veel algebralise täisarvu mõistel.

Arvu α nimetatakse algebraliseks täisarvuks, kui ta on mingi t ä i s a r v u l i s t e kordajatega n o r m e e r i t u d polünoomi

(1) $$x^n + a_1 x^{n-1} + \ldots + a_n$$

juur.

Kõigi algebraliste täisarvude hulk on ring, mitte enam korpus, sest algebraliste täisarvude α, β jagatis pole alati algebraline täisarv. On aga huvitav märkida, et kui polü-

noomi (1) kordajad on algebralised täisarvud, siis on selle polünoomi juurteks ikkagi algebralised täisarvud. Seega on algebraliste täisarvude ring algebraliselt kinnine.

Algebraliste arvude teoorias on kaks suurt suunda. Üheks suunaks on algebraline arvuteooria, mis on loodud E.Kummeri poolt eelmise sajandi keskel ja uurib algebraliste arvude omadusi. Nimelt on algebralistel täisarvudel rida omadusi, mis on analoogilised tavaliste (ratsionaalsete) täisarvude omadustega. Peamine erinevus on aga selles, et arvu lahutamine algteguriteks pole ühene. Ühesuse saavutamiseks kasutas Kummer nn. ideaalseid arve. Teiseks suunaks on algebraliste arvude lähendamine ratsionaalarvudega. Peatumata küsimustel, mis kuuluvad algebralise arvuteooria valdkonda, vaatleme järgmises paragrahvis algebraliste arvude lähendamist ratsionaalarvudega.

§2. ALGEBRALISTE ARVUDE RATSIONAALSED LÄHENDID

Nagu järeldasime teoreemist 2.8, kehtib 2. astme algebralise arvu $\alpha = \frac{1+\sqrt{5}}{2}$ ja küllalt väikese positiivse reaalarvu c korral iga ratsionaalarvu*) $\frac{a}{b}$ puhul võrratus

$$\left|\alpha - \frac{a}{b}\right| \geq \frac{c}{b^2} .$$

Viimane võrratus näitab, et nimetatud arvu α ei saa ratsionaalarvudega eriti hästi lähendada. Osutub, et siin on tege-

*) Eeldame alati, et ratsionaalmurru nimetaja b on positiivne.

mist reaalsete algebraliste arvude ühe üldise omadusega. Kehtib nimelt järgmine teoreem.

Teoreem 3.4 (Liouville, 1844). Iga reaalse n-astme ($n \geqslant 1$) algebralise arvu α jaoks leidub positiivne arv c, nii et kõikide ratsionaalarvude $\frac{a}{b}$ ($\frac{a}{b} \neq \alpha$) korral kehtib võrratus

(1) $$\left|\alpha - \frac{a}{b}\right| \geqslant \frac{c}{b^n}.$$

Tõestus. Olgu $f(x) = A_0x^n + A_1x^{n-1} + \ldots + A_n$ täisarvuliste kordajatega n-astme polünoom, mille üheks juureks on n-astme algebraline arv α (polünoomi $f(x)$ võib saada minimaalpolünoomist ratsionaalsete kordajate ühise nimetajaga läbikorrutamise teel). Siis Bézout' teoreemi kohaselt

$$f(x) = (x - \alpha)g(x),$$

kus $g(x)$ on r e a a l s e t e kordajatega (n-1)-astme polünoom. Fikseerime suvalise positiivse reaalarvu δ ja vaatleme lõiku $[\alpha - \delta, \alpha + \delta]$. Kuna $|g(x)|$ on igal lõigul pidev ja seega ka tõkestatud, siis eksisteerib positiivne arv M, nii et $|g(x)| \leq M$, kui $x \in [\alpha - \delta, \alpha + \delta]$. Valime positiivse reaalarvu c nii, et $c \leqslant \frac{1}{M}$ ja $c \leqslant \delta$. Suvalise ratsionaalarvu $\frac{a}{b}$ jaoks on kaks järgmist võimalust.

1) Arv $\frac{a}{b}$ asub väljaspool lõiku $[\alpha - \delta, \alpha + \delta]$. Siis

$$\left|\alpha - \frac{a}{b}\right| > \delta \geqslant c \geqslant \frac{c}{b^n}.$$

2) Arv $\frac{a}{b}$ asub lõigus, s.t. $\alpha - \delta \leqslant \frac{a}{b} \leqslant \alpha + \delta$.

Siis $\left|g\left(\frac{a}{b}\right)\right| \leqslant M$ ja saame

$$\left|f\left(\frac{a}{b}\right)\right| = \left|\frac{a}{b} - \alpha\right| \cdot \left|g\left(\frac{a}{b}\right)\right| \leqslant M\left|\alpha - \frac{a}{b}\right| \leqslant \frac{1}{c}\left|\alpha - \frac{a}{b}\right|.$$

Kuna $f(x)$ on ratsionaalarvude korpuses taandumatu (teoreem 3.1), siis pole tal r a t s i o n a a l s e i d juuri, kui $n \geqslant 2$; kui $n = 1$, pole tal aga juuri, mis erineksid α-st. Seepärast

$$\left|f\left(\frac{a}{b}\right)\right| = \frac{\left|A_0a^n + A_1a^{n-1}b + \ldots + A_nb^n\right|}{b^n} \neq 0.$$

Kuna lugeja on positiivne täisarv, s.t.

$$\left|A_0a^n + A_1a^{n-1}b + \ldots + A_nb^n\right| \geqslant 1,$$

siis $\left|f\left(\frac{a}{b}\right)\right| \geqslant \frac{1}{b^n}$ ja saame

$$\left|\alpha - \frac{a}{b}\right| \geqslant c\left|f\left(\frac{a}{b}\right)\right| \geqslant \frac{c}{b^n}.$$

Teoreem on tõestatud.

Liouville'i teoreem näitab, et n-astme algebraliste arvude lähendamine ratsionaalarvudega $\frac{a}{b}$ on alt tõkestatud suurusega järku $\frac{1}{b^n}$, ruutirratsionaalide lähendamine seega suurusega järku $\frac{1}{b^2}$. Järgmine teoreem näitab, et peale ruutirratsionaalide leidub ka teisi irratsionaalarve, mille korral lähendamine ratsionaalarvudega on järku $\frac{1}{b^2}$.

Teoreem 3.5. Kui irratsionaalarvu α ahelmurru elemendid on tõkestatud, siis leidub positiivne reaalarv c, nii et iga ratsionaalarvu $\frac{a}{b}$ korral kehtib võrratus

$$\left|\alpha - \frac{a}{b}\right| > \frac{c}{b^2}. \tag{2}$$

Tõestus. Olgu $\alpha = a_1 + \frac{1}{a_2} + \frac{1}{a_3} + \ldots$ ja tähistagu $\frac{P_k}{Q_k}$ selle ahelmurru k-ndat lähismurdu. Eelduse kohaselt ek-

sisteerib tõke M, nii et iga $m = 1,2,\ldots$ puhul on $a_m \leqq M$. Võtame suvalise ratsionaalarvu $\frac{a}{b}$. Selle nimetaja rahuldab mingi $s \geqslant 2$ puhul tingimust $Q_{s-1} \leqq b < Q_s$. Et lähismurrud on arvule α parimad ratsionaalsed lähendid, siis

$$\left|\alpha - \frac{a}{b}\right| > \left|\alpha - \frac{P_s}{Q_s}\right| > \frac{1}{Q_s(Q_{s+1} + Q_s)} .$$

Hindame nimetajas esinevaid suurusi:

$$Q_s = Q_{s-1}a_s + Q_{s-2} \leqq bM + b = b(M + 1),$$

$$Q_{s+1} + Q_s = Q_s a_{s+1} + Q_{s-1} + Q_s = Q_s(a_{s+1} + 1) + Q_{s-1} \leqq$$

$$\leqq b(M + 1)(M + 1) + b = b(M^2 + 2M + 2).$$

Seega

$$\left|\alpha - \frac{a}{b}\right| > \frac{1}{b^2(M + 1)(M^2 + 2M + 2)} ,$$

s.t. kehtib võrratus (2), kus $c = \frac{1}{(M + 1)(M^2 + 2M + 2)}$.

Teoreem 3.6. Kui reaalarvu α ahelmurru elemendid ei ole tõkestatud, siis iga $c > 0$ korral eksisteerib lõpmata palju ratsionaalarve $\frac{a}{b}$, nii et

$$\left|\alpha - \frac{a}{b}\right| < \frac{c}{b^2} .$$

Tõestus. Võtame suvalise positiivse reaalarvu c. Eelduse kohaselt leidub ahelmurrul

$$\alpha = a_1 + \frac{1}{a_2} + \frac{1}{a_3} + \ldots$$

lõpmata palju elemente a_{s+1}, mis rahuldavad võrratust $a_{s+1} > \frac{1}{c}$. Siis aga iga sellise indeksi s korral

$$\left|\alpha - \frac{P_s}{Q_s}\right| \leq \frac{1}{Q_s Q_{s+1}} = \frac{1}{Q_s(Q_s a_{s+1} + Q_{s-1})} \leq$$

$$\leq \frac{1}{Q_s^2 a_{s+1}} < \frac{c}{Q_s^2},$$

s.t. ratsionaalarvudeks $\frac{a}{b}$ sobivad kõik selliste indeksitega lähismurrud $\frac{P_s}{Q_s}$, mille korral $a_{s+1} > \frac{1}{c}$.

Järeldus. Positiivse arvu c e k s i s t e e r i m i n e, nii et i g a ratsionaalarvu $\frac{a}{b}$ korral kehtiks võrratus (2), on tarvilik ja piisav selleks, et irratsionaalarvu α ahelmurru elemendid oleksid tõkestatud.

Tingimuse tarvilikkus on tõestatud teoreemis 3.5. Piisavus järeldub teoreemist 3.6. Tõepoolest, eksisteerigu $c > 0$, mis iga ratsionaalarvu $\frac{a}{b}$ korral rahuldab võrratust (2). Kui arvu α ahelmurru elemendid oleksid siiski tõkestamata, siis teoreemi 3.6 kohaselt kehtiks i g a $c > 0$ puhul lõpmata paljude ratsionaalarvude $\frac{a}{b}$ korral võrratusele (2) vastupidine võrratus. Eelduse tõttu pole see võimalik. Järelikult on arvu α ahelmurru elemendid tõkestatud.

Liouville'i teoreem (teoreem 3.4) annab vahe $\left|\alpha - \frac{a}{b}\right|$ jaoks hinnangu (1). Algebraliste arvude jaoks, mille aste $n > 2$, on teoreemi väidet korduvalt tugevdatud. Kehtib nimelt järgmine teoreem, mida seostatakse Thue, Siegeli ja Roth'i nimedega (esimene neist parandas teoreemi 1908.a., viimane 1955.a.) ja mille me esitame tõestuseta.

Teoreem 3.7. Kui α on reaalne n-astme algebraline arv ($n \geq 2$), siis iga $\varepsilon > 0$ korral eksisteerib ülimalt lõplik

hulk ratsionaalarve $\frac{a}{b}$, mis rahuldavad tingimust

(3) $$\left|\alpha - \frac{a}{b}\right| < \frac{1}{b^{2+\varepsilon}}.$$

Järeldus. I g a n-astme ($n \geqslant 2$) algebralise arvu ja s u v a l i s e $\varepsilon > 0$ jaoks eksisteerib $c > 0$, nii et iga ratsionaalarv $\frac{a}{b}$ rahuldab võrratust

$$\left|\alpha - \frac{a}{b}\right| \geqslant \frac{c}{b^{2+\varepsilon}}.$$

Algebraliste arvude jaoks, mille aste $n \geqslant 3$, on see tulemus märksa tugevam Liouville'i teoreemist. Teda loetakse algebraliste arvude teooria üheks sügavaimaks tulemuseks. Teoreemis 3.7 ei saa asendada võrratuse (3) paremat poolt suurusega $\frac{1}{b^2}$, sest leidub l õ p m a t a p a l j u arve $\frac{a}{b}$ (arvu α ahelmurru kõik lähismurrud), mille korral $\left|\alpha - \frac{a}{b}\right| < \frac{1}{b^2}$ (vt. II pt., § 4, valem (7)). Kuid pole välistatud võimalus, et peale teise astme algebraliste arvude ka mõne või isegi iga kõrgema astme algebralise arvu α korral eksisteerib $c > 0$, nii et i g a ratsionaalarvu $\frac{a}{b}$ korral kehtib võrratus

$$\left|\alpha - \frac{a}{b}\right| \geqslant \frac{c}{b^2}.$$

Kui nii, siis oleksid teoreemide 3.5 ja 3.6 järelduse põhjal arvu α ahelmurru elemendid tõkestatud. Praegu on see küsimus lahtine, sest ühegi algebralise arvu kohta, mille aste $n \geqslant 3$, pole teada, kas tema ahelmurru elemendid on tõkestatud või mitte.

§ 3. TRANSTSENDENTSED ARVUD

Mittealgebralisi arve nimetatakse transtsendentseteks. Pikka aega arvati, et kõik arvud on algebralised. Alles prantsuse matemaatik Liouville tõestas 1844.a., et eksisteerib transtsendentseid arve, s.t. irratsionaalarve, mis ei rahulda ühtki täisarvuliste kordajatega algebralist võrrandit. Praegu on aga teada, et algebraliste arvude hulk on vaid loenduv, samal ajal kui transtsendentsete arvude hulk on kontiinuumi võimsusega.

Teoreem 3.8. Algebraliste arvude hulk on loenduv.

Tõestus (Cantor, 1874). Kõikide n-astme algebraliste arvude hulk on määratud täisarvuliste kordajatega, ratsionaalarvude korpuses taandumatute n-astme polünoomide hulgaga. Igale täisarvuliste kordajatega polünoomile

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$$

vastab naturaalarv

$$N = |a_0| + |a_1| + \ldots + |a_n|.$$

On selge, et eksisteerib vaid lõplik hulk täisarvuliste kordajatega taandumatuid n-astme polünoome, millele vastab üks ja sama N. Igal sellisel polünoomil on n erinevat juurt.*) Seega iga antud N jaoks eksisteerib vaid lõplik hulk n-astme algebralisi arve. Andes N-le väärtused 1,2,3,... ja

*) Ratsionaalarvude korpuses taandumatul polünoomil ei saa olla kordseid juuri.

võttes kõik vastavate ratsionaalarvude korpuses taandumatute n-astme polünoomide juured, saame n-astme algebraliste arvude hulga M_n, mis on esitatud loenduva hulga lõplike hulkade summana. Seega on M_n loenduv. Kõikide algebraliste arvude hulk

$$M = \bigcup_{n=1}^{\infty} M_n$$

on loenduv kui loenduva hulga loenduvate hulkade summa.

Järeldus 1. Eksisteerivad transtsendentsed arvud. Nende hulk on kontiinuumi võimsusega.

Tõepoolest, kuna loenduv algebraliste arvude hulk on kontiinuumi võimsusega kompleksarvude hulga alamhulk, siis selle alamhulga täiend pole tühi ja on kontiinuumi võimsusega.

Järeldus 2. Eksisteerivad transtsendentsed reaalarvud. Nende hulk on kontiinuumi võimsusega. (Põhjendada!)

Teoreemist 3.2 järeldub, et kahe nullist erineva arvu summa, vahe, korrutis ja jagatis, kus üks arvudest on algebraline, teine aga transtsendentne, on transtsendentne arv. (Tõestada (vastuväiteliselt)!)

Järgnev teoreem, mis on otsene järeldus Liouville'i teoreemist (teoreem 3.4), võimaldab konstrueerida transtsendentseid arve.

Teoreem 3.9. Olgu antud reaalarv α. Kui i g a naturaalarvu n ja i g a reaalarvu $c > 0$ korral e k s i s t e e r i b kasvõi üksainus ratsionaalarv $\frac{a}{b} \neq \alpha$, mis rahuldab tingimust

(1) $$\left|\alpha - \frac{a}{b}\right| < \frac{c}{b^n},$$

siis α on transtsendentne.

Tõestus. Olgu arvu α jaoks teoreemi tingimused täidetud. Kui α oleks algebraline, siis leiduks teoreemi 3.4 kohaselt naturaalarv n ja reaalarv $c > 0$, nii et i g a ratsionaalarvu $\frac{a}{b}$ korral oleks

$$\left|\alpha - \frac{a}{b}\right| \geqslant \frac{c}{b^n},$$

mis on vastuolus eeldustega. Järelikult on α transtsendentne.

Arve α, mille jaoks iga naturaalarvu n ja iga positiivse reaalarvu c korral on võrratusel (1) olemas täisarvuline lahend a, b, nimetatakse Liouville'i transtsendentseteks arvudeks.

Näide 1. Tõestame, et arv

$$\alpha = \frac{1}{10^{1!}} + \frac{1}{10^{2!}} + \frac{1}{10^{3!}} + \ldots = 0{,}11000100\ldots$$

on transtsendentne.

Võtame suvalise naturaalarvu n ja suvalise reaalarvu $c > 0$ ning defineerime

$$a = 10^{k!}\left(\frac{1}{10^{1!}} + \frac{1}{10^{2!}} + \ldots + \frac{1}{10^{k!}}\right), \quad b = 10^{k!},$$

kus k on valitud nii suur, et $10^{k!} \geqslant \frac{2}{c}$ ja $k \geqslant n$. Siis

$$\left|\alpha - \frac{a}{b}\right| = \frac{1}{10^{(k+1)!}} + \frac{1}{10^{(k+2)!}} + \ldots <$$

$$< \frac{1}{10^{(k+1)!}}\left(1 + \frac{1}{2} + \frac{1}{2^2} + \ldots\right) =$$

$$= \frac{2}{10^{k!}} \cdot \frac{1}{10^{k!k}} \leq c \cdot \frac{1}{b^k} \leq \frac{c}{b^n} .$$

Teoreemi 3.9 kohaselt on vaadeldav arv transtsendentne.

Näide 2. Konstrueerime irratsionaalarvu α lõpmatu ahelmurruna, võttes ette mingid suvalised k elementi:

$$a_1, a_2, \ldots, a_k; \quad a_i \geq 1, \text{ kui } i \geq 2.$$

Arvutame $\frac{P_k}{Q_k}$ ja valime järgmise elemendi a_{k+1} nii, et $a_{k+1} \geq Q_k^k$. Nii valime järk-järgult ka kõik järgnevad elemendid:

$$a_{s+1} \geq Q_s^s, \text{ kui } s \geq k.$$

Näitame, et niiviisi lõpmatu ahelmurruna defineeritav reaalarv α rahuldab teoreemi 3.9 tingimusi ja on seega transtsendentne.

Fikseerime suvalise naturaalarvu n ja reaalarvu $c > 0$. Valime nii suure indeksi s, et $\frac{1}{Q_s^2} \leq c$, $s \geq k$ ja $s \geq n$. Nüüd

$$\left| \alpha - \frac{P_s}{Q_s} \right| < \frac{1}{Q_s Q_{s+1}} = \frac{1}{Q_s(Q_s a_{s+1} + Q_{s-1})} < \frac{1}{Q_s^2 a_{s+1}} \leq$$

$$\leq \frac{1}{Q_s^2 Q_s^s} = \frac{1/Q_s^2}{Q_s^s} \leq \frac{c}{Q_s^n} .$$

Seega eksisteerib iga naturaalarvu n ja iga reaalarvu $c > 0$ jaoks vähemalt üks ratsionaalarv $\frac{a}{b} = \frac{P_s}{Q_s}$, mis rahuldab võrratust (1). Järelikult on α transtsendentne. Niiviisi saame konstrueerida lõpmata palju transtsendentseid arve.

Kasutades Liouville'i teoreemi asemel teoreemi 3.7, võime teoreemi 3.9 märksa tugevdada. Saame nimelt järgmise tulemuse.

Teoreem 3.10. Olgu α reaalarv. Kui m i n g i $\varepsilon > 0$ korral i g a $c > 0$ jaoks eksisteerib ratsionaalarv $\frac{a}{b}$ $\left(\frac{a}{b} \neq \alpha\right)$, mis rahuldab tingimust

$$\left|\alpha - \frac{a}{b}\right| < \frac{c}{b^{2+\varepsilon}},$$

siis α on transtsendentne.

Tõestus. Kui α oleks n-astme algebraline arv, kus $n \geqslant 2$, siis leiduks teoreemi 3.7 järelduse põhjal iga $\varepsilon > 0$ jaoks reaalarv $c > 0$, nii et iga ratsionaalarv $\frac{a}{b}$ rahuldaks võrratust $\left|\alpha - \frac{a}{b}\right| \geqslant \frac{c}{b^{2+\varepsilon}}$. See on aga vastuolus eeldusega. Teoreemi 3.4 põhjal (võttes seal $n = 1$) järeldame (kuidas?), et α ei saa olla ka esimese astme algebraline arv.

Esitatud teoreemid ei võimalda kindlaks määrata kõikide meid huvitavate reaalarvude iseloomu. Arvud e ja π on näiteks transtsendentsed, kuid selle tõestus nõuab omaette meetodeid (vt. näit. [1], lk. 273-276).

Märgime tõestuseta veel ühe olulise teoreemi.

Teoreem 3.11 (Gelfond, 1934). Kui α on algebraline arv, mis ei ole 0 ega 1, ja β on vähemalt teise astme algebraline arv, siis α^{β} on transtsendentne.

Selle teoreemi tõestamist nõukogude matemaatiku A.O.Gelfondi (1906-1968) poolt peetakse üheks tähelepanuväärseimaks saavutuseks algebraliste ja transtsendentsete

arvude teoorias. Vastav hüpotees oli püstitatud Hilberti poolt rahvusvahelisel matemaatikute kongressil 1900. aastal ja see oli üks 23-st Hilberti probleemist, mis seati 20. sajandi matemaatikute ette.

Gelfondi teoreem võimaldab küllalt laia klassi arvude kohta öelda, et nad on transtsendentsed (näit. $3^{\sqrt{2}}$, $2^{i\sqrt{3}}$, $5^{2-i\sqrt{2}}$, $e^{\pi} = (-1)^{-i}$).

Järeldus. Algebralise arvu b logaritm algebralisel alusel c, kus $c > 0$ ja $c \neq 1$, on kas ratsionaalarv või transtsendentne arv, s.t. ei saa olla algebraline irratsionaalarv.

Tõepoolest, olgu $\alpha = \log_c b$ ehk, mis on sama, $c^{\alpha} = b$. Kui α oleks algebraline irratsionaalarv, siis b oleks transtsendentne.

Harjutusülesandeid.

3.1. Teha kindlaks järgmiste algebraliste arvude aste:

a) $\sqrt{2} - \sqrt{3}$, b) $\sqrt[3]{2} - 1$, c) $a + bi$,

kus a ja b on ratsionaalarvud.

3.2. Tõestada, et arvud

a) $\cos \frac{\pi}{n} + i \sin \frac{\pi}{n}$, b) $\sin 10^{\circ}$

on algebralised.

3.3. Tõestada, et arv

$$\alpha = \frac{1}{2^{1!}} + \frac{1}{2^{2!}} + \frac{1}{2^{3!}} + \dots$$

on transtsendentne.

3.4. Kasutades teoreemi 3.10 tõestada, et arv

$$\beta = \sum_{n=0}^{\infty} \frac{(-1)^n}{2^{3^n}}$$

on transtsendentne.

3.5. Kasutades teoreemi 3.10 konstrueerida ahelmurd, mille väärtus on transtsendentne.

IV. A R V U T E O R E E T I L I S E D F U N K T S I O O N I D

Elementaarses arvuteoorias käsitletakse peamiselt funktsioone, mille määramispiirkonnaks on naturaalarvude hulk, ja funktsioone, mille väärtused on täisarvud. Järgnevas vaatleme mõningaid selliseid arvuteoreetilisi funktsioone.

§ 1. ARVU JAGAJATE SUMMA JA JAGAJATE ARV

1. Multiplikatiivsed funktsioonid. Funktsiooni $\vartheta(a)$, mis on defineeritud kõikide naturaalarvude hulgal ja mille väärtus on nullist erinev vähemalt ühe naturaalarvu korral, nimetatakse multiplikatiivseks, kui

$$\vartheta(a_1 a_2) = \vartheta(a_1)\vartheta(a_2).$$

Kui viimane võrdus kehtib suvaliste naturaalarvude a_1 ja a_2 korral, siis nimetatakse funktsiooni tugevalt multiplikatiivseks; kui see võrdus kehtib kõigi ü h i s t e g u r i t a naturaalarvude korral, siis nõrgalt multiplikatiivseks.

Näiteks on tugevalt multiplikatiivne funktsioon $\vartheta(a) = a^s$ iga reaalarvu s korral.

1° Multiplikatiivne funktsioon rahuldab tingimust

$$\vartheta(1) = 1.$$

Tõepoolest, $\vartheta(a_0) = \vartheta(1a_0) = \vartheta(1)\cdot\vartheta(a_0)$. Kui a_0 on nüüd selline naturaalarv, mille korral $\vartheta(a_0) \neq 0$, siis järeldubki siit vajalik võrdus.

2° Multiplikatiivsete funktsioonide korrutis on multiplikatiivne.

Tõestus on triviaalne.

2. Summad üle arvu jagajate. Olgu $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ arvu a kanooniline kuju. Siis arvu a jagajad avalduvad kõik kujul $d = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$, kus $0 \le \beta_i \le \alpha_i$. Tähistame sümboliga $\sum_{d|a}$ summat üle kõikide naturaalarvude d, mis on a jagajad.

Teoreem 4.1. Kui $\vartheta(a)$ on nõrgalt multiplikatiivne funktsioon, siis kehtib valem

$$(1)\quad \sum_{d|a} \vartheta(d) = \left[1 + \vartheta(p_1) + \vartheta(p_1^2) + \dots + \vartheta(p_1^{\alpha_1})\right] \dots \left[1 + \vartheta(p_k) + \dots + \vartheta(p_k^{\alpha_k})\right],$$

kusjuures juhul, kui $a = 1$, tuleb võrduse parem pool lugeda võrdseks ühega.

Tõestus. Avame sulud võrduse (1) paremal poolel. Siis saame summa, mille üldliikmeks on (kasutame nõrka multiplikatiivsust)

$$(2)\quad \vartheta(p_1^{\beta_1})\vartheta(p_2^{\beta_2}) \dots \vartheta(p_k^{\beta_k}) = \vartheta(p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}),$$

kus $0 \le \beta_i \le \alpha_i$. Siinjuures saame parajasti kõik vasakul esinevad liidetavad. Sellega ongi teoreem tõestatud.

Võtame $\vartheta(a) = a^s$. Siis valem (1) omandab kuju

$$(3)\quad \sum_{d|a} d^s = (1 + p_1^s + p_1^{2s} + \dots + p_1^{\alpha_1 s}) \dots (1 + p_k^s + \dots + p_k^{\alpha_k s}) = \frac{p_1^{\alpha_1 s+s} - 1}{p_1^s - 1} \cdot \frac{p_2^{\alpha_2 s+s} - 1}{p_2^s - 1} \dots \frac{p_k^{\alpha_k s+s} - 1}{p_k^s - 1}.$$

Viimane valem annab arvu a jagajate s-ndate astmete summa. Erijuhul, kui s = 1, saame a jagajate summa, mida tähistatakse S(a),

$$S(a) = \sum_{d|a} d = (1 + p_1 + \ldots + p_1^{\alpha_1})\ldots(1 + p_k + \ldots + p_k^{\alpha_k}) =$$
$$= \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdots \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}.$$

Näiteks arvu $720 = 2^4 \cdot 3^2 \cdot 5$ kõigi jagajate summa on

$$S(720) = \frac{2^5 - 1}{2 - 1} \cdot \frac{3^3 - 1}{3 - 1} \cdot \frac{5^2 - 1}{5 - 1} = 2418.$$

Eriti on $S(p) = p + 1$, kui p on algarv.

Kui $s = 0$, saame valemist (3) arvu a jagajate arvu $\tau(a)$,

$$\tau(a) = \sum_{d|a} 1 = (\alpha_1 + 1)(\alpha_2 + 1)\ldots(\alpha_k + 1).$$

Näiteks on $\tau(720) = (4 + 1)(2 + 1)(1 + 1) = 30$.

Teoreem 4.2. Funktsioonid $S(a)$ ja $\tau(a)$ on nõrgalt multiplikatiivsed.

Tõestus. Olgu $a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}$ ja $b = q_1^{\beta_1} q_2^{\beta_2} \ldots q_m^{\beta_m}$, kus $(a,b) = 1$. Siis kõik tegurid p_i, q_j on üksteisest erinevad ja seega

$$S(a)S(b) = \frac{p_1^{\alpha_1+1} - 1}{q_m - 1} \cdots \frac{p_n^{\alpha_n+1} - 1}{p_n - 1} \cdot \frac{q_1^{\beta_1+1} - 1}{q_1 - 1} \cdots$$
$$\cdots \frac{q_m^{\beta_m+1} - 1}{q_m - 1} = S(ab),$$

$$\tau(a) \cdot \tau(b) = (\alpha_1+1)\ldots(\alpha_n+1)(\beta_1+1)\ldots(\beta_m+1) = \tau(ab).$$

Kui nüüd $(a,b) > 1$, siis a ja b kanoonilises kujus leidub vähemalt üks ühine tegur. Olgu näiteks $p_i = q_j$. Siis aga $S(a)S(b) \neq S(ab)$, $\tau(a)\tau(b) \neq \tau(ab)$, sest ei kehti samasused

$$\frac{p_i^{\alpha_i+1} - 1}{p_i - 1} \cdot \frac{p_i^{\beta_j+1} - 1}{p_i - 1} = \frac{p_i^{\alpha_i+\beta_j+1} - 1}{p_i - 1},$$

$$(\alpha_i + 1)(\beta_j + 1) = \alpha_i + \beta_j + 1.$$

3*. Täiuslikud arvud. Nimetame arvu pärisjagajateks kõiki jagajaid, mis on temast väiksemad. Arvu, mis võrdub oma pärisjagajate summaga, nimetatakse täiuslikuks arvuks. Sellisteks arvudeks on näiteks

$$6 = 1 + 2 + 3,$$

$$28 = 1 + 2 + 4 + 7 + 14.$$

Juba Eukleides leidis valemi, mis annab kõik täiuslikud paarisarvud. Ta näitas, et tema poolt leitud valem annab ainult täiuslikke arve, kuid ei tõestanud, et sellega on antud kõik täiuslikud paarisarvud. Viimase asjaolu tõestas L.Euler alles 2000 a. hiljem.

Teoreem 4.3. Paarisarv a on täiuslik parajasti siis, kui ta avaldub kujul

$$a = 2^{k-1}M_k \quad (k > 1), \tag{4}$$

kus Mersenne'i arv $M_k = 2^k - 1$ on algarv.

Tõestus. Kõigepealt paneme tähele, et a on täiuslik parajasti siis, kui $S(a) = 2a$. Arvutamegi $S(a)$:

$$S(a) = S(2^{k-1}(2^k - 1)) = S(2^{k-1})S(2^k - 1) =$$

$$= (2^k - 1)2^k = 2a.$$

Seega Eukleidese valem annab täiusliku arvu.

Tõestame ka vastupidi, et iga täiuslik paarisarv on antud valemiga (4). Olgu a täiuslik paarisarv, s.t. $a = 2^{k-1}b$, $(b,2) = 1$ ja $S(a) = 2a$. Teisiti,

$$S(2^{k-1}b) = 2^k b$$

ehk

$$S(2^{k-1})S(b) = 2^k b = (2^k b - b) + b,$$

millest

$$S(b) = b + \frac{b}{2^k - 1}.$$

Tähistame $\frac{b}{2^k - 1} = c$, siis $S(b) = b + c$. On selge, et c on täisarv, sest $S(b)$ ja b on täisarvud. Et $b = c(2^k - 1)$, siis c on b jagaja. Võrduses

$$S(b) = b + c$$

on vasakul arvu b kõikide jagajate summa, paremal aga kahe jagaja summa $b + c$. Võrdus kehtib parajasti siis, kui naturaalarvul b on täpselt 2 jagajat. Seega on b algarv ja $c = 1$. Siis aga $b = 2^k - 1 = M_k$ eeldusel, et $2^k - 1$ on algarv. Teoreem on tõestatud.

Nagu eespool mainitud (vt. I pt. § 4), oli 1971. aastaks teada 24 Mersenne'i algarvu. Seega on ühtlasi teada 24 täiuslikku arvu, millest esimesed on 6, 28, 496, 8128, suurim teadaolev aga $2^{19936}(2^{19937} - 1)$. On muidugi lahtine küsimus, kas täiuslikke arve on lõplik või lõpmatu hulk,

sest pole teada, kas Mersenne'i algarve on lõplik hulk või lõpmata palju. Mis puutub paaritutesse täiuslikesse arvudesse, siis võib üsna suure tõenäosusega öelda, et neid pole olemas. On tõestatud, et kui paarituid täiuslikke arve eksisteerib, siis on nad väga suured, igal juhul suuremad kui e^{52729}. Sealjuures on nad siis kujuga $p^{4k+1}M^2$, kus $p = 4m + 1$ on algarv, $(M, p) = 1$, ja nende erinevate algtegurite arv ei ole väiksem kui 2800 (vt. [2], lk. 233).

Arvu a nimetatakse <u>alatäiuslikuks</u>, kui $S(a) < 2a$, ja <u>ületäiuslikuks</u>, kui $S(a) > 2a$.

Täiuslikest arvudest võib lugeda ka J.Gabovitši artiklist "Täiuslikud arvud" ("Matemaatika ja kaasaeg" VIII, lk. 58-64).

<u>Harjutusülesandeid</u>.

4.1. Kui palju erinevaid jagajaid on arvul 2475 ja milline on nende summa?

4.2. Leida arvu 360 kõigi jagajate ruutude summa ja arvu 360^2 kõigi jagajate summa.

4.3. Arvul N^2 on 15 erinevat jagajat. Kui palju erinevaid jagajaid on arvul N^3 ? Leida vähim nimetatud omadusega arv.

4.4. Leida arv, mille kõigi jagajate korrutis on 5832.

4.5. Leida arv, mille kõigi jagajate korrutis on $3^{30}.5^{40}$.

466. Tõestada, et algarvude astmed on alatäiuslikud arvud.

4.7. Tõestada, et kahe algarvulise jagajaga paaritu arv on alatäiuslik.

4.8. Leida vähim naturaalarv kujul $2^{\alpha} p_1 p_2$ (p_1 ja p_2 on paaritud algarvud), mille jagajate summa on kaks korda suurem arvust endast (Fermat' ülesanne).

4.9. Leida arv kujul $m = 2^x \cdot 3^y \cdot 5^z$, teades, et poolel sellest arvust on 30 jagajat vähem kui arvul endal, ühel kolmandikul arvust m on aga 35 jagajat vähem ja ühel viiendikul 42 jagajat vähem kui arvul endal.

§ 2. ARVU TÄISOSA

Arvu täisosa on funktsioon, mis on määratud reaalarvude hulgal ja mille väärtused on täisarvud.

Kui m on täisarv ja kehtivad võrratused

$$m \leqslant x < m + 1,$$

siis ütleme, et reaalarvu x täisosa on m, ja kirjutame $[x] = m$. Seega on

$$[x] \leqslant x < [x] + 1.$$

Siit järelduvad järgmised omadused (tõestada!).

1° Kui a on täisarv, siis

$$[x + a] = [x] + a.$$

2° Kui a on täisarv ja kehtib võrratus $a \leqslant x$, siis kehtib ka võrratus $a \leqslant [x]$.

Teoreem 4.4. Reaalarvu x mitte ületavate ja naturaalarvuga k jaguvate naturaalarvude arv on $\left[\frac{x}{k}\right]$.

Tõestus. Kirjutame välja kõik arvu x mitteületavad naturaalarvud, mis on arvu k kordsed: 1k, 2k, ..., hk.

Et $hk \leqslant x < (h+1)k$, siis $h \leqslant \frac{x}{k} < h+1$ ja seega $h = \left[\frac{x}{k}\right]$.

Teoreem 4.5. Olgu x suvaline positiivne reaalarv ja a mistahes naturaalarv, siis

$$\left[\frac{x}{a}\right] = \left[\frac{[x]}{a}\right].$$

Tõestus. Tähistame $b = \left[\frac{x}{a}\right]$. Siis

$$b \leqslant \frac{x}{a} < b+1,$$

$$ab \leqslant x < a(b+1).$$

Omaduse 2° põhjal

$$ab \leqslant [x] \leqslant x < a(b+1),$$

millest

$$b \leqslant \frac{[x]}{a} < b+1.$$

Seega $b = \left[\frac{[x]}{a}\right] = \left[\frac{x}{a}\right]$.

Teoreem 4.6. Algarv p kuulub tegurina korrutisse $n!$ parajasti

$$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \ldots$$

korda.

Tõestuseks leiame korrutisest $1\cdot2\cdot3\ldots n$ kõik tegurid, mis on arvu p kordsed. Sellised on

$$1p,\ 2p,\ 3p,\ldots,\ hp = \left[\frac{n}{p}\right]p\ .$$

Seega esineb p korrutises $n!$ üldse $\left[\frac{n}{p}\right]$ teguris. Võttes igast sellisest tegurist välja p, saame p astmes $\left[\frac{n}{p}\right]$. Algarvu p kordsetest jäävad siis järele tegurid

$$1,\ 2,\ 3,\ldots,\ \left[\frac{n}{p}\right].$$

Ka mõnedes nendest arvudest võib p veel tegurina esineda. Arvu p kordsed on

$$(1) \qquad 1p,\ 2p,\ \ldots,\ \left\lfloor \frac{\left\lfloor \frac{n}{p} \right\rfloor}{p} \right\rfloor p .$$

Eraldades igast kordsest teguri p, saame siit p veel astmes

$$\left\lfloor \frac{\left\lfloor \frac{n}{p} \right\rfloor}{p} \right\rfloor = \left\lfloor \frac{\frac{n}{p}}{p} \right\rfloor = \left\lfloor \frac{n}{p^2} \right\rfloor .$$

Teguri p eraldamisel jäävad jada (1) elementidest järele tegurid

$$1,\ 2,\ \ldots,\ \left\lfloor \frac{n}{p^2} \right\rfloor .$$

Siit eraldame jälle välja p kordsed; saame lisaks p astmes $\left\lfloor \frac{n}{p^3} \right\rfloor$, jne. Seega esineb korrutises $n!$ algarv p astmes

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \ldots$$

Kui $p^k > n$, siis liidetavad tulevad nullid. Seega $n! = a \cdot p^{\alpha}$, kus

$$\alpha = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor \quad \text{ja} \quad (a,p) = 1,$$

ja

$$(2) \qquad n! = \prod_{p \le n} p^{\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \ldots} .$$

X peatükis kasutame funktsiooni

$$T(x) = \sum_{n \le x} \ln n = \ln \lfloor x \rfloor !$$

Valemi (2) ja teoreemi 4.5 tõttu võib selle funktsiooni esitada kujul

(3) $$T(x) = \sum_p (\ln p)\left(\left[\frac{x}{p}\right] + \left[\frac{x}{p^2}\right] + \dots\right).$$

Näide 1. Mitmendas astmes esineb 7 arvu 6522 faktoriaalis?

Kasutame seost $\left[\frac{a}{p^k}\right] = \left[\frac{\left[\frac{a}{p^{k-1}}\right]}{p}\right]$ ja rakendame teoreemi 4.6:

$$\left[\frac{6522}{7}\right] = 931, \quad \left[\frac{6522}{7^2}\right] = \left[\frac{931}{7}\right] = 133,$$

$$\left[\frac{6522}{7^3}\right] = \left[\frac{133}{7}\right] = 19, \quad \left[\frac{6522}{7^4}\right] = \left[\frac{19}{7}\right] = 2.$$

Seega arv 7 esineb astmes 931 + 133 + 19 + 2 = 1085.

Näide 2. Leida 21! kanooniline kuju.

Arvus 21! esinevad algtegurid 2,3,5,7,11,13,17,19.

$$\alpha_1 = \left[\frac{21}{2}\right] + \left[\frac{21}{4}\right] + \left[\frac{21}{8}\right] + \left[\frac{21}{16}\right] = 10 + 5 + 2 + 1 = 18,$$

$$\alpha_2 = \left[\frac{21}{3}\right] + \left[\frac{21}{9}\right] = 7 + 2 = 9, \quad \alpha_3 = \left[\frac{21}{5}\right] = 4,$$

$$\alpha_4 = \left[\frac{21}{7}\right] = 3, \quad \alpha_5 = \left[\frac{21}{11}\right] = 1, \quad \alpha_6 = \alpha_7 = \alpha_8 = 1.$$

Seega $21! = 2^{18} \cdot 3^9 \cdot 5^4 \cdot 7^3 \cdot 11 \cdot 13 \cdot 17 \cdot 19$.

Algarv p, kus $n \geq p > \frac{n}{2}$, kuulub n! kanoonilisse kujusse esimeses astmes.

Harjutusülesandeid.

4.10. Mitmendas astmes esineb 3 arvu 333 faktoriaalis?

4.11. Leida arvu 120! kanooniline kuju.

4.12. Mitme nulliga lõpeb 1974! ?

4.13. Tõestada, et $\left[\sum_{i=1}^{n} a_i\right] \geq \sum_{i=1}^{n} [a_i]$.

4.14. Leida suurim naturaalarv n, mille korral

$$N = \frac{101 \cdot 102 \ldots 1000}{7^n}$$

on täisarv.

4.15. Kui palju on 10^5 ja 10^6 vahel naturaalarve, mis on arvu 222 kordsed?

4.16. Kui palju on naturaalarve, mis on väiksemad kui 1000 ja ei jagu ei 5 ega 7-ga ?

4.17. Kui palju on naturaalarve, mis ei ületa 400 ja on 36-ga ühistegurita?

§ 3. EULERI φ-FUNKTSIOON

Euleri φ-funktsioon $\varphi(a)$ on defineeritud kõikide naturaalarvude hulgal järgmiselt:

$\varphi(a)$ on naturaalarvu a mitteületavate ja arvuga a ühistegurita naturaalarvude arv.

Sama definitsiooni võib anda ka valemiga

$$\varphi(a) = \sum_{\substack{b \le a \\ (b,a)=1}} 1$$

või valemiga

$$\varphi(a) = |\{b \mid b \le a,\ (a,b) = 1\}|,$$

kus üldiselt $|H|$ tähendab lõpliku hulga H elementide arvu.

Teoreem 4.7. Kehtib valem

$$|\{b \mid b \le a,\ (a,b) = d\}| = \varphi\left(\frac{a}{d}\right).$$

Tõestus. Vaatleme naturaalarve b, mis ei ületa arvu

a ja rahuldavad tingimust $(a,b) = d$. Kõiki neid saab esitada kujul $b = db_1$, kusjuures $a = da_1$ ja $(a_1,b_1) = 1$. Siin a ja a_1 on fikseeritud, b ja b_1 aga muutuvad arvud, kusjuures $b_1 \leq a_1$. Igale b-le, mis rahuldab tingimusi $b \leq a$, $(a,b) = d$, vastab parajasti üks b_1, mis rahuldab tingimusi $b_1 \leq a_1$, $(a_1,b_1) = 1$. Seega

$$\left|\{b \mid b \leq a,\ (a,b) = d\}\right| = \left|\{b_1 \mid b_1 \leq a_1,\ (a_1,b_1) = 1\}\right| = \varphi(a_1) = \varphi\left(\frac{a}{d}\right).$$

Näide 1. Olgu $a = 60$ ja $d = 5$. Siis

$$\left|\{b \mid b \leq 60,\ (b,60) = 5\}\right| = \varphi\left(\frac{60}{5}\right) = \varphi(12) = 4.$$

Teoreem 4.8. Kehtib valem

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

Tõestus. Kirjutame kasvavas järjekorras välja arvu a kõik jagajad:

(1) $\quad d_1, d_2, d_3, \ldots, d_{\tau(a)} \quad (d_1=1,\ d_{\tau(a)}=a).$

Eelmise teoreemi põhjal

$$\begin{aligned}
&\left|\{b \mid b \leq a,\ (b,a) = d_1\}\right| = \varphi\left(\tfrac{a}{d_1}\right),\\
&\left|\{b \mid b \leq a,\ (b,a) = d_2\}\right| = \varphi\left(\tfrac{a}{d_2}\right),\\
&\qquad\qquad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&\left|\{b \mid b \leq a,\ (b,a) = d_{\tau(a)}\}\right| = \varphi\left(\frac{a}{d_{\tau(a)}}\right).
\end{aligned} \tag{2}$$

Liidame kõik võrdused (2). Selleks et kindlaks teha, millega võrdub vasakul pool saadav summa, jaotame kõik naturaalarvud b, mis ei ületa arvu a, s.t. arvud

(3) $\qquad 1, 2, 3, \ldots, a,$

klassidesse, võttes ühte klassi kokku kõik need arvud, millel on arvuga a üks ja sama suurim ühistegur d_i ($i = 1,2,\dots,\tau(a)$). Selliste klasside arv on ilmselt $\tau(a)$ ja arvude arv kõikides klassides kokku a , sest klassidesse jaotamisel ei jää arvudest (3) ühtki üle, samuti ei kuulu üks ja sama arv kahte erinevasse klassi. Seega võrduste (2) vasakute poolte summa võrdub a-ga ja saame

$$a = \varphi\left(\frac{a}{d_1}\right) + \varphi\left(\frac{a}{d_2}\right) + \dots + \varphi\left(\frac{a}{d_{\tau(a)}}\right).$$

Tähistame $\frac{a}{d_i} = c_i$. Siis $a = c_i d_i$, millest nähtub, et c_i on a jagaja. Sealjuures vastab igale jagajale d_i parajasti üks jagaja c_i. Niisiis erinevaid jagajaid c_i on täpselt niisama palju kui jagajaid d_i, s.o. arvult $\tau(a)$. Et aga jagajatega d_i on ammendatud kõik a jagajad, siis on ka jadas

$$c_1, c_2, \dots, c_{\tau(a)}$$

parajasti kõik a jagajad. Sealjuures on nad nüüd kahanevas järjekorras. Seega $\frac{a}{d_i} = c_i = d_{\tau(a)+1-i}$. Siit järeldubki vajalik võrdus:

$$a = \varphi(d_{\tau(a)}) + \dots + \varphi(d_2) + \varphi(d_1).$$

Teoreem 4.9. Euleri φ-funktsioon on nõrgalt multiplikatiivne.

Tõestuseks kasutame täieliku induktsiooni meetodit. Kui $a = b = 1$, siis kehtib võrdus

$$\varphi(1)\cdot\varphi(1) = \varphi(1); \quad (1,1) = 1.$$

Oletame nüüd, et iga naturaalarvude paari α, β korral, mis

rahuldab tingimusi

$$(\alpha, \beta) = 1 \quad \text{ja} \quad \alpha\beta < ab,$$

kehtib võrdus $\varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta)$. Tarvitseb näidata, et $(a,b) = 1$ korral

$$\varphi(ab) = \varphi(a)\varphi(b).$$

Jaotame a ja b jagajad kahte rühma: a ja kõik pärisjagajad α; b ja kõik pärisjagajad β.

Teoreemi 4.8 kohaselt

$$a = \varphi(a) + \sum_{\alpha} \varphi(\alpha),$$

$$b = \varphi(b) + \sum_{\beta} \varphi(\beta).$$

Korrutame võrduste vastavad pooled. Saame

$$ab = \varphi(a)\varphi(b) + \sum_{\beta} \varphi(a)\varphi(\beta) + \sum_{\alpha} \varphi(b)\varphi(\alpha) + \sum_{\alpha,\beta} \varphi(\alpha)\varphi(\beta).$$

Eelduse kohaselt $(a,b) = 1$, seega ka $(a, \beta) = (\alpha, b) = 1$. Et $a\beta < ab$, $\alpha b < ab$, $\alpha\beta < ab$, siis võime saadud seose esitada kujul

$$(4) \quad ab = \varphi(a)\varphi(b) + \sum_{\beta} \varphi(a\beta) + \sum_{\alpha} \varphi(\alpha b) + \sum_{\alpha,\beta} \varphi(\alpha\beta).$$

Lähtudes seosest

$$ab = \sum_{d \mid ab} \varphi(d)$$

jaotame ab jagajad nelja rühma: 1) ab, 2) kõik jagajad kujuga αb, 3) kõik jagajad kujuga $a\beta$, 4) kõik jagajad kujuga $\alpha\beta$, kus α ja β on endise tähendusega. Siis

$$(5) \quad ab = \varphi(ab) + \sum_{\beta} \varphi(a\beta) + \sum_{\alpha} \varphi(\alpha b) + \sum_{\alpha,\beta} \varphi(\alpha\beta).$$

Lahutades võrdusest (4) võrduse (5) leiame, et $0 = \varphi(a)\varphi(b) - \varphi(ab)$ ehk

$$\varphi(ab) = \varphi(a)\varphi(b).$$

Teoreem on tõestatud.

Selles, et φ-funktsioon ei ole tugevalt multiplikatiivne, võib veenduda näite varal. Olgu $a = 6$, $b = 2$. Siis

$$\varphi(a) = \varphi(6) = 2, \quad \varphi(b) = \varphi(2) = 1,$$

kuid

$$\varphi(ab) = \varphi(12) = 4 \neq \varphi(a)\cdot\varphi(b).$$

Tuletame valemi Euleri φ-funktsiooni väärtuste arvutamiseks. Kõigepealt teame, et kui p on algarv, siis

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

Täieliku induktsiooni meetodil tõestame, et $\varphi(p^k) = p^k - p^{k-1}$. Oletame, et iga $j < k$ puhul

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

Siis

$$p^k = \sum_{d \mid p^k} \varphi(d) = \varphi(p^k) + \varphi(p^{k-1}) + \ldots + \varphi(p) + \varphi(1) = \varphi(p^k) + (p^{k-1} - p^{k-2}) + (p^{k-2} - p^{k-3}) + \ldots + (p - 1) + 1 = \varphi(p^k) + p^{k-1},$$

millest

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

Kasutades φ-funktsiooni multiplikatiivsust, rakendame teda arvu a kanoonilisele kujule

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

Siis saame

$$\varphi(a) = p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right)p_2^{\alpha_2}\left(1 - \frac{1}{p_2}\right)\dots p_n^{\alpha_n}\left(1 - \frac{1}{p_n}\right) = a\prod_{k=1}^{n}\left(1 - \frac{1}{p_k}\right).$$

Näide 2. $\varphi(360) = \varphi(2^3 \cdot 3^2 \cdot 5) =$

$$= 360\left(1 - \tfrac{1}{2}\right)\left(1 - \tfrac{1}{3}\right)\left(1 - \tfrac{1}{5}\right) = 96.$$

Harjutusülesandeid.

4.18. Kui palju on arvust 1000 väiksemaid naturaalarve, mis on temaga ühistegurita?

4.19. Kui palju leidub naturaalarve, mis on väiksemad kui 10 000 ja mille suurim ühistegur 10 000-ga on 8?

4.20. Kui palju leidub naturaalarve, mis on väiksemad kui 10 000 ja mille suurim ühistegur 10 000-ga ei ületa 10?

4.21. Kui palju on 1000-st väiksemaid naturaalarve a, mille vähim ühiskordne 1000-ga on 100 a? Kirjutada välja viis esimest ja kaks viimast sellist arvu.

4.22. Arvutada a) $\varphi(1000)$, b) $\varphi(1001)$, c) $\varphi(460)$.

4.23. Kui palju eksisteerib taandumatuid lihtmurde, mille nimetaja on m?

4.24. Tõestada, et kas $\varphi(2m) = \varphi(m)$ või $\varphi(2m) = 2\varphi(m)$. Leida kriteerium kummagi juhu jaoks.

4.25. Tõestada, et

a) $\varphi(4n+2) = \varphi(2n+1)$;

b) $\varphi(4n) = \begin{cases} 2\varphi(n), & \text{kui } (n,2) = 1 \\ 2\varphi(2n), & \text{kui } (n,2) = 2. \end{cases}$

4.26. Tõestada, et juhul, kui $m \geqslant 3$, on $\varphi(m)$ paarisarv.

§ 4. MÖBIUSE FUNKTSIOON $\mu(a)$

Möbiuse funktsioon defineeritakse kõikide naturaalarvude hulgal järgmiste valemitega

1) $\mu(1) = 1$,

2) $\mu(ab^2) = 0$,

3) $\mu(p_1p_2 \dots p_n) = (-1)^n$, kui $p_1, p_2, \dots, p_n$ on üksteisest erinevad algarvud.

