Časopis pro pěstování mathematiky a fysiky

Karel Rychlík

O poslední větě Fermatově pro $n = 4$ a pro $n = 3$

Časopis pro pěstování mathematiky a fysiky, Vol. 39 (1910), No. 1, 65--86

Persistent URL: http://dml.cz/dmlcz/123359

Příloha k Časopisu pro pěstování mathematiky a fysiky.

O poslední větě Fermatově pro $n = 4$ a pro $n = 3$.

Napsal Dr. **K. Rychlík.**

Fermat vyslovil větu, že není možno rovnici

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

pro celistvé positivní exponenty $n > 2$ řešiti celými racionálnými čísly x, y, z, nehledíme-li ovšem k takovým řešením, kdy některá z neznámých rovná se nulle. Fermat připojuje, že větu tu dokázal. V jeho spisech zachován jest však pouze důkaz, že rovnice

$$x^4 + y^4 = z^2$$

v uvedeném smyslu není řešitelná. Důkaz případu obecného Fermat neuvádí a také se nepodařilo až dosud jej provésti *).

Prací o větě uvedené, kterou Kronecker nazval „posledním theoremem Fermatovým“, jest veliké množství **). Ovšem, že jest z nich mnoho nesprávných, poněvadž věta ta svou zdánlivou jednoduchostí svádí mnohé, i nemathematiky, k tomu, aby se jí zabývali. Zájem vzrostl v poslední době tím více, že na základě odkazu P. Wolfskehla z Darmstadtu vypsala akademie

*) Při důkazu stačí se omeziti na případy, kdy n jest prvočíslo, resp. $= 4$. Je-li totiž n číslo složené a l jeden z jeho prvočinitelů neb $l = 4$, tak že $n = ln'$, plyne z nemožnosti řešení v celých částech $\neq 0$ při rovnici

$$x^l + y^l = z^l$$

okamžitě nemožnost řešení v celých číslech $\neq 0$ při rovnici

$$(x^{n'})^l + (y^{n'})^l = (z^{n'})^l,$$

neboli

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

**) Literaturu, jakož i poukaz na další literaturu viz v práci p. dr E. Schoenbauma: Ke Kummerovým pracím o Fermatově větě, Časopis pro pěst. math. a fys. r. 37, str. 484.

v Göttingách cenu 100.000 marek pro toho, kdo by tvrzení Fermatovo dokázal.

Největší význam mají práce Kummerovy, již proto, že jimi dokázána správnost tvrzení Fermatova pro celou řadu prvočísel n (tak pro všechna prvočísla $n < 100$). V následujícím podáme důkaz pro nejjednodušší případy $n = 4, 3, 5$. K tomu cíli jest třeba rozšířiti pojem čísla celého a sevšeobecniti pojem dělitelnosti. Aby vše bylo spíše srozumitelno, pojednáme nejprve o pojmech těch při číslech racionálných.

§ 1.

Racionálná čísla mají tu vlastnost, že se reprodukují racionálnými operacemi (sčítáním, odčítáním, násobením, dělením), t. j. součet, rozdíl, součin a podíl libovolných dvou čísel racionálných (vyloučíme-li případ, kdy jest dělitelem 0) jest opět číslo racionálné. Systémy čísel reprodukujících se racionálnými operacemi nazývají se tělesy číselnými. Tvoří tedy čísla racionálná číselně těleso, které označíme R. Čísla celistvá reprodukují se pouze sčítáním, odčítáním a násobením.

O čísle celistvém a pravíme, že jest dělitelno číslem celistvým d, je-li $\frac{a}{d}$ opět číslem celistvým. Pak jest a násobkem čísla d, d jest dělitelem čísla a. Tu platí věty snadno dokázatelné:

a) *Je-li celé číslo a násobkem celého čísla b, b opět násobkem celého čísla c, jest a násobkem c.*

b) *Je-li jak celé číslo a, tak celé číslo b násobkem celého čísla c, bude součet i rozdíl čísel a, b násobkem čísla c.*

Čísla ± 1, jednotky, mají to zvláštní postavení, že každé číslo celistvé jest jimi dělitelno. Mimo to jest každé číslo celistvé dělitelno samo sebou. Má-li celé číslo p pouze dělitele ± 1, $\pm p$, nazývá se prvočíslem, jinak nazývá se číslem složeným.

Pro číselnou theorii má základní důležitost věta, že lze každé číslo celé rozložiti jediným způsobem v součin prvočinitelů, nehledíme-li ke znaménku prvočinitelů těch. Důkaz spočívá na

tak zvaném „Euklidově algorithmu“, který slouží k určení největšího společného dělitele (největší společné míry) dvou čísel.

Předpokládejme, že jsou dána dvě celá čísla a, b, pro jednoduchost kladná, a že $a > b$.

Je-li b obsaženo v a, jsou společnými děliteli čísel a, b dělitelé čísla b a číslo b samo. Číslo b jest ze všech největší, jest tedy b největším společným dělitelem čísel a, b.

