TARTU RIIKLIK ÜLIKOOL

JAKOB GABOVITŠ, LEMBIT KIVISTIK

ARVUTEOORIA

TARTU 1968

Tagastage raamat õigeaegselt!
Возвратите книгу вовремя!
121080

A-29535

TARTU RIIKLIK ÜLIKOOL
Arvutusmatemaatika kateeder

Jakob Gabovitš, Lembit Kivistik

A R V U T E O O R I A

N
121080

Tartu 1968

Venekeelne tõlge:

Я.Габович, Л.Кивистик. Теория чисел.

N

Tartu Riikliku Ülikooli
Raamatukogu
121080

TARTU ÜLIKOOLI
RAAMATUKOGU

Якоб Габович, Лембит Кивистик

ТЕОРИЯ ЧИСЕЛ

На эстонском языке

Тартуский государственный университет
ЭССР, г.Тарту, ул. Юликооли, 18

Vastutav toimetaja E. Tamme
Korrektor A. Norberg

==========

TRÜ rotaprint 1968. Paljundamisele antud 17. IX 1968.
Trükipoognaid 14,25. Tingtrükipoognaid 12,97. Arvestus-
poognaid 12,5. Trükiarv 600. Paber 30 x 42. 1/4.
MB 06734. Tell. nr. 583.

Hind 35 kop.

S I S U K O R D.

SISSEJUHATUS 7

I. TÄISARVUDE JAGUVUS 12

§ 1. Jagaja mõiste ja jaguvuse lihtsamad omadused 12

§ 2. Suurim ühistegur. Eukleidese algoritm. 15

Ülesandeid 19

§ 3. Vähim ühiskordne 19

Ülesandeid 22

§ 4. Algarvud 22

1. Naturaalarvude vähim ühest erinev jagaja 22

2. Algarvude hulga lõpmatus. Algarvude tabelid 24

3. Erikujulisi algarve 27

4. Algarvud aritmeetilistes jadades. . 32

§ 5. Arvu lahutamine algteguriteks. 34

Ülesandeid 38

II. AHELMURRUD 39

§ 1. Lõplikud ahelmurrud 39

Ülesandeid 47

§ 2. Kahe tundmatuga lineaarne diofantiline võrrand. 48

Ülesandeid 52

§ 3. Lõpmatud ahelmurrud 53

1. Irratsionaalarvu arendamine ahelmurruks 53

2. Reaalarvu parimad ratsionaalsed lahendid. 59

Ülesandeid 67

§ 4. Reaalsed ruutirratsionaalid 68

1. Ruutirratsionaal ja perioodiline ahelmurd 68
2. Puhtperioodilised ahelmurrud . . . 73
3. Pelli võrrand 77

Ülesandeid. 81

III. ARVUTEOREETILISED FUNKTSIOONID 82

§ 1. Arvu jagajate summa ja jagajate arv 82

1. Multiplikatiivsed funktsioonid . . 82
2. Summad üle arvu jagajate 83
3. Täiuslikud arvud 85

Ülesandeid 87

§ 2. Arvu täisosa 88

Ülesandeid 91

§ 3. Euleri φ-funktsioon. 92

Ülesandeid. 96

§ 4. Möbiuse funktsioon $\mu(a)$. 97

Ülesandeid. 98

§ 5. Algarvude jaotumine naturaalarvude jadas. Funktsioon $\pi(x)$ 99

1. Algarvude jaotusfunktsioon 99
2. Funktsiooni $\pi(x)$ hinnang ja asümptootilised avaldised 101
3. Euleri tõestus algarvude hulga lõpmatuse kohta. Euleri valem. . . 108
4. Algarvude pöördväärtuste rea hajuvus 111

IV. KONGRUENTSID 113

§ 1. Kongruentside omadused 113

1. Kongruentsi definitsioon 113
2. Omadused, mis ei ole seotud mooduli muutumisega 114

3. Mooduli muutumisega seotud omadused 117
4. Rakendusi 119
Ülesandeid 122

§ 2. Jääkide süsteemid. 122

1. Jäägiklassid 122
2. Täielik jääkide süsteem 125
3. Taandatud jääkide süsteem 126
4. Euleri ja Fermat' teoreemid 127
Ülesandeid 129

§ 3. Tundmatut sisaldavad kongruentsid. . . 129
Ülesandeid 133
§4. Lineaarkongruentsid 134
1. Juhtum, kus x kordaja ja moodul on ühistegurita 134
2. Juhtum, kus x kordaja ja moodul on ühisteguriga 137
Ülesandeid 138

§ 5. Lineaarkongruentside süsteemid 139
Ülesandeid 144

§ 6. Kõrgema astme kongruentsid 144

1. Kongruentsid algarvulise mooduli järgi 144
2. Kongruentsid kordarvulise mooduli järgi 150
3. Kongruents algarvu astme järgi. . . 152
Ülesandeid 156

§ 7. Ruutkongruentsid 156

1. Üldised teoreemid 156
2. Legendre'i sümbol 162
3. Tarvilik ja piisav tingimus selleks, et arv -1 oleks ruutjääk. . . 164
4. Gaussi lemma 165
5. Tarvilik ja piisav tingimus selleks, et arv 2 oleks ruutjääk 167

6. Legendre'i sümboli pööratavus . . . 169
7. Jacobi sümbol 173
8. Ruutkongruentside lahendamine . . . 177
9. Ruutkongruentsid kordarvulise mooduli järgi 180
Ülesandeid 187

V. ALGJUURED JA INDEKSID 189

§ 1. Algjuured 189

1. Algjuur ja astendaja, millele antud arv kuulub. 189
2. Algjuurte olemasolu ja arv algarvulise mooduli korral 195
3. Algjuured moodulite p^{α} ja $2p^{\alpha}$ järgi 198
4. Algjuured mooduli 2^{α} ja mistahes kordarvulise mooduli järgi. 201
Ülesandeid 203

§ 2. Indeksid 204

1. Indeksi definitsioon 204
2. Indeksite omadusi 208
3. Indeksite rakendamine kaheliikmeliste kongruentside lahendamisel. . 210
Ülesandeid 216

ÜLESANNETE VASTUSED 217

INDEKSITE TABELID 220

ALGARVUDE JA NENDE VÄHIMATE ALGJUURTE TABEL. . 226

KIRJANDUS 228

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

Käesolev arvuteooria konspekt on määratud esmajoones TRÜ Matemaatikateaduskonna üliõpilastele. Olles seotud ametliku programmi nõuetega olid autorid sunnitud välja jätma suure osa kaasaja arvuteooria ainestikust. Seepärast anname siin põgusa ülevaate arvuteooria sisut, probleemidest ja meetoditest.

Arvuteooria tekkis aritmeetika edasiarenemise tulemusena ja tema aineks oli esialgu naturaalarvude spetsiifiliste omaduste uurimine. Käesoleval ajal haarab arvuteooria märksa laiema probleemide hulga. Arvuteoorias vaadeldakse 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. <u>Määramatute ehk diofantiliste võrrandite lahendamine</u>. Diofantilisteks (kreeka matemaatiku Diophantose nime järgi, kes elas III saj.) nimetatakse ratsionaalarvuliste kordajatega algebralisi võrrandeid ja nende süsteeme, kus tundmatute arv on suurem võrrandite arvust. Selliste võrrandite lahendamise all mõistetakse kõigi täisarvuliste või ratsionaalarvuliste lahendite leidmist.

Diofantilise võrrandi lahendamisele viib kasvõi järgmine lihtsalt sõnastatav ülesanne: Osteti kaht liiki tükikaupa, millest esimese ühik maksis a rbl. ja teise ühik b rbl. Kokku maksti kauba eest c rbl. Kui palju osteti kumbagi kaupa? Kui esimest liiki kaupa osteti x ühikut ja teist liiki kaupa y ühikut, siis ülesande lahendiks on võrrandi

$$ax + by = c$$

mittenegatiivsed täisarvulised lahendid.

Saadud võrrand kuulub nn. lineaarsete diofantiliste võrrandite hulka, mille lahenduvuse küsimust on ammendavalt uuritud. Ka teist järku diofantiliste võrrandite teooria on põhjalikult välja töötatud. Näitena võime tuua nn. Pythagorase võrrandi $x^2 + y^2 = z^2$, mille kõik naturaalarvulised lahendid on antud valemitega $x = k(m^2 - n^2)$, $y = 2kmn$, $z = k(m^2 + n^2)$, kus k, m, n on suvalised naturaalarvud, nii et $m > n$ ja üks arvudest m, n on paaritu.

Kõrgemat järku diofantiliste võrrandite lahendamiseks puudub 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 lahendamata kuulus Fermat' probleem võrrandi $x^n + y^n = z^n$ $(n \geqslant 3)$ lahenduvuse kohta jne.

2. <u>Diofantiline lähendamine</u>. 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. saj. on seotud arvude e ja π transtsendentsuse tõestamisega. 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. [4]).

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 arendas 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, reateooria, tõenäosusteooria jt. matemaatika harude vahendeid. Arvuteooria selle haru loojaks on L.Euler (1707-1783). Suurt mõju analüütilise arvuteooria arengule avaldasid C.F.Gaussi tööd.

Reaalarvude piirkonnas arendasid analüütilisi meetodeid saksa matemaatik L.Dirichlet (1805-1859) ja vene matemaatik 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 matemaatikut 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 (sünd. 1906) ja J.V.Linnik (sünd. 1915).

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 konspektis leiab vastavalt programmile käsitlemist peamiselt elementaarne arvuteooria. Teatud 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. Me ei esita siin naturaalarvude aksiomaatilist definitsiooni, kuid 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.

Arhimedese 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 kirjutame $a \vdots b$, ehk b on a jagaja ja märgime $b|a$. Siinjuures nimetame arvu b ka arvu a teguriks ja arvu a arvu b kordseks. Asjaolu, et d ei ole a jagaja, märgitakse sageli nii: $d \nmid a$. Täisarvude jaguvusel on järgmised, definitsioonist lihtsalt järelduvad omadused, mil-

le kontrollimise jätame enamasti lugejale.*

Teoreem 1.1.

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

2° $0 \vdots a$ iga a korral.

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

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

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

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

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

1) $0 \leqslant r < |b|$ 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,... Arhimedese aksioomi kohaselt leidub naturaalarv k, nii et $kb > a$. Järeli-

---

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

kult leidub selline naturaalarv q, et

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

Tähistame $a - qb = r$; siis $r \geqslant 0$. 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 eelneva tõttu $-a = q_1 b + r_1$, $0 \leqslant r_1 < b$; 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 $a = (-b)q + r$, $0 \leqslant r < |b|$, ehk $a = (-q)b + r$.

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

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

kus $0 \leqslant r < |b|$ ja $0 \leqslant r_1 < |b|$. 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 $q_1 = q$.

§ 2. SUURIM ÜHISTEGUR. EUKLEIDESE ALGORITM.

Vaatleme vaid positiivseid arve ja nende positiivseid tegureid.

Arvude $a_1, a_2, \ldots, a_n$ ühisteguriks nimetatakse 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 suurem 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 iga b tegur 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 ühiste-

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

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

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

$$b > r_1 > r_2 > r_3 > \ldots > 0$$

ja seega ei saa jadas $b, r_1, r_2 \ldots$ olla rohkem kui b elementi. Võrdustest (1) järeldub teoreemi 1.6 tõttu, et

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

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

Teoreem 1.7. Arvude a ja b ühistegurite hulk ühtib Eukleidese 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. $(am,bm) = (a,b)m$.

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. Olgu k arvude a ja b mingi ühistegur. Siis

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

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

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

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

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

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

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

Tõepoolest, eelmise teoreemi põhjal $(ac,b) = (c,b)$. Et aga $ac\vdots b$, siis teoreemi 1.5 kohaselt $(ac,b) = b$ ja seega ka

$(c,b) = b$, s.t. c on b kordne.

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

$$(a_1a_2\ldots a_m,\ b_1b_2\ldots b_n) = 1.$$

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

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

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 $a_1,a_2,\ldots,a_n$ ühistegurite hulk ühtib d_{n-1} tegurite hulgaga. Nende hulkade suurimad elemendid on sealjuures võrdsed:

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

Ülesandeid.

Leida arvude järgmised suurimad ühistegurid:

1. (6188, 4709).
2. (81 719, 52 003).
3. (81 719, 52 003, 33 649).
4. (42 914, 66 397).

§ 3. VÄHIM ÜHISKORDNE.

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

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

On selge, et $0 < m \leqslant a_1 a_2 \ldots a_n$.

Teoreem 1.15. Arvude iga ühiskordne jagub vähima ühiskordsega.

Tõestus. Olgu M arvude $a_1, a_2, \ldots, a_n$ mingi ühiskordne. Siis teoreemi 1.4 kohaselt

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

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. Kahe arvu suurima ühisteguri ja vähima ühiskordse korrutis võrdub nende arvude eneste korrutisega, s.t.

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

Tõestus. Tähistame lühidalt $[a,b] = m$. Teoreemi 1.15 kohaselt $ab \vdots m$, s.o. $ab = qm$, kus q on täisarv. Siit

$$\frac{a}{q} = \frac{m}{b}, \quad \frac{b}{q} = \frac{m}{a}.$$

Võrduste paremad, seega aga ka vasakud pooled on täisarvud. Järelikult on q arvude a ja b ühistegur. Näitame, et $q = (a,b)$. Selleks tõestame, et q jagub arvude a ja b iga teise ühisteguriga (vt. järeldus teoreemist 1.7).

Olgu q_1 arvude a ja b mingi ühistegur. Siis

$$\frac{ab}{q_1} = a \cdot \frac{b}{q_1} = b \cdot \frac{a}{q_1},$$

mis näitab, et $M = \frac{ab}{q_1}$ on arvude a ja b mingi ühiskordne. Teoreemi 1.15 põhjal $M \vdots m$, s.t.

$$\frac{M}{m} = \frac{ab}{q_1} : \frac{ab}{q} = \frac{q}{q_1}$$

on täisarv. Seega q jagub arvuga q_1 ja järelikult on q arvude a ja b suurim ühistegur

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

Nüüd saame

$$\frac{ab}{m} = (a,b) \quad \text{ehk} \quad ab = (a,b)\cdot[a,b].$$

Järeldus. Arvud a ja b on ühistegurita parajasti siis, kui $[a,b] = ab$.

Tõepoolest, tarvitseb eelmises teoreemis võtta $(a,b) = 1$.

Märgime, et teoreem 1.16 ei laiene rohkem kui kahele arvule. Näiteks

$$(6,4,9)\cdot[6,4,9] = 1\cdot 36 < 6\cdot 4\cdot 9.$$

Teoreem 1.16 võimaldab leida kahe arvu vähimat ühiskordset

$$[a,b] = \frac{a}{(a,b)} \cdot b = a \cdot \frac{b}{(a,b)}.$$

Et Eukleidese algoritmi abil on leitav iga kahe arvu suurim ühistegur, siis on viimase seose tõttu leitav ka iga kahe arvu vähim ühiskordne.

Teoreem 1.17. 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.

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

Teoreem 1.18. Paarikaupa ühisjagajata arvude vähim

ühiskordne võrdub nende arvude korrutisega, s.t. kui

$$(a_i, a_j) = 1, \quad i,j=1,2,\ldots,n; \quad i \neq j,$$

siis

$$[a_1, a_3, \ldots, a_n] = a_1 a_2 \ldots a_n.$$

Tõestus. Kui n = 2, siis järeldub tõestus teoreemist 1.16. Üldjuhul

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

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

Tõepoolest, c on arvude $a_1, \ldots, a_n$ ühiskordne. Seega jagub ta vähima ühiskordsega $a_1 a_2 \ldots a_n$.

Ülesandeid.

Leida arvude järgmised vähimad ühiskordsed:

5. [10 001, 8103].

6. [8407, 21 111].

§ 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 eri-

nevat 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 $a \vdots b$. 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 $(1 < b \leqslant a)$,

$$a = bc.$$

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

$$b > p.$$

Korrutame võrratust arvuga $a = pb$. Saame

$$ab > p^2 b,$$

millest

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

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 $\sqrt{337} = 18,\ldots$, ja seejärel kontrollime, kas 337 jagub algarvudega 2,3,5,7,11,13,17. Osutub, et ei jagu. Järelikult on 337 algarv.

2. Algarvude hulga lõpmatus. Algarvude tabelid.

Teoreem 1.21. 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:

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

Moodustame naturaalarvu

$$a = p_1 p_2 \ldots p_n + 1. \tag{1}$$

On kaks teineteist välistavat võimalust: 1) a on algarv, 2) a on kordarv.

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. Seega

$$a \vdots p_i ,$$

kus i on mingi naturaalarv lõplikust jadast 1,2,...,n. Et võrduse (1) vasak pool ja esimene liidetav paremal pool 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 oletu-

sest, et algarve on lõplik hulk. Teoreem on tõestatud.

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 hiljuti trükist venekeelse väljaandena (Д.Н.Лемер. Таблицы простых чисел от 1 до 10 006 721, Москва, 1967). 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 tänaseni Eratosthenese poolt III sajandil e.m.a. väljatöötatud lihtsat meetodit 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:

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

Esimene arv 2 jagub ainult arvuga 1 ja iseendaga. Järelikult on 2 algarv. Kriipsutame jadas (2) 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 vahemikus 1 kuni N.

Märgime, et kui on juba läbi kriipsutatud kõik algarvust p väisemate 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 $q \leq \sqrt{a} < p$ 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. <u>Erikujulisi algarve.</u> Peale suurte algarvude, mida võib leida koostatud algarvude tabelitest, on teada veel mõningaid erikujulisi algarve, mis asuvad kaugel väljas-

pool 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, on viimasel ajal hakatud Mersenne'i arvude hulgast algarve otsima elektronarvutite abil. Suurim teadaolev algarv on $2^{11\,213} - 1$, mis kümnendsüsteemis kirjapandult koosneb 3376-st numbrist (numbrite

arvu saab lihtsalt leida kümnendlogaritmide abil:

$\log 2^{11\,213} = 11\,213 \cdot \log 2 = 11\,213 \cdot 0{,}30103 = 3375{,}4$). Praegu on üldse teada 23 Mersenne'i algarvu. Need saadakse n väärtustel 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11 213. Ülejäänud n väärtustel kuni 12 000 on kõik Mersenne'i arvud kordarvud.

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

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

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:

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

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 arvud 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 $n = 2^k p_1 p_2 \cdots p_n$, kus $p_1, p_2, \ldots, p_n$ on 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 täisarvulise n korral alati algarvud. Euler tõestas, et sellist polünoomi ei leidu. Nimelt kehtib järgmine teoreem.

Teoreem 1.28. Ühegi täisarvuliste kordajatega 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 $n = c$ puhul olgu $f(c)$ 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

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

mis nagu lubaks p_n arvutada, kuid α täpne väärtus pole teada. On teada selle reaalarvu (arvatavsti irratsionaalarvu) mõned esimesed kohad (vt. [4], lk. 193). On teada ka teisi analoogilisi valemeid, kuid need on sama laadi puudustega.

4. <u>Algarvud aritmeetilistes jadades</u>. 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 väitevastaselt, et algarve kujuga $4n-1$ on lõplik hulk. Olgu need

$$p_1, p_2, \ldots, p_k. \tag{2}$$

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

$$4p_1p_2\ldots p_k - 1 = q_1q_2\ldots q_m . \tag{3}$$

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 (3) parem pool vähemalt ühega algarvudest (2). 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. Analoogiliselt 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 suuruse n kordaja ja vabaliige ühisteguriga, sest need osajadad võivad sisaldada ülimalt üht algarvu.

Dirichlet' poolt on 1837.a. tõestatud järgmine teoreem.

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

Teoreemi tõestus on komplitseeritud, seda me siin ei esita.

§ 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 ei kehti, kui jagaja on kordarv.

Teoreem 1.33. Iga naturaalarvu, mis on ühest suurem,

saab lahutada algarvude korrutiseks parajasti ühel viisil (teguriteks lahutusi, mis erinevad vaid tegurite järjekorra poolest, loetakse identseteks).

Tõestus. 1) Tõestame algul, et leidub vähemalt üks arvu a 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 $p_1, p_2, \ldots, p_k$ 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 $p_1p_2 \cdots p_k$. 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.

Peale põhiteoreemi tõestust võime kirjutada

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

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 vähimad algtegurid kõikide naturaalarvude jaoks, mis ei ületa 10 miljonit ning ei jagu ühegagi algarvudest 2, 3, 5 ja 7 (viimaste tegurite leidmi-

ne on ka ilma tabelita lihtne). Märgime, et õpiku [6] lõpus on esitatud analoogiline tabel kõikide 10 000-st väiksemate arvude jaoks.

Teoreem 1.34. Olgu naturaalarvu a 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 $d|a$ ja $p|d$, kus p on algarv. Siis teoreemi 1.1 põhjal $p|a$. 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 viimases seoses a ja d nende kanooniliste teguriteks lahutustega (1) ja (2):

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

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 algarvu p_i, teine sisaldab. Põhiteoreemi põhjal pole see võimalik. Seega $\beta_i \leq \alpha_i$.

Piisavus. Olgu arv d antud korrutisena (2). Näitame,

et a:d. Selleks leiame jagatise

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

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 $\tau(a)$:

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

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

Teoreemi järeldusena võib tuletada ka juba koolikursusest tuntud reeglid arvude suurima ühisteguri ja vähima ühiskordse arvutamiseks. Nendel me aga ei peatu.

Ülesandeid.

7. Leida arvu 81 057 226 000 kanooniline kuju ja jagajate arv.

8. Leida arvu 968 kõik jagajad.

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

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

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

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

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$

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

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

Järk-järgulisel 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 $\frac{a}{b}$ <u>ahelmurruks</u>. See-

juures $a_1, a_2, \ldots, a_n$ 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 $a_n > 1$. Seega saame Eukleidese algoritmi abil iga ratsionaalarvu $\frac{a}{b}$ arendada lõplikuks ahelmurruks.

Ahelmurdu (1) tähistatakse sageli ka kompaktsemalt:

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

või

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

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

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

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

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

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 eletusega, et $a_k \neq a_k'$. Seega $a_1 = a_1', \ldots, a_n = a_n'$. Kirjutades välja võrduse (3) $k = n$ korral, saame

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

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,...,n-1) võivad ka ühega võrduda. Mõnikord osutub kasulikuks ahelmurd, kus ka 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 $a_i \geq 1$, i = 2,3,...,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

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

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

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

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} = 1 + \frac{1}{2} + \frac{4}{13} = 1 + \frac{13}{40} = \frac{53}{40}.$$

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

Ahelmurru (1) lähismurdudeks 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 väärtusi. Tähistame i-ndat lähismurdu $\frac{P_i}{Q_i}$. Seega

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

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

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

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

$$P_k = P_{k-1}a_k + P_{k-2} ,$$
$$Q_k = Q_{k-1}a_k + Q_{k-2} \quad (k \geq 3).$$

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

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

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

Seega

$$P_{k+1} = P_k a_{k+1} + P_{k-1},$$

(4)

$$Q_{k+1} = Q_k a_{k+1} + Q_{k-1},$$

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

<u>Näide 1.</u> 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 $\frac{P_1}{Q_1} = 0, \quad \frac{P_2}{Q_2} = 1, \quad \frac{P_3}{Q_3} = \frac{8}{9}, \quad \frac{P_4}{Q_4} = \frac{9}{10},$

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

Näitame, et kahe järjestikuse lähismurru lugejate ja nimetajate vahel kehtib seos

(5) $$P_k Q_{k-1} - P_{k-1} Q_k = (-1)^k.$$

Valemi (5) tõestame täieliku induktsiooni meetodil. Kõigepealt veendume, et valem 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.

Siit saame tähtsa järelduse:

Iga ahelmurru mistahes lähismurd on taandumatu.