Näiteks:

a	1	2	3	4	5	6	7	8	9	10	11	12	13
$\mu(a)$	1	-1	-1	0	-1	1	-1	0	0	1	-1	0	-1

Niisiis võib Möbiuse funktsioon omandada vaid väärtusi -1, 0, 1.

Teoreem 4.10. Funktsioon $\mu(a)$ on nõrgalt multiplikatiivne, kuid ei ole tugevalt multiplikatiivne.

Tõestus. Olgu $(a,b) = 1$. Vaatleme erinevaid võimalusi.

1) Kui a või b sisaldab ruuttegurit, siis $\mu(ab) = 0 = \mu(a)\mu(b)$.

2) Kui $a = p_1p_2 \dots p_n$, $b = q_1q_2 \dots q_k$, kus teguriteks lahutustes on kõik tegurid erinevad, siis

$$\mu(a) = (-1)^n, \quad \mu(b) = (-1)^k.$$

Et $(a,b) = 1$, siis ükski p_i ei võrdu ühegi q_j-ga. Seega

$$\mu(ab) = (-1)^{n+k} = (-1)^n \cdot (-1)^k = \mu(a)\mu(b).$$

Seega nõrk multiplikatiivsus on tõestatud. Selle tõestami-

seks, et $\mu(a)$ ei ole tugevalt multiplikatiivne, võtame $a = p_1 \dots p_n$, $b = q_1 \dots q_k$, kus $(a,b) \neq 1$. Siis a ja b teguriteks lahutuses leidub vähemalt üks ühine tegur, näiteks $p_i = q_j$. Siis aga

$$\mu(a)\mu(b) = (-1)^{n+k}, \text{ kuid } \mu(ab) = 0.$$

Teoreem 4.11. Kui $\vartheta(a)$ on nõrgalt multiplikatiivne funktsioon ja

$$(1) \qquad a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n},$$

siis

$$(2) \quad \sum_{d|a} \mu(d)\vartheta(d) = (1 - \vartheta(p_1)) \dots (1 - \vartheta(p_n)),$$

kusjuures juhul kui $a = 1$, tuleb võrduse parem pool lugeda võrdseks ühega.

Tõestuseks tarvitseb arvestada, et funktsioon $\mu(a)\vartheta(a)$ on nõrgalt multiplikatiivne, ja kasutada §-s 1 tõestatud võrdust (1).

Teoreemi 4.11 järeldusena saame järgmise tulemuse.

Teoreem 4.12. Kehtib valem

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

Tõestuseks tarvitseb võrduses (2) võtta $\vartheta(a) \equiv 1$.

Harjutusülesandeid.

4.27. Arvutada $\mu(182)$, $\mu(183)$, $\mu(184)$.

4.28. Kontrollida otseselt (vasakul seisva summa arvutamise teel) teoreemi 4.12 kehtivust $a = 40$ korral.

V. KONGRUENTSID

§ 1. KONGRUENTSIDE OMADUSED

1. Kongruentsi definitsioon. Olgu antud fikseeritud naturaalarv m ja mistahes täisarvud a ja b. Siis teoreemi 1.4 kohaselt

$$(1)\qquad \begin{aligned} a &= q_1 m + r_1, \quad 0 \leqq r_1 < m, \\ b &= q_2 m + r_2, \quad 0 \leqq r_2 < m, \end{aligned}$$

kusjuures q_1, q_2, r_1 ja r_2 on üheselt määratud. Järgnevas uurime täisarve nende jääkide järgi, tuues selleks sisse kongruentsi mõiste.

Definitsioon 1. Arve a ja b nimetatakse kongruentseteks modulo* m ja märgitakse

$$(2)\qquad a \equiv b \pmod{m},$$

kui a ja b annavad jagamisel arvuga m ühe ja sama jäägi.

Kirjutist (2) nimetatakse kongruentsiks, arvu m - mooduliks. Asjaolu, et a ei ole kongruentne b-ga mooduli m järgi, märgime nii:

$$a \not\equiv b \pmod{m}.$$

Arve a ja b nimetatakse sel juhul inkongruentse-

---

* Modulo (lad. k.) - mooduli järgi. Mõnikord kasutame väljendi "modulo m" asemel ka eestikeelset "mooduli m järgi".

teks modulo m.

Kui $a \equiv b \pmod m$, siis $a = q_1 m + r$, $b = q_2 m + r$ $(0 \leq r < m)$, millest $a - b = (q_1 - q_2)m$, s.t. $(a - b) \vdots m$. Vastupidi, kui $(a - b) \vdots m$, s.t. $a - b = qm$, siis võrdustest (1) järeldub, et $r_1 = r_2$. Seega kehtib kongruents $a \equiv b \pmod m$ parajasti siis, kui $(a - b) \vdots m$. Eriti on aga $a \equiv 0 \pmod m$ parajasti siis, kui $a \vdots m$. Viimase asjaolu tõttu defineeritakse arvude kongruentsi sageli ka järgmiselt.

Definitsioon 2. Arve a ja b nimetatakse kongruentseteks modulo m, kui vahe a - b jagub arvuga m.

Et $(a - b) \vdots m$ parajasti siis, kui leidub täisarv t, nii et $a = b + mt$, siis võib kasutada ka järgmist definitsiooni.

Definitsioon 3. Arve a ja b nimetatakse kongruentseteks modulo m, kui leidub täisarv t, nii et

$$a = b + mt. \tag{3}$$

Arvude kongruentsuse definitsioonist järeldub rida lihtsal: kontrollitavaid kongruentsi omadusi, millest osa on analoogilised võrduse omadustega. Allpool on esitatud need omadused teoreemidena, kusjuures teoreemide tõestamine on mitmel juhul jäetud lugejale.

2. Omadused, mis ei ole seotud mooduli muutumisega.

Teoreem 5.1. Kongruents on refleksiivne, s.t.

$$a \equiv a \pmod m,$$

sümmeetriline, s.t.

kui $a \equiv b \pmod m$, siis $b \equiv a \pmod m$,

ja transitiivne, s.t.

kui $a \equiv b \pmod m$ ja $b \equiv c \pmod m$, siis $a \equiv c \pmod m$.

Teoreem 5.2. Kui $a_1 \equiv b_1 \pmod m$, $a_2 \equiv b_2 \pmod m$, ..., $a_k \equiv b_k \pmod m$, siis

$$a_1 + a_2 + \dots + a_k \equiv b_1 + b_2 + \dots + b_k \pmod m,$$

s.t. kongruentse ühe ja sama mooduli järgi võib liikmeti liita.

Teoreem 5.3. Kongruentsi iga liiget võib üle kanda kongruentsi teisele poolele, muutes liikme märgi vastupidiseks; näiteks

kui $a + b \equiv c \pmod m$, siis $a \equiv c - b \pmod m$.

Teoreem 5.4. Kui $a \equiv b \pmod m$, siis mistahes täisarvude k ja n korral

$$a \pm km \equiv b \pm nm \pmod m,$$

s.t. kongruents jääb kehtima, kui kongruentsi ühele või mõlemale poolele liita (või nendest lahutada) mooduli kordne.

Teoreem 5.5. Kui $a_1 \equiv b_1 \pmod m$, $a_2 \equiv b_2 \pmod m$, ..., $a_k \equiv b_k \pmod m$, siis

$$a_1 a_2 \dots a_k \equiv b_1 b_2 \dots b_k \pmod m,$$

s.t. kongruentse ühe ja sama mooduli järgi võib liikmeti korrutada.

Teoreem 5.6. Kui $a \equiv b \pmod m$, siis iga naturaalarvu n korral

$$a^n \equiv b^n \pmod m,$$

s.t. kongruentsi mõlemaid pooli võib astendada ühe ja sama naturaalarvuga.

Teoreem 5.6 on järeldus teoreemist 5.5.

Teoreem 5.7. Kui $a \equiv b \pmod m$, siis mistahes täisarvu k korral

$$ka \equiv kb \pmod m,$$

s.t. kongruentsi mõlemaid pooli võib korrutada ühe ja sama täisarvuga.

Teoreem 5.7 on erijuht teoreemist 5.5.

Teoreem 5.8. Kui $a_0 \equiv b_0 \pmod m$, $a_1 \equiv b_1 \pmod m$, ..., $a_n \equiv b_n \pmod m$, $x_1 \equiv x_2 \pmod m$, siis

$$a_0x_1^n + a_1x_1^{n-1} + \ldots + a_n \equiv b_0x_2^n + b_1x_2^{n-1} + \ldots + b_n \pmod m.$$

Tõestus. Teoreemide 5.6 ja 5.5 põhjal

$$a_ix_1^{n-i} \equiv b_ix_2^{n-i} \pmod m \quad (i=0,1,\ldots,n),$$

millest teoreemi 5.2 põhjal saamegi tõestatava kongruentsi.

Järeldus. Kui $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$ ja $x_1 \equiv x_2 \pmod m$, siis

$$f(x_1) \equiv f(x_2) \pmod m.$$

Teoreem 5.9. Kui täisarvuliste kordajatega täisratsionaalses funktsioonis

$$f(x_1, x_2, \ldots, x_n) = \sum A_{\alpha_1\ldots\alpha_k} x_1^{\alpha_1} \ldots x_k^{\alpha_k}$$

asendada arvud $A_{\alpha_1\ldots\alpha_k}$ ja $x_1, \ldots, x_k$ vastavalt mooduli m järgi kongruentsete arvudega $B_{\alpha_1\ldots\alpha_k}$ ja $y_1, \ldots, y_k$, siis saadud uus avaldis $\sum B_{\alpha_1\ldots\alpha_k} y_1^{\alpha_1} \ldots y_k^{\alpha_k}$

on kongruentne esialgsega mooduli m järgi.

Tõestus on analoogiline teoreemi 5.8 tõestusega.

Teoreem 5.10. Kui $c|a$ ja $c|b$ ning $(c,m) = 1$, siis kongruentsist

$$a \equiv b \pmod{m}$$

järeldub kongruents

$$\frac{a}{c} \equiv \frac{b}{c} \pmod{m},$$

s.t. kongruentsi mõlemaid pooli võib jagada a ja b ühise teguriga, kui see tegur on mooduliga ühisjagajata.

Tõestus. Olgu $a \equiv b \pmod{m}$ ja $a = a_1c$, $b = b_1c$, kusjuures $(c,m) = 1$. Siis $a - b = (a_1 - b_1)c = mt$. Et $(a_1 - b_1)c \vdots m$ ja $(c,m) = 1$, siis teoreemi 1.11 põhjal $a_1 - b_1 \vdots m$ ehk $a_1 - b_1 = mt$. Seega $a_1 \equiv b_1 \pmod{m}$ ehk

$$\frac{a}{c} \equiv \frac{b}{c} \pmod{m}.$$

Märgime eriti, et kongruentsi ei tohi jagada a ja b ühisteguriga, kui sel on ühine tegur mooduliga. Näiteks kehtib ilmselt seos

$$84 \equiv 24 \pmod{10}.$$

Kui jagaksime kongruentsi mõlemaid pooli 4-ga, siis saaksime

$$21 \equiv 6 \pmod{10},$$

mis pole õige.

3. Mooduli muutumisega seotud omadused.

Teoreem 5.11. Kongruentsi mõlemaid pooli ja moodulit võib korrutada ühe ja sama arvuga, s.t.

kui $a \equiv b \pmod{m}$, siis $ak \equiv bk \pmod{mk}$.

Teoreem 5.12. Kongruentsi mõlemaid pooli ja moodulit võib jagada iga nende ühise teguriga, s.t. kui $a \equiv b \pmod{m}$ ja $a = a_1 d$, $b = b_1 d$, $m = m_1 d$, siis

$$a_1 \equiv b_1 \pmod{m_1}.$$

Teoreem 5.13. Kongruentsi

$$ac \equiv bc \pmod{m}$$

mõlemaid pooli võib jagada c-ga, kuid siis peab moodulit jagama c ja m suurima ühisteguriga (c,m).

Tõestus. Olgu $(c, m) = d$; siis $c = c_1 d$, $m = m_1 d$, kusjuures $(c_1, m_1) = 1$. Saame

$$ac_1 d \equiv bc_1 d \pmod{m_1 d}.$$

Teoreemi 5.12 põhjal järeldub siit kongruents

$$ac_1 \equiv bc_1 \pmod{m_1},$$

teoreemi 5.10 põhjal aga

$$a \equiv b \pmod{m_1}.$$

Kui eelmise punkti lõpul toodud näites kongruentsi

$$84 \equiv 24 \pmod{10}$$

mõlemat poolt jagada 4-ga, siis peab moodulit jagama arvuga (10, 4) = 2. Saame

$$21 \equiv 6 \pmod{5},$$

mis on juba õige.

Teoreem 5.14. Kui $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$, ..., $a \equiv b \pmod{m_k}$, siis $a \equiv b \pmod{m}$, kus $m =$

$= [m_1, m_2, \ldots, m_k]$.

Tõestus. Vahe $a - b$ jagub arvudega $m_1, m_2, \ldots, m_k$. Seega on $a - b$ arvude $m_1, m_2, \ldots, m_k$ mingi ühiskordne, s.t. nende arvude vähima ühiskordse kordne:

$$a - b = mt$$

ehk

$$a \equiv b \pmod{m}.$$

Teoreem 5.15. Kui kongruents kehtib mingi mooduli järgi, siis ta kehtib ka selle mooduli mistahes jagaja järgi, s.t. kui $a \equiv b \pmod{m}$ ja $d|m$, siis $a \equiv b \pmod{d}$.

Tõestus järeldub samasusest

$$a = b + mt = b + dm_1t = b + dt_1,$$

kus $t_1 = m_1t$ on täisarv.

Teoreem 5.16. Kui kongruentsi üks pool ja moodul jagub mingi arvuga, siis jagub selle arvuga ka kongruentsi teine pool.

Tõestus. Olgu $a \equiv b \pmod{m}$, kus $d|a$ ja $d|m$. Siis $a = b + mt$ ehk $a_1d = b + m_1dt$, millest teoreemi 1.2 põhjal järeldub, et $d|b$.

Teoreem 5.17. Kui $a \equiv b \pmod{m}$, siis

$$(a, m) = (b, m).$$

Teoreem 5.17 järeldub teoreemist 1.6.

4. Jagamisel tekkiva jääägi leidmine ja jaguvustunnuste tuletamine. Kongruentside omaduste rakendusena vaatleme, kuidas võimalikult lihtsalt leida jääki r, mis tekib mis-

tahes täisarvu N jagamisel antud naturaalarvuga m. Ühtlasi saame arvuga m jaguvuse tunnuse, sest N jagub arvuga m parajasti siis, kui r = 0.

Vaatleme kõigepealt korraga juhte, kus m = 9 ja m = 3. Selleks esitame arvu N tema numbrite a_n, a_{n-1}, ..., a_1 kaudu kümnendsüsteemis:

(4) $N = a_n \cdot 10^{n-1} + a_{n-1} \cdot 10^{n-2} + \ldots + a_2 \cdot 10 + a_1$.

Et $10 \equiv 1 \pmod 9$ ja mod 3), siis ka $10^k \equiv 1 \pmod 9$ ja mod 3). Järelikult

$$N \equiv a_n + a_{n-1} + \ldots + a_2 + a_1 \pmod 9 \text{ ja mod } 3).$$

Seega arvu N jagamisel 9-ga (3-ga) tekib jääk, mis ühtib arvu numbrite summa jagamisel 9-ga (3-ga) tekkiva jäägiga. Järelikult arv jagub 9-ga (3-ga) parajasti siis, kui jagub 9-ga (3-ga) tema numbrite summa.

Edasi vaatleme juhtu, kus m = 11. Et $10 \equiv -1 \pmod{11}$, siis $10^k \equiv (-1)^k \pmod{11}$ ja

$$N \equiv (a_1 + a_3 + \ldots) - (a_2 + a_4 + \ldots) \pmod{11}.$$

Järelikult arvu jagamisel 11-ga tekib jääk, mis ühtib selle arvu paaritutel kohtadel asuvate numbrite summa ja paariskohtadel asuvate numbrite summa vahe jagamisel tekkiva jäägiga. Arv jagub 11-ga parajasti siis, kui nimetatud summade vahe jagub 11-ga.

101-ga jaguvuse tunnuse tuletamiseks esitame arvu N sajandsüsteemis

$$N = b_n \cdot 100^{n-1} + b_{n-1} \cdot 100^{n-2} + \ldots + b_2 \cdot 100 + b_1 =$$

$$= (10a_{2n} + a_{2n-1})\cdot 100^{n-1} + \ldots + (a_4\cdot 10 + a_3)\cdot 100 +$$

$$+ (a_2\cdot 10 + a_1).$$

Et $100 \equiv -1 \pmod{101}$, siis $100^k \equiv (-1)^k \pmod{101}$ ja

$$N \equiv (b_1+b_3+\ldots) - (b_2+ b_4+ \ldots) \pmod{101}.$$

Seega jagub arv 101-ga parajasti siis, kui 101-ga jagub vahe

$$(b_1+ b_3+ \ldots) - (b_2+ b_4+ \ldots)$$

ehk summa

$$(b_1- b_2) + (b_3- b_4) + \ldots .$$

Näiteks arv 1234567891011 ei jagu arvuga 101, sest (11-10)+ + (89-67)+(45-23)+1 = 1+22+22+1 = 46 ei jagu 101-ga.

Siin esitatud meetodi jäägi määramiseks ja jaguvustunnuste tuletamiseks soovitas prantsuse matemaatik B.Pascal (1623-1662). Üldjuhul võib Pascali meetodit kasutada mistahes arvusüsteemis esitatud arvude korral. Vaatlemegi meetodit üldjuhul. Olgu arv N esitatud q-ndsüsteemis (q - arvusüsteemi alus):

$$(5) \qquad N = a_n q^{n-1} + a_{n-1} q^{n-2} + \ldots + a_2 q + a_1,$$

kus a_i $(0 \leq a_i < q)$ on q-ndsüsteemi numbrid. Olgu

$$q^k \equiv r_k \pmod{m}, \quad k=1,2,\ldots,n-1.$$

Siis

$$(6) \quad N \equiv a_n r_{n-1} + a_{n-1} r_{n-2} + \ldots + a_2 r_1 + a_1 \pmod{m}.$$

Kongruents (6) näitab, et arv N annab jagamisel m-ga sama jäägi, mis selle kongruentsi paremal poolel asuv avaldis.

Ühtlasi saame siit jaguvustunnuse: N jagub antud arvuga m parajasti siis, kui jagub paremal poolel seisev avaldis.

Selleks et kongruentsi (6) parem pool oleks absoluutväärtuselt võimalikult väike, valitakse arvuks r_k ($k = 1,2,\ldots,n-1$) absoluutväärtuselt vähim arv, mis on kongruentne astmega q^k. Kui kongruentsi (6) parem pool on absoluutväärtuselt suurem kui q, võib ka selle asendada väiksemaga - samal viisil nagu toimisime arvuga N.

Saadud tulemuse rakendusena erijuhtudel tuletame veel 7-ga jaguvuse tunnuse kümnendsüsteemis ja kaheksandsüsteemis. Võtame alguses kümnendsüsteemi ja vaatleme arvu N kujul (4). Koostame tabeli:

$$10^0 \equiv 1 \pmod 7$$
$$10 \equiv 3 \pmod 7$$
$$10^2 \equiv 3^2 \equiv 2 \pmod 7$$
$$10^3 \equiv 3\cdot 2 \equiv -1 \pmod 7$$
$$10^4 \equiv 2^2 \equiv -3 \pmod 7$$
$$10^5 \equiv 2\cdot(-1) \equiv -2 \pmod 7$$
$$10^6 \equiv 1 \pmod 7$$
$$10^7 \equiv 3 \pmod 7$$
$$\ldots\ldots\ldots\ldots$$

Alates 10^6-st hakkavad jäägid korduma. Seega

$$N = a_1 + a_2\cdot 10 + a_3\cdot 10^2 + a_4\cdot 10^3 + \ldots \equiv a_1 + 3a_2 + 2a_3 - a_4 - 3a_5 - 2a_6 + a_7 + 3a_8 + 2a_9 - \ldots \pmod 7.$$

Järelikult kümnendsüsteemi arv N jagub 7-ga parajasti siis, kui 7-ga jagub algebraline summa

$$a_1 + 3a_2 + 2a_3 - a_4 - 3a_5 - 2a_6 + \dots .$$

Viimast summat võib arvutada näiteks järgmise skeemi alusel:

$N =$	8	9	1	0	1	1	1	2	3	4	5	6	7	8
kordajad:		3	1	-2	-3	-1	2	3	1	-2	-3	-1	2	3	1

korrutised mod 7: $+3+2-2+0-1+2+3+2-6+2-5-2+0+1 = -1 \equiv 6$.

Näitena võetud arvu N jagamisel 7-ga tekib jääk 6, seega see arv ei jagu 7-ga.

Kaheksandsüsteemi arv N on esitatav kujul (5), kus $0 \leq a_i \leq 7$ ja $q = 8$ (tegelikult esitatakse süsteemi alus 8 kujul 10; numbrit 8 kaheksandsüsteemis ei kasutata). Kuna

$$8^k \equiv 1 \pmod 7,$$

siis

$$N \equiv a_n + a_{n-1} + \dots + a_2 + a_1 \pmod 7.$$

Seega kaheksandarv N jagub 7-ga parajasti siis, kui 7-ga jagub selle arvu numbrite summa. Näeme, et 7-ga jaguvuse tunnus kaheksandsüsteemis on täpselt samasugune nagu 9-ga jaguvuse tunnus kümnendsüsteemis.

Vaatleme veel kongruentsi omaduste rakendusi järgmise näite korral.

Näide. Leida jääk, mis tekib korrutise

$$a = 141 \cdot 263 \cdot 843 \cdot 721$$

jagamisel arvuga 101.

Ülesanne on samaväärne arvuga a kongruentse vähima positiivse arvu x leidmisega:

$$141 \cdot 263 \cdot 843 \cdot 721 \equiv x \pmod{101},$$

kus $0 \leq x < 101$. Teoreemi 5.5 põhjal võib kõik tegurid

asendada kongruentsetega modulo 101:

$$x \equiv 40 \cdot 61 \cdot 35 \cdot 14 \pmod{101}.$$

Korrutist pole vaja leida. Võib leida kahe arvu korrutise ja jätta ära mooduli kordse (millise omaduse põhjal?), tulemuse võib korrutada kolmanda teguriga ja jätta jälle ära mooduli kordse jne. Saame

$$40 \cdot 61 = 2440 \equiv 16 \pmod{101},$$
$$40 \cdot 61 \cdot 35 \equiv 16 \cdot 35 = 560 \equiv 55 \pmod{101},$$
$$40 \cdot 61 \cdot 35 \cdot 14 \equiv 55 \cdot 14 = 770 \equiv 63 = x \pmod{101}.$$

Seega korrutis annab jagamisel 101-ga jäägi 63.

Analoogiliselt võib leida jääägi, mis tekib antud astme jagamisel antud arvuga.

5. Aritmeetiliste tehete tulemuste kontroll.

Arvude täpsel liitmisel, lahutamisel ja korrutamisel kasutatakse sageli järgnevas kirjeldatavat kontrollimise võtet.

Olgu

$$\begin{aligned} N_1 + N_2 &= N_3, \\ N_1 - N_2 &= N_4, \\ N_1 \cdot N_2 &= N_5. \end{aligned} \tag{7}$$

Kui

$$N_i \equiv r_i \pmod{m}, \quad i=1,2,\ldots,5,$$

siis

$$\begin{aligned} r_1 + r_2 &\equiv r_3 \pmod{m}, \\ r_1 - r_2 &\equiv r_4 \pmod{m}, \\ r_1 \cdot r_2 &\equiv r_5 \pmod{m}. \end{aligned} \tag{8}$$

Kui mõni viimastest kongruentsidest ei kehti, siis arvudega N_1 ja N_2 sooritatud vastava tehte tulemus ei ole õige. Kui aga kongruentsid (8) kehtivad, siis võib loota, et ka võrdused (7) on õiged. Tulemuste (7) usaldatavuse tõstmiseks võib seoseid (8) kontrollida mitme erineva mooduli m korral. Arvutamisel kümnendsüsteemis valitakse tavaliselt mooduliks kas 9 või 11 või kontrollitakse tulemusi mõlema mooduli korral. Nimetatud mooduleid eelistatakse kontrolli lihtsuse tõttu. Arvestades eelneva punkti alguses saadud tulemust, võib mooduli m = 9 korral arvutada arvude N_i numbrite summad r_i ja kontrollida tehtele (7) vastava kongruentsi (8) õigsust.

Kirjeldatud kontrollimeetod sobib ka siis, kui tulemus on saadud rohkem kui kahe arvuga sooritatud liitmiste, lahutamiste ja korrutamiste tulemusel, kusjuures neid tehteid on sooritatud suvalises järjekorras (põhjendada!).

Näide. Kontrollida tulemust:

$$(9765613 - 23\cdot 6217)\cdot 53 + 58796 = 510057762.$$

Kuna mooduli 9 järgi

$9765613 \equiv 9+7+6+5+6+1+3 \equiv 0-2-3+5-3+1+3 \equiv 1$, $23 \equiv 5$, $6217 \equiv -2$, $53 \equiv -1$, $58796 \equiv -1$, siis vasak pool on kongruentne arvuga $(1-5\cdot(-2))\cdot(-1)-1 = -12$, parem pool on aga kongruentne arvuga $5+1+0+0+5+7+7+6+2 \equiv 6$. Et $-12 \equiv 6 \pmod 9$, siis tulemuse õigsuse tarvilik tingimus on täidetud.

Kontrollida sama tulemust mooduli 11 järgi!

Kontroll mooduli 9 järgi ei avasta vigu, mis seisnevad kahe numbri äravahetamises ja 0 või 9 ärajätmises.

Harjutusülesandeid.

5.1. Esitades täisarvu tuhandendsüsteemis ja arvestades, et $1001 = 7 \cdot 11 \cdot 13$ ja $999 = 27 \cdot 37$, tuletada arvudega 7, 11, 13 ja 37 jaguvuse tunnused.

5.2. Tuletada jaguvustunnused jagamiseks 4-ga, 8-ga, 99-ga.

5.3. Leida jääk, mis tekib arvu 5361^{67} jagamisel 97-ga.

5.4. Leida jääk, mis tekib arvu $(12371^{56} + 34)^{28}$ jagamisel 111-ga.

5.5. Leida arvu 321^{53} kaks viimast numbrit.

5.6. Kuidas kontrollida jagamist

$$a : b = c \text{ (jääk } r)?$$

5.7. Kontrollida järgmiste aritmeetiliste tehete tulemusi, kasutades mooduleid 9 ja 11:

a) $535738 + 678913 = 124165$;

b) $3234653 - 817838 = 2614815$;

c) $2543 \cdot 783 = 1984122$;

d) $(213 \cdot 93 + 31873) \cdot 11 = 568502$;

e) $783897 : 3914 = 200$ (jääk 1097).

§ 2. JÄÄKIDE SÜSTEEMID

1. Jäägiklassid. Jagamisel arvuga m üht ja sama jääki andvate arvude hulka nimetatakse jäägiklassiks mooduli m järgi (ehk jäägiklassiks modulo m). Tähistame jäägiklassi, kuhu kuuluvad arvud, mis on kongruentsed r-ga mooduli m järgi, sümboliga $\bar{r}$. Seega jäägiklass $\bar{r}$ modulo m on kongruentsi

(1) $$x \equiv r \pmod{m}$$

rahuldavate kõikide täisarvude x hulk. Teisiti öeldes, kõik jäägiklassi $\bar{r}$ kuuluvad arvud saame, kui laseme avaldises

$$xm + r$$

muutujal x omandada kõik täisarvulised väärtused. Eriti $r \in \bar{r}$. Et täisarvude jagamisel m-ga võib mittenegatiivne jääk olla vaid

$$0, 1, 2, \ldots, m-1,$$

siis mooduli m järgi on olemas m erinevat jäägiklassi

$$\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{m-1}.$$

Teoreem 5.18. Võrdus $\bar{a} = \bar{r}$ kehtib parajasti siis, kui $a \equiv r \pmod{m}$.

Tõestus. Kui $a \equiv r \pmod{m}$, s.t. kui $a \in \bar{r}$, siis kongruentsi transitiivsuse ja sümmeetria omaduse (teoreem 5.1) tõttu järeldub kongruentsist (1) kongruents

(2) $$x \equiv a \pmod{m}$$

ja vastupidi, kongruentsist (2) järeldub kongruents (1). Järelikult

$$\bar{a} = \bar{r}.$$

Kui aga $\bar{a} = \bar{r}$, siis $a \in \bar{r}$ ja seega $a \equiv r \pmod{m}$.

Tõestusest järeldub ühtlasi, et jäägiklass $\bar{r}$ on iga oma elemendiga üheselt määratud.

Teatavasti moodustab kõikide jäägiklasside hulk antud mooduli m järgi ringi, kui jäägiklasside summa ja korrutis defineerida valemitega

$$\bar{a} + \bar{b} = \overline{a + b}, \quad \bar{a}\bar{b} = \overline{ab}$$

(vt. näit. G.Kangro. Kõrgem algebra, Tln., 1962, lk. 145--150, või [1], lk. 80-85). Sealjuures on selles ringis olemas nullitegurid, kui moodul m on kordarv; nullitegurid puuduvad, kui moodul on algarv. Viimasel juhul on jäägiklassiring ühtlasi korpus. Muide, sellise moodulist tingitud erinevuse tõttu kaotavad mitmed kongruentside teooria teoreemid oma kehtivuse, kui neis algarvuline moodul asendada kordarvuga. Olles defineerinud tavalisel viisil ringi elemendi kordse ja astme valemitega

$$n\bar{a} = \underbrace{\bar{a} + \bar{a} + \ldots + \bar{a}}_{n \text{ liidetavat}}, \quad 0 \cdot \bar{a} = \bar{0}, \quad -n\bar{a} = n(-\bar{a}),$$

$$(\bar{a})^n = \underbrace{\bar{a}\,\bar{a} \ldots \bar{a}}_{n \text{ tegurit}}, \quad (\bar{a})^0 = \bar{1},$$

võime lihtsalt tõestada, et kehtib järgmine teoreem.

Teoreem 5.19. Iga täisarvuliste kordajatega polünoomi

$$f(x) = c_0x^n + c_1x^{n-1} + \ldots + c_{n-1}x + c_nx^0$$

ja antud mooduli m korral kehtib valem

$$f(\bar{a}) = \overline{f(a)}.$$

Tõestus. Kasutades jäägiklasside summa ja korrutise definitsioone, saame

$$c\bar{a} = \underbrace{\bar{a} + \ldots + \bar{a}}_{c} = \overline{\underbrace{a + \ldots + a}_{c}} = \overline{ca},$$

$$(\bar{a})^n = \underbrace{\bar{a}\cdot\bar{a} \ldots \bar{a}}_{n} = \overline{\underbrace{aa \ldots a}_{n}} = \overline{a^n}.$$

Seetõttu

$$\begin{aligned} f(\bar{a}) &= c_0(\bar{a})^n + c_1(\bar{a})^{n-1} + \ldots + c_{n-1}\bar{a} + c_n\cdot 1 = \\ &= \overline{c_0a^n} + \overline{c_1a^{n-1}} + \ldots + \overline{c_{n-1}a} + \overline{c_n\cdot 1} = \\ &= \overline{c_0a^n + c_1a^{n-1} + \ldots + c_{n-1}a + c_n} = \overline{f(a)}. \end{aligned}$$

2. Täielik jäägide süsteem. Nagu nägime, on mooduli m järgi olemas parajasti m erinevat jäägiklassi. Võttes igast klassist vabalt ühe elemendi ehk esindaja, saame arvude hulga, mida nimetatakse täielikuks jäägide süsteemiks modulo m. Näiteks on täielikuks jäägide süsteemiks modulo 8 arvude

$$0, -7, 10, 3, 4, -3, 14, 7$$

hulk. Enamasti võetakse klasside esindajateks vähimad mittenegatiivsed jäägid

$$0, 1, 2, 3, 4, 5, 6, 7 \pmod 8;$$

mõnikord on kasulik võtta aga absoluutväärtuselt vähimad jäägid. Näiteks modulo 8 on nendeks

$$-3, -2, -1, 0, 1, 2, 3, 4$$

või

$$-4, -3, -2, -1, 0, 1, 2, 3.$$

Teoreem 5.20. Kui (a, m) = 1 ja

(3) $$x_0, x_1, \ldots, x_{m-1}$$

on täielik jääkide süsteem modulo m, siis iga fikseeritud täisarvu b korral on

(4) $$ax_0+b, ax_1+b, \ldots, ax_{m-1}+b$$

samuti täielik jääkide süsteem modulo m.

Tõestus. Vastupidi väitele oletame, et arvud (4) ei moodusta täielikku jääkide süsteemi, s.t. süsteemis (4) leidub kaks arvu, mis on omavahel kongruentsed:

$$ax_i + b \equiv ax_j + b \pmod{m}.$$

Lahutades viimase kongruentsi mõlemalt poolelt arvu b, saame

$$ax_i \equiv ax_j \pmod{m}.$$

Et (a, m) = 1, siis teoreemi 5.10 põhjal on

$$x_i \equiv x_j \pmod{m}.$$

Tulemus on vastuolus eeldusega, et (3) on täielik jääkide süsteem.

Näide 1. Olgu m = 6 ja x = 6, -5, 2, 15, 4, -1, s.t. $x \equiv 0, 1, 2, 3, 4, 5 \pmod 6$; siis

$$5x - 3 = 27, -28, 7, 72, 17, -8,$$

s.o.

$$5x - 3 \equiv 3, 2, 1, 0, 5, 4 \pmod 6.$$

3. Taandatud jääkide süsteem. Teoreemi 5.17 põhjal on ühte ja samasse jäägiklassi kuuluvatel arvudel mooduli-

ga üks ja sama suurim ühistegur. Eriti tähtsad on need klassid, mille puhul see suurim ühistegur on 1. Võttes igast sellisest klassist vabalt ühe esindaja, saame arvude hulga, mida nimetatakse taandatud jääkide süsteemiks modulo m.

Taandatud jääkide süsteemi võib seega koostada täieliku jääkide süsteemi elementidest, võttes sealt kõik need, mis on mooduliga ühistegurita. Võttes eriti aluseks täieliku jääkide süsteemi

$$1,\ 2,\ \ldots,\ m-1,\ m\ ,$$

saame siit mooduliga ühistegurita arve

$$|\{a|\ (a,\ m) = 1,\quad a \leqslant m\}| = \varphi(m)$$

tükki. Seega on taandatud jääkide süsteemis mooduli m järgi $\varphi(m)$ arvu.

Teoreem 5.21. Kui $(a,\ m) = 1$ ja

$$x_1,\ x_2,\ \ldots,\ x_{\varphi(m)} \tag{5}$$

on taandatud jääkide süsteem modulo m, siis ka

$$ax_1,\ ax_2,\ \ldots,\ ax_{\varphi(m)} \tag{6}$$

on taandatud jääkide süsteem modulo m.

Tõestus. Olgu teoreemi eeldused täidetud. Kui süsteemis (6) oleks mooduli järgi kongruentseid, s.t.

$$ax_i \equiv ax_j \pmod{m},$$

siis $(a,\ m) = 1$ tõttu järelduks siit

$$x_i \equiv x_j \pmod{m},$$

mis on vastuolus eeldusega. Seega kuuluvad arvud (6) erinevatesse jäägiklassidesse, mida on arvult $\varphi(m)$. Tuleb veel

näidata, et $(ax_1, m) = 1$. See aga järeldub sellest, et $(a, m) = 1$ ja $(x_1, m) = 1$.

Näide 2. Mooduli 8 järgi on taandatud jääkide süsteemis $\varphi(8) = 4$ elementi, kusjuures süsteem ise on järgmine:

$$1, 3, 5, 7.$$

Olgu $a = 5$, siis $5x$ omandab väärtused 5, 15, 25, 35, mis on kongruentsed vastavalt arvudega 5, 7, 1, 3.

4. Euleri ja Fermat' teoreemid.

Teoreem 5.22 (Euler). Kui $(a, m) = 1$, siis

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

Tõestus. Kirjutame välja taandatud jääkide süsteemi modulo m:

$$r_1, r_2, \ldots, r_{\varphi(m)}. \tag{7}$$

Siis teoreemi 5.21 põhjal ka

$$ar_1, ar_2, \ldots, ar_{\varphi(m)}$$

on taandatud jääkide süsteem sama mooduli järgi. See tähendab, et

$$\begin{aligned} ar_1 &\equiv r_{i_1} \pmod{m}, \\ ar_2 &\equiv r_{i_2} \pmod{m}, \\ &\cdots\cdots\cdots\cdots \\ ar_{\varphi(m)} &\equiv r_{i_{\varphi(m)}} \pmod{m}, \end{aligned} \tag{8}$$

kus kongruentside (8) paremad pooled on jäägid hulgast (7) ja sealjuures kõik erinevad. Korrutame kõik kongruentsid (8) omavahel läbi; saame

$$a^{\varphi(m)} r_1 r_2 \dots r_{\varphi(m)} \equiv r_{i_1} r_{i_2} \dots r_{i_{\varphi(m)}} \pmod{m}.$$

Korrutis $r_1 r_2 \dots r_{\varphi(m)}$ vasakul võrdub kongruentsi parema poolega. Et $(r_i, m) = 1$ iga i korral, siis

$$(r_1 r_2 \dots r_{\varphi(m)}, m) = 1.$$

Seega võime teoreemi 5.10 põhjal viimast kongruentsi korrutisega taandada ja saame

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

Näide 3. Olgu $m = 9$, $\varphi(9) = 6$, $a = 1, 2, 4, 5, 7, 8$. Siis Euleri teoreemi põhjal

$$2^6 \equiv 1 \pmod 9, \qquad 7^6 \equiv 1 \pmod 9,$$
$$4^6 \equiv 1 \pmod 9, \qquad 8^6 \equiv 1 \pmod 9.$$
$$5^6 \equiv 1 \pmod 9,$$

Teoreem 5.23 (Fermat). Kui p on algarv, siis

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

Tõestus. Vaatleme eraldi kahte juhtu, Olgu esiteks $(a, p) = 1$. Siis arvestades, et $\varphi(p) = p-1$, võime Euleri teoreemi põhjal kirjutada

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

Kongruentsi mõlemate poolte korrutamisel arvuga a saamegi väite.

Teiseks olgu $p \mid a$. Siis

$$a \equiv 0 \pmod{p} \quad \text{ja} \quad a^p \equiv 0 \pmod{p}.$$

Seega kehtib väide ka sel juhul.

Harjutusülesandeid.

5.8. Kirjutada välja taandatud jääkide süsteem mooduli 30 järgi.

5.9. Kas arv $6\,781\,207^{24} - 1$ jagub 39-ga?

*5.10. Kasutades Euleri teoreemi arvutada jääk, mis tekib arvu 34^{59522} jagamisel 110-ga.

*5.11. Näidata, et $2^{73\cdot 37-1} \equiv 1 \pmod{37\cdot 73}$.

5.12. Kui palju elemente on taandatud jääkide süsteemis modulo 78? modulo 178?

VI. TUNDMATUT SISALDAVAD KONGRUENTSID

§ 1. ÜLDISI TEOREEME

Kongruentsi

(1) $$f(x) \equiv 0 \pmod{m},$$

kus $f(x)$ on täisarvuliste kordajatega polünoom

(2) $$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n,$$

nimetatakse tundmatut sisaldavaks kongruentsiks.

Kui sealjuures $a_0 \not\equiv 0 \pmod{m}$, siis nimetatakse kongruentsi (1) n-astme kongruentsiks.

Kui x asemele paigutada erinevaid täisarve, siis võib juhtuda, et mõned neist rahuldavad kongruentsi (1), s.t. nende korral $f(x) \vdots m$.

Kui kongruentsi (1) rahuldab mingi $x = x_1$, siis järelduse põhjal teoreemist 5.8 rahuldavad seda kongruentsi ka kõik arvud, mis on kongruentsed x_1-ga modulo m. Seepärast loetakse tavaliselt kongruentsi (1) lahendiks kogu jäägiklassi $\overline{x}_1$, lahendit märgitakse aga järgmiselt:

$$x \equiv x_1 \pmod{m}.$$

Sellise kokkuleppe puhul on kongruentsil niisama palju lahendeid, kui palju jääke täielikust jääkide süsteemist teda rahuldab.

Kongruentsi (1) rahuldavate arvude leidmise ülesanne

on samaväärne võrrandit

(3) $$f(\overline{x}) = \overline{0}$$

rahuldavate jäägiklasside leidmise ülesandega. Tõepoolest, kongruents $f(x_1) \equiv 0 \pmod m$ kehtib teoreemi 5.18 kohaselt parajasti siis, kui $\overline{f(x_1)} = 0$; teoreemi 5.19 tõttu on aga $\overline{f(x_1)} = f(\overline{x}_1)$.

Et mooduli m järgi on olemas m jäägiklassi, siis kongruentsi (1) (samuti võrrandi (3)) lahendamine on teostatav ülimalt m proovimise teel. Selleks et kontrollida, kas jäägiklass rahuldab kongruentsi (1), tarvitseb kontrollida, kas selle klassi mingi esindaja rahuldab kongruentsi (1). Kõikide lahendite leidmiseks tuleb läbi proovida kõik elemendid täielikust jääkide süsteemist modulo m. Kui moodul m on väike, on selline meetod praktikas hästi kasutatav.

Näide 1. Leiame kongruentsi

$$x^2 + x + 1 \equiv 0 \pmod 7$$

lahendid. Täielik jääkide süsteem modulo 7 on järgmine:

$$-3, -2, -1, 0, 1, 2, 3.$$

Proovimine näitab, et neist rahuldavad kongruentsi -3 ja 2. Seega on kongruentsi lahenditeks

$$x \equiv -3 \pmod 7 \text{ ja } x \equiv 2 \pmod 7$$

ehk

$$x \equiv 4 \pmod 7, \quad x \equiv 2 \pmod 7.$$

Samu lahendeid võib esitada ka kujul

$$x = 4 + 7t \quad \text{ja} \quad x = 2 + 7t,$$

kus t omandab kõiki täisarvulisi väärtusi.

Näide 2. Kongruentsil

$$x^3 + x + 1 \equiv 0 \pmod 5$$

ei ole lahendeid, sest ükski arvudest

$$-2, -1, 0, 1, 2$$

ei rahulda teda.

Juhul kui moodul m on suur, on kongruentsi (1) praktiline lahendamine proovimise teel tülikas. Järgnevates paragrahvides vaatleme kongruentside lahendamise meetodeid, mis võimaldavad kindlaks teha lahendite arvu ja leida lahendid võimalikult väheste operatsioonidega. Lahendamisel tuleb mõnikord kongruents asendada temaga ekvivalentse kongruentsiga. Sealjuures võivad kongruentsid esineda kujul

$$f(x) \equiv g(x) \pmod{m},$$

kus $f(x)$ ja $g(x)$ on täisarvuliste kordajatega polünoomid. Kaht kongruentsi

$$f_1(x) \equiv g_1(x) \pmod{m_1}$$

ja

$$f_2(x) \equiv g_2(x) \pmod{m_2}$$

nimetatakse <u>ekvivalentseteks</u>, kui arvude hulk, mis rahuldab üht kongruentsi, ühtib arvude hulgaga, mis rahuldab teist kongruentsi.

<u>Teoreem 6.1</u>. Kongruentsid

$$bf(x) \equiv bg(x) \pmod{m}, \quad (b,m) = 1, \tag{4}$$

$$kf(x) \equiv kg(x) \pmod{km}, \tag{5}$$

$$f(x) + \omega(x) \equiv g(x) + \omega(x) \pmod{m}, \tag{6}$$

kus $\omega(x)$ on suvaline polünoom, on kõik ekvivalentsed kongruentsiga

$$f(x) \equiv g(x) \pmod{m}. \tag{7}$$

<u>Tõestus</u>. Kui mingi x_0 korral

(8) $$f(x_o) \equiv g(x_o) \pmod m,$$

siis teoreemide 5.7, 5.11, ja 5.2 põhjal kehtivad kongruentsid, mis saadakse tundmatut sisaldavatest kongruentsidest (4) - (6) x asendamisel x_o-ga. Vastupidi, viimastest järeldub kongruents (8) teoreemide 5.10, 5.12 ja 5.3 põhjal. Seega rahuldavad kongruentse (4) - (7) ühed ja samad arvud ning nad on ekvivalentsed.

Teoreemist järeldub, et kongruentsid $f(x) \equiv g(x) \pmod m$ ja $f(x) - g(x) \equiv 0 \pmod m$ on ekvivalentsed.

Rakendustes kasutatakse peamiselt kongruentside lihtsustamist, s.t. üleminekut kongruentsidelt (4), (5) või (6) kongruentsile (7), kuigi on muidugi õigustatud ka vastupidine üleminek.

Teoreem 6.2. Kui $a_o \equiv b_o \pmod m$, $a_1 \equiv b_1 \pmod m$, ... , $a_n \equiv b_n \pmod m$, siis kongruentsid

$$f(x) = a_o x^n + \ldots + a_{n-1}x + a_n \equiv 0 \pmod m$$

ja

$$g(x) = b_o x^n + \ldots + b_{n-1}x + b_n \equiv 0 \pmod m$$

on ekvivalentsed.

Tõestus. Kui $f(x_o) \equiv 0 \pmod m$, siis teoreemi 5.8 kohaselt $g(x_o) \equiv f(x_o) \equiv 0 \pmod m$. Kui aga $f(x_o) \not\equiv 0 \pmod m$, siis ka $f(x_o) \equiv g(x_o) \not\equiv 0 \pmod m$. Teoreem on tõestatud.

Tundmatut sisaldav kongruents võib esineda ka (1)-st erineval kujul, näiteks eksponentkongruentsina

$$a^x \equiv b \pmod m,$$

kus a ja b on täisarvud. Osutub, et eksponentkongruentsi

lahendeid ei saa esitada kujul $x \equiv c \pmod m$, kuid neid saab esitada jäägiklassidena m-st erineva mooduli järgi.

Harjutusülesandeid.

6.1. Proovimismeetodil lahendada järgmised kongruentsid:

a) $x^5 + x^4 + x + 1 \equiv 0 \pmod 6$;

b) $3x^4 + 2x^2 - 1 \equiv 0 \pmod 5$;

c) $4x^3 - 7x^2 + 10 \equiv 0 \pmod{11}$;

d) $3x \equiv 13 \pmod{11}$.

6.2. Asendanud kordajad eelnevalt väiksematega, lahendada järgmised kongruentsid:

a) $90x^{12} + 46x^2 - 52x - 48 \equiv 0 \pmod 5$;

b) $25x^3 - 36x^2 + 18x + 13 \equiv 0 \pmod 9$;

c) $53x^4 + 9x^3 - 19x^2 + 25x + 17 \equiv 0 \pmod 5$.

§ 2. LINEAARKONGRUENTSID

1. Juhtum, kus x kordaja ja moodul on ühistegurita.

Lineaarkongruentsiks nimetatakse kongruentsi

(1) $$ax \equiv b \pmod m.$$

Käesolevas punktis vaatleme juhtu, kus $(a, m) = 1$. Näitame, et siis on lineaarkongruentsil parajasti üks lahend. Kongruentsi parem pool kuulub teatud jäägiklassi $\bar{k}$, s.t. $b \in \bar{k}$ ehk $b \equiv k \pmod m$. Kirjutame välja täieliku jääkide süsteemi modulo m:

(2) $$0, 1, 2, 3, \ldots, m-1.$$

Siis teoreemi 5.20 kohaselt on

(3) $$a\cdot 0, a\cdot 1, a\cdot 2, \ldots, a(m-1)$$

samuti täielik jääkide süsteem, kusjuures jäägiklassi $\overline{k}$ kuulub parajasti üks jääkidest (3). Olgu selleks ax_0. See tähendab, et $ax_0 \equiv k \pmod m$, kusjuures ükski teine jääk süsteemist (3) ei ole kongruentne k-ga modulo m. Kongruentsi (1) ainsaks lahendiks on seega

$$x \equiv x_0 \pmod m.$$

Eeldades endiselt, et $(a, m) = 1$, vaatleme lineaarkongruentsi (1) lahendamise meetodeid.

A. <u>Mooduli kordse liitmise meetod</u>. Kirjeldame meetodit näidete varal.

<u>Näide 1</u>. Võtame kongruentsi

$$5x \equiv 4 \pmod 7$$

ja liidame paremale poolele või lahutame sellest arvu 7 kordseid, kuni saame arvu 5 kordse:

$$5x \equiv 4 - 2\cdot 7 = -10 \pmod 7.$$

Jagamisel 5-ga saame lahendiks

$$x \equiv -2 \pmod 7$$

ehk

$$x \equiv 5 \pmod 7.$$

Meetodi rakendamise käigus võime kongruentsi pooli korduvalt jagada. Seda asjaolu kasutame järgmises näites.

<u>Näide 2</u>. Kongruentsi

$$210x \equiv 103 \pmod{353}, \quad ((210, 353) = 1)$$

lahendamiseks liidame kõigepealt paremale poolele mooduli kordse:

$$210x \equiv 456 \pmod{353}.$$

Nüüd jagame mõlemat poolt ühise teguriga 6:

$$35x \equiv 76 \pmod{353},$$

lahutame kahekordse mooduli:

$$35x \equiv 76 - 706 = -630 \pmod{353}$$

ja jagamisel 35-ga saame vastuse

$$x \equiv -18 \equiv 335 \pmod{353}.$$

B. Ahelmurdude meetod. Arendame $\frac{m}{a}$ ahelmurruks. Siis $\frac{m}{a} = \frac{P_n}{Q_n}$. Kuna $P_nQ_{n-1} - P_{n-1}Q_n = (-1)^n$ ja (a, m) = 1 tõttu $P_n = m$, $Q_n = a$, siis

$$mQ_{n-1} - aP_{n-1} = (-1)^n$$

ehk

$$aP_{n-1} = (-1)^{n-1} + mQ_{n-1}.$$

Nüüd aga

$$aP_{n-1} \equiv (-1)^{n-1} \pmod{m},$$

millest pärast korrutamist arvuga $(-1)^{n-1}b$ saame

$$a(-1)^{n-1}bP_{n-1} \equiv b \pmod{m}.$$

Seega kongruentsi (1) lahendiks on

$$x \equiv (-1)^{n-1}bP_{n-1} \pmod{m},$$

mis eeltõestatu põhjal on ainus.

Näide 3. Lahendame kongruentsi $97x \equiv 53 \pmod{149}$.