Není-li b obsaženo v a, dává dělení $a : b$ jistý zbytek r_0, který můžeme voliti tak, že

$$b > r_0 > 0.$$

Označíme-li pak částečný podíl q, bude

$$a = qb + r_0.$$

Je-li d celé číslo obsažené jak v a tak v b, jest d obsaženo také v r_0; lze totiž psáti

$$r_0 = a - qb,$$

a ježto a i b, tedy i qb, jsou násobky d, lze užíti věty b). Můžeme tedy říci: každý společný dělitel čísel a, b jest také společným dělitelem čísel b, r_0. Naopak, je-li d společný dělitel čísel b, r_0, jest, poněvadž d jest obsaženo také v qb, součet

$$qb + r_0 = a$$

obou násobků qb a r_0 čísla d rovněž násobkem čísla d; jest tedy každý společný dělitel čísel b, r_0 také společným dělitelem čísel a, b. Společní dělitelé obou čísel a, b souhlasí tudíž úplně se společnými děliteli čísel b, r_0. Hledání dělitelů a, b převedeno tak na hledání dělitelů čísel b, r_0. Je-li $r_0 = 1$, nemají a, b společného dělitele (vyjma ± 1), jsou to čísla nesoudělná. Je-li $r_0 \neq 1$, dělme číslem $r_0 < b$ číslo b; obdržíme

$$b = q_1 r_0 + r_1, \quad \text{kdež} \quad r_0 > r_1 \geqq 0.$$

Stejnou úvahou jako dříve bychom shledali, že čísla r_0, r_1 mají tudíž společné dělitele jako b, r_0, tedy i jako a, b.

Pokračujme dále, dělíce $r_0 : r_1$ atd.

Tak obdržíme soustavu rovnic

$$\begin{aligned} a &= qb + r_0 \\ b &= q_1 r_0 + r_1 \\ r_0 &= q_2 r_1 + r_2 \\ &\cdots\cdots \\ r_{n-3} &= q_{n-1}\, r_{n-2} + r_{n-1} \\ r_{n-2} &= q_n \quad r_{n-1} + r_n, \end{aligned}$$

jichž jest konečný počet a poslední zbytek $r_n = 1$ neb $= 0$. Čísla b, r_0, $r_1 \ldots r_{n-1}$, r_n tvoří totiž posloupnost čísel kladných ubývajících a poněvadž jest jen konečný počet čísel $< b$, kladných, vyskytne se nutně konečně jako zbytek buď 1 neb 0.

Společní dělitelé čísel a, b souhlasí se společnými děliteli dvojic číselných

$$(b, r_0), (r_0, r_1), (r_1, r_2), \ldots (r_{n-2}, r_{n-1}), (r_{n-1}, r_n).$$

Je-li $r_n = 1$, mají čísla a, b za společného dělitele pouze 1, jsou to čísla nesoudělná. Je-li $r_n = 0$, jest r_{n-2} dělitelno r_{n-1} (na základě poslední rovnice). Společní dělitelé čísel a, b budou obsaženy v r_{n-1} a každý dělitel čísla r_{n-1} (a číslo r_{n-1} samo), bude obsažen také v a i v b. Číslo r_{n-1} bude mezi děliteli čísel a, b největší. Odtud název největší společný dělitel (míra).

Místo nejmenších zbytků kladných lze voliti absolutně nejmenší zbytky, určené tak, že v rovnici

$$a = bq + r_0$$

jest

$$\frac{b}{2} < r_0 \leqq \frac{b}{2}.$$

Nyní můžeme přistoupiti k důkazu věty pomocné:

1. *Má-li součin dvou celých čísel aa_1 s celým číslem b společného dělitele d a je-li a nesoudělné s b, jest d nutně společným dělitelem čísel a_1, b.*

Užijme Euklidova algorithmu na dvojici čísel a, b. Ježto jsou to čísla nesoudělná, jest v soustavě rovnic, která tak vznikne, klásti $r_n = 1$. Násobíme-li všechny ty rovnice po sobě a_1, obdržíme

$$aa_1 = qba_1 + r_0a_1$$
$$ba_1 = q_1r_0a_1 + r_1a_1$$
$$r_0a_1 = q_2r_1a_1 + r_2a_1$$
$$\cdots\cdots\cdots$$
$$r_{n-2}a_1 = q_nr_{n-1}a_1 + r_na_1.$$

Je-li d libovolný dělitel čísel aa_1, b, jest d obsaženo také v qba_1, tedy i v $aa_1 - qba_1 = r_0a_1$; d jest obsaženo v ba_1, $q_1r_0a_1$, tedy i v $r_1a_1 = ba_1 - q_1r_0a_1$. Pokračujíce podobně, shledáme, že d jest obsaženo i v r_na_1, t. j. v a_1, což bylo dokázati.

Z věty právě vyslovené plyne:

2. *Jsou-li a, b čísla nesoudělná a je-li součin aa_1 dělitelný b, jest nutně a_1 dělitelno b.*

Obrácením věty 1. obdržíme:

3. *Součin dvou čísel aa_1, jež jsou obě nesoudělná s b, jest také nesoudělný s b.*

Neboť dle věty té mají aa_1, b tytéž společné dělitele jako a_1, b; ježto jsou a_1, a b čísla nesoudělná, bude platiti totéž i o aa_1 a b.

Jako důsledek platí věta:

4. *Nejsou-li čísla a, a_1 dělitelna prvočíslem p, není ani jich součin aa_1 dělitelný p.*

Nyní lