IV. Kvadratické zbytky, kvadratický zákon reciprocity

In: Karel Rychlík (author): Úvod do elementární teorie číselné. (Czech). Praha: Jednota čs. matematiků a fysiků, 1931. pp. 66–87.

Persistent URL: http://dml.cz/dmlcz/402941

IV. Kvadratické zbytky, kvadratický zákon reciprocity.

§ 41. Budeme uvažovati kongruenci

$$x^2 \equiv a \pmod{p}, \tag{1}$$

kdež a je číslo celé a p liché prvočíslo.

Je-li a dělitelno p, je kongruence (1) splněna pro každé $x \equiv 0 \pmod{p}$. Není-li a dělitelno p a existuje-li číslo celé, hovící kongruenci (1), nazveme a kvadratickým zbytkem (mod p), neexistuje-li pak takové číslo celé, nazveme a kvadratickým nezbytkem (mod p).

Předpokládejme tedy, že a není dělitelno p.

Lze snadno nahlédnouti, že, je-li kongruence (1) řešitelná, má právě dvě spolu (mod p) nekongruentní řešení. Je-li α kořen kongruence (1), tedy $\alpha^2 \equiv a \pmod{p}$, vyhovuje (1) též $x \equiv -\alpha \pmod{p}$, ježto je $(-\alpha)^2 \equiv \alpha^2 \equiv a \pmod{p}$. α a $-\alpha$ nejsou spolu kongruentní (mod p). Z $\alpha \equiv -\alpha \pmod{p}$ by plynulo $2\alpha \equiv 0 \pmod{p}$, $\alpha \equiv 0 \pmod{p}$, tedy i $a \equiv 0 \pmod{p}$ proti předpokladu o a.

Každý zbytek kvadratický je (mod p) kongruentní s jedním z čísel

$$1^2, 2^2, 3^2, \ldots, \left(\frac{p-1}{2}\right)^2.$$

Žádná dvě z těchto čísel nejsou spolu kongruentní (mod p). Označíme-li totiž dvě z těch čísel x, y, $x > y$, bylo by pak $x^2 - y^2 = (x+y)(x-y)$ dělitelno p, což není možno, ježto i $x+y$ i $x-y$ jsou čísla celá kladná $< p$.

Platí tedy věta:

Mezi čísly $1, 2, 3, \ldots, p-1$ *redukované soustavy zbytků (mod* p*) je právě* $\frac{1}{2}(p-1)$ *zbytků a stejný počet nezbytků spolu nekongruentních (mod* p*).*

Je-li g primitivní kořen (mod p), tvoří čísla $1, g, g^2, \ldots g^{p-2}$ redukovanou soustavu zbytků (mod p) (§ 35, str. 53). Čísla

$1, g^2, g^4, \ldots, g^{p-3}$ jsou kvadratické zbytky (mod p) spolu nekongruentní (mod p). Ježto je těchto čísel na počet $\frac{1}{2}(p-1)$, jsou jimi všechny kvadratické zbytky (mod p) spolu (mod p) nekongruentní vyčerpány. Čísla $g, g^3, g^5, \ldots, g^{p-2}$ jsou pak spolu (mod p) nekongruentní kvadratické nezbytky (mod p).

Je-li číslo a, nedělitelné p, kvadratickým zbytkem (mod p), existuje číslo celé α té vlastnosti, že pro ně platí $\alpha^2 \equiv a \pmod{p}$. α je opět nedělitelné p. I bude

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

tedy podle věty Fermatovy $a^{\frac{1}{2}(p-1)} \equiv 1 \pmod{p}$.

Kongruence $x^{\frac{1}{2}(p-1)} \equiv 1 \pmod{p}$ má za kořeny $\frac{1}{2}(p-1)$ spolu (mod p) nekongruentních kvadratických zbytků (mod p), a ježto je stupně $\frac{1}{2}(p-1)$, nemá podle věty z § 33 str. 49 jiných kořenů (mod p).

Podle věty Fermatovy má kongruence $x^{p-1} - 1 \equiv 0 \pmod{p}$ za kořeny všechna čísla celá nedělitelná p. Je však $x^{p-1} - 1 = (x^{\frac{1}{2}(p-1)} - 1)(x^{\frac{1}{2}(p-1)} + 1)$. Pro každé číslo celé nedělitelné p je tedy buď $x^{\frac{1}{2}(p-1)} \equiv 1 \pmod{p}$ anebo $x^{\frac{1}{2}(p-1)} \equiv -1 \pmod{p}$. Obě tyto kongruence nemohou býti splněny pro totéž číslo x, sice by jejich rozdíl 2 musil býti $\equiv 0 \pmod{p}$, což při $p > 2$ je nemožno. Kongruence $x^{\frac{1}{2}(p-1)} \equiv -1 \pmod{p}$ má tedy za kořeny kvadratické nezbytky.

Platí tedy věta (Eulerovo kriterium):

Číslo celé a nedělitelné p je kvadratický zbytek, je-li $a^{\frac{1}{2}(p-1)} \equiv 1$ (mod p), kvadratický nezbytek, je-li $a^{\frac{1}{2}(p-1)} \equiv -1$ (mod p).

§ 42. Legendre zavedl jednoduchý symbol na označení kvadratického charakteru čísla celého a nedělitelného prvočíslem $p > 2$, t. j. na označení, zda a je kvadratický zbytek nebo nezbytek (mod p). Klade

$$\left(\frac{a}{p}\right) = 1, \text{ je-li } a \text{ kvadratický zbytek,}$$

$$\left(\frac{a}{p}\right) = -1, \text{ je-li } a \text{ kvadratický nezbytek.}$$

I bude podle Eulerova kriteria $a^{\frac{1}{2}(p-1)} \equiv \left(\frac{a}{p}\right) \pmod{p}$.

$\left(\frac{a}{p}\right)$ je absolutně nejmenší zbytek (mod p) čísla $a^{\frac{1}{2}(p-1)}$.

Je patrno, že

$$\left(\frac{a'}{p}\right) = \left(\frac{a}{p}\right), \text{ je-li } a' \equiv a \pmod{p}.$$

Je-li totiž $a' \equiv a \pmod{p}$, je též $a'^{\frac{1}{2}(p-1)} \equiv a^{\frac{1}{2}(p-1)} \pmod{p}$ a tedy, ježto

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

též

$$\left(\frac{a'}{p}\right) \equiv \left(\frac{a}{p}\right) \pmod{p}.$$

Z této kongruence plyne ihned rovnost $\left(\frac{a'}{p}\right) = \left(\frac{a}{p}\right)$, ježto obě ta čísla jsou absolutně nejmenší zbytky (mod p).

Jsou-li a, a' celá čísla nedělitelná p, je

$$\left(\frac{aa'}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{a'}{p}\right).$$

Je totiž podle Eulerova kriteria

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

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

Násobením prvých dvou kongruencí dostaneme

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

a tedy

$$\left(\frac{aa'}{p}\right) \equiv \left(\frac{a}{p}\right)\left(\frac{a'}{p}\right) \pmod{p}.$$

Rovnost odtud plyne jako v předešlém případě.

Z definice Legendreova znaménka plyne ihned, že $\left(\frac{1}{p}\right) = 1$ a obecně $\left(\frac{a^2}{p}\right) = 1$ pro každé celé a nesoudělné s p.

Eulerovo kriterium poskytuje možnost určiti $\left(\frac{-1}{p}\right)$. Je

totiž

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

a ježto $(-1)^{\frac{1}{2}(p-1)} = \pm 1$, plyne z této kongruence rovnost $\left(\frac{-1}{p}\right) = (-1)^{\frac{1}{2}(p-1)}$.

Je tedy

$$\left(\frac{-1}{p}\right) = 1 \text{ pro } p \equiv 1 \pmod 4,$$

$$\left(\frac{-1}{p}\right) = -1 \text{ pro } p \equiv -1 \pmod 4.$$

§ 43. Budiž p libovolné celé číslo liché kladné a a celé číslo nesoudělné s p. Určeme absolutně nejmenší zbytky (mod p) čísel

$$1 \,.\, a,\ 2 \,.\, a,\ 3 \,.\, a,\ \ldots,\ \pi a,\ \pi = \tfrac{1}{2}(p-1).$$

Ty nechť jsou

$$\varepsilon_1 1',\ \varepsilon_2 2',\ \ldots,\ \varepsilon_\pi \pi',$$

kdež $1', 2', 3', \ldots, \pi'$ jsou absolutní hodnoty těchto zbytků a $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_\pi = \pm 1$. Mezi $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_\pi$ nechť se vyskytuje μ-krát -1. Je tedy

$$ia \equiv \varepsilon_i i' \pmod p,\quad i = 1, 2, 3, \ldots, \pi. \tag{1}$$

$1', 2', 3', \ldots, \pi'$ jsou, jak lze snadno dokázati, až snad na pořádek, rovna číslům $1, 2, 3, \ldots, \pi$. Nejsou totiž žádná dvě z těchto čísel sobě rovna. Z $i' = j'$, $i \neq j$ $(j = 1, 2, \ldots, \pi)$ by totiž plynulo na základě (1)

$$\varepsilon_i i \equiv \varepsilon_j j \pmod p,$$

což není možno, ježto čísla $-\frac{1}{2}(p-1), \ldots, -2, -1, 0, 1, 2, \ldots, \frac{1}{2}(p-1)$ tvoří úplnou soustavu zbytků (mod p), takže není možno, aby $i \equiv \pm j \pmod p$. Předpokládejme nejprve, že p je prvočíslo. Z (1) pak plyne znásobením

$$1 \,.\, 2 \,.\, 3 \ldots \pi a^\pi \equiv \varepsilon_1 \varepsilon_2 \ldots \varepsilon_\pi \,.\, 1' \,.\, 2' \ldots \pi' \pmod p$$

a tedy podle toho, co právě dokázáno, $a^\pi \equiv \varepsilon_1 . \varepsilon_2 \ldots \varepsilon_\pi \pmod p$. Ježto pak $a^\pi \equiv \left(\frac{a}{p}\right) \pmod p$, je $\left(\frac{a}{p}\right) \equiv \varepsilon_1 \varepsilon_2 \ldots \varepsilon_\pi \pmod p$. Odtud plyne $\left(\frac{a}{p}\right) = \varepsilon_1 \varepsilon_2 \ldots \varepsilon_\pi = (-1)^\mu$.