Arendame $\frac{149}{97}$ ahelmurruks ja arvutame suurused P_k:

149		97	52	45	7	3	1
		1	1	1	6	2	3
0	1	1	2	3	20	43	149

Et n = 6, $P_{n-1} = 43$ ja b = 53, siis lahendiks on

$$x \equiv -53 \cdot 43 = -2279 \equiv -44 \equiv 105 \pmod{149}.$$

C. Lineaarkongruentsi lahendamine Euleri teoreemi alusel. Teatavasti, kui (a, m) = 1, siis

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

Korrutame kongruentsi b-ga. Saame

$$a^{\varphi(m)}b \equiv b \pmod{m}$$

ehk

$$a\left(a^{\varphi(m)-1}b\right) \equiv b \pmod{m}.$$

Siit näeme, et kongruentsi $ax \equiv b \pmod{m}$ rahuldab

$$x \equiv a^{\varphi(m)-1}b \pmod{m}.$$

Näide 4. Lahendame kongruentsi $17x \equiv 15 \pmod{44}$. Siin $(17, 44) = 1$ ja $\varphi(44) = \varphi(4)\cdot\varphi(11) = 2\cdot 10 = 20$. Seega lahendiks on

$$x \equiv 17^{19}\cdot 15 \equiv 19 \pmod{44}.$$

2. Juhtum, kus x kordaja ja moodul on ühisteguriga.

Olgu $(a, m) = d$. Siis $a = a_1d$ ja $m = m_1d$, kusjuures $(a_1, m_1) = 1$. Pärast a ja m asendamist saame kongruentsile (1) kuju

$$a_1dx \equiv b \pmod{m_1d}. \tag{4}$$

Kui kongruents (4) on lahenduv, siis teoreemi 5.16 põhjal peab b jaguma d-ga. Tingimus $d \mid b$ on kongruentsi (4) ehk (1) lahenduvuseks tarvilik. Kui see tingimus ei ole täidetud, s.t. kui b ei jagu d-ga, siis konguents

$$ax \equiv b \pmod{m}$$

ei ole lahenduv. Näiteks pole lahendeid lineaarkongruentsil

$$15x \equiv 7 \pmod{21},$$

sest 7 ei jagu arvuga $(15, 21) = 3$.

Olgu $b = b_1d$. Siis

$$da_1x \equiv db_1 \pmod{dm_1},$$

millest peale jagamist d-ga saame esialgsega ekvivalentse

kongruentsi

(5) $$a_1x \equiv b_1 \pmod{m_1}, \quad (a_1, m_1) = 1.$$

Nagu eelmises punktis nägime, on viimasel kongruentsil mooduli m_1 järgi parajasti üks lahend. Seega on tingimus

$$(a, m) \mid b$$

tarvilik ja piisav lahendi olemasoluks.

Teeme kindlaks vaadeldava kongruentsi lahendite arvu modulo m. Kongruentsil (5), samuti kongruentsil (1) on mooduli m_1 järgi parajasti üks lahend, kuid modulo m on lahendeid rohkem.

Olgu c vähim positiivne jääk modulo m_1, mis kongruentsi rahuldab. Siis kõik arvud x, mis moodustavad lahendi modulo m_1, on antud valemiga

(6) $$x \equiv c \pmod{m_1}.$$

Kuid mooduli m järgi moodustavad need arvud mitte ühe jäägiklassi, vaid rohkem; nimelt nii palju, kui palju arve kujul (6) leidub täielikus jääkide süsteemis modulo m:

$$0, 1, 2, \ldots, m-1.$$

Arvudest (6) kuuluvad siia

$$c, c+m_1, c+2m_1, \ldots, c+(d-1)m_1,$$

s.t. d arvu. Järelikult on kongruentsil (1) mooduli m järgi d lahendit:

$$x \equiv c \pmod{m}, \quad x \equiv c + m_1 \pmod{m}, \ldots,$$

$$x \equiv c + (d-1)m_1 \pmod{m}.$$

Neid lahendeid on tavaks märkida järgmiselt:

(7) $$x \equiv c, c + m_1, \ldots, c + (d-1)m_1 \pmod{m}.$$

On arusaadav, et arvude hulgad (6) ja (7) ühtivad.

Harjutusülesandeid.

6.3. Mooduli kordse liitmise meetodil lahendada lineaarkongruentsid

a) $30x \equiv 53 \pmod{77}$;

b) $42x \equiv 11 \pmod{67}$;

c) $27x \equiv 14 \pmod{25}$;

d) $6x \equiv 1 \pmod{37}$.

6.4. Ahelmurdude meetodit kasutades lahendada kongruentsid

a) $256x \equiv 179 \pmod{337}$;

b) $221x \equiv 111 \pmod{360}$;

c) $23x \equiv 667 \pmod{693}$.

6.5. Euleri teoreemi alusel lahendada kongruents

$$11x \equiv 32 \pmod{36}.$$

Lahendi õigsust kontrollida asendamise teel.

6.6. Lahendada kongruentsid

a) $1215x \equiv 560 \pmod{2755}$;

b) $78x \equiv 30 \pmod{198}$;

c) $8934x \equiv 5789 \pmod{10113}$.

§ 3. LINEAARKONGRUENTSIDE SÜSTEEMID

Käesolevas paragrahvis vaatleme lineaarkongruentside süsteemi

$$(1)\qquad \begin{aligned} a_1x &\equiv b_1 \pmod{m_1} \\ a_2x &\equiv b_2 \pmod{m_2} \\ &- - - - - - - - - \\ a_kx &\equiv b_k \pmod{m_k} \end{aligned}$$

lahendamist.

1. Eeldame algul, et moodulid on paarikaupa ühisteguritа, s.t. iga i j korral, kus i ≠ j, on $(m_i, m_j) = 1$, ja peale selle $(a_i, m_i) = 1$. Siis on süsteemi (1) igal kongruentsil parajasti üks lahend:

$$(2)\qquad \begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \\ &- - - - - - - - \\ x &\equiv c_k \pmod{m_k}. \end{aligned}$$

Ilmselt on süsteemid (1) ja (2) ekvivalentsed (neil on ühed ja samad lahendid). Süsteemi (1) lahendi saamiseks tuleb teatud mooduli järgi leida jäägiklass, mis rahuldab korraga süsteemi kõiki kongruentse.

Teoreem 6.3. Kui $(m_i, m_j) = 1$ $(i,j = 1,2,\ldots,k;$ $i \neq j)$ ja arvud M_i, M_i' $(i = 1,2,\ldots,k)$ on määratud tingimustest

$$m_1m_2 \ldots m_k = M_im_i, \quad M_iM_i' \equiv 1 \pmod{m_i},$$

siis süsteemi (2) ja seega ka süsteemi (1) lahendiks on

$$(3)\quad x \equiv M_1M_1'c_1 + M_2M_2'c_2 + \ldots + M_kM_k'c_k \pmod{m_1m_2 \ldots m_k}.$$

Mooduli $m_1m_2 \ldots m_k$ järgi on see lahend ainus.

Tõestus. Kõigepealt märgime, et teoreemi tingimustes esinevad kongruentsid $M_iM_i' \equiv 1 \pmod{m_i}$ on M_i' suhtes üheselt lahenduvad, sest $(M_i, m_i) = 1$. Edasi näitame, et arv $M_1M_1'c_1 + M_2M_2'c_2 + \ldots + M_kM_k'c_k$ rahuldab süsteemi i-ndat kongruentsi $(i = 1,2,\ldots,k)$. Tõepoolest, kuna $M_j \vdots m_i$ $(j \neq i)$ ja $M_iM_i' \equiv 1 \pmod{m_i}$, siis

$$M_1M_1'c_1 + \ldots + M_iM_i'c_i + \ldots + M_kM_k'c_k \equiv M_iM_i'c_i \equiv c_i \pmod{m_i}.$$

Seega süsteemi (2) üheks lahendiks on (3).

Oletame, et peale lahendi (3) leidub veel arve, mis rahuldavad kongruentse (2). Rahuldagu süsteemi (2) arv c. Siis $c \equiv c_i \pmod{m_i}$, $i = 1,2,\ldots,n$ ja seetõttu

$$c \equiv c_i \equiv M_1M_1'c_1 + \ldots + M_kM_k'c_k \pmod{m_i}, \quad i = 1,2,\ldots,n.$$

Teoreemi 5.14 põhjal on

$$c \equiv M_1M_1'c_1 + \ldots + M_kM_k'c_k \pmod{m_1m_2 \ldots m_k},$$

mis näitabki, et teisi lahendeid peale (3) ei ole.

Näide 1. Leida naturaalarv x, mis annab jagamisel 3-ga jäägi 1, jagamisel 5-ga jäägi 2, jagamisel 7-ga jäägi 3 ja jagamisel 11-ga jäägi 4.

Ülesande tingimuste kohaselt peab x rahuldama kongruentside süsteemi

$$x \equiv 1 \pmod 3$$
$$x \equiv 2 \pmod 5$$
$$x \equiv 3 \pmod 7$$
$$x \equiv 4 \pmod{11}.$$

Määrame M_i ja M_i'. Seosest

$$3\cdot5\cdot7\cdot11 = M_im_i$$

saame

i	1	2	3	4
m_i	3	5	7	11
M_i	385	231	165	105

M_i' leidmiseks tuleb lahendada abikongruentsid

$385\,M_1' \equiv 1 \pmod 3$ ehk $M_1' \equiv 1 \pmod 3$,

$231\,M_2' \equiv 1 \pmod 5$ ehk $M_2' \equiv 1 \pmod 5$,

$165\,M_3' \equiv 1 \pmod 7$ ehk $4M_3' \equiv 1 \pmod 7$,

$105\,M_4' \equiv 1 \pmod{11}$ ehk $6M_4' \equiv 1 \pmod{11}$.

Lahendite jäägiklassidest võtame absoluutväärtuselt vähimad elemendid:

$$M_1' = 1, \quad M_2' = 1, \quad M_3' = 2, \quad M_4' = 2.$$

Seega $c = 385 \cdot 1 \cdot 1 + 231 \cdot 1 \cdot 2 + 165 \cdot 2 \cdot 3 + 105 \cdot 2 \cdot 4 = 2677$ ja otsitav lahend on

$$x \equiv 2677 \equiv 367 \pmod{1155}, \quad x > 0.$$

Nõutud omadusega on arvud

$$367 + 1155\,k, \text{ s.o. } 367, 1522, 2677, \ldots .$$

2. Vaatleme süsteemi (1) teist lahendusmeetodit. Eeldame esialgu ka siin, et iga i,j korral $(m_i, m_j) = 1$ $(i \neq j)$ ja $(a_i, m_i) = 1$. Konstrueerime lahendi järk-järgult. Esimest kongruentsi rahuldavad arvud

$$x = c_1 + m_1 t_1$$

iga täisarvu t_1 puhul. Asendame saadud x teise kongruentsi. Saame lineaarkongruentsi t_1 suhtes

$$a_2 c_1 + a_2 m_1 t_1 \equiv b_2 \pmod{m_2}. \tag{4}$$

Kaht esimest kongruentsi rahuldavad arvudest $x = c_1 + m_1 t_1$ need, mille korral t_1 rahuldab teist kongruentsi. Et $(a_2 m_1, m_2) = 1$, siis see kongruents on t_1 suhtes lahenduv. Olgu kongruentsi (4) lahendiks

$$t_1 \equiv d_1 \pmod{m_2} \quad \text{ehk} \quad t_1 = d_1 + m_2 t_2.$$

Seega esimest kaht kongruentsi rahuldavad arvud

$$x = c_1 + m_1(d_1 + m_2 t_2) = e_1 + m_1 m_2 t_2,$$

kus $e_1 = c_1 + m_1 d_1$, s.t. esimesest kahest kongruentsist koosneva süsteemi lahendiks on

$$x \equiv e_1 \pmod{m_1 m_2}.$$

Edasi toimime analoogiliselt. Asendame x kolmandasse kong-

ruentsi

$$a_3e_1 + a_3m_1m_2t_2 \equiv b_3 \pmod{m_3},$$

millest lahendamisel saame

$$t_2 \equiv d_2 \pmod{m_3} \quad \text{ehk} \quad t_2 = d_2 + m_3t_3.$$

Seega kolme esimest kongruentsi rahuldavad arvud

$$x = e_1 + m_1m_2(d_2 + m_3t_3) = e_2 + m_1m_2m_3t$$

ehk

$$x \equiv e_2 \pmod{m_1m_2m_3}.$$

Niiviisi saame lõpuks süsteemi (1) lahendi

(5) $$x \equiv e_{k-1} \pmod{m_1m_2 \dots m_k}.$$

Et igal sammul lahendatavale kongruentsile saame parajasti ühe lahendi, siis valemiga (5) on antud kõik lahendid.

Juhul kui tingimused $(m_i, m_j) = 1$, $(m_i, a_i) = 1$ ei ole täidetud, on sama meetod ikkagi kasutatav, kuid siis võib juhtuda, et 1) mõnel sammul saab moodulit ja kongruentsi mõlemaid pooli jagada ühise teguriga või et 2) mõnel sammul saame lahendamatu kongruentsi. Esimesel juhul saame lahendi mooduli m järgi, mis on moodulite $m_1, m_2, \dots, m_k$ vähim ühiskordne. Mooduli $m_1m_2 \dots m_k$ järgi on siis süsteemil rohkem kui üks lahend. Teisel juhul on juba esialgne süsteem vastuoluline, s.t. süsteemil puudub lahend.

Näide 2. Leida naturaalarv, mis lõpeb 37-ga, mille 3-kordne annab jagamisel 16-ga jäägi 7 ja mis jagub 7-ga.

Otsitav arv x peab rahuldama kongruentside süsteemi

$$x \equiv 37 \pmod{100}, \quad 3x \equiv 7 \pmod{16}, \quad x \equiv 0 \pmod{7}.$$

Esimest kongruentsi rahuldavad arvud $x = 37 + 100t_1$. Asenda-

misel teise saame kongruentsi t_1 suhtes

$$111 + 300t_1 \equiv 7 \pmod{16}$$

ehk

$$-1 + 12t_1 \equiv 7 \pmod{16}$$

ehk

$$12t_1 \equiv 8 \pmod{16},$$

millest

$$3t_1 \equiv 2 \pmod{4}$$

ja

$$t_1 \equiv 2 \pmod{4}.$$

Seega $t_1 = 2 + 4t_2$ ja $x = 37 + 100(2 + 4t_2) = 237 + 400t_2$.

Edasi leiame t_2, mille korral on rahuldatud ka kolmas kongruents:

$$237 + 400t_2 \equiv 0 \pmod{7}.$$

Asendades kordajad kongruentsetega mod 7 saame kohe lahendi

$$t_2 \equiv 1 \pmod{7} \quad \text{ehk} \quad t_2 = 1 + 7t_3.$$

Seega $x = 237 + 400(1 + 7t_3) = 637 + 2800t_3$. Süsteemi lahendiks on

$$x \equiv 637 \pmod{2800}$$

ja otsitavateks naturaalarvudeks arvud 637, 3437, 6237, ...

Otsene kontroll näitab, et need arvud rahuldavad tõepoolest nõutud tingimusi.

Näide 3. Süsteemil

$x \equiv 1 \pmod{6}$, $3x \equiv 4 \pmod{10}$, $2x \equiv -1 \pmod{15}$

ei ole lahendit, sest $x = 1 + 6t$ asendamisel teise kongruentsi saame t suhtes lahendumatu kongruentsi.

Harjutusülesandeid.

6.7. Kasutades esimest meetodit, lahendada järgmised kongruentside süsteemid:

a) $4x \equiv 5 \pmod 7$, $x \equiv 3 \pmod 5$, $7x \equiv 1 \pmod{11}$;

b) $x \equiv 1 \pmod 3$, $2x \equiv 1 \pmod 7$, $3x \equiv 1 \pmod 8$;

c) $5x \equiv 4 \pmod 9$, $3x \equiv 7 \pmod{10}$, $x \equiv 1 \pmod{11}$.

6.8. Kasutades teist meetodit, lahendada järgmised kongruentside süsteemid:

a) $3x \equiv 7 \pmod{10}$, $x \equiv 7 \pmod{15}$, $3x \equiv 1 \pmod{18}$;

b) $4x \equiv 5 \pmod 7$, $x \equiv 3 \pmod 5$, $7x \equiv 1 \pmod{11}$;

c) $x \equiv 17 \pmod{60}$, $x \equiv 10 \pmod{31}$, $3x \equiv 1 \pmod{10}$.

6.9. Leida vähim naturaalarv, mis annab jagamisel 2-ga jäägi 1, jagamisel 3-ga jäägi 2, jagamisel 4-ga jäägi 3, jagamisel 5-ga jäägi 4, jagamisel 6-ga jäägi 5 ja jagamisel 7-ga jäägi 6.

6.10. Leida naturaalarvud, mis lõpevad 3-ga, mille jagamisel 15-ga tekib jääk 8 ja mille 7-kordse jagamisel 13-ga tekib jääk 1.

§ 4. KÕRGEMA ASTME KONGRUENTSID ALGARVULISE MOODULI JÄRGI

Vaatleme n-astme kongruentsi

(1) $$f(x) \equiv 0 \pmod p,$$

kus $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$, $a_0 \not\equiv 0 \pmod p$ ja kus p on algarv.

Teoreem 6.4. Algarvulise mooduli korral saab kongru-

entsi, mille aste n on suurem kui moodul või võrdub sellega, asendada ekvivalentse kongruentsiga, mille aste on moodulist väiksem.

Tõestus. Olles jaganud $f(x)$ vahega $x^p - x$, võime kirjutada

$$f(x) = g(x)(x^p - x) + r(x), \tag{2}$$

kus polünoomi $r(x)$ aste on väiksem kui p. Et Fermat' teoreemi kohaselt

$$x^p - x \equiv 0 \pmod{p} \tag{3}$$

iga x korral, siis asendub kongruents (1) ekvivalentse kongruentsiga

$$r(x) \equiv 0 \pmod{p}. \tag{4}$$

Tõepoolest, kui x rahuldab kongruentsi (1), siis seoste (2) ja (3) tõttu on rahuldatud (4). Vastupidi, kui x rahuldab kongruentsi (4), siis kongruentsile (4) arvuga $g(x)$ korrutatud kongruentsi (3) liitmisel saame, et on rahuldatud (1). Teoreem on tõestatud.

Nagu teoreemi tõestusest selgub, on kongruentsid

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

ja

$$r_1(x) = f(x) - g(x)(x^p - x) \equiv 0 \pmod{p}$$

ekvivalentsed ka sel juhul, kui $r_1(x)$ aste pole väiksem kui p. Seda asjaolu võib kasutada ekvivalentse madalama astme kongruentsi leidmiseks. Selleks tarvitseb asendada igas liikmes eraldi aste x^s, kus $s \geqslant p$, astmega

$$x^{s-(p-1)} = x^s - (x^p - x)x^{s-p}.$$

Kui veel $s - (p - 1) \geqslant p$, siis võib seda asendamist korrata. See on aga samaväärne sellega, et juhul kui s =

$= (p-1)k + r$, kus $1 \leq r \leq p-1$, asendatakse aste x^s astmega x^r. Kui selline asendus teha läbi kõigi liikmetega, siis saame sama tulemuse, nagu polünoomi jagamisel vahega $x^p - x$.

Näide. Asendame kongruentsi

$$x^{18} + 2x^{15} + 3x^{12} + 4x^{10} + 5x^7 + 3x^6 + 8x^3 + 9x^2 + 10x + 11 \equiv 0 \pmod 7$$

ekvivalentse madalama kui 7.astme kongruentsiga. Jagame astendajad, mis on suuremad kui 6, arvuga $p - 1 = 6$ ja asendame nad jäägiga r, kus $1 \leq r \leq 6$. Saame

$$x^6 + 2x^3 + 3x^6 + 4x^4 + 5x + 3x^6 + 8x^3 + 9x^2 + 10x + 11 \equiv 0 \pmod 7$$

ehk

$$4x^4 + 3x^3 + 2x^2 + x + 4 \equiv 0 \pmod 7.$$

(Ülesanne: Teha sama asendus läbi, jagades polünoomi vahega $x^7 - x$.)

Teoreem 6.5. Algarvulise mooduli p korral on n-astme kongruentsil ülimalt n lahendit.

Tõestus. Eelmise teoreemi põhjal võib piirduda juhuga, kus $n < p$. Oletame vastupidi, et mingil n-astme kongruentsil

$$f(x) \equiv 0 \pmod p$$

on $n + 1$ lahendit:

$$x \equiv x_1, x_2, \ldots, x_n, x_{n+1} \pmod p.$$

Lugedes arvud $x_1, x_2, \ldots, x_n$ interpolatsioonisõlmedeks, esitame polünoomi $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$ Newtoni interpolatsioonivalemi abil kujul (vt. näit. G.Kangro. Kõrgem algebra. Tln., 1962, lk. 236-240)

$$
\begin{aligned}
f(x) = {} & b_0(x-x_1)(x-x_2)\ \dots\ (x-x_{n-1})(x-x_n) + \\
& + b_1(x-x_1)(x-x_2)\ \dots\ (x-x_{n-1}) + \\
& + \ .\ .\ .\ .\ .\ .\ .\ .\ .\ .\ .\ .\ .\ + \\
& + b_{n-2}(x-x_1)(x-x_2) + b_{n-1}(x-x_1) + b_n,
\end{aligned}
\tag{5}
$$

kus kordajad b_i on üheselt määratud ja täisarvud, sest nad on arvutatavad Horneri skeemi abil polünoomi $f(x) = a_0x^n + a_1x^{n-1} + \dots + a_n$ esialgsete kordajate $a_0, a_1, \dots, a_n$ kaudu, kusjuures $b_0 = a_0$. Sealjuures, vastupidi, avalduvad kõik kordajad a_i omakorda kordajate $b_0, b_1, \dots, b_n$ lineaarsete homogeensete funktsioonidena. Tõepoolest, kordajate võrdlemine annab seosed

$$
\begin{aligned}
a_0 &= b_0, \\
a_1 &= b_1 - b_0\,\sigma_1^{(n)}, \\
a_2 &= b_2 - b_1\,\sigma_1^{(n-1)} + b_0\,\sigma_2^{(n)}, \\
a_3 &= b_3 - b_2\,\sigma_1^{(n-2)} + b_1\,\sigma_2^{(n-1)} - b_0\,\sigma_3^{(n)}, \\
&- \\
a_n &= b_n - b_{n-1}\,\sigma_1^{(1)} + b_{n-2}\,\sigma_2^{(2)} - \dots + (-1)^n\,b_0\,\sigma_n^{(n)},
\end{aligned}
$$

kus

$$
\sigma_j^{(k)} = \sum_{1 \le i_1 < \dots < i_j \le k} x_{i_1}\,x_{i_2} \cdots x_{i_j}.
$$

Tõestame, et $b_i \vdots p$, s.t. $b_i \equiv 0 \pmod p$ $(i = n, n-1, n-2, \dots, 1, 0)$. Anname samasuses (5) x-le väärtuse $x = x_1$. Saame $f(x_1) = b_n$. Et jäägiklass $\bar{x}_1$ on kongruentsi lahend, siis $f(x_1) \equiv 0 \pmod p$, mistõttu

$$b_n \equiv 0 \pmod p.$$

Edasi anname x-le väärtuse $x = x_2$. Siis $f(x_2) \equiv 0 \pmod p$ ehk

$$b_n + b_{n-1}(x_2 - x_1) \equiv 0 \pmod{p}.$$

Et siin $b_n \equiv 0 \pmod{p}$, $x_2 - x_1 \not\equiv 0 \pmod{p}$ ja p on algarv, siis

$$b_{n-1} \equiv 0 \pmod{p}.$$

Edasi anname x-le järjekorras väärtused $x_3, x_4, \ldots, x_n$. Viimasel juhul muutub $f(x)$ avaldises (5) nulliks esimene liidetav. Arvestades aga, et

$$b_n \equiv b_{n-1} \equiv \ldots \equiv b_2 \equiv 0 \pmod{p},$$

saame

$$b_1(x_n - x_1) \ldots (x_n - x_{n-1}) \equiv f(x_n) \equiv 0 \pmod{p}.$$

Et kõik arvud $x_1, x_2, \ldots, x_n$ kuuluvad erinevatesse jäägiklassidesse, siis $b_1 \equiv 0 \pmod{p}$. Anname x-le väärtuse x_{n+1}. Arvestades, et $\bar{x}_{n+1}$ on lahend ja $b_n \equiv \ldots \equiv b_1 \equiv 0 \pmod{p}$, saame siit

$$b_0(x_{n+1} - x_1) \ldots (x_{n+1} - x_n) \equiv f(x_{n+1}) \equiv 0 \pmod{p},$$

millest järeldub, et $b_0 \equiv 0 \pmod{p}$. Tulemus on aga vastuolus eeldusega, et kongruentsi aste on n, s.t. et $b_0 = a_0 \not\equiv 0 \pmod{p}$.

Järeldus. Kui algarvulise mooduli korral kongruentsi lahendite arv ületab kongruentsi kõrgeima liikme astme, siis on selles kongruentsis esineva polünoomi kordajad kõik kongruentsed nulliga modulo p.

Tõepoolest, kuna a_i avaldub kordajate b_j lineaarse kombinatsioonina ja $b_j \equiv 0 \pmod{p}$ iga j korral, siis ka $a_i \equiv 0 \pmod{p}$ iga i korral.

Teoreem 6.6 (Wilson). Naturaalarv $p \neq 1$ on algarv pa-

rajasti siis, kui

(6) $$(p-1)! \equiv -1 \pmod{p}.$$

Tõestus. Tarvilikkus. Olgu p algarv. Võtame kongruentsi

$$(x-1)(x-2) \ldots [x - (p-1)] - (x^{p-1} - 1) \equiv 0 \pmod{p}.$$

Selle kongruentsi aste on ülimalt p-2, sest astmed x^{p-1} korrutises ja lahutatavas polünoomis koonduvad. Samal ajal rahuldavad kongruentsi arvud 1, 2, 3, ..., p-1, mis kuuluvad kõik erinevatesse jäägiklassidesse mod p. Tõepoolest, need arvud muudavad nulliks korrutise ja rahuldavad Euleri teoreemi põhjal kongruentsi

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

sest nad on mooduliga ühistegurita. Et lahendite arv ületab kongruentsi kõrgeima liikme astme, siis on kõik kordajad kongruentsed nulliga. Eriti on kongruentne nulliga vabaliige, s.o.

$$(p-1)! + 1 \equiv 0 \pmod{p}.$$

Piisavus. Kehtigu konguents

$$(p-1)! \equiv -1 \pmod{p},$$

kusjuures oletame, et p on kordarv. Siis on tal aga jagaja d, $1 < d < p$, mis on üks arvudest 2, 3, ..., p-1. Et vasak pool ja moodul jaguvad d-ga, siis peab viimasega jaguma ka kongruentsi parem pool, mis on aga võimatu. Järelikult on p algarv.

Teoreetilisslt saab teoreemi abil kindlaks teha, kas antud arv on alg- või kordarv. Praktilisslt nõuab see aga vähegi suuremate arvude korral tohutuid arvutusi.

Kui n-astme kongruentsil

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n \equiv 0 \pmod{p}$$

on n lahendit, siis võib teda esitada kujul

$$a_0(x-x_1)(x-x_2) \ldots (x-x_n) \equiv 0 \pmod{p}.$$

Tõepoolest, kuna võrduses (5) on $b_1 \equiv b_2 \equiv \ldots \equiv b_n \equiv 0 \pmod{p}$ ja $b_0 = a_0$, siis saamegi märgitud kuju.

Kõrgema astme kongruentside lahendamiseks ei ole üldist meetodit. Algarvulise mooduli korral leitakse lahendid proovimise teel. Kordarvulise mooduli korral taandub lahendamine algarvuliste moodulitega kongruentside lahendamisele.

Harjutusülesandeid.

6.11. Lahendada järgmised kongruentsid, alandades eelnevalt nende astet:

a) $x^5 - 2x^3 + x^2 - 2 \equiv 0 \pmod{3}$;

b) $x^7 - x^6 + 5x^2 - 3 \equiv 0 \pmod{5}$;

c) $x^{10} + x^8 + x^7 - x^4 - x^2 + 4x - 3 \equiv 0 \pmod{7}$;

d) $x^{12} - 2x^7 + x^3 + 1 \equiv 0 \pmod{5}$;

e) $x^{101} + 3x^{15} + x^{11} - 3x^5 + 9x^2 + 10x - 5 \equiv 0 \pmod{11}$;

f) $2x^{35} - 17x^{15} + 13x^8 - 3x^5 + 12x + 5 \equiv 0 \pmod{11}$.

§ 5. KONGRUENTSID KORDARVULISE MOODULI JÄRGI

1. Kongruentsi asendamine süsteemiga. Vaatleme n-astme kongruentsi

(1) $$f(x) \equiv 0 \pmod{m}$$

lahendamist, kus mooduli m kanooniline kuju on

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

Tähistame $p_i^{\alpha_i} = m_i$. Siis $(m_i, m_j) = 1$ ja kongruents (1) on esitatav kujul

$$f(x) \equiv 0 \pmod{m_1 m_2 \dots m_n}. \tag{2}$$

Teoreem 6.7. Kongruents (2) on ekvivalentne kongruentside süsteemiga

$$\begin{aligned} f(x) &\equiv 0 \pmod{m_1}, \\ f(x) &\equiv 0 \pmod{m_2}, \\ &\dots\dots\dots \\ f(x) &\equiv 0 \pmod{m_n}, \end{aligned} \tag{3}$$

s.t. neid rahuldavate arvude hulgad ühtivad.

Tõestus. Kui x rahuldab süsteemi (3), siis teoreemi 5.14 kohaselt on rahuldatud ka kongruents (2). Vastupidi, kui x rahuldab kongruentsi (2), siis teoreemi 5.15 tõttu rahuldab x süsteemi (3) kõiki kongruentse. Teoreem on tõestatud.

Eeldades, et oleme leidnud süsteemi (3) üksikute kongruentside lahendid, avaldame süsteemi (3) ja sellega ka kongruentsi (2) lahendid. Olgu süsteemi (3) esimese kongruentsi lahenditeks

$$x \equiv x_1^{(1)}, x_1^{(2)}, \dots, x_1^{(k_1)} \pmod{m_1},$$

teise lahenditeks

$$x \equiv x_2^{(1)}, x_2^{(2)}, \dots, x_2^{(k_2)} \pmod{m_2},$$

. . . . . .

n-nda kongruentsi lahenditeks

$$x \equiv x_n^{(1)}, x_n^{(2)}, \dots, x_n^{(k_n)} \pmod{m_n}.$$

Võtame esimese kongruentsi lahendite hulgast lahendi

$x \equiv x_1^{(i_1)} \pmod{m_1}$, teise kongruentsi lahendite hulgast lahendi $x \equiv x_2^{(i_2)} \pmod{m_2}$, ..., n-nda kongruentsi lahendite hulgast lahendi $x \equiv x_n^{(i_n)} \pmod{m_n}$. Saame lineaarse süsteemi

$$(4)\qquad \begin{aligned} x &\equiv x_1^{(i_1)} \pmod{m_1},\\ x &\equiv x_2^{(i_2)} \pmod{m_2},\\ &\cdots\cdots\cdots\\ x &\equiv x_n^{(i_n)} \pmod{m_n}, \end{aligned}$$

mille lahend ühtib süsteemi (3) ja seega ka kongruentsi (2) ühe lahendiga. Teoreemi 6.3 kohaselt on nimetatud lahendiks

$$(5)\qquad x \equiv M_1M_1' x_1^{(i_1)} + \ldots + M_nM_n' x_n^{(i_n)} \pmod{m},$$

kus $M_im_i = m$ ja $M_iM_i' \equiv 1 \pmod{m_i}$.

Teeme kindlaks kongruentsi (2) lahendite arvu mooduli m järgi. Kui muutuks vaid i_1, siis oleks lahendeid k_1. Kui muutuks veel vaid i_2, saaksime k_1k_2 lahendit, jne. Üldiselt saame mooduli m järgi

$$k = k_1k_2 \ldots k_n$$

lahendit. Eeldame, et $k > 1$ ja näitame, et need lahendid on kõik üksteisest erinevad. Võtame veel lahendi

$$x \equiv M_1M_1' x_1^{(j_1)} + \ldots + M_nM_n' x_n^{(j_n)} \pmod{m},$$

mille kohta üldsust kitsendamata võime eeldada, et näiteks $i_1 \neq j_1$. Oletame, et need lahendid ühtivad, s.t.

$$M_1M_1' x_1^{(i_1)} + \ldots + M_nM_n' x_n^{(i_n)} \equiv$$
$$\equiv M_1M_1' x_1^{(j_1)} + \ldots + M_nM_n' x_n^{(j_n)} \pmod{m}.$$

Teoreemi 5.15 tõttu kehtib siis see kongruents ka mooduli m_1 järgi. Arvestades aga, et $M_i \equiv 0 \pmod{m_1}$, kui $i > 1$, saame

$$M_1 M_1' x_1^{(i_1)} \equiv M_1 M_1' x_1^{(j_1)} \pmod{m_1}$$

ja $M_1 M_1' \equiv 1 \pmod{m_1}$ tõttu

$$x_1^{(i_1)} \equiv x_1^{(j_1)} \pmod{m_1},$$

mis on vastuolus eeldusega.

2. Kongruents algarvu astme järgi. Nagu nägime, taandub kongruentsi lahendamine mistahes mooduli m järgi kongruentside

(6) $$f(x) \equiv 0 \pmod{p^\alpha}$$

lahendamisele. Kongruentsi (6) lahendamiseks lähtume kongruentsist

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

Iga x, mis rahuldab kongruentsi (6), rahuldab ka kongruentsi (7), vastupidine väide üldiselt ei kehti.

Leiame (näiteks proovimise teel) kongruentsi (7) kõik lahendid. Olgu üheks lahendiks

$$x \equiv x_1 \pmod{p},$$

s.t. $x = x_1 + pt$ rahuldab kongruentsi (7) iga täisarvu t korral. Asendame $x = x_1 + pt$ kongruentsis

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

ja lahendame saadud kongruentsi

(9) $$f(x_1 + pt) \equiv 0 \pmod{p^2}$$

t suhtes. $f(x_1 + pt)$ on t suhtes täisarvuliste kordajatega polünoom. Arendades ta Taylori ritta kohal x_1, saame kongruent-

entsi (9) kirjutada kujul

$$f(x_1) + f'(x_1)pt + \frac{1}{2!} f''(x_1)p^2t^2 + \ldots \equiv 0 \pmod{p^2}$$

ehk

$$f(x_1) + f'(x_1)pt \equiv 0 \pmod{p^2}, \tag{10}$$

sest $p^k \equiv 0 \pmod{p^2}$, kui $k \geqslant 2$, ja $\frac{1}{k!} f^{(k)}(x_1)$ on täisarv.

Et $x \equiv x_1 \pmod{p}$ on kongruentsi (7) lahend, siis $f(x_1) \vdots p$. Seega jagades kongruentsi (10) mõlemaid pooli ja moodulit ühise teguriga p, saame (10)-ga ekvivalentse kongruentsi

$$\frac{f(x_1)}{p} + f'(x_1)t \equiv 0 \pmod{p}. \tag{11}$$

Eeldame, et $f'(x_1) \not\equiv 0 \pmod{p}$. Siis $(f'(x_1), p)=1$ ja lineaarkongruentsil (11) on parajasti üks lahend. Olgu lahendiks

$$t \equiv t_1 \pmod{p} \quad \text{ehk} \quad t = t_1 + ps.$$

Siis kongruentsi (7) rahuldavatest arvudest $x = x_1 + pt$ rahuldavad kongruentsi (8) iga s korral arvud $x = x_1 + p(t_1 + ps) = x_2 + p^2s$, kus $x_2 = x_1 + pt_1$.

Edasi vaatleme juba kongruentsi

$$f(x) \equiv 0 \pmod{p^3}. \tag{12}$$

Selle lahendamiseks tuleb leida s väärtused, mis rahuldavad kongruentsi

$$f(x_2 + p^2s) \equiv 0 \pmod{p^3}.$$

Taylori valemi abil saame nagu ennegi viimase kongruentsi asendada ekvivalentse kongruentsiga

$$f(x_2) + f'(x_2)p^2s \equiv 0 \pmod{p^3}. \tag{13}$$

Et x_2 on kongruentsi (8) lahend, siis $f(x_2) \vdots p^2$ ja kongru-

entsi (13) saame asendada omakorda ekvivalentse kongruentsiga

$$\frac{f(x_2)}{p^2} + f'(x_2)s \equiv 0 \pmod{p}. \tag{14}$$

Eelduse kohaselt $f'(x_1) \not\equiv 0 \pmod{p}$. Et $x_2 \equiv x_1 \pmod{p}$ ja seega $f'(x_2) \equiv f'(x_1) \pmod{p}$, siis ka $f'(x_2) \not\equiv 0 \pmod{p}$. Seetõttu on lineaarkongruents (14) s suhtes üheselt lahenduv. Olgu selle lahendiks $s \equiv s_1 \pmod{p}$ ehk $s = s_1 + pu$. Siis kongruentsi (12) rahuldavad iga u korral x väärtused

$$x = x_2 + p^2(s_1 + pu) = x_3 + p^3u,$$

s.t. kongruentsi (12) lahendiks on

$$x \equiv x_3 \pmod{p^3},$$

kus $x_3 = x_2 + p^2s_1$. Nii jätkates saame kongruentsi (6) lahendi.

Eelnevast mõttekäigust järeldub, et kui kongruentsil (7) on k lahendit mod p ja iga lahendi x_1 korral $f'(x_1) \not\equiv 0 \pmod{p}$, siis ka kongruentsil (6) on k lahendit.

Näide. Lahendame kongruentsi

$$f(x) = x^3 + x^2 + 2 \equiv 0 \pmod{343}.$$

Arvestades, et $343 = 7^3$, leiame kõigepealt proovimismeetodil kongruentsi $f(x) \equiv 0 \pmod{7}$ lahendid. Viimase kongruentsi ainsaks lahendiks on $x \equiv 2 \pmod{7}$. Kuna $f'(x) = 3x^2 + 2x$ ja $f'(2) \not\equiv 0 \pmod{7}$, siis ka lähtekongruentsil on parajasti üks lahend. Selle saamiseks leiame järgmisel sammul kongruentsi $f(x) \equiv 0 \pmod{7^2}$ lahendi. Selleks lahendame t suhtes kongruentsi (11) ehk

$$2 + 16t \equiv 0 \pmod{7}.$$

Lahendiks saame

$$t \equiv -1 \pmod 7 \quad \text{ehk} \quad t = -1 + 7s.$$

Siis aga $x = 2 + 7t = -5 + 49s$. Edasi lahendame s suhtes kongruentsi (14) ehk

$$-2 + 65s \equiv 0 \pmod 7,$$

millest

$$s \equiv 1 \pmod 7 \quad \text{ehk} \quad s = 1 + 7u.$$

Seega esialgse kongruentsi lahendiks on

$$x = -5 + 49(1 + 7u) = 44 + 343u$$

ehk

$$x \equiv 44 \pmod{343}.$$

Harjutusülesandeid.

6.12. Lahendada järgmised kongruentsid:

a) $6x^3 - 3x^2 - 13x - 10 \equiv 0 \pmod{30}$;

b) $x^5 + x^4 + 7x^3 + 6x^2 + 5x + 1 \equiv 0 \pmod{420}$;

c) $x^3 + x + 3 \equiv 0 \pmod{125}$;

d) $x^3 + x^2 + 2 \equiv 0 \pmod{7^4}$;

e) $4x^3 + 7x^2 - 7x - 10 \equiv 0 \pmod{225}$;

f) $x^3 + x^2 + x + 1 \equiv 0 \pmod{2^2.3^3.5^2}$.

VII. RUUTKONGRUENTSID

§1. RUUTJÄÄGID

Ruutkongruentsid on mittelineaarsete kongruentside lihtsaimaks erijuhuks. Ruutkongruentsi jaoks on olemas lahendusalgoritmid, mis ei nõua kõigi jäägiklasside läbiproovimist. Samuti on võimalik juba enne lahendamisele asumist kindlaks määrata, kas antud ruutkongruents on lahenduv või mitte. Vaatleme kaheliikmelist kongruentsi

$$x^n \equiv a \pmod{m}, \quad (a, m) = 1.$$

Kui sellel kongruentsil on olemas lahend, siis arvu a nimetatakse n-astme jäägiks mooduli m järgi, vastasel juhul nimetatakse arvu a n-astme mittejäägiks. Kui n = 2, siis räägime ruutjäägist ja mitteruutjäägist.

Käesolevas paragrahvis vaatlemegi juhtu, kus n = 2. Siinjuures eeldame, et moodul on paaritu algarv (juhtu, kus p = 2, vaatleme 4. paragrahvis). Seega käsitleme kongruentse

$$x^2 \equiv a \pmod{p}, \quad (a, p) = 1, \quad p \neq 2. \tag{1}$$

Sellisele kongruentsile saab taandada ka üldise ruutkongruentsi

$$bx^2 + cx + d \equiv 0 \pmod{p}, \quad (b, p) = 1.$$

Tõepoolest, korrutades viimast kongruentsi teguriga 4b, saame

$$4b^2x^2 + 4bcx + 4bd \equiv 0 \pmod{p}$$

ehk

$$(2bx + c)^2 \equiv c^2 - 4bd \pmod{p}.$$

Olles tähistanud $y = 2bx + c$ ja $a = c^2 - 4bd$, jõuame kongruentsini

$$y^2 \equiv a \pmod{p}.$$

Lähtekongruentsi lahendi saame sel teel, et leiame viimase kongruentsi lahendi $y \equiv y_0 \pmod{p}$ ja lahendame x suhtes lineaarkongruentsi

$$2bx \equiv y_0 - c \pmod{p}.$$

Mooduli p järgi on erinevaid ruutkongruentse kujul (1) arvult p. Näiteks, kui $p = 5$, siis saame järgmised kongruentsid:

$$x^2 \equiv -2 \pmod{5},$$
$$x^2 \equiv -1 \pmod{5},$$
$$x^2 \equiv 0 \pmod{5},$$
$$x^2 \equiv 1 \pmod{5},$$
$$x^2 \equiv 2 \pmod{5}.$$

Kõik teised taanduvad nendeks.

Kuna me eeldame, et $(a, p) = 1$, siis jääb vaatluse alt välja kongruents $x^2 \equiv 0 \pmod{p}$, millel on parajasti üks lahend $x \equiv 0 \pmod{p}$ ja mis seetõttu lahendamise seisukohalt edasist huvi ei paku.

Märgime, et kui $x \equiv x_1 \pmod{p}$ on kongruentsi (1) lahend, siis $(x_1, p) = 1$. Tõepoolest, siis $x_1^2 \equiv a \pmod{p}$. Kui oleks $(x_1, p) = p$, siis oleks ka $(a, p) = p$, s.t. $a \equiv 0 \pmod{p}$, mis oleks vastuolus eeldusega.

Teoreem 7.1. Kui a on ruutjääk mod p, siis on kongruentsil (1) parajasti kaks lahendit.

Tõestus. Kui a on ruutjääk, siis kongruentsil (1) on vähemalt üks lahend

$$x \equiv x_1 \pmod{p}.$$

Kuid, et $(-x_1)^2 = x_1^2$, siis on sellel kongruentsil ka lahend

$$x \equiv -x_1 \pmod{p}.$$

Need lahendid on erinevad, sest kui oleks

$$x_1 \equiv -x_1 \pmod{p},$$

siis saaksime, et

$$2x_1 \equiv 0 \pmod{p},$$

mis on aga võimatu, sest $(2, p) = (x_1, p) = 1$. Näidatud kahe lahendiga on ammendatud kõik lahendid, sest teoreemi 6.5 põhjal ei saa teise astme kongruentsil algarvulise mooduli järgi olla üle kahe lahendi.

Leidub ruutkongruentse, millel pole ühtki lahendit. Vaatleme näiteks kongruentse

$$x^2 \equiv -2 \pmod{5},$$

$$x^2 \equiv -1 \pmod{5},$$

$$x^2 \equiv 1 \pmod{5},$$

$$x^2 \equiv 2 \pmod{5}.$$

Lahenditena tulevad kõne alla jäägiklassid, mille esindajateks on taandatud jääkide süsteemi elemendid

$$-2, -1, 1, 2.$$

Nimetatud arvude ruudud on

$$4, 1, 1, 4,$$

mis on mooduli 5 järgi kongruentsed vastavalt arvudega

$$-1, 1, 1, -1.$$

Seega kongruentsid

$$x^2 \equiv -1, \quad x^2 \equiv 1 \pmod{5}$$

on lahenduvad, kusjuures esimese lahenditeks on $x \equiv -2$ ja

$x \equiv 2 \pmod 5$, teise lahenditeks on $x \equiv -1$ ja $x \equiv 1 \pmod 5$. Kongruentsid

$$x^2 \equiv -2, \quad x^2 \equiv 2 \pmod 5$$

pole aga lahenduvad. Seega modulo 5 on taandatud jääkide süsteemis kaks ruutjääki (-1 ja 1) ning kaks mitteruutjääki (-2 ja 2).

Teise näitena võtame jäägiklassid, mis vastavad taandatud jääkide süsteemile modulo 11:

$$x \equiv -5, -4, -3, -2, -1, 1, 2, 3, 4, 5 \pmod{11}.$$

Siis

$$x^2 \equiv 1, 4, 9, 16, 25 \pmod{11}$$

ehk

$$x^2 \equiv 1, 4, -2, 5, 3 \pmod{11}.$$

Seega lahenduvad on viis kongruentsi:

$$x^2 \equiv -2, 1, 3, 4, 5 \pmod{11},$$

mittelahenduvad samuti viis kongruentsi:

$$x^2 \equiv -5, -4, -3, -1, 2 \pmod 5.$$

Teoreem 7.2. Taandatud jääkide süsteemis paaritu algarvulise mooduli p järgi on olemas $\frac{p-1}{2}$ ruutjääki ja $\frac{p-1}{2}$ mitteruutjääki. Ruutjäägid on modulo p kongruentsed arvudega

$$1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2. \tag{2}$$

Tõestus. Igas taandatud jääkide süsteemis modulo p on ruutjääkideks parajasti need arvud, mis on kongruentsed taandatud jääkide süsteemi

$$-\frac{p-1}{2}, \ldots, -2, -1, 1, 2, \ldots, \frac{p-1}{2} \tag{3}$$

elementide ruutudega, s.o. arvudega (2). Niisiis tarvitseb

näidata, et arvude (2) seas pole omavahel kongruentseid modulo p. Kui oleks

$$k^2 \equiv l^2 \pmod{p}, \quad 0 < k < l \leq \frac{p-1}{2},$$

siis oleks ruutkongruentsil

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

neli erinevat lahendit: $x \equiv -l, l, -k, k \pmod{p}$, mida ei saa olla. Teoreem on tõestatud.

Seega ruutkongruentsil $x^2 \equiv a \pmod{p}$, $(a, p) = 1$, on kas kaks lahendit või pole ühtki.

Teoreem 7.3. Arv a, mis on ühistegurita paaritu algarvulise mooduliga p, on ruutjääk parajasti siis, kui

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p} \tag{4}$$

ja mitteruutjääk parajasti siis, kui

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}. \tag{5}$$

Tõestus. Euleri teoreemi kohaselt

$$(a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) = a^{p-1} - 1 \equiv 0 \pmod{p}.$$

Et tegurid

$$a^{\frac{p-1}{2}} - 1 \quad \text{ja} \quad a^{\frac{p-1}{2}} + 1$$

erinevad teineteisest vaid 2 võrra, siis sellest, et nende korrutis jagub p-ga, järeldub $p \neq 2$ tõttu, et parajasti üks teguritest jagub p-ga. Seega kehtib iga a korral, kus $(a, p) = 1$, parajasti üks kongruentsidest (4), (5). Edasi tarvitseb tõestada, et a on ruutjääk parajasti siis, kui kehtib tingimus (4).

Tarvilikkus. Olgu a ruutjääk modulo p. See tähendab,

et leidub täisarv x, nii et

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

Võtame kongruentsi mõlemad pooled astmesse $\frac{p-1}{2}$. Saame

$$x^{p-1} \equiv a^{\frac{p-1}{2}} \pmod{p}. \tag{6}$$

Et aga $(x, p) = 1$ ja Euleri teoreemi järgi

$$x^{p-1} \equiv 1 \pmod{p},$$

siis seosest (6) järeldubki (4).

Piisavus. Olgu täidetud tingimus (4). Vaatleme kongruentsi

$$z^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p}, \tag{7}$$

millel ei saa olla rohkem kui $\alpha = \frac{p-1}{2}$ lahendit. Tingimuse (4) tõttu rahuldab kongruentsi arv a. Näitame, et kõik kongruentsi (7) rahuldavad arvud on ruutjäägid modulo p. Kui nii, siis on ka a ruutjääk.

Ruutjääkide $r_1, r_2, \ldots, r_\alpha$ $(\alpha = \frac{p-1}{2})$ jaoks leiduvad taandatud jääkide süsteemis arvud $x_1, x_2, \ldots, x_\alpha$, nii et kehtivad kongruentsid

$$x_1^2 \equiv r_1 \pmod{p},$$
$$x_1^2 \equiv r_2 \pmod{p},$$
$$\ldots\ldots\ldots$$
$$x_\alpha^2 \equiv r_\alpha \pmod{p}.$$

Tõstes kõik kongruentsid astmesse $\alpha = \frac{p-1}{2}$ ja arvestades Euleri teoreemi, saame

$$r_1^{\alpha} \equiv x_1^{p-1} \equiv 1 \pmod{p},$$
$$r_2^{\alpha} \equiv x_2^{p-1} \equiv 1 \pmod{p},$$
$$\cdots\cdots\cdots\cdots$$
$$r_{\alpha}^{\alpha} \equiv x_{\alpha}^{p-1} \equiv 1 \pmod{p}$$

ehk

$$r_1^{\alpha} - 1 \equiv 0 \pmod{p},$$
$$r_2^{\alpha} - 1 \equiv 0 \pmod{p},$$
$$\cdots\cdots\cdots\cdots$$
$$r_{\alpha}^{\alpha} - 1 \equiv 0 \pmod{p}.$$

Seega kõik ruutjäägid modulo p rahuldavad kongruentsi (7). Et aga lahendite jäägiklasse ja ruutjääke on ühepalju, siis ka vastupidi, iga lahend on ruutjääk. Järelikult on a ruutjääk.

Harjutusülesandeid.

7.1. Vaadelda kõiki kongruentse kujul $x^2 \equiv a \pmod{p}$

a) p = 13 korral,

b) p = 17 korral

ja teha kindlaks, millised neist on lahenduvad, millised mitte. Leida vastavad lahendid.

7.2. Teoreemi 7.3 alusel kontrollida, millised arvudest 3, 5, 7, 11 on ruutjäägid

a) modulo 19,

b) modulo 17.

§ 2. LEGENDRE'I JA JACOBI SÜMBOLID

1. Legendre'i sümbol ja selle omadused. Tõestame kõigepealt järgnevas vajamineva abitulemuse.

Lemma. Kui $\varepsilon \equiv \eta \pmod p$, $p \neq 2$ ja $|\varepsilon| = |\eta| = 1$, siis $\varepsilon = \eta$.

Tõestus. Kui lemma eeldustel oleks $\varepsilon \neq \eta$, siis kongruents $\varepsilon \equiv \eta \pmod p$ tähendaks, et $1 \equiv -1$ ehk $2 \equiv 0 \pmod p$, mis on võimatu, kui $p \neq 2$.

Käesolevas paragrahvis tuletame praktilise võtte ruutjääkide kindlakstegemiseks suurte moodulite korral (teoreemi 7.3 abil on ruutjääkide leidmine suhteliselt tülikas). Selleks lahendame teistsuguse probleemi: teeme kindlaks, milliste moodulite p korral on kongruents

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

lahenduv, kui a on antud arv.

Viimase probleemi lahendamine nõuab üsna suurt eeltööd. Sealjuures kasutame nn. Legendre'i sümbolit $\left(\frac{a}{p}\right)$, mis defineeritakse juhul, kui p on paaritu algarv ja $(a, p) = 1$. Sümbolit $\left(\frac{a}{p}\right)$ loetakse "a p suhtes".

Definitsioon:

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

Vaatleme Legendre'i sümboli o m a d u s i.