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.

Ülesandeid.

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

1) paarisarv elemente,

2) paaritu arv elemente.

10. Arendada ahelmurruks 2,3547 ja leida kõik lähismurrud.

11. Leida arv, mille ahelmurruks on

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

12. 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. KAHE TUNDMATUGA LINEAARNE DIOFANTILINE VÕRRAND.

Olgu antud kahe tundmatuga täisarvuliste kordajatega lineaarvõrrand

$$ax + by = c.$$

Sellist võrrandit nimetatakse diofantiliseks võrrandiks, 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 $(a_1, b_1) = 1$. Peale 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 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 peale asendamist võrrandisse ning d-ga läbijagamist saame eel-

nevaga ekvivalentse võrrandi

$$a_1x + b_1y = c_1,$$

kus juba $(a_1,b_1) = 1$. Allpool näeme, et vaadeldaval juhul on võrrand lahenduv, s.t. tingimus $(a,b)|c$ 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

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

P_n ja Q_n vastavalt väärtustega a ja b:

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

Korrutame võrduse mõlemat poolt teguriga $(-1)_nc$. Saame seose

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

Siit näeme, et võrrandit rahuldavad täisarvud

(2) $$x_o = (-1)^ncQ_{n-1}, \quad y_o = (-1)^{n-1}cP_{n-1}.$$

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 (x_0,y_0) võrrandi (1) erilahend (ükskõik, kas äsja leitud lahend või mingi teine), s.t. kehtigu samasus

$$ax_0 + by_0 = c. \tag{3}$$

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

$$ax + by = c. \tag{4}$$

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

$$\begin{aligned} x &= x_0 + bt, \\ y &= y_0 - at \end{aligned} \tag{5}$$

on lahend iga t korral. Tõepoolest,

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

Niisiis on juhul, kui $(a,b) = 1$ 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):

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

TARTU ÜLIKOOLI RAAMATUKOGU

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

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

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

Ülesandeid.

13. Lahendada diofantilised võrrandid

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

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

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

15. Leida võrrandi

$$25x + 18y = 2423$$

positiivsed täisarvulised lahendid.

16. 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. LÕPMATUD AHELMURRUD.

1. Irratsionaalarvu arendamine ahelmurruks. 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

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

Analoogiliselt leiame

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

$$\alpha_4 = a_4 + \frac{1}{\alpha_5}, \quad \text{kus} \quad \alpha_5 > 1 \quad \text{jne.}$$

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 (lõplik on ta ratsionaalarvu korral). Kui katkestame

täisosa väljaeraldamise n-ndal sammul, siis saame ahelmurru

$$(4) \qquad \alpha = a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots + \cfrac{1}{a_n + \cfrac{1}{\alpha_{n+1}}}}}$$

Siin a_1 on täisarv (võib olla ka null või negatiivne), $a_2, a_3, \ldots a_n$ on naturaalarvud, α_{n+1} on ühest suurem irratsionaalarv.

Ahelmurdu, mille elemendid a_k $(k = 2,3,\ldots)$ on naturaalarvud, nimetatakse korrapäraseks. Ahelmurd (4) pole korrapärane, sest α_{n+1} ei ole naturaalarv. Jätkates aga täisosade väljaeraldamise protsessi piiramatult, s.t. lastes $n \to \infty$, saame lõpmatu korrapärase ahelmurru.

$$(5) \qquad a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots + \cfrac{1}{a_n + \ddots}}}$$

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

Enne kui kirjutada, et ahelmurd (5) võrdub α-ga, tuleb defineerida lõpmatu ahelmurru väärtus ja näidata, et antud juhul see väärtus võrdub α-ga. Vaatleme esialgu mistahes lõpmatult ahelmurdu kujul (5), 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

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

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

mida nimetame ahelmurru (5) lähismurdude jadaks. Lõpmatut ahelmurdu (5) nimetatakse koonduvaks, kui eksisteerib lõplik piirväärtus

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

Viimast piirväärtust nimetatakse lõpmatu ahelmurru (5) väärtuseks.

Teoreem 2.2. Iga lõpmatu ahelmurd koondub teatud reaalarvuks.

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

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

Kuna lähismurrud (6) on lõplikud ahelmurrud ja igale ahelmurrule jadas (6) eelnevaid ahelmurde võib lugeda tema lähismurdudeks, siis kehtivad §-s 1 leitud seosed. Eriti on

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

Seega

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

Et $Q_{n+1} = Q_na_{n+1} + Q_{n-1}$ ja $Q_1 = 1$, $Q_2 = a_2 \geq 1$,

$Q_3 \geq Q_2 + Q_1 \geq 2$, $Q_4 \geq Q_3 + Q_2 \geq 3$, $Q_5 \geq Q_4 + Q_3 \geq 5$, 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 (7). 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 2.3. Kui ahelmurd (5) on saadud irratsionaalarvust α täisosade väljaeraldamise protsessi piiramatul jätkamisel (nagu on kirjeldatud käesoleva punkti alguses), siis tema väärtus on α.

Tõestus. Võrreldes lähismurru $\frac{P_n}{Q_n}$ avaldist jadas (6) ja α avaldist (4) näeme, et α saadakse lähismurrust $\frac{P_n}{Q_n}$, kui a_n asendatakse summaga $a_n + \frac{1}{\alpha_{n+1}}$. Et

$$\frac{P_n}{Q_n} = \frac{P_{n-1}\, a_n + P_{n-2}}{Q_{n-1}\, a_n + Q_{n-1}} ,$$

siis

---

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

$$\alpha = \frac{P_{n-1}\left(a_n + \frac{1}{\alpha_{n+1}}\right) + P_{n-2}}{Q_{n-1}\left(a_n + \frac{1}{\alpha_{n+1}}\right) + Q_{n-2}} = \frac{P_n \alpha_{n+1} + P_{n-1}}{Q_n \alpha_{n+1} + Q_{n-1}} .$$

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

$$\lim_{n \to \infty} \left(\frac{P_n}{Q_n} - \alpha \right) = 0$$

ehk

$$\lim_{n \to \infty} \frac{P_n}{Q_n} = \alpha , \tag{9}$$

mida oligi tarvis tõestada.

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

Teoreem 2.4. Kui kaks lõpmatut ahelmurdu kujul (5), 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.

$$a_1 + \frac{1}{a_2} + \frac{1}{a_3} + \ldots = a_1' + \frac{1}{a_2'} + \frac{1}{a_3'} + \ldots , \tag{10}$$

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

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

Tähistame

(11) $\alpha_k = a_k + \frac{1}{a_{k+1}} + \dots$, $\alpha'_k = a'_k + \frac{1}{a'_{k+1}} + \dots$

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

siis

$$\frac{1}{a_{k+1}} + \dots < 1, \quad \frac{1}{a'_{k+1}} + \dots < 1$$

ja seega

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

Kuna iga lõpmatu ahelmurd koondub, siis seoste (11) tõttu on α_k ja α'_k teatud irratsionaalarvud ning võrduse (10) võib kirjutada kujul

(12)
$$a_1 + \frac{1}{a_2} + \dots + \frac{1}{a_{k-1}} + \frac{1}{\alpha_k} =$$
$$= a'_1 + \frac{1}{a'_2} + \dots + \frac{1}{a'_{k-1}} + \frac{1}{\alpha'_k} .$$

Et $a_1 = a'_1$, $\dots$, $a_{k-1} = a'_{k-1}$, siis toimime samuti nagu teoreemi 2.1 tõestamisel: lahutame võrduse (12) pooltest vastavalt võrdsed elemendid a_1, a'_1 ja võrdsustame saadavas võrduses murdude nimetjad (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.

<u>Näide 1.</u> 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 vastavate täisosade võrdsus. 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 järgmises paragrahvis.

Käesoleva punkti 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 ahelmurd on aga järgmine:

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

s.t.

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

Valemite tuletuse arvu e ahelmurru elementide jaoks võib leida näiteks õpikust [2], lk. 221-223. Arvu e ahelmurd on leitud Euleri poolt.

2. <u>Reaalarvu parimad ratsionaalsed lähendid.</u> Nagu järeldub võrdusest (9), võib lähismurdudega arvu α kui tahes hästi lähendada. Järgnevas uurime sellise lähendamise viga, jada $\left\{\frac{P_n}{Q_n}\right\}$ elementide α -le lähenemise iseloomu ja

näitame, et lähismurd on α -le teatud mõttes parimad lähendid. Vaatleme kõigepealt, kuidas toimub lähismurdude jada $\left\{\frac{P_n}{Q_n}\right\}$ elementide lähenemine arvule α. Selleks lähtume teoreemi 2.3 tõestamisel saadud seosest

$$(13) \qquad \alpha - \frac{P_n}{Q_n} = \frac{(-1)^{n+1}}{Q_n(Q_n\alpha_{n+1} + Q_{n-1})} .$$

Võrduse (9) 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

$$(14) \qquad \frac{P_{2k+1}}{Q_{2k+1}} < \alpha < \frac{P_{2m}}{Q_{2m}} .$$

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

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

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

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

Niisiis

$$(15) \qquad \left|\frac{P_{n+1}}{Q_{n+1}} - \alpha\right| < \left|\frac{P_n}{Q_n} - \alpha\right| < \left|\frac{P_{n-1}}{Q_{n-1}} - \alpha\right| .$$

Arvestades võrratusi (14) ja (15) võime kirjutada, et

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

Edasi hindame viga, mis tekib α lähendamisel ratsionaalarvuga $\frac{P_n}{Q_n}$. Valemist (13) saadav täpne hinnang

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

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

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

Seega

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

mistõttu

$$(17) \qquad \left|\frac{P_n}{Q_n} - \alpha\right| < \frac{1}{Q_n Q_{n+1}} .$$

Seos (16) 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

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

Seega

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

Näeme, et vea ülemine ja alumine tõke erinevad suhteliselt vähe. Seepärast annab valem (17) väga täpse hinnangu.

Näide 2. Leiame arvu π mõned esimesed lähismurrud ja hindame nende erinevust arvust π.

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

Valem (17) 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. See on seotud sellega, et ahelmurru järgmine element $a_5 = 292$ on võrdlemisi suur ja selletõttu ka valemis (17) esinev nimetaja Q_5 on võrreldes eelneva nimetajaga $Q_4 = 113$ järsult kasvanud. Märgime, et π ja $\frac{355}{113}$ tegelik erinevus on 0,00000025... ; niisiis valemi (17) abil saadav veahinnang peaaegu ühtib tegeliku veaga.

Märgime, et juba Arhimedes leidis arvu π jaoks lähendi $\frac{22}{7}$; 16. sajandil leidis aga lähendi $\frac{355}{113}$ hollandi matemaatik Adriaen Metius.

Ratsionaalarvu $\frac{a}{b}$ $(b > 0)$ nimetatakse reaalarvu α parimaks lähendiks, kui ei eksisteeri ühtki naturaalarvust b väiksema või temaga võrdse nimetajaga ratsionaalarvu $\frac{x}{y}$, mis erineks α-st vähem kui erineb $\frac{a}{b}$. Seega on $\frac{a}{b}$ reaal-

arvu 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 $(\alpha - \frac{a}{b},\ \alpha + \frac{a}{b})$, kus $\frac{a}{b}$ on α parim lähend, siis kõigi selles vahemikus asuvate ratsionaalmurdude nimetajad on suuremad kui b. Tõestame teoreemi.

Teoreem 2.5. 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

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

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 vahepealsed murrud osutuvad ahelmurruks arendatud reaalarvu parimateks lähenditeks (vt. [2, 6]).

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 hammasrataste 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 mehhaanik, füüsik ja matemaatik C.Huygens (1629-1695) päikesesüsteemi mudeli konstrueerimisel, kui oli tarvis realiseerida planeetide tiirlemisperioodide te-

gelikke suhteid hammasratasülekannete abil. Huygens kasutaski nimetatud suhetele sobivate parimate lähendite saamiseks ahelmurdude lähismurde.

Näide 3. Leida irratsionaalarvu $\sqrt{2} = 1{,}4142\ldots$ parim ratsionaalne lähend, mille nimetaja ei ületa 100.

Arvu $\sqrt{2}$ esitusest kümnendmurruna võib saada lihtsalt lähendi nimetajaga 100, s.o. ratsionaalmurru $\frac{141}{100}$, mille viga on 0,0042. Võrdleme seda lähendit ahelmurrust

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

saadavate parimate lähenditega. Leiame lähismurrud.

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

Sajast väiksema nimetajaga parim lähend on $\frac{P_6}{Q_6} = \frac{99}{70}$. Selle lähendi viga

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

Niisiis on ratsionaalarv $\frac{99}{70}$ reaalarvule $\sqrt{2}$ märksa paremaks lähendiks kui $\frac{141}{100}$. Lihtne on kontrollida, et isegi lähismurrud $\frac{41}{29}$ ja $\frac{17}{12}$ erinevad $\sqrt{2}$-st vähem kui erineb $\frac{141}{100}$.

Järgmine teoreem näitab, et ratsionaalmurd, mis teatud mõttes küllalt hästi aproksimeerib reaalarvu, ühtib tingimata selle reaalarvu ahelmurru ühe lähismurruga.

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 arvu 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

$$\omega = \frac{P_{k-1} - \alpha Q_{k-1}}{\alpha Q_k - P_k}. \tag{18}$$

Siis

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

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

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 ahelmurdu, mille väärtus on mingi reaalarv β. Arvu β võib esitada mittekorrapärase lõpliku ahelmurruna

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

mistõttu valemi (7) kohaselt

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

Asendades siia ω avaldise (18), saame, et $\beta = \alpha$.
Seega on

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

reaalarvu α lähismurd.

Ülesandeid.

17. Arendada ahelmurruks a) $\sqrt{3}$, b) $\sqrt{13}$, c) $\sqrt{37}$,
d) $\frac{\sqrt{5}+2}{3}$, e) $\frac{\sqrt{13}-7}{6}$.

18. Kasutades 1. punkti lõpul esitatud ahelmurdu, leida arvu e parim ratsionaalne lähend, mille nimetaja ei ületa 100. Hinnata lähendi täpsust.

19. Teoreemi 2.6. abil kontrollida, kas $\frac{38}{17}$ on $\sqrt{5}$ ahelmurru üks lähismurdudest.

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

§ 4. REAALSED RUUTIRRATSIONAALID.

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

(1) $$\frac{A + \sqrt{D}}{B},$$

kus A, B, D on täisarvud, $D>0$ ja D ei ole täisruut. Ruutirratsionaaliga (1) 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 puhtperioodiliseks, 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 2.7. Reaalarv α, mis annab arendamisel perioodilise ahelmurru, on ruutirratsionaal.

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

$$\alpha = a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_{i-1} + \cfrac{1}{\alpha_i}}} = \frac{P_i'}{Q_i'} = \frac{P_{i-1}\alpha_i + P_{i-2}}{Q_{i-1}\alpha_i + Q_{i-2}}$$

$$\alpha = a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_{i+k-1} + \cfrac{1}{\alpha_i}}} = \frac{P_{i+k}'}{Q_{i+k}'} = \frac{P_{i+k-1}\alpha_i + P_{i+k-2}}{Q_{i+k-1}\alpha_i + Q_{i+k-2}}$$

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 ruut-

võrrandit

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

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

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

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

Siit

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

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

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

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

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

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 2.8. (Lagrange). Iga ruutirratsionaal avaldub perioodilise ahelmurruna.

Tõestus (vt. [10]). Olgu α ruutirratsionaal, s.t. täisarvuliste kordajatega ruutvõrrandi irratsionaalne lahend. Nimetatud võrrandiks olgu

(1) $$b_1x^2 - 2c_1x + d_1 = 0,$$

kus ka c_1 on täisarv (alati võib saavutada, et x kordaja on paarisarv, tarvitseb vaid võrrandit 2-ga läbi korrutada). Leiame võrrandi järjestikuste α_i-de jaoks. Kõigepealt

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

mistõttu võime võrrandi (1) esitada kujul

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

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

(3) $$b_2x^2 - 2c_2x + d_2 = 0,$$

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

(4) $$b_2 = b_1a_1^2 - 2c_1a_1 + d_1,$$
$$c_2 = c_1 - b_1a_1,$$
$$d_2 = b_1.$$

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

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

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+d}, 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 $D_{i+1} = D_i = \dots = D_1 = c_1^2 - b_1 d_1 = D$.

Vaatleme lõpmatut kordajate jada

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

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 $d_{k+1} = b_k$. Teiselt poolt näitab valem (7), et siis

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

sest $a_i > 0$. Et kõik c_i on täisarvud, siis teatud kohast alates on kõik c_i negetiivsed. 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 tõsiasjaga, 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 ükski $b_i \neq 0$. 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) $$b_{m+1}x^2 - 2c_{m+1} + b_m = 0.$$

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, sest $\frac{b_m}{b_{m+1}} < 0$. Positiivseks lahendiks on α_{m+1}. 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

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

ja

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

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 2.9. Ruutirratsionaali

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

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

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

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

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

$$f(0) = -P_{k-2} < 0, \quad f(-1) = (Q_{k-1} - Q_{k-2}) +$$

$$+ (P_{k-1} - P_{k-2}) > 0,$$

millest nähtub, et polünoomi teine juur $\bar{\alpha} = \frac{A - \sqrt{D}}{B}$ rahuldab võrratust $-1 < \bar{\alpha} < 0$.

Piisavus. Olgu $\alpha = \frac{A + \sqrt{D}}{B} > 1$ ja $-1 < \bar{\alpha} = \frac{A - \sqrt{D}}{B} < 0$. Nagu nähtus teoreemi 2.8. 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 $\bar{\alpha}_1 = \bar{\alpha}$. 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

$$\bar{\alpha}_n = a_n + \frac{1}{\bar{\alpha}_{n+1}} \qquad \text{(Tõestada!)}.$$

Siit

$$\bar{\alpha}_{n+1} = \frac{1}{\bar{\alpha}_n - a_n}.$$

Et $a_n \geqslant 1$ ja $-1 < \bar{\alpha}_n < 0$, siis saamegi, et $-1 < \bar{\alpha}_{n+1} < 0$. 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 $a_{i-1} = \left[-\frac{1}{\bar{\alpha}_i}\right]$. 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 $\bar{\alpha}_{i+k} = \bar{\alpha}_i$, siis $a_{i+k-1} = a_{i-1}$. Et võrduste

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

paremad pooled on võrdsed, siis on $\bar{\alpha}_{i+k-1} = \bar{\alpha}_{i-1}$ 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 $\bar{\alpha} = \frac{2-\sqrt{7}}{3}$ asub vahemikus $(-1,0)$. Ahelmurruks arendamisel saamegi

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

Teoreem 2.10. Olgu D mitteruutarv ja $\sqrt{D} > B > 0$. Siis ruutirratsionaali $\frac{\sqrt{D}}{B}$ ahelmurd on järgmine

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

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 $\bar{\alpha} =$

$= a_1 - \frac{\sqrt{D}}{B}$ 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. [11], lk. 336).

3. Pelli võrrand. Vaatleme diofantilise võrrandi

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

lahendamist. Euler nimetas seda võrrandit (13) mingi arusaamatuse tõttu J.Pelli (1610–1685) nime järgi Pelli võrrandiks. See nimetus kandus Euleri töödest edasi ja on kirjanduses kasutusel senini. On selgunud, 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. Pelli võrranditel on tähtis koht kogu diofantiliste võrrandite teoorias.

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 (x_0, y_0). Märgime veel, et x_0, y_0 on seose

(14) $$x_0^2 - Dy_0^2 = 1$$

tõttu ühistegurita. Kirjutame samasuse (14) kujul

$$(x_0 - y_0\sqrt{D})(x_0 + y_0\sqrt{D}) = 1$$

ehk

$$\frac{x_0}{y_0} - \sqrt{D} = \frac{1}{y_0^2\left(\frac{x_0}{y_0} + \sqrt{D}\right)} .$$

Kuna siit järeldub, et $\frac{x_0}{y_0} > \sqrt{D} > 1$, siis

$$\frac{x_0}{y_0} + \sqrt{D} > 2\sqrt{D} > 2 .$$

Viimast võrratust arvestades saame, et

$$0 < \frac{x_0}{y_0} - \sqrt{D} < \frac{1}{2y_0^2} .$$

Teoreemi 2.6. kohaselt peab siis $\frac{x_0}{y_0}$ olema ruutirratsionaali $\sqrt{D}$ ahelmurru üks lähismurdudest $\frac{P_n}{Q_n}$, kusjuures $x_0 = P_n$, $y_0 = Q_n$. Et $\frac{x_0}{y_0} > \sqrt{D}$, siis indeks n peab olema paarisarv. Niisiis tuleb Pelli võrrandi kõiki lahendeid otsida vaid $\sqrt{D}$ ahelmurru paariarvulise indeksiga lähismurdude lugejate ja (vastavate) nimetajate hulgast.

Edasi uurime, millised lähismurrud võivad anda võr-

randi lahendi ja teeme kindlaks, kas Pelli võrrand on lahenduv iga D korral.

Avaldame $\sqrt{D}$ P_n ja Q_n kaudu:

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

Siit

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

ehk arvestades, et n on paarisarv,

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

kus $b = Q_{n-1}Q_n D - P_{n-1}P_n$ on täisarv. Murru nimetaja $P_n^2 - DQ_n^2$ võrdub võrrandi (13) vasaku poolega, kus $x = P_n$, $y = Q_n$. Täisarvude paar (P_n, Q_n) on seega võrrandi (13) lahendiks parajasti siis, kui

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

Et seose (15) tõttu

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

siis

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

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

millest

$$\sqrt{D} = [a_1, a_2, \ldots, a_n, b+a_1, a_2, \ldots, a_n, b+a_1, \ldots] = \tag{16}$$

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

Niisiis (P_n, Q_n) on võrrandi (13) lahend parajasti siis, kui $\sqrt{D}$ avaldub perioodilise ahelmurruna kujul (16), kus perioodi pikkus n on paarisarv. Kujul (16) avaldub aga teo-

reemi 2.10. 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 (16), 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. $(3,2)$, $(17,12)$, $(99,70)$,... .

Ülesandeid.

21. Leida ruutirratsionaal, mille ahelmurruks on $[(1)]$.

22. Leida ruutirratsionaal, mille ahelmurd on $[-1, (1,2)]$.

23. Kasutades teoreemi 2.9. teha kindlaks, kas järgmiste ruutirratsionaalide ahelmurrud on puhtperioodilised või mitte:

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

24. 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) $\frac{-4+\sqrt{7}}{3}$.

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

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

25. Lahendada järgmised Pelli võrrandid:

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

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

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

III. ARVUTEOREETILISED FUNKTSIOONID.

Arvuteoorias vaadeldakse enamasti funktsioone, mille määramispiirkonnaks on naturaalarvude hulk või mille väärtused on täisarvud.

§ 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 ühistegurita 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.

Milline on nõrga ja tugeva multiplikatiivsuse vahe-

kord?

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 $0 \leqslant \beta_i \leqslant \alpha_i$. Tähistame sümboliga $\sum_{d|a}$ summat üle kõigi arvu a jagajate d.