Platí tedy věta, která nazývá se Gaussovo lema:

Budiž a číslo celé nedělitelné lichým prvočíslem p. Pak $\left(\frac{a}{p}\right) = (-1)^{\mu}$, *kdež μ značí, kolik mezi absolutně nejmenšími zbytky čísel*

$$1 \,.\, a,\ 2 \,.\, a,\ 3 \,.\, a,\ \ldots,\ \pi \,.\, a,\quad \pi = \tfrac{1}{2}(p-1)$$

je záporných.

§ 44. Předpokládejme nyní, že p je číslo liché kladné, a číslo celé s ním nesoudělné. Podle Scheringa a Kroneckera budeme definovati symbol $\left(\frac{a}{p}\right)$ pomocí $(-1)^{\mu} = \varepsilon_1 \varepsilon_2 \ldots \varepsilon_{\pi}$. Udává tedy μ, kolik absolutně nejmenších zbytků (mod p) čísel

$$1 \,.\, a,\ 2 \,.\, a,\ 3 \,.\, a,\ \ldots,\ \pi a \tag{1}$$

je záporných, neboli kolik nejmenších kladných zbytků těchto čísel (mod p) je $> \frac{1}{2} p$. V případě, že je p prvočíslo, shoduje se $\left(\frac{a}{p}\right)$ na základě Gaussova lematu se symbolem Legendreovým.

Nejprve je patrno, že platí

$$\left(\frac{a}{p}\right) = \left(\frac{a'}{p}\right),$$

je-li $a' \equiv a \pmod{p}$.

Z $a' \equiv a \pmod{p}$ plyne, že a' je nesoudělné s p, takže, má-li význam $\left(\frac{a}{p}\right)$, má význam i $\left(\frac{a'}{p}\right)$. Rovnost $\left(\frac{a}{p}\right) = \left(\frac{a'}{p}\right)$ plyne pak ihned z té okolnosti, že čísla $1 \,.\, a', 2 \,.\, a', 3 \,.\, a', \ldots \pi \,.\, a'$ poskytují tytéž absolutně nejmenší zbytky (mod p) jako $1 \,.\, a$, $2 \,.\, a$, $3 \,.\, a, \ldots, \pi \,.\, a$.

Dále dokážeme, že, jsou-li a, a' čísla nesoudělná s p, tedy i aa' nesoudělné s p, je

$$\left(\frac{aa'}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{a'}{p}\right).$$

Abychom určili $\left(\frac{aa'}{p}\right)$, nutno určiti počet záporných, absolutně nejmenších zbytků (mod p) čísel

$$1 \,.\, aa',\ 2 \,.\, aa',\ 3 \,.\, aa',\ \ldots,\ \pi aa'. \tag{2}$$

Ježto $1 \,.\, a, 2 \,.\, a, \ldots, \pi a$ jsou (mod p) kongruentní resp. s čísly

$$\varepsilon_1 1',\ \varepsilon_2 2',\ \ldots,\ \varepsilon_{\pi} \pi',$$

budou čísla (2) poskytovati tytéž absolutně nejmenší zbytky (mod p) jako čísla

$$\varepsilon_1 1'a', \varepsilon_2 2'a', \ldots, \varepsilon_\pi \pi' a'.$$

Čísla $1', 2', \ldots, \pi'$ jsou až na pořádek rovna číslům $1, 2, 3, \ldots, \pi$. Jsou-li tedy $\varepsilon'_1 1'', \varepsilon'_2 2'', \ldots, \varepsilon'_\pi \pi''$ absolutně nejmenší zbytky (mod p) čísel $1'a', 2'a', \ldots, \pi' a'$, při čemž $\varepsilon'_i = \pm 1$, pak čísla $1'', 2'', \ldots, \pi''$ jsou až na pořádek rovna číslům $1, 2, \ldots, \pi$, a bude

$$\left(\frac{a'}{p}\right) = \varepsilon'_1 \varepsilon'_2, \ldots \varepsilon'_\pi.$$

Vidíme tudíž, že absolutně nejmenší zbytky čísel (2) jsou

$$\varepsilon_1 \varepsilon'_1 1'', \varepsilon_2 \varepsilon'_2 2'', \ldots, \varepsilon_\pi \varepsilon'_\pi \pi'',$$

takže

$$\left(\frac{aa'}{p}\right) = \varepsilon_1 \varepsilon'_1 \varepsilon_2 \varepsilon'_2 \ldots \varepsilon_\pi \varepsilon'_\pi = \left(\frac{a}{p}\right)\left(\frac{a'}{p}\right).$$

Je ihned patrno, že $\left(\frac{1}{p}\right) = 1$ a obecně $\left(\frac{a^2}{p}\right) = 1$ pro každé celé a nesoudělné s p.

Obraťme se nyní k určení $\left(\frac{-1}{p}\right)$ a $\left(\frac{2}{p}\right)$ (věty doplňkové k zákonu reciprocity).

Pro $a = -1$ je $\varepsilon_i = -1$ $(i = 1, 2, \ldots, \pi)$; i bude $\left(\frac{-1}{p}\right) = (-1)^\pi = (-1)^{\frac{1}{2}(p-1)}$ jako pro případ, že p je prvočíslo.

Pro $a = 2$ zní řada (1)

$$2, 4, 6, 8, \ldots, p - 1. \tag{3}$$

Jsou to nejmenší kladné zbytky (mod p). Je tedy $\left(\frac{2}{p}\right) = (-1)^\mu$, kdež μ udává, kolik z čísel (3) je $> \frac{1}{2} p$.

Budiž nejprve $p = 4k + 1$. Pak je řada (3):

$$2, 4, 6, \ldots, 2k \mid 2k + 2, 2k + 4, \ldots, 4k.$$

Členy této řady za čárkou | jsou $> \frac{1}{2} p$, jejich počet je k, tedy $\mu = k$.

$\left(\frac{2}{p}\right) = 1$, je-li k sudé $= 2h$, tedy $p = 8h + 1$,

$\left(\frac{2}{p}\right) = -1$, je-li k liché $2h - 1$, tedy $p = 8h - 3$.

Uvažujme nyní případ $p = 4k + 3$. Pak je řada (3)

$$2, 4, 6, \ldots, 2k \mid 2k + 2, 2k + 4, \ldots, 4k + 2$$

a počet zbytků $> \frac{1}{2}p$ je $\mu = k + 1$. Z toho plyne

$$\left(\frac{2}{p}\right) = 1, \text{ je-li } k \text{ liché } 2h - 1, \text{ tedy } p = 8h - 1,$$

$$\left(\frac{2}{p}\right) = -1, \text{ je-li } k \text{ sudé } 2h, \text{ tedy } p = 8h + 3.$$

Je tedy

$$\left(\frac{2}{p}\right) = 1 \text{ pro } p = 8h \pm 1,$$

$$\left(\frac{2}{p}\right) = -1 \text{ pro } p = 8h \pm 3.$$

Je však

pro $p = 8h \pm 1$, $\frac{1}{8}(p^2 - 1) = 8h^2 \pm 2h$ sudé,
pro $p = 8h \pm 3$, $\frac{1}{8}(p^2 - 1) = 8h^2 \pm 6h + 1$ liché,

takže

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

§ 45. Kvadratický zákon reciprocity.

Buďtež p, q dvě čísla celá lichá kladná spolu nesoudělná. Pak je

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

$$\text{t. j. } \left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$$

vyjma v případě, kdy $p \equiv q \equiv -1 \pmod 4$; *v tomto případě je*

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

Z celé řady důkazů snad je nejjednodušší důkaz Zellerův v modifikaci Frobeniově*); ten zde podáváme.

V rovnicích

$$\left(\frac{q}{p}\right) = (-1)^{\mu}, \quad \left(\frac{p}{q}\right) = (-1)^{\nu}$$

μ, ν mají tento význam:

*) Frobenius: Über das quadratische Reziprozitätsgesetz I, II. Sitzungsber. d. k. preuss. Akad. d. Wiss. 10, 18; 1914. K historii zákona reciprocity srov. Bachmann *3*. I.

