Prof. *Dr. math. h. c.* **E. Lejnieks**

Skaitļu teōrija

Lekcijas,

lasītas Latvijas Ūniversitātes
Matēmatikas un dabas zinātņu fakultātē

Sakārtojis *cand. math.* **E. Fogelis**

Rediģējis doc. **A. Lūsis**

Rīgā, 1936

Matēmatisko zinātņu darbinieku biedrības izdevums

Iespiests R. Eks, J. Kronis un b-dri spiestuvē
Jelgavā, Čakstes bulvārī 10, tā]runis 2-2-1

Priekšvārdi.

„Skaitļu teōrija" aptveŗ lekcijas, ko prof. E. Lejnieks lasīja 1922.—1931. g. ik pa diviem gadiem reiz Mat. un dabas zinātņu fakultātes tīrās matēmatikas grupas studentiem. Bez vispārīgā kursa par veselo racionālo skaitļu teōriju kā atsevišķs kurss 1927. un 1931. g. lasīta „Algebrisko skaitļu teōrija". Šajā grāmatā ir apvienoti abi kursi.

Prof. E. Lejnieka kgs atļauju savu lekciju publikācijai laipni deva, bet gan gŗūtās slimības dēļ viņš šī darba sagatavošanā nav piedalījies. Manā redakcijā lekcijas sakārtojis un uzrakstījis *cand. math.* E. Fogelis, par ko izteicu viņam atzinību. Esam centušies restaurēt mūsu bij. ļoti cienījamā skolotāja un vadītāja lekcijās sniegto vielas apstrādājumu, izņemot dažus grozījumus terminoloģijā un valodā.

Lai nepalielinātu grāmatas apjomu, neesam ievietojuši lekcijās lietotos detalizētos paskaidrojumus un starpaprēķinus.

Izsaku pateicību Kultūras Fondam, kas grāmatas izdošanai piešķīris pabalstu Matēmatisko zinātņu darbinieku biedrībai.

Jelgavā, 1936. g maijā.

A. Lūsis.

Ievads.

§ 1. Vispārigas piezimes par veselu skaitļu īpašībām.

Skaitļu teōrija ir viena no vecākām matēmatikas disciplinām, ar ko nodarbojušies jau indieši, ķīnieši un senie grieķi. Divas galvenās skaitļu teōrijas nozares ir: 1) mācība par veselu skaitļu īpašībām un 2) mācība par nenoteikto vienādojumu atrisināšanu veselos skaitļos.

Runājot **par veselu skaitļu īpašībām**, pirmā vietā jāmin **pirmskaitlis**

$$p = 2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots$$

Tas ir tāds skaitlis, kam ir tikai divi dalītāji: 1 un pats skaitlis $p > 1$. Visi pirmskaitļi, izņemot $p = 2$, ir nepāru skaitļi, kuŗu starpība ir $\geqslant 2$.

Ap 300. g. pr. Kr. **Euklids** ir sarakstījis „Elementus", no kuŗu 13 grāmatām septītā, astotā un devītā ir veltītas aritmētikai. Te atrodams pierādījums par to, ka pirmskaitļu ir bezgala daudz. Ja $p_1, p_2, \ldots, p_n$ ir visi mums pazīstamie pirmskaitļi, tad skaitlis

$$x = p_1 p_2 \ldots p_n + 1$$

nedalās ne ar vienu no tiem. Tādēļ vai nu x pats ir kāds jauns pirmskaitlis q, vai arī x dalās ar tādiem pirmskaitļiem $q_1, q_2, \ldots$ kas neatrodas starp mums pazīstamiem $p_1, p_2, \ldots, p_n$. Tādā kārtā katru galīgu pirmskaitļu vairumu $p_1, p_2, \ldots, p_n$ var papildināt vismaz ar vienu jaunu elementu q, tā tad pirmskaitļu vairums ir bezgalīgs.

No 3. g. s. pr. Kr. vēl atzīmējams **Eratostena siets**, t. i. metode, ar kuŗas palīdzību no dabisko skaitļu rindas var izslēgt

visus saliktos skaitļus tā, ka pāri paliek tikai pirmskaitļi. Ja no rindas

$$2, 3, 4, 5, 6, 7, \ldots, n$$

izmet katru otro skaitli, kas stāv pēc 2, no atlikušiem katru trešo, kas stāv pēc 3, katru piekto, kas stāv pēc 5, u. t. t. un beidzot katru p^{to} no tiem, kas stāv pēc p (p ir lielākais pirmskaitlis, kas $\leqslant \sqrt{n}$), tad pāri palikušie skaitļi visi būs pirmskaitļi. Tiešām, katrs salikts skaitlis $a < n$ dalās ar kādu pirmskaitli $q < \sqrt{n}$, un tādi a no rindas ir jau izmesti.

Skaitli A var **sadalīt pirmreizinātājos** tā, ka A dala pēc kārtas ar visiem pirmskaitļiem, kas $\leqslant \sqrt{A}$. Ja A nedalās ne ar vienu no tādiem pirmskaitļiem, tad A pats ir pirmskaitlis. Ļoti lieliem A šī metode ir pārāk garlaicīga. Tādēļ vajadzētu atrast ērtāku kritēriju, kas izšķir, vai dotais skaitlis ir pirmskaitlis vai salikts. Par visām lietām — vajadzētu atrast likumu, pēc kura pirmskaitļi sakārtojas, t. i. vajadzētu noteikt, kurš pirmskaitlis seko dotajam skaitlim A, cik pirmskaitļu atrodas dotā intervallā u. t. t. Visas tās ir problēmas, kam apmierinoši atrisinājumi nav atrasti pat vēl šodien. Priekš 70 gadiem vācu matēmatiķis Meisels (*Meissel*) gan ir devis metodi, ar kuras palīdzību, intervallu pakāpeniski samazinot, var diezgan ātrā laikā aprēķināt, cik pirmskaitļu atrodas dotajā intervallā. Bet noslēgtā formā rezultāts nav uzrakstāms.

Vēl šodien nav arī atrasta tāda izteiksme $F(n)$, kurā liekot n vietā veselu skaitli katrreiz dabū pirmskaitli. P. Fermā (*Fermat*) (1601.—1665.) ir izteicis domas, ka izteiksme

$$2^{2^n} + 1$$

ar katru veselu n dod tikai pirmskaitļus. Ja $n = 0, 1, 2, 3$ un 4, tad izteiksme tiešām dod pirmskaitļus 3, 5, 17, 257 un 65537. Bet jau $2^{2^5} + 1$, kā to pierādījis Eulers 1732. g., dalās ar 641. Ta tad minētais skaitlis ir salikts, un Fermā uzskats izrādās maldīgs. Ir tiešām grūts uzdevums pateikt, kuriem n **Fermā skaitlis**

$$N = 2^{2^n} + 1$$

ir pirmskaitlis vai salikts. Ja $n = 6$, tad N dalās ar 274177

(*Landry* 1880. g). Ja $n = 7$ vai 8, tad N ir salikts skaitlis, bet tā dalītāji nav zināmi (*Klein* 1895., *Western* un *Morehead* 1909. g.) Ja $n = 11, 12, 18, 23, 36, 38$, tad N ir salikts skaitlis, un viens vai vairāki N dalītāji ir zināmi. Par $n = 10$ jautājums vēl neizšķirts. Skaitlis

$$N = 2^{2^{73}} + 1$$

dalās ar $5 \cdot 2^{75} + 1$ (*Morehead* 1906. g.); uzrakstīts bez kāpinātājiem šis N saturētu vairāk kā $2 \cdot 10^{21}$ ciparus. Rakstot 20000 ciparu dienā, tā uzrakstīšanai vajadzētu vismaz 10^{17} dienas.

Nav iespējams konstruēt tādu polinomu $f(x)$ ar veseliem koeficientiem, ka visām veselām x nozīmēm $f(x)$ būtu pirmskaitlis. Tiešām, ja pieņem

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n$$

un k kautkādu veselu skaitli, tad $f(ka_n)$ dalās ar a_n. Nav iespējams, ka visām k nozīmēm būtu $f(ka_n) = a_n$.

Ir tomēr polinomi, kas daudzām x nozīmēm dod pirmskaitļus. Viens tāds, Eulera uzrādīts, polinoms ir

$$f(x) = x^2 + x + 41,$$

kas visām veselām x nozīmēm ar

$$0 \leqslant x \leqslant 39$$

izteic tikai pirmskaitļus.

Runājot par pirmskaitļiem, jāatzīmē vēl šāda **teorēma**, ko pierādījis Čebiševs (Чебышев) 1852. g. Ja $a > 1$, tad starp a un $2a$ atrodas vismaz viens pirmskaitlis.

Jautājumus par veselu skaitļu īpašībām iedala **multiplikatīvā skaitļu teorijā**, kur veselu skaitli uzskata kā pirmskaitļu produktu, un **additīvā skaitļu teorijā**, kur skaitli uztver kā zināma veida citu skaitļu summu. Kā piemēri jāmin trijstūra (trigonālie), četrstūra (tetragonālie), piecstūra (pentagonālie), . . . un vispārīgi **poligonālie skaitļi**, ar ko daudz nodarbojušies senie grieķi, arābi un arī vēl Fermā 17. g. s.

Definīcija. Par r-stūŗa skaitli R_n sauc tādas aritmētiskās progresijas pirmo n locekļu, summu, kuŗas pirmais loceklis ir 1, bet diferenče $r-2$.

Vispārīgais trijstūŗa skaitlis ir

$$T_n = 1 + 2 + 3 + \ldots + n = \frac{1}{2} n (n + 1),$$

četrstūŗa skaitlis

$$Q_n = 1 + 3 + 5 + \ldots + (2n - 1) = n^2,$$

piecstūŗa skaitlis

$$P_n = 1 + 4 + 7 + \ldots + (3n - 2) = \frac{1}{2} n (3n - 1),$$

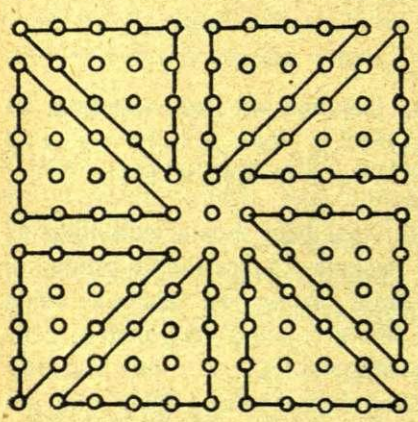
un r-stūŗa skaitlis

$$R_n = n + \frac{1}{2} n (n - 1)(r - 2).$$

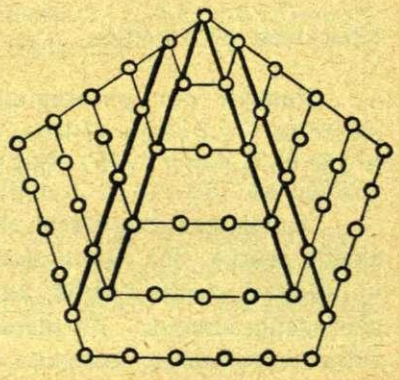
Atsevišķi trijstūŗa skaitļi ir 1, 3, 6, 10, 15, . . ., četrstūŗa skaitļi 1, 4, 9, 16, 25, . . ., piecstūŗa skaitļi 1, 5, 12, 22, 35, u. t. t. Poligonālo skaitļu nosaukumiem ir sakars ar šo skaitļu sekojošu **ģeometrisku interpretāciju.** R_n vienādus priekšmetus var novietot vienu pie otra tā, ka sagrupējums veido r-stūri, kuŗa katrā malā atrodas n priekšmetu.

Tā kā algebras metodes grieķu laikā vēl nebija pazīstamas, tad daudzas poligonālo skaitļu īpašības pierādīja ar zīmējuma palīdzību. Te divi klāt pieliktie zīmējumi uzskatāmi skaidri pierāda šādas poligonālo skaitļu īpašības:

(1) $8 T_n + 1 = Q_{2n+1}$ un (2) $P_n = 3 T_{n-1} + n$



Zīm. 1.



Zīm. 2.

Ļoti ievērojama ir **Fermā teorēma par poligonāliem skaitļiem.** Ikvienu veselu skaitli var izteikt kā r-stūŗa skaitļu summu, nelietojot vairāk kā r saskaitāmo. Teorēma izteic, ka katrs skaitlis ir vai nu trijstūŗa skaitlis, vai divu, vai augstākais triju trijstūŗa skaitļu summa (pierādījis Gauss 1801.), vai nu kvadrāts, vai augstākais četru kvadrātu summa (*Lagrange* 1770.), u. t. t, Teorēmas pirmo vispārīgo pierādījumu ir devis Košī (*Cauchy*) 1813. g. Fermā pierādījumi šai un arī daudz citām viņa teorēmām nav nekur uzglabājušies.

Additīvai skaitļu teorijai pieskaitāma **Goldbacha teorēma,** kas pazīstama jau no 18. g. s. vidus un vēl līdz pat pēdējam laikam nav pierādīta. Teorēma šāda: ikvienu pāru skaitli, kas lielāks par 2, var izteikt ar divu pirmskaitļu summu.

Teorēmas **sekas:** ikkatrs vesels skaitlis ir vai nu pirmskaitlis vai augstākais triju pirmskaitļu summa.

Ir minama vēl cita, arī līdz šim laikam nepierādīta **teorēma par pirmskaitļiem:** ir bezgala daudz tādu pirmskaitļu, kuŗu diference ir 2.

Viena no ievērojamākām additīvās skaitļu teorijas problēmām, pie kuŗas strādāja bez panākumiem gandrīz 200 gadu, ir **Uoringa** (*Waring*) **problēma** (1770. g.). Te pierāda **teorēmu:** ikkatrs vesels skaitlis ir izteicāms augstākais ar deviņu kubu summu, vai augstākais ar 19 bikvadrātu summu, u. t. t.

Līdzīgu teorēmu par vesela skaitļa sadalīšanu augstākais četru kvadrātu summā izteica jau **Bašē** (*Bachet de Méziriac*) 1621. g., un pierādīja Lagranžs (*Lagrange*) 1770. g. Uoringa teorēmas pareizību par 9 kubiem pierādīja Viferichs (*Wieferich*) 1909. g. Tanī pat gadā D. Hilberts (*Hilbert*) pierādīja **Uoringa teorēmas vispārīgo gadījumu:** katru veselu pozitīvu skaitli var izteikt ar veselu pozitīvu n. pakāpju summu, kuŗas saskaitāmo skaits ir galīgs skaitlis, kas atkarīgs tikai no n. Pēc tam Hardi

un Litlevūds (*Hardy and J. E. Littlewooa*) 1919. g. deva saskaitāmo skaita ievērojamu augšējās robežas novērtējumu.

Vēl jāatzīmē **teorēma**, kuŗu bez kāda pierādījuma publicējis **Bašē** ap 1613. g.: katru pirmskaitli $p = 4n + 1$ var sadalīt divu kvadrātu summā un tikai vienā vienīgā veidā. — Minētais nosacījums ir nepieciešams un pietiekošs. Tādēļ Eulers šo teorēmu izlietoja kā kritēriju. Teorēmu bieži izlietoja arī Fermā, tādēļ to daudzreiz sauc arī Fermā vārdā.

Bašē-Fermā teorēmu pirmo reiz pierādīja **Gauss** 1801. g. savā darbā „*Disquisitiones Arithmeticae*".*) Šī teorēma pavedināja Gausu uz domām pirmskaitli $p = 4n + 1$ sadalīt kompleksos reizinātājos.

Ja

$$p = a^2 + b^2,$$

tad

$$p = (a + bi)\,(a - bi), \quad (i = \sqrt{-1}),$$

un komplekso skaitļu laukā p vairs nav pirmskaitlis. Tad Gauss piegriežas veselo komplekso skaitļu teorijai un atrod gan īpatnības, bet arī daudz līdzības ar reālo skaitļu teoriju. Dažas īpašības, ko nevarēja pierādīt reālo skaitļu teorijā, bez pūlēm bija pierādāmas komplekso skaitļu laukā. Radās ideja par **algebrisku skaitļu teoriju.**

1826. g. Dirichlē (*L. Dirichlet*) pierādīja, ka katrā aritmētiskā progresijā, kuŗas pirmais loceklis un diference ir bez kopīga dalītāja, atrodas bezgala daudz pirmskaitļu. Ar šo pierādījumu Dirichlē deva iesākumu **analītiskai skaitļu teorijai**, kas pēta skaitļu teorijas problēmas ar analīzes un funkciju teorijas palīdzību. Jau pirms Dirichlē tāda metode ir saskatāma arī daudzos Eulera (1707.—1783.) darbos.

---

*) Jāpiezīmē ka Gausa „*Disq. Arithm.*" un Ležandra (*Legendre*) „*Théorie des nombres*" (1798. g.) ilgu laiku bija vienīgās zinātniskās grāmatas par skaitļu teoriju.

§ 2. Vispārīgas piezīmes par nenoteiktiem vienādojumiem un skaitļu laukiem.

Ar **nenoteiktiem vienādojumiem** daudz nodarbojies jau Diofants ap 350. g. pēc Kristus dz. Tādēļ viņam par godu nenoteikto vienādojumu teōriju sauc arī par diofantisko analīzi un nenoteiktos vienādojumos vispārīgi par diofantiskiem vienādojumiem. Vispārīgas metodes un vispārīgu atrisinājumu Diofants nemeklē. Visbiežāk viņš apmierinās ar vienu racionālu pozitīvu atrisinājumu, ko atrod ar kādu mākslotu un tikai tam uzdevumam derīgu metodi. Liela daļa Diofanta uzdevumu saistās ar taisnleņķa trijstūŗa jeb **Pitagora vienādojumu**

$$x^2 + y^2 = z^2,$$

ar ko, kā domā, ir nodarbojies arī Platons. Šī vienādojuma vispārīgo atrisinājumu

$$\begin{cases} x = k^2 - n^2 \\ y = 2kn \\ z = k^2 + n^2, \end{cases}$$

kur k un n veseli skaitļi, ir pazinuši jau senie indieši.

Pirmās pakāpes nenoteiktais vienādojums

$$ax + by + c = 0$$

ir pilnīgi atrisināts jau labi sen. Daudz grūtāks bija jautājums par vispārīgo **otrās pakāpes vienādojumu**

$$ax^2 + bxv + cy^2 + dx + ex + f = 0$$

ar diviem nezināmiem x un y. Tā atrisināšanai 18. g. s. Lagranžs (1736.—1812.), Eulers un Gauss (1777.—1855.) izstrādāja plašu teōriju par kvadrātiskām formām. Lagranžs pierādīja, ka vispārīgo otrās pakāpes vienādojumu var reducēt kanoniskā formā

$$x^2 - Ay^2 = 1,$$

ko Eulers bez pietiekoša iemesla nosauca par **Pella vienādojumu**.

Šis nosaukums ir palicis līdz pat mūsu dienām. Ar vienādojumu $x^2 - Ay^2 = 1$ nodarbojās jau Fermā, un arī indiešiem tas ir bijis pazīstams.

Ja

$$A < 0 \quad \text{vai} \quad A = k^2 > 0,$$

tad Pella vienādojumam ir tikai divas atrisinājumu kopas:

$$x = \pm 1, \; y = 0.$$

Ja A ir vesels pozitīvs skaitlis, kas nav cita vesela skaitļa kvadrāts, tad var atrast arī vēl citus atrisinājumus.

Piemērs. Fermā uzdevums: $x^2 - 3y^2 = 1$.

Liekot vienādojumā y vietā skaitļus 1, 2, 3, . . ., bez triviāliem atrisinājumiem $x_1 = \pm 1$, $y_1 = 0$ var atrast arī vēl sekojošus atrisinājumus:

$$x_2 = \pm 2, \quad y_2 = \pm 1$$
$$x_3 = \pm 7 \quad y_3 = \pm 4$$
$$\ldots$$

Jau 1765. g. Eulers ievēroja, ka katrā atsevišķā gadījumā, izvirzot $\sqrt{A}$ nepārtrauktā jeb ķēžu daļā, ir iespējams atrast Pella vienādojuma bezgala daudzus atrisinājumus. Bet Eulers nevarēja pierādīt, ka tas ir iespējams arī vispārīgā gadījumā. Pirmo reiz tādu pierādījumu un līdz ar to arī drošu metodi Pella vienādojuma atrisināšanai deva Lagranžs 1766. g. Par šī jautājuma principiālo nozīmi liecina piem., vienādojums

$$x^2 - 97y^2 = 1,$$

kam absolūti mazākais atrisinājums ar $y \neq 0$ ir 30 zīmju skaitlis. Tā tad eksperimentālā ceļā par šī vienādojuma iespējamību vai neiespējamību nevarētu neko uzzināt.

Ja Pella vienādojums ir atrisināts un ir izpildīti daudz citu nosacījumu, tad var atrisināt arī vispārīgo otrās pakāpes nenoteikto vienādojumu. Dažos gadījumos atrisinājumu skaits ir 0 vai galīgs skaitlis, dažos gadījumos to ir bezgala daudz. Mācība par otrās pakāpes nenoteikto vienādojumu ir pilnīgi noslēgta un uzskatāma par 18. g. s. ievērojamāko sasniegumu skaitļu teorijā.

Trešās, ceturtās un vēl augstāku pakāpju nenoteikto vienādojumu atrisināšana saistās ar nepārvaramām grūtībām. Ir zināmi tikai atsevišķi vienādojumu tipi, ko var atrisināt, vai pierādīt, ka tie nav atrisināmi. Bet vispārīgas metodes un vispārīgu rezultātu te vēl nav. Vienādojums

$$x^n + y^n = z^n$$

ir jāatzīmē tā slavenās vēstures dēļ. Par vienādojuma $x^2 + y^2 = z^2$ atrisināšanu raksta jau Diofants savā „Aritmētikā". Pie šī apraksta lapas puses malā Fermā ir atzīmējis vienādojumu

$$x^n + y^n = z^n$$

līdz ar piezīmi, ka viņam izdevies atrast brīnišķīgu pierādījumu, ka šis vienādojums veselos skaitļos nav atrisināms, ja $n \geqslant 3$. Starp Fermā atstātām piezīmēm tādu pierādījumu nekur neatrada; hipotēzi nosauca par Fermā lielo teorēmu*). Daudzi autori bezsekmīgi pūlējās to pierādīt. Par $n = 3$ vai 4 pierādījumu deva jau Eulers (1753., 1747. g.); gadījumiem $n = 5$, 7 un 11 pierādījumu atrada Ležandrs 1823. g. Arī daudz citi atsevišķi gadījumi (no $n = 3$ līdz $n = 100$) ir pierādīti, bet visā pilnībā vēl līdz pat pēdējam laikam teorēma nav pierādīta.

Kad no 1830. līdz 1840. gadam Parīzes zinātņu akadēmija izsludināja konkursa tēmu par Fermā lielo teorēmu, tad Kummers (*Kummer*) ķērās pie darba ar algebrisko skaitļu teorijas metodēm. Viņam izdevās teorēmu pierādīt bezgala daudziem noteikta veida eksponentiem, bet tomēr ne katram n. Kummers rakstīja grūti saprotāmā formā un lietāja „ideālus skaitļus", par kuŗu eksistenci, tāpat kā vispār par Kummera pierādījuma drošību, pastāvēja dažādas domas. Kummera teoriju uz vienkāršākiem pamatiem nostādīja Dedekinds.

Ap 1840. g. daudz zinātnieku piegriezās algebrisko skaitļu teorijai. Definēja **algebrisku skaitli, veselu algebrisku skaitli, skaitļu lauku** un daudz citu jēdzienu.

---

*) Par Fermā mazo teorēmu sk. § 23.

Definīcijas. Ja algebriska vienādojuma

$$a_0x^n + a_1x^{n-1} + \ldots + a_n = 0$$

visi koeficienti $a_0, a_1, \ldots, a_n$ ir veseli racionāli skaitļi, tad vienādojuma sakni α sauc par **algebrisku skaitli.** Ja bez tam $a_0 = 1$, tad α ir **vesels algebrisks skaitlis.**

Visu to skaitļu vairumu, ko ar racionālām aritmētiskām darbībām (saskaitīšanu, atņemšanu, reizināšanu un dalīšanu) var sastādīt no dota algebriska skaitļa α, sauc par **algebrisku skaitļu lauku** $K(\alpha)$. Lauks $K(1)$ ir identisks ar visu racionālo skaitļu vairumu, un šis lauks ir ikkatra lauka $K(\alpha)$ sastāvdaļa, jo līdz ar skaitli α laukā atrodas arī skaitlis

$$\frac{\alpha}{\alpha} = 1.$$

Apskatīsim tuvāk **Dirichlē lauku** $K(\sqrt{-5})$.

Te $\alpha = \sqrt{-5}$ jeb α ir vienādojuma

$$x^2 + 5 = 0$$

sakne. Šī lauka katru skaitli β var uzrakstīt formā

$$\beta = \frac{f(\alpha)}{g(\alpha)},$$

kur $f(\alpha)$ un $g(\alpha)$ ir polinomi ar racionāliem koeficientiem. Ievērojot, ka $\alpha = \sqrt{-5}$, $\alpha^2 = -5$, $\alpha^3 = -5\sqrt{-5}$, u. t. t., polinomu $f(\alpha)$ un $g(\alpha)$ pakāpes var pazemināt līdz nozīmei, kas $\leqslant 1$.

Tad

$$\beta = \frac{a + b\sqrt{-5}}{c + d\sqrt{-5}},$$

kur a, b, c un d ir racionāli skaitļi. Tālāk var pārveidot

$$\beta = \frac{(a + b\sqrt{-5})(c - d\sqrt{-5})}{c^2 + 5d^2} = A + B\sqrt{-5},$$

kur arī A un B ir racionāli. Algebrisks vienādojums ar sakni β ir

$$x^2 - 2Ax + A^2 + 5B^2 = 0.$$

No tā seko, ka $\beta = A + B\sqrt{-5}$ ir vesels **algebrisks** skaitlis tad un tikai tad, ja A un B ir veseli racionāli skaitļi.

Veselu algebrisku skaitli β sauc par **lauka** $K(\alpha)$ **pirmskaitli** tad, ja β šinī laukā nav sadalāms divu veselu skaitļu reizinājumā.

Noskaidrosim, ka skaitļi

$$3,\ 7,\ 4 - \sqrt{-5} \text{ un } 4 + \sqrt{-5}$$

ir pirmskaitļi laukā $K(\sqrt{-5})$.

Tiešām, ja pieņem

$$7 = (A + B\sqrt{-5})\ (A - B\sqrt{-5}),$$

tad dabū nenoteiktu vienādojumu

$$A^2 + 5B^2 = 7,$$

kas nav atrisināms veselos racionālos skaitļos. Tāpat nav atrisināms arī attiecīgais vienādojums skaitlim 3. Bet ja pieņem

$$4 + \sqrt{-5} = (A + B\sqrt{-5})\ (C + D\sqrt{-5})$$

un identitātes abās pusēs $\sqrt{-5}$ apmaina pret $-\sqrt{-5}$, tad rodas

$$4 - \sqrt{-5} = (A - B\sqrt{-5})\ (C - D\sqrt{-5}).$$

Sareizinot ar iepriekšējo, dabū

$$21 = (A^2 + 5B^2)\ (C^2 + 5D^2)$$

Tādēļ $A^2 + 5B^2$ ir vai nu 1 vai 3 (un tam atbilstošais faktors $C^2 + 5D^2$ ir 21 vai 7). Nenoteiktais vienādojums

$$A^2 + 5B^2 = 1$$

gan ir iespējams (ar $A = \pm 1$, $B = 0$), bet tas nedod nekādu īstu skaitļa $4 + \sqrt{-5}$ sadalījumu. Turpretīm vienādojums

$$A^2 + 5B^2 = 3$$

veselos skaitļos vispār nav iespējams.

Veselo racionālo skaitļu teorijā ir **pamatteorēma**, ka katrs vesels skaitlis ir izteicams ar pirmskaitļu produktu un tikai vienā veidā (sk. § 12.). Katrā algebriskā skaitļu laukā šī teorēma nav pareiza. Piemēram, nule apskatītā laukā $K(\sqrt{-5})$ vesels skaitlis 21 ir sadalāms pirmreizinātājos vairāk veidos:

$$21 = 3 \cdot 7 = (4 + \sqrt{-5})(4 - \sqrt{-5})$$

Lai tādu nenoteiktību novērstu, Kummers definēja „ideālus skaitļus" tā, lai ar to palīdzību katrs lauka skaitlis būtu sadalāms pirmreizinātājos tikai vienā veidā. Ideālo skaitļu jēdzienu Dedekinds pārstrādāja par „ideāla" jēdzienu, ko definēja kā jaunu skaitļu lauku dotajā laukā. Šie ideālie skaitļi ir jāuzskata par vienu no 19. g. s. lielākajiem atklājumiem.

Beidzot jāpiezīmē, ka pilnīgu pārskatu par skaitļu teorijas dažādām problēmām līdz ar attiecīgo literatūru var atrast Diksona (*L. E. Dickson*) darbā „*History of the Theory of Numbers*" (3 sējumi, *Stechert & Co. New-York*, 1934.)

Pirmā daļa.

Veselo racionālo skaitļu teōrija.

I. Skaitļu dalāmība.

§ 3. Skaitļu dalāmības definīcija un vispārīgās teorēmas.

Šīs grāmatas pirmajā daļā apskatīsim parastā nozīmē veselus skaitļus, ko apzīmēsim ar latiņu burtiem $a, b, c, \ldots$ Dažas veselu skaitļu elementāras īpašības, kā summas un reizinājuma kommūtātīvo, asociātīvo un distribūtīvo likumu, uzskatīsim par pazīstamām. Definēsim ļoti svarīgu jēdzienu par skaitļu dalāmību.

Definīcija. Ja a un b ir veseli skaitļi, un var atrast veselu skaitli q tā, ka

$$a = bq,$$

tad saka, ka a dalās ar b jeb b dala a, un raksta

$$a|b$$

Ja tāds vesels skaitlis q nav iespējams, tad a nedalās ar b.

Piemēri. $a|1$, $a|a$, $0|a$; a nedalās ar b, ja $a < b$.

Teorēma 1. Ja $a|b$ un $b|c$, tad arī $a|c$.

Pierādījums. No $a = bq$, $b = cq'$ seko $a = c \cdot qq'$. Dalījumi q un q' ir veseli skaitļi.

Teorēma 2. Ja $a|b$, tad $ak|bk$ un arī $\frac{a}{k}\Big|\frac{b}{k}$, kad $a|k$ un $b|k$.

Pierādījums viegli izdarāms.

Teorēma 3. Ja $a|n$ un $b|n$, tad arī $(a \pm b)|n$.

Pierādījums. No

$$a = nq, \; b = nq'$$

seko

$$a \pm b = n(q \pm q').$$

Archimeda aksioma. Ja skaitlis $b \neq 0$, tad, pietiekoši daudz reižu atkārtots, tas pārsniedz katru iepriekš dotu skaitli a. Tādēļ, ja a un b ir divi doti skaitļi $(a > b)$ un sastāda diferences

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

tad dabū tādu pozitīvu skaitli

$$r = a - qb,$$

kas mazāks par b. Ja šis skaitlis r ir nulle, tad

$$a = bq \quad \text{jeb} \quad a|b.$$

Ja $r \neq 0$, tad

(I) $$a = qb + r, \quad 0 < r < b$$

jeb

$$qb < a < (q + 1)\, b,$$

un šinī gadījumā a nedalās ar b. Formula (I) izsaka sakaru skaitļa a dalīšanā ar skaitli b; te q ir nepilnīgais kvocients (īsi dalījums), bet r atlikums. Ņemot, ja vajadzīgs, q vietā $q + 1$, var iekārtot tā, lai dalīšanas atlikuma absolūtā vērtība nepārsniegtu pusi no dalītāja, t. i. lai

$$|r| \leqslant \frac{b}{2}.$$

Teorēma 4. Ja $a|n$, $b|n$ un $a = bq + r$, tad arī $r|n$.

Pierādījumam izlieto 3. teorēmu.

Atzīmēsim vēl šādu īpašību: Ja dalāmo un dalītāju reizina (vai dala) ar kādu skaitli k, tad arī atlikums pareizinās (resp. izdalās) ar to pašu skaitli k. Tas seko tieši no formulas (I).

§ 4. Divu skaitļu lielākais kopīgais dalītājs.

Ik diviem skaitļiem a un b eksistē vismaz viens kopīgais dalītājs $d = 1$, jo tiklab a kā arī b dalās ar 1. Ir iespējams, ka

bez šī triviālā dalītāja skaitļiem a un b ir arī vēl citi kopīgi dalītāji. Tad vislielāko skaitli d, kas dala divus dotus skaitļus a un b sauc par šo skaitļu a un b **lielāko kopīgo dalītāju**, un raksta $d=(a, b)$.

Ja $a \geqslant b$, tad

$$(a, b) \leqslant b$$

jeb (a, b) ir viens no skaitļiem

$$1, 2, 3, \ldots, b,$$

ko visus vajaga pārbaudīt. Saprotams, ka tāds ceļš ir garlaicīgs. Tādēļ jau Euklids ir devis īsāku metodi divu skaitļu lielākā kopīgā dalītāja atrašanai. Šo metodi, ko sauc par **Euklida algoritmu**, tagad apskatīsim tuvāk.

Pieņemsim, ka dotie skaitļi ir a, b un $a > b > 0$. Ja $a|b$, tad saprotams, ka $(a, b) = b$. Bet ja a nedalās ar b, tad a dalīšanā ar b rodas atlikums r, kas skaitliski mazāks par b un nav nulle. Tādēļ b var dalīt ar $|r|$, ja dabū atlikumu r_1, kas skaitliski mazāks par $|r|$ un $\neq 0$, tad var dalīt tālāk $|r|$ ar $|r_1|$ u. t. t. Atlikumu skaitliskās nozīmes

$$|r|, \ |r_1|, \ |r_2| \ldots$$

sastāda veselu pozitīvu dilstošu skaitļu rindu, kas nevar būt bezgalīga. Tādēļ dalīšanas procesam jāizbeidzas ar kādu atlikumu $r_n = 0$, un var uzrakstīt sakarību tabulu

$$\text{(E)} \quad \begin{cases} a = qb + r \\ b = q_1 r + r_1 \\ r = q_2 r_1 + r_2 \\ \ldots\ldots\ldots\ldots \\ r_{n-3} = q_{n-1} r_{n-2} + r_{n-1} \\ r_{n-2} = q_n r_{n-1} \end{cases}$$

Apskatām uzrakstītās vienlīdzības, ejot tabulā no augšas uz leju. Ja k ir a un b kāds kopīgs dalītājs, tad:

$a|k$, $b|k$, tādēļ arī $r|k$;
$b|k$, $r|k$, tādēļ arī $r_1|k$;
. . . . . .

Beidzot arī $r_{n-1}|k$. Tā tad r_{n-1} dalās ar a un b katru kopīgu dalītāju — arī ar a un b lielāko kopīgo dalītāju d. Tādēļ

(1) $$r_{n-1} \geqslant d.$$

Tagad ejam tabulā no apakšas uz augšu. Tad

$r_{n-2}|r_{n-1}$; $r_{n-1}|r_{n-1}$, $r_{n-2}|r_{n-1}$, tādēļ arī $r_{n-3}|r_{n-1}$;

. . . . . .

Beidzot arī $b|r_{n-1}$ un $a|r_{n-1}$. Tā tad r_{n-1} ir a un b kopīgs dalītājs un

(2) $$r_{n-1} \leqslant d$$

Tagad, salīdzinot formulas (1) un (2), redzam, ka nevienlīdzības zīmes abās vietās ir jāatmet. Tad paliek formula

(3) $$d = (a, b) = r_{n-1},$$

kas noteic metodi divu skaitļu lielākā kopīgā dalītāja atrašanai.

Ja tabulā (E) visas formulas reizina vai dala ar kādu skaitli k un atkārto vajadzīgos slēdzienus, tad dabū

teorēmu 1. Ja katru no diviem dotiem skaitļiem reizina (vai dala) ar vienu un to pašu skaitli k, tad arī šo skaitļu lielākais kopīgais dalītājs pareizinās (resp. izdalās) ar to pašu skaitli k.

Tā tad

$$(ka, kb) = k\,(a, b) \quad \text{un} \quad \left(\frac{a}{k}, \frac{b}{k}\right) = \frac{(a, b)}{k}$$

Piezīme. Pēdējai formulai ir jēga tikai tad, ja $a|k$ un $b|k$, jo runāt par divu daļskaitļu $\frac{a}{k}$ un $\frac{b}{k}$ lielāko kopīgo dalītāju nav iespējams.

Liksim minētā formulā k vietā $(a, b) = d$ (to var, jo $a|d$ un $b|d$). Tad dabūsim

$$\left(\frac{a}{d}, \frac{b}{d}\right) = 1,$$

kas izteic **teorēmu 2.** Ja katru no diviem skaitļiem

a un b dala ar to lielāko kopīgo dalītāju, tad dabū divus veselus skaitļus $a_1 = \frac{a}{d}$ un $b_1 = \frac{b}{d}$, kuŗu lielākais kopīgais dalītājs ir 1.

Tādus skaitļus a_1, b_1, kam $(a_1, b_1) = 1$, sauc par **relātiviem pirmskaitļiem.** Arī saka, ka šiem skaitļiem nav kopīga dalītāja.

No Euklida algoritma tabulas visus atlikumus r_i var izteikt kā lineāras a un b funkcijas, kuŗu koeficienti ir veseli skaitļi, jo tie sastādās no q, q_1, q_2, . . . ar saskaitīšanas, atņemšanas un reizināšanas darbībām. Par to var pārliecināties, iesākot tabulā no augšas:

$$r = a - bq,$$
$$r_1 = b - q_1 r = b - q_1 a + qq_1 b = a(-q_1) + b(1 + qq_1),$$
. . . . . .

Beidzot dabū

$$d = r_{n-1} = ax + by.$$

Tā tad var atrast divus veselus skaitļus x un y, tā, ka a un b lielākais kopīgais dalītājs d ir izteicāms formā

(II) $$d = ax + by$$

Izdalot formulas (II) abas puses ar d, dabū iepriekšējās teorēmas šādu atsevišķu gadījumu: ik diviem relātiviem pirmskaitļiem a_1 un b_1 var atrast divus veselus skaitļus x un y tā, ka

$$a_1 x + b_1 y = 1.$$

Arī **otrādi**: ja $a_1 x + b_1 y = 1$, tad a_1 un b_1 ir relātīvi pirmskaitļi. Tiešām, pieņemot

$$(a_1, b_1) = d_1,$$

dabū:

$$a_1 | d_1, \quad b_1 | d_1.$$

Tādēļ arī

$$(a_1 x + b_1 y) | d_1 \quad \text{jeb} \quad 1 | d_1.$$

Tā tad $d_1 = 1$.

Piemērs. Atrast skaitļu 864 un 468 lielāko kopīgo dalītāju.

Te

$$(864, 468) = 4\ (216, 117) = 4 \cdot 9\ (24,13) = 36,$$

jo 24 un 13 ir relātīvi pirmskaitļi. Par to vēl lieku reizi var pārliecināties ar Euklida algoritmu:

$$24 = 2 \cdot 13 - 2$$
$$13 = 6 \cdot 2 + 1$$
$$2 = 2 \cdot 1$$

Te pēdējais dalīšanas atlikums un līdz ar to 24 un 13 lielākais kopīgais dalītājs ir 1, ko ar skaitļu 24 un 13 palīdzību var izteikt šādā kārtā:

$$1 = 13 - 6 \cdot 2 = 13 - 6\,(2 \cdot 13 - 24) = 6 \cdot 24 - 11 \cdot 13$$

Ar to ir arī atrasti divi veseli skaitļi $x = 6$ un $y = -11$ tā, ka

$$24x + 13y = 1.$$

§ 5. Teorēmas par relātiviem pirmskaitļiem.

Izlietosim formulu (II) dažu teorēmu pierādījumiem.

Teorēma 1. Ja $(a, b) = 1$, tad $(ak, b) = (k, b)$.

Pierādījums. No $(a, b) = 1$ seko

$$ax + by = 1, \quad ak \cdot x + b \cdot ky = k.$$

Ja $(ak, b) = d$, tad no iepriekšējās formulas redzam, ka $k|d$. Arī $b|d$, tādēļ

$$(k, b) \geqslant d.$$

Bet tā kā

$$ak|(k, b), \quad b|(k,b),$$

tad arī

$$d \geqslant (k, b).$$

Salīdzinot šo rezultātu ar iepriekšējo, dabū $d = (k, b)$. Teorēma ir pierādīta.

Teorēma 2. Ja $(a_1, b) = 1$ un $(a_2, b) = 1$, tad arī $(a_1 a_2, b) = 1$.

Pirmais pierādījums. Ar teorēmas nosacījumu var atrast veselus skaitļus x_1, y_1, x_2, y_2 tā, ka

$$a_1x_1 + by_1 = 1 \quad \text{un} \quad a_2x_2 + by_2 = 1.$$

Ja šīs vienlīdzības sareizina un apzīmē

$$x_1 x_2 = X, \quad a_1 x_1 y_2 + a_2 x_2 y_1 + by_1 y_2 = Y$$

(X un Y ir veseli skaitļi), tad dabū

$$a_1 a_2 X + b Y = 1.$$

Tādēļ

$$(a_1 a_2, b) = 1,$$

un teorēma ir pierādīta.

Otrs pierādījums. No

$$a_1 x_1 + by_1 = 1$$

seko

$$a_1 a_2 x_1 + ba_2 y_1 = a_2.$$

Ja pieņem

$$(a_1 a_2, b) = d_1 > 1,$$

tad seko

$$a_2 | d_1 \quad \text{un} \quad b | d_1$$

t. i. pretēji pieņēmumam, skaitļiem a_2 un b būtu kopīgs dalītājs $d_1 > 1$.

Teorēma 3. Ja $ak|b$ un $(a, b) = 1$, tad $k|b$.

Pierādījums. No $(a, b) = 1$ seko

$$ax + by = 1 \text{ un } akx + bky = k.$$

Pēdējā formulā kreisajā pusē katrs saskaitāmais dalās ar b. Tādēļ arī summai k jādalās ar b.

§ 6. Mazākais kopīgais dalāmais.

Definīcija. Par divu skaitļu a un b **mazāko kopīgo dalāmo** (jeb m. k. vairojumu) sauc tādu trešo vismazāko skaitli m, kas $\neq 0$ un dalās bez atlikuma ar a un b.

Ja $a > b$, tad m ir viens no skaitļiem

$$a,\ 2a,\ 3a,\ \ldots,\ ba,$$

kuŗu dalāmība ar b ir jāpārbauda. Sliktākā gadījumā

$$m = ab.$$

Lemma. Ja $x|a$ un $x|b$, tad x dalās arī ar a un b mazāko kopīgo dalāmo m.

Pieņemsim, ka x, dalīts ar m, dod atlikumā r. Tad

$$x = qm + r, \qquad (0 \leqslant r < m).$$

No šīs formulas seko, ka $r|a$ (jo $x|a$ un $m|a$) un $r|b$ (jo $x|b$ un $m|b$). Tā kā bez tam vēl $r < m$, tad, lai nerastos pretruna m definīcijai, jāpieņem, ka $r = 0$. Tā tad $x|m$, un lemma ir pierādīta.

Teorēma. Ja skaitļu a un b mazākais kopīgais dalāmais ir m, bet lielākais kopīgais dalītājs $d = (a, b)$, tad

$$ab = md.$$

Piezīme. Ja ir zināms skaitļu a un b lielākais kopīgais dalītājs d, tad ar šo formulu var atrast a un b mazāko kopīgo dalāmo m.

Pierādījums. Apzīmēsim

$$\frac{a}{d} = a_1, \qquad \frac{b}{d} = b_1 \quad \text{un} \quad \frac{ab}{d} = x.$$

Tad

$$a_1 b = x \quad \text{un arī} \quad ab_1 = x.$$

Tā kā $x|a$ un $x|b$, tad arī $x|m$ jeb

$$x = qm, \quad (q \geqslant 1).$$

Liekam šo x nozīmi iepriekšējās formulās. Tad dabūjam

$$a_1 b = qm \quad \text{un} \quad ab_1 = qm$$

jeb

$$a_1 = \frac{m}{b} q \quad \text{un} \quad b_1 = \frac{m}{a} q.$$

Bet a_1 un b_1 ir relātīvi pirmskaitļi. Tādēļ to kopīgam dalītājam q jābūt $= 1$. Tad

$$x = m \quad \text{jeb} \quad \frac{ab}{d} = m,$$

un teorēma pierādīta.

Sekas 1. Ja m ir a un b mazākais kopīgais dalāmais, tad $\frac{m}{a}$ un $\frac{m}{b}$ ir relātīvi pirmskaitļi.

Sekas 2. Ja $(a, b) = 1$, tad $m = ab$.

Teorēma 2. Ja skaitļu a un b mazāko kopīgo dalāmo apzīmē ar $[a, b]$, tad

$$[ak, bk] = k\,[a, b];$$

ja $a|k$, $b|k$, tad arī

$$\left[\frac{a}{k}, \frac{b}{k}\right] = \frac{[a, b]}{k}.$$

Pierādījums. Izlietojot 1. teorēmu izteic

$$[ak, bk] = \frac{ak \cdot bk}{(ak, bk)}.$$

Tā kā lielākais kopīgais dalītājs

$$(ak, bk) = k\,(a, b),$$

tad

$$[ak, bk] = k \cdot \frac{ab}{(a, b)} = k\,[a, b].$$

Tamlīdzīgi pierāda teorēmas otro daļu par

$$\left[\frac{a}{k}, \frac{b}{k}\right]$$

§ 7. Vairāku skaitļu lielākais kopīgais dalītājs un mazākais kopīgais dalāmais.

Var runāt arī par triju un vairāku skaitļu lielāko kopīgo dalītāju d un mazāko kopīgo dalāmo m.

Definīcija. Ar

$$d = (a, b, c)$$

apzīmē vislielāko veselo skaitli, kas dala visus dotos skaitļus a, b un c, bet ar

$$m = [a, b, c]$$

apzīmē vismazāko skaitli, kas dalās ar katru no dotajiem skaitļiem a, b, c. Ir saprotams, ka $d \leqslant c$ un $m \leqslant a\,b\,c$, ja $a \geqslant b \geqslant c$.

Teorēma 1. Ja $(a, b) = d_1$, tad $(a, b, c) = (d_1, c)$

Apzīmēsim (d_1, c) ar d. Tad

$$a|d_1, \quad d_1|d.$$

Tādēļ arī $a|d$. Līdzīgā kārtā var pierādīt, ka arī $b|d$ un $c|d$. Atliek tikai pierādīt, ka d ir a, b un c lielākais kopīgais dalītājs. Tā kā

$$(d_1, c) = d \quad \text{un} \quad (a, b) = d_1$$

tad ir tādi veseli skaitļi $x_1, y_1, x_2 y_2$, ka

$$d_1 x_1 + c y_1 = d \quad \text{un} \quad a x_2 + b y_2 = d_1.$$

Ja šo d_1 nozīmi ievieto pirmā vienlīdzībā, tad dabū formulu

$$a x_1 x_2 + b x_1 y_2 + c y_1 = d.$$

No tās redzams, ka a, b, c lielākais kopīgais dalītājs (a, b, c) nevar būt lielāks par d, jo tad formulas kreisā puse gan dalītos ar (a, b, c) bet labā puse nedalītos. Tā tad $(a, b, c) = d$, un var atrast veselus skaitļus $x = x_1 x_2$, $y = x_1 y_2$, $z = y_1$ tā, ka a, b un c lielākais kopīgais dalītājs ir uzrakstāms ar formulu

$$a x + b y + c z = d.$$

Tamlīdzīgi var pierādīt **teorēmu** par četru un vairāku skaitļu lielāko kopīgo dalītāju: Ja skaitļu $a_1, a_2, \ldots, a_n$ lielākais kopīgais dalītājs ir d, tad var atrast veselus skaitļus $x_1, x_2, \ldots, x_n$ tā, ka pastāv formula

$$\text{(III)} \qquad a_1 x_1 + a_2 x_2 + \ldots + a_n x_n = d.$$

Izdalot formulas (III) abas puses ar d, dabū **teorēmu 2.** Ja katru no n dotiem skaitļiem dala ar to lielāko kopīgo dalītāju, tad dabū n skaitļus, kas ir relātīvi pirmskaitļi.

Tagad apskatīsim teorēmu par vairāku skaitļu mazāko kopīgo dalāmo. Te iepriekš vajadzīga šāda **lemma.**

Ja $x|a_1$, $x|a_2$, . . ., $x|a_n$, tad x dalās arī ar $a_1, a_2, \ldots, a_n$ mazāko kopīgo dalāmo m.

Tiešām, ja pieņem, ka

$$x = mq + r \quad \text{ar} \quad r < m,$$

tad

$$r|a_1,\ r|a_2, \ldots, r|a_n$$

Kad $r \neq 0$, tad rodas pretruna m definīcijai. Ar to lemma pierādīta.

Teorēma. Ja skaitļu $a_1, a_2, \ldots, a_n$ mazākais kopīgais dalāmais ir m,

$$A = a_1 a_2 \ldots a_n, \quad \frac{A}{a_1} = A_1, \quad \frac{A}{a_2} = A_2, \quad \ldots, \quad \frac{A}{a_n} = A_n$$

un $$(A_1, A_2, \ldots, A_n) = d$$

tad

$$A = md.$$

Pierādījums. Pieņemsim, ka

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

Tad

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

Redzam, ka $x|a_1$, $x|a_2$, . . ., $x|a_n$; tādēļ ari $x|m$. Var pieņemt, ka

$$x = qm, \quad \text{kur} \quad q \geqslant 1.$$

Ja šo x nozīmi ievieto iepriekšējās vienlīdzībās, tad dabū formulas

$$\frac{A_1}{d} = \frac{m}{a_1} q$$

$$\frac{A_2}{d} = \frac{m}{a_2} q$$

. . . . . .

$$\frac{A_n}{d} = \frac{m}{a_n} q,$$

kur kreisās puses visiem skaitļiem kopīga dalītāja nav, bet labās puses skaitļiem ir kopīgs dalītājs q. Tādēļ

$$q = 1 \quad \text{un} \quad \frac{A}{d} = m.$$

Teorēma pierādīta.

Trim skaitļiem a, b, c nupat pierādītā teorēma izteicama šādi:

$$abc = m\,(ab, bc, ca)$$

Ja $n = 2$, tad dabū § 6. pierādīto formulu

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

Uzdevumi.

1. Pierādīt sekojošas poligonālo skaitļu īpašības.
   1. Starp diviem sekojošiem trijstūŗa skaitļiem atrodas viens kvadrāts.
   2. Divu sekojošu trijstūŗa skaitļu summa ir kvadrāts.
   3. Neviens pentagonālais skaitlis nebeidzas ar cipariem 3, 4, 8 vai 9.
   4. Ja ar P_n, Q_n un T_n apzīmē attiecīgi pentagonālu, tetragonālu un trigonālu skaitli, tad pastāv formulas:

$$T_n = n^2 - (n-1)^2 + (n-2)^2 - \ldots \pm 1;$$

$$P_n = Q_n + T_{n-1}; \quad 3P_n = T_{3n-1}.$$

2. Katra nepāru skaitļa kvadrātu var uzrakstīt formā $8n + 1$.
3. Skaitlis $4n + 3$ nevar būt ne kvadrāts, ne arī divu kvadrātu summa.
4. Skaitlis $8n + 7$ nav ne kvadrāts, ne divu, ne arī triju kvadrātu summa.
5. Divu nepāru skaitļu kradrātu summa nav kvadrāts.
6. Skaitļi $p = a^4 + 4b^4$ un $q = a^{4n} + a^{2n} + 1$ ir pirmskaitļi tikai tad, ja $a = 1$ un $b = 1$.
7. Skaitlis $a^n + b^m$ var būt pirmskaitlis tikai tad, ja $(m, n) = 1$ vai 2^k.
8. Triju sekojošu dabisko skaitļu reizinājums dalās ar 6.
9. Visām x nozīmēm skaitlis $x^4 - 4x^3 + 5x^2 - 2x$ dalās ar 12.
10. $n^3 - n$ dalās ar 6, bet ja n ir nepāru skaitlis, tad ar $24n$.
11. Ja $(a, b) = 1$ un skāitļiem $a - b$, $\dfrac{a^n - b^n}{a - b}$ ir kopīgs dalītājs d, tad $d \mid n$.
12. Ja p ir pirmskaitlis, tad skaitļa $a^p \pm 1$ visi nepāru dalītāji, kas nedala $a \pm 1$, ir formā $2pk + 1$.
13. Ja $(2^{2^n} + 1) \mid p$, tad $p = 2 \cdot 2^n k + 1$.
14. Atrast divus skaitļus, kuŗu lielākais kopīgais dalītājs $d = 30$, bet mazākais kopīgais dalāmais $m = 5040$.

II. Pirmās pakāpes nenoteiktie vienādojumi.

§ 8. Pamatteorēma par lineāriem vienadojumiem.

No Euklida algoritma atvasināsim **metodi** pirmās pakāpes jeb lineāra nenoteiktā vienādojuma atrisināšanai veselos skaitļos. Pieņemsim, ka dots vienādojums

$$Ax + By = C,$$

kam koeficienti A, B, C ir veseli skaitļi. Meklēsim tādus veselus skaitļus x un y, kas der par vienādojuma saknēm. Ja tādu x un y nav, tad saka, ka vienādojums nav iespējams. Pierādīsim šādu svarīgu sekojošu **teorēmu.**

Lai pirmās pakāpes nenoteiktais vienādojums

(1) $$Ax + By = C$$

būtu atrisināms veselos skaitļos x, y, tad ir nepieciešami un pietiekoši, ka brīvais loceklis C dalās ar koeficientu A un B lielāko kopīgo dalītāju d.

Tiešām, ja

$$(A, B) = d \quad \text{un} \quad C \text{ nedalās ar } d,$$

tad vienādojumam (1) veselu atrisinājumu nemaz nav: kad x un y ir veseli skaitļi, tad vienādojuma labā puse dalās ar d, det kreisā puse nedalās.

Tagad pieņemsim, ka C dalās ar A un B lielāko kopīgo dalītāju d. Apzīmējam

$$\frac{A}{d} = a, \quad \frac{B}{d} = b, \quad \frac{C}{d} = c.$$

Tad vienādojuma (1) abas puses dalot ar d, dabū vienādojumu

(2) $$ax + by = c$$

ar $(a, b) = 1$. Pierādīsim, ka šim vienādojumam var atrast vienu atrisinājumu kopu x_0, y_0, kur x_0 un y_0 ir veseli skaitļi.

Pirmais pierādījums. Tā kā $(a, b) = 1$, tad ar Euklida algoritmu var atrast divus veselus skaitļus a_0 un b_0 tā, ka

$$aa_0 + bb_0 = 1$$

(sk. § 4). Tad arī

$$aa_0c + bb_0c = c.$$

Tas nozīmē, ka par dotā vienādojuma speciālu atrisinājumu kopu var izvēlēties skaitļus

$$x_0 = a_0c \quad \text{un} \quad y_0 = b_0c.$$

Otrais pierādījums. No nenoteiktā vienādojuma (2) izteic

$$y = \frac{c - ax}{b}$$

Te liksim x vietā pēc kārtas skaitļus

$$x_i = 0, 1, 2, \ldots, b - 1.$$

Dalīsim visus $c - ax_i$ ar b un atlikumus r_i atstāsim pozitīvus un mazākus par b. Tad ir sakarības

$$c - ax_i = q_i b + r_i, \quad i = 1, 2, \ldots, b.$$

Pierādīsim, ka visi atlikumi r_i ir dažādi.

Tiešām, ja pieņem, ka

$$r_i = r_j, \quad 1 \leqslant j < i \leqslant b,$$

tad dabū formulu

$$c - ax_i - q_i b = c - ax_j - q_j b$$

jeb

$$a(x_i - x_j) = b(q_j - q_i)$$

Tā nav iespējama, jo formulas labā puse dalās ar b, bet kreisā nedalās. Tas tādēļ, ka $(a, b) = 1$ un $x_i - x_j < b$.

Tā tad visi atlikumi ir dažādi, atlikumu skaits ir b, visi atlikumi ir mazāki par b, un neviens atlikums nav negātīvs. Tādēļ šie atlikumi ir citā kārtībā uzrakstīti skaitļi

$$0, 1, 2, \ldots, b - 1.$$

Viens no tiem ir 0. Tas nozīmē, ka var sameklēt veselu skaitli

$$x < b$$

tā, ka arī y ir vesels skaitlis. Vienādojumam (2) ar $(a, b) = 1$ var atrast vienu veselu atrisinājumu pāri.

Sekas. Vienādojumu

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

vienmēr ir iespējams atrisināt veselos skaitļos.

§ 9. Vispārigais atrisinājums.

Ja $(a, b) = 1$ un vienādojumam

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

ir atrasts viens speciāls atrisinājums x_0, y_0, tad

$$ax_0 + by_0 = c$$

Ja šo vienlīdzību atņem no iepriekšējās, tad dabū formulu

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

no kuŗas izteic

$$x - x_0 = -\frac{b(y - y_0)}{a}$$

Ja bez x_0, y_0 dotajam vienādojumam ir vēl citi atrisinājumi ar veseliem x, y, tad $x - x_0$ ir vesels skaitlis un $b(y - y_0)|a$. Tā kā $(b, a) = 1$, tad nepieciešams, ka

$$(y - y_0)|a \qquad \text{jeb} \qquad y - y_0 = at,$$

kur t ir vesels skaitlis. Dabūjam formulas

$$\begin{cases} x = x_0 - bt \\ y = y_0 + at, \end{cases} \tag{3}$$

kas ar $t = 0, \pm 1, \pm 2, \ldots$ dod vienādojuma (2) bezgala daudz atrisinājumu. Tiešām, ja tādas x un y nozīmes ievieto vienādojumā (2), tad ikkatrai t nozīmei dabū tāpatību

$$ax_0 + by_0 + t(ab - ab) = c \qquad \text{jeb} \qquad c = c.$$

Ja bez tiem atrisinājumiem, ko izteic formulas (3), būtu vēl kāds cits atrisinājums x_1, y_1, tad no vienlīdzības

$$ax_1 + by_1 = c$$

atņemot vienlīdzību

$$ax_0 + by_0 = c$$

var izteikt atrisinājumus x_1 un y_1 tādā pat formā kā x un y formulās (3). Tādēļ x_1 un y_1 ir tikai vispārīgo atrisinājumu x un y speciālas nozīmes.

Ja $a>0$, $b>0$ un vienādojuma (2) atrisinājumiem jābūt nevien veseliem, bet arī pozitīviem, tad t vietā jāliek tādi veseli skaitļi, kam

$$x_0 - bt > 0,\ y_0 + at > 0$$

Tā tad t ir ierobežots ar

$$-\frac{y_0}{a} < t < \frac{x_0}{b},$$

un līdz ar to ir ierobežots arī dotā vienādojuma veselo atrisinājumu skaits.

Ja turpretim $a>0$ un $b<0$, tad t ir ierobežots tikai no vienas puses:

$$t > \frac{x_0}{b} \quad \text{un} \quad t > -\frac{y_0}{a}$$

Šinī gadījumā vienādojuma (2) veselu pozitīvu atrisinājumu ir bezgala daudz.

Piemērs: $35x + 48y = 23.$

Tā kā $(35, 48) = 1$, tad ar Euklida algoritmu var atrast veselus skaitļus a_0, b_0, kam

$$35a_0 + 48b_0 = 1.$$

Tā kā

$$48 = 1 \cdot 35 + 13, \qquad 35 = 3 \cdot 13 - 4, \qquad 13 = 3 \cdot 4 + 1,$$

tad

$$1 = 13 - 3 \cdot 4 = 13 - 3(3 \cdot 13 - 35) = 3 \cdot 35 - 8 \cdot 13 =$$
$$= 3 \cdot 35 - 8 \cdot (48 - 35) = 11 \cdot 35 - 8 \cdot 48.$$

Tādēļ

$$a_0 = 11, \qquad b_0 = -8$$

un

$$x_0 = 11 \cdot 23 = 253, \qquad y_0 = -8 \cdot 23 = -184.$$

Vienādojuma vispārīgo atrisinājumu izteic formulas

$$\begin{cases} x = 253 - 48t \\ y = -184 + 35t \end{cases}$$

ar $t = 0, \pm 1, \pm 2, \ldots$

Ja izvēlas $t = 5$, tad dabū speciālu atrisinājumu pāri $x_1 = 13$,

$y_1 = -9$. Vienādojuma vispārīgo atrisinājumu var uzrakstīt arī ar formulām

$$x = 13 - 48t, \qquad y = -9 + 35t, \qquad (t = 0, \pm 1, \pm 2, \ldots).$$

Veselu pozitīvu atrisinājumu vienādojumam nav.

Piezīme. Nenoteikto vienādojumu var atrisināt arī ar **grafisko metodi.** Tad jākonstruē taisne

$$ax + by = c$$

un jāatzīmē tie koordinātu tīkla mezglu punkti (tā nosauc punktus ar veselām koordinātām), kas atrodas uz šīs taisnes.

§ 10. Eulera metode.

Ja vienādojumā

$$ax + by = c$$

viens no koeficientiem a, b ir ± 1, piem. $b = 1$, tad

$$y = c - ax.$$

Ar šo formulu var atrast vienādojuma veselos atrisinājumus, ja x vietā liek veselus skaitļus.

Tagad pieņemsim, ka $|a| \neq 1$, $|b| \neq 1$ un $(a, b) = 1$.

No dotā vienādojuma izteicam atklātā veidā to nezināmo, kuŗa koeficienta absolūtā vērtība ir mazākā, piem.

$$y = \frac{c - ax}{b}, \qquad \text{ja} \quad |b| < |a|$$

Dalām a un c ar b un atstājam atlikumus a_1 un c_1 ar absolūto vertību $\leqslant \frac{|b|}{2}$. Ja

$$a = b \cdot A + a_1 \quad \text{un} \quad c = b \cdot C + c_1,$$

tad

$$y = C - Ax + \frac{c_1 - a_1 x}{b}.$$

Lai y būtu vesels skaitlis, ir nepieciešami, ka skaitlis

$$u = \frac{c_1 - a_1 x}{b}$$

būtu vesels. To pieprasot, dabū jaunu nenoteikto vienādojumu

$$bu + a_1x = c_1,$$

kam koeficienti pēc absolūtās vērtības ir mazāki par dotā vienādojuma koeficientiem. Reducēšana jātvirpina līdz tādam vienādojumam, kam viena nezināmā koeficients ir $+1$ vai -1.

Līdzīga metode ir lietojama arī triju un vairāk nezināmo vienādojumiem.

Piemērs. 1. Atrisināt veselos pozitīvos skaitļos nenoteikto vienādojumu $22x + 13y = 435$.

Atrisinājums.

$$y = \frac{435 - 22x}{13} = 33 - 2x + 2 \cdot \frac{3 + 2x}{13}$$

Ja apzīmē

$$\frac{3 + 2x}{13} = u,$$

tad dabū vienādojumu $2x = 13u - 3$, no kurienes

$$x = 6u - 1 + \frac{u - 1}{2}$$

Ja vēl apzīmē $\frac{u - 1}{2} = t$, tad $u = 1 + 2t$,

$$x = 6(1 + 2t) - 1 + t = 5 + 13t$$

un

$$y = 33 - 2(5 + 13t) + 2(1 + 2t) = 25 - 22t$$

Veselie pozitīvie atrisinājumi $x > 0$ un $y > 0$ ir tad, ja

$$5 + 13t > 0 \quad \text{un} \quad 25 - 22t > 0,$$

t. i.

$$-\frac{5}{13} < t < \frac{25}{22}.$$

Tādas veselas t nozīmes ir iespējamas tikai divas: $t_1 = 0$ un $t_2 = 1$. Tādēļ dotajam vienādojumam arī ir tikai divi veseli pozitīvi atrisinājumi

$$x_1 = 5, \quad y_1 = 25 \quad \text{un} \quad x_2 = 18, \quad y_2 = 3.$$

Piemērs 2. $34x - 19y = 85.$

Te x koeficientam un brīvajam loceklim ir kopīgs dalītājs 17, bet 19 nedalās ar 17. Tādēļ ir nepieciešams, ka

$$y|17 \quad \text{jeb} \quad y=17u.$$

Ja vienādojumu ar 17 saīsina, tad dabū vienādojumu

$$2x - 19u = 5,$$

kam ir speciāls atrisinājums $x_0 = 12$, $u_0 = 1$. Tādēļ dotā vienādojuma speciāls atrisinājums ir $x_0 = 12$, $y_0 = 17$ un vispārīgais atrisinājums

$$x = 12 + 19t, \qquad y = 17 + 34t.$$

§ 11. Lineāri vienādojumi ar vairāk nezināmiem.

Ar līdzīgām metodēm var atrisināt arī līneārus nenoteiktos vienādojumus ar vairāk nezināmiem. Vienādojumam

$$AX + BY + CZ = D$$

veseli atrisinājumi ir iespējami tikai tad, ja D dalās ar skaitļu A, B, C lielāko kopīgo dalītāju (A, B, C). Tad ar (A, B, C) abas puses var dalīt, un dabū jaunu vienādojumu

$$aX + bY + cZ = d,$$

kuŗa koeficientiem a, b, c kopīga dalītāja nav. Ja šim vienādojumam zināms vienu atrisinājumu X_0, Y_0, Z_0, tad nezināmo

$$X - X_0 = x, \qquad Y - Y_0 = y, \qquad Z - Z_0 = z$$

atrašanai sastāda vienādojumu

$$ax + by + cz = 0, \tag{4}$$

kam reizē ar x_1, y_1, z_1 un x_2, y_2, z_2 par atrisinājumu der arī skaitļi

$$k_1x_1 + k_2x_2, \qquad k_1y_1 + k_2y_2, \qquad k_1z_1 + k_2z_2$$

ar patvaļīgiem k_1 un k_2. Par to pārliecinās, liekot šīs nozīmes vienādojumā (4).

Piemērs. $4X + 5Y - 6Z = 1$

Tā kā $(4, 6) = 2$, tad jāpieņem

$$4X - 6Z = 2T$$

Dabū vienādojumu

$$2T + 5Y = 1,$$

kam ir speciāls atrisinājums $T_0 = 3$, $Y_0 = -1$. No vienādojuma $4X - 6Z = 2T$ ar $T_0 = 3$ dabū vienādojumu

$$2X - 3Z = 3,$$

kam par speciālu atrisinājumu var izvēlēties skaitļus

$$X_0 = 6 \quad \text{un} \quad Z_0 = 3.$$

Ja $X - X_0$, $Y - Y_0$ un $Z - Z_0$ apzīmē attiecīgi ar x, y un z, tad no dotā vienādojuma dabū vienādojumu

$$4x + 5y - 6z = 0.$$

Ja vienreiz izvēlas $x_1 = 2$, otrreiz $x_2 = 1$, tad var dabūt šādas speciālas nozīmes:

x	y	z
2	2	3
1	−2	−1

Bezgala daudz citu x, y, z nozīmju var uzrakstīt ar formulām

$$\begin{cases} x = 2k_1 + k_2 \\ y = 2k_1 - 2k_2 \\ z = 3k_1 - k_2. \end{cases}$$

Var pierādīt, ka ar veseliem patvaļīgiem skaitļiem k_1 un k_2 šīs formulas izsaka vienādojuma $4x + 5y - 6z = 0$ visus veselos atrisinājumus.

III. Aritmētiskās funkcijas.

§ 12. Skaitļu teōrijas pamatteōrēma.

Skaitli, kuŗa vienīgie dalītāji ir 1 un pats skaitlis, sauc par **pirmskaitli**. Tādi skaitļi ir

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \ldots$$

Pirmskaitļu apzīmēšanai parasti lietosim burtus $p, q, r, \ldots$ vai $p_1, p_2, \ldots, p_n, \ldots$ Atzīmēsim šadu acīmredzamu īpašību: Ja p un q ir pirmskaitļi un $p|q$, tad $p = q$.

Teōrēma. Ja reizinājums ab dalās ar pirmskaitli p, tad vismaz viens no reizinātājiem a vai b dalās ar p.

Ja $ab|p$ un arī $a|p$, tad teōrēma ir pierādīta. Ja a nedalās ar p, tad $(a, p) = 1$, un tādēļ $b|p$. To pierāda ar 5. § teōrēmu 3.

Teōrēmu var vispārināt: Ja reizinājums $a_1 a_2 \ldots a_n$ dalās ar p, tad vismaz viens faktors a_i dalās ar p.

Pretējās teōrēmas arī pareizas. Ja a nedalās ar p un b nedalās ar p, tad arī ab nedalās ar p. Ja a nedalās ar n un b nedalās ar n, bet $ab|n$, tad n nav pirmskaitlis.

Visus veselos skaitļus var iedalīt 3 klasēs. Pirmā klasē atrodas skaitlis 1, otrā visi pirmskaitļi, bet trešā klasē saliktie skaitļi. Par pēdējiem pierādīsim šādu **pamatteōrēmu.**

Katru skaitli var sadalīt pirmreizinātājos un tikai vienā veidā.

Ja N nav pirmskaitlis, tad N dalās ar kādu pirmskaitli p un $N = pN_1$. Ja arī N_1 nav pirmskaitlis, tad N_1 dalās ar pirmskaitli p_1. Tādēļ $N_1 = p_1 N_2$, $N_2 = p_2 N_3$, u. t. t. līdz beidzot

$$N = pp_1p_2 \ldots p_n$$

Ja N būtu sadalāms pirmskaitļu reizinājumā vēl kādā citā veidā, piem.

$$N = qq_1q_2 \ldots q_m,$$

tad varētu uzrakstīt vienlīdzību

$$pp_1p_2 \ldots p_n = qq_1q_2 \ldots q_m,$$

kuŗas kreisā puse dalās ar pirmskaitli p. Tādēļ arī labajai pusei ir jādalās ar p. Bet ja reizinājums $qq_1q_2 \ldots q_m$ dalās ar pirmskaitli p, tad vismaz viens no reizinātājiem dalās ar p, piem. $q|p$. No tā seko, ka $p = q$ un augšējo vienlīdzību ar p un q var saīsināt. Pēc tam tādā pat kārtā var pierādīt, ka p_1 vienlīdzīgs kādam q_i un abas puses ar tiem saīsināt. Tā turpina līdz vienlīdzības vienā pusē paliek 1. Tad arī otrā pusē jābūt 1. Tā tad arī pirmreizinātāju skaits abās pusēs ir vienlīdzīgs. Ar to teorēma pierādīta.

Daži pirmreizinātāji var būt arī vienādi. Tādēļ vispārīgā gadījumā kautkuŗa skaitļa N **sadalījums pirmreizinātājos** ir šāds:

(IV) $$N = p^a q^b \ldots r^k$$

Te p, q, . . ., r ir dažādi pirmskaitļi, bet a, b, . . ., k ir veseli pozitīvi skaitļi, kas $\geqslant 1$.

No formulas (IV) var secināt skaitļa N dalītāju d formu. Ja $N|d$, tad

$$d = p^\alpha q^\beta \ldots r^\varkappa,$$

kur $$0 \leqslant \alpha \leqslant a, \quad 0 \leqslant \beta \leqslant b, \ldots, \quad 0 \leqslant \varkappa \leqslant k.$$

§ 13. Skaitļa dalītāju skaits un summa.

Ja reizinājumā

$$S = (1+p+p^2+\ldots+p^a)(1+q+q^2+\ldots+q^b)\ldots(1+r+r^2+\ldots+r^k)$$

atveŗ visas iekavas, tad rodas $(a+1)(b+1)\ldots(k+1)$ dažādu locekļu summa

$$\Sigma p^\alpha q^\beta \ldots r^\varkappa,$$

kur $\alpha = 0, 1, 2, \ldots, a$; $\beta = 0, 1, 2, \ldots b$; $\ldots$, $\varkappa = 0, 1, 2, \ldots, k$. Summas katrs loceklis ir skaitļa $N = p^a q^b \ldots r^k$ dalītājs, un otrādi: katrs N dalītājs ir arī loceklis augšējā summā. Tādēļ skaitļa N visu **dalītāju skaits**, ko apzīmēsim ar $\varrho(N)$, ir

(V) $$\varrho(N) = (a+1)(b+1)\ldots(k+1)$$

un **dalītāju summa**

$$\int(N) = (1+p+p^2+\ldots+p^a)(1+q+q^2+\ldots+q^b)\ldots(1+r+r^2\ldots+r^k)$$

jeb

(VI) $$\int(N) = \frac{p^{a+1}-1}{p-1} \cdot \frac{q^{b+1}-1}{q-1} \cdot \ldots \cdot \frac{r^{k+1}-1}{r-1}$$

Šo formulu pirmie atradēji nav pazīstami. Abas formulas lieto jau *Wallis* ap 1680. g., bet formulu dalītāju skaita aprēķināšanai sastop jau ap 1673. g. kāda maz pazīstama angļu autora *John Kersey* darbos. Apzīmējumus $\rho(N)$ un $\int(N)$ ir lietojis Eulers. Liuvils (*Liouville*) skaitļa N visu dalītāju k. pakāpju summu apzīmēja ar $\zeta_k(N)$. Tad $\rho(N)$ un $\int(N)$ vietā ir jāraksta $\zeta_0(N)$ vai vienkārši $\zeta(N)$ un $\zeta_1(N)$. Bieži $\int(N)$ vietā raksta arī $S(N)$ vai $\sigma(N)$.

Funkcijas, kas definētas tikai veselām argūmentu nozīmēm, sauc par aritmētiskām funkcijām. Pie tām pieder arī funkcijas $\rho(N)$ un $\int(N)$. Tādiem simboliem, kā piem $\rho\left(\frac{3}{4}\right)$ vai $\int(\sqrt{2})$, nav jēgas.

Piezīme. Skaitļa N dalītāju skaits nav atkarīgs no pirmskaitļiem, kuŗus satur skaitlis N, bet tikai no šo pirmskaitļu eksponentiem. Piemēram, skaitļiem $60 = 2^2 . 3 . 5$ un $220 = 2^2 . 5 . 11$ ir viens un tas pats dalītāju skaits

$$\rho(60) = \rho(220) = (2+1)(1+1)(1+1) = 12.$$

Bet dalītāju summas

$$\int(60) = (1+2+4)(1+3)(1+5) = 168$$

un

$$\int(220) = (1+2+4)(1+5)(1+11) = 504$$

ir dažādas.

§ 14. Pilnigie skaitļi.

Tos skaitļa N dalītājus, kas mazāki par pašu skaitli N, sauc par skaitļa īstiem dalītājiem. Skaitli, kas vienlīdzīgs ar visu savu īsto dalītāju summu, sauc par **pilnīgu skaitli.**

Var arī definēt pilnīgu skaitli N ar formulu

$$\int(N) = 2N.$$

Pilnīgā skaitļa jēdzienu ir devuši senie grieķi; formula pilnīgu pāŗu skaitļu aprēķināšanai ir pazīstama jau Euklidam. Par pilnīgu nepāŗu skaitļu eksistenci pat šodien vēl nekas nav zināms.

Ikkatrs pilnīgais pāŗu skaitlis ir uzrakstāms ar formulu

$$N = 2^{k-1} . n,$$

kur $k > 1$ un nezināmais n ir nepāru skaitlis. Ja izlieto pilnīgā skaitļa definīciju un funkcijas $\int(N)$ viegli pierādāmu īpašību

$$\int(AB) = \int(A) \cdot \int(B),$$

kad

$$(A, B) = 1,$$

tad skaitļa n aprēķināšanai var sastādīt vienādojumu

$$\int(2^{k-1}) \cdot \int(n) = 2 \cdot 2^{k-1} \cdot n$$

jeb

$$(2^k - 1) \int(n) = 2^k \cdot n.$$

No tā seko

$$\int(n) = \frac{2^k n}{2^k - 1} = n + \frac{n}{2^k - 1}$$

Tā tad $n \mid (2^k - 1)$. Tā kā $2^k - 1 > 1$, tad

$$\frac{n}{2^k - 1} < n$$

t. i. $\frac{n}{2^k - 1}$ ir **īsts** skaitļa n dalītājs. Redzam, ka skaitļa n visu dalītāju summa sastāv no paša skaitļa n un viena īsta dalītāja $\frac{n}{2^k - 1}$. Bet tas iespējams tikai tad, ja n ir pirmskaitlis. Tādā gadījumā vienīgais īstais dalītājs ir 1. Pieprasot, lai

$$\frac{n}{2^k - 1} = 1,$$

dabū

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

Tā tad, ja $2^k - 1$ **ir pirmskaitlis, tad formula**

$$N = 2^{k-1}(2^k - 1)$$

izsaka visus pilnīgos pāru skaitļus. Šo īpašību pirmais pierādīja **Eulers.**

Nav zināms, vai pilnīgo skaitļu ir bezgala daudz. Mūsu dienās ir pazīstami ne vairāk kā 10 pilnīgie skaitļi. **Izteiksme** $2^k - 1$ **var būt pirmskaitlis tikai tad, ja** k **ir pirmskaitlis** p. Tiešām, ja $k = k_1 k_2$ ir salikts skaitlis, tad $2^k - 1$ var sadalīt reizinātājos tā, ka viens faktors ir $2^{k_1} - 1$. Tomēr ne visi $2^p - 1$ ir pirmskaitļi, piem., ja $p = 11$.

Daudz interesantu teorēmu par skaitļiem $2^k - 1$ ir devis Fermā [laika biedrs — franču mūks Mersenns (*Mersenne*). Tādēļ šos skaitļus sauc arī par Mersenna skaitļiem. Vai, piem. $2^{231} - 1$ ir pirmskaitlis, to nevar izšķirt tiešā aprēķinu ceļā, jo pirmskaitļu tabulas ir sastādītas tikai līdz 10 000 000.

Bez pilnīgiem skaitļiem Eulers ir rakstījis arī par pārpilnīgiem, resp. trūcīgiem skaitļiem, t. i. tādiem, kam īsto dalītāju summa ir lielāka, resp. mazāka par pašu skaitli.

No Aristoteļa laikiem ir pazīstams jēdziens par sabiedrotiem skaitļiem. Tie ir tādi divi skaitļi a un b, (piem. 220 un 284), ka viena skaitļa a visu īsto dalītāju summa $= b$ un b īsto dalītāju summa $= a$. Citāda veida definīcija: a un b ir sabiedroti skaitļi, tad, ja

$$\int(a) = \int(b) = a + b.$$

Par sabiedrotiem skaitļiem maz kas zināms.

§ 15. Veselo funkcija E(x).

Pēc Ležandra parauga lielāko veselo skaitli, kas $\leqslant x$, apzīmē ar $E(x)$. Gauss $E(x)$ vietā lietoja apzīmējumu $[x]$.

Piemēri. $E(\pi) = 3$, $E(-\sqrt{2}) = -2$, $E(2{,}999) = 2$, u. t. t.

Izrādās, ka daudz funkcijas, kas sastopamas skaitļu teorijā, var izvirzīt rindā

$$a_1 E\left(\frac{n}{1}\right) + a_2 E\left(\frac{n}{2}\right) + a_3 E\left(\frac{n}{3}\right) + \ldots,$$

kas atgādina Teilora (*Taylor*) rindu analīzē. Par šo jautājumu daudz rakstījis ap 1870. g. krievu autors Bugajevs (Бураев). Mēs apskatīsim tikai sekojošās funkcijas $E(x)$ vienkāršās īpašības un dažus izlietojumus.

1. Pēc funkcijas $E(x)$ definīcijas:

$$x_1 = E(x_1) + a_1$$
$$x_2 = E(x_2) + a_2$$
$$\ldots\ldots$$
$$x_n = E(x_n) + a_n,$$

kur $a_1 < 1$, $a_2 < 1$, . . ., $a_n < 1$. Vienlīdzības saskaitot, dabū formulu

$x_1+x_2+\ldots+x_n=E(x_1)+E(x_2)+\ldots+E(x_n)+(a_1+a_2+\ldots+a_n)$, kur summa $a_1+a_2+\ldots+a_n$ var būt arī lielāka par 1. Tādēļ pastāv **sakars**

(VIII) $E(x_1+x_2+\ldots+x_n)\geqslant E(x_1)+E(x_2)+\ldots+E(x_n)$

2. Pierādīsim **formulu**

(IX) $$E\left\{\frac{E\left(\frac{x}{a}\right)}{b}\right\}=E\left(\frac{x}{ab}\right),$$

kur a un b ir veseli skaitļi (x var arī nebūt vesels).

Ja x dala ar a, tad dabū atlikumu $r<a$. Tā tad $r=a-\varepsilon$, kur ε pozitīvs skaitlis No vienlīdzības

$$x=qa+r \qquad (0<r<a)$$

seko vienlīdzība

$$\frac{x}{a}=q+\frac{r}{a}=E\left(\frac{x}{a}\right)+\frac{r}{a}.$$

No pēdējās atrod formulu

$$\frac{x}{ab}=\frac{E\left(\frac{x}{a}\right)}{b}+\frac{r}{ab}=E\left\{\frac{E\left(\frac{x}{a}\right)}{b}\right\}+\frac{r_1}{b}+\frac{r}{ab},$$

kur r_1 ir vesels skaitlis, kas mazāks par b. Tā kā $r_1\leqslant b-1$, un $r=a-\varepsilon$ tad

$$\frac{r_1}{b}+\frac{r}{ab}\leqslant\frac{b-1}{b}+\frac{a-\varepsilon}{ab}<1$$

Tā tad

$$E\left(\frac{x}{ab}\right)=E\left\{\frac{E\left(\frac{x}{a}\right)}{b}\right\}$$

Tagad apskatīsim divus **piemērus**, kuŗos šīs $E(x)$ īpašības izlieto.

Vispirms pierādīsim **Ležandra teorēmu par faktoriālu.**

Faktoriāls $n!=1.2.3\ldots n$ satur pirmskaitli $p\leqslant n$ pakāpē, kuŗas kāpinātājs

$$k=E\left(\frac{n}{p}\right)+E\left(\frac{n}{p^2}\right)+E\left(\frac{n}{p^3}\right)+\ldots$$

Uzrakstīsim atsevišķi skaitļa $n!$ tos faktorus

$$p, 2p, 3p, \ldots, E\left(\frac{n}{p}\right).p,$$

kas satur pirmskaitli p. Šo faktoru reizinājums

$$p \cdot 2p \cdot 3p \ldots E\left(\frac{n}{p}\right) p = p^{E\left(\frac{n}{p}\right)} 1.2.3 \ldots E\left(\frac{n}{p}\right) = p^{E\left(\frac{n}{p}\right)} \cdot \left[E\left(\frac{n}{p}\right)\right]!$$

satur pirmskaitli p pakāpē ar kāpinātāju

$$k = E\left(\frac{n}{p}\right) + k_1$$

Te k_1 ir kāpinātājs pakāpei, kādā pirmsksitli p satur faktoriāls $n_1!$, ja $n_1 = E\left(\frac{n}{p}\right)$. Pēc iepriekšējā parauga jābūt

$$k_1 = E\left(\frac{n_1}{p}\right) + k_2 = E\left\{\frac{E\left(\frac{n}{p}\right)}{p}\right\} + k_2 = E\left(\frac{n}{p^2}\right) + k_2,$$

kur k_2 ir kāpinātājs pakāpei, kādā pirmskaitlis p ieiet faktoriālā $n_2!$, ja $n_2 = E\left(\frac{n_1}{p}\right) = E\left(\frac{n}{p^2}\right)$. Tādēļ

$$k_2 = E\left(\frac{n}{p^3}\right) + k_3, \qquad \text{u. t. t.}$$

Rezultātus apvienojot, dabū formulu

$$k = E\left(\frac{n}{p}\right) + E\left(\frac{n}{p^2}\right) + E\left(\frac{n}{p^3}\right) + \ldots,$$

un teorēma pierādīta.

Otrs piemērs. Pierādīsim, ka izteiksme

$$\frac{(a + b + c + \ldots + h)!}{a!\, b!\, c! \ldots h!}$$

katrreiz ir vesels skaitlis.

Ja kaut kuŗu pirmskaitli p skaitītājs, resp. saucējs, satur pakāpē ar kāpinātāju K, resp. k, un $K \geqslant k$, tad teorēma ir pierādīta. Atsaucoties uz formulu (VIII), var rakstīt nevienlīdzības

$$E\left(\frac{a + b + \ldots + h}{p}\right) \geqslant E\left(\frac{a}{p}\right) + E\left(\frac{b}{p}\right) + \ldots + E\left(\frac{h}{p}\right)$$

$$E\left(\frac{a + b + \ldots + h}{p^2}\right) \geqslant E\left(\frac{a}{p^2}\right) + E\left(\frac{b}{p^2}\right) + \ldots + E\left(\frac{h}{p^2}\right)$$

. . . . . .

Ja tās saskaita un izlieto Ležandra teorēmu par faktoriālu, tad dabū formulu

$$E\left(\frac{a+b+...+h}{p}\right)+E\left(\frac{a+b+.+h}{p^2}\right)+...\geqslant\begin{cases}E\left(\frac{a}{p}\right)+E\left(\frac{a}{p^2}\right)+\ldots\\+E\left(\frac{b}{p}\right)+E\left(\frac{b}{p^2}\right)+\ldots\\\ldots\ldots\\+E\left(\frac{h}{p}\right)+E\left(\frac{h}{p^2}\right)+\ldots,\end{cases}$$

kas identiska ar $K\geqslant k$.

Teorēmu var pierādīt arī sekojošā algebriskā ceļā. Ja polinomu $x+y+z+\ldots+s$ kāpina n. pakāpē, tad visi izvirzījuma koeficienti ir veseli skaitļi. No algebras ir zināms, ka

$$(x+y+z+\ldots+s)^n=\Sigma\frac{(a+b+c+...+h)!}{a!\,b!\,c!\ldots h!}x^a y^b z^c\ldots s^h,$$

kur summēšana jādara tā, kā
$a+b+c+...+h=n$ un $0\leqslant a\leqslant n$, $0\leqslant b\leqslant n$,.. , $0\leqslant h\leqslant n$.

Tādēļ katra izteiksme

$$\frac{(a+b+c+\ldots+h)!}{a!\,b!\,c!\ldots h!}$$

ir vesels skaitlis.

§ 16. Eulera-Gausa funkcija $\varphi(n)$.

Ar $\varphi(n)$ skaitļu teorijā apzīmē to dabisko skaitļu skaitu, kas nav lielāki par n un kam ar n lielākais kopīgais dalītājs ir 1.

Piemērs. Skaitļi, kas mazāki par 15 un kam ar 15 nav kopīga dalītāja ir šādi : 1, 2, 4, 7, 8, 11, 13, 14. Tādēļ $\varphi(15)=8$.

No $\varphi(n)$ definīcijas seko, ka

$$\varphi(1)=1$$

Ja p ir pirmskaitlis, tad

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

Lai noteiktu $\varphi(p^a)$, uzrakstīsim visus dabiskos skaitļus, kas nav lielāki par p^a un kam ar p^a ir kopīgs dalītājs, lielāks par 1. Tādi skaitļi ir

$$1p,\ 2p,\ 3p,\ldots,p^{a-1}.p$$

Kā redzams, to skaits ir p^{a-1}. Tādēļ

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

Funkcijas $\varphi(n)$ vispārīgās izteiksmes aprēķināšanai ir ap 50 dažādas metodes. Divas no tām ir devis jau Eulers ap 1760. g. Mēs te apskatīsim **Gausa metodi**, kur izlieto vienu lemmu un tai sekojošu teorēmu.

Lemma. Ja $(a, b)=1$, tad aritmētiskā progresijā

$$h,\ h+b,\ h+2b,\ \ldots,\ h+ib,\ \ldots,\ h+(a-1)b$$

ir tik pat daudz skaitlim a relatīvu pirmskaitļu, cik tādu skaitļu ir rindā

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

— tā tad pavisam $\varphi(a)$.

Pierādījums. Ja katru progresijas locekli $h+ib$ dala ar a un ņem pozitīvu atlikumu, tad var sastādīt formulas

$$h+ib=q_i\,a+r_i,\qquad (i=0,\ 1,\ 2,\ \ldots,\ a-1),$$

kur $0\leqslant r_i<a$. Tā kā $(h+ib,\ a)=(r_i,\ a)$, tad dotajā progresijā ir tikpatdaudz skaitlim a relatīvu pirmskaitļu, cik tādu ir atlikumu rindā

$$r_0,\ r_1,\ r_2,\ \ldots,\ r_{a-1}.$$

Visi šie atlikumi ir dažādi, jo pretējā gadījumā, kad

$$r_i=r_j,\qquad 0\leqslant j<i<a,$$

seko formula

$$h+ib-q_i\,a=h+jb-q_i\,b$$

jeb

$$b(i-j)=a(q_i-q_j)$$

Tā nav iespējama, jo formulas labā puse dalās ar a, bet kreisā puse nedalās. Tas tādēļ, ka $(a,\ b)=1$ un $i-j<a$.

Tā tad visi atlikumi ir dažādi, pozitīvi, mazāki par a, un to skaits ir a. Tādēļ šie atlikumi ir skaitļi

$$0,\ 1,\ 2,\ 3,\ \ldots,\ a-1,$$

bet iespējams, ka citādā kārtībā.

Ja atlikumu 0 apmaina pret a, tad lemma ir pierādīta.

Teorēma. Ja $(a,\ b)=1$, tad $\varphi(ab)=\varphi(a).\varphi(b)$.

Lai teorēmu pierādītu, sakārtosim visus veselos skaitļus no 1 līdz ab pa a rindām un b kolonnām sekojošā tabulā.

1	2	3	$\ldots h$	$\ldots b$
$1+b$	$2+b$	$3+b$	$\ldots h+b$	$\ldots 2b$
$1+2b$	$2+2b$	$3+2b$	$\ldots h+2b$	$\ldots 3b$
. .	. . . .	. . . .	. . . . .	. . . .
$1+kb$	$2+kb$	$3+kb$	$\ldots h+kb$	$\ldots (k+1)b$
. .	. . . .	. . . .	. . . . .	. . . .
$1+(a-1)b$	$2+(a-1)b$	$3+(a-1)b$	$\ldots h+(a-1)b$	$\ldots ab$

Pēc iepriekšējās lemmas katrā rindā ir $\varphi(b)$ skaitļu, kam nav kopīga dalītāja ar b. Visi šie skaitļi sakārtojas pa vienām un tām pašām kolonnām, jo, ja $(h, b) = 1$, tad arī $(h+kb, b)=1$ un otrādi. Tādēļ augšējā tabulā visi tie skaitļi n, kam $(n, b)=1$ piepilda tieši $\varphi(b)$ kolonnas.

Katrā kolonnā skaitlim a relatīvu pirmskaitļu ir $\varphi(a)$. Tādēļ visā tabulā ir pavisam $\varphi(a).\varphi(b)$ skaitļu, kas ir relatīvi pirmskaitļi reizē ar a un b, tā tad relatīvi pirmskaitļi ar ab. Bet tas nozīmē to, ka

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

Sekas 1. Ja $n = p^a q^b \ldots r^k$, kur $p, q, \ldots, r$ ir dažādi pirmskaitļi, tad

$$\varphi(n)=\varphi(p^a)\varphi(q^b)\ldots\varphi(r^k) \text{ jeb}$$

$$(X) \qquad \varphi(n) = n\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)\ldots\left(1-\frac{1}{r}\right)$$

$$=p^{a-1}q^{b-1}\ldots r^{k-1}(p-1)(q-1)\ldots(r-1)$$

Sekas 2. Pirmskaitļu ir bezgala daudz.

Kummera pierādījums. Pieņemsim, ka pirmskaitļu ir galīgs skaits. Uzrakstīsim visus pirmskaitļus ar simboliem

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

Sareizinot tos, dabūsim skaitli

$$N = p_1 p_2 \ldots p_n.$$

Tad no vienas puses $\varphi(N) = 1$, jo rindā

$$1, 2, 3, \ldots, k, \ldots, N$$

katram skaitlim $k \neq 1$ ir ar N kāds kopīgs dalītājs, kas lielāks par 1. Tas tādēļ, ka k katrā ziņā dalās ar kādu pirmskaitli $p_i \leqslant k$ un arī N dalās ar p_i. No otras puses $\varphi(N)$ nekad nevar būt $= 1$, jo

$$\varphi(N)=\varphi(p_1)\varphi(p_2)\ldots\varphi(p_n)=(p_1-1)(p_2-1)\ldots(p_n-1) > 1.$$

§ 17. Gausa teorēma.

Lemma. Ja $n|d$, tad rindā

$$1, 2, 3, \ldots, n$$

ir pavisam $\varphi\left(\frac{n}{d}\right)$ skaitļu, kam ar n lielākais kopīgais dalītājs ir d.

Pierādījums. Ja $k = 1, 2, 3, \ldots, \frac{n}{d}$, tad kd izsaka visus dabiskos skaitļus, kas dalās ar d un nav lielāki kā n. Bet $(kd, n) = d$ tikai tad, ja $\left(k, \frac{n}{d}\right) = 1$. Tādi k rindā $1, 2, 3, \ldots, \frac{n}{d}$ ir pavisam $\varphi\left(\frac{n}{d}\right)$.

Gausa teorēma. Ja $d_1, d_2, \ldots, d_\rho$ ir skaitļa n visi dalītāji, tad ir sakars

$$\varphi(d_1) + \varphi(d_2) + \ldots + \varphi(d_\rho) = n.$$

Gausa pierādījums. Sakārtosim skaitļus

$$1, 2, 3, \ldots, n$$

ρ **klasēs** tā, lai pirmā klasē atrastos visi tie $\varphi\left(\frac{n}{d_1}\right)$ skaitļi, kam ar n lielākais kopīgais dalītājs ir d_1, otrā klasē visi tie $\varphi\left(\frac{n}{d_2}\right)$ skaitļi, kam ar n lielākais kopīgais dalītājs ir d_2, u. t. t. Beidzot, ρ. klasē ietilpst visi tie $\varphi\left(\frac{n}{d_\rho}\right)$ skaitļi, kam ar n lielākais kopīgais dalītājs ir d_ρ.

Visi dalītāji $d_1, d_2, \ldots, d_\rho$ ir dažādi skaitļi (no tiem $d_1 = 1$ un $d_\rho = n$), un ikkatrs dabiskais skaitlis, kas $\leqslant n$, pieder vienai un tikai vienai no ρ klasēm. Tādēļ der formula

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

Ja $n|d_k$, tad $n = d_k d$, kur arī $d = \frac{n}{d_k}$ ir skaitļa n dalītājs. Tādēļ reizē ar $d_1, d_2, \ldots, d_\rho$ arī $\frac{n}{d_1}, \frac{n}{d_2}, \ldots, \frac{n}{d_\rho}$ ir skaitļa

n dalītāju virkne, tikai citādā sakārtojumā. Ar to teorēma pierādīta.

Apskatīsim vēl otru pierādījumu. Gadījumā, kad $n=p^a$, tad visi dalītāji ir skaitļi $1, p, p^2, \ldots, p^a$. Formula

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

rāda, ka šinī atsevišķā gadījumā teorēma ir pareiza.

Vispārīgā gadījumā, kad

$$n=p^a q^b \ldots r^k$$

izlieto Eulera — Gausa funkcijas īpašību

$$\varphi(ab)=\varphi(a)\varphi(b), \qquad \text{ja} \qquad (a,b)=1$$

Tad var rakstīt formulu

$$\varphi(d_1)+\varphi(d_2)+\ldots+\varphi(d_\varrho)=[\varphi(1)+\varphi(p)+\ldots+\varphi(p^a)]$$
$$[\varphi(1)+\varphi(q)+\ldots+\varphi(q^b)]\ldots[\varphi(1)+\varphi(r)+\ldots+\varphi(r^k)]$$

jeb

$$\varphi(d_1)+\varphi(d_2)+\ldots+\varphi(d_\varrho)=p^a q^b \ldots r^k=n$$

Ar to teorēma ir pierādīta arī vispārīgā gadījumā.

Piezīme. Gausa teorēmu var pierakstīt īsāk ar formulu

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

Ja definē simbolu

$$\left\{x\right\}=\begin{cases}0, & \text{kad } x \text{ ir nesaīsināms daļskaitlis}\\ 1, & \text{kad } x \text{ ir vesels skaitlis,}\end{cases}$$

tad var rakstīt arī formulu

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

§ 18. Möbiusa-Mertena funkcija $\mu(n)$.

Definīcija. Funkcijas $\mu(n)$ nozīmes ir: $\mu(1)=1$, $\mu(n)=0$, ja n dalās ar kāda pirmskaitļa kvadrātu; citādi $\mu(n)$ ir $+1$ vai -1 atkarīgi no tā, vai n satur dažādus pirmreizinātājus pāru vai nepāru skaitā.

Piemēri. $\mu(11)=-1$, $\mu(15)=1$, $\mu(18)=0$.

Möbiusa teorēma:

$$\sum_{n|d} \mu(d) = \begin{cases} 1, & \text{ja } n = 1 \\ 0, & \text{ja } n > 1. \end{cases}$$

Gadījumā, kad $n = 1$, teorēmas pareizība seko no $\mu(1)$ definīcijas.

Ja $n > 1$, tad var pieņemt, ka

$$n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k},$$

un uzrakstīt visus tos skaitļa n dalītājus d, kam $\mu(d) \neq 0$. Tādi dalītāji ir skaitlis 1, k pirmskaitļi, $\frac{k(k-1)}{1.2}$ divu dažādu pirmskaitļu reizinājumi u. t. t. Tādēļ var rakstīt formulu

$$\sum_{n|d} \mu(d) = 1 - k + \frac{k(k-1)}{1.2} - \frac{k(k-1)(k-2)}{1.2.3} + \dots + (-1)^k = (1-1)^k = 0,$$

ar ko teorēma pierādīta.

§ 19. Skaitliskais diferenciāls un integrāls.

Ja $f(n)$ ir aritmētiska funkcija, kas definēta veselām argūmenta n nozīmēm, tad funkciju

$$F(n) = \sum_{n|d} f(d)$$

sauc par funkcijas $f(n)$ **skaitlisko integrālu**, bet f par F **skaitlisko diferenciālu.** Šādu funkciju piemērus dod Gausa un Möbiusa teorēmas.

Ja ir dots diferenciāls, tad skaitlisko integrālu var atrast ar tiešu aprēķinu. Mēs apskatīsim **apgrieztu problemu:** ir dots skaitliskais integrāls F, bet jāatrod skaitliskais diferenciāls f. To varētu panākt sekošā kārtā. No F definīcijas formulas var rakstīt vienlīdzības:

$$\begin{aligned} F(1) &= f(1) \\ F(2) &= f(1) + f(2) \\ F(3) &= f(1) + f(3) \\ F(4) &= f(1) + f(2) + f(4) \\ F(5) &= f(1) + f(5) \\ &\dots\dots \end{aligned}$$

No tām izteic

$f(1)=F(1)$, $f(2)=F(2)-F(1)$, $f(3)=F(3)-F(1)$, $f(4)=F(4)-F(2)$, u. t. t. Bet šāda metode ir garlaicīga. Tādēļ pierādīsim **Dedekinda formulu** (1854. g.), kas aprēķinu lielā mērā saīsina.

Pieņemsim, ka

$$F(n) = \sum_{n|k} f(k)$$

un $n|t$. Tad arī

$$F\left(\frac{n}{t}\right) = \sum_{\frac{n}{t}|k} f(k) = \sum_{k=1}^{k=n} \left\{\frac{n}{kt}\right\} f(k),$$

kur simbols

$$\{x\} = \begin{cases} 0, \text{ ja } x \text{ ir nesaīsināms daļskaitlis} \\ 1, \text{ ja } x \text{ ir vesels skaitlis.} \end{cases}$$

Reizināsim pēdējās formulas abas puses ar $\mu(t)$:

$$\mu(t) F\left(\frac{n}{t}\right) = \mu(t) \sum_{k=1}^{n} \left\{\frac{n}{kt}\right\} f(k),$$

un summēsim pa visiem n dalītājiem t. Tad rodas

$$\sum_{n|t} \mu(t) F\left(\frac{n}{t}\right) = \sum_{n|t} \mu(t) \sum_{k=1}^{n} \left\{\frac{n}{kt}\right\} f(k) = \sum_{n|t} \sum_{k=1}^{n} \left\{\frac{n}{kt}\right\} f(k) \mu(t).$$

Pēdējā izteiksmē apmainīsim summēšanu kārtību. To, saprotams, var darīt, ja no saskaitāmo kārtības summa nav atkarīga. Tad rodas formula

$$\sum_{n|t} \mu(t) F\left(\frac{n}{t}\right) = \sum_{k=1}^{n} \sum_{n|t} \left\{\frac{n}{kt}\right\} f(k) \mu(t).$$

Te iekšējā summā nosacījumu $n|t$ var arī ignorēt, jo ja n nedalās ar t, tad $\left\{\frac{n}{kt}\right\} = 0$. Pārveidojumus turpinot, dabū formulu

$$\sum_{n|t} \mu(t) F\left(\frac{n}{t}\right) = \sum_{k=1}^{n} f(k) \sum_{t=1}^{n} \left\{\frac{n}{kt}\right\} \mu(t) = \sum_{n|k} f(k) \sum_{\frac{n}{k}|t} \mu(t).$$

Tagad no Möbiusa teorēmas seko, ka pēdējā summā

visi locekļi ar $\frac{n}{k} > 1$ ir nulles. Ja tādus locekļus atmet, tad paliek vienīgi loceklis ar $\frac{n}{k} = 1$ jeb $k = n$. Var rakstīt formulu

$$\sum_{n|t} \mu(t) F\left(\frac{n}{t}\right) = f(n) \cdot 1$$

jeb

$$f(n) = \sum_{n|t} \mu(t) F\left(\frac{n}{t}\right) \qquad \text{(XI)}$$

Pēdējo sakaru sauc par **Dedekinda formulu** Ja t un $\frac{n}{t}$ vietā raksta d un δ, tad

$$d\delta = n,$$

t. i. d un δ ir skaitļa n divi p a p i l d u d a l ī t ā j i. D e d e k i n d a formulu var arī uzrakstīt šadā veidā:

$$f(n) = \sum \mu(d) F(\delta).$$

Piemērs 1. $f(4) = \mu(1) F(4) + \mu(2) F(2) + \mu(4) F(1)$
jeb $f(4) = F(4) - F(2).$

Piemērs 2. No G a u s a teorēmas

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

ar D e d e k i n d a formulu var uzrakstīt sakaru

$$\varphi(n) = \sum_{n|t} \mu(t) \frac{n}{t} = n \sum_{n|t} \frac{\mu(t)}{t}, \qquad (X^a)$$

kas identisks ar agrāk pierādītu formulu (X).

Par to pārliecināsimies ar **piemēru**: $n = 40$. Šinī gadījumā no formulas (X^a) seko

$$\varphi(40) = 40 \sum_{40|t} \frac{\mu(t)}{t}$$

Bet skaitlim $40 = 2^3 \cdot 5$ ir tikai četri dalītāji t, kam $\mu(t) \neq 0$; tie ir 1, 2, 5 un $2 \cdot 5$. Tādēļ $\varphi(40)$ aprēķinu var turpināt šādā veidā:

$$\varphi(40) = 40\left(\frac{\mu(1)}{1} + \frac{\mu(2)}{2} + \frac{\mu(5)}{5} + \frac{\mu(2 \cdot 5)}{2 \cdot 5}\right)$$

jeb

$$\varphi(40) = 40\left(1 - \frac{1}{2} - \frac{1}{5} + \frac{1}{2} \cdot \frac{1}{5}\right) = 40\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right)$$

Tamlīdzīgi pierāda, ka formulas (X) un (X^a) ir identiskas arī vispārīgā gadījumā.

Uzdevumi.

1. Atrast skaitļa n visu dalītāju produktu.

2. Noteikt, cik veidos skaitli n var sadalīt divos faktoros, un cik veidos tā, ka abiem faktoriem nav kopīga dalītāja.

3. Atrast mazāko skaitli, kam ir 15 dalītāji.

4. Pierādīt, ka $\varphi(n)$ ir pāru skaitlis, ja $n > 2$.

Arī pierādīt, ka $\varphi(n) \leqslant \frac{n}{2}$

un

$$\varphi(2n) = \begin{cases} \varphi(n), \text{ ja } n \text{ ir nepāru skaitlis.} \\ 2\varphi(n), \text{ ja } n \text{ ir pāru skaitlis.} \end{cases}$$

6. Atrisināt vienādojumu $\varphi(n) = a$, ja $a = 1, 2, 4, 6, 8, 10, 12$ un 14.

7. Pierādīt, ka vienādojums $\varphi(x) = 2(6k + 1)$ nav iespējams, ja $6k + 1$ ir pirmskaitlis.

8. Atrast visu to $\varphi(n)$ skaitļu summu, kas mazāki par n un bez kopīga dalītāja ar n.

9. Aprēķināt, cik ir īstu pozitīvu daļskaitļu $\frac{a}{b}$ ar $(a, b) = 1$ un $a < b \leqslant n$.

10. Pierādīt, ka funkcijas $\varrho(n)$, $\int(n)$, $\varphi(n)$, $\mu(n)$ ir ar tādu īpašību, ka $F(ab) = F(a)\,F(b)$, ja $(a, b) = 1$. Izteikt arī $F(ab)$ ar $F(a)$ un $F(b)$ vispārīgā gadījumā, kad $(a, b) = d > 1$.

11. Uzrakstīt 15 pēc kārtas sekojošos saliktus skaitļus.

Piezīme. Jaievēro, ka $p_1 p_2 \ldots p_n + k$ ir salikts skaitlis, ja $k \leqslant p_n + 1$ un $p_1, p_2, \ldots, p_n$ ir pirmie n pirmskaitļi.

12. Pierādīt, ka

$$E(x) + E\left(x + \frac{1}{n}\right) + E\left(x + \frac{2}{n}\right) + \ldots + E\left(x + \frac{n-1}{n}\right) = E(nx),$$

ja n ir vesels skaitlis.

13. Pierādīt, ka $(pq)!$ dalās ar $(p!)^q q!$ un $(q!)^p p!$

14. Aprēķināt, ar cik nullēm beidzas skaitlis 1000!

15. Atrast vismazāko skaitli n tā, lai $n! \mid 500\,000$.

16. Pierādīt, ka nav faktoriāla $n!$, kas saturētu pirmskaitli 3 tieši 7. pakāpē.

IV. Kongruenti skaitļi.

§ 20. Kongruentu skaitļu vispārīgās īpašības.

Pirmā definīcija. Ja divi skaitļi a un b, dalīti ar m, dod vienādus atlikumus, tad saka, ka šie skaitļi ir **kongruenti attiecībā pret moduli** m. Pēc Gausa parauga raksta

$$a \equiv b \pmod{m}.$$

Ja nekādi pārpratumi nerodas, tad (mod m) var arī nerakstīt.

Otrā definīcija. Divi skaitļi a un b ir kongruenti attiecībā pret moduli m, ja diference $a - b$ dalās ar m. Abas definīcijas ir līdzvērtīgas.

No tām tiešā ceļā secināmas šādas **kongruentu skaitļu īpašības**.

1. **Refleksivitāte:** $a \equiv a \pmod{m}$.
2. **Simmetrija:** ja $a \equiv b \pmod{m}$, tad arī $b \equiv a \pmod{m}$.
3. **Transitivitāte:** ja $a \equiv b \pmod{m}$ un $b \equiv c \pmod{m}$ tad, arī $a \equiv c \pmod{m}$.

Teorēma 1. Ja $a \equiv b \pmod{mk}$, tad arī

$$a \equiv b \pmod{m},$$ bet ne otrādi.

Pierādījums seko no § 3. teorēmas I.

Teorēma 2. Ja

$$a \equiv b \pmod{m_1},\ a \equiv b \pmod{m_2},\ \ldots,\ a \equiv b \pmod{m_k}$$

un m ir moduļu $m_1, m_2, \ldots, m_k$ mazākais kopīgais dalāmais, tad arī

$$a \equiv b \pmod{m}.$$

Pierādījums. No noteikumiem

$$(a - b) \mid m_1,\ (a - b) \mid m_2,\ \ldots,\ (a - b) \mid m_k$$

ar § 7. lemmu seko, ka $a - b$ dalās arī ar $m_1, m_2, \ldots, m_k$ mazāko kopīgo dalāmo m, t. i. $a \equiv b \pmod{m}$.

3. Saskaitīšanas un atņemšanas teōrēma.

Ja $a \equiv b \pmod{m}$ un $c \equiv d \pmod{m}$, tad arī

$$a \pm c \equiv b \pm d \pmod{m}.$$

Pierādījums. Ja $(a - b) \mid m$ un $(c - d) \mid m$, tad arī $(a - b) \pm (c - d) = (a \pm c) - (b \pm d)$ dalās ar m.

No šīs teōrēmas seko, ka kongruences katru locekli var pārnest no vienas puses otrā, ja maina šī locekļa zīmi ar pretēju.

4. Teōrēmas par kongruenču reizināšanu.

Pirmā teōrēma.

Ja $a \equiv b \pmod{m}$, tad arī $ac \equiv bc \pmod{mc}$.

Pierādījums seko no § 3. teōrēmas 2.

Otrā teōrēma:

Ja $a \equiv b \pmod{m}$ un $c \equiv d \pmod{m}$, tad arī $ac \equiv bd \pmod{m}$.

Pierādījums. No dotām prēmisām var secināt kongruences

$$ac \equiv bc \pmod{m} \quad \text{un} \quad bc \equiv bd \pmod{m},$$

un no tām kongruenci

$$ac \equiv bd \pmod{m}.$$

Sekas. Ja

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

un

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

ir polinoms ar veseliem koeficientiem $a_0, a_1, \ldots, a_n$ tad var rakstīt kongruences

$$a_0a^n \equiv a_0b^n \pmod{m}$$
$$a_1a^{n-1} \equiv a_1b^{n-1} \pmod{m},$$
$$\ldots\ldots\ldots$$
$$a_n \equiv a_n \pmod{m}$$

Tās saskaitot, dabū formulu

$$f(a) \equiv f(b) \pmod{m}.$$

5. Teōrēma par kongruences dalīšanu.

Ja $a \equiv b \pmod{m}$ un lielākie kopīgie dalītāji ir $(a, b) = d$ un $(d, m) = d_1$, tad no dotās kongruences var secināt kongruenci

$$\frac{a}{d} \equiv \frac{b}{d} \left(\bmod \frac{m}{d_1} \right)$$

Pierādījums. Pieņemsim, ka

$$a = da_1,\ b = db_1,\ d = d_1d_2 \text{ un } m = d_1m_1.$$

No

$$(a - b) \mid m \text{ jeb } d_1d_2\,(a_1 - b_1) \mid d_1m_1$$

seko

$$d_2\,(a_1 - b_1) \mid m_1$$

Tā kā $(d_2, m_1) = 1$, tad arī

$$(a_1 - b_1) \mid m_1 \text{ jeb } a_1 \equiv b_1 \pmod{m_1}.$$

Piemēri. No $36 \equiv 16 \pmod{20}$ seko $9 \equiv 4 \pmod 5$.

No $42 \equiv 12 \pmod{10}$ seko $7 \equiv 2 \pmod 5$.

Reizē ar $24 \equiv 4 \pmod 5$ pastāv arī kongruence $6 \equiv 1 \pmod 5$.

§ 21. Kongruenču izlietošanas piemēri.

Kā paraugu kongruenču izlietošanai apskatīsim šādu vēsturisku **piemēru** (Eulers, 1732. g.).

Skaitlis $2^{2^5} + 1$ dalās ar 641.

Apgalvojumu var pierādīt, ja pārbauda sekojošas kongruences:

$$2^{10} = 1024 \equiv -258 \pmod{641},$$

$$2^{20} \equiv (250 + 8)^2 = 66564 \equiv -100 \pmod{641}$$

$$2^{12} \equiv -4 \cdot 258 \equiv 250 \pmod{641}.$$

No tām seko kongruence

$$2^{32} \equiv -25000 \equiv -1 \pmod{641} \quad \text{jeb} \quad 2^{32} + 1 \equiv 0 \pmod{641}.$$

Kā **otru piemēru** apskatīsim jautājumu par **skaitļa dalāmības pazīmēm.** Pieņemsim, ka skaitļa sistēmas baze ir g (parasti $g=10$). Ir dots skaitlis N formā

$$N = a_0g^n + a_1g^{n-1} + \ldots + a_{n-1}g + a_n$$

un modulis $m < N$. Jānoteic atlikums, kas rastos, dalot N ar m.

Dalām $g, g^2, \ldots, g^n$ ar moduli m un atlikumus apzīmējam ar $r_1, r_2, \ldots, r_n$. Tad

$$g \equiv r_1,\ g^2 \equiv r_2, \ldots, g^n \equiv r_n \ldots \pmod m$$

un

$$N \equiv a_0r_n + a_1r_{n-1} + \ldots + a_{n-1}r_1 + a_n \pmod m.$$

Apzīmējam

$$a_0r_n + a_1r_{n-1} + \ldots + a_n = N_1.$$

Tad

$$N_1 < N \qquad \text{un} \qquad N \equiv N_1 \pmod{m}.$$

Ja tādu pat procesu atkārto ar skaitli N_1, tad dabū skaitli $N_2 < N_1$ tā, ka

$$N \equiv N_1 \equiv N_2 \pmod{m} \text{ u. t. t.}$$

Piemēram, pieņemsim $g=10$ un par moduļiem izvēlēsimies 9 un 11. Tad var rakstīt kongruences

$$g \equiv 1, \quad g^2 \equiv 1, \quad g^3 \equiv 1, \ldots, \quad g^n \equiv 1 \ldots \pmod 9$$
$$g \equiv -1, \quad g^2 \equiv 1, \quad g^3 \equiv -1, \ldots, \quad g^n \equiv (-1)^n \ldots \pmod{11}.$$

No tām seko formulas

$$N \equiv a_0 + a_1 + a_2 + \ldots + a_n \pmod 9$$

un

$$N \equiv a_n - a_{n-1} + a_{n-2} - \ldots + (-1)^n a_0 \pmod{11}.$$

Pirmā no šīm formulām izteic vispārpazīstamo likumu par skaitļa dalāmību ar 9. Piemēram, skaitlis 12474 dalās ar 9, jo $1 + 2 + 4 + 7 + 4$ dalās ar 9. Šis skaitlis dalās arī ar 11, jo $(4 - 7 + 4 - 2 + 1) \mid 11$.

§ 22. Skaitļu iedalīšana klasēs.

Attiecībā pret moduli m visus veselos skaitļus iedala m **klasēs** tā, ka pirmā klasē atrodas visi tie skaitļi, kas $\equiv 1 \pmod m$, otrā tie, kas $\equiv 2 \pmod m$, ... un beidzot m. klasē visi tie skaitļi, kas $\equiv m \equiv 0 \pmod m$.

Piemēram, kad $m = 10$, tad pirmā klasē atrodas skaitļi ..., $-19, -9, 1, 11, 21, \ldots$, otrā klasē ... $-18, -8, 2, 12, 22, \ldots$ un pēdējā (10.) klasē skaitļi ... $-20, -10, 0, 10, 20, \ldots$

Jāatzīmē sekošas raksturīgas **klašu īpašības.**

1. Katrs veselais skaitlis atrodas moduļa m vienā un tikai vienā klasē.

2. Visi vienas klases skaitļi ir savā starpā kongruenti, bet divi dažādu klašu skaitļi nav kongruenti attiecībā pret moduli m.

Pierādījums. Ja ar indekiem k un t norāda klašu numurus un pieņem, ka

$$a_k \equiv a_t \pmod m, \qquad 1 \leqslant t < k \leqslant m,$$

tad seko

$$k \equiv t \pmod{m} \quad \text{jeb} \quad (k - t) \mid m,$$

kas nav iespējams.

3. Visiem vienas kases skaitļiem ar moduli m ir viens un tas pats lielākais kopīgais dalītājs.

Tiešām, ja $a \equiv b \pmod{m}$, tad no vienlīdzības

$$a - b = mk$$

seko, ka $b \mid (a, m)$. Tas nozīmē, ka $(b, m) \geqslant (a, m)$. Tamlīdzīgi spriežot, pierāda, ka $(a, m) \geqslant (b, m)$. Tā tad

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

No 3. īpašības seko

4. Ir pavisam $\varphi(m)$ klases, kuŗās (un vienīgi šinīs klasēs) atrodas visi tie skaitļi, kas ir relatīvi pirmskaitļi ar moduli m.

Ja no katras klases izvēlas pa vienam skaitlim, tad dabū mod m **pilnīgu atlikumu sistēmu**. Ja izvēlas pa vienam skaitlim tikai no tām klasēm, kuŗu skaitļiem ar m nav kopīga dalītāja, tad dabū mod m **reducētu atlikumu sistēmu.**

Definīcija. Par moduļa m **pilnīgu atlikumu sistēmu** sauc m skaitļus, starp kuŗiem attiecībā pret mod m nav divu kongruentu skaitļu, bet par moduļa m **reducētu atlikumu sistēmu** sauc tādus $\varphi(m)$ skaitļus, kas ir bez kopīga dalītāja ar mod m, un ik divi no tiem nav kongruenti.

Piemērs. Skaitļi -2, -1, 0, 1, 2, 3 sastāda mod 6 pilnīgu atlikumu sistēmu, bet skaitļi 1 un -1 reducētu atlikumu sistēmu.

Teorēma. Ja $(a, m) = 1$ un $r_1, r_2, \ldots, r_m$ ir mod m pilnīga, bet $r_1, r_2, \ldots, r_n$ reducēta atlikumu sistēma, tad arī $ar_1, ar_2, \ldots, ar_m$ ir pilnīga, bet $ar_1, ar_2, \ldots, ar_n$ reducēta atlikumu sistēma (tam pašam modulim).

Pieradījums. Ja atlikums r_i nav kongruents ar r_j attiecībā pret moduli m jeb $r_i - r_j$ nedalās ar m,

tad arī $a(r_i - r_j)$ nedalās ar m, resp.

ar_i nav kongruents ar ar_j attiecībā pret moduli m.

Ja $(r, m) = 1$, tad arī $(ar_i\ m) = 1$. Ar to viss vajadzīgais ir pierādīts.

§ 23. Fermā (*Fermat*) mazā teorēma.

Teorēma. Ja p ir pirmskaitlis un a veselsskaitlis, tad $a^p \equiv a \pmod p$; ja a nedalās ar p, tad arī

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

Šī Fermā mazā teorēma (1640. g.) ir viena no svarīgākām teorēmām skaitļu teorijā. Teorēmas atsevišķs gadījums, ka $(2^p - 2) \mid p$, ir pazīstams jau senajā Ķīnā. Pirmos trīs pierādījumus deva Eulers (1736., 1747. un 1758. g.). Apskatīsim Eulera otro pierādījumu, kur izlieto Ņūtona binoma formulu un pilnīgo indukciju.

Ja uzraksta formulu

$$(a+1)^p - a^p - 1 = \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \binom{p}{3}a^{p-3} + \ldots + \binom{p}{p-1}a,$$

tad labajā pusē katrs binoma koeficients

$$\binom{p}{k} = \frac{p(p-1)(p-2)\ldots(p-k+1)}{1.2.3\ldots k}, \qquad 0 < k < p,$$

ir vesels skaitlis. Tā tad skaitītāju $p(p-1)\ldots(p-k+1)$ var izdalīt ar saucēju $1.2\ldots k$, pie kam paliek faktoris p, jo saucējā visi reizinātāji ir mazāki par pirmskaitli p. Tādēļ labajā pusē polinoma visi koeficienti dalās ar p, un var rakstīt kongruenci

$$(a+1)^p - a^p - 1 \equiv 0 \pmod p$$

jeb

$$(a+1)^p \equiv a^p + 1 \pmod p.$$

Ja te no abām pusēm atņem $a+1$, tad dabū kongruenci

$$(a+1)^p - (a+1) \equiv a^p - a \pmod p$$

Ja a vietā liek pēc kārtas skaitļus $1, 2, 3, \ldots, a-1$, tad dabū formulas

$$2^p - 2 \equiv 1^p - 1 \pmod{p}$$
$$3^p - 3 \equiv 2^p - 2 \pmod{p}$$
$$\cdots\cdots$$
$$a^p - a \equiv (a-1)^p - (a-1) \pmod{p}.$$

Ja tās saskaita un vienkāršo, tad paliek formula

$$a^p - a \equiv 0 \pmod{p} \quad \text{jeb} \quad a^p \equiv a \pmod{p}$$

Gadījumā, kad a nedalās ar p, var abas puses dalīt ar a un dabū kongruenci

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

Ar to teorēma pierādīta.

Apskatīsim vēl otru pierādījumu, kuŗa ideju devis Aivori (*Ivory*) 1806. g.

Ja $a \mid p$, tad teorēmas pareizība ir acīmredzama. Tādēļ pieņemsim, ka a nedalās ar p jeb $(a,p) = 1$. Par moduļa p reducētu atlikumu sistēmu var izvēlēties skaitļus

$$1, 2, 3, \ldots, p-1.$$

Reizē ar tiem moduļa p reducētu atlikumu sistēmu sastāda (§ 22) arī skaitļi

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

Tas nozīmē, ka kongruencēs

$$a \equiv r_1 \pmod{p}$$
$$2a \equiv r_2 \pmod{p}$$
$$3a \equiv r_3 \pmod{p}$$
$$\cdots\cdots$$
$$(p-1)a \equiv r_{p-1} \pmod{p}$$

visi atlikumi r_i ir pozitīvi, dažādi un mazāki par p. Tā tad $r_1, r_2, \ldots, r_{p-1}$ ir citādā kārtībā uzrakstīti skaitļi $1, 2, 3, \ldots, p-1$. Ja visas minētās kongruences sareizina un abas puses dala ar $(p-1)!$, tad rodas formula

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

Ja pareizina tās abas puses ar a, tad dabū teorēmā prasīto vispārīgo kongruenci

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

§ 24. Eulera teorēma. Apgrieztā Fermā teorēma.

Eulera teorēma. Ja $(a, m) = 1$, tad

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

Pierādījums. Pieņemsim, ka

$$m = p^{\alpha} q^{\beta} \dots r^{\lambda}$$

Tad

$$\varphi(m) = p^{\alpha-1} q^{\beta-1} \dots r^{\lambda-1} (p-1)(q-1) \dots (r-1).$$

No Fermā teorēmas seko

$$(a^{p-1} - 1) \mid p \quad \text{jeb} \quad a^{p-1} - 1 = p h_1,$$

kur h_1 ir vesels skaitlis. Var rakstīt formulas

$$a^{p-1} = 1 + p h_1,$$

$$a^{p(p-1)} = (1 + p h_1)^p = 1 + p^2 h_1 + \binom{p}{2} p^2 h_1^2 + \dots = 1 + p^2 h_2,$$

$$a^{p^2(p-1)} = 1 + p^3 h_3, \dots, \qquad a^{p^{\alpha-1}(p-1)} = 1 + p^{\alpha} h_{\alpha},$$

kur $h_1, h_2, \dots, h_{\alpha}$ ir veseli skaitļi.

Pēdējo formulu var uzrakstīt kā kongruenci

$$a^{p^{\alpha-1}(p-1)} \equiv 1 \pmod{p^{\alpha}}$$

Ja tās abas puses kāpina ar

$$q^{\beta-1}(q-1) \dots r^{\lambda-1}(r-1),$$

tad dabū kongruenci

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

Līdzīgā kārtā pierāda, ka tāda pat kongruence pastāv arī moduļiem $q^{\beta}, \dots, r^{\lambda}$. Tādēļ (§ 20. teor. 2.) tā pastāv arī modulim $m = p^{\alpha} q^{\beta} \dots r^{\lambda}$

Šis pierādījums nav sevišķi elegants. Bez tam te izlieto Fermā teorēmu, ko dabiskāk būtu uzskatīt kā Eulera teorēmas sekas. Tādēļ apskatīsim Eulera teorēmai vēl otru pierādījumu *(Horner* 1826. g*)*, kur izlieto teorēmu par mod m reducēto atlikumu sistēmu (§ 22).

Ja $r_1, r_2, \ldots r_n$ ir $n = \varphi(m)$ skaitļi, kas sastāda mod m reducēto atlikumu sistēmu un $(a, m) = 1$, tad tādu sistēmu sastāda arī skaitļi

$$ar_1, ar_2, \ldots, ar_n,$$

kam jābūt kongruentiem ar pirmās sistēmas skaitļiem $r_1, r_2, \ldots r_n$, bet citādā kārtībā. Domāsim, ka šīs kongruences ir uzrakstītas un sareizinātas. Ja pēc tam abas puses dala ar $r_1 r_2 \ldots r_n$ (to var, jo visi „r“ ir bez kopīga dalītāja ar m), tad rodas kongruence

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

q. e. d.

Fermā mazo teorēmu nevar apgriezt. Tiešām, ja

$$a^{m-1} \equiv 1 \pmod{m},$$

tad nevar secināt, ka m ir pirmskaitlis. Pirmo pretrunīgo piemēru ar

$$m = 37 \cdot 73 \quad \text{un} \quad a = 2$$

deva Likā (*Lucas*) 1876. g. Šinī piemērā skaitlis $m - 1$ dalās ar 36, tā tad arī ar 9. No Fermā teorēmas seko kongruence

$$2^{36} \equiv 1 \pmod{37}$$

Var pārliecināties, ka arī kongruence

$$2^9 \equiv 1 \pmod{73},$$

ir pareiza. No abām pēdējām kongruencēm seko formulas

$$2^{m-1} \equiv 1 \pmod{37} \quad \text{un} \quad 2^{m-1} \equiv 1 \pmod{73},$$

un no tām kongruence

$$2^{m-1} \equiv 1 \pmod{m},$$

kur $m = 37 \cdot 73$ nav pirmskaitlis.

Vēl vienkāršāks piemērs, kas noliedz apgriezto Fermā teorēmu, ir kongruence

$$2^{11 \cdot 31 - 1} \equiv 1 \pmod{11 \cdot 31}.$$

Pareiza ir šāda **apgriezta teorēma.** Ja $(a, m) = 1$ un $a^{m-1} \equiv 1 \pmod{m}$, bet visas kongruences $a^k \equiv 1 \pmod{m}$ ar $0 < k < m-1$ nav iespējamas, tad m ir pirmskaitlis.

Pierādījumam pieņemam pretējo, ka m nav pirmskaitlis. Tad pastāv kongruence

$$a^{\varphi(m)} \equiv 1 \pmod{m} \quad \text{un} \quad \varphi(m) < m - 1.$$

Ar to rodas pretruna teorēmas nosacījumam.

Uzdevumi.

1. Ja $(a, m) = 1$, $aa' \equiv bb' \pmod{m}$ un $a \equiv b \pmod{m}$, tad arī $a' \equiv b' \pmod{m}$.

2. Pierādīt, ka divu nesaīsināmu daļskaitļu summa nevar būt vesels skaitlis, ja saucējiem nav kopīga dalītāja.

3. Pierādīt, ka $(2^{64} + 1) | 274\,177$ un $a^{13} - a$ dalās ar 2730.

4. Pierādīt, ka $5^p - 2 \cdot 3^p + 1$ dalās ar p, ja p ir pirmskaitlis.

5. Ja $a, b, \ldots, k$ ir veseli skaitļi un p ir pirmskaitlis, tad $(a + b + \ldots + k)^p \equiv a^p + b^p + \ldots + k^p \pmod{p}$.

6. Pierādīt formulas:

$$1^m + 2^m + 3^m + \ldots + (p-1)^m \equiv \begin{cases} -1 \pmod{p}, \text{ ja } m | p \\ 0 \pmod{p}, \text{ ja } m \text{ nedalās ar } p \end{cases}$$

$\varphi(a^p) \equiv \varphi(a) \pmod{p}$, ja a nedalās ar p un p ir pirmskaitlis.

7. Pierādīt, ka attiecībā pret moduļiem 7, 11, 13 katrs decimālā sistēmā izteikts skaitlis ir kongruents ar triju pēdējo ciparu skaitli, pamazinātu par pārējo ciparu skaitli.

8. Ja $(a, p) = 1$ un p ir pirmskaitlis, tad $a^{\frac{p(p-1)}{2}} + 1$ vai $a^{\frac{p(p-1)}{2}} - 1$ dalās ar p.

9. Ja $2^{m-1} \equiv 1 \pmod{m}$ un $m | p$, tad pastāv kongruence

$$2^{\frac{m}{p}-1} - 1 \equiv 0 \pmod{p}.$$

V. Pirmās pakāpes jeb lineārās kongruences.

§ 25. Jēdziens par kongruences atrisinājumu jeb sakni.

Ja $f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_n$ ir polinoms ar veseliem koeficientiem un ir sastādīta kongruence

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

tad atrisināt tādu kongruenci nozīmē atrast visus tos skaitļus $x = a$, kam $f(a) \equiv 0 \pmod{m}$.

No § 20. zinām šādu **īpašību**: ja $a \equiv b \pmod{m}$, tad arī

$$f(a) \equiv f(b) \pmod{m}.$$

Tas nozīmē, ka reizē ar skaitli a par dotās kongruences atrisinājumu der arī visa skaitļu klase

$$x \equiv a \pmod{m},$$

ko uzskata par vienu atrisinājumu jeb sakni. Tad kongruences $f(x) \equiv 0 \pmod{m}$ atrisinājumu skaitu nosaka ar derīgo atrisinājumu skaitu moduļa m pilnīgā atlikumu sistēmā.

Kongruenci, kam ikkatrs veselais skaitlis der par sakni, sauc par **identisku kongruenci**. Identiskas kongruences piemēru

$$x^p - x \equiv 0 \pmod{p}$$

dod Fermā mazā teorēma. Otrs piemērs ir katra kongruence $f(x) \equiv 0 \pmod{m}$, kam visi koeficienti dalās ar moduli m. Tādai kongruencei algebrā atbilst vienādojums, kam visi koeficienti ir nulles.

Vispārīgi, kongruencēm skaitļu teorijā lielā mērā atbilst vienādojumi algebrā, bet pastāv arī ievērojamas atšķirības. Tā katram n. pakāpes algebriskam vienādojumam ir tieši n saknes, bet par katru n. pakāpes kongruenci to nevar apgalvot. Piemēram, pirmās

pakāpes kongruencei

$$6x \equiv 3 \pmod 9$$

ir trīs atrisinājumi: 2, 5, 8. Turpretim kongruencei

$$6x \equiv 2 \pmod 9$$

nav neviena atrisinājuma, jeb saka, ka šī kongruence nav iespējama.

§ 26. Atrisināšanas metodes.

Pirmās pakāpes kongruences vispārīgais veids varētu būt šāds:

$$a_1x + b_1 \equiv a_2x + b_2 \pmod m,$$

bet to var pārveidot vienkāršākā veidā, rakstot

$$(a_1 - a_2)\, x \equiv b_2 - b_1 \pmod m,$$

jeb

$$Ax \equiv B \pmod m,$$

kur $A = a_1 - a_2$ un $B = b_2 - b_1$. Ja $A > m$ vai $B > m$, tad šo kongruenci var atvietot ar kongruenci

$$ax \equiv b \pmod m,$$

kuŗā $|a|$ un $|b|$ nav lielāki par $\frac{m}{2}$.

Lai kongruenci atrisinātu, vajadzētu x vietā likt pēc kārtas moduļa m visus kādas pilnīgās atlikumu sistēmas skaitļus (piem. $1, 2, 3, \ldots, m$) un pārbaudīt to derīgumu. Bet dažreiz tāda metode ir pārāk gaŗlaicīga. Tādēļ jāmeklē citi paņēmieni.

Var, piemēram, izlietot Eulera teorēmu (§ 24.): ja $(a, m) = 1$, tad

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

Reizinot abas puses ar b, sastāda kongruenci

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

Tādēļ kongruencei

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

viens atrisinājums ir

$$x \equiv ba^{\varphi(m)-1} \pmod{m}.$$

Šī formula norāda, ka kongruence $ax \equiv b \pmod{m}$ ir iespējama, ja $(a, m) = 1$. Bet x aprēķināšanai tā nav praktiska, jo jau pie nelieliem a un m skaitlis $ba^{\varphi(m)-1}$ var iznākt ļoti liels.

Pierādīsim, ka kongruence $ax \equiv b \pmod{m}$ ar $(a, m) = 1$ ir iespējama un tai eksistē tikai viens atrisinājums.

Tiešām, ja $r_1, r_2, \ldots, r_n$ ir moduļa m reducēta atlikumu sistēma, tad arī $ar_1, ar_2, \ldots, ar_n$ ir tāda sistēma (§ 22). Tādēļ viens un tikai viens ar_k ir kongruents ar 1 attiecībā pret moduli m. No tā seko kongruence

$$ar_k b \equiv b \pmod{m}.$$

un tā tad $a(x_1 - x_2) \mid m$.

Tas nozīmē, ka dotajai kongruencei ir viens atrisinājums

$$x_1 \equiv r_k b \pmod{m}.$$

Ja bez tā eksistētu vēl otrs atrisinājums x_2, tad varētu rakstīt kongruences

$$ax_1 \equiv b \pmod{m}, \quad ax_2 \equiv b \pmod{m}.$$

No tām secinātu kongruenci

$$ax_1 \equiv ax_2 \pmod{m},$$

Tā kā $(a, m) = 1$, tad

$$x_1 \equiv x_2 \pmod{m}.$$

Tā tad x_1 un x_2 atrodas moduļa m vienā un tanī pat atlikumu klasē. Kongruencei $ax \equiv b \pmod{m}$ ir tikai viens atrisinājums.

Var atzīmēt vēl šādu atrisināšanas **metodi**. Ja $ax \equiv b \pmod{m}$, tad

$$(ax - b) \mid m \quad \text{jeb} \quad ax - b = my,$$

kur y ir vesels skaitlis. Tādēļ kongruence

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

ir līdzvērtīga ar nenoteikto vienādojumu

$$ax - my = b,$$

kam atrisināšanas metodes apskatījām §§ 8.—10 Izlietosim šīs metodes, lai analizētu pirmās pakāpes kongruences atsevišķus gadījumus.

§ 27. Pirmās pakāpes kongruences atsevišķi gadījumi.

I. gadījums. Kongruence

$$ax \equiv 1 \pmod{m}$$

ir līdzvērtīga ar nenoteikto vienādojumu

$$ax - my = 1.$$

Ja $(a, m) = 1$, tad vienādojumam var atrast vienu atrisinājumu x_0, y_0. Tā tad

$$ax_0 - my_0 = 1.$$

Var sastādīt homogena tipa vienādojumu

$$a(x - x_0) - m(y - y_0) = 0,$$

kam atbilst kongruence

$$a(x - x_0) \equiv 0 \pmod{m}.$$

Te abas puses ar a var dalīt, jo $(a, m) = 1$. Tad visi dotās kongruences atrisinājumi ir izsakāmi ar formulu

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

Ja vēl ievēro, ka no formulas

$$ax_0 - my_0 = 1$$

seko $(x_0, m) = 1$, tad var izteikt sekojošu **teorēmu**. Ja $(a, m) = 1$, tad kongruencei $ax \equiv 1 \pmod{m}$ ir tikai viens atrisinājums $x \equiv x_0 \pmod{m}$, un šim atrisinājumam ar kongruences moduli nav kopīga dalītāja

Kongruences $ax \equiv 1 \pmod{m}$ atrisinājumu x_0 Eulers sauc par skaitļa a **sabiedroto** (asocieto) **skaitļi attiecībā pret moduli** m. Iepriekšējā teorēma izteic, ka katram skaitlim a, kas ir relātīvs pirmskaitlis ar m, eksistē sabiedrots skaitlis attiecībā pret moduli m.

Ja $(a, m) > 1$, tad attiecīgais nenoteiktais vienādojums un līdz ar to arī kongruence $ax \equiv 1 \pmod{m}$ nav iespējama.

II. gadījums. Kongruence $ax \equiv b \pmod{m}$ ar $(a, m) = 1$.

1. Kad arī $(b, m)=1$,tad šo kongruenci var pārveidot iepriekšējā veidā, pareizinot tās abas puses ar lietderīgi izvēlētu skaitli y. Ir vajadzīgs, lai

$$by \equiv 1 \pmod{m} \quad \text{un} \quad (ay, m) = 1.$$

Pierādīsim, ka tādu y var atrast. Tā kā $(b, m) = 1$, tad kongruence

$$by \equiv 1 \pmod{m}$$

ir iespējama. Tai ir atrisinājums y, kam ar moduli m nav kopīga dalītāja. Tā kā $(y, m) = 1$ un $(a, m) = 1$, tad arī $(ay, m) = 1$.

Te seko šāds **slēdziens.** Ja $(a, m) = 1$ un $(b, m) = 1$, tad kongruence $ax \equiv b \pmod{m}$ ir iespējama, un tai eksistē tikai viens atrisinājums.

2. Ja $(a, m) = 1$ un $(b, m) = d > 1$, tad nenoteiktajam vienādojumam

$$ax - my = b$$

ir derīgi tikai tādi x, kas dalās ar d. Liekam

$$x = d \cdot \xi, \quad b = d \cdot b_1, \quad m = d \cdot m_1.$$

Tad vienādojumu un kongruenci ar d var saīsināt. Dabū iepriekš apskatīto gadījumu

$$a\xi \equiv b_1 \pmod{m_1} \quad \text{ar} \quad (a, m_1) = 1, \ (b_1, m_1) = 1.$$

III. gadījums. Kongruence $ax \equiv b \pmod{m}$ ar $(a, m) = d > 1$.

Ja b nedalās ar d, tad attiecīgais nenoteiktais vienādojums nav atrisināms veselos skaitļos, un tā tad arī dotā kongruence nav iespējama.

Tādēļ pieņemsim, ka $b|d$. Izteicam

$$b = d b_1, \quad a = d a_1, \quad m = d m_1.$$

Tad ar d saīsinot, dabū kongruenci

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

Šī kongruence ir iespējama, un attiecībā pret moduli m_1 tās atrisinājumi ietilpst visi vienā klasē

$$x \equiv x_1 \pmod{m_1}.$$

Attiecībā pret moduli $m = d m_1$ skaitļi

$$x = x_1 + m_1 t$$

sadalās d nekongruentās klasēs, par kuŗu pārstāvjiem var izvēlēties skaitļus

$$x_1 + m_1, \quad x_1 + 2m_1, \quad x_1 + 3m_1, \ldots, x_1 + d m_1.$$

Tiešām, attiecībā pret moduli m divi skaitļi

$$x_1 + k_1 m_1 \quad \text{un} \quad x_1 + k_2 m_1$$

ir kongruenti tikai tad, ja

$$k_1 \equiv k_2 \pmod{d_1}.$$

Tas seko no kongruences

$$x_1 + k_1 m_1 \equiv x_1 + k_2 m_1 \pmod{m} \text{ jeb } k_1 m_1 \equiv k_2 m_1 \pmod{d m_1}.$$

Tā tad, ja $(a, m) = d > 1$ un b nedalās ar d, tad kongruence

$$a x \equiv b \pmod{m}$$

nav iespējama. Ja $b|d$, tad kongruence ir iespējama un moduļa m pilnīgā atlikumu sistēmā tai ir d atrisinājumi.

Piemērs. $12x \equiv 8 \pmod{40}$.

Apzīmēsim $x = 2\xi$. Tad kongruenci ar 8 var saīsināt. Dabū kongruenci

$$3\xi \equiv 1 \pmod 5,$$

kam atrisinājums ir

$$\xi \equiv 2 \pmod 5.$$

Ja reizina ar 2, tad dabū dotās kongruences atrisinājumu

$$x = 2\xi \equiv 4 \pmod{10} \quad \text{jeb} \quad x = 4 + 10t.$$

Attiecībā pret moduli 40 šie skaitļi x sadalās 4 klasēs, kuŗas var noteikt ar skaitļiem

4, 14, 24 un 34.

§ 28. Kongruenču sistēmas.

Ir dota kongruenču sistēma

$$\begin{cases} a_1 x \equiv b_1 \pmod{m_1} \\ a_2 x \equiv b_2 \pmod{m_2}, \end{cases}$$

kuŗai moduļi m_1 un m_2 ir relātīvi pirmskaitļi t. i.,

$$(m_1, m_2) = 1.$$

Ja viena no kongruencēm nav iespējama, tad arī sistēma nav iespējama. Tādēļ pieņemsim, ka abas kongruences ir iespējamas. Ja katru no tām atrisina atsevišķi, tad dabū formulas

$$x \equiv x_1 \pmod{m_1} \quad \text{un} \quad x \equiv x_2 \pmod{m_2}.$$

Pirmo atrisinājumu izteic formā

$$x = x_1 + m_1 y$$

un ievieto otrajā. Tad radīsies kongruence

$$m_1 y \equiv x_2 - x_1 \pmod{m_2}$$

Tā kā $(m_1, m_2) = 1$, tad šī kongruence ir iespējama, un tai ir viens atrisinājums

$$y \equiv y_1 \pmod{m_2} \quad \text{jeb} \quad y = y_1 + tm_2.$$

Ja y ievieto atpakaļ formulā $x = x_1 + m_1 y$, tad dabū rezultātu

$$x = x_1 + m_1 y_1 + t m_1 m_2.$$

Tas nozīmē, ka dotajai sistēmai ir viens atrisinājums, kas uzrakstāms formā

$$x \equiv x_0 \pmod{m_1 m_2}, \quad \text{ja} \quad x_0 = x_1 + m_1 y_1.$$

Vispārīgā gadījumā, kad $(m_1, m_2) > 1$, sistēmas atrisinājumi sastāda vienu skaitļu klasi attiecībā pret moduli m, kas ir m_1 un m_2 mazākais kopīgais dalāmais.

Aprakstīto metodi var izlietot arī triju vai vairāku kongruenču sistēmām tā, ka meklē kopīgos atrisinājumus ik divām sekojošām kongruencēm.

Apskatīsim vēl **Gausa metodi** kongruenču sistēmu atrisināšanai. Šis metodes sākumi bijuši pazīstami jau seno ķīniešu autoriem.

Pieņemsim, ka ik divi no skaitļiem $m_1, m_2, \ldots, m_n$ ir bez kopīga dalītāja. Meklēsim atrisinājumu sistēmai

$$\text{(I)} \quad \begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad \ldots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

Piezīme. Ja izlieto asociētos skaitļus, tad katru pirmās pakāpes kongruenču sistēmu var uzrakstīt tādā formā.

Vispirms konstruēsim n skaitļus $\xi_1, \xi_2, \ldots, \xi_n$ tā, ka

$$\text{(A)} \quad \begin{cases} \xi_1 \equiv 1 \pmod{m_1}, \ \xi_1 \equiv 0 \pmod{m_2}, \ \xi_1 \equiv 0 \pmod{m_3}, \ldots \xi_1 \equiv 0 \pmod{m_n} \\ \xi_2 \equiv 0 \pmod{m_1}, \ \xi_2 \equiv 1 \pmod{m_2}, \ \xi_2 \equiv 0 \pmod{m_3}, \ldots \xi_2 \equiv 0 \pmod{m_n} \\ \quad \ldots \\ \xi_n \equiv 0 \pmod{m_1}, \ \xi_n \equiv 0 \pmod{m_2}, \ \xi_n \equiv 0 \pmod{m_3}, \ldots \xi_n \equiv 1 \pmod{m_n} \end{cases}$$

jeb

$$\xi_k \equiv \begin{cases} 1 \pmod{m_k} \\ 0 \pmod{m_i} \end{cases}, \quad \text{ja} \quad i \neq k.$$

Tādu skaitļu aprēķināšana nav sevišķi grūta. Ja pieņem, ka

$$\xi_1 \equiv 1 \pmod{m_1} \quad \text{jeb} \quad \xi_1 = 1 + m_1 y$$

un pieprasa, lai $\xi_1 | m_2 m_3 \ldots m_n$, tad dabū kongruenci

$$(B) \qquad 1 + m_1 y \equiv 0 \pmod{m_2 m_3 \ldots m_n}$$

un to var atrisināt*). Ja kongruencei (B) viens speciāls atrisinājums ir y_1, tad

$$\xi_1 = 1 + m_1 y_1.$$

Pārējos ξ_i aprēķina pēc tās pašas metodes, un tad dotās sistēmas vispārīgo atrisinājumu var uzrakstīt ar formulu

$$x \equiv x_0 \pmod{m_1 m_2 \ldots m_n}, \quad \text{ja} \quad x_0 = a_1 \xi_1 + a_2 \xi_2 + \ldots + a_n \xi_n.$$

Pierādīsim, ka šis x nozīmes apmierina katru sistēmas kongruenci atsevišķi, un otrādi: ja kāds skaitlis x_1 apmierina sistēmas (I) katru kongruenci, tad $x_1 \equiv x_0 \pmod{m_1 m_2 \ldots m_n}$.

Tiešām, ja liek sistēmas (I) pirmajā kongruencē x vietā x_0 un ievēro, ka

$$\xi_1 \equiv 1 \quad \text{un} \quad \xi_2 \equiv \xi_3 \equiv \ldots \xi_n \equiv 0 \pmod{m_1},$$

tad dabū kongruenci

$$x_0 \equiv a_1 \pmod{m_1}$$

Tamlīdzīgi pierāda, ka

$$x_0 \equiv a_2 \pmod{m_2}, \ldots, x_0 \equiv a_n \pmod{m_n}.$$

Ja pieņem, ka bez x_0 sistēmai eksistē arī atrisinājums x_1, tad var rakstīt formulas

$$x_0 \equiv a_i \pmod{m_i} \quad \text{un} \quad x_1 \equiv a_i \pmod{m_i}, \quad i = 1, 2, \ldots, m.$$

No tām seko kongruences

$$x_1 \equiv x_0 \pmod{m_i}, \quad i = 1, 2, \ldots, m$$

---

*) Var arī pieņemt $\xi_1 = h_1 m_2 m_3 \ldots m_n$, un h_1 aprēķināt tā, lai $\xi_1 \equiv 1 \pmod{m_1}$. Tad h_1 ir asociēts skaitlis ar $m_2 m_3 \ldots m_n$ atiecībā pret moduli m_1.

Ja izlieto § 20 teorēmu 2, tad dabū formulu

$$x_1 \equiv x_0 \pmod{m_1 m_2 \ldots m_n},$$

ar ko viss vajadzīgais ir pierādīts.

Jāpiezīmē, ka skaitļi $\xi_1, \xi_2, \ldots, \xi_n$ ir atkarīgi tikai no moduļu sistēmas $m_1, m_2, \ldots, m_n$ bet nav atkarīgi no atlikumiem $a_1, a_2, \ldots, a_n$. Tādēļ vairākas kongruenču sistēmas ar vienādiem moduļiem var atrisināt ar vienām un tām pašām $\xi_1, \xi_2, \ldots, \xi_n$ nozīmēm.

Ja moduļiem $m_1, m_2, \ldots, m_n$ ir kopīgs dalītājs un sistēma ir iespējama, tad sistēmas kopīgais atrisinājums sastāda vienu skaitļu klasi attiecībā pret moduli m, kas ir skaitļu $m_1, m_2, \ldots, m_n$ mazākais kopīgais dalāmais. Tikai šinī gadījumā ir jālieto jau apskatītā pakāpeniskā ievietošanas metode. Gausa metodi te nevar izlietot: ja, piemēram, modulim m_1 ir kopīgs dalītājs ar kādu no atlikušajiem moduļiem $m_2, m_3, \ldots, m_n$, tad kongruence (B) nav iespējama, un skaitli ξ_1 nevar konstruēt.

§ 29. Vilsona (*Wilson*) teorēma.

Teorēma. Ja p ir pirmskaitlis, tad $(p-1)! + 1$ dalās ar p.

Šo teorēmu bez pierādījuma publicēja E. Uorings savā „*Meditationes algebraicae*" (Kembridžā, 1770. g.) un par tās atradēju minēja juristu Vilsonu (*J. Wilson*). Pirmo pierādījumu deva Lagranžs 1771. g. (sk. § 31). Apskatīsim vispirms Gausa pierādījumu.

Ar $p = 2$ vai 3 teorēmas pareizību var pārbaudīt tieši. Tādēļ pieņemsim $p > 3$. Pierādīsim, ka tad katram rindas

$$2, 3, 4, \ldots, a, \ldots, x, \ldots, p-2$$

skaitlim a turpat rindā ir atrodams asociētais skaitlis $x \neq a$, un dažādiem skaitļiem a atbilst arī dažādi x.

Tiešām, ja pieņem $x = a$, tad kongruence

$$ax \equiv 1 \pmod{p}$$

top par

$$a^2 \equiv 1 \pmod{p}.$$

No pēdējās seko, ka $(a - 1)(a + 1) \mid p$. Tādēļ vai nu $(a - 1) \mid p$, vai arī $(a + 1) \mid p$. Pirmā gadījumā $a = 1$ un otrā $a = p - 1$. Bet tādas a nozīmes 1 un $p - 1$ augšējā rindā nav sastopamas. Bez tam, ja divām a nozīmēm $a_1 > a_2$ atbilstu viens un tas pats x, tad būtu

$$a_1 x \equiv a_2 x \pmod{p}.$$

Te secinātu

$$x(a_1 - a_2) \mid p.$$

Bet tas nav iespējams, jo tiklab x, kā arī $a_1 - a_2$ ir mazāki par p.

Tagad saprotams, ka rindas 2, 3, 4, . . ., $p - 2$ visus skaitļus skaitā $p - 3$ var saistīt $\frac{p-3}{2}$ pāros ($p - 3$ ir pāru skaitlis) tā, ka ikviena pāŗa produkts ir kongruents ar 1 attiecībā pret moduli $p > 3$. Visus pārus sareizinot, dabū kongruenci

$$2 \cdot 3 \cdot 4 \ldots (p - 2) \equiv 1 \pmod{p}.$$

Ja tās abas puses reizina ar $p - 1$, tad dabū formulu

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

Ar to teōrēma ir pierādīta

Apgrieztā teōrēma. Ja skaitlis $N = (m - 1)! + 1$ dalās ar m, tad m ir pirmskaitlis.

Pierādījums. Pieņemsim, ka m nav pirmskaitlis. Tad m dalās ar kādu pirmskaitli $p < m$ un $m = pm_1$. Ja $N \mid m$, tad arī $N \mid p$. Bet tas nav iespējams, jo N ir divu skaitļu summa, no kuŗiem pirmais skaitlis

$$(m - 1)! = 1 \cdot 2 \cdot 3 \ldots p \ldots (m - 1)$$

ar p dalās, bet otrs skaitlis 1 ar p nedalās.

Tā kā tiešā un apgrieztā teorēma ir pareiza, tad Vilsona teorēma der par **kritēriju**, lai izzinātu, vai skaitlis m ir pirmskaitlis, vai salikts. Lai m būtu pirmskaitlis, tad ir nepieciešami un pietiekoši, ka $(m-1)!+1$ dalās ar m Šis kritērijs ir izlietojams dažos teorētiskos jautājumos; praktikā tam nav lielas nozīmes.

Kā Vilsona teorēmas **sekas** var minēt šādu **teorēmu**. Ja $4n+1$ ir pirmskaitlis p, tad var konstruēt divus kvadrātus, kuru summa dalās ar p.

Pierādījums. Ja $p=4n+1$, tad var sastādīt $2n$ kongruences:

$$4n \equiv -1 \pmod{p}$$
$$4n-1 \equiv -2 \pmod{p}$$
$$4n-2 \equiv -3 \pmod{p}$$
$$\ldots\ldots$$
$$2n+1 \equiv -2n \pmod{p}.$$

Ja tās sareizina, tad dabū kongruenci

$$(2n+1)(2n+2)\ldots(4n) \equiv (-1)^{2n}(2n)! \pmod{p}$$

un

$$(4n)! \equiv [(2n)!]^2 \pmod{p},$$

kad iepriekšējai kongruencei abas puses pareizina ar $(2n)!$ Ievērojot Vilsona kongruenci

$$(4n)! = (p-1)! \equiv -1 \pmod{p},$$

var rakstīt formulu

$$[(2n)!]^2 + 1 \equiv 0 \pmod{p}.$$

Ar to teorēma pierādīta.

Uzdevumi

1 Atrisināt kongruences: $32x \equiv 1 \pmod{73}$, $12x \equiv 4 \pmod{20}$, $89x \equiv 1 \pmod{144}$, $11x \equiv 81 \pmod{85}$, $72x \equiv 27 \pmod{75}$.

2. Sadalīt skaitli 100 divās daļās tā, lai pirmā daļa, dalīta ar 5, dotu atlikumā 2, bet otrā, dalīta ar 7, dotu atlikumā 4

3. Atrast mazāko skaitli, kas dalīts ar 67, 15, 7, dotu atlikumā attiecīgi 10, 13, 5.

4. Atrast visus tos skaitļus, kas dalīti ar 11 dod atlikumā 3, dalīti ar 19, dod atlikumā 5 un, dalīti ar 28, dod atlikumā 10.

5. Ar Gausa metodi atrisināt sistēmas:

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

VI. Augstāku pakāpju kongruences.

§ 30. Kongruences moduļa reducēšana.

Pieņemsim, ka ir dota kongruence šādā vispārīgā veidā:

$$A_0x^n + A_1x^{n-1} + \ldots + A_n = B_0x^k + B_1x^{k-1} + \ldots + B_k \pmod{m}.$$

Ja visus locekļus pārnes vienā pusē, savelk līdzīgos locekļus un katra koeficienta vietā ņem kongruentu skaitli ar absolūto nozīmi $\leqslant \frac{m}{2}$, tad rodas kongruence normālā veidā

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n \equiv 0 \pmod{m}.$$

Var gadīties, ka polinoma $f(x)$ visi koeficienti $a_0, a_1, \ldots, a_n$ dalās ar moduli, tad $f(x) \equiv 0 \pmod{m}$ ir identiska kongruence (x vietā var likt katru veselu skaitli). Apgrieztais apgalvojums nav pareizs. Ir kongruences $f(x) \equiv 0 \pmod{p}$, kur x vietā var likt katru skaitli, tomēr visi $f(x)$ koeficienti ar moduli nedalās. Viens tāds piemērs ir kongruence

$$x^p - x \equiv 0 \pmod{p}.$$

Pierādīsim, ka kongruence

$$f(x) \equiv 0 \pmod{p^\alpha q^\beta \ldots r^\lambda}$$

ir līdzvērtīga ar kongruenču sistēmu

$$\text{(A)} \qquad \begin{cases} f(x) \equiv 0 \pmod{p^\alpha} \\ f(x) \equiv 0 \pmod{q^\beta} \\ \quad \ldots \\ f(x) \equiv 0 \pmod{r^\lambda}, \end{cases}$$

t i. katrs dotās kongruences atrisinājums x_0 der arī sistēmai (A), un katrs sistēmas (A) atrisinājums x_1 der dotai kongruencei.

Tiešām, ja

$$f(x_0) \mid p^\alpha q^\beta \ldots r^\lambda,$$

tad arī

$$f(x_0) \mid p^\alpha, \quad f(x_0) \mid q^\beta, \ldots, f(x_0) \mid r^\lambda.$$

Otrādi, ja

$$f(x_1) \mid p^\alpha, \quad f(x_1) \mid q^\beta, \ldots, \quad f(x_1) \mid r^\lambda,$$

tad $f(x_1)$ dalās arī ar skaitļu p^α, q^β, . . ., r^λ mazāko kopīgo dalāmo $p^\alpha q^\beta \ldots r^\lambda$.

Kongruenču sistēmu (A) atrisina tā, ka atrisina tās katru kongruenci atsevišķi ar formulām

$$x \equiv a \pmod{p^\alpha}, \quad x \equiv b \pmod{q^\beta}, \ldots, \quad x \equiv h \pmod{r^\lambda}.$$

Tad atrod kopīgo atrisinājumu, kas uzrakstāms formā

$$x \equiv x_1 \pmod{p^\alpha q^\beta \ldots r^\lambda}.$$

Lai atrisinātu kongruenci

$$f(x) \equiv 0 \pmod{m} \quad \text{ar} \quad m = p^\alpha q^\beta \ldots r^\lambda$$

ir jāprot atrisināt vienkāršākās formas kongruence

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

Pierādīsim, ka tās atrisināšana reducējas uz kongruences

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

atrisināšanu. Konstatēsim, ka kongruences

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

katrs atrisinājums x_1 der arī kongruencei

$$f(x) \equiv 0 \pmod{p^{\alpha-1}}.$$

Tiešām, ja $f(x_1) | p^{\alpha}$, tad arī $f(x_1) | p^{\alpha-1}$, bet n e o t r ā d i. Tas nozīmē, ka visi pirmās kongruences atrisinājumi ietilpst otrās kongruences atrisinājumos, bet ne katrs otrās kongruences atrisinājums ir derīgs pirmajai.

Pieņemsim, ka kongruenci

$$f(x) \equiv 0 \pmod{p^{\alpha-1}}$$

protam atrisināt, un viens tās atrisinājums ir

$$x \equiv a \pmod{p^{\alpha-1}}$$

jeb

$$x = a + yp^{\alpha-1}.$$

Meklēsim tādas y nozīmes, ar kuŗām iepriekšējā izteiksme dod arī kongruences

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

atrisinājumu. Tā tad

$$f(a + yp^{\alpha-1}) \equiv 0 \pmod{p^{\alpha}}.$$

Te izlieto T e i l o r a f o r m u l u

$$f(a + h) = f(a) + hf'(a) + h^2\frac{f''(a)}{2!} + \ldots + h^n\frac{f^{(n)}(a)}{n!},$$

kur visi koeficienti $f'(a), \frac{f''(a)}{2!}, \ldots, \frac{f^{(n)}(a)}{n!}$ ir veseli skaitļi, kad a ir vesels. Ja ievēro, ka

$$f(a) \equiv 0 \pmod{p^{\alpha-1}},$$

tad

$$C = \frac{f(a)}{p^{\alpha-1}}$$

ir vesels un zināms skaitlis. Sastādīto kongruenci

$$f(a+yp^{\alpha-1}) = Cp^{\alpha-1} + yp^{\alpha-1}f'(a) + y^2p^{2(\alpha-1)}\frac{f''(a)}{2!} + \ldots +$$

$$+ y^np^{n(\alpha-1)}\frac{f^{(n)}(a)}{n!} \equiv 0 \pmod{p^{\alpha}}$$

ar $p^{\alpha-1}$ var saīsināt. Ja pēc tam vēl atmet tos locekļus, kas dalās ar moduli, tad paliek pirmās pakāpes kongruence

(XII) $$C + y.f'(a) \equiv 0 \pmod{p}$$

Ir iespējami sekojošie **trīs gadījumi.**

1. Ja $f'(a) | p$, bet C nedalās ar p, tad kongruence (XII) un līdz ar to arī kongruence

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

n a v i e s p ē j a m a.

2. Ja $f'(a)$ nedalās ar p, tad kongruencei (XII) ir tikai viena atrisinājumu klase

$$y \equiv y_0 \pmod{p}.$$

Kongruences

$$f(x) \equiv 0 \pmod{p^{\alpha-1}}$$

atrisinājumam

$$x \equiv a \pmod{p^{\alpha-1}}$$

atbilst tikai v i e n s kongruences

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

a t r i s i n ā j u m s

$$x \equiv a + y_0 p^{\alpha-1} \pmod{p^{\alpha}}.$$

3. Ja $f'(a) | p$ un $C | p$, tad kongruencei (XII) par sakni der katrs

$$y \equiv 0, 1, 2, \ldots, p - 1.$$

Šinī gadījumā kongruencēm

$$f(x) \equiv 0 \pmod{p^{\alpha}} \quad \text{un} \quad f(x) \equiv 0 \pmod{p^{\alpha-1}}$$

ir k o p ī g s a t r i s i n ā j u m s

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

Moduļa reducēšanu parasti sāk ar kongruenci

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

Ja tai saknes ir zināmas, tad ar tikko apskatīto metodi var atrisināt kongruenci modulim p^2, tad modulim p^3, . . ., un beidzot arī modulim p^α.

Piemēri. 1. Viens kongruences

$$f(x) = x^3 - x^2 - 2 \equiv 0 (\mathrm{mod}\ 7)$$

atrisinājums ir $x_1 \equiv -2 (\mathrm{mod}\ 7)$. Atrast kongruences $f(x) \equiv 0 (\mathrm{mod}\ 7^2)$ atrisinājumu.

Šinī gadījumā

$$a = -2,\ f(a) \equiv -14,\ C = -2,\ f'(x) = 3x^2 - 2x \text{ un } f'(a) = 16.$$

No formulas (XII) seko kongruence

$$-2 + 16y \equiv 0 (\mathrm{mod}\ 7),$$

kuŗai atrisinājums ir

$$y \equiv 1 (\mathrm{mod}\ 7) \quad \text{jeb} \quad y = 1 + 7t.$$

Tādēļ kongruencei

$$f(x) \equiv 0 (\mathrm{mod}\ 7^2)$$

viena sakne ir

$$x = -2 + 7(1 + 7t) \quad \text{jeb} \quad x \equiv 5 (\mathrm{mod}\ 7^2).$$

2. Dotai kongruencei $f(x) = x^3 - x^2 - 2 \equiv 0 (\mathrm{mod}\ 7)$ viens atrisinājums $x_1 \equiv -2 (\mathrm{mod}\ 7)$. Jāatrod kongruences $f(x) \equiv 0 (\mathrm{mod}\ 7^5)$ atrisinājums.

Pieņemsim, ka $f(x) \equiv 0 (\mathrm{mod}\ 7^5)$ atrisinājums ir

$$x = 7a - 2 \quad \text{ar} \quad |a| \leqslant 7^4.$$

Šo x nozīmi ievietojot kongruencē, dabūjam

$$f(x) = (7a - 2)^3 - (7a - 2)^2 - 2 \equiv 0 (\mathrm{mod}\ 7^5).$$

Ja atveŗ iekavas un saīsina ar 7, tad paliek kongruence

$$7^2(a^3 - a^2) + 16a - 2 \equiv 0 (\mathrm{mod}\ 7^4)$$

Pazeminām moduli no 7^4 līdz 7, tad rodas kongruence

$$16a - 2 \equiv 0 (\mathrm{mod}\ 7)$$

ar atrisinājumu

$$a \equiv 1 \pmod 7 \quad \text{jeb} \quad a = 1 + 7t.$$

Ja šo a nozīmi liek atpakaļ kongruencē ar moduli 7^4 un atmet locekļus, kas dalās ar 7^4, tad paliek kongruence

$$7^3 . t + 7 . 16t + 2 . 7 \equiv 0 \pmod{7^4}.$$

Ja saīsina ar 7, tad dabū kongruenci

$$65t + 2 \equiv 0 \pmod{7^3}$$

ar atrisinājumu

$$t \equiv 153 \pmod{7^3} \quad \text{jeb} \quad t = 153 + 7^3 k.$$

Tagad var aprēķināt

$$x = 7a - 2 = 7(1 + 7t) - 2 = 5 + 7^2 . 153 + 7^5 k$$

jeb

$$x \equiv 5 + 7^2 . 153 \pmod{7^5},$$

t. i.

$$x \equiv 7502 \pmod{7^5}.$$

Kā blakus rezultātu te var secināt kongruences

$$f(x) \equiv 0 \pmod{7^n} \quad (n < 5)$$

atrisinājumu. Piemēram, ja $n = 3$, tad $x \equiv 7502 \equiv -44 \pmod{7^3}$.

§ 31. Kongruences, kam modulis ir pirmskaitlis.

Tagad apskatīsim tikai tādas kongruences

$$a_0 x^n + a_1 x^{n-1} + \ldots + a_n \equiv 0 \pmod p,$$

kam modulis ir pirmskaitlis p, un augstākā locekļa koeficients a_0 ar moduli nedalās. Tad $(a_0, p) = 1$, un no kongruences

$$a_0 y \equiv 1 \pmod p$$

var atrast koeficientam a_0 asc ēto skaitli y. Ja ar to pareizina doto kongruenci, tad augstākā locekļa koeficients top $\equiv 1 \pmod p$.

Tādēļ turpmāk pieņemsim, ka kongruencē $f(x) \equiv 0 \pmod{p}$ augstākā locekļa koeficients ir 1, t. i.

$$f(x) = x^n + a_1 x^{n-1} + \ldots + a_n.$$

Teorēma. Ja modulis ir pirmskaitlis p, tad kongruences pakāpi n var samazināt līdz nozīmei $\leqslant p - 1$.

Pierādījums. Ja $f(x)$ dalot ar $x^p - x$ dalījumā dabū $q(x)$ un atlikumā polinomu $r(x)$ ar pakāpi $\leqslant p - 1$, tad ir sakars

$$f(x) = (x^p - x)q(x) + r(x).$$

No tā redzam, ka kongruences

$$f(x) \equiv 0 \pmod{p} \quad \text{un} \quad r(x) \equiv 0 \pmod{p}$$

ir līdzvērtīgas, t. i. abām ir vienas un tās pašas saknes. Tiešām, ja x_1 ir kongruences

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

sakne, tad $f(x_1) \mid p$. Tā kā pēc Fermā teorēmas $(x_1^p - x_1) \mid p$, tad no augšējās identitātes seko arī

$$r(x_1) \mid p \quad \text{jeb} \quad r(x_1) \equiv 0 \pmod{p}.$$

Tamlīdzīgi pierāda, ka kongruences $r(x) \equiv 0 \pmod{p}$ katra sakne ir arī kongruences $f(x) \equiv 0 \pmod{p}$ sakne.

Visā turpmākā teorijā apskatīsim tikai tādas kongruences, kam pakāpe $n \leqslant p - 1$.

Lemma. Ja a ir n. pakāpes kongruences $f(x) \equiv 0 \pmod{p}$ sakne, tad kongruenci var uzrakstīt formā

$$(x - a)f_1(x) \equiv 0 \pmod{p},$$

kur $f_1(x)$ ir polinoms ar veseliem koeficientiem un pakāpi $n - 1$.

No algebras zinām*), ka $f(x) - f(a)$ dalās bez atlikuma ar $x - a$. Tādēļ var izteikt

$$f(x) - f(a) = (x - a)\, f_1(x).$$

Ja ievēro, ka $f(a) \equiv 0 \pmod{p}$, tad seko kongruence

$$f(x) \equiv (x - a) f_1(x) \equiv 0 \pmod{p}.$$

Lagranža teorēma. Ja modulis p ir pirmskaitlis, tad n. pakāpes kongruencei $f(x) \equiv 0 \pmod{p}$ nevar būt vairāk kā n atrisinājumu.

Par pirmās pakāpes kongruenci teorēma ir pārbaudīta jau § 27. Pieņemsim, ka teorēma ir pareiza arī $2, 3., \ldots, (n-1)$. pakāpes kongruencēm, bet n. pakāpes kongruencei

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

būtu vismaz $n + 1$ saknes

$$a_1, a_2, a_3, \ldots, a_n \quad \text{un} \quad a,$$

kur $|a|$ un visi $|a_k|$ ar $k = 1, 2, \ldots, n$ ir dažādi skaitļi un mazāki kā p. Tad ar iepriekšējo lemmu var uzrakstīt kongruenci

$$f(x) \equiv (x - a) f_1(x) \equiv 0 \pmod{p},$$

Te

$$f_1(x) \equiv 0 \pmod{p}$$

ir $(n-1)$. pakāpes kongruence, kam pēc pieņēmuma nav vairāk kā $n - 1$ sakņu. Tas nozīmē, ka starp skaitļiem $a_1, a_2, \ldots, a_n$ ir vismaz viens tāds a_k, kas neder šai kongruencei

Tā kā

$$f(a_k) \equiv 0 \pmod{p},$$

---

*) Pierādījums. Ja $f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n$, tad no formulas

$$f_1(x) = \frac{f(x) - f(a)}{x - a} = a_0 \frac{x^n - a^n}{x - a} + a_1 \frac{x^{n-1} - a^{n-1}}{x - a} + \ldots a_{n-1} \frac{x - a}{x - a}$$

redzam, ka $f_1(x)$ ir polinoms ar veseliem koeficientiem. No tā seko, ka $f(x) - f(a)$ dalās ar $x - a$.

tad var rakstīt kongruenci

$$(a_k - a)\, f_1(a_k) \equiv 0 \pmod{p}.$$

Ja to saīsina ar $f_1(a_k)$, tad dabū formulu

$$a_k - a \equiv 0 \pmod{p}.$$

Tādēļ

$$(a_k - a) \mid p.$$

Bet tas nav iespējams, jo $|a_k - a| < p$.

Sekas. Ja $f(x) \equiv 0 \pmod{p}$ ir identiska kongruence, tad vai nu $f(x)$ pakāpe ir p, vai arī $f(x)$ visi koeficienti dalās ar p.

Tas nozīmē sekošu. Ja n. pakāpes kongruencei $f(x) \equiv 0 \pmod{p}$ modulis ir pirmskaitlis p, pakāpe $n < p$ un vairāk kā n atrisinājumu, tad visi kongruences koeficienti dalās ar p.

Šo piezīmi var izlietot Vilsona teorēmas pierādījumam pēc Lagranža metodes (1771. g.). Apskatām kongruenci

$$(x-1)(x-2)x-3)\ldots[x-(p-1)] - (x^{p-1}-1) \equiv 0 \pmod{p},$$

kam pakāpe $p-2$, bet atrisinājumi skaitļi $1, 2, 3, \ldots, p-1$ skaitā $p-1$. Tādēļ visi kongruences koeficienti dalās ar moduli. Starp citu, arī brīvais loceklis

$$(p-1)! + 1 \qquad (p > 2)$$

dalās ar p. Vilsona kongruences pareizību tieši pārbauda gadījumā, kad $p = 2$.

Ja n. pakāpes kongruencei $f(x) \equiv 0 \pmod{p}$ ir n saknes, tad saka, ka tai ir **maksimālais sakņu skaits.**

Piemērs. Katrai identiskai p. pakāpes kongruencei

$$x^p - x - pf(x) \equiv 0 \pmod{p}$$

ir maksimālais sakņu skaits.

Teorēma. Ja kongruencei $f(x) \equiv 0 \pmod{p}$ ir maksimālais sakņu skaits un $f(x)$ sadalās divos reizinātājos:

$$f(x) = g(x) \cdot h(x),$$

tad arī kongruencēm $g(x) \equiv 0 \pmod{p}$ un $h(x) \equiv 0 \pmod{p}$ katrai atsevišķi ir maksimālais sakņu skaits.

Tiešām, pieņemsim, ka polinomu $f(x)$, $g(x)$ un $h(x)$ pakāpes ir attiecīgi n,k un j. Tad

$$n = k + j.$$

Ja vienai no kongruencēm

$$g(x) \equiv 0, \quad h(x) \equiv 0 \pmod{p}$$

sakņu skaits būtu mazāks par maksimālo, tad otrās kongruences sakņu skaitam jābūt lielākam par maksimālo. Bet tas pēc Lagranža teorēmas nav iespējams.

Tagad apskatīsim Čebiševa kritēriju (1849. g.), ar ko var izšķirt jautājumu, vai kongruencei $f(x) \equiv 0 \pmod{p}$ ir maksimālais sakņu skaits, vai mazāks par n. Pēc norunas $f(x)$ pakāpe n ir $\leqslant p - 1$. Tādēļ $x^p - x$ var dalīt ar $f(x)$ un dabūt atlikumu $R(x)$, kam pakāpe ir $\leqslant n - 1$. Tad pastāv sakars

$$x^p - x = f(x) \cdot Q(x) + R(x).$$

Čebiševa kritērijs. Lai kongruencei $f(x) \equiv 0 \pmod{p}$ būtu maksimālais sakņu skaits, ir nepieciešami un pietiekoši, ka atlikuma $R(x)$ visi koeficienti dalās ar p.

Tiešām, ja kongruencei

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

ir n saknes $x_1, x_2, \ldots, x_n$, tad tās visas der arī kongruencei

$$R(x) \equiv 0 \pmod{p},$$

kam pakāpe ir mazāka kā n. Tādēļ $R(x)$ visiem koeficientiem ir jādalās ar p.

Otrādi: ja $R(x)$ visi koeficienti dalās ar p, tad

$$f(x) \cdot Q(x) \equiv 0 \pmod{p}$$

ir identiska kongruence ar pakāpi p. Tādēļ tās sakņu skaits ir maksimālais, un no tā seko maksimālais sakņu skaits arī kongruencei

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

Jāpiezīmē, ka

$$f(x) \equiv 0 \quad \text{un} \quad Q(x) \equiv 0 \pmod{p}$$

atsevišķi nav identiskas kongruences, jo to pakāpes ir zemākas kā p un vismaz $f(x)$ un $Q(x)$ augstāko locekļu koficienti ar p nedalās.

Piemērs. Kongruence $f(x) = x^3 - x^2 - 2 \equiv 0 \pmod{7}$,

Tās sakņu skaita noteikšanai jāmeklē $f(x)$ un $x^7 - x$ augstākais kopīgais dalītājs. Polinoma $x^7 - x$ dalīšanā ar $f(x)$ rodas atlikums

$$R(x) = 7x^2 + 5x + 10.$$

Kongruencei $R(x) \equiv 0 \pmod{7}$ ir visas tās pašas saknes, kas dotajai kongruencei $f(x) \equiv 0 \pmod{7}$. Bet

$$R(x) \equiv 5x + 3 \equiv 0 \pmod{7}$$

ir tikai viena sakne

$$x \equiv -2 \pmod{7},$$

kas der arī dotajai kongruencei. Tādēļ vairāk sakņu nav arī dotajai kongruencei

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

Uzdevumi.

1. Atrisināt kongruences:

$x^3 + x^2 - 1 \equiv 0 \pmod{11^2}$; $x^4 - 8x^3 + 9x^2 + 9x + 14 \equiv 0 \pmod{25}$;

$x^4 + 6x^3 - 8x^2 + 13x + 5 \equiv 0 \pmod{7}$; $x^3 - x^2 - 2x \equiv 0 \pmod{5}$;

$$x^3 - 2x^2 + 1 \equiv 0 \pmod{128}.$$

2. Pierādīt teorēmu: ja p ir pirmskaitlis un par x_1, x_2 ņem visos iespējamos veidos divus dažādus skaitļus no rindas $1, 2, 3, \ldots, p - 1$, tad

$$\Sigma x_1 x_2 \equiv 0 \pmod{p}.$$

3. Noteikt, cik atrisinājumu klašu ir kongruencei

$$x^{p-2} + x^{p-3} + \ldots + x + 1 \equiv 0 \pmod{p}?$$

VII. Otrās pakāpes jeb kvadrātiskās kongruences.

§ 32. Kongruences kanoniskā forma.

Otrās pakāpes kongruenci ar moduli 2 apskatīsim atsevišķi.

Ja modulis ir pirmskaitlis p, tad kongruences pakāpi var samazināt līdz nozīmei $\leqslant p-1$. Tādēļ katra kongruence ar moduli 2 ir līdzvērtīga pirmās pakāpes kongruencei ar to pašu moduli. Ja ir dota otrās pakāpes kongruence

$$ax^2 + bx + c \equiv 0 \pmod 2 \qquad (a, b, c \text{ — veseli skaitļi}),$$

tad to var pārveidot par

$$ax^2 + ax - ax + bx + c \equiv 0 \pmod 2$$

jeb

$$ax(x+1) + (b-a)x + c \equiv 0 \pmod 2.$$

Viens no diviem sekojošiem veseliem skaitļiem x un $x+1$ ir pāru skaitlis. Tādēļ reizinājums $ax(x+1)$ dalās ar 2, un paliek pirmās pakāpes kongruence

$$(b-a)x + c \equiv 0 \pmod 2$$

jeb citādā apzīmējumā

$$Ax + B \equiv 0 \pmod 2,$$

kur A un B ir 0 vai 1.

Ja $A = 0$, tad arī B jābūt nullei, un x vietā var likt katru skaitli.

Ja $A = 1$, $B = 0$, tad x ir kaut kuŗš pāru skaitlis.

Bet ja A un B abi ir 1, tad x ir nepāru skaitlis.

Turpmāk apskatīsim kongruenci

(1) $$ax^2 + bx + c \equiv 0 \pmod p,$$

kam modulis p ir nepāru pirmskaitlis ($p > 2$). Ja a nedalās ar p, tad $(a, p) = 1$ un kongruenci var reizināt ar $4a$ Tad dabū kongruenci

$$4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{p}, \tag{2}$$

kas ir līdzvērtīga ar doto. Tiešām, ja kongruences (2) sakne ir x_0, tad no

$$4a\,(ax_0^2 + bx_0 + c) \equiv 0 \pmod{p} \quad \text{un} \quad (4a, p) = 1$$

seko

$$ax_0^2 + bx_0 + c \equiv 0 \pmod{p}.$$

Tā tad kongruences (2) sakne ir arī kongruences (1) sakne, un, saprotams, arī otrādi.

Kongruenci (2) var pārveidot par

$$4a^2x^2 + 4abx + b^2 \equiv b^2 - 4ac \pmod{p}$$

jeb

$$(2ax + b)^2 \equiv b^2 - 4ac \pmod{p}.$$

Ja apzīmē

$$2ax + b = z \quad \text{un} \quad b^2 - 4ac = q$$

(te q nav domāts pirmskaitlis), tad dabū otrās pakāpes kongruences kanonisko formu

$$z^2 \equiv q \pmod{p}.$$

Ja tās atrisinājums

$$z \equiv z_0 \pmod{p}$$

būtu zināms, tad kongruences (1) atrisinājumu x varētu atrast no pirmās pakāpes kongruences

$$2ax + b \equiv z_0 \pmod{p},$$

kas ir iespējama, jo $(2a, p) = 1$.

§ 33. Moduļa kvadrātiskie atlikumi.

Ja dota otrās pakāpes kongruence, piem.

$$x^2 \equiv 8 \pmod{13},$$

tad saknes var meklēt tā, ka x vietā liek pēc kārtas skaitļus 1, 2, 3, . . ., 12. Ja uzraksta šo skaitļu kvadrātu atlikumus attiecībā pret moduli 13, tad dabū moduļa 13 kvadrātisko atlikumu virkni

$$1, 4, 9, 3, 12, 10, 10, 12, 3, 9, 4, 1.$$

No tās redzam, ka nav tāda skaitļa, kuŗa kvadrāts, dalīts ar 13, dotu atlikumā 8. Tādēļ kongruence $x^2 \equiv 8 \pmod{13}$ nav iespējama.

Definīcija. Visus tos skaitļus q, kas nedalās ar p un kuŗiem kongruence $x^2 \equiv q \pmod{p}$ ir iespējama, sauc par moduļa p **kvadrātiskiem atlikumiem**, bet tos q, kam šī kongruence nav iespējama par moduļa p **kvadrātiskiem neatlikumiem**.

Iepriekšējā piemērā moduļa 13 kvadrātiskie atlikumi ir skaitļi 1, 3, 4, 9, 10, 12, bet neatlikumi 2, 5, 6, 7, 8, 11.

Noskaidrosim, ka modulim p kvadrātisku atlikumu un neatlikumu ir vienāds skaits.

Uzrakstīsim visus pozitīvos veselos skaitļus, kas mazāki par moduļa pusi, t. i. skaitļus

$$x = 1, 2, 3, \ldots, \frac{p-1}{2}.$$

Kāpināsim tos kvadrātā un dalīsim ar p. Tad radīsies skaitā $\frac{p-1}{2}$ moduļa p kvadrātiskie atlikumi

$$r_1, r_2, r_3, \ldots, r_{\frac{p-1}{2}}.$$

Tie visi ir dažādi. Tiešām, ja pieņem

$$r_i = r_j, \quad 1 \leqslant j < i \leqslant \frac{p-1}{2},$$

tad dabū kongruenci

$$i^2 \equiv j^2 \pmod{p} \quad \text{jeb} \quad i^2 - j^2 \equiv 0 \pmod{p}.$$

No tās seko, ka

$$(i-j)(i+j) \mid p.$$

Bet tas nav iespējams, jo katrs no skaitļiem $i-j$ un $i+j$ ir mazāks par p.

Ja skaitļu x rindu turpina pāri moduļa p pusei, tad atkārtojas tie paši kvadrātiskie atlikumi, jo pastāv formula

$$(p-i)^2 \equiv i^2 \pmod{p}.$$

Tādēļ, ja ignorē gadījumu $q=0$, tad moduļa p kvadrātisko atlikumu $q<p$ skaits ir $\frac{p-1}{2}$. Pārējie $\frac{p-1}{2}$ skaitļi ir moduļa p kvadrātiskie neatlikumi. Ar to ir pierādīts, ka kvadrātisko atlikumu un neatlikumu ir vienāds skaits.

Piezīme. Jēdziens par kvadrātiskiem atlikumiem, resp. neatlikumiem, attiecināms arī moduļiem, kas ir **salikti skaitļi**. Tādā gadījumā kvadrātisko atlikumu un neatlikumu skaits vispārīgi nav vienāds. Piemēram, lai atrastu skaitļa **12** kvadrātiskos atlikumus, kāpinām

$$0, 1, 2, 3, 4, 5, 6$$

kvadrātā

$$0^2, 1^2, 2^2, 3^2, 4^2, 5^2, 6^2$$

un dalām ar 12. Rodas dalīšanā atlikumi

$$0, 1, 4, 9, 4, 1, 0.$$

Tā tad moduļa 12 kvadrātiskie atlikumi 0, 1, 4, 9 ir skaitā 4, bet kvadrātiskie neatlikumi 2, 3, 5, 6, 7, 8, 10, 11 skaitā 8.

§ 34. Eulera kritērijs.

No identitātes

$$(p-x_1)^2 \equiv x_1^2 \pmod{p}$$

var secināt sekošo. Ja kongruencei $x^2 \equiv q \pmod{p}$ ir viena sakne x_1, tad tai ir arī vēl otra sakne

$$x_2 = p - x_1$$

un $x_2 \neq x_1$. Pretējā gadījumā, kad $x_2 = x_1$, pirmskaitlis p būtu pāru skaitlis $= 2x_1$. Tā tad, ja kongruence

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

ir iespējama, tad kongruences sakņu skaits ir maksimālais. Tādēļ no Čebiševa kritērija var atvasināt kritēriju, ar ko izšķirt, vai kongruence $x^2 \equiv q \pmod{p}$ ir iespējama, vai nav.

Ja kongruence $x^2 \equiv q \pmod{p}$ ir iespējama un polinomu $x^p - x$ dala ar $x^2 - q$, tad dalīšanas atlikuma $R(x)$ koeficientiem ir jādalās ar p. Šis nosacījums ir nepieciešams un pietiekošs.

Noteiksim atlikumu $R(x)$ ar sekojošiem pārveidojumiem:

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

jeb

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

Tā kā izteiksme $a^n - b^n$ vienmēr dalās ar $a - b$, tad arī $(x^2)^{\frac{p-1}{2}} - q^{\frac{p-1}{2}}$ dalās ar $x^2 - q$. Dalot $x^p - x$ ar $x^2 - q$, dabūjam atlikumu

$$R(x) = (q^{\frac{p-1}{2}} - 1)\, x.$$

Varam formulēt sekošu **kritēriju**, ko devis **Eulers**. Lai kongruence $x^2 \equiv q \pmod{p}$ būtu iespējama, ir nepieciešami un pietiekoši, ka

$$(q^{\frac{p-1}{2}} - 1) \mid p \quad \text{jeb} \quad q^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Piezīme. Ja q nedalās ar p, tad $q^{\frac{p-1}{2}}$ attiecībā pret moduli p ir kongruents vai nu ar $+1$, vai -1. To pierāda ar Fermā mazo teorēmu. Tiešām, ja q nedalās ar p, tad

$$q^{p-1} - 1 \equiv 0 \pmod{p}$$

jeb

$$(q^{\frac{p-1}{2}} - 1)(q^{\frac{p-1}{2}} + 1) \equiv 0 \pmod{p}.$$

Tā kā abi faktori reizē ar p nedalās (to starpība ir 2 un 2 ne-

dalās ar p), tad iespējami tikai sekojošie **divi gadījumi.** Pirmā gadījumā

$$(q^{\frac{p-1}{2}} - 1) \mid p \quad \text{jeb} \quad q^{\frac{p-1}{2}} \equiv 1 \pmod{p},$$

un kongruence $x^2 \equiv q \pmod{p}$ ir iespējama. Otrā gadījumā

$$q^{\frac{p-1}{2}} \equiv -1 \pmod{p},$$

un, saprotams, kongruence $x^2 \equiv q \pmod{p}$ nav iespējama.

Piemērs. Kongruence $x^2 \equiv 8 \pmod{13}$ nav iespējama, jo

$$8^{\frac{13-1}{2}} = 8^6 \equiv 5^6 \equiv 25^3 \equiv (-1)^3 \equiv -1 \pmod{13}.$$

§ 35. Ležandra (*Legendre*) simbols.

Pirmā definīcija. Ja p ir pirmskaitlis, kas lielāks par 2 un q nedalās ar p, tad Ležandra simbols

$$\left(\frac{q}{p}\right) = \begin{cases} +1, \text{ ja } q \text{ ir moduļa } p \text{ kvadrātiskais atlikums,} \\ -1 \text{ pretējā gadījumā.} \end{cases}$$

Otrā definīcija. Ležandra simbols $\left(\frac{q}{p}\right)$ ir $+1$ vai -1 un

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

Piemēri. Katrs kradrāts m^2 ir moduļa p kvadrātisks atlikums. Tādēļ

$$\left(\frac{m^2}{p}\right) = +1.$$

Arī $\left(\frac{1}{p}\right) = +1$, bet $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$ jeb

$$\left(\frac{-1}{p}\right) = \begin{cases} +1, \text{ ja } p = 4n+1 \\ -1, \text{ ja } p = 4n+3. \end{cases}$$

Šo rezultātu (tikai citādā formā) ir izteicis jau Eulers.

Ležandra simbola īpašības.

1. Ja $q_1 \equiv q_2 \pmod{p}$, tad $\left(\frac{q_1}{p}\right) = \left(\frac{q_2}{p}\right)$,

t. i. kongruence $x^2 \equiv q \pmod{p}$ ir iespējama vai neiespējama reizē visiem skaitļiem q, kas atrodas vienā un tanī pat moduļa p atlikumu klasē.

Pierādījums. No $q_1 \equiv q_2 \pmod{p}$ seko kongruence

$$q_1^{\frac{p-1}{2}} \equiv q_2^{\frac{p-1}{2}} \pmod{p} \quad \text{jeb} \quad \left(\frac{q_1}{p}\right) - \left(\frac{q_2}{p}\right) \equiv 0 \pmod{p}.$$

Šī kongruence ir iespējama tikai tad, ja simboli $\left(\frac{q_1}{p}\right)$ un $\left(\frac{q_2}{p}\right)$ ir vienlīdzīgi. Pretējā gadījumā dabū kongruenci

$$2 \equiv 0 \pmod{p},$$

kas nav iespējama, jo $p > 2$.

2. Ja $q \equiv q_1 q_2 \pmod{p}$, tad $\left(\frac{q}{p}\right) = \left(\frac{q_1}{p}\right)\left(\frac{q_2}{p}\right)$.

Ar šo teorēmu katru Ležandra simbolu var izteikt ar tādu simbolu $\left(\frac{q}{p}\right)$ produktu, kur q ir pirmskaitlis.

Pierādījums līdzīgs iepriekšējam. No

$$q \equiv q_1 q_2 \pmod{p}$$

seko

$$q^{\frac{p-1}{2}} \equiv q_1^{\frac{p-1}{2}} q_2^{\frac{p-1}{2}} \pmod{p} \quad \text{jeb} \quad \left(\frac{q}{p}\right) - \left(\frac{q_1}{p}\right)\left(\frac{q_2}{p}\right) \equiv 0 \pmod{p}.$$

Šī kongruence ir iespējama tikai tad, ja

$$\left(\frac{q}{p}\right) - \left(\frac{q_1}{p}\right)\left(\frac{q_2}{p}\right) = 0 \quad \text{jeb} \quad \left(\frac{q}{p}\right) = \left(\frac{q_1}{p}\right)\left(\frac{q_2}{p}\right).$$

Sekas. Ja q_1 un q_2 abi ir moduļa p kvadrātiskie atlikumi vai abi neatlikumi, tad reizinājums $q_1 q_2$ ir moduļa p atlikums.

Speciālā gadījumā

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

§ 36. Gausa lemma.

Lemma. Ja q nedalās ar p un rindā

$$(I) \qquad 1q, 2q, 3q, \ldots, \frac{p-1}{2} q$$

ir μ skaitļi, kas, dalīti ar p, dod negātīvus atlikumus ar absolūto vērtību $< \frac{p}{2}$, tad Ležandra simbols

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

Pierādījums. Ja rindas (I) visus skaitļus

$$iq \qquad \left(i = 1, 2, \ldots, \frac{p-1}{2}\right)$$

dala ar p, tad dabū $\frac{p-1}{2}$ atlikumus, un no tiem neviens nav nulle. Katra atlikuma absolūtā vērtība ir mazāka par $\frac{p}{2}$, tā tad tā ir $\leqslant \frac{p-1}{2}$. Ik divu atlikumu absolūtās vērtības ir dažādas. Tiešām, ja pieņem pretējo:

$$|r_i| = |r_j|, \qquad 1 \leqslant j < i \leqslant \frac{p-1}{2},$$

tad seko vai nu

$$r_i = r_j, \quad iq \equiv jq \pmod{p}, \quad q(i-j) \mid p \text{ un } (i-j) \mid p,$$

vai arī

$r_i = -r_j$, $iq \equiv -jq \pmod{p}$, $q(i+j) \mid p$ un $(i+j) \mid p$.

Bet neviens no abiem gadījumiem nav iespējams, jo tiklab $i-j$, kā arī $i+j$, ir mazāki par p. Tādēļ saprotams, ka atlikumu absolūtas nozīmes

$$|r_1|, |r_2|, |r_3|, \ldots, |r_{\frac{p-1}{2}}|$$

ir citādā kārtībā skaitļi $1, 2, 3, \ldots, \frac{p-1}{2}$. Ja sastāda kongruences:

$$\begin{aligned} 1q &\equiv r_1 \pmod{p} \\ 2q &\equiv r_2 \pmod{p} \\ &\ldots\ldots \\ \frac{p-1}{2} q &\equiv r_{\frac{p-1}{2}} \pmod{p}, \end{aligned}$$

un tās sareizina, tad seko formula

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

Saīsinot ar $\left(\frac{p-1}{2}\right)!$, dabū

$$q^{\frac{p-1}{2}} \equiv (-1)^{\mu} \pmod{p}$$

jeb

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

Ja ievēro, ka skaitlis

$$\left(\frac{q}{p}\right) - (-1)^{\mu}$$

ir 2, 0, vai -2, bet tas dalās ar $p > 2$ tikai tad, kad

$$\left(\frac{q}{p}\right) - (-1)^{\mu} = 0,$$

tad seko formula

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

Gausa lemma ir pierādīta.

Izlietojumi. 1. Ja $q = -1$, tad rindā (I) visi locekļi ir negātīvi un to absolūtā vērtība $< \frac{p}{2}$. Tādēļ

$$\mu = \frac{p-1}{2},$$

un Ležandra simbols

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

Gadījumā, kad $q = 1$, tad μ ir 0 un

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

2. Aprēķināsim ar šo metodi arī simbolu $\left(\frac{2}{p}\right)$. Ja $q = 2$, tad rinda (I) top par rindu

$$1 \cdot 2,\quad 2 \cdot 2,\quad 3 \cdot 2, \ldots, k \cdot 2, \ldots, \frac{p-1}{2} \cdot 2,$$

kuŗā visi skaitļi ir mazāki par p. Dalīšanā ar p negatīvus atlikumus dod visi tie skaitļi $k \cdot 2$, kas lielāki par $\frac{p}{2}$.

Ja $p = 4n + 1$, tad tādi k ir skaitļi

$$n + 1,\quad n + 2, \ldots, 2n;$$

to skaits ir $n = \frac{p-1}{4}$.

Ja $p = 4n + 3$, tad

$$k = n + 1,\quad n + 2, \ldots, 2n + 1.$$

Tādu skaitļu k skaits ir $n + 1 = \frac{p+1}{4}$. Izlietojot Gausa lemmu, var rakstīt formulas:

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

Abus rezultātus var apvienot sekojošā veidā. Ja $p = 4n+1$, tad $\frac{p+1}{2}$ ir nepāru skaitlis, bet ja $p = 4n + 3$, tad $\frac{p-1}{2}$ ir nepāru skaitlis. Visām veselām skaitļu a un n nozīmēm der kongruence

$$a \equiv (2n + 1)\, a \pmod 2.$$

Ja to izlieto, tad var rakstīt pirmā gadījumā formulu

$$\mu = \frac{p-1}{4} \equiv \frac{p-1}{4} \cdot \frac{p+1}{2} \pmod 2,$$

bet otrā gadījumā

$$\mu = \frac{p+1}{4} \equiv \frac{p+1}{4} \cdot \frac{p-1}{2} \pmod 2.$$

Tagad abus gadījumus var uzrakstīt ar kopīgu rezultātu

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

No Gausa lemmas secinām formulu

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

Attiecībā pret moduli 8 katrs pirmskaitlis $p > 2$ ir izteicāms ar vienu no 4 sekojošām formām:

$$8n + 1, \quad 8n - 1, \quad 8n + 3, \quad 8n - 3.$$

Var pārliecināties, ka divos pirmajos gadījumos kāpinātājs $\frac{p^2-1}{8}$ ir pāru skaitlis, bet divos pēdējos — nepāru skaitlis. Tādēļ var izteikt **teorēmu**: Ležandra simbols

$$\left(\frac{2}{p}\right) = \begin{cases} +1, & \text{ja } p = 8n \pm 1 \\ -1, & \text{ja } p = 8n \pm 3. \end{cases}$$

To atradis Lagranžs 1775. g.

§ 37. Pirmskaitļu reciprocitātes (savstarpības) likums.

Teorēma. Ja p un q ir divi pirmskaitļi, kas abi izteicāmi formā $4n - 1$, tad viena no kongruencēm

$$(\alpha) \qquad x^2 \equiv q \pmod{p}$$

$$(\beta) \qquad x^2 \equiv p \pmod{q}$$

ir iespējama, bet otra nav iespējama; ja vismaz viens no abiem pirmskaitļiem ir formā $4n + 1$, tad dotās kongruences abas reizē ir iespējamas vai reizē neiespējamas.

Var pārbaudīt, ka ar Ležandra simboliem teorēma uzrakstāma šādi:

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

Teorēmu atrada Eulers 1783. g., bet to pierādīt viņam neizdevās. Arī Lagranžam neveicās. Ležandrs izteica teorēmu ar formulu (XIII) un deva arī nepilnīgu pierādījumu, izlietodams toreiz vēl nepierādīto Dirichlē teorēmu par aritmētisko progresiju (§ 1). Pirmo pierādījumu deva Gauss 1796. g. Līdz 1818. g. tam sekoja vēl 7 citi Gausa pierādījumi. Mūsu dienās ir jau ap 100 dažādu pierādījumu; no tiem lielākā daļa izlieto Gausa lemmu. Mēs apskatīsim Zellera pierādījumu (1872. g.), ko pārlabojis Frobēniuss 1914. g.

Kongruenču (α) un (β) iespējamību vai neiespējamību izšķir skaitļu rindas

$$(1) \qquad q,\ 2q,\ 3q,\ \ldots,\ xq,\ \ldots,\ \frac{p-1}{2}\,q$$

un

$$(2) \qquad p,\ 2p,\ 3p,\ \ldots,\ yp,\ \ldots,\ \frac{q-1}{2}\,p.$$

Ja pirmajā rindā ir μ skaitļi xq, kas dalīti ar p, dod negātīvus atlikumus ar absolūto vērtību mazāku par $\frac{p}{2}$, bet otrā rindā

ν tādi skaitļi $y p$, kas dalīti ar q, dod negātīvus atlikumus ar absolūto vērtību $< \frac{q}{2}$, tad, kā zināms,

$$\left(\frac{q}{p}\right) = (-1)^{\mu} \qquad \text{un} \qquad \left(\frac{p}{q}\right) = (-1)^{\nu}.$$

No tā seko

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

Ja izrādīsies, ka $\mu + \nu$ ir nepāru skaitlis tikai tad, ja abi pirmskaitļi p un q ir formā $4n - 1$, tad teorēma būs pierādīta.

Dalām rindas (1) katru locekli

$$xq \qquad \left(x = 1, 2, \ldots, \frac{p-1}{2}\right)$$

ar p. Dabūjam formulu

$$xq = ap + r,$$

kur r ir dalīšanas atlikums. Varam izteikt

$$r = xq - ap.$$

Ja atlikums r ir negātīvs, bet r absolūtā vērtība ir $< \frac{p}{2}$, tad var rakstīt formulu

$$-\frac{p}{2} < r < 0 \qquad \text{jeb} \qquad -\frac{p}{2} < xq - ap < 0.$$

No tās seko nevienlīdziba

$$ap < xq + \frac{p}{2},$$

kuŗā liekot $x < \frac{p}{2}$ dabū formulu

$$ap < \frac{q+1}{2} p \qquad \text{jeb} \qquad a < \frac{q+1}{2}.$$

Redzams, ka a ir viens no skaitļiem

$$y = 1, 2, \ldots, \frac{q-1}{2},$$

un a vietā var rakstīt y. Tad dabū nevienlīdzību

$$(1^a) \qquad -\frac{p}{2} < xq - yp < 0,$$

kam ir μ veselu atrisinājumu pāŗu

$$x, y \qquad \left(0 < x < \frac{p}{2} \quad \text{un} \quad 0 < y < \frac{q}{2}\right).$$

Līdzīgā kārtā no rindas (2) dabū nevienlīdzību

$$(2^a) \qquad -\frac{q}{2} < yp - xq < 0,$$

Tai ir ν veselu atrisinājumu pāŗu

$$x, y \qquad \left(0 < x < \frac{p}{2} \quad \text{un} \quad 0 < y < \frac{q}{2}\right).$$

Nevienlīdzības (1^a) un (2^a) var apvienot par nevienlīdzību

$$(3) \qquad -\frac{q}{2} < py - qx < \frac{p}{2},$$

kam ir $\mu + \nu$ veselu atrisinājumu pāŗu

$$x, y \qquad \left(0 < x < \frac{p}{2} \quad \text{un} \quad 0 < y < \frac{q}{2}\right).$$

Ja x un y vietā ieved jaunus mainīgos

$$(4) \qquad x' = \frac{p+1}{2} - x \quad \text{un} \quad y' = \frac{q+1}{2} - y,$$

tad redzams, ka x' mainās tādās pat robežās kā x un y' tādās robežās kā y (tikai apgrieztā kārtībā). No tā seko, ka reizē ar atrisinājumu x, y nevienlīdzībai (3) ir arī atrisinājums x', y'. Par to var pārliecināties, ja nevienlīdzībā (3) x un y vietā liek

$$\frac{p+1}{2} - x' \quad \text{un} \quad \frac{q+1}{2} - y'.$$

Tad ar nelielu pārveidojumu dabū tādu pat nevienlīdzību ar x' un y'. Tā tad nevienlīdzības (3) katram atrisinājumam x, y ar transformāciju (4) var piesaistīt tās pašas nevienlīdzības otru atrisinājumu x', y', Acīmredzams, ka dažādiem x, y atbilst arī dažādi x', y'. Tādēļ **vispārīgā gadījumā** nevienlīdzības (3) visus atrisinājumus var apvienot pāros. Tas nozīmē, ka atrisinājumu skaits $\mu + \nu$ ir pāru skaitlis. No tā seko formula

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = +1,$$

kas izsaka simbolu $\left(\frac{p}{q}\right)$ un $\left(\frac{q}{p}\right)$ vienlīdzību.

Izņēmuma gadījums ir tad, ja starp (3) nevienlīdzības $\mu + \nu$ atrisinājumiem atrodas tāds atrisinājums x, y, kas ir saistīts pats ar sevi. Tad pastāv vienlīdzības

$$x = x', \qquad y = y'.$$

Ar tām no formulām (4) seko, ka abi pirmskaitļi p un q ir formā $4n - 1$. Šinī gadījumā $\mu + \nu$ ir nepāru skaitlis. Tādēļ

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = -1,$$

t. i simboliem $\left(\frac{p}{q}\right)$ un $\left(\frac{q}{p}\right)$ ir pretējas zīmes. Ar to reciprocitātes likums pierādīts.

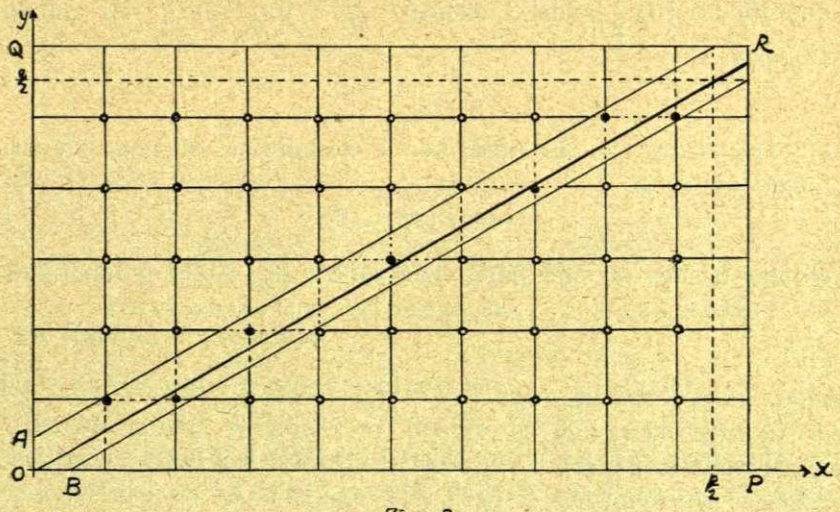
Apskatīsim vēl sekošu **pierādījuma variāciju**. Nevienlīdzības (1^a) un (2^a) ir līdzvērtīgas sistēmām:

$$(1^b) \qquad \begin{cases} xq - yp + \frac{p}{2} < 0 \\ xq - yp < 0 \end{cases}$$

un

$$(2^b) \qquad \begin{cases} xq - yp - \frac{q}{2} < 0 \\ xq - yp > 0, \end{cases}$$

kam atrisinājumu skaitu μ un ν pēc Eizenšteina (*Eisenstein*) parauga (1844. g.) noteiksim ar ģeometrisku metodi.



Zīm. 3.

Attēlosim (zīm. 3) Dekarta koordinātu sistēmā taisnes:

$$xq - yp = 0 \qquad (o)$$

$$xq - yp + \frac{p}{2} = 0 \qquad (a)$$

$$xq - yp - \frac{q}{2} = 0 \qquad (b)$$

Pirmā taisne (o) iet caur koordinātu sākumu un punktu $\left(\frac{p}{2}, \frac{q}{2}\right)$, otrā (a) — tai parallēli caur punktu $A\left(0, \frac{1}{2}\right)$ un trešā (b) — arī parallēli caur punktu $B\left(\frac{1}{2}, 0\right)$.

No analistiskās ģeometrijas zinām: ja taisnes vienādojuma $Ax + By + C = 0$ kreisā pusē ieliek to punktu koordinātas (x, y), kas atrodas vienpus taisnes, tad polinoma $Ax + By + C$ vērtības ir ar vienādām zīmēm. Liekot taisnes (a) vienādojuma kreisā pusē sākuma punkta O koordinātas (0, 0), dabū skaitli

$\frac{p}{2} > 0$. Bet liekot taisnes (o) vienādojuma kreisā pusē punkta A koordinātas $\left(0, \frac{1}{2}\right)$, dabū skaitli $-\frac{p}{2} < 0$. Tādēļ visi punkti (x, y) ar

$$xq - yp > 0$$

atrodas taisnes (a) tajā pusē, kur ir koordinātu sākums, bet visi punkti (x, y) ar

$$xq - yp < 0$$

atrodas taisnes (o) tajā pusē, kur punkts A. Ar to ir pierādīts, ka sistēmas (I^b) visi veselie atrisinājumi

$$(x, y) \qquad \left(0 < x < \frac{p}{2} \text{ un } 0 < y < \frac{q}{2}\right)$$

ir tie punkti ar veselām koordinātām, kas atrodas taisnsstūrī $POQR$ starp taisnēm (a) un (o). Minētais taisnstūris $POQR$ noteikts ar taisnēm:

$$x = 0, \quad y = 0, \quad x = \frac{p+1}{2}, \quad y = \frac{q+1}{2}.$$

Tamlīdzīgi spriežot, var noskaidrot, ka sistēmas (2^b) visi atrisinājumi x, y ar to pašu blakus nosacījumu ģeometriski attēlojas kā veselu koordinātu punkti starp taisnēm (o) un (b) taisnstūrī $POQR$.

Punkti uz taisnstūŗa $POQR$ malām nav līdzi skaitāmi, jo mūs interesē tikai tie veselo koordinātu punkti (x, y), kam $0 < x < \frac{p}{2}$ un $0 < y < \frac{q}{2}$. Taisnstūŗa $POQR$ iekšpusē tādu punktu ir pavisam

$$\frac{p-1}{2} \cdot \frac{q-1}{2}.$$

Tie sadalās pa diviem kongruentiem taisnleņķa trijstūŗiem un vienu sešstūri starp taisnēm (a), (b), kuŗā ir $\mu + \nu$ punktu. Ja vienā no taisnleņķu trijstūŗiem ir n punktu ar veselām koordinā-

tām, tad arī otrā ir tikpat daudz punktu. Tādēļ var rakstīt formulu

$$\frac{p-1}{2} \cdot \frac{q-1}{2} = \mu + \nu + 2n$$

jeb

$$\mu + \nu \equiv \frac{p-1}{2} \cdot \frac{q-1}{2} \pmod 2.$$

No tā seko formula

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\mu+\nu} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}},$$

un teorēma ir pierādīta.

P i e z ī m e. Taisnstūŗa $POQR$ katra iekšēja punkta piederība pie minētā trijstūŗa vai 6-stūŗa ir pilnīgi noteikta, jo u z taisnēm (a), (b) un (o) n e v i e n s v e s e l u k o o r d i n ā t u p u n k t s n e v a r a t r a s t i e s. Tiešām, taisnēm (a) un (b) brīvie locekļi ir daļskaitļi, pārējie koeficienti ir veseli. Tādēļ uz šīm taisnēm vispār nav punktu ar veselām koordinātām. Uz taisnes (o) var atrasties tikai tādi veselu koordinātu punkti (x, y), kam

$$\frac{x}{y} = \frac{p}{q}$$

jeb

$$x = pt \quad \text{un} \quad y = qt \qquad (t = 0, \pm 1, \pm 2, \pm \ldots).$$

Bet no tiem neviens nav taisnstūŗa $POQR$ iekšpusē.

Piemērs. K o n g r u e n c e

$$x^2 \equiv 5124 \pmod{(2^{2^4} + 1)}.$$

Jautājumu par šīs kongruences iespējamību var gan noskaidrot ar Eulera kritēriju. Tomēr ērtāki izlietot iepriekšējo teorēmu un Ležandra simbola īpašības.

Tā kā $2^{2^4} + 1$ ir pirmskaitlis $p = 65537 = 4n + 1$ un $5124 = 2^2 \cdot 3 \cdot 7 \cdot 61$, tad var rakstīt Ležandra simboliem sekošus pārveidojumus:

$$\left(\frac{2^2}{p}\right)=\left(\frac{2}{p}\right)^2=+1,$$

$$\left(\frac{3}{p}\right)=\left(\frac{p}{3}\right)=\left(\frac{2}{3}\right)=-1,$$

$$\left(\frac{7}{p}\right)=\left(\frac{p}{7}\right)=\left(\frac{3}{7}\right)=-\left(\frac{7}{3}\right)=-\left(\frac{1}{3}\right)=-1,$$

$$\left(\frac{61}{p}\right)=\left(\frac{p}{61}\right)=\left(\frac{23}{61}\right)=\left(\frac{61}{23}\right)=\left(\frac{15}{23}\right)=\left(\frac{3}{23}\right)\left(\frac{5}{23}\right)=-\left(\frac{23}{3}\right)\left(\frac{23}{5}\right)$$

jeb $$\left(\frac{61}{p}\right)=-\left(\frac{2}{3}\right)\left(\frac{3}{5}\right)=\left(\frac{3}{5}\right)=\left(\frac{5}{3}\right)=\left(\frac{2}{3}\right)=-1.$$

No tiem seko, ka simbols

$$\left(\frac{5124}{p}\right)=\left(\frac{2^2}{p}\right)\left(\frac{3}{p}\right)\left(\frac{7}{p}\right)\left(\frac{61}{p}\right)=(+1).(-1).(-1).(-1)=-1.$$

Tādēļ dotā kongruence nav iespējama.

§ 38. Atrisināšanas metodes.

Ja kongruence

(1) $$x^2 \equiv q \pmod{p}$$

ir iespējama, tad no Eulera kritērija seko formula

(XIV) $$q^{\frac{p-1}{2}} \equiv +1 \pmod{p},$$

ar ko sekojošos gadījumos var atrast kongruences saknes.

I. Ja $p = 4n + 3$, tad formula (XIV) identiska ar formulu

$$q^{2n+1} \equiv 1 \pmod{p}.$$

No tās seko kongruence

$$q^{2n+2} \equiv q \pmod{p} \quad \text{jeb} \quad (q^{n+1})^2 \equiv q \pmod{p}.$$

Redzam, ka dotās kongruences atrisinājumi ir

$$x \equiv \pm q^{n+1} \pmod{p} \quad \text{jeb} \quad x \equiv \pm q^{\frac{p+1}{4}} \pmod{p}.$$

Šādu atrisināšanas metodi ir pazinis jau Lagranžs.

Piemērs. Kongruences $x^2 \equiv 5 \pmod{11}$ atrisinājumi ir

$$x \equiv \pm 5^3 \pmod{11} \quad \text{jeb} \quad x \equiv \pm 4 \pmod{11}.$$

II. Ja $p = 8n + 5$ un kongruence (1) ir iespējama, tad no formulas (XIV) seko kongruence

$$q^{4n+2} - 1 \equiv 0 \quad \text{jeb} \quad (q^{2n+1} - 1)(q^{2n+1} + 1) \equiv 0 \pmod{p}.$$

Pēdējā kongruence satur divus faktorus, kuŗu starpība ir 2. Tādēļ abi faktori reizē ar p nedalās. Ir iespējami sekojoši d i v i (II^a un II^b) g a d ī j u m i.

II^a. $\quad q^{2n+1} - 1 \equiv 0 \pmod{p}.$

Tad

$$(q^{n+1})^2 \equiv q \pmod{p}$$

un dabū L e ž a n d r a atrasto formulu

$$x \equiv \pm q^{\frac{p+3}{8}} \pmod{p}.$$

II^b. $\quad q^{2n+1} + 1 \equiv 0 \pmod{p}.$

Tad

$$q^{2n+2} = q^{\frac{p+3}{8} \cdot 2} \equiv -q \pmod{p}.$$

Zinām, ka

$$2^{\frac{p-1}{2}} \equiv \left(\frac{2}{p}\right) \pmod{p} \quad \text{un} \quad \left(\frac{2}{p}\right) = -1, \quad \text{ja} \quad p = 8n + 5.$$

Tādēļ var rakstīt kongruences

$$2^{\frac{p-1}{2}} \equiv -1 \pmod{p} \quad \text{un} \quad \left(q^{\frac{p+3}{8}}\right)^2 \equiv -q \pmod{p}.$$

Ja tās sareizina, tad seko formula

$$\left(2^{\frac{p-1}{4}} q^{\frac{p+3}{8}}\right)^2 \equiv q \pmod{p}.$$

Redzam, ka dotās kongruences (1) atrisinājumi ir

$$x \equiv \pm \frac{1}{2}(4q)^{\frac{p+3}{8}} \pmod{p}.$$

Pēdējo formulu ir devis angļu autors Poklingtons (*Pocklington*) 1917. g.

Piemērs: $x^2 \equiv 20 \pmod{29}$.

Tā kā

$$\left(\frac{20}{29}\right)=\left(\frac{5}{29}\right)=\left(\frac{4}{5}\right)=+1 \qquad \text{un} \qquad q^{2n+1}=20^7 \equiv 1 \pmod{29},$$

tad dotā kongruence ir iespējama un atbilst gadījumam (II^a). Izlietojot Ležandra formulu, dabū rezultātu

$$x \equiv \pm 20^4 \equiv \pm 7 \pmod{29}.$$

Kongruences $x^2 \equiv q \pmod{p}$ vispārīgā atrisinājuma formulas ir atrastas arī dažām citām moduļa p formām. Ja p un q ir lieli skaitļi, tad praktiskas nozīmes šīm formulām nav.

Praktikā daudz ērtāka ir **Gausa metode**, ko sauc arī par izslēgšanas (ekskludentu) metodi. To tagad apskatīsim.

Ja kongruence

(1) $$x^2 \equiv q \pmod{p}$$

ir iespējama un tai ir viena sakne x_1, tad tai ir arī otra sakne $p - x_1$. Viena no abām saknēm ir mazāka par moduļa pusi. To varētu atrast, ja izmēģinātu skaitļus

(2) $$x = 1, 2, 3, \ldots, E\left(\frac{p}{2}\right).$$

Tomēr ir ērtāki apmainīt kongruenci (1) ar nenoteiktu vienādojumu

(3) $$x^2 = q + py.$$

No tā izteic

$$y = \frac{x^2}{p} - \frac{q}{p}.$$

Ja $x < \frac{p}{2}$, tad redzam, ka $y < \frac{p}{4}$, t. i. y ir viens no skaitļiem

(4) $$y = 0, 1, 2, 3, \ldots, E\left(\frac{p}{4}\right),$$

kas visi jāpārbauda. Tagad, salīdzinot ar rindu (2) pārbaudāmo atrisinājumu skaits ir uz pusi samazinājies (ja $p > 5$). To var vēl

vairāk samazināt, ja no rindas (4) izslēdz tās y nozīmes, kas neder vienādojumam (3). Izslēgšanas metodi noskaidrosim ar sekošu piemēru, ko devis Gauss savā „*Disquisitiones Arithmeticae*".

Piemērs. $x^2 \equiv 22 \pmod{97}$.

Ležandra simbols

$$\left(\frac{22}{97}\right)=\left(\frac{2}{97}\right)\left(\frac{11}{97}\right)=\left(\frac{97}{11}\right)=\left(\frac{-2}{11}\right)=\left(\frac{-1}{11}\right)\left(\frac{2}{11}\right)=(-1)\cdot(-1)=+1.$$

Tādēļ dotā kongruence ir iespējama.

Ja to pārraksta formā

$$x^2 = 22 + 97y,$$

tad y ir viens no skaitļiem

$$y = 0, 1, 2, 3, \ldots, 24. \tag{5}$$

Lai visi šie skaitļi nebūtu jāpārbauda, mēģināsim nederīgos y izslēgt. No vienlīdzības

$$x^2 = 22 + 97y,$$

var secināt kongruenci

$$x^2 \equiv 22 + 97y \pmod{k},$$

kur par moduli k var izvēlēties katru veselu skaitli. Ja skaitlis n ir moduļa k kvadrātisks neatlikums, tad kongruence

$$x^2 \equiv n \pmod{k}$$

nav iespējama, un no rindas (5) var svītrot tos y, kam

$$22 + 97y \equiv n \pmod{k}.$$

Modulim 2 kvadrātisku neatlikumu nav. Ja par moduli izvēlas $k = 3$, kam ir kvadrātisks neatlikums $n = 2$, tad no kongruences

$$22 + 97y \equiv 2 \pmod{3}$$

atrod

$$y \equiv 1 \pmod{3}.$$

Ja izvēlas $k = 4$, tad n ir 2 un 3. No kongruencēm:

$$22 + 97y \equiv 2 \pmod 4, \qquad 22 + 97y \equiv 3 \pmod 4$$

dabū

$$y \equiv 0 \pmod 4 \quad \text{un} \quad y \equiv 1 \pmod 4.$$

Beidzot, ja pieņem $k = 5$, tad n ir 2 un 3, un atbilstošo kongruenču atrisinājumi ir

$$y \equiv 0 \pmod 5 \quad \text{un} \quad y \equiv 3 \pmod 5.$$

Ja no rindas (5) izmet visus skaitļus, kas $\equiv 1 \pmod 3$, vai $\equiv 0 \pmod 4$, vai $\equiv 1 \pmod 4$, vai $\equiv 0$ un $3 \pmod 5$, tad pāri paliek tikai četri skaitļi

$$y = 2,\ 6,\ 11,\ 14.$$

Tos pārbaudot par derīgu izrādās

$$y = 11.$$

No vienlīdzības

$$22 + 97 . 11 = 33^2$$

atrod dotās kongruences atrisinājumu

$$x \equiv \pm 33 \pmod{97}.$$

Piezīme. Var pierādī, ka skaitļiem p^a un $2p^a$ ir tie paši kvadrātiskie atlikumi, resp. neatlikumi, bet moduļa $p^a q^b$ katrs neatlikums ir reizē arī moduļa p^a vai q^b neatlikums. No tā seko, ka par moduli k ir vērts izvēlēties tikai pirmskaitļus un to pakāpes.

§ 39. Jakobi (*Jacobi*) simbols $\left(\frac{Q}{P}\right)$.

Jakobi (*Jacobi*) simbolu var uzskatīt par Ležandra simbola vispārinājumu.

Definīcija. Ja $(P, Q) = 1$ un P ir nepāru skaitlis $= p_1 p_2 \ldots p_n$, kur $p_1, p_2, \ldots, p_n$ ir vienādi vai dažadi pirmskaitļi, tad Jakobi simbolu $\left(\frac{Q}{P}\right)$ definē ar Ležandra simbolu $\left(\frac{Q}{p_i}\right)$ produktu, t. i.

$$\left(\frac{Q}{P}\right) = \left(\frac{Q}{p_1}\right)\left(\frac{Q}{p_2}\right) \ldots \left(\frac{Q}{p_n}\right)$$

Noskaidrosim Jakobi simbola $\left(\frac{Q}{P}\right)$ nozīmi kvadrātiskas kongruences $x^2 \equiv Q \pmod{P}$ atrisināšanā.

Pieņemsim, ka $(P, Q) = 1$, $P = p_1 p_2 \ldots p_n$ ir nepāru skaitlis un kongruence

$$x^2 \equiv Q \pmod{P}$$

ir iespējama. Tad reizē ar to ir iespējamas arī kongruences

$$x^2 \equiv Q \pmod{p_1}, \quad x^2 \equiv Q \pmod{p_2}, \ldots, x^2 \equiv Q \pmod{p_n}.$$

Tādēļ visi attiecīgie Ležandra simboli ir ar vērtību $+1$. Ja tos uzraksta un sareizina, tad seko, ka Jakobi simbols

$$\left(\frac{Q}{P}\right) = +1.$$

Šis nosacījums ir gan nepieciešams, bet nav pietiekošs, jo apgrieztā teorēma nav pareiza. Tiešām, ja simbols

$$\left(\frac{Q}{P}\right) = \left(\frac{Q}{p_1}\right)\left(\frac{Q}{p_2}\right) \ldots \left(\frac{Q}{p_n}\right) = +1,$$

bet atsevišķi reizinātāji pāru skaitā, piem. $\left(\frac{Q}{p_1}\right)$ un $\left(\frac{Q}{p_2}\right)$ ir negātīvi, tad nevar atrast veselu skaitli x tā, ka $x^2 - Q$ dalītos ar p_1, resp. p_2 un vēl jo mazāk ar P. Tādēļ kongruence $x^2 \equiv Q \pmod{P}$ nav iespējama. Dabūjam sekošo: ja simbols $\left(\frac{Q}{P}\right) = +1$, tad kongruence $x^2 \equiv Q \pmod{P}$ var būt iespējama, var arī nebūt iespējama. Turpretim, ja $\left(\frac{Q}{P}\right) = -1$, tad kongruence $x^2 \equiv Q \pmod{P}$ nav iespējama.

No definīcijas seko, ka $\left(\frac{Q}{P}\right)$ ir $+1$ vai -1 un $\left(\frac{Q^{2k}}{P}\right) = +1$.

Jakobi simbola īpašību noskaidrošanai ir vajadzīga sekoša lemma.

Lemma. Ja

$$P = p_1 p_2 \ldots p_n,$$

tad

$$\sum_{i=1}^{n} \frac{p_i - 1}{2} \equiv \frac{P - 1}{2} \pmod{2}$$

un

$$\sum_{i=1}^{n} \frac{p_i^2 - 1}{8} \equiv \frac{P^2 - 1}{8} \pmod 2.$$

Pierādījums. Izlietosim no algebras pazīstamo Vjeta (*Viète*) identitāti:

$$(x + a_1)(x + a_2) \ldots (x + a_n) = x^n + (a_1 + a_2 + \ldots + a_n) x^{n-1} + \\ + (a_1 a_2 + a_1 a_3 + \ldots + a_{n-1} a_n) x^{n-2} + \ldots + a_1 a_2 \ldots a_n .$$

Ar to var pamatot formulu

$$P = p_1 p_2 \ldots p_n = (1 + p_1 - 1)(1 + p_2 - 1) \ldots (1 + p_n - 1)$$

jeb

$$P = 1 + \sum_{i=1}^{n} (p_i - 1) + \sum_{i,j}^{1,n} (p_i - 1)(p_j - 1) + \ldots$$

Ja ievēro, ka visi „p" ir nepāru skaitļi, tad katrs $(p_i - 1) \mid 2$, un var rakstīt formulu

$$P = 1 + \sum_{i=1}^{n} (p_i - 1) + 4k,$$

kur k ir vesels skaitlis. Ja dala ar 2, tad seko formula

$$\sum_{i=1}^{n} \frac{p_i - 1}{2} = \frac{P - 1}{2} - 2k,$$

ar ko lemmas viena daļa pierādīta.

Tamlīdzīgi pierāda lemmas otru daļu. Ja ievēro, ka katra nepāru skaitļa kvadrāts pamazināts pār 1, dalās ar 8, tad no identitātes

$$P^2 = p_1^2 p_2^2 \ldots p_n^2 = (1 + p_1^2 - 1)(1 + p_2^2 - 1) \ldots (1 + p_n^2 - 1)$$

jeb

$$P^2 = 1 + \sum_{i=1}^{n} (p_i^2 - 1) + \sum_{i,j}^{1,n} (p_i^2 - 1)(p_j^2 - 1) + \ldots$$

seko formula

$$P^2 - 1 = \sum_{i=1}^{n} (p_i^2 - 1) + 8^2 k \quad \text{vai} \quad \sum_{i=1}^{n} \frac{p_i^2 - 1}{8} = \frac{P^2 - 1}{8} - 8k.$$

Aprēķināsim **Jakobi simbolu** $\left(\frac{1}{P}\right)$, $\left(\frac{-1}{P}\right)$, $\left(\frac{2}{P}\right)$ **nozīmes.**

No $\left(\frac{Q}{P}\right)$ definīcijas seko:

$$\left(\frac{1}{P}\right) = +1$$

un

$$\left(\frac{-1}{P}\right)=\left(\frac{-1}{p_1}\right)\left(\frac{-1}{p_2}\right)\ldots\left(\frac{-1}{p_n}\right)=$$

$$=(-1)^{\frac{p_1-1}{2}}(-1)^{\frac{p_2-1}{2}}\ldots(-1)^{\frac{p_n-1}{2}}=(-1)^{\sum_{i=1}^{n}\frac{p_i-1}{2}}.$$

Ievērojot lemmu dabū

$$\left(\frac{-1}{P}\right)=(-1)^{\frac{P-1}{2}}.$$

Analogā kārtā atrod

$$\left(\frac{2}{P}\right)=\left(\frac{2}{p_1}\right)\left(\frac{2}{p_2}\right)\ldots\left(\frac{2}{p_n}\right)=(-1)^{\sum_{i=1}^{n}\frac{p_i^2-1}{8}}$$

Tā tad

$$\left(\frac{2}{P}\right)=(-1)^{\frac{P^2-1}{8}}.$$

Tagad apskatīsim sekojošas **Jakobi simbola īpašības.**

1. Ja $Q_1 \equiv Q_2 \pmod P$, tad $\left(\frac{Q_1}{P}\right)=\left(\frac{Q_2}{P}\right)$

Pierādījums. Ja $P=p_1 p_2 \ldots p_n$, tad no $Q_1 \equiv Q_2 \pmod P$ seko kongruences

$Q_1 \equiv Q_2 \pmod{p_1}$, $Q_1 \equiv Q_2 \pmod{p_2}$,. . ., $Q_1 \equiv Q_2 \pmod{p_n}$.

Izlietojot Ležandra simbolu īpašības, var rakstīt formulas:

$$\left(\frac{Q_1}{p_1}\right)=\left(\frac{Q_2}{p_1}\right),\quad \left(\frac{Q_1}{p_2}\right)=\left(\frac{Q_2}{p_2}\right),\ldots,\left(\frac{Q_1}{p_n}\right)=\left(\frac{Q_2}{p_n}\right).$$

Tās sareizinot, dabū formulu

$$\left(\frac{Q_1}{P}\right)=\left(\frac{Q_2}{P}\right).$$

Līdzīgi pierāda arī sekojošu īpašību.

2. Ja $Q \equiv Q_1 Q_2 \pmod{P}$, tad $\left(\frac{Q}{P}\right)=\left(\frac{Q_1}{P}\right)\cdot\left(\frac{Q_2}{P}\right)$.

3. **Reciprocitātes likums.** Ja P un Q ir nepāru skaitļi un $(P, Q) = 1$, tad

$$\left(\frac{Q}{P}\right)\left(\frac{P}{Q}\right)=(-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}.$$

Pierādījums. Pieņemsim, ka

$$P=p_1 p_2 \ldots p_n=\prod_{i=1}^{n} p_i \quad \text{un} \quad Q=q_1 q_2 \ldots q_m=\prod_{j=1}^{m} q_j,$$

kur p_i un q_j ir pirmskaitļi. Tad $\left(\frac{Q}{P}\right)\left(\frac{P}{Q}\right)$ aprēķina ar sekošu pārveidojumu:

$$\left(\frac{Q}{P}\right)\left(\frac{P}{Q}\right)=\prod_{i,j}\left(\frac{q_j}{p_i}\right)\left(\frac{p_i}{q_j}\right)=\prod_{i,j}(-1)^{\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}}$$

jeb

$$\left(\frac{Q}{P}\right)\left(\frac{P}{Q}\right)=(-1)^{\sum_{i=1}^{n}\frac{p_i-1}{2}\cdot\sum_{j=1}^{m}\frac{q_j-1}{2}}.$$

Ievērojot lemmu, dabū

$$\left(\frac{Q}{P}\right)\cdot\left(\frac{P}{Q}\right)=(-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}.$$

Ar šo formulu izteic

$$\left(\frac{Q}{P}\right)=(-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}\left(\frac{P}{Q}\right).$$

Minētās īpašības izlieto Jakobi un Ležandra simbolu aprēķināšanā.

Piemērs. Kongruence $x^2 \equiv Q \pmod{P}$ ar $Q = 2371$ un $P = 5971$.

P un Q ir nepāru skaitļi Ar Euklida algoritmu var pārliecināties, ka $(P, Q) = 1$. Tādēļ var izlietot iepriekšējās īpašības un aprēķināt Jakobi simbolu sekojoši:

$$\left(\frac{Q}{P}\right)=\left(\frac{2371}{5971}\right)=-\left(\frac{5971}{2371}\right)=-\left(\frac{1229}{2371}\right)=-\left(\frac{2371}{1229}\right)=-\left(\frac{-87}{1229}\right)$$

$$=-\left(\frac{87}{1229}\right)\left(\frac{-1}{1229}\right)=-\left(\frac{87}{1229}\right)=-\left(\frac{1229}{87}\right)=-\left(\frac{11}{87}\right)=\left(\frac{87}{11}\right)$$

jeb

$$\left(\frac{Q}{P}\right)=\left(\frac{-1}{11}\right)=-1.$$

Rezultāts liecina, ka kongruence $x^2 \equiv 2371 \pmod{5971}$ nav iespējama.

4. Jakobi simbola īpašību izteic ar formulu

$$\left(\frac{Q}{P}\right)=\left(\frac{Q}{P+4Q}\right).$$

Uzskatot P kā mainīgu lielumu x, kas ir nepāru skaitlis un relātivs pirmskaitlis ar Q, t. i. $(Q,x)=1$, dabū aritmētisku funkciju $F(x) = \left(\frac{Q}{x}\right)$. Pierādīsim, ka $F(x) = \left(\frac{Q}{x}\right)$ ir periodiska funkcija ar periodu $4Q$, t. i.

$$\left(\frac{Q}{x+4Q}\right)=\left(\frac{Q}{x}\right).$$

Pieņemsim, ka

$$Q = (-1)^a \cdot 2^b \, T,$$

kur T pozitīvs nepāru skaitlis, a ir 0 vai 1 un b ir vesels pozitīvs skaitlis vai nulle. Tad var rakstīt formulu

$$\left(\frac{Q}{x}\right)=\left(\frac{-1}{x}\right)^a\left(\frac{2}{x}\right)^b\left(\frac{T}{x}\right)=(-1)^{\frac{x-1}{2}\cdot a}\cdot(-1)^{\frac{x^2-1}{8}\cdot b}\cdot(-1)^{\frac{x-1}{2}\cdot\frac{T-1}{2}}\left(\frac{x}{T}\right).$$

Ja x vietā liek $x+4Q$ un ignorē faktoru $(-1)^{2k}$, tad dabū formulu

$$\left(\frac{Q}{x+4Q}\right)=(-1)^{\frac{x-1}{2}\cdot a}\cdot(-1)^{\frac{x^2-1}{8}\cdot b}\cdot(-1)^{\frac{x-1}{2}\cdot\frac{T-1}{2}}\left(\frac{x+4Q}{T}\right).$$

Tā kā $(4Q)|T$, tad

$$\left(\frac{x+4Q}{T}\right)=\left(\frac{x}{T}\right).$$

Redzām, ka simboli $\left(\frac{Q}{x}\right)$ un $\left(\frac{Q}{x+4Q}\right)$ tiešām ir vienlidzīgi.

Minēto īpašību izlieto **simboliskā vienādojuma**

$$\left(\frac{Q}{x}\right)=1$$

atrisināšanai.

Šī vienādojuma visi atrisinājumi ir meklējami starp tiem **nepāru** skaitļiem

$$1, 3, 5, 7, \ldots, 4Q-1,$$

kam ar Q nav kopīga dalītāja.

Piemērs. $\left(\frac{7}{x}\right)=1.$

Nepāru skaitļi, kas mazāki par $4.8=28$ un relātīvi pirmskaitļi ar 7 ir sekoši:

$$1, 3, 5, 9, 11, 13, 15, 17, 19, 23, 25, 27.$$

Tos pārbaudot, atrod, ka $\left(\frac{7}{x}\right)=1$ tikai tad, ja

$$x=1, 3, 9, 19, 25, 27.$$

Tādēļ vienādojuma $\left(\frac{7}{x}\right)=1$ atrisinājumi ir

$$x\equiv 1, 3, 9, 19, 25, 27 \pmod{28}.$$

Uzdevumi.

1. Atrisināt kongruences:

$x^2 + 15x + 18 \equiv 0 \pmod{a}$, ja $a = 12, 19, 20$;

$3x^2 + 25x + 38 \equiv 0 \pmod{53}$; $5x^2 - 3x - 2 \equiv 0 \pmod{12}$;

$4x^2 - x + 1 \equiv 0 \pmod{24}$; $x^2 - 3x - 6 \equiv 0 \pmod{12}$;

$x^2 \equiv -229 \pmod{641}$; $x^2 \equiv 1135 \pmod{2311}$.

2. Atrisināt veselos skaitļos vienādojumu $x^2 - 67y = 3$.

3. Noteikt, kuŗiem pirmskaitļiem Ležandra simbols

$$\left(\frac{-2}{p}\right) = +1; \quad \left(\frac{3}{p}\right) = +1; \quad \left(\frac{5}{p}\right) = +1; \quad \left(\frac{6}{p}\right) = +1.$$

4. Kuŗiem skaitļiem a kongruence $x^2 \equiv 512\ a \pmod{65537}$ ir iespējama?

5. Noteikt moduļa 60 kvadrātiskos atlikumus.

6. Atrisināt vienādojumu $\left(\frac{10}{x}\right) = -1$

7. Pierādīt teorēmu: ja $Q = 4n + 1$, tad skaitļa x funkcijai $\left(\frac{Q}{x}\right)$ ir periods $2Q$.

8. Pierādīt, ka formas $x^2 - Qy^2$ katrs dalītājs ir vienādojuma

$$\left(\frac{Q}{x}\right) = 1$$

atrisinājums.

VIII. Pakāpju atlikumi.

§ 40. Jēdziens par skaitļa piederibu eksponentam.

Moduļa m pilnīgā atlikumu sistēma sastāv no m nekongruentiem skaitļiem. Tādēļ, ja $\mu > m$, tad rindā

$$a,\ a^2,\ a^3,\ \ldots,\ a^{\mu}$$

atrodas vismaz divi skaitļi

$$a^i \text{ un } a^j, \qquad 1 \leqslant j < i \leqslant \mu,$$

kas kongruenti attiecībā pret moduli m. Ja $(a, m) = 1$, tad kongruenci

$$a^i \equiv a^j \pmod{m}$$

ar a^j var saīsināt, un dabū kongruenci

$$a^{\lambda} \equiv 1 \pmod{m},$$

kur $\lambda = i - j$. Tā tad rindā $a,\ a^2,\ a^3,\ \ldots$, atrodas skaitlis a^x, kas dalīts ar m dod atlikumā 1.

Ja a ir relatīvs pirmskaitlis ar moduli m, t i. $(a, m) = 1$ un $k > 0$ ir mazākais kāpinātājs, kam

$$a^k \equiv 1 \pmod{m},$$

tad saka, ka pamats a pieder eksponentam k attiecībā pret moduli m.

Ja

$$a \equiv b \pmod{m},$$

tad arī

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

Tas nozīmē, ka attiecībā pret moduli m visi

vienas klases skaitļi pieder vienam un tam pašam eksponentam.

No Eulera teorēmas

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

seko, ka

$$k \leqslant \varphi(m).$$

Gadījumā, kad

$$k = \varphi(m),$$

tad a sauc par moduļa m **primitīvo sakni**.

Jēdzienu par skaitļa piederību eksponentam ir devis Gauss. Ar pakāpju atlikumiem daudz nodarbojies Eulers un jau ap 1770. g. pierādījis zemāk minētās teorēmas.

Teorēma 1. Ja $a^x \equiv 1 \pmod{m}$ un a pieder eksponentam k attiecībā pret moduli m, tad ir nepiešami un pietiekoši, ka $x \mid k$ jeb $x \equiv 0 \pmod{k}$.

Pierādījums. Pieņemsim, ka

$$x = q \cdot k + r \quad \text{un} \quad 0 \leqslant r < k.$$

Tad, ievērojot, ka

$$a^k \equiv 1 \pmod{m},$$

no kongruences

$$a^{kq+r} \equiv 1 \pmod{m} \quad \text{jeb} \quad (a^k)^q \cdot a^r \equiv 1 \pmod{m}$$

seko kongruence

$$a^r \equiv 1 \pmod{m} \quad \text{ar} \quad r < k.$$

Bet tā pēc k definīcijas ir iespējama tikai tad, ja $r = 0$.

Otrādi: ja

$$a^k \equiv 1 \pmod{m} \quad \text{un} \quad x \mid k,$$

tad acīmredzams, ka arī

$$a^x \equiv 1 \pmod{m}.$$

Sekas. Ja a pieder eksponentam k attiecībā pret moduli m, tad $\varphi(m)$ dalās ar k.

Piemērs. Meklēsim eksponentu k, kuŗam pieder skaitļi 2 un 3 attiecībā pret moduli 17.

Tā kā $\varphi(m)|k$, tad k ir meklējams tikai starp $\varphi(m)$ dalītājiem. Skaitļa $\varphi(17)$ dalītāji ir 1, 2, 4, 8, 16, un tie pēc kartas jāpārbauda.

No $2^4 \equiv -1 \pmod{17}$ seko, ka $2^8 \equiv +1 \pmod{17}$. Tā tad 2 pieder eksponentam 8 attiecībā pret moduli 17.

Ja pārbauda skaitli 3, tad dabū kongruences

$3^4 \equiv -4 \pmod{17}$, $3^8 \equiv -1 \pmod{17}$ un $3^{16} \equiv 1 \pmod{17}$.

Tā tad skaitlis 3 pieder eksponentam 16 attiecībā pret moduli 17, jeb 3 ir moduļa 17 primitīvā sakne.

Teorēma 2. Ja $(a,m) = 1$ un $a^i \equiv a^j \pmod{m}$, tad $i \equiv j \pmod{k}$ un otrādi.

Pierādījums. Ja $i > j$, tad no kongruences

$$a^i \equiv a^j \pmod{m}$$

seko, ka

$$a^{i-j} \equiv 1 \pmod{m}.$$

Tādēļ

$$i - j \equiv 0 \pmod{k} \quad \text{jeb} \quad i \equiv j \pmod{k}.$$

Otrādi: ja $i \equiv j \pmod{k}$, tad $i - j \equiv 0 \pmod{k}$ un

$$a^{i-j} \equiv 1 \pmod{m} \quad \text{vai} \quad a^i \equiv a^j \pmod{m}.$$

Ja $(a,m) = 1$ un katru skaitli rindā

$$a, a^2, a^3, \ldots, a^k$$

dala ar m un atlikumus atstāj pozitīvus un mazākus par m, tad dabū k atlikumus

$$r_1, r_2, r_3, \ldots, r_k = 1,$$

kas visi ir dažādi, un neviens no tiem nav nulle.

Tiešām, ja pieņem, ka

$$r_i = r_j \quad \text{un} \quad 0 < j < i \leqslant k,$$

tad seko kongruence

$$a^i \equiv a^j \pmod{m}.$$

Tādēļ $(i-j)|k$. Bet tas nav iespējams, jo $i-j<k$. Arī kongruence

$$a^i \equiv 0 \pmod{m}$$

nav iespējama, ja $(a,m)=1$.

Tā kā $k<m$, tad atlikumu rindā $r_1, r_2, \ldots, r_k$ nevar atrasties visi dabiskie skaitļi, kas mazāki par m, bet tikai daži. Ja pakāpju rindu turpina, tad atlikumi atkārtojas tādā pat kārtībā un ar to pašu periodu. Tiešām, sakars

$$r_{k+i} \equiv a^{k+i} = a^k \cdot a^i \equiv a^i \equiv r_i \pmod{m}$$

izteic, ka

$$r_{k+1} = r_1, \quad r_{k+2} = r_2, \text{ u. t. t.}$$

Teorēma 3. Ja a pieder eksponentam k, cits skaitlis a_1 — eksponentam k_1 un $(k,k_1)=1$, tad reizinājums aa_1 pieder eksponentam kk_1 (attiecībā pret vienu un to pašu moduli).

Pierādījums. Ir dots, ka

$$a^k \equiv 1 \pmod{m} \quad \text{un} \quad a_1^{k_1} \equiv 1 \pmod{m}.$$

Pieņemsim, ka

$$(aa_1)^x \equiv 1 \pmod{m}.$$

Kāpinot šīs kongruences abas puses ar k, dabū kongruenci

$$(a^k)^x a_1^{kx} \equiv 1 \pmod{m} \quad \text{jeb} \quad a_1^{kx} \equiv 1 \pmod{m}.$$

No tās seko, ka $kx|k_1$. Tā kā $(k,k_1)=1$, tad

$$x|k_1.$$

Ja kongruences

$$(aa_1)^x \equiv 1 \pmod{m}$$

abas puses kāpina ar k_1, tad tamlīdzīgā kārtā secina, ka $x|k$. Tā tad

$$x|k, \; x|k_1 \quad \text{un} \quad (k,k_1)=1.$$

Tādēļ x dalās arī ar kk_1. Mazākais pozitīvais skaitlis x ar tādu īpašību ir

$$x = kk_1,$$

un tiešām

$$(aa_1)^{kk_1} \equiv (a^k)^{k_1} (a_1^{k_1})^k \equiv 1 \pmod{m}.$$

Teorēmu var vispārināt. Ja a_1 pieder eksponentam k_1, a_2 — eksponentam k_2, ..., a_n — eksponentam k_n, un ik divi no skaitļiem $k_1, k_2, \ldots, k_n$ ir bez kopīga dalītāja, tad reizinājums $a_1 a_2 \ldots a_n$ pieder eksponentam $k_1 k_2 \ldots k_n$.

Teorēma 4. Ja a pieder eksponentam k, tad a^i pieder eksponentam $k_1 = \frac{k}{(k, i)}$, kur (k, i) ir skaitļu k un i lielākais kopīgais dalītājs.

Pierādījums. Pieņemsim, ka a^i pieder eksponentam x. Tad

$$a^{ix} \equiv 1 \pmod{m},$$

un

$$ix \equiv 0 \pmod{k}.$$

Ja $(i, k) = d > 1$, tad kongruenci ar i var saīsināt. Dabū formulu

$$x \equiv 0 \left(\mathrm{mod}\ \frac{k}{d}\right) \quad \text{jeb} \quad x = \frac{k}{d} \cdot t.$$

Mazākais tāda veida skaitlis x ir $k_1 = \frac{k}{d}$, un tiešām

$$(a^i)^{k_1} = a^{i_1 d \cdot k_1} = a^{i_1 k} = (a^k)^{i_1} \equiv 1 \pmod{m},$$

ja $i_1 = \frac{i}{d}$.

Lemma. Divu skaitļu k un s mazāko kopīgo dalāmo m var sadalīt divos faktoros k_1, s_1 tā, ka

$$(k_1, s_1) = 1 \quad \text{un} \quad k | k_1,\ s | s_1.$$

Ja uzraksta k, s un m sadalījumu pirmreizinātājos, tad lemmas pareizība top acīmredzama.

Teorēma 5. Ja a pieder eksponentam k, b — eksponentam s un k_1, s_1, m ir iepriekšējā lemmā minētie skaitļi, tad

$$a^{\frac{k}{k_1}} \cdot b^{\frac{s}{s_1}}$$

pieder eksponentam m (attiecībā pret vienu un to pašu moduli)

Pierādījums. Tā kā $a^{\frac{k}{k_1}}$ pieder eksponentam

$$\frac{k}{\left(k, \frac{k}{k_1}\right)} = \frac{k}{\frac{k}{k_1}} = k_1,$$

$b^{\frac{s}{s_1}}$ pieder eksponentam s_1 un $(k_1, s_1) = 1$, tad $a^{\frac{k}{k_1}} \cdot b^{\frac{s}{s_1}}$ pieder eksponentam $k_1 s_1 = m$.

Šo teorēmu Gauss izlieto primitīvo sakņu noteikšanai.

§ 41. Pirmskaitļu primitīvās saknes.

Definicija. Par pirmskaitļa p primitīvo sakni sauc skaitli g, kas attiecībā pret moduli p pieder eksponentam $\varphi(p) = p - 1$.

Iepriekšējā paragrafa piemērā atradām, ka pirmskaitlim $p = 17$ ir primitīva sakne $g = 3$.

Izlietosim iepriekšejā § pēdējo teorēmu, lai noteiktu primitīvo sakni pirmskaitlim $p = 41$.

Var pārliecināties, ka

$$2^{10} \equiv -1 \pmod{41}.$$

Tādēļ

$$2^{20} \equiv 1 \pmod{41}.$$

Tas nozīmē, ka attiecībā pret moduli 41 skaitlis 2 pieder eksponentam 20. Tā kā

$$3^4 \equiv -1 \pmod{41},$$

tad

$$3^8 \equiv 1 \pmod{41}.$$

Attiecībā pret moduli 41 skaitlis 3 pieder eksponentam 8. Skaitļu 20 un 8 mazākais kopīgais dalāmais $m = 40$ uzrakstāms ar reizinājumu $8 \cdot 5$. Lietojot iepr. § pēdējās teorēmas apzīmējumus, var teikt, ka

$$a = 2,\ b = 3,\ k = 20,\ s = 8,\ k_1 = 5,\ s_1 = 8,\ \frac{k}{k_1} = 4,\ \frac{s}{s_1} = 1.$$

Tā tad skaitlis $2^4 \cdot 3$ pieder eksponentam 40 jeb skaitlis

$$7 \equiv 2^4 \cdot 3 \pmod{41}$$

ir pirmskaitļa 41 primitīvā sakne.

Pierādīsim, ka ar līdzīgu metodi var atrast primitīvo sakni ikkatram pirmskaitlim $p > 2$.

Ja a ir patvaļīgs skaitlis, kas attiecībā pret moduli p pieder eksponentam k un $1 < k < p - 1$, tad skaitļa a pakāpju atlikumi

$$r_1, r_2, \ldots, r_k$$

satur tikai k dažādus pozitīvus skaitļus. Tādēļ var izvēlēties skaitli b, kas nav kongruents nevienam no šiem r_i, un pierādīt, ka b pieder tādam eksponentam s, ar ko k nedalās.

Tiešām, ja pieņem, ka $k|s$, tad, kāpinot kongruenci

$$b^s \equiv 1 \pmod{p}$$

ar $\frac{k}{s}$, dabū

$$b^k \equiv 1 \pmod{p}.$$

Ja b uzskata par nezināmo, tad b ir kongruences

$$x^k \equiv 1 \pmod{p}$$

sakne. Bet tādai kongruencei nav vairak kā k nekongruenti atrisinājumi. Var pārliecināties, ka šie atrisinājumi ir skaitļa a visi pakāpju atlikumi $r_1, r_2, \ldots, r_k$. Te rodas pretruna pieņēmumam, ka b nav kongruents nevienam a pakāpes atlikumam. Ar to ir pierādīts, ka k nedalās ar s

Ja $s|k$, tad $s > k$, un ir atrasts skaitlis b, kas pieder lielākam eksponentam kā iepriekšējais skaitlis a. Ja s nedalās ar k, tad s un k mazākais kopīgais dalāmais m ir lielāks tiklab par s kā par k. Ar iepriekšējā § 5. teorēmu var atrast skaitli

$$c = a^{\frac{k}{k_1}} b^{\frac{s}{s_1}},$$

kas pieder eksponentam m.

Redzam, ka katrā gadījumā var atrast skaitli, kas pieder lielākam eksponentam, kā iepriekš izvēlēta skaitļa a eksponents $k < p - 1$. Ja procesu turpina, tad atrod skaitli g, kas attiecībā pret moduli p pieder eksponentam $p - 1$. Ar to ir pierādīts, ka **katram pirmskaitlim $p > 2$ ir primitīva sakne.**

Šādu teorēmu izteica jau Lamberts 1769. g., un Eulers veltīgi pūlējās to pierādīt (1773. g). Divi pirmie pierādījumi (no tiem vienu jau apskaitjām) ir atrodami Gausa „*Disquisitiones Arithmeticae*". Apskatīsim šai ievērojamai teorēmai vēl otru pierādījumu, kur izlieto sekojošu lemmu.

Lemma. Ja p un q ir pirmskaitļi un $(p-1)|q^n$, tad var atrast skaitli A, kas attiecībā pret moduli p pieder eksponentam q^n.

Pierādījums. Kongruencei

$$x^{\frac{p-1}{q}} \equiv 1 \pmod{p}$$

ir augstākais

$$\frac{p-1}{q} \leqslant p-2$$

atrisinājumi. Tādēļ eksistē skaitlis a, kas neder šai kongruencei, pie kam $0 < a < p$.

Ja apzīmē

$$a^{q^n} = A,$$

tad A nav kongruents ar 1 attiecībā pret moduli p, bet

$$A^{q^n} = a^{p-1} \equiv 1 \pmod{p}.$$

Pieņemsim, ka A pieder eksponentam $x \leqslant q^n$. Tad $q^n | x$ un, ja $q^n > x$, tad arī $q^{n-1} | x$. Tādēļ seko kongruence

$$A^{q^{n-1}} \equiv 1 \pmod{p}.$$

Bet tā nav iespējama, jo

$$A^{q^{n-1}} = a^{\frac{p-1}{q}},$$

un pēc norunas $a^{\frac{p-1}{q}}$ nav kongruents ar 1 attiecībā pret moduli p. Tādēļ $x = q^n$, un lemma pierādīta.

Tagad pierādīsim **teorēmu par primitīvās saknes eksistenci.** Pieņemsim, ka

$$p - 1 = q_1^{a_1} q_2^{a_2} \ldots q_s^{a_s}.$$

Ar iepriekšējo lemmu var atrast skaitļus $A_1, A_2, \ldots, A_s$ tā, ka attiecībā pret moduli p skaitlis A_1 pieder eksponentam $q_1^{a_1}$, A_2 — eksponentam $q_2^{a_2}, \ldots, A_s$ — eksponentam $q_s^{a_s}$. Tā kā ik divi no skaitļiem $q_1^{a_1}, q_2^{a_2}, \ldots, q_s^{a_s}$ ir bez kopīga dalītāja, tad ar iepr. § 3. teorēmu skaitlis

$$g = A_1 A_2 \ldots A_s$$

pieder eksponentam

$$q_1^{a_1} q_2^{a_2} \ldots q_s^{a_s} = p - 1.$$

Tādēļ g ir pirmskaitļa p primitīvā sakne.

Piezīme. Ja pirmskaitļa p primitīvās saknes g pakāpes

$$g, g^2, g^3, \ldots, g^{p-1}$$

dala ar p un atlikumus patur pozitīvus un mazākus par p, tad šie atlikumi ir citādā kārtībā skaitļi 1, 2, 3, . . ., $p - 1$. Minēto pakāpju rindu turpinot, dabū atlikumus, kas atkārtojas iepriekšējā kārtībā. Tiešām, ja

$$i \equiv j \pmod{p-1},$$

tad

$$g^i \equiv g^j \pmod{p},$$

un otrādi.

Teorēma. Katram pirmskaitlim $p > 2$ ir pavisam $\varphi(p-1)$ attiecībā pret moduli p nekongruentas primitīvas saknes.

Pierādījums. Ja g ir pirmskaitļa p primitīvā sakne t. i. g pieder eksponentam $p - 1$ attiecībā pret moduli p, tad g^i pieder eksponentam

$$x = \frac{p-1}{(p-1, i)} \leqslant p - 1.$$

Ir nozīme $x = p - 1$ tikai tad, ja $(p-1, i) = 1$. Tādu skaitļu $i < p - 1$ ir pavisam $\varphi(p-1)$.

Ja bez šīm nozīmēm g^i eksistētu vēl kāda cita primitīva sakne G, tad attiecībā pret moduli p skaitlis G būtu kongruents kādam r ar $0 < r < p$. Tā kā r savukārt kongruents skaitļa g pakāpei g^j ar $0 < j < p - 1$, tad arī

$$G \equiv g^j \pmod{p}.$$

Ja nu pieņemtu, ka G nav kongruents nevienai pakāpei g^i ar $(p-1, i) = 1$, tad

$$(p-1, j) > 1,$$

t. i. G pieder eksponentam $\frac{p-1}{(p-1, j)} < p-1$. Tā tad G nav pirmskaitļa p primitīvā sakne.

Ar šo pierādījumu ir dota arī metode pirmskaitļa p visu primitīvo sakņu noteikšanai gadījumā, ja ir zināma viena sakne.

Piemērs. Pirmskaitļa 17 viena primitīva sakne ir 3. Skaitļi, kas mazāki un bez kopīga dalītāja ar 16, ir 1, 3, 5, 7, 9, 11, 13 un 15. Tādēļ visas pārējās pirmskaitļa 17 primitīvās saknes ir kongruentas ar

$$3^1, 3^3, 3^5, 3^7, 3^9, 3^{11}, 3^{13}, 3^{15}.$$

Jo šos skaitļus atvieto ar to mazākiem pozitīviem atlikumiem attiecībā pret moduli 17, tad dabū sekošas primitīvās saknes:

$$3, 5, 6, 7, 10, 11, 12, 14.$$

Ir pazīstamas Čebiševa teorēmas, kas dažiem pirmskaitļiem nosaka vienu primitīvu sakni. Apskatīsim šo jautājumu par pirmskaitļiem

$$p = 2^m + 1 \quad \text{un} \quad p = 4q + 1.$$

Čebiševa teorēma 1 Ja $p = 2^m + 1$ ir pirmskaitlis, tad tam ir primitīva sakne $g = 3$.

Pierādījums. Vispirms var noskaidrot, ka $2^m + 1$ ir pirmskaitlis tikai tad, ja $m = 0$ vai $m = 2^n$. Tiešām, ja pieņem, ka

$$m = am_1,$$

kur m_1 ir nepāru skaitlis, kas lielāks par 1, tad skaitlis

$$p = 2^m + 1$$

dalās ar

$$2^a + 1 \geqslant 3.$$

Tā tad p nav pirmskaitlis.

Ja skaitlis 3 pieder eksponentam k attiecībā pret moduli $p = 2^m + 1$, tad $p - 1 = 2^m$ dalās ar k, t. i.

$$k = \frac{p-1}{2^a}, \quad \text{kur} \quad a \geqslant 0.$$

Pierādīsim, ka kongruence

$$3^{\frac{p-1}{2}} \equiv 1 (\text{mod } p)$$

ir neiespējama. Tad neiespējama būs arī katra kongruence

$$3^{\frac{p-1}{2^a}} \equiv 1 \ (\text{mod } p) \quad \text{ar} \quad a \geqslant 1,$$

jo no pēdējās kongruences ar kāpināšanu dabū pirmo kongruenci. Tādēļ sekos, ka $a = 0$, $k = p - 1$, un būs pierādīts, ka skaitlis 3 ir p primitīvā sakne.

No kongruences

$$2 \equiv -1 \ (\text{mod } 3)$$

secinām, ka

$$2^{2^n} \equiv 1 \ (\text{mod } 3) \quad \text{un} \quad p = 2^{2^n} + 1 \equiv 2 \ (\text{mod } 3).$$

Tā kā p ir formā $4m+1$, tad Ležandra simbols $\left(\frac{3}{p}\right)$ ir vienāds ar apgriezto, un to var aprēķināt sekojoši:

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

Rezultāts liecina, ka kongruence

$$x^2 \equiv 3 \ (\text{mod } p)$$

nav iespējama. Ar Eulera kritēriju dabū formulu

$$3^{\frac{p-1}{2}} \equiv -1 \ \text{mod } p).$$

Tagad ir acīmredzams, ka kongruence

$$3^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

nav iespējama. Ar to arī viss vajadzīgais ir pierādīts.

Čebiševa teorēma 2. Ja pirmskaitlis $p = 4q + 1$, kur arī q ir pirmskaitlis, tad pirmskaitlim p ir primitīva sakne $g = 2$.

Pierādījums. Pieņemsim, ka attiecībā pret moduli p skaitlis 2 pieder eksponentam k. Tā kā

$$p - 1 = 4q \quad \text{un} \quad 4q|k,$$

tad k ir

$$1, 2, 4, q, 2q, 4q.$$

Pierādīsim, ka ir iespējams tikai pēdējais gadījums, kad $k = 4q$.

Minētās k nozīmes 1, 2 var pārbaudīt tieši.

Ja pieņem $k = 4$, tad dabū kongruenci

$$2^4 \equiv 1 \pmod{p} \quad \text{jeb} \quad 15 \equiv 0 \pmod{p},$$

kas ir iespējama, ja $p = 5$. Tiešām, pirmskaitlim 5 ir primitīva sakne 2. Bet $p = 5$ nav izsakāms ar pirmskaitli q formā $4q + 1$. Tādēļ šo gadījumu, kad $k = 4$, var ignorēt.

Pierādīsim, ka gadījums, kad

$$k = 2q,$$

arī nav iespējams. Tad vēl jo mazāk būs iespējams gadījums, kad $k = q$. Atliks vienīga iespēja $k = 4q$. Tiešām, ja $q = 2$, tad $p = 4q + 1 = 9$ nav pirmskaitlis. Visi pārējie q ir nepāru skaitļi. Tādēļ Ležandra simbola izteiksmē

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

kāpinātājs

$$\frac{p^2 - 1}{8} = q\,(2q + 1)$$

ir nepāru skaitlis.

Tā tad

$$\left(\frac{2}{p}\right) = -1$$

un

$$2^{\frac{p-1}{2}} = 2^{2q} \equiv -1 \pmod{p}.$$

Bet kongruence

$$2^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

nav iespējama.

§ 42. Indeki.

Definīcija. Ja skaitlim A var atrast pirmskaitļa p primitīvās saknes g tādu pakāpi g^a, ka

$$g^a \equiv A \pmod{p},$$

tad eksponentu a sauc par skaitļa A **indeku** (attiecībā pret moduļa p primitīvo sakni g). Raksta:

$$a = \mathrm{Ind}_g A.$$

Indeka jēdzienu ir lietojis jau Eulers, bet nosaukumu un apzīmējumu ir devis Gauss. Indeka nosaukumu var izskaidrot ar sekošo. Moduļa p primitīvās saknes pakāpju

$$g^1, g^2, g^3, \ldots, g^i, \ldots, g^{p-1}$$

atlikumi

$$r_1, r_2, r_3, \ldots, r_i, \ldots, r_{p-1}$$

satur visus dabiskos skaitļus no 1 līdz $p-1$. Ja skaitlis $N < p$ ir vienlīdzīgs atlikumam r_i, tad šī atlikuma rādītāju (indeku) i sauc par skaitļa N indeku. Tas nozīmē: ja $N = r_i$, tad $\mathrm{Ind}_g N = i$.

Teorēma 1. Katram skaitlim A, kas nedalās ar moduli p, ir indeks.

Pierādījums. No vienas puses A kongruents ar vienu pozitīvu skaitli r_i, kas mazāks par p. No otras puses tāds r_i kongruents primitīvās saknes kādai pakāpei g^i, kur $0 \leqslant i < p-1$. Tādēļ arī

$$A \equiv g^i \pmod{p} \quad \text{jeb} \quad \mathrm{Ind}_g A = i.$$

Skaitlim A nav indeka tad, ja $A \equiv 0 \pmod{p}$ Tiešām, ja pieņem $\operatorname{Ind}_g 0 = i$, tad seko, ka $g^i \mid p$. Tā tad arī $g \mid p$, un g nevar būt moduļa p primitīvā sakne.

Katram skaitlim A, kas nedalās ar p ir bezgala daudz indeku. Tiešām, ja

$$\operatorname{Ind}_g A = a \quad \text{jeb} \quad g^a \equiv A \pmod{p},$$

tad arī

$$g^{a+t(p-1)} \equiv A \pmod{p},$$

kur t ir vesels skaitlis. No tā seko $\operatorname{Ind}_g A$ vispārīgā nozīme

$$\operatorname{Ind}_g A = a + t(p-1).$$

Noteiklības dēļ pieņem, ka $\operatorname{Ind}_g A$ ir pozitīvs skaitlis, kas mazāks par $p - 1$.

Sekas. Ja $A \equiv B \pmod{p}$, tad $\operatorname{Ind}_g A \equiv \operatorname{Ind}_g B \pmod{p-1}$.

Aprēķināsim indekus skaitļiem g, 1 un

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

Rezultāti:

$$\operatorname{Ind}_g g = 1 \quad \text{un} \quad \operatorname{Ind}_g 1 = 0$$

ir paši par sevi saprotami.

Lai noteiktu $\operatorname{Ind}_g (-1)$, izlietosim kongruenci mazā Fermā teorēmā:

$$g^{p-1} - 1 \equiv 0 \pmod{p} \quad \text{jeb} \quad (g^{\frac{p-1}{2}} - 1)(g^{\frac{p-1}{2}} + 1 \equiv 0 \pmod{p}).$$

Ja g ir pirmskaitļa p primitīvā sakne, tad pirmais faktors pēdējā kongruencē nedalās ar p. Tādēļ otrajam faktoram ir jādalās ar p. No tā seko, ka

$$g^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

jeb

$$\operatorname{Ind}_g (-1) = \frac{p-1}{2}.$$

Teorēma 2. $\operatorname{Ind}_g (AB) \equiv \operatorname{Ind}_g A + \operatorname{Ind}_g B \pmod{p-1}$.

Pierādījumam pieņemsim, ka

$g^a \equiv A \pmod{p}$, $g^b \equiv B \pmod{p}$ un $g^c \equiv AB \pmod{p}$.

Tad

$$g^{a+b} \equiv AB \pmod{p} \quad \text{jeb} \quad g^{a+b} \equiv g^c \pmod{p}.$$

No § 40. teōr. 2. seko, ka

$$c \equiv a + b \pmod{p-1}.$$

Teorēma pierādīta. Vairāk reizinātājiem $A_1, A_2, \ldots, A_n$ to var vispārināt ar formulu

$$\mathrm{Ind}_g (A_1 A_2 \ldots A_n) \equiv \mathrm{Ind}_g A_1 + \mathrm{Ind}_g A_2 + \ldots + \mathrm{Ind}_g A_n \pmod{p-1}.$$

Ja pieņem $A_1 = A_2 = \ldots = A_n = A$, tad seko formula

$$\mathrm{Ind}_g (A^n) \equiv n \, \mathrm{Ind}_g A \pmod{p-1}.$$

Gadījumā, kad $A|B$, tad

$$\mathrm{Ind}_g A = \mathrm{Ind}_g \left(\frac{A}{B} \cdot B\right) \equiv \mathrm{Ind}_g \left(\frac{A}{B}\right) + \mathrm{Ind}_g B \pmod{p-1}.$$

Tā tad

$$\mathrm{Ind}_g \left(\frac{A}{B}\right) \equiv \mathrm{Ind}_g A - \mathrm{Ind}_g B \pmod{p-1}.$$

Indeku īpašības aritmētikā lielā mērā atgādina **logaritmu** īpašības algebrā. Analoģiju vēl pastiprina divas sekojosas sakarības.

Ja a un b ir pirmskaitļa p divas primitīvas saknes, tad

(1) $\mathrm{Ind}_a A \equiv \mathrm{Ind}_b A \cdot \mathrm{Ind}_a b \pmod{p-1}$,

un

(2) $\mathrm{Ind}_a b \cdot \mathrm{Ind}_b a \equiv 1 \pmod{p-1}$.

Šīs īpašības pierāda tamlīdzīgi, kā attiecīgās logaritmu īpašības algebrā. Ja pieņem ka

$$\mathrm{Ind}_a A = x \quad \text{un} \quad \mathrm{Ind}_b A = y,$$

tad seko formula

$$A \equiv a^x \equiv b^y \pmod{p}.$$

Kongruentiem skaitļiem a^x un b^y ir vienādi indeki. Ja uzraksta to indekus attiecībā pret primitīvo sakni a un liek x vietā $\mathrm{Ind}_a A$ un y vietā $\mathrm{Ind}_b A$, tad formula (1) ir pierādīta. Formula (2) seko no (1), ja pieņem $A = a$.

Noslēgsim šo nodaļu ar **indeku izlietošanu praktikā.** Sastadot indeku tabulu, piem., pirmskaitļa 13 primitīvai saknei 2, dabūsim sekošo:

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

Pirmās indeku tabulas pirmskaitļiem $p < 200$ sastādīja Ostrogradskis 1837. g. Jakobi publicēja indeku tabulas pirmskaitļiem līdz 1000 („*Canon Arithmeticus*“ 1839. g.). Tagad indeku tabulas sniedzas pirmskaitļos jau līdz 10000 (*E. Maillet* 1910. g.).

Kā pirmo piemēru indeku tabulu izlietošanai, atrisināsim kongruenci

$$5x \equiv 9 \pmod{13}.$$

Ja izlieto 2. teorēmu un pirmskaitļa 13 indeku tabulu, tad dabū kongruenci

$$\mathrm{Ind}\ 5 + \mathrm{Ind}\ x \equiv \mathrm{Ind}\ 9 \pmod{12}$$

jeb

$$9 + \mathrm{Ind}\ x \equiv 8 \pmod{12}.$$

No šejienes atrod, ka

$$\mathrm{Ind}\ x \equiv -1 \equiv 11 \pmod{12} \quad \text{un} \quad x \equiv 7 \pmod{13}.$$

Otrs piemērs. Binomāla kongruence

$$7x^{16} \equiv 11 \pmod{13}.$$

Atrisinājumu atrod, sastādot indeku:

$$\mathrm{Ind}\ 7 + 16\ \mathrm{Ind}\ x \equiv \mathrm{Ind}\ 11 \pmod{12}$$

un pārveidojot:

$$11 + 16 \operatorname{Ind} x \equiv 7 \pmod{12}$$

jeb

$$16 \operatorname{Ind} x \equiv 8 \pmod{12}.$$

Ja saīsina, tad dabū kongruenci

$$2 \operatorname{Ind} x \equiv 1 \pmod{3}$$

ar atrisinājumu

$$\operatorname{Ind} x \equiv -1 \pmod{3}.$$

Attiecībā pret moduli 12 Ind x ir kongruents ar 2, 5, 8, 11. Tādēļ dotajai kongruencei ir četri atrisinājumi:

$$x \equiv 4, 6, 9, 7 \pmod{13}.$$

IX. Binomālās kongruences.

§ 43. Eulera kritērijs.

Ja binomālā kongruence ir dota sekojošā vispārīgā veidā

$$Ax^m \equiv Bx^k \pmod{p},$$

tad viens atrisinājums ir $x_1 \equiv 0 \pmod{p}$. Pārējie atrisinājumi ar p nedalās. Tādēļ kongruences abas puses ar x^k var dalīt, ja $k < m$. Ja atrod skaitli A_1, kas ir asociētais ar A, t. i.

$$AA_1 \equiv 1 \pmod{p},$$

tad kongruenci var parveidot **kanoniskā formā**

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

Ja šī kongruence ir iespējama, tad ir iespējama arī pirmās pakāpes kongruence

$$n \operatorname{Ind} x \equiv \operatorname{Ind} a \pmod{p-1},$$

attiecībā pret Ind x, kur indeks sastādīts ar kautkādu pirmskaitļa p primitīvo sakni. Tādēļ Ind a jādalās ar n un $p-1$ lielāko kopīgo dalītāju $d = (n, p-1)$. Ja Ind $a \mid d$, tad kongruenci ar d var saīsināt. Rodas kongruence

$$\frac{n}{d} \operatorname{Ind} x \equiv \frac{\operatorname{Ind} a}{d} \left(\operatorname{mod} \frac{p-1}{d} \right)$$

ar

$$\left(\frac{n}{d}, \frac{p-1}{d} \right) = 1.$$

Tādēļ no šejienes Ind x var aprēķināt, un tad ar indeku tabulām atrast x. Ar to ir pierādīts sekošais.

Lai kongruence $x^n \equiv a \pmod{p}$ būtu iespējama, ir nepieciešami un pietiekoši, ka Ind $a \mid (n, p-1)$.

Izteiksim šo **kritēriju** citādā formā. Ja $(n, p-1)=d$ un $\operatorname{Ind} a \mid d$, tad

$$\operatorname{Ind} a = kd \qquad \text{jeb} \qquad a \equiv g^{kd} \pmod{p}.$$

Pēdējās kongruences abas puses kāpinot ar $\frac{p-1}{d}$, dabū

$$a^{\frac{p-1}{d}} \equiv (g^{p-1})^k \equiv 1 \pmod{p}.$$

Arī otrādi: ja

$$a^{\frac{p-1}{d}} \equiv 1 \pmod{p},$$

tad

$$\frac{p-1}{d} \operatorname{Ind} a \equiv 0 \pmod{p-1}.$$

Saīsinot ar $\frac{p-1}{d}$, dabū

$$\operatorname{Ind} a \equiv 0 \pmod{d}, \qquad \text{t. i.} \qquad \operatorname{Ind} a \mid d.$$

Tādēļ var izteikt sekošu **kritēriju**, ko atradis Eulers 1755. g.

Lai kongruence $x^n \equiv a \pmod{p}$ būtu iespējama, ir nepieciešams un pietiekošs noteikums, ka

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

Piemērs. 1. Kongruence $x^2 \equiv a \pmod{p}$ ir iespējama tad, ja $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ jeb Ležandra simbols $\left(\frac{a}{p}\right) = +1$.

2. Kongruence $x^n \equiv 1 \pmod{p}$ ir vienmēr iespējama.

Teorēma. Ja kongruence

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

ir iespējama, viens tās atrisinājums ir x_0 un kongruences

$$\xi^n \equiv 1 \pmod{p}$$

atrisinājumi ir $\xi_1, \xi_2, \ldots$, tad dotās kongruences $x^n \equiv a \pmod{p}$ atrisinājumi ir skaitļi

$$x_0\,\xi_1,\quad x_0\,\xi_2,\ \ldots$$

Par to pārliecinājas sekojošā veidā. Ja

$$\xi_k^n \equiv 1 \pmod{p} \quad \text{un} \quad x_0^n \equiv a \pmod{p},$$

tad

$$(x_0\,\xi_k)^n \equiv a \pmod{p},$$

t. i. $x_0\,\xi_k$ ir kongruences $x^n \equiv a \pmod{p}$ sakne. Ja bez šiem skaitļiem $x_0\,\xi_k$ eksistētu vēl kāda cita sakne y, tad no formulām

$$x_0^n \equiv a \pmod{p}, \quad y^n \equiv a \pmod{p}$$

secinātu

$$x_0^n \equiv y^n \pmod{p}.$$

Varētu atrast skaitli b tā, ka

$$x_0\,b \equiv 1 \pmod{p} \quad \text{un} \quad x_0^n b^n \equiv 1 \pmod{p}.$$

Liekot x_0^n vietā y^n, dabū kongruenci

$$y^n\,b^n \equiv 1 \pmod{p} \quad \text{jeb} \quad (y\,b)^n \equiv 1 \pmod{p}.$$

No tās sekotu, ka yb ir kongruences $\xi^n \equiv 1 \pmod{p}$ kāda sakne ξ_k. Tā tad

$$yb \equiv \xi_k \pmod{p}.$$

Ja pēdējai kongruencei abas puses reizinātu ar x_0, tad dabūtu

$$y \equiv x_0\,\xi_k \pmod{p}.$$

Ar to izteiktais apgalvojums ir pierādīts.

Turpmāk kongruences $x^n \equiv a \pmod{p}$ vietā var apskatīt vienkāršāku gadījumu $x^n \equiv 1 \pmod{p}$.

§ 44. Kongruence $x^n \equiv 1 \pmod{p}$.

Par šo kongruenci pierādīsim sekojošas teorēmas.

Teorēma 1: Divu kongruenču $x^m \equiv 1 \pmod{p}$ un $x^n \equiv 1 \pmod{p}$ katra kopīga sakne x_1 ir sakne arī kongruencei $x^d \equiv 1 \pmod{p}$, kur $d=(m, n)$, un otrādi.

Pierādījums. Ja $(m, n) = d$, tad var atrast divus veselus pozitīvus skaitļus M, N tā, ka

$$Mm - Nn = d.$$

Ja

$$x_1^m \equiv 1 \pmod{p} \quad \text{un} \quad x_1^n \equiv 1 \pmod{p},$$

tad kāpinot šīs kongruences attiecīgi ar M un N un salīdzinot dabūsim kongruenci

$$x_1^{Mm} \equiv x_1^{Nn} \pmod{p}.$$

Tā kā $(x_1, p) = 1$, tad abas puses ar x_1^{Nn} var izdalīt. Rodas kongruence

$$x_1^{Mm-Nn} \equiv 1 \pmod{p} \quad \text{jeb} \quad x_1^d \equiv 1 \pmod{p}.$$

Otrādi: ja

$$m = dm_1, \quad n = dn_1, \quad \text{un} \quad x_0^d \equiv 1 \pmod{p},$$

tad arī

$$x_0^{dn_1} \equiv 1 \pmod{p} \quad \text{un} \quad x_0^{dm_1} \equiv 1 \pmod{p}.$$

Tā tad

$$x_0^m \equiv 1 \pmod{p} \quad \text{un} \quad x_0^n \equiv 1 \pmod{p}.$$

Tagad var izteikt sekošu apgalvojumu. Lai atrastu kongruences $x^n \equiv 1 \pmod{p}$ visas saknes, pietiek atrast kongruenču

$$x^n \equiv 1 \pmod{p} \quad \text{un} \quad x^{p-1} \equiv 1 \pmod{p}$$

kopīgās saknes. Tas tādēļ, ka katrs x, kas nedalās ar p, ir otrās kongruences sakne. Tā tad „kopīgās saknes" patiesībā nozīmē visas pirmās kongruences saknes.

Ja $(n, p-1) = d$, tad kongruence $x^n \equiv 1 \pmod{p}$ ir līdzvērtīga ar kongruenci

$$x^d \equiv 1 \pmod{p},$$

kam sakņu skaits ir maksimālais. Tiešām $x^{p-1} - 1$ dalās ar $x^d - 1$ un kongruencei

$$x^{p-1} - 1 \equiv 0 \pmod{p}$$

sakņu skaits ir maksimālais. Tas nozīmē, ka kongruencei

$$x^n \equiv 1 \pmod{p}, \quad \text{resp.} \quad x^d \equiv 1 \pmod{p}$$

ir tieši

$$d = (n, p - 1)$$

atrisinājumu. Var pārbaudīt, ka šie atrisinājumi ir skaitļi

$$g^{\frac{p-1}{d}},\ g^{2\cdot\frac{p-1}{d}},\ g^{3\cdot\frac{p-1}{d}},\ \ldots,\ g^{d\cdot\frac{p-1}{d}}$$

(g ir moduļa p primitīvā sakne), kas visi ir dažādi. Tiešām, der kongruence

$$(g^{i\cdot\frac{p-1}{d}})^d \equiv (g^{p-1})^i \equiv 1 \pmod{p}.$$

Ja pieņem, ka

$$g^{i\cdot\frac{p-1}{d}} = g^{j\cdot\frac{p-1}{d}} \pmod{p}, \quad 0 < j < i \leqslant d,$$

tad seko kongruence

$$\frac{p-1}{d}\cdot i \equiv \frac{p-1}{d}\cdot j \pmod{p-1} \quad \text{jeb} \quad i \equiv j \pmod{d},$$

kas nav iespējama.

Piemērs. Kongruence $x^{16} \equiv 1 \pmod{13}$.

Moduļa $p=13$ primitīvā sakne $g=2$ un $(n, p-1)=(16, 12)=4$. Tādēļ kongruencei $x^{16} \equiv 1 \pmod{13}$ ir 4 atrisinājumi:

$$2^3,\ 2^6,\ 2^9,\ 2^{12} \quad \text{jeb} \quad -5,\ -1,\ 1,\ 5.$$

§ 45. Kubiskie atlikumi.

Kubisko kongruenču

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

atrisināšanā ir iespējami divi gadījumi.

1. Ja $p = 3k + 1$, tad $(3,\ p - 1) = 3$. Kad ir izpildīts nosacījums

$$a^{\frac{p-1}{3}} \equiv 1 \pmod{p},$$

tad kongruence $x^3 \equiv a \pmod{p}$ ir iespējama, un tai ir trīs atrisinājumi. Eksistē

$$\left(\frac{p-1}{3}, p-1\right) = \frac{p-1}{3}$$

veseli pozitīvi skaitļi $a < p$ tā, ka

$$a^{\frac{p-1}{3}} \equiv 1 \pmod{p}.$$

Šādus a sauc par moduļa p kubiskiem atlikumiem. Tā tad, ja ignorē gadījumu, kad $a = 0$, tad modulim $p = 3k + 1$ ir $\frac{p-1}{3}$ kubisku atlikumu un $2 \cdot \frac{p-1}{3}$ neatlikumu.

2. Ja $p = 3k + 2$, tad $(3, p - 1) = 1$, un kongruencei

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

der ikkatrs a, kas nedalās ar p. Tas nozīmē, ka modulim $p = 3k + 2$ kubisku neatlikumu nemaz nav. Kongruence $x^3 \equiv a \pmod{p}$ ir iespējama ikkatram veselam a, un tai ir $(3, p - 1) = 1$ atrisinājums.

Ar tamlīdzīgu metodi var apskatīt arī augstāku pakāpju atlikumus.

Piezīme. Reciprocitātes likums binomālām kongruencēm mūsu dienās ir pilnīgi izstrādāts. Pēc kvadrātisko kongruenču reciprocitātes likuma pierādīšanas Gauss, izlietojot kompleksos skaitļus $a + bi$ $(i = \sqrt{-1})$, deva reciprocitātes likumu arī 4. pakāpes binomālām kongruencēm. Gausa idejas ierosināts Eizenšteins (*Eisenstein*) pētīja algebriskos skaitļus

$$a + b\varrho \quad \text{ar} \quad \varrho = \sqrt[3]{1} = \frac{-1 + i\sqrt{3}}{2}$$

un 1844. g. deva reciprocitātes likumu kubiskām kongruencēm (*Crelles Journal für Mathematik, Bd.* 27). Ar šiem Gausa un Eizenšteina darbiem tika ievadīta algebrisko skaitļu teōrija.

X. Skaitļu sadalīšana kvadrātu summā.

§ 46. Bašē (*Bachet*) un Lagranža (*Lagrange*) teorēma.

Bašē un Lagranža teorēmu minējām jau § 1. Izmēģinot ar veseliem skaitļiem no 1 līdz 325, Bašē ievēroja, ka katru veselu skaitli var izteikt ar četru kvadrātu summu, bet šo īpašību nevarēja pierādīt. Arī Euleram tas neizdevās. Tā vietā Eulers pierādīja, ka katru pirmskaitli $p = 4n + 1$ var izteikt ar divu kvadrātu summu un tikai vienā veidā. Pirmo reiz Bašē teorēmu pierādīja Lagranžs 1770. g. un publicēja 1772. g. (*Nouv. Mém. Acad. Roy., Berlin*). No vēlākiem pierādījumiem vienkāršākais pieder franču inženieram Matrō (*Matrot*) 1890. g. Šajā pierādījumā izlieto trīs lemmas, no kuŗām pirmo devis Eulers, otro Lagranžs un trešo Matrō.

I. lemma. Ja četru kvadrātu summu reizina ar citu (vai to pašu) četru kvadrātu summu, tad arī rezultātu var izteikt ar četru kvadrātu summu.

Šo lemmu pierāda ar formulu

$$(1)\quad (a^2+b^2+c^2+d^2)(x^2+y^2+z^2+t^2)=(ax+by+cz+dt)^2+$$
$$+(ay-bx+ct-dz)^2+(az+bt-cx-dy)^2+(at+bz-cy-dx)^2,$$

ko sauc par Eulera identitāti. Formulu var pārbaudīt, atveŗot iekavas. Var arī pierādīt ar determinantu reizināšanas teorēmu. Ir acīmredzams, ka determinants

$$\begin{vmatrix} a+bi & c+di \\ -c+di & a-bi \end{vmatrix} \qquad (i=\sqrt{-1})$$

ir vienlīdzīgs ar $a^2 + b^2 + c^2 + d^2$. Tādēļ var rakstīt sekošu pārveidojumu:

$$(a^2+b^2+c^2+d^2)(x^2+y^2+z^2+t^2)=\begin{vmatrix} a+bi, & c+di \\ -c+di & a-bi \end{vmatrix} \cdot \begin{vmatrix} x+iy & z-it \\ -z+it & x-iy \end{vmatrix}.$$

Ar determinantu reizināšanas teorēmu izteic pēdējo divu determinantu reizinājumu ar

$$\begin{vmatrix} (ax-by+cz-dt)+i(ay+bx+ct+dz), & (-az-bt+cx+dy)+i(at-bz-cy+dx) \\ -(-az-bt+cx+dy)+i(at-bz-cy+dx), & (ax-by+cz-dt)-i(ax+by+ct+dz) \end{vmatrix}.$$

Tādēļ

$$(a^2 + b^2 + c^2 + d^2)(x^2 + y^2 + z^2 + t^2) = (ax - by + cz - dt)^2 + (ay+bx+ct+dz)^2+(-az-bt+cx+dy)^2+(at - bz - cy + dx)^2.$$

Rezultāts nav formāli identisks ar formulu (1). Tas norāda, ka reizinājumu $(a^2 + b^2 + c^2 + d^2)(x^2 + y^2 + z^2 + t^2)$ var izteikt ar četru kvadrātu summu vairāk veidos.

II. lemma. Ja kāds nepāru skaitlis $m > 2$ dala tādu četru kvadrātu summu, kam visiem nav kopīga dalītāja, tad šis skaitlis m pats ir četru kvadrātu summa, t. i.

ja $(A^2 + B^2 + C^2 + D^2) \mid m$, tad $m = \alpha^2 + \beta^2 + \gamma^2 + \delta^2$.

Šo lemmu pierādīja Lagranžs, un Eulers pierādījumu vienkāršoja tādā veidā, kā te apskatīsim.

Ja pieņemam, ka

$$A \equiv a,\ B \equiv b,\ C \equiv c,\ D \equiv d \pmod{p},$$

kur a, b, c un d absolūtās vērtības ir mazākas par $\frac{m}{2}$, tad dabūjam kongruenci

$$A^2 + B^2 + C^2 + D^2 \equiv a^2 + b^2 + c^2 + d^2 \equiv 0 \pmod{m}.$$

Redzam, ka

$(a^2 + b^2 + c^2 + d^2) < m^2$ un $(a^2 + b^2 + c^2 + d^2) | m$.

Tas nozīmē, ka

$$(2) \qquad a^2 + b^2 + c^2 + d^2 = m \cdot n \qquad (n < m).$$

Ja gadītos, ka $n = 1$, tad lemma būtu pierādīta. Ja $n \neq 1$, tad pierādīsim, ka var atrast četrus skaitļus a_1, b_1, c_1, d_1 tā, ka

$$a_1^2 + b_1^2 + c_1^2 + d_1^2 = m \cdot n_1 \quad \text{un} \quad n_1 < n.$$

Ja arī $n_1 \neq 1$, tad procesu var turpināt līdz tādam skaitlim n_k, kas vienlīdzīgs ar 1.

Vispirms pieņemsim, ka formulā (2) n ir pāru skaitlis $2k$. Ja ievērojam, ka attiecībā pret moduli 2, katrs vesels skaitlis ir kongruents ar savu kvadrātu, tad no formulas

$$(3) \qquad a^2 + b^2 + c^2 + d^2 = 2mk$$

seko kongruence

$$a + b + c + d \equiv 0 \pmod 2.$$

No skaitļiem a, b, c, d visi četri nevar būt pāru skaitļi (tad tiem būtu kopīgs dalītājs 2, ar ko formulu (3) varētu saīsināt), ne arī trīs pāru un viens nepāru skaitlis. Pierādījumu nemaz nesašaurinot, var pieņemt, ka

$$d + b \equiv 0 \pmod 2 \quad \text{un} \quad c + d \equiv 0 \pmod 2.$$

Tad $\frac{a \pm b}{2}$ un $\frac{c \pm d}{2}$ ir veseli skaitļi, un no (3) seko formula

$$(4) \qquad \left(\frac{a+b}{2}\right)^2 + \left(\frac{a-b}{2}\right)^2 + \left(\frac{c+a}{2}\right)^2 + \left(\frac{c-d}{2}\right)^2 = mk$$

ar $k < n$.

Ja formulā (2) n ir nepāru skaitlis un ievēro, ka $(a^2 + b^2 + c^2 + d^2) | n$, tad ar tādu pat metodi kā iepriekš var atrast veselus skaitļus x, y, z, t tā, ka

$$a \equiv x, \quad b \equiv y, \quad c \equiv z, \quad d \equiv t \pmod{n}$$

un

$$(5) \qquad x^2 + y^2 + z^2 + t^2 = nn_1 \quad \text{ar} \quad n_1 < n$$

Formulas (2) un (5) sareizinot, dabū formulu

$$(6) \qquad A^2 + B^2 + C^2 + D^2 = mn^2n_1,$$

kur katrs no skaitļiem A, B, C un D dalās ar n. Pēdējo pierāda ar Eulera identitāti (1), ja x, y, z, t vietā liek attiecīgi

$$a - nl_1, \quad b - nl_2, \quad c - nl_3, \quad d - nl_4.$$

Tad dabū

$$A = ax + by + cz + dt = a(a - nl_1) + b(b - nl_2) + c(c - nl_3) + d(d - nl_4)$$

jeb

$$A = a^2 + b^2 + c^2 + d^2 - n(al_1 + bl_2 + cl_3 + dl_4) \equiv 0 \pmod{n}.$$

Tamlīdzīgi pierāda, ka arī

$$B \equiv 0, \quad C \equiv 0 \quad \text{un} \quad D \equiv 0 \pmod{n}.$$

Ja formulas (6) abas puses dala ar n^2 un apzīmē

$$\frac{A}{n} = a_1, \quad \frac{B}{n} = b_1, \quad \frac{C}{n} = c_1, \quad \frac{D}{n} = d_1,$$

tad dabū formulu

$$a_1^2 + b_1^2 + c_1^2 + d_1^2 = mn_1 \quad \text{ar} \quad n_1 < n.$$

Ja $n_1 = 1$, tad lemma ir pierādīta; ja $n_1 > 1$, tad tamlīdzīgā kārtā var konstruēt formulu

$$a_2^2 + b_2^2 + c_2^2 + d_2^2 = mn_2 \quad \text{ar} \quad n_2 < n_1, \quad \text{u. t. t.}$$

Ja lemmā minēto nepāru skaitli m pieņem par **pirmskaitli** $p > 2$, tad ir pierādīts sekošais: **Ja p ir pirmskaitlis, kas dala četru kvadrātu summu $A^2 + B^2 + C^2 + D^2$ un $(A, B, C, D) = 1$, tad arī p var izteikt ar četru kvadrātu summu**

III. lemma. Ikkatrs pirmskaitlis $p > 2$ dala divu vai triju tādu kvadrātu summu, kam nav kopīga dalītāja.

Pieņemsim, ka $p = 2n + 1$, un apskatīsim sekojošus **trīs gadījumus.**

1. Ir iespējams, ka $2n$ ir moduļa p kvadrātisks atlikums. Tad var atrast veselu skaitli x tā, ka

$$x^2 \equiv 2n \equiv p - 1 \pmod{p} \quad \text{jeb} \quad x^2 + 1 \equiv 0 \pmod{p}.$$

Ar to šim gadījumam lemma pierādīta.

2. Ja skaitlis n ir moduļa p kvadrātisks atlikums, tad pastāv kongruence

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

vai

$$2x^2 \equiv 2n \equiv -1 \pmod{p}.$$

Var atrast veselu skaitli x tā, ka

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

3. Ja n un $2n$ ir moduļa p kvadrātiski neatlikumi, tad visus dabiskos skaitļus, kas mazāki par p un nav vienlīdzīgi ne ar n, ne $2n$, var savienot $\frac{p-3}{2}$ pāros

$(1, 2n-1), (2, 2n-2), (3, 2n-3), \ldots, (q, 2n-q), \ldots, (n-1, n+1)$

tā, ka katrā pārī skaitļu summa ir $2n$. Ievērojot, ka pāru ir skaitā $\frac{p-3}{2}$, bet kvadrātisku atlikumu $\frac{p-1}{2}$, var apgalvot, ka vismaz viens skaitļu pāris satur divus moduļa p kvadrātiskus atlikumus. Ja šis pāris ir $(q, 2n-q)$, tad pastāv veseli skaitļi x un y tā, ka

$$x^2 \equiv q \pmod{p} \quad \text{un} \quad y^2 \equiv 2n - q \pmod{p}$$

jeb

$$x^2 + y^2 + 1 \equiv 0 \pmod{p}$$

Tagad var pierādīt **Bašē teorēmu**. Tā kā pirmskaitli 2 var

izteikt ar četru kvadrātu summu $1^2 + 1^2 + 0^2 + 0^2$, un katrs pirmskaitlis $p > 2$ dala četru kvadrātu summu

$$x^2 + 1 + p^2 + p^2 \quad \text{vai} \quad x^2 + y^2 + 1 + p^2,$$

tad ar Lagranža lemmu (II) katru pirmskaitli var izteikt ar četru kvadrātu summu. Ja izlieto Eulera identitāti, tad arī katru pirmskaitļu reizinājumu, un tā tad vispār katru skaitli var izteikt ar četru kvadrātu summu.

Piezīme 1. Ir skaitļi, kas izteicāmi ar mazāk kā četru kvadrātu summu, bet skaitļiem

$$4^m.(8n + 7) \quad \text{ar} \quad m \geqslant 0, \quad n \geqslant 0$$

ir nepieciešami četri kvadrāti.

2. Skaitļu sadalīšanā kubu summā tādas izņēmuma formas nepastāv. 1909. g. Landavs (*Landau*) pierādīja, ka visus skaitļus, kas lielāki par noteiktu robežu, var izteikt ar 8 kubu summu un vēl lielākus ar 7 kubu summu.

§ 47. Uōringa (*Waring*) problēma.

Dažas vēsturiskas ziņas par Uōringa problēmu ir dotas § 1. Te apskatīsim **Liuviļa pierādījumu***), ka katru veselu skaitli var izteikt ar veselu skaitļu ceturto pakāpju summu, nelietojot vairak kā 53 saskaitāmos. Saprotams, tāds novērtējums ir diezgan nepilnīgs, bet tam pierādījums ir elementārs. Ar analītiskām metodēm Hardī un Litlevūds pierādīja (1921.g.), ka saskaitāmo nevajaga vairāk kā 21, bet Landavs pierādīja, ka ir bezgala daudz skaitļu, ko nevar izteikt ar mazāk kā 15 bikvadrātiem.

*) Pierādījums publicēts 1859. g. darbā: *Lebesque „Exercices d'analyse numérique"*.

Liuviļa pierādījumā izlieto sekošas 6 identitātes:

$$(x+y)^4+(x-y)^4=2x^4+2y^4+12x^2y^2$$
$$(x+z)^4+(x-z)^4=2x^4+2z^4+12x^2z^2$$
$$(x+t)^4+(x-t)^4=2x^4+2t^4+12x^2t^2$$
$$(y+z)^4+(y-z)^4=2y^4+2z^4+12y^2z^2$$
$$(y+t)^4+(y-t)^4=2y^4+2t^4+12y^2t^2$$
$$(z+t)^4+(z-t)^4=2z^4+2t^4+12z^2t^2.$$

Ja tās saskaita, tad kreisajā pusē dabū 12 bikvadrātu summu, bet labajā pusē skaitli

$$6[x^4+y^4+z^4+t^4+2x^2y^2+2x^2z^2+2x^2t^2+2y^2z^2+2y^2t^2+2z^2t^2]$$

jeb

$$6\,(x^2+y^2+z^2+t^2)^2=6A^2,$$

kur

$$A=x^2+y^2+z^2+t^2.$$

Ar to ir pierādīts, ka katru skaitli $6A^2$ var izteikt ar 12 bikvadrātu summu.

Tā kā katru skaitli M var izteikt ar četru kvadrātu summu $A^2+B^2+C^2+D^2$, tad skaitli

$$6M=6A^2+6B^2+6C^2+6D^2$$

var izteikt ar 48 bikvadrātu summu.

Ja ievēro, ka katrs skaitlis X ir izteicams ar vienu no sekošām 6 formām:

$$6M,\quad 6M+1,\quad 6M+2,\quad 6M+3,\quad 6M+4,\quad 6M+5$$

un ka

$$1=1^4,\ 2=1^4+1^4,\ 3=1^4+1^4+1^4,$$
$$4=1^4+1^4+1^4+1^4,\ 5=1^4+1^4+1^4+1^4+1^4,$$

tad seko, ka X var izteikt ar ceturto pakāpju skaitļu summu, nelietojot vairāk kā

$$48,\ 49,\ 50,\ 51,\ 52 \text{ vai } 53$$

saskaitāmos. Ar to apgalvojums pierādīts.

§ 48. Pirmskaitļa $p = 4n + 1$ sadalīšana divu kvadrātu summā.

Lemma. Ja $(a, b) = 1$ un $a^2 + b^2$ dalās ar pirmskaitli p, tad var atrast veselus skaitļus x un y ar $(x, y) = 1$ tā, ka $p = x^2 + y^2$.

Pierādījums tamlīdzīgs kā Lagranža pierādījums par četru kvadrātu summu (§ 46.).

Ja $p = 4n + 1$, tad Ležandra simbols

$$\left(\frac{-1}{p}\right) = +1.$$

Tas nozīmē, ka var atrisināt kongruenci

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

un atrast skaitli x tā, ka $(x^2 + 1) \mid p$. Ja izlietojam iepriekšējo lemmu, tad secinām, ka katru pirmskaitli $p = 4n + 1$ var izteikt ar divu kvadrātu summu. Pierādīsim, ka tas iespējams tikai vienā veidā.

Pieņemsim, ka $p = 4n + 1$ var izteikt ar kvadrātu summu divos dažādos veidos*)

$$(1) \qquad p = x^2 + y^2 = x_1^2 + y_1^2$$

un $x > x_1$ (ja pieņem $x = x_1$, tad seko, ka arī $y = y_1$). Tad $y < y_1$ un $x - x_1$, $y_1 - y$ ir pozitīvi skaitļi. Ja izteic

$$(2) \qquad \begin{cases} x - x_1 = da \\ y_1 - y = db \end{cases}$$

ar lielāko kopīgo dalītāju d, tad $(a, b) = 1$. No vienlīdzībām (2) izteicam x un y un ievietojam formulā (1). Dabūjam rezultātu

$$(3) \qquad 2adx_1 + a^2d^2 = 2bdy_1 - b^2d^2.$$

---

*) Izteiksmes $x^2 + y^2$, $y^2 + x^2$, $(-x)^2 + y^2$, ... nav jāuzskata par dažādiem veidiem.

Formulas (3) kreisā puse dalās ar ad, labā puse ar bd. Tā kā $(a, b)=1$, tad formulas abas puses dalās ar abd. Ja katru no tām apzīmē ar skaitli $abd.c$, tad pēc pārveidojuma dabū formulas

$$2x_1 + ad = bc, \qquad 2y_1 - bd = ac$$

jeb

$$(4) \qquad \begin{cases} 2x_1 = bc - ad \\ 2y_1 = ac + bd \end{cases}$$

Ja formulas (4) kāpina kvadrātā, saskaita un izlieto identitāti

$$(ac + bd)^2 + (ad - bc)^2 = (a^2 + b^2)(c^2 + d^2),$$

tad dabū rezultātu

$$(a^2 + b^2)(c^2 + d^2) = 4p$$

un

$$(5) \qquad p = (a^2 + b^2) \cdot \frac{c^2 + d^2}{4}.$$

Tā kā

$$p = x^2 + y^2 = x_1^2 + y_1^2$$

ir nepāru skaitlis, tad vienam no skaitļiem x, y un vienam no x_1, y_1 jābūt pāru, otram nepāru skaitlim.

Pieņemsim, ka x un x_1 ir pāru, bet y un y_1 nepāru skaitļi. Tad no formulas (2) slēdzam, ka d ir pāru skaitlis. No formulas (4) seko, ka

$$bc \mid 2 \quad \text{un} \quad ac \mid 2.$$

Tā kā $(a, b) = 1$, tad nepieciešams, ka $c \mid 2$.

Tagad no formulas (5) redzam, ka

$$(c^2 + d^2) \mid 4.$$

Skaitlis p ir sadalīts divos faktoros, kas lielāki par vienu. Tiešām, no formulas (2) dabū, ka

$$a^2 + b^2 \geqslant 1^2 + 1^2.$$

Tā kā c un d ir pāru skaitļi, tad

$$c^2 + d^2 \geqslant 2^2 + 2^2.$$

Tā tad, ja skaitlis $p = 4n + 1$ ir izteicams vairākos veidos ar divu kvadrātu summu, tad p nav pirmskaitlis.

Ne katru skaitli N, kam ir forma $4n + 1$, var izteikt ar divu kvadrātu summu, Tas nav iespējams, piemēram, ar skaitļiem 21 un 33. Tādi gadījumi ir vienmēr tad, ja N ir salikts skaitlis, kas satur divus pirmreizinātājus ar formu $4n + 3$. Tiešām, divu tādu skaitļu reizinājums ir izsakāms formā $4n + 1$, jo

$$(4n_1 + 3)(4n_2 + 3) = 4 . (4n_1n_2 + 3n_1 + 3n_2 + 2) + 1 = 4n + 1.$$

Minētā pierādījuma metodi var izlietot skaitļa $N = 4n + 1$ sadalīšanai reizinātājos. Tam nolūkam no skaitļa N atņem pēc kārtas sekojošo dabisko skaitļu kvadrātus:

$$1^2 , 2^2, 3^2, \ldots, [E(\sqrt{N})]^2.$$

Ja rezultātā rodas kvadrāts vairākas reizes, vai arī nevienu reizi nerodas kvadrāts, tad N ir salikts skaitlis.

Piemērs. $N = 65 = 8^2 + 1^2 = 4^2 + 7^2$.

Te

$$x - x_1 = 4, \quad y_1 - y = 6, \quad d = 2, \quad a = 2, \quad b = 3, \quad a^2 + b^2 = 13.$$

Tādēļ

$$65 | 13$$

Piezīme. Minēto izmēģināšanu ar skaitļiem

$$N - i^2 \qquad [i = 1, 2, 3, \ldots, E(\sqrt{N})]$$

var stipri saīsināt, ja izvēlas kādu moduli m, kam ir kvadrātisks neatlikums k, un atmet visus tos skaitļus i, kam

$$N - i^2 \equiv k \pmod{m}.$$

Par tādu metodi jau bija runa § 38.

Par skaitļa $N = 4n + 1$ sadalīšanu faktoros Eulers savā darbā „*De numeris qui sunt aggregata duorum quadratorum*“ (*Nov. Comm. Acad. Petropolitanae, vol. 4. 1758. g.*) *Propositio 7, Corollarium 1* aizrāda uz šādu vienkāršu paņēmienu, kas pilnīgi saskan ar minēto faktoru aprēķināšanu.

Ja skaitlis N ir izteikts divos veidos ar divu kvadrātu summu

$$N = x^2 + y^2 = x_1^2 + y_1^2,$$

ta N var sadalīt reizinātājos, ja izlieto identitāti

$$(a^2+b^2)(c^2+d^2) = (ac+bd)^2 + (ad-bc)^2 = (ac-bd)^2 + (ad+bc)^2.$$

Tiešām, ja apzīmē

$$\begin{aligned} x &= ac + bd \\ y &= ad - bc \\ x_1 &= ac - bd \\ y_1 &= ad + bc, \end{aligned}$$

tad atrod, ka

$$x - x_1 = 2bd, \quad y_1 - y = 2bc.$$

Tā tad

$$\frac{c}{d} = \frac{y_1 - y}{x - x_1}.$$

Ja daļskaitli $\frac{y_1 - y}{x - x_1}$ saīsina, skaitītāju izvēlas par c un saucēju par d, tad var sastādīt skaitļa N vienu dalītāju $c^2 + d^2$.

Šo metodi Eulers paskaidro ar piemēru:

$$1000009 = 1000^2 + 3^2 = 235^2 + 972^2 = 293 \cdot 3413.$$

Jaukti uzdevumi.

1. Četru pēc kārtas sekojošu dabisko skaitļu reizinājums, palielināts par 1, ir kvadrāts.

2. Ja $(a+1)^2 > N > a^2$, tad $N - [(a+1)^2 - N][N - a^2]$ ir kvadrāts.

3. Ja p ir pirmskaitlis, tad

$$\frac{2^{p-1} - 1}{p}$$

ir kvadrāts tikai tad, ja $p = 3$ vai **7**.

4. Ja p un q ir pirmskaitļi, tad $p^{q-1}+q^{p-1}-1$ dalās ar pq.

5. Ja n ir pāru skaitlis, tad $2^{4n+2}+7^{2n+4}$ dalās ar 13; pretējā gadījumā nedalās.

6. Ja $p=16n+1$ ir pirmskaitlis, tad n^n+1 vai n^n-1 dalās ar p.

7. Ja $(a, b)=1$ un a^n+b^n dalās ar pirmskaitli p, tad $p=2nk+1$.

8. Ja skaitli p var izteikt ar divu kvadrātu starpību un tikai vienā veidā, tad p ir pirmskaitlis. Noskaidrot, kādus skaitļus nevar izteikt ar divu kvadrātu starpību.

9. Ja $p=Ax^2+By^2=Ax_1^2+By_1^2$, tad p nav pirmskaitlis.

10. Atrisināt nenoteiktos vienādojumus:

$$x^2-y^2=z^3 \quad \text{un} \quad x^2+y^2=z^n.$$

11. Pierādīt, ka pirmskaitļu $p=4n+1$ ir bezgala daudz. Aizrādījums: skaitlis $(2p_1 p_2 \ldots p_n)^2+1$ nedalās ne ar vienu pirmskaitli $q=4n+3$, jo $\left(\frac{-1}{q}\right)=-1$. Izlietojot izteiksmi $2p_1 p_2 \ldots p_n+1$, var pierādīt, ka pirmskaitļu $q=4n-1$ ir bezgala daudz.

12. Pierādīt, ka pirmskaitļu $p=an+1$ ir bezgala daudz.

13. Atrisināt nenoteiktos vienādojumus:

$$4x^2-12xy+9y^2+5x-7y-23=0;$$

$$9x^2+30xy+25y^2+7x+11y-222=0;$$

$$x^2-2xy+y^2+2x-5y+6=0.$$

14. Atrast kritēriju, kad kongruence $x \equiv a \pmod{2x+1}$ ir iespējama.

15. Pierādīt, ka katrs kvadrāts ir izteicāms ar vienu no trim sekojošām formām: $5n$, $5n-1$, $5n+1$, katrs kubs ar vienu no formām $7n$, $7n-1$, $7n+1$. Vispārināt teorēmu.

16 Pierādīt, ka vesela skaitļa 5 · pakāpe beidzas ar tādu pat ciparu, kā pats skaitlis

17. Ja p ir pirmskaitlis,

$$p-1=q_1^{a_1}q_2^{a_2}\ldots q_k^{a_k}$$

un neviena no kongruencēm

$$g^{\frac{p-1}{q_i}} = 1 \pmod{p} \qquad (i = 1, 2, \ldots, k)$$

nav iespējama, tad g ir moduļa p primitīva sakne.

18. Kāda veida pirmskaitļiem ir primitīva sakne $g = 10$?

19. Pierādīt, ka katrs pirmskaitlis, izņemot 2 un 5, dala, bezgala daudz skaitļos, kas uzrakstāmi tikai ar ciparu 9 vai tikai ar ciparu 1.

20. Pierādīt, ka -1 ir bikvadrātisks atlikums tikai tādiem pirmskaitļiem, kam ir forma $8n + 1$.

21. Ja p ir pirmskaitlis, tad visi pirmskaitļi, kas dala $2^p - 1$ ir formā $8np + 1$ vai $8np + 6p + 1$ (ja $p = 4k + 1$), vai $8np + 2p + 1$ (ja $p = 4k - 1$).

22. Rinda

$$0, 1, 1, 2, 3, 5, 8, 13, 21, \ldots \qquad \text{(Fibonači rinda)}$$

definēta ar formulu

$$a_n = a_{n-1} + a_{n-2} \qquad (a_0 = 0, \quad a_1 = 1).$$

Pierādīt sekošas īpašības.

1. Katram pāŗu skaitlim rindā seko divi nepāŗu skaitļi; katram nepāŗu skaitlim augstākais viens pāŗu skaitlis.

2. $a_0 + a_1 + a_2 + \ldots + a_{n-2} = a_n - 1.$

3. Kautkuŗa locekļa kvadrāts atšķiŗas no blakus stāvošo reizinājuma par 1, t. i. $a_n^2 = a_{n-1}\, a_{n+1} \pm 1$.

4. Attiecības $\frac{a_n}{a_{n+1}}$ robeža, kad $n \to \infty$, ir rēgulāra 10-stūŗa malas attiecība pret apvilkta riņķa radiju.

5. $$a_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right].$$

Otrā daļa.

Algebrisko skaitļu teōrija.

I. Dažas polinomu īpašības.

§ 49. Jēdziens par algebrisku skaitli.

Par algebriskās skaitļu teorijas sākumu ir jāuzskata Gausa ideja par komplekso skaitli $a + bi$, kur $i = \sqrt{-1}$ ir vienādojuma

$$x^2 + 1 = 0$$

sakne. Pēc Gausa parauga Kummers pētīja speciālus algebriskus skaitļus

$$\xi = a + b\omega + c\omega^2 + \ldots + k\omega^{n-1},$$

kur ω ir vienādojuma

$$x^n - 1 = 0$$

sakne. Ar šo skaitļu palīdzību Kummers pierādīja lielo Fermā teorēmu bezgala daudziem, bet tomēr ne visiem gadījumiem (sk. §§ 1., 2.).

Atzīmēsim vispārīga algebriska skaitļa **definīciju.** Par algebrisku skaitli α sauc tāda algebriska vienādojuma

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n = 0$$

sakni, kuŗa koeficienti $a_0, a_1, \ldots, a_n$ ir veseli racionāli skaitļi.

Turpmāk algebriskos skaitļus apzīmēsim grieķu burtiem, bet racionālos skaitļus (veselos vai daļskaitļus) ar latiņu burtiem.

No algebras ir zināms, ka vispārīgā gadījumā algebriska vienādojuma saknes var izteikt ar algebriskiem simboliem (radikāliem) atkarībā no vienādojuma koeficientiem tikai tad, ja vienādojuma pakāpe nav augstāka par 4. Tā tad ir algebriski

skaitļi, kas nav izsakāmi atklātā veidā ar algebriskiem simboliem.

Ilgu laiku matēmatikā valdīja uzskats, ka visi skaitļi ir algebriski skaitļi. Tikai 1851. g. Liuvils (*Liouville*) pierādīja, ka ir skaitļi, kas nevar noderēt par sakni nevienam algebriskam vienādojumam ar veseliem koeficientiem. Tos nosauc par **transcendentiem skaitļiem**. 1874. g. Kantors (*G. Cantor*) pierādīja, ka transcendento skaitļu ir bezgala daudz (sk. § 59.), un ar to deva sākumu **daudzumu teōrijai** (*Mengenlehre*). 1873. g. Ermīts (*Hermite*) pierādīja, ka skaitlis e (naturālo logaritmu baze) ir transcendents. 1882. g. par skaitli π to pašu pierādīja Lindemanis (*Lindemann*). Vēlāk šie pierādījumi sipri vienkāršoti*).

1900. g. matēmatiķu kongresā Parizē Hilberts, runājot par toreiz neatrisinātām problēmām matēmatikā**), starp citu min jautājumu, kā noskaidrot, vai dotais skaitlis, piem. $2^{\sqrt{2}}$, ir algebrisks vai transcendents? — 1930. g. Bīberbachs (*Bieberbach*) runājot par tagad neatrisinātām problēmām, rāda***), ka 1900. g. problēmas tagad gandrīz visas atrisinātas. $2^{\sqrt{2}}$ un tamlīdzīgu skaitļu transcendenci pierādījis krievu matēmatiķis Gelfonds.

§ 50. Algebriska skaitļa raksturigais vienādojums.

Algebriska skaitļa **definīciju** var modificēt sekojoši: algebrisks skaitlis ir tāda algebriska vienādojuma sakne, kuŗa koeficienti ir racionāli skaitļi.

Tiešām, ja vienādojumu pareizina ar visu koeficientu kopīgo saucēju, tad dabū vienādojumu, kam visi koeficienti ir veseļi skaitļi. Otrādi: ja vienādojuma

$$a_0x^n + a_1x^{n-1} + \ldots + a_n = 0$$

---

*) Sk. piem. *Landau „Vorlesungen über Zahlentheorie“*, Bd. III, lp. 90. Pierādījumu par skaitļa e transcendenci var atrast arī *Goursat „Cours d'analyse“* I. daļā.

**) *Nachrichten der Göttingen Gelehrtengesellschaft*, 1900.

***) *„Die Naturwissenschaften“* 1930. g. dec. burtnīcā.

abas puses izdala ar augstākā locekļa koeficientu a_0 un apzīmē

$$\frac{a_i}{a_0} = b_i \qquad (i = 1, 2, \ldots, n),$$

tad dabū vienādojumu

$$f(x) = x^n + b_1 x^{n-1} + b_2 x^{n-2} + \ldots + b_n = 0,$$

kam augstākā locekļa koeficients ir 1 un visi pārējie koeficienti $b_1, b_2, \ldots, b_n$ ir racionāli skaitļi. Tādu vienādojumu $f(x) = 0$ sauc par **vienkāršu vienādojumu.**

Ja polinomu $f(x)$ nevar sadalīt divos faktoros, kuŗu pakāpes $\geqslant 1$ un koeficienti ir racionāli skaitļi, tad $f(x)$ sauc par **irreducīblu polinomu. Vienādojumu** $f(x) = 0$ sauc par **irreducīblu** tad, ja polinoms $f(x)$ ir irreducībls.

Ja vienādojuma $f(x) = 0$ augstākā locekļa koeficients ir 1 un visi pārējie koeficienti veseli racionāli skaitļi, tad vienādojuma saknes sauc par **veseliem algebriskiem skaitļiem.**

Ja a ir n. pakāpes vienādojuma $f(x) = 0$ vienkārša sakne un $g(x)$ ir kautkāds polinoms, tad a ir sakne arī vienādojumam

$$f(x) \cdot g(x) = 0,$$

kam pakāpe $> n$. Tā tad vienmēr var atrast par $f(x) = 0$ augstākas pakāpes vienādojumus, kam a ir sakne. Bet ja nevar atrast nevienu zemākas pakāpes vienādojumu, kam a būtu sakne, tad a sauc par n. pakāpes algebrisku skaitli un $f(x)=0$ par a **raksturīgo** (karakteristisko) **vienādojumu.**

Definīcija. Viszemākās pakāpes vienkāršu vienādojumu, kam dotais algebriskais skaitlis a ir sakne, sauc par šī skaitļa raksturīgo vienādojumu.

Teorēma. Katram algebriskam skaitlim ir tikai viens raksturīgais vienādojums.

Ja pieņem, ka n. pakāpes algebriskam skaitlim a ir divi raksturīgie vienādojumi:

$$f(x) = 0 \quad \text{un} \quad g(x) = 0,$$

tad tie ir vienkārši vienādojumi, kuŗu pakāpēm jābūt vienlīdzīgām ar n. Var sastādīt vienādojumu

$$f(x) - g(x) = 0.$$

kam par sakni ir a. Ja saīsina ar tā augstākā locekļa koeficientu, tad dabū vienkāršu vienādojumu, k.m pakāpe $\leqslant n - 1$. Bet tā ir pretruna nosacījumam, ka a ir n. pakāpes algebrisks skaitlis.

No definīcijas seko, ka **raksturīgais vienādojums** $f(x) = 0$ **ir irreducībls vienādojums.**

Tiešām, ja a ir vienādojuma $f(x) = 0$ sakne, un polinoms $f(x)$ sadalās divos faktoros

$$f(x) = \varphi(x)\,\psi(x),$$

tad a ir arī sakne vismaz vienam no vienādojumiem

$$\varphi(x) = 0, \quad \psi(x) = 0,$$

kuŗu pakāpes zemākas kā $f(x)$ pakāpe.

Tagad pierādīsim, ka **algebriskā skaitļa** a **raksturīgais vienādojums** $f(x) = 0$ **ir vienīgais irreducīblais vienādojums ar sakni** a.

Pieņemsim, ka a apmierina bez raksturīgā vienādojuma

$$f(x) = 0$$

arī vēl kādu irreducīblu vienādojumu

$$F(x) = 0,$$

kuŗa pakāpei jābūt augstākai par $f(x)$ pakāpi n. Tad, $F(x)$ dalot ar $f(x)$, atlikumā dabū polinomu $r(x)$ ar racionāliem koeficientiem un pakāpi $\leqslant n - 1$. Sakarā

$$F(x) = f(x) \cdot q(x) + r(x),$$

liekot x vietā a dabū, ka

$$r(a) = 0.$$

Tā kā a ir n. pakāpes algebrisks skaitlis, bet $r(x)$ pakāpe $\leqslant n - 1$, tad nepieciešami, ka $r(x)$ visi koeficienti ir nulles. Tā tad

$$F(x) = f(x) \cdot q(x),$$

un teorēma pierādīta.

Iepriekšējos rezultātus apvienojot, var teikt, ka katram algebriskam skaitlim α ir raksturīgs viens irreducībls vienādojums, kas ir vienīgais irreducīblais vienādojums ar sakni α.

Piemērs. Atrast skaitļa $\alpha = \sqrt{2} + \sqrt{3}$ raksturīgo vienādojumu.

Ja vienādojumu

$$x - \alpha = 0 \quad \text{jeb} \quad x = \sqrt{2} + \sqrt{3}$$

kāpina kvadrātā, tad dabū vienādojumu

$$x^2 - 5 = 2\sqrt{6},$$

Vēlreiz kāpinot kvadrātā, dabū 4. pakāpes vienkāršu vienādojumu

$$f(x) = x^4 - 10x^2 + 1 = 0$$

ar racionāliem koeficientiem. Skaitlis α ir šī vienādojuma sakne. Ja pierādīsim, ka $f(x) = 0$ ir irreducībls vienādojums, tad tas būs arī α raksturīgais vienādojums.

Ja vienkāršs polinoms sadalās racionālu koeficientu faktoros, tad vienmēr var iekārtot tā, lai šie faktori būtu vienkārši polinomi. Tādēļ, ja

$$f(x) = x^4 - 10x^2 + 1$$

sadalās faktoros, tad $f(x)$ dalās ar kādu vienkāršu pirmās vai vienkāršu otrās pakāpes polinomu. Var pieņemt, ka I. gadījumā

$$f(x) = (x - a)(x^3 + bx^2 + cx + d)$$

un II. gadījumā

$$f(x) = (x^2 + Ax + B)(x^2 + Cx + D),$$

ja a, b, c, d un A, B, C, D ir racionāli skaitļi.

I. gadījums. Tā ka $f(x)$ dalās ar $x - a$, t. i. skaitlis a ir vienādojuma $f(x) = 0$ racionāla sakne. Bet algebrā zināma

teorēma*): ja vienkārša vienādojuma visi koeficienti ir veseli skaitļi un brīvais loceklis ir + 1 vai — 1, tad vienādojumam var būt racionālas saknes tikai +1 vai — 1. Bet dotā piemērā ne + 1, ne arī — 1 nav vienādojuma $f(x) = 0$ saknes.

II. gadījums. Ja pieņem

$$x^4 - 10x^2 + 1 = (x^2 + Ax + B)(x^2 + Cx + D)$$

un salīdzina abās pusēs koeficientus pie x vienādām pakāpēm, tad dabū sakarus

$$A + C = 0, \quad B + AC + D = -10, \quad AD + BC = 0, \quad BD = 1.$$

No divi pēdējām formulām izsledzot D rodas

$$A = -B^2C.$$

Ievērojot pirmo formulu, dabū

$$C(1 - B^2) = 0.$$

Tā tad

$$C = 0 \quad \text{vai} \quad B^2 = 1.$$

Kad $C = 0$, tad $A = 0$ un

$$\begin{cases} B + D = -10 \\ BD = 1. \end{cases}$$

Pēdējai sistēmai nav racionālu atrisinājumu.

Ja turpretim pieņem $B^2 = 1$, resp. $B = \pm 1$, tad arī $D = \pm 1$. Ar šīm nozīmēm dabū vai nu vienādojumu $A^2 = 12$, vai vienādojumu $A^2 = 8$. Bet ne pirmam, ne arī otram vienādojumam nav racionālu atrisinājumu.

Tā kā neviens no diviem vienīgi pieļaujamiem gadījumiem nav iespējams, tad

$$f(x) = x^4 - 10x^2 + 1$$

ir irreducībls polinoms, un $f(x) = 0$ ir skaitļa $a = \sqrt{2} + \sqrt{3}$ raksturīgais vienādojums.

*) Sk. piem., prof. Lejnieka — Augstākā algebra, lp. 145.

Turpmāk (§ 53) apskatīsim **vispārīgu metodi**, ar ko izšķir, vai dotais polinoms ir reducībls, vai irreducībls. Bet iepriekš apskatīsim dažas irreducīblu polinomu īpašības.

§ 51. Irreduciblu polinomu īpašibas.

Abela teorēma (1819. g.). Ja vienādojumam $F(x)=0$ der dotā irreducībla vienādojuma $f(x) = 0$ viena sakne, tad tam der arī $f(x) = 0$ visas saknes.

No algebras zinām: ja diviem vienādojumiem

$$F(x) = 0, \quad f(x) = 0$$

ir kopīga sakne, tad polinomiem $F(x)$ un $f(x)$ ir kopīgs dalītājs $d(x)$, kas ir vismaz pirmās pakāpes polinoms un kam koeficienti racionāli izsakāmi ar $F(x)$ un $f(x)$ koeficientiem. Ja $f(x) = 0$ ir irreducībls vienādojums, tad polinomam $f(x)$ nav citu dalītāju kā tikai pats polinoms $f(x)$ ko pēc patikas var vēl reizināt ar pastāvīgu skaitli. Tā tad $F(x)$ un $f(x)$ kopīgais dalītājs ir $f(x)$, un

$$F(x) = f(x)\ q(x).$$

Tādēļ vienādojuma $f(x) = 0$ visas saknes apmierina arī vienādojumu $F(x) = 0$.

Sekas 1. Irreducīblam vienādojumam nevar būt kopīgas saknes ne ar vienu zemākas pakāpes vienādojumu.

2. Nevienam irreducīblam vienādojumam nevar būt vairākkārtējas saknes.

Tiešām, ja irreducīblam n. pakāpes vienādojumam $f(x) = 0$ būtu vairākkārtēja sakne, tad tam arī būtu kopīga sakne ar $(n - 1)$. pakāpes vienādojumu $f'(x) = 0$, kur $f'(x)$ ir $f(x)$ atvasinātais polinoms.

3. Ja diviem irreducībliem vienādojumiem $f(x) = 0$, $g(x) = 0$ ir kopīga sakne a, tad abi vienādojumi ir identiski.

Pirmkārt, $f(x)$ un $g(x)$ pakāpēm jābūt vienlīdzīgām un, otrkārt, abu polinomu augstāko locekļu koeficientus var nolīdzināt.

Ja pēc tam arī visi pārējie $f(x)$ un $g(x)$ koeficienti nebūtu vienlīdzīgi, tad a apmierinātu zemākas pakāpes vienādojumu

$$f(x) - g(x) = 0.$$

4. Ja divu polinomu $F(x)$ un $G(x)$ reizinājums $F(x)\,G(x)$ dalās ar irreducīblu polinomu $f(x)$, tad vismaz viens no faktoriem $F(x)$ vai $G(x)$ dalās ar $f(x)$.

Ar pēdējo īpašību pierāda, ka katru polinomu var izteikt ar irreducīblu polinomu reizinājumu un tikai vienā veidā.

§ 52. Gausa teorēma.

Šinī un turpmākos §§ apskatīsim polinomu

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

kam visi koeficienti $a_0, a_1, \ldots, a_n$ ir veseli skaitļi. Par tāda polinoma dalītāja sauc skaitli

$$d = (a_0, a_1, \ldots, a_n),$$

kas ir visu koeficientu $a_0, a_1, \ldots, a_n$ lielākais kopīgais dalītājs. Šī definīcija ir saprotama, ievērojot, ka katrai veselai x nozīmei polinoma $F(x)$ vērtība dalās ar d.

Ja $d=(a_0,a_1,\ldots,a_n)=1$, tad $F(x)=a_0x^n+a_1x^{n-1}+\ldots+a_n$ sauc par **primitīvu polinomu.**

Teorēma. Ja $A(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$ un $B(x) = b_0x^m + b_1x^{m-1} + \ldots + b_m$ ir primitīvi polinomi, tad arī to reizinājums $C(x) = A(x) \cdot B(x)$ ir primitīvs polinoms.

Pierādījums. Tā kā polinomu $A(x)$ un $B(x)$ koeficienti ir veseli skaitļi, tad arī polinoma

$$C(x) = c_0x^{m+n} + c_1x^{m+n-1} + c_2x^{m+n-2} + \ldots + c_{m+n}$$

koeficienti „c“ ir veseli skaitļi. Tos izteic ar koeficientu „a“, „b“ homogenām un izobarām funkcijām:

$$c_0 = a_0 b_0$$
$$c_1 = a_0 b_1 + a_1 b_0$$
$$c_2 = a_0 b_2 + a_1 b_1 + a_2 b_0$$
$$\cdots\cdots\cdots$$
$$c_k = a_0 b_k + a_1 b_{k-1} + a_2 b_{k-2} + \ldots + a_k b_0 = \sum_{i=0}^{k} a_i b_{k-i},$$

kur visi a_i ar indeku $i > n$ un b_j ar $j > m$ ir nulles.

Pieņemsim, ka pretēji teorēmas apgalvojumam $C(x)$ visiem koeficientiem ir kopīgs dalītājs d. Tad ir pirmskaitlis p, kas dala visus polinoma $C(x)$ koeficientus. Ja $c_0 = a_0 b_0$ dalās ar p, tad vai nu a_0, vai b_0 dalās ar p. Pierādījumu nemaz nesašaurinot, var pieņemt, ka a_0 dalās ar p. Ir iespējams, ka arī $a_1, a_2, \ldots$ dalās ar p. Bet visi „a“ ar p nedalīsies, jo $A(x)$ ir primitīvs polinoms Pieņemsim, ka

$$a_0 | p, \quad a_1 | p, \quad a_2 | p, \ldots, a_{k-1} | p,$$

bet

$$a_k \text{ nedalās ar } p \qquad (k < n).$$

Tad ievērojot, ka $c_k | p$ un

$$c_k = a_0 b_k + a_1 b_{k-1} + \ldots + a_{k-1} b_1 + a_k b_0,$$

secinām, ka

$$a_k b_0 | p.$$

Tā kā a_k nedalās ar p, tad $b_0 | p$. Ja ievēro, ka $c_{k+1} | p$ un

$$c_{k+1} = a_0 b_{k+1} + a_1 b_k + \ldots a_{k-1} b_2 + a_k b_1 + a_{k+1} b_0,$$

tad seko, ka $a_k b_1 | p$, un reizē ar to $b_1 | p$. Tamlīdzīgā kārtā no pieņēmumiem

$$c_{k+2} | p, \quad c_{k+3} | p, \ldots, \quad c_{k+m} | p \qquad (k + m < m + n)$$

seko arī

$$b_2 | p, \quad b_3 | p, \ldots, \quad b_m | p.$$

Tā tad visi „b“ dalās ar p, un $B(x)$ nav primitīvs polinoms.

Sekas. Polinomu reizinājuma dalītājs ir vienlīdzīgs ar atsevišķo polinomu dalītāju reizinājumu.

Ja polinoma $A(x)$ dalītājs ir a un $B(x)$ dalītājs b, tad var izteikt

$$A(x) = a \cdot A_1(x), \quad B(x) = b \cdot B_1(x),$$

kur $A_1(x)$ un $B_1(x)$ ir primitīvi polinomi. Tad arī $A_1(x)$ un $B_1(x)$ reizinājums ir primitīvs polinoms. Tādēļ polinoma

$$A(x) \cdot B(x) = ab \cdot A_1(x)\, B_1(x)$$

dalītājs ir ab.

Gausa teorēma. Ja polinomu $F(x)=a_0x^n+a_1x^{n-1}+\ldots+a_n$ ar veseliem koeficientiem var sadalīt faktoros, kuŗu koeficienti ir racionāli skaitļi, tad $F(x)$ var sadalīt arī faktoros ar veseliem koeficientiem.

Pierādījums. Pieņemsim, ka $F(x)$ ir primitīvs polinoms, kas izteicāms ar divu polinomu produktu

$$F(x) = \varphi(x) \cdot \psi(x),$$

kur $\varphi(x)$ un $\psi(x)$ ir polinomi ar racionāliem koeficientiem. Ja a un b ir attiecīgi polinomu $\varphi(x)$ un $\psi(x)$ koeficientu kopīgie saucēji un $ab = c$, tad var rakstīt formulu

$$cF(x) = A(x) \cdot B(x),$$

kur

$$A(x) = a\,\varphi(x) \quad \text{un} \quad B(x) = b\,\psi(x)$$

ir polinomi ar veseliem koeficientiem. Pieņemot, ka polinomu $A(x)$ un $B(x)$ dalītāji ir attiecīgi a_1 un b_1, dabū sakaru

$$c\,F(x) = a_1b_1A_1(x)B_1(x),$$

kur $A_1(x)$, $B_1(x)$ un $F(x)$ ir primitīvi polinomi. Tādēļ

$$c = a_1b_1.$$

Formulu saīsinot, dabū

$$F(x) = A_1(x)\,B_1(x).$$

Tā tad gadījumā, kad $F(x)$ ir primitīvs polinoms, teorēma ir pierādīta.

Ja $F(x)$ nav primitīvs polinoms, tad var izteikt

$$F(x) = d\,F_1(x)$$

ar veselu skaitli d un primitīvu polinomu $F_1(x)$ Pēc tam pietiek atkārtot Gausa teorēmas pierādījumu par primitīvo polinomu $F_1(x)$.

Lai tagad noskaidrotu, vai dotais n. pakāpes polinoms $F(x)$ ir vai nav sadalāms faktoros, pietiek meklēt tikai tādus $F(x)$ faktorus, kuŗu koeficienti ir veseli skaitļi un pakāpes $\leqslant \frac{n}{2}$. Bet tādu polinomu liekas būt bezgala daudz. Metodi, ar ko $F(x)$ pieļaujamo dalītāju skaitu var ierobežot līdz galīgam skaitlim tā, ka šos dalītājus pārbaudot var izšķirt, vai dotais polinoms ir vai nav irreducībls, ir devis Kronekers 1881. g. To tagad apskatīsim.

§ 53. Kronekera (*Kronecker*) metode.

Pieņemam, ka n. pakāpes primitīvs polinoms $F(x)$ ir sadalāms faktoros:

$$F(x) = f(x) \cdot g(x).$$

Tad $f(x)$ un $g(x)$ ir polinomi ar veseliem koeficientiem, un vienam no tiem, piem. $f(x)$, ir pakāpe $r \leqslant \frac{n}{2}$. Liekam x vietā $r+1$ veselus un dažādus skaitļus

$$a_0,\ a_1,\ a_2,\ \ldots,\ a_r,$$

un pieņemam, ka šīm x nozīmēm $F(x) \neq 0$**). Tad

$$F(a_i) \quad \text{un} \quad f(a_i) \qquad (i = 0,\ 1,\ 2,\ \ldots,\ r)$$

---

*) *Kronecker* — „*Grundzüge einer arithmetischen Theorie der algebraischen Grössen*".

**) Ja tomēr kādai veselai nozīmei $x = a$ būtu $F(a) = 0$, tad $F(x)$ sadalītos reizinātājos $F(x) = (x - a)\,F_1(x)$, un apskatāmo jautājumu varētu attiecināt uz $(n-1)$. pakāpes polinomu $F_1(x)$.

ir veseli skaitļi, pie kam $F(a_i)$ dalās ar $f(a_i)$. Tā kā katram veselam skaitlim $F(a_i)$ ir tikai galīgs skaits dalītāju, tad funkcijas $f(x)$ vērtību $f(a_i)$ izvēle ir ierobežota. Ja

$$d_0, d_1, d_2, \ldots, d_r$$

ir viena no galīgā skaitā iespējamām veselu skaitļu sistēmām, kas sastādītas tā, ka

$$F(a_0)|d_0, \quad F(a_1)|d_1, \quad F(a_2)|d_2, \ldots, F(a_r)|d_r$$

tad polinoma $F(x)$ pieļaujamu dalītāju $f(x)$ konstruē ar Lagranža vai Ņūtona interpolācijas formulu*). Ja ar Lagranža formulu $f(x)$ izteic formā

$$f(x)=d_0\frac{(x-a_1)(x-a_2)\ldots(x-a_r)}{(a_0-a_1)(a_0-a_2)\ldots(a_0-a_r)}+d_1\frac{(x-a_0)(x-a_2)(x-a_3)\ldots(x-a_r)}{(a_1-a_0)(a_1-a_2)(a_1-a_3)\ldots(a_1-a_r)}+$$

$$+\ldots+d_r\frac{(x-a_0)(x-a_1)\ldots(x-a_{r-1})}{(a_r-a_0)(a_r-a_1)\ldots(a_r-a_{r-1})},$$

tad acīmredzams, ka

$$f(a_0)=d_0,\ f(a_1)=d_1,\ \ldots,\ f(a_r)=d_r.$$

Sakārtojot $f(x)$ pēc x dilstošām pakāpēm, vispārīgā gadījumā dabū r. pakāpes polinomu ar racionāliem koeficientiem. Gadījumā, kad $f(x)$ koeficienti ir veseli skaitļi, ir jāpārbauda, vai $F(x)$ dalās ar $f(x)$.

Ja tā nav, tad izvēlas citu skaitļu sistēmu

$$d_0, d_1, d_2, \ldots, d_r$$

un sastāda jaunu polinomu $f(x)$ Tāpat turpina līdz apskatīti visi iespējamie gadījumi. Ja $F(x)$ nedalās ne ar vienu no atrastajiem $f(x)$, tad dotajam polinomam $F(x)$ nav r. pakāpes dalītāju.

Apskatītais process jāatkārto ar visiem

$$r=1, 2, 3, \ldots, E\left(\frac{n}{2}\right).$$

---

*) Sk. prof. Lejnieka — Augstākā algebra. lp. 52.

Piemērs. Vai polinomam

$$F(x) = x^4 - 10x^2 + 1$$

ir otrās pakāpes dalītāji?

Izvēlamies $a_0 = -1$, $a_1 = 0$, $a_2 = 1$. Tā kā

$$F(-1) = -8, \quad F(0) = 1, \quad F(1) = -8$$

dalītāji ir attiecīgi

$-8, -4, -2, -1, 1, 2, 4, 8 \ldots$ (skaitā 8)
$-1, 1 \ldots\ldots\ldots\ldots\ldots\ldots$ („ 2)
$-8, -4, -2, -1, 1, 2, 4, 8 \ldots$ („ 8),

tad iespējamas pavisam $128 = 8 \cdot 2 \cdot 8$ dažādas skaitļu d_0, d_1, d_2 sistēmas un arī tikpat daudz dažādi pieļaujami $F(x)$ otrās pakāpes dalītāji $f(x)$, kas visi jāpārbauda. Ja ievēro, ka no visiem $128 = 8 \cdot 2 \cdot 8$ polinomiem $f(x)$ ik divi ir ar pretējām zīmēm, tad mēģinājumu skaitu var samazināt uz pusi. Ar vēl citiem paņēmieniem pārbaudāmo polinomu skaitu gan var vēl vairāk samazināt, tomēr atlikušo polinomu skaits nav mazs. Tādēļ praktikā Kronekera metode gaŗlaicīga.

Izvēlētām a_0, a_1, a_2 nozīmēm Lagranža formula dod

$$f(x) = d_0 \frac{x^2 - x}{2} + d_1 \frac{x^2 - 1}{-1} + d_2 \frac{x^2 + x}{2},$$

Ja liek, piem.

$$d_0 = 4, \quad d_1 = -1, \quad d_2 = -2,$$

tad dabū polinomu

$$f(x) = 2x^2 - 3x - 1,$$

bet $F(x)$ ar to nedalās. Tagad būtu jāņem citas d_0, d_1, d_2 nozīmes un jāsastāda jauns polinoms $f(x)$. Bet arī ar to $F(x)$ nedalīsies, jo jau 50. § noskaidrojām, ka $F(x)$ ir irreducibls polinoms.

§ 54. Eizenšteina (*Eisenstein*) teorēma.

Pierādīsim sekošu principiāli svarīgu **teorēmu**, ko devis Eizenšteins (*Eisenstein*) 1840. g.

Ja polinoma $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$ augstākā locekļa koeficients a_0 nedalās ar pirmskaitli p, visi pārējie koeficienti dalās ar p un brīvais loceklis a_n dalās ar p, bet nedalās ar p^2, tad polinoms $f(x)$ ir irreducībls.

Pieņemsim, ka $f(x)$ sadalās divos faktoros:

$$a_0x^n + a_1x^{n-1} + \ldots + a_n = (b_0x^r + b_1x^{r-1} + \ldots + b_r)(c_0x^s + c_1x^{s-1} + \ldots + c_s),$$

kuŗu koeficienti „b“ un „c“ (tāpat kā visi „a“) ir veseli skaitļi. Tad

$$r + s = n$$

un ir sekojošie sakari starp koeficientiem:

$$\begin{aligned}
a_0 &= b_0c_0 \\
a_1 &= b_0c_1 + b_1c_0 \\
&\ldots\ldots \\
a_{k+s} &= b_k c_s + b_{k+1}c_{s-1} + b_{k+2}c_{s-2} + \ldots + b_{k+s}c_0 \\
&\ldots\ldots \\
a_n &= b_r c_s .
\end{aligned}$$

Tā kā a_0 nedalās ar p, tad pirmā formula rāda, ka arī b_0 nedalās ar p. Ievērojot nosacījumu, ka $a_n = b_r c_s$ dalās ar p, bet nedalās ar p^2, apgalvojam, ka **viens no koeficientiem** b_r vai c_s ar p dalās, **otrs nedalās**. Pierādījumu nemaz nesašaurinot, pieņemam, ka c_s nedalās ar p un

$b_r, b_{r-1}, b_{r-2}, \ldots, b_{k+1}$ dalās ar p, bet b_k nedalās ar p $(k \geqslant 0)$.

Tad formulas

$$a_{k+s} = b_k c_s + b_{k+1}c_{s-1} + \ldots + b_{k+s}c_0$$

labajā pusē pirmais loceklis $b_k c_s$ ar p nedalās, bet visi pārējie locekļi dalās. Tādēļ arī summa a_{k+s} nedalās ar p, kas ir pretruna teorēmas nosacījumam.

Sekas. Eksistē ikkatras pakāpes bezgala daudz irreducīblu polinomu.

Tiešām, ar Eizenšteina teorēmu var konstruēt bezgala daudz irreducīblus n pakāpes polinomus. Ja p ir pirmskaitlis, tad, piem.

$$f(x) = x^n + px^{n-1} + px^{n-2} + \ldots + px + p$$

ir n. pakāpes irreducībls polinoms.

Uzdevumi.

1. Noteikt raksturīgos vienādojumus skaitļiem:

$$\sqrt[3]{3} + i\sqrt{2}; \quad \sqrt[3]{2} + \sqrt[3]{3}; \quad \sqrt{2} + \sqrt[4]{2}.$$

2. Sadalīt faktoros polinomus:

$x^4 + x^3 - 5x^2 + 2$
$2x^5 - x^4 + 4x^3 - 4x^2 + 5x - 2$
$2x^5 + 3x^4 + 3x^3 - 9x^2 + 12x - 6$
$6x^7 - 29x^6 + 58x^5 - 40x^4 - 57x^3 + 139x^2 - 111x + 36.$

3. Pierādīt, ka polinoms $x^{p-1} + x^{p-2} + x^{p-3} + \ldots + x + 1$ ir irreducībls, ja p pirmskaitlis.

4. Pierādīt teorēmu: ja veselais algebriskais skaitlis α ir racionāls, tad tas ir vesels racionāls skaitlis.

II. Algebrisko skaitļu pamatīpašibas.

§ 55. Algebriska skaitļa kritērijs.

Runājot par kritēriju, ar ko izšķirt, vai dotais skaitlis ir algebrisks vai transcendents, vispirms jāpiezīmē sekošais. Par otrās pakāpes algebrisku skaitli (irreducībla kvadrātvienādojuma sakni) Lagranžs ir devis šādu nepieciešamu un pietiekošu nosacījumu: katrs otrās pakāpes algebrisks skaitlis ir izteicams ar periodisku nepārtrauktu (ķēžu) daļskaitli.

Augstāku pakāpju algebriskiem skaitļiem tāda perioditāte nav novērota. Ar šo problēmu par trešās pakāpes algebriskiem skaitļiem ir nodarbojies Jakobi (*Jacobi*), vēlāk krievu autors Voronoi (Вороной) devis komplicētu kritēriju.

Mēs te apskatīsim vienu vispārīgu metodi, ar ko dažos teorētiskos jautājumos var pierādīt, ka dotais skaitlis α ir algebrisks. Pietiekošais nosacījums ir šāds: ja dotam skaitlim α var atrast k skaitļus $\xi_1, \xi_2, \ldots, \xi_k$ (kas visi reizē nav nulles) tā, ka ar racionāliem koeficientiem a_{ij} $(i, j = 1, 2, \ldots, k)$ pastāv sakari

$$(A)\qquad \begin{cases} \alpha\xi_1 = a_{11}\xi_1 + a_{12}\xi_2 + \ldots + a_{1k}\xi_k \\ \alpha\xi_2 = a_{21}\xi_1 + a_{22}\xi_2 + \ldots + a_{2k}\xi_k \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \alpha\xi_k = a_{k1}\xi_1 + a_{k2}\xi_2 + \ldots + a_{kk}\xi_k, \end{cases}$$

tad α ir algebrisks skaitlis ar pakāpi $\leqslant k$.

Tiešām, no formulām (A) seko k līneāru homogenu vienādojumu sistēma

$$\begin{cases} (a_{11} - \alpha)\xi_1 + a_{12}\xi_2 + \ldots + a_{1k}\xi_k = 0 \\ a_{21}\xi_1 + (a_{22} - \alpha)\xi_2 + \ldots + a_{2k}\xi_k = 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{k1}\xi_1 + a_{k2}\xi_2 + \ldots + (a_{kk} - \alpha)\xi_k = 0 \end{cases}$$

ar k nezināmiem $\xi_1, \xi_2, \ldots, \xi_k$, kas visi reizē nav nulles. Tādeļ sistēmas determinantam jābūt 0. To izteicot, dabū k. pakāpes vienādojumu

$$(B) \qquad \begin{vmatrix} a_{11} - a & a_{12} \ldots & a_{1k} \\ a_{21} & a_{22} - a \ldots & a_{2k} \\ \ldots\ldots\ldots\ldots\ldots & & \\ a_{k1} & a_{k2} \ldots & a_{kk} - a \end{vmatrix} = 0$$

ar racionāliem koeficientiem un nezināmo a. Tādēļ a ir algebrisks skaitlis. Atkarībā no tā, vai vienādojums (B) ir vai nav reducībls, a pakāpe ir mazāka vai vienlīdzīga ar k.

§ 56. Algebrisku skaitļu summa un reizinājums.

Ar tikko apskatīto teorēmu var pierādīt, ka algebrisku skaitļu summa, starpība, reizinājums uu dalījums arī ir algebriski skaitļi. Pirmo reizi šīs svarīgās īpašības ir pierādījis Dedekinds; viņa pierādījums vēlāk vienkāršots.

I. Divu algebrisku skaitļu summa ir algebrisks skaitlis.

Pieņemsim, ka α un β ir algebriski skaitļi, kas der vienādojumiem

$$(1) \qquad \alpha^n + a_1\alpha^{n-1} + a_2\alpha^{n-2} + \ldots + a_{n-1}\alpha + a_n = 0$$

un

$$(2) \qquad \beta^m + b_1\beta^{m-1} + b_2\beta^{m-2} + \ldots + b_{m-1}\beta + b_m = 0$$

ar racionāliem koeficientiem „a“ un „b“.

Par iepriekšējā § minētiem skaitļiem „ξ“ izvēlēsimies mn skaitļus

$$(3) \qquad \begin{cases} 1 & \alpha & \alpha^2 & \ldots & \alpha^{n-1} \\ \beta & \alpha\beta & \alpha^2\beta & \ldots & \alpha^{n-1}\beta \\ \beta^2 & \alpha\beta^2 & \alpha^2\beta^2 & \ldots & \alpha^{n-1}\beta^2 \\ \ldots\ldots\ldots\ldots\ldots\ldots & & & & \\ \beta^{m-1}, & \alpha\beta^{m-1}, & \alpha^2\beta^{m-1} & \ldots & \alpha^{n-1}\beta^{m-1} \end{cases}$$

jeb, īsi pierakstot, skaitļus

$$\alpha^i \beta^j, \qquad \begin{cases} i = 0, 1, 2, \ldots, n-1 \\ j = 0, 1, 2, \ldots, m-1. \end{cases}$$

Pierādīsim, ka tad summas

$$\sigma = \alpha + \beta$$

reizinājums ar katru „ξ" ir izsakāms ar $\xi_1, \xi_2, \ldots, \xi_{mn}$ līneāru homogenu funkciju, kuŗas koeficienti ir racionāli skaitļi.

Tiešām, **1. gadījumā, kad**

$$\xi = \alpha^i \beta^j \quad \text{ar} \quad i < n-1, \quad j < m-1,$$

tad skaitļi

$$\alpha^{i+1}\beta^j = \xi_r, \qquad \alpha^i \beta^{j+1} = \xi_s,$$

atrodas tabulā (3). Reizinājumu $\sigma\xi$ izteic

$$\sigma\xi = (\alpha + \beta)\,\alpha^i \beta^j = \alpha^{i+1}\beta^j + \alpha^i \beta^{j+1} = \xi_r + \xi_s$$

jeb

$$\sigma\xi = \xi_r + \xi_s.$$

Ja formulas labajai pusei vēl pievieno tabulas (3) pārējos elementus reizinātus ar 0, tad redzam, ka šinī gadījumā $\sigma\xi$ var izteikt ar $\xi_1, \xi_2, \ldots, \xi_{mn}$ līneāru homogenu funkciju, kuŗas koeficienti ir racionāli skaitļi (0 vai 1).

2. gadījumā, kad

$$\xi = a^i \beta^j \qquad \text{ar} \quad i = n-1, \quad j < m-1,$$

tad, ievērojot skaitļa α vienādojumu (1), izteic

$$\sigma\xi = \alpha^n \beta^j + \alpha^{n-1}\beta^{j+1}$$

ar

$$\sigma\xi = (-a_1\alpha^{n-1} - a_2\alpha^{n-2} - \ldots - a_n)\,\beta^j + \alpha^{n-1}\beta^{j+1}$$

jeb

$$\sigma\xi = -a_1\alpha^{n-1}\beta^j - a_2\alpha^{n-2}\beta^j - \ldots - a_n\beta^j + \alpha^{n-1}\beta^{j+1}.$$

Pēc šī pārveidojuma $\sigma\xi$ ir izteikts ar skaitļiem $\alpha^{n-1}\beta^j$, $\alpha^{n-2}\beta^j$, . . ., kas visi atrodas tabulā (3).

3. gadījumā, kad

$$i < n-1, \quad j = m-1 \quad \text{vai} \quad i = n-1, \quad j = m-1,$$

dara līdzīgu pārveidojumu, izlietojot vienādojumu (2).

Redzam, ka 55. § pietiekošais nosacījums ir izpildīts, un

$$\sigma = \alpha + \beta$$

ir algebrisks skaitlis.

II. Algebrisko skaitļu α un β reizinājums $\rho=\alpha\beta$ ir algebrisks skaitlis.

Pierādījumam izlietosim tos pašus skaitļus $\xi = \alpha^i \beta^j$, kas uzrakstīti tabulā (3).

Ja $i < n-1$, $j < m-1$, tad

$$\rho\xi = \alpha\beta \cdot \alpha^i \beta^j = \alpha^{i+1} \beta^{j+1}$$

jeb

$$\rho\xi = \xi_r,$$

kur $\xi_r = \alpha^{i+1} \beta^{j+1}$ ir viens no skaitļiem (3).

Ja viens vai abi nosacījumi

$$i < n-1, \quad j < m-1$$

nav izpildīti, tad izlieto tamlīdzīgus pārveidojumus, kā pierādījumā par algebrisku skaitļu summu.

Ja β ir algebrisks skaitlis, kas der vienādojumam

$$x^m + b_1 x^{m-1} + b_2 x^{m-2} + \ldots + b_m = 0$$

ar racionāliem koeficientiem, tad arī $-\beta$ un $\frac{1}{\beta}$ ir algebriski skaitļi, jo $-\beta$ der vienādojumam

$$x^m - b_1 x^{m-1} + b_2 x^{m-2} - \ldots + (-1)^m b_m = 0$$

un $\frac{1}{\beta}$ — vienādojumam

$$b_m x^m + b_{m-1} x^{m-1} + \ldots + b_1 x + 1 = 0.$$

Ar šo piezīmi ir saprotams, ka algebrisku skaitļu starpību un dalījumu var izteikt ar citu algebrisku skaitļu summu un reizinājumu

$$\alpha - \beta = \alpha + (-\beta), \qquad \frac{\alpha}{\beta} = \alpha \cdot \frac{1}{\beta}.$$

Tādēļ no pierādītajām īpašībām (I) un (II) seko, ka arī algebrisku skaitļu starpība un dalījums ir algebriski skaitļi.

Šīs īpašības vispārina ar **teorēmu**, ka algebrisku skaitļu katra racionāla funkcija arī ir algebrisks skaitlis.

§ 57. Veseli algebriski skaitļi.

Veselu algebrisku skaitli mēs definējam, kā tāda vienādojuma

$$f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_n = 0$$

sakni, kam augstākā locekļa koeficients $a_0 = 1$ un visi pārējie koeficienti ir veseli racionāli skaitļi. Izlietojot Gausa teorēmu, var pierādīt, ka vesela algebriska skaitļa raksturīgajam vienādojumam arī visi koeficienti ir veseli skaitļi un augstākā locekļa koeficients ir 1.

Teorēma. Veselu algebrisku skaitļu summa, starpība un reizinājums arī ir veseli algebriski skaitļi.

Tiešām, ja pieņem, ka α un β ir veseli algebriski skaitļi, un atkārto vārdu pa vārdam 56. § pierādījumu, tad vienādojumu (1) un (2) visi koeficienti $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_m$ ir veseli racionāli skaitļi, un katrs skaitlis $\sigma\xi_i$ ir izsakāms ar $\xi_1, \xi_2, \ldots, \xi_k$ ($k = mn$) līneāru homogenu funkciju

$$\sigma\xi_i = a_{i1}\xi_1 + a_{i2}\xi_2 + \ldots + a_{ik}\xi_k \qquad (i = 1, 2, \ldots, k)$$

ar veseliem racionāliem skaitļiem a_{ij}. Tādēļ skaitlis

$$\sigma = \alpha + \beta$$

apmierina 55. § vienādojumu

$$\begin{vmatrix} a_{11}-\sigma & a_{12} & \ldots & a_{1k} \\ a_{21} & a_{22}-\sigma & \ldots & a_{2k} \\ \ldots & \ldots & \ldots & \ldots \\ a_{k1} & a_{k2} & \ldots & a_{kk}-\sigma \end{vmatrix} = 0.$$

Ja to sakārto pēc σ dilstošām pakāpēm un reizina ar $(-1)^k$, tad dabū vienādojumu

$$\sigma^k + A_1\sigma^{k-1} + A_2\sigma^{k-2} + \ldots + A_k = 0,$$

kuŗa koeficienti $A_1, A_2, \ldots, A_k$ ir veseli racionāli skaitļi. Tādēļ σ ir vesels algebrisks skaitlis.

Tamlidzīgi pierāda, ka arī veselu algebrisku skaitļu starpība un reizinājums ir veseli algebriski skaitļi, bet par dalījumu to katrreiz nevar apgalvot

Ja α un β ir divi veseli algebriski skaitļi un var atrast trešo veselo algebrisko skaitli γ tā, ka

$$\alpha = \beta\gamma,$$

tad saka, ka α dalās ar β. Šinī gadījumā dalījums $\frac{\alpha}{\beta}$ ir vesels algebrisks skaitlis γ.

Ja 1 dalās ar algebrisku skaitli ε, t. i. ja reizē ar ε arī $\frac{1}{\varepsilon}$ ir vesels algebrisks skaitlis, tad ε sauc par algebrisku vienieku. Katrs algebriskais vienieks ir tāda vienādojuma

$$x^n + a_1x^{n-1} + \ldots + a_{n-1}x \pm 1 = 0,$$

sakne, kam galējie koeficienti ir $+1$ vai -1 un visi pārējie koeficienti veseli racionāli skaitļi.

Piemērs. Skaitļi

$$\varepsilon = \frac{1}{2}(-1 + i\sqrt{3}) \quad \text{un} \quad \eta = 2 - \sqrt{5}$$

ir algebriski vienieki, jo tie der attiecīgi vienādojumiem:

$$x^2 + x + 1 = 0, \quad x^2 - 4x - 1 = 0.$$

§ 58. Vispārigi algebriski vienādojumi.

Par **vispārīgu** algebrisku vienādojumu **sauksim** tādu, kuŗa koeficienti ir algebriski **skaitļi.**

Pierādīsim šādu ievērojamu **teorēmu.** Ja **algebriska** vienādojuma koeficienti ir algebriski **skaitļi,** tad arī vienādojuma saknes ir **algebriski** skaitļi.

Pierādījums. Dotā vienādojuma abas puses dalot ar augstākā locekļa koeficientu (kas nav nulle), dabū vienādojumu

$$x^N + \alpha x^{N-1} + \beta x^{N-2} + \ldots + \gamma = 0, \tag{4}$$

kur $\alpha, \beta, \ldots, \gamma$ ir algebriski skaitļi, kas der vienādojumiem:

$$\begin{aligned} &a^n + a_1 a^{n-1} + a_2 a^{n-2} + \ldots + a_n = 0 \\ &\beta^m + b_1 \beta^{m-1} + b_2 \beta^{m-2} + \ldots + b_m = 0 \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ &\gamma^s + c_1 \gamma^{s-1} + c_2 \gamma^{s-2} + \ldots + \gamma_s = 0 \end{aligned}$$

ar racionāliem koeficientiem $a_1, \ldots, b_1, \ldots, c_1, \ldots$ Lai izlietotu 55. § metodi, apzīmēsim ar x vienādojuma (4) sakni un sastādīsim $k = Nmm \ldots s$ skaitļus

$$\xi = x^h \alpha^i \beta^j \ldots \gamma^r, \qquad \begin{cases} h = 0, 1, 2, \ldots, N-1 \\ i = 0, 1, 2, \ldots, n-1 \\ j = 0, 1, 2, \ldots, m-1 \\ \ldots\ldots\ldots \\ r = 0, 1, 2, \ldots, s-1. \end{cases}$$

Pierādīsim, ka katrs reizinājums $x\xi$ ir izsakāms ar $\xi_1, \xi_2, \ldots, \xi_k$ līneāru homogenu funkciju ar racionāliem koeficientiem.

Tiešām, ja $h < N-1$, tad

$$x\xi = x^{h+1} \alpha^i \beta^j \ldots \gamma^r$$

ir viens no skaitļiem $\xi_1, \xi_2, \ldots, \xi_k$.

Ja turpretīm $h = N-1$, tad

$$x\xi = x^N \alpha^i \beta^j \ldots \gamma^r = (\alpha x^{N-1} - \beta x^{N-2} - \ldots \gamma)\, \alpha^i \beta^j \ldots \gamma^r$$

jeb

$$(5)\quad x\xi = -x^{N-1}\alpha^{i+1}\beta^j \ldots \gamma^r - x^{N-2}\alpha^i \beta^{j+1} \ldots \gamma^r - \ldots - \alpha^i \beta^j \ldots \gamma^{r+1}.$$

Pieņemot, ka ir izpildītas nevienlīdzības

$$i < n-1, \quad j < m-1, \ldots, r < s-1,$$

redzam, ka $x\xi$ ir izteikts ar $\xi_1, \xi_2, \ldots, \xi_k$ līneāru homogenu funkciju, kuŗas koeficienti ir 0 vai -1. Ja turpretīm dažas (vai visas) nevienlīdzības nav izpildītas, piem. $i = n-1$, tad, izlietojot skaitļa α vienādojumu, formulas (5) pirmo locekli pārveido par

$$-x^{N-1}\alpha^n \beta^j \ldots \gamma^r = x^{N-1}(a_1 \alpha^{n-1} + a_2 \alpha^{n-2} + \ldots + a_n)\, \beta^j \ldots \gamma^r =$$

$$= a_1 x^{N-1} \alpha^{n-1} \beta^j \ldots \gamma^r + a_2 x^{N-1} \alpha^{n-2} \beta^j \ldots \gamma^r + \ldots + a_n x^{N-1} \beta^j \ldots \gamma^r,$$

kur koeficienti $a_1, a_2, \ldots, a_n$ ir racionāli skaitļi.

Izdarot tamlīdzīgus pārveidojumus arī pārējos gadījumos, kad $j = m-1, \ldots, r = s-1$, pārliecināmies, ka 55. § nosacījums ir izpildīts. Tādēļ x ir algebrisks skaitlis ar pakāpi $\leqslant Nnm \ldots s$.

Gadījumā, kad $\alpha, \beta, \ldots, \gamma$ ir veseli algebriski skaitļi, tad koeficienti „$a, b, \ldots, c$“ ir veseli racionāli skaitļi, un no pierādījuma saprotams, ka x būs vesels algebrisks skaitlis. Tā tad, ja vienādojuma augstākā locekļa koeficients ir 1 un pārējie koeficienti ir veseli algebriski skaitļi, tad arī vienādojuma saknes ir veseli algebriski skaitļi.

§ 59. Kantora (Cantor) teorēmas.

Veselo algebrisko skaitļu teorija lielā mērā analoga veselo racionālo skaitļu teorijai. Grūtības sagādā tikai divas sekojošas atšķirības.

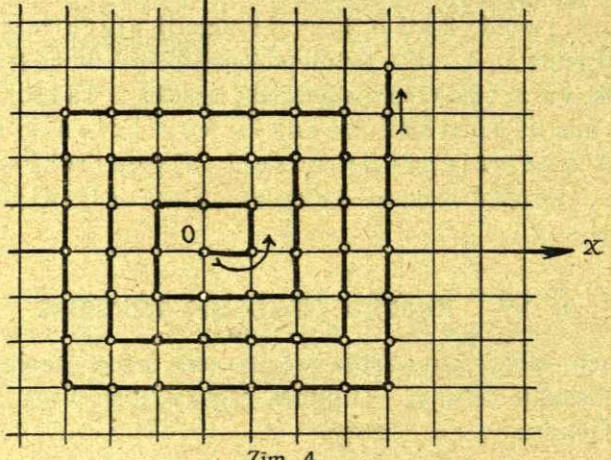
I. Veselo racionālu skaitļu teorijā ir tikai divi vienīnieki: $+1$ un -1, kamēr veselo algebrisko skaitļu teorijā vieninieku ir bezgala daudz.

II. Katrā galīgā intervallā atrodas galīgs skaits veselu racionālu skaitļu, bet veselu algebrisku skaitļu tur ir bezgala daudz. Tādēļ nevar pateikt, kuŗš ir dotā veselā algebriska skaitļa sekojošais skaitlis.

Tomēr daudzumu teōrijā ir metodes, kas katram algebriskam skaitlim viennozīmīgi piekārto veselu racionālu skaitli, un otrādi. Tā tad algebrisku skaitļu ir „tikpatdaudz" cik veselu racionālu skaitļu, jeb saka, ka algebrisko skaitļu daudzums ir sanumerējams (*abzählbar*) Saka arī, ka algebrisko un veselo racionālo skaitļu daudzumiem ir vienādas pakāpes (*Mächtigkeit*) jeb vienādi kardinālskaitļi.

1874. g. Kantors (*Cantor*) pierādīja, ka visu racionālo skaitļu daudzums ir sanumerējams.

To pierāda, uzrakstot rindā pēc augoša lieluma visus daļskaitļus, kam skaitītāja un saucēja summa ir 2, pēc tam visus daļskaitļus, kam šī summa ir 3, tad 4, u. t. t. Ja atmet daļskaitļus, kuŗu skaitītājam un saucējam ir kopīgs dalītājs, tad starp atlikušiem noteiktā vietā būs atrodams ikkatrs racionālais skaitlis un tikai vienreiz. Tādā veidā katram racionālam skaitlim būs piekārtots viens dabiskais skaitlis (vietas numers rindā), un otrādi.



Zīm. 4.

Arī visi veselu racionālu skaitļu pāŗi (a, b) ir sanumerējami. Ja izlieto koordinātu sistēmu (x, y), tad (a, b)

ir punkti ar veselām koordinātām. Tos sanumerē, ejot pa, 4. zīmējumā parādīto, spirālveidīgo lauzto līniju. No tā atsevišķā gadījumā seko, ka visu racionālo skaitļu $\frac{a}{b}$ daudzums ir sanumerējams.

Piemērs. Lai sanumerētu racionālos daļskaitļus intervallā (0, 1), raksta visus īstos nesaīsināmos daļskaitļus ar saucēju 2, tad ar saucēju 3 u. t. t.:

$$\frac{1}{2'}\ \frac{1}{3'}\ \frac{2}{3'}\ \frac{1}{4'}\ \frac{3}{4'}\ \frac{1}{5'}\ \frac{2}{5'}\ \frac{3}{5'}\ \frac{4}{5'}\ \ldots$$

1874. g. Kantors pierādīja, ka arī visu algebrisko skaitļu daudzums ir sanumerējams.

Ja

$$f(x) = a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_n = 0$$

ir vienādojums ar veseliem racionāliem koeficientiem, tad par vienādojuma augstumu h sauc skaitli

$$h = n - 1 + |a_0| + |a_1| + |a_2| + \ldots + |a_n|.$$

Ir tikai galīgs skaits vienādojumu ar dotu augstumu h; to pakāpes

$$N < h + 1.$$

Piemērs. Gadījumam ar $h = 4$ atbilst sekoši 24 vienādojumi:

$x^4 = 0$

$x^3 \pm 1 = 0,\quad 2x^3 = 0$

$x^2 \pm 2x = 0,\quad x^2 \pm 2 = 0,\quad x^2 \pm x + 1 = 0,\quad x^2 \pm x - 1 = 0,\quad 2x^2 \pm x = 0,$
$2x^2 \pm 1 = 0,\quad 3x^2 = 0$

$x \pm 3 = 0,\quad 2x \pm 2 = 0,\quad 3x \pm 1 = 0,\quad 4x = 0.$

Kantora teorēmas pierādījums. Ja uzraksta visus vienādojumus ar dotu augstumu h, tos atrisina un no saknēm patur (no katras pa vienai) tikai tās, kas nepieder nevienam vienādojumam ar zemāku augstumu h, tad saprotams, ka tādā kartā katram h atbilst galīgs skaits algebrisku skaitļu. Tos pēc kautkāda priekšraksta

var sakārtot rindā. Ja sāk ar $h = 1$ un turpina ar $h = 2, 3,$ u.t.t., tad dabū algebrisku skaitļu rindu, kuŗā atrodas katrs algebriskais skaitlis un tikai vienreiz. Pierakstot katram algebriskajam skaitlim tā vietas numeru rindā, dabū viennozīmīgu piekārtošanos starp algebriskiem skaitļiem un veseliem racionāliem skaitļiem. Tā tad visu algebrisko skaitļu daudzums ir sanumerējams.

Kā atsevišķs gadījums no pierādītā seko, ka arī visi reālie algebriskie skaitļi ir sanumerējami.

Ilgu laiku pastāvēja ieskats, ka visi reālie skaitļi ir algebriski skaitļi, vai, ka reālo skaitļu taisnes katrs punkts attēlo algebrisku skaitli. Tomēr tā nav, jo 1874. g. Kantors pierādīja, ka visi reālie skaitļi nav sanumerējami. Arī reālo skaitļu daudzums ikkatrā galīgā intervallā nav sanumerējams. Tā tad katrā intervallā eksistē bezgala daudz skaitļu, kas nav algebrisku vienādojumu saknes. Redzam, ka šī Kantora teorēma pierāda bezgala daudzu transcendentu skaitļu eksistenci, kaut arī nedod iespēju tos konstruēt.

Pierādīsim vispirms Kantora teorēmas atsevišķu gadījumu, ka visi reālie skaitļi intervallā (0, 1) nav sanumerējami.

Pieņemsim, ka ir metode, ar ko intervalla (0, 1) visus skaitļus var sanumurēt. Izteicot tos ar galīgiem vai bezgaligiem decimāldaļskaitļiem, var uzrakstīt tabulu:

$$x_1 = 0, a_1 b_1 c_1 d_1 \ldots$$
$$x_2 = 0, a_2 b_2 c_2 d_2 \ldots$$
$$x_3 = 0, a_3 b_3 c_3 d_3 \ldots$$
$$x_4 = 0, a_4 b_4 c_4 d_4 \ldots,$$
$$\ldots\ldots\ldots$$

kuŗā ikviens skaitlis $0 < x_k < 1$ atrodas pilnīgi noteiktā vietā ar vietas numeru k. Pierādīsim, ka, to pieņemot, atrod pretrunu.

Tiešām, ja konstruē skaitli

$$x = 0, a\,b\,c\,d \ldots,$$

kur cipari $a, b, c, d, \ldots$ izvēlēti tā, ka

$$a \neq a_1, \quad b \neq b_2, \quad c \neq c_3, \quad d \neq d_4, \ldots,$$

tad x gan ir intervalla (0, 1) skaitlis, bet neatrodas uzrakstītā tabulā. Tas tādēļ, ka x atšķiras no x_1 vismaz ar pirmo decimālzīmi, no x_2 vismaz ar otro decimālzīmi, no x_3 vizmaz ar trešo zīmi, u. t. t.

Šī pierādījuma metodi labi saprotama iemesla dēļ sauc par diagonālmetodi (*Diagonalverfahren*). Daudzos daudzumu teorijas jautājumos tā ļoti izdevīga.

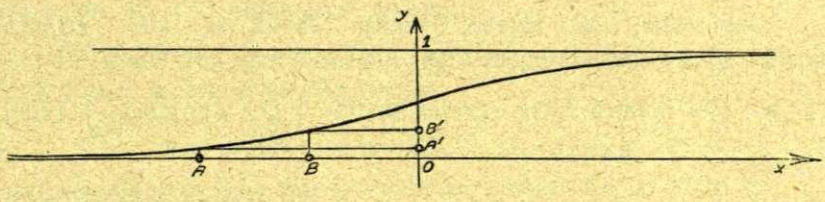
Pierādīto var izlietot teorēmas vispārīgam gadījumam. Sekojošā veidā katram reālam skaitlim var noteikt vienozīmīgi atbilstošu punktu intervallā (0, 1) vai nu ar ģeometrisku konstrukciju, vai analitisku transformāciju. Piemēram, transformācija

$$y = \frac{1}{2} + \frac{1}{\pi} \operatorname{arctg} x,$$

katram reālam x intervallā $(-\infty, +\infty)$ viennozīmīgi piekārto reālu y nozīmi, kas atrodas intervallā (0, 1). Tā tad punktu skaits šajos intervallos (un vispār ikkuŗos divos intervallos) ir vienlīdzīgs. Ir pierādīts, ka visi reālie skaitļi nav sanumerējami.

Visus skaitļus dotā intervallā sauc par kontinuumu. No pierādītā seko, ka kontinuums nav sanumerējams. Tā tad kontinuuma pakāpe ir augstāka par sanumerējama daudzuma pakāpi.

Piezīme. Pierādījumam lietotā transformācija attēlojas koordinātu sistēmā $(x\,y)$ ar sekojošo līkni (zīm. 5).



Zīm. 5.

III. Skaitļu lauki.

§ 60. Skaitļu lauka definīcija.

Definīcija. Par **skaitļa lauku** sauksim reālu vai kompleksu skaitļu sistēmu Ω ar tādu īpašību, ka katrs skaitlis, kas ar racionālām darbībām (saskaitīšanu, atņemšanu, reizināšanu un dalīšanu) ir sastādīts no sistēmas kaut kuŗiem diviem skaitļiem, arī ir tās pašas sistēmas skaitlis*).

Ja skaitļu laukam Ω pievieno kādu jaunu elementu ϑ, tad dabū ar ϑ paplašinātu lauku $\Omega(\vartheta)$. Gadījumā, kad ϑ jau ir Ω elements, tad $\Omega(\vartheta) = \Omega$.

Lauku, ko ar četrām racionālām darbībām sastāda, izlietojot tikai skaitli a, apzīmē ar

$$K(a).$$

Ja a ir algebrisks skaitlis, tad $K(a)$ ir algebrisku skaitļu lauks jeb īsi algebrisks lauks. Visus pārējos skaitļu laukus sauc par transcendentiem laukiem.

Speciālā gadījumā, kad $a = 1$, dabū absolūto racionalitātes lauku (jeb racionālo skaitļu lauku)

$$K(1),$$

kas satur visus racionālos skaitļus (un tikai tos).

Japiezīmē, ka ikkatrā skaitļu laukā Ω, kur atrodas skaitlis ω, atrodas arī lauks $K(\omega)$, ko sauc par lauka Ω dalītāju. Bet ikkātrā laukā atrodas skaitlis 1 $\left(\text{kā dalījums } \frac{\omega}{\omega}\right)$ Tādēļ

*) Dedekinds apzīmē par „*Zahlenkörper*“ un Kronekers — par „*Rationalitätsbereich.*“

racionālo skaitļu lauks $K(1)$ ir ikkatra skaitļu lauka sastāvdaļa.

Ja a ir racionāls skaitlis, tad

$$K(a) = K(1) = K$$

Piemēri. Skaitļu lauku noteic:

1. visi reālie skaitļi,
2. visi kompleksie skaitļi,
3. visi algebriskie skaitļi
4. Ja $F(x)$ ir racionāla funkcija ar racionāliem koeficientiem, un x ir kaut kāds (algebrisks vai transcendents) skaitlis, tad visi skaitļi, kas izteicāmi formā $F(x)$, sastāda skaitļu lauku.

Tiešām, ja $F(x)$ un $G(x)$ ir divas racionālas funkcijas ar racionāliem koeficientiem, tad arī

$$F(x) \pm G(x), \quad F(x) \cdot G(x) \quad \text{un} \quad \frac{F(x)}{G(x)}$$

ir tādas funkcijas.

Skaitļu lauku nenoteic:

1. visi veselie skaitļi,
2. visi pozitīvie skaitļi,
3. visi skaitļi $F(\tau)$, kur τ ir transcendents skaitlis un $F(x)$ polinoms ar racionāliem koeficientiem.

Tiešām, ja $F(x)$, $G(x)$, $H(x)$ ir polinomi ar racionāliem koeficientiem, un

$$\frac{F(\tau)}{G(\tau)} = H(\tau),$$

tad seko vienādojums

$$F(\tau) - G(\tau)\, H(\tau) = 0,$$

kas izteic, ka τ ir algebrisks skaitlis.

Turpmāk apskatīsim tikai algebriskus laukus $K(\alpha)$, kur α ir sakne vienādojumam

$$f(x) = x^n + a_1 x^{n-1} + \ldots + a_n = 0$$

ar racionāliem koefientiem $a_1, \ldots, a_n$.

§ 61. Lauka $K(a)$ skaitļu normālais veids.

Lemma. Ja $f(x)$ un $g(x)$ ir divi polinomi ar racionāliem koeficientiem, pie kam $f(x)$ ir reducībls un tā pakāpe n ir augstāka par $g(x)$ pakāpi k, tad vienmēr var atrast citus divus polinomus $A(x)$ un $B(x)$ ar racionāliem koeficientiem un racionālu skaitli $R \neq 0$ tā, ka pastāv identisks sakars

$$A(x) \cdot f(x) + B(x) \cdot g(x) = R.$$

Gadījumā, kad $g(x)$ ir pirmās pakāpes polinoms ($k = 1$), teorēmas pareizība viegli pierādāma. Tiešām, ja dala $f(x)$ ar

$$g(x) = ax + b,$$

tad dalījumā dabū polinomu $q(x)$ un atlikumā skaitli r, kas $\neq 0$, jo pretējā gadījumā $f(x)$ būtu reducībls polinoms. Sakars

$$f(x) - g(x)\, q(x) = r$$

izteic šim gadījumam teorēmu, ja liek

$$A(x) = 1, \quad B(x) = -q(x), \quad R = r.$$

Tagad pieņemsim, ka teorēma ir pareiza arī, kad $g(x)$ pakāpe ir $2, 3, \ldots k-1$. Pierādīsim, ka tad teorēma pareiza arī k. pakāpes polinomam $g(x)$.

Ja $f(x)$ dala ar $g(x)$, tad dalījumā dabū polinomu $q_1(x)$ un atlikumā polinomu $r_1(x)$ ar pakāpi $\leqslant k-1$. Šo polinomu koeficienti ir racionāli. Pastāv sakars

$$f(x) - q_1(x)\, g(x) = r_1(x).$$

Ievērojot, ka $r_1(x)$ pakāpe $\leqslant k-1$, pēc pieņēmuma var atrast polinomus $A_1(x)$, $B_1(x)$ ar racionāliem koeficientiem un racionālu skaitli $R \neq 0$, tā, ka

$$A_1(x)\, f(x) + B_1(x)\, r_1(x) = R.$$

Ja šai formulai pieskaita iepriekšējo, reizinātu ar $B_1(x)$, tad seko identitāte

$$[A_1(x) + B_1(x)]\, f(x) - q_1(x)\, B_1(x) \cdot g(x) = R$$

Ja apzīmē

$$A_1(x) + B_1(x) = A(x), \quad -q_1(x)\, B_1(x) = B(x),$$

tad teorēma ir pierādīta.

No algebriskā lauka $K(a)$ definīcijas seko, ka šī lauka katrs skaitlis ξ ir izsakāms ar a racionālu funkciju ar racionāliem koeficientiem. Tā tad

$$\xi = \frac{P(a)}{Q(a)},$$

kur $P(x)$ un $Q(x)$ ir polinomi ar racionāliem koeficientiem un $Q(a) \neq 0$. Ja tos dala ar skaitļa a raksturīgā vienādojuma polinomu

$$(1) \qquad f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_n,$$

tad dabū dalījumā polinomus $p_1(x)$, $q_1(x)$ un atlikumā $p(x)$, $q(x)$. Pastāv sakari

$$P(x) = p_1(x)\, f(x) + p(x)$$
$$Q(x) = q_1(x)\, f(x) + q(x),$$

kur polinomu $p(x)$ un $q(x)$ koeficienti ir racionāli (pie kam $q(x)$ visi koeficienti nav nulles) un pakāpes $\leqslant n - 1$. Liekot šajās formulās $x = a$ un ievērojot, ka $f(a) = 0$, dabū

$$P(a) = p(a), \quad Q(a) = q(a).$$

Tā tad

$$\xi = \frac{p(a)}{q(a)}.$$

Ja tagad attiecina iepriekšējo lemmu uz n. pakāpes irreducīblo polinomu $f(x)$ un zemākas pakāpes polinomu $q(x)$, tad atrod polinomus $A(x)$, $B(x)$ ar racionāliem koeficientiem un racionālu skaitli $R \neq 0$ tā, ka pastāv sakars

$$A(x) \cdot f(x) + B(x) \cdot q(x) = R.$$

Ja te liek $x = a$, tad dabū

$$B(a) \cdot q(a) = R$$

jeb

$$\frac{1}{q(a)} = \frac{B(a)}{R}.$$

Tādēļ

$$\xi = p(a) \cdot \frac{1}{q(a)} = \frac{1}{R} p(a)\ B(a).$$

Ja vēl polinomu $\frac{1}{R} p(x)\ B(x)$ dala ar $f(x)$, tad atlikumā dabū polinomu $r(x)$ ar racionāliem koeficientiem un pakāpi $\leqslant n - 1$, pie kam

$$\frac{1}{R} p(a)\, B(a) = r(a).$$

Tā tad ir pierādīts, ka skaitli ξ var attēlot ar a veselu racionālu funkciju

$$r(a) = c_0 + c_1 a + c_2 a^2 + \ldots + c_{n-1} a^{n-1}$$

ar racionāliem koeficientiem $c_0, c_1, \ldots, c_{n-1}$ un pakāpi $\leqslant n - 1$*).

Vēl pierādīsim, ka tāds attēlojums ir iespējams tikai vienā vienīgā veidā.

Tiešām, pieņemot, ka ir iespējami divi dažādi attēlojumi

$$\xi = c_0 + c_1 a + c_2 a^2 + \ldots + c_{n-1} a^{n-1}$$

un

$$\xi = d_0 + d_1 a + d_2 a^2 + \ldots + d_{n-1} a^{n-1}$$

ar racionāliem koeficientiem „c“ un „d“, secinam, ka n. pakāpes algebrisks skaitlis a der vienādojumam

$$(c_0 - d_0) + (c_1 - d_1)a + (c_2 - d_2)a^2 + \ldots + (c_{n-1} - d_{n-1})a^{n-1} = 0$$

ar pakāpi $\leqslant n - 1$. Bet tas iespējams tikai tad, ja šī vienādojuma visi koeficienti ir nulles, vai

*) Sk. arī prof. Lejnieka — Augstākā algebra, lpp. 77.

$$c_0 = d_0,\quad c_1 = d_1, \ldots, c_{n-1} = d_{n-1}.$$

Ar to ir pierādīta **teorēma**: algebriska lauka $K(a)$ katru skaitli ξ var viennozīmīgi izteikt normalā formā

$$(2)\qquad \xi = c_0 + c_1 a + c_2 a^2 + \ldots + c_{n-1} a^{n-1}$$

ar racionāliem koeficientiem $c_0, c_1, \ldots, c_{n-1}$.

Formulā (2) koeficientus $c_0, c_1, \ldots, c_{n-1}$ sauc par skaitļa ξ koordinātām. Ir skaidrs, ka lauka katram elementam atbilst n racionālas koordinātas, un katriem n racionāliem skaitļiem $(c_0, c_1, \ldots, c_{n-1})$ atbilst noteikts lauka elements ξ.

Piezīme. Ja ξ ir racionāls skaitlis c, tad tā koordinātas ir $(c, 0, 0, \ldots, 0)$.

Tiešām, ja

$$c = c_0 + c_1 a + c_2 a^2 + \ldots + c_{n-1} a^{n-1}$$

un pieņem, ka visi koeficienti $c_1, c_2, \ldots, c_{n-1}$ nav nulles, tad a der vienādojumam

$$c_{n-1} a^{n-1} + \ldots + c_1 a + (c_0 - c) = 0$$

ar racionāliem koeficientiem un pakāpi $\leqslant n - 1$. Te ir pretruna ar n. pakāpes algebriska skaitļa a definīciju.

§ 62. Lineāri atkarīgie elementi.

Definīcija. Ja dotiem n skaitļiem $\xi_1, \xi_2, \ldots, \xi_n$ var atrast n racionālus koeficientus $a_1, a_2, \ldots, a_n$, kas nav visi reizē nulles, tā, ka

$$a_1 \xi_1 + a_2 \xi_2 + \ldots + a_n \xi_n = 0,$$

tad dotos n skaitļus „ξ" sauc par lineāri atkarīgiem. Pretējā gadījumā, kad tādus koeficientus „a" nevar atrast, skaitļi „ξ" ir lineāri neatkarīgi.

Piemērs. Ja $\sqrt{m}$ nav racionāls skaitlis, tad skaitļi 1 un $\sqrt{m}$ ir lineāri neatkarīgi.

Tiešām, pieņemot, ka

$$a + b\sqrt{m} = 0$$

ar racionāliem a un $b \neq 0$, secinām, ka irracionāls skaitlis $\sqrt{m}$ vienlīdzīgs racionālam skaitlim $-\frac{a}{b}$.

Līdzīgā kārtā k homogenas funkcijas

$$f_i = a_{i1}x_1 + a_{i2}x_2 + \ldots + a_{in}x_n \qquad (i = 1, 2, \ldots, k)$$

ar racionāliem koeficientiem a_{ij} un n neatkarīgiem mainīgajiem $x_1, x_2, \ldots, x_n$ sauc par lineāri atkarīgām tad, ja ir atrodami k racionāli koeficienti $c_1, c_2, \ldots, c_k$, kas visi reizē nav nulles, tā, ka ikkuŗām $x_1, x_2, \ldots, x_n$ nozīmēm pastāv sakars

$$c_1f_1 + c_2f_2 + \ldots + c_kf_k = 0.$$

Pierādīsim, ka vairāk kā n lineāras funkcijas ar n mainīgajiem vienmēr ir lineāri atkarīgas.

Tiešām, ja funkcijas ($k \geqslant 1$):

$$\begin{aligned}
f_1 &= a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n \\
f_2 &= a_{21}x_1 + a_{22}x_1 + \ldots + a_{2n}x_n \\
&\ldots\ldots\ldots\ldots\ldots\ldots \\
f_{n+k} &= a_{n+k\,1}x_1 + a_{n+k\,2}x_2 + \ldots + a_{n+k\,n}x_n
\end{aligned}$$

reizina ar pagaidām nezināmiem skaitļiem $c_1, c_2, \ldots, c_{n+k}$ un prasa, lai

$$(3) \quad \begin{cases}
a_{11}c_1 + a_{21}c_2 + \ldots + a_{n+k\,1}c_{n+k} = 0 \\
a_{12}c_1 + a_{22}c_2 + \ldots + a_{n+k\,2}c_{n+k} = 0 \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
a_{1n}c_1 + a_{2n}c_2 + \ldots + a_{n+k\,n}c_{n+k} = 0,
\end{cases}$$

tad ikkatrām $x_1, x_2, \ldots, x_n$ nozīmēm izteiksme

$$c_1f_1+c_2f_2+\ldots+c_{n+k}f_{n+k}=x_1(a_{11}c_1+a_{21}c_2+\ldots+a_{n+k\,1}c_{n+k})+$$
$$+x_2(a_{12}c_1+a_{22}c_2+\ldots+a_{n+k\,2}c_{n+k})+\ldots+x_n(a_{1n}c_1+a_{2n}c_2+\ldots+a_{n+k\,n}c_{n+k})$$

ir vienlīdzīga nullei.

Sakarus (3) var uzskatīt par n līneāru homogenu vienādojumu sistēmu ar $n+k$ nezināmiem $c_1, c_2, \ldots, c_{n+k}$ un racionāliem koeficientiem a_{ij}. No algebras zināms, ka tādai sistēmai vienmēr eksistē racionāli atrisinājumi, kas visi reizē nav nulles*). Tā tad var atrast racionālus skaitļus $c_1, c_2, \ldots, c_{n+k}$ (kas visi nav nulles) tā, lai pastāvētu identisks sakars

$$c_1f_1+c_2f_2+\ldots+c_{n+k}f_{n+k}=0.$$

Tādēļ funkcijas $f_1, f_2, \ldots, f_{n+k}$ ir līneāri atkarīgas.

No pierādītā kā atsevišķs gadījums seko, ka $n+1$ homogenas līneāras funkcijas ar n mainīgiem vienmēr ir lineāri atkarīgas.

§ 63. Lauka $\mathfrak{K}(a)$ pakāpe.

Skaitļu lauka pakāpi nosaka lauka līneāri neatkarīgo elementu skaits.

Definicija. Ja starp lauka Ω visiem skaitļiem var atrast n līneāri neatkarīgus skaitļus, bet ikkatri $n+1$ skaitļi ir līneāri atkarīgi, tad lauka pakāpe ir n.

Teorēma I. Ja lauka Ω pakāpe n ir galīgs skaitlis, tad Ω visi elementi ir algebriski skaitļi ar pakāpēm $\leqslant n$.

Lauku Ω šinī gadījumā apzīmē par galīgu lauku.

Pierādījums. Reizē ar skaitli ξ laukā Ω atrodas arī skaitļi:

$$1, \xi, \xi^2, \xi^3, \ldots, \xi^n.$$

Tā kā lauka pakāpe ir n, tad šie $n+1$ skaitļi ir līneāri atkarīgi.

*) Sk. piem. prof. Lejnieka — Augstākā algebra, lp. 35.

Var atrast racionālus koeficientus $a_0, a_1, \ldots, a_n$ tā, lai pastāvētu sakars

$$a_0 \xi^n + a_1 \xi^{n-1} + \ldots + a_n = 0,$$

kas izteic, ka ξ ir algebrisks skaitlis ar pakāpi $\leqslant n$.

Tos lauka elementus, kuŗu pakāpe vienlīdzīga ar lauka pakāpi n, sauc par lauka primitīviem elementiem. Lauka visu pārējo elementu pakāpes ir zemākas ka n, un tos sauc par lauka neprimitīviem elementiem. Ja lauka visi elementi ir primitīvi, tad arī pašu lauku sauc par primitīvu. Tāds lauks ir, piemēram, visu racionālo skaitļu lauks $K(1)$.

Teorēma II. Ja α ir lauka Ω primitīvs elements, tad visu lauku var konstruēt ar skaitļa α racionālām funkcijām, un izteikt $\Omega = K(\alpha)$.

Pierādījums. Lauka Ω un skaitļa α pakāpes apzīmējam ar n. Reizē ar skaitli α laukā atrodas ikkatrs racionālais skaitlis un skaitļi

$$1, \alpha, \alpha^2, \ldots, \alpha^{n-1}.$$

Ja pieņemtu, ka pastāv n racionāli skaitļi $a_0, a_1, \ldots, a_{n-1}$, ar kuŗiem

$$a_0 \alpha^{n-1} + a_1 \alpha^{n-2} + \ldots + a_{n-1} = 0,$$

tad dabūtu pretrunu nosacījumam, ka α ir n. pakāpes algebrisks skaitlis. Tā tad lauka n skaitļi $1, \alpha, \ldots, \alpha^{n-1}$ ir līneāri neatkarīgi. Ja tiem pievieno lauka kaut kuŗu elementu ξ, tad dabū $n + 1$ elementus. Pēdējiem jābūt līneāri atkarīgiem (jo lauka pakāpe ir n). Tā tad pastāv racionāli koeficienti $b_0, b_1, \ldots, b_n$, ar kuŗiem

$$b_0 + b_1 \alpha + \ldots + b_{n-1} \alpha^{n-1} + b_n \xi = 0.$$

Tā kā $b_n \neq 0$ (jo pretējā gadījumā skaitļi $1, \alpha, \ldots, \alpha^{n-1}$ tomēr būtu līneāri atkarīgi), tad elementu

$$\xi = c_0 + c_1 \alpha + c_2 \alpha^2 + \ldots + c_{n-1} \alpha^{n-1}$$

var izteikt ar skaitļa α pakāpēm un racionāliem koeficientiem

$$c_i = -\frac{b_i}{b_n} \qquad (i = 0, 1, 2, \ldots, n-1).$$

Ar to teorēma pierādīta.

Teorēma III. Katrā galīgā skaitļu laukā Ω eksistē vismaz viens primitīvs elements.

Šis teorēmas pierādījums diezgan garš. Mēs to neapskatīsim. Pierādīsim **apgriezto teorēmu.**

Ja α ir n. pakāpes algebrisks skaitlis, tad arī lauks $K(\alpha)$ ir ar pakāpi n.

Tiešām, 61. § pierādījām, ka lauka $K(\alpha)$ katrs elements ξ_i ir izteicams formā

$$\xi_i = a_{i1}\, x_1 + a_{i2}\, x_2 + a_{i3}\, x_3 + \ldots + a_{in}\, x_n$$

ar racionāliem koeficientiem a_{ij} un

$$x_1 = 1, \quad x_2 = \alpha, \quad x_3 = \alpha^2, \ldots, x_n = \alpha^{n-1}.$$

Bet 62. § pierādījām, ka $n+1$ tādas formas funkcijas ξ_i vienmēr ir lineāri atkarīgas. Tā tad lauka $K(\alpha)$ ikkatri $n+1$ elementi ir lineāri atkarīgi, un lauka pakāpe nevar būt augstāka kā n.

Bet no otras puses lauka $K(\alpha)$ pakāpe arī nevar būt zemāka kā n, jo laukā atrodas n lineāri neatkarīgi skaitļi

$$1, \alpha, \alpha^2, \ldots, \alpha^{n-1}.$$

No tā seko, ka lauka pakāpe ir tieši n.

§ 64. Lauka $K(\alpha)$ elementu pakāpes.

Pierādīsim sekošu svarīgu **teorēmu.** Ja α ir n. pakāpes algebrisks skaitlis, tad lauks $K(\alpha)$ satur tikai tādus elementus, kuŗu pakāpes ir skaitļa n dalītāji.

Pieņemam, ka skaitļa α raksturīgais vienādojums ir

$$f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_n = 0.$$

Šī vienādojuma saknes ir skaitļi $\alpha_1 = \alpha, \ \alpha_2, \alpha_3, \ldots, \alpha_n$, ko sauc

par **saistītiem algebriskiem skaitļiem.** Tie ir visi dažādi, jo raksturīgajam vienādojumam $f(x) = 0$ nav vairākkārtēju sakņu (sk. §§ 50, 51).

Izvēlamies lauka $K(a_1)$ kautkuŗu skaitli β_1, un to izteicam formā

$$\beta_1 = c_0 + c_1 a_1 + c_2 a_1^2 + \ldots + c_{n-1} a_1^{n-1} = \psi(a_1),$$

ja

$$\psi(x) = c_0 + c_1 x + c_2 x^2 + \ldots + c_{n-1} x^{n-1}.$$

Uzrakstām n skaitļus:

$$\beta_1 = \psi(a_1), \quad \beta_2 = \psi(a_2), \ldots, \beta_n = \psi(a_n),$$

un sastādam vienādojumu

$$F(x) = (x-\beta_1)(x-\beta_2)\ldots(x-\beta_n) = x^n + A_1 x^{n-1} + A_2 x^{n-2} + \ldots + A_n = 0,$$

kam šie n skaitļi ir saknes. Tāda vienādojuma koeficienti:

$$A_1 = -(\beta_1 + \beta_2 + \ldots + \beta_n) = -[\psi(a_1) + \psi(a_2) + \ldots + \psi(a_n)]$$

$$A_2 = \beta_1\beta_2 + \beta_1\beta_3 + \ldots + \beta_{n-1}\beta_n = \psi(a_1)\psi(a_2) + \psi(a_1)\psi(a_3) + \ldots + \psi(a_{n-1})\psi(a_n)$$

. . . . . .

$$A_n = (-1)^n \beta_1 \beta_2 \ldots \beta_n = (-1)^n \psi(a_1)\psi(a_2)\ldots\psi(a_n)$$

ir sakņu $a_1, a_2, \ldots, a_n$ **simmetriskas funkcijas.** Tādēļ tās racionālā kārtā izsakamas ar vienādojuma $f(x) = 0$ koeficientiem, kas ir racionāli skaitļi. Tā tad arī **vienādojuma $F(x) = 0$ koeficienti ir racionāli.**

Pieņemsim, ka skaitļa β_1 raksturīgais vienādojums

$$\varphi(x) = 0$$

ir ar pakāpi h. Tad $\varphi(x)$ augstākā locekļa koeficientu var pieņemt par 1 un visus pārējos par racionāliem skaitļiem. Tā kā

$$\varphi(\beta_1) = 0 \quad \text{jeb} \quad \varphi[\psi(a_1)] = 0$$

un a_1 ir irreducibla vienādojuma $f(x) = 0$ sakne, tad vienādojumam

$$\varphi[\psi(x)] = 0$$

der visas irreducīblā vienādojuma saknes $\alpha_1, \alpha_2, \ldots, \alpha_n$. Tādēļ

$$\varphi(\beta_1) = 0, \quad \varphi(\beta_2) = 0, \ldots, \varphi(\beta_n) = 0.$$

Salīdzinot vienādojumus

$$F(x) = 0 \quad \text{un} \quad \varphi(x) = 0$$

ar racionāliem koeficientiem, atrodam sekošo. Vienādojums $\varphi(x) = 0$ ir irreducībls, un tam der vienādojuma $F(x) = 0$ visas saknes. Tādēļ polinoma $F(x)$ pakāpe n nav zemāka par $\varphi(x)$ pakāpi h, t. i. $n \geqslant h$. Tā kā $F(x)$ dalās ar $\varphi(x)$, tad var pieņemt

$$F(x) = [\varphi(x)]^q \cdot \omega(x),$$

kur veselais skaitlis $q \geqslant 1$ un $\omega(x)$ ir racionālu koeficientu polinoms, kas nedalās ar $\varphi(x)$.

Redzam, ka polinoms $\omega(x)$ top par nulli tikai tādām x nozīmēm, kam $F(x) = 0$. Tā tad vismaz vienam no skaitļiem $\beta_1, \beta_2, \ldots, \beta_n$, piem. $x = \beta_k$ ir $\omega(\beta_k) = 0$. Tā kā vienādojumam $\omega(x) = 0$ der irreducībla vienādojuma $\varphi(x) = 0$ viena sakne, tad līdz ar to der arī visas saknes (§ 51). No tā seko, ka polinoms $\omega(x)$ tomēr dalās ar $\varphi(x)$, bet tā ir pretruna pieņēmumam. Atliek tikai pieņemt, ka $\omega(x)$ ir konstante A, kam jābūt vienādai ar 1, jo $F(x)$ un $\varphi(x)$ augstāko locekļu koeficienti ir 1. Tad dabū formulu

$$F(x) = [\varphi(x)]^q.$$

Salīdzinot te polinomu pakāpes, redzam, ka

$$n = qh,$$

t. i. n dalās ar h. Tā tad lauka $K(\alpha_1)$ kaut kuŗa skaitļa β_1 pakāpe h ir skaitļa n dalītājs. Ar to teorēma pierādīta.

Piemērs. Ja α ir 6. pakāpes algebrisks skaitlis, tad lauks $K(\alpha)$ satur 1., 2., 3. un 6. pakāpes algebriskus skaitļus.

Sekas. Ja algebriska skaitļa α pakāpe ir pirmskaitlis p, tad lauka $K(\alpha)$ visi irracionālie skaitļi ir primitīvi elementi.

§ 65. Identiski skaitļu lauki.

Definīcija. Divus laukus $K(\alpha)$ un $K(\beta)$ sauc par identiskiem tad, ja visi pirmā lauka skaitļi atrodas arī otrajā un visi otrā lauka skaitļi pirmajā. Tad raksta

$$K(\alpha) = K(\beta).$$

Piemēri. 1. Pierādīsim, ka $K(\sqrt{2}) = K(1 - \sqrt{2})$.

Tiešām, lauka $K(\sqrt{2})$ katrs skaitlis ξ ir izsakāms formā

$$a + b\sqrt{2}$$

ar racionāliem skaitļiem a, b. Bet tā kā

$$a + b\sqrt{2} = (a + b) - b(1 - \sqrt{2}) = c + d(1 - \sqrt{2})$$

ar racionāliem skaitļiem

$$c = a + b \quad \text{un} \quad d = -b,$$

tad skaitlis ξ atrodas arī laukā $K(1 - \sqrt{2})$. Tāpat pierāda, ka arī lauka $K(1 - \sqrt{2})$ katrs skaitlis η atrodas laukā $K(\sqrt{2})$.

2. $$K(\sqrt{2}) \neq K(\sqrt{3}).$$

Ja pieņem pretējo, ka $K(\sqrt{2}) = K(\sqrt{3})$, tad skaitlis $\sqrt{2}$ atrastos laukā $K(\sqrt{3})$ un būtu izsakāms formā

$$\sqrt{2} = a + b\sqrt{3}$$

ar racionāliem skaitļiem a un b. Pieņemot, ka $a \neq 0$, $b \neq 0$, un kāpinot kvadrātā, dabū formulu

$$\sqrt{3} = \frac{2 - a^2 - 3b^2}{2ab}.$$

Te ir pretruna: irracionāls skaitlis $\sqrt{3}$ vienlīdzīgs racionālam

skaitlim $\frac{2 - a^2 - 3b^2}{2ab}$. Gadījumā, kad $a = 0$, resp. $b = 0$, tad seko pretruna:

$$\sqrt{\frac{2}{3}} = b, \quad \text{resp.} \quad \sqrt{2} = a.$$

Teorēma 1. Ja lauki $K(\alpha)$ un $K(\beta)$ ir identiski, tad nepieciešams, ka skaitļu α un β pakāpes ir vienlīdzīgas.

Ka šis nosacījums nav pietiekošs, ir jau redzams iepriekšējā piemērā ar laukiem $K(\sqrt{2})$ un $K(\sqrt{3})$.

Pierādījums. Ar teorēmas nosacījumu skaitlis β atrodas laukā $K(\alpha)$. Tādēļ β pakāpe m ir α pakāpes n dalītājs un

$$m \leqslant n.$$

Bet skaitlis α savukārt atrodas laukā $K(\beta)$. Tādēļ

$$n \leqslant m.$$

Salīdzinot ar iepriekšējo, secinām

$$m = n.$$

Lai dotu nepieciešamu un pietiekošu nosacījumu, kad lauki $K(\alpha)$ un $K(\beta)$ ir identiski, ir iepriekš jāpierāda sekoša **lemma.** Lai n. pakāpes lauka $K(\alpha)$ elementi

$$\xi_i = c_{i1} + c_{i2}\alpha + c_{i3}\alpha^2 + \ldots + c_{in}\alpha^{n-1} \qquad (i = 1, 2, \ldots, n)$$

būtu lineāri neatkarīgi, ir nepieciešami un pietiekoši, ka šo elementu koordinātu determinats

$$(4) \qquad \begin{vmatrix} c_{11} & c_{12} & \ldots & c_{1n} \\ c_{21} & c_{22} & \ldots & c_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ c_{n1} & c_{n2} & \ldots & c_{nn} \end{vmatrix}$$

nav vienlīdzīgs nullei.

P i e r ā d ī j u m s. Pieņemsim, ka $k_1, k_2, \ldots, k_n$ ir n racionāli skaitļi, ar kuŗiem

$$k_1\xi_1 + k_2\xi_2 + \ldots + k_n\xi_n = 0$$

jeb

$$(c_{11}k_1 + c_{21}k_2 + \ldots + c_{n1}k_n) + (c_{12}k_1 + c_{22}k_2 + \ldots + c_{n2}k_n)a + \ldots + (c_{1n}k_1 + c_{2n}k_2 + \ldots + c_{nn}k_n)a^{n-1} = 0.$$

Pēdējā formulā koeficientiem pie katras a pakāpes atsevišķi jābūt nullēm, jo pretējā gadījumā dabūtu, ka n. pakāpes algebrisks skaitlis a der vienādojumam ar racionāliem koeficientiem un pakāpi $\leqslant n - 1$, kas nav iespējams. Tādēļ liekam

$$\begin{cases} c_{11}k_1 + c_{21}k_2 + \ldots + c_{n1}k_n = 0 \\ c_{12}k_1 + c_{22}k_2 + \ldots + c_{n2}k_n = 0 \\ \cdots\cdots\cdots\cdots \\ c_{1n}k_1 + c_{2n}k_2 + \ldots + c_{nn}k_n = 0. \end{cases}$$

Ar to rodas n lineāro homogeno vienādojumu sistēma ar n nezināmiem $k_1, k_2, \ldots, k_n$. Ja sistēmas determinants

$$\Delta = \begin{vmatrix} c_{11}\, c_{21} \ldots c_{n1} \\ c_{12}\, c_{22} \ldots c_{n2} \\ \cdots\cdots \\ c_{1n}\, c_{2n} \ldots c_{nn} \end{vmatrix}$$

n a v n u l l e, tad visi n nezināmie $k_1, k_2, \ldots k_n$ ir vienlīdzīgi nullei. Tā tad skaitļi $\xi_1, \xi_2, \ldots, \xi_n$ ir lineāri neatkarīgi. Ja turpretim sistēmas determinants $\Delta = 0$, tad vienmēr eksistē racionālie atrisinājumi $k_1, k_2, \ldots k_n$, kas visi reizē nav nulles. Tad skaitļi $\xi_1, \xi_2, \ldots, \xi_n$ ir lineāri atkarīgi.

Tā kā determinants (4) atšķiras no Δ tikai ar to, ka rindas ir mainītas ar kolonnām, tad abi determinanti ir identiski, un teorēma pierādīta.

Tagad pierādīsim teorēmu, kas nosaka, kad divi lauki ir identiski.

Teorēma II. Ja α un β ir algebriski skaitļi ar vienlīdzīgām pakāpēm n un β atrodas laukā $K(\alpha)$

vai α atrodas laukā $K(\beta)$, tad abi lauki ir identiski, t. i. $K(\alpha) = K(\beta)$.

Pierādījums. Ja laukā $K(\alpha)$ atrodas skaitlis β, tad tur atrodas arī skaitļi $1, \beta, \beta^2, \ldots, \beta^{n-1}$. Pēdējie ir lineāri neatkarīgi, jo pretējā gadījumā būtu β pakāpe $\leqslant n-1$. Izsakot šos skaitļus ar to koordinātām laukā $K(\alpha)$, dabūjam:

$$(5)\quad \begin{cases} 1 = c_{11} + c_{12}\alpha + \ldots + c_{1n}\alpha^{n-1}{}^{*}) \\ \beta = c_{21} + c_{22}\alpha + \ldots + c_{2n}\alpha^{n-1} \\ \qquad \ldots\ldots\ldots \\ \beta^{n-1} = c_{n1} + c_{n2}\alpha + \ldots + c_{nn}\alpha^{n-1}. \end{cases}$$

No iepriekšējās lemmas ir zināms, ka koordinātu determinants nav nulle. Uzskatot skaitli α par nezināmu, to no sistēmas (5) var aprēķināt ar

$$\alpha = \frac{1}{\Delta}\begin{vmatrix} c_{11} & 1 & \ldots & c_{1n} \\ c_{21} & \beta & \ldots & c_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ c_{n1} & \beta^{n-1} & \ldots & c_{nn} \end{vmatrix}$$

un izteikt kā skaitļa β racionālu funkciju

$$(6)\qquad \alpha = d_0 + d_1\beta + d_2\beta^2 + \ldots + d_{n-1}\beta^{n-1}$$

ar racionāliem koeficientiem $d_0, d_1, \ldots, d_{n-1}$.

Izlietojot formulu (6) un skaitļa β raksturīgo vienādojumu

$$\beta^n + b_1\beta^{n-1} + b_2\beta^{n-2} + \ldots + b_n = 0,$$

lauka $K(\alpha)$ katru skaitli

$$\xi = c_0 + c_1\alpha + c_2\alpha^2 + \ldots + c_{n-1}\alpha^{n-1}$$

var izteikt formā

$$\xi = e_0 + e_1\beta + e_2\beta^2 + \ldots + e_{n-1}\beta^{n-1}$$

---

*) Te $c_{11} = 1$ un $c_{12} = c_{13} = \ldots = c_{1n} = 0$ (sk. § 61).

ar racionāliem koeficientiem $e_0, e_1, \ldots, e_{n-1}$. Tas liecina, ka lauka $K(\alpha)$ katrs skaitlis ξ atrodas arī laukā $K(\beta)$.

Ar formulām (5) pierāda, ka arī lauka $K(\beta)$ katrs skaitlis atrodas laukā $K(\alpha)$. Tā tad abi lauki ir identiski.

Sekas. Ja ξ ir lauka $K(\alpha)$ primitīvs elements, tad lauki $K(\alpha)$ un $K(\xi)$ ir identiski.

Pierādīsim, ka speciālā gadījumā arī lauki $K(\alpha)$ un $K(c\alpha)$ ir identiski (c — racionāls skaitlis).

Tiešām, ja skaitļa α raksturīgo vienādojumu

$$x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_n = 0$$

transformē ar

$$y = cx,$$

tad dabū skaitļa $c\alpha$ raksturīgo vienādojumu

$$y^n + a_1 c y^{n-1} + a_2 c^2 y^{n-2} + \ldots + a_n c^n = 0.$$

Ja pieņemtu, ka pēdējais vienādojums ir reducībls, tad sekotu, ka skaitlis $c\alpha$ apmierina kādu zemākas pakāpes vienādojumu

$$y^k + b_1 y^{k-1} + b_2 y^{k-2} + \ldots + b_k = 0$$

ar racionāliem koeficientiem un pakāpi $k < n$. Bet tad arī α apmierinātu zemākas pakāpes vienādojumu

$$c^k x^k + b_1 c^{k-1} x^{k-1} + \ldots + b_k = 0,$$

kas runā pretī nosacījumam, ka α ir n. pakāpes algebrisks skaitlis.

Tā kā $c\alpha$ ir lauka $K(\alpha)$ elements un tā pakāpe vienlīdzīga ar α pakāpi, tad lauki $K(\alpha)$ un $K(c\alpha)$ ir identiski.

Piemērs. $K(1) = K(n)$, ja n ir racionāls skaitlis.

Pēdējo īpašību izlieto lauku vienkāršošanai. Ja α ir algebrisks skaitlis, kuŗa raksturīgais vienādojums ir

$$a_0 x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_n = 0$$

ar veseliem koeficientiem $a_0, a_1, \ldots, a_n$, tad ar transformāciju

$$y = a_0 x$$

dabū vienādojumu

$$y^n + a_1 y^{n-1} + a_2 a_0 y^{n-2} + \ldots + a_n a_0^{n-1} = 0,$$

kam sakne ir vesels algebrisks skaitlis $a_0 a$. Tā kā lauki $K(a)$ un $K(a_0 a)$ ir identiski, tad, turpmāk runājot par algebrisku lauku $K(a)$, var aprobežoties ar gadījumu, kad a ir vesels algebrisks skaitlis.

§ 66. Saistītie lauki.

Algebriska skaitļa a_1 raksturīgā vienādojuma

$$x^n + a_1 x^{n-1} + \ldots + a_n = 0$$

n saknes $a_1, a_2, \ldots, a_n$ sauc par saistītiem algebriskiem skaitļiem. Ar šīm saknēm konstruētos laukus

$$K(a_1), \quad K(a_2), \ldots, K(a_n)$$

arī sauc par **saistītiem laukiem**.

Vispārīgā gadījumā saistītie lauki ir dažādi. Atsevišķā gadījumā, kad visi saistītie lauki ir identiski, tos sauc par **Galuā** (*Galois*) **laukiem** jeb normāliem laukiem.

Piemēri. 1. Lauks

$$K(i) \qquad (i = \sqrt{-1})$$

ir Galuā lauks, jo tas identisks ar savu saistīto lauku $K(-i)$.

2. Pierādīsim, ka lauki $K(x_1)$, $K(x_2)$, $K(x_3)$ nav identiski tad, ja x_1, x_2, x_3 ir vienādojuma

$$f(x) = x^3 + 2x + 2 = 0$$

saknes.

Ja vienādojums $f(x) = 0$ būtu reducibls, tad polinoms $f(x)$ dalītos ar kādu pirmās pakāpes faktoru $x - a$. Skaitlis a būtu vienādojuma racionāla sakne. Bet vienādojumam $f(x) = 0$ nav racionālu sakņu, jo neviens no brīvā locekļa 2 dalītājiem $-2, -1, 1, 2$ neder par sakni. Tā tad $f(x) = 0$ ir irredu-

cībls vienādojums. Tā saknes x_1, x_2, x_3 ir trešās pakāpes algebriski skaitļi. Viena no šīm saknēm, piem. x_1, ir reāls skaitlis, kas atrodas intervallā (0, — 1), jo $f(0)$ un $f(-1)$ zīmes ir pretējas. Ja pieņemtu, ka arī x_2 ir reāls skaitlis, tad pēc Rolla teorēmas intervallā (x_1, x_2) jāatrodas vienādojuma

$$f'(x) = 0$$

vismaz viena reāla sakne. Te

$$f'(x)=3x^2 + 2$$

ir $f(x)$ atvasinātais polinoms. Bet pēdējam vienādojumam $f'(x)=0$ nav reālas saknes.

Tā tad no vienādojuma $f(x) = 0$ trim saknēm x_1 ir reāls un x_2, x_3 saistīti kompleksi skaitļi. Tādēļ pats par sevi saprotams, ka

$$K(x_1) \neq K(x_2), \quad \text{un} \quad K(x_1) \neq K(x_3).$$

Pierādīsim, ka arī lauki $K(x_2)$ un $K(x_3)$ nav identiski. Izteiksim

$$x_2 = \alpha + \beta i, \qquad x_3 = \alpha - \beta i$$

ar reāliem skaitļiem α un β. Tā kā

$$x_1 + x_2 + x_3 = 0,$$

(jo dotā vienādojumā nav locekļa ar x^2), tad

$$x_1 + 2\alpha = 0.$$

Tā tad

$$\alpha = -\frac{x_1}{2}$$

ir irracionāls skaitlis, kas nav vienlīdzīgs nullei. Arī $\beta \neq 0$, jo pretējā gadījumā x_2, x_3 būtu reāli skaitļi.

Ja pieņemtu, ka $K(x_2) = K(x_3)$, tad ar racionāliem skaitļiem c_0, c_1, c_2 varētu izteikt

$$x_3 = c_0 + c_1 x_2 + c_2 x_2^2$$

jeb

$$\alpha - \beta i = c_0 + c_1(\alpha + \beta i) + c_2(\alpha + \beta i)^2.$$

Salīdzinot abās pusēs imāginārо daļu koeficientus, dabū

$$-\beta = c_1\beta + 2c_2\alpha\beta.$$

Izdalot abas puses ar $\beta \neq 0$, secinātu, ka gadījumā, kad $c_2 \neq 0$, α ir racionāls skaitlis

$$\alpha = -\frac{1 + c_1}{2c_2}.$$

Bet tas runā pretī iepriekšējam.

Gadījumā, kad $c_2 = 0$, tad $c_1 = -1$. Salīdzinot reālās daļas, dabūtu pretrunu:

$$\alpha = \frac{c_0}{2}.$$

Ar pēdējo piemēru pierāda, ka visi algebriskie lauki nav Galuā lauki.

Visiem algebriskiem laukiem ir raksturīga tā īpašība, ka identiskiem laukiem ir arī identiski saistītie lauki. Tas nozīmē, ka saistītie lauki ir raksturīgi pašam laukam $K(\alpha)$, bet ne tieši tam skaitlim α, ar ko lauks konstruēts. To pierāda ar sekošu **teorēmu.**

Ja lauki $K(\alpha)$ un $K(\beta)$ ir identiski, t. i. $K(\alpha)=K(\beta)$, tad arī $K(\alpha)$ saistītie lauki ir identiski ar $K(\beta)$ saistītiem laukiem, bet iespējams, ka citādā kārtībā.

Pierādījums. Pieņemsim, ka ar $\alpha = \alpha_1$ saistītie algebriskie skaitļi ir

$$\alpha_2, \ldots, \alpha_n.$$

Tā kā skaitlis β atrodas laukā $K(\alpha)$, tad var izteikt

$$\beta = c_0 + c_1\alpha + c_2\alpha^2 + \ldots + c_{n-1}\alpha^{n-1}$$

ar racionāliem koeficientiem $c_0, c_1, \ldots, c_{n-1}$. Uzrakstīsim ar β līdzīgus skaitļus

$$(7)\quad \begin{cases} \beta_1 = c_0 + c_1\alpha_1 + c_2\alpha_1^2 + \ldots + c_{n-1}\alpha_1^{n-1} \\ \beta_2 = c_0 + c_1\alpha_2 + c_2\alpha_2^2 + \ldots + c_{n-1}\alpha_2^{n-1} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \beta_n = c_0 + c_1\alpha_n + c_2\alpha_n^2 + \ldots + c_{n-1}\alpha_n^{n-1} \end{cases}$$

skaitā n, un sastādīsim vienādojumu

$$F(x)=(x-\beta_1)(x-\beta_2)\ldots(x-\beta_n)=x^n+B_1x^{n-1}+B_2x^{n-2}+\ldots+B_n=0$$

ar saknēm $\beta_1, \beta_2, \ldots, \beta_n$. Šī vienādojuma koeficienti $B_1, B_2, \ldots, B_n$, kā sakņu $\alpha_1, \alpha_2, \ldots, \alpha_n$ veselas simmetriskas funkcijas, ir racionāli skaitļi.

Pieņemsim, ka skaitļa β raksturīgais vienādojums ir

$$\varphi(x) = x^n + b_1x^{n-1} + b_2x^{n-2} + \ldots + b_n = 0.$$

Tā saknes ir saistītie skaitļi

$$\beta' = \beta, \beta'', \ldots, \beta^{(n)}.$$

Vienādojumam

$$F(x) = 0$$

der irreducībla vienādojuma

$$\varphi(x) = 0$$

viena sakne $\beta_1 = \beta$. Tādēļ der arī pārējās saknes (§ 51). Tas nozīmē, ka $F(x) = 0$ visas n saknes $\beta_1, \beta_2, \ldots, \beta_n$ sakrīt ar $\varphi(x) = 0$ saknēm $\beta', \beta'', \ldots, \beta^{(n)}$, bet iespējams, ka citādā kārtībā. Var likt, piemēram,

$$\beta_1 = \beta', \quad \beta_2 = \beta'', \ldots, \beta_n = \beta^{(n)}.$$

Tā kā visu „α" un „β" pakāpes ir vienlīdzīgas, tad formulas (7) rāda, ka attiecīgie lauki ir identiski:

$$K(\alpha_1) = K(\beta_1), \quad K(\alpha_2) = K(\beta_2), \ldots, K(\alpha_n) = K(\beta_n).$$

§ 67. Algebriska skaitļa diskriminants, norma un pēda.

Definīcija. Ja n. pakāpes algebriska skaitļa α saistītie skaitļi ir

$$\alpha_1 = \alpha, \quad \alpha_2, \ldots, \alpha_n$$

un lauka $K(\alpha)$ skaitlim

$$\beta = \varphi(\alpha) = c_0 + c_1\alpha + c_2\alpha^2 + \ldots + c_{n-1}\alpha^{n-1}$$

sastāda līdzīgos skaitļus

$$(7)\quad \begin{cases} \beta_1 = c_0 + c_1\alpha_1 + c_2\alpha_1^2 + \ldots + c_{n-1}\alpha_1^{n-1} \\ \beta_2 = c_0 + c_1\alpha_2 + c_2\alpha_2^2 + \ldots + c_{n-1}\alpha_2^{n-1} \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \beta_n = c_0 + c_1\alpha_n + c_2\alpha_n^2 + \ldots + c_{n-1}\alpha_n^{n-1}, \end{cases}$$

tad par skaitļa β diskriminantu $d(\beta)$ laukā $K(\alpha)$ sauc Vandermonda determinanta kvadrātu, t. i.

$$d(\beta) = \begin{vmatrix} 1 & 1 \ldots 1 \\ \beta_1 & \beta_2 \ldots \beta_n \\ \beta_1^2 & \beta_2^2 \ldots \beta_n^2 \\ \ldots & \ldots\ldots \\ \beta_1^{n-1} & \beta_2^{n-1} \ldots \beta_n^{n-1} \end{vmatrix}^2 = \prod_{\substack{1,\,n \\ i>j}} (\beta_i - \beta_j)^2.$$

Ja vienādojuma

$$(8)\qquad F(x) = x^n + B_1x^{n-1} + \ldots + B_n = 0$$

saknes ir $\beta_1, \beta_2, \ldots, \beta_n$, tad $d(\beta)$ ir arī polinoma $F(x)$ diskriminants, kas, kā vienādojuma sakņu vesela simmetriska funkcija, ir racionālā kārtā izsakāms ar vienādojuma $F(x) = 0$ koeficientiem. Tā tad $d(\beta)$ ir racionāls skaitlis, ko nosaka kā skaitlis β, tā arī lauks $K(\alpha)$.

Diskriminants $d(\beta)$ ir vesels skaitlis tad, kad β ir vesels algebrisks skaitlis (t. i. kad racionālie koeficienti $B_1, B_2, \ldots, B_n$ ir veseli skaitļi). Šis nosacījums ir pietiekošs, bet nav nepieciešams.

Piemērs. Gausa laukā $K(i)$ skaitlis

$$\beta_1 = a + bi \qquad (i = \sqrt{-1})$$

ar saistīto skaitli

$$\beta_2 = a - bi$$

nav veseli algebriski skaitļi, ja a nav vesels skaitlis, bet diskriminants

$$d(\beta) = \begin{vmatrix} 1 & 1 \\ a+bi & a-bi \end{vmatrix}^2 = (-2bi)^2 = -4b^2$$

nav atkarīgs no a un ir vesels skaitlis, ja b ir vesels.

Teorēma 1. Skaitļa β diskriminants $d(\beta)$ nav nulle tad un tikai tad, ja β ir lauka $K(\alpha)$ primitīvs elements.

Tiešām, ja β ir lauka $K(\alpha)$ primitīvs elements, tad β ir n. pakāpes algebrisks skaitlis, un

$$F(x) = 0$$

ir β raksturīgais vienādojums, kam visas saknes $\beta_1, \beta_2, \ldots, \beta_n$ ir dažādas. Šinī gadījumā β diskriminants

$$\prod_{i>j}^{1,n} (\beta_i - \beta_j)^2 \neq 0.$$

Ja β nav lauka $K(\alpha)$ primitīvs elements, tad, kā pierādīts 64 § $F(x)$ ir cita polinoma q. pakāpe ($q > 1$). Tādēļ vienādojumam $F(x) = 0$ ir vairākkārtējas saknes, un

$$\prod_{i>j}^{1,n} (\beta_i - \beta_j)^2 = 0.$$

Definīcija. Ja

$$\beta = \varphi(\alpha) = c_0 + c_1\alpha + c_2\alpha^2 + \ldots + c_{n-1}\alpha^{n-1}$$

ir lauka $K(\alpha)$ skaitlis un $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ ir algebriski saistīti skaitļi, tad skaitļa β **pēdu** $S(\beta)$ un **normu** $N(\beta)$ dēfinē ar formulām*):

$$S(\beta) = \beta_1 + \beta_2 + \ldots + \beta_n = \varphi(\alpha_1) + \varphi(\alpha_2) + \ldots + \varphi(\alpha_n)$$

un

$$N(\beta) = \beta_1 \beta_2 \ldots \beta_n = \varphi(\alpha_1)\,\varphi(\alpha_2) \ldots \varphi(\alpha_n).$$

Kā zināms,

$$S(\beta) = -B_1 \quad \text{un} \quad N(\beta) = (-1)^n B_n,$$

ja B_1, B_n ir vienādojuma (8) koeficienti. Tādēļ $S(\beta)$ un $N(\beta)$

*) Dedekinds šo funkciju ir nosaucis par „*Spur*"; latiņu autori lieto apzīmējumu $T(\beta)$ (*trace*). Normas jēdzienu ir ievedis Gauss kompleksiem skaitļiem $a + bi$, kuŗu norma ir moduļa kvadrāts.

ir racionāli skaitļi. Gadījumā, kad β ir vesels algebrisks skaitlis, tad β pēda un norma ir veseli racionāli skaitļi.

Ja a ir racionāls skaitlis, tad

$$N(a) = a^n,$$

jo a koordinātas ir $(a, 0, 0, \ldots, 0)$. Kā speciālu gadījumu vēl atzīmējam

$$N(1) = 1.$$

Teorēma II. $S(\beta+\gamma) = S(\beta) + S(\gamma)$, $N(\beta\gamma) = N(\beta) \cdot N(\gamma)$.

Pierādījums. Pieņemam, ka

$$\beta = c_0 + c_1\alpha + c_2\alpha^2 + \ldots + c_{n-1}\alpha^{n-1} = \varphi(\alpha)$$

un

$$\gamma = d_0 + d_1\alpha + d_2\alpha^2 + \ldots + d_{n-1}\alpha^{n-1} = \psi(\alpha).$$

Tad

$$\beta + \gamma = \varphi(\alpha) + \psi(\alpha) \quad \text{un} \quad \beta\gamma = \varphi(\alpha)\psi(\alpha).$$

Gadījumā, kad polinoma $\varphi(\alpha)\psi(\alpha)$ pakāpe ir augstāka par $n - 1$, tad, izlietojot skaitļa α raksturīgo vienādojumu

$$f(x) = x^n + a_1x^{n-1} + \ldots + a_n = 0,$$

to var samazināt līdz nozīmei $\leqslant n - 1$. Izlietojot definīciju, rakstām

$$S(\beta + \gamma) = \varphi(a_1) + \psi(a_1) + \varphi(a_2) + \psi(a_2) + \ldots + \varphi(a_n) + \psi(a_n)$$
$$= \varphi(a_1) + \varphi(a_2) + \ldots + \varphi(a_n) + \psi(a_1) + \psi(a_2) + \ldots + \psi(a_n)$$

jeb

$$S(\beta + \gamma) = S(\beta) + S(\gamma).$$

Līdzīgā kārtā

$$N(\beta\gamma) = \varphi(a_1)\psi(a_1) \cdot \varphi(a_2)\psi(a_2) \ldots \varphi(a_n)\psi(a_n)$$
$$= \varphi(a_1)\varphi(a_2) \ldots \varphi(a_n) \cdot \psi(a_1)\psi(a_2) \ldots \psi(a_n)$$

jeb

$$N(\beta\gamma) = N(\beta) \cdot N(\gamma).$$

Pierādīto teorēmu var vispārināt ikkatram algebrisku skaitļu $\beta, \gamma, \ldots, \mu$ galīgam skaitam sekojoši:

$$S(\beta + \gamma + \ldots + \mu) = S(\beta) + S(\gamma) + \ldots + S(\mu),$$

un

$$N(\beta\gamma \ldots \mu) = N(\beta) \cdot N(\gamma) \ldots N(\mu).$$

Sekas. Ja β dalās ar γ (tā tad β un γ ir veseli algebriski skaitļi), tad arī $N(\beta)$ dalās ar $N(\gamma)$.

Bet apgrieztā kārtā no normu $N(\beta)$, $N(\gamma)$ dalīšanās nevar secināt skaitļu β, γ dalīšanos (sk. piemēru 73. §).

Definīcija. Lauka veselu skaitli ε, kas dala lauka katru veselo skaitli, sauc par **lauka vieninieku.** Reālo skaitļu laukā $K(1)$ ir tikai divi vieninieki: $+1$ un -1.

Teorēma. Ja vesels skaitlis ε ir lauka vieninieks, tad ir nepieciešami un pietiekoši, ka norma $N(\varepsilon) = \pm 1$.

Tiešām, ja ε ir lauka vieninieks, tad arī skaitlis 1 dalās ar ε, t. i.

$$1 = \varepsilon . \delta,$$

kur δ ir lauka vesels skaitlis. No tā seko, ka

$$N(\varepsilon\delta) = N(1) \quad \text{jeb} \quad N(\varepsilon) . N(\delta) = 1.$$

Tā kā $N(\varepsilon)$ un $N(\delta)$ ir veseli racionāli skaitļi, tad katrs no tiem ir $+1$ vai -1.

Arī otrādi: ja ε ir lauka vesels skaitlis un $N(\varepsilon) = \pm 1$, tad

$$\varepsilon_1 \varepsilon_2 \ldots \varepsilon_n = \pm 1,$$

kur $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$ ir ar $\varepsilon_1 = \varepsilon$ līdzīgi saistīto lauku skaitļi (tie ir veseli algebriski skaitļi). Apzīmējot ar $\eta = \varepsilon_2 \ldots \varepsilon_n$ dotā lauka veselu skaitli, dabū sakaru

$$\varepsilon\eta = \pm 1,$$

kas norāda, ka 1 dalās ar ε. Tādēļ arī lauka katrs veselais skaitlis dalās ar ε, t. i. ε ir lauka vieninieks.

Sekas. Ja ε un η ir lauka $K(\alpha)$ vieninieki, tad arī

$\varepsilon\eta$, $\frac{\varepsilon}{\eta}$ un ε^k (k vesels pozitīvs vai negātīvs skaitlis)

ir lauka vieninieki.

Gadījumā, kad $K(\alpha)$ ir Galuā lauks, tad arī ar ϵ algebriski saistītie skaitļi ir lauka vienīnieki.

§ 68. Skaitļu sistēmas diskriminants.

Turpmāk runāsim par lauka $K(\alpha)$ skaitļiem

$$\xi_i = \varphi_i(\alpha) = c_{i1} + c_{i2}\alpha + c_{i3}\alpha^2 + \ldots + c_{in}\alpha^{n-1} \qquad (i = 1, 2, \ldots, n)$$

skaitā n, un ar tiem līdzīgus saistīto lauku skaitļus apzīmēsim ar

$$(9)\quad \begin{cases} \xi_i' = c_{i1} + c_{i2}\alpha_1 + c_{i3}\alpha_1^2 + \ldots + c_{in}\alpha_1^{n-1} = \xi_i \\ \xi_i'' = c_{i1} + c_{i2}\alpha_2 + c_{i3}\alpha_2^2 + \ldots + c_{in}\alpha_2^{n-1} \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ \xi_i^{(n)} = c_{i1} + c_{i2}\alpha_n + c_{i3}\alpha_n^2 + \ldots + c_{in}\alpha_n^{n-1}, \end{cases}$$

kur $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ ir α raksturīgā vienādojuma saknes.

Skaitļu sistēmas $\xi_1, \xi_2, \ldots, \xi_n$ **diskriminantu** $\Delta(\xi_1, \xi_2, \ldots, \xi_n)$ definē ar sekojošā determinanta kvadrātu:

$$\Delta(\xi_1, \xi_2, \ldots, \xi_n) = \begin{vmatrix} \xi_1' & \xi_2' & \ldots & \xi_n' \\ \xi_1'' & \xi_2'' & \ldots & \xi_n'' \\ \ldots & \ldots & \ldots & \ldots \\ \xi_1^{(n)} & \xi_2^{(n)} & \ldots & \xi_n^{(n)} \end{vmatrix}^2.$$

Ja izlieto determinantu reizināšanas likumu (kolonnas ar kolonnām), tad ar pārveidojumu

$$\Delta(\xi_1, \xi_2, \ldots, \xi_n) = \begin{vmatrix} \xi_1' & \xi_2' & \ldots & \xi_n' \\ \xi_1'' & \xi_2'' & \ldots & \xi_n'' \\ \ldots & \ldots & \ldots & \ldots \\ \xi_1^{(n)} & \xi_2^{(n)} & \ldots & \xi_n^{(n)} \end{vmatrix} \begin{vmatrix} \xi_1' & \xi_2' & \ldots & \xi_n' \\ \xi_1'' & \xi_2'' & \ldots & \xi_n'' \\ \ldots & \ldots & \ldots & \ldots \\ \xi_1^{(n)} & \xi_2^{(n)} & \ldots & \xi_n^{(n)} \end{vmatrix} = \begin{vmatrix} S(\xi_1^2) & S(\xi_1\xi_2) & \ldots & S(\xi_1\xi_n) \\ S(\xi_2\xi_1) & S(\xi_2^2) & \ldots & S(\xi_2\xi_n) \\ \ldots & \ldots & \ldots & \ldots \\ S(\xi_n\xi_1) & S(\xi_n\xi_2) & \ldots & S(\xi_n^2) \end{vmatrix}$$

(te $S(\xi)$ ir skaitļa ξ pēda) pierāda, ka sistēmas diskriminants $\Delta(\xi_1, \xi_2, \ldots, \xi_n)$ ir racionāls skaitlis. Gadījumā, kad $\xi_1, \xi_2, \ldots, \xi_n$ ir veseli algebriski skaitļi, Δ ir vesels racionāls skaitlis.

Teorēma. Ja β ir lauka $K(a)$ primitīvs elements (piem. $\beta = a$), tad

$$\Delta(1, \beta, \beta^2, \ldots, \beta^{n-1}) \neq 0.$$

Pierādījums. Ar $\beta_1, \beta_2, \ldots, \beta_n$ apzīmējot saistīto lauku līdzīgos skaitļus (kam tādas pat koordinātas kā skaitlim β), var pārveidot

$$\Delta(1, \beta, \beta, \ldots, \beta^{n-1}) = \begin{vmatrix} 1 & \beta_1 & \beta_1^2 & \ldots & \beta_1^{n-1} \\ 1 & \beta_2 & \beta_2^2 & \ldots & \beta_2^{n-1} \\ & \ldots & \ldots & \ldots & \\ 1 & \beta_n & \beta_n^2 & \ldots & \beta_n^{n-1} \end{vmatrix}^2 = \prod_{i>j}^{1,n} (\beta_i - \beta_j)^2.$$

Tā tad

$$\Delta(1, \beta, \beta^2, \ldots, \beta^{n-1}) = d(\beta),$$

kur $d(\beta)$ ir skaitļa β diskriminants, kas nav nulle, ja β ir primitīvs elements (§ 67).

Ja izsakam sistēmas diskriminantu $\Delta(\xi_1, \xi_2, \ldots, \xi_n)$ ar skaitļu „ξ" koordinātām c_{ij} (9), tad redzam, ka rezultāts uzrakstāms ar divu determinantu kvadrātu produktu

$$\Delta(\xi_1\, \xi_2, \ldots, \xi_n) = \begin{vmatrix} c_{11} & c_{12} & \ldots & c_{1n} \\ c_{21} & c_{22} & \ldots & c_{2n} \\ & \ldots & \ldots & \\ c_{n1} & c_{n2} & \ldots & c_{nn} \end{vmatrix}^2 \begin{vmatrix} 1 & a_1 & a_1^2 & \ldots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \ldots & a_2^{n-1} \\ & \ldots & \ldots & \ldots & \\ 1 & a_n & a_n^2 & \ldots & a_n^{n-1} \end{vmatrix}^2.$$

Tā tad

$$\Delta(\xi_1, \xi_2, \ldots, \xi_n) = C^2 \cdot d(a) \tag{10}$$

var izteikt ar elementu $\xi_1, \xi_2, \ldots, \xi_n$ koordinātu determinantu

$$C = \|c_{ij}\| \qquad (i, j = 1, 2, \ldots, n),$$

kas ir nulle tikai tad, ja $\xi_1, \xi_2, \ldots, \xi_n$ ir līnearī atkarīgi (§ 65), un ar skaitļa a diskriminantu $d(a)$, kas nav nulle, jo a ir lauka primitīvs elements.

Ar to ir pierādīts, ka sistēmas diskriminants $\Delta(\xi_1, \xi_2, \ldots, \xi_n)$ ir nulle tikai tad, ja sistēmas elementi ir līnearī atkarīgi, un otrādi: ja $\Delta(\xi_1, \xi_2, \ldots, \xi_n) = 0$, tad skaitļi $\xi_1, \xi_2, \ldots, \xi_n$ ir līnearī atkarīgi.

Bez tam formula (10) norāda, ka lauka $K(\alpha)$ līnēāri neatkarīgu skaitļu sistēmas diskriminanta zīme (+ vai —) saskan ar $d(\alpha)$ zīmi, jo C^2 kā pozitīvs lielums zīmi nemaina. Tā tad dotā laukā $K(\alpha)$ visu līnēāri neatkarīgu skaitļu sistēmu diskriminanti ir ar vienādām zīmēm. Tie visi ir pozitīvi, ja

$$d(\alpha) > 0,$$

un negātīvi, ja

$$d(\alpha) < 0.$$

§ 69. Lauka baze.

Definīcija. Ikvienu algebriska lauka skaitļu sistēmu ar diskriminantu $\Delta \neq 0$ sauc par lauka bazi.

Par n. pakāpes algebriska lauka $K(\alpha)$ bazi var izvēlēties lauka kaut kuŗus n līnēāri neatkarīgus skaitļus, piem.

$$1, \alpha, \alpha^2, \ldots, \alpha^{n-1},$$

kam, saprotams, $\Delta \neq 0$.

Bezgala daudz citas bazes noteic ar skaitļiem

$$\xi_i = c_{i1} + c_{i2}\alpha + c_{i3}\alpha^2 + \ldots + c_{in}\alpha^{n-1} \quad (i = 1, 2, \ldots, n),$$

kas izvēlēti tā, lai to koordinātu determinants

$$\| c_{ij} \| \qquad (i, j = 1, 2, \ldots, n)$$

nebūtu nulle. Tādu c_{ij} izvēle ir iespējama bezgala daudz veidos.

Teorēma. Lauka $K(\alpha)$ katru skaitli β var izteikt ar kaut kuŗas bazes $\xi_1, \xi_2, \ldots, \xi_n$ elementu līnēāru kombināciju

$$(11) \qquad \beta = c_1\xi_1 + c_2\xi_2 + \ldots + c_n\xi_n$$

ar racionāliem koeficientiem $c_1, c_2, \ldots, c_n$.

Ja speciālā gadījumā par bazi izvēlas skaitļus $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$, tad teorēmas pareizība ir pierādīta jau 61. §.

Vispārīgā gadījumā, kad baze $\xi_1, \xi_2, \ldots, \xi_n$, tad

n. pakāpes algebriskā lauka $n+1$ skaitļi $\xi_1, \xi_2, \ldots, \xi_n, \beta$ ir lineāri atkarīgi. Var atrast racionālus koeficientus $b_1, b_2, \ldots, b_{n+1}$ tā, ka

$$b_1\xi_1 + b_2\xi_2 + \ldots + b_n\xi_n + b_{n+1}\beta = 0.$$

Šeit

$$b_{n+1} \neq 0,$$

jo pretējā gadījumā, kad $b_{n+1} = 0$, bazes elementi $\xi_1, \xi_2, \ldots, \xi_n$ būtu lineāri atkarīgi, kas nav iespējams. Tādēļ, dalot ar b_{n+1} un apzīmējot

$$-\frac{b_k}{b_{n+1}} = c_k,$$

dabū tieši formulu (11).

To pašu var pierādīt arī citādi sekojošā veidā. Tā kā $\xi_1, \xi_2, \ldots, \xi_n$ un β ir lauka $K(a)$ elementi, tad tos var izteikt ar $1, a, a^2, \ldots, a^{n-1}$ un racionāliem koeficientiem. No sistēmas

$$\begin{cases} \xi_1 = c_{11} + c_{12}a + c_{13}a^2 + \ldots + c_{1n}a^{n-1} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \xi_n = c_{n1} + c_{n2}a + c_{n3}a^2 + \ldots + c_{nn}a^{n-1}, \end{cases}$$

kuŗas determinants $\|c_{ij}\| \neq 0$, izteic $1, a, a^2, \ldots, a^{n-1}$, kā $\xi_1, \xi_2, \ldots, \xi_n$ lineāras funkcijas ar racionāliem koeficientiem. Ja dabūtās izteiksmes liek formulā

$$\beta = b_0 + b_1a + b_2a^2 + \ldots + b_{n-1}a^{n-1},$$

kur $b_0, b_1, \ldots, b_{n-1}$ ir racionāli skaitļi, tad izteic

$$\beta = c_1\xi_1 + c_2\xi_2 + \ldots + c_n\xi_n.$$

Ar to teorēma pierādīta.

Racionālos koeficientus $c_1, c_2, \ldots, c_n$ sauc par skaitļa β koordinātām attiecībā pret bazi $\xi_1, \xi_2, \ldots, \xi_n$.

Tagad noskaidrosim, kā ar lauka vienas bazes palīdzību var konstruēt citu bazi.

Pieņemsim, ka $\xi_1, \xi_2, \ldots, \xi_n$ ir lauka $K(a)$ baze; tā tad

$$\Delta(\xi_1, \xi_2, \ldots, \xi_n) \neq 0.$$

Ja $\eta_1, \eta_2, \ldots, \eta_n$ ir lauka n skaitļi, tad ar racionāliem koeficientiem a_{ij} izteic:

$$\begin{aligned}
\eta_1 &= a_{11}\xi_1 + a_{12}\xi_2 + \ldots + a_{1n}\xi_n \\
\eta_2 &= a_{21}\xi_1 + a_{22}\xi_2 + \ldots + a_{2n}\xi_n \\
&\ldots\ldots\ldots\ldots\ldots \\
\eta_n &= a_{n1}\xi_1 + a_{n2}\xi_2 + \ldots + a_{nn}\xi_n .
\end{aligned}$$

Izlietojot determinantu reizināšanas teorēmu, pierāda, ka

$$(12) \qquad \Delta(\eta_1, \eta_2, \ldots, \eta_n) = \begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ & \ldots & \ldots & \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{vmatrix}^2 \Delta(\xi_1, \xi_2, \ldots, \xi_n).$$

Šis rezultāts norāda sekojošo. Ja attiecībā pret bazi $\xi_1, \xi_2, \ldots, \xi_n$ skaitļu $\eta_1, \eta_2, \ldots, \eta_n$ koordinātu determinants $\|a_{ij}\| \neq 0$, tad arī skaitļi $\eta_1, \eta_2, \ldots, \eta_n$ veido bazi, jo $\Delta(\eta_1, \eta_2, \ldots, \eta_n) \neq 0$.

Katram algebriskam skaitlim ξ_k var atrast atbilstošu veselu skaitli m_k tā, ka reizinājums $m_k \xi_k$ ir vesels algebrisks skaitlis (sk. § 65). Ja bazes $\xi_1, \xi_2, \ldots, \xi_n$ skaitļiem atbilstošie m_k ir $m_1, m_2, \ldots, m_n$, tad

$$m_1\xi_1, \quad m_2\xi_2, \ldots, m_n\xi_n ,$$

ir veseli algebriski skaitļi. Tie ir līnearī neatkarīgi, jo, pieņemot, ka

$$c_1m_1\xi_1 + c_2m_2\xi_2 + \ldots + c_n m_n \xi_n = 0$$

ar racionāliem koeficientiem $c_1, c_2, \ldots, c_n$ (kas visi nav nulles), secinātu, ka $\xi_1, \xi_2, \ldots, \xi_n$ ir līnearī atkarīgi.

To pašu pierāda arī ar formulu (12).

Rezultāts liecina, ka katrā laukā $K(\alpha)$ var konstruēt bezgala daudz bažu ar veseliem algebriskiem skaitļiem.

Ja viena tāda baze ir $\eta_1, \eta_2, \ldots, \eta_n$ ar veseliem algebriskiem skaitļiem η_k, tad lauka katru skaitli β var izteikt ar

$$\beta = c_1\eta_1 + c_2\eta_2 + \ldots + c_n\eta_n,$$

kur $c_1, c_2, \ldots, c_n$ ir racionāli skaitļi. Speciālā gadījumā, kad visi koeficienti „c" ir veseli skaitļi, tad β ir vesels algebrisks skaitlis (sk. 57. § teorēmu).

Bet ir iespējams, ka β ir vesels algebrisks skaitlis arī tad, kad visi vai daži „c" ir daļskaitļi. Par to liecina sekojošais **piemērs.**

Var viegli pārliecināties, ka par lauka

$$K(\sqrt{-3})$$

bazi var izvēlēties veselos algebriskos skaitļus

$$1, \sqrt{-3},$$

jo tie ir lineāri neatkarīgi. Saprotams, ka katrs skaitlis

$$\beta = a + b\sqrt{-3}$$

ir vesels algebrisks skaitlis tad, ja a un b ir veseli racionāli skaitļi. Bet ja izvēlas

$$a = \frac{1}{2}, \quad b = \frac{1}{2},$$

tad atbilstošais β ir vesels algebrisks skaitlis ar raksturīgo vienādojumu

$$x^2 - x + 1 = 0.$$

§ 70. Lauka minimālā baze.

Dēfinicija. Lauka veselu skaitļu bazi, ar kuŗu izteic veselus algebriskus skaitļus tikai tad, ja visi racionālie koeficienti $c_1, c_2, \ldots, c_n$ ir veseli skaitļi, sauc par lauka **minimālo bazi** jeb pamatbazi.

Var dēfinēt lauka minimālo bazi arī sekojoši.

Par lauka **minimālo bazi** sauc tādu veselu algebrisku skaitļu bazi, ka attiecībā pret to lauka katra veselā skaitļa koordinātas ir veseli racionāli skaitļi.

Pierādīsim, ka katrā algebriskā laukā eksistē minimālā baze.

Lauka katrai veselo skaitļu bazei diskriminants Δ ir vesels skaitlis, kas nav nulle. Dažādām bazēm ir dažādi diskriminanti ar vienādām zīmēm. No visām bazēm, kam atbilst Δ vismazākā absolūtā vērtība (tādas bazes var būt bezgala daudz), vienu apzīmēsim ar

$$\omega_1, \omega_2, \ldots, \omega_n.$$

Pierādīsim, ka tā ir lauka minimālā baze.

Pieņemsim pretējo, ka laukā $K(\alpha)$ atrodas tāds vesels algebrisks skaitlis β, ka izteiksmē

$$\beta = a_1\omega_1 + a_2\omega_2 + \ldots + a_n\omega_n$$

ar bazi $(\omega_1, \omega_2, \ldots, \omega_n)$ un racionāliem koeficientiem $a_1, a_2, \ldots, a_n$ vismaz viens koeficients, piem. a_1, nav vesels skaitlis. Tad a_1 var izteikt ar vesela skaitļa a un īsta daļskaitļa d summu

$$a_1 = a + d,$$

kur $|d| < 1$. Sastādām citu veselu algebrisku skaitli

$$\gamma = \beta - a\omega_1 = d\omega_1 + a_2\omega_2 + \ldots + a_n\omega_n.$$

Ja aprēķina n skaitļu:

$$\begin{aligned}
\gamma &= d\omega_1 + a_2\omega_2 + \ldots + a_n\omega_n \\
\omega_2 &= 0\cdot\omega_1 + 1\cdot\omega_2 + \ldots + 0\cdot\omega_n \\
&\ldots\ldots\ldots\ldots \\
\omega_n &= 0\cdot\omega_1 + 0\cdot\omega_2 + \ldots + 1\cdot\omega_n
\end{aligned}$$

diskriminantu $\Delta(\gamma, \omega_2, \ldots, \omega_n)$, tad ar (12) formulu atrod

$$\Delta(\gamma, \omega_2, \ldots, \omega_n) = \begin{vmatrix} d & a_2 & \ldots & a_n \\ 0 & 1 & \ldots & 0 \\ & & \ldots & \\ 0 & 0 & \ldots & 1 \end{vmatrix}^2 \cdot \Delta(\omega_1, \omega_2, \ldots, \omega_n)$$

jeb

$$\Delta(\gamma, \omega_2, \ldots, \omega_n) = d^2 \cdot \Delta(\omega_1, \omega_2, \ldots, \omega_n).$$

Pēdējais rezultāts norāda, ka

$$\Delta(\gamma, \omega_2, \ldots, \omega_n) \neq 0,$$

jo ne d, ne arī $\Delta(\omega_1, \omega_2, \ldots, \omega_n)$ nav nulles. Tādēļ arī $\Delta(\gamma, \omega_2, \ldots, \omega_n)$ ir lauka veselu skaitļu baze, bet tās diskriminanta absolūtā vērtība ir mazāka par bazes $(\omega_1, \omega_2, \ldots, \omega_n)$ diskriminanta absolūto vērtību:

$$|\Delta(\gamma, \omega_2, \ldots, \omega_n)| < |\Delta(\omega_1, \omega_2, \ldots, \omega_n)|.$$

Ar to rodas pretruna bazes $(\omega_1, \omega_2, \ldots, \omega_n)$ minimālā diskriminanta nosacījumam. Tādēļ atliek pieņemt, ka

$$\beta = a_1 \omega_1 + a_2 \omega_2 + \ldots + a_n \omega_n$$

ir vesels algebrisks skaitlis tikai tad, ja visi koeficienti $a_1, a_2, \ldots, a_n$ ir veseli racionāli skaitļi. Tā tad $(\omega_1, \omega_2, \ldots, \omega_n)$ ir minimālā baze, un teorēma pierādīta.

No pierādītā gan seko minimālās bazes eksistence, bet ne metode tās sastādīšanai. Praktisku metodi tādas bazes noteikšanai otrās pakāpes laukos ir devis Dirichlē (*Dirichlet*). To apskatīsim 72. §.

Definīcija. Par lauka $K(\alpha)$ diskriminantu D jeb pamatskaitli sauc lauka minimālās bazes diskriminantu

$$D = \Delta(\omega_1, \omega_2, \ldots, \omega_n).$$

Pierādīsim, ka lauka katra veselā skaitļa ξ diskriminants $d(\xi)$ dalās ar lauka diskriminantu D.

Ja ξ izteic ar minimālo bazi $(\omega_1, \omega_2, \ldots, \omega_n)$:

$$\xi = a_1 \omega_1 + a_2 \omega_2 + \ldots + a_n \omega_n,$$

tad koeficienti $a_1, a_2, \ldots, a_n$ ir veseli skaitļi. Skaitļa ξ diskriminantu var pārveidot par

$$d(\xi) = \| c_{ij} \|^2 \Delta(\omega_1, \omega_2, \ldots, \omega_n),$$

kur determinanta $\|c_{ij}\|$ elementi c_{ij} ir veseli skaitļi, kas konstruēti no $a_1, a_2, \ldots, a_n$ ar saskaitīšanas, atņemšanas un reizināšanas darbībām. Tādēļ determinanta vērtība ir vesels skaitlis, un veselais skaitlis $d(\xi)$ dalās ar lauka pamatskaitli $D = \Delta(\omega_1, \omega_2, \ldots, \omega_n)$.

Piemērs. Var pierādīt, ka lauka $K(i)$ skaitlis

$$\beta = a + bi \qquad (i = \sqrt{-1}),$$

kas apmierina vienādojumu

$$x^2 - 2ax + (a^2 + b^2) = 0,$$

ir vesels algebrisks skaitlis tikai tad, ja a un b ir veseli skaitļi*). Tādēļ $(1, i)$ ir lauka minimālā baze ar diskriminantu

$$D = \begin{vmatrix} 1 & i \\ 1 & -i \end{vmatrix}^2 = -4.$$

Bet skaitļa $\beta = a + bi$ diskriminants (§ 67)

$$d(\beta) = -4b^2.$$

Tiešām, $d(\beta)$ dalās ar D.

Ja $(\omega_1, \omega_2, \ldots, \omega_n)$ ir lauka $K(\alpha)$ minimālā baze un $\eta_1, \eta_2, \ldots, \eta_n$ ir lauka n veseli skaitļi

$$\eta_i = a_{i1}\omega_1 + a_{i2}\omega_2 + \ldots + a_{in}\omega_n \qquad (i = 1, 2, \ldots, n)$$

ar koordinātu determinantu $\|a_{ij}\| = \pm 1$, tad no formulas (12) seko rezultāts

$$\Delta(\eta_1, \eta_2, \ldots, \eta_n) = \Delta(\omega_1, \omega_2, \ldots, \omega_n).$$

Redzam, ka arī $(\eta_1, \eta_2, \ldots, \eta_n)$ ir lauka minimālā baze. Tā kā veselus racionālus koeficientus a_{ij} ar nosacījumu $\|a_{ij}\| = \pm 1$ var

---

*) Vienādojuma $x^2 - 2ax + (a^2 + b^2) = 0$ koeficients $-2a$ ir vesels skaitlis arī tad, ja $a = \frac{2k+1}{2}$ (k vesels sk.). Bet tādā gadījumā $a^2 + b^2$ ir vesels skaitlis tikai tad, ja b^2 ir formā $\frac{4n+3}{4}$ (n vesels), kas ar racionālu b nav iespējams (sk. arī 72. §.)

izvēlēties bezgala daudz veidos, tad laukā eksistē bezgala daudz minimālo bažu.

Minkovskis ir pierādījis, ka katrā laukā minimālās bazes diskriminanta (lauka pamatskaitļa) D absolutā vērtība ir lielāka par 1. Tomēr nevar apgalvot apgrieztā kārtā, ka katram dotam pamatskaitlim D ar absolūto vērtību $|D|>1$ tiešām atbilst kāds lauks $K(\alpha)$.

Uzdevumi.

1. Pierādīt, ka katrs algebriskais skaitlis α var būt tikai viena lauka primitīvs elements.

2. Pierādīt, ka lauki $K(\sqrt[3]{2})$ un $K(\sqrt[3]{3})$ nav identiski.

3. Pierādīt, ka $K(\alpha)$ ir Galuā lauks, ja α ir vienādojuma

$$x^4+10x^2+1=0$$

sakne.

4. Pierādīt teorēmu: ja $K(\alpha)$ ir Galuā lauks, tad α raksturīgais vienādojums ir normāls vienādojums, t. noz., šī vienādojuma katra sakne ir kaut kuŗas saknes racionāla funkcija ar racionāliem koeficientiem.

5. Pierādīt, ka $x^4+x^3+x^2+x+1=0$ ir normāls vienādojums.

6. Aprēķināt pēc iespējas vienkāršu skaitļu lauku, kuŗā visi vienādojumi:

$$x^2+2x+1=0, \quad x^4+x^2+1=0,$$
$$x^2+x+1=0, \quad x^2+x-1=0 \quad \text{un} \quad x^2+1=0$$

būtu reducībli.

7. Aprēķināt skaitļa $i=\sqrt{-1}$ diskriminantu laukā $K(i)$ un laukā $K(i+\sqrt{2})$.

IV. Kvadrātiskie skaitļu lauki.

§ 71. Kvadrātisko lauku kanoniskā forma.

Definīcija. $K(\alpha)$ sauc par kvadrātisku lauku tad, ja α ir sakne irreducīblam kvadrātvienādojumam

$$ax^2 + bx + c = 0 \tag{1}$$

ar veseliem koeficientiem a, b un c.

Ar tādu nosacījumu vienādojuma diskriminants

$$\Delta = b^2 - 4ac$$

nav racionāla skaitļa kvadrāts, jo pretējā gadījumā vienādojums būtu reducībls.

Ja A ir lielākais veselais skaitlis, kuŗa kvadrāts dala diskriminantu Δ, tad var izteikt

$$\Delta = A^2 . n,$$

kur n vesels (pozitīvs vai negātīvs) skaitlis, kas nedalās ne ar vienu kvadrātskaitli lielāku par 1. Tā tad skaitlis n ir dažādu pirmskaitļu p_i produkts, kas katru pirmskaitli p_i satur tikai pirmajā pakāpē. Tādēļ var rakstīt

$$|n| = p_1 p_2 \dots p_k . \tag{2}$$

Algebrisko skaitli α un tā saistīto skaitli α' dod formulas:

$$\alpha = \frac{-b + A\sqrt{n}}{2a}, \qquad \alpha' = \frac{-b - A\sqrt{n}}{2a}.$$

65. § otrās teorēmas sekas norāda, ka tiklab lauks $K(\alpha)$ kā arī $K(\alpha')$ ir identiski ar lauku $K(\sqrt{n})$. Tādēļ katru kvadrātisko lauku var izteikt kanoniskā formā

$$K(\sqrt{n}),$$

kur n vesels skaitlis, kas nedalās ne ar viena pirmskaitļa kvadrātu.

Tā kā

$$K(\alpha) = K(\sqrt{n}) \quad \text{un arī} \quad K(\alpha') = K(\sqrt{n}),$$

tad kā blakus rezultāts seko (to var pierādīt arī tieši), ka saistītie kvadrātiskie lauki ir identiski:

$$K(\alpha) = K(\alpha').$$

Ta tad visi kvadrātiskie lauki ir Galuā lauki.

Atkarīgi no tā, vai n ir pozitīvs vai negātīvs skaitlis, lauks $K(\sqrt{n})$ ir reāls vai imāginārs. Pēdējais, saprotams, satur arī reālus elementus — visus racionālos skaitļus. Dažas reālo lauku īpašības ir pavisam citādas kā imāgināro lauku atbilstošās īpašības.

Par lauka $K(\sqrt{n})$ bazi var izvēlēties skaitļus

$$1, \sqrt{n},$$

jo tie ir lineāri neatkarīgi (sk. 60. §). Tad lauka katru skaitli β var izteikt ar

$$\beta = A + B\sqrt{n},$$

kur A un B ir racionāli skaitļi*).

Dažos gadījumos baze $(1, \sqrt{n})$ ir arī lauka minimālā baze, piem. ja $n = -1$. Bet 69. § piemērā redzējām, ka gadījumā, kad $n = -3$, baze $(1, \sqrt{-3})$ nav minimālā.

§ 72. Lauka $K(\sqrt{n})$ minimālā baze.

Pieņemsim, ka

$$\beta = A + B\sqrt{n}$$

ar racionāliem skaitļiem A un B ir lauka $K(\sqrt{n})$ vesels skaitlis. Nolīdzinot saucējus un saīsinot (ja iespējams), dabūjam izteiksmi

*) Neatkarīgi no jēdziena par bazi, lauka $K(\sqrt{n})$ katru skaitli var izteikt šādā formā, ja lieto pārveidojumu, ko apskatījām 2. § piemērā ar lauku $K(\sqrt{-5})$

(3) $$\beta = \frac{p + q\sqrt{n}}{r},$$

kur p, q, r ir veseli skaitļi ar lielāko kopīgo dalītāju $(p, q, r)=1$. Tā kā β ir vesels algebrisks skaitlis, tad β pēdai

$$S(\beta) = \frac{p + q\sqrt{n}}{r} + \frac{p - q\sqrt{n}}{r} = \frac{2p}{r}$$

un normai

$$N(\beta) = \frac{p + q\sqrt{n}}{r} \cdot \frac{p - q\sqrt{n}}{r} = \frac{p^2 - nq^2}{r^2}$$

jābūt veseliem racionāliem skaitļiem. Tādu pat prasību arī dabū, uzrakstot β raksturīgo vienādojumu

$$x^2 - S(\beta) \cdot x + N(\beta) = 0,$$

kur koeficientiem $S(\beta)$ un $N(\beta)$ jābūt veseliem skaitļiem, ja β ir vesels algebrisks skaitlis.

Apskatīsim sekojošus **divus gadījumus**.

I. gadījumā, kad r ir nepāru skaitlis, tad pēda

$$S(\beta) = \frac{2p}{r}$$

ir vesels skaitlis tikai tad, ja p dalās ar r jeb

$$p = rp_1 \qquad (p_1 \text{ ir vesels skaitlis}).$$

Prasot, lai norma $N(\beta)$ būtu vesels skaitlis N, dabū formulu

$$p_1^2 - N = n\frac{q^2}{r^2},$$

kuŗas kreisā puse $p_1^2 - N$ ir vesels skaitlis, bet labā puse izteic veselu skaitli tikai tad, ja $r = 1$. Tas tādēļ, ka n nedalās ar r^2, ja $r > 1$. Ja q^2 dalītos ar r^2, tad pretēji pieņēmumam būtu lielākais kopīgais dalītājs $(p, q, r) > 1$.

Tā tad dabūjam, ka ar nepāŗu skaitli r formula (3) izteic veselu algebrisku skaitli tikai tad, ja $r = 1$.

II. gadījumā, kad r ir pāru skaitlis, pieņemam

$$r = 2r_1.$$

Tad $S(\beta)$ ir vesels skaitlis tikai tad, ja p dalās ar r_1; liekam

$$p = r_1 p_1.$$

Bet ja $N(\beta)$ ir vesels skaitlis, tad tamlīdzīgi kā iepriekšējā gadījumā no formulas

$$p_1^2 - 4N = n\frac{q^2}{r_1^2}$$

seko, ka $r_1 = 1$ un $p_1 = p$. Tā tad

$$r = 2.$$

Rakstām kongruenci

$$p^2 \equiv nq^2 \pmod 4,$$

un ievērojam, ka p un q nevar būt abi pāru skaitļi, jo $(p, q, r) = 1$. Ja q būtu pāru skaitlis, tad sekotu, ka arī p ir pāru skaitlis, kas neder. Kad p pāru un q nepāru skaitlis, tad

$$nq^2 | 4.$$

Tā tad arī $n|4$, kas ir pretruna nosacījumam, ka n nedalās ar kvadrātskaitļiem. Atliek tikai, ka p un q abi ir nepāru skaitļi:

$$p = 2k + 1, \quad q = 2h + 1.$$

Šinī gadījumā no kongruences

$$4k^2 + 4k + 1 \equiv n(4h^2 + 4h + 1) \pmod 4$$

jeb

$$1 \equiv n \pmod 4$$

seko, ka n ir formā $4m + 1$.

Tā tad pēdējā gadījumā, kad

$$n = 4m + 1,$$

lauka $K(\sqrt{n})$ veselie skaitļi β ir izsakāmi formā

$$\beta = a + b\sqrt{n} \tag{4}$$

ar kaut kādiem veseliem a, b un arī formā

$$\beta = \frac{p + q\sqrt{n}}{2}, \tag{5}$$

kur p un q ir nepāru skaitļi.

Pārējos gadījumos, kad

$$n = 4m + 2 \quad \text{vai} \quad n = 4m + 3,$$

lauka veselie skaitļi izsakāmi tikai formā (4).

Piezīme. Gadījums, kad $n = 4m$, ir izslēgts.

Ar šiem rezultātiem konstruēsim lauka $K(\sqrt{n})$ vienu minimālo bazi. To zinot, var atrast bezgala daudz citu minimālu bāzu (apskatīts jau 70. §).

Teorēma. Ja n nedalās ne ar vienu kvadrātskaitli un n nav formā $4m + 1$, tad lauka $K(\sqrt{n})$ minimālā baze ir $(1, \sqrt{n})$, bet, ja $n = 4m + 1$, tad minimālā baze ir $\left(1, \frac{1 + \sqrt{n}}{2}\right)$

Kad $n \neq 4m + 1$, apgalvojums ir acīmredzams.

Gadījumā, kad $n = 4m + 1$, formulu (4) uzraksta ar

$$\beta = (a - b) + 2b\,\frac{1 + \sqrt{n}}{2},$$

un formulu (5), kur $p = 2k + 1$, $q = 2h + 1$, pārveido par

$$\beta = (k - h) + (2h + 1)\,\frac{1 + \sqrt{n}}{2}.$$

Dabūtie rezultāti liecina, ka abos gadījumos lauka $K(\sqrt{n})$ veselais skaitlis β ir izsakāms formā

$$\beta = A + B\,\frac{1 + \sqrt{n}}{2}$$

ar veseliem racionāliem skaitļiem A, B. Tā tad $\left(1, \frac{1 + \sqrt{n}}{2}\right)$ ir lauka minimālā baze.

Vēl noteiksim lauka $K(\sqrt{n})$ pamatskaitli D, resp. minimālās bazes diskriminantu. Gadījumā, kad $n \neq 4m+1$, dabūjam

$$D = \Delta(1, \sqrt{n}) = \begin{vmatrix} 1 & \sqrt{n} \\ 1 & -\sqrt{n} \end{vmatrix}^2 = 4n,$$

bet, kad $n = 4m+1$, tad

$$D = \Delta\left(1, \frac{1+\sqrt{n}}{2}\right) = \begin{vmatrix} 1 & \frac{1+\sqrt{n}}{2} \\ 1 & \frac{1-\sqrt{n}}{2} \end{vmatrix}^2 = n.$$

Redzam, ka abos gadījumos D un n zīmes ir vienlīdzīgas. Tādēļ reāla lauka pamatskaitlis ir pozitīvs, bet imāginära — negātīvs.

Aprēķinot pamatskaitļus laukiem $K(\sqrt{n})$ ar

$$n = -1, -2, -3, -7, \ldots \text{ un } n = 2, 3, 5, \ldots$$

atrodam, ka visiem imāgināriem laukiem pamatskaitļa absolūtā vērtība $\geqslant 3$, bet reāliem laukiem $D \geqslant 5$.

§ 73. Lauka vieninieki.

Ja α un β ir lauka $K(\sqrt{n})$ veseli skaitļi, tad, izteicot tos ar minimālo bazi, var pārliecināties, ka veselo skaitļu summa $\alpha+\beta$ un reizinājums $\alpha\beta$ arī ir veseli skaitļi. Turpretim veselu skaitļu dalījums katrreiz nav vesels skaitlis.

Piemērs. $\alpha = 8+i$ un $\beta = 3-2i$ ir lauka $K(i)$ veseli skaitļi. Norma $N(\alpha)$ dalās ar $N(\beta)$, bet α nedalās ar β, jo dalījums

$$\frac{\alpha}{\beta} = \frac{22}{13} + \frac{19}{13}i \qquad (i = \sqrt{-1})$$

nav vesels algebrisks skaitlis.

No 67. § apskatītās lauka vieninieku vispārīgās teōrijas seko, ka veselais algebriskais skaitlis ε ir lauka $K(\sqrt{n})$ vieninieks tad, ja ε norma ir $+1$ vai -1.

Gadījumā, kad $n \neq 4m + 1$, ar veseliem x un y izteic

$$\varepsilon = x + y\sqrt{n},$$

un

$$N(\varepsilon) = (x + y\sqrt{n})(x - y\sqrt{n}) = x^2 - ny^2.$$

Skaitlis ε ir lauka vienīnieks tad, ja

$$x^2 - ny^2 = \pm 1. \tag{6}$$

Gadījumā, kad $n = 4m + 1$, tad

$$\varepsilon = x + y\,\frac{1 + \sqrt{n}}{2}$$

ar veseliem x, y. Tā kā

$$N(\varepsilon) = \left(x + \frac{y}{2}\right)^2 - n\frac{y^2}{4},$$

tad šinī gadījumā ε ir vienīnieks, ja

$$(2x + y)^2 - ny^2 = \pm 4 \tag{7}$$

Ar to jautājums par lauka $K(\sqrt{n})$ vieniniekiem ir reducēts uz nenoteikto vienādojumu (6) un (7) atrisināšanu veselos skaitļos x, y.

Vispirms atrisināsim šos vienādojumus, gadījumā, kad n ir **negatīvs skaitlis**, t. i. $n = -|n|$. Tad tiklab vienādojums (6), kā arī (7) ir iespējami tikai tad, ja labā pusē no $\pm 1, \pm 4$ zīmēm izvēlas pozitīvo zīmi.

Uzrakstot (6) formā

$$x^2 + |n|\,y^2 = 1,$$

redzam, ka gadījumā, kad

$$|n| = 1,$$

šī vienādojuma vienīgie atrisinājumi ir

$$x = \pm 1, \quad y = 0 \quad \text{un} \quad x = 0, \quad y = \pm 1.$$

Atbilstošā laukā, kas ir **Gausa lauks** $K(i)$, ir tieši četri vieninieki

$$\varepsilon = 1, \quad -1, \quad i, \quad -i.$$

Gadījumā, kad $|n| > 1$, tad (6) vienīgie atrisinājumi ir

$$x = \pm 1, \quad y = 0.$$

Tas nozīmē, ka pārējiem imāgināriem laukiem $K(\sqrt{n})$ ar $n \neq 4m + 1$, ir tikai divi vieninieki

$$\varepsilon = 1, \quad -1.$$

Tagad apskatīsim **imāginārus laukus** ar

$$n = 4m + 1, \quad \text{t. i.} \quad n = -3, \quad -7, \ldots$$

Gadījumā, kad $n = -3$, vienādojums (7) uzrakstāms formā

$$(2x + y)^2 + 3y^2 = 4,$$

un tam ir vienīgi šādi atrisinājumi, kas sarakstīti tabulā.

y	$2x+y$	x	$\varepsilon = x + y\frac{1+\sqrt{-3}}{2}$
0	± 2	± 1	± 1
$+1$	± 1	$0, -1$	$\frac{1+\sqrt{-3}}{2}, \quad \frac{-1+\sqrt{-3}}{2}$
-1	± 1	$0, 1$	$\frac{-1-\sqrt{-3}}{2}, \quad \frac{1-\sqrt{-3}}{2}$

Gadījumā, kad $n = 4m + 1$ un $|n| > 3$, resp. $|n| \geqslant 7$, tad vienādojuma (7)

$$(2x + y)^2 + |n|\, y^2 = 4$$

vienīgie veselie atrisinājumi ir

$$y = 0 \quad \text{un} \quad x = \pm 1;$$

šinī gadījumā lauka vieninieki ir

$$\varepsilon = 1, \quad -1.$$

Ar to imāginārос kvadrātiskos laukos vieninieku problēma ir atrisināta. Atrādām, ka vispārīgā gadījumā imāginārā laukā $K(\sqrt{n})$ ir tikai divi vieninieki: $+1$ un -1. Izņēmuma gadījumi ir Gausa lauks $K(i)$ ar 4 vieniniekiem $+1$, -1, $+i$, $-i$ un Eizenšteina (vai Jakobi) lauks $K(\sqrt{-3})$ ar 6 vieniniekiem

$$\pm 1, \quad \frac{1 \pm \sqrt{-3}}{2}, \quad \frac{-1 \pm \sqrt{-3}}{2}.$$

Tā tad imagināros kvadrātiskos laukos vieninieku ir **galīgs skaits**: 2, 4 vai 6. Šie vieninieki ir attiecīgu binomālu vienādojumu

$$x^2 - 1 = 0, \quad x^4 - 1 = 0, \quad x^6 - 1 = 0$$

saknes.

Reālos kvadrātiskos laukos $K(\sqrt{n})$ ar $n>0$ vieninieku dod vienādojums (6), kad $n \neq 4m+1$, un (7), kad $n=4m+1$. Vienādojumu brīvie locekļi ± 1, ± 4 te jāņem ar abām zīmēm. Redzam, ka problēma atrast reāla kvadrātiska lauka vieninieku ir līdzvērtīga problēmai: atrisināt veselos skaitļos nenoteiktos vienādojumus

$$x^2 - ny^2 = 1, \quad x^2 - ny^2 = -1, \quad X^2 - nY^2 = \pm 4.$$

Te $X = 2x + y$, $Y = y$. Šo vienādojumu katram atrisinājumam atbilst viena attiecīgā lauka vieninieks, un otrādi.

§ 74. Pella vienādojuma $x^2 - ny^2 = 1$ atrisinājuma eksistence.

Šo vienādojumu minējām jau 2. § Izlietojot nepārtraukto (ķēžu) daļu teoriju, Lagranžs pierādīja, ka vienādojumam

$$x^2 - ny^2 = 1 \qquad (n > 0)$$

vienmēr ir bezgala daudz atrisinājumu. Viņš deva arī metodi, kā tos aprēķināt. Mēs te apskatīsim **eksistences**

pierādījumu, kur izlieto irracionālu skaitļu racionālus tuvinājumus (aproksimāciju). Šī pierādījuma ideju ir devis Dirichlē (*Dirichlet*) ap 1850. g. Tā ir izlietojama ikkatrā algebriskā laukā.

Lemma I. Ja $\sqrt{n}$ ir irracionāls skaitlis, tad eksistē bezgala daudz veselu pozitīvu skaitļu x, y, kas apmierina nevienlīdzību

$$|x - y\sqrt{n}| < \frac{1}{y}. \tag{8}$$

Pierādījums. Diferencē

$$z = x - y\sqrt{n}$$

liksim y vietā veselus pozitīvus skaitļus 1, 2, 3, . . ., $m + 1$, un katrai y nozīmei par atbilstošu x nozīmi izvēlēsimies veselo pozitīvo skaitli, kas atrodas vistuvāk irracionālajam skaitlim $y\sqrt{n}$ un ir lielāks par to, t. i.

$$x_k = E(y_k\sqrt{n}) + 1 \qquad (k = 1, 2, 3, \ldots, m + 1).$$

Tad dabūsim $m + 1$ skaitļus

$$z_k = x_k - y_k\sqrt{n} \qquad (k = 1, 2, \ldots, m + 1),$$

kas visi ir dažādi. Tiešām, pieņemot

$$z_k = z_h \qquad (1 \leqslant h < k \leqslant m + 1),$$

dabūtu

$$x_k - x_h = (y_k - y_h)\sqrt{n}.$$

Tā kā $y_k - y_h \neq 0$, tad sekotu pretruna, ka irracionāls skaitlis $\sqrt{n}$ ir vienlīdzīgs racionālam skaitlim

$$\frac{x_k - x_h}{y_k - y_h}.$$

Tā tad skaitļi $z_1, z_2, \ldots, z_{m+1}$ ir dažādi. Bez tam tie ir īsti pozitīvi daļskaitļi, kas atrodas intervallā (0, 1), un to skaits ir $m + 1$. Tādēļ, ja intervallu (0, 1) sadala m vienādos intervallos, tad vismaz vienā šādā intervallā atrodas divi skaitļi z, piem. z_k, z_h. No nevienlīdzības

$$|z_k - z_h| < \frac{1}{m}$$

seko

$$|(x_k - x_h) - (y_k - y_h)\sqrt{n}| < \frac{1}{m}.$$

Tagad apzīmējam

$$x_k - x_h = x, \quad y_k - y_h = y,$$

un pieņemam, ka $y_k > y_h$ (pretējā gadījumā mainām indeku h, k lomas). Tad arī $x_k > x_h$, jo lielākam y_i atbilst lielāks x_i. Dabūjam nevienlīdzību

$$|x - y\sqrt{n}| < \frac{1}{m}$$

ar veseliem pozitīviem x un y. No šī rezultāta redzam, ka katrreiz var atrast racionālu skaitli $\frac{x}{y}$, kas izteic $\sqrt{n}$ ar kādu patīk tuvinājumu.

Ievērojam, ka

$$y = y_k - y_h \leqslant m + 1 - 1$$

jeb

$$y \leqslant m \quad \text{un} \quad \frac{1}{m} \leqslant \frac{1}{y}.$$

Tādēļ arī

$$|x - y\sqrt{n}| < \frac{1}{y}.$$

Tā tad nevienlīdzībai

$$|x - y\sqrt{n}| < \frac{1}{y}$$

ir vismaz viens atrisinājums ar veseliem pozitīviem skaitļiem x, y.

Iepriekš pierādījām, ka visi $m + 1$ pozitīvie skaitļi $z_1, z_2, \ldots, z_{m+1}$ ir dažādi. Ievērojot, ka $|z_k - z_h|$ ir pozitīvs skaitlis, var atrast veselu pozitīvu skaitli

$$M > m$$

tā, ka

$$|z_k - z_h| > \frac{1}{M} > 0.$$

Ja ar šo M (tāpat kā iepriekš ar m) atrod veselu pozitīvu skaitļu pāri X, Y, kas apmierina nevienlīdzību

$$|X - Y\sqrt{n}| < \frac{1}{M},$$

tad šis pāris X, Y atšķiras no agrākā pāŗa x, y. Tiešām:

$$|x - y\sqrt{n}| = |z_k - z_h|, \quad \text{bet} \quad |X - Y\sqrt{n}| < |z_k - z_h|.$$

Nevienlīdzības

$$|X - Y\sqrt{n}| < \frac{1}{M}$$

vietā var rakstīt

$$|X - Y\sqrt{n}| < \frac{1}{Y}.$$

Tad nevienlīdzībai

$$|x - y\sqrt{n}| < \frac{1}{y}$$

ir atrasts vēl otrs atrisinājums

$$x = X, \quad y = Y.$$

Minēto procesu atkārtojot, šai nevienlīdzībai atrod bezgala daudz veselus pozitīvus atrisinājumus.

Lemma II. Var atrast bezgala daudz veselu racionālu skaitļu x, y, kas apmierina nevienlīdzību

$$|x^2 - ny^2| < 1 + 2\sqrt{n}. \tag{9}$$

Ja x, y ir veselu pozitīvu skaitļu pāris, kas der nevienlīdzībai (8), tad no

$$|x + y\sqrt{n}| = |x - y\sqrt{n} + 2y\sqrt{n}| \leqslant |x - y\sqrt{n}| + 2y\sqrt{n}$$

seko

$$|x + y\sqrt{n}| < \frac{1}{y} + 2y\sqrt{n}.$$

Pareizinot ar nevienlīdzību (8), dabū

$$|x^2 - n^2| < \frac{1}{y^2} + 2\sqrt{n}.$$

Ievērojot, ka $\frac{1}{y^2} \leqslant 1$, var rakstīt nevienlīdzību (9). Tā tad nevienlīdzības (8) katrs atrisinājums der arī nevienlīdzībai (9), t. i. (9) ir (8) sekas.

Līdz ar veselu pozitīvu atrisinājumu pāri x, y nevienlīdzībai (9) arī atrisinājumi

$$+x, \quad -y \quad \text{un} \quad -x, \quad \pm y.$$

Sekas. Tā kā veselu skaitļu $x^2 - ny^2$ ar absolūto vērtību mazāku par $1+2\sqrt{n}$ ir tikai galīgs skaits, tad ir vismaz viens tāds skaitlis k ar

$$|k| < 1 + 2\sqrt{n},$$

ka starp nevienlīdzības (9) bezgala daudzajiem atrisinājumiem ir arī bezgala daudz atrisinājumu

$$(10) \qquad (x_1, y_1), \quad (x_2, y_2), \ldots,$$

kas apmierina nosacījumu

$$(11) \qquad x_1^2 - n y_1^2 = x_2^2 - n y_2^2 = \ldots = k \qquad (k \neq 0).$$

Eksistences teorēmas pierādījums. Ja katra vesela skaitļa vietā liek tā mazāko pozitīvo atlikumu attiecībā pret moduli k un visus iespējamos skaitļu pāŗus (x, y) sadala klasēs (attiecībā pret moduli k), tad klašu skaits ir galīgs skaitlis k^2. Tādēļ, ja bezgala daudzos skaitļu pāŗus (10) sadalīsim pa moduļa k atlikumu klasēm, tad vismaz vienā klasē būs bezgala daudz pāŗu. Apzīmējot tos ar

$$(12) \qquad (x_a, y_a), \quad (x_b, y_b), \ldots$$

rakstām kongruences:

$$(13) \qquad \begin{cases} x_a \equiv x_b \equiv \ldots \pmod{k} \\ y_a \equiv y_b \equiv \ldots \pmod{k}. \end{cases}$$

Krustiski reizinot, dabūjam formulu

$$x_a y_b - x_b y_a \equiv 0 \pmod{k}$$

jeb

$$x_a y_b - x_b y_a = ku, \tag{14}$$

ja u vesels skaitlis, kas nav nulle*).

Līdzīgā kārtā reizinām pirmo kongruenci (13) ar x_b, otro ar ny_b un atņemam. Tad ievērojot, ka ar formulu (11) ir

$$x_b^2 - ny_b^2 = k,$$

dabūjam rezultātu

$$x_a x_b - ny_a y_b \equiv x_b^2 - ny_b^2 \equiv 0 \pmod{k}$$

jeb

$$x_a x_b - ny_a y_b = kt, \tag{15}$$

kur t vesels skaitlis.

Tagad pārveidojot reizinājumu

$$(x_a - y_a\sqrt{n})(x_b + y_b\sqrt{n}) = (x_a x_b - ny_a y_b) + (x_a y_b - x_b y_a)\sqrt{n}$$

un ievērojot formulas (14) un (15), dabū identitāti

$$(x_a - y_a\sqrt{n})(x_b + y_b\sqrt{n}) = k(t + u\sqrt{n}).$$

Līdzīgā kārtā, liekot iepriekšējā identitātē $\sqrt{n}$ vietā $-\sqrt{n}$, atrod

$$(x_a + y_a\sqrt{n})(x_b - y_b\sqrt{n}) = k(t - u\sqrt{n}).$$

Abas pēdējās formulas reizinot un ievērojot, ka

$$x_a^2 - ny_a^2 = x_b^2 - ny_b^2 = k,$$

dabū

$$k^2 = k^2(t^2 - nu^2).$$

---

*) Pieņemot $u = 0$, dabūtu $\frac{x_b}{x_a} = \frac{y_b}{y_a} = q$. Ievērojot (11), secinātu $q = 1$ jeb $x_a = x_b$, $y_a = y_b$.

Saīsinot ar k^2, redzam, ka ir atrasti veseli skaitļi t un u, kas apmierina vienādojumu

$$t^2 - nu^2 = 1.$$

Tā tad Pella vienādojumam

(16) $$x^2 - ny^2 = 1$$

eksistē vismaz viens atrisinājums veselos skaitļos:

$$x = t \quad \text{un} \quad y = u \neq 0.$$

§ 75. Pella vienādojuma $x^2 - ny^2 = 1$ vispārīgais atrisinājums.

Pieņemsim, ka bez atrastā atrisinājuma t, u Pella vienādojumam (16) eksistē arī vēl citi atrisinājumi. Ar x_1, y_1 apzīmēsim vismazāko pozitīvo atrisinājumu pāri, ko nosauksim par fundāmentālo jeb pamatatrisinājumu*). Ar to konstruētu lauka $K(\sqrt{n})$ vienīnieku.

$$\varepsilon_1 = x_1 + y_1\sqrt{n}$$

arī sauksim par lauka fundāmentālo jeb pamatvieniniekU. Kā jau teikts 67. §, reizē ar ε_1 lauka vieninieks ir arī

(17) $$\varepsilon_1^k = (x_1 + y_1\sqrt{n})^k = x_k + y_k\sqrt{n},$$

ja k vesels pozitivs vai negātīvs skaitlis. Tādēļ arī x_k, y_k ir Pella vienādojuma atrisinājumi. Tā kā, arīmredzot, dažādiem k arī atbilst dažādi x_k, y_k, tad seko, ka Pella vienādojumam (16) ir bezgala daudz atrisinājumu.

Tas nozīmē, ka reālā laukā $K(\sqrt{n})$ ar $n \neq 4m + 1$ ir bezgala daudz vieninieku.

Pierādīsim, ka formula (17) ar $k = 1, 2, 3, \ldots$ izteic Pella vienādojuma visus pozitīvos veselos atrisinājumus x_k, y_k.

---

*) Ja (x_1, y_1), (x_2, y_2), ... ir Pella vienādojuma pozitīvu atrisinājumu pāri, tad lielākam x_i atbilst arī lielāks y_i un otrādi. Tādēļ pamatatrisinājuma (x_1, y_1) jēdziens ir pilnīgi noteikts.

Pieņemsim, ka a un b ir veseli pozitīvi skaitļi kas apmierina vienādojumu (16), t. i.

$$a^2 - nb^2 = 1,$$

bet $a + b\sqrt{n}$ nav vienlīdzīgs nevienam ε_1^k ar veselu pozitīvu kāpinātāju k. Tād ievērojot, ka ε_1 pakāpes veido augošu pozitīvu skaitļu rindu

$$1 < \varepsilon_1 < \varepsilon_1^2 < \ldots,$$

ir saprotams, ka var atrast tādu veselu eksponentu k, ka $a + b\sqrt{n}$ ieslēgts starp ε_1^k un ε_1^{k+1}, t. i.

$$\varepsilon_1^k < a + b\sqrt{n} < \varepsilon_1^{k+1}$$

jeb

$$x_k + y_k\sqrt{n} < a + b\sqrt{n} < (x_k + y_k\sqrt{n})(x_1 + y_1\sqrt{n}).$$

Pēdējo nevienlīdzību reizinām ar $x_k - y_k\sqrt{n}$, kas ir pozitīvs skaitlis, jo formulā

$$(x_k - y_k\sqrt{n})(x_k + y_k\sqrt{n}) = 1$$

faktors $x_k + y_k\sqrt{n}$ ir pozitīvs. Dabūjam rezultātu

$$1 < (a + b\sqrt{n})(x_k - y_k\sqrt{n}) < x_1 + y_1\sqrt{n}. \tag{18}$$

Ja ievēro, ka $a + b\sqrt{n}$ un $x_k + y_k\sqrt{n}$ saistītais skaitlis $x_k - y_k\sqrt{n}$ ir lauka $K(\sqrt{n})$ vienīnieki, tad seko, ka arī reizinājums

$$(a + b\sqrt{n})(x_k - y_k\sqrt{n})$$

ir lauka vienīnieks. Ar veseliem A un B var izteikt

$$(a + b\sqrt{n})(x_k - y_k\sqrt{n}) = A + B\sqrt{n}.$$

Pierādīsim, ka A un B ir pozitīvi skaitļi.

No formulas (18) redzam, ka $A + B\sqrt{n}$ ir pozitīvs skaitlis, kas lielāks par 1. Tā kā

$$(A + B\sqrt{n})(A - B\sqrt{n}) = 1$$

(jo katrs no abiem faktoriem ir lauka vienīnieks), tad arī $A - B\sqrt{n}$ ir pozitīvs skaitlis, bet mazāks par 1. Saskaitot nevienlīdzības

$$A + B\sqrt{n} > 0, \quad A - B\sqrt{n} > 0$$

dabū, ka

$$A > 0.$$

Bet no nevienlīdzībām

$$A - B\sqrt{n} < 1, \qquad 0 < A + B\sqrt{n}$$

dabū nevienlīdzību

$$1 + 2B\sqrt{n} > 0,$$

kas iespējama tikai ar

$$B > 0.$$

Tā tad A, B ir veseli pozitīvi skaitļi, kas tāpat kā x_1, y_1 ir Pella vienādojuma atrisinājumi. No formulas (18)

$$1 < A + B\sqrt{n} < x_1 + y_1\sqrt{n}$$

dabūjam

$$A < x_1 \quad B < y_1,$$

kas runā pretī pamatatrisinājuma x_1, y_1 dēfinīcijai.

Ar to ir pierādīts, ka formula (17) tiešām izteic Pella vienādojuma (16) visus pozitīvos atrisinājumus x_k, y_k. Bet no pozitīviem atrisinājumiem dabū vienādojuma visus veselos atrisinājumus, ņemot x_k un y_k (vienu vai abus) ar zīmi —.

Ģeometriskā interpretācijā Pella vienādojuma (16) atrisinājumi ir tie punkti ar veselām koordinātām, kas atrodas uz hiperbolas

$$\frac{x^2}{1^2} - \frac{y^2}{\left(\frac{1}{\sqrt{n}}\right)^2} = 1.$$

Tādu punktu, kā pierādīts, ir bezgala daudz. No šiem punktiem visus tos, kas atrodas uz hiperbolas pozitīvā zara un I. kvadrantā izteic ar formulu

$$\varepsilon_1^k \qquad (k = 0, 1, 2, \ldots),$$

kur $\varepsilon_1 = x_1 + y_1\sqrt{n}$, un šī zara punkts (x_1, y_1) ir hiperbolas virsotnei vistuvākais punkts ar veselām pozitīvām koordinātām.

Piemērs. $x^2 - 2x^2 = 1.$

No vienādojuma izteicam

$$x^2 = 1 + 2y^2.$$

Ja liekam y vietā skaitļus 1, 2, 3, . . . un pārbaudam*), tad atrodam pamatatrisinājumu

$$x_1 = 3, \qquad y_1 = 2.$$

Visus pozitīvos atrisinājumus noteic ar formulu

$$x_k + y_k\sqrt{2} = (3 + 2\sqrt{2})^k \qquad (k = 0, 1, 2, 3, \ldots)$$

Piemēram, ja $k = 2$, tad dabū

$$x_2 + y_2\sqrt{2} = 17 + 12\sqrt{2}.$$

Tā tad

$$x_2 = 17, \; y_2 = 12.$$

§ 76. Vienādojumi $x^2 - ny^2 = -1$ un $X^2 - nY^2 = \pm 4$.

Šo vienādojumu teorija vēl nav pilnīgi noslēgta. Vispārīgā gadījumā ir zināms tikai nepieciešamais nosacījums: lai vienādojums

$$x^2 - ny^2 = -1 \tag{19}$$

būtu iespējams, ir nepieciešami, ka skaitļa n visi pirmreizinātāji būtu ar formu $4k + 1$.

Tiešām, ja vienādojums (19) ir iespējams, tad iespējama arī kongruence

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

*) Ja ievēro, ka vesela skaitļa kvadrāts katrā ziņā beidzas vai nu ar cipariem 1, 4, 5, 6, 9 vai 00, tad dažu y nozīmju pārbaudīšanu var aiztaupit.

un līdz ar to arī kongruence

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

kur p ir kaut kuŗš pirmskaitlis, kas dala n. Tādēļ p forma ir $4k + 1$, jo ar $p = 4k + 3$ pēdējā kongruence nav iespējama.

Atsevišķām n formām ir pazīstams arī pietiekošais nosacījums. Jau 1785. g. Ležandrs (*Legendre*) ir devis metodi, kā atrisināt vienādojumu

$$(20) \qquad x^2 - py^2 = -1, \quad \text{ja} \quad p = 4k + 1.$$

Reizē ar (20) apskatām vienādojumu

$$(21) \qquad x^2 - py^2 = 1.$$

Pieņemam, ka (21) mazākais pozitīvais atrisinājums ir x_1, y_1. Tad y_1 ir pāŗu un x_1 nepāŗu skaitlis. Tiešām, tie abi nevar būt pāŗu, ne abi nepāŗu skaitļi. Ja pieņemtu, ka x_1 ir pāŗu skaitlis un y_1 nepāŗu skaitlis, tad no (21) sekotu

$$-p \equiv 1 \pmod{4}$$

jeb

$$p \equiv 3 \pmod{4},$$

kas runā pretī nosacījumam: $p = 4k + 1$.

Liekam vienādojumā (21) atrisinājumu x_1, y_1, un rakstam

$$x_1^2 - 1 = py_1^2$$

jeb

$$(x_1 - 1)(x_1 + 1) = py_1^2.$$

Tad kreisajā pusē abiem faktoriem $x_1 - 1$, un $x_1 + 1$ ir kopīgs dalītājs 2. Tas ir arī lielākais kopīgais dalītājs, jo abu faktoru starpība ir 2. Tādēļ tikai viens no skaitļiem $x_1 - 1$, $x_1 + 1$ dalās ar p. Ir jāizšķiŗ divi sekojoši gadījumi.

I. gadījums, kad $x_1 + 1$ dalās ar p. Var rakstīt formulu

$$4 \cdot \frac{x_1 - 1}{2} \cdot \frac{x_1 + 1}{2p} = y_1^2.$$

Tai kreisajā pusē ir trīs faktori, kam nav kopīgu dalītāju. Tādēļ katrs faktors atsevišķi ir kvadrāts. Liekot

$$\frac{x_1 - 1}{2} = a^2, \qquad \frac{x_1 + 1}{2p} = b^2,$$

dabū sakaru

$$a^2 - pb^2 = -1.$$

Tā tad veselie zināmie skaitļi a un b ir vienādojuma (20) saknes.

Pierādīsim, ka II. gadījums, kad $x_1 - 1$ dalās ar p, īstenībā nemaz nav iespējams.

Tiešām, pieņemot, ka $x_1 - 1$ dalās ar p, no

$$4 . \frac{x_1 + 1}{2} . \frac{x_1 - 1}{2p} = y_1^2$$

izteiktu skaitļus

$$\frac{x_1 + 1}{2} = A^2, \qquad \frac{x_1 - 1}{2p} = B^2,$$

starp kuŗiem ir sakars

$$A^2 - pB^2 = 1.$$

Tā tad A un B būtu vienādojuma (21) saknes. Bet uzrakstot reizinājumu

$$pA^2B^2 = \frac{x_1^2 - 1}{4}$$

jeb

$$pA^2B^2 = \frac{py_1^2}{4},$$

dabū rezultātu

$$B^2 = \frac{y_1^2}{4A^2},$$

kas norāda, ka $|B| < y_1$. Te ir pretruna nosacījumam, ka x_1, y_1 ir vienādojuma (21) pamatatrisinājums.

Tā tad iespējams tikai pirmais gadījums, kur atrod vienādojuma (20) veselu atrisinājumu a, b un konstruē lauka vieninieku

$$\eta = a + b\sqrt{n}$$

ar normu

$$N(\eta) = -1.$$

Bezgala daudz citus lauka vieniniekus ar normu —1 dod vienieka η nepāŗu pakāpes

$$\eta^{2k+1} = (a + b\sqrt{n})^{2k+1} = a_k + b_k\sqrt{n}. \tag{22}$$

Līdz ar to atrod vienādojumam (20) bezgala daudz atrisinājumu.

Beidzot apskatīsim vienādojumus

$$X^2 - nY^2 = \pm 4, \tag{23}$$

kuŗu atrisinājumi noteic vieniniekus laukā $K(\sqrt{n})$ ar $n = 4m + 1$ (sk. 73. §). Pierādīsim, ka vienādojumam

$$X^2 - nY^2 = +4$$

eksistē atrisinājums ar $Y \neq 0$.

Tiešām, no vienādojuma redzam, ka X un Y ir abi reizē pāŗu vai abi nepāŗu skaitļi. Ja, pieņemot pirmo hipotēzi, liek

$$X = 2u, \qquad Y = 2v,$$

tad dabū Pella vienādojumu

$$u^2 - nv^2 = 1,$$

kas vienmēr ir atrisināms veselos skaitļos u, v ar $v > 0$.

Pēdējos §§ iegūtie rezultāti pierāda sekošu **teorēmu.**

Katrā reālā kvadrātiskā laukā $K(\sqrt{n})$ ir vismaz viens irracionāls vieninieks ε, kas atšķiŗas no ± 1.

§ 77. Lauka pamatvieninieks.

Pierādīsim, ka katrā kvadrātiskā laukā var atrast tādu irracionālu vieninieku ε_1, ka lauka ikkatru vieninieku var izteikt ar

$$\pm \varepsilon_1^k,$$

ja $k = 0, \pm 1, \pm 2, \ldots$

Šo ε_1 Dirichlē sauc par lauka fundāmentālo jeb pamatvienīnieku.

Augstākas pakāpes laukos katrs vienīnieks izsakāms ar vairāku pamatvienīnieku pakāpju produktu.

Hilberta lemma. Ja A ir reāls pozitīvs skaitlis, tad eksistē tikai galīgs skaits otrās pakāpes veselu algebrisku skaitļu a, kas reizē ar savu saistīto skaitli a' ir ar absolūto vērtību mazāku kā A, t. i.

$$|a| < A, \qquad |a'| < A. \tag{24}$$

Tiešām, ja a un a' ir otrās pakāpes saistīti veseli algebriski skaitļi, tad tie apmierina irreducīblu kvadrātvienādojumu

$$x^2 + ax + b = 0$$

ar veseliem koeficientiem a un b. Ir sakari:

$$|a| = |a + a'| \leqslant |a| + |a'|, \qquad |b| = |aa'| = |a||a'|.$$

levērojot, ka jābūt $|a| < A$, $|a'| < A$, redzam, ka a raksturīgā vienādojuma koeficienti a, b ir ierobežoti ar nepieciešamiem nosacījumiem*)

$$|a| < 2A, \qquad |b| < A^2.$$

Tādus veselu skaitļu pāŗus (a, b) var izvēlēties tikai galīgā skaitā.

No pierādītā seko, ka arī speciālā gadījumā laukā $K(\sqrt{n})$ ir tikai galīgs skaits veselu algebrisku skaitļu, kas izpilda nosacījumus (24).

Tagad pierādīsiņm pamatvienīnieka ε_1 eksistenci. levērojot iepriekšējā § beigās izteikto rezultātu, apgalvojām, ka katrā kvadrļātiskā laukā $K(\sqrt{n})$ var atrast

*) Šie nosacījumi tomēr nav pietiekoši, jo apgrieztā kartā nevar secināt, ka $|a| < A$ un $|a'| < A$. Tādēļ, lai visus lemmā minētos skaitļus uzrakstītu, tad vienādojumi $x^2 + ax + b = 0$ (kur izvēlas a un b ar noteikumiem: $|a| < 2A$, $|b| < A^2$) ir jāatrisina un to saknes jāpārbauda.

vismaz vienu irracionālu vieninieku ε, kas lielāks par 1. Tiešām, ja laukā ir irracionāls vieninieks ε, tad tur ir arī vismaz četri vienināki

$$\varepsilon, \quad -\varepsilon, \quad \frac{1}{\varepsilon}, \quad -\frac{1}{\varepsilon},$$

no kuriem tieši viens, ko apzīmējam ar ε_0, ir lielāks par 1.

Ja intervallā $(1, \varepsilon_0)$ būtu vēl kāds lauka vieninieks η, tad būtu

$$1 < \eta < \varepsilon_0.$$

Apzīmējam η saistīto algebrisko skaitli ar η' un ievērojam, ka η ir lauka vieninieks. Rakstām

$$N(\eta) = \eta\eta' = \pm 1,$$

no kurienes

$$|\eta'| = \frac{1}{\eta} < \eta.$$

Tādēļ arī

$$|\eta'| < \varepsilon_0.$$

Izlietojot Hilberta lemmu secinām, ka ir tikai galīgs skaits veselu algebrisku skaitļu η, kas izpilda nosacījumus

$$|\eta| < \varepsilon_0 \quad \text{un} \quad |\eta'| < \varepsilon_0.$$

Tādēļ arī intervallā $(1, \varepsilon_0)$ ir tikai galīgs skaits lauka $K(\sqrt{n})$ vieninieku. Ja no tiem vismazāko, kas nav 1, apzīmē ar ε_1, tad ε_1 ir lauka pamatvieninieks*).

Pamatvieninieka ε_1 visas pozitīvās un negātīvās pakāpes ar veseliem eksponentiem izteic lauka $K(\sqrt{n})$ vieninieku. Dažādiem eksponentiem arī atbilst dažādi vienināki, jo pieņemot

$$\varepsilon_1^a = \varepsilon_1^b \qquad (a > b)$$

sekotu, ka

$$\varepsilon_1 = \sqrt[a-b]{1}.$$

Bet tad ε_1 būtu vai nu 1, vai komplekss skaitlis, kas ir pretruna ar pieņemto. Tamlīdzīgu pretrunu dabū pieņemot, ka

$$\varepsilon_1^a = -\varepsilon_1^b.$$

*) Ja intervallā $(1, \varepsilon_0)$ nav neviena vieninieka η, tad liekam $\varepsilon_0 = \varepsilon_1$.

Apskatīsim atsevišķi sekojošus **divus gadījumus.**

1. Pierādīsim, ka lauka $K(\sqrt{n})$ katrs pozitīvs vienineks ξ ir izsakāms formā ε_1^k ar veselu eksponentu k.

Ievērojam, ka ε_1 ir pozitīvs skaitlis, kas lielāks par 1. Tādēļ ar pietiekoši lielu pozitīvu eksponentu pakāpe ε_1^k ir lielāka par katru iepriekš dotu pozitīvu skaitli, bet pēc absolūtās vērtības lielam negātīvam eksponentam ε_1^k tuvojas nullei. Ir saprotams, ka pozitīvais skaitlis ξ ir vai nu bezgalīgās rindas

$$\ldots \varepsilon_1^{-2}, \varepsilon_1^{-1}, \varepsilon_1^0, \varepsilon_1^1, \varepsilon_1^2, \ldots$$

loceklis (tad vajadzīgais būtu pierādīts), vai pretējā gadījumā ξ ir ieslēgts starp diviem sekojošiem locekļiem: ξ_1^a un ξ_1^{a+1}, t. i.

$$\varepsilon_1^a < \xi < \varepsilon_1^{a+1}.$$

Ja nevienlīdzību dala ar pozitīvu skaitli ε_1^a un lauka $K\sqrt{(n)}$ vienineku ξ un ε_1^a dalījumu $\frac{\xi}{\varepsilon_1^a}$ apzīmē ar η, tad arī η ir tā paša lauka vienineks. Nevienlīdzība

$$1 < \eta < \varepsilon_1$$

runā pretī ε_1 definīcijai.

2. Ja ξ ir lauka $K(\sqrt{n})$ negātīvs vienineks, tad $-\xi$ ir pozitīvs vienineks. Var atrast veselu eksponentu k tā, ka

$$-\xi = \varepsilon_1^k \quad \text{jeb} \quad \xi = -\varepsilon_1^k.$$

Ar to ir pierādīts apgalvojums, ka lauka $K(\sqrt{n})$ visi vieninieki ir izsakāmi ar pamatvienineka ε_1 pakāpēm

$$\pm \varepsilon_1^k \qquad (k = 0, \pm 1, \pm 2, \ldots)$$

Šī pierādījuma metodi var izlietot, lai konstruētu reālā lauka $K(\sqrt{n})$ pamatvienineku ε_1.

Piemērs. Apskatīsim lauku $K(\sqrt{n})$ ar $n = 5$.

Tā kā $5 = 4 . 1 + 1$, tad lauka $K(\sqrt{5})$ katru vienīnieku izteic formā

$$\varepsilon = x + y\frac{1+\sqrt{5}}{2}$$

ar veseliem skaitļiem x un y, kuŗus dabū, atrisinot vienādojumu (sk. § 73)

$$(25) \qquad (2x + y)^2 - 5y^2 = \pm 4.$$

Izmēģinot atrod, ka var likt

$$2x + y = 3, \qquad y = 1.$$

Tā tad

$$x = 1, \quad y = 1,$$

un viens lauka $K(\sqrt{5})$ vienīnieks ir

$$\varepsilon = \frac{3+\sqrt{5}}{2}.$$

Tagad ar Hilberta lemmā minēto metodi meklēsim lauka $K(\sqrt{5})$ vienīniekus η, kas atrodas intervallā $(1, \varepsilon)$. Tādi vienīnieki apmierina vienādojumu

$$x^2 + ax + b = 0$$

ar $b = \pm 1$ un $|a| < 2\varepsilon$. Tā tad

$$|a| \leqslant 5.$$

Liekot ($a = 0$ var ignorēt)

$$a = \pm 1, \quad \pm 2, \quad \pm 3, \quad \pm 4, \quad \pm 5,$$

dabū pavisam 20 vienādojumus. Bet no tiem pusi var atmest, jo, ja vienādojuma

$$x^2 + ax + b = 0$$

saknes ir skaitļi η, η', tad vienādojumam

$$x^2 - ax + b = 0$$

ir saknes $-\eta$, $-\eta'$. Ja vēl atmet vienādojumus ar racionālām

saknēm un tos, kuŗu saknes nav lauka $K(\sqrt{5})$ skaitļi, tad paliek tikai trīs vienādojumi

$$x^2 - x - 1 = 0, \quad x^2 - 3x + 1 = 0, \quad x^2 - 4x - 1 = 0.$$

To saknes ir attiecīgi

$$\frac{1 \pm \sqrt{5}}{2}, \quad \frac{3 \pm \sqrt{5}}{2}, \quad 2 \pm \sqrt{5}.$$

No šiem 6 skaitļiem intervallā $(1, \varepsilon)$ atrodas tikai viens skaitlis

$$\frac{1 + \sqrt{5}}{2},$$

kas tā tad ir lauka $K(\sqrt{5})$ pamatvienīnieks. Visus pārējos lauka vieniniekus un, līdz ar to, arī vienādojuma (25) visus atrisinājumus dod skaitļi

$$\pm\left(\frac{1 + \sqrt{5}}{2}\right)^k \quad \text{ar} \quad k = 0, \pm 1, \pm 2, \ldots$$

§ 78. Euklida algoritms kvadrātiskos laukos.

Veselo racionālo skaitļu teōrijā jautājumu par divu skaitļu a, b lielāko kopīgo dalītāju un vēl citas problēmas, kas ar to sakarā, atrisinājām, lietojot Euklida algoritmu. Šīs metodes pamatā ir teōrēma, ka ar diviem dotiem veseliem skaitļiem a un b $(a > b)$, vienmēr var atrast citus divus veselus skaitļus q un r tā, ka

$$a = bq + r \quad \text{un} \quad |r| < |b|.$$

Ja varētu pierādīt, ka analoga īpašība der arī lauka $K(\sqrt{n})$ veseliem skaitļiem, tad šinī laukā būtu pareiza visa racionālo skaitļu aritmetika. Izrādās, ka dažos kvadrātiskos laukos gan der tāda īpašība, bet vispārīgā gadījumā tā nav pareiza. To vispirms noskaidrosim ar diviem piemēriem.

1 piemērs. Apskatīsim **Gausa lauku** $K(i)$.

Pieņemsim, ka α un β ir šī lauka veseli skaitļi. Apzīmējot β saistīto algebrisko skaitli ar β', var pārveidot dalījumu

$$\frac{\alpha}{\beta} = \frac{\alpha\beta'}{\beta\beta'}.$$

Apzīmējot veselo algebrisko skaitli $\alpha\beta'$ ar $a + bi$ (a un b veseli racionāli skaitļi) un ievērojot, ka

$$\beta\beta' = N(\beta)$$

ir vesels racionāls un pozitīvs*) skaitlis, dabūjam formulu

$$\frac{\alpha}{\beta} = \frac{a}{N(\beta)} + i\,\frac{b}{N(\beta)}.$$

Ar to lauka $K(i)$ veselo algebrisko skaitļu α un β dalīšana ir reducēta uz veselu racionālu skaitļu a, b, $N(\beta)$ dalīšanu. Tādēļ var izteikt

$$a = N(\beta)\cdot a_1 + r_1, \qquad b = N(\beta)\cdot b_1 + r_2$$

ar veseliem racionāliem skaitļiem a_1, b_1, r_1, r_2, pie kam

$$|r_1| \leqslant \frac{1}{2}N(\beta), \qquad |r_2| \leqslant \frac{1}{2}N(\beta).$$

Liekam

$$a_1 + ib_1 = \gamma$$

un turpinām pārveidojumu:

$$\frac{\alpha}{\beta} = \gamma + \frac{r_1 + ir_2}{\beta\beta'}.$$

Tā tad

$$\alpha = \beta\gamma + \frac{r_1 + ir_2}{\beta'}.$$

Ja apzīmējam

$$\frac{r_1 + ir_2}{\beta'} = \rho,$$

*) Ikkatrā imāginārā kvadrātiskā laukā norma ir pozitīvs skaitlis.

tad ρ ir lauka $K(i)$ vesels skaitlis (kā veselo skaitļu starpība $\alpha - \beta\gamma$. Izteicam

$$\alpha = \beta\gamma + \rho$$

un

$$N(\rho) = \frac{N(r_1 + ir_2)}{N(\beta')} = \frac{r_1^2 + r_2^2}{N(\beta)}.$$

Tādēļ

$$N(\rho) \leqslant \frac{\frac{1}{4}[N(\beta)]^2 + \frac{1}{4}[N(\beta)]^2}{N(\beta)} = \frac{1}{2}N(\beta)$$

un

$$N(\rho) < N(\beta).$$

Tā tad laukā $K(i)$ Euklida algoritma pastāvēšanai vajadzīgā īpašība ir pierādīta. Atkārtojot apskatīto dalīšanas procesu ar skaitļiem β un ρ, atrod atlikumā veselu algebrisku skaitli ρ_1 ar normu

$$N(\rho_1) < N(\rho).$$

Dalīšanu turpinot un ievērojot, ka katra atlikuma norma ir vesels pozitīvs skaitlis, ir saprotams, ka beidzot dabūsim atlikumu ρ_n ar normu 0 vai 1.

Pirmajā gadījumā arī dalīšanas atlikums ir 0, un pēdējais dalītājs ir skaitļu α un β kopīgais dalītājs*).

Otrā gadījumā ρ_n ir lauka vienīnieks

$$1, \quad -1, \quad i \quad \text{vai} \quad -i,$$

un dotie skaitļi α, β ir relātīvi pirmskaitļi.

2. piemērs. Dirichlē lauka $K(\sqrt{-5})$ veseli skaitļi: $\alpha = 3$, $\beta = 1 + \sqrt{-5}$.

Pieņemsim, ka var izteikt

$$\alpha = \beta\gamma + \rho,$$

kur γ un ρ ir lauka veseli skaitļi, pie kam

$$N(\rho) < N(\beta) \quad \text{jeb} \quad \frac{N(\rho)}{N(\beta)} < 1.$$

*) Te nesaka „lielākais kopīgais dalītājs", jo nav teikts kā izšķirt, kuŗš no diviem kompleksiem skaitļiem ir lielākais.

Tā kā

$$\frac{N(\rho)}{N(\beta)} = N\left(\frac{\rho}{\beta}\right) = N\left(\frac{a}{\beta} - \gamma\right)$$

un lauka minimālā baze ir $(1, \sqrt{-5})$, tad ar veseliem racionāliem skaitļiem x un y varētu konstruēt skaitli

$$\gamma = x + y\sqrt{-5}$$

tā, lai derētu nevienlīdzība

$$N\left[\frac{a}{\beta} - (x + y\sqrt{-5})\right] < 1.$$

Liekot te $a = 3$, $\beta = 1 + \sqrt{-5}$ un pārveidojot, dabū nevienlīdzību

$$\left(x - \frac{1}{2}\right)^2 + 5\left(y + \frac{1}{2}\right)^2 < 1,$$

kas ar veseliem skaitļiem x un y nav iespējama, jo kreisās puses vismazākā vērtība ir

$$\frac{1}{4} + 5 \cdot \frac{1}{4} > 1.$$

Tas liecina, ka šinī gadījumā

$$N(\rho) > N(\beta).$$

Tādēļ nevar apgalvot, ka laukā $K(\sqrt{-5})$ Euklida algoritms ir galīgs process.

Tagad noskaidrosim līdzīgu jautājumu **vispārīgā** laukā $K(\sqrt{n})$, apskatot šādus **divus gadījumus.**

I. Vispirms apskatīsim **gadījumu,** kad $n \neq 4k + 1$. Tad lauka minimālā baze ir

$$1, \sqrt{n},$$

un lauka katrs veselais skaitlis izteicams formā

$$a = a_0 + a_1 \sqrt{n}$$

ar veseliem racionāliem skaitļiem a_0, a_1.

Pieņemsim, ka lauka dotiem veseliem skaitļiem α un β var atrast lauka veselus skaitļus γ un ρ tā, ka

$$\alpha = \beta\gamma + \rho \quad \text{un} \quad |N(\rho)| < |N(\beta)|.$$

Ievērojot, ka $\frac{\alpha}{\beta}$ ir lauka $K(\sqrt{n})$ skaitlis, ar racionāliem skaitļiem b_0, b_1 var izteikt

$$\frac{\alpha}{\beta} = b_0 + b_1 \sqrt{n}.$$

Ja noteic veselus racionālus skaitļus c_0, c_1 tā, ka

$$b_0 = c_0 + r_0, \quad b_1 = c_1 + r_1$$

ar

$$|r_0| \leqslant \frac{1}{2} \quad \text{un} \quad |r_1| \leqslant \frac{1}{2},$$

tad pārveido

$$\frac{\alpha}{\beta} = (c_0 + c_1 \sqrt{n}) + (r_0 + r_1 \sqrt{n})$$

jeb

$$\frac{\alpha}{\beta} = \gamma + (r_0 + r_1 \sqrt{n}),$$

kur

$$\gamma = c_0 + c_1 \sqrt{n}$$

ir lauka vesels skaitlis. Beidzot rakstām

$$\alpha = \beta\gamma + \rho,$$

kur

$$\rho = \beta (r_0 + r_1 \sqrt{n})$$

ir lauka vesels skaitlis (kā veselo starpība $\alpha - \beta\gamma$). Prasam, lai

$$|N(\rho)| < |N(\beta)|.$$

Dalot ar $|N(\beta)|$, dabūjam nevienlīdzību

$$|N(r_0 + r_1 \sqrt{n})| < 1$$

jeb

$$|r_0^2 - nr_1^2| < 1. \tag{26}$$

Izlietojot formulu

$$|a + b| \leqslant |a| + |b|,$$

ir skaidrs, ka nevienlīdzību (26) var sašaurināt, tās vietā prasot, lai

$$|r_0|^2 + |-nr_1^2| < 1.$$

Ja pēc tam liek

$$|r_0| \leqslant \frac{1}{2}, \quad |r_1| \leqslant \frac{1}{2},$$

tad seko

$$1 + |n| < 4 \quad \text{jeb} \quad |n| < 3.$$

Šis nosacījums ir p i e t i e k o š s, lai laukā $K(\sqrt{n})$ ar $n \neq 4k + 1$ varētu lietot Euklida algoritmu.

II. Noskaidrosim tādu pat jautājumu laukā $K(\sqrt{n})$ ar

$$n = 4k + 1.$$

Šinī gadījumā lauka minimālā baze ir

$$\left(1, \frac{1 + \sqrt{n}}{2}\right),$$

un lauka katrs veselais skaitlis α izteicams ar

$$\alpha = a_0 + a_1 \frac{1 + \sqrt{n}}{2},$$

kur a_0, a_1 v e s e l i racionāli skaitļi.

Pieņemam, ka α un β ir lauka v e s e l i skaitļi. Uzrakstām

$$\frac{\alpha}{\beta} = b_0 + b_1 \frac{1 + \sqrt{n}}{2}$$

ar racionāliem skaitļiem b_0, b_1 un izteicam

$$b_0 = c_0 + r_0, \quad b_1 = c_1 + r_1 \text{ ar } |r_0| \leqslant \frac{1}{2}, \quad |r_1| \leqslant \frac{1}{2}.$$

Tad tamlīdzīgi kā iepriekš dabū

$$\frac{a}{\beta} = \gamma + r_0 + r_1 \frac{1+\sqrt{n}}{2},$$

ja

$$\gamma = c_0 + c_1 \frac{1+\sqrt{n}}{2}.$$

Apzīmējot ar

$$\rho = \beta \left(r_0 + r_1 \frac{1+\sqrt{n}}{2} \right)$$

un prasot, lai $|N(\rho)| < |N(\beta)|$, dabū nevienlīdzību

$$\left| N\left(r_0 + r_1 \frac{1+\sqrt{n}}{2} \right) \right| < 1.$$

Tā kā

$$N\left(r_0+r_1\frac{1+\sqrt{n}}{2}\right)=\left(r_0+r_1\frac{1+\sqrt{n}}{2}\right)\left(r_0+r_1\frac{1-\sqrt{n}}{2}\right)=r_0^2+r_0r_1-\frac{(n-1)r_1^2}{4}$$

un $n - 1 = 4k$, tad vajadzīgais nosacījums top

$$(27) \qquad |r_0^2 + r_0 r_1 - k r_1^2| < 1 \qquad \left(k = \frac{n-1}{4}\right).$$

Ja tā vietā prasa, lai

$$|r_0^2| + |r_0 r_1| + |k r_1^2| < 1$$

(kas ir vairāk nekā vajadzīgs), un ievēro, ka

$$|r_0| \leqslant \frac{1}{2}, \quad |r_1| \leqslant \frac{1}{2},$$

tad dabū p i e t i e k o š u (b e t n e n e p i e c i e š a m u) nosacījumu

$$|k| < 2.$$

To izpilda skaitļi:

$$n = 1, 5 \text{ un } -3.$$

Ievērojot arī I. gadījumā atrastos n, apgalvojam, ka v i s a p a r a s t ā a r i t m ē t i k a, k o p a m a t o a r E u k l i d a a l g o-

ritmu ir pareiza sekošos laukos:

$$K(1),\quad K(i),\quad K(\sqrt{2}),\quad K(\sqrt{-2}),\quad K(\sqrt{-3}),\quad K(\sqrt{5}).$$

Bet atceroties, ka vienkāršības dēļ nevienlīdzības (26) un (27) sašaurinājām, var domāt, ka arī vēl citos kvadrātiskos laukos ir lietojams Euklida algoritms. Tiešām, nākošā § noskaidrosim, ka jau minētiem laukiem var pievienot vēl

$$K(\sqrt{3}),\quad K(\sqrt{13}),\quad K(\sqrt{-7}),\quad K(\sqrt{-11}).$$

§ 79. Ģeometriska metode.

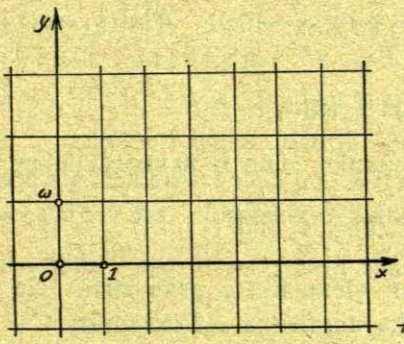
Pieņemsim, ka $K(\sqrt{n})$ ir **imāginārs lauks** ($n < 0$) ar minimālo bazi $(1, \omega)$, kur

$$\omega = \sqrt{n},\ \text{ja}\ n \not\equiv 4k+1,\ \text{bet}\ \omega = \frac{1+\sqrt{n}}{2},\ \text{ja}\ n \equiv 4k+1.$$

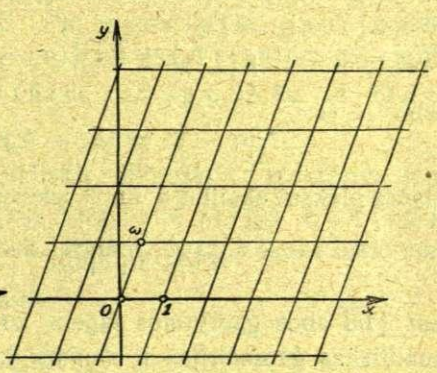
Tad lauka katrs skaitlis α ir izteicams formā

$$\alpha = a_0 + a_1\omega$$

ar racionāliem koeficientiem a_0, a_1. Speciālā gadījumā, kad α ir lauka vesels skaitlis, tad koeficienti a_0 un a_1 ir veseli racionāli skaitļi.



Zīm. 6.



Zīm. 7.

Ja lauka visus veselos skaitļus atzīmē Gausa komplekso skaitļu plāksnē, tad ar komplekso skaitļu saskai-

tīšanas teorēmu (parallēlogramma likumu) pierāda sekojošo. Visu plāksni var sadalīt kongruentos parallēlogrammos tā, ka lauka katrs veselais skaitlis sakrīt ar viena parallēlogramma virsotni, un otrādi — katra virsotne attēlo lauka veselu skaitli.

Lauka katrs cits skaitlis (kas nav vesels skaitlis) attēlojas ar punktu, kas atrodas viena parallēlogramma iekšpusē vai uz kontūra.

Visus parallēlogrammus kopīgi sauksim par lauka $K(\sqrt{n})$ **skaitļu tīklu**.

Zīmējumos 6. un 7. ir doti lauku $K(\sqrt{-2})$ un $K(\sqrt{-7})$ skaitļu tīkli.

Teorēma. Ja komplekso skaitļu plāksnē punkti A un B izteic imāginārā lauka $K(\sqrt{n})$ skaitļus

$$\alpha = a_0 + a_1\omega \quad \text{un} \quad \beta = b_0 + b_1\omega,$$

tad nogriežņa AB kvadrāts izteic normu $N(\alpha-\beta)$.

Pierādījumā apskatam sekojošus gadījumus.

1. gadījums. Ja

$$\omega = \sqrt{n} = i\sqrt{|n|},$$

tad

$$\alpha - \beta = (a_0 - b_0) + i\sqrt{|n|}\,(a_1 - b_1)$$

un

$$N(\alpha - \beta) = [(a_0 - b_0) + i\sqrt{|n|}\,(a_1 - b_1)][(a_0 - b_0) - i\sqrt{|n|}\,(a_1 - b_1)]$$

jeb

$$N(\alpha - \beta) = (a_0 - b_0)^2 + |n|(a_1 - b_1)^2.$$

Gausa plāksnē skaitļus α un β izteic punkti A un B ar koordinātām

$$A\,(a_0,\ a_1\sqrt{|n|}), \qquad B(b_0,\ b_1\sqrt{|n|}),$$

kur $\sqrt{|n|}$ abos gadījumos jāņem ar vienu un to pašu zīmi. No analītiskās ģeometrijas ir zināms, ka nogriežņa AB kvadrāts

$$(AB)^2 = (a_0 - b_0)^2 + |n|(a_1 - b_1)^2.$$

Tā tad

$$(AB)^2 = N(\alpha - \beta).$$

2. gadījumā, kad

$$\omega = \frac{1 + \sqrt{n}}{2} = \frac{1 + i\sqrt{|n|}}{2},$$

punktu A un B koordinātas ir

$$A\left(a_0 + \frac{a_1}{2},\ \frac{a_1}{2}\sqrt{|n|}\right), \qquad B\left(b_0 + \frac{b_1}{2},\ \frac{b_1}{2}\sqrt{|n|}\right).$$

Attāluma kvadrāts

$$(AB)^2 = \left(a_0 + \frac{a_1}{2} - b_0 - \frac{b_1}{2}\right)^2 + |n|\left(\frac{a_1}{2} - \frac{b_1}{2}\right)^2,$$

bet norma

$$N(\alpha-\beta)=\left[\left(a_0+\frac{a_1}{2}-b_0-\frac{b_1}{2}\right)+i\sqrt{|n|}\left(\frac{a_1}{2}-\frac{b_1}{2}\right)\right]\left[\left(a_0+\frac{a_1}{2}-b_0-\frac{b_1}{2}\right)-i\sqrt{|n|}\left(\frac{a_1}{2}-\frac{b_1}{2}\right)\right]$$

jeb

$$N(\alpha - \beta) = \left(a_0 + \frac{a_1}{2} - b_0 - \frac{b_1}{2}\right)^2 + |n|\left(\frac{a_1}{2} - \frac{b_1}{2}\right)^2.$$

Tā tad

$$(AB)^2 = N(\alpha - \beta).$$

Ar to teorēma pierādīta. Ja speciālā gadījumā liek $\beta = 0$, tad pierāda, ka skaitļa α norma izteic attāluma kvadrātu no punkta A līdz koordinātu sākumam.

Izlietojot lauka skaitļu grafisku attēlošanu, meklēsim tos imāginārus laukus $K(\sqrt{n})$, kur ir derīgs Euklida algoritms. Iepriekšējā § noskaidrojām, ka tādā laukā ikkatram skaitlim $\frac{\alpha}{\beta}$ var atrast veselu skaitli

$$\gamma = x + y\omega$$

tā, ka

$$N\left(\frac{\alpha}{\beta} - \gamma\right) < 1.$$

Ģeometriskā interpretācijā šo noteikumu izteic sekošā veidā. Lai imāginārā laukā $K(\sqrt{n})$ būtu derīgs Euklida algoritms, ir nepieciešami un pietiekoši, ka lauka skaitļu tīkla katrā parallēlogrammā ikviena punkta attālums līdz parallēlogramma tuvākai virsotnei būtu mazāks par 1.

Tā kā skaitļu tīkla visi parallēlogrammi ir vienlīdzīgi, tad no tiem pietiek izvēlēties vienu, piem parallēlogrammu ar virsotnēm

$$0,\ \omega,\ 1+\omega,\ 1.$$

Ja ap parallēlogramma virsotnēm velk riņķus ar radiju 1, tad ir vajadzīgs, lai parallēlogramma ikviens punkts atrastos vismaz vienā no šiem riņķiem. Bet parallēlogramma diagonāļu krustpunkts šo prasību izpilda tikai tad, ja īsākā diagonāle ir mazāka par 2. To prasot, dabū noteikumus sekojošos gadījumos.

1. Imāginārā laukā $K(\sqrt{n})$ ar $n \neq 4k+1$ skaitļu tīkla parallēlogramms ir taisnstūris ar diagonāli

$$d = \sqrt{1+|n|}.$$

Lai laukā derētu Euklida algoritms, ir nepieciešami (un ar zīmējumu saprotams, ka arī pietiekoši), ka

$$d < 2.$$

Tad dabū nosacījumu

$$1+|n| < 4 \quad \text{jeb} \quad |n| < 3,$$

Tādi imāginări lauki $K(\sqrt{n})$ ar $n \neq 4k+1$ ir:

$$K(\sqrt{-1}) \quad \text{un} \quad K(\sqrt{-2}).$$

2. Imāginārā laukā $K(\sqrt{n})$ ar $n = 4k+1$ parallēlogramma īsākā diagonāle ir punktu

$$\omega \text{ un } 1$$

attālums, kas vienlīdzīgs ar

$$d = \frac{1}{2}\sqrt{1+|n|}.$$

Tādēļ $d < 2$, tad, ja

$$1 + |n| < 16 \qquad \text{jeb} \qquad |n| < 15.$$

Tādi negātīvi skaitļi $n = 4k + 1$ ir:

$$-3, \quad -7, \quad -11.$$

Var ģeometriski pierādīt, ka šīm n nozīmēm atbilstošos laukos prasība $d < 2$ ir arī pietiekoša. Tādēļ ir pavisam 5 imāginārī lauki:

$$K(\sqrt{-1}), \quad K(\sqrt{-2}), \quad K(\sqrt{-3}), \quad K(\sqrt{-7}), \quad K(\sqrt{-11}),$$

kur der Euklida algoritms.

Reālos skaitļu laukos nevar dot tik vienkāršu ģeometrisku interpretāciju. Tādēļ te jautājumu par Euklida algoritma iespējamību apskatīsim ar analītisku metodi. Ja

$$\frac{\alpha}{\beta} = a + b\omega$$

ir lauka kaut kuŗš skaitlis, tad jāmeklē skaitlis

$$\gamma = x + y\omega$$

ar veseliem racionāliem skaitļiem x un y tā, lai būtu izpildīta prasība

$$\left| N\left(\frac{\alpha}{\beta} - \gamma\right) \right| < 1$$

jeb

$$|N[(a - x) + (b - y)\omega]| < 1.$$

Tagad jāatšķiŗ **divi gadījumi**: 1) $\omega = \sqrt{n}$ un 2) $\omega = \frac{1+\sqrt{n}}{2}$.

Pirmā gadījumā lauka pamatskaitlis ir $D = 4n$, un normu $N[(a - x) + (b - y)\omega]$ izteic ar

$$(x - a)^2 - \frac{D}{4}(y - b)^2.$$

Otrā gadījumā, kad $D = n$, izteic normu

$$N[(a - x) + (b - y)\omega]$$

ar

$$[(a-x)+\tfrac{1}{2}(b-y)+\tfrac{1}{2}(b-y)\sqrt{n}]\,[(a-x)+\tfrac{1}{2}(b-y)-\tfrac{1}{2}(b-y)\sqrt{n}]$$

jeb

$$[(a-x)+\tfrac{1}{2}(b-y)]^2-\tfrac{n}{4}(b-y)^2=[(x-a)+\tfrac{1}{2}(y-b)]^2-\tfrac{D}{4}(y-b)^2.$$

Redzam, ka abus gadījumus var apvienot, ja (28) vietā raksta

$$(29)\qquad \left|[(x-a)+\tfrac{r}{2}(y-b)]^2-\tfrac{D}{4}(y-b)^2\right|<1,$$

kur

$r=0$, ja $n\neq 4k+1$ un $r=1$, ja $n=4k+1$.

Ikkatrām a un b nozīmēm var atrast veselus skaitļus x, y tā, ka

$$|x-a|\leqslant\tfrac{1}{2}\quad\text{un}\quad|y-b|\leqslant\tfrac{1}{2}.$$

Tādēļ redzam, ka gadījumā, kad

$$D<16,$$

nevienlīdzības (29) kreisā puse ir mazāka par 1, bet ar $D>16$ tas katrreiz nav iespējams. Reāli lauki ar $D<16$ ir tikai četri sekojošie:

$$K(\sqrt{2}),\quad K(\sqrt{3}),\quad K(\sqrt{5}),\quad K(\sqrt{13}).$$

Ar to ir pierādīts, ka parastā aritmētika der tikai četros reālos un piecos imāginā ros kvadrātiskos laukos.

§ 80. Lauka pirmskaitļi.

Katrs veselais lauka skaitlis a dalās pats ar sevi un lauka vieniniekiem ε_k. Bez tam saprotams, ka a dalās arī ar visiem skaitļiem

$$\varepsilon_k\, a,$$

ko sauc par a asociētiem skaitļiem (tādu dažos laukos ir bezgala daudz). Bet šos skaitļus dalāmības gadījumos uzskata par līdzvērtīgiem ar a.

Definīcija. Par algebriska lauka pirmskaitli sauc lauka veselu skaitli, kas dalās tikai pats ar sevi un ar lauka vieniniekiem.

Katrā skaitļu laukā atrodas visi racionālie skaitļi un pirmskaitļi. Salikts racionāls skaitlis arī algebriskā laukā tāpat ir salikts skaitlis, bet arī racionāli pirmskaitļi var būt salikti algebriski skaitļi.

Piemērs. Gausa laukā $K(i)$ racionālais pirmskaitlis 2 ir salikts skaitlis, jo sadalāms divos faktoros

$$2 = (1 + i)\,(1 - i),$$

no kuŗiem neviens nav lauka vieninieks. Bet racionālais pirmskaitlis 7 arī laukā $K(i)$ ir pirmskaitlis. Tiešām, pieņemot, ka 7 sadalās veselu skaitļu reizinajumā

$$7 = (a + bi)\,(c + di),$$

kur neviens faktors $a+bi$ un $c+di$ nav lauka vieninieks, dabū sakaru

$$N(7) = N(a + bi)\,N(c + di) \quad \text{jeb} \quad 49 = (a^2 + b^2)\,(c^2 + d^2).$$

Tā kā

$$N(a + bi) \neq 1, \quad N(c + di) \neq 1,$$

tad

$$a^2 + b^2 = 7 \quad \text{un} \quad c^2 + d^2 = 7.$$

Bet neviens no abiem pēdējiem vienādojumiem nav iespējams, jo divu kvadrātu summa vienmēr ir formā $4k$, $4k + 1$ vai $4k + 2$; turpretim

$$7 = 4k - 1 \quad \text{ar} \quad k = 2.$$

Teorēma. Ja racionāls pirmskaitlis p kvadrātiskā laukā sadalās reizinātājos, tad laukā eksistē veseli skaitļi ar normas absolūto vērtību p.

Tiešām, ja

$$p = \alpha \cdot \beta$$

ir izteicams ar lauka veseliem skaitļiem α un β (ne α, ne β nav vieninieks), tad, uzrakstot normas, dabūjam vienlīdzību

$$p^2 = N(\alpha) \cdot N(\beta).$$

Tā tad

$$|N(\alpha)| = p \quad \text{un} \quad |N(\beta)| = p,$$

jo p ir pirmskaitlis.

Racionālo skaitļu teōrijā, izlietojot Euklida algoritmu, pierādījām pamatteōrēmu, ka katrs veselais skaitlis ir izteicāms ar pirmskaitļu reizinājumu un tikai vienā veidā. Tādēļ saprotams, ka kvadrātiskos laukos, kur ir derīgs Euklida algoritms (§ 79) ir pareiza arī šī pamatteōrēma, bet par citiem laukiem to nevar apgalvot. Vienkāršākie lauki, kur neder Euklida algoritms, ir

$$K(\sqrt{-5}), \quad K(\sqrt{6}).$$

Tiešām, laukā $K(\sqrt{-5})$ ir veseli skaitļi, ko var sadalīt pirmreizinātājos vairāk veidos*). Tāds piemērs ir skaitlis 21, ko var sadalīt sekošos veidos:

$$21 = 3 \cdot 7$$
$$21 = (4 + \sqrt{-5})\,(4 - \sqrt{-5})$$
$$21 = (1 + 2\sqrt{-5})\,(1 - 2\sqrt{-5}).$$

Ir viegli pierādāms, ka katrs no lietotiem faktoriem ir lauka $K(\sqrt{-5})$ pirmskaitlis (sk. § 2).

Lai novērstu nenoteiktību un dabūtu parasto dalāmības teōriju, Kummers ieveda t. s. ideālus skaitļus. Ar to palīdzību lauka katrs skaitlis ir sadalāms pirmreizinātājos tikai vienā veidā. Savu teōriju Kummers apskatīja laukā

$$K\left(\sqrt[n]{1}\right),$$

bet Dedekinds deva vispārinājumu, kas derīgs visos algebriskos laukos.

Kummera idejas labākai saprašanai apskatīsim vienu vēlākā laikā izdomātu interpretāciju ar racionāliem skaitļiem. Iedomāsimies būtnes, kas pazīst tikai veselos racionālos skaitļus formā $4n + 1$, t. i. skaitļus

(30) 1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, . . .

Tad šīm būtnēm skaitlis $45 = 9 \cdot 5$ ir salikts skaitlis, kamēr skaitļi, piem., 9, 21, 33, 77 ir pirmskaitļi, jo tie nav izsakāmi ar rindas (30) skaitļu reizinājumu. Bet nu rindā ir arī skaitļi, kas izsa-

*) Ir lauki, kur neder Euklida algoritms, bet tomēr lauka veselie skaitļi sadalās pirmreizinātājos tikai vienā veidā, piem., $K\sqrt{6}$.

kāmi ar pirmskaitļu reizinājumu vairāk veidos. Tādu piemēru dod skaitlis 693, ko sadala ar

$$693 = 21 \cdot 33 \quad \text{un} \quad 693 = 9 \cdot 77.$$

Tas liecina, ka rindas (30) skaitļiem neder parastie aritmētikas likumi. Bet, ja lieto „ideālus skaitļus"

$$4n - 1,$$

kas neatrodas rindā (30), tad rindas pirmskaitļi 9, 21, 33 un 77 ir sadalāmi. Ar šādiem ideāliem faktoriem rindas katrs skaitlis ir sadalāms reizinātājos tikai vienā veidā, piem. $693 = 3 \cdot 3 \cdot 7 \cdot 11$.

Šis piemērs liek domāt, ka gadījumā, ja kāds lauka skaitlis ir sadalāms pirmreizinātājos vairāk veidos, tad paši pirmreizinātāji ir sadalāmi ideālos faktoros, un tie ir attiecīgi vienlīdzīgi. Tā ja iepriekšējā piemērā ar

$$693 = 21 \cdot 33 = 9 \cdot 77$$

pieņem

$$21 = i_1 i_2, \quad 33 = j_1 j_2,$$

tad var domāt, ka

$$9 = i_1 j_1, \quad 77 = i_2 j_2.$$

Lai tas attaisnotos, starp citu ir vajadzīgs, lai „pirmskaitļiem" 21 un 9 būtu kopīgs ideāls dalītājs i_1. Ja liek

$$i_1 = 3, \quad i_2 = 7, \quad j_1 = 3, \quad j_2 = 11,$$

tad

$$693 = i_1 i_2 j_1 j_2.$$

Te visas vajadzīgās prasības ir izpildītas.

Uzdevumi.

1. Konstruēt lauku: $K(\sqrt{5})$, $K(\sqrt{6})$, $K(\sqrt{-10})$, $K(\sqrt{-13})$, $K(\sqrt{-15})$, $K(\sqrt{-21})$ minimālās bazes.

2. Noskaidrot, vai skaitļu pāŗus:

$$(2 + 3\sqrt{6},\quad 1 + \sqrt{6}),\quad (1 + \sqrt{6},\quad 7 + 6\sqrt{6}),$$
$$\left[\frac{1}{2}(3 + 7\sqrt{5}),\quad \frac{1}{2}(-1 - 3\sqrt{5})\right]$$

var uzskatīt par attiecigo lauku minimālām bazēm?

3. Konstruēt kvadrātisku lauku ar dotu pamatskaitli a. Noskaidrot, kad uzdevums iespējams.

4. Kādā kārtā, zinot vienādojuma

$$x^2 - ny^2 = a$$

vienu atrisinājumu (x_1, y_1) un vienādojuma

$$x^2 - ny^2 = b$$

atrisinājumu (x_2, y_2), var konstruēt atrisinājuma vienādojumam

$$x^2 - ny^2 = ab?$$

5. Atrast trigonālskaitļus, kas ir reizē arī kvadrātskaitļi.

6. Atrast dabisko skaitļu rindā divus blakusstāvošus skaitļus, no kuŗiem viens ir kvadrāts, otrs — trigonālskaitlis.

7. Vai ir iespējams taisnleņķa trijstūris, kuŗa visas trīs malas izsakāmas ar kvadrātskaitļiem?

8. Pierādīt, ka lauka $K(\sqrt{2})$ visi vienīnieki izsakāmi formā

$$\pm(1 + \sqrt{2})^n$$

ar veselu eksponentu n.

Izteikt tamlīdzīgā formā lauka $K(\sqrt{3})$ vieniniekus.

9. Atrast skaitļu $5 + 7i$ un $3 + 2i$ kopīgo dalītāju.

10. Ar 79. § ģeometrisko metodi pierādīt, ka laukā $K(\sqrt{-11})$ ir derīgs Euklida algoritms, bet laukā $K(\sqrt{-15})$ tas neder.

V. Ideālu teōrija.

§ 81. Ideālu definīcija.

Pirmā definīcija. Ja $a_1, a_2, \ldots, a_n$ un $\lambda_1, \lambda_2, \ldots, \lambda_n$ ir algebriska lauka veselie skaitļi, pie kam pirmie ir pastāvīgi, bet otrie mainās visos iespējamos veidos, tad sistēmu no visiem skaitļiem

$$\xi = \lambda_1 a_1 + \lambda_2 a_2 + \ldots + \lambda_n a_n$$

sauc par **lauka ideālu** un apzīmē ar

$$A = \{ a_1, a_2, \ldots, a_n \}.$$

No definīcijas seko, ka ideāla A katrs skaitlis ξ ir lauka vesels skaitlis; tā tad ideāls ir lauka noteikta veida veselu skaitļu sistēma.

Otrā definīcija. Par **ideālu** sauc lauka veselu skaitļu sistēmu ar tādu īpašību, ka reizē ar veseliem skaitļiem $\xi_1 + \xi_2$ sistēmā atrodas arī summa $\xi_1 + \xi_2$ (resp. starpība) un reizinājums $\lambda\xi_1$ ar lauka kaut kuŗu veselo skaitli λ.

Acīmredzams, ka abas definīcijas ir līdzvērtīgas.

Definīcija. Lauka divus ideālus A un B sauc par **identiskiem** tad, ja ideāla A katrs skaitlis ξ atrodas arī ideālā B, un ideālā B katrs skaitlis η atrodas arī ideālā A. Tad raksta:

$$A = B.$$

Teōrēma 1. Ja ideāla $A = \{ a_1, a_2, \ldots, a_n \}$ katrs elements α atrodas ideālā $B = \{ \beta_1, \beta_2, \ldots, \beta_m \}$ un

B katrs elements β ideālā A, tad ideāli A un B ir identiski, t. i. $A = B$.

Pierādījums. Ar teorēmas nosacījumu laukā atrodas veseli algebriski skaitļi λ_{ij} tā, ka var izteikt:

$$\begin{aligned}
\beta_1 &= \lambda_{11}a_1 + \lambda_{12}a_2 + \ldots + \lambda_{1n}a_n \\
\beta_2 &= \lambda_{21}a_1 + \lambda_{22}a_2 + \ldots + \lambda_{2n}a_n \\
&\ldots\ldots\ldots\ldots\ldots \\
\beta_m &= \lambda_{m1}a_1 + \lambda_{m2}a_2 + \ldots + \lambda_{mn}a_n .
\end{aligned}$$

Liekot šīs $\beta_1, \beta_2, \ldots, \beta_m$ nozīmes izteiksmē

$$\eta = \mu_1\beta_1 + \mu_2\beta_2 + \ldots + \mu_m\beta_m ,$$

kur η ir ideāla B kaut kurš skaitlis un $\mu_1, \mu_2, \ldots, \mu_m$ lauka veseli skaitļi, dabū izteiksmi

$$\eta = \lambda_1a_1 + \lambda_2a_2 + \ldots + \lambda_n a_n$$

ar lauka veseliem skaitļiem $\lambda_1, \lambda_2, \ldots, \lambda_n$. Tā norāda, ka η atrodas ideālā A. Tādā pat kārtā pierāda, ka ideāla A kaut kurš skaitlis ξ atrodas arī ideālā B.

Piemēri. 1. Lauka $K(\sqrt{-5})$ ideāli

$$A = \{2,\ 1 + \sqrt{-5}\} \quad \text{un} \quad B = \{2,\ 1 - \sqrt{-5}\}$$

ir identiski. Tiešām abiem ideāliem ir kopīgs elements 2, un nevienlīdzīgos elementus

$$\begin{aligned}
1 - \sqrt{-5} &= \lambda_1 . 2 + \lambda_2(1 + \sqrt{-5}) \\
1 + \sqrt{-5} &= \mu_1 . 2 + \mu_2(1 - \sqrt{-5})
\end{aligned}$$

var izteikt ar $\lambda_1 = \mu_1 = 1$, $\lambda_2 = \mu_2 = -1$, kas ir lauka veseli skaitļi.

2. Lauka $K(\sqrt{-5})$ ideāli

$$C = \{3,\ 1 + \sqrt{-5}\} \quad \text{un} \quad D = \{3,\ 1 - \sqrt{-5}\}$$

nav identiski.

Tiešām, pieņemot pretējo, varētu izteikt

$$1 + \sqrt{-5} = \lambda_1 . 3 + \lambda_2(1 - \sqrt{-5})$$

ar lauka veseliem skaitļiem λ_1, λ_2. Ja te liek

$$\lambda_1 = x_1 + y_1\sqrt{-5}, \qquad \lambda_2 = x_2 + y_2\sqrt{-5}$$

(x_1, x_2, y_1, y_2 veseli racionāli skaitļi) un salīdzina atsevišķi racionālos un irracionālos lielumus, tad dabū vienādojumu sistēmu

$$\begin{cases} 3x_1 + x_2 + 5y_2 = 1 \\ 3y_1 - x_2 + y_2 = 1. \end{cases}$$

Ja tās saskaita, tad seko formula

$$3(x_1 + y_1 + 2y_2) = 2,$$

kas nav iespējama, jo kreisā puse dalās ar 3, bet labā nedalās. Tā tad $A \neq B$.

Pēdējais piemērs rāda, ka visi lauka ideāli nav identiski.

Definīcija. Ideālu A, kuŗa visi skaitļi $\xi_1, \xi_2, \ldots$ dalās ar lauka vienu un to pašu skaitli α (tā tad $\xi_1 = \lambda_1 \alpha$, $\xi_2 = \lambda_2 \alpha, \ldots$ ar lauka veseliem skaitļiem $\lambda_1, \lambda_2, \ldots$), sauc par **galveno ideālu***) un apzīmē ar

$$A = \{\alpha\}.$$

Teorēma 2. Ja divi galvenie ideāli $\{\alpha\}$ uu $\{\beta\}$ ir identiski, tad α un β ir asociēti skaitļi.

Pierādījums. Ja

$$\{\alpha\} = \{\beta\},$$

tad

$$\beta = \lambda\alpha \quad \text{uu} \quad \alpha = \mu\beta,$$

kur λ un μ ir lauka veseli skaitļi. Vienlīdzības reizinot, dabū

$$\alpha\beta = \lambda\mu\alpha\beta.$$

Pēc saīsināšanas rodas

$$\lambda\mu = 1.$$

Tā tad λ un μ ir lauka vieninieki.

Pareiza arī apgrieztā teorēma.

Teorēma 3. Ja algebriskā laukā ir derīgs Euklida algoritms, tad šī lauka visi ideāli ir galvenie ideāli.

---

*) Dedekinda „*Hauptideal*".

Pierādījums. Pieņemsim, ka ideāls A satur elementus $\alpha, \beta, \gamma, \ldots$, un laukā ir derīgs Euklida algoritms. Tad ar to var atrast skaitļu α un β kopīgu dalītāju ρ un lauka veselus skaitļus ξ, η tā, ka pastāv formula (sk. § 4)

$$\rho = \alpha\xi + \beta\eta$$

Tā tad skaitlis ρ atrodas ideālā A. Ja tagad ar Euklida algoritmu savukārt atrod ρ un γ kopīgu dalītāju σ, tad arī σ atrodas ideālā A, un α, β, γ dalās ar σ. Tāpat turpinot var atrast ideāla A skaitli δ, ar ko dalās visi ideāla skaitļi. Tādēļ A identisks ar galveno ideālu $\{\delta\}$.

Sekas. Racionālo skaitļu laukā katrs ideāls ir galvenais ideāls $\{d\}$. Tas izteic visus veselos skaitļus, kas dalās ar skaitli d.

No galvenājiem ideāliem ievērojamākais ir **vieninieka ideāls**

$$I = \{1\},$$

kas satur lauka visus veselos skaitļus. Vēlāk redzēsim(§ 84), ka katrs ideāls „dalās" ar vieninieka ideālu.

Teorēma 4. Ja ideālā A atrodas skaitlis 1, tad A ir vieninieka ideāls I.

Tiešām, ideāla A visiem elementiem ir kopīgs dalītājs 1, kas atrodas ideālā. Tādēļ

$$A = \{1\} = I.$$

To pašu pierāda, ievērojot, ka reizē ar skaitli 1 ideālā A atrodas lauka ikkuŗš veselais skaitlis $\lambda = \lambda . 1$.

Teorēmu var vispārināt sekošā veidā. Ja ideālā A atrodas lauka vieninieks ε, tad $A = I$.

Piemērs. Noskaidrosim, ka lauka $K(\sqrt{-5})$ ideāls $C = \{3, 1 + \sqrt{-5}\}$ nav galvenais ideāls.

Tiešām, ja pieņemtu pretējo, tad skaitļiem 3 un $1 + \sqrt{-5}$ būtu kopīgs dalītājs

$$x + y\sqrt{-5}$$

ar veseliem racionaliem skaitļiem x, y.

Tad $N(3) = 9$ un $N(1 + \sqrt{-5}) = 6$ dalītos ar

$$N(x + y\sqrt{-5}) = x^2 + 5y^2.$$

Iespējami divi gadījumi:

$$N(x + y\sqrt{-5}) = 3 \quad \text{vai} \quad N(x + y\sqrt{-5}) = 1.$$

No tiem pirmais atkrīt, jo vienādojums

$$x^2 + 5y^2 = 3$$

nav atrisināms veselos racionālos skaitļos x, y. Bet arī otrais gadījums nav iespējams, jo tad C būtu identisks ar vienīnieka ideālu $I = \{1\}$ un saturētu lauka visus veselos skaitļus. Starp citu C saturētu arī skaitli 1, un varētu izteikt

$$1 = 3(x_1 + y_1\sqrt{-5}) + (1 + \sqrt{-5})(x_2 + y_2\sqrt{-5})$$

ar veseliem racionāliem skaitļiem x_1, x_2, y_1, y_2. Salīdzinot abās pusēs racionālos un irracionālos lielumus, dabūtu vienādojumu sistēmu

$$\begin{cases} 1 = 3x_1 + x_2 - 5y_2 \\ 0 = 3y_1 + x_2 + y_2. \end{cases}$$

Atņemot dabūtu neiespējamu formulu

$$1 = 3(x_1 - y_1 - 2y_2).$$

Šis piemērs rāda, ka lauka visi ideāli nav galvenie ideāli.

§ 82. Ideāla baze.

Ja $A = \{a_1, a_2, \ldots, a_n\}$ ir ideāls un elementiem $a_1, a_2 \ldots, a_n$ pievieno ideāla A skaitli $a = a_1\lambda_1 + a_2\lambda_2 + \ldots + a_n\lambda_n$ ar lauka veseliem skaitļiem $\lambda_1, \lambda_2, \ldots, \lambda_n$, tad dabū ar A identisku ideālu, t. i.

$$\{a_1, a_2, \ldots, a_n, a\} = \{a_1, a_2, \ldots, a_n\}.$$

To pierāda ar iepriekšējā § teorēmu. Šī formula rāda, ka vispārīgā gadījumā doto ideālu $\{a_1, a_2, \ldots, a_n, a\}$ var vienkāršot, samazinot elementu skaitu līdz minimālajam. Bet tā kā katrs ideāls nav galvenais, tad ir ideāli, ko nevar uzrakstīt ar mazāk kā divi elementiem.

Pierādīsim, ka kvadrātiskā laukā $K(\sqrt{n})$ katru ideālu A var izteikt ar divi elementiem. Pat vēl vairāk: var atrast ideāla divus elementus λ un μ, ko reizinot ar veseliem racionāliem skaitļiem un saskaitot dabū ideāla visus elementus. Tādus elementus λ, μ sauc par **ideāla bazi**. Pierādīsim tās eksistenci.

Izteicam ideāla A katru elementu a_1, a_2, a_3, ... ar lauka minimālo bazi $(1, \omega)$:

$$a_1 = a_1 + b_1\omega$$
$$a_2 = a_2 + b_2\omega$$
$$a_3 = a_3 + b_3\omega$$
$$\ldots\ldots\ldots$$

Pieņemam, ka skaitļu b_1, b_2 lielākais kopīgais dalītājs ir d. Tad atrodam veselus racionālus skaitļus x, y tā, ka pastāv sakars (sk. 4. §)

$$b_1x + b_2y = d_1.$$

Ar skaitļiem x, y noteicam ideāla A elementu

$$a_1x + a_2y = (a_1x + a_2y) + (b_1x + b_2y)\omega$$

jeb

$$c_1 + d_1\omega,$$

kur $c_1 = a_1x + a_2y$ ir vesels racionāls skaitlis.

Tādā pat kārtā ar skaitļu b_3, d_1 lielāko kopīgo dalītāju d_2 atrod, ka ideālā A atrodas skaitlis

$$c_2 + d_2\omega.$$

Te d_2 ir b_1, b_2, b_3 lielākais kopīgais dalītājs. Ja tāpat turpina, tad atrod ideāla A skaitli

$$c + d\omega,$$

kur d ir visu skaitļu b_k $(k = 1, 2, 3, \ldots)$ lielākais kopīgais dalītājs.

Reizē ar skaitli

$$a_k + b_k \omega$$

ideālā A atrodas arī šī skaitļa reizinājums ar saistīto skaitli

$$a_k + b_k \omega',$$

kas ir tā paša lauka vesels skaitlis. Tā tad katrā ideālā atrodas veseli racionāli skaitļi — ideāla elementu normas.

Ja ideāla A visi racionālie elementi ir a, b, c... (tie ir veseli skaitļi), tad tādiem pat slēdzieniem kā iepriekš pierāda, ka ideālā atrodas vesels racionāls skaitlis e, kas ir ideāla visu racionālo skaitļu lielākais kopīgais dalītājs.

Pierādīsim, ka skaitļi e un $c + d\omega$ ir ideāla baze.

Ievērojam, ka $\frac{b_k}{d}$ ir vesels skaitlis. Reizē ar elementu $a_k + b_k\omega$ ideālā A atrodas arī diference

$$(a_k + b_k\omega) - \frac{b_k}{d}(c + d\omega),$$

kas ir vesels racionāls skaitlis

$$a_k - \frac{b_k}{d} c.$$

Pēc pieņēmuma ideāla visi racionālie skaitļi dalās ar e. Tādēļ var izteikt

$$a_k - \frac{b_k}{d} c = eq$$

ar veselu racionālu skaitli q. Formula

$$a_k + b_k\omega = eq + \frac{b_k}{d}(c + d\omega),$$

rāda, ka skaitļi e, $c + d\omega$ tiešām ir ideāla A baze.

Lietojot atrasto bazi e, $c + d\omega$, ideālu A izteic ar

$$A = \{e,\ c + d\omega\},$$

un ideāla katru elementu var uzrakstīt formā

$$ex + (c + d\omega)y$$

ar veseliem racionāliem skaitļiem x, y.

Ir saprotams, ka arī liekot x un y vietā veselus lauka skaitļus dabū ideāla A elementus. Ja pirmoreiz izvēlas

$$x = \omega \quad \text{un} \quad y = 1,$$

tad dabū ideāla A skaitli

$$c + (d + e)\omega.$$

Redzam, ka $d + e$ dalās ar d. Tā tad arī e dalās ar d.

Ja otrreiz liek

$$x = 0, \quad y = \omega',$$

kur ω' ir ar ω saistītais algebriskais skaitlis, tad atrod ideāla elementu

$$a = c\omega' + d\omega\omega'.$$

Ievērojot, ka

$$\omega + \omega' = S(\omega) \quad \text{un} \quad \omega\omega' = N(\omega)$$

ir veseli racionāli skaitļi, pārveidojam

$$a = [d\,N(\omega) + c\,S(\omega)] - c\omega.$$

Te secinam, ka c dalās ar d.

Beidzot apzīmējam ideāla A bazi ar $(i, i_1 + i_2\omega)$ un rakstām

$$A = \{i, i_1 + i_2\omega\}.$$

Tad i, i_1, i_2 ir veseli racionāli skaitļi, pie kam i un i_1 dalās ar i_2. Šo bazi $(i, i_1 + i_2\omega)$ sauc par ideāla A **kanonisko bazi**.

Vēl piezīmējam, ka katram ideālam ir bezgala daudz bažu. Ja ideāla A viena baze ir (ω_1, ω_2), un sastāda skaitļus

$$(1) \qquad \begin{cases} \varphi_1 = a\omega_1 + b\omega_2 \\ \varphi_2 = c\omega_1 + d\omega_2 \end{cases}$$

ar veseliem racionāliem koeficientiem a, b, c, d, kas ierobežoti vienīgi ar nosacījumu

(2) $$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = \pm 1,$$

tad arī φ_1, φ_2 ir tā paša ideāla baze. Tiešām, no sistēmas (1) var izteikt ω_1, ω_2 ar φ_1, φ_2 sekojošā veidā

$$\omega_1 = \pm\begin{vmatrix} \varphi_1 & b \\ \varphi_2 & d \end{vmatrix} = \pm\,(d\varphi_1 - b\varphi_2), \quad \omega_2 = \pm\begin{vmatrix} a & \varphi_1 \\ c & \varphi_2 \end{vmatrix} = \pm(-c\varphi_1 + a\varphi_2)$$

ar tādu pat zīmi $\pm$ kā determinantam (2). Tad ideālā A katru skaitli

$$a = k_1\,\omega_1 + k_2\,\omega_2,$$

ko izteic ar bazi (ω_1, ω_2) un veseliem racionāliem koeficientiem k_1 un k_2, var izteikt arī ar φ_1, φ_2 un veseliem racionāliem koeficientiem sekojošā veidā

$$a = \pm\,k_1\,(d\varphi_1 - b\varphi_2) \pm k_2(-c\varphi_1 + a\varphi_2)$$

jeb

$$a = \pm\,(k_1 d - k_2 c)\varphi_1 \pm (-k_1 b + k_2 a)\varphi_2.$$

Tā tad arī φ_1, φ_2 ir ideāla baze.

§ 83. Ideālu reizināšana.

Definīcija. Par divu ideālu $A = \{a_1, a_2, \ldots, a_n\}$ un $B = \{\beta_1, \beta_2, \ldots, \beta_m\}$ reizinājumu sauc ideālu

$$C = \{a_1\beta_1,\ a_1\beta_2, \ldots, a_n\beta_m\},$$

kas satur abu doto ideālu elementu visus iespējamos reizinājumus

$$a_i\beta_j \quad (i = 1, 2, \ldots, n;\ j = 1, 2, \ldots, m).$$

Raksta:

$$C = A \cdot B.$$

Piemērs. Ideālu $A = \{3,\ 1 + \sqrt{-5}\}$, $B = \{3, 1 - \sqrt{-5}\}$ reizinājums ir

$$C = \{9,\ 3 + 3\sqrt{-5},\quad 3 - 3\sqrt{-5},\quad 6\}.$$

Ja ievēro, ka ideālā C atrodas skaitlis $9 - 6 = 3$ un ideāla visi elementi dalās ar 3, tad saprotams, ka C identisks ar galveno ideālu $\{3\}$. Tā tad $C = \{3\}$.

No definīcijas seko, ka ideālu reizināšanā der **kommutatīvā un asociatīvā īpašība:**

$$AB = BA \quad \text{un} \quad A(BC) = (AB)C.$$

Ja I ir vieninieka ideāls, tad

$$AI = A.$$

Iepriekšējā piemērā ievērojām, ka ideālu A un B reizinājums dod galveno ideālu. Pierādīsim, ka arī vispārīgā gadījumā katram ideālam A var atrast citu ideālu B tā, ka reizinājums AB ir galvenais ideāls.

Atsevišķā gadījumā, ja A ir galvenais ideāls $\{\alpha\}$, tad par B var ņemt kaut kuŗu galveno ideālu $\{\beta\}$. Šinī gadījumā teorēmas pareizība acīmredzama.

Vispārīgam pierādījumam izlietosim sekošu Hurvica **lemmu** (*Hurwitz*, 1895. g). Ja α_1, α_2, β_1, β_2 ir lauka $K(\bar{n})$ veseli algebriski skaitļi, pie kam

$$\alpha_1\beta_1, \quad \alpha_1\beta_2 + \alpha_2\beta_1 \quad \text{un} \quad \alpha_2\beta_2$$

dalās ar vienu un to pašu skaitli δ, tad arī atsevišķi

$$\alpha_1\beta_2 \quad \text{un} \quad \alpha_2\beta_1$$

dalās ar δ.

Pierādījums. Identitāti

$$(\alpha_1\beta_2)^2 - (\alpha_1\beta_2 + \alpha_2\beta_1)\,\alpha_1\beta_2 + \alpha_1\beta_1 \cdot \alpha_2\beta_2 = 0$$

dalām ar δ^2 un apzīmējam lauka veselus skaitļus

$$\frac{\alpha_1\beta_2 + \alpha_2\beta_1}{\delta} = \alpha, \quad \frac{\alpha_1\beta_1\,\alpha_2\beta_2}{\delta^2} = \beta.$$

Tad seko, ka skaitlis $\frac{\alpha_1\beta_2}{\delta}$ apmierina vienādojumu

$$\left(\frac{\alpha_1\beta_2}{\delta}\right)^2 + a\frac{\alpha_1\beta_2}{\delta} + \beta = 0$$

Tā kā vienādojuma koeficienti a un β ir veseli algebriski skaitļi, tad arī sakne $\frac{\alpha_1\beta_2}{\delta}$ ir vesels algebrisks skaitlis. Tā tad $\alpha_1\beta_2$ dalās ar δ. Līdzīgā kārtā pierāda, ka arī $\alpha_2\beta_1$ dalās ar δ

Definīcija. Ja ideālā $A = \{a_1, a_2, \ldots, a_n\}$ katra skaitļa a_i vietā liek tā saistīto algebrisko skaitli a_i', tad dabūto ideālu

$$A' = \{a_1', \quad a_2', \ldots, a_n'\}$$

sauc par A **saistīto ideālu***).

Pierādīsim, ka ideāla A reizinājums ar saistīto ideālu A' ir galvenais ideāls.

Pieņemsim, ka ideāla A baze ir a_1, a_2. Tad

$$A = \{a_1, a_2\}, \quad A' = \{a_1', a_2'\}$$

un

$$AA' = \{a_1a_1', \quad a_2'a_1, \quad a_1'a_2, \quad a_2a_2'\}.$$

Ideāla AA' elementi a_1a_1' un a_2a_2' ir veseli racionāli skaitļi, kā algebrisko skaitļu a_1, a_2 normas. Apzīmēsim tos attiecīgi ar

$$a_1a_1' = a, \quad a_2a_2' = c.$$

Arī $(a_1 + a_2)(a_1' + a_2')$ ir vesels racionāls skaitlis. Formula

$$(a_1 + a_2)(a_1' + a_2') = a + (a_1a_2' + a_1'a_2) + c,$$

rāda, ka arī $a_1a_2' + a_1'a_2$ ir vesels racionāls skaitlis, un var apzīmēt

$$a_1a_2' + a_1'a_2 = b.$$

---

*) Var viegli pierādīt, ka A' apmierina nosacījumus ideāla definīcijā (lp. 263.).

Pieņemsim, ka skaitļu a, b, c lielākais kopīgais dalītājs ir $d \geqslant 1$. Tad no iepriekšējās lemmas seko, ka ideāla AA' visi elementi

$$a_1a_1', \quad a_1a_2', \quad a_1'a_2, \quad a_2a_2'$$

dalās ar d. Ja vēl pierādīsim, ka d atrodas ideālā AA', tad būs pierādīts, ka AA' ir identisks ar galveno ideālu $\{d\}$.

Tā kā d ir a, b, c lielākais kopīgais dalītājs, tad var atrast (sk. § 7) veselus racionālus skaitļus x, y, z tā, ka

$$ax + by + cz = d.$$

Liekot a, b, c vietā izteiksmes ar „a“, dabū formulu

$$d = x \cdot a_1a_1' + y \cdot a_1a_2' + y \cdot a_1'a_2 + z \cdot a_2a_2',$$

kas rāda, ka d tiešām ir ideāla AA' elements. Tādēļ

$$AA' = \{d\},$$

un teorēma pierādīta.

Piezīme 1. Šo teorēmu pierāda arī bez Hurvica lemmas, ja izlieto ideāla kanonisko bazi $(i, i_1 + i_2\omega)$ un apskata atsevišķi katru no divi gadījumiem

$$\omega = \sqrt{n} \quad \text{un} \quad \omega = \frac{1 + \sqrt{n}}{2}.$$

2. Katram ideālam A var atrast bezgala daudz ideālu B tā, lai reizinājums AB būtu galvenais ideāls.

Tiešām, ja β ir lauka vesels skaitlis, A' ir A saistītais ideāls un par B izvēlas ideālu

$$A' \{\beta\},$$

tad AB ir divu galveno ideālu reizinājums

$$\{d\}\{\beta\} = \{d\beta\}.$$

Saīsināšanas teorēma. No ideālu reizinājumu vienlīdzības

$$AC = BC. \tag{3}$$

seko vienlīdzība

$$A = B.$$

Pierādījums. Pieņemam, ka

$$A = \{a_1, a_2, \ldots, a_n\} \quad \text{un} \quad B = \{\beta_1, \beta_2, \ldots, \beta_m\}.$$

Konstruējam ideālu M tā, lai reizinājums CM būtu galvenais ideāls $\{\mu\}$. Reizinot vienlīdzības (3) abas puses ar M, dabūjam formulu

$$A\{\mu\} = B\{\mu\}$$

jeb

$$\{a_1\mu, a_2\mu, \ldots, a_n\mu\} = \{\beta_1\mu, \beta_2\mu \ldots, \beta_m\mu\}.$$

No ideālu $A\{\mu\}$ un $B\{\mu\}$ vienlīdzības seko, ka šo ideālu elementi atrodas viens otrā. Tādēļ ar lauka veseliem skaitļiem „λ" var izteikt

$$a_i\,\mu = \lambda_1\beta_1\mu + \lambda_2\beta_2\mu + \ldots + \lambda_m\beta_m\mu.$$

Saīsinot šo formulu ar μ, dabū sakaru

$$a_i = \lambda_1\beta_1 + \lambda_2\beta_2 + \ldots + \lambda_m\beta_m,$$

kas izteic, ka ideāla A kaut kurš elements a_i atrodas ideālā B. Līdzīgā kārtā pierāda, ka arī ideāla B kaut kurš elements β_j atrodas ideālā A. Tā tad abi ideāli identiski, t. i.

$$A = B.$$

Teorēma. Ja $A = BC$, tad ideāla A katrs elements atrodas arī ideālā B (resp. C).

Tā tad vispārīgā gadījumā, kad $C \neq I$ faktors B ir plašāks nekā produkts BC.

Pierādījums. Pieņemsim, ka

$$B = \{\beta_1, \beta_2, \ldots, \beta_n\} \quad \text{un} \quad C = \{\gamma_1, \gamma_2, \ldots, \gamma_m\};$$

tad

$$A = \{\beta_1\gamma_1, \beta_1\gamma_2, \ldots, \beta_n\gamma_m\}.$$

Ar lauka veseliem skaitļiem „λ" ideāla A kaut kuŗš elements a ir izsakāms formā

$$a = \lambda_1\beta_1\gamma_1 + \lambda_2\beta_2\gamma_2 + \ldots + \lambda_{mn}\beta_n\gamma_m$$

jeb

$$a = \mu_1\beta_1 + \mu_2\beta_2 + \ldots + \mu_n\beta_n,$$

kur arī „μ" ir lauka veseli skaitļi. Pēdēja formula rāda, ka ideāla A katrs elements a atrodas arī ideālā B. Bet vispārīgā gadījumā nevar apgalvot, ka ideāla B katrs elements β atrastos arī ideālā A.

Apgrieztā teorēma. Ja ideāla A visi elementi atrodas ideālā B, tad var atrast ideālu C tā, ka

$$A = BC.$$

Pieņemsim, ka

$$A = \{a_1, a_2, \ldots, a_n\} \quad \text{un} \quad B = \{\beta_1, \beta_2, \ldots, \beta_m\}.$$

Tā kā A visi elementi atrodas ideālā B, tad var izteikt

$$B = \{a_1, a_2, \ldots, a_n, \quad \beta_1, \beta_2, \ldots, \beta_m\}.$$

Konstruējam ideālu

$$M = \{\mu_1, \mu_2, \ldots, \mu_k\}$$

tā, lai reizinājums BM būtu galvenais ideāls $\{\lambda\}$. Tad ideāla

$$BM = \{a_1\mu_1, a_1\mu_2, \ldots, a_n\mu_k, \quad \beta_1\mu_1, \beta_1\mu_2, \ldots, \beta_m\mu_k\}$$

visi elementi dalās ar λ. Arī elementi $a_1\mu_1, a_1\mu_2, \ldots, a_n\mu_k$ dalās ar λ, un ar tiem konstruētu ideālu var izteikt

$$\{a_1\mu_1, a_1\mu_2, \ldots, a_n\mu_k\} = \{\lambda\gamma_1, \lambda\gamma_2, \ldots, \lambda\gamma_{nk}\}$$

ar lauka veseliem skaitļiem $\gamma_1, \gamma_2, \ldots, \gamma_{nk}$. Ja definē ideālu

$$C = \{\gamma_1, \gamma_2, \ldots, \gamma_{nk}\},$$

tad pēdējo formulu var uzrakstīt ar

$$AM = C\{\lambda\}.$$

Reizinot abas puses ar B un saīsinot ar

$$BM = \{\lambda\},$$

dabū formulu

$$A = BC.$$

Ar to teorēma pierādīta.

§ 84. Ideālu dalāmiba.

Definīcija. Ideāls A dalās ar ideālu B tad, ja var atrast tādu ideālu C, ka

$$A = B \cdot C.$$

Ar iepriekšējā § pēdējo teorēmu definīciju var modificēt par šādu. Ideāls A dalās ar ideālu B tad, ja A visi elementi atrodas ideālā B.

Teorēma I. Katrs ideāls A dalās ar vieninieka ideālu $I = \{1\}$

Tas tādēļ, ka

$$A = A \cdot I$$

t. i. A katrs elements atrodas ideālā I.

Apgrieztā teorēma. Ja katrs ideāls dalās ar ideālu X, tad X ir vieninieka ideāls I.

Tiešām, ar teorēmas nosacījumu arī vieninieka ideāls I dalās ar X jeb I katrs elements, starp citu arī skaitlis 1, atrodas ideālā X. Tādēļ

$$X = I.$$

Definīcija. Par divu ideālu

$$A = \{a_1, a_2, \ldots, a_n\} \quad \text{un} \quad B = \{\beta_1, \beta_2 \ldots, \beta_m\}$$

kopīgo dalītāju sauc ideālu C, kas dala kā ideālu A, tā arī B.

Tādu ideālu C konstruē ar A un B elementiem, kam vēl pievieno lauka patvaļīgus (veselus) elementus $\gamma_1, \gamma_2, \ldots, \gamma_k$, t. i.

$$C = \{a_1, a_2, \ldots, a_n, \beta_1, \beta_2, \ldots \beta_m, \gamma_1, \gamma_2, \ldots, \gamma_k\}.$$

Ideālu

$$D = \{a_1, a_2, \ldots, a_n, \beta_1, \beta_2, \ldots, \beta_m\},$$

kas satur tikai A un B elementus, sauc par ideālu A, B **lielāko kopīgo dalītāju**. D dalās ar A un B katru kopīgo dalītāju C.

Ideālus A un B, kam nav cita kopīga dalītāja kā tikai vieninieka ideāls I, sauc par relātīviem pirmideāliem.

Piemērs. Ideāli

$$A = \{2, \ 1 + \sqrt{-5}\} \quad \text{un} \quad B = \{3, \ 1 + \sqrt{-5}\}$$

ir relātīvi pirmideāli. Tiešām, lielākais kopīgais dalītājs ir

$$D = \{2, 1 + \sqrt{-5}, 3\}.$$

Tā kā D satur elementu $1 = 3 - 2$, tad $D = I$.

Ideālu A, kas dalās tikai pats ar sevi un vieninieka ideālu sauc par **pirmideālu**.

Piemērs. Pierādīsim, ka $A = \{2, \ 1 + \sqrt{-5}\}$ ir pirmideāls.

Pieņemsim, ka A dalās ar ideālu B, kur $B \neq A$ un $B \neq I$. Tad katrs A elements atrodas ideālā B; tādēļ

$$B = \{2, \ 1 + \sqrt{-5}, \ \beta_1, \beta_2, \ldots\}.$$

Ideāla B katru elementu β_i izteic formā

$$\beta_i = a_i + b_i \sqrt{-5}$$

jeb

$$\beta_i = (a_i - b_i) + b_i (1 + \sqrt{-5})$$

ar veseliem racionāliem skaitļiem a_i, b_i.

Gadījumā, ja visas diferences $a_i - b_i$ ir pāru skaitļi $2k_i$, tad katrs β_i ir izsakāms ar elementu 2 un $1 + \sqrt{-5}$ lineāru kombināciju

$$\beta_i = 2k_i + b_i (1 + \sqrt{-5}).$$

Ideāls B reducējas uz $A = \{2, 1 + \sqrt{-5}\}$.

Turpretīm gadījumā, kad vismaz viena diference $a_i - b_i$ ir nepāru skaitlis $2k_i + 1$, tad ideālā B atrodas elements

$$\beta_i = 2k_i + b_i (1 + \sqrt{-5}) + 1.$$

Līdz ar to arī skaitlis 1, kā elementu β_i, 2 un $1 + \sqrt{-5}$ lineārs kombinējums:

$$1 = \beta_i - 2k_i - b_i (1 + \sqrt{-5}).$$

Tādēļ šinī gadījumā $B = I$ Redzam, ka katrs A dalītājs ir vai nu A, vai I. Tā tad A ir pirmideāls.

Šis piemērs norāda uz pirmideālu eksistenci.

Teorēma II. Laukā $K(\sqrt{n})$ ir tikai galīgs skaits tādu ideālu, kas satur veselu racionālu skaitli $a > 0$.

Pieņemsim, ka viens tāds ideāls ir

$$A = \{a_1, a_2, \ldots, a_n\}.$$

Tā elementus $a_1, a_2, \ldots, a_n$ izteicot ar lauka minimālo bazi $(1, \omega)$, dabūjam formulas:

$$a_1 = a_1 + b_1\omega, \quad a_2 = a_2 + b_2\omega, \ldots, \quad a_n = a_n + b_n\omega.$$

Visus veselos racionālos koeficientus a_i, b_i dalām ar a un paturam mazākos pozitīvos atlikumus r_i, s_i, kas var pieņemt vērtības

$$0, 1, 2, \ldots, a - 1.$$

Ar dalīšanu atrastos veselo racionālo skaitļu sakarus

$$a_i = aq_i + r_i, \quad b_i = ap_i + s_i$$

izlietojam pārveidojumam

$$a_i = a_i + b_i\,\omega = a(q_i + p_i\,\omega) + (r_i + s_i\,\omega)$$

jeb

$$a_i = a\gamma_i + \delta_i\,,$$

kur

$$\gamma_i = q_i + p_i\,\omega \quad \text{un} \quad \delta_i = r_i + s_i\,\omega$$

ir lauka veseli skaitļi. Ievērojot, ka a ir ideāla A elements, redzam, ka ideāli

$$A = \{\, a,\ a\gamma_1 + \delta_1,\ a\gamma_2 + \delta_2,\ \ldots,\ a\gamma_n + \delta_n \,\}$$

un

$$\{\, a,\ \delta_1,\ \delta_2,\ \ldots,\ \delta_n \,\}$$

ir identiski. Tādēļ var izteikt

$$A = \{\, a,\ \delta_1,\ \delta_2,\ \ldots,\ \delta_n \,\}. \tag{4}$$

Bet lauka dažādu veselu skaitļu

$$\delta_i = r_i + s_i\,\omega$$

skaits nav lielāks kā a^2. Tādēļ $\delta_1, \delta_2, \ldots, \delta_n$ izvēle ir ierobežota, un laukā atrodas tikai galīgs skaits ideālu (4), kas satur racionālu skaitli a.

Teorēma III. Katram ideālam ir galīgs dalītāju skaits.

Pierādījumam izlietosim 3. § atrasto īpašību, ka ideāla A reizinājums ar saistīto ideālu A' ir galvenais ideāls $\{a\}$. Te a vesels racionāls skaitlis.

Ja A dalās ar ideālu B, tad arī reizinājums

$$AA' = \{a\}$$

dalās ar B. Ideāls B satur ideāla $\{a\}$ katru elementu, arī racionālo skaitli a. Bet tādu ideālu B ir tikai galīgs skaits.

Teorēma IV. Ja B ir ideāla A īsts dalītājs $(B \neq A)$, tad ideālam B ir mazāk dalītāju kā ideālam A.

Tiešām, ja

$$A = BC,$$

tad A dalās pats ar sevi un ar B katru dalītāju. Bet B nedalās ar A, jo pretējā gadījumā, kad A dalās ar B un B dalās ar A, tad ideāli A un B ir identiski.

Tā tad ideālam A ir vismaz viens dalītājs (pats A) vairāk kā ideālam B.

§ 85. Pamatteorēma.

Teorēma I. Katrs ideāls A dalās vismaz ar vienu pirmideālu P.

Uzrakstīsim ideāla A visus dalītājus (to ir galīgs skaits m):

$$A_1 = I,\ A_2,\ A_3,\ \ldots,\ A_m = A.$$

Ar A_k apzīmēsim vienu no A dalītājiem, kam pašam ir vismazākais dalītāju skaits. Pierādīsim, ka tāds A_k ir pirmideāls.

Tiešām, ja ideālam A_k būtu kāds īsts dalītājs B, tad ideālam B būtu mazāk dalītāju kā ideālam A_k. Tad B būtu arī ideāla A dalītājs t. i. B vienlīdzīgs ar kādu A_i. Rastos pretruna nosacījumam par A_k dalītāju vismazāko skaitu.

Teorēma II. Katru ideālu A var izteikt ar pirmideālu reizinājumu.

Ja pieņem, ka A ir pirmideāls, tad teorēma ir pierādīta. Bet ja A nav pirmideāls, tad A dalās ar vienu pirmideālu P_1. Var izteikt

$$A = P_1 . A_1,$$

kur A_1 ir ideāls, kam mazāk dalītāju kā ideālam A. Tādā pat kārtā analizējot ideālu A_1, atrod pirmideālu P_2 un izteic

$$A_1 = P_2 A_2.$$

Tā tad

$$A = P_1 P_2 A_2.$$

Ja tāpat turpina un ievēro, ka katram ideālam A ir tikai galīgs dalītāju skaits, tad agri vai vēlu process izbeidzas ar tādu A_k, kas ir pirmideāls P_k. Dabū formulu

$$A = P_1 P_2 P_3 \ldots P_k .$$

Lemma. Ja A un B ir relātīvi pirmideāli (to lielākais kopīgais dalītājs ir vieninieka ideāls), tad A elementos var atrast tādu skaitli a un B elementos tādu β, ka

$$a + \beta = 1.$$

Pierādījums. Ja

$$A = \{ a_1, a_2, \ldots, a_n \} \text{ un } B = \{ \beta_1, \beta_2, \ldots, \beta_m \},$$

tad A un B lielākais kopīgais dalītājs ir

$$D = \{ a_1, a_2, \ldots, a_n, \beta_1, \beta_2, \ldots, \beta_m \}.$$

Tā kā $D = I$, tad D elementos atrodas skaitlis 1. Var izteikt

$$1 = (a_1\lambda_1 + a_2\lambda_2 + \ldots + a_n\lambda_n) + (\beta_1\mu_1 + \beta_2\mu_2 + \ldots + \beta_m\mu_m)$$

jeb

$$1 = a + \beta,$$

kur

$$a = a_1\lambda_1 + \ldots + a_n\lambda_n$$

ir ideāla A elements un

$$\beta = \beta_1\mu_1 + \ldots + \beta_m\mu_m$$

atrodas ideālā B.

Teorēma III. Ja divu ideālu reizinājums AB dalās ar pirmideālu P, tad vismaz viens no reizinātājiem dalās ar P.

Ja A dalītos ar P, tad teorēma būtu pierādīta. Pieņemam, ka A nedalās ar P. Tad A un P ir relātīvi pirmideāli. Var atrast šo ideālu tādus elementus a un π, kuŗu summa ir 1, t. i.

$$a + \pi = 1.$$

Reizinot ar ideāla B kaut kuŗu elementu β, dabūjam sakaru

$$\alpha\beta + \pi\beta = \beta.$$

Ievērojam, ka

$$\alpha\beta$$

ir ideāla AB elements, kas reizē ir P elements, jo AB dalās ar P. Bet arī

$$\pi\beta$$

ir P elements, un līdz ar to arī summa

$$\alpha\beta + \pi\beta = \beta$$

atrodas ideālā P. Tā tad ideāla B ikkatrs elements β atrodas ideālā P. Tādēļ B dalās ar P.

Vispārinājums. Ja ideālu reizinājums $A_1 A_2 \ldots A_n$ dalās ar pirmideālu P, tad vismaz viens no faktoriem dalās ar P.

To pierāda indukcijas ceļā, ja apzīmē

$$A_2 A_3 \ldots A_n = B,$$

un iepriekšējo teorēmu izlieto produktam $A_1 B$.

Sekas. Ja pirmideālu produkts $P_1 . P_2 \ldots P_n$ dalās ar pirmideālu P, tad vismaz viens no faktoriem $P_1, P_2, \ldots, P_n$ ir identisks ar P.

Dedekinda pamatteorēma. Katru ideālu A var izteikt ar pirmideālu reizinājumu un tikai vienā veidā.

Iespējamību A izteikt ar pirmideālu reizinājumu jau pierādījām. Tagad pieņemsim, ka ideālu A var izteikt ar pirmideālu reizinājumu divos dažādos veidos:

$$(5) \qquad A = P_1 P_2 \ldots P_n \text{ un } A = Q_1 Q_2 \ldots Q_m,$$

kur visi reizinātāji „P“ un „Q“ ir pirmideāli. Tad no vienlīdzības

$$P_1 P_2 \ldots P_n = Q_1 Q_2 \ldots Q_m$$

seko, ka pirmideālu reizinājums $P_1 P_2 \ldots P_n$ dalās ar pirmideālu Q_1. Tādēļ viens P_i, piem., P_1 ir identisks ar Q_1, un ar tiem var saīsināt. Paliek vienlīdzība

$$P_2 \ldots P_n = Q_2 \ldots Q_m,$$

no kuŗas tādā pat kārtā seko, piem. $P_2 = Q_2$, u. t. t. Katrs pirmideāls P_i ir identisks ar vienu Q_j un otrādi. Tādēļ arī pirmideālu skaits abos sadalījumos (5) ir vienlīdzīgs:

$$m = n.$$

Daži no ideāla A pirmreizinātājiem $P_1, P_2, \ldots, P_n$ var būt savā starpā vienlīdzīgi. Tādēļ definējot ideāla pakāpes:

$P^0 = I$, $P^1 = P$, $P^2 = P \cdot P$, $P^3 = P^2 \cdot P, \ldots$, $P^a = P^{a-1} P$ (a vesels pozitīvs skaitlis), katru ideālu A var viennozīmīgi izteikt ar dažādu pirmideālu $P_1, P_2, \ldots, P_k$ pakāpju reizinājumu

$$A = P_1^{a_1} P_2^{a_2} \ldots P_k^{a_k}. \tag{6}$$

Te $a_1, a_2, \ldots, a_k$ ir veseli pozitīvi skaitļi.

Šī formula rāda, ka ideālu aritmētika ir identiska ar parasto veselo skaitļu aritmētiku. Piemēram, ideāla A dalītāju skaitu, divu ideālu

$$A = P_1^{a_1} P_2^{a_2} \ldots P_k^{a_k} \text{ un } B = P_1^{b_1} P_2^{b_2} \ldots P_k^{b_k}$$

lielāko kopīgo dalītāju un mazāko kopīgo dalāmo noteic ar tādām pat formulām, kādas lieto veselo racionālo skaitļu aritmētikā.

§ 86. Ideālu klases.

Veselo racionālo skaitļu aritmētikā vesels skaitlis a dalās ar veselu skaitli b tad, ja a atrodas rindā

$$1b, 2b, 3b, 4b, \ldots,$$

ko var uzskatīt par ideālu $\{b\}$.

Līdzīgi tam ideālu aritmētikā saka, ka vesels algebrisks skaitlis α dalās ar ideālu A tad, ja α ir ideāla A elements.

Reizē ar skaitli α ideālā A atrodas arī galvenais ideāls $\{\alpha\}$, kas tā tad dalās ar A. Tādēļ nosacījums, ka skaitlis α dalās ar

ideālu A, ir līdzvērtīgs ar nosacījumu, ka ideāls $\{a\}$ dalās ar ideālu A.*)

Pieņemsim, ka skaitlis a dalās ar skaitli β. Tad no skaitļu vienlīdzības

$$a = \beta\gamma \qquad (\gamma \text{ vesels algebrisks skaitlis})$$

seko ideālu vienlīdzība

$$\{a\} = \{\beta\gamma\} \quad \text{jeb} \quad \{a\} = \{\beta\} \cdot \{\gamma\},$$

kas izteic sekošo. Ja skaitlis a dalās ar skaitli β, tad arī ideāls $\{a\}$ dalās ar ideālu $\{\beta\}$.

Tādā kārtā jautājumu par skaitļu dalāmību reducē uz jautājumu par ideālu dalāmību.

Ja skaitļu laukā nevar lietot Euklida algoritmu, tad skaitļu a un β kopīgo dalītāju noteic ar ideālu $\{a\}$ un $\{\beta\}$ kopīgo dalītāju $\{a, \beta\}$. Ja šis ideāls $\{a, \beta\}$ ir galvenais ideāls $\{\delta\}$, tad skaitli δ sauc par skaitļu a un β kopīgo dalītāju. Ja turpretim $\{a, \beta\}$ nav galvenais ideāls, tad dotajā laukā a un β kopīgo dalītāju nevar izteikt ar vienu algebrisku skaitli, bet tas ir Kummera ideālais skaitlis $\{a, \beta\}$.

Ja ideāls A ir galvenais ideāls $\{a\}$, tad tā visi elementi dalās ar lauka veselu skaitli a. Ja turpretim A nav galvenais ideāls, tad var pierādīt, ka ideāla A visiem elementiem ir kopīgs dalītājs ϑ, kas pieder augstākas kārtas skaitļu laukam.

Šo īpašību pierāda, lauka visus ideālus iedalot **ekvivalentu ideālu klasēs.**

Dedekinds ekvivalentus ideālus definē šādi. Ideāli

---

*) Ja skaitlis a dalās ar ideālu A, tad raksta ar kongruenci

$$a \equiv 0 \pmod{A}.$$

Divus skaitļus a un β sauc par kongruentiem attiecībā pret ideālu A tad, ja $a - \beta$ dalās ar A. Raksta:

$$a \equiv \beta \pmod{A} \text{ jeb } a - \beta \equiv 0 \pmod{A}.$$

No šīm definīcijām atvasina visu parasto kongruenču teoriju.

A un B ir ekvivalenti tad, ja var atrast tādu ideālu M, ka reizinājumi AM un BM ir galvenie ideāli. Raksta:

$$A \sim B.$$

No dēfinīcijas seko, ka visi galvenie ideāli ir ekvivalenti.

Piemērs: $A = \{3,\ 1 + \sqrt{-5}\}$, $B = \{3,\ 1 - \sqrt{-5}\}$. Ja izvēlas $M = \{2,\ 1 + \sqrt{-5}\}$, tad

$$AM = \{1 + \sqrt{-5}\},\quad BM = \{1 - \sqrt{-5}\}.$$

Tā tad $A \sim B$.

Ja $A \sim B$, tad var atrast ideālus: M, $\{\alpha\}$ un $\{\beta\}$ tā, ka

$$AM = \{\beta\} \text{ un } BM = \{\alpha\}.$$

Reizinot attiecīgi ar B un A, dabū formulas

$$ABM = B\{\beta\},\qquad ABM = A\{\alpha\},$$

no kā seko

$$A\{\alpha\} = B\{\beta\}.$$

Ar to ir pierādīta **teorēma**: ja A un B ir ekvivalenti ideāli, tad var atrast galvenos ideālus $\{\alpha\}$ un $\{\beta\}$ tā, ka reizinājumi $A\{\alpha\}$ un $B\{\beta\}$ ir identiski.

Var pierādīt arī **apgriezto teorēmu.**

Ekvivalentu ideālu īpašības.

1. Ja $A = B$, tad arī $A \sim B$.

Sekas $A \sim A$.

2. Ja $A \sim B$, tad $B \sim A$.

3. Ja $A \sim B$ un $B \sim C$, tad $A \sim C$.

4. Ja $A \sim B$, $C \sim D$, tad $AC \sim BD$.

Pierādīsim, piemēram, 3. īpašību. Ja $A \sim B$ un $B \sim C$, tad var atrast galvenos ideālus $\{\alpha\}$, $\{\beta\}$, $\{\gamma\}$, $\{\delta\}$ tā, ka pastāv sakari:

$$A\{\alpha\} = B\{\beta\}$$
$$B\{\gamma\} = C\{\delta\}.$$

Ja tos sareizina un pēc tam saīsina ar B, tad dabū formulu

$$A\{\alpha\gamma\} = C\{\beta\delta\},$$

kas izteic, ka $A \sim C$.

Tamlīdzīgi pierāda pārējās īpašības.

Ja lauka ideālus iedala klasēs tā, ka katrā klasē atrodas visi tie ideāli, kas ekvivalenti savā starpā, tad izrādās, ka ideālu klašu skaits h ir galīgs skaitlis. Pieņemsim, ka šīs klases ir

$$\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \ldots$$

un tās satur attiecīgi ideālus

$$A_1, A_2, A_3, \ldots, B_1, B_2, B_3, \ldots, C_1, C_2, C_3, \ldots$$

Ja reizinot vienu $\mathfrak{A}$ klases ideālu A_i ar $\mathfrak{B}$ klases ideālu B_j dabū reizinājumu

$$A_i B_j = C_k,$$

kas ir $\mathfrak{C}$ klases ideāls C_k, tad 4. īpašība rāda, ka katrs $\mathfrak{A}$ klases ideāls, reizināts ar kaut kuŗu $\mathfrak{B}$ klases ideālu, katrreiz dod $\mathfrak{C}$ klases ideālu.

Šī teorēma dod tiesību runāt par **klašu reizināšanu** un rakstīt simboliski

$$\mathfrak{A} . \mathfrak{B} = \mathfrak{C}.$$

Lauka visi galvenie ideāli atrodas vienā klasē, ko sauc par **galveno klasi** $\mathfrak{J}$. Klašu reizināšanā $\mathfrak{J}$ atbilst vienīnieka loma.

Ja sastāda ideālu klases $\mathfrak{A}$ pakāpes

$$\mathfrak{A}, \mathfrak{A}^2, \mathfrak{A}^3, \mathfrak{A}^4, \ldots$$

tad vispārīgā gadījumā, kad $\mathfrak{A} \neq \mathfrak{Z}$, katra sekojošā pakāpe izteic jaunu ideālu klasi. Bet tā kā ideālu klašu skaits ir galīgs, tad klases atkārtosies. Dabūsim formulu

$$\mathfrak{A}^m = \mathfrak{A}^{m+k} \qquad \text{jeb} \qquad \mathfrak{A}^m = \mathfrak{A}^m . \mathfrak{A}^k .$$

Ja ar $\mathfrak{A}^m$ saīsina (protams, iepriekš jānoskaidro, ka tāda saīsināšana ir likumīga), tad rezultāts

$$\mathfrak{A}^k = \mathfrak{Z}$$

rāda sekojošo. Katram ideālam

$$A = \{ a_1, a_2, \ldots, a_n \}$$

var atrast tādu kāpinātāju k, ka pakāpe A^k ir galvenais ideāls $\{ a \}$, t. i.

$$A^k = \{ a \}. \tag{7}$$

Var pierādīt, ka klašu skaits h dalās ar k, ja $k \neq 0$ ir vismazākais kāpinātājs ar minēto īpašību, t. i.

$$h = kq.$$

Ja formulu (7) kāpina ar veselo pozitīvo skaitli q un apzīmē

$$a^q = \omega,$$

tad seko rezultāts, ka katrs ideāls pakāpē h ir galvenais ideāls.

Pieņemsim, ka a ir ideāla A kaut kurš elements, tad a^h ir ideāla

$$A^h = \{ \omega \}$$

elements. Var izteikt

$$a^h = \omega\lambda,$$

kur α, ω un λ ir dotā lauka skaitļi. Velkot radikālu ar rādītāju h, dabūjam sakaru

$$\alpha = \sqrt[h]{\omega} \cdot \sqrt[h]{\lambda},$$

kas norāda sekojošo. Gadījumā, kad A nav galvenais ideāls, tad A katrs elements α dalās ar veselu algebrisku skaitli

$$\sqrt[h]{\omega},$$

kas pieder augstākas pakāpes skaitļu laukam.

Tādā kārtā katrs ideāls A noteic vienu veselu algebrisku skaitli, kas pieder tam pašam laukam, ja A ir galvenais ideāls, vai pretējā gadījumā — augstākas pakāpes skaitļu laukam.

Piezīme. Šajā nodaļā par ideālu teorijas elementiem daži pierādījumi vienkāršības dēļ attiecināti kvadrātiskiem skaitļu laukiem. Bet dabūtos rezultātus viegli var vispārināt jebkurā algebriskā skaitļu laukā.

Daži papildinājumi.

1. Lpp. 7., r. 16.

Ja $|a_n| = 1$, tad ar transformāciju $x = \xi + h$ (h — vesels skaitlis) var dabūt polinomu, kam brīvais loceklis nav $+1$ vai -1.

Otrs pierādījums. Ja a vesels skaitlis un $f(a)$ ir pirmskaitlis p, tad kongruencei $f(x) \equiv 0 \pmod{p}$ ir sakne $x \equiv a \pmod{p}$. Tas nozīmē, ka bezgala daudzām x nozīmēm

$$x_i = a + pt \qquad (t = 0, \pm 1, \pm 2, \ldots)$$

skaitļi $f(x_i)$ dalās ar p. Bet visi $f(x_i)$ nevar būt $+p$ vai $-p$.

2. Lpp. 42., r. 26.

Ir pazīstami 12 pilnīgie skaitļi. Tie atbilst eksponenta k nozīmēm:

$$k = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127.$$

3. Lpp. 151., r. 21.

Ja $c = 0$, ļtad no (4) seko: $d = 2$, $x_1 = -a$, $y_1 = b$. Ar šīm nozīmēm formula (2) dod $x = a$, $y = -b$. Bet

$$p = a^2 + (-b)^2 \qquad \text{un} \qquad p = (-a)^2 + b^2$$

nav skaitļa p dažādi sadalījumi.

4. Lpp. 242., r. 1.

Šis vienīnieks atšķiras no 75. § minētā fundāmentālā vienīnieka tad, ja laukā eksistē vienīnieki ar normu -1 (sk. piemēru lpp. 245.).

5. Lpp. 265.

3. teorēmai apgrieztā nav pareiza. Kvadrātiskos laukos $K(\sqrt{n})$ ar

$n = \ldots -67, -43, -19, -11, -7, -3, -2, -1, 2, 3, 5, 6, 7, 11, 14, 17, 19, 21, 22, 23, 29, 33, \ldots$

visi ideāli ir galvenie ideāli. Bet Euklida algoritms der tikai dažos laukos (sk. 79. §).

Saturs.

Otrā daļa.

Algebrisko skaitļu teorija.

Pamanītās iespieduma kļūdas.

Lapp.:	Rinda:	Iespiests:	Jābūt:
11	8. no apakšas	ex	ey
30	6. „ „	$d\|n$	$n\|d$
47	13. „ „	$q_i\, b$	$q_j\, a$
68	15. „ augšas		svītrot
86	16. „ „	p	$\frac{p}{2}$
104	5. „ apakšas	$+\frac{p}{2}<0$	$+\frac{p}{2}>0$
106	4. „ augšas	$xq - yp > 0$	$xq - yp + \frac{p}{2} > 0$
144	3. „ „	$z - it$	$z + it$
144	8. „ „	$ax + by$	$bx + ay$
144	5. „ apakšas	mod p	mod m
160	5. „ „	kaitļi	skaitļi
176	13. no augšas	$\alpha^i\, \beta^i$	$\alpha_i\, \beta_j$
180	15. „ „	γ_s	c_s
192	10. no apakšas	$a_{22}\, x_1$	$a_{22}\, x_2$
233	2. no augšas	n^2	ny^2