Teoreem 3.1. 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 $0 \leqslant \beta_i \leqslant \alpha_i$. Siinjuures saame parajasti kõik vasakul esinevad liidetavad, sest koondumisi ei esine. 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 3.2. 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

$$S(a)S(b) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdots \frac{p_n^{\alpha_n+1} - 1}{p_n - 1} \cdot \frac{q_1^{\beta_1+1} - 1}{q_1 - 1} \cdots$$

$$\cdots \frac{q_m^{\beta_m+1} - 1}{q_m - 1} = S(ab),$$

$$\tau(a) \cdot \tau(b) = (\alpha_1+1) \ldots (\alpha_n+1)(\beta_1+1) \ldots (\beta_m+1) = \tau(ab).$$

Kui nüüd $(a,b) > 1$, siis a ja b kanoonilises kujus laidub vähemalt üks ühine tegur. Olgu näiteks $p_i = q_j$. Siis aga $S(a)S(b) \neq S(ab)$, $\tau(a) \cdot \tau(b) \neq \tau(ab)$, 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 paariarvud. 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 3.3. **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 kõikide b jagajate summa, paremal aga kahe b 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 varem mainitud, on praegu teada 23 Mersenne'i algarvu. Seega on ühtlasi teada 23 täiuslikku arvu, millest esimesed on 6, 28, 496, 8128, suurim teadaolev aga $2^{11212}(2^{11213} - 1)$. 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^{5279}. Sealjuures on nad siis kujuga $p^{4k+1}N^2$, kus $p = 4m + 1$ on algarv, $(N,p) = 1$, ja nende erinevate algtegurite arv ei ole väik-

sem kui 2800 (vt. [4],lk.188).

Täiuslikest arvudest võib lugeda ka J.Gabovitši artiklist "Täiuslikud arvud" ("Matemaatika ja kaasaeg" VIII, lk. 58–64).

Ülesandeid.

27. Kui palju erinevaid jagajaid on arvul 2475 ja milline on nende summa?

28. Leida arvu 360 kõigi jagajate ruutude summa ja arvu 360^2 kõigi jagajate summa.

29. Arvul N^2 on 15 erinevat jagajat. Kui palju erinevaid jagajaid on arvul N^3?

30. Leida arv, mille kõigi jagajate korrutis on 5832.

31. Leida arv, mille kõigi jagajate korrutis on $3^{30}.4^{40}$.

§ 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 täiosa 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 3.4. Olgu antud positiivne reaalarv x ja naturaalarv $k < x$. Arvu x mitteületavate k kordsete arv võrdub $\left[\frac{x}{k}\right]$.

Tõestus. Kirjutame välja kõik arvu x mitteületavad naturaalarvu k kordsed $1 \cdot k, 2 \cdot k, \ldots, h \cdot k$. Et $hk \leqslant x < (h+1)k$, siis $h \leqslant \frac{x}{k} < h + 1$ ja seega $h = \left[\frac{x}{k}\right]$.

Teoreem 3.5. 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 3.6. Algarv p kuulub tegurina korrutisse $n!$ parajasti

$$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \dots$$

korda.

Tõestuseks leiame korrutisest $1\cdot2\cdot3\dots n$ kõik tegurid, mis on arvu p kordsed. Sellised on

$$1p,\ 2p,\ 3p,\dots,\ hp = \left[\frac{n}{p}\right] p\ .$$

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

$$1,\ 2,\ 3,\dots,\ \left[\frac{n}{p}\right].$$

Ka mõnedes nendest arvudest võib p veel tegurina esineda. Arvu p kordsed on

(1) $$1p,\ 2p,\dots,\ \left[\frac{\left[\frac{n}{p}\right]}{p}\right] p.$$

Eraldades igast kordsest teguri p, saame siit p veel astmes

$$\left[\frac{\left[\frac{n}{p}\right]}{p}\right] = \left[\frac{\frac{n}{p}}{p}\right] = \left[\frac{n}{p^2}\right].$$

Teguri p eraldamisel jäävad jada (1) elementidest järele tegurid

$$1,\ 2,\dots,\ \left[\frac{n}{p^2}\right].$$

Siit eraldame jälle välja p kordsed; saame lisaks p astmes $\left[\frac{n}{p^3}\right]$, jne. Seega esineb korrutises n! algarv p astmes

$$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \dots$$

Kui $p^k > n$, siis liidetavad tulevad nullid. Seega $n! = a \cdot p^{\alpha}$, kus

$$\alpha = \sum_{k=1}^{\infty} \left[\frac{n}{p^k}\right] \quad \text{ja} \quad (a,p) = 1,$$

ja

(2)
$$n! = \prod_{p \leq n} p^{\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \dots}.$$

Paragrahvis 5 kasutame funktsiooni

$$T(x) = \sum_{n \leq x} \ln n = \ln [x]!$$

Valemi (2) ja teoreemi 3.5. 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 3.6:

$$\left[\frac{6522}{7}\right] = 931, \quad \left[\frac{6522}{7^2}\right] = \left[\frac{931}{7}\right] = 133,$$

$$\left[\frac{6522}{7^3}\right] = \left[\frac{133}{7}\right] = 19, \quad \left[\frac{6522}{7^4}\right] = \left[\frac{19}{7}\right] = 2.$$

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 $211 = 2^{18} \cdot 3^9 \cdot 5^4 \cdot 7^3 \cdot 11 \cdot 13 \cdot 17 \cdot 19$.

Algarv p, kus $n \geq p > \frac{n}{2}$, kuulub $n!$ kanoonilisse kujusse esimeses astmes.

Ülesandeid.

32. Mitmendas astmes esineb 3 arvu 333 faktoriaalis?

33. Leida arvu $120!$ kanooniline kuju.

§ 3. EULERI φ-FUNKTSIOON.

Euleri φ-funktsioon $\varphi(a)$ on defineeritud kõikide naturaalarvude hulgal järgmiselt:

$\varphi(a)$ on naturaalarvu a mitteületavate ja arvuga a ühisjagajata naturaalarvude arv.

Olgu T (b) mingi tingimus, mida rahuldab naturaalarv b. Tähistades sümboliga $N[b;\ T(b)]$ tingimust T(b) rahuldavate naturaalarvude b arvu, võime φ-funktsiooni defineerida ka valemiga

$$\varphi(a) = N[b;\ b \leqslant a,\ (b,a) = 1].$$

Teoreem 3.7. $N[b;\ b \leqslant a,\ (a,b) = d] = \varphi\left(\frac{a}{b}\right)$.

Tõestus. Otsime 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 d_1 on fikseeritud, b ja b_1 aga muutuvad arvud, kusjuures $b_1 \leqslant a_1$. Igale b-le, mis rahuldab tingimusi $b \leqslant a$, $(a,b)=d$, vastab parajasti üks b_1, mis rahuldab tingimusi $b_1 \leqslant a_1$, $(a_1,b_1) = 1$. Seega

$$N[b;\ b \leqslant a,\ (b,a)=d] = N[b_1;\ b_1 \leqslant a_1,\ (b_1,a_1)=1] = \varphi(a_1) = \varphi\left(\frac{a}{d}\right).$$

Näide 1. Olgu a = 60 ja d = 5. Siis

$$N[b;\ b \leqslant 60,\ (b,60) = 5] = \varphi\left(\frac{60}{5}\right) = \varphi(12) = 4.$$

Teoreem 3.8. $\sum\limits_{d|a} \varphi(d) = a.$

Tõestus. Kirjutame kasvavas järjekorras välja arvu a kõik jagajad:

(1) $d_1, d_2, d_3, \ldots, d_{\tau(a)}$ $\quad (d_1=1,\ d_{\tau(a)}=a).$

Eelmise teoreemi põhjal

$$N[b;\ b \leqslant a,\ (b,a) = d_1] = \varphi\left(\frac{a}{d_1}\right) = \varphi(d_{\tau(a)}),$$

$$N[b;\ b \leqslant a,\ (b,a) = d_2] = \varphi\left(\frac{a}{d_2}\right)$$

(2) -

$$N[b;\ b \leqslant a,\ (b,a) = d_{\tau(a)}] = \varphi\left(\frac{a}{d_{\tau(a)}}\right) = \varphi(d_1).$$

Liidame kõik võrdused (2). Selleks et kindlaks teha, millega võrdub vasakul saadav summa, jaotame kõik naturaalarvud b, mis ei ületa arvu a, s.t. arvud

(3) $1, 2, 3, \ldots, a$

klassidesse, võttes ühte klassi kokku kõik need arvud, millel on arvuga a üks ja sama suurim ühistegur d_i ($i = 1,2,\ldots, \tau(a)$). 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

$$a = \varphi\left(\frac{a}{d_1}\right) + \varphi\left(\frac{a}{d_2}\right) + \ldots + \varphi\left(\frac{a}{d_{\tau(a)}}\right).$$

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 c_i. Niisiis erinevaid jagajaid c_i on täpselt niisama palju kui on jagajaid d_i, s.o. arvult $\tau(a)$. Et aga jagajatega d_i on ammendatud kõik a jagajad, siis on ka jadas

$$c_1, c_2, \ldots, c_{\tau(a)}$$

parajasti kõik a jagajad. Sealjuures on nad nüüd kahanevas järjekorras. Seega $\frac{a}{d_i} = c_i = d_{\tau(a)-i}$. Siit järeldubki

vajalik võrdus

$$a = \varphi(a_{\tau(a)}) + \varphi(a_{\tau(a)-1}) + \ldots + \varphi(a_2) + \varphi(a_1).$$

Teoreem 3.9. Euleri φ-funktsioon on nõrgalt multiplikatiivne.

Tõestuseks kasutame täieliku induktsiooni meetodit. Kui $a = b = 1$, siis kehtib võrdus

$$\varphi(1)\,\varphi(1) = \varphi(1);\quad (1,1) = 1.$$

Oletame, et φ-funktsioon on nõrgalt multiplikatiivne iga naturaalarvude paari α, β, $(\alpha, \beta) = 1$, korral, mille korrutis $\alpha\beta < ab$, $(a,b) = 1$. Näitame, et siis φ on multiplikatiivne ka a ja b suhetes, s.t.

$$\varphi(ab) = \varphi(a)\varphi(b).$$

Jaotame a ja b jagajad kahte rühma: a ja kõik pärisjagajad α; b ja kõik pärisjagajad β.

Teoreemi 3.8 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

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

Kasutades $\varphi(a)$ multiplikatiivsust, rakendame φ-funktsiooni arvu a kanoonilisele kujule

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

Siis saame

$$\varphi(a) = p_1^{\alpha_1}(1 - \frac{1}{p_1})p_2^{\alpha_2}(1 - \frac{1}{p_2}) \dots p_n^{\alpha_n}(1 - \frac{1}{p_n}) = a \prod_{k=1}^{n}(1 - \frac{1}{p_k}).$$

Näide 2. $\varphi(360) = \varphi(2^3 \cdot 3^2 \cdot 5) =$

$$= 360(1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{5}) = 96.$$

Ülesandeid.

34. Kui palju on arvust 1000 väiksemaid naturaalarve, mis on temaga ühistegurita?

35. Kui palju leidub naturaalarve, mis on väiksemad kui 10 000 ja mille suurim ühistegur 10 000-ga on 8?

36. Kui palju leidub naturaalarve, mis on väiksemad kui 10 000 ja mille suurim ühistegur 10 000-ga ei ületa 10?

37. 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. MÖBIUSE FUNKTSIOON $\mu(a)$.

Möbiuse funktsioon defineeritakse kõikide naturaalarvude hulgal järgmiste valemitega

1) $\mu(1) = 1$,

2) $\mu(ab^2) = 0$,

3) $\mu(p_1p_2 \cdots p_n) = (-1)^n$, kui $p_1, p_2, \ldots, p_n$ 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 3.10. 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 $a = p_1p_2 \cdots p_n$, $b = q_1q_2 \cdots q_k$, 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 tõestamiseks, et $\mu(a)$ ei ole tugevalt multiplikatiivne, võtame $a = p_1 \cdots p_n$, $b = q_1 \cdots q_k$, 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 3.11. Kui $\vartheta(a)$ on nõrgalt multiplikatiivne funktsioon ja

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

siis

(2) $$\sum_{d|a} \mu(d)\vartheta(d) = \left(1 - \vartheta(p_1)\right) \dots \left(1 - \vartheta(p_n)\right),$$

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 3.11 järeldusena saame järgmise tulemuse.

Teoreem 3.12. $\sum_{d|a} \mu(d) = 0$, kui $a > 1$.

Tõestuseks tarvitseb võrduses (2) võtta $\vartheta(a) \equiv 1$.

Ülesandeid.

38. Arvutada $\mu(182)$, $\mu(183)$, $\mu(184)$.

39. Kontrollida otseselt (vasakul seisva summa arvutamise teel) teoreemi 3.12 kehtivust $a = 40$ korral.

§ 5. ALGARVUDE JAOTUMINE NATURAALARVUDE JADAS. FUNKTSIOON $\pi(x)$.

Käesolevas paragrahvis käsitleme algarvude jaotumist naturaalarvude jadas ja uurime vastava jaotusfunktsiooni mõningaid omadusi. Märgime, et küsimus algarvude jaotumisest on arvuteooria üks raskemaid ja osalt veel lahendamata küsimusi.

1. Algarvude jaotusfunktsioon. Olgu $\pi(x)$ reaalarvu x mitteületavate algarvude arv, s.t.

$$\pi(x) = \sum_{p \le x} 1 .$$

Seega on $\pi(x)$ arvuteoreetiline funktsioon, mis on määratud kõigi reaalarvude hulgal ja omandab vaid täisarvulisi väärtusi. Nimetame teda algarvude jaotusfunktsiooniks.

Tähistame järgnevas (kogu käesoleva paragrahvi ulatuses) järjekorras n-ndat algarvu sümboliga p_n. Siis funktsiooni $\pi(x)$ definitsioonist järeldub, et

$$\pi(x) = n, \quad \text{kui} \quad p_n \le x < p_{n+1};$$

eriti on

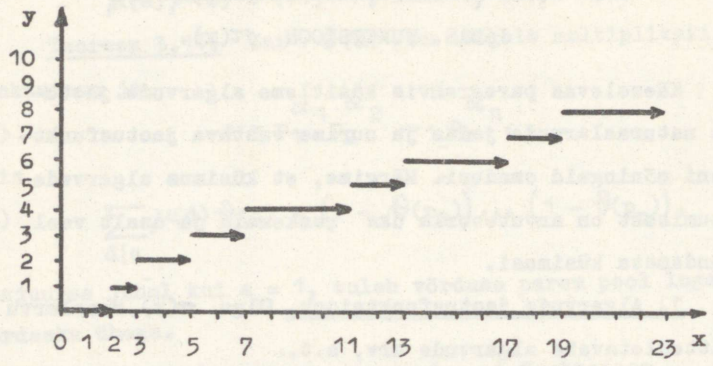
$$\pi(p_n) = n.$$

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 x-ga piiramatult, leidub kuitahes pikki arvtelje lõike, kus $\pi(x)$ on konstantne. See nähtub järgnevast teoreemist.

Teoreem 3.13. Iga täisarvu $n \geq 1$ korral leidub naturaalarvude jadas vahemik, milles n järjestikust naturaalarvu on kordarvud.

Tõestus. Kirjutame välja n järjestikust naturaalarvu

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

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 naturaal-

arvu seas leidub 152 892 paari kaksikuid . On püstitatud hüpotees, 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

$$p,\ p+2,\ p+6 \text{ ja } p+8,$$

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.

Funktsiooni $\pi(x)$ jaoks on teada mitmeid valemeid (vt. näit. [6], lk. 88-91, või [2], lk. 349-353), kuid arvutamine nende valemite järgi muutub seda tülikamaks, mida suurem on x. Pealegi ei võimalda nimetatud valemid uurida funktsiooni $\pi(x)$ kasvamise keskmist kiirust. Viimase suhtes on mugavamad asümptootilised valemid, millest tuleb juttu järgmises punktis.

2. Funktsiooni $\pi(x)$ hinnang ja asümptootilised avaldised. Tõestame järgmise teoreemi.

Teoreem 3.14 (Tšebõšov). Eksisteerivad konstandid a ja b, kusjuures $0 < a < 1$, $b > 1$, nii et iga $x \geqslant 2$ kor-

ral kehtivad võrratused

$$(1) \qquad a\frac{x}{\ln x} < \pi(x) < b\frac{x}{\ln x}.$$

Tõestus. 1) Hindame kõigepealt avaldist $T(x) - 2T(\frac{x}{2})$, kus funktsioon $T(x)$ on defineeritud 2. paragrahvis, s.t.

$$(2) \qquad T(x) = {}_n{}_x \ln n = \ln[x]! = \sum_p (\ln p)\left(\left[\frac{x}{p}\right] + \left[\frac{x}{p^2}\right] + \ldots\right).$$

Eeldame, et $n \geqslant 3$. Siis

$$(3) \qquad T(2n) - 2T(n) = \sum_{k=n+1}^{2n} \ln k - \sum_{k=1}^{n} \ln k =$$

$$= \ln\frac{n+1}{1} + \ln\frac{n+2}{2} + \ldots + \ln\frac{n+n}{n} \geqslant (n+1)\ln 2,$$

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

$$(5) \qquad T(x) - 2T(\tfrac{x}{2}) \geqslant (n+1)\ln 2 > \frac{\ln 2}{2}x,$$

$$(6) \qquad T(x) - 2T(\tfrac{x}{2}) \leqslant 2n\ln 2 + \ln(2n+1) \leqslant x\ln 2 + \ln(x+1) <$$

$$< x(\ln 2 + 1).$$

2) Hindame $\pi(x)$ alt. Valemist (2) saame

(7) $T(x)-2T(\frac{x}{2})=\sum_{p\leqslant x}(\ln p)\left(\left(\left[\frac{x}{p}\right]-2\left[\frac{x}{2p}\right]\right)+\left(\left[\frac{x}{p^2}\right]-2\left[\frac{x}{2p^2}\right]\right)+\ldots\right)$.

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 $\alpha - 1 < [\alpha] < \alpha$ 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. Lähtume seosest (7), jättes parempoolses summas ära mittenegatiivsed liikmed, kus $p \leqslant \frac{x}{2}$. Sellega summa võib ainult väheneda. Sealjuures

ülejäänud liidetavates on $\ln p$ kordajad

$$\left(\left[\frac{x}{p}\right] - 2\left[\frac{x}{2p}\right]\right) + \left(\left[\frac{x}{p^2}\right] - 2\left[\frac{x}{2p^2}\right]\right) + \ldots = 1,$$

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

$$T(x) - 2T\left(\frac{x}{2}\right) \geqslant \sum_{\frac{x}{2} < p \leqslant x} \ln p \geqslant \ln \frac{x}{2} \sum_{\frac{x}{2} < p \leqslant x} 1 = \left(\pi(x) - \pi\left(\frac{x}{2}\right)\right) \ln \frac{x}{2}.$$

Liites viimase võrratuse mõlemale poolele $\pi(x) \ln 2$, mis on väiksem kui $x \ln 2$, ja kasutades hinnangut (6) saame

$$\pi(x) \ln x - \pi\left(\frac{x}{2}\right) \ln \frac{x}{2} \leqslant T(x) - 2T\left(\frac{x}{2}\right) + x \ln 2 <$$

$$< x(2 \ln 2 + 1) = cx,$$

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

$$\pi(x) \ln x \leqslant cx + \pi\left(\frac{x}{2}\right) \ln \frac{x}{2} \leqslant cx + c\frac{x}{2} + \pi\left(\frac{x}{2^2}\right) \ln \frac{x}{2^2} \leqslant \ldots$$

$$\ldots \leqslant cx + c\frac{x}{2} + \ldots + c\frac{x}{2^{s-1}} + \pi\left(\frac{x}{2^s}\right) \ln \frac{x}{2^s} <$$

$$< cx\left(1 + \frac{1}{2} + \frac{1}{2^2} + \ldots\right) = 2cx.$$

Tähistades $b = 2c = 2(2 \ln 2 + 1)$, saame $x \geqslant b$ korral

$$\pi(x) < b \frac{x}{\ln x}.$$

Kui konstanti b suurendada, hakkab võrratus kehtima juba alates väärtusest $x = 2$. Teoreem on tõestatud.

Võtnud $T(x) - 2T\left(\frac{x}{2}\right)$ asemel avaldise

$$T(x) - T\left(\frac{x}{2}\right) - T\left(\frac{x}{3}\right) - T\left(\frac{x}{5}\right) + T\left(\frac{x}{30}\right)$$

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. Piiväärtuse olemasolu ei õnnestunud tal aga tõestada. Alles 1896.a. tõestasid J.Hadamard ja de la Vallee Poussin teineteisest sõltumatult, et nimetatud piirväärtus eksisteerib. Tõestus nõuab kompleksmuutuja funktsiooniteooria kasutamist. 1948.a. andis Selberg tõestuse, mis ei kasuta kompleksmuutuja funktsiooniteooriat. Seega kehtib asümptootiline valem*

(8) $$\pi(x) \sim \frac{x}{\ln x}.$$

Teisiti võib tulemust tõlgendada nii: küllalt suurel lõigul $[1,x]$ on algarve ligikaudu $\frac{1}{\ln x}$ osa kõikidest naturaalarvudest.

Suhet $\frac{\pi(x)}{x}$, kus x on naturaalarv, võib nimetada algarvude keskmiseks tiheduseks lõigul $[1,x]$. 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 ligikaud-

---

*Meenutame, et $f(x) \sim g(x)$ mingi piirprotsessi suhtes, kui selles piirprotsessis $\lim \frac{f(x)}{g(x)} = 1$.

se valemi:

$$\pi(x) \approx \frac{x}{\ln x - 1{,}08366} .$$

Samal viisil sai Gauss valemi

$$(9) \qquad \pi(x) \approx \int_2^x \frac{dt}{\ln t} .$$

Tšebõšov põhjendas aastatel 1849-1852 nende valemite kehtivuse, tõestades ühtlasi, et valem

$$(10) \qquad \pi(x) \sim \frac{x}{\ln x - a}$$

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 valemitest (10) märksa täpsem. Ülevaate valemite (8) ja (9) täpsusest annab järgmine tabel.

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	178	0,94	1,159
10^4	1229	1246	0,98	1,132
10^5	9592	9630	0,996	1,104
10^6	78498	78628	0,9983	1,084
$5 \cdot 10^6$	348513	348638	0,9996	1,075
10^7	664579	664918	0,9994	1,071
10^8	5761455	5762209	0,99986	1,061
10^9	50847478	50849275	0,99996	1,053
10^{10}	455052512			1,0023

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

$$\lim_{x \to \infty} \frac{x}{\pi(x) \ln \pi(x)} = \lim_{x \to \infty} \frac{x}{\pi(x) \ln \pi(x)} \lim_{x \to \infty} \frac{\ln x}{\ln \pi(x)} = 1.$$

Kui võtame siin $x = p_n$, siis viimane võrdus omandab kuju

$$\lim_{n\to\infty} \frac{p_n}{n \ln n} = 1$$

ehk

$$p_n \sim n \ln n .$$

3. Euleri tõestus algarvude hulga lõpmatuse kohta.

Euleri valem. I peatüki 4. paragrahvis tõestasime, et algarve on lõpmata palju (teoreem 1.21). Esitame nüüd nimetatud teoreemi Euleri tõestuse, mis kasutab matemaatilise analüüsi aparatuuri ja mis pani aluse analüütilisele arvuteooriale.