μ značí počet násobků čísla q:

$$1 \,.\, q, 2 \,.\, q, 3 \,.\, q, \ldots, \frac{p-1}{2} q, \qquad (P)$$

jichž absolutně nejmenší zbytky (mod p) jsou záporné.

ν pak značí počet násobků čísla p:

$$1 \,.\, p, 2 \,.\, p, 3 \,.\, p, \ldots, \frac{q-1}{2} p, \qquad (Q)$$

jichž absolutně nejmenší zbytky (mod q) jsou záporné. Dlužno dokázati, že $\mu + \nu \equiv \frac{1}{2}(p-1) \,.\, \frac{1}{2}(q-1) \pmod 2$.

Budiž x proměnná, která může nabývati hodnot

$$1, 2, 3, \ldots, \tfrac{1}{2}(p-1). \qquad (x)$$

a y proměnná nabývající hodnot

$$1, 2, 3, \ldots, \tfrac{1}{2}(q-1). \qquad (y)$$

Čísla z řady (P) lze psáti ve tvaru qx a čísla z řady (Q) ve tvaru py. Absolutně nejmenší zbytek čísla $qx \pmod p$ je $qx - pm$, zvolíme-li m tak, že tento rozdíl je mezi $-\frac{1}{2}p$ a $\frac{1}{2}p$. Ke každému x lze zvoliti m podle § 2 str. 9 jediným způsobem. Udává tedy μ, kolikrát bude při tom $-\frac{1}{2}p < qx - pm < 0$. Zde neodpovídá každé z $\frac{1}{2}(p-1)$ hodnot x hodnota m, nýbrž jen μ hodnotám x odpovídá jisté m a to každé z oněch hodnot x jediné m. Pro takové m je $0 < qx < pm < qx + \frac{1}{2}p < \frac{1}{2}pq + \frac{1}{2}p$, t. j. $0 < m < \frac{1}{2}(q+1)$; m je tedy omezeno na řadu (y). Lze tedy místo m psáti y a říci: μ udává, pro kolik dvojic (x, y), při nichž x je z řady (x), y z řady (y), platí $-\frac{1}{2}p < qx - py < 0$, t. j. $0 < py - qx < \frac{1}{2}p$. Podobně bude ν udávati, pro kolik dvojic (x, y), při nichž x je z řady (x), y z řady (y), platí $-\frac{1}{2}q < py - qx < 0$. Všech možných dvojic (x, y) je na počet $\varrho = \frac{1}{2}(p-1) \,.\, \frac{1}{2}(q-1)$, je-li x omezeno na hodnoty z (x) a y na hodnoty z (y). Pro každou z těchto ϱ dvojic je buď

	I	$\frac{1}{2}p < py - qx$,
neb	II	$0 < py - qx < \frac{1}{2}p$,
neb	III	$-\frac{1}{2}q < py - qx < 0$,
nebo konečně	IV	$py - qx < -\frac{1}{2}q$.

Pro žádnou dvojici není

$$py - qx = 0.$$

Podmínce I nechť vyhovuje δ, podmínce IV δ' dvojic. Pak je

$$\varrho = \mu + \nu + \delta + \delta'.$$

Je však

$$\delta' = \delta.$$

neboť substitucemi

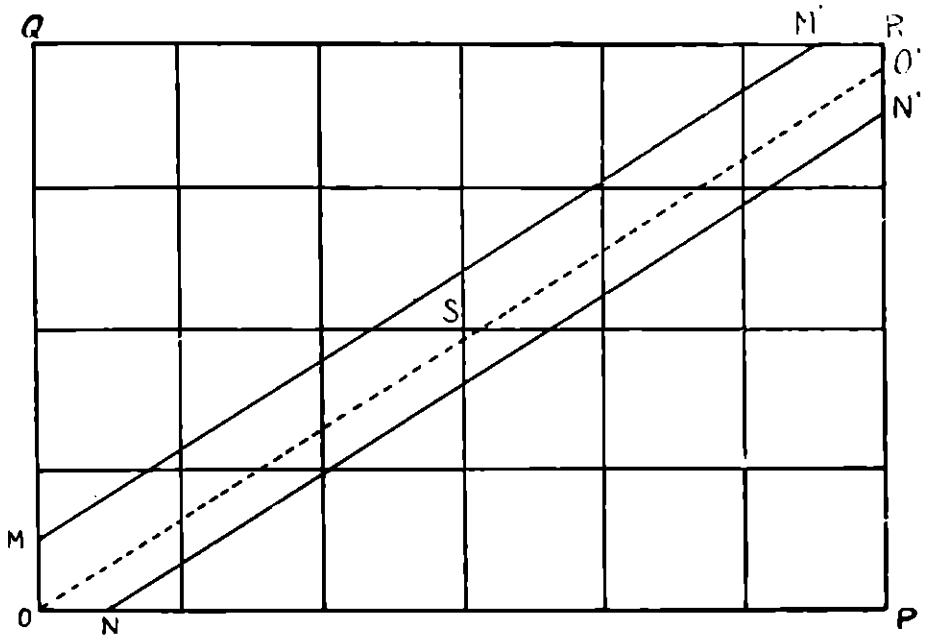
$$x = \tfrac{1}{2}(p+1) - x', \quad y = \tfrac{1}{2}(q+1) - y' \qquad (S)$$

přejde I ve IV, a probíhá-li x hodnoty (x), probíhá x' tytéž hodnoty (x). Stejně, probíhá-li y hodnoty (y), probíhá i y' hodnoty (y). Je tedy skutečně $\delta' = \delta$, t. j.

$$\varrho \equiv \mu + \nu \pmod 2$$

a konečně

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



Geometrický význam těchto úsudků je jasný. (Obrazec je proveden pro $p = 11$, $q = 7$.) R má souřadnice $\frac{1}{2}(p+1)$, $\frac{1}{2}(q+1)$. M, M', N, N' jsou středy stran příslušných čtverců. Spolu rovnoběžné přímky OO', MM', NN' mají rovnice

$$py = qx,\ py = qx + \tfrac{1}{2}p,\ py = qx - \tfrac{1}{2}q.$$

Substitucí (S) jsou si přiřazeny body ležící souměrně vzhledem ke středu S obdélníku $OPRQ$. S má souřadnice $\frac{1}{4}(p+1), \frac{1}{4}(q+1)$. Uvnitř obdélníku $OPRQ$ leží ϱ bodů mřížových (t. j. bodů, jejichž souřadnice x, y jsou čísla celá), μ jich leží mezi OO' a MM', ν mezi OO' a NN'. Připadne-li δ bodů na trojúhelník $MM'Q$, připadne jich na trojúhelník $NN'P$ symetrický vzhledem ke středu S stejný počet. Je tedy

$$\varrho = \mu + \nu + 2\delta.$$

Lze však souditi též takto:

Podle II a III je $\mu + \nu$ počet hodnot x, y hovících podmínkám

$$-\tfrac{1}{2}q < py - qx < \tfrac{1}{2}p. \qquad (*)$$

Tyto přejdou substitucí (S) samy v sebe. Patří-li (x, y) k oněm $\mu + \nu$ párům splňujícím (*), patří k nim i (x', y'). Je tedy $\mu + \nu$ sudé vyjma v případě, že

$$x = x' = \tfrac{1}{4}(p + 1), \quad y = y' = \tfrac{1}{4}(q + 1)$$

jsou čísla celá, t. j. kdy $p \equiv q \equiv -1 \pmod 4$. Jen v tomto případě je $\mu + \nu$ liché.

Leží-li bod (x, y) v proužku obdélníku $OPRQ$ mezi MM' a NN' (v šestiúhelníku $ONN'RM'M$), leží bod (x', y'), symetrický vzhledem k S, tamtéž. Tento proužek (i body mřížové v něm obsažené) je totiž sám k sobě symetrický vzhledem k S. Je tedy počet $\mu + \nu$ mřížových bodů uvnitř proužku toho sudý, vyjma v případě, kdy střed souměrnosti $\frac{1}{4}(p + 1)$, $\frac{1}{4}(q + 1)$ je bod mřížový.

Dokážeme nyní platnost vztahu

$$\left(\frac{a}{p}\right)\left(\frac{a}{p'}\right) = \left(\frac{a}{pp'}\right), \qquad (1)$$

kdež p, p' značí čísla lichá kladná, a číslo celé nesoudělné s p i s p', tedy i s pp'.

Předpokládejme nejprve, že a je liché kladné. Pak je podle zákona reciprocity

$$\left(\frac{a}{p}\right) = (-1)^{\frac{1}{2}(p-1)\cdot\frac{1}{2}(a-1)}\left(\frac{p}{a}\right) \qquad (2)$$

$$\left(\frac{a}{p'}\right) = (-1)^{\frac{1}{2}(p'-1)\cdot\frac{1}{2}(a-1)}\left(\frac{p'}{a}\right) \qquad (3)$$

$$\left(\frac{a}{pp'}\right) = (-1)^{\frac{1}{2}(pp'-1)\cdot\frac{1}{2}(a-1)}\left(\frac{pp'}{a}\right).$$

Násobením (2) a (3) dostaneme

$$\left(\frac{a}{p}\right)\left(\frac{a}{p'}\right) = (-1)^{\frac{1}{2}(a-1)\left[\frac{1}{2}(p-1)+\frac{1}{2}(p'-1)\right]}\left(\frac{p}{a}\right)\left(\frac{p'}{a}\right) =$$

$$= (-1)^{\frac{1}{2}(a-1)\left[\frac{1}{2}(p-1)+\frac{1}{2}(p'-1)\right]}\left(\frac{pp'}{a}\right), \quad \text{podle § 44.}$$

Bude tedy platiti (1), bude-li

$$\tfrac{1}{2}(a-1)\,[\tfrac{1}{2}(p-1)+\tfrac{1}{2}(p'-1)] \equiv \tfrac{1}{2}(a-1)\,.\,\tfrac{1}{2}(pp'-1) \pmod 2. \quad (4)$$

Je však

$$pp' = [1+(p-1)]\,[1+(p'-1] \equiv 1+(p-1)+ \\ +(p'-1) \pmod 4.$$

Součin $(p-1)(p'-1)$ je totiž dělitelný 4 jako součin dvou čísel sudých. I je

$$\tfrac{1}{2}(pp'-1) \equiv \tfrac{1}{2}(p-1)+\tfrac{1}{2}(p'-1) \pmod 2.$$

Odtud pak ihned plyne (4).

Předpokládejme dále, že a je sudé, kladné. Pak $\bar{a} = a + pp'$ je liché kladné, takže platí pro $\bar{a}$ vzorec $\left(\frac{\bar{a}}{p}\right)\left(\frac{\bar{a}}{p'}\right) = \left(\frac{a}{pp'}\right)$.

Je však $\bar{a} \equiv a \pmod p$ i $(\mathrm{mod}\ p')$ i $(\mathrm{mod}\ pp')$, takže

$$\left(\frac{\bar{a}}{p}\right) = \left(\frac{a}{p}\right), \quad \left(\frac{\bar{a}}{p'}\right) = \left(\frac{a}{p'}\right), \quad \left(\frac{\bar{a}}{pp'}\right) = \left(\frac{a}{pp'}\right).$$

Platí tedy (1) i pro a.

Tak dokázali jsme (1) pro a kladné.

Budiž nyní a záporné. I lze určiti $\bar{a} \equiv a \pmod{pp'}$ tak, aby $\bar{a}$ bylo kladné. Pak bude $\bar{a} \equiv a$ též $(\mathrm{mod}\ p)$ a $(\mathrm{mod}\ p')$. Pro $\bar{a}$ platí (1), tedy i pro a.

Tím dokázáno (1) úplně.

Je-li p liché kladné číslo $p = p_1 p_2 \ldots p_\nu$, kdež $p_1, p_2, \ldots p_\nu$ jsou prvočísla lichá, bude pro a nesoudělné s p

$$\left(\frac{a}{p}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\ldots\left(\frac{a}{p_\nu}\right).$$

Takto definoval $\left(\frac{a}{p}\right)$ pro případ čísla složeného p Jacobi.

Buďtež p, q čísla lichá, kladná, spolu nesoudělná. Ze zákona reciprocity plyne

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

Dále je

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

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

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

ježto pak $-p-1 \equiv p+1 \pmod 4$, tedy

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

Jsou-li tedy p, q čísla lichá spolu nesoudělná, q kladné, p kladné neb záporné, je

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

§ 46. Obrátíme se nyní k úloze, určiti všechna čísla celá kladná lichá n taková, že při daném číslu m symbol $\left(\frac{m}{n}\right)$ má význam a platí

$$\left(\frac{m}{n}\right) = 1 \quad \text{neb} \quad \left(\frac{m}{n}\right) = -1.$$

Doplňovací věty řeší nám úlohu pro $m = -1$ a $m = 2$.

$\left(\frac{-1}{n}\right) = 1$ pro všechna čísla celá kladná tvaru $n = 4k+1$ (k celé),

$= -1$ pro všechna čísla celá kladná tvaru $n = 4k+3$.

$\left(\frac{2}{n}\right) = 1$ pro všechna čísla celá kladná tvaru $n = 8k+1, 8k+7$,

$\left(\frac{2}{n}\right) = -1$ pro všechna čísla celá kladná tvaru $n = 8k+3, 8k+5$.

Z toho plyne dále

$\left(\frac{-2}{n}\right) = 1$ pro všechna čísla celá kladná tvaru $n = 8k+1, 8k+3$,

$\left(\frac{-2}{n}\right) = -1$ pro všechna čísla celá kladná tvaru $n = 8k+5, 8k+7$.

Vidíme, že čísla celá n, pro něž -1 má určitý kvadratický charakter, tvoří jednu posloupnost aritmetickou, číslo n, pro něž ± 2 má určitý kvadratický charakter, tvoří dvě posloupnosti aritmetické.

Dokážeme, že obecně všechna čísla celá n, pro něž $\left(\frac{m}{n}\right)$ má jednu z hodnot $+1$ neb -1, tvoří několik aritmetických postoupností.

Celé číslo m, které může býti kladné neb záporné, sudé neb liché, lze psáti ve tvaru

$$m = 2^c r s^2,$$

kdež $c=0$ neb 1, r je číslo celé liché nedělitelné čtvercem žádného prvočísla, tedy součin lichých mezi sebou různých prvočísel s kladným neb záporným znaménkem neb ± 1, s je číslo celé kladné.

Pak je

$$\left(\frac{m}{n}\right) = \left(\frac{2^c r s^2}{n}\right) = \left(\frac{2^c r}{n}\right).$$

Lze se tedy omeziti na případ

$$m = 2^c r$$

a o r lze předpokládati, že není $= 1$ ani -1, ježto pak bychom přišli k některému z případů již projednaných $m = \pm 1, \pm 2$; r je tedy součin lichých mezi sebou různých prvočísel s kladným neb záporným znaménkem.

Pak dostaneme

$$\left(\frac{m}{n}\right) = \left(\frac{2^c r}{n}\right) = \left(\frac{2}{n}\right)^c \left(\frac{r}{n}\right) = (-1)^{\frac{1}{8}c(n^2-1)} (-1)^{\frac{1}{2}(n-1)\cdot\frac{1}{2}(r-1)} \left(\frac{n}{r}\right).$$

Položme

$$(-1)^{\frac{1}{2}(r-1)} = \delta, \quad (-1)^c = \varepsilon.$$

Pak bude

$\delta = \quad 1$ pro $r \equiv 1 \pmod 4$, $\quad \varepsilon = \quad 1$ pro $c = 0$,
$\delta = -1$ pro $r \equiv 3 \pmod 4$, $\quad \varepsilon = -1$ pro $c = 1$.

I dostaneme

$$\left(\frac{m}{n}\right) = \delta^{\frac{1}{2}(n-1)} \varepsilon^{\frac{1}{8}(n^2-1)} \left(\frac{n}{r}\right). \qquad (*)$$

Na základě tohoto vzorce bude míti $\left(\frac{m}{n}\right)$ tutéž hodnotu pro čísla n patřící do téže třídy (mod $8r$), při $\varepsilon = 1$ již pro čísla n patřící do téže třídy (mod $4r$), a je-li též $\delta = 1$, dokonce pro čísla n patřící do téže třídy (mod $2r$). Stačí tedy uvažovati n jen z redukované soustavy zbytků podle uvedených modulů.

Označíme v redukované soustavě zbytků (mod $2r$) čísla n, pro něž $\left(\frac{n}{r}\right) = 1$, písmenem a, čísla, pro něž $\left(\frac{n}{r}\right) = -1$,

písmenem b. Počet čísel a je roven počtu čísel b. Dokážeme nejprve, že existuje aspoň jedno číslo b.

Budiž p prvočíslo obsažené v r, tedy $|r| = pr'$, r' číslo celé kladné nedělitelné p, β nezbytek (mod p). Určeme b_0 kongruencemi

$$b_0 \equiv \beta \pmod{p}, \quad b_0 \equiv 1 \pmod{r'}.$$

Pak je

$$\left(\frac{b_0}{|r|}\right) = \left(\frac{b_0}{pr'}\right) = \left(\frac{\beta}{p}\right)\left(\frac{1}{r'}\right) = -1,$$

takže b_0 je skutečně číslo druhu b.

O b_0 lze nad to předpokládati, že je liché. Kdyby totiž bylo sudé, byla by $b_0 + |r|$ liché a o $b_0 + |r|$ by platilo $\left(\frac{b_0 + |r|}{|r|}\right) = \left(\frac{b_0}{|r|}\right) = -1$. Pak je b_0 nesoudělné s $2r$. Násobme b_0 každé číslo z množství čísel a i b, t. j. z redukované soustavy zbytků (mod $2r$). Dostaneme zase redukovanou soustavu zbytků (mod $2r$). I dostáváme

$$\sum\left(\frac{n}{|r|}\right) = \sum\left(\frac{b_0 n}{|r|}\right) = \left(\frac{b_0}{|r|}\right)\sum\left(\frac{n}{|r|}\right) = -\sum\left(\frac{n}{|r|}\right),$$

t. j.

$$\sum\left(\frac{n}{|r|}\right) = 0,$$

kdež Σ se vztahuje na redukovanou soustavu zbytků (mod $2r$).