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

Tõepoolest, kui a on ruutjääk, siis $a^{\frac{p-1}{2}} \equiv 1 \pmod p$;

kui a on mitteruutjääk, siis $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

2) Kui $a \equiv b \pmod{p}$, siis $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

Tõepoolest, kui a on ruutjääk, siis ka kõik teised sama jäägiklassi elemendid on ruutjäägid, ja vastupidi, kui a pole ruutjääk, siis ei saa ruutjääk olla ka ükski teine sama jäägiklassi element.

3) Legendre'i sümbol on tugevalt multiplikatiivne, s.t.

$$\left(\frac{a_1 a_2 \cdots a_n}{p}\right) = \left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right) \cdots \left(\frac{a_n}{p}\right) \quad ((a_1, p) = 1).$$

Tõestuseks kasutame omadust 1:

$$\left(\frac{a_1 a_2 \cdots a_n}{p}\right) = (a_1 a_2 \cdots a_n)^{\alpha} = a_1^{\alpha} a_2^{\alpha} \cdots a_n^{\alpha} \equiv$$
$$\equiv \left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right) \cdot \ldots \cdot \left(\frac{a_n}{p}\right) \pmod{p}.$$

Saadud kongruentsist järeldub võrdus käesoleva punkti alguses toodud lemma põhjal.

4) Kehtib võrdus $\left(\frac{b^2}{p}\right) = 1$.

Viimane omadus järeldub sellest, et b^2 on alati ruutjääk. Võib aga kasutada eelmist omadust:

$$\left(\frac{b^2}{p}\right) = \left(\frac{b}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{b}{p}\right)^2 = (\pm 1)^2 = 1.$$

5) Kehtib valem $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$,

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

2. <u>Tarvilik ja piisav tingimus selleks, et arv -1 oleks ruutjääk</u>. Küsimusele, mille püstitasime eelmise punk-

ti algul, saame nüüd vastata a = -1 korral. Niisiis teeme kindlaks, milliste algarvuliste moodulite p korral on kongruents

$$x^2 \equiv -1 \pmod{p}$$

lahenduv. Selleks arvutame Legendre'i sümboli $\left(\frac{-1}{p}\right)$ väärtuse. 1. omaduse põhjal

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

Lemma põhjal järeldub siit võrdus

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

Viimasest võrdusest näeme, et -1 on ruutjääk parajasti siis, kui $\frac{p-1}{2} = 2n$ ehk algarv p on kujuga $p = 4n + 1$, ja mitteruutjääk parajasti siis, kui $\frac{p-1}{2} = 2n - 1$ ehk algarv p on kujuga $p = 4n - 1$. Teisiti öeldes, ruutkongruents

$$x^2 \equiv -1 \pmod{p} \quad \text{ehk} \quad x^2 + 1 \equiv 0 \pmod{p}$$

on lahenduv parajasti siis, kui algarv p avaldub kujul $p = 4n + 1$. Ühtlasi järeldub siit, et arvu $x^2 + 1$ algarvulisteks jagajateks saavad olla vaid algarvud kujuga $p = 4n + 1$ ja arv 2. Tõepoolest, algarvulise mooduli $4n - 1$ puhul ei kehti kongruents

$$x^2 + 1 \equiv 0 \pmod{4n-1}$$

ühegi arvu x korral.

3. Gaussi lemma. Uurime edasi kongruentsi

$$x^2 \equiv a \pmod{p}, \quad (a, p) = 1$$

lahenduvust sõltuvalt moodulist p.

Koostame kongruentsid modulo p:

$$
\begin{aligned}
a &\equiv \varepsilon_1 r_1 , \\
2a &\equiv \varepsilon_2 r_2 , \\
3a &\equiv \varepsilon_3 r_3 , \\
&\cdots\cdots \\
\alpha a &\equiv \varepsilon_\alpha r_\alpha \qquad (\alpha = \tfrac{p-1}{2}),
\end{aligned} \tag{1}
$$

kus paremad pooled $\varepsilon_i r_i$ on absoluutväärtuselt vähimad taandatud jääkide süsteemi elemendid, $\varepsilon_i = \pm 1$ olenevalt nimetatud jäägi märgist,

$$0 < r_1 \leq \frac{p-1}{2} .$$

Näitame, et jääkide r_i seas ei saa olla võrdseid arve. Kui oleks

$$r_i = r_j ,$$

siis kongruentsidest

$$ia \equiv \varepsilon_i r_i \pmod p ,$$

$$ja \equiv \varepsilon_j r_j = \varepsilon_j r_i \pmod p$$

saaksime

$$ia\varepsilon_i \equiv r_i \pmod p ,$$

$$ja\varepsilon_j \equiv r_i \pmod p$$

ehk

$$ia\varepsilon_i \equiv ja\varepsilon_j \pmod p \text{ ehk } i\varepsilon_i \equiv j\varepsilon_j \pmod p .$$

Et $\varepsilon_i = \pm 1$ ja $\varepsilon_j = \pm 1$, siis viimase kongruentsi tõttu peaks avaldis $\pm i \pm j$ jaguma mooduliga p, mis on aga võimatu, sest $i \neq j$ ja $0 < i + j < p$. Seega on $r_1, r_2, \ldots, r_\alpha$ mingi permutatsioon arvudest $1, 2, \ldots, \alpha$. Korrutame kõik kongruentsid (1) omavahel läbi. Saame

$$a^\alpha \cdot \alpha! \equiv E \cdot \alpha! \pmod p ,$$

kus

(2) $$E = \varepsilon_1 \varepsilon_2 \dots \varepsilon_\alpha = \pm 1.$$

Siit

$$a^\alpha \equiv E \pmod p$$

ehk

$$\left(\frac{a}{p}\right) \equiv E \pmod p.$$

Punktis 1 esitatud lemma põhjal saame siit võrduse. Seega jõudsime järgmise tulemuseni.

Teoreem 7.4 (Gaussi lemma). Kehtib valem

(3) $$\left(\frac{a}{p}\right) = E,$$

kus E on defineeritud võrdusega (2).

Anname E avaldisele teise kuju. Selleks lähtume seosest

$$\frac{ia}{p} = \left[\frac{ia}{p}\right] + \left\{\frac{ia}{p}\right\} \quad (i = 1, 2, \dots,),$$

korrutame seda kahega ja võtame täisosa:

(4) $$\left[\frac{2ia}{p}\right] = \left[2\left[\frac{ia}{p}\right] + 2\left\{\frac{ia}{p}\right\}\right] = 2\left[\frac{ia}{p}\right] + \left[2\left\{\frac{ia}{p}\right\}\right].$$

Edasi arvestame ε_i definitsiooni. Kui $\varepsilon_i = 1$, s.t. kui ia vähim positiivne jääk modulo p on väiksem kui $\frac{1}{2}p$, siis $\left[\frac{2ia}{p}\right]$ on paarisarv $\left(\left\{\frac{ia}{p}\right\} < \frac{1}{2}$ ja võrduse (4) paremal poolel $\left[2\left\{\frac{ia}{p}\right\}\right] = 0\right)$. Seega võime kirjutada

(5) $$\varepsilon_i = (-1)^{\left[\frac{2ia}{p}\right]}.$$

Kui $\varepsilon_i = -1$, siis arvu ia vähim p o s i t i i v n e jääk modulo p on suurem kui $\frac{1}{2}p$ ja $\left[\frac{2ia}{p}\right]$ on paaritu arv $\left(\left\{\frac{ia}{p}\right\} > \frac{1}{2}$ ja $\left[2\left\{\frac{ia}{p}\right\}\right] = 1\right)$. Seetõttu kehtib võrdus (5) ka antud juhul ja järelikult on valem (5) õige iga i korral. Gaussi lemma

tõttu saame nüüd seose

$$(6) \qquad \left(\frac{a}{p}\right) = \left(-1\right)^{\sum_{i=1}^{\alpha}\left[\frac{2ia}{p}\right]} \qquad (\alpha = \tfrac{p-1}{2}).$$

4. <u>Tarvilik ja piisav tingimus selleks, et arv 2 oleks ruutjääk</u>. Olgu a paaritu arv, siis a+p on paarisarv. Valemi (6) põhjal

$$\left(\frac{2a}{p}\right) = \left(\frac{2a+2p}{p}\right) = \left(\frac{4 \cdot \frac{a+p}{2}}{p}\right) = \left(\frac{\frac{a+p}{2}}{p}\right) =$$

$$= \left(-1\right)^{\sum_{i=1}^{\alpha}\left[\frac{i(a+p)}{p}\right]} = \left(-1\right)^{\sum_{i=1}^{\alpha}\left[\frac{ia}{p}\right] + \sum_{i=1}^{\alpha} i}$$

ehk teisiti

$$(7) \qquad \left(\frac{2}{p}\right)\left(\frac{a}{p}\right) = \left(-1\right)^{\sum_{i=1}^{\alpha}\left[\frac{ia}{p}\right] + \frac{p^2-1}{8}} .$$

Kui valemis (7) võtta a = 1, siis saame

$$(8) \qquad \left(\frac{2}{p}\right) = \left(-1\right)^{\frac{p^2-1}{8}} .$$

Nüüd võime otsustada, millise mooduli p korral on kongruents

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

lahenduv, millise korral mitte. Näiteks mooduli 13 puhul

$$\left(\frac{2}{13}\right) = \left(-1\right)^{\frac{168}{8}} = \left(-1\right)^{21} = -1 ,$$

mistõttu 2 ei ole ruutjääk modulo 13. Seega kongruents $x^2 \equiv 2 \pmod{13}$ pole lahenduv.

Selleks, et algarvu kuju järgi kindlaks teha, millise mooduli p korral on 2 ruutjääk, jaotame kõik paaritud arvud

nelja rühma: $8n \pm 1$, $8n \pm 3$. Arvutame

$$\left(\frac{2}{8n \pm 1}\right) = (-1)^{\frac{(8n \pm 1)^2-1}{8}} = (-1)^{8n^2 \pm 2n} = 1,$$

$$\left(\frac{2}{8n \pm 3}\right) = (-1)^{\frac{(8n \pm 3)^2-1}{8}} = (-1)^{8n^2 \pm 6n+1} = -1.$$

Seega, kui algarv p on kujuga $8n \pm 1$, on arv 2 ruutjääk, kui aga algarv p on kujuga $8n \pm 3$, siis arv 2 on mitteruutjääk.

Järeldus. Arvu $x^2 - 2$ paarituid algarvulisi jagajaid tuleb otsida vaid algarvude hulgast, millel on kuju $8n \pm 1$. Tõepoolest, ühegi arvu x korral ei kehti kongruents

$$x^2 \equiv 2 \pmod{8n \pm 3},$$

kui $8n \pm 3$ on algarv.

Ka arvu -2 kohta võime nüüd öelda, kas ta on antud algarvu p korral ruutjääk või mitte. Tõepoolest,

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\cdot\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2} + \frac{p^2-1}{8}} = (-1)^{\frac{(p+2)^2-9}{8}}.$$

Siit saame, et kui $p = 8n + 1$ või $p = 8n + 3$, siis -2 on ruutjääk, kui aga $p = 8n + 5$ või $8n + 7$, siis mitteruutjääk. Seega $x^2 + 2$ algteguriteks võivad olla vaid algarvud kujuga $p = 8n + 1$ või $p = 8n + 3$ ja arv 2.

5. Legendre'i sümboli pööratavus. Jagades võrduse (7) võrdusega (8), saame paaritu arvu a jaoks valemi

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{i=1}^{\alpha}\left[\frac{ia}{p}\right]}, \quad \text{kus } \alpha = \frac{p-1}{2}. \tag{9}$$

Olgu q paaritu algarv. Siis saame valemist (9) järgmised seosed:

$$\left(\frac{q}{p}\right) = \left(-1\right)^{\sum_{i=1}^{\alpha}\left[\frac{iq}{p}\right]}, \quad \alpha = \frac{p-1}{2},$$

$$\left(\frac{p}{q}\right) = \left(-1\right)^{\sum_{j=1}^{\beta}\left[\frac{jp}{q}\right]}, \quad \beta = \frac{q-1}{2}.$$

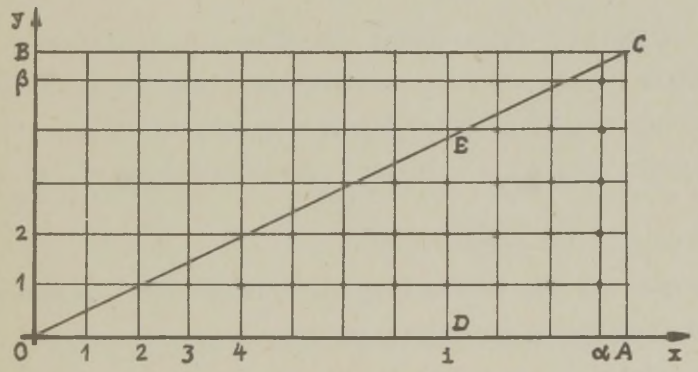
Korrutame saadud võrdused omavahel,

$$(10) \qquad \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \left(-1\right)^{\sum_{i=1}^{\alpha}\left[\frac{iq}{p}\right] + \sum_{j=1}^{\beta}\left[\frac{jp}{q}\right]},$$

ja tõestame, et

$$(11) \qquad \sum_{i=1}^{\alpha}\left[\frac{iq}{p}\right] + \sum_{j=1}^{\beta}\left[\frac{jp}{q}\right] = \alpha\beta = \frac{p-1}{2}\cdot\frac{q-1}{2}.$$

Selleks märgime xy-tasandil ära koordinaatide alguspunkti



O ja punktid $A\left(\frac{p}{2}, 0\right)$, $B\left(0, \frac{q}{2}\right)$, $C\left(\frac{p}{2}, \frac{q}{2}\right)$. Vaatleme sirget

$$y = \frac{qx}{p},$$

mis läbib punkte O ja C. Jagatis $\frac{iq}{p}$ võrdub sirge ordinaadiga kohal i, täisosa $\left[\frac{iq}{p}\right]$ aga lõigul DE asuvate sisemiste

täisarvuliste koordinaatidega punktide arvuga. Seega võrdub summa

$$\sum_{i=1}^{\alpha}\left[\frac{iq}{p}\right] = \left[\frac{q}{p}\right] + \left[\frac{2q}{p}\right] + \left[\frac{3q}{p}\right] + \ldots + \left[\frac{\alpha q}{p}\right]$$

kolmnurga OAC täisarvuliste koordinaatidega sisemiste punktide arvuga.

Vaadeldes samal viisil sirget $x = \frac{py}{q}$ veendume, et summa $\sum_{j=1}^{\beta}\left[\frac{jp}{q}\right]$ võrdub täisarvuliste koordinaatidega sisemiste punktide arvuga kolmnurgas OBC.

Kuna lõigul OC ei leidu täisarvuliste koordinaatidega sisemisi punkte, siis võrdub summa

$$\sum_{i=1}^{\alpha}\left[\frac{iq}{p}\right] + \sum_{j=1}^{\beta}\left[\frac{jp}{q}\right]$$

ristküliku OACB täisarvuliste koordinaatidega sisemiste punktide arvuga. Teiselt poolt on aga ristküliku OACB täisarvuliste koordinaatidega sisemiste punktide arv $\alpha\beta$. Seeka kehtib võrdus (11). Viimast arvestades saame valemi

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \left(-1\right)^{\frac{p-1}{2}\,\frac{q-1}{2}}. \tag{12}$$

Korrutame võrduse mõlemaid pooli teguriga $\left(\frac{p}{q}\right)$ ja esitame saadava tulemuse järgmise teoreemina.

Teoreem 7.5. Kehtib valem

$$\left(\frac{q}{p}\right) = \left(-1\right)^{\frac{p-1}{2}\,\frac{q-1}{2}}\left(\frac{p}{q}\right). \tag{13}$$

Valem (13) on tuntud ruutjääkide pööratavuse lause nime all. Pööratavuse lause koos Legendre'i sümboli teiste omadustega võimaldab sümboli väärtust arvutada iga algarvu-

lise nimetaja ja mistahes lugeja korral. Arvutuste lihtsustamiseks paneme veel tähele, et kui $p = 4n + 1$, siis $\frac{p-1}{2} = 2n$, kui aga $p = 4n + 3$, siis $\frac{p-1}{2} = 2n + 1$. Seega, kui vähemalt üks algarvudest p, q on kujuga $4n + 1$, on korrutis $\frac{p-1}{2} \cdot \frac{q-1}{2}$ paarisarv ja $(-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} = 1$; kui aga mõlemad algarvud on kujuga $4n + 3$, siis korrutis $\frac{p-1}{2} \cdot \frac{q-1}{2}$ on paaritu ja $(-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} = -1$. Niisiis juhul, kui $p \equiv 1 \pmod 4$ või $q \equiv 1 \pmod 4$ on $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$; kui aga $p \equiv q \equiv 3 \pmod 4$, siis $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$.

Näide 1. Teha kindlaks, kas kongruents $x^2 \equiv 97 \pmod{223}$ on lahenduv.

Et $97 \equiv 1 \pmod 4$, siis

$$\left(\frac{97}{223}\right) = \left(\frac{223}{97}\right).$$

Edasi $223 = 97 \cdot 2 + 29$. Seega

$$\left(\frac{223}{97}\right) = \left(\frac{29}{97}\right) = \left(\frac{10}{29}\right) = \left(\frac{2}{29}\right) \cdot \left(\frac{5}{29}\right).$$

Leiame, et $\left(\frac{2}{29}\right) = -1$, sest $29 \equiv -3 \pmod 8$; $\left(\frac{5}{29}\right) = \left(\frac{29}{5}\right) = \left(\frac{4}{5}\right) = 1$. Seega $\left(\frac{97}{223}\right) = -1$ ja vaadeldav ruutkongruents pole lahenduv.

Näide 2. Teha kindlaks, kas ruutkongruents $x^2 \equiv 265 \pmod{353}$ on lahenduv (353 on algarv).

Arvutame Legendre'i sümboli väärtuse:

$$\left(\frac{265}{353}\right) = \left(\frac{5}{353}\right) \cdot \left(\frac{53}{353}\right); \quad \left(\frac{5}{353}\right) = \left(\frac{353}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{2}{3}\right) = -1;$$

$$\left(\frac{53}{353}\right) = \left(\frac{353}{53}\right) = \left(\frac{35}{53}\right) = \left(\frac{5}{53}\right) \cdot \left(\frac{7}{53}\right);$$

$$\left(\frac{5}{53}\right) = \left(\frac{53}{5}\right) = \left(\frac{3}{5}\right) = -1; \quad \left(\frac{7}{53}\right) = \left(\frac{53}{7}\right) = \left(\frac{4}{7}\right) = 1.$$

Seega $\left(\frac{265}{353}\right) = 1$ ja kongruents on lahenduv.

6. Jacobi sümbol. Legendre'i sümboli väärtuse arvutamise ja seega kongruentsi

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

lahenduvuse üle otsustamise lihtsustamiseks kasutatakse Jacobi sümbolit. Jacobi sümbol on Legendre'i sümboli üldistuseks juhule, kus nimetaja ei ole algarv. Kui $P = p_1 p_2 \cdots p_n$, kus $p_1, p_2, \ldots, p_n$ on erinevad paaritud algarvud, ja $(a, P) = 1$, siis Jacobi sümbol $\left(\frac{a}{P}\right)$ (a P suhtes) defineeritakse võrdusega

$$\left(\frac{a}{P}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right) \cdots \left(\frac{a}{p_n}\right). \tag{14}$$

Märgime, et Jacobi sümboli võrdumisest -1-ga järeldub kongruentsi

$$x^2 \equiv a \pmod{P} \tag{15}$$

mittelahenduvus, kuid juhul, kui $\left(\frac{a}{P}\right) = 1$, jääb küsimus lahtiseks. Tõepoolest, kui $p_1, p_2, \ldots, p_n$ on erinevad algarvud, siis kongruents (15) on ekvivalentne süsteemiga

$$x^2 \equiv a \pmod{p_i}, \quad i=1,2,\ldots,n \tag{16}$$

ja võrdusest $\left(\frac{a}{P}\right) = -1$ järeldub, et vähemalt üks $\left(\frac{a}{p_i}\right) = -1$. Kui aga $\left(\frac{a}{P}\right) = 1$ ja $n > 1$, siis Legendre'i sümbolite $\left(\frac{a}{p_i}\right)$ seas võib ikkagi esineda neid, mis võrduvad -1-ga. Sel juhul on aga süsteem (16) ja koos sellega kongruents (15) mittelahenduvad.

Jacobi sümbolil on formaalselt samad omadused mis Legendre'i sümbolil. Järgnevas vaatlemegi Jacobi sümboli omadusi.

1) Kui $a \equiv b \pmod P$, siis $\left(\frac{a}{P}\right) = \left(\frac{b}{P}\right)$.

2) $\left(\frac{a^2}{P}\right) = 1$.

3) $\left(\frac{ab}{P}\right) = \left(\frac{a}{P}\right)\left(\frac{b}{P}\right)$, eriti $\left(\frac{a^2b}{P}\right) = \left(\frac{b}{P}\right)$.

Omadused 1 - 3 järelduvad Jacobi sümboli definitsioonist ja Legendre'i sümboli vastavaist omadusist. (Vaenduda!)

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

Tõestus. Definitsiooni (14) ja Legendre'i sümboli vastava omaduse tõttu saame

$$\left(\frac{-1}{P}\right) = \left(\frac{-1}{p_1}\right)\left(\frac{-1}{p_2}\right)\dots\left(\frac{-1}{p_n}\right) = (-1)^{\frac{p_1-1}{2}} \dots (-1)^{\frac{p_n-1}{2}} =$$

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

Leiame seose $\sum_{i=1}^{n} \frac{p_i-1}{2}$ ja $\frac{P-1}{2}$ vahel. Selleks esitame $\frac{P-1}{2}$ järgmisel kujul:

$$\frac{P-1}{2} = \frac{p_1p_2\dots p_n - 1}{2} =$$

$$= \frac{\left(1 + \frac{p_1-1}{2} \cdot 2\right)\left(1 + \frac{p_2-1}{2} \cdot 2\right)\dots\left(1 + \frac{p_n-1}{2} \cdot 2\right) - 1}{2}.$$

Kasutades valemit

$$(x + 2a_1)(x + 2a_2) \dots (x + 2a_n) = x^n + 2(a_1 + \dots + a_n)x^{n-1} +$$

$$+ 4(a_1a_2 + a_1a_3 + \dots)x^{n-2} + 8(a_1a_2a_3 + \dots)x^{n-3} + \dots ,$$

milles võtame $x = 1$ ja $a_i = \frac{p_i-1}{2}$, saame

$$\frac{P-1}{2} = \sum_{i=1}^{n} \frac{p_i-1}{2} + 2N,$$

kus N on täisarv. Seega

$$\left(\frac{-1}{P}\right) = \left(-1\right)^{\frac{P-1}{2} - 2N} = \left(-1\right)^{\frac{P-1}{2}} .$$

$\left(\frac{-1}{P}\right)$ arvutamiseks on tarvis kindlaks teha, kas paaritu arv P on kujuga $4n + 1$ või kujuga $4n + 3$. Esimesel juhul $\left(\frac{-1}{P}\right) = 1$, teisel juhul $\left(\frac{-1}{P}\right) = -1$.

5) $\left(\frac{2}{P}\right) = \left(-1\right)^{\frac{P^2-1}{8}}$.

Tõestus. Lähtume seosest

$$\left(\frac{2}{P}\right) = \left(\frac{2}{p_1}\right)\left(\frac{2}{p_2}\right) \cdots \left(\frac{2}{p_n}\right) = \left(-1\right)^{\sum_{i=1}^{n} \frac{p_i^2-1}{8}} .$$

Kasutades valemit

$$(x + 8a_1)(x + 8a_2)\ldots(x + 8a_n) = x^n + 8(a_1 + a_2 + \ldots + a)x^{n-1} + \\ + 64(a_1a_2 + a_1a_3 + \ldots + a_{n-1}a_n)x^{n-2} + \ldots$$

ja seost

$$\frac{P^2-1}{8} = \frac{p_1^2\, p_2^2 \cdots p_n^2 - 1}{8} =$$

$$= \frac{\left(1 + 8\frac{p_1^2-1}{8}\right)\left(1 + 8\frac{p_2^2-1}{8}\right) \ldots \left(1 + 8\frac{p_n^2-1}{8}\right) - 1}{8} ,$$

saame

$$\frac{P^2-1}{8} = \sum_{i=1}^{n} \frac{p_1^2-1}{8} + 2N,$$

kus N on täisarv. Siit järeldubki omaduse kehtivus.

Märgime, et kui $P = 8m \pm 1$, siis $\left(\frac{2}{P}\right) = 1$, kui aga $P = 8m \pm 3$, siis $\left(\frac{2}{P}\right) = -1$.

6) Kui P ja Q on paaritud arvud, kusjuures $(P, Q) = 1$, siis

$$\left(\frac{Q}{P}\right) = \left(-1\right)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}} \left(\frac{P}{Q}\right)$$

(Jacobi sümboli pööratavuse lause).

Tõestus. Olgu $P = p_1p_2\ldots p_n$, $Q = q_1q_2\ldots q_m$. Kasutades Jacobi sümboli definitsiooni, Legendre'i sümboli multiplikatiivsust ning pööratavuse lauset ja arvestades, et $(p_i, q_j) = 1$ $(i = 1, 2, \ldots, n;\ j = 1, 2, \ldots, m)$, võime kirjutada:

$$\left(\frac{Q}{P}\right) = \left(\frac{Q}{p_1}\right)\left(\frac{Q}{p_2}\right)\cdots\left(\frac{Q}{p_n}\right) = \left(\frac{q_1}{p_1}\right)\left(\frac{q_2}{p_1}\right)\cdots\left(\frac{q_m}{p_1}\right)\cdot$$

$$\cdot\left(\frac{q_1}{p_2}\right)\left(\frac{q_2}{p_2}\right)\cdots\left(\frac{q_m}{p_2}\right)\ \cdots\ \left(\frac{q_1}{p_n}\right)\left(\frac{q_2}{p_n}\right)\cdots\left(\frac{q_m}{p_n}\right) =$$

$$= \left(-1\right)^{\sum_{i=1}^{n}\frac{p_i-1}{2}\ \sum_{j=1}^{m}\frac{q_j-1}{2}} \left(\frac{p_1}{q_1}\right)\left(\frac{p_1}{q_2}\right)\cdots\left(\frac{p_1}{q_m}\right)\cdot$$

$$\cdot\left(\frac{p_2}{q_1}\right)\left(\frac{p_2}{q_2}\right)\cdots\left(\frac{p_2}{q_m}\right)\cdots\left(\frac{p_n}{q_1}\right)\left(\frac{p_n}{q_2}\right)\cdots\left(\frac{p_n}{q_m}\right) =$$

$$= \left(-1\right)^{\sum_{i=1}^{n}\frac{p_i-1}{2}\ \sum_{j=1}^{m}\frac{q_j-1}{2}} \left(\frac{P}{Q}\right).$$

Et $\sum_{i=1}^{n}\frac{p_i-1}{2} = \frac{P-1}{2} - 2N$ ja $\sum_{j=1}^{m}\frac{q_j-1}{2} = \frac{Q-1}{2} - 2M$, siis

$$\sum_{i=1}^{n}\frac{p_i-1}{2}\cdot\sum_{j=1}^{m}\frac{q_j-1}{2} = \frac{P-1}{2}\,\frac{Q-1}{2} + 2L,$$

kus L on täisarv. Viimasest seosest järeldubki pööratavuse lause.

Nagu juba käesoleva punkti algul märgitud, võimaldab Jacobi sümbol Legendre'i sümboli arvutamist lihtsustada. Seal-

juures peame silmas, et Legendre'i sümbol on Jacobi sümboli erijuht.

Näide 3. Teeme kindlaks, kas kongruents $x^2 \equiv 265 \pmod{353}$ on lahenduv. Sama näidet vaatlesime eelmises punktis.

Arvutame Legendre'i sümboli $\left(\frac{265}{353}\right)$ väärtuse. Kuna 265 on kordarv, siis Legendre'i sümboli pööratavuse lauset ei saa rakendada. Samal ajal võib aga sümbolit vaadelda ka Jacobi sümbolina ja kasutada viimase pööratavuse lauset. Seda märkust arvestades saame

$$\left(\frac{265}{353}\right) = \left(\frac{353}{265}\right) = \left(\frac{88}{265}\right) = \left(\frac{22}{265}\right) = \left(\frac{2}{265}\right) \cdot \left(\frac{11}{265}\right) = \left(\frac{11}{265}\right) =$$

$$= \left(\frac{265}{11}\right) = \left(\frac{1}{11}\right) = 1.$$

Seega kongruents on lahenduv.

Harjutusülesandeid.

7.3. Teha kindlaks, kas p-1 on ruutjääk mod p, kui

a) p = 19, b) p = 23, c) p = 29, d) p = 83.

7.4. Kontrollida kongruentside

a) $x^2 \equiv 3 \pmod{17}$,

b) $x^2 \equiv 17 \pmod{19}$,

c) $x^2 \equiv 10 \pmod{19}$

lahenduvust Gaussi lemma põhjal ja seejärel Legendre'i sümboli abil.

7.5. Kirjutada välja arvude x^2+1, x^2+2, x^2-2 jagajad x = 1, 2, ..., 10 korral ja jälgida nende kuju.

7.6. Kasutades Legendre'i sümbolit, leida algarvu p üldkuju, mille korral arv 3 on ruutjääk, ja p üldkuju,

mille korral 3 on mitteruutjääk.

7.7. Millise üldkujuga võivad olla arvu $x^2 - 3$ algarvulised jagajad (kasutada ülesande 7.6 tulemusi)?

7.8. Teha kindlaks, kas järgmised ruutkongruentsid on lahenduvad (kõik moodulid on algarvud):

a) $x^2 \equiv 111 \pmod{271}$,

b) $x^2 \equiv 343 \pmod{677}$,

c) $x^2 \equiv 589 \pmod{1283}$,

d) $x^2 \equiv 891 \pmod{4441}$.

7.9. Teha kindlaks, kas järgmised ruutkongruentsid kordarvulise mooduli järgi on lahenduvad või mitte:

a) $x^2 \equiv 111 \pmod{215}$;

b) $x^2 \equiv 343 \pmod{678}$;

c) $x^2 \equiv 10 \pmod{143}$;

d) $x^2 \equiv 21 \pmod{143}$;

e) $x^2 \equiv -1 \pmod{13 \cdot 89}$;

f) $x^2 \equiv -1 \pmod{11 \cdot 13 \cdot 89}$.

7.10. Arvutada Legendre'i sümbolite a) $\left(\frac{2115}{6269}\right)$, b) $\left(\frac{93}{131}\right)$, c) $\left(\frac{116}{379}\right)$ väärtused, kasutades 1) ainult Legendre'i sümboli omadusi ja 2) ka Jacobi sümbolit.

7.11. Arvutada Jacobi sümbolite a) $\left(\frac{521}{825}\right)$, b) $\left(\frac{721}{111}\right)$, c) $\left(\frac{3955}{12727}\right)$ väärtused. Kas saab midagi öelda vastavate ruutkongruentside kohta?

§ 3*. RUUTKONGRUENTSIDE LAHENDAMINE

Ruutkongruentside

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

lahendamiseks pole ühtset meetodit, lahendusmeetod sõltub algarvu p kujust. Paaritu algarv võib olla kas kujuga $p = 4m + 1$ või $p = 4m + 3$.

a) Olgu $p = 4m + 3$ ja $\left(\frac{a}{p}\right) = 1$. Lähtume sellest, et kui a on ruutjääk modulo p, siis $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ (vastasel juhul $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$). Antud juhul $\frac{p-1}{2} = 2m + 1$. Seega

$$a^{2m+1} \equiv 1 \pmod{p}$$

ehk

$$(a^{m+1})^2 \equiv a \pmod{p}.$$

Siit saamegi lahendid

$$x \equiv \pm a^{m+1} \pmod{p} \quad \text{ehk} \quad x \equiv \pm a^{\frac{p+1}{4}} \pmod{p}.$$

Näide. Lahendame kongruentsi

$$x^2 \equiv 12 \pmod{23}.$$

Kuna

$$\left(\frac{12}{23}\right) = \left(\frac{3}{23}\right) = -\left(\frac{23}{3}\right) = -\left(\frac{2}{3}\right) = -(-1)^{\frac{9-1}{8}} = 1$$

ja $23 = 5 \cdot 4 + 3$, siis

$$x \equiv \pm 12^6 \equiv \pm 144^3 \equiv \pm 6^3 \equiv \pm 6 \cdot 13 \equiv \pm 9 \pmod{23}.$$

Juhtu $p = 4m + 1$ ei saa korraga käsitleda. Jaotame jada $\{4m + 1\}$ osajadadeks $\{8m + 1\}$ ja $\{8m + 5\}$ ning vaatleme eraldi algarve kujuga $p = 8m + 5$ ja $p = 8m + 1$.

b) Olgu $p = 8m + 5$ ja $\left(\frac{a}{p}\right) = 1$. Siis $a^{4m+2} \equiv 1 \pmod{p}$, millest $a^{2m+1} \equiv 1 \pmod{p}$ või $a^{2m+1} \equiv -1 \pmod{p}$ (miks?). . . . Kuna üks ja sama arv a^{2m+1} ei saa kuuluda korraga kahte erinevasse jäägiklassi, siis arusaadavalt mõlemad kongru-

entsid korraga kehtida ei saa. Siit edasi

$$a^{2m+2} \equiv a \pmod{p} \quad \text{või} \quad a^{2m+2} \equiv -a \pmod{p}.$$

Kui esineb esimene juht, siis

$$x \equiv \pm a^{m+1} \pmod{p} \quad \text{ehk} \quad x \equiv \pm a^{\frac{p+3}{8}} \pmod{p}.$$

Kui esineb teine juht, siis arvestame, et

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = -1,$$

s.t. 2 ei ole ruutjääk modulo p ja järelikult

$$2^{4m+2} \equiv -1 \pmod{p}.$$

Korrutame viimase kongruentsi kongruentsiga

$$a^{2m+2} \equiv -a \pmod{p}.$$

Saame

$$2^{4m+2}\, a^{2m+2} \equiv a \pmod{p},$$

millest

$$x \equiv \pm 2^{2m+1}\, a^{m+1} \pmod{p}.$$

c) Olgu lõpuks $p = 8m + 1$ ja $\left(\frac{a}{p}\right) = 1$. Olgu N mingi mitteruutjääk modulo p, mille võib leida näiteks proovimise teel. Märgime, et N ei maksa otsida arvude -1, 2, -2 seast, sest need on mooduli $8m + 1$ korral ruutjäägid. Niisiis on $\left(\frac{N}{p}\right) = -1$ ehk

$$N^{4m} \equiv -1 \pmod{p}.$$

Esitame p kujul $p = 2^k h + 1$, kus $k \geq 3$ ja h on paaritu arv. Kasutame jälle seost $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ ehk $a^{2^{k-1}h} \equiv 1 \pmod{p}$, millest

$$a^{2^{k-2}h} \equiv \pm 1 \pmod{p},$$

kusjuures esineb vaid üks märkidest, + või − . Kui esineb +, võime analoogiliselt eelnevaga asendada kongruentsi madalama astme kongruentsiga, kui aga esineb −, siis korrutame teda kongruentsiga

$$N^{2^{k-1}h} \equiv -1 \pmod{p}. \tag{1}$$

Tegelikult võib mõlemad juhud kokku võtta, kirjutades

$$a^{2^{k-2}h}\, N^{s 2^{k-1} h} \equiv +1 \pmod{p},$$

kus esimesel juhul s = 0 (või mistahes teine paarisarv), teisel juhul aga s = 1 (või mistahes teine paaritu arv). Viimasest kongruentsist saame

$$a^{2^{k-3}h}\, N^{s_2 2^{k-2}} \equiv \pm 1 \pmod{p}, \quad s_2 = sh. \tag{2}$$

Juhul, kui esineb +, võime kongruentsi otsekohe asendada madalama astme kongruentsiga; kui esineb −, korrutame saadud kongruentsi kongruentsiga (1), mida võib esitada kujul

$$N^{2^{k-2}u} \equiv -1 \pmod{p}, \text{ kus } u = 2h.$$

Seega kongruentsist (2) järeldub kongruents

$$a^{2^{k-3}h}\, N^{s_3 2^{k-2}} \equiv 1 \pmod{p},$$

kus s_3 on mittenegatiivne täisarv. Viimasest saame

$$a^{2^{k-4}h}\, N^{s_3 2^{k-3}} \equiv \pm 1 \pmod{p} \quad \text{jne.}$$

Lõpuks jõuame kongruentsini

$$a^{h}\, N^{s_k 2} \equiv 1 \pmod{p},$$

millest peale a-ga korrutamist leiame, et

$$x \equiv \pm a^{\frac{h+1}{2}}\, N^{s_k} \pmod{p}.$$

Kogu konstruktsioon on vajalik vasakule täisruudu ja parema-

le a saamiseks.

Harjutusülesandeid.

7.12. Lahendada ruutkongruentsid

a) $x^2 \equiv 11 \pmod{59}$,

b) $x^2 \equiv 30 \pmod{37}$,

c) $x^2 \equiv 11 \pmod{97}$,

d) $x^2 \equiv 29 \pmod{67}$,

e) $x^2 \equiv -16 \pmod{101}$,

f) $x^2 \equiv 14 \pmod{113}$.

§4*. RUUTKONGRUENTSID KORDARVULISE MOODULI JÄRGI

Käesolevas paragrahvis järgime õpikus [4] toodud käsitlust. Alustame ruutkongruentsist

(1) $x^2 \equiv a \pmod{p^\alpha}$, $\alpha > 1$, $(a, p) = 1$,

kus p on paaritu algarv. Tähistades $f(x) = x^2 - a$, saame $f'(x) = 2x$. Olgu $x \equiv \pm x_1 \pmod{p}$ kongruentsi

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

lahendid. Et $\pm x_1 \not\equiv 0 \pmod{p}$ ja $2 \not\equiv 0 \pmod{p}$, siis $f'(x_1) \not\equiv 0 \pmod{p}$. Eelmise peatüki üldistest tulemustest järeldub, et kongruentsil (1) on kas kaks lahendit või ei ole ühtki, olenevalt sellest, kas a on ruutjääk modulo p või mitte. Lahendusmeetod on sama, nagu üldiselt n-astme kongruentsi korral.

Edasi vaatleme kongruentsi

(2) $x^2 \equiv a \pmod{2^\alpha}$, $\alpha \geq 1$, $(a, 2) = 1$.

Siin $f'(x_1) = 2x_1 \equiv 0 \pmod{2}$ ja eelmise peatüki üldised

tulemused pole kasutatavad. Nüüd arutleme teisiti. Vaatleme eraldi järgmisi alajuhte.

a) $\alpha = 1$, s.o. $x^2 \equiv a \pmod 2$. Kuna eelduse kohaselt $(a, 2) = 1$, siis $a \equiv 1 \pmod 2$. Seega vaatleme kongruentsi $x^2 \equiv 1 \pmod 2$, mida rahuldavad kõik paaritud arvud. Viimased moodustavad modulo 2 vaid ühe jäägiklassi. Et paarisarvud kongruentsi ei rahulda, siis on kongruentsil parajasti üks lahend: $x \equiv 1 \pmod 2$.

b) $\alpha = 2$, s.o. $x^2 \equiv a \pmod 4$. Et $(a, 2) = 1$, siis on võimalikud kaks juhtu: $a \equiv 1, 3 \pmod 4$. Lahend x peab ilmselt olema paaritu, s.t. kujuga $x = 4t \pm 1$. Kuid siis $x^2 = 16t^2 \pm 8t + 1 \equiv 1 \pmod 8$. Seega iga paaritu arvu ruut on kongruentne 1-ga modulo 8, järelikult ka modulo 4. Niisiis, kongruents pole lahenduv, kui $a \equiv 3 \pmod 4$. Kui aga $a \equiv 1 \pmod 4$, siis rahuldavad kongruentsi kõik paaritud arvud. Seega kongruentsil on kaks lahendit: $x \equiv 1, 3 \pmod 4$ ehk $x \equiv \pm 1 \pmod 4$.

c) $\alpha = 3$, s.o. $x^2 \equiv a \pmod 8$. Siin võib a omandada järgmisi väärtusi: $a \equiv 1, 3, 5, 7 \pmod 8$, lahend x on aga paaritu. Kuid nagu nägime, on siis $x^2 \equiv 1 \pmod 8$. Järelikult juhtudel $a \equiv 3, 5, 7 \pmod 8$ pole kongruents lahenduv. Kui aga $a \equiv 1 \pmod 8$, siis rahuldavad kongruentsi kõik paaritud arvud. Seega on kongruentsil 4 lahendit:

$$x \equiv 1, 3, 5, 7 \pmod 8 \quad \text{ehk} \quad x \equiv \pm 1, \pm 3 \pmod 8.$$

d) $\alpha > 3$. Kui kongruentsil

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

on lahendid olemas, siis need lahendid rahuldavad (teoreemi 5.15 põhjal) sama kongruentsi ka mooduli 8 järgi. Kuid siis peab lahenduvuseks olema täidetud tingimus

(3) $$a \equiv 1 \pmod 8.$$

Niisiis on viimane tingimus tarvilik kongruentsi lahenduvuseks, kui $\alpha \geqslant 3$. Allpool näeme, et ta on ka piisav. Enne aga teeme kindlaks, kui palju on kongruentsil (2) lahenduval juhul lahendeid.

Olgu b mingi kindel lahend ja x suvaline lahend. Siis

$$b^2 \equiv a \pmod{2^\alpha} \quad \text{ja} \quad x^2 \equiv a \pmod{2^\alpha},$$

millest

$$x^2 - b^2 \equiv 0 \pmod{2^\alpha}$$

ehk

$$(x - b)(x + b) \equiv 0 \pmod{2^\alpha}.$$

Olgu

$$x - b = 2^\varkappa k, \quad x + b = 2^\lambda l,$$

kus k ja l on paaritud arvud ja $\varkappa + \lambda \geqslant \alpha$. Liites ja jagades 2-ga saame siis

$$x = 2^{\varkappa-1} k + 2^{\lambda-1}.$$

Arvestades, et x kui kongruentsi (2) lahend peab olema paaritu, saame siit

$$\text{kas } \varkappa - 1 = 0 \quad \text{või} \quad \lambda - 1 = 0.$$

1) Olgu $\lambda = 1$; siis $\varkappa \geqslant \alpha - 1$ ja $x - b = 2^{\alpha-1}s$, kus s on täisarv. Saame

$$x = b + 2^{\alpha-1}s.$$

Kui s on paarisarv, siis $x \equiv b \pmod{2^\alpha}$, kui aga s on paaritu, s.t. $s = 1 + 2t$, siis $x \equiv b + 2^{\alpha-1} \pmod{2^\alpha}$. Esimene

jäägiklass rahuldab kongruentsi (2) eelduse kohaselt, s.t. $b^2 \equiv a \pmod{2^\alpha}$. Näitame, et kongruentsi rahuldab sellel eeldusel ka jäägiklass $x \equiv b + 2^{\alpha-1} \pmod{2^\alpha}$. Tõepoolest, $x^2 \equiv (b + 2^{\alpha-1})^2 = b^2 + 2^\alpha b + 2^{2\alpha-2} \equiv b^2 \equiv a \pmod{2^\alpha}$.

2) Olgu $\varkappa = 1$; siis $\lambda \geqslant \alpha - 1$ ja $x + b = 2^{\alpha-1}s$. Analoogiliselt esimese juhuga saame lahendid

$$x \equiv -b \pmod{2^\alpha} \quad \text{ja} \quad x \equiv -b + 2^{\alpha-1} \pmod{2^\alpha}.$$

Viimast lahendit võib ilmselt esitada ka kujul $x \equiv -b - 2^{\alpha-1} \pmod{2^\alpha}$.

Seega lahenduval juhul on kongruentsil (2) neli erinevat lahendit

$$x \equiv \pm b, \pm (b + 2^{\alpha-1}) \pmod{2^\alpha}.$$

Tõestame lõpuks, et tingimusel (3) on kongruents (2) lahenduv, s.t. et tingimus (3) on kongruentsi (2) lahenduvuseks piisav. Tingimuse (3) piisavus on teada juhul, kui $\alpha = 3$. Edasi kasutame täieliku induktsiooni meetodit. Olgu tingimus (3) täidetud ja kongruents

$$x^2 \equiv a \pmod{2^{\alpha-1}} \quad (\alpha \geqslant 4) \tag{4}$$

lahenduv. Nagu eespool näidatud, on kongruentsil (4) siis neli lahendit:

$$x \equiv \pm c, \pm (c + 2^{\alpha-2}) \pmod{2^{\alpha-1}},$$

kus c on mingi erilahend. Seega kehtivad kongruentsid

$$c^2 \equiv a \pmod{2^{\alpha-1}} \quad \text{ja} \quad (c + 2^{\alpha-2})^2 \equiv a \pmod{2^{\alpha-1}}.$$

Esimesel juhul

$$c^2 = a - 2^{\alpha-1} k,$$

kus k on mingi kindel täisarv. Kui osutub, et k on paaris-

arv, siis $c^2 \equiv a \pmod{2^\alpha}$, s.t. jäägiklassid $x \equiv \pm c \pmod{2^\alpha}$ on kongruentsi (2) lahenditeks. Kui k on paaritu arv, siis arvutame kongruentsi (4) lahendi $c + 2^{\alpha-2}$ ruudu

$$(c + 2^{\alpha-2})^2 = c^2 + 2^{\alpha-1}c + 2^{2\alpha-4} =$$
$$= a + 2^{\alpha-1}k + 2^{\alpha-1}c + 2^{2\alpha-4}.$$

Et $\alpha \geqslant 4$, siis $2\alpha - 4 \geqslant \alpha$ ja seega

$$(c + 2^{\alpha-2})^2 \equiv a + 2^{\alpha-1}(k + c) \pmod{2^\alpha}.$$

Et k on paaritu eelduse kohaselt, c aga selletõttu, et ta on kongruentsi (4) lahend, siis k + c on paarisarv ja

$$(c + 2^{\alpha-2})^2 \equiv a \pmod{2^\alpha}.$$

Niisiis ka sellel juhul on kongruents (2) lahenduv, kusjuures tema lahenditeks on

$$x \equiv \pm (c + 2^{\alpha-2}) \pmod{2^\alpha}.$$

Tingimuse (3) piisavus kongruentsi (2) lahenduvuseks on näidatud. Ühtlasi näeme, et kongruentsi (4) kaks lahendit, kas $x \equiv \pm c \pmod{2^{\alpha-1}}$ või $x \equiv \pm (c + 2^{\alpha-2}) \pmod{2^{\alpha-1}}$, osutuvad ka kongruentsi (2) lahenditeks mod 2^α. Tähistame nimetatud lahendid $x \equiv \pm b \pmod{2^\alpha}$. Siis ülejäänud on $x \equiv \equiv \pm (b + 2^{\alpha-1}) \pmod{2^\alpha}$.

Saadud tulemused võtame kokku järgmiseks teoreemiks.

Teoreem 7.6. Kongruentsil

(5) $$x^2 \equiv a \pmod{2^\alpha}$$

on paaritu a korral 1) parajasti üks lahend, kui $\alpha = 1$; 2) kaks lahendit, kui $\alpha = 2$ ja $a \equiv 1 \pmod 4$, mitte ühtki lahendit, kui $\alpha = 2$ ja $a \equiv 3 \pmod 4$, 3) neli erinevat lahendit, kui $\alpha \geqslant 3$ ja $a \equiv 1 \pmod 8$, mitte ühtki lahendit, kui

$\alpha \geqslant 3$ ja $a \not\equiv 1 \pmod 8$. Lahenduval juhul leidub kongruentsi (5) lahendite hulgas ka kongruentsi $x^2 \equiv a \pmod{2^{\alpha+1}}$ lahendeid, ülejäänud lahendid avalduvad aga viimaste kaudu.

Näide. Lahendame kongruentsi

$$x^2 \equiv 17 \pmod{64}.$$

Et $17 \equiv 1 \pmod 8$, siis kongruentsil on neli lahendit. Vaatleme kongruentse

$$x^2 \equiv 17 \equiv 1 \pmod 8,$$
$$x^2 \equiv 17 \equiv 1 \pmod{16},$$
$$x^2 \equiv 17 \pmod{32},$$
$$x^2 \equiv 17 \pmod{64}.$$

Kongruentsi $x^2 \equiv 1 \pmod{16}$ lahenditeks on ilmselt $x \equiv \pm 1 \pmod{16}$. Seega on lahenditeks ka $x \equiv \pm (1 + 8) = \pm 9 \pmod{16}$. Kuna kongruentsi $x^2 \equiv 17 \pmod{32}$ lahendeiks ei ole $x \equiv \pm 1 \pmod{32}$, siis on lahenditeks $x \equiv \pm 9 \pmod{32}$ ja $x \equiv \pm (9 + 16) = \pm 25 \pmod{32}$. Et $9^2 = 81 \equiv 17 \pmod{64}$, siis lähtekongruentsi lahenditeks on

$$x \equiv \pm 9 \pmod{64} \quad \text{ja} \quad x \equiv \pm 41 \pmod{64}.$$

Vaatleme lõpuks kongruentsi

(6) $$x^2 \equiv a \pmod m,$$

kus

$$m = 2^{\alpha} p_1^{\alpha_1} \dots p_n^{\alpha_n}, \quad (a, m) = 1.$$

Kasutades eelmise paragrahvi üldist tulemust, võime öelda, et selle kongruentsi lahendid ühtivad järgmise kongruentside süsteemi lahenditega:

$$x^2 \equiv a \pmod{2^{\alpha}},$$
$$x^2 \equiv a \pmod{p_1^{\alpha_1}},$$
$$\text{- - - - - - - - -}$$
$$x^2 \equiv a \pmod{p_n^{\alpha_n}}.$$

Kui süsteemi üksikute kongruentside lahendite arv on vastavalt $k_0, k_1, k_2, \ldots, k_n$, siis teatavasti on süsteemil ja lähtekongruentsil modulo m arvult $k_0k_1k_2\ldots k_n$ lahendit. Kui süsteemis mõni kongruents osutub mittelahenduvaks (vastav $k_i = 0$), siis ka esialgsel kongruentsil pole lahendit. Niisiis on kongruentsi (6) lahenduvuse tarvilikud ja piisavad tingimused kokku võetavad järgmiseks teoreemiks.

Teoreem 7.7. Selleks, et kongruents (6) oleks lahenduv, on tarvilik ja piisav, et juhul, kui $\alpha = 0$ või $\alpha = 1$, oleks

(7) $$\left(\frac{a}{p_1}\right) = 1, \left(\frac{a}{p_2}\right) = 1, \ldots, \left(\frac{a}{p_n}\right) = 1;$$

juhul kui $\alpha = 2$, oleksid täidetud tingimused (7) ja tingimus $a \equiv 1 \pmod 4$; juhul kui $\alpha \geqslant 3$, oleksid täidetud tingimused (7) ja tingimus $a \equiv 1 \pmod 8$. Kui nimetatud tingimused on täidetud, siis lahendite arv on 2^n, kui $\alpha = 0$ või $\alpha = 1$; 2^{n+1}, kui $\alpha = 2$; 2^{n+2}, kui $\alpha \geqslant 3$.

Juhtu $(a, m) \neq 1$ me ei käsitle. Ka sellel juhul on terve rida võimalusi (vt. näit. [4]).

Harjutusülesandeid.

7.13. Lahendada ruutkongruentsid

a) $x^2 \equiv 89 \pmod{256}$; d) $x^2 \equiv 46 \pmod{105}$;

b) $x^2 \equiv 24 \pmod{125}$; e) $x^2 \equiv 17 \pmod{104}$;

c) $x^2 \equiv 18 \pmod{343}$; f) $x^2 \equiv 19 \pmod{90}$.