Olgu p_λ algarv. Siis rida $\sum_{k=0}^{\infty} \frac{1}{p_\lambda^k}$ koondub ja kehtib valem

$$(11) \quad \frac{1}{1 - \frac{1}{p_\lambda}} = 1 + \frac{1}{p_\lambda} + \frac{1}{p_\lambda^2} + \ldots = \sum_{k=0}^{\infty} \frac{1}{p_\lambda^k} .$$

Oletame, et algarve on vaid lõplik hulk

$$p_1, p_2, \ldots, p_n .$$

Kirjutame välja valemid (11) 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

$$(12) \quad \frac{1}{p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}} ,$$

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 $p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \dots p_n^{\alpha_n}$, sest nagu me eeldasime, leidub ainult n algarvu $p_1, p_2, \dots, p_n$. Järelikult üldliikme (12) võib esitada ka kujul $\frac{1}{m}$, kus m on mistahes naturaalarv. Et liikmed kujul (12) on kõik üksteisest erinevad, siis võib ridade (11) 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 3.15. Kui $s > 1$, siis kehtib nn. Euleri valem

$$\prod_{\lambda=1} \frac{1}{1 - \frac{1}{p_\lambda^s}} = \sum_{m=1}^{\infty} \frac{1}{m^s}.$$

Tõestus. Lähtume valemist

$$\frac{1}{1 - \frac{1}{p_\lambda^s}} = 1 + \frac{1}{p_\lambda^s} + \frac{1}{p_\lambda^{2s}} + \frac{1}{p_\lambda^{3s}} + \dots . \tag{13}$$

Kirjutame välja valemid (13) kõikide algarvude $p_1, p_2, \dots p_n$ jaoks, mis ei ületa mingit etteantud naturaalarvu N. Korrutame kõikide saadud valemite 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

(14) $$\prod_{\lambda=1}^{n} \frac{1}{1-\frac{1}{p_\lambda^s}} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \ldots + \frac{1}{N^s} + \frac{1}{N_1^s} + \frac{1}{N_2^s} + \ldots ,$$

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 $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}$. Arvude $N_1 \geqslant N + 1$, $N_2 \geqslant N_1 + 1, \ldots$ seas ei esine enam kõiki järjestikuseid naturaalarve (näiteks ei esine p_{n+1}). Kui $s > 1$, siis rida

$$1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \ldots$$

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 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

$$\zeta(s) = \sum_{m=1} \frac{1}{m^s} .$$

Euleri valemi abil ja ζ-funktsiooni uurimise alusel on

saadud algarvude kohta üsna kaugeleulatuvaid tulemusi.

4. Algarvude pöördväärtuste rea hajuvus. Käesoleva paragrahvi lõpul tõestame veel algarvude järgmise tähelepanuväärse omaduse.

Teoreem 3.16. Algarvude pöördväärtuste rida

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \ldots = \sum_{\lambda=1} \frac{1}{p_\lambda}$$

hajub.

Tõestus. Valem (13) kehtib, kui s = 1. Seega kehtib s = 1 korral ka valem (14), mis on esimesest tuletatud. Valemist (14) 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

$$0 < -\ln\left(1 - \frac{1}{p_\lambda}\right) = \frac{1}{p_\lambda} + \frac{1}{2}\left(\frac{1}{p_\lambda}\right)^2 + \frac{1}{3}\left(\frac{1}{p_\lambda}\right)^3 + \ldots <$$

$$< \frac{1}{p_\lambda} + \left(\frac{1}{p_\lambda}\right)^2 + \left(\frac{1}{p_\lambda}\right)^3 + \ldots = \frac{1}{p_\lambda - 1} \leq 2 \frac{1}{p_\lambda} .$$

Rea $2\sum_{\lambda=1}^{\infty}\frac{1}{p_\lambda}$ liikmed on suuremad kui positiivsete liikmetega hajuva rea vastavad liikmed. Seega hajub ka rida $2\sum\frac{1}{p_\lambda}$ ja rida $\sum\frac{1}{p_\lambda}$.

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 $s>1$.

IV. K O N G R U E N T S I D.

§ 1. KONGRUENTSIDE OMADUSED.

1. Kongruentsi definitsioon. Olgu antud fikseeritud naturaalarv m ja mistahes täisarvud a ja b. Siis teoreemi 1.4 kohaselt

$$(1)\qquad \begin{aligned} a &= q_1 m + r_1, \quad 0 \leqslant r_1 < m, \\ b &= q_2 m + r_2, \quad 0 \leqslant r_2 < m, \end{aligned}$$

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 inkongruentseteks modulo m.

---

* Modulo (lad. k.) - mooduli järgi. Mõnikord kasutame väljendi "modulo m" asemel ka eestikeelset "mooduli m järgi".

Kui $a \equiv b \pmod m$, siis $a = q_1 m + r$, $b = q_2 m + r$ $(0 \leq r < m)$, millest $a - b = (q_1 - q_2)m$. 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 m-ga.

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, kui leidub täisarv t, nii et

$$a = b + mt. \tag{3}$$

Arvude kongruentsuse definitsioonist järeldub rida lihtsalt 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 4.1. 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 4.2. Kui $a_1 \equiv b_1 \pmod m$, $a_2 \equiv b_2 \pmod m$, ..., $a_k \equiv b_k \pmod m$, siis

$$a_1 + a_2 + \ldots + a_k \equiv b_1 + b_2 + \ldots + b_k \pmod{m},$$

s.t. kongruentse ühe ja sama mooduli järgi võib liikmeti liita.

Teoreem 4.3. 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 4.4. 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 4.5. Kui $a_1 \equiv b_1 \pmod{m}$, $a_2 \equiv b_2 \pmod{m}$, ..., ..., $a_k \equiv b_k \pmod{m}$, siis

$$a_1 a_2 \ldots a_k \equiv b_1 b_2 \ldots b_k \pmod{m},$$

s.t. kongruentse ühe ja sama mooduli järgi võib liikmeti korrutada.

Teoreem 4.6. Kui $a \equiv b \pmod{m}$, siis

$$a^n \equiv b^n \pmod{m}$$

iga $n > 0$ korral, s.t. kongruentsi mõlemaid poole võib tõsta ühte ja samasse astmesse.

Teoreem 4.6 on järeldus teoreemist 4.5.

Teoreem 4.7. 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 4.8. 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 4.6 ka 4.5 põhjal

$$a_ix_1^{n-i} \equiv b_ix_2^{n-i} \pmod m \quad (i=0,1,\ldots,n),$$

millest teoreemi 4.2 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 4.9. 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 $A_{\alpha_1\ldots\alpha_k}$, $x_1,\ldots,x_k$ vastavalt mooduli m järgi kongruentsete arvudega $B_{\alpha_1\ldots\alpha_k}$, $y_1,\ldots,y_k$, 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 4.8 tõestusega.

Teoreem 4.10. 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 te-

guriga, kui see tegur on mooduliga ühisjagajata.

Tõestus. Olgu $a \equiv b \pmod{m}$ ja $a = a_1 c$, $b = b_1 c$, 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 see on ühtlasi mooduli teguriks. 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 4.11. 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 4.12. 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 4.13. Kongruentsi

$$ac \equiv bc \pmod{m}$$

mõlemaid pooli võib jagada c-ga, kuid siis peab moodulit jagama (c,m)-ga.

Tõestus. Olgu $(c,m) = d$; siis $c = c_1 d$, $m = m_1 d$, kusjuures $(c,m_1) = 1$. Saame

$$ac_1 d \equiv bc_1 d \pmod{m_1 d}.$$

Teoreemi 4.12 põhjal järeldub siit kongruents

$$ac_1 \equiv bc_1 \pmod{m_1},$$

teoreemi 4.10 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 4.14. 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 4.15. Kui kongruents kehtib mingi mooduli järgi, siis ta kehtib ka selle mooduli mistahes jagaja järgi, s.t. kui $a \equiv b \pmod{m}$ ja $d \mid m$, siis $a \equiv b \pmod{d}$.

Tõestus järeldub samasusest

$$a = b + mt = b + dm_1 t = b + dt_1,$$

kus $t_1 = m_1 t$ on täisarv.

Teoreem 4.16. 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 $a_1 d = b + m_1 dt$, millest teoreemi 1.2 põhjal järeldub, et $d|b$.

Teoreem 4.17. Kui $a \equiv b \pmod{m}$, siis

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

Teoreem 4.17 järeldub teoreemist 1.6.

4. Rakendusi. Käesolevas punktis vaatleme kongruentsi omaduste rakendusi jaguvustunnuste tuletamisel ning arvude korrutise ja astme jagamisel tekkiva jäägi leidmisel.

Tuletame kõigepealt arvudega 9 ja 3 jaguvuse tunnuse. Iga arvu N võib tema numbrite $a_n, a_{n-1}, \ldots, a_1$ kaudu esitada kümnendsüsteemis kujul

$$N = a_n \cdot 10^{n-1} + a_{n-1} \cdot 10^{n-2} + \ldots + a_2 \cdot 10 + a_1.$$

Et $10 \equiv 1 \pmod{9 \text{ ja mod } 3}$, siis ka $10^k \equiv 1 \pmod{9 \text{ ja mod } 3}$. 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 tuletame arvuga 11 jaguvuse tunnuse. 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 arv jagub 11-ga parajasti siis, kui paaritutel kohtadel asuvate numbrite summa ja paariskohtadel asuvate numbrite summa 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.

Tuletame veel 7-ga jaguvuse tunnuse. Selleks koostame tabeli:

$$10^0 \equiv 1 \pmod{7}$$

$$10 \equiv 3 \pmod{7}$$

$$10^2 \equiv 3^2 \equiv 2 \pmod{7}$$

$$10^3 \equiv 3 \cdot 2 \equiv -1 \pmod{7}$$

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

$$10^5 \equiv 2 \cdot (-1) \equiv -2 \pmod{7}$$

$$10^6 \equiv 1 \pmod 7$$

$$10^7 \equiv 3 \pmod 7$$

- - - - - - - - -

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 arv N jagub 7-ga parajasti siis, kui 7-ga jagub algebraline summa

$$a_1 + 3a_2 + 2a_3 - a_4 - 3a_5 - 2a_6 + \ldots .$$

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

$\equiv -1 \equiv 6$

Näitena võetud arvu N jagamisel 7-ga tekib jääk 6, seega see arv ei jagu 7-ga.

Analoogilisel viisil võib tuletada mistahes arvuga m jaguvuse tunnuse.

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 vähima positiivse arvu x leidmisega, mis on kongruentne arvuga a:

$$141 \cdot 263 \cdot 843 \cdot 721 \equiv x \pmod{101},$$

kus $0 \leq x < 101$. Teoreemi 4.5 põhjal võib kõik tegurid asen-

dada 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 jäägi, mis tekib antud astme jagamisel antud arvuga.

Ülesandeid.

40. Esitades täisarvu tuhandendsüsteemis ja arvestades, et $1001 = 7 \cdot 11 \cdot 13$, $999 = 27 \cdot 37$ tuletada arvudega 7, 11, 13 ja 37 jaguvuse tunnused.

41. Tuletada jaguvustunnused jagamiseks 4-ga, 8-ga, 99-ga.

42. Leida jääk, mis tekib arvu 5361^{67} jagamisel 97-ga.

43. Leida jääk, mis tekib arvu $(12371^{56} + 34)^{28}$ jagamisel 111-ga.

44. Leida arvu 321^{53} kaks viimast numbrit.

§ 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 $\overline{r}$. Seega jäägiklass $\overline{r}$ on kongruentsi

(1) $$x \equiv r \pmod{m}$$

rahuldavate kõikide täisarvude x hulk. Teisiti öeldes, kõik jäägiklassi $\overline{r}$ kuuluvad arvud saame, kui laseme avaldises

$$xm + r$$

muutujal x omandada kõik täisarvulised väärtused. Eriti $r \in \overline{r}$. 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

$$\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{m-1}.$$

Teoreem 4.18. $\overline{a} = \overline{r}$ parajasti siis, kui $a \equiv r \pmod{m}$.

Tõestus. Kui $a \equiv r \pmod{m}$, s.t. kui $a \in \overline{r}$, siis kongruentsi transitiivsuse ja sümmeetria omaduse (teoreem 4.1) tõttu järeldub kongruentsist (1) kongruents

(2) $$x \equiv a \pmod{m}$$

ja vastupidi, kongruentsist (2) järeldub kongruents (1). Järelikult

$$\overline{a} = \overline{r}.$$

Kui aga $\overline{a} = \overline{r}$, siis $a \in \overline{r}$ ja seega $a \equiv r \pmod{m}$.

Tõestusest järeldub ühtlasi, et jäägiklass $\overline{r}$ on iga oma elemendiga üheselt määratud.

Teatavasti moodustab kõikide jäägiklasside hulk antud mooduli m järgi ringi, kui jäägiklasside summa ja korrutis defineerida valemitega

$$\overline{a} + \overline{b} = \overline{a + b}, \quad \overline{a}\,\overline{b} = \overline{ab}.$$

(vt. näit. G.Kangro. Kõrgem algebra, Tln., 1962, lk. 145-150, või [2], 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

$$n\bar{a} = \underbrace{\bar{a} + \bar{a} + \ldots + \bar{a}}_{\text{n liidetavat}}, \quad 0\cdot\bar{a} = \bar{0}, \quad -n\bar{a} = n(-\bar{a}),$$

$$(\bar{a})^n = \underbrace{\bar{a}\,\bar{a}\ldots\bar{a}}_{\text{n tegurit}}, \quad (\bar{a})^0 = \bar{1},$$

võime lihtsalt tõestada, et kehtib järgmine teoreem.

Teoreem 4.19. 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. Klassidel $c\bar{a}$ ja $\overline{ca}$ on ühine element ca; seega need klassid ühtivad: $c\bar{a} = \overline{ca}$. Täpselt samuti on klassidel $(\bar{a})^n$ ja $\overline{a^n}$ ühine element a^n; järelikult $(\bar{a})^n = \overline{a^n}$. Seetõttu

$$f(\bar{a}) = c_0(\bar{a})^n + c_1(\bar{a})^{n-1} + \ldots + c_{n-1}\,\bar{a} + c_n\cdot\bar{1} =$$

$$= \overline{c_0a^n} + \overline{c_1a^{n-1}} + \ldots + \overline{c_{n-1}a} + \overline{c_n\cdot 1} =$$

$$= \overline{c_0a^n + c_1a^{n-1} + \ldots + c_{n-1}a + c_n} = \overline{f(a)}.$$

2. Täielik jääkide 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 jääkide süsteemiks modulo m. Näiteks on täielikuks jääkide süsteemiks modulo 8 arvude

$$-7,\ 0,\ 10,\ 3,\ 4,\ -3,\ 14,\ 7$$

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 4.20. Kulgegu x üle täieliku jääkide süsteemi modulo m. Siis arvud ax+b, kus (a,m) = 1 ja b on suvaline täisarv, moodustavad samuti täieliku jääkide süsteemi.

Tõestus. Omandagu x väärtusi

$$x_0, x_1, \ldots, x_{m-1},$$

kus viimases jadas ei ole elemente, mis kuuluksid ühte ja samasse jäägiklassi, s.t. pole kongruentseid modulo m. Avaldis ax+b saab nüüd järgmised väärtused

$$ax_0 + b,\ ax_1 + b,\ \ldots,\ ax_{m-1} + b.$$

Kui selles süsteemis ei leidu kongruentseid modulo m, siis iga arv satub eri klassi. Oletame vastupidi, et leidub kaks arvu, mis on omavahel kongruentsed, s.o.

$$ax_i + b \equiv ax_j + b \pmod m.$$

Mõlemalt poolt võib lahutada ühe ja sama arvu:

$$ax_i \equiv ax_j \pmod{m}.$$

Et $(a,m) = 1$, siis teoreemi 4.10 põhjal

$$x_i \equiv x_j \pmod{m},$$

mis on vastuolus eeldusega. Seega ka ax+b kulgeb üle täieliku jääkide süsteemi. Teoreem on tõestatud.

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 4.17 põhjal on ühte ja samasse jäägiklassi kuuluvatel arvudel mooduliga 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

$$N[a;\ (a,m) = 1,\ a \leq m] = \varphi(m)$$

tükki. Seega on taandatud jääkide süsteemis mooduli m järgi $\varphi(m)$ arvu.

Teoreem 4.21. Kui (a,m) = 1 ja x kulgeb üle taandatud jääkide süsteemi, siis arvud ax moodustavad samuti taandatud jääkide süsteemi.

Tõestus on analoogiline teoreemi 4.20 tõestusega. Laseme muutujal x kulgeda üle taandatud jääkide süsteemi

$$x_1, x_2, \ldots, x_{\varphi(m)},$$

siis ax omandab väärtused

$$ax_1, ax_2, \ldots, ax_{\varphi(m)}.$$

Kui viimaste hulgas oleks mooduli m järgi kongruentseid,

$$ax_i \equiv ax_j \pmod{m},$$

siis (a,m) = 1 tõttu järelduks siit

$$x_i \equiv x_j \pmod{m},$$

mis on vastuolus eeldusega. Seega arvud $ax_1, \ldots, ax_{\varphi(m)}$ kuuluvad erinevatesse jäägiklassidesse, mida on arvult $\varphi(m)$. Tuleb veel näidata, et $(ax_i, m) = 1$. See aga järeldub sellest, et (a,m) = 1 ja $(x_i, m) = 1$.

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 4.22 (Euler). Kui (a,m) = 1, siis

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

Tõestus. Kirjutame välja taandatud jääkide süsteemi modulo m:

(1) $$r_1, r_2, \ldots, r_{\varphi(m)}.$$

Siis ka

$$ar_1, ar_2, \ldots, ar_{\varphi(m)}$$

on taandatud jääkide süsteem sama mooduli järgi. See tähendab, et

$$ar_1 \equiv r_{i_1} \pmod{m},$$
$$ar_2 \equiv r_{i_2} \pmod{m}$$
$$\ldots\ldots\ldots$$
$$ar_{\varphi(m)} \equiv r_{i_{\varphi(m)}} \pmod{m},$$

kus kongruentside paremad pooled on jäägid hulgast (1) ja sealjuures kõik erinevad. Korrutame kõik kongruentsid omavahel läbi; saame

$$a^{\varphi(m)} r_1 r_2 \cdots r_{\varphi(m)} \equiv r_{i_1} r_{i_2} \cdots r_{i_{\varphi(m)}} \pmod{m}.$$

Korrutis $r_1 r_2 \cdots r_{\varphi(m)}$ vasakul võrdub kongruentsi parema poolega. Et $(r_i, m) = 1$ iga i korral, siis

$$(r_1 r_2 \cdots r_{\varphi(m)}, m) = 1.$$

Seega võime teoreemi 4.10 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 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 4.23 (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.

Ülesandeid.

45. Kirjutada välja taandatud jääkide süsteem mooduli 30 järgi.

46. Kasutades Euleri teoreemi arvutada jääk, mis tekib arvu 34^{59522} jagamisel 110-ga.

47. Kas arv $6\,781\,207^{24} - 1$ jagub 39-ga?

48. Näidata, et $2^{73\cdot37-1} \equiv 1 \pmod{37\cdot73}$.

§ 3. TUNDMATUT SISALDAVAD KONGRUENTSID.

Kongruentsi

$$f(x) \equiv 0 \pmod{m}, \tag{1}$$

kus $f(x)$ on täisarvuliste kordajatega polünoom

$$f(x) = ax^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n, \tag{2}$$

nimetatakse tundmatut sisaldavaks kongruentsiks.

Kui sealjuures $a \not\equiv 0 \pmod{m}$, 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 4.8 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

$$f(\overline{x}) = \overline{0} \tag{3}$$

rahuldavate jäägiklasside leidmise ülesandega. Tõepoolest, kongruents $f(x_1) \equiv 0 \pmod{m}$ kehtib teoreemi 4.18 kohaselt parajasti siis, kui $\overline{f(x_1)} = \overline{0}$; teoreemi 4.19 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. Teoreetiliselt on sellega kongruentside (1) lahendamise ülesanne täielikult ammendatud. Kui moodul m on väike, on selline

meetod ka 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

$$x = 4 + 7t \text{ ja } x = 2 + 7t,$$

kus t omab 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 vaatlemegi 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

(4) $$f(x) \equiv g(x) \pmod m,$$

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 ekvivalentseteks, kui arvude hulk, mis rahuldab üht kongruentsi, ühtib arvude hulgaga, mis rahuldab teist kongruentsi.

Teoreem 4.24. Kongruentsiga (4) ekvivalentse kongruentsi saame, kui

1) kongruentsi (4) mõlemale poolele liidame ühe ja sama suvalise polünoomi $\omega(x)$;

2) kongruentsi (4) mõlemaid pooli korrutame ühe ja sama täisarvuga, mis on mooduliga m ühistegurita;

3) kongruentsi (4) mõlemaid pooli ja moodulit korrutame ühe ja sama naturaalarvuga k.

Tõestus. 1) Kui mingi x_0 korral

$$f(x_0) \equiv g(x_0) \pmod{m},$$

siis

$$f(x_0) + \omega(x_0) \equiv g(x_0) + \omega(x_0) \pmod{m};$$

vastupidi, viimasest kongruentsist järeldub ka esimene (teoreem 4.3).

2) Kui mingi x_0 korral

$$f(x_0) \equiv g(x_0) \pmod{m} \text{ ja } (b,m) = 1,$$

siis

$$bf(x_0) \equiv bg(x_0) \pmod{m};$$

vastupidi, viimasest kongruentsist järeldub ka esimene (teoreemid 4.7 ja 4.10).

3) Kui mingi x_0 korral

$$f(x_0) \equiv g(x_0) \pmod{m},$$

siis

$$kf(x_0) \equiv kg(x_0) \pmod{km};$$

vastupidi, viimasest kongruentsist järeldub ka esimene (teoreemid 4.11 ja 4.12).

Teoreemist järeldub, et kongruentsid $f(x) \equiv g(x) \pmod{m}$ ja $f(x) - g(x) \equiv 0 \pmod{m}$ on ekvivalentsed.

Teoreem 4.25. Kui $a_0 \equiv b_0 \pmod{m}$, $a_1 \equiv b_1 \pmod{m}$, ... , $a_n \equiv b_n \pmod{m}$, siis kongruentsid

$$f(x) = a_0x^n + \ldots + a_1x + a_0 \equiv 0 \pmod{m}$$

ja

$$g(x) = b_0x^n + \ldots + b_1x + b_0 \equiv 0 \pmod{m}$$

on ekvivalentsed.

Tõestus. Kui $f(x_0) \equiv 0 \pmod{m}$, siis teoreemi 4.8 kohaselt $g(x_0) \equiv f(x_0) \equiv 0 \pmod{m}$. Kui aga $f(x_0) \not\equiv 0 \pmod{m}$, siis ka $f(x_0) \equiv g(x_0) \not\equiv 0 \pmod{m}$. 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, $a > 0$. Osutub, et eksponentkongruentsi lahendeid ei saa esitada kujul $x \equiv c \pmod{m}$, vaid neid saab esitada jäägiklassidena m-st erineva mooduli järgi.

Ülesandeid.

49. Lahendada kongruents

$$x^5 + x^4 + x + 1 \equiv 0 \pmod{6}.$$

50. Lahendada kongruents

$$53x^4 + 9x^3 - 19x^2 + 25x + 17 \equiv 0 \pmod{5},$$

asendades eelnevalt kordajad väiksematega.

§ 4. 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 $\overline{k}$, s.t. $b \in \overline{k}$ ehk $b \equiv k \pmod{m}$. Kirjutame välja täieliku jääkide süsteemi modulo m:

(2) $$0, 1, 2, 3, \ldots, m-1.$$

Siis

(3) $$a\cdot 0, a\cdot 1, a\cdot 2, \ldots, a(m-1)$$

moodustab teoreemi 4.20 kohaselt samuti täieliku jääkide süsteemi, 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. Mooduli kordse liitmise meetod. Kirjeldame meetodit näidete varal.

Näide 1. Võtame kongruentsi

$$5x \equiv 4 \pmod 7$$

ja liidame paremale poolele või lahutame sellest arvu 7 kordseid kuni saame arvu 5 kordse

$$5x \equiv 4 - 2\cdot 7 \equiv -10 \pmod 7).$$

Jagamisel 5-ga saame lahendiks

$$x \equiv -2 \pmod 7)$$

ehk

$$x \equiv 5 \pmod 7).$$

Meetodi rakendamisel võime kongruentsi pooli jagada ühe ja sama arvuga.