Avšak

$$\sum\left(\frac{n}{|r|}\right) = \sum_a\left(\frac{a}{|r|}\right) + \sum_b\left(\frac{b}{|r|}\right) = 0,$$

takže počet čísel druhu a je roven počtu čísel druhu b.

Je-li nejprve $\delta = 1$, $\varepsilon = 1$, tedy $m \equiv 1 \pmod 4$, bude podle (*)

$$\left(\frac{m}{n}\right) = \quad 1 \quad \text{pro } n \equiv a \pmod{2r}$$

$$\left(\frac{m}{n}\right) = -1 \quad \text{pro } n \equiv b \pmod{2r}.$$

Lichá čísla n, pro něž $\left(\frac{m}{n}\right) = 1$ neb -1, tvoří $\frac{1}{2}\varphi(2r) = \frac{1}{2}\varphi(r) = \frac{1}{2}\varphi(m)$ aritmetických posloupností o diferenci $2r = 2m$.

Je-li za druhé $\delta = -1$, $\varepsilon = 1$, tedy $m \equiv 3 \pmod 4$, bude

$$\left(\frac{m}{n}\right) = 1, \text{ je-li buď } n \equiv 1 \pmod 4, \quad n \equiv a \pmod r,$$
$$\text{neb } n \equiv 3 \pmod 4, \quad n \equiv b \pmod r,$$

$$\left(\frac{m}{n}\right) = -1, \text{ je-li buď } n \equiv 3 \pmod 4, \quad n \equiv a \pmod r,$$
$$\text{neb } n \equiv 1 \pmod 4, \quad n \equiv b \pmod r.$$

Lichá n, pro něž $\left(\frac{m}{n}\right)$ má hodnotu $+1$ neb -1, jsou čísla r jistých aritmetických posloupností, jichž je na počet $\frac{1}{2}\varphi(4r) = \frac{1}{2}\varphi(4m)$.

Je-li za třetí $\delta = 1$, $\varepsilon = -1$, tedy $m \equiv 2 \pmod 8$, bude

$$\left(\frac{m}{n}\right) = 1, \text{ je-li buď } n \equiv 1, 7 \pmod 8, \quad n \equiv a \pmod r,$$
$$\text{neb } n \equiv 3, 5 \pmod 8, \quad n \equiv b \pmod r,$$

$$\left(\frac{m}{n}\right) = -1, \text{ je-li buď } n \equiv 3, 5 \pmod 8, \quad n \equiv a \pmod r,$$
$$\text{neb } n \equiv 1, 7 \pmod 8, \quad n \equiv b \pmod r.$$

Je-li konečně za čtvrté $\delta = -1$, $\varepsilon = -1$, tedy $m \equiv 6 \pmod 8$, bude

$$\left(\frac{m}{n}\right) = 1, \quad \text{je-li buď } n \equiv 1, 3 \pmod 8, \quad n \equiv a \pmod r,$$
$$\text{neb } n \equiv 5, 7 \pmod 8, \quad n \equiv b \pmod r,$$

$$\left(\frac{m}{n}\right) = -1, \text{ je-li buď } n \equiv 5, 7 \pmod 8, \quad n \equiv a \pmod r,$$
$$\text{neb } n \equiv 1, 3 \pmod 8, \quad n \equiv b \pmod r.$$

Ve třetím a čtvrtém případě lichá n, pro něž $\left(\frac{m}{n}\right)$ má určitou hodnotu, tvoří aritmetické posloupnosti o diferenci $8r = 4m$, na počet $\frac{1}{2}\varphi(8r) = \frac{1}{2}\varphi(4m)$.

Je-li $\left(\frac{m}{p}\right) = 1$ pro prvočíslo p, je kongruence $t^2 - m \equiv 0 \pmod p$ řešitelná celým číslem t nedělitelným p. Lze snadno nahlédnouti, že kongruence $t^2 - m \equiv 0 \pmod p$ je řešitelná celým číslem t nedělitelným p tehdy a jen tehdy, existují-li celá čísla x, y nedělitelná p taková, že platí

$$x^2 - my^2 \equiv 0 \pmod p.$$

Z řešitelnosti $t^2 - m \equiv 0 \pmod p$ celým číslem t nedělitelným p plyne $x^2 - my^2 \equiv 0 \pmod p$, klademe-li $x = t$, $y = 1$. Je-li $x^2 - my^2 \equiv 0 \pmod p$, x, y čísla celá nedělitelná p, pak pro

$t \equiv x/y \pmod{p}$ (viz § 23 str. 34), což je číslo celé nedělitelné p, bude

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

Existují-li celá čísla x, y nedělitelná prvočíslem p taková, že platí $x^2 - my^2 \equiv 0 \pmod{p}$, říká se (podle Eulera a Legendrea), že p je dělitelem formy kvadratické $x^2 - my^2$. Jsou tedy prvočísla p, pro něž $\left(\frac{m}{p}\right) = 1$, dělitelé formy $x^2 - my^2$.

Budiž N celé číslo. Existují-li celá čísla x, y taková, že $N = x^2 - my^2$, říká se, že N se dá znázorniti formou $x^2 - my^2$. Znázornění je vlastní, jsou-li x, y čísla nesoudělná, nejsou-li nesoudělná, je znázornění nevlastní.

Je-li p prvočíslo obsažené v N, je podmínka nutná pro vlastní znázornění N formou $x^2 - my^2$, aby p bylo dělitelem formy $x^2 - my^2$.

Hledejme čísla celá n, pro něž $\left(\frac{5}{n}\right) = 1$.

Zde $m = 5$, $c = 0$, $r = 5$, $\delta = 1$, $\varepsilon = 1$, $m \equiv 1 \pmod 4$, (případ první). Redukovaná soustava zbytků mod $2m = 2r = 10$ je

$$1, 3, 7, 9.$$

Kvadratické zbytky jsou 1, 9, nezbytky 3, 7.

Je tedy

$\left(\frac{5}{n}\right) = 1$ pro $n \equiv 1, 9 \pmod{10}$, t. j. pro $n \equiv \pm 1 \pmod{10}$,

$\left(\frac{5}{n}\right) = -1$ pro $n \equiv 3, 7 \pmod{10}$, t. j. pro $n \equiv \pm 3 \pmod{10}$.

Dělitelé formy $x^2 - 5y^2$ jsou prvočísla tvaru $p = 10k \pm 1$, k číslo celé kladné.

Uvažujme nyní případ $m = -6$.

Zde $m = -6 = 2 \cdot -3$, $c = 1$, $r = -3$, $\delta = 1$, $\varepsilon = -1$, $m \equiv 2 \pmod 8$ (případ třetí).

Redukovaná soustava zbytků mod $2r$, t. j. mod 6, je 1, 5;

1 je zbytek (mod r), t. j. (mod 3),
5 je nezbytek (mod r), t. j. (mod 3).

Bude tedy

$$\left(\frac{-6}{n}\right) = 1 \text{ pro } n \equiv 1 \pmod 3, \equiv 1, 7 \pmod 8$$

$$n \equiv 5 \equiv 2 \pmod 3, \equiv 3, 5 \pmod 8$$

t. j. pro $n \equiv 1, 5, 7, 11 \pmod{24}$, a pro $n > 0$.*)

§ 47. Znázornění čísla celého formou kvadratickou lze užíti k rozhodnutí, zda číslo ono je prvočíslo neb číslo složené, a v tomto případě provésti rozklad v prvočinitele.

Uvažujme číslo

$$P_{13} = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30\,031 \ (\S\ 10).$$

Není dělitelno žádným kladným prvočíslem $\leqq 13$. Ježto pak $[\sqrt{30\,031}] = 173$, stačí uvažovati prvočísla $\geqq 17$ a $\leqq 173$.

Lze zjistiti, že $30\,031 = 174^2 - 5 \cdot 7^2$. Prvočinitelé čísla 30 031 budou tedy dělitelé formy $x^2 - 5y^2$, tedy prvočísla tvaru $10k \pm 1$.

V uvedených mezích leží tato prvočísla takového tvaru: 19, 29, 31, 41, 59, 61, 71, 79, 89, 101, 109, 131, 139, 149, 151.

Konečně možno uvážiti, že 30 031 je tvaru $4n - 1$ a má tedy aspoň jednoho prvočinitele tohoto tvaru. Zbývá tedy z uvedených prvočísel uvažovati jen prvočísla tvaru $4n - 1$:

19, 31, 59, 71, 79, 131, 139, 151.

30 031 prvočísly 19, 31 není dělitelno, 59 je však dělitelno. Dostaneme

$$30\,031 = 59 \cdot 509.$$

509 je také prvočíslo.

§ 48. Budeme se zabývati znázorněním prvočísel formami $x^2 + my^2$ pro kladné m v některých jednoduchých případech. Tu platí věta**):

Je-li nejmenší liché prvočíslo, pro které $-m$ je kvadratický zbytek (které tedy je dělitelem formy $x^2 + my^2$), znázornitelno formou $x^2 + my^2$, je každé prvočíslo, pro něž je $-m$ kvadratický zbytek, jediným způsobem touto formou znázornitelno.