VIII. ALGJUURED JA INDEKSID

§ 1. ASTENDAJA, MILLELE ARV KUULUB. ALGJUUR

Olgu (a, m) = 1. Siis Euleri teoreemi kohaselt rahuldab eksponentkongruentsi

(1) $$a^x \equiv 1 \pmod{m} \quad (x \geqslant 0)$$

arv $x = \varphi(m)$, samuti kõik arvud $n\varphi(m)$, kus n on mittenegatiivne täisarv. Võib aga juhtuda, et kongruentsi (1) rahuldab ka mõni arvust $\varphi(m)$ väiksem naturaalarv. Vähimat naturaalarvu δ, mis rahuldab kongruentsi (1), nimetatakse <u>astendajaks, millele kuulub arv a modulo m</u>.

Definitsioonist järeldub, et $1 \leqslant \delta \leqslant \varphi(m)$.

Kui arv a kuulub astendajale $\varphi(m)$, siis nimetatakse teda <u>algjureks modulo m</u>.

Saab tõestada, et kui (a, m) > 1, siis kongruentsi (1) rahuldab ainult arv 0 (vt. harjutusülesanne 8.1). Seepärast ei kuulu selline arv a ühelegi astendajale, eriti ei saa ta olla algjuur modulo m. Seega kui a kuulub mingile astendajale modulo m, sealhulgas kui a on algjuur modulo m, siis (a, m) = 1.

<u>Näide 1</u>. Teeme kindlaks, millistele astendajatele modulo 7 kuuluvad taandatud jääkide süsteemi elemendid

a = 1, 2, 3, 4, 5, 6,

ja leiame nende hulgast algjuured modulo 7 (kui neid eksis-

teerib). Arvutuste tulemused on sobiv esitada tabelina, milles vastavalt vaadeldavatele arvudele a ja x ($1 \leq x \leq \varphi(m)$) on toodud astmed a^x:

x \ a	1	2	3	4	5	6
1	1	2	3	4	5	6
2	1	4	2	2	4	1
3	1	1	6	1	6	6
4	1	2	4	4	2	1
5	1	4	5	2	3	6
6	1	1	1	1	1	1

Nagu siit näha, kuulub

arv 1 astendajale 1 (mod 7),
" 2 " 3 " ,
" 3 " 6 " ,
" 4 " 3 " ,
" 5 " 6 " ,
" 6 " 2 " .

Et $\varphi(7) = 6$, siis modulo 7 on algjuurteks arvud 3 ja 5.

Teoreem 8.1. Kui $(a, m) = 1$ ja

$$b \equiv a \pmod{m},$$

siis b ja a kuuluvad ühele ja samale astendajale modulo m.

Tõestus. Kuulugu a astendajale δ. Siis eelduses esineva kongruentsi astendamisel saame

$$b^{\delta} \equiv a^{\delta} \equiv 1 \pmod{m}.$$

Sealjuures ei saa olla $b^{\eta} \equiv 1 \pmod{m}$, kui $0 < \eta < \delta$, sest

siis oleks ka $a^{\eta} \equiv 1 \pmod m$, mis on vastuolus eeldusega.

Järeldus. Kui a on algjuur modulo m ja $b \equiv a \pmod m$, siis ka b on algjuur modulo m.

Teoreem 8.2. Kui arv a kuulub astendajale $\delta \pmod m$, siis on arvud

$$1,\ a,\ a^2,\ \ldots,\ a^{\delta-1}$$

paarikaupa inkongruentsed modulo m.

Tõestus. Kui oleks $a^i \equiv a^k \pmod m$, kus näiteks $0 \leq k < i < \delta$, siis saaksime

$$a^{i-k} \equiv 1 \pmod m \quad (1 \leq i - k < \delta),$$

mis on vastuolus eeldusega.

Järeldus. Kui g on algjuur modulo m, siis astmed

$$1,\ g,\ g^2,\ \ldots,\ g^{\varphi(m)-1}$$

moodustavad taandatud jääkide süsteemi modulo m.

Tõepoolest, nende arv on $\varphi(m)$, nad on paarikaupa inkongruentsed ja $(g^k, m) = 1$, sest $(g, m) = 1$.

Teoreem 8.3. Kui a kuulub astendajale δ modulo m, siis

$$a^x \equiv a^y \pmod m \tag{2}$$

parajasti siis, kui

$$x \equiv y \pmod \delta. \tag{3}$$

Tõestus. 1) Näitame, et kongruentsist (2) järeldub kongruents (3). Selleks jagame x ja y arvuga δ:

$$x = q_1\delta + r_1, \quad 0 \leq r_1 < \delta,$$
$$y = q_2\delta + r_2, \quad 0 \leq r_2 < \delta.$$

Seose (2) tõttu kehtib kongruents

$$(a^{\delta})^{q_1} a^{r_1} \equiv (a^{\delta})^{q_2} a^{r_2} \text{ ehk } a^{r_1} \equiv a^{r_2} \pmod{m}.$$

Oletame nüüd, et $x \not\equiv y \pmod{\delta}$, s.t. $r_1 \neq r_2$. Siis teoreemi 8.2 põhjal $a^{r_1} \not\equiv a^{r_2} \pmod{m}$. Seega peab olema $r_1 = r_2$ ehk $x \equiv y \pmod{\delta}$.

2) Näitame, et kongruentsist (3) järeldub kongruents (2). Olgu $x \equiv y \pmod{\delta}$. Siis $x = q_1\delta + r_1$, $y = q_2\delta + r_2$ ja $r_1 = r_2$, $a^{r_1} = a^{r_2}$. Korrutades viimast võrdust kongruentsiga $(a^{\delta})^{q_1} \equiv (a^{\delta})^{q_2} \equiv 1 \pmod{m}$, saamegi (2).

Näide 2. Kas kehtib kongruents

$$2^{53} \equiv 2^{8} \pmod{7}?$$

Et 2 kuulub astendajale 3 modulo 7 ja

$$53 \equiv 8 \pmod{3},$$

siis see kongruents kehtib.

Järeldus 1. Kui a kuulub astendajale δ modulo m, siis selleks, et

$$a^{x} \equiv 1 \pmod{m},$$

on tarvilik ja piisav, et

$$x \equiv 0 \pmod{\delta}, \text{ s.t. } x = k\delta.$$

Tarvitseb võtta teoreemis $y = 0$.

Järeldus 2. Astendaja δ, millele arv a kuulub modulo m, on $\varphi(m)$ jagaja.

Tõepoolest, $a^{\varphi(m)} \equiv 1 \pmod{m}$ ja seetõttu

$$\varphi(m) \equiv 0 \pmod{\delta}.$$

Seega antud mooduli m korral võivad arvud kuuluda vaid astendajatele, mis on $\varphi(m)$ jagajad. Näiteks mooduli 7 järgi

võivad arvud kuuluda vaid arvu $\varphi(7) = 6$ jagajatele, s.o. astendajatele 1, 2, 3 ja 6. Kui $m = p$ on algarv, siis $\varphi(m) = p - 1$ ja arvud võivad kuuluda vaid astendajatele, mis on $p - 1$ jagajad.

Järeldus 3. Kui a kuulub astendajale δ modulo m, siis a^k kuulub astendajale $\frac{\delta}{(\delta, k)}$ modulo m. Eriti kuuluvad a ja a^k ühele ja samale astendajale δ parajasti siis, kui $(\delta, k) = 1$.

Tõestus. Kuulugu a^k astendajale γ modulo m, s.t. γ on väikim naturaalarv, mis rahuldab tingimust

$$(a^k)^\gamma \equiv 1 \pmod{m} \quad \text{ehk} \quad a^{k\gamma} \equiv 1 \pmod{m}.$$

Järelduse 1 kohaselt kehtib viimane kongruents parajasti siis, kui $k\gamma \equiv 0 \pmod{\delta}$, millest teoreemi 5.13 tõttu saame $\gamma \equiv 0 \left(\mathrm{mod}\ \frac{\delta}{(k, \delta)}\right)$. Väikim naturaalarv γ, mis rahuldab viimast kongruentsi, on $\frac{\delta}{(k, \delta)}$. Seda tuligi näidata.

Esitame veel mõned astendajate ja algjuurte leidmise näited.

Näide 3. Olgu $m = 11$, siis $\varphi(m) = 10$. Astendajateks, millele täisarvud kuuluvad modulo 11, saavad olla vaid 1, 2, 5 ja 10. Arvutame taandatud jääkide süsteemi elementide 1, 2, ..., 10 vastavad astmed. Tulemused esitame alljärgnevas tabelis.

x \ a	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2		4	9	5	3	3	5	9	4	1
5		10	1	1	1	10	10	10	1	
10		1				1	1	1		

Seega arvude kuuluvus astendajatele on järgmine:

a	1	2	3	4	5	6	7	8	9	10
δ	1	10	5	5	5	10	10	10	5	2

Algjuurteks modulo 11 on 2, 6, 7 ja 8.

Näide 4. Olgu m = 10. Siis $\varphi(m) = 4$ ja astendajateks, millele kuulub a, (a, 10) = 1, saavad olla vaid arvud 1, 2 ja 4. Tulemused on järgmised:

x \ a	1	3	7	9
1	1	3	7	9
2		9	9	1
4		1	1	

a	1	3	7	9
δ	1	4	4	2

Algjuured on seega 3 ja 7.

Näide 5. Olgu m = 15. Siis $\varphi(m) = 8$, kusjuures taandatud jääkide süsteem koosneb arvudest

a = 1, 2, 4, 7, 8, 11, 13, 14.

Astendajateks, millele need arvud kuuluvad, saavad olla 1, 2, 4, 8. Arvutamine annab järgmised tulemused:

χ \ a	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2		4	1	4	4	1	4	1
4		1		1	1		1	
8								

a	1	2	4	7	8	11	13	14
δ	1	4	2	4	4	2	4	2

Seega modulo 15 ei eksisteeri algjuuri.

Hiljem tõestame, et algjuured eksisteerivad vaid moodulite

$$2,\ 4,\ p^{\alpha} \quad \text{ja} \quad 2p^{\alpha}$$

puhul, kus p on paaritu algarv ja α - suvaline naturaalarv. Meid huvitavad eriti algjuured algarvulise mooduli järgi.

Anname suhteliselt lihtsalt kontrollitava tarviliku ja piisava tingimuse selleks, et antud arv oleks algjuur modulo m.

Teoreem 8.4. Kui m on moodul, mille korral algjuured eksisteerivad ja

$$\varphi(m) = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n},$$

siis selleks, et mooduliga m ühistegurita arv g oleks algjuur modulo m, on tarvilik ja piisav, et oleksid rahuldatud tingimused

$$g^{\frac{\varphi(m)}{p_i}} \not\equiv 1 \pmod{m}, \quad i=1,2, \dots, n. \tag{4}$$

Tõestus. Tarvilikkus. Olgu g algjuur modulo m, s.t.

$$g^{\varphi(m)} \equiv 1 \pmod{m}$$

ja

$$g^{\eta} \not\equiv 1 \pmod{m}, \quad \text{kui} \quad 0 < \eta < \varphi(m).$$

Kuna $\frac{\varphi(m)}{p_i} < \varphi(m)$, siis tingimused (4) on rahuldatud.

Piisavus. Olgu tingimused (4) rahuldatud. Oletame, et g ei ole siiski algjuur. Siis ta kuulub mingile astendajale $\delta < \varphi(m)$:

$$g^{\delta} \equiv 1 \pmod{m}.$$

Teoreemi 8.3 järelduse 2 kohaselt on δ arvu $\varphi(m)$ jagaja. Seega

$$\frac{\varphi(m)}{\delta} = p_i q ,$$

kus p_i on $\varphi(m)$ kanoonilise kuju üks teguritest, q aga teatud naturaalarv. Siis

$$\frac{\varphi(m)}{p_i} = \delta q$$

ja

$$g^{\frac{\varphi(m)}{p_i}} = g^{\delta q} = (g^{\delta})^{q} \equiv 1 \pmod{m},$$

mis on vastuolus eeldusega.

Teoreem 8.4 võimaldab algjuuri praktiliselt leida.

Näide 6. Olgu m = 31; siis $\varphi(m) = 30 = 2 \cdot 3 \cdot 5$. Ilmselt g = 2 ei saa olla algjuureks modulo 31, sest $2^5 \equiv 1 \pmod{31}$. Juhul g = 3 leiame kergesti, et $3^6 \equiv -15$, $3^{10} \equiv -6$ ja $3^{15} \equiv -1 \pmod{31}$. Seega tingimused (4) on täidetud ja arv 3 on algjuur modulo 31.

Harjutusülesandeid.

8.1. Tõestada, et kui $(a, m) > 1$, siis kongruentsi $a^x \equiv 1 \pmod{m}$ ei rahulda ükski naturaalarv.

8.2. Teha kindlaks, millistele astendajatele modulo 9 kuuluvad taandatud jääkide süsteemi elemendid. Millised viimastest on algjuured modulo 9 ?

8.3. Kasutades näite 1 tulemusi, määrata, millistele astendajatele modulo 7 kuuluvad arvud 10, 13, 27, 141, -5, -3, -1. Millised neist arvudest on algjuured modulo 7 ?

8.4. Millistele astendajatele modulo 31 võivad kuuluda arvud a, mille korral $(a, 31) = 1$?

8.5. Kas saab eksisteerida arvu, mis kuulub astendajale 5 modulo 26 ? Põhjendada.

8.6. Kontrollida, kas $2^{23} \equiv 2^6 \pmod{11}$?

8.7. Teades, et 12 kuulub astendajale $\cdot 6$ modulo 19, leida astendajad arvude 12^3, 12^4 ja 12^5 jaoks sama mooduli korral.

8.8. Kasutades teoreemi 8.4 leida kaks algjuurt modulo 43.

§ 2. ALGJUURTE OLEMASOLU

1. Algjuurte olemasolu ja arv algarvulise mooduli korral. Järgnevalt näitame, et iga algarvulise mooduli p järgi eksisteerivad algjuured, ja teeme kindlaks, kui palju neid leidub taandatud jääkide süsteemis modulo p. Selleks tõestame järgmise üldisema teoreemi.

Teoreem 8.5. Olgu p algarv. Arvu $\varphi(p) = p-1$ igale jagajale δ kui astendajale kuulub $\varphi(\delta)$ arvu taandatud jääkide süsteemist modulo p.

Järeldus. Et algjuur on arv, mis kuulub astendajale $\varphi(p)$, siis leidub algarvulise mooduli korral igas taandatud jääkide süsteemis $\varphi(\varphi(p)) = \varphi(p-1)$ algjuurt.

Teoreemi 8.5 tõestus. 1) Olgu δ arvu p-1 jagaja. Eeldame esialgu täiendavalt, et taandatud jääkide süsteemis modulo p

(1) $\qquad 1, 2, \ldots, p-1$

leidub vähemalt üks arv a, mis kuulub astendajale δ modulo p, s.t. arvu a jaoks on δ vähim naturaalarv, mille korral

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

Tehtud eeldusel leiame süsteemi (1) ülejäänud elemendid x, mis kuuluvad samale astendajale δ. Selleks lahendame kongruentsi

(2) $\qquad x^{\delta} \equiv 1 \pmod{p}.$

Viimasel on δ lahendit:

(3) $\qquad x \equiv 1, a, a^2, \ldots, a^{\delta-1} \pmod{p},$

kus a on arv, mis eelduse kohaselt kuulub astendajale δ.

Tõepoolest, olgu $x \equiv a^k \pmod{p}$ $(k = 0, 1, \ldots, \delta-1)$; siis $x^{\delta} \equiv (a^k)^{\delta} = (a^{\delta})^k \equiv 1 \pmod{p}$, s.t. jäägiklassid (3) on kõik lahendid; lahendite (3) erinevus üksteisest järeldub aga teoreemist 8.2. Et kongruentsi (2) aste on δ, siis rohkem lahendeid olla ei saa. Teoreemi 8.3 järelduse 3 põhjal kuuluvad astendajale δ arvude a^k $(k = 0, 1, \ldots, \delta-1)$ hulgast parajasti need, mille korral $(k, \delta) = 1$. Selliseid

astmeid on aga $\varphi(\delta)$, sest täielikus jääkide süsteemis 0, 1, ..., $\delta - 1$ modulo δ on parajasti $\varphi(\delta)$ elementi k, mis rahuldavad tingimust $(k, \delta) = 1$. Et astmed 1, a, ..., ..., $a^{\delta-1}$ on paarikaupa inkongruentsed modulo p, siis on nad vastavalt kongruentsed taandatud jääkide süsteemi (1) erinevate elementidega. Teoreemi 8.1 ja eeltõestatu põhjal kuulub siis astendajale δ süsteemist (1) $\varphi(\delta)$ arvu.

2) Näitame, et p-1 igale jagajale δ kuulub taandatud jääkide süsteemist vähemalt üks arv, s.t. näitame, et tõestuse algul püstitatud täiendav eeldus on iseendast täidetud. Kirjutame välja kõik p-1 jagajad:

$$\delta_1, \delta_2, \delta_3, \ldots, \delta_\tau.$$

Siis φ-funktsiooni omaduse põhjal

$$\sum_{i=1}^{\tau} \varphi(\delta_i) = p - 1.$$

Teoreemi 8.3 järelduse 2 põhjal kuulub taandatud jääkide süsteemi (1) iga element tingimata arvu p-1 mingile jagajale. Kui sealjuures jagajale δ_i mingi arv kuulub, siis eeltõestatu põhjal kuulub talle üldse $\varphi(\delta_i)$ arvu hulgast (1). Kui oletada, et leidub jagaja δ_j, millele ei kuulu ühtki arvu süsteemist (1), siis p-1 jagajatele kokku kuulub mitte rohkem kui

$$\varphi(\delta_1) + \ldots + \varphi(\delta_{j-1}) + \varphi(\delta_{j+1}) + \ldots + \varphi(\delta_\tau) < p - 1$$

arvu. Et aga taandatud jääkide süsteemi iga element mingile astendajale kuulub, siis peaks mõni arvudest (1) kuuluma astendajale, mis ei ole p-1 jagaja. See on aga vastuolus teoreemi 8.3 järeldusega 2.

2. Algjuured moodulite p^α ja $2p^\alpha$ järgi. Olgu g algjuur modulo p, mille olemasolu on eelmises punktis tõestatud.

Teoreem 8.6. Kui g on algjuur algarvulise mooduli $p > 2$ korral, siis vähemalt üks arvudest g ja g + p on algjuur modulo p^α iga $\alpha \geqslant 2$ puhul. Sealjuures on g algjuureks modulo p^α parajasti siis, kui

$$g^{p-1} \not\equiv 1 \pmod{p^2}.$$

Tõestus. Teeme kindlaks, mis tingimusel on g algjuureks modulo p^2. Kuulugu g astendajale δ modulo p^2. Siis $g^\delta \equiv 1 \pmod{p^2}$ ja ammugi $g^\delta \equiv 1 \pmod{p}$. Seega $\delta \mid (p-1)$. Teiselt poolt δ on $\varphi(p^2) = p(p-1)$ jagaja. Seega kas 1) $\delta = p-1$ või 2) $\delta = p(p-1)$. Teisel juhul on g algjuur ka modulo p^2, esimesel juhul mitte. Teiste sõnadega: mistahes algjuur g modulo p on algjuureks ka modulo p^2 parajasti siis, kui

$$g^{p-1} \not\equiv 1 \pmod{p^2}.$$

Kui algjuur g viimast tingimust ei täida, s.o. kehtib $g^{p-1} \equiv 1 \pmod{p^2}$, siis võtame arvu $a = g + p$, mis teoreemi 8.1 järelduse põhjal on samuti algjuur modulo p, ja arvutame a^{p-1}:

$$\begin{aligned} a^{p-1} &= (g+p)^{p-1} = g^{p-1} + (p-1)g^{p-2}\,p + \\ &+ C_{p-1}^2\, g^{p-3}\, p^2 + \ldots + p^{p-1} \equiv \\ &\equiv g^{p-1} + (p-1)g^{p-2}\,p \equiv \\ &\equiv 1 + (p-1)g^{p-2}\,p \pmod{p^2}. \end{aligned}$$

Et $(p-1)g^{p-2}p$ ei jagu p^2-ga, siis

$$a^{p-1} \not\equiv 1 \pmod{p^2}.$$

Järelikult, kui g ei ole algjuur modulo p^2, siis on seda g + p. Selleks, et näidata, et leitud arv a (s.o. kas g või g + p) on algjuur ka modulo p^α ($\alpha > 2$), arvestame, et

$$a^{p-1} = 1 + t_1 p,$$

kus t_1 ei jagu p-ga ($a^{p-1} \equiv 1 \pmod{p}$, kuid $a^{p-1} \not\equiv 1 \pmod{p^2}$).

Konstrueerime järk-järgult $a^{\varphi(p^\alpha)}$, kus $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$. Saame

$$a^{p(p-1)} = (1 + t_1 p)^p = 1 + t_1 p^2 + C_p^2 t_1^2 p^2 + \ldots = 1 + t_2 p^2,$$

kus $t_2 = t_1 + \frac{p-1}{2} t_1^2 p + \ldots$ ei jagu p-ga (t_1 ei jagu ja kõik järgnevad liikmed jaguvad);

$$a^{p^2(p-1)} = (1 + t_2 p^2)^p = 1 + t_2 p^3 + C_p^2 t_2^2 p^4 + \ldots = 1 + t_3 p^3,$$

kus $t_3 = t_2 + C_p^2 t_2^2 p + \ldots$ ei jagu p-ga. Täieliku induktsiooniga saame üldiselt

$$a^{p^\alpha(p-1)} = 1 + t_{\alpha+1} p^{\alpha+1},$$

kus $t_{\alpha+1}$ ei jagu p-ga.

Kuulugu a mooduli p^α järgi astendajale δ. Siis

$$a^\delta \equiv 1 \pmod{p^\alpha}. \tag{4}$$

Kongruents kehtib muidugi ka modulo p:

$$a^\delta \equiv 1 \pmod{p},$$

mistõttu δ on p-1 kordne. Et aga δ on $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$ jagaja, siis avaldub ta kujul

$$\delta = p^{k-1}(p-1),$$

kus k on üks arvudest 1, 2, ..., α. Asendame seoses (4), millel on nüüd kuju

$$a^{p^{k-1}(p-1)} \equiv 1 \pmod{p^\alpha},$$

vasaku poole tema avaldisega, mille me varem leidsime. Saame

$$1 + t_k p^k \equiv 1 \pmod{p^\alpha},$$

kus t_k ei jagu p-ga. Siit

$$p^k \equiv 0 \pmod{p^\alpha}.$$

Järelikult $k = \alpha$ ja a kuulub astendajale $p^{\alpha-1}(p-1) = \varphi(p^\alpha)$. Seega on a algjuur modulo p^α.

Järeldus. Et iga paaritu algarvu p korral leidub algjuuri, siis leidub neid ka modulo p^α.

Näide 1. Leida üks algjuur modulo 11^α, kus $\alpha \geqslant 2$.

Varem leidsime, et modulo 11 on üheks algjuureks arv 2. Tõestatud teoreemi põhjal on siis modulo 11^α algjuureks kas arv 2 ise või arv 2 + 11 = 13. Et

$$2^{10} = 1024 \equiv 56 \not\equiv 1 \pmod{11^2},$$

siis on 2 algjuur ka modulo 11^α.

Teoreem 8.7. Olgu $p > 2$, $\alpha \geqslant 1$ ja g algjuur modulo p^α. Siis arvude g ja $g + p^\alpha$ hulgast paaritu arv on algjuureks ka modulo $2p^\alpha$.

Tõestus. Iga paaritu arv a, mis rahuldab ühte kongruentsidest

$$a^{\gamma} \equiv 1 \pmod{p^{\alpha}} \quad \text{ja} \quad a^{\gamma} \equiv 1 \pmod{2p^{\alpha}},$$

rahuldab ka teist (vt. teoreemid 5.14 ja 5.15, pidades silmas, et paaritu arv $a^{\gamma} \equiv 1 \pmod 2$). Arvestades, et $\varphi(p^{\alpha}) = \varphi(2p^{\alpha})$, näeme, et iga paaritu arv a, mis on algjuur ühe järgi moodulitest p^{α}, $2p^{\alpha}$, on seda ka teise järgi.

Kahest algjuurest g ja $g + p^{\alpha}$ modulo p^{α} on üks tingimata paaritu ja on seega algjuureks ka modulo $2p^{\alpha}$.

Näide 2. Nägime (vt. näide 1), et 2 on algjuureks modulo 11^{α}. Algjuureks modulo $2 \cdot 11^{\alpha}$ on seega $2 + 11^{\alpha}$. Näiteks mooduli 242 järgi on algjuureks arv $2 + 121 = 123$.

3. Algjuurte olemasolu mooduli 2^{α} ja mistahes kordarvulise mooduli korral. Näitame, et enamiku kordarvuliste moodulite korral algjuured puuduvad. Olgu moodul antud kanoonilisel kujul

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$$

ja olgu $(a, m) = 1$. Siis Euleri teoreemi kohaselt

$$a^{\varphi(p_1^{\alpha_1})} \equiv 1 \pmod{p_1^{\alpha_1}},$$
$$a^{\varphi(p_2^{\alpha_2})} \equiv 1 \pmod{p_2^{\alpha_2}},$$
$$\dots\dots\dots\dots\dots\dots$$
$$a^{\varphi(p_n^{\alpha_n})} \equiv 1 \pmod{p_n^{\alpha_n}}.$$

Olgu astendajate

$$\varphi(p_1^{\alpha_1}) = p_1^{\alpha_1-1}(p_1 - 1),$$

$$\varphi(p_2^{\alpha_2}) = p_2^{\alpha_2-1}(p_2 - 1), \tag{5}$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$\varphi(p_n^{\alpha_n}) = p_n^{\alpha_n-1}(p_n - 1)$$

vähim ühiskordne s. Siis kehtivad kongruentsid

$$a^s \equiv 1 \pmod{p_1^{\alpha_1}}, \ \ldots, \ a^s \equiv 1 \pmod{p_n^{\alpha_n}}.$$

Et moodulid on ühistegurita, siis teoreemi 5.14 põhjal

$$a^s \equiv 1 \pmod{m}.$$

Juhul, kui iga a korral on $s < \varphi(m)$, ei leidu algjuuri modulo m. Teeme kindlaks, millistel juhtudel $s < \varphi(m)$.

Arvude (5) vähim ühiskordne s on väiksem kui nende arvude korrutis $\varphi(p_1^{\alpha_1}) \ldots \varphi(p_n^{\alpha_n}) = \varphi(m)$ parajasti siis, kui arvude (5) hulgas leidub vähemalt kaks ühisteguriga arvu. See on kindlasti nii, kui arvude $p_1, \ldots, p_n$ seas leidub vähemalt kaks paaritut algarvu p_i ja p_j, sest siis $\varphi(p_i^{\alpha_i})$ ja $\varphi(p_j^{\alpha_j})$ on paarisarvud. Samuti ei eksisteeri algjuuri modulo m, kui m sisaldab tegurina paaritut algarvu ja astet 2^α, kus $\alpha > 1$, sest siis $\varphi(2^\alpha) = 2^{\alpha-1}$ on paarisarv ja jällegi $s < \varphi(m)$.

Jääb veel vaadelda juhtu $m = 2^\alpha$, mille korral $\varphi(m) = 2^{\alpha-1}$. Arv a, olles ühistegurita arvuga 2^α, on paaritu ja teda võib esitada kujul

$$a = \pm 1 + 2^2 t,$$

kus t on täisarv. Tõstes järjest ruutu, saame

$$a^2 = 1 + 2^3 t_1,$$

$$a^{2^2} = 1 + 2^4 t_2,$$

$$\cdots\cdots\cdots\cdots$$

$$a^{2^{\alpha-2}} = 1 + 2^{\alpha} t_{\alpha-2},$$

kus $t_1, t_2, \ldots, t_{\alpha-2}$ on täisarvud. Kuid $2^{\alpha-2} = \frac{\varphi(m)}{2}$ ja järelikult iga a korral, mis täidab tingimust (a, 2) = 1, on

$$a^{\frac{\varphi(m)}{2}} = a^{2^{\alpha-2}} = 1 + 2^{\alpha} t_{\alpha-2} \equiv 1 \pmod{2^{\alpha}}.$$

Seega arv a ei saa olla algjuur modulo 2^{α}, kui $\alpha > 2$. Juhul, kui $\alpha = 1$ või $\alpha = 2$, algjuured eksisteerivad. Tõepoolest, kui $\alpha = 1$, siis m = 2 on algarv (algjuureks on arv 1); kui aga $\alpha = 2$, siis m = 4, $\varphi(m) = 2$ ja algjuureks on 3, sest $3^{\varphi(4)} = 3^2 \equiv 1 \pmod 4$, kuid $3^1 \not\equiv 1 \pmod 4$.

Järelikult saavad algjuured eksisteerida vaid moodulite 2, 4, p^{α} ja $2p^{\alpha}$ järgi. Nendel juhtudel on aga algjuurte olemasolu ka tõestatud.

Harjutusülesandeid.

8.9. Kui palju algjuuri leidub taandatud jääkide süsteemis a) modulo 43, b) modulo 109, c) modulo 3989 ?

8.10. Teades, et moodulo 13 on algjuureks arv 6 (kontrollida seda!), leida algjuured moodulite 13^2, 13^3, 26 ja $2 \cdot 13^2$ järgi.

8.11. Milliste järgi järgmistest moodulitest eksisteerivad algjuured: a) 109; b) 115; c) 172; d) 226; e) 250; f) 230; g) 32; h) 4 ?

§ 3. INDEKSID

1. Indeksi definitsioon. Olgu m moodul, mille puhul eksisteerib algjuuri, g aga olgu algjuur modulo m. Arvude a jaoks, mille korral (a, m) = 1, toome sisse indeksi mõiste, mis on analoogiline logaritmi mõistega.

Definitsioon. Kui

$$a \equiv g^{\gamma} \pmod{m} \quad (\gamma \geqslant 0),$$

siis astendajat γ nimetatakse arvu a indeksiks alusel g (moodulo m) ja tähistatakse

$$\gamma = \operatorname{ind}_g a.$$

Juhul, kui aluseks on kogu aeg üks ja sama algjuur g, jäetakse ta tavaliselt märkimata ja kirjutatakse

$$\gamma = \operatorname{ind} a.$$

Eespool käsitletud näidetes nägime, et näiteks modulo 11 on algjuurteks 2, 6, 7, 8, kusjuures

$$2^5 \equiv 6^5 \equiv 7^5 \equiv 8^5 \equiv 10 \pmod{11}.$$

Seega

$$\operatorname{ind}_2 10 = \operatorname{ind}_6 10 = \operatorname{ind}_7 10 = \operatorname{ind}_8 10 = 5.$$

Kuid

$$2^2 \equiv 4,\ 6^2 \equiv 3,\ 7^2 \equiv 5,\ 8^2 \equiv 9 \pmod{11}$$

ja seega

$$2 = \operatorname{ind}_2 4 = \operatorname{ind}_6 3 = \operatorname{ind}_7 5 = \operatorname{ind}_8 9.$$

Teises näites leidsime, et modulo 10 on algjuured 3 ja 7. Et $9 \equiv 7^2 \pmod{10}$, siis $\operatorname{ind}_7 9 = 2$.

Niisiis on arvu a indeks alusel g mittenegatiivne asten-

daja, millega algjuurt g astendades saame arvuga a kongruentse arvu modulo m.

Igal elemendil taandatud jääkide süsteemist modulo m on olemas indeks.

Tõepoolest, arvud

$$(1) \qquad g^0, g^1, g^2, \ldots, g^{\varphi(m)-1}$$

moodustavad taandatud jääkide süsteemi modulo m (järeldus teoreemist 8.2). Seega mistahes teise taandatud jääkide süsteemi

$$a_1, a_2, \ldots, a_{\varphi(m)}$$

elemendi a_i jaoks leidub süsteemis (1) parajasti üks element, nii et

$$a_i \equiv g^{\gamma_i} \pmod m \quad \text{ehk} \quad \gamma_i = \operatorname{ind}_g a_i.$$

Märgime, et arvu indeks antud alusel pole üheselt määratud. Kuna iga täisarvu $k \geqslant 0$ korral on Euleri teoreemi tõttu

$$g^{\gamma} \equiv g^{\gamma} g^{k\varphi(m)} = g^{\gamma + k\varphi(m)} \pmod m,$$

siis juhul, kui $\gamma = \operatorname{ind}_g a$, on ka $\gamma_k = \gamma + k\varphi(m)$ arvu a indeksiks alusel g modulo m. Sealjuures

$$\gamma_k \equiv \gamma \pmod{\varphi(m)}.$$

Tavaliselt kasutatakse vähimaid indekseid

$$0, 1, 2, \ldots, \varphi(m)-1$$

või vähimaid naturaalarvulisi indekseid

$$1, 2, \ldots, \varphi(m).$$

Indekside on tõhusaks vahendiks kahendliikmeliste kõrgema astme kongruentside ja eksponentkongruentside lahendamisel.

Seepärast on koostatud indeksite tabelid algarvuliste moodulite jaoks. Peaaegu iga ôpiku lôpus leiduvad indeksite tabelid moodulite jaoks, mis ei ületa 100. Spetsiaalsed indeksite tabelid on koostatud märksa suuremate algarvude jaoks. Käesoleva ôppevahendi lôppu paigutatud indeksite tabelid on äratrükk ôpikust [3]. Neis on aluseks vähim algjuur.

Koostame indeksite tabeli modulo 19. Leiame ühe algjuure modulo 19. Et $\varphi(p) = p - 1 = 18 = 2 \cdot 3^2$ ja $p_1 = 2$, $p_2 = 3$, siis tuleb algjuur g määrata tingimustest

$$g^{\frac{18}{3}} = g^6 \not\equiv 1 \pmod{19},$$

$$g^{\frac{18}{2}} = g^9 \not\equiv 1 \pmod{19}.$$

Proovime g = 2:

$$2^6 = 64 \equiv 7 \not\equiv 1 \pmod{19},$$

$$2^9 = 2^6 \cdot 2^3 \equiv 7 \cdot 8 = 56 \equiv 18 \not\equiv 1 \pmod{19}.$$

Seega 2 on algjuur ja võtamegi selle aluseks. Selleks et saada kõikide arvude 1, 3, ..., 18 indekseid modulo 19, tuleb arvutada algjuure 2 kõik astmed $2^0, \ldots, 2^{17}$:

$2^0 \equiv 1 \pmod{19}$, seega ind $1 \equiv 0 \pmod{18}$,
$2^1 \equiv 2 \pmod{19}$, " ind $2 \equiv 1 \pmod{18}$,
$2^2 \equiv 4 \pmod{19}$, " ind $4 \equiv 2 \pmod{18}$,
$2^3 \equiv 8 \pmod{19}$, " ind $8 \equiv 3 \pmod{18}$,
$2^4 \equiv 16 \pmod{19}$, " ind $16 \equiv 4 \pmod{18}$,
$2^5 \equiv 13 \pmod{19}$, " ind $13 \equiv 5 \pmod{18}$,
$2^6 \equiv 7 \pmod{19}$, " ind $7 \equiv 6 \pmod{18}$,
$2^7 \equiv 14 \pmod{19}$, " ind $14 \equiv 7 \pmod{18}$,
$2^8 \equiv 9 \pmod{19}$, " ind $9 \equiv 8 \pmod{18}$,

$2^9 \equiv 18 \pmod{19}$, seega $\operatorname{ind} 18 \equiv 9 \pmod{18}$,
$2^{10} \equiv 17 \pmod{19}$, " $\operatorname{ind} 17 \equiv 10 \pmod{18}$,
$2^{11} \equiv 15 \pmod{19}$, " $\operatorname{ind} 15 \equiv 11 \pmod{18}$,
$2^{12} \equiv 11 \pmod{19}$, " $\operatorname{ind} 11 \equiv 12 \pmod{18}$,
$2^{13} \equiv 3 \pmod{19}$, " $\operatorname{ind} 3 \equiv 13 \pmod{18}$,
$2^{14} \equiv 6 \pmod{19}$, " $\operatorname{ind} 6 \equiv 14 \pmod{18}$,
$2^{15} \equiv 12 \pmod{19}$, " $\operatorname{ind} 12 \equiv 15 \pmod{18}$,
$2^{16} \equiv 5 \pmod{19}$, " $\operatorname{ind} 5 \equiv 16 \pmod{18}$,
$2^{17} \equiv 10 \pmod{19}$, " $\operatorname{ind} 10 \equiv 17 \pmod{18}$.

Seega saame järgmised tabelid:

Algarv 19

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

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

Esimesest tabelist saab antud arvu N jaoks leida tema indeksi, teisest aga indeksi I järgi vastava arvu N. Tegelikult piisab ainult esimesest tabelist, sest ka sealt saab indeksi I järgi leida arvu N, teist tabelit on aga viimaseks otstarbeks mugavam kasutada.

2. Indeksite omadusi. Olgu m nagu ennegi moodul, mille korral algjuured eksisteerivad, g aga algjuur modulo m. Märgime kõigepealt ära järgmised vahetult definitsioonist järel-

duvad omadused:

$$\operatorname{ind}_g 1 \equiv 0 \pmod{\varphi(m)},$$
$$\operatorname{ind}_g g \equiv 1 \pmod{\varphi(m)}.$$

Tõepoolest

$$g^0 \equiv 1 \pmod{m},$$
$$g^1 \equiv g \pmod{m}.$$

Teoreem 8.8. Kongruents

(2) $$a \equiv b \pmod{m}$$

kehtib parajasti siis, kui

(3) $$\operatorname{ind}_g a \equiv \operatorname{ind}_g b \pmod{\varphi(m)}.$$

Tõestus. Indeksi definitsiooni kohaselt

$$a \equiv g^{\operatorname{ind}_g a}, \quad b \equiv g^{\operatorname{ind}_g b} \pmod{m}.$$

Kasutame teoreemi 8.3, arvestades, et algjuur g kuulub astendajale $\varphi(m)$. Seega kehtib kongruents

$$g^{\operatorname{ind} a} \equiv g^{\operatorname{ind} b} \pmod{m} \quad \text{ehk} \quad a \equiv b \pmod{m}$$

parajasti siis, kui

$$\operatorname{ind}_g a \equiv \operatorname{ind}_g b \pmod{\varphi(m)}.$$

Üleminekut kongruentsilt (2) kongruentsile (3) nimetatakse indekseerimiseks, üleminekut kongruentsilt (3) kongruentsile (2) aga potentseerimiseks. Kui mooduliks on algarv p, siis $\varphi(p) = p - 1$ ja indekseerimisel moodul väheneb ühe võrra, potentseerimisel aga suureneb ühe võrra. Analoogiline on olukord järgnevates teoreemides.

Teoreem 8.9. Kui g on algjuur modulo m, siis

$$\operatorname{ind}_g (ab) \equiv \operatorname{ind}_g a + \operatorname{ind}_g b \pmod{\varphi(m)}.$$

Tõestus. Definitsiooni kohaselt

$$g^{\text{ind } a} \equiv a \pmod m, \quad g^{\text{ind } b} \equiv b \pmod m.$$

Seega

$$g^{\text{ind } a + \text{ind } b} \equiv ab \equiv g^{\text{ind } (ab)} \pmod m.$$

Nagu teoreemi 8.8 tõestamiselgi saame

$$\text{ind } a + \text{ind } b \equiv \text{ind } (ab) \pmod{\varphi(m)}.$$

Teoreem 8.10. Kui g on algjuur modulo m, siis

$$\text{ind } (a^n) \equiv n \text{ ind } a \pmod{\varphi(m)}.$$

Tõestus. Kongruentsi $g^{\text{ind } a} \equiv a \pmod m$ astendamisel saame

$$g^{n \text{ ind } a} \equiv a^n \equiv g^{\text{ind } (a^n)} \pmod m.$$

Siit

$$n \text{ ind } a \equiv \text{ind } (a^n) \pmod{\varphi(m)}.$$

Teoreem 8.11. Olgu g ja h algjuured modulo m. Siis

$$\text{ind}_h a \equiv \text{ind}_h g \cdot \text{ind}_g a \pmod{\varphi(m)}.$$

Tõestus. Et (g, m) = 1, siis arvul g on olemas indeks alusel h. Seose

$$a \equiv g^{\text{ind}_g a} \pmod m$$

indekseerimisel alusel h saame

$$\text{ind}_h a \equiv \text{ind}_g a \cdot \text{ind}_h g \pmod{\varphi(m)}.$$

3. Indeksite kasutamine kaheliikmeliste kongruentside lahendamisel. Vaatleme kongruentsi

$$x^n \equiv a \pmod p. \tag{4}$$

Teatavasti nimetatakse arvu a n-astme jäägiks modulo p, kui kongruents (4) on lahenduv. Kongruentsi (4) indekseerimisel saame ekvivalentse kongruentsi

(5) $$n \operatorname{ind} x \equiv \operatorname{ind} a \pmod{p-1}.$$

Tähistame siin $(n, p-1) = d$. Selleks, et ind x suhtes lineaarne kongruents (5) oleks lahenduv, on tarvilik ja piisav, et

$$\operatorname{ind} a \mid d.$$

Et aga esialgne kongruents on saadud kongruentsiga ekvivalentne, siis ka kongruentsi (4) lahenduvuseks on tarvilik ja piisav, et

(6) $$\operatorname{ind} a \vdots (n, p-1).$$

Teisiti öeldes, tingimus (6) on tarvilik ja piisav selleks, et arv a oleks n-astme jääk modulo p. Kui viimane tingimus on täidetud, siis lahendeid on arvult $d = (n, p-1)$. Eriti kui $d = 1$, on kongruentsil (4) parajasti üks lahend.

Vaatleme veel erijuhte $n = 2$ ja $n = 3$. Kui $n = 2$ ja p on paaritu algarv, siis $(2, p-1) = 2$. Seega selleks, et arv a oleks ruutjääk modulo p, on tarvilik ja piisav, et ind a oleks paarisarv. Indeksite tabeli järgi on lihtne määrata, millised arvud on ruutjäägid, millised mitte. Nii on modulo 19 ruutjääkideks 1, 4, 5, 6, 7, 9, 11, 16, 17, sest nende arvude indeksid on paarisarvud; mitteruutjäägid on aga 2, 3, 8, 10, 12, 13, 14, 15, 18, sest nende arvude indeksid on paaritud arvud.

Kui p on paaritu algarv, $n = 3$ ja $(3, p-1) = 1$, siis on iga arv kuupjääk modulo p. Kui aga $(3, p-1) = 3$, siis

tarvilikuks ja piisavaks tingimuseks selleks, et arv a oleks kuupjääk, on tingimus

$$\text{ind } a \mid 3.$$

Taandatud jääkide süsteemis on kuupjääke arvult $\frac{p-1}{3}$. Ilmselt on $(3, p-1) = 1$ parajasti siis, kui algarv p on 3 või kujuga $3n + 2$; kui aga algarv p on kujuga $3n + 1$, siis $(3, p-1) = 3$.

Näide 1. Lahendame kongruentsi $x^7 \equiv 7 \pmod{19}$.

Indekseerimisel saame

$$7 \text{ ind } x \equiv \text{ind } 7 \pmod{18}$$

ehk leides algarvu 19 indeksite tabelist ind 7 väärtuse,

$$7 \text{ ind } x \equiv 6 \pmod{18}.$$

Kuna $(7, 18) = 1$, siis on kongruentsil parajasti üks lahend. Leiame selle:

$$7 \text{ ind } x \equiv 6 + 36 = 42 \text{ (ind 18)},$$

$$\text{ind } x \equiv 6 \pmod{18}.$$

Tabelist leiame, et

$$x \equiv 7 \pmod{19}.$$

Näide 2. Lahendame kongruentsi

$$x^8 \equiv 78 \pmod{89}.$$

Indekseerimisel saame

$$8 \text{ ind } x \equiv 40 \pmod{88}.$$

Siin $(8, 88) = 8$, kusjuures $40 \mid 8$. Seega on kongruentsil 8 lahendit. Kongruentsi mõlema poole ja mooduli jagamisel 8-ga saame ekvivalentse kongruentsi

$$\text{ind } x \equiv 5 \pmod{11}.$$

Selleks et kasutada indeksite tabelit, peab moodul olema 88.

Mooduli 88 järgi on aga ind x suhtes lineaarsel kongruentsil 8 lahendit:

$$\text{ind } x \equiv 5,\ 16,\ 27,\ 38,\ 49,\ 60,\ 71,\ 82 \pmod{88}.$$

Tabelist saame nüüd esialgse kongruentsi lahendid:

$$x \equiv 65,\ 2,\ 74,\ 68,\ 24,\ 87,\ 15,\ 21 \pmod{89}$$

ehk

$$x \equiv \pm 2,\ \pm 15,\ \pm 21,\ \pm 24 \pmod{89}.$$

Näide 3. Lahendame kongruentsi $4x^3 \equiv 13 \pmod{19}$.

Indekseerimisel saame

$$\text{ind } 4 + 3 \text{ ind } x \equiv \text{ind } 13 \pmod{18},$$

$$3 \text{ ind } x \equiv 5 - 2 \pmod{18},$$

$$\text{ind } x \equiv 1 \pmod{6}.$$

Minnes üle moodulile 18, saame

$$\text{ind } x \equiv 1,\ 7,\ 13 \pmod{18}$$

ja tabelist

$$x \equiv 2,\ 14,\ 3 \pmod{19}.$$

Näide 4. Lahendame lineaarkongruentsi

$$43x \equiv 65 \pmod{79}.$$

Indekseerimine annab

$$\text{ind } 43 + \text{ind } x \equiv \text{ind } 65 \pmod{78},$$

millest

$$\text{ind } x \equiv 18 - 49 = -31 \equiv 47 \pmod{78}.$$

Potentseerimisel leiame tabelist lahendi

$$x \equiv 75 \pmod{79}.$$

Kõikide ülesannete lahendite õigsust saab kontrollida otsese asendamise teel.

Näide 5. Lahendame eksponentkongruentsi

$$3^x \equiv 13 \pmod{23}, \quad x \geqslant 0.$$

Indekseerimisel leiame

$$x \operatorname{ind} 3 \equiv \operatorname{ind} 13 \pmod{22}$$

ehk

$$16x \equiv 14 \pmod{22}$$

ehk

$$8x \equiv 7 \equiv -4 \pmod{11}.$$

Siit saame edasi

$$2x \equiv -1 \equiv 10 \pmod{11}$$

ja

$$x \equiv 5 \pmod{11}, \quad x \geqslant 5.$$

Näeme, et lahendiks on jäägiklassi 5 positiivsed elemendid mooduli 11 järgi. Teisiti võib lahendi esitada kujul

$$x = 5 + 11t, \quad t \geqslant 0.$$

Lahendi õigsuse kontrollimiseks esitame ta kahe jäägiklassina mod 22:

$$x \equiv 5, 16 \pmod{22}, \quad x > 0$$

ehk teisiti:

$$x = 5 + 22t \quad \text{ja} \quad x = 16 + 22t, \quad t \geqslant 0.$$

Asendamine esialgse kongruentsi vasakusse poolde annab Euleri teoreemi alusel esimesel juhul

$$3^{5+22t} = 3^5 \cdot (3^{\varphi(23)})^t \equiv 3^5 \pmod{23}$$

ja teisel juhul

$$3^{16+22t} \equiv 3^{16} \pmod{23}.$$

Jääb veel kontrollida, et kehtivad kongruentsid

$$3^5 \equiv 13 \quad \text{ja} \quad 3^{16} \equiv 13 \pmod{23}.$$

Näide 6. Lahendada kongruents

$$5x^9 \equiv 14 \pmod{418},$$

kui see on lahenduv.

Mooduli 418 järgi ei eksisteeri algjuuri, sest $418 = 2 \cdot 11 \cdot 19$. Sellele vaatamata saab kongruentsi lahendamisel kasutada indeksite tabeleid. Teatavasti on kongruents kordarvulise mooduli järgi ekvivalentne kongruentside süsteemiga mooduli algarvuliste astmete järgi. Seega lahendame süsteemi

$$5x^9 \equiv 14 \pmod{2}$$
$$5x^9 \equiv 14 \pmod{11}$$
$$5x^9 \equiv 14 \pmod{19},$$

mis on ekvivalentne süsteemiga

$$x^9 \equiv 0 \pmod{2}$$
$$5x^9 \equiv 3 \pmod{11}$$
$$5x^9 \equiv 14 \pmod{19}.$$

Lahendame eraldi iga kongruentsi. Esimese ainsaks lahendiks on ilmselt

$$x \equiv 0 \pmod{2}.$$

Teise lahendamiseks kasutame algarvu 11 indeksite tabelit. Saame

$$\text{ind } 5 + 9 \text{ ind } x \equiv \text{ind } 3 \pmod{10}$$

ehk

$$9 \text{ ind } x \equiv \text{ind } 3 - \text{ind } 5 = 8 - 4 = 4 \pmod{10}.$$

Et $(9, 10) = 1$, siis viimane kongruents on ind x suhtes lahenduv. Siit

$$-\text{ind } x \equiv 4 \pmod{10}$$

ehk

$$\text{ind } x \equiv -4 \equiv 6 \pmod{10},$$

$$x \equiv 9 \pmod{11}.$$

Kolmanda kongruentsi lahendamiseks kasutame algarvu 19 indeksite tabelit. Saame

$$\text{ind } 5 + 9 \text{ ind } x \equiv \text{ind } 14 \pmod{18}$$

ehk

$$9 \text{ ind } x \equiv 7 - 16 \equiv -9 \pmod{18}.$$

Et $(9, 18) = 9$ ja $-9 \vdots 9$, siis modulo 18 on viimasel kongruentsil $\text{ind } x$ suhtes 9 lahendit. Edasi

$$\text{ind } x \equiv -1 \equiv 1 \pmod{2},$$

$$\text{ind } x \equiv 1, 3, 5, 7, 9, 11, 13, 15, 17 \pmod{18},$$

$$x \equiv 2, 8, 13, 14, 18, 15, 3, 12, 10 \pmod{19}.$$

Seega

$$x \equiv c_1 \equiv 0 \pmod{2}$$

$$x \equiv c_2 \equiv 9 \pmod{11}$$

$$x \equiv c_3 \equiv 2, 3, 8, 10, 12, 14, 15, 18 \pmod{19}.$$

Esialgsel kongruentsil mod 418 on seega $1 \cdot 1 \cdot 9 = 9$ lahendit.

Lahend avaldub kujul

$$x \equiv c = M_1 M_1' c_1 + M_2 M_2' c_2 + M_3 M_3' c_3 \pmod{418},$$

kus

$M_i m_i = m = 418$ ja $M_i M_i' \equiv 1 \pmod{m_i}$, $i = 1, 2, 3$.

Leiame M_i ja M_i':

m_i	2	11	19
M_i	209	38	22

$209 M_1' \equiv 1 \pmod{2}$, $M_1' = 1$;

$38 M_2' \equiv 1 \pmod{11}$, $M_2' = -2$;

$22 M_3' \equiv 1 \pmod{19}$, $M_3' = -6$.

Seega

$$x \equiv -76 \cdot 9 - 132\, c_3 \pmod{418} \equiv -684 - 132\, c_3 \equiv$$
$$\equiv 152 - 132\, c_3 \pmod{418}.$$

Pärast c_3 asendamist saame

$$x \equiv 306,\ 174,\ 348,\ 86,\ 240,\ 108,\ 394,\ 262,\ 284 \pmod{418}.$$

4. Astendajate ja algjuurte leidmine indeksite tabelite abil. Indeksite tabeleid saab kasutada ka näiteks järgmist tüüpi ülesannete lahendamiseks.

a) Määrata astendaja, millele kuulub antud arv a modulo p.

b) Leida kõik algjuured modulo p.

c) Leida kõik arvud, mis kuuluvad antud astendajale δ, kus $\delta \mid p-1$ (p - algarv).

Kõikide nende ülesannete lahendamiseks lähtume kongruentsist

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

Esimese ülesande lahendamiseks tuleb leida vähim naturaalarv δ, mis seda kongruentsi rahuldab.

Indekseerimine annab

$$\delta \operatorname{ind} a \equiv 0 \pmod{p-1},$$

millest

$$\delta \equiv 0 \left(\bmod \frac{p-1}{(\operatorname{ind} a,\ p-1)} \right).$$

Vähim naturaalarv, mis kongruentsi rahuldab, võrdub mooduliga. Seega arv a kuulub astendajale

$$\delta = \frac{p-1}{(\operatorname{ind} a,\ p-1)} \qquad (7)$$

Erijuhul, kui (ind a, p-1) = 1, kuulub arv a astendajale p-1 = $\varphi(p)$ ja on järelikult algjuur. Niisiis kõigi algjuurte leidmiseks modulo p tuleb leida kõik arvud a, mille korral

(8) (ind a, p-1) = 1.

Lõpuks saame valemi (7) abil kätte ka kõik arvud a, mis kuuluvad antud astendajale δ, kus δ on arvu p-1 jagaja. Nagu näha, kuuluvad astendajale δ parajasti need arvud a, mille korral

$$(\text{ind } a,\ p-1) = \frac{p-1}{\delta}\ .$$

Erijuhul, kui δ = p-1, saame siit valemi (8), mis annab tarviliku ja piisava tingimuse selleks, et arv a oleks algjuur.

Näide 7. Leiame astendajad, millele kuuluvad arvud 2, 3 ja 4 modulo 13, ning teeme kindlaks, kas nende arvude hulgas leidub algjuuri.

Tulemused saame otsekohe valemist (7), kui oleme indeksite tabelist leidnud, et ind 2 = 1, ind 3 = 4, ind 4 = 2. Selleks aga, et valemit (7) mitte meeles pidada, vaatleme ülesande lahendamist astendaja definitsioonist lähtudes. Arvu 2 korral leiame väikima naturaalarvu δ, mille puhul

$$2^{\delta} \equiv 1 \pmod{13}.$$

Siit saame indekseerimisel

$$\delta \text{ ind } 2 \equiv 0 \pmod{12}$$

ehk

$$\delta \equiv 0 \pmod{12}.$$

Väikim naturaalarv, mis seda kongruentsi rahuldab, on δ = 12. Seega kuulub arv 2 astendajale 12 ja on järelikult algjuur.

Astendaja leidmiseks, millele kuulub arv 3, lahendame kongruentsi

$$3^{\delta} \equiv 1 \pmod{13}.$$

Indekseerimisel saame

$$\delta \operatorname{ind} 3 \equiv 0 \pmod{12}$$

ehk

$$4\delta \equiv 0 \pmod{12}.$$

Viimase kongruentsiga on ekvivalentne kongruents

$$\delta \equiv 0 \pmod{3}.$$

Väikseim naturaalarv, mis seda kongruentsi rahuldab, on $\delta = 3$. Seega kuulub arv 3 astendajale 3 modulo 13.

Analoogiliselt saame, et arv 4 kuulub astendajale 6.

Näide 8. Leiame kõik algjuured modulo 19.

Algjuurteks on kõik need arvud a, mille indeks on arvuga 18 ühistegurita. Sellisteks indeksiteks on

$$\operatorname{ind} a \equiv 1, 5, 7, 11, 13, 17 \pmod{18},$$

millest

$$a \equiv 2, 13, 14, 15, 3, 10 \pmod{19}.$$

Kõik arvud a, mis neid kongruentse rahuldavad, on algjuured. Väikseimatest naturaalarvudest koosnevas jääkide süsteemis mod 19 on algjuurteks seega 2, 3, 10, 13, 14 ja 15. Viimaste arv on $\varphi(18) = 6$.

Harjutusülesandeid.

8.12. Modulo 13 on algjuurteks arvud 6 ja 7 (kontrollida!). Koostada indeksite tabelid mod 13 alusel 6 ja alusel 7.

8.13. Koostada indeksite tabel modulo 10, valides aluseks vähima algjuure.

8.14. Milliste algarvu p üldkujude korral on iga arv 5. astme jäägiks modulo p, milliste p üldkujude korral mitte? Kui palju on viimasel juhul 5. astme jääke taandatud jääkide süsteemis modulo p?

8.15. Kasutades indeksite tabelit modulo 23, lahendada järgmised kongruentsid:

a) $15x^{13} \equiv 14 \pmod{23}$; b) $x^{10} \equiv 10 \pmod{23}$;

c) $12x^{11} \equiv 1000 \pmod{23}$; d) $13^x \equiv 6 \pmod{23}$;

e) $5 \cdot 17^{3x+2} \equiv 12 \pmod{23}$.

8.16. Indeksite tabelite abil leida jääk, mis tekib arvu 17^{17} jagamisel 43-ga.

8.17. Leida jääk, mis tekib arvu $198^{10\,000}$ jagamisel 97-ga.

8.18. Lahendada kongruentsid:

a) $37x^{15} \equiv 62 \pmod{73}$; b) $2x^8 \equiv 5 \pmod{13}$;

c) $27x^5 \equiv 25 \pmod{31}$; d) $8x^{26} \equiv 37 \pmod{41}$;

e) $23x^3 \equiv 15 \pmod{73}$; f) $37x^8 \equiv 59 \pmod{61}$;

g) $x^2 \equiv 3 \pmod{37}$; h) $2x^2 \equiv 57 \pmod{71}$.

8.19. Lahendada lineaarkongruentsid:

a) $39x \equiv 84 \pmod{97}$; b) $125x \equiv 7 \pmod{79}$;

c) $4x \equiv 13 \pmod{37}$; d) $37x \equiv 5 \pmod{221}$;

e) $47x \equiv 13 \pmod{667}$.

8.20. Lahendada eksponentkongruentsid:

a) $2^x \equiv 7 \pmod{67}$; b) $16^x \equiv 11 \pmod{53}$;

c) $5^x \equiv 16 \pmod{19}$; d) $2 \cdot 3^{2x+1} \equiv 6 \pmod{37}$;

e) $3^{5x+3} \equiv 34 \pmod{61}$; f) $79^x \equiv 69 \pmod{89}$.

8.21. Lahendada kongruentsid kordarvulise mooduli järgi:

a) $x^2 \equiv 3 \pmod{13 \cdot 23}$; b) $x^3 \equiv 12 \pmod{13 \cdot 19}$;

c) $x^5 \equiv 10 \pmod{77}$; d) $x^4 \equiv 7 \pmod{29.31}$.

8.22. Leida kõik algjuured

a) modulo 31,

b) modulo 29,

c) modulo 43.

8.23. Teha kindlaks, millistele astendajatele kuuluvad arvud 2, 11, 17, 77 ja 103 modulo 37. Kas mõni neist arvudest on algjuur modulo 37?

8.24. Leida kõik arvud, mis kuuluvad astendajale 7 modulo 29.

8.25. Jaotada kõik mooduliga 31 ühistegurita arvud klassidesse nende kuuluvuse järgi erinevatele astendajatele modulo 31 (ühele ja samale astendajale kuuluvad arvud peavad kuuluma ühte ja samasse klassi, erinevatele astendajatetele kuuluvad arvud aga erinevatesse klassidesse).

§ 4.* RATSIONAALARVU q-NDMURRU PERIOODI PIKKUS

Hariliku murru teisendamisel kümnendmurruks saadakse kas lõplik kümnendmurd või lõpmatu perioodiline kümnendmurd. Sama juhtub murru teisendamisel 8-ndmurruks (8-ndsüsteemi murruks) ja üldiselt q-ndmurruks (q - arvusüsteemi alus). Mõnede käesoleva peatüki mõistete ja tulemuste rakendusena tõestame järgmise teoreemi.

Teoreem 8.12. Kui $(q, b) = 1$ ja q kuulub astendajale δ modulo b, siis taandumatu lihtmurru $\frac{a}{b}$ teisendamisel q-ndmurruks

$$\frac{c_1}{q} + \frac{c_2}{q^2} + \frac{c_3}{q^3} + \ldots = 0,c_1c_2c_3 \ldots$$

saadakse lõpmatu puhtperioodiline (q-nd)murd, mille perioodi pikkus on δ.

Tõestus. Kasutades jäägiga jagamise algoritmi, võime kirjutada:

$$qa = bc_1 + r_1, \quad 0 \leq r_1 < b.$$

Siinjuures $(r_1, b) = (qa, b) = 1$, sest $(q, b) = 1$ ja $(a, b) = 1$. Seega $r_1 \neq 0$, s.t. $1 \leq r_1 < b$ ja $\frac{r_1}{b}$ on taandumatu lihtmurd. Niisiis on arvupaari r_1, b jaoks täidetud samad tingimused, mis paari a, b jaoks. Seetõttu saame jäägiga jagamise algoritmi korduval rakendamisel lõpmatu seoste jada:

$$
\begin{aligned}
qa &= bc_1 + r_1, && 1 \leq r_1 < b \\
qr_1 &= bc_2 + r_2, && 1 \leq r_2 < b \\
qr_2 &= bc_3 + r_3, && 1 \leq r_3 < b \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
qr_{k-1} &= bc_k + r_k, && 1 \leq r_k < b \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots
\end{aligned}
\qquad (1)
$$

Siinjuures iga $i = 1,2, \ldots$ korral

$$0 \leq c_i = \frac{qr_{i-1} - r_i}{b} < \frac{qb - r_i}{b} = q - \frac{r_i}{b} < q.$$

Seega kujutavad kõik täisarvud c_i endast q-ndsüsteemi <u>numbreid</u>. Jaganud võrdused vastavalt suurustega qb, q^2b, q^3b,... ..., q^kb, ..., saame järk-järgult asendades

$$\frac{a}{b} = \frac{c_1}{q} + \frac{r_1}{qb} = \frac{c_1}{q} + \frac{c_2}{q^2} + \frac{r_2}{q^2b} = \ldots =$$

$$= \frac{c_1}{q} + \frac{c_2}{q^2} + \frac{c_3}{q^3} + \ldots + \frac{c_k}{q^k} + \frac{r_k}{q^kb}.$$

Korrutades viimast võrdust suurusega q^kb, saame

$$q^ka = \left(c_1q^{k-1} + c_2q^{k-2} + \ldots + c_k\right)b + r_k.$$

Võtame $k = \delta$ ja arvestame, et q kuulub astendajale δ modulo b, s.t. $q^\delta \equiv 1 \pmod b$. Seosest

$$q^\delta a = \left(c_1q^{\delta-1} + c_2q^{\delta-2} + \ldots + c_\delta\right)b + r_\delta$$

saame siis

$$r_\delta \equiv q^\delta a \equiv a \pmod b.$$

Kuna aga $1 \leq a < b$ ja $1 \leq r_\delta < b$, siis $r_\delta = a$. Viimasest järeldub, et δ sammu järel võrdused (1) korduvad perioodili-

selt. Sealjuures on δ ilmselt vähima perioodi pikkus ($q^{\eta} \not\equiv 1 \pmod{b}$, kui $1 \leq \eta < \delta$). Seega on

$$\frac{a}{b} = 0,(c_1 c_2 \ldots c_\delta),$$

kus c_1, c_2, ..., c_δ on q-ndsüsteemi numbrid ($0 \leq c_i < q$). Teoreem on tõestatud.

Teatavasti saab arv q kuuluda modulo b vaid $\varphi(b)$ jagajatele (teoreemi 8.3 järeldus 2). Seetõttu võib arvu $\frac{a}{b}$ q-ndmurru perioodi pikkus erinevatel q väärtustel olla ikka vaid $\varphi(b)$ jagaja. Näiteks võib see arvu $\frac{a}{11}$ korral olla kas 1, 2, 5 või 10, sest $\varphi(11) = 10$.

Erijuhul, kui b on moodul, mille korral eksisteerivad algjuured (näiteks b on algarv), ja q on algjuur modulo b, siis sellises arvusüsteemis on arvu $\frac{a}{b}$ q-ndmurru perioodi pikkus maksimaalne, nimelt $\varphi(b)$.

Algjuured mod 11 on 2, 6, 7, 8, aga ka 13, 17, 18, 19, 24, 28, 29, 30, ... Seetõttu on 2-nd-, 6-nd-, 7-nd-, 8-nd-, 13-nd-, 17-nd- jne. -süsteemis taandumatu lihtmurru $\frac{a}{11}$ perioodi pikkus 10, teistes arvusüsteemides (kus $q \neq k \cdot 11$) kas 1, 2 või 5 (10-ndsüsteemis näiteks 2, 12-ndsüsteemis 1). Mujide, lihtne on näha, et kui $q = kb + 1$, siis arvu $\frac{a}{b}$ q-ndmurru perioodi pikkus on 1, sest siis $q^1 \equiv 1 \pmod{b}$ ja q kuulub astendajale 1. On ka selge, et teistel juhtudel on perioodi pikkus suurem, näiteks $q = kb - 1$ korral on see alati 2 (tõestada!).

Teoreem 8.13. Kui eelmise teoreemi tingimustel $\frac{a}{b} = 0,(c_1 c_2 \ldots c_\delta)$ ja arvud c_1, c_2, ..., c_δ ning r_1, r_2, ...

..., r_δ on määratud seostega (1), siis

$$(2)\qquad \frac{r_i}{b} = 0,(c_{i+1}\ldots c_\delta c_1 \ldots c_i), \quad i = 0,1,\ldots,\delta-1,$$

kus $r_o = a$.

Tõestus. Kuna $r_\delta = r_o = a$, $r_{\delta+1} = r_1$, ..., siis võib võrdused (1), alates i-ndast kirjutada kujul

$$(3)\qquad \begin{aligned} qr_i &= bc_{i+1} + r_{i+1},\\ &- - - - - - - - - - -\\ qr_{\delta-1} &= bc_\delta + r_o,\\ qr_o &= bc_1 + r_1,\\ &- - - - - - - - - - -\\ qr_{i-1} &= bc_i + r_i, \end{aligned}$$

kus $0 \leqslant c_k < b$, $1 \leqslant r_k < b$. Et $(r_i, b) = 1$ ja q kuulub astendajale δ modulo b, siis eelmise teoreemi põhjal moodustavad esimesed δ numbrit c_k murru $\frac{r_i}{b}$ perioodi tema q-ndmurruks arenduses, s.t. kehtib seos (2).

Nagu näha, võib murdude $\frac{r_1}{b}, \frac{r_2}{b}, \ldots, \frac{r_{\delta-1}}{b}$ perioodilised q-ndmurrud saada arvu $\frac{a}{b}$ q-ndmurrust tsüklilise ülekandega.

Kui q on algjuur modulo b ja b on algarv, siis perioodi pikkus on b-1 ja erinevate jääkide arv seostes (1) on b-1 (s.t. jäägid moodustavad modulo b taandatud jääkide süsteemi). Siis saadakse kõikide lihtmurdude $\frac{1}{b}, \frac{2}{b}, \ldots, \frac{b-1}{b}$ q-ndmurrud ühest q-ndmurrust tsüklilise ülekande teel.

Näide 1. Olgu q = 10. Arvusüsteemi alus 10 on algjuureks mod 17. Teades, et

$$\frac{1}{17} = 0,(0588\ 2352\ 9411\ 7647),$$

leiame $\frac{13}{17}$ kümnendmurru. Kuna otsesel jagamisel saame perioodi esimesteks numbriteks $\frac{13}{17} = 0,76...$, siis $\frac{13}{17} = 0,(7647\ 0588\ 2352\ 9411)$.

Üldjuhul, kui q ei ole algjuur, on $\delta < \varphi(b)$ ja kõikide taandumatute lihtmurdude $\frac{a}{b}$ q-ndmurde ei saa ühest murrust tsüklilise ülekandega.

Näide 2. Olgu $q = 10$ ja $b = 13$. Alus 10 ei ole algjuur modulo 13, vaid kuulub astendajale 6. Siin $\frac{1}{13} = 0,(076923)$ ja $\frac{2}{13} = 0,(153846)$. Nendest kahest murrust saadakse kõik ülejäänud tsükliliste ülekannetega. Nimelt saadakse esimesest murdude $\frac{3}{13}$, $\frac{4}{13}$, $\frac{9}{13}$, $\frac{10}{13}$ ja $\frac{12}{13}$ kümnendmurrud, teisest $\frac{5}{13}$, $\frac{6}{13}$, $\frac{7}{13}$, $\frac{8}{13}$ ja $\frac{11}{13}$ kümnendmurrud.

Märgime, et arv 10 on algjuur järgmiste 100-st väiksemate algarvuliste moodulite b korral:

$$7,\ 17,\ 19,\ 23,\ 29,\ 47,\ 59,\ 61,\ 97.$$

Seega on sellise nimetajaga hariliku murru $\frac{a}{b}$ perioodi pikkus $b-1$.

Näide 3. Teeme kindlaks arvu $\frac{a}{97}$ 8-ndmurru perioodi pikkuse.

Leiame, millisele astendajale kuulub 8 modulo 97. Selleks leiame vähima naturaalarvu δ, mis rahuldab kongruentsi

$$8^{\delta} \equiv 1 \pmod{97}.$$

Indekseerimisel saame

$$\delta \operatorname{ind} 8 \equiv 0 \pmod{96}$$

ehk

$$6\delta \equiv 0 \pmod{96},$$

millest

$$\delta \equiv 0 \pmod{16}.$$

Seega arvu $\frac{a}{97}$ 8-ndmurru perioodi pikkus on 16.

Juhtu $(q, b) > 1$ käsitleme lihtsuse mõttes vaid $q = 10$ korral. Üldjuhul on käsitlus analoogiline.

Olgu taandumatu murru $\frac{a}{b}$ nimetaja $b = 2^{\alpha} 5^{\beta} b_1$, kus $(b_1, 10) = 1$ ja $b_1 > 1$ (kui $b_1 = 1$, siis saame lõpliku kümnendmurru). Tähistame $n = \max\{\alpha, \beta\}$. Siis

$$\frac{a}{b} = \frac{1}{10^n} \cdot \frac{2^{n-\alpha} 5^{n-\beta} a}{b_1} = \frac{1}{10^n}\left(T + \frac{a_1}{b_1} \right),$$

kus T on täisarv, $(a_1, b_1) = 1$ ja $1 \leq a_1 < b_1$. Taandumatu lihtmurd $\frac{a_1}{b_1}$ annab arendamisel puhtperioodilise kümnendmurru, mille perioodi pikkus võrdub astendajaga δ, millele kuulub 10 modulo b_1. Sellele lisandub täisosa T ja lõpuks tuleb kogu murdu jagada 10^n-ga, s.t. nihutada koma n koha võrra vasakule. Saame segaperioodilise kümnendmurru, mille perioodi ees on n kümnendkohta. Seega saame tulemuse järgmiselt:

$$\frac{a}{b} = \frac{1}{10^n}\left(T + \frac{a_1}{b_1} \right) = \frac{1}{10^n} \cdot T,(c_1 c_2 \ldots c_{\delta}) =$$

$$= t,t_1 t_2 \ldots t_n (c_1 c_2 \ldots c_{\delta}).$$

Näide 4. Nagu ülal märgitud, on 10 algjuur modulo 7, s.t. 10 kuulub astendajale $\varphi(7) = 6$ modulo 7. Seetõttu on kõikide taandumatute murdude $\frac{a}{7 \cdot 2^{\alpha} \cdot 5^{\beta}}$ kümnendmurdude perioodi pikkus 6, enne esimest perioodi on aga n kümnendkohta,

kus $n = \max\{\alpha, \beta\}$. Näiteks saame $\frac{101}{140} = \frac{101}{2^2 \cdot 5 \cdot 7}$ korral

$$\frac{101}{140} = \frac{1}{10^2} \cdot \frac{505}{7} = \frac{1}{10^2}\left(72 + \frac{1}{7}\right) = \frac{1}{10^2} \cdot 72,(142857) =$$

$$= 0,72(142857).$$

Harjutusülesandeid.

8.26. Leida numbrite arv perioodis taandumatute hariliku murdude $\frac{a}{b}$ teisendamisel kümnendmurdudeks, kui b on järgmine: a) 37, b) 43, c) 59, d) 67, e) 89, f)97, g) 77, h) 91, i) 51.

8.27. Leida numbrite arv kümnendmurru perioodis ja kümnendkohtade arv enne perioodi, kui kümnendmurruks teisendatava hariliku taandumatu murru nimetaja on a) 220, b) 1150, c) 2380.

8.28. Leida taandumatu murru $\frac{a}{b}$ kaheksandmurru perioodi pikkus samadel b väärtustel, mis ülesandes 8.26.

9.29. Teha kindlaks, millistes arvusüsteemides on murru $\frac{1}{17}$ perioodi pikkus 16, millistes 4.

8.30. Teades, et kümnendsüsteemis

$\frac{1}{19} = 0,(052631578947368421)$, leida $\frac{2}{19}$, $\frac{5}{19}$, $\frac{10}{19}$.

*8.31. Määrata taandumatu kümnendmurru $\frac{a}{10^k}$ perioodi pikkus kaheksandsüsteemis.

*8.32. Leida kümnendmurru 0,(14634) perioodi pikkus kaheksandsüsteemis.

IX. ADITIIVSE ARVUTEOORIA KÜSIMUSI

Aditiivne arvuteooria on arvuteooria osa, mis käsitleb naturaalarvude esitamist etteantud tüüpi liidetavate summana. Võidakse näiteks nõuda, et liidetavad oleksid algarvud, täisarvude ruudud, nende n-ndad astmed või ka muud tüüpi täisarvud. Taoliste esituste eksisteerimise probleemi võib vaadelda kui vastavate diofantiliste võrrandite lahenduvuse küsimust, esituste leidmist aga kui nende diofantiliste võrrandite lahendamist.

§1. NATURAALARVUDE ESITAMINE KAHE RUUDU SUMMANA

On ilmne, et leidub lõpmata palju naturaalarve, mis on esitatavad kahe täisarvu ruudu summana, kasvõi arvud $n^2 + 1^2$, kus $n = 0,1,2,\ldots$ Aga juba esimeste naturaalarvude seas leidub selliseid, mida ei saa esitada kahe ruudu summana (küll aga saab esitada suurema arvu täisarvude ruutude summana):

$$3 = 1^2 + 1^2 + 1^2,$$
$$6 = 2^2 + 1^2 + 1^2,$$
$$7 = 2^2 + 1^2 + 1^2 + 1^2 \text{ jne.}$$

Käesolevas paragrahvis püüame lahendada küsimuse, millised

naturaalarvud on esitatavad kahe täisarvu ruudu summana, millised mitte. Teisiti öeldes, püüame kindlaks teha, milliste naturaalarvude N korral on diofantiline võrrand

$$x^2 + y^2 = N$$

lahenduv, milliste korral mitte.

Olgu N = p esialgu paaritu algarv. Märgime kõigepealt, et kui mingite täisarvude x ja y korral

(1) $$x^2 + y^2 = p,$$

siis (x, p) = (y, p) = 1. Tõepoolest, kui oleks (x, p) = p, siis oleks ka (y, p) = p ja vasak pool jaguks p^2-ga, mis on aga võimatu.

Teoreem 9.1. Selleks et paaritu algarv p oleks esitatav kahe naturaalarvu ruudu summana, on tarvilik ja piisav, et p oleks kujuga 4n + 1.

Tõestus. Tarvilikkus. Võrduse (1) kehtivuseks on tarvilik, et

$$x^2 + y^2 \equiv 0 \pmod{p}$$

ehk

(2) $$x^2 \equiv -y^2 \pmod{p}.$$

Kuna siin $(-y^2, p) = (y, p) = 1$, siis ruutkongruentsi (2) lahenduvuseks on tarvilik ja piisav (vt. VII pt. § 2), et Legendre'i sümbol $\left(\frac{-y^2}{p}\right) = 1$. Kuid

$$\left(\frac{-y^2}{p}\right) = \left(\frac{y^2}{p}\right)\cdot\left(\frac{-1}{p}\right) = \left(\frac{-1}{p}\right) = \left(-1\right)^{\frac{p-1}{2}} = \begin{cases} 1, \text{ kui } p = 4n + 1 \\ -1, \text{ kui } p = 4n + 3. \end{cases}$$

Seega ükski algarv kujul 4n + 3 ei ole esitatav kahe täis-

arvu ruudu summana. Selleks aga, et p oleks esitatav kahe täisarvu ruudu summana, on tarvilik, et tal oleks kuju $p = 4n + 1$.

Piisavus. Näitame, et iga algarv $p = 4n + 1$ on esitatav kahe naturaalarvu ruudu summana.

Et $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = (-1)^{2n} = 1$, siis on lahenduv kongruents

$$t^2 \equiv -1 \pmod{p}. \tag{3}$$

Kuna kongruentsil (3) on kaks lahendit, mis avalduvad kujul

$$t \equiv \pm t_0 \pmod{p},$$

siis võib üldsust kitsendamata eeldada, et (miks?)

$$0 < t_0 < \frac{p}{2}. \tag{4}$$

Arendame ratsionaalarvu $\frac{t_0}{p}$ ahelmurruks (täisosa $a_1 = 0$):

$$\frac{t_0}{p} = [0, a_2, a_3, \ldots, a_n]$$

ja arvutame lähismurrud $\frac{P_1}{Q_1} = \frac{0}{1}$, $\frac{P_2}{Q_2} = \frac{1}{a_2}$, ... Kuna $Q_1 < Q_2 < \ldots < Q_{n-1} < Q_n$, $Q_1 = 1$ ja $Q_n = p$, siis leiduvad alati sellised naabermurrud $\frac{P_s}{Q_s}$ ja $\frac{P_{s+1}}{Q_{s+1}}$, mille korral $Q_s < \sqrt{p} < Q_{s+1}$. Kuna

$$\left| \frac{t_0}{p} - \frac{P_s}{Q_s} \right| = \frac{|t_0 Q_s - p P_s|}{p Q_s} < \frac{1}{Q_s Q_{s+1}},$$

siis

$$(t_0 Q_s - p P_s)^2 < \frac{p^2}{Q_{s+1}^2} < p,$$

millest

(5) $$(t_0Q_s - pP_s)^2 + Q_s^2 < p + Q_s^2 < 2p.$$

Võrratuse (5) vasaku osa saame pärast sulgude avamist esitada kujul

(6) $$(t_0^2 + 1)Q_s^2 + Np,$$

kus N on täisarv. Et $t_0^2 \equiv -1 \pmod p$, siis $(t_0^2 + 1) \vdots p$ ja seega avaldis (6) ehk võrratuse (5) vasak pool jagub p-ga. Et ta on positiivne ja väiksem kui 2p, siis

(7) $$(t_0Q_s - pP_s)^2 + Q_s^2 = p.$$

Sellega on näidatud, et algarv $p = 4n + 1$ on esitatav kahe naturaalarvu ruudu summana. Saab tõestada, et see esitus on ühene (vt. näit. [4], lk. 158).

Teoreemi 9.1 tõestuse käigus saime ühtlasi meetodi algarvu $p = 4n + 1$ esitamiseks kahe ruudu summana. Kasutame seda järgnevas näites.

Näide 1. Esitame algarvu $89 = 4 \cdot 22 + 1$ kahe ruudu summana.

Kongruentsi

$$t^2 \equiv -1 \equiv 88 \pmod{89}$$

lahendamisel (näit. indeksite tabeli abil) saame $t \equiv \pm 34 \pmod{89}$. Seega $t_0 = 34 < \frac{89}{2}$. Arendame murru $\frac{34}{89}$ ahelmurruks ja leiame lähismurrud:

34		89	34	21	13	8	5	3	2	1
		0	2	1	1	1	1	1	1	2
0	1	0	1	1	2	3	5	8	13	34
1	0	1	2	3	5	8	13	21	34	89

Kuna $\sqrt{89} = 9,\ldots$, siis $Q_s = 8$ ja $Q_{s+1} = 13$. Arvestades veel, et $P_s = 3$, saame valemi (7) abil esituse

$$89 = (34\cdot 8 - 89\cdot 3)^2 + 8^2 = 5^2 + 8^2.$$

Praktiliselt saab tulemuse tavaliselt kiiremini proovimise meetodil. Selleks tarvitseb arvust p lahutada järjestikuste naturaalarvude ruute seni, kuni vahe tuleb täisruut.

Edasi käsitleme kordarvu lahutamist kahe täisarvu ruudu summaks.

Teoreem 9.2. Selleks et naturaalarv N oleks esitatav kahe täisarvu ruudu summana, on tarvilik ja piisav, et ta ei sisaldaks teguritena algarve kujuga $4n + 3$ paaritul astmel.

Tõestus. Tarvilikkus. Olgu naturaalarv N esitatav kujul

$$N = x^2 + y^2 \tag{8}$$

ja sisaldagu ta algtegurit $q = 4n + 3$ teatud astmel (võib eeldada, et astendaja on vähemalt 1, sest muidu polegi midagi tõestada). Näitame, et siis N sisaldab seda tegurit paarisastmel. Seose (8) tõttu kehtib kongruents

$$x^2 + y^2 \equiv 0 \pmod{q} \tag{9}$$

ehk

$$x^2 \equiv -y^2 \pmod{q}.$$

Siin ei saa olla $(y^2, q) = 1$, sest $q = 4n + 3$ tõttu saaksime siis Legendre'i sümboli väärtuseks

$$\left(\frac{-y^2}{q}\right) = \left(\frac{-1}{q}\right) = -1,$$

mis näitab, et kongruents (9) pole võimalik. Niisiis

$(y^2, q) = q$ ehk $y \equiv 0 \pmod q$, millest (9) tõttu ka $x \equiv 0 \pmod q$. Siis aga x ja y jaguvad q-ga ja seose (8) tõttu N jagub q^2-ga. Seega sisaldab N tegurit q vähemalt astmel 2. Seetõttu $N = q^2 N_1$ ja pärast võrduse (8) jagamist q^2-ga saame, et N_1 on jälle kahe ruudu summa. Kui sealjuures N_1 sisaldab veel tegurit q, siis sama arutlus näitab, et ta sisaldab ka tegurit q^2. Niiviisi edasi minnes saame, et arv N, mis on esitatav kahe ruudu summana, sisaldab algtegureid kujul $q = 4n + 3$ vaid paarisastmel.

Piisavus. Sisaldagu naturaalarv N teguritena arvu 2, paaritute algarvude $p_i = 4m_i + 1$ ja kordarvude q_j^2 astmeid, kus q_j on algarvud kujul $q_j = 4n_j + 3$. Ilmselt on kõik need tegurid esitatavad kahe täisarvu ruudu summana:

$$2 = 1^2 + 1^2, \quad p_i = x_i^2 + y_i^2, \quad q_j^2 = q_j^2 + 0^2.$$

Teoreemi väide: "arv N on esitatav kahe täisarvu ruudu summana", järeldub nüüd järgmisest samasusest, kui seda korduvalt rakendada:

$$(10) \qquad (a^2 + b^2)(c^2 + d^2) = A^2 + B^2,$$

kus $A = ac - bd$, $B = ad + bc$.

Samasust (10) võib vahetult kontrollida, kuid ta järeldub ka kompleksarvude $\alpha = a + bi$, $\beta = c + di$ moodulite korrutise omadusest

$$|\alpha|^2 |\beta|^2 = |\alpha\beta|^2.$$

Järeldus. Ükski naturaalarv kujul $4m + 3$ ei ole esitatav kahe ruudu summana.

Tõepoolest, selline arv sisaldab vähemalt üht algtegu-

rit $q = 4n + 3$ paaritul astmel.

Märgime, et järelduses sisalduva väite võib tõestada ka otseselt: kui paaritu arv $4m + 3$ oleks esitatav kahe ruudu summana, siis üks liidetavatest peaks olema paarisarvu ruut, teine paaritu arvu ruut, s.t.

$$4m + 3 = (2k)^2 + (2l + 1)^2.$$

Viimane võrdus ei saa aga kehtida, sest $4m + 3 \equiv 3 \pmod 4$ ja $(2k)^2 + (2l + 1)^2 \equiv 1 \pmod 4$.

Näide 2. Kordarv 319 ei ole esitatav kahe ruudu summana, sest $319 = 4 \cdot 79 + 3$.

Teoreemi 9.2 võib sõnastada veel teisiti: diofantiline võrrand $x^2 + y^2 = N$ on lahenduv parajasti siis, kui N ei sisalda algarvulisi tegureid $q = 4n + 3$ paaritul astmel.

Olukord muutub mõnevõrra, kui lubame vaid selliseid naturaalarvude esitusi kahe ruudu summana, milles liidetavad on ühistegurita, s.t.

(11) $$N = x^2 + y^2, \quad (x, y) = 1.$$

Võrduse (11) kehtivusest järeldub kongruentsi

$$x^2 + y^2 \equiv 0 \pmod N, \quad (x, y) = 1,$$

kehtivus, millest omakorda saame

(12) $$x^2 + y^2 \equiv 0 \pmod p, \quad (x, y) = 1,$$

kus p on arvu N mistahes algtegur. Siin ei saa olla $(x, p) = p$ ega $(y, p) = p$, sest vastasel juhul oleks $(x, y) = p$. Tingimusel $(y, p) = 1$ on aga kongruentsi (12) kehtivuseks tarvilik ja piisav, et $\left(\frac{-y^2}{p}\right) = \left(\frac{-1}{p}\right) = 1$, mis on

võimalik vaid juhul, kui $p = 4n + 1$. Seega ei saa tingimusi (11) rahuldav arv N sisaldada tegurina algarvu $q = 4n + 3$. Ta ei saa jaguda ka 4-ga, sest jagumise korral oleksid liidetavad paarisarvud.

Arvestades veel teoreemi 9.2 oleme saanud järgmise tulemuse.

Teoreem 9.3. Võrrandil

$$x^2 + y^2 = N \quad (N > 0)$$

on olemas lahend ühistegurita täisarvudes parajasti siis, kui arvu N kanooniline kuju ei sisalda algtegureid p kujul $4n + 3$ ja kui $4 \nmid N$.

Teoreemi 9.3 võib kasutada arvude teguriteks lahutamise lihtsustamiseks. Kui naturaalarv N on esitatav kujul $N = x^2 + y^2$, kus $(x, y) = 1$, siis võib ta sisaldada algteguritena arvu 2 ja algarve kujul $p = 4n + 1$, ei saa aga sisaldada tegureid kujul $4n + 3$.

Näide 3. Arvu $N = 20^2 + 17^2 = 689$ algtegureid tarvitseb otsida arvust $\sqrt{689} = 26,...$ väiksemate algarvude $p = 4n + 1$ hulgast. Sellisteks algarvudeks on vaid 5, 13 ja 17. Kontroll näitabki, et $689 = 13 \cdot 53$.

Analoogiliselt eeltooduga võib uurida küsimust, milliseid arve N saab esitada kujul

(13) $\quad N = x^2 + ay^2$, kus $(x, y) = 1$ (a - antud arv),

ja otsustada, millise kujuga algtegureid võivad sisaldada seda tüüpi arvud. Selleks paneme tähele, et võrdusest (13) järeldub arvu N iga algteguri p korral kongruents

(14) $$x^2 \equiv -ay^2 \pmod{p}.$$

Kui $(a, p) = 1$, siis tingimuse $(x, y) = 1$ tõttu $(-ay^2, p) = 1$ ja kongruents (14) kehtib parajasti siis, kui

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

Siit järeldub (kuidas?), et kui $\left(\frac{-a}{p}\right) = -1$, siis arv N ei ole esitatav kujul (13). Kui aga arv N on esitatav kujul (13), siis ta ei saa sisaldada neid algtegureid p, mille korral $\left(\frac{-a}{p}\right) = -1$. Näiteks erijuhul $a = 2$ saame

$$\left(\frac{-2}{p}\right) = \begin{cases} 1, \text{ kui } p = 8n + 1 \text{ või } p = 8n + 3 \\ -1, \text{ kui } p = 8n + 5 \text{ või } p = 8n + 7, \end{cases}$$

millest järeldub, et arvud kujul $N = x^2 + 2y^2$, $(x, y) = 1$, ei saa sisaldada teguritena algarve $p = 8n + 5$ ja $p = 8n + 7$ (ühegi naturaalarvu n korral).

Näide 4. Arvu $N = 11^2 + 2 \cdot 30^2 = 1921$ tegureid tarvitseb otsida arvust $\sqrt{1921} = 43,...$ väiksemate algarvude hulgast, mille kuju ei ole $p = 8n + 5$ ega $p = 8n + 7$, seega arvude 2, 3, 11, 17, 19, 41 ja 43 hulgast. Kasutades nimetatud arvudega jagumise tunnuseid või kontrollides otseselt, leiame, et $1921 = 17 \cdot 113$.

Harjutusülesandeid.

9.1. Kasutades teoreemi 9.1 tõestamise käigus näidatud meetodit, esitada kahe ruudu summana järgmised arvud:

a) 97, b) 197, c) 1997, d) 2221.

9.2. Teoreemide 9.1 ja 9.2 alusel kontrollida, kas järgmised arvud on esitatavad kahe ruudu summana, ja kui on,

siis leida vastav esitus käesolevas paragrahvis kirjeldatud proovimise meetodil (on soovitav kasutada täisarvude ruutude tabelit):

a) 1951, b) 3257, c) 3521,

d) 3543, e) 6824, f) 3590, g) 3592.

*9.3. Uurida, millise kujuga algtegureid ei sisalda arvud $N = x^2 + 3y^2$, kus $(x, y) = 1$.

*9.4. Uurida, millise kujuga algtegureid ei sisalda arvud $N = x^2 + 5y^2$, kus $(x, y) = 1$.

§ 2. NATURAALARVUDE ESITAMINE NELJA RUUDU SUMMANA

Nagu nägime eelmises paragrahvis, ei ole mitte iga naturaalarv esitatav kahe täisarvu ruudu summana. Tekib küsimus: ülimalt mitu liidetavat kulub suvalise naturaalarvu esitamiseks täisarvude ruutude summana ja kas liidetavate arv on üldse tõkestatud? Vastuse annab allpool esitatav Lagrange'i teoreem. Viimase tõestamisel on oluline tähtsus järgmisel Euleri samasusel:

$$(a_1^2 + a_2^2 + a_3^2 + a_4^2)(b_1^2 + b_2^2 + b_3^2 + b_4^2) = c_1^2 + c_2^2 + c_3^2 + c_4^2,$$

kus

$$c_1 = a_1b_1 + a_2b_2 + a_3b_3 + a_4b_4,$$
$$c_2 = a_1b_2 - a_2b_1 + a_3b_4 - a_4b_3,$$
$$c_3 = a_1b_3 - a_3b_1 + a_4b_2 - a_2b_4,$$
$$c_4 = a_1b_4 - a_4b_1 + a_2b_3 - a_3b_2.$$

Samasuse kehtivust on võimalik vahetult kontrollida.

Asume nüüd käesoleva paragrahvi põhilise väite tõestamisele.

Teoreem 9.4 (Lagrange, 1770). Iga naturaalarv on esitatav nelja täisarvu ruudu summana.

Tõestus. Tõestame alguses väite mistahes a l g a r v u jaoks. Kuna $2 = 1^2 + 1^2 + 0^2 + 0^2$, siis tarvitseb piirduda vaid paaritute algarvudega (teoreemi 9.1 tõttu võib piirduda isegi vaid algarvudega kujul $4n + 3$, kuid järgnevas tõestuses pole algarvu p kuju oluline). Parema jälgitavuse huvides jaotame tõestuse mitmeks osaks.

1. Näitame, et iga algarvu $p > 2$ jaoks eksisteerivad täisarvud m, x_0, y_0, nii et $1 \leq m < \frac{p}{2}$ ja

$$mp = x_0^2 + y_0^2 + 1,$$

s.t. et algarvu p teatav kordne on esitatav kolme ruudu summana, kus üks liidetavatest on 1.

Vaatleme täisarvude süsteemi

$$0^2,\ 1^2,\ 2^2,\ \ldots,\ \left(\frac{p-1}{2}\right)^2 \tag{1}$$

ja sellest saadavat süsteemi

$$-0^2-1,\ -1^2-1,\ -2^2-1,\ \ldots,\ -\left(\frac{p-1}{2}\right)^2 - 1. \tag{2}$$

Teoreemi 7.2 tõestamise käigus näitasime, et süsteemis (1), millest on 0^2 välja jäetud, ei leidu paarikaupa kongruentseid modulo p. Kuid lihtne on näha, et ükski viimati nimetatud arv ei ole kongruentne ka nulliga modulo p. Niisiis on arvud (1) paarikaupa inkongruentsed modulo p. Siit järeldub, et ka arvud (2) on paarikaupa inkongruentsed. Süsteemides (1) ja (2) on kokku $p + 1$ arvu. See aga tähendab, et süstee-

mis, mis saadakse süsteemide (1) ja (2) ühendamisel, ei saa kõik arvupaarid olla inkongruentsed mod p. Sealjuures modulo p kongruentsetest arvudest kuulub üks süsteemi (1), teine süsteemi (2). Seega leiduvad x_0, y_0, nii et

$$x_0^2 \equiv -y_0^2 - 1 \pmod{p}$$

ehk

$$x_0^2 + y_0^2 + 1 = mp, \tag{3}$$

kus $0 \leq x_0 \leq \frac{p-1}{2}$ ja $0 \leq y_0 \leq \frac{p-1}{2}$. Sealjuures

$$m = \frac{1}{p}(x_0^2 + y_0^2 + 1) \leq \frac{1}{p}\left(2\left(\frac{p-1}{2}\right)^2 + 1\right) =$$

$$= \frac{1}{p} \cdot \frac{p^2 - 2p + 3}{2} < \frac{p}{2}.$$

Seosest (3) nähtub otseselt, et $m \neq 0$, s.t. $m \geq 1$.

2. Eeltõestatu põhjal saab algarvu $p > 2$ teatud kordse mp, kus $1 \leq m < \frac{p}{2}$, esitada nelja ruudu summana (seose (3) vasakule poole lisame liidetava 0^2). Tähistame m_0-ga v ä h i m a sellise naturaalarvu ($1 \leq m_0 < \frac{p}{2}$), mille korral $m_0 p$ on esitatav nelja ruudu summana:

$$m_0 p = a_1^2 + a_2^2 + a_3^2 + a_4^2. \tag{4}$$

Näitame, et siis m_0 on p a a r i t u. Oletame vastupidi, et m_0 on paarisarv, $m_0 = 2m_1$. Siis paaritute liidetavate arv võrduse (4) paremal poolel peab olema paarisarv, s.o. kas 0, 2 või 4. Seega võime arvud a_1, a_2, a_3, a_4 jaotada kaheks paariks nii, et ühte ja samasse paari kuuluvad kas ainult paaritud või ainult paarisarvud. Ühte ja samasse paari kuuluvate arvude summa ja vahe on paarisarvud. Kui ühte paari

kuuluvad arvud a_1 ja a_2, teise aga a_3 ja a_4, siis võime seose (4) esitada kujul

$$m_1 p = \frac{1}{2}(a_1^2 + a_2^2 + a_3^2 + a_4^2) =$$

$$= \left(\frac{a_1+a_2}{2}\right)^2 + \left(\frac{a_1-a_2}{2}\right)^2 + \left(\frac{a_3+a_4}{2}\right)^2 + \left(\frac{a_3-a_4}{2}\right)^2 ,$$

kus paremal seisvad liidetavad on kõik täisarvud ja $1 \leq m_1 < m_0$. See on aga vastuolus eeldusega, et m_0 on vähim naturaalarv, mille korral $m_0 p$ on esitatav nelja täisruudu summana. Seega on m_0 paaritu.

3. Tõestame, et $m_0 = 1$. Teades esialgu vaid seda, et m_0 on paaritu arv, võtame absoluutväärtuselt vähimad jäägid r_i, mille korral

$$a_i \equiv r_i \pmod{m_0}, \qquad i = 1,2,3,4. \tag{5}$$

Siis $|r_i| \leq \frac{m_0-1}{2} < \frac{m_0}{2}$. Kongruentside (5) ja seose (4) tõttu kehtivad kongruentsid

$$r_1^2 + r_2^2 + r_3^2 + r_4^2 \equiv a_1^2 + a_2^2 + a_3^2 + a_4^2 = m_0 p \equiv 0 \pmod{m_0},$$

mistõttu leidub täisarv t, nii et

$$m_0 t = r_1^2 + r_2^2 + r_3^2 + r_4^2 , \tag{6}$$

millest

$$0 \leq t = \frac{1}{m_0}(r_1^2 + r_2^2 + r_3^2 + r_4^2) < \frac{1}{m_0} \cdot 4 \left(\frac{m_0}{2}\right)^2 = m_0 ,$$

s.t.

$$0 \leq t < m_0.$$

Korrutades võrdused (4) ja (6) ning kasutades paragrahvi alguses esitatud Euleri samasust, saame

(7) $m_o^2 pt = (a_1^2 + a_2^2 + a_3^2 + a_4^2)(r_1^2 + r_2^2 + r_3^2 + r_4^2) =$

$= c_1^2 + c_2^2 + c_3^2 + c_4^2$,

kus seoste (5) tõttu

$$c_1 = a_1r_1 + a_2r_2 + a_3r_3 + a_4r_4 \equiv$$
$$\equiv a_1^2 + a_2^2 + a_3^2 + a_4^2 \equiv 0 \pmod{m_o},$$
$$c_2 = a_1r_2 - a_2r_1 + a_3r_4 - a_4r_3 \equiv 0 \pmod{m_o},$$
$$c_3 \equiv 0 \pmod{m_o}, \quad c_4 \equiv 0 \pmod{m_o}.$$

Seega $c_i \vdots m_o$ $(i = 1,2,3,4)$, s.t. $\frac{c_i}{m_o}$ on täisarv. Võrdusest (7) saame

(8) $$pt = \left(\frac{c_1}{m_o}\right)^2 + \left(\frac{c_2}{m_o}\right)^2 + \left(\frac{c_3}{m_o}\right)^2 + \left(\frac{c_4}{m_o}\right)^2.$$

Kuna m_o on v ä h i m n a t u r a a l a r v, mille korral $m_o p$ on esitatav nelja ruudu summana, siin aga tp on nelja ruudu summa, kusjuures $0 \leq t < m_o$, siis $t = 0$. Seetõttu annab võrdus (6) $r_1^2 + r_2^2 + r_3^2 + r_4^2 = 0$, millest $r_i = 0$ $(i = 1,2,3,4)$ ja seoste (5) tõttu

$$a_i \equiv 0 \pmod{m_o} \text{ ehk } m_o \mid a_i, \quad i = 1,2,3,4.$$

Siit $m_o^2 \mid a_1^2 + a_2^2 + a_3^2 + a_4^2$, millest seose (4) tõttu $m_o^2 \mid m_o p$ ja $m_o \mid p$. Kuna p on algarv ja $1 \leq m_o < p$, siis $m_o = 1$ ja seega algarv $p > 2$ on esitatav kujul

$$p = a_1^2 + a_2^2 + a_3^2 + a_4^2.$$

Sellega on teoreem tõestatud kõikide algarvude korral.

4. Teoreemi tõestus mistahes naturaalarvu jaoks järeldub vahetult Euleri samasusest (kuidas?).

§ 3*. ADITIIVSE ARVUTEOORIA TEISI PROBLEEME

1. Waringi probleem. Samal aastal (1770), kui Lagrange tõestas, et iga naturaalarv on esitatav nelja täisarvu ruudu summana, püstitas inglise matemaatik E.Waring üldisema hüpoteesi: iga naturaalarvu $n \geqslant 2$ jaoks eksisteerib selline naturaalarv $r = r(n)$, nii et i g a naturaalarv N on esitatav arvult r mittenegatiivse täisarvu n-nda astme summana, s.t.

$$N = x_1^n + x_2^n + \ldots + x_r^n , \tag{1}$$

kus r ei sõltu N-st. Probleemiks kujunes hüpoteesi tõestamine ja v ä h i m a liidetavate arvu $r = g(n)$ leidmine.

Waringi hüpoteesi tõestus on antud 1909.a. Hilberti poolt. Vähima liidetavate arvu g(n) kohta on teada, et $g(2) = 4$ (Lagrange' teoreem), $g(3) = 9$, $19 \leqslant g(4) \leqslant 35$, $37 \leqslant g(5) \leqslant 40$, $g(6) = 73$, $g(7) = 143$, $g(8) = 279$, ... Lihtne on tõestada järgmist väidet.

Teoreem 9.5. Kehtib hinnang

$$g(n) \geqslant 2^n + \left[\frac{3^n}{2^n}\right] - 2. \tag{2}$$

Tõestus. Võtame naturaalarvu

$$N = 2^n \left[\frac{3^n}{2^n}\right] - 1. \tag{3}$$

Selle arvu esitus kujul (1) võib sisaldada vaid arvude 2 ja 1 n-ndaid astmeid, sest $N < 3^n$. Arvu N kuju tõttu saab liidetavaid kujul 2^n olla kõige enam $\left[\frac{3^n}{2^n}\right] - 1$, ülejäänud lii-

detavad on 1^n. Kui võtta liidetavaid 2^n maksimaalarv, siis liidetavaid kujul 1^n on arvult

$$N - 2^n\left(\left[\frac{3^n}{2^n}\right] - 1\right) = 2^n - 1.$$

Liidetavate üldarv on sel korral

$$\left[\frac{3^n}{2^n}\right] + 2^n - 2. \tag{4}$$

Mõne liidetava 2^n asendamine ühtedega suurendab liidetavate arvu ja seega kujutab arv (4) endast vähimat liidetavate arvu naturaalarvu (3) jaoks. Mõne teise naturaalarvu N jaoks võib vähim liidetavate arv olla suurem kui arv (4). Sellega on teoreem tõestatud.

On huvitav märkida, et kui mitte kõigil, siis vähemalt enamikul juhtudel võib võrratuse seoses (2) asendada võrdusega. Kehtib nimelt järgmine teoreem (vt. [1], lk. 304), mille me esitame tõestuseta.

Teoreem 9.6. Kui $n \neq 4$, $n \neq 5$ ja kehtib võrratus

$$3^n - 2^n\left[\frac{3^n}{2^n}\right] \leq 2^n - \left[\frac{3^n}{2^n}\right], \tag{5}$$

siis

$$g(n) = 2^n + \left[\frac{3^n}{2^n}\right] - 2. \tag{6}$$

Võrratust (5) pole õnnestunud kõikide n väärtuste korral tõestada, kuid on tõestatud, et eksisteerib n_0, millest kõikide suuremate n väärtuste korral on võrratus (5) õige. Teiselt poolt on elektronarvuti abil kontrollitud, et võrratus (5) kehtib iga $n \leq 200\,000$ korral. Seega võib vähima liidetavate arvu $r = g(n)$ seoses (1) leida valemist (6) vähemalt kõikidel nendel n väärtustel, mis ei ületa 200 000

ja ei võrdu 4 ega 5-ga.

Nagu me märkisime, on $g(3) = 9$. Sealjuures ainukesteks arvudeks, mille esitamiseks läheb tarvis 9 kuubi summat, on 23 ja 239. Kõik ülejäänud naturaalarvud on esitatavad mitte rohkem kui 8 kuubi summana. Osutub, et iga n jaoks eksisteerivad suhteliselt väikesed naturaalarvud N, mille esitamiseks kulub maksimaalarv liidetavaid. N suurematel väärtustel asi enamasti paraneb. Seepärast pakub huvi veel vähim liidetavate arv $r = G(n)$ valemis (1) kõikide küllalt suurest arvust N_0 suuremate naturaalarvude N jaoks. Et leidub kuitahes suuri arve, mis ei ole esitatavad vähema kui nelja ruudu summana, siis $G(2) = g(2) = 4$, kuid on teada, et $G(3) \leqslant 7 < g(3)$, $g(4) = 16 < g(4)$, $G(5) \leqslant 23 < g(5)$, $G(6) \leqslant 36 < g(6)$, $G(7) \leqslant 52 < g(7)$, $G(8) \leqslant 73 < g(8)$. Nagu näitab I.M.Vinogradovi poolt saadud hinnang

$$G(n) < (2 + \varepsilon(n))n \ln n \quad (\lim \varepsilon(n) = 0),$$

kasvab funktsioon $G(n)$ märksa aeglasemalt kui funktsioon $g(n)$.

2. Goldbachi-Euleri probleem. Peterburi akadeemik H.Goldbach esitas 1742. a. kirjas L. Eulerile hüpoteesi, et iga täisarvu $N \geqslant 6$ saab esitada kolme algarvu summana:

$$N = p_1 + p_2 + p_3.$$

Euler omalt poolt avaldas vastuseks hüpoteesi, et iga paarisarv, mis ületab arvu 2, on kahe algarvu summa:

$$2N = p_1 + p_2.$$

Euleri probleemi lahendusest järelduks Goldbachi prob-

leemi lahendus, sest $2N + 1 = 3 + 2(N - 1) = 3 + p_1 + p_2$ ja $2N = 2 + 2(N - 1) = 2 + p_1 + p_2$. Vastupidi, kui iga paarisarv alates 6-st on kolme algarvu summa, siis peab üks liidetav olema kindlasti 2 ja alates 4-st on siis kõik paarisarvud ka kahe algarvu summad.

Goldbachi-Euleri probleem on seni lõpuni lahendamata. On tõestatud rida nõrgemaid väiteid, milledest mõned esitame järgnevas teoreemidena (tõestuseta).

Teoreem 9.7 (Šnirelman, 1930). Eksisteerib selline konstant k, et iga naturaalarv $N > 1$ on esitatav mitte rohkem kui k algarvu summana, s.t.

$$N = p_1 + p_2 + \ldots + p_k,$$

kus p_i $(i = 1,2,\ldots,k)$ on algarv või 0.

Kui piirduda arvudega $N \geq N_0$, kus N_0 on küllalt suur, siis Šnirelmani meetod võimaldab võtta $k = 18$.

Teoreem 9.8 (Vinogradov, 1934). Eksisteerib N_0, nii et kõik p a a r i t u d arvud N, mis on suuremad kui N_0, on esitatavad kolme algarvu summana.

Vinogradov tõestas oma teoreemi tema poolt kasutusele võetud lõplike trigonomeetriliste summade meetodil. See on võrdlemisi võimas meetod, mis on leidnud kasutamist ka paljude teiste raskete probleemide lahendamisel. Teoreemis võib võtta $N_0 = e^{e^{16,038}}$.

Teoreem 9.9 (Buhštab, 1964). Iga küllalt suur paarisarv 2N on esitatav kujul

$$2N = p + n,$$

kus p on algarv ja n - naturaalarv, mis sisaldab mitte rohkem kui kolm algarvulist tegurit.

Sageli vaadeldakse naturaalarvu esitamist mõnel teisel kujul. Näiteks on tõestatud järgmine tulemus.

Teoreem 9.10 (Linnik, 1959). Iga küllalt suur naturaalarv N on esitatav kujul $N = p + k^2 + l^2$, kus p on algarv, k ja l - täisarvud.

3. Fermat' probleem. Fermat' probleem seisneb diofantilise võrrandi

$$x^n + y^n = z^n \tag{7}$$

lahenduvuse küsimuses ja on arvuteooria üks tuntumaid ja kõige enam kõmu tekitanud probleeme. Kuigi diofantiliste võrrandite lahenduvuse ja lahendamise küsimused moodustavad arvuteoorias omaette haru, paigutame probleemi tinglikult aditiivse arvuteooria probleemide hulka, sest nagu märkisime käesoleva peatüki alguses, on diofantiliste võrrandite lahenduvuse küsimused tihedalt seotud aditiivse arvuteooria vastavate küsimustega; diofantilistele võrranditele me aga omaette peatükki ei eralda.

Prantsuse juristi ja asjaarmastaja-matemaatiku Pierre Fermat' (1601-1665) väite kohaselt ei ole võrrand (7) n a t u r a a l a r v u d e s lahenduv ühegi täisarvulise astendaja $n > 2$ korral. Nimetatud väide on tuntud Fermat' suure teoreemi nime all.

Kuigi Fermat'lt on säilinud käsikirjaline märge, et tal

õnnestus leida nimetatud teoreemile imetlusväärne tõestus, pole tema tõestust leitud (saadud teaduslikke tulemusi Fermat ei publitseerinud). Ka hilisemad paljude matemaatikute jõupingutused pole andnud probleemile täielikku lahendust.

Märgime, et Fermat' teoreemi tarvitseb tõestada vaid $n = 4$ ja algarvuliste n väärtuste korral, sest kui võrrand (7) pole mingi n korral lahenduv, siis pole ta lahenduv ka astendaja kn korral. See järeldub asjaolust, et võrrandi $x^{kn} + y^{kn} = z^{kn}$ võib esitada kujul $(x^k)^n + (y^k)^n = (z^k)^n$.

Kõige lihtsam on Fermat' teoreemi tõestada $n = 4$ korral (tõestuse toome allpool). Tõestuse $n = 3$ puhul esitas Euler 1774, $n = 5$ puhul - Legendre ja Dirichlet 1823 - 27, $n = 7$ puhul - G.Lamé 1837. Üldisema lähenemise Fermat' probleemile andis saksa matemaatik E.Kummer (1810-1893), kes kasutades algebraliste arvude teooriat tõestas Fermat' väite kõigi algarvuliste astendajate $n < 100$ korral. Tänapäeval on Fermat' teoreem tõestatud juba kõikide algarvuliste astendajate $n < 6000$ korral, millest omakorda järeldub väite õigsus kõigi nende kordarvuliste astendajate korral, mis jaguvad nimetatud algarvudega.

Huvi Fermat' probleemi vastu kasvas eriti käesoleva sajandi alguses, kui Saksamaal asutati suur rahaline preemia, mis tuli välja maksta sellele, kes tõestab Fermat' teoreemi enne aastat 2007. Tohutu vigaste "tõestuste" vool igasuguste elukutsete esindajatelt seadis matemaatika-alaste ajakirjade toimetused ja preemia komitee tõsistesse raskustesse (vt. näit. В. Лицман. Теорема Пифагора, М., 1960, стр.

101-104). Kõik selliste "tõestuste" saatjad kasutasid elementaarmatemaatika vahendeid ja olid arvamusel, et nad on leidnud Fermat' probleemi täieliku lahenduse. Ometi viis tõestuse otsimine juba erijuhtudel matemaatikud mõttele, et Fermat' probleem ei ole lahendatav elementaarmatemaatika vahenditega. Alles pärast seda, kui preemia kaotas I maailmasõja ajal inflatsiooni tõttu oma väärtuse, vähenes Fermat' teoreemi "tõestajate" arv.

Diofantilise võrrandi (7) erijuhuks on võrrand

$$x^2 + y^2 = z^2, \tag{8}$$

millel on olemas positiivsed täisarvulised lahendid (näiteks $x = 3$, $y = 4$, $z = 5$ või $x = 5$, $y = 12$, $z = 13$). Geomeetriliselt võib võrrandi (8) lahendamise nõuet formuleerida kui selliste täisnurksete kolmnurkade leidmist, mille kõikide külgede pikkused on täisarvud. Positiivseid täisarve x, y, z, mis rahuldavad võrrandit (8), nimetatakse Pythagorase arvudeks. Ühistegurita Puthagorase arve nimetatakse põhilisteks, ühisteguriga arve aga tuletatud arvudeks. On ilmne, et igast põhilisest Pythagorase arvude kolmikust võib saada lõpmata palju tuletatud kolmikuid, korrutades põhilise kolmiku kõiki komponente ühe ja sama suvalise naturaalarvuga $k \geqslant 2$. Pythagorase arvude kolmikuid, mis erinevad üksteisest vaid komponentide järjekorra poolest, me ei loe erinevateks.

Järgnevalt leiame kõik põhilised Pythagorase arvud. Peatume võrrandi (8) lahendamisel esiteks sellepärast, et see pakub omaette huvi, ja teiseks sellepärast, et teades

võrrandi (8) lahendeid, saame lahendada Fermat' probleemi $n = 4$ korral.

Tarvitseb vaadelda vaid neid lahendeid, mille komponendid x, y, z on p a a r i k a u p a ühistegurita, sest kui kahel neist oleks ühine tegur, siis peaks ka kolmas komponent jaguma sellega (seose (8) läbijagamisel arvude x, y, z suurima ühisteguriga saame juba seose, kus uued arvud x_1, y_1, z_1 on ühistegurita). On lihtne näha, et kui x, y, z on paarikaupa ühistegurita ja rahuldavad võrrandit (8), siis on arvudest x ja y üks paaris, teine paaritu. Tõepoolest, kui $(x, y) = 1$, siis nad ei saa olla mõlemad paarisarvud; kui nad oleksid aga mõlemad paaritud, s.t. $x = 2k_1 + 1$, $y = 2k_2 + 1$, siis oleks z paarisarv ja saaksime, et $x^2 + y^2 = (2k_1 + 1)^2 + (2k_2 + 1)^2 \equiv 2 \pmod 4$, kuid $z^2 = (2k)^2 \equiv 0 \pmod 4$, mis on võimatu.

Rahuldagu ühistegurita arvud x, y, z võrrandit (8). Üldsust kitsendamata võime eeldada, et x on paarisarv. Siis y ja z on paaritud, nende summa ja vahe aga paarisarvud. Seetõttu on võrdus (8) samaväärne võrdusega

$$\left(\frac{x}{2}\right)^2 = \frac{z + y}{2} \cdot \frac{z - y}{2}, \tag{9}$$

kus nii vasak pool kui ka mõlemad tegurid paremal on täisarvud. Olgu $\left(\frac{z + y}{2}, \frac{z - y}{2}\right) = d$, siis $d \mid z$ ja $d \mid y$ (näidata!), mistõttu $d = 1$. Kuna seose (9) kohaselt on ühistegurita arvude $\frac{z + y}{2}$ ja $\frac{z - y}{2}$ korrutis täisarvu ruut, siis peavad need arvud ka ise olema täisruudud (tõestada!), s.t. leiduvad positiivsed täisarvud a ja b, nii et

$$\frac{z+y}{2} = a^2, \quad \frac{z-y}{2} = b^2 \quad \text{ja} \quad \left(\frac{x}{2}\right)^2 = a^2b^2.$$

Siit saame

(10) $$x = 2ab, \quad y = a^2 - b^2, \quad z = a^2 + b^2.$$

Otsene kontroll näitab, et valemitega (10) defineeritud x, y, z rahuldavad võrrandit (8) i g a a ja b korral. On muidugi selge, et kui x ja y osad vahetada, siis saame jälle lahendi.

Selleks et y ja z oleksid positiivsed paaritud täisarvud ja et oleks (x, y, z) = 1, on tarvilik ja piisav, et positiivsed täisarvulised parameetrid a, b valemites (10) rahuldaksid järgmisi tingimusi:

1) üks arvudest a, b on paarisarv, teine paaritu;

2) $a > b \geqslant 1$;

3) (a, b) = 1.

Seega oleme saanud tulemuse, mille võime sõnastada järgmise teoreemina.

Teoreem 9.11. 1) Kui x, y, z on paarikaupa ühistegurita arvud, mis rahuldavad võrrandit (8), siis arvudest x, y on üks paaris, teine paaritu.

2) Ühistegurita arvud x, y, z ($x > 0$, $y > 0$, $z > 0$), millest x on paarisarv, rahuldavad võrrandit (8) parajasti siis, kui nad on defineeritud valemitega (10):

$$x = 2ab, \quad y = a^2 - b^2, \quad z = a^2 + b^2,$$

kus $a > b \geqslant 1$, (a, b) = 1 ja arvudest a, b on üks paaris, teine paaritu.

Võrrandi (8) üksikud lahendid olid teada juba palju sajandeid enne meie ajaarvamist vanaaja matemaatikutele Egiptuses, Indias jm., üldlahend (10) on aga antud Eukleidese (umbes 300 a. e. m. a.) ja Diophantose (III saj. m. a. j.) töödes.

Edasi tõestame järgmise teoreemi.

Teoreem 9.12. Võrrand

$$x^4 + y^4 = z^2 \tag{11}$$

ei ole positiivsetes täisarvudes lahenduv.

Tõestus ([1], lk. 309-310). Kasutame täielikku induktsiooni meetodit, andes z-le kõikvõimalikud naturaalarvulised väärtused. Kõik tõestuses esinevad sümbolid tähistavad p o s i t i i v s e i d täisarve.

Kui $z = 1$, siis on vahetult näha, et diofantilisel võrrandil $x^4 + y^4 = 1$ pole positiivseid lahendeid.

Oletame, et $z < n$ puhul pole võrrandil (11) (x ja y suhtes) positiivseid lahendeid, kuid $z = n$ korral on selliseks lahendiks $x = x_0$, $y = y_0$, s.t.

$$\left(x_0^2\right)^2 + \left(y_0^2\right)^2 = n^2. \tag{12}$$

Vaatleme kahte juhtu.

1) Olgu $(x_0, y_0, n) = d > 1$. Siis võrduse (12) vasak ja järelikult ka parem pool jagub d^4-ga, mistõttu $d^2 \mid n$. Siis aga

$$\left(\frac{x_0}{d}\right)^4 + \left(\frac{y_0}{d}\right)^4 = \left(\frac{n}{d^2}\right)^2 ,$$

mis on vastuolus eeldusega, sest täisarv $\frac{n}{d^2} < n$.

2) Olgu $(x_0, y_0, n) = 1$. Siis teoreemist 9.11 järeldub, et kas $2|x_0$ või $2|y_0$. Kui $2|x_0$, siis valemite (10) kohaselt

(13) $x_0^2 = 2ab$, $y_0^2 = a^2 - b^2$, $(a, b) = 1$, y_0 - paaritu.

Paaritute arvude ruudud on kujuga $4k + 1$, millest järeldub, et kahe ühistegurita arvu a ja b ruutude vahe saab võrduda paaritu arvu y_0 ruuduga vaid siis, kui a on paaritu ja b paarisarv (veenduda!).

Seosest $a^2 = y_0^2 + b^2$, mis järeldub (13)-st, saame teoreemi 9.11 tõttu, et

$$a = u^2 + v^2, \quad b = 2uv, \quad (u, v) = 1.$$

Kuna $x_0^2 = a(2b)$ ja $(a, 2b) = 1$, siis tegurid a ja 2b peavad olema täisruudud: $a = s^2$ ja $2b = t^2$. Kuna aga $b = 2uv$, siis $t^2 = 4uv$. Et $(u, v) = 1$, siis võrdus $\left(\frac{t}{2}\right)^2 = uv$ saab kehtida vaid juhul, kui u ja v on täisruudud, s.t. $u = x_1^2$, $v = y_1^2$. Asendades saadud väärtused võrduses $a = u^2 + v^2$, saame

(14) $$x_1^4 + y_1^4 = s^2.$$

Samasusest (12) on näha, et $x_0^2 < n$; peale selle saime, et $s^2 = a$ ja $2a|x_0^2$. Siis aga $s \leqslant a < x_0^2 < n$, mistõttu võrdus (14) on vastuolus eeldusega, et võrrandil (11) ei ole positiivseid täisarvulisi lahendeid (x ja y suhtes), kui $z < n$.

Kui $2|y_0$, siis analoogilise arutlusega jõuame samale vastuolule.

Järeldus. Võrrand

$$x^4 + y^4 = z^4$$

ei ole positiivsetes täisarvudes lahenduv.

Tõepoolest, kui tal oleks lahend x_0, y_0, z_0 ($x_0 > 0$, $y_0 > 0$, $z_0 > 0$), siis oleks võrrandil (11) lahend x_0, y_0, z_0^2.

X. ALGARVUDE JAOTUMINE

Käesolevas peatükis käsitleme algarvude jaotumist naturaalarvude jadas ja teistes aritmeetilistes progressioonides ning uurime vastavate jaotusfunktsioonide mõningaid omadusi. Märgime, et küsimus algarvude jaotumisest on arvuteooria üks raskemaid ja osalt veel lahendamata probleeme.

Kogu käesoleva peatüki ulatuses tähistagu p_n järjekorras n-ndat algarvu, p aga mistahes algarvu.

§ 1. ALGARVUDE JAOTUSFUNKTSIOON

1. Jaotusfunktsiooni $\pi(x)$ definitsioon. Tähistame sümboliga $\pi(x)$ reaalarvu x mitteületavate algarvude arvu, s.t.

$$\pi(x) = \sum_{p \le x} 1 = |\{p \mid p \le x\}|.$$

Seega on $\pi(x)$ arvuteoreetiline funktsioon, mis on defineeritud kõigi reaalarvude hulgal ja omandab vaid täisarvulisi väärtusi. Nimetame teda algarvude jaotusfunktsiooniks.

Funktsiooni $\pi(x)$ definitsioonist järeldub, et

$$\pi(x) = n, \quad \text{kui} \quad p_n \le x < p_{n+1};$$

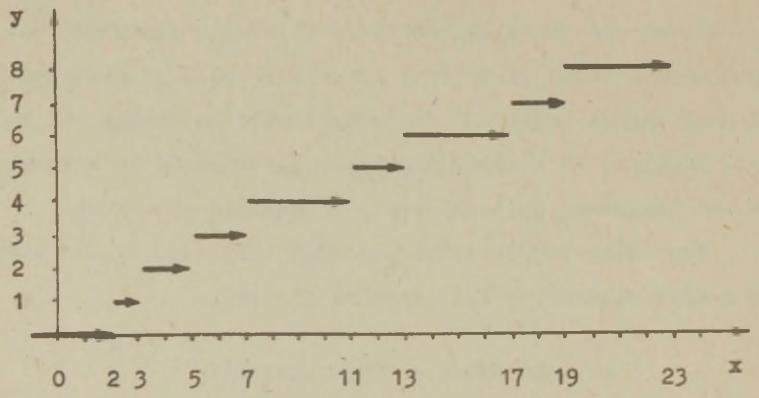
eriti on

$$\pi(p_n) = n.$$

Funktsioon $\pi(x)$ on mittekahanev katkev funktsioon, kusjuures algarvude hulga lõpmatuse tõttu

$$\lim_{x \to \infty} \pi(x) = +\infty.$$

Juuresoleval joonisel on esitatud funktsiooni $y = \pi(x)$ graafik x väikestel positiivsetel väärtustel. Funktsiooni katkevuspunktide ja kõigi algarvude hulk on üksüheses vastavuses.



Kuigi $\pi(x)$ kasvab koos argumendiga piiramatult, leidub arvtelje positiivses osas kuitahes pikki lõike, kus $\pi(x)$ on konstantne. See nähtub järgnevast teoreemist.

Teoreem 10.1. Iga täisarvu $n \geq 1$ korral leidub naturaalarvude jadas vahemik, milles n järjestikust naturaalarvu on kordarvud.

Tõestus. Kirjutame välja n järjestikust naturaalarvu

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

Kõik need arvud on kordarvud, sest esimene jagub vähemalt arvuga 2, teine arvuga 3, ..., viimane arvuga n+1.

Algarvude tabeli vahetu vaatlus näitab, et olemasolevate tabelite piirides leidub isegi väga suurte algarvude paare, kus algarvud erinevad teineteisest vaid 2 võrra. Tabeli

alguses on sellisteks arvudeks 3, 5; 5, 7; 11, 13; 17, 19; 29, 31. Niisuguseid algarvude paare nimetatakse kaksikuteks. Esimese 30 miljoni naturaalarvu seas leidub 152 892 paari kaksikuid. On püstitatud hüpoteese, et kaksikuid on lõpmata palju, kuid senini pole õnnestunud seda tõestada. Leidub ka neljast järjestikusest algarvust koosnevaid komplekse, mis sisaldavad kaks paari kaksikuid. Kui selline kompleks koosneb algarvudest

$$p,\ p+2,\ p+6 \quad \text{ja} \quad p+8,$$

siis öeldakse, et on tegemist nelikuga; näiteks 5, 7, 11, 13; 11, 13, 17, 19; 101, 103, 107, 109; 191, 193, 197, 199. Esimese 10 miljoni naturaalarvu seas leidub 899 nelikut, esimese 15 miljoni seas 1209. Kõige kaugem teadaolev nelik saadakse, kui $p = 2\,863\,308\,731$. Arvatakse, et ka nelikuid on lõpmata palju.

Kaksikute olemasolu suurte algarvude korral ja tõestatud teoreem näitavad, et algarvud paiknevad naturaalarvude jadas väga ebaühtlaselt.

2.* <u>Funktsiooni $\pi(x)$ arvutusvalemid</u>. Funktsiooni $\pi(x)$ jaoks on teada mitmeid valemeid.

Päris lihtne on näiteks kontrollida, et

$$\pi(x) = 1 + \sum_{n=3}^{[x]} \left(1 - \left[1 - \prod_{k=2}^{n-1} \sin^2 \frac{n\pi}{k} \right] \right),$$

kus nurksulud märgivad täisosa võtmist. Siin

$$\left[1 - \prod_{k=2}^{n-1} \sin^2 \frac{n\pi}{k} \right] = \begin{cases} 0, & \text{kui } n \text{ on algarv,} \\ 1, & \text{kui } n \text{ on kordarv.} \end{cases}$$

Esitatud valemist pole $\pi(x)$ väärtuste praktiliseks leidmiseks siiski suuremat kasu. Teatud määral praktilise valemi annab Eratosthenese meetod (vt. I pt., §4). Nimelt kui reaalarvu x mitte ületavate naturaalarvude jadas maha kriipsutada kõik algarvud $p_i \leq \sqrt{x}$ koos nende kordsetega, siis jääb jadas esinenud naturaalarvudest järele vaid $\pi(x) - \pi(\sqrt{x})$ algarvu (need, mis on suuremad kui $\sqrt{x}$) ja arv 1. See protsess viib valemini

$$(1)\quad \pi(x) - \pi(\sqrt{x}) + 1 = [x] - \sum_{i=1}^{r} \left[\frac{x}{p_i}\right] + \sum_{1 \leq i < j \leq r} \left[\frac{x}{p_i p_j}\right] - \sum_{1 \leq i < j < k \leq r} \left[\frac{x}{p_i p_j p_k}\right] + \ldots,$$

kus r on suurim järjekorranumber, mille korral $p_r \leq \sqrt{x}$ (teisiti öeldes $r = \pi(\sqrt{x})$).

Tõepoolest, naturaalarve on jadas kokku $[x]$. Algarvu p_i kordsete mahakriipsutamise tõttu tuleb sellest jadast ära jätta iga i korral $\left[\frac{x}{p_i}\right]$ arvu (vaatluse all olevas jadas on p_i kordseteks p_i, $2p_i$, $3p_i$, ..., $\left[\frac{x}{p_i}\right] p_i$, mida on arvult $\left[\frac{x}{p_i}\right]$). Seejuures p_i ja p_j ühiskordsed, mida on arvult $\left[\frac{x}{p_i p_j}\right]$, arvatakse maha kahekordselt. Seepärast tuleb lisada $\left[\frac{x}{p_i p_j}\right]$ arvu iga i ja j kombinatsiooni korral. Sealjuures $\left[\frac{x}{p_i p_j p_k}\right]$ arvu, mis on arvu $p_i p_j p_k$ kordsed, lisatakse juurde kahekordselt ja seepärast tuleb nad uuesti ära jätta jne.

Selleks, et arvutada valemi (1) järgi $\pi(x)$ väärtust, on tarvis teada kõiki algarve, mis ei ületa $\sqrt{x}$.

Näide 1. Leiame $\pi(150)$.

Et $12 < \sqrt{150} < 13$, siis tuleb kasutada algarve $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$ ja $p_5 = 11$. Seega $r = 5$, $\pi(\sqrt{150}) = 5$ ja valem (1) annab

$$\begin{aligned}\pi(150) - 5 + 1 &= 150 - (75 + 50 + 30 + 21 + 13) + \\ &+ (25 + 15 + 10 + 6 + 10 + 7 + 4 + 4 + 2 + 1) - \\ &- (5 + 3 + 2 + 2 + 1 + 0 + 1 + 0 + 0 + 0) + \\ &+ (0 + 0 + 0 + 0 + 0) - 0 = 150 - 189 + 84 - 14 = \\ &= 31,\end{aligned}$$

millest $\pi(150) = 35$. Saime, et 150-st väiksemaid algarve on 35.

$\pi(x)$ väärtuse arvutamine valemist (1) nõuab rohkesti arvutusi, sest valemi parem pool sisaldab palju liidetavaid Allpool tuletame valemi, mis võimaldab $\pi(x)$ väärtuste arvutamist tunduvalt lihtsustada.

Tähistame sümboliga $\varphi(x, r)$ reaalarvu x mitte ületavate ja algarvudega $p_1, \ldots, p_r$ mitte jaguvate naturaalarvude arvu. Nõuet, et naturaalarv n ei jagu algarvudega p_i $(i = 1,2, \ldots, r)$ võib väljendada nii: $(n, p_1 \ldots p_r) = 1$. Seetõttu võib $\varphi(x, r)$ defineerida järgmiste valemitega:

$$\varphi(x, r) = \sum_{\substack{n \le x \\ (n, p_1 \ldots p_r) = 1}} 1 = \left|\{n \mid n \le x, \ (n, p_1 \ldots p_r) = 1\}\right|.$$

Teoreem 10.2. Kehtib valem

$$\varphi(x, r) = \sum_{d \mid p_1 \ldots p_r} \left[\frac{x}{d}\right] \mu(d). \tag{2}$$

Tõestus. Teoreemi 4.12 kohaselt

$$\sum_{d|(n,p_1\dots p_r)} \mu(d) = \begin{cases} 1, \text{ kui } (n, p_1\dots p_r) = 1, \\ 0, \text{ kui } (n, p_1\dots p_r) \neq 1. \end{cases}$$

Arvestades veel, et

$$\left[\frac{x}{d}\right] = \sum_{\substack{n \leq x \\ n \,:\, d}} 1 ,$$

saame

$$\sum_{d|p_1\dots p_r} \left[\frac{x}{d}\right]\mu(d) = \sum_{d|p_1\dots p_r} \mu(d) \sum_{\substack{n \leq x \\ n:d}} 1 =$$

$$= \sum_{n \leq x} \sum_{d|(n,p_1\dots p_r)} \mu(d) = \sum_{\substack{n \leq x \\ (n,p_1\dots p_r)=1}} 1 = \varphi(x, r).$$

Kui võtta $p_r \leq \sqrt{x} < p_{r+1}$, siis valem (2) annab valemi (1). Tõepoolest, $\varphi(x, r)$ on algarvudega $p_i \leq \sqrt{x}$ $(i = 1,2,\dots,r)$ mittejaguvate naturaalarvude $n \leq x$ arv. Naturaalarvudeks $n \leq x$, mis ei jagu algarvudega $p \leq \sqrt{x}$, on aga algarvud poollõigust $(\sqrt{x}, x]$ ja arv 1 (I pt., §4, punkt 2). Seega vaadeldaval juhul

$$\varphi(x, r) = \pi(x) - \pi(\sqrt{x}) + 1.$$

Selleks et veenduda valemite (1) ja (2) paremate poolte ühtimises, tuleb arvestada jagajate d kuju ja Möbiuse μ-funktsiooni definitsiooni (vt. IV pt., §4).

1870. a. tõestas saksa matemaatik D.Meissel teoreemi, mis lubab arvutada $\pi(x)$ väärtusi märksa väiksema vaevaga kui seda võimaldab valem (1).

Teoreem 10.3 (Meissel). Olgu tähistatud $\pi(\sqrt[3]{x}) = r$ ja $\pi(\sqrt{x}) = s$. Siis

(3) $$\pi(x) = \varphi(x, r) + \frac{1}{2}(s - r + 1)(s + r - 2) - \sum_{i=r+1}^{s} \pi\left(\frac{x}{p_i}\right).$$

Tõestus. Kasutatud tähistuste tõttu on

(4) $$p_r \leq \sqrt[3]{x} < p_{r+1} < p_{r+2} < \ldots < p_s \leq \sqrt{x} < p_{s+1}.$$

Olgu M hulk, mille elementideks on naturaalarvud $n \leq x$, mis ei jagu algarvudega $p \leq \sqrt[3]{x}$. Siis hulka M kuuluvad: 1) arv 1; 2) kõik algarvud poollõigust $(\sqrt[3]{x}, x]$; viimaste arv on $\pi(x) - \pi(\sqrt[3]{x}) = \pi(x) - r$; 3) teatud kordarvud, mille vähimaks algarvuliseks teguriks on algarvud hulgast (vt. teor. 1.20)

(5) $$p_{r+1}, p_{r+2}, \ldots, p_s.$$

Määrame hulka M kuuluvate kordarvude arvu. Kuna $p_{r+1}^3 > x$, siis (4) tõttu sisaldavad hulka M kuuluvad kordarvud paarajasti kaht algarvulist tegurit, s.t. nimetatud kordarvudel on kuju $p_i p_j$, kusjuures vähim neist, olgu see p_j, kuulub kindlasti hulka (5). Sealjuures

(6) $$p_i p_j \leq x.$$

Tarvitseb leida kõigi selliste korrutiste arv. Võrratuse (6) tõttu on

(7) $$p_i \leq p_j \leq \frac{x}{p_i}.$$

Iga p_i korral, kus $r < i \leq s$, on tingimust (7) rahuldavate algarvude p_j arv võrdne

$$\pi\left(\frac{x}{p_i}\right) - \pi(p_i) + 1 = \pi\left(\frac{x}{p_i}\right) - i + 1$$

ja seega korrutiste $p_i p_j$ ehk kordarvude arv hulgas M võrdub

$$\sum_{i=r+1}^{s}\left(\pi\left(\frac{x}{p_i}\right) - i + 1\right) = \sum_{i=r+1}^{s}\pi\left(\frac{x}{p_i}\right) - \frac{(s-r)(r+s-1)}{2}.$$

Seega saame kôigi hulka M kuuluvate naturaalarvude arvu $\varphi(x, r)$ jaoks valemi

$$\varphi(x, r) = 1 + \pi(x) - r + \sum_{i=r+1}^{s}\pi\left(\frac{x}{p_i}\right) - \frac{(s-r)(r+s-1)}{2} =$$

$$= \pi(x) + \sum_{i=r+1}^{s}\pi\left(\frac{x}{p_i}\right) - \frac{1}{2}(s-r+1)(s+r-2).$$

Siit saamegi seose (3).

Märgime, et viimast summat valemis (3) vôib esitada ka kujul

$$\sum_{\sqrt[3]{x} < p \le \sqrt{x}}\pi\left(\frac{x}{p}\right).$$

Näide 2. Kasutades Meisseli teoreemi, leiame 1200 mitte ületavate algarvude arvu.

Antud juhul $x = 1200$. Arvude $\sqrt[3]{1200} = 10{,}6\ldots$ ja $\sqrt{1200} = 34{,}6\ldots$ vahele kuuluvateks algarvudeks on 11, 13, 17, 19, 23, 29 ja 31; $r = \pi(\sqrt[3]{1200}) = 4$, $s = \pi(\sqrt{1200}) = 11$; $\frac{1}{2}(s - r + 1)(s + r - 2) = \frac{1}{2}\cdot 8 \cdot 13 = 52$. Arvutame viimase summa valemis (3):

$$\sum_{i=r+1}^{s}\pi\left(\frac{x}{p_i}\right) = \sum_{\sqrt[3]{x} < p \le \sqrt{x}}\pi\left(\frac{x}{p}\right) = \pi\left(\frac{1200}{11}\right) + \pi\left(\frac{1200}{13}\right) +$$

$$+ \pi\left(\frac{1200}{17}\right) + \pi\left(\frac{1200}{19}\right) + \pi\left(\frac{1200}{23}\right) + \pi\left(\frac{1200}{29}\right) +$$

$$+ \pi\left(\frac{1200}{31}\right) = 29 + 24 + 19 + 18 + 15 + 13 + 12 =$$

$$= 130.$$

Suuruse $\varphi(x, r) = \varphi(1200, 4)$ arvutamiseks kasutame valemit (2):

$$\varphi(1200, 4) = \sum_{d \mid 2\cdot3\cdot5\cdot7} \left[\frac{1200}{d}\right] \mu(d) = \left[\frac{1200}{1}\right] -$$

$$- \left[\frac{1200}{2}\right] - \left[\frac{1200}{3}\right] - \left[\frac{1200}{5}\right] - \left[\frac{1200}{7}\right] + \left[\frac{1200}{2\cdot3}\right] +$$

$$+ \left[\frac{1200}{2\cdot5}\right] + \left[\frac{1200}{2\cdot7}\right] + \left[\frac{1200}{3\cdot5}\right] + \left[\frac{1200}{3\cdot7}\right] + \left[\frac{1200}{5\cdot7}\right] -$$

$$- \left[\frac{1200}{2\cdot3\cdot5}\right] - \left[\frac{1200}{2\cdot3\cdot7}\right] - \left[\frac{1200}{2\cdot5\cdot7}\right] - \left[\frac{1200}{3\cdot5\cdot7}\right] + \left[\frac{1200}{2\cdot3\cdot5\cdot7}\right] =$$

$$= 1200 - 600 - 400 - 240 - 171 + 200 + 120 +$$

$$+ 85 + 80 + 57 + 34 - 40 - 28 - 17 - 11 + 5 =$$

$$= 1781 - 1507 = 274.$$

Seega $\pi(1200) = 274 + 52 - 130 = 196$, s.t. lõigus $[1, 1200]$ leidub 196 algarvu.

Valemi (3) kasutamisel on kõige enam vaevanõudvaks tööks $\varphi(x, m)$ arvutamine (valemis (2) on liidetavate arv 2^r). Selleks et suuruse $\varphi(x, m)$ arvutamist lihtsustada, võib kasutada järgnevas tõestatavaid rekurrentseid seoseid.

Teoreem 10.4. Kui lugeda $\varphi(x, 0) = [x]$, siis iga $r = 1,2,\ldots$ korral

$$\varphi(x, r) = \varphi(x, r - 1) - \varphi\left(\frac{x}{p_r}, r - 1\right). \tag{8}$$

Kui $[x] = tp_1p_2\ldots p_r + s$, kus t ja s on mittenegatiivsed täisarvud, siis

$$\varphi(x, r) = t\varphi(p_1p_2\ldots p_r) + \varphi(s, r) \tag{9}$$

ja valemis esinev Euleri φ-funktsioon

$$\varphi(p_1p_2\cdots p_r) = (p_1 - 1)(p_2 - 1)\cdots(p_r - 1).$$

Tõestus ([9], lk. 61-63). Eksisteerib $\varphi(x, r - 1)$ naturaalarvu $n \leq x$, mis on ühistegurita algarvudega $p_1, p_2, \ldots, p_{r-1}$. Neist naturaalarvudest täpselt $\varphi\left(\frac{x}{p_r}, r - 1\right)$ jagub algarvuga p_r, sest nimetatud $\varphi(x, r - 1)$ naturaalarvu hulka on arvatud p_r kordsed hp_r $\left(1 \leq h \leq \frac{x}{p_r}\right)$, mille korral $(h, p_1p_2\cdots p_{r-1}) = 1$. Seega kehtib valem (8).

Valemi (9) tõestamiseks arvestame, et arvude

(10) $\qquad 1, 2, \ldots, p_1p_2\cdots p_r, \ldots, tp_1p_2\cdots p_r$

hulgas on täpselt $t\varphi(p_1p_2\cdots p_r)$ arvu, mis on ühistegurita korrutisega $p_1p_2\cdots p_r$, sest iga täielik jääkide süsteem mod $p_1p_2\cdots p_r$ sisaldab $\varphi(p_1p_2\cdots p_r)$ sellist arvu (arvud (10) võib jaotada t täielikuks jääkide süsteemiks). Selleks et arv

(11) $\qquad tp_1p_2\cdots p_r + u \quad (u = 1,2,\ldots,s)$

oleks ühistegurita korrutisega $p_1\cdots p_r$ on tarvilik ja piisav, et see omadus oleks arvul u. Ühistegurita arve (11) on seega $\varphi(s, r)$. Saamegi valemi (9).

Näide 3. Kasutades rekurrentseid valemeid (8) ja (9), leiame näites 2 kasutatud suuruse $\varphi(1200, 4)$:

$$\varphi(1200, 4) = 5\varphi(2\cdot3\cdot5\cdot7) + \varphi(150, 4) = 240 + \varphi(150, 4),$$
$$\varphi(150, 4) = \varphi(150, 3) - \varphi(21, 3) =$$
$$= 5\varphi(30) - \varphi(21, 3) = 40 - \varphi(21, 3),$$

$\varphi(21, 3) = \varphi(21, 2) - \varphi(4, 2) =$

$= 3\varphi(2\cdot3) + \varphi(3, 2) - \varphi(4, 2) = 6;$

$\varphi(1200, 4) = 240 + 40 - 6 = 274.$

Märgime lõpuks, et peale Meisseli valemi (3) on teada valemeid $\pi(x)$ arvutamiseks, kus $\pi(x)$ avaldub suhteliselt väikeste $\pi(y)$ väärtuste ja $\varphi(x, r)$ kaudu, $r = \pi(\sqrt[n]{x})$ ja $n > 3$. Sellised valemid nõuavad väiksema hulga algarvude ja $\pi(y)$ väärtuste teadmist, kuid on märksa keerukamad kui valem (3).

Valemi (3) abil on leitud $\pi(10^9) = 50\ 847\ 478$.

Harjutusülesandeid.

10.1. Arvutada Meisseli teoreemi abil arvust 2000 väiksemate algarvude arv. Valemis esinev suurus $\varphi(x, r)$ leida rekurrentsete seoste (8) ja (9) abil. Tulemust kontrollida algarvude tabeli järgi.

10.2. Kui palju liikmeid tuleks leida

a) $\pi(2000)$ arvutamisel valemist (1);

b) $\varphi(2000, \pi(\sqrt[3]{2000}))$ arvutamisel valemist (2)?

10.3. Arvutada $\pi(3000)$.

§2. JAOTUSFUNKTSIOONI HINNANGUD JA ASÜMPTOOTILISED VALEMID

Arvutamine eelmises paragrahvis toodud valemite järgi muutub seda tülikamaks, mida suurem on x. Pealegi ei võimalda nimetatud valemid uurida täpsemalt funktsiooni $\pi(x)$ kasvamise iseloomu, näiteks kasvamise keskmist kiirust. Selles suhtes on mugavamad asümptootilised valemid, millest tuleb juttu käesolevas paragrahvis. Tõestame eelnevalt järgmise teoreemi.

Teoreem 10.5 (Tšebõšov). Eksisteerivad konstandid a ja b, kusjuures $0 < a < 1$ ja $b > 1$, nii et iga $x \geqslant 2$ korral kehtivad võrratused

$$(1) \qquad a\,\frac{x}{\ln x} < \pi(x) < b\,\frac{x}{\ln x}\,.$$

Tõestus ([1], lk. 334-337). 1) Hindame kõigepealt avaldist $T(x) - 2T(\frac{x}{2})$, kus funktsioon $T(x)$ on defineeritud IV peatüki 2. paragrahvis, s.t.

$$(2) \qquad T(x) = \sum_{n\leqslant x} \ln n = \ln[x]! = \sum_{p} (\ln p)\left(\left[\frac{x}{p}\right] + \left[\frac{x}{p^2}\right] + \ldots\right).$$

Eeldame, et $n \geqslant 3$. Siis

$$(3) \qquad \begin{aligned} T(2n) - 2T(n) &= \sum_{k=n+1}^{2n} \ln k - \sum_{k=1}^{n} \ln k = \\ &= \ln\frac{n+1}{1} + \ln\frac{n+2}{2} + \ldots + \ln\frac{n+n}{n} \geqslant (n+1)\ln 2, \end{aligned}$$

sest $\ln\frac{n+1}{1} \geqslant \ln 4 = 2\ln 2$ ja ülejäänud liidetavad $\ln\frac{n+s}{s} = \ln(1+\frac{n}{s}) \geqslant \ln 2$. Teisest küljest

$\frac{(2n)!}{n!n!} = C_{2n}^{n} < 1 + C_{2n}^{1} + \ldots + C_{2n}^{n} + \ldots + C_{2n}^{2n} = (1+1)^{2n} = 2^{2n}$

ja seega

$$(4) \qquad T(2n) - 2T(n) = \ln \frac{(2n)!}{n!n!} < 2n \ln 2.$$

Võtame suvalise $x \geqslant 6$ ja valime n nii, et $2n \leqslant x < 2(n+1)$. Kuna T(x) on mittekahanev tükati konstantne funktsioon, siis T(x) on võrdne kas arvuga T(2n) või on sellest $\ln(2n+1)$ võrra suurem ja $T(\frac{x}{2}) = T(n)$. Seetõttu

$$T(2n) - 2T(n) \leqslant T(x) - 2T(\tfrac{x}{2}) \leqslant T(2n) - 2T(n) + \ln(2n+1).$$

Arvestades hinnanguid (3), (4) ja võrratust $n+1 > \frac{x}{2}$, saame

$$(5) \qquad T(x) - 2T(\tfrac{x}{2}) \geqslant (n+1) \ln 2 > \frac{\ln 2}{2} x,$$

$$(6) \quad T(x) - 2T(\tfrac{x}{2}) \leqslant 2n \ln 2 + \ln(2n+1) \leqslant x \ln 2 + \ln(x+1) < x(\ln 2 + 1).$$

2) Hindame $\pi(x)$ alt. Valemist (2) saame

$$(7) \quad T(x) - 2T(\tfrac{x}{2}) = \sum_{p \leqslant x} (\ln p)\left(\left(\left[\frac{x}{p}\right] - 2\left[\frac{x}{2p}\right]\right) + \left(\left[\frac{x}{p^2}\right] - 2\left[\frac{x}{2p^2}\right]\right) + \ldots\right).$$

Kui $p^k > x$, siis liidetavad $\left[\frac{x}{p^k}\right] - 2\left[\frac{x}{2p^k}\right]$ võrduvad nulliga. Need liidetavad aga, kus $p^k \leqslant x$, ei ületa 1. Tõepoolest, iga reaalarvu α korral $\alpha - 1 < [\alpha] \leqslant \alpha$ ja seega $[\alpha] - 2\left[\frac{\alpha}{2}\right] < \alpha - 2(\frac{\alpha}{2} - 1) = 2$. Seega avaldises (7) on ln p kordajaks

$$\alpha_p = \sum_{k=1}^{s} \left(\left[\frac{x}{p^k}\right] - 2\left[\frac{x}{2p^k}\right]\right) \leqslant s,$$

kus liidetavate arv s on määratud tingimusega $p^s \leqslant x$. Viimase võrratuse logaritmimisel saame, et $s \ln p \leqslant \ln x$, millest

$$s \leqslant \frac{\ln x}{\ln p}.$$

Seega $\alpha_p \leqslant \frac{\ln x}{\ln p}$ ja

$$T(x) - 2T(\tfrac{x}{2}) \leqslant \sum_{p \leqslant x} \ln p \, \frac{\ln x}{\ln p} = \ln x \sum_{p \leqslant x} 1 = \pi(x) \ln x.$$

Arvestades hinnangut (5) saame siit

$$\pi(x) \ln x \geqslant \frac{\ln 2}{2} x,$$

s.t.

$$\pi(x) > a \frac{x}{\ln x}, \quad \text{kus} \quad a = \frac{\ln 2}{2} < 1.$$

Võrratus on tõestatud $x \geqslant 6$ korral. On selge, et konstandi a vähendamisega saab võrratuse muuta kehtivaks kõikide $x \geqslant 2$ korral.

3) Hindame $\pi(x)$ ülalt. Kuna võrduse (7) paremal poolel on kõik liidetavad mittenegatiivsed, siis jättes neist ära need, kus $p \leqslant \frac{x}{2}$, me ei suurenda summat. Sealjuures ülejäänud liidetavates on ln p kordajaks

$$\left(\left[\frac{x}{p}\right] - 2\left[\frac{x}{2p}\right]\right) + \left(\left[\frac{x}{p^2}\right] - 2\left[\frac{x}{2p^2}\right]\right) + \ldots = 1,$$

sest $\frac{x}{2} < p \leqslant x$, $x \geqslant 6$ ja seega $2p > x$, $p^2 > \frac{x^2}{4} > x$, $2p^2 > x$, $p^3 > x$, ... Seosest (7) saame

$$T(x) - 2T(\tfrac{x}{2}) \geqslant \sum_{\frac{x}{2} < p \leqslant x} \ln p > \ln \tfrac{x}{2} \sum_{\frac{x}{2} < p \leqslant x} 1 =$$

$$= (\pi(x) - \pi(\tfrac{x}{2})) \ln \tfrac{x}{2}.$$

Liites viimase võrratuse mõlemale poolele $\pi(x)\ln 2$, mis on väiksem kui $x \ln 2$, ja kasutades hinnangut (6), saame

$$\pi(x)\ln x - \pi(\tfrac{x}{2})\ln\tfrac{x}{2} < T(x) - 2T(\tfrac{x}{2}) + x\ln 2 <$$

$$< x(2\ln 2 + 1) = cx,$$

kus $c = 2\ln 2 + 1$. Arvestades, et küllalt suure s korral $\pi\left(\frac{x}{2^s}\right) = 0$, saame viimast võrratust korduvalt rakendades

$$\pi(x)\ln x \leqslant cx + \pi(\tfrac{x}{2})\ln\tfrac{x}{2} \leqslant cx + c\tfrac{x}{2} + \pi\left(\tfrac{x}{2^2}\right)\ln\tfrac{x}{2^2} \leqslant \dots$$

$$\dots \leqslant cx + c\tfrac{x}{2} + \dots + c\tfrac{x}{2^{s-1}} + \pi\left(\tfrac{x}{2^s}\right)\ln\tfrac{x}{2^s} <$$

$$< cx(1 + \tfrac{1}{2} + \tfrac{1}{2^2} + \dots) = 2cx.$$

Tähistades $b = 2c = 2(2\ln 2 + 1)$, saame $x \geqslant 6$ korral

$$\pi(x) < b\,\frac{x}{\ln x}\,.$$

Kui konstanti b suurendada, hakkab võrratus kehtima juba alates väärtusest $x = 2$. Teoreem on tõestatud.

Võtnud $T(x) - 2T(\frac{x}{2})$ asemel avaldise

$$T(x) - T(\tfrac{x}{2}) - T(\tfrac{x}{3}) - T(\tfrac{x}{5}) + T(\tfrac{x}{30}),$$

tõestas P.L.Tšebõšov 1850.a., et teatud (küllalt suurest) x väärtusest alates kehtivad võrratused (1), kus $a = 0{,}921$, $b = 1{,}106$. Peale selle tõestas Tšebõšov, et kui eksisteerib piirväärtus

$$\lim_{x\to\infty}\left(\pi(x) : \frac{x}{\ln x}\right),$$

siis see võrdub ühega. Piirväärtuse olemasolu ei õnnestunud tal aga näidata. Alles 1896.a. tõestasid J.Hadamard ja de la Vallée Poussin teineteisest sõltumatult, et nimetatud piirväärtus eksisteerib. Tõestus nõuab kompleksmuutuja funktsiooniteooria kasutamist. 1949.a. andsid taani matemaatik

A. Selberg ja ungari matemaatik P.Erdös "elementaarse" tõestuse, mis ei kasuta kompleksmuutuja funktsiooniteooriat. Seega kehtib asümptootiline valem*

(8) $$\pi(x) \sim \frac{x}{\ln x} .$$

Teisiti võib tulemust tõlgendada nii: küllalt suures lõigus $[1,x]$ on algarve ligikaudu $\frac{1}{\ln x}$ osa kõikidest naturaalarvudest.

Suhet $\frac{\pi(x)}{x}$, kus x on naturaalarv, võib nimetada algarvude keskmiseks tiheduseks lõigus $[1, x]$. Kuna võrratusest (1) järeldub, et

$$\lim_{x\to\infty} \frac{\pi(x)}{x} = 0,$$

siis algarvude keskmine tihedus kõigi naturaalarvude hulgas on null.

Peale valemi (8) on teada ka teisi funktsiooni $\pi(x)$ asümptootilisi valemeid. 1808.a. leidis Legendre empiirilisel teel, algarvude tabeli uurimisel, järgmise ligikaudse valemi:

$$\pi(x) \approx \frac{x}{\ln x - 1{,}08366} .$$

Samal viisil sai Gauss valemi

(9) $$\pi(x) \approx \int_2^x \frac{dt}{\ln t} .$$

Tšebõšov põhjendas aastatel 1849-1852 nende valemite kehtivuse, tõestades ühtlasi, et valem

(10) $$\pi(x) \sim \frac{x}{\ln x - a}$$

* Meenutame, et $f(x) \sim g(x)$ mingi piirprotsessi suhtes, kui selles piirprotsessis $\lim \frac{f(x)}{g(x)} = 1$.

on suurte x väärtuste puhul kõige täpsem siis, kui a = 1.

Lähtudes sellest, et valem (8) kehtib, näitame ka valemi (9) kehtivuse, s.t. tõestame, et

$$\lim_{x\to\infty}\left(\pi(x) : \int_2^x \frac{dt}{\ln t}\right) = 1.$$

Selleks tarvitseb näidata, et

$$\lim_{x\to\infty}\left(\int_2^x \frac{dt}{\ln t} : \frac{x}{\ln x}\right) = 1.$$

Kasutades L'Hospitale'i võtet saamegi

$$\lim_{x\to\infty}\left(\int_2^x \frac{dt}{\ln t} : \frac{x}{\ln x}\right) = \lim_{x\to\infty}\left(\frac{1}{\ln x} : \frac{\ln x - 1}{\ln^2 x}\right) =$$

$$= \lim_{x\to\infty}\frac{\ln x}{\ln x - 1} = 1.$$

Osutub, et Gaussi valem (9) on valemist (10) märksa täpsem. Ülevaate valemite (8) ja (9) täpsusest annab juuresolev tabel, mis on põhiliselt koostatud A.E.Inghami raamatus

x	$\pi(x)$	$\int_2^x \frac{dt}{\ln t}$	$\pi(x) : \int_2^x \frac{dt}{\ln t}$	$\pi(x) : \frac{x}{\ln x}$
10^3	168	177	0,94	1,159
10^4	1229	1245	0,98	1,132
10^5	9592	9629	0,996	1,104
10^6	78498	78627	0,9983	1,084
$5\cdot10^6$	348513	348637	0,9996	1,075
10^7	664579	664917	0,9994	1,071
10^8	5761455	5762208	0,99986	1,061
104395301	6000000	6000535	0,99991	1,061
10^9	50847478	50849234	0,99996	1,053
10^{10}	455052512	455055613	0,999993	1,048

(А.Е.Инхам. Распределение простых чисел, М.-Л., 1936) toodud tabeli põhjal; $\pi(10^{10})$ väärtus on võetud W.Sierpiński raamatust (В.Серпинский. Что мы знаем и чего не знаем о простых числах, М.-Л., 1963) lk. 29. Tuleb märkida, et nimetatud raamatus, samuti õpikus [2], lk. 274 on $\pi(10^9)$ väärtuseks märgitud 50 847 534. Käesolevas tabelis toodud väärtus on antud peale Inghami raamatu ka näiteks raamatutes [5], lk. 105 ja [9], lk. 61. Tabeli kolmandas veerus oleva integraali väärtused (ümardatuna täisarvudeks) on 1969.a. üle kontrollitud TRÜ elektronarvutil "Ural-4". Alt kolmandas reas on esitatud vastavad andmed suurima algarvude tabeli viimase arvu kohta (vt. I pt., § 4, punkt 2).