Näide 2. Kongruentsi

$$210x \equiv 103 \pmod{353}, \quad (210, 353) = 1$$

võime lahendada järgmiselt:

$$210x \equiv 456 \pmod{353},$$

$$35x \equiv 76 \pmod{353},$$

$$35x \equiv 76 - 706 = -630 \pmod{353},$$

$$x \equiv -18 \equiv 335 \pmod{353}.$$

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:

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 $a = a_1 d$ ja $m = m_1 d$, kusjuures $(a_1, m_1) = 1$. Peale a ja m asendamist saame kongruentsile (1) kuju

(4) $$a_1 dx \equiv b \pmod{m_1 d}.$$

Kui kongruents (4) on lahenduv, siis teoreemi 4.16 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 kongruents

$$ax \equiv b \pmod{m}$$

ei ole lahenduv. Näiteks pole lahendeid lineaarkongruentsil

$$15x \equiv 7 \pmod{21},$$

sest 7 ei jagu arvuga $(15, 21) = 3$.

Olgu $b = b_1 d$. Siis

$$da_1 x = db_1 \pmod{dm_1},$$

millest peale jagamist d-ga saame esialgsega ekvivalentse kongruentsi

(5) $$a_1 x \equiv b_1 \pmod{m_1}, \quad (a_1, m_1) = 1.$$

Nagu eelmises punktis nägime, on viimasel kongruentsil mooduli m_1 järgi parajasti üks lahend. Seega on tingimus

$$b \vdots (a,m)$$

tarvilik ja piisav lahendi olemasoluks.

Teeme kindlaks vaadeldava kongruentsi lahendite arvu

modulo m. Kongruentsil (5), samuti kongruentsil (1) on mooduli m_1 järgi paarajasti 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 modulo m 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:

$$x \equiv c, c + m_1, \ldots, c + (d-1)m_1 \pmod{m}.$$

Ülesandeid.

51. Mooduli kordse liitmise meetodil lahendada lineaarkongruents

$$30x \equiv 53 \pmod{77}.$$

52. Ahelmurdude meetodit kasutades lahendada kongruents

$$256x \equiv 179 \pmod{337}.$$

53. Euleri teoreemi alusel lahendada kongruents

$$11x \equiv 32 \pmod{36}.$$

54. Lahendada kongruentsid:

a) $1215x \equiv 560 \pmod{2755}$;

b) $78x \equiv 30 \pmod{198}$;

c) $8934x \equiv 5789 \pmod{10113}$.

§ 5. LINEAARKONGRUENTSIDE SÜSTEEMID.

Käesolevas paragrahvis vaatleme lineaarkongruentside süsteemi

$$(1)\qquad \begin{aligned} a_1x &\equiv b_1 \pmod{m_1} \\ a_2x &\equiv b_2 \pmod{m_2} \\ &\text{- - - - - - - - -} \\ a_kx &\equiv b_k \pmod{m_k} \end{aligned}$$

lahendamist.

1. Eeldame algul, et moodulid on paarikaupa ühistegurita, s.t. iga i,j korral, kus $i \neq j$, on $(m_i,m_j) = 1$ ja peale selle $(a_i,m_i) = 1$. Siis on süsteemi (1) igal kongruentsil parajasti üks lahend:

$$(2)\qquad \begin{aligned} x &\equiv c_1 \pmod{m_1} \\ x &\equiv c_2 \pmod{m_2} \\ &\text{- - - - - - - - -} \\ x &\equiv c_k \pmod{m_k}. \end{aligned}$$

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 4.26. 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

$$m_1 m_2 \dots m_k = M_i m_i, \quad M_i M_i' \equiv 1 \pmod{m_i},$$

siis süsteemi (2) ja seega ka süsteemi (1) lahendiks on

$$(3) \quad x \equiv M_1 M_1' c_1 + M_2 M_2' c_2 + \dots + M_k M_k' c_k \pmod{m_1 m_2 \dots m_k}.$$

Mooduli $m_1 m_2 \dots m_k$ järgi on see lahend ainus.

Tõestus. Kõigepealt märgime, et teoreemi tingimustes esinevad kongruentsid $M_i M_i' \equiv 1 \pmod{m_i}$ on M_i' suhtes üheselt lahenduvad, sest $(M_i, m_i) = 1$. Edasi näitame, et arv $M_1 M_1' c_1 + M_2 M_2' c_2 + \dots + M_k M_k' c_k$ rahuldab süsteemi i-ndat kongruentsi ($i = 1,2,\dots,k$). Tõepoolest, kuna $M_j \vdots m_i$ ($j \neq i$) ja $M_i M_i' \equiv 1 \pmod{m_i}$, siis

$$M_1 M_1' c_1 + \dots + M_i M_i' c_i + \dots + M_k M_k' c_k \equiv M_i M_i' c_i \equiv c_i \pmod{m_i}.$$

Seega süsteemi (2) üheks lahendiks on (3).

Oletame, et peale lahendi (3) leidub veel teisi jäägiklasse modulo $m_1 m_2 \dots m_k$, mis on kongruentsi (2) lahendiks. Olgu mingi teine lahend

$$x \equiv c \pmod{m_1 m_2 \dots m_k}.$$

Siis $c \equiv c_i \pmod{m_i}$ ja seetõttu

$$c \equiv c_i \equiv M_1 M_1' c_1 + \dots + M_k M_k' c_k \pmod{m_i}.$$

Teoreemi 4.14 põhjal on

$$c \equiv M_1 M_1' c_1 + \dots + M_k M_k' c_k \pmod{m_1 m_2 \dots m_k},$$

mis näitabki, et teisi lahendeid peale (3) ei ole.

Näide 1. Leida arv 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 kongru-

entside 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

$$3 \cdot 5 \cdot 7 \cdot 11 = M_i m_i$$

saame

i	1	2	3	4
m_i	3	5	7	11
M_i	385	231	165	105

M_i' leidmiseks tuleb lahendada abikongruentsid

$$385\,M_1' \equiv 1 \pmod 3 \quad \text{ehk} \quad M_1' \equiv 1 \pmod 3,$$
$$231\,M_2' \equiv 1 \pmod 5 \quad \text{ehk} \quad M_2' \equiv 1 \pmod 5,$$
$$165\,M_3' \equiv 1 \pmod 7 \quad \text{ehk} \quad 4M_3' \equiv 1 \pmod 7,$$
$$105\,M_4' \equiv 1 \pmod{11} \quad \text{ehk} \quad 6M_4' \equiv 1 \pmod{11}.$$

Lahendite jäägiklassidest võtame absoluutväärtuselt vähimad elemendid:

$$M_1' = 1, \quad M_2' = 1, \quad M_3' = 2, \quad M_4' = 2.$$

Seega $c = 385 \cdot 1 + 231 \cdot 2 + 165 \cdot 3 + 105 \cdot 2 \cdot 4 = 2677$ ja otsitav lahend on

$$x \equiv 2677 \equiv 367 \pmod{1155}.$$

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 kongruentsi

$$a_3 e_1 + a_3 m_1 m_2 t_2 \equiv b_3 \pmod{m_3},$$

millest lahendamisel saame

$$t_2 \equiv d_2 \pmod{m_3} \quad \text{ehk} \quad t_2 = d_2 + m_3 t_3.$$

Seega kolme esimest kongruentsi rahuldavad arvud

$$x = e_1 + m_1 m_2 (d_2 + m_3 t_3) = e_2 + m_1 m_2 m_3 t$$

ehk

$$x \equiv e_2 \pmod{m_1 m_2 m_3}.$$

Niiviisi saame lõpuks süsteemi (1) lahendi

(5) $$x \equiv e_{k-1} \pmod{m_1 m_2 \dots m_k}.$$

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 $m_1 m_2 \dots m_k$ järgi on siis süsteemil rohkem kui üks lahend. Teisel juhul on juba esialgne süsteem vastuoluline, s.t. süsteemil puudub lahend.

Näide 2. Lahendame süsteemi

$$x \equiv 3 \pmod 4, \quad x \equiv 5 \pmod 6, \quad x \equiv 11 \pmod{15}.$$

Esimest kongruentsi rahuldavad arvud $x = 3 + 4t_1$. Asendamisel teise kongruentsi saame kongruentsi t_1 suhtes:

$$3 + 4t_1 \equiv 5 \pmod 6$$

ehk

$$4t_1 \equiv 2 \pmod 6$$

ehk

$$2t_1 \equiv 1 \pmod 3,$$

millest

$$t_1 \equiv 2 \pmod 3).$$

Seega $x = 3 + 4t_1 = 3 + 4(2+3t_2) = 11 + 12t_2$.

Edasi leiame t_2, mille korral on rahuldatud ka kolmas kongruents

$$11 + 12t_2 \equiv 11 \pmod{15}.$$

Lahendamisel saame

$$12t_2 \equiv 0 \pmod{15},$$

$$4t_2 \equiv 0 \pmod{5},$$

$$t_2 \equiv 0 \pmod{5}.$$

Seega $x = 11 + 12(0 + 5t_3) = 11 + 60t_3$ ja süsteemi lahendiks on

$$x \equiv 11 \pmod{60}.$$

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.

Ülesandeid.

55. Lahendada kongruentside süsteem

$4x \equiv 5 \pmod{7}$, $x \equiv 3 \pmod{5}$, $7x \equiv 1 \pmod{11}$.

56. Lahendada kongruentside süsteem

$3x \equiv 7 \pmod{10}$, $x \equiv 7 \pmod{15}$, $3x \equiv 1 \pmod{18}$.

57. 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. KÕRGEMA ASTME KONGRUENTSID.

1. 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. Osutub, et algarvulise mooduli korral on oluliselt erinevaid kongruentse vaid lõplik hulk. See järeldub järgmisest teoreemist.

Teoreem 4.27. Algarvulise mooduli korral saab kongruentsi, 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 on kongruentsi (1) lahend, siis seoste (2) ja (3) tõttu on rahuldatud (4). Vastupidi, kui x on kongruentsi (4) lahend, 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

$$x^s - (x^p - x)x^{s-p} = x^{s-(p-1)}.$$

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 $1 \leqslant r \leqslant p-1$, asendatakse aste x^s astmega x^r. Kui selline asendus läbi teha kõigi liikmetega, siis saame sama tulemuse, nagu polünoomi jagamisel vahega $x^p - x$.

Näide 1. 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 $1 \leqslant r \leqslant 6$. Saame

$$x^6 + 2x^3 + 3x^6 + 4x^4 + 5x + 3x^6 + 8x^3 + 9x^2 + 10x + 11 \equiv 0 \pmod 7$$

ehk

$$4x^4 + 3x^3 + 2x^2 + x + 4 \equiv 0 \pmod 7.$$

(Harjutusülesanne: Teha sama asendus läbi jagades polünoomi vahega $x^7 - x$.)

Teoreem 4.28. 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)

$$
\begin{aligned}
f(x) = {} & b_0(x-x_1)(x-x_2)\ldots(x-x_{n-1})(x-x_n) + \\
& + b_1(x-x_1)(x-x_2)\ldots(x-x_{n-1}) + \\
& + \ldots\ldots\ldots\ldots\ldots + \\
& + b_{n-2}(x-x_1)(x-x_2) + b_{n-1}(x-x_1) + b_n,
\end{aligned}
\tag{5}
$$

kus kordajad b_i on üheselt määratud ja täisarvud, sest nad on arvutatavad Horneri skeemi abil polünoomi $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$ esialgsete kordajate $a_0, a_1, \ldots, a_n$ kaudu, kusjuures $b_0 = a_0$. Sealjuures, vastupidi, avalduvad kõik kordajad a_i omakorda kordajate $b_0, b_1, \ldots, b_n$ lineaarsete homogeensete funktsioonidena. Tõepoolest, kordajate võrdlemine annab seosed

$$
\begin{aligned}
a_0 &= b_0, \\
a_1 &= b_1 - b_0\sigma_1^{(n)}, \\
a_2 &= b_2 - b_1\sigma_1^{(n-1)} + b_0\sigma_2^{(n)}, \\
a_3 &= b_3 - b_2\sigma_1^{(n-2)} + b_1\sigma_2^{(n-1)} - b_0\sigma_3^{(n)}, \\
&\text{- -} \\
a_n &= b_n - b_{n-1}\sigma_1^{(1)} + b_{n-2}\sigma_2^{(2)} - \ldots + (-1)^n b_0\sigma_n^{(n)},
\end{aligned}
$$

kus

$$
\sigma_j^{(k)} = \sum_{1 \le i_1 < \ldots < i_j \le k} x_{i_1} x_{i_2} \cdots x_{i_j}.
$$

Tõestame, et $b_i \vdots p$, s.t. $b_i \equiv 0 \pmod p$ $(i = n, n-1, n-2, \ldots, 1, 0)$. 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 4.29 (Wilson). Naturaalarv $p \neq 1$ on algarv parajasti 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 kõik kordajad on kongruentsed nulliga. Eriti on kongruentne nulliga vabaliige, s.o.

$$(p-1)! + 1 \equiv 0 \pmod{p}.$$

Piisavus. Kehtigu kongruents

$$(p-1)! \equiv -1 \pmod{p},$$

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.

Teoreetiliselt saab teoreemi abil kindlaks teha, kas antud arv on alg- või kordarv. Praktiliselt 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.

2. Kongruentsid kordarvulise mooduli järgi. Vaatleme n-astme kongruentsi

(7) $$f(x) \equiv 0 \pmod{m}$$

lahendamist, kus mooduli m kanooniline kuju on

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}.$$

Tähistame $p_i^{\alpha_i} = m_i$. Siis $(m_i, m_j) = 1$ ja kongruents (7) on esitatav kujul

(8) $$f(x) \equiv 0 \pmod{m_1 m_2 \ldots m_n}.$$

Teoreem 4.30. Kongruents (8) on ekvivalentne kongruentside süsteemiga

$$
(9)\qquad
\begin{aligned}
&f(x) \equiv 0 \pmod{m_1}\\
&f(x) \equiv 0 \pmod{m_2}\\
&\text{- - - - - - - - -}\\
&f(x) \equiv 0 \pmod{m_n},
\end{aligned}
$$

s.t. nende lahendite hulgad ühtivad.

Tõestus. Kui x on süsteemi (9) lahend, siis teoreemi 4.14 kohaselt on rahuldatud ka kongruents (8). Vastupidi, kui x on kongruentsi (8) lahend, siis teoreemi 4.15 tõttu rahuldab x süsteemi (9) kõiki kongruentse. Teoreem on tõestatud.

Eeldades, et oleme leidnud süsteemi (9) üksikute kongruentside lahendid, avaldame süsteemi (9) ja sellega ka kongruentsi (8) lahendid. Olgu süsteemi (9) esimese kongruentsi lahenditeks

$$x \equiv x_1^{(1)}, x_1^{(2)}, \dots, x_1^{(k_2)} \pmod{m_1},$$

- -

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

$$
(10)\qquad
\begin{aligned}
&x \equiv x_1^{(i_1)} \pmod{m_1}\\
&x \equiv x_2^{(i_2)} \pmod{m_2}\\
&\text{- - - - - - - - -}\\
&x \equiv x_n^{(i_n)} \pmod{m_n},
\end{aligned}
$$

mille lahend ühtib süsteemi (9) ja seega ka kongruentsi (8) ühe lahendiga. Teoreemi 4.26 kohaselt on nimetatud lahendiks

$$x \equiv M_1M_1' x_1^{(i_1)} + \ldots + M_nM_n' x_n^{(i_n)} \pmod{m}, \tag{11}$$

kus $M_im_i = m$ ja $M_iM_i' \equiv 1 \pmod{m_i}$.

Teeme kindlaks kongruentsi (8) 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 $k > 1$, 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

$$M_1M_1'x_1^{(i_1)} + \ldots + M_nM_n' x_n^{(i_n)} \equiv$$
$$\equiv M_1M_1' x_1^{(j_1)} + \ldots + M_nM_n' x_n^{(j_n)} \pmod{m}.$$

Teoreemi 4.15 tõttu kehtib see kongruents ka mooduli m_1 järgi. Arvestades aga, et $M_i \equiv 0 \pmod{m_1}$, kui $i > 1$, saame

$$M_1M_1' x_1^{(i_1)} \equiv M_1M_1' x_1^{(j_1)} \pmod{m_1}$$

ja $M_1M_1' \equiv 1 \pmod{m_1}$ tõttu

$$x_1^{(i_1)} \equiv x_1^{(j_1)} \pmod{m_1},$$

mis on vastuolus eeldusega.

3. <u>Kongruents algarvu astme järgi</u>. Nagu nägime, taandub kongruentsi lahendamine mistahes mooduli m järgi kongruentside

(12) $$f(x) \equiv 0 \pmod{p^{\alpha}}$$

lahendamisele. Kongruentsi (12) lahendamiseks lähtume kongruentsist

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

Iga x, mis rahuldab kongruentsi (12), rahuldab ka kongruentsi (13), vastupidine üldiselt ei kehti.

Leiame näiteks proovimise teel kongruentsi (13) kõik lahendid. Olgu kongruentsi (13) üheks lahendiks

$$x \equiv x_1 \pmod{p},$$

s.t. $x = x_1 + pt$ rahuldab kongruentsi (13) iga täisarvu t korral. Asendame $x = x_1 + pt$ kongruentsis

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

ja lahendame saadud kongruentsi

(15) $$f(x_1 + pt) \equiv 0 \pmod{p^2}$$

t suhtes. $f(x_1 + pt)$ on t suhtes täisarvuliste kordajatega polünoom. Arendades ta Taylori ritta kohal x_1 saame kongruentsi (15) 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

(16) $$f(x_1) + f'(x_1)pt \equiv 0 \pmod{p^2}.$$

Et $x \equiv x_1 \pmod{p}$ on kongruentsi (13) lahend, siis $f(x_1) \vdots p$. Seega jagades kongruentsi (16) mõlemaid pooli ja moodulit ühise teguriga p saame (16)-ga ekvivalentse kongruentsi

(17) $$\frac{f(x_1)}{p} + f'(x_1)t \equiv 0 \pmod{p}.$$

Eeldame, et

$$f'(x_1) \not\equiv 0 \pmod{p}.$$

Siis $(f'(x_1), p) = 1$ ja lineaarkongruentsil (17) on parajasti üks lahend. Olgu lahendiks

$$t \equiv t_1 \pmod{p} \quad \text{ehk} \quad t = t_1 + ps.$$

Siis kongruentsi (13) rahuldavatest arvudest $x = x_1 + pt$ rahuldavad kongruentsi (14) iga s korral arvud $x = x_1 + p(t_1 + ps) = x_2 + p^2 s$, kus $x_2 = x_1 + pt_1$.

Edasi vaatleme juba kongruentsi

$$f(x) \equiv 0 \pmod{p^3}. \tag{18}$$

Selle lahendamiseks tuleb leida s väärtused, mis rahuldavad kongruentsi

$$f(x_2 + p^2 s) \equiv 0 \pmod{p^3}.$$

Taylori valemi abil saame nagu ennegi viimase kongruentsi asendada ekvivalentse kongruentsiga

$$f(x_2) + f'(x_2)p^2 s \equiv 0 \pmod{p^3}. \tag{19}$$

Et x_2 on kongruentsi (14) lahend, siis $f(x_2) \vdots p^2$ ja kongruentsi (19) saame asendada omakorda ekvivalentse kongruentsiga

$$\frac{f(x_2)}{p^2} + f'(x_2)s \equiv 0 \pmod{p}. \tag{20}$$

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 (20) s suhtes üheselt lahenduv. Olgu selle lahendiks $s \equiv s_1 \pmod{p}$ ehk $s = s_1 + pu$. Siis kongruentsi (18) rahuldavad iga u korral x väärtused

$$x = x_2 + p^2(s_1 + pu) = x_3 + p^3 u,$$

s.t. kongruentsi (18) lahendeiks on

$$x \equiv x_3 \pmod{p^3},$$

kus $x_3 = x_2 + p^2 s_1$. Nii jätkates saame kongruentsi (12) lahendi.

Eelnevast mõttekäigust järeldub, et kui kongruentsil (13) on k lahendit mod p ja iga lahendi x_1 korral $f'(x_1) \not\equiv 0 \pmod{p}$, siis ka kongruentsil (12) on k lahendit.

Näide 2. 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 $f'(x) = 3x + 2x$ 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 (17) 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 (20) 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

$$x \equiv 44 \pmod{343}.$$

Ülesandeid.

58. Asendada kongruents

$$x^{10}+x^8+x^7-x^4-x^2+4x-3 \equiv 0 \pmod 7$$

ekvivalentse madalama astme kongruentsiga ja seejärel lahendada.

59. Lahendada kongruents

$$x^5+x^4+7x^3+6x^2+5x+1 \equiv 0 \pmod{420}.$$

60. Lahendada kongruents

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

61. Lahendada kongruents

$$x^3+x+3 \equiv 0 \pmod{125}.$$

62. Lahendada kongruents

$$x^3+x^2+x+1 \equiv 0 \pmod{2^2.3^3.5^2}.$$

§ 7. RUUTKONGRUENTSID.

1. Üldised teoreemid. 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 n-astme mittejäägiks. Kui n = 2, siis räägi-

me ruutjäägist ja mitteruutjäägist; kui $n = 3$, siis kuupjäägist ja mittekuupjäägist.

Käesolevas paragrahvis vaatleme juhtu, kus $n = 2$. Siinjuures eeldame, et moodul on paaritu algarv (juhtu, kus $p = 2$, vaatleme käesoleva paragrahvi viimases punktis). Seega käsitleme kongruentse

(1) $$x^2 \equiv a \pmod{p}, \quad (a,p) = 1, \quad p \neq 2.$$

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 oluliselt erinevaid ruutkongruentse 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 4.31. 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 4.28 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 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 4.32. Taandatud jääkide süsteemis paaritu algarvulise mooduli p järgi on olemas $\frac{p-1}{2}$ ruutjääki ja $\frac{p-1}{2}$ mitteruutjääki. Ruutjäägid on kongruentsed modulo p arvudega

$$1^2, 2^2, \ldots, (\tfrac{p-1}{2})^2. \tag{2}$$

Tõestus. Taandatud jääkide süsteemis on ruutjääkideks parajasti need arvud, mis on kongruentsed arvude

$$-\tfrac{p-1}{2}, \ldots, -2, -1, 1, 2, \ldots, \tfrac{p-1}{2} \tag{3}$$

ruutudega, s.o. arvudega (2). Niisiis tarvitseb näidata, et arvude (2) seas pole kongruentseid. Kui oleks

$$k^2 \equiv l^2 \pmod{p}, \quad 0 < k < l \leq \tfrac{p-1}{2},$$

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 4.33. 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

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

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

(6) $$x^{p-1} = a^{\frac{p-1}{2}} \pmod{p}.$$

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

(7) $$z^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p},$$

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 $r_1, r_2, \dots, r_\alpha$ $(\alpha = \frac{p-1}{2})$ jaoks leiduvad taandatud jääkide süsteemis arvud $x_1, x_2, \dots, x_\alpha$, nii et kehtivad kongruentsid

$$x_1^2 \equiv r_1 \pmod p,$$
$$x_2^2 \equiv r_2 \pmod p,$$
$$\dots\dots\dots$$
$$x_\alpha^2 \equiv r_\alpha \pmod p.$$

Tõstes kõik kongruentsid astmesse $\alpha = \frac{p-1}{2}$ ja arvestades Euleri teoreemi, saame

$$r_1^\alpha \equiv x_1^{p-1} \equiv 1 \pmod p,$$
$$r_2^\alpha \equiv x_2^{p-1} \equiv 1 \pmod p,$$
$$\dots\dots\dots\dots$$
$$r_\alpha^\alpha \equiv x^{p-1} \equiv 1 \pmod p$$

ehk

$$r_1^\alpha - 1 \equiv 0 \pmod p,$$
$$r_2^\alpha - 1 \equiv 0 \pmod p,$$
$$\dots\dots\dots\dots$$
$$r_\alpha^\alpha - 1 \equiv 0 \pmod p.$$

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.

2. Legendre'i sümbol. Järgnevas tuletame praktilise võtte ruutjääkide leidmiseks suurte moodulite korral (teo-

reemi 4.33 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. Defineerime kõigepealt nn. Legendre'i sümboli.

Legendre'i sümbol $\left(\frac{a}{p}\right)$ defineeritakse juhul, kui p on algarv ja (a,p) = 1. Sümbolit $\left(\frac{a}{p}\right)$ loetakse "a p suhtes".

Definitsioon: $\left(\frac{a}{p}\right) = 1$, kui a on ruutjääk; $\left(\frac{a}{p}\right) = -1$, kui a on mitteruutjääk.

Vaatleme Legendre'i sümboli omadusi.

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

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) $\left(\frac{a_1 a_2 \cdots a_n}{p}\right) = \left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right)\cdots\left(\frac{a_n}{p}\right)$,

s.t. Legendre'i sümbol on tugevalt multiplikatiivne.

Tõestuseks kasutame omadust 1

$$\left(\frac{a_1a_2\dots a_n}{p}\right) \equiv (a_1a_2\dots a_n)^{\alpha} = a_1^{\alpha}\, a_2^{\alpha} \dots a_n^{\alpha} \equiv \left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right)\dots$$
$$\dots\left(\frac{a_n}{p}\right) \pmod p.$$

Kongruentsist järeldub võrdus järgmise lemma põhjal:

Kui $\varepsilon \equiv \eta \pmod p$, $p \neq 2$ ja $|\varepsilon| = |\eta| = 1$, siis $\varepsilon = \eta$.

Lemma ise on aga lihtsalt tõestatav. Tõepoolest, kui $\varepsilon \neq \eta$, siis kongruents $\varepsilon \equiv \eta \pmod p$ tähendab, et $1 \equiv -1 \pmod p$ ehk $2 \equiv 0 \pmod p$, mis on võimatu, kui $p \neq 2$.

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

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

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

3. <u>Tarvilik ja piisav tingimus selleks, et arv -1 oleks ruutjääk.</u> Küsimusele, mille püstitasime eelmise punkti 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.

4. <u>Gaussi lemma</u>. Uurime edasi kongruentsi

$$x^2 \equiv a \pmod{p}, \quad (a,p) = 1,$$

lahenduvust sõltuvalt moodulist p.

Koostame kongruentsid modulo p:

$$\begin{aligned} a \cdot 1 &\equiv \varepsilon_1 r_1 \\ a \cdot 2 &\equiv \varepsilon_2 r_2 \\ a \cdot 3 &\equiv \varepsilon_3 r_3 \\ &\cdots\cdots \\ a \cdot \alpha &\equiv \varepsilon_\alpha r_\alpha \qquad (\alpha = \tfrac{p-1}{2}), \end{aligned} \tag{6}$$

kus paremad pooled $\varepsilon_i r_i$ on absoluutväärtuselt vähimad taan-

datud jääkide süsteemi elemendid, $\varepsilon_i = \pm 1$ olenevalt nimetatud jäägi märgist,

$$0 < r_i \leqslant \frac{p-1}{2}.$$

Näitame, et jääkide r_i seas ei saa olla võrdseid arve. Kui oleks

$$r_i = r_j,$$

siis kongruentsidest

$$a \cdot i \equiv \varepsilon_i r_i \pmod{p},$$

$$a \cdot j \equiv \varepsilon_j r_j = \varepsilon_j r_i \pmod{p}$$

saaksime

$$\varepsilon_i a \cdot i \equiv r_i \pmod{p},$$

$$\varepsilon_j a \cdot j \equiv r_i \pmod{p}$$

ehk

$$\varepsilon_i \cdot ia \equiv \varepsilon_j \cdot ja \pmod{p} \quad \text{ehk} \quad \varepsilon_i \cdot i \equiv \varepsilon_j \cdot j \pmod{p}$$

Et $\varepsilon_i = \pm 1$ ja $\varepsilon_j = \pm 1$, siis peaks $\pm i \pm j$ 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 (6) omavahel läbi. Saame

$$a^\alpha \cdot \alpha! \equiv E \cdot \alpha! \pmod{p},$$

kus

$$E = \varepsilon_1 \varepsilon_2 \ldots \varepsilon_\alpha = \pm 1$$

Siit

$$a^\alpha \equiv E \pmod{p}$$

ehk

$$\left(\frac{a}{p}\right) \equiv E \pmod{p}.$$

Punktis 2 esitatud lemma põhjal kehtib võrdus

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

Viimast tulemust nimetatakse Gaussi lemmaks.

Anname saadud avaldisele E teise kuju. Selleks lähtume seosest

$$\frac{ax}{p} = \left[\frac{ax}{p}\right] + \left\{\frac{ax}{p}\right\} \quad (x = 1, 2, \ldots, \alpha).$$

Korrutame seda kahega ja võtame täisosa

$$\left[\frac{2ax}{p}\right] = \left[2\left[\frac{ax}{p}\right] + 2\left\{\frac{ax}{p}\right\}\right] = 2\left[\frac{ax}{p}\right] + \left[2\left\{\frac{ax}{p}\right\}\right].$$

Kui $\varepsilon_x = 1$, s.t. kui ax vähim positiivne jääk (mod p) on väiksem kui $\frac{1}{2}$ p, siis tulemus on paarisarv (sest $\left\{\frac{ax}{p}\right\} < \frac{1}{2}$ ja $\left[2\left\{\frac{ax}{p}\right\}\right] = 0$). Seega võib kirjutada

$$\varepsilon_x = (-1)^{\left[\frac{2ax}{p}\right]}.$$

Kui $\varepsilon_x = -1$, siis ax vähim positiivne jääk mod p on suurem kui $\frac{1}{2}$ p ja $\left[\frac{2ax}{p}\right]$ on paaritu arv (sest $\left\{\frac{ax}{p}\right\} > \frac{1}{2}$ ja $\left[2\left\{\frac{ax}{p}\right\}\right] = 1$). Ka antud juhul

$$\varepsilon_x = (-1)^{\left[\frac{2ax}{p}\right]}.$$

Seega Gaussi lemmast saame

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{x=1}^{\alpha}\left[\frac{2ax}{p}\right]} \quad (\alpha = \frac{p-1}{2}). \tag{7}$$

5. Tarvilik ja piisav tingimus selleks, et arv 2 oleks ruutjääk. Olgu a paaritu arv, siis a+p on paarisarv. Arvutame valemi (7) põhjal

$$\left(\frac{2a}{p}\right) = \left(\frac{2a+2p}{p}\right) = \left(\frac{4 \cdot \frac{a+p}{2}}{p}\right) = \left(\frac{\frac{a+p}{2}}{p}\right) = (-1)^{\sum_{x=1}^{\frac{p}{2}} \left[\frac{(a+p)x}{p}\right]} =$$

$$= (-1)^{\sum_{x=1}^{\frac{p}{2}} \left[\frac{ax}{p}\right] + \sum_{x=1}^{\frac{p}{2}} x}$$

ehk teisiti

$$\left(\frac{2}{p}\right)\left(\frac{a}{p}\right) = (-1)^{\sum_{x=1}^{\frac{p}{2}} \left[\frac{ax}{p}\right] + \frac{p^2-1}{8}} . \tag{8}$$

Kui valemis (8) võtta a = 1, siis saame

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} . \tag{9}$$

Nüüd võime otsustada, millise mooduli p korral on kongruents

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

lahenduv, millise korral mitte. Näiteks mooduli 13 puhul

$$\left(\frac{2}{13}\right) = (-1)^{\frac{168}{8}} = (-1)^{21} = -1,$$

mistõttu 2 ei ole mod 13 ruutjääk. Seega kongruents $x^2 \equiv 2 \pmod{13}$ pole lahenduv.

Selleks, et kohe 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

$$\left(\frac{2}{8n \pm 1}\right) = (-1)^{\frac{(8n \pm 1)^2 - 1}{8}} = (-1)^{8n^2 \pm 2n} = 1,$$

$$\left(\frac{2}{8n \pm 1}\right) = (-1)^{\frac{(8n \pm 3)^2 - 1}{8}} = (-1)^{8n^2 \pm 6n + 1} = -1.$$

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.

6. Legendre'i sümboli pööratavus. Jagades võrduse (8) võrdusega (9) saame paaritu arvu a jaoks valemi

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{x=1}^{\alpha} \left[\frac{ax}{p}\right]}, \quad \text{kus} \quad \alpha = \frac{p-1}{2}. \tag{10}$$

Olgu q paaritu algarv. Siis saame valemist (10) järgmised seosed:

$$\left(\frac{q}{p}\right) = (-1)^{\sum_{x=1}^{\alpha}\left[\frac{qx}{p}\right]}, \quad \alpha = \frac{p-1}{2}$$

$$\left(\frac{p}{q}\right) = (-1)^{\sum_{y=1}^{\beta}\left[\frac{py}{q}\right]}, \quad \beta = \frac{q-1}{2}.$$

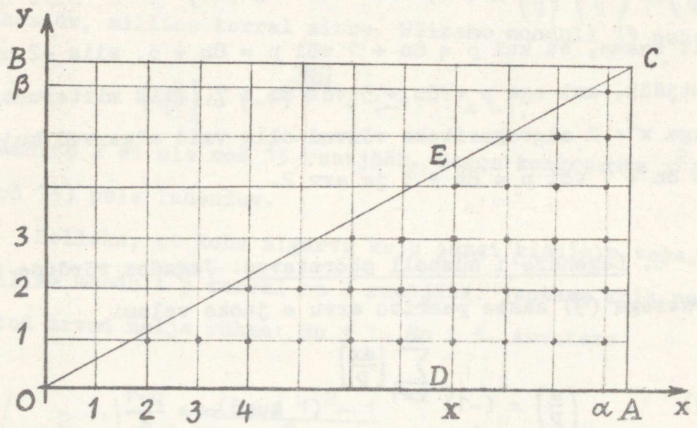
Korrutame saadud võrdused

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\sum_{x=1}^{\alpha}\left[\frac{qx}{p}\right] + \sum_{y=1}^{\beta}\left[\frac{py}{q}\right]} \tag{11}$$

ja tõestame, et

$$\sum_{x=1}^{\alpha}\left[\frac{qx}{p}\right] + \sum_{y=1}^{\beta}\left[\frac{py}{q}\right] = \alpha\beta = \frac{p-1}{2} \cdot \frac{q-1}{2}. \tag{12}$$

Selleks märgime xy-tasandil ära koordinaatide algus-



punkti 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 $\frac{qx}{p}$ võrdub sirge ordinaadiga kohal x, täisosa $\left[\frac{qx}{p}\right]$ aga lõigul DE asuvate sisemiste täisarvuliste koordinaatidega punktide arvuga. Seega võrdub summa

$$\sum_{x=1}^{\alpha} \left[\frac{qx}{p}\right] = \left[\frac{q}{p}\right] + \left[\frac{2q}{p}\right] + \left[\frac{3q}{p}\right] + \ldots + \left[\frac{\alpha q}{p}\right]$$

kolmnurga OAC täisarvuliste koordinaatidega sisemiste punktide arvuga.

Vaadeldes samal viisil sirget $x = \frac{py}{q}$ veendume, et summa $\sum_{x=1}^{\beta} \left[\frac{py}{q}\right]$ võrdub täisarvuliste koordinaatidega sisemiste punktide arvuga kolmnurgas OBC.

Kuna lõigul OC ei leidu täisarvuliste koordinaatidega sisemisi punkte, siis võrdub summa

$$\sum_{x=1}^{\alpha} \left[\frac{qx}{p}\right] + \sum_{y=1}^{\beta} \left[\frac{py}{q}\right]$$

ristküliku OACB täisarvuliste koordinaatidega sisemiste punktide arvuga. Teiselt poolt on aga ristküliku OACB täisarvuliste koordinaatidega sisemiste punktide arv $\alpha \cdot \beta$. Seega kehtib võrdus (12). Viimast arvestades saame valemi

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\,\frac{q-1}{2}}. \tag{13}$$

Korrutades võrduse mõlemaid pooli teguriga $\left(\frac{p}{q}\right)$, saame valemile praktiliseks rakendamiseks sobiva kuju

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

Valem (14) on tuntud ruutjääkide pööratavuse lause nime all. Pööratavuse lause koos Legendre'i sümboli teiste omadustega võimaldab sümboli väärtust arvutada iga algarvulise 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.

Arvutame Legendre'i sümboli väärtuse:

$$\left(\frac{265}{353}\right) = \left(\frac{5}{353}\right)\cdot\left(\frac{53}{353}\right);\ \left(\frac{5}{353}\right) = \left(\frac{353}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{2}{3}\right) = -1;$$

$$\left(\frac{53}{353}\right) = \left(\frac{353}{5}\right) = \left(\frac{35}{53}\right) = \left(\frac{5}{53}\right)\cdot\left(\frac{7}{53}\right);$$

$$\left(\frac{5}{53}\right) = \left(\frac{53}{5}\right) = \left(\frac{3}{5}\right) = -1;\ \left(\frac{7}{53}\right) = \left(\frac{53}{7}\right) = \left(\frac{4}{7}\right) = 1.$$

Seega $\left(\frac{265}{353}\right) = 1$ ja kongruents on lahenduv.

7. 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

$$\left(\frac{a}{P}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_n}\right). \tag{15}$$

Märgime, et Jacobi sümbol ei ole seotud ruutkongruentsiga $x^2 \equiv a \pmod{P}$, vaid on loodud, nagu ülalpool märgitud, ruutkongruentsi lahenduvuse küsimuse lihtsustamiseks algarvulise mooduli korral.

Jacobi sümbolil on formaalselt samad omadused mis Legendre'i sümbolil. Järgnevas vaatlemegi Jacobi sümboli oma-

dusi.

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.(Veenduda!)

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

Tõestus. Definitsiooni (15) ja Legendre'i sümboli vastava omaduse tõttu saame

$$\left(\frac{-1}{P}\right) = \left(\frac{-1}{p_1}\right)\left(\frac{-1}{p_2}\right)\cdots\left(\frac{-1}{p_n}\right) = (-1)^{\frac{p_1-1}{2}} \cdots (-1)^{\frac{p_n-1}{2}} =$$

$$= (-1)^{\sum_{i=1}^{n}\frac{p_i-1}{2}}.$$

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

$$\frac{P-1}{2} = \frac{p_1p_2\cdots p_n - 1}{2} =$$

$$= \frac{\left(1 + \frac{p_1-1}{2}\cdot 2\right)\left(1 + \frac{p_2-1}{2}\cdot 2\right)\cdots\left(1 + \frac{p_n-1}{2}\cdot 2\right) - 1}{2}.$$

Kasutades valemit

$$(x + 2a_1)(x + 2a_2)\cdots(x + 2a_n) = x^n + 2(a_1 + \ldots + a_n)x^{n-1} +$$

$$+ 4(a_1a_2 + a_1a_3 + \ldots)x^{n-2} + 8(a_1a_2a_3 + \ldots)x^{n-3} + \ldots,$$

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

$$\left(\frac{-1}{P}\right) = (-1)^{\frac{P-1}{2} - 2N} = (-1)^{\frac{P-1}{2}}.$$

$\left(\frac{-1}{P}\right)$ 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) $\left(\frac{2}{P}\right) = (-1)^{\frac{p^2-1}{8}}$.

Tõestus. Lähtume seosest

$$\left(\frac{2}{P}\right) = \left(\frac{2}{p_1}\right)\left(\frac{2}{p_2}\right) \ldots \left(\frac{2}{p_n}\right) = (-1)^{\sum_{i=1}^{n} \frac{p_i^2-1}{8}}.$$

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

$$\frac{p^2-1}{8} = \frac{p_1^2 p_2^2 \ldots p_n^2 - 1}{8} =$$

$$= \frac{\left(1 + 8\,\frac{p_1^2-1}{2}\right)\left(1 + 8\,\frac{p_2^2-1}{8}\right) \ldots \left(1 + 8\,\frac{p_n^2-1}{8}\right) - 1}{8}$$

saame

$$\frac{p^2-1}{8} = \sum_{i=1}^{n} \frac{p_i^2-1}{8} + 2N,$$

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 siis

$$\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}} \left(\frac{P}{Q}\right)$$

(Jacobi sümboli pööratavuse lause).

Tõestus. Olgu $P = p_1p_2\cdots p_n$, $Q = q_1q_2\cdots q_m$. 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

$$\left(\frac{Q}{P}\right) = \left(\frac{Q}{p_1}\right)\left(\frac{Q}{p_2}\right)\cdots\left(\frac{Q}{p_n}\right) = \left(\frac{q_1}{p_1}\right)\left(\frac{q_2}{p_1}\right)\cdots\left(\frac{q_m}{p_1}\right) \times$$

$$\times \left(\frac{q_1}{p_2}\right)\left(\frac{q_2}{p_2}\right)\cdots\left(\frac{q_m}{p_2}\right) \times \cdots \times \left(\frac{q_1}{p_n}\right)\left(\frac{q_2}{p_n}\right)\cdots\left(\frac{q_m}{p_n}\right) =$$

$$= (-1)^{\sum_{i=1}^{n}\frac{p_i-1}{2}\ \sum_{j=1}^{n}\frac{q_j-1}{2}} \left(\frac{p_1}{q_1}\right)\left(\frac{p_1}{q_2}\right)\cdots\left(\frac{p_1}{q_m}\right) \times$$

$$\times \left(\frac{p_2}{q_1}\right)\left(\frac{p_2}{q_2}\right)\cdots\left(\frac{p_2}{q_m}\right)\cdots\left(\frac{p_n}{q_1}\right)\left(\frac{p_n}{q_2}\right)\cdots\left(\frac{p_n}{q_m}\right) =$$

$$= (-1)^{\sum_{i=1}^{n}\frac{p_i-1}{2}\ \sum_{j=1}^{n}\frac{q_j-1}{2}} \left(\frac{P}{Q}\right).$$

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. Sealjuures 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.

8. 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

$$x \equiv \pm a^{m+1} \pmod{p} \quad \text{ehk} \quad x \equiv a^{\frac{p+1}{4}} \pmod{p}.$$

Näide 4. 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 kongruentsid 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 $p = 8m + 1$, $\left(\frac{a}{p}\right) = 1$. 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 $k \geqslant 3$ 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

$$N^{2^{k-1}h} \equiv -1 \pmod{p}. \tag{16}$$

Tegelikult võib mõlemad juhud kokku võtta kirjutades

$$a^{2^{k-2}h}\, N^{s2^{k-1}h} \equiv +1 \pmod{p},$$

kus esimesel juhul $s = 0$ (või mistahes teine paarisarv), teisel juhul aga $s = 1$ (või mistahes teine paaritu arv).

Viimasest kongruentsist saame

$$a^{2^{k-3}h} N^{s_2 2^{k-2}} \equiv \pm 1 \pmod{p}, \quad s_2 = sh. \tag{17}$$

Juhul, kui esineb +, võime kongruentsi otsekohe asendada madalama astme kongruentsiga; kui esineb -, korrutame saadud kongruentsi kongruentsiga (16), mida võib esitada kujul

$$N^{2^{k-2}u} \equiv -1 \pmod{p}, \quad \text{kus} \quad u = 2h.$$

Seega kongruentsist (17) 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 paremale a saamiseks.

9. <u>Ruutkongruentsid kordarvulise mooduli järgi</u>. Käesolevas punktis järgime õpikus [3] toodud käsitlust. Alustame ruutkongruentsist

$$x^2 \equiv a \pmod{p^\alpha}, \quad \alpha > 1, \quad (a,p) = 1, \tag{18}$$

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 paragrahvi üldistest tulemustest järeldub, et kongruentsil (18) 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

(19) $$x^2 \equiv a \pmod{2^\alpha}, \quad \alpha \geqslant 1, \quad (a,2) = 1.$$

Siin $f'(x_1) = 2x_1 \equiv 0 \pmod{2}$ ja eelmise paragrahvi 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 a võib 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 4.15 põhjal) sama kongruentsi ka mooduli 8 järgi. Kuid siis peab lahenduvuseks olema täidetud tingimus

$$a \equiv 1 \pmod 8. \tag{20}$$

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 (19) 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 (19) lahend peab olema paaritu, saame siit

$$\text{kas } \varkappa - 1 = 0 \text{ või } \lambda - 1 = 0.$$

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 $x \equiv b + 2^{\alpha-1} \pmod 2$. Esimene jäägiklass rahuldab kongruentsi (19) 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 (19) neli erinevat lahendit

$$x \equiv \pm b, \quad \pm(b + 2^{\alpha-1}) \pmod{2^{\alpha}}.$$

Tõestame lõpuks, et tingimusel (20) on kongruents (19) lahenduv, s.t. et tingimus (20) on kongruentsi (19) lahenduvuseks piisav. Tingimuse (20) piisavus on teada juhul, kui $\alpha = 3$. Edasi kasutame täieliku induktsiooni meetodit. Olgu tingimus (20) täidetud ja kongruents

(21) $$x^2 \equiv a \pmod{2^{\alpha-1}} \quad (\alpha \geqslant 4)$$

lahenduv. Nagu eespool näidatud, on kongruentsil (21) siis neli lahendit

$$x \equiv \pm c, \quad \pm(c + 2^{\alpha-2}) \pmod{2^{\alpha-1}},$$

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 paarisarv, siis $c^2 \equiv a \pmod{2^{\alpha}}$, s.t. jäägiklassid $x \equiv \pm c \pmod{2^{\alpha}}$ on kongruentsi (18) lahenditeks. Kui k on paaritu arv, siis arvutame kongruentsi (21) 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 (21) lahend, siis k + c on paarisarv ja

$$(c + 2^{\alpha-2})^2 \equiv a \pmod{2^{\alpha}}.$$

Niisiis ka sellel juhul on kongruents (19) lahenduv, kusjuures tema lahenditeks on

$$x \equiv \pm(c + 2^{\alpha-2}) \pmod{2^{\alpha}}.$$

Tingimuse (20) piisavus kongruentsi (19) lahenduvuseks on näidatud. Ühtlasi näeme, et kongruentsi (21) 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 (19) lahenditeks mod 2^{α}. Tähistame nimetatud lahendid $x \equiv \pm b \pmod{2^{\alpha}}$. Siis ülejäänud on

$x \equiv \pm(b + 2^{\alpha-1}) \pmod{2^{\alpha}}$.

Saadud tulemused võtame kokku järgmiseks teoreemiks.

Teoreem 4.34. Kongruentsil

(22) $$x^2 \equiv a \pmod{2^{\alpha}}$$

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 $a \equiv 1 \pmod 8$. Lahenduval juhul leidub kongruentsi (22) lahendite hulgas ka kongruentsi $x^2 \equiv a \pmod{2^{\alpha+1}}$ lahendeid, ülejäänud lahendid avalduvad aga viimaste kaudu.

Näide 5. 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

$$x^2 \equiv a \pmod{m}, \tag{23}$$

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:

$$x^2 \equiv a \pmod{2^{\alpha}},$$
$$x^2 \equiv a \pmod{p_1^{\alpha_1}},$$
$$- - - - - - - - - -$$
$$x^2 \equiv a \pmod{p_n^{\alpha_n}}.$$

Kui süsteemi üksikute kongruentside lahendite arv on vastavalt k, k_1, k_2, ... , k_n, siis teatavasti on süsteemil ja lähtekongruentsil modulo m arvult $kk_1k_2 \dots k_n$ lahendit. Kui süsteemis mõni kongruents osutub mittelahenduvaks (vastav $k_i = 0$), siis ka esialgsel kongruentsil pole lahendit. Niisiis on kongruentsi (23) lahenduvuse tarvilikud ja piisavad tingimused kokkuvõetavad järgmiseks teoreemiks.

Teoreem 4.36. Selleks, et kongruents (23) oleks lahenduv, on tarvilik ja piisav, et juhul, kui $\alpha = 0$ või $\alpha = 1$, oleks

(24) $\left(\frac{a}{p_1}\right) = 1, \left(\frac{a}{p_2}\right) = 1, \ldots, \left(\frac{a}{p_n}\right) = 1;$

juhul kui $\alpha = 2$, oleksid täidetud tingimused (24) ja tingimus $a \equiv 1 \pmod 4$; juhul kui $\alpha \geqslant 3$, oleksid täidetud tingimused (24) 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. [3]).

Ülesandeid.

63. Kontrollida kongruentside a) $x^2 \equiv 3 \pmod{19}$ ja b) $x^2 \equiv 17 \pmod{18}$ lahenduvust Gaussi lemma põhjal ja seejärel Legendre'i sümboli abil.

64. Kirjutada välja arvude x^2+1, x^2+2, x^2-2 jagajad $x = 1, 2, \ldots, 10$ korral ja jälgida nende kuju.

65. Kasutades Legendre'i sümbolit leida algarvu p üldkuju, mille korral arv 3 on mitteruutjääk.

66. Millise üldkujuga võivad olla arvu x^2-3 algarvulised jagajad (kasutada ülesande 65 tulemusi)?

67. Teha kindlaks, kas järgmised ruutkongruentsid on lahenduvad:

a) $x^2 \equiv 111 \pmod{271}$,

b) $x^2 \equiv 343 \pmod{677}$,

c) $x^2 \equiv 589 \pmod{1283}$.

68. Arvutada Legendre'i sümbolite a) $\left(\frac{2115}{6269}\right)$, b) $\left(\frac{93}{131}\right)$, c) $\frac{116}{379}$ väärtused, kasutades 1) ainult Legendre'i sümboli omadusi ja 2) ka Jacobi sümbolit.

69. Arvutada Jacobi sümboli $\left(\frac{521}{825}\right)$ väärtus.

70. Lahendada ruutkongruentsid

a) $x^2 \equiv 11 \pmod{59}$,

b) $x^2 \equiv 30 \pmod{37}$,

c) $x^2 \equiv 11 \pmod{97}$.

71. Lahendada ruutkongruentsid

a) $x^2 \equiv 46 \pmod{105}$,

b) $x^2 \equiv 17 \pmod{104}$,

c) $x^2 \equiv 19 \pmod{90}$.

V. ALGJUURED JA INDEKSID.

§ 1. ALGJUURED.

1. Algjuur ja astendaja, millele antud arv kuulub. Olgu (a, m) = 1. Siis Euleri teoreemi kohaselt on eksponentkongruentsi

(1) $$a^x \equiv 1 \pmod{m}$$

üheks lahendiks $x = \varphi(m)$. Lahendiks on samuti $n\varphi(m)$, kuid võib juhtuda, et kongruentsi rahuldab ka mõni arvust $\varphi(m)$ väiksem arv.

Kui $x = \varphi(m)$ on kongruentsi (1) vähim naturaalarvuline lahend, siis arvu a nimetatakse algjuureks modulo m.

Ilmselt rahuldab vähim naturaalarvuline lahend tingimust $\delta \leq \varphi(m)$. Kongruentsi (1) vähimat naturaalarvulist lahendit nimetatakse astendajaks, millele a kuulub modulo m. Seega $\varphi(m)$ on astendaja, millele kuulub algjuur modulo m. Teisiti, arvu g, mis kuulub astendajale $\varphi(m)$, nimetatakse algjuureks modulo m.

Leiame näiteks algjuured modulo 7 (kui neid leidub) ja teeme kindlaks, millisele astendajale kuulub üks või teine arvudest

$$a = 1, 2, 3, 4, 5, 6.$$

Arvutuste tulemused on sobiv esitada tabelina, milles vastavalt vaadeldavatele arvudele a ja $(1 \leq x \leq m-1)$ 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 5.1. Kui $b \equiv a \pmod m$, siis b ja a kuuluvad ühele ja samale astendajale.

Tõestus. Kuulugu a astendajale δ. Siis 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 $a^{\eta} \equiv 1 \pmod m$.

Järeldus. Kui a on algjuur modulo m ja $b \equiv a \pmod m$, siis on algjuur ka b.

Teoreem 5.2. Kui arv a kuulub astendajale $\delta \pmod m$, siis on arvud

$$1,\ a,\ a^2,\ \ldots,\ a^{\delta-1}$$

inkongruentsed modulo m.

Tõestus. Kui oleks $a^i \equiv a^k \pmod m$, kus näiteks $0 \leq k < i < \delta$, siis saaksime

$$a^{i-k} \equiv 1 \pmod m \quad (i - k < \delta),$$

mis on vastuolus sellega, et a kuulub astendajale δ.

Teoreem 5.3. 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

$$(a^\delta)^{q_1} a^{r_1} \equiv (a^\delta)^{q_2} a^{r_2} \quad \text{ehk} \quad a^{r_1} \equiv a^{r_2} \pmod m.$$

Oletame nüüd, et $x \not\equiv y \pmod \delta$, s.t. $r_1 \neq r_2$. Siis teoreemi 5.2 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 võrdust kongruentsiga $(a^\delta)^{q_1} \equiv (a^\delta)^{q_2} \equiv 1 \pmod m$ saamegi (2).

Näide 1. Kas kehtib kongruents

$$2^{53} \equiv 2^{71} \pmod 7?$$

Et 2 kuulub astendajale 3 ja

$$53 \equiv 71 \pmod 3,$$

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 seega

$$\varphi(m) \equiv 0 \pmod \delta.$$

Näiteks mooduli 7 järgi võivad arvud kuuluda vaid astendajatele 1, 2, 3, 6, mis on arvu $\varphi(7) = 6$ jagajateks. Kui m = p on algarv, siis $\varphi(m) = p-1$ ja arv a võib kuuluda vaid astendajale δ, mis on p-1 jagaja.

Esitame mõned näited.

Näide 2. 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 3. 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 4. Olgu m = 15. Siis $\varphi(m) = 8$, kusjuures taandatud jääkide süsteem koosneb järgmistest 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:

x \ 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 $\alpha \geqslant 1$. Meid huvitavad eriti algjuured algarvulise mooduli järgi.

Anname suhteliselt lihtsalt kontrollitava tarviliku ja piisava tingimuse selleks, et arv a oleks algjuur modulo m.

Teoreem 5.4. Kui

$$\varphi(m) = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n},$$

siis selleks, et arv a oleks algjuur modulo m, on tarvilik ja piisav, et kehtiksid järgmised tingimused

$$a^{\frac{\varphi(m)}{p_1}} \not\equiv 1 \pmod{m},$$

$$a^{\frac{\varphi(m)}{p_2}} \not\equiv 1 \pmod{m},$$

- - - - - - - - - - -

$$a^{\frac{\varphi(m)}{p_n}} \not\equiv 1 \pmod{m}.$$

Tõestus. Tarvilikkus. Olgu a algjuur modulo m, s.t.

$$a^{\varphi(m)} \equiv 1 \pmod{m},$$

$$a^{\eta} \not\equiv 1 \pmod{m}, \quad \text{kui } 0 < \eta < \varphi(m).$$

Kui oleks $a^{\frac{\varphi(m)}{p_i}} \equiv 1 \pmod{m}$, siis selletõttu, et $\frac{\varphi(m)}{p_i} < \varphi(m)$, ei oleks a algjuur. Seega kehtivad tingimused (4).

Piisavus. Kehtigu tingimused (4). Oletame, et a ei ole siiski algjuur. Siis ta kuulub mingile astendajale $\delta < \varphi(m)$:

$$a^{\delta} \equiv 1 \pmod{m}.$$

Teoreemi 5.3 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

$$\frac{\varphi(m)}{p_i} = \delta \cdot q$$

ja

$$a^{\frac{\varphi(m)}{p_i}} = a^{\delta q} = (a^{\delta})^{q} \equiv 1 \pmod{m},$$

mis on vastuolus eeldusega.

Teoreem 5.4 võimaldab algjuuri praktiliselt leida.

Näide 5. Olgu m = 31; siis $\varphi(m) = 30 = 2 \cdot 3 \cdot 5$. Ilmselt a = 2 ei saa olla algjuureks modulo 31, sest $2^5 \equiv 1 \pmod{31}$. Juhul a = 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.

2. Algjuurte olemasolu ja arv algarvulise mooduli korral. Järgnevalt näitame, et iga algarvulise mooduli korral leidub algjuuri ja teeme kindlaks viimaste arvu.

Olgu moodul m = p algarv. Siis $\varphi(m) = p-1$.

Teoreem 5.5. Arvu p-1 igale jagajale δ kui astendajale kuulub $\varphi(\delta)$ arvu taandatud jääkide süsteemist modulo p.

Järeldus. Et algjuur on arv, mis kuulub astendajale p-1, siis leidub algarvulise mooduli korral arvult $\varphi(p-1)$ algjuurt, mis on omavahel inkongruentsed.

Teoreemi 5.5 tõestus. 1. Olgu δ arvu p-1 jagaja. Eeldame esialgu täiendavalt, et taandatud jääkide süsteemis modulo p

(5) $\qquad 1, 2, \ldots, p-1$

leidub vähemalt üks arv a, mis kuulub astendajale δ (mod p):

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

Tehtud eeldusel leiame süsteemi (5) ülejäänud elemendid x, mis kuuluvad samale astendajale δ. Selleks lahendame kongruentsi

(6) $\qquad x^{\delta} \equiv 1 \pmod{p}.$

Viimasel kongruentsil on δ lahendit:

(7) $\qquad x \equiv 1, a, a^2, \ldots, a^{\delta-1} \pmod{p},$

kus a on arv, mis eelduse kohaselt kuulub astendajale δ.

Tõepoolest, olgu $x \equiv a^i \pmod{p}$ $(i = 0, 1, \ldots, \delta-1)$; siis $x^{\delta} \equiv (a^i)^{\delta} = (a^{\delta})^i \equiv 1 \pmod{p}$, s.t. jäägiklassid (7) on kõik lahendid, lahendite (7) erinevus üksteisest järeldub aga teoreemist 5.2. Et kongruentsi (6) aste on δ, siis rohkem lahendeid olla ei saa. Saadud lahendid ei tarvitse aga kuuluda kõik astendajale δ, osa neist võib kuuluda ka mõnele väiksemale astendajale.

2. Näitame, et astendajale δ kuulub $\varphi(\delta)$ arvu jadast

$$1, a, a^2, \ldots, a^{\delta-1}.$$

Iga arv kuulub mingile astendajale. Kuulugu arv a^k astendajale h, s.t. h olgu minimaalne naturaalarv, mille korral

(8) $\qquad a^{kh} \equiv 1 \pmod{p}.$

Järelduse 1 põhjal teoreemist 5.3 on aga kongruentsi (8)

kehtivuseks tarvilik ja piisav, et

(9) $$kh \equiv 0 \pmod{\delta}.$$

Kui $(k,\delta) = 1$, siis järeldub siit, et $h \equiv 0 \pmod{\delta}$, ja seega minimaalne naturaalarv, mis seda kongruentsi ja seega ka kongruentsi (8) rahuldab, on $h = \delta$. Seega nende astendajate k korral, mis on δ-ga ühistegurita, kuulub a^k δ-le. Kui aga $(k,\delta) = d > 1$, siis $k = k_1 d$, $\delta = \delta_1 d$, $(k_1,\delta_1) = 1$ ja kongruentsist (9) järeldub, et

$$h \equiv 0 \pmod{\delta_1}.$$

Siis minimaalne naturaalarv h, mis rahuldab kongruentsi (8) on $h = \delta_1$. Sel juhul a^k kuulub astendajale $\delta_1 < \delta$. Seega, kui a kuulub astendajale δ, siis kuuluvad astendajale $\delta \pmod p$ parajasti kõik need arvud hulgast a^k ($k = 0, 1, \ldots, \delta-1$), mille korral $(k,\delta) = 1$. Selliseid arve on $\varphi(\delta)$. Et kõik astmed $1, 2, \ldots a^{\delta-1}$ on üksteise suhtes inkongruentsed, siis on nad vastavalt kongruentsed taandatud jääkide süsteemi (5) erinevate elementidega. Teoreemi 5.1 ja eeltõestatu põhjal kuulub siis astendajale δ süsteemist (5) $\varphi(\delta)$ arvu.

3. 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

$$\delta_1 = 1, \delta_2, \delta_3, \ldots, \delta_\tau = p - 1.$$

Siis φ-funktsiooni omaduse põhjal

$$\sum_{i=1}^{\tau} \varphi(\delta_i) = p - 1.$$

Järelduse 2 põhjal teoreemist 5.3 kuulub taandatud jääkide süsteemi (5) 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 jadast (5). Kui oletada, et leidub jagaja δ_j, millele ei kuulu ühtki arvu süsteemist (5), 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 iga arv mingile astendajale kuulub, siis peaks mõni arvudest (5) kuuluma astendajale, mis ei ole p-1 jagaja. See on aga vastuolus teoreemi 5.3 järeldusega 2.

3. <u>Algjuured moodulite p^α ja $2 \cdot p^\alpha$ järgi.</u> Olgu g algjuur modulo p, mille olemasolu on eelmises punktis tõestatud.

<u>Teoreem 5.6.</u> Kui g on algjuur algarvulise mooduli $p > 2$ korral, siis vähemalt üks arvudest g, g+p on algjuur modulo p^α iga $\alpha \geqslant 2$ puhul. Sealjuures on g algjuureks modulo p^α parajasti siis, kui

$$g^{p-1} \not\equiv 1 \pmod{p^2}.$$

<u>Tõestus</u>. 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 $\delta : p-1$. 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 5.1 järelduse põhjal on samuti algjuur modulo p, ja arvutame a^{p-1}:

$$a^{p-1} = (g+p)^{p-1} = g^{p-1} + (p-1)g^{p-2}p +$$
$$+ C^2_{p-1}g^{p-3}p^2 + \ldots + p^{p-1} \equiv$$
$$\equiv g^{p-1} + (p-1)g^{p-2}p \equiv 1 +$$
$$+ (p-1)g^{p-2}p \pmod{p^2}.$$

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 ($a^{p-1} \not\equiv 1 \pmod{p}$, 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

$$a^{p(p-1)} = (1 + t_1 p)^p = 1 + t_1 p^2 +$$
$$+ C^2_p t_1^2 p^2 + \ldots = 1 + t_2 p^2,$$

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);

$$a^{p^2(p-1)} = (1 + t_2 p^2)^p = 1 + t_2 p^3 + C^2_p t_2^2 p^4 + \ldots =$$
$$= 1 + t_3 p^3,$$

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

$$a^{\delta} \equiv 1 \pmod{p^{\alpha}}. \tag{10}$$

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 (10), 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 6. 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.

Teoreem 5.7. Olgu $p > 2$, $\alpha \geq 1$ 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

$$a^{\gamma} \equiv 1 \pmod{p^{\alpha}} \text{ ja } a^{\gamma} \equiv 1 \pmod{2p^{\alpha}},$$

rahuldab ka teist (vt. IV ptk., teoreemid 4.14 ja 4.15, 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 on üks tingimata paaritu ja on seega algjuureks ka modulo $2p^{\alpha}$.

Näide 7. Nägime (vt. näide 6), 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 $2 + 121 = 123$.

4. Algjuured mooduli 2^{α} ja mistahes kordarvulise mooduli järgi.

Näitame, et enamiku kordarvuliste moodulite korral algjuured puuduvad. Olgu moodul antud kanoonolisel kujul

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

ja olgu $(a,m) = 1$. Siis Euleri teoreemi kohaselt

$$a^{\varphi(p_1^{\alpha_1})} \equiv 1 \pmod{p_1^{\alpha_1}},$$
$$a^{\varphi(p_2^{\alpha_2})} \equiv 1 \pmod{p_2^{\alpha_2}},$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$a^{\varphi(p_n^{\alpha_n})} \equiv 1 \pmod{p_n^{\alpha_n}}.$$

Olgu astendajate

$$\varphi(p_1^{\alpha_1}) = p_1^{\alpha_1 - 1}(p_1 - 1)$$
$$\varphi(p_2^{\alpha_2}) = p_2^{\alpha_2 - 1}(p_2 - 1) \qquad (11)$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\varphi(p_n^{\alpha_n}) = p_n^{\alpha_n - 1}(p_n - 1)$$

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 4.14 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 (11) vähim ühiskordne s on väiksem kui nende arvude korrutis $\varphi(p_1^{\alpha_1}) \ldots \varphi(p_n^{\alpha_n}) = \varphi(m)$ juhul, kui arvudel (11) leidub ühiseid tegureid. 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

$$a = \pm 1 + 2^2 l,$$

kus l on täisarv. Tõstes järjest ruutu saame

$$a^2 = 1 + 2^3 l_1,$$

$$a^{2^2} = 1 + 2^4 l_2$$

$$\cdots\cdots\cdots\cdots$$

$$a^{2^{\alpha-2}} = 1 + 2^{\alpha} l_{\alpha-2}$$

kus $l_1, l_2, \ldots, l_{\alpha-2}$ on täisarvud. Kuid $2^{\alpha-2} = \frac{\varphi(m)}{2}$ ja järelikult iga a korral, mis täidab tingimust $(a,2) = 1$, on

$$a^{\frac{\varphi(m)}{2}} = a^{2^{\alpha-2}} = 1 + 2^{\alpha} l_{\alpha-2} \equiv 1 \pmod{2^{\alpha}}.$$

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.

Ülesandeid.

72. Teha kindlaks, millistele astendajatele modulo 9

kuuluvad taandatud jääkide süsteemi elemendid. Millised viimastest on algjuured modulo 9?

73. Millistele astendajatele modulo 31 võivad kuuluda arvud a, mille korral (a, 31) = 1? Kui palju arve taandatud jääkide süsteemist modulo 31 kuulub astendajale 10; astendajale 9?

74. Kasutades teoreemi 5.4 leida kaks algjuurt modulo 43. Kui palju leidub algjuuri modulo 43?

75. Teades, et modulo 41 on algjuureks arv 11 (kontrollida seda!) leida algjuured moodulite 41^2, 41^3, 82 ja $2 \cdot 41^2$ järgi.

76. Milliste järgi järgmistest moodulitest eksisteerivad algjuured: a) 109; b) 115; c) 172; d) 226; e) 250; f) 230; g) 32; h) 4?

§ 2. 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

$$a \equiv g^{\gamma} \pmod{m} \qquad (\gamma \geqslant 0),$$

siis astendajat γ nimetatakse arvu a indeksiks modulo m alusel g ja tähistatakse

$$\gamma = \operatorname{ind}_g a.$$

Juhul, kui aluseks on kogu aeg üks ja sama algjuur g, jäetakse ta tavaliselt märkimata ja kirjutatakse

$\gamma = \text{ind } a.$

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

$$\text{ind}_2 10 = \text{ind}_6 10 = \text{ind}_7 10 = \text{ind}_8 10 = 5.$$

Kuid

$$2^2 \equiv 4,\ 6^2 \equiv 3,\ 7^2 \equiv 5,\ 8^2 \equiv 9 \pmod{11}$$

ja seega

$$2 = \text{ind}_2 4 = \text{ind}_6 3 = \text{ind}_7 5 = \text{ind}_8 9.$$

Teises näites leidsime, et modulo 10 on algjuured 3 ja 7. Et $9 \equiv 7^2 \pmod{10}$, siis $\text{ind}_7 9 = 2$.
Niisiis arvu a indeks alusel g on astendaja, millega tuleb astendada algjuurt g, selleks et saada antud arvuga a kongruentset arvu modulo m.

Enne kui käsitleda indeksite omadusi, tõestame järgmise teoreemi.

Teoreem 5.8. Olgu m moodul, mille korral eksisteerivad algjuured ja g algjuur modulo m. Kui γ kulgeb üle vähimate mittenegatiivsete jääkide

$$0,\ 1,\ \ldots,\ \varphi(m) - 1 \pmod{\varphi(m)}, \tag{1}$$

siis g^γ kulgeb üle taandatud jääkide süsteemi modulo m.

Tõestus. Teoreemi 5.2 põhjal on arvud

$$g^0,\ g^1,\ g^2,\ \ldots,\ g^{\varphi(m)-1} \tag{2}$$

inkongruentsed modulo m. Neid arve on $\varphi(m)$, s.o. niisa-

ma palju, kui elemente taandatud jääkide süsteemis modulo m. Et $(g,m) = 1$, (vt. algjuure definitsiooni!), siis ka $(g^j,m) = 1$. Seega moodustavad arvud (2) taandatud jääkide süsteemi modulo m, mida oligi tarvis näidata.

Kuna jadasse (2) kuuluvatest arvudest on igaüks kongruentne parajasti ühe elemendiga taandatud jääkide süsteemist, siis igal taandatud jääkide süsteemi elemendil modulo m on antud alusel g olemas indeks, mis kuulub jadasse

(3) $$0, 1, \ldots, \varphi(m) - 1.$$

Eriti kui $m = p$ on algarv, on kõikidel arvudel

$$1, 2, \ldots, p - 1$$

olemas indeks alusel g, mis kuulub jadasse

$$0, 1, \ldots, p - 2.$$

Olgu $\gamma' = \operatorname{ind}_g a$, kus γ' kuulub jadasse (3). Siis juhul, kui $\gamma \equiv \gamma' \pmod{\varphi(m)}$ ja $\gamma \geqslant 0$, ka $\gamma = \operatorname{ind}_g a$ (vt. teoreem 5.3). Tavaliselt vaadeldakse vähimaid indekseid.

Indeksid on tõhusaks vahendiks kaheliikmeliste kõrgema astme kongruentside ja eksponentkongruentside lahendamisel. Seepärast on koostatud indeksite tabelid algarvuliste moodulite jaoks. Peaaegu iga õpiku lõpus leiduvad indeksite tabelid moodulite jaoks, mis ei ületa 100. Spetsiaalsed indeksite tabelid on koostatud märksa suuremate algarvude jaoks. Käesoleva õppevahendi lõppu paigutatud indeksite tabelid on äratrükk õpikust [1].

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:

$2^3 = 8$, $2^6 = 64 \equiv 7 \not\equiv 1 \pmod{19}$

$$2^9 = 2^6 \cdot 2^3 \equiv 7 \cdot 8 = 56 \equiv 18 \not\equiv 1 \pmod{19}.$$

Seega 2 on algjuur ja võtamegi selle aluseks. Selleks et saada kõikide arvude 1, 2, ... , 18 indekseid modulo 19, tuleb arvutada algjuure 2 kõik astmed $2^0, \ldots, 2^{17}$

$2^0 \equiv 1 \pmod{19}$, seega ind 1 = 0,
$2^1 \equiv 2 \pmod{19}$, " ind 2 = 1,
$2^2 \equiv 4 \pmod{19}$, " ind 4 = 2,
$2^3 \equiv 8 \pmod{19}$, " ind 8 = 3,
$2^4 \equiv 16 \pmod{19}$, " ind 16 = 4,
$2^5 \equiv 13 \pmod{19}$, " ind 13 = 5,
$2^6 \equiv 7 \pmod{19}$, " ind 7 = 6,
$2^7 \equiv 14 \pmod{19}$, " ind 14 = 7,
$2^8 \equiv 9 \pmod{19}$, " ind 9 = 8,
$2^9 \equiv 18 \pmod{19}$, " ind 18 = 9,
$2^{10} \equiv 17 \pmod{19}$, " ind 17 = 10,
$2^{11} \equiv 15 \pmod{19}$, " ind 15 = 11,
$2^{12} \equiv 11 \pmod{19}$, " ind 11 = 12,
$2^{13} \equiv 3 \pmod{19}$, " ind 3 = 13,
$2^{14} \equiv 6 \pmod{19}$, " ind 6 = 14,
$2^{15} \equiv 12 \pmod{19}$, " ind 12 = 15,
$2^{16} \equiv 5 \pmod{19}$, " ind 5 = 16
$2^{17} \equiv 10 \pmod{19}$, " ind 10 = 17.

Seega saame järgmise tabeli:

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		

2. Indeksite omadusi.

Kõigepealt märgime ära järgmised vahetult definitsioonist järelduvad omadused:

$$\text{ind } 1 \equiv 0 \pmod{\varphi(m)},$$

$$\text{ind}_g\, g \equiv 1 \pmod{\varphi(m)}$$

iga mooduli m puhul, mille korral algjuured eksisteerivad, ja iga algjuure g korral.

Tõepoolest,

$$g^0 \equiv 1 \pmod{m},$$

$$g^1 \equiv g \pmod{m}.$$

Olgu m moodul, mille korral eksisteerib algjuuri, p olgu algarv.

Teoreem 5.9. Kongruents

(4) $$a \equiv b \pmod{m}$$

kehtib parajasti siis, kui

(5) $$\text{ind } a \equiv \text{ind } b \pmod{\varphi(m)};$$

eriti kehtib kongruents

$$a \equiv b \pmod{p}$$

parajasti siis, kui

$$\operatorname{ind} a \equiv \operatorname{ind} b \pmod{p-1}.$$

Tõestus. Definitsiooni kohaselt

$$a \equiv g^{\operatorname{ind}_g a}, \quad b \equiv g^{\operatorname{ind}_g b} \pmod{m}.$$

Kasutame teoreemi 5.3. Antud juhul algjuur g kuulub astendajale $\varphi(m)$. Seega

$$g^{\operatorname{ind} a} \equiv g^{\operatorname{ind} b} \pmod{m} \quad \text{ehk} \quad a \equiv b \pmod{m}$$

parajasti siis, kui

$$\operatorname{ind}_g a \equiv \operatorname{ind}_g b \pmod{\varphi(m)}.$$

Üleminekut kongruentsilt (4) ekvivalentsele kongruentsile (5) nimetatakse kongruentsi indekseerimiseks.

Teoreem 5.10. Kui g on algjuur modulo m, siis

$$\operatorname{ind}_g (ab) \equiv \operatorname{ind}_g a + \operatorname{ind}_g b \pmod{\varphi(m)};$$

kui g on algjuur modulo p, siis

$$\operatorname{ind}_g (ab) \equiv \operatorname{ind}_g a + \operatorname{ind}_g b \pmod{p-1}.$$

Tõestus. Definitsiooni kohaselt

$$g^{\operatorname{ind} a} \equiv a \pmod{m},$$
$$g^{\operatorname{ind} b} \equiv b \pmod{m}.$$

Seega

$$g^{\operatorname{ind} a + \operatorname{ind} b} \equiv ab \equiv g^{\operatorname{ind} (ab)} \pmod{m}.$$

Nagu teoreemi 5.9 tõestamiselgi saame

$$\operatorname{ind} a + \operatorname{ind} b \equiv \operatorname{ind} (ab) \pmod{\varphi(m)}.$$

Teoreem 5.11. Kui g on algjuur modulo m, siis

$$\operatorname{ind} (a^n) \equiv n \operatorname{ind} a \pmod{\varphi(m)};$$

eriti algarvulise mooduli p korral

$$\text{ind}\,(a^n) \equiv n \text{ ind } a \pmod{p-1}.$$

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 5.12. 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 rakendamine kaheliikmeliste kongruentside lahendamisel. Vaatleme kongruentsi

(6) $$x^n \equiv a \pmod p.$$

Teatavasti nimetatakse arvu a n-astme jäägiks modulo p, kui kongruents (6) on lahenduv. Kongruentsi (6) indekseerimisel saame ekvivalentse kongruentsi

(7) $$n \text{ ind } x \equiv \text{ind } a \pmod{p-1}.$$

Tähistame siis (n, p-1) = d. Selleks, et kongruents (7) oleks ind x suhtes lahenduv, on tarvilik ja piisav, et

$$\text{ind } a \vdots d.$$

Et aga esialgne kongruents on saadud kongruentsiga ekviva-

lentne, siis ka kongruentsi (6) lahenduvuseks on tarvilik ja piisav, et

(8) $\qquad\qquad \text{ind } a \vdots (n, p-1).$

Teisiti öeldes, tingimus (8) 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 (6) 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

$$\text{ind } a \vdots 3.$$

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, (3, p-1) = 3 aga siis, kui algarv p on kujuga 3n + 1.

Näide 1. Lahendame kongruentsi $x^7 \equiv 7 \pmod{19}$.

Indekseerimisel saame

$$7 \text{ ind } x \equiv \text{ind } 7 \pmod{18}$$

ehk

$$7 \text{ ind } x \equiv 6 \pmod{18}$$

(ind 7 leiame punktis 1 koostatud tabelist). 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 $x^6 \equiv 11 \pmod{19}$.

Indekseerimisel saame ekvivalentse kongruentsi

$$6 \text{ ind } x \equiv \text{ind } 11 \pmod{18}.$$

Siin (6, 18) = 6 ja ind 11 = 12 ⋮ 6.

Seega lahendeid on 6. Edasi saame

$$6 \text{ ind } x \equiv 12 \pmod{18},$$

$$\text{ind } x \equiv 2 \pmod{3}.$$

Selleks, et oleks võimalik kasutada indeksite tabelit, peab moodul olema 18. Mooduli 18 järgi on aga lineaarkongruentsil ind x suhtes 6 lahendit:

$$\text{ind } x \equiv 2, 5, 8, 11, 14, 17 \pmod{18}.$$

Tabelist leiame nüüd ka x jaoks 6 jäägiklassi:

$$x \equiv 4, 13, 9, 15, 6, 10 \pmod{19}.$$

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 $15x \equiv 17 \pmod{19}$.

Indekseerimisel saame ind x kordajaks 1:

$$\text{ind } 15 + \text{ind } x \equiv \text{ind } 17 \pmod{18},$$

$$\text{ind } x \equiv 10 - 11 \equiv 17 \pmod{18}$$

ja tabelist

$$x \equiv 10 \pmod{19}.$$

Näide 5. Lahendame eksponentkongruentsi $3^x \equiv 8 \pmod{19}$.

Indekseerimisel leiame

$$x \text{ ind } 3 \equiv \text{ind } 8 \pmod{18}$$

ehk

$$13x \equiv 3 \pmod{18},$$

$$(13 - 18)x \equiv 3 - 18 \pmod{18},$$

$$-5x \equiv -15 \pmod{18},$$

$$x \equiv 3 \pmod{18}.$$

Kontroll: Et $x = 3 + 18t$, kus t on mistahes täisarv, siis $3^x = 3^{3+18t} = 27 \cdot 3^{18t} = 27\,(3^{\varphi(19)})^t \equiv 27 \cdot 1 \equiv 8 \pmod{19}$.

Näide 6. Lahendada kongruents $5x^9 \equiv 14 \pmod{418}$,

kui see on lahenduv.

Mooduli 418 järgi ei eksisteeri algjuuri, sest 418 = = 2·11·19. 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 lahendiks on ilmselt

$$x \equiv 0 \pmod 2.$$

Teise lahendamiseks kasutame algarvu 11 indeksite tabelit (vt. [1]). 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

$$9 \text{ ind } x \equiv 7 - 16 = -9 \pmod{18}.$$

Et (9, 18) = 9, siis on viimasel kongruentsil modulo 18 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

$$x \equiv c_1 = 0 \pmod{2}$$

$$x \equiv c_2 = 9 \pmod{11}$$

$$x \equiv c_3 = 2, 3, 8, 10, 12, 13, 14, 15, 18 \pmod{19}.$$

Esialgsel kongruentsil mod 418 on seega 1·1·9 = 9 lahendit.

Lahend avaldub kujul

$$x \equiv c = M_1M_1'c_1 + M_2M_2'M_2 + M_3M_3'c_3 \pmod{m},$$

kus

$$M_im_i = m \quad \text{ja} \quad M_iM_i' \equiv 1 \pmod{m_i}.$$

Leiame M_i ja M_i':

m_i	2	11	19
M_i	209	88	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

$$x \equiv -76 \cdot 9 - 132\, c_3 \pmod{418} \equiv -684 - 132\, c_3 \equiv$$

$$\equiv 152 - 132\, c_3 \pmod{418}.$$

Peale c_3 asendamist saame

$$x \equiv 306, 174, 348, 86, 240, 108, 394, 262, 284 \pmod{418}.$$

Ülesandeid.

77. Modulo 7 on algjuurteks arvud 3 ja 5 (kontrolli-da!). Leida arvude 1, 2, 3, 4, 5, 6 indeksid modulo 7 alustel 3 ja 5.

78. Milliste algarvu p üldkujude korral on iga arv 5. astme jäägiks modulo p, milliste p üldkujude korral mitte? Kui palju on viimasel juhul 5. astmo jääke taandatud jääkide süsteemis modulo p?

79. Kasutades indeksite tabelit modulo 23 lahendada järgmised kongruentsid

a) $15\, x^{13} \equiv 14 \pmod{23}$; b) $x^{10} \equiv 10 \pmod{23}$;

c) $12\, x^{11} \equiv 1000 \pmod{23}$; d) $13^x \equiv 6 \pmod{23}$;

e) $5 \cdot 17^{3x+2} \equiv 12 \pmod{23}$.

80. Indeksite tabelite abil leida jääk, mis tekib arvu 17^{17} jagamisel 23-ga.

1. 17. 2. 7429. 3. 437. 4. 1. 5. 1 110 111. 6. 177 480 177. 7. $2^3 \cdot 3^3 \cdot 5^4 \cdot 7^3 \cdot 11^2 \cdot 17 \cdot 23 \cdot 37$; jagajate arv on 7680. 8. 1, 2, 4, 8, 11, 22, 44, 88, 121, 242, 484, 968. 9. [1, 1, 2, 1, 1, 6, 1, 1], [1, 1, 2, 1, 1, 6, 2]. 10. [2, 2, 1, 4, 1, 1, 6, 1, 20, 2]. 11. $\frac{516\,901}{740\,785}$. 12. $\frac{34}{21}$; $\frac{1}{1}, \frac{2}{1}, \frac{3}{2}, \frac{5}{3}, \frac{8}{5}, \frac{13}{8}, \frac{21}{13}, \frac{34}{21}$. Paaritu elementide arvu korral jääb ära eelviimane lähismurd; ülejäänud lähismurrud jäävad muutumatuks. 13. a) $x = 17 + 35t$, $y = 44 - 97t$; b) $x = 6 + 19t$, $y = -2 - 10t$. 14. 31 raamatut 23 kop. tükk, 17 raamatut 38 kop. tükk. 15. 17, 111; 35, 86; 53, 61; 71, 36; 89, 11. 16. 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 $y = 61$. 17. 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)]. 18. $\frac{193}{71}$, $\left|e - \frac{193}{71}\right| < \frac{1}{33015} < 0{,}000\,031$. 19. On. 20. [1, 2, 3, 1, ...]. 21. $\frac{1+\sqrt{5}}{2}$. 22. $-2+\sqrt{3}$. 23. a) Ei ole, b) on. 24. a) [3,(1, 1, 4, 1)], b) [0,(1, 1, 4, 1)], c) [-1,(1, 1, 4, 1)]. 25. [0,(9, 2)]. 26. Vähimad lahendid; a) $x = 2$, $y = 1$; b) $x = 17$, $y = 3$; c) $x = 649$, $y = 180$. 27. 18; 4836. 28. 201 110; 476 377. 29. 28 või 22. 30. 18. 31. 16 875. 32. 165. 33. 2^{116}.

33. $2^{116}.3^{58}.5^{31}.7^{19}.11^{10}.13^{9}.17^{7}.19^{6}.23^{5}.29^{4}.31^{3}.37^{3}.41^{2}.$
$.43^{2}.47^{2}.53^{2}.61.67.71.73.79.83.89.97.101.103.107.113.$
34. 400. 35. 500. 36. 8700. 37. 40 arvu; 10, 30, 70, 90, 110, ... , 970, 990. 38. -1, 1, 0. 42. 83, 43. 70. 44. 61. 46. 56. 47. Jagub. 49. $x \equiv 5 \pmod 6$. 50. $x \equiv 1 \pmod 5$. 51. $x \equiv 30 \pmod{77}$. 52. $x \equiv 81 \pmod{337}$. 53. $x \equiv 12 \pmod{36}$. 54. a) $x \equiv 200 \pmod{551}$ ehk $x \equiv 200, 751, 1302, 1853, 2404 \pmod{2755}$; b) $x \equiv 8 \pmod{33}$ ehk $x \equiv 8, 41, 74, 107, 140, 173 \pmod{198}$. 55. $x \equiv 283 \pmod{385}$. 56. Pole lahenduv. 57. 419. 58. $x \equiv 2 \pmod 7$. 60. $x \equiv 2102 \pmod{7^4}$. 61. $x \equiv 106 \pmod{125}$. 62. Kongruentsil on kuus lahendit: $x = -757, -163, -1, 593, 1187, 1349 \pmod{2^2.3^3.5^2}$. 65. $\left(\frac{3}{p}\right) = 1$, kui $p = 12k \pm 1$; $\left(\frac{3}{p}\right) = -1$, kui $p = 12k \pm 5$. 66. Jagajateks võivad olla vaid algarvud 2, 3 ja algarvud kujuga $12k \pm 1$. 67. a) Ei ole, b) on, c) on. 68. a) +1, b) -1, c) +1. 69. -1. 70. a) Lahendeid ei ole; b) $x \equiv \pm 17 \pmod{37}$; c) $x \equiv \pm 37 \pmod{97}$. 71. a) $x \equiv \pm 16, \pm 19, \pm 26, \pm 44 \pmod{105}$; b) $x \equiv \pm 11, \pm 15, \pm 37, \pm 41 \pmod{104}$; c) $x \equiv \pm 17, \pm 37 \pmod{90}$. 75. Mooduli 41^{α} järgi on algjuur $11 + 41 = 52$, mooduli $2 \cdot 41$ järgi on algjuureks 11, mooduli $2 \cdot 41^{2}$ järgi on algjuur $52 + 41^{2}$. 78. 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 $\frac{p-1}{5}$ 5.astme jääki. 79. a) $x \equiv 2 \pmod{23}$; b) ei ole la-

henduv; c) $x \equiv 5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22 \pmod{23}$; d) $x \equiv 6 \pmod{11}$; e) $x \equiv 17 \pmod{22}$. 80. 11.

INDEKSITE TABELID.

Простое число 3.

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								

Простое число 5.

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						

Простое число 7.

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				

Простое число 11.

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										

Простое число 13.

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							

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

Простое число 17.

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			

I	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				

Простое число 19.

N	0	1	2	3	4	5	6	7	8	9
0		0	1	13	2	16	14	6	3	8
4	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		

Простое число 23.

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							

I	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								

Простое число 29.

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	

I	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		

Простое число 31.

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

Простое число 37.

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				

Простое число 41.

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

Простое число 43.

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								

Простое число 47.

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	9	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				

Простое число 53.

N	0	1	2	3	4	5	6	7	8	9
0		0	1	17	2	47	18	14	3	34
1	48	6	19	24	15	12	4	10	35	37
2	49	31	7	39	20	42	25	51	16	46
3	13	33	5	23	11	9	36	30	38	41
4	50	45	32	22	8	29	40	44	21	28
5	43	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								

Простое число 59.

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		

Простое число 61.

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

Простое число 67.

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	2
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				

Простое число 71.

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

Простое число 73.

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								

Простое число 79.

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		

Простое число 83.

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								

Простое число 89.

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		

Простое число 97.

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	1 229	2	1 523	2
3	2	181	2	421	2	673	5	953	3	1 231	3	1 531	2
5	2	191	19	431	7	677	2	967	5	1 237	2	1 543	5
7	3	193	5	433	5	683	5	971	6	1 249	7	1 549	2
11	2	197	2	439	15	691	3	977	3	1 259	2	1 553	3
13	2	199	3	443	2	701	2	983	5	1 277	2	1 559	19
17	3	211	2	449	3	709	2	991	6	1 279	3	1 567	3
19	2	223	3	457	13	719	11	997	7	1 283	2	1 571	2
23	5	227	2	461	2	727	5	1 009	11	1 289	6	1 579	3
29	2	229	6	463	3	733	6	1 013	3	1 291	2	1 583	5
31	3	233	3	467	2	739	3	1 019	2	1 297	10	1 597	11
37	2	239	7	479	13	743	5	1 021	10	1 301	2	1 601	3
41	6	241	7	487	3	751	3	1 031	14	1 303	6	1 607	5
43	3	251	6	491	2	757	2	1 033	5	1 307	2	1 609	7
47	5	257	3	499	7	761	6	1 039	3	1 319	13	1 613	3
53	2	263	5	503	5	769	11	1 049	3	1 321	13	1 619	2
59	2	269	2	509	2	773	2	1 051	7	1 327	3	1 621	2
61	2	271	6	521	3	787	2	1 061	2	1 361	3	1 627	3
67	2	277	5	523	2	797	2	1 063	3	1 367	5	1 637	2
71	7	281	3	541	2	809	3	1 069	6	1 373	2	1 657	11
73	5	283	3	547	2	811	3	1 087	3	1 381	2	1 663	3
79	3	293	2	557	2	821	2	1 091	2	1 399	13	1 667	2
83	2	307	5	563	2	823	3	1 093	5	1 409	3	1 669	2
89	3	311	17	569	3	827	2	1 097	3	1 423	3	1 693	2
97	5	313	10	571	3	829	2	1 103	5	1 427	2	1 697	3
101	2	317	2	577	5	839	11	1 109	2	1 429	6	1 699	3
103	5	331	3	587	2	853	2	1 117	2	1 433	3	1 709	3
107	2	337	10	593	3	857	3	1 123	2	1 439	7	1 721	3
109	6	347	2	599	7	859	2	1 129	11	1 447	3	1 723	3
113	3	349	2	601	7	863	5	1 151	17	1 451	2	1 733	2
127	3	353	3	607	3	877	2	1 153	5	1 453	2	1 741	2
131	2	359	7	613	2	881	3	1 163	5	1 459	5	1 747	2
137	3	367	6	617	3	883	2	1 171	2	1 471	6	1 753	7
139	2	373	2	619	2	887	5	1 181	7	1 481	3	1 759	6
149	2	379	2	631	3	907	2	1 187	2	1 483	2	1 777	5
151	6	383	5	641	3	911	17	1 193	3	1 487	5	1 783	10
157	5	389	2	643	11	919	7	1 201	11	1 489	14	1 787	2
163	2	397	5	647	5	929	3	1 213	2	1 493	2	1 789	6
167	5	401	3	653	2	937	5	1 217	3	1 499	2	1 801	11
173	2	409	21	659	2	941	2	1 223	5	1 511	11	1 811	6

Продолжение

p	g	p	g	p	g	p	g	p	g	p	g	p	g
1 823	5	2 129	3	2 417	3	2 729	3	3 049	11	3 373	5	3 691	2
1 831	3	2 131	2	2 423	5	2 731	3	3 061	6	3 389	3	3 697	5
1 847	5	2 137	10	2 437	2	2 741	2	3 067	2	3 391	3	3 701	2
1 861	2	2 141	2	2 441	6	2 749	6	3 079	6	3 407	5	3 709	2
1 867	2	2 143	3	2 447	5	2 753	3	3 083	2	3 413	2	3 719	7
1 871	14	2 153	3	2 459	2	2 767	3	3 089	3	3 433	5	3 727	3
1 873	10	2 161	23	2 467	2	2 777	3	3 109	6	3 449	3	3 733	2
1 877	2	2 179	7	2 473	5	2 789	2	3 119	7	3 457	7	3 739	7
1 879	6	2 203	5	2 477	2	2 791	6	3 121	7	3 461	2	3 761	3
1 889	3	2 207	5	2 503	3	2 797	2	3 137	3	3 463	3	3 767	5
1 901	2	2 213	2	2 521	17	2 801	3	3 163	3	3 467	2	3 769	7
1 907	2	2 221	2	2 531	2	2 803	2	3 167	5	3 469	2	3 779	2
1 913	3	2 237	2	2 539	2	2 819	2	3 169	7	3 491	2	3 793	5
1 931	2	2 239	3	2 543	5	2 833	5	3 181	7	3 499	2	3 797	2
1 933	5	2 243	2	2 549	2	2 837	2	3 187	2	3 511	7	3 803	2
1 949	2	2 251	7	2 551	6	2 843	2	3 191	11	3 517	2	3 821	3
1 951	3	2 267	2	2 557	2	2 851	2	3 203	2	3 527	5	3 823	3
1 973	2	2 269	2	2 579	2	2 857	11	3 209	3	3 529	17	3 833	3
1 979	2	2 273	3	2 591	7	2 861	2	3 217	5	3 533	2	3 847	5
1 987	2	2 281	7	2 593	7	2 879	7	3 221	10	3 539	2	3 851	2
1 993	5	2 287	19	2 609	3	2 887	5	3 229	6	3 541	7	3 853	2
1 997	2	2 293	2	2 617	5	2 897	3	3 251	6	3 547	2	3 863	5
1 999	3	2 297	5	2 621	2	2 903	5	3 253	2	3 557	2	3 877	2
2 003	5	2 309	2	2 633	3	2 909	2	3 257	3	3 559	3	3 881	13
2 011	3	2 311	3	2 647	3	2 917	5	3 259	3	3 571	2	3 889	11
2 017	5	2 333	2	2 657	3	2 927	5	3 271	3	3 581	2	3 907	2
2 027	2	2 339	2	2 659	2	2 939	2	3 299	2	3 583	3	3 911	13
2 029	2	2 341	7	2 663	5	2 953	13	3 301	6	3 593	3	3 917	2
2 039	7	2 347	3	2 671	7	2 957	2	3 307	2	3 607	5	3 919	3
2 053	2	2 351	13	2 677	2	2 963	2	3 313	10	3 613	2	3 923	2
2 063	5	2 357	2	2 683	2	2 969	3	3 319	6	3 617	3	3 929	3
2 069	2	2 371	2	2 687	5	2 971	10	3 323	2	3 623	5	3 931	2
2 081	3	2 377	5	2 689	19	2 999	17	3 329	3	3 631	21	3 943	3
2 083	2	2 381	3	2 693	2	3 001	14	3 331	3	3 637	2	3 947	2
2 087	5	2 383	5	2 699	2	3 011	2	3 343	5	3 643	2	3 967	6
2 089	7	2 389	2	2 707	2	3 019	2	3 347	2	3 659	2	3 989	2
2 099	2	2 393	3	2 711	7	3 023	5	3 359	11	3 671	13		
2 111	7	2 399	11	2 713	5	3 037	2	3 361	22	3 673	5		
2 113	5	2 411	6	2 719	3	3 041	3	3 371	2	3 677	2		

KIRJANDUS.

1. Виноградов И.М. Основы теории чисел, М., 1965.
2. Бухштаб А.А. Теория чисел, М., 1966.
3. Сушкевич А.К. Теория чисел, Харьков, 1954.
4. Михелович Ш.Х. Теория чисел, М., 1962.
5. Окунев Л.Я. Краткий курс теории чисел, М., 1956.
6. Арнольд И.В. Теория чисел, М., 1939.
7. Хассе Г. Лекции по теории чисел, М., 1953.
8. Боревич З.И и Шафаревич И.Р. Теория чисел, М., 1964.
9. Трост Э. Простые числа, М., 1959.
10. Литвер Е.Л. Теория чисел. Методические указания для студентов-заочников механико-математических и физико-математических факультетов государственных университетов. М., 1968.

Hind 35 kop.

A
29535
263877

TÜ RAAMATUKOGU
1 0300 00626387 7