---

*) Kraitchik *1.* I. str. 164—186 (errata *2.* II str. 180), *2.* I. str. 205—215 udává tabulku aritmetických posloupností, v nichž leží n při daném m a platí $\left(\frac{m}{n}\right) = 1$ resp. -1 pro m mezi -250 a $+250$. Menší tabulky viz Cahen *1.*, Wertheim *2.*

**) S. Eichenberg, Über das quadr. Reciprocitätsgesetz und einige quadr. Zerfällungen d. Primzahlen, Diss. Göttingen 1886. Viz též: Weber-Wellstein, str. 266—272.

Uveďme nejprve identitu

$$(a^2 + mb^2)(\alpha^2 + m\beta^2) = A^2 + mB^2, \qquad (*)$$

kdež buď

$$A = a\alpha + mb\beta, \qquad B = a\beta - b\alpha,$$

anebo

$$A = a\alpha - mb\beta, \qquad B = a\beta + b\alpha.$$

Tato identita dá se snadno dokázati přímým výpočtem obou jejích stran; ještě snadněji však, když činitele na levé straně rozložíme v komplexní činitele

$$(a + i\sqrt{m}b)(a - i\sqrt{m}b)(\alpha + i\sqrt{m}\beta)(\alpha - i\sqrt{m}\beta).$$

Násobme prvního činitele se čtvrtým, druhého se třetím. I dostaneme

$$[a\alpha + mb\beta - i\sqrt{m}(a\beta - b\alpha)][a\alpha + mb\beta + i\sqrt{m}(a\beta - b\alpha)] = (a\alpha + mb\beta)^2 + m(a\beta - b\alpha)^2.$$

Násobíme-li však prvního činitele se třetím, druhého se čtvrtým, nebo klademe-li $-b$ místo b, dostaneme jako součin hodnotu $(a\alpha - mb\beta)^2 + m(a\beta + b\alpha)^2$.

Dokážeme si nejprve větu pomocnou:

Lze-li číslo znázornitelné formou

$$x^2 + my^2 \qquad (1)$$

rozložiti v součin

$$A^2 + mB^2 = pP, \qquad (2)$$

kdež p je prvočíslo rovněž formou (1) znázornitelné, je též celé číslo P formou (1) znázornitelné.

Budiž $p = a^2 + mb^2$. Položme

$$\alpha = \frac{aA + mbB}{a^2 + mb^2}, \quad \beta = \frac{aB - bA}{a^2 + mb^2}. \qquad (3)$$

I je

$$(aB + bA)(aB - bA) = a^2B^2 - b^2A^2 = B^2(a^2 + mb^2) - b^2(A^2 + mB^2) = p(B^2 - Pb^2).$$

Je tudíž jedno z čísel $aB \pm bA$ dělitelno $p = a^2 + mb^2$. Můžeme však znamení u b voliti tak, aby bylo $aB - bA$ číslo prvočíslem p dělitelné, takže β je číslo celé.

Podle (*) je

$$(aA + mbB)^2 + m(aB - bA)^2 = (a^2 + mb^2)(A^2 + mB^2); \qquad (4)$$

jest tedy též $aA + mbB$ dělitelno p a je tudíž i α celé číslo. Podle (3) a (4) je však

$$\alpha^2 + m\beta^2 = \frac{A^2 + mB^2}{a^2 + mb^2} = P,$$

čímž věta dokázána.

Budiž $-m$ kvadratický zbytek lichého prvočísla, které není nejmenším prvočíslem této vlastnosti. Předpokládejme, že všechna prvočísla $< p$, jejichž zbytkem kvadratickým je $-m$, lze znázorniti pomocí formy $x^2 + my^2$, a dokážeme, že p dá se znázorniti touto formou.

Každé prvočíslo formou $x^2 + my^2$ znázornitelné je $\geqq m$, takže pro p platí $p > m$. Ježto $-m$ je kvadratický zbytek prvočísla p, existuje číslo celé z té vlastnosti, že $z^2 \equiv -m \pmod{p}$.

Tato kongruence má dvě řešení, o nichž lze předpokládati, že jsou kladná a $< p$. Jedno je liché, druhé sudé. Lze tedy vždy dosíci, že

$$z^2 + m = gp \qquad (5)$$

je liché. Pak je i g liché.

Ježto $z \leqq p - 1$ a $m < p$, je $z^2 + m < p^2 - 2p + 1 + p < p^2$, tedy v (5) $g < p$.

Lze tedy najíti celá čísla c, d taková, že $c^2 + md^2 = gp$, při čemž g je liché číslo kladné $< p$. Uvažujme množství $\mathfrak{G}$ všech celých čísel lichých kladných g takových, že pro ně existují čísla celá x, y té vlastnosti, že $x^2 + my^2 = gp$. Podle toho, co právě bylo řečeno, množství $\mathfrak{G}$ jistě není prázdné. Mezi čísly z $\mathfrak{G}$ je jistě jisté nejmenší g_0. Dokážeme, že je rovno 1. Pro g_0 platí $a_0^2 + mb_0^2 = g_0 p$ a podle toho, co dokázáno, je jistě $g_0 < p$. Kdyby nebylo $g_0 = 1$, bylo by g_0 dělitelno aspoň jedním prvočíslem $q < p$. Toto prvočíslo q je dělitelem formy $x^2 + my^2$, $-m$ je pro ně kvadratickým zbytkem. Ježto pak je $q < p$, lze q znázorniti formou $x^2 + my^2$, t. j. existují čísla celá a, b takové, že

$$a^2 + mb^2 = q.$$

Nechť je $g_0 p = qP$. Ježto $qP = a_0^2 + mb_0^2$ a $q = a^2 + mb^2$, je podle věty pomocné $P = \frac{g_0 p}{q} = g_1 p = \alpha^2 + m\beta^2$. Je pak $g_1 < g_0$, proti předpokladu o g_0.

Z toho plyne úplnou indukcí, že, je-li nejmenší liché prvočíslo, jehož kvadratickým zbytkem je $-m$, znázornitelno formou $x^2 + my^2$, je každé prvočíslo, jehož kvadratickým zbytkem je $-m$, znázornitelno onou formou.

Ukážeme ještě, že prvočíslo p lze znázorniti formou $x^2 + my^2$

jen jedním způsobem. Při tom nebudeme čtyři znázornění $(\pm x, \pm y)$, která se od (x, y) liší jen znaménky, považovati za různá.

Kdyby bylo

$$p = x^2 + my^2 = \xi^2 + m\eta^2, \tag{6}$$

kdež $$\xi \neq \pm x, \quad \eta \neq \pm y,$$

bylo by podle (*)

$$p^2 = (x\xi + my\eta)^2 + m(x\eta - y\xi)^2. \tag{7}$$

Jest však

$$(x\eta - y\xi)(x\eta + y\xi) = x^2\eta^2 - y^2\xi^2 = \eta^2(x^2 + my^2) - y^2(\xi^2 + m\eta^2) = p(\eta^2 - y^2),$$

musilo by tedy jedno z obou čísel $x\eta \pm y\xi$ býti p dělitelno a $\neq 0$. Zvolme znamení u y tak, aby bylo $x\eta - y\xi$ dělitelno p. Pak by bylo $(x\eta - y\xi)^2 \geqq p^2$, což podle (7) pro $m > 1$ není možno.

Zbývá všimnouti si případu $m = 1$. Pak by musilo býti

$$x\eta - y\xi = \pm p \quad \text{a} \quad x\xi + y\eta = 0, \quad \text{t. j.}$$

$$\frac{x}{y} = -\frac{\eta}{\xi}. \tag{8}$$

x, y jakož i ξ, η jsou dvojice čísel spolu nesoudělných; bylo by tedy podle (8) $x = \pm\eta$, $y = \mp\xi$, takže by se tato znázornění nelišila. (Při tom znázornění $(\pm x, \pm y)$, $(\pm y, \pm x)$ nepovažujeme za různá.) Tím tvrzení dokázáno.

Užijeme věty nejprve na případ $m = 1$, t. j. na formu $x^2 + y^2$. — 1 je kvadratický zbytek všech prvočísel tvaru $4k + 1$. Nejmenší z nich 5 lze znázorniti pomocí formy $x^2 + y^2$, $5 = 1^2 + 2^2$. Platí tedy věta:

Každé prvočíslo tvaru $4k + 1$ lze znázorniti jediným způsobem jako součet dvou čtverců.

Žádné prvočíslo tvaru $4k + 3$ nelze znázorniti jako součet dvou čtverců, neboť jeden z nich jako čtverec čísla sudého by byl $\equiv 0 \pmod 4$, druhý jako čtverec čísla lichého by byl $\equiv 1 \pmod 4$, takže by součet byl tvaru $4k + 1$.

Samozřejmě platí věta:

Každé liché prvočíslo obsažené v součtu dvou nesoudělných čtverců je tvaru $4k + 1$, tedy zase součet dvou čtverců.

p je totiž dělitelem formy $x^2 + y^2$.

Snadno lze nahlédnouti, že platí identita (podle (*), str. 83)

$$(a^2 + b^2)(\alpha^2 + \beta^2) = (a\alpha + b\beta)^2 + (a\beta - b\alpha)^2$$

a pro $\alpha = \beta = 1$

$$2\,(a^2 + b^2) = (a + b)^2 + (a - b)^2.$$

Součet dvou nesoudělných čtverců je buď lichý (je-li jedno z obou čísel sudé, druhé liché) neb dvojnásobek lichého čísla (jsou-li oba čtverce liché). Plyne tedy z věty předešlé:

Každý celý dělitel součtu dvou nesoudělných čtverců je zase součet dvou čtverců.

$m = 4$ věta také platí:

Každé prvočíslo tvaru $4n + 1$ *lze znázorniti jediným způsobem, formou* $x^2 + 4y^2$.

Ostatně plyne věta tato z předešlé. Při znázornění prvočísel tvaru $4n + 1$ formou $x^2 + y^2$ je jedno z čísel x, y liché, druhé sudé. Je-li tedy na př. $y = 2y'$, je $x^2 + y^2 = x^2 + 4y'^2$.

Užijme věty na případ $m = 2$, t. j. uvažujme formu $x^2 + 2y^2$. -2 je kvadratický zbytek prvočísel tvaru $8k + 1$, $8k + 3$. Nejmenší z nich je $3 = 1^2 + 2 \cdot 1^2$, je tedy znázornitelné pomocí formy $x^2 + 2y^2$. I platí věta:

Každé prvočíslo tvaru $8k + 1$ *aneb* $8k + 3$ *lze znázorniti jediným způsobem jako součet jednoduchého a dvojnásobného čtverce.*

Pro prvočíslo tvaru $8k + 1$ je x liché, y sudé, pro tvar $8k + 3$ je x i y liché.

Prvočísla tvaru $8k + 1$ *lze znázorniti jak formou* $x^2 + y^2$, *tak formou* $x^2 + 2y^2$.

Uvažujme případ $m = 3$, t. j. znázornění formou $x^2 + 3y^2$. -3 je kvadratický zbytek prvočísel tvaru $6k + 1$. Nejmenší z nich $7 = 2^2 + 3 \cdot 1^2$ je znázornitelné pomocí formy $x^2 + 3y^2$. *Každé prvočíslo tvaru* $6k + 1$ *lze jediným způsobem znázorniti jako součet čtverce a trojnásobného čtverce.*

Prvočísla tvaru $24k + 1$ *lze znázorniti každou ze tří forem* $x^2 + y^2$, $x^2 + 2y^2$, $x^2 + 3y^2$.

Klaďme konečně $m = 7$. -7 je kvadratický zbytek prvočísel tvaru $14k + 1$, $14k + 9$, $14k + 11$. Nejmenší z nich je 11 a pro to platí $11 = 2^2 + 7 \cdot 1^2$. I máme větu:

Každé prvočíslo tvaru $14k+1$, $14k + 9$, $14k + 11$ *lze jediným způsobem znázorniti jako součet čtverce jednoduchého a sedminásobného.*

Při znázornění prvočísla $p = 4k + 1$ ve tvaru

$$p = x^2 + 3y^2$$

nesmí býti x dělitelno třemi, zato však y může býti třemi dělitelno. Pak lze psáti

$$4p = (2x)^2 + 3\,(2y)^2 = (2x)^2 + 27\left(\frac{2y}{3}\right)^2.$$

Není-li y dělitelno třemi a je sudé, je buď $\equiv 2$ neb $\equiv 4 \pmod 6$; x musí býti liché, tedy buď $\equiv 1$ neb $\equiv 5 \pmod 6$. V každém případě je pak buď $x + y$ neb $x - y$ dělitelno třemi. Není-li y dělitelno třemi a je liché, je buď $\equiv 1$ neb $\equiv 5 \pmod 6$; x je pak buď sudé, tedy $\equiv 2$ neb $\equiv 4 \pmod 6$, takže je zase buď $x + y$ neb $x - y$ dělitelno třemi.

Jest však

$$4p = (1^2 + 3 \,.\, 1^2)\,(x^2 + 3y^2),$$

a je-li $x + y \equiv 0 \pmod 3$, pišme

$$4p = (x - 3y)^2 + 3\,(x + y)^2 = (x - 3y)^2 + 27\left(\frac{x+y}{3}\right)^2.$$

Je-li však $x - y \equiv 0 \pmod 3$, pak

$$4p = (x + 3y)^2 + 3\,(x - y)^2 = (x + 3y)^2 + 27\left(\frac{x-y}{3}\right)^2.$$

Platí tedy věta:

Čtyřnásobek prvočísla tvaru $4k + 1$ *lze znázorniti ve tvaru*

$$4p = X^2 + 27Y^2.$$

Toto znázornění je možné jediným způsobem.

Kdyby bylo

$$4p = X^2 + 27Y^2 = X_1^2 + 27Y_1$$

a

$$X_1 \neq \pm X,\quad Y_1 \neq \pm Y,$$

bylo by podle (*) str. 83

$$\begin{aligned} 16p^2 &= (X^2 + 27Y^2)\,(X_1^2 + 27Y_1^2) \\ &= (XX_1 + 27YY_1)^2 + 27\,(XY_1 - YX_1)^2. \end{aligned} \tag{9}$$

Jest však

$$\begin{aligned} (XY_1 - YX_1)\,(XY_1 + YX_1) &= X^2Y_1^2 - Y^2X_1^2 = \\ &= Y_1^2\,(X^2 + 27Y^2) - Y^2\,(X_1^2 + 27Y_1^2) = \\ &= 4p\,(Y_1^2 - Y^2). \end{aligned}$$

Bylo by tedy jedno z čísel $XY_1 \pm YX_1$ dělitelno p a $\neq 0$. Vhodným stanovením znamení Y bylo by možno dosíci, aby bylo $XY_1 - YX_1$ dělitelno p, tedy

$$|\,XY_1 - YX_1\,| \geqq p.$$

Pak by v (9) pravá strana byla $\geqq 27p^2$, levá strana je $16p^2$, což by vedlo k rozporu.

V. Znázornění čísel celých kladných formou

$$x_1^2 + x_2^2 + x_3^2 + x_4^2.$$

§ 49. Fermat vyslovil a Lagrange dokázal větu: *Každé celé kladné číslo lze rozložiti na součet čtyř neb méně čtverců celých čísel.* Jinými slovy: *Je-li n celé číslo kladné, je možno určiti čtyři celá čísla x_1, x_2, x_3, x_4 (o nichž lze beze všeho předpokládati, že jsou $\geqq 0$), splňující rovnici $n = x_1^2 + x_2^2 + x_3^2 + x_4^2$.**) (Všechna čísla x_1, x_2, x_3, x_4 nemusí býti $\neq 0$. Je-li na př. n rovno prvočíslu $p \equiv 1 \pmod 4$, je $p = x_1^2 + x_2^2$, takže lze klásti $x_3 = x_4 = 0$.)

Dokážeme si nejprve několik vět pomocných. V prvé řadě tak zvanou Eulerovu identitu.

1. *Jsou-li x_i, y_i libovolná čísla reální, je*

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) =$$
$$= (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 + (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2 +$$
$$+ (x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4)^2 + (x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2)^2. \quad (1)$$

Provedeme-li násobení na levé straně, dostaneme součet 16 členů $x_i^2y_k^2$ $(i, k = 1, 2, 3, 4)$. Na pravé straně vyskytuje se též těchto 16 členů a mimo to ještě dalších 24 členů tvaru $\pm 2x_ix_jy_ky_l$ $(i, j, k, l = 1, 2, 3, 4)$, kdež možno beze všeho předpokládati $i < j$, $k < l$. Ale těchto 24 členů se dohromady ruší, neboť koeficient u:

$$\begin{aligned}
2x_1x_2 &\text{ je } y_1y_2 - y_1y_2 - y_3y_4 + y_3y_4 = 0,\\
2x_1x_3 &\text{ je } y_1y_3 + y_2y_4 - y_1y_3 - y_2y_4 = 0,\\
2x_1x_4 &\text{ je } y_1y_4 - y_2y_3 + y_2y_3 - y_1y_4 = 0,\\
2x_2x_3 &\text{ je } y_2y_3 - y_1y_4 + y_1y_4 - y_2y_3 = 0,\\
2x_2x_4 &\text{ je } y_2y_4 + y_1y_3 - y_2y_4 - y_1y_3 = 0,\\
2x_3x_4 &\text{ je } y_3y_4 - y_3y_4 - y_1y_2 + y_1y_2 = 0.
\end{aligned}$$

Tím dokázána identita (1).

2. *Je-li p liché prvočíslo, je možno určiti celé číslo x, y splňující kongruenci*

$$x^2 + y^2 + 1 \equiv 0 \pmod p,$$

---

*) Důkaz následující podán v podstatě podle Landaua, I. str. 107.

takže

$$0 \leqq x < \tfrac{1}{2}p,\ 0 \leqq y < \tfrac{1}{2}p.^*)$$

Uvažujme soustavu A čísel x^2 pro $x = 0, 1, 2, \ldots, \frac{p-1}{2}$, t. j. pro $0 \leqq x < \frac{1}{2}p$ a soustavu B čísel $-y^2 - 1$ pro $y = 0, 1, 2, \ldots, \frac{p-1}{2}$, t. j. pro $0 \leqq y < \frac{1}{2}p$. Žádná dvě čísla ze soustavy A nejsou spolu kongruentní (mod p). Z $x'^2 \equiv x''^2 \pmod{p}$ by plynulo $x' \equiv \pm x'' \pmod{p}$, což není možné, ježto čísla $0, \pm 1, \pm 2, \ldots, \pm \frac{p-1}{2}$ tvoří úplnou soustavu zbytků (mod p) (§ 21). Ze stejného důvodu žádná dvě čísla ze soustavy B nejsou spolu kongruentní (mod p). V každé ze soustav A i B je $\frac{p+1}{2}$ čísel. Musí tedy býti aspoň jedno číslo ze soustavy A kongruentní (mod p) s jedním číslem ze soustavy B, ježto by jinak bylo $p + 1$ čísel, z nichž žádná dvě by nebyla kongruentní (mod p). Tím tvrzení dokázáno.

3. *Ke každému prvočíslu $p > 2$ lze určiti číslo celé m splňující vztah*

$$0 < m < p \tag{2}$$

té vlastnosti, že rovnice

$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2 \tag{3}$$

je řešitelná celými čísly x_1, x_2, x_3, x_4.

(Kdybychom nekladli pro m podmínku (2), byla by věta samozřejmá, neboť je $p \,.\, p = p^2 + 0^2 + 0^2 + 0^2$; pro další byla by pak věta zcela bezcenná.)

Podle předešlé věty je možno určiti celá čísla x, y splňující kongruenci

$$x^2 + y^2 + 1 \equiv 0 \pmod{p}$$

a taková, že $0 \leqq x < \frac{1}{2}p$, $0 \leqq y < \frac{1}{2}p$. Pak je $x^2 + y^2 + 1 = mp$, kdež m je celé číslo kladné. I platí

---

*) Zcela podobně by se dokázala obecnější věta:

Jsou-li a, b celá čísla, a nedělitelné p, lze určiti celá čísla x, y splňující kongruenci

$$x^2 + ay^2 + b \equiv 0 \pmod{p},$$

takže $0 \leqq x < \frac{1}{2}p$, $0 \leqq y < \frac{1}{2}p$. Uvedený důkaz pochází v podstatě od Bolzana a upozornil na něj Daublebsky v. Sterneck, Monatshefte f. Math. u. Phys. 15, 1904, p. 235—238. Je obsažen v rukopisné číselné teorii Bolzanově, uložené v Národní knihovně ve Vídni. Tato vyjde jako další svazek spisů Bolzanových s poznámkami od autora.

$$x^2 + y^2 + 1 < \tfrac{1}{4}p^2 + \tfrac{1}{4}p^2 + 1 = \tfrac{1}{2}p^2 + 1 < p^2,$$

tedy $mp < p^2$, t. j. $m < p$. Je tedy rovnice (3) i vztah (2) splněn, klademe-li $x_1 = x$, $x_2 = y$, $x_3 = 1$, $x_4 = 0$.

4. *Pro každé prvočíslo p je rovnice*

$$p = x_1^2 + x_2^2 + x_3^2 + x_4^2$$

řešitelná celými čísly x_1, x_2, x_3, x_4.

Pro $p = 2$ je

$$2 = 1^2 + 1^2 + 0^2 + 0^2,$$

takže věta platí. Zbývá tedy zabývati se dále případem prvočísla lichého, $p > 2$. Označme $\mathfrak{M}$ množství čísel celých m, pro něž rovnice (3) je řešitelná celými čísly x_1, x_2, x_3, x_4. m_0 nechť je nejmenší číslo z množství $\mathfrak{M}$. Pak podle předešlé věty je jistě $0 < m_0 < p$. Dokážeme, že je $m_0 = 1$.

Především je možno o m_0 dokázati, že je liché. Kdyby totiž bylo m_0 sudé, plynulo by z rovnice

$$m_0 p = x_1^2 + x_2^2 + x_3^2 + x_4^2, \tag{3'}$$

že

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod 2.$$

Tato kongruence může býti splněna, jen když buď všechna čtyři čísla x_1, x_2, x_3, x_4 jsou sudá, neb všechna čtyři lichá neb dvě z nich sudá a druhá dvě lichá. Přečíslujeme-li pak po případě tato čísla, lze dosáhnouti, aby platilo

$$x_1 + x_2 \equiv 0, \quad x_3 + x_4 \equiv 0 \pmod 2.$$

Pak by bylo možno psáti rovnici (3') ve tvaru

$$\tfrac{1}{2}m_0 p = \left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_1 - x_2}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2 + \left(\frac{x_3 - x_4}{2}\right)^2.$$

Pak by nemohlo býti m_0 nejmenší číslo z množství $\mathfrak{M}$, ježto by tam patřilo též číslo $\frac{1}{2}m_0$, které je $< m_0$. Je tedy m_0 jistě liché. Dokážeme, že nemůže býti $m_0 > 1$. Důkaz provedeme nepřímo. Dokážeme nemožnost předpokladu, že m_0 jest číslo liché > 1.

Budiž tedy m_0 číslo liché > 1.

Ustanovme čtyři celá čísla $y_i (i = 1, 2, 3, 4)$, tak aby platilo

$$y_i \equiv x_i \pmod{m_0}, \quad |y_i| < \tfrac{1}{2}m_0. \tag{4}$$

To je možno, neboť čísla

$$0, \pm 1, \pm 2, \ldots, \pm \frac{m_0 - 1}{2} \tag{5}$$

tvoří úplnou soustavu zbytků (mod m_0) (§ 21, absolutně nejmenší zbytky), takže každé celé číslo je (mod m_0) kongruentní s jedním a jen s jedním z čísel (5).

Podle (3′) je

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod{m_0}, \tag{6}$$

tedy též

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv 0 \pmod{m_0},$$

t. j.

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 = m_0 n, \tag{7}$$

kdež n je celé číslo $\geqq 0$.

Především je možno snadno dokázati, že jest $n \neq 0$. Při $n = 0$ by nutně musilo býti

$$y_1 = y_2 = y_3 = y_4 = 0,$$

t. j.

$$x_1 \equiv x_2 \equiv x_3 \equiv x_4 \pmod{m_0},$$

tedy

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod{m_0^2}.$$

Ze (3′) pak by plynulo

$$m_0 p \equiv 0 \pmod{m_0^2},$$

t. j.

$$p \equiv 0 \pmod{m_0},$$

což není možné, ježto p je prvočíslo a $1 < m_0 < p$. Bylo by tedy skutečně $n > 0$.

Dále by bylo $n < m_0$, neboť podle (4) by bylo $|y_i| < \frac{1}{2} m_0$ a tedy podle (7)

$$m_0 n < 4 \cdot \tfrac{1}{4} m_0^2 = m_0^2,$$

z čehož by ihned plynulo

$$n < m_0.$$

Z kongruencí (4) plyne však dále

$$x_1 y_1 + x_2 y_2 + x_3 y_3 + x_4 y_4 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \pmod{m_0},$$

z čehož na základě (6) též

$$x_1 y_1 + x_2 y_2 + x_3 y_3 + x_4 y_4 \equiv 0 \pmod{m_0},$$

t. j.

$$x_1 y_1 + x_2 y_2 + x_3 y_3 + x_4 y_4 = m_0 z,$$

kdež z je celé číslo.

Z týchž kongruencí (4) plyne dále

$$x_i y_k - x_k y_i \equiv x_i x_k - x_k x_i \equiv 0 \pmod{m_0},$$

$$(i, k = 1, 2, 3, 4, i \neq k),$$

t. j. $x_i y_k - x_k y_i = m_0 z_{ik}$, kdež z_{ik} jsou celá čísla.

Z Eulerovy identity pak plyne dále

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) =$$
$$= m_0^2 z^2 + m_0^2 (z_{12} + z_{34})^2 + m_0^2 (z_{13} + z_{42})^2 + m_0^2 (z_{14} + z_{23})^2.$$

Dosaďme do této rovnice z rovnic (3′) a (7) a kraťme m_0^2. Dostaneme

$$np = z^2 + (z_{12} + z_{34})^2 + (z_{13} + z_{42})^2 + (z_{14} + z_{23})^2.$$

Ježto $n < m_0$, nebylo by m_0 nejmenší číslo z množství $\mathfrak{M}$. Vede tedy předpoklad $m_0 > 1$ ke sporu a je $m_0 = 1$. Tím pak tvrzení dokázáno.

Tak dokázali jsme tvrzení Fermatovo pro případ, že $n = p$ je prvočíslo. Každé číslo kladné je však možno vyjádřiti jako součin prvočísel $p_1, p_2, \ldots, p_s$: $n = p_1 p_2 \ldots p_s$. Pro každé z prvočísel $p_1, p_2, \ldots, p_s$ věta Fermatova platí, tedy na základě Eulerovy identity i pro jich součin n.

Waring vyslovil větu:

Pro každého mocnitele celého $k > 0$ je možno najíti číslo N_k té vlastnosti, že rovnice

$$n = x_1^k + x_2^k + \ldots + x_{N_k}^k$$

je řešitelná celými čísly $x_i \geqq 0$, ať je n jakékoliv číslo. Větu tuto dokázal Hilbert.

Je tedy $N_2 = 4$ a bylo by na př. $N_3 \leqq 9$, $N_4 \leqq 38$.

O této otázce viz na př. Bachmann 3, II., Landau I., str. 235; literaturu viz Dickson II.