Märgime, et valemist (8) võib saada asümptootilise valemi ka n-nda algarvu p_n jaoks. Selleks lähtume seosest

$$\frac{\pi(x)\ln x}{x} = 1 + \alpha(x),$$

mis on lõpmata väikese $\alpha(x)$ korral samaväärne valemiga (8). Logaritmimisel saame

$$\ln \pi(x) + \ln \ln x - \ln x = \ln(1 + \alpha(x)),$$

millest

$$\frac{\ln \pi(x)}{\ln x} = 1 + \frac{\ln (1 + \alpha(x))}{\ln x} - \frac{\ln \ln x}{\ln x}$$

ja

$$\lim_{x \to \infty} \frac{\ln \pi(x)}{\ln x} = 1.$$

Nüüd leiame

$$\lim_{x \to \infty} \frac{x}{\pi(x) \ln \pi(x)} = \lim_{x \to \infty} \frac{x}{\pi(x) \ln x} \lim_{x \to \infty} \frac{\ln x}{\ln \pi(x)} = 1.$$

Kui võtame siin $x = p_n$, siis viimane võrdus omandab kuju

$$\lim_{n\to\infty} \frac{p_n}{n \ln n} = 1$$

ehk

(11) $$p_n \sim n \ln n.$$

Tuleb mainida, et valem (11) ei ole eriti täpne. Tema rakendusena arvutame näiteks algarvu $p_{6\ 000\ 000}$ ligikaudse väärtuse. Naturaallogaritmide tabelist leiame

$$\ln 6 = 1,\ 791\ 759\ 47,$$

$$\ln 10^6 = 6 \ln 10 = 13,815\ 510\ 56.$$

Seega $\ln 6\ 000\ 000 = \ln 6 + \ln 10^6 = 15,607\ 270\ 03$ ja

$$n \ln n = 93\ 643\ 620.$$

Võrreldes saadud tulemust $p_{6\ 000\ 000}$ täpse väärtusega 104 395 301 näeme, et relatiivne viga on ligikaudu 10 %. On muidugi selge, et n piiramatul kasvamisel relatiivne viga läheneb nullile.

§ 3*. EULERI VALEM. ALGARVUDE PÖÖRDVÄÄRTUSTE REA HAJUVUS

Käesolevas paragrahvis esitame veel mõningaid tulemusi, mis on seotud algarvude jaotumisega, eriti aga iseloomustavad algarvude "tihedust" naturaalarvude hulgas.

1. Euleri tõestus algarvude hulga lõpmatuse kohta. Euleri valem. I peatüki 4. paragrahvis tõestasime, et algarve on lõpmata palju (teoreem 1.21). Esitame nüüd nimetatud teoreemile Euleri tõestuse, mis kasutab matemaatilise

analüüsi aparatuuri ja pani aluse analüütilisele arvuteooriale.

Olgu p_λ algarv. Siis rida $\sum_{k=0}^{\infty} \frac{1}{p_\lambda^k}$ koondub ja kehtib valem

$$(1) \qquad \frac{1}{1-\frac{1}{p_\lambda}} = 1 + \frac{1}{p_\lambda} + \frac{1}{p_\lambda^2} + \ldots = \sum_{k=0}^{\infty} \frac{1}{p_\lambda^k} .$$

Oletame, et algarve on vaid lõplik hulk:

$$p_1, p_2, \ldots, p_n .$$

Kirjutame välja valemid (1) kõikide algarvude jaoks ja korrutame saadud n seose vastavad pooled. Vasakul saame

$$\prod_{\lambda=1}^{n} \frac{1}{1-\frac{1}{p_\lambda}} ,$$

paremal aga absoluutselt koonduva korrutisrea, mille üldliikme võib esitada kujul

$$(2) \qquad \frac{1}{p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}} ,$$

kus $\alpha_1, \alpha_2, \ldots, \alpha_n$ on suvalised mittenegatiivsed täisarvud. Kuid aritmeetika põhiteoreemi (teoreemi 1.33) kohaselt saab iga naturaalarvu esitada ühesel viisil kujul $p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \ldots p_n^{\alpha_n}$, sest nagu me eeldasime, leidub ainult n algarvu $p_1, p_2, \ldots, p_n$. Järelikult üldliikme (2) võib esitada ka kujul $\frac{1}{m}$, kus m on mistahes naturaalarv. Et liikmed kujul (2) on kõik üksteisest erinevad, siis võib ridade (1) korrutise esitada kujul

$$\sum_{m=1}^{\infty} \frac{1}{m} ,$$

kusjuures meie arutluse kohaselt on see rida koonduv. Kuid matemaatilises analüüsis tõestatakse, et saadud harmooniline rida hajub. Järelikult oletus, et algarvude hulk on lõplik, ei pea paika.

Teoreem 10.6. Kui $s > 1$, siis kehtib nn. Euleri valem

$$\prod_{\lambda=1}^{\infty} \frac{1}{1-\frac{1}{p_\lambda^s}} = \sum_{m=1}^{\infty} \frac{1}{m^s}.$$

Tõestus. Lähtume valemist

$$\frac{1}{1-\frac{1}{p_\lambda^s}} = 1 + \frac{1}{p_\lambda^s} + \frac{1}{p_\lambda^{2s}} + \frac{1}{p_\lambda^{3s}} + \dots \tag{3}$$

ja kirjutame ta välja kõikide algarvude $p_1, p_2, \dots, p_n$ jaoks, mis ei ületa mingit etteantud naturaalarvu N. Korrutame kõikide saadud valemite (3) vastavad pooled. Kuna korrutatavaid ridu on lõplik hulk, siis korrutisrida on absoluutselt koonduv ja tema liikmeid võib välja kirjutada suvalises järjekorras. Arvestades seda, paigutame korrutisrea liikmed kahanevas järjekorras. Saame tulemuseks seose

$$\prod_{\lambda=1}^{n} \frac{1}{1-\frac{1}{p_\lambda^s}} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \dots + \frac{1}{N^s} + \frac{1}{N_1^s} + \frac{1}{N_2^s} + \dots , \tag{4}$$

kus esimesed N liiget võrduse paremal poolel on järjestikuste naturaalarvude 1, 2, 3, 4, ..., N pöördväärtuste s-ndad astmed, sest naturaalarvud 1, 2, ..., N on kõik esitatavad kujul $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n}$. Arvude $N_1 \geqslant N + 1$, $N_2 \geqslant N_1 + 1$, ... seas ei esine enam kõiki järjestikuseid naturaalarve (näiteks ei esine p_{n+1}). Kui $s > 1$, siis rida

$$1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \dots$$

koondub ja seepärast võib iga kuitahes väikese positiivse reaalarvu ε jaoks leida naturaalarvu N, nii et

$$\frac{1}{(N+1)^s} + \frac{1}{(N+2)^s} + \ldots < \varepsilon .$$

Siis aga ammugi

$$\frac{1}{N_1^s} + \frac{1}{N_2^s} + \ldots < \varepsilon .$$

Seega valemist (4) järeldub, et lõpmatu korrutis $\prod_{\lambda=1}^{\infty} \frac{1}{1 - \frac{1}{p_\lambda^s}}$ koondub. Minnes valemis (4) üle piirile $n \to \infty$ ja arvestades, et siis ka $N \to \infty$, saamegi Euleri valemi. Euleri valemis esinevat summat, vaadelduna s funktsioonina, nimetatakse Riemanni dzeetafunktsiooniks ja tähistatakse $\zeta(s)$. Seega

$$\zeta(s) = \sum_{m=1}^{\infty} \frac{1}{m^s} .$$

Euleri valemi abil ja ζ-funktsiooni uurimise alusel on saadud algarvude kohta üsna kaugeleulatuvaid tulemusi.

2. Algarvude pöördväärtuste rea hajuvus. Käesoleva paragrahvi lõpul tõestame veel algarvude järgmise tähelepanuväärse omaduse.

Teoreem 10.7. Algarvude pöördväärtuste rida

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \ldots = \sum_{\lambda=1}^{\infty} \frac{1}{p_\lambda}$$

hajub.

Tõestus. Valem (3) kehtib, kui $s = 1$. Seega kehtib $s = 1$ korral ka valem (4), mis on esimesest tuletatud. Valemist (4) järeldub, et

$$\prod_{\lambda=1}^{n} \frac{1}{1 - \frac{1}{p_\lambda}} > \sum_{m=1}^{N} \frac{1}{m} ,$$

kus n on naturaalarvu N mitteületavate kõikide algarvude $p_1, \ldots, p_n$ arv. Laseme N piiramatult kasvada: $N \to \infty$; siis ka $n \to \infty$. Et harmooniline rida hajub ja tema summa on $+\infty$, siis hajub ka korrutis $\prod_{\lambda=1}^{\infty} \frac{1}{1 - \frac{1}{p_\lambda}}$ ja tema väärtus on $+\infty$. Siit järeldub, et hajub rida

$$\sum_{\lambda=1}^{\infty} \left(- \ln\left(1 - \frac{1}{p_\lambda}\right)\right) = \ln \prod_{\lambda=1}^{\infty} \frac{1}{1 - \frac{1}{p_\lambda}},$$

kusjuures tema summa on $+\infty$. Arendame $-\ln\left(1 - \frac{1}{p_\lambda}\right)$ ritta, arvestades, et $\frac{1}{p_\lambda} < 1$. Saame

$$0 < - \ln\left(1 - \frac{1}{p_\lambda}\right) = \frac{1}{p_\lambda} + \frac{1}{2}\left(\frac{1}{p_\lambda}\right)^2 + \frac{1}{3}\left(\frac{1}{p_\lambda}\right)^3 + \ldots <$$

$$< \frac{1}{p_\lambda} + \left(\frac{1}{p_\lambda}\right)^2 + \left(\frac{1}{p_\lambda}\right)^3 + \ldots = \frac{1}{p_\lambda - 1} \leqslant 2\,\frac{1}{p_\lambda}.$$

Rea $2\sum_{\lambda=1}^{\infty} \frac{1}{p_\lambda}$ liikmed on suuremad kui positiivsete liikmetega hajuva rea vastavad liikmed. Seega hajub ka rida

$2\sum_{\lambda} \frac{1}{p_\lambda}$ ja rida $\sum_{\lambda} \frac{1}{p_\lambda}$.

Tõestatud teoreemist järeldub näiteks, et küllalt suured algarvud paiknevad reaalarvude hulgas märksa tihedamalt kui naturaalarvude astmed reaalarvulise astendajaga $s > 1$. Tõepoolest, rida $\sum \frac{1}{n^s}$ koondub, kui $s > 1$.

§4. ALGARVUDE JAOTUMINE ARITMEETILISTES PROGRESSIOONIDES

Analoogiliselt sellega, nagu uurisime algarvude jaotumist kõigi naturaalarvude hulgas, võime uurida algarvude jaotumist aritmeetilistes progressioonides. Käesolevas pa-

ragrahvis anname ülevaate mõnedest sellel alal saadud tulemustest.

Vaatleme jada $\{an+b\}$, kus a ja b on ühistegurita täisarvud ($a > 0$), n aga naturaalarvuline muutuja. Nagu märkisime juba I peatükis, tõestas Dirichlet (teor. 1.30), et iga selline jada sisaldab lõpmata palju algarve.

Dirichlet kasutas oma teoreemi tõestamisel erilisi arvuteoreetilisi funktsioone $\chi(n)$, mida nimetatakse <u>karakteriteks</u>, ja neid funktsioone sisaldavaid ridu (Dirichlet' L-read)

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s},$$

kus s on kompleksne argument (erijuhul, kui $\chi(n) \equiv 1$ iga n korral, saame dzeetafunktsiooni $\zeta(s)$).

<u>Karakteriks</u> mooduli a järgi nimetatakse funktsiooni $\chi(n)$, mis rahuldab järgmisi tingimusi:

1) $\chi(1) = 1$;

2) $\chi(c) = 0$, kui $(c, a) > 1$;

3) $\chi(cd) = \chi(c)\chi(d)$ iga c ja d korral (tugev multiplikatiivsus);

4) $\chi(c) = \chi(d)$, kui $c \equiv d \pmod a$.

Dirichlet' tõestus kasutab asjaolu, et karakteritel on üks ja sama väärtus kõikide arvude korral, mis on mooduli a järgi kongruentsed, s.t. kuuluvad ühte ja samasse aritmeetilisse progressiooni vahega a.

Üksikutel erijuhtudel (jadad $\{4n-1\}$, $\{4n+1\}$, $\{6n+1\}$) on Dirichlet' teoreemi tõestus lihtne (vt. näit. [1], lk.

356-358). 1949.a. leidis A.Selberg teoreemile ka üldjuhul elementaarse tõestuse.

Analoogiliselt jaotusfunktsioonile $\pi(x)$, mis näitab arvu x mitte ületavate algarvude arvu kõigi naturaalarvude jadas, võib defineerida algarvude jaotusfunktsiooni aritmeetilisel progressioonil $\{an+b\}$. Tähistame reaalarvu x mitte ületavate algarvude arvu aritmeetilises progressioonis $\{an+b\}$, kus $(a, b) = 1$, sümboliga $\pi(x, a, b)$. Dirichlet' teoreemist järeldub, et

$$\pi(x, a, b) \to \infty \text{ , kui } x \to \infty .$$

Ka siin huvitab meid jaotusfunktsiooni asümptootiline hinnang. On tõestatud, et

$$\pi(x, a, b) \sim \frac{1}{\varphi(a)} \pi(x), \tag{1}$$

kus $\varphi(a)$ on Euleri φ-funktsioon. Arvestades funktsiooni $\pi(x)$ asümptootilisi valemeid, võime kirjutada:

$$\pi(x, a, b) \sim \frac{1}{\varphi(a)} \int_2^x \frac{dt}{\ln t}$$

ja

$$\pi(x, a, b) \sim \frac{1}{\varphi(a)} \frac{x}{\ln x} .$$

Valem (1) näitab, et fikseeritud a korral on kõikides progressioonides $\{an+b\}$, mis erinevad üksteisest vaid b poolest ja milles $(a, b) = 1$, ligikaudu ühesugune hulk arvu x mitte ületavaid algarve - keskmiselt $\frac{100}{\varphi(a)}$ % kõikidest algarvudest lõigust $[1, x]$.

Aritmeetiline progressioon kujutab endast lineaarse funktsiooni $f(t) = at + b$ väärtuste jada argumendi järjes-

tikustel naturaalarvulistel väärtustel. Võib aga vaadelda ka kõrgema astme polünoome, näiteks ruutpolünoomi

$$f(t) = at^2 + bt + c$$

argumendi täisarvulistel väärtustel, eeldades ühtlasi, et (a, b, c) = 1. Peab aga ütlema, et pole õnnestunud tõestada ühegi kõrgema kui esimese astme polünoomi f(t) korral, et jada $\{f(n)\}$ sisaldaks lõpmata palju algarve. Pole ka tõestatud, et ta sisaldab vaid lõpliku hulga algarve. See on üks seni lahendamata probleemidest. Isegi kõige lihtsama jada $\{n^2+1\}$ kohta ei saa midagi öelda. Vähemalt alguses sisaldab ta üsna palju algarve: esimese 3000 liikme kohta on neid loendatud 300.

Analoogilist huvi pakub ka näiteks lahendamata probleem, kas leidub lõpmata palju algarve Fibonacci arvude jadas

$$1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots,$$

kus iga järgnev arv on kahe eelneva summa ($u_{n+1} = u_{n-1} + u_n$, $u_1 = u_2 = 1$).

Lõpetades käesolevat peatükki ja ühtlasi kogu kursust, märgime, et arvuteoorias leidub hulgaliselt lihtsalt sõnastatavaid lahendamata probleeme, sealhulgas eriti ka neid, mis on seotud algarvudega ja nende jaotumisega. Mõningate lahendamata probleemide loetelu võib leida õpikust [1], lk. 367-368, ja ülesannete kogust [12], lk. 57-60.

HARJUTUSÜLESANNETE VASTUSED JA NÄPUNÄITED

1.1. b = 182, r = 115. 1.2. 233. 1.3. Olgu vaadeldav arv $N = 10^4a + 10^3b + 10^2c + 10d + e$. Pärast ühe numbri ümberpaigutamist saadav arv $N_1 = 10^4b + 10^3c + 10^2d + 10e + a$ esitada kujul $10N - 99999a$. 1.4. Esitada korrutis kujul $n(n+1)(n+2) + (n-1)n(n+1)$ ja näidata, et kumbki liidetav jagub 6-ga. 1.6. $n^5 - n = (n-1)n(n+1)(n^2+1) =$
$= (n-2)(n-1)n(n+1)(n+2) + 5(n-1)n(n+1)$. Näidata, et kumbki liidetav jagub 30-ga. 1.7. a) 17; b) 7429; c) 437; d) 1. 1.8. x = - 6, y = 11. Seose saamiseks avaldada Eukleidese algoritmi eelviimasest võrdusest d. Sellele eelneva võrduse abil avaldada d suuruste r_{k-2} ja r_{k-3} kaudu jne., kuni lõpuks d on avaldatud a ja b lineaarse kombinatsioonina. 1.9. Kasutada teoreemi 1.14. 1.10. a) 1 110 111; b) b) 177 480 177; d) 96 577. 1.11. Kasutada täieliku induktsiooni meetodit ja teoreemi 1.16. 1.12. Näpunäide: Esitada arvud n kujul: n = 3q+r, r = 0, 1, 2. 1.13. Tõestus on analoogiline teoreemi 1.29 tõestusega. 1.14. $2^3 \cdot 3^3 \cdot 5^4 \cdot 7^3 \cdot 11^2 \cdot 17 \cdot 23 \cdot 37$; jagajate arv on 7680. 1.15. 1, 2, 4, 8, 11, 22, 44, 88, 121, 242, 484, 968.

2.1. [1, 1, 2, 1, 1, 6, 1, 1], [1, 1, 2, 1, 1, 6, 2]. 2.2. [2, 2, 1, 4, 1, 1, 6, 20, 2]. 2.3. $\frac{516901}{740785}$. 2.4. $\frac{34}{21}$; $\frac{1}{1}, \frac{2}{1}, \frac{3}{2}, \frac{5}{3}, \frac{8}{5}, \frac{13}{8}, \frac{21}{13}, \frac{34}{21}$. Paaritu elementide arvu korral

jääb ära eelviimane lähismurd; ülejäänud lähismurrud jäävad muutumatuks. 2.7. a) $x = 17 + 35t$, $y = 44 - 97t$; b) $x = 6 + 19t$, $y = -2 - 10t$. 2.8. 31 raamatut 23 kop. tükk, 17 raamatut 38 kop. tükk. 2.9. 17, 111; 35, 86; 53, 61; 71, 36; 89, 11. 2.10. Kui x on kasutatavate pikemate torude arv ja y lühemate torude arv, siis $x = 8$, 15, 22, 29 ja vastavalt $y = 61$, 49, 37, 25. Kui tahetakse säilitada võimalikult palju pikemaid torusid, siis tuleb võtta $x = 8$ ja $y = 61$. 2.11. a) $[1,(1, 2)]$, b) $[3,(1, 1, 1, 1, 6)]$, c) $[5,(1, 1, 3, 5, 3, 1, 1, 10)]$, d) $[1,(2, 2, 2, 1, 12, 1)]$, e) $[-1, 2,(3)]$. 2.12. $[1, 2, 3, 1, \ldots]$. 2.13. $\frac{193}{71}$, $\left|e - \frac{193}{71}\right| < \frac{1}{33015} < 0{,}000031$. 2.14. $\frac{649}{180}$. 2.17. a) $\frac{1+\sqrt{5}}{2}$, b) $-2+\sqrt{3}$, c) $9+\sqrt{89}$, d) $-5+\sqrt{29}$, e) $\sqrt{57}$, f) $\sqrt{99}$. 2.19. a) $[3,(1, 1, 4, 1)]$, b) $[0,(1, 1, 4, 1)]$, c) $[-1,(1, 1, 4, 1)]$. 2.20. $[0,(9, 2)]$, $[2,(9, 2)]$. 2.21. Vähimad lahendid: a) $x = 2$, $y = 1$; b) $x = 17$, $y = 3$; c) $x = 649$, $y = 180$; d) $x = 500\,001$, $y = 53\,000$; e) $x = 99$, $y = 10$.

3.1. a) 4, b) 3, c) 2. 3.2. a) Tähistanud $\cos\frac{\pi}{n} + i\sin\frac{\pi}{n} = z$, saame $z^n = \cos\pi + i\sin\pi = -1$ ehk $z^n + 1 = 0$. b) Näpunäide: kasutada seost $\sin 3\varphi = 3\sin\varphi - 4\sin^3\varphi$. 3.4. Näpunäide: Võtta $\varepsilon = \frac{1}{2}$ ja valida $b = \frac{1}{2^{3^k}}$; edasine on analoogiline tekstis toodud näitega.

4.1. 18; 4836. 4.2. 201 110; 476 377. 4.3. Erinevaid jagajaid on kas 28 või 22. 4.4. 18. 4.5. 16 875. 4.8. Näpunäide: uurida nõutud kujuga arve α väärtustel 0, 1, ... 4.9. $x = 6$, $y = 5$, $z = 4$. 4.10. 165. 4.11. $2^{116}\cdot 3^{58}\cdot 5^{28}\cdot 7^{19}\cdot 11^{10}\cdot 13^{9}\cdot 17^{7}\cdot 19^{6}\cdot 23^{5}\cdot 29^{4}\cdot 31^{3}\cdot 37^{3}\cdot 41^{2}\cdot 43^{2}\cdot 47^{2}\cdot 53^{2}\cdot 61$.

·67·71·73·79·83·89·97·101·103·107·113. 4.12. 490. 4.14. 148. 4.15. 4054. 4.16. $999 - \left[\frac{999}{5}\right] - \left[\frac{999}{7}\right] + \left[\frac{999}{5\cdot7}\right] = 686$. 4.17. $400 - \left[\frac{400}{2}\right] - \left[\frac{400}{3}\right] + \left[\frac{400}{6}\right] = 133$. 4.18. 400. 4.19. 500. 4.20. 8700. 4.21. 40 arvu: 10, 30, 70, 90, ..., 970, 990. 4.23. $\varphi(m)$. 4.24. Esimene juht leiab aset, kui $(m, 2) = 1$, teine, kui $(m, 2) = 2$. 4.26. Näpunäide: Kasutada $\varphi(m)$ avaldist kujul $\varphi(m) = p_1^{\alpha_1-1}(p_1-1)\ldots p_n^{\alpha_n-1}(p_n-1)$.

5.3. 83. 5.4. 70. 5.5. 61. 5.7. a) Tulemus on ebaõige. b) Tulemus on ebaõige, kuid kontroll moodulite 9 ja 11 järgi seda ei avasta. 5.9. Jagub. 5.10. 56. Näpunäide: Siin $a = 34$, $m = 110$, $(a, m) = 2$. Et jagamisel tekkiv jääk on paarisarv, siis otsida teda kujul $2x$. Pärast kongruentsi $2\cdot17.34^{59521} \equiv 2x \pmod{110}$ mõlemate poolte ja mooduli jagamist 2-ga saame juba rakendada Euleri teoreemi. 5.11. Näpunäide: Kasutades Euleri teoreemi näidata, et kongruents kehtib eraldi moodulite 37 ja 73 korral. Seejärel rakendada teoreemi 5.14.

6.1. a) $x \equiv 5 \pmod 6$; b) $x \equiv 2 \pmod 5$ ja $x \equiv -2 \pmod 5$. 6.2. a) $x \equiv -1 \pmod 5$ ja $x \equiv -2 \pmod 5$. 6.3. a) $x \equiv 30 \pmod{77}$, b) $x \equiv 21 \pmod{67}$, c) $x \equiv 7 \pmod{25}$. 6.4. a) $x \equiv 81 \pmod{337}$, b) $x \equiv 51 \pmod{360}$. 6.5. $x \equiv 16 \pmod{36}$. 6.6. a) $x \equiv 200 \pmod{551}$ ehk $x \equiv 200, 751, 1302, 1853, 2404 \pmod{2755}$; b) $x \equiv 8 \pmod{33}$. 6.7. a) $x \equiv 283 \pmod{385}$. 6.8. c) $x \equiv 1157 \pmod{1860}$. 6.10. $353 + 390t$, kus $t = 0, 1, 2, \ldots$ 6.11. a) $x \equiv 2 \pmod 3$; b) $x \equiv 3, 4 \pmod 5$; c) $x \equiv 2 \pmod 7$; e) Pärast lihtsustamist:

$2x^2 - x - 5 \equiv 0 \pmod{11}$; lahendid: $x \equiv 2, 4 \pmod{11}$; f) Pärast lihtsustamist: $2x^8 + 4x^5 + x + 5 \equiv 0 \pmod{11}$, lahendid: $x \equiv 3, 5 \pmod{11}$. 6.12. a) $x \equiv -13, -10, -4, 2, 5, 11 \pmod{30}$; c) $x \equiv 106 \pmod{125}$; d) $x \equiv 2102 \pmod{7^4}$; e) $x \equiv 70, 124, 223 \pmod{225}$; f) $x \equiv -757, -163, -1, 593, 1187, 1349 \pmod{2^2 \cdot 3^3 \cdot 5^2}$.

7.6. $\left(\frac{3}{p}\right) = 1$, kui $p = 12 \pm 1$; $\left(\frac{3}{p}\right) = -1$, kui $p = 12 \pm 5$. 7.7. Jagajateks võivad olla vaid algarvud 2, 3 ja algarvud kujuga 12 ± 1. 7.8. a) Ei ole, b) on, c) on. 7.9. Näpunäide: Asendada kongruents ekvivalentse süsteemiga algarvuliste moodulite järgi. a) Lahenduv, b) lahenduv, c) ei ole, d) ei ole, e) lahenduv, f) ei ole. 7.10. a) +1, b) -1. 7.11. a) -1. 7.12. b) $x \equiv \pm 17 \pmod{37}$; c) $x \equiv \pm 37 \pmod{97}$; d) $x \equiv \pm 30 \pmod{67}$; e) $x \equiv \pm 40 \pmod{101}$; f) $x \equiv \pm 50 \pmod{113}$. 7.13. a) $x \equiv \pm 37, \pm 91 \pmod{256}$; b) $x \equiv \pm 32 \pmod{125}$; c) $x \equiv \pm 19 \pmod{343}$; d) $x \equiv \pm 16, \pm 19, \pm 26, \pm 44 \pmod{105}$; e) $x \equiv \pm 11, \pm 15, \pm 37, \pm 41 \pmod{104}$; f) $x \equiv \pm 17, \pm 37 \pmod{90}$.

8.1. Näpunäide: Kasutada vastuväitelist tõestust. 8.9. a) 12; b) 36; c) 1992. 8.10. Mooduli 13^α järgi on algjuureks arv 6 iga $\alpha \geqslant 1$ korral, mooduli 26 järgi on algjuureks arv 19, mooduli $2 \cdot 13^2$ järgi arv 175. 8.14. Iga arv on 5. astme jääk modulo p, kui algarv p on kujuga 5n+2, 5n+3 või 5n+4. Kõik arvud ei ole 5. astme jäägid, kui $p = 5n+1$; viimasel juhul on taandatud jääkide süsteemis modulo p arvult $\frac{p-1}{5} = n$ viienda astme jääki. 8.15. a) $x \equiv 2 \pmod{23}$; b) ei

ole lahenduv; c) $x \equiv 5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22 \pmod{23}$; d) $x \equiv 6 \pmod{11}$; e) $x \equiv 17 \pmod{22}$. 8.16. 23. 8.17. 35. 8.18. a) $x \equiv 17, 63, 66 \pmod{73}$; b) $x \equiv 2, 3, 10, 11 \pmod{13}$; c) pole lahenduv; e) $x \equiv 13, 29, 31 \pmod{73}$; g) $x \equiv \pm 15 \pmod{37}$. 8.19. b) $x \equiv 74 \pmod{79}$; d) $x \equiv 30 \pmod{221}$. 8.20. a) $x \equiv 23 \pmod{66}$, $x > 0$; b) pole lahendit; c) $x \equiv 7 \pmod{9}$, $x > 0$; d) $x \equiv 0 \pmod{9}$, $x \geqslant 0$; e) $x \equiv 1 \pmod{2}$, $x > 0$; f) $x \equiv 37 \pmod{44}$, $x > 0$. 8.21. b) $x \equiv -38c_1 + 39c_2 \pmod{13 \cdot 19}$, kus $c_1 = 4, 10, 12$ ja $c_2 = 10, 13, 15$ (kokku 9 lahendit). 8.24. Astendajale 7 kuuluvad arvud $a \equiv 7, 16, 20, 23, 24, 25 \pmod{29}$. 8.26. a) 3; b) 21; c) 58; e) 44; g) 6; h) 6; i) 16. 8.27. a) 2; 2; b) 2; 22; c) 4; 48. 8.28. a) 12; b) 14; c) 58; e) 11; g) 10; h) 6; i) 8. 8.30. $\frac{2}{19} = 0,(105263157894736842)$. 8.31. Näpunäide: Esitada murd kujul $\frac{a}{10^k} = \frac{1}{8^n} \cdot \frac{2^\alpha a}{5^k}$ ja rakendada lk-l 243 esitatud mõttekäiku. Vaadelda eraldi juhte $k = 1$ ja $k > 1$. Viimasel juhul kasutada teoreemi 8.6. Vastus: Perioodi pikkus on $4 \cdot 5^{k-1}$. 8.32. Näpunäide: Teisendada kümnendmurd eelnevalt harilikuks murruks.

9.3. Ei sisalda algtegureid kujuga $6n+5$. 9.4. Ei sisalda algtegureid kujuga $20n+11$, $20n+13$, $20n+17$, $20n+19$.

INDEKSITE TABELID

$p=3,\ p-1=2,\ g=2$

N	0	1	2	3	4	5	6	7	8	9
0		0	1							

I	0	1	2	3	4	5	6	7	8	9
0	1	2								

$p=5,\ p-1=2^2,\ g=2$

N	0	1	2	3	4	5	6	7	8	9
0		0	1	3	2					

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	3						

$p=7,\ p-1=2\cdot 3,\ g=3$

N	0	1	2	3	4	5	6	7	8	9
0		0	2	1	4	5	3			

I	0	1	2	3	4	5	6	7	8	9
0	1	3	2	6	4	5				

$p=11,\ p-1=2\cdot 5,\ g=2$

N	0	1	2	3	4	5	6	7	8	9
0		0	1	8	2	4	9	7	3	6
1	5									

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	5	10	9	7	3	6
1										

$p = 13,\ p - 1 = 2^2 \cdot 3,\ g = 2$

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

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

$p = 17,\ p - 1 = 2^4,\ g = 3$

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

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

$p = 19,\ p - 1 = 2 \cdot 3^2,\ g = 2$

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

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

$p = 23,\ p - 1 = 2 \cdot 11,\ g = 5$

N	0	1	2	3	4	5	6	7	8	9
0		0	2	16	4	1	18	19	6	10
1	3	9	20	14	21	17	8	7	12	15
2	5	13	11							

l	0	1	2	3	4	5	6	7	8	9
0	1	5	2	10	4	20	8	17	16	11
1	9	22	18	21	13	19	3	15	6	7
2	12	14								

$p = 29,\ p - 1 = 2^2 \cdot 7,\ g = 2$

N	0	1	2	3	4	5	6	7	8	9
0		0	1	5	2	22	6	12	3	10
1	23	25	7	18	13	27	4	21	11	9
2	24	17	26	20	8	16	19	15	14	

l	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	3	6	12	24	19
1	9	18	7	14	28	27	25	21	13	26
2	23	17	5	10	20	11	22	15		

$p = 31, \quad p - 1 = 2 \cdot 3 \cdot 5, \quad g = 3$

N	0	1	2	3	4	5	6	7	8	9
0		0	24	1	18	20	25	28	12	2
1	14	23	19	11	22	21	6	7	26	4
2	8	29	17	27	13	10	5	3	16	9
3	15									

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	19	26	16	17	20	29
1	25	13	8	24	10	30	28	22	4	12
2	5	15	14	11	2	6	18	23	7	21

$p = 37, \quad p - 1 = 2^2 3^2, \quad g = 2$

N	0	1	2	3	4	5	6	7	8	9
0		0	1	26	2	23	27	32	3	16
1	24	30	28	11	33	13	4	7	17	35
2	25	22	31	15	29	10	12	6	34	21
3	14	9	5	20	8	19	18			

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	27	17	34	31
1	25	13	26	15	30	23	9	18	36	35
2	33	29	21	5	10	20	3	6	12	24
3	11	22	7	14	28	19				

$p = 41, \quad p - 1 = 2^3 \cdot 5, \quad g = 6$

N	0	1	2	3	4	5	6	7	8	9
0		0	26	15	12	22	1	39	38	30
1	8	3	27	31	25	37	24	33	16	9
2	34	14	29	36	13	4	17	5	11	7
3	23	28	10	18	19	21	2	32	35	6
4	20									

I	0	1	2	3	4	5	6	7	8	9
0	1	6	36	11	25	27	39	29	10	19
1	32	28	4	24	21	3	18	26	33	34
2	40	35	5	30	16	14	2	12	31	22
3	9	13	37	17	20	38	23	15	8	7

$p = 43, \quad p - 1 = 2 \cdot 3 \cdot 7, \quad g = 3$

N	0	1	2	3	4	5	6	7	8	9
0		0	27	1	12	25	28	35	39	2
1	10	30	13	32	20	26	24	38	29	19
2	37	36	15	16	40	8	17	3	5	41
3	11	34	9	31	23	18	14	7	4	33
4	22	6	21							

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	38	28	41	37	25	32
1	10	30	4	12	36	22	23	26	35	19
2	14	42	40	34	16	5	15	2	6	18
3	11	33	13	39	31	7	21	20	17	8
4	24	29								

$p = 47, \quad p - 1 = 2 \cdot 23, \quad g = 5$

N	0	1	2	3	4	5	6	7	8	9
0		0	18	20	36	1	38	32	8	40
1	19	7	10	11	4	21	26	16	12	45
2	37	6	25	5	28	2	29	14	22	35
3	39	3	44	27	34	33	30	42	17	31
4	6	15	24	13	43	41	23			

I	0	1	2	3	4	5	6	7	8	9
0	1	5	25	31	14	23	21	11	8	40
1	12	13	18	43	27	41	17	38	2	10
2	3	15	28	46	42	22	16	33	24	26
3	36	39	7	35	34	29	4	20	6	30
4	9	45	37	44	32	19				

$p = 53, \quad p - 1 = 2^2 \cdot 13, \quad g = 2$

N	0	1	2	3	4	5	6	7	8	9
0	48	0	1	17	2	47	18	14	3	34
1	49	6	19	24	15	12	4	10	35	37
2	13	31	7	39	20	42	25	51	16	46
3	50	33	5	23	11	9	36	30	38	41
4	43	45	32	22	8	29	40	44	21	28
5		27	26							

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	11	22	44	35
1	17	34	15	30	7	14	28	3	6	12
2	24	48	43	33	13	26	52	51	49	45
3	37	21	42	31	9	18	36	19	38	23
4	46	39	25	50	47	41	29	5	10	20
5	40	27								

$p = 59, \quad p - 1 = 2 \cdot 29, \quad g = 2$

N	0	1	2	3	4	5	6	7	8	9
0		0	1	50	2	6	51	18	3	42
1	7	25	52	45	19	56	4	40	43	38
2	8	10	26	15	53	12	46	34	20	28
3	57	49	5	17	41	24	44	55	39	37
4	9	14	11	33	27	48	16	23	54	36
5	13	32	47	22	35	31	21	30	29	

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	5	10	20	40
1	21	42	25	50	41	23	46	33	7	14
2	28	56	53	47	35	11	22	44	29	58
3	57	55	51	43	27	54	49	39	19	38
4	17	34	9	18	36	13	26	52	45	31
5	3	6	12	24	48	37	15	30		

$p = 61, \quad p - 1 = 2^2 \cdot 3 \cdot 5, \quad g = 2$

N	0	1	2	3	4	5	6	7	8	9
0		0	1	6	2	22	7	49	3	12
1	23	15	8	40	50	28	4	47	13	26
2	24	55	16	57	9	44	41	18	51	35
3	29	59	5	21	48	11	14	39	27	46
4	25	54	56	43	17	34	58	20	10	38
5	45	53	42	33	19	37	52	32	36	31
6	30									

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	3	6	12	24
1	48	35	9	18	36	11	22	44	27	54
2	47	33	5	10	20	40	19	38	15	30
3	60	59	57	53	45	29	58	55	49	37
4	13	26	52	43	25	50	39	17	34	7
5	14	28	56	51	41	21	42	23	46	31

$p = 67, \quad p - 1 = 2 \cdot 3 \cdot 11, \quad g = 2$

N	0	1	2	3	4	5	6	7	8	9
0		0	1	39	2	15	40	23	3	12
1	16	59	41	19	24	54	4	64	13	10
2	17	62	60	28	42	30	20	51	25	44
3	55	47	5	32	65	38	14	22	11	58
4	18	53	63	9	61	27	29	50	43	46
5	31	37	21	57	52	8	26	49	45	36
6	56	7	48	35	6	34	33			

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	64	61	55	43
1	19	38	9	18	36	5	10	20	40	13
2	26	52	37	7	14	28	56	45	23	46
3	25	50	33	66	65	63	59	51	35	3
4	6	12	24	48	29	58	49	31	62	57
5	47	27	54	41	15	30	60	53	39	11
6	22	44	21	42	17	34				

$p = 71, \quad p - 1 = 2 \cdot 5 \cdot 7, \quad g = 7$

N	0	1	2	3	4	5	6	7	8	9
0		0	6	26	12	28	32	1	18	52
1	34	31	38	39	7	54	24	49	58	16
2	40	27	37	15	44	56	45	8	13	68
3	60	11	30	57	55	29	64	20	22	65
4	46	25	33	48	43	10	21	9	50	2
5	62	5	51	23	14	59	19	42	4	3
6	66	69	17	53	36	67	63	47	61	41
7	35									

I	0	1	2	3	4	5	6	7	8	9
0	1	7	49	59	58	51	2	14	27	47
1	45	31	4	28	54	23	19	62	8	56
2	37	46	38	53	16	41	3	21	5	35
3	32	11	6	42	10	70	64	22	12	13
4	20	69	57	44	24	26	40	67	43	17
5	48	52	9	63	15	34	25	33	18	55
6	30	68	50	66	36	39	60	65	29	61

$p = 73, \quad p - 1 = 2^3 \cdot 3^2, \quad g = 5$

N	0	1	2	3	4	5	6	7	8	9
0		0	8	6	16	1	14	33	24	12
1	9	55	22	59	41	7	32	21	20	62
2	17	39	63	46	30	2	67	18	49	35
3	15	11	40	61	29	34	28	64	70	65
4	25	4	47	51	71	13	54	31	38	66
5	10	27	3	53	26	56	57	68	43	5
6	23	58	19	45	48	60	69	50	37	52
7	42	44	36							

I	0	1	2	3	4	5	6	7	8	9
0	1	5	25	52	41	59	3	15	2	10
1	50	31	9	45	6	30	4	20	27	62
2	18	17	12	60	8	40	54	51	36	34
3	24	47	16	7	35	29	72	68	48	21
4	32	14	70	58	71	63	23	42	64	28
5	67	43	69	53	46	11	55	56	61	13
6	65	33	19	22	37	39	49	26	57	66
7	38	44								

$p = 79, \quad p - 1 = 2 \cdot 3 \cdot 13, \quad g = 3$

N	0	1	2	3	4	5	6	7	8	9
0		0	4	1	8	62	5	53	12	2
1	66	68	9	34	57	63	16	21	6	32
2	70	54	72	26	13	46	38	3	61	11
3	67	56	20	69	25	37	10	19	36	35
4	74	75	58	49	76	64	30	59	17	28
5	50	22	42	77	7	52	65	33	15	31
6	71	45	60	55	24	18	73	48	29	27
7	41	51	14	44	23	47	40	43	39	

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	2	6	18	54	4	12
1	36	29	8	24	72	58	16	48	65	37
2	32	17	51	74	64	34	23	69	49	68
3	46	59	19	57	13	39	38	35	26	78
4	76	70	52	77	73	61	25	75	67	43
5	50	71	55	7	21	63	31	14	42	47
6	62	28	5	15	45	56	10	30	11	33
7	20	60	22	66	40	41	44	53		

$p = 83, \quad p - 1 = 2 \cdot 41, \quad g = 2$

N	0	1	2	3	4	5	6	7	8	9
0		0	1	72	2	27	73	8	3	62
1	28	24	74	77	9	17	4	56	63	47
2	29	80	25	60	75	54	78	52	10	12
3	18	38	5	14	57	35	64	20	48	67
4	30	40	81	71	26	7	61	23	76	16
5	55	46	79	59	53	51	11	37	13	34
6	19	66	39	70	6	22	15	45	58	50
7	36	33	65	69	21	44	49	32	68	43
8	31	42	41							

I	0	1	2	3	4	5	6	7	8	9
0	1	2	4	8	16	32	64	45	7	14
1	28	56	29	58	33	66	49	15	30	60
2	37	74	65	47	11	22	44	5	10	20
3	40	80	77	71	59	35	70	57	31	62
4	41	82	81	79	75	67	51	19	38	76
5	69	55	27	54	25	50	17	34	68	53
6	23	46	9	18	36	72	61	39	78	73
7	63	43	3	6	12	24	48	13	26	52
8	21	42								

$p = 89,\ p - 1 = 2^3 \cdot 11,\ g = 3$

N	0	1	2	3	4	5	6	7	8	9
0		0	16	1	32	70	17	81	48	2
1	86	84	33	23	9	71	64	6	18	35
2	14	82	12	57	49	52	39	3	25	59
3	87	31	80	85	22	63	34	11	51	24
4	30	21	10	29	28	72	73	54	65	74
5	68	7	55	78	19	66	41	36	75	43
6	15	69	47	83	8	5	13	56	38	58
7	79	62	50	20	27	53	67	77	40	42
8	46	4	37	61	26	76	45	60	44	

I	0	1	2	3	4	5	6	7	8	9
0	1	3	9	27	81	65	17	51	64	14
1	42	37	22	66	20	60	2	6	18	54
2	73	41	34	13	39	28	84	74	44	43
3	40	31	4	12	36	19	57	82	68	26
4	78	56	79	59	88	86	80	62	8	24
5	72	38	25	75	47	52	67	23	69	29
6	87	83	71	35	16	48	55	76	50	61
7	5	15	45	46	49	58	85	77	53	70
8	32	7	21	63	11	33	10	30		

$p = 97,\ p - 1 = 2^5 \cdot 3,\ g = 5$

N	0	1	2	3	4	5	6	7	8	9
0		0	34	70	68	1	8	31	6	44
1	35	86	42	25	65	71	40	89	78	81
2	69	5	24	77	76	2	59	18	3	13
3	9	46	74	60	27	32	16	91	19	95
4	7	85	39	4	58	45	15	84	14	62
5	36	63	93	10	52	87	37	55	47	67
6	43	64	80	75	12	26	94	57	61	51
7	66	11	50	28	29	72	53	21	33	30
8	41	88	23	17	73	90	38	83	92	54
9	79	56	49	20	22	82	48			

I	0	1	2	3	4	5	6	7	8	9
0	1	5	25	28	43	21	8	40	6	30
1	53	71	64	29	48	46	36	83	27	38
2	93	77	94	82	22	13	65	34	73	74
3	79	7	35	78	2	10	50	56	86	42
4	16	80	12	60	9	45	31	58	96	92
5	72	69	54	76	89	57	91	67	44	26
6	33	68	49	51	61	14	70	59	4	20
7	3	15	75	84	32	63	24	23	18	90
8	62	19	95	87	47	41	11	55	81	17
9	85	37	88	52	66	39				

ALGARVUDE JA NENDE VÄHIMATE ALGJUURTE TABEL

p	g	p	g	p	g	p	g	p	g	p	g	p	g
2	1	179	2	419	2	661	2	947	2	1229	2	1523	2
3	2	181	2	421	2	673	5	953	3	1231	3	1531	2
5	2	191	19	431	7	677	2	967	5	1237	2	1543	5
7	3	193	5	433	5	683	5	971	6	1249	7	1549	2
11	2	197	2	439	15	691	3	977	3	1259	2	1553	3
13	2	199	3	443	2	701	2	983	5	1277	2	1559	19
17	3	211	2	449	3	709	2	991	6	1279	3	1567	3
19	2	223	3	457	13	719	11	997	7	1283	2	1571	2
23	5	227	2	461	2	727	5	1009	11	1289	6	1579	3
29	2	229	6	463	3	733	6	1013	3	1291	2	1583	5
31	3	233	3	467	2	739	3	1019	2	1297	10	1597	11
37	2	239	7	479	13	743	5	1021	10	1301	2	1601	3
41	6	241	7	487	3	751	3	1031	14	1303	6	1607	5
43	3	251	6	491	2	757	2	1033	5	1307	2	1609	7
47	5	257	3	499	7	761	6	1039	3	1319	13	1613	3
53	2	263	5	503	5	769	11	1049	3	1321	13	1619	2
59	2	269	2	509	2	773	2	1051	7	1327	3	1621	2
61	2	271	6	521	3	787	2	1061	2	1361	3	1627	3
67	2	277	5	523	2	797	2	1063	3	1367	5	1637	2
71	7	281	3	541	2	809	3	1069	6	1373	2	1657	11
73	5	283	3	547	2	811	3	1087	3	1381	2	1663	3
79	3	293	2	557	2	821	2	1091	2	1399	13	1667	2
83	2	307	5	563	2	823	3	1093	5	1409	3	1669	2
89	3	311	17	569	3	827	2	1097	3	1423	3	1693	2
97	5	313	10	571	3	829	2	1103	5	1427	2	1697	3
101	2	317	2	577	5	839	11	1109	2	1429	6	1699	3
103	5	331	3	587	2	853	2	1117	2	1433	3	1709	3
107	2	337	10	593	3	857	3	1123	2	1439	7	1721	3
109	6	347	2	599	7	859	2	1129	11	1447	3	1723	3
113	3	349	2	601	7	863	5	1151	17	1451	2	1733	2
127	3	353	3	607	3	877	2	1153	5	1453	2	1741	2
131	2	359	7	613	2	881	3	1163	5	1459	5	1747	2
137	3	367	6	617	3	883	2	1171	2	1471	6	1753	7
139	2	373	2	619	2	887	5	1181	7	1481	3	1759	6
149	2	379	2	631	3	907	2	1187	2	1483	2	1777	5
151	6	383	5	641	3	911	17	1193	3	1487	5	1783	10
157	5	389	2	643	11	919	7	1201	11	1489	14	1787	2
163	2	397	5	647	5	929	3	1213	2	1493	2	1789	6
167	5	401	3	653	2	937	5	1217	3	1499	2	1801	11
173	2	409	21	659	2	941	2	1223	5	1511	11	1811	6

p	g	p	g	p	g	p	g	p	g	p	g	p	g
1823	5	2131	2	2437	2	2749	6	3083	2	3433	5	3733	2
1831	3	2137	10	2441	6	2753	3	3089	3	3449	3	3739	7
1847	5	2141	2	2447	5	2767	3	3109	6	3457	7	3761	3
1861	2	2143	3	2459	2	2777	3	3119	7	3461	2	3767	5
1867	2	2153	3	2467	2	2789	2	3121	7	3463	3	3769	7
1871	14	2161	23	2473	5	2791	6	3137	3	3467	2	3779	2
1873	10	2179	7	2477	2	2797	2	3163	3	3469	2	3793	5
1877	2	2203	5	2503	3	2801	3	3167	5	3491	2	3797	2
1879	6	2207	5	2521	17	2803	2	3169	7	3499	2	3803	2
1889	3	2213	2	2531	2	2819	2	3181	7	3511	7	3821	3
1901	2	2221	2	2539	2	2833	5	3187	2	3517	2	3823	3
1907	2	2237	2	2543	5	2837	2	3191	11	3527	5	3833	3
1913	3	2239	3	2549	2	2843	2	3203	2	3529	17	3847	5
1931	2	2243	2	2551	6	2851	2	3209	3	3533	2	3851	2
1933	5	2251	7	2557	2	2857	11	3217	5	3539	2	3853	2
1949	2	2267	2	2579	2	2861	2	3221	10	3541	7	3863	5
1951	3	2269	2	2591	7	2879	7	3229	6	3547	2	3877	2
1973	2	2273	3	2593	7	2887	5	3251	6	3557	2	3881	13
1979	2	2281	7	2609	3	2897	3	3253	2	3559	3	3889	11
1987	2	2287	19	2617	5	2903	5	3257	3	3571	2	3907	2
1993	5	2293	2	2621	2	2909	2	3259	3	3581	2	3911	13
1997	2	2297	5	2633	3	2917	5	3271	3	3583	3	3917	2
1999	3	2309	2	2647	3	2927	5	3299	2	3593	3	3919	3
2003	5	2311	3	2657	3	2939	2	3301	6	3607	5	3923	2
2011	3	2333	2	2659	2	2953	13	3307	2	3613	2	3929	3
2017	5	2339	2	2663	5	2957	2	3313	10	3617	3	3931	2
2027	2	2341	7	2671	7	2963	2	3319	6	3623	5	3943	3
2029	2	2347	3	2677	2	2969	3	3323	2	3631	15	3947	2
2039	7	2351	13	2683	2	2971	10	3329	3	3637	2	3967	6
2053	2	2357	2	2687	5	2999	17	3331	3	3643	2	3989	2
2063	5	2371	2	2689	19	3001	14	3343	5	3659	2	4001	3
2069	2	2377	5	2693	2	3011	2	3347	2	3671	13	4003	2
2081	3	2381	3	2699	2	3019	2	3359	11	3673	5	4007	5
2083	2	2383	5	2707	2	3023	5	3361	22	3677	2	4013	2
2087	5	2389	2	2711	7	3037	2	3371	2	3691	2	4019	2
2089	7	2393	3	2713	5	3041	3	3373	5	3697	5	4021	2
2099	2	2399	11	2719	3	3049	11	3389	3	3701	2	4027	3
2111	7	2411	6	2729	3	3061	6	3391	3	3709	2	4049	3
2113	5	2417	3	2731	3	3067	2	3407	5	3719	7	4051	6
2129	3	2423	5	2741	2	3079	6	3413	2	3727	3	4057	5

KIRJANDUS

I. Бухштаб А.А. Теория чисел. М., I966.

2. Михелович Ш.Х. Теория чисел. М., I967.

3. Виноградов И.М. Основы теории чисел. М., I972.

4. Сушкевич А.К. Теория чисел. Харьков, I954.

5. Арнольд И.В. Теория чисел. М., I939.

6. Окунев Л.Я. Краткий курс теории чисел. М., I956.

7. Хассе Г. Лекции по теории чисел. М., I953.

8. Боревич З.И. и Шафаревич И.Р. Теория чисел. М., I964.

9. Трост Э. Простые числа. М., I959.

I0. Литвер Е.Л. Теория чисел. Методические указания для студентов-заочников механико-математических и физико-математических факультетов государственных университетов. М., I963.

II. Дэвенпорт Г. Высшая арифметика. Введение в теорию чисел. М., I965.

I2. Кудреватов Г.А. Сборник задач по теории чисел. М., I970.

I3. Грибанов В.У., Титов П.И. Сборник упражнений по теории чисел. М., I964.

I4. Серпинский В. 250 задач по элементарной теории чисел. М., I968.

I5. Александров В.А., Горшенин С.М. Задачник-практикум по теории чисел для студентов заочных отделений физико-математических факультетов педагогических институтов. М., I963.

AINEREGISTER

SISUKORD

Л. Кивистик, Я.Габович
ТЕОРИЯ ЧИСЕЛ
Второе, переработанное издание
На эстонском языке
Тартуский государственный университет
ЭССР, г. Тарту, ул. Юликооли, 18.

Vastutav toimetaja E. Tamme
Korrektor L. Uba

Paljundamisele antud 18.01.74.Trükipaber nr.2. 30x42. 1/4. Trükipoognaid 20.Tingtrükipoognaid 18,6. Arvestuspoognaid 12,44 Trükiarv 600.
MB 00167. Tell. nr. 110.

Hind 43 kop.

TRÜ rotaprint 1974. ENSV, Tartu, Pälsoni tn.14.

43 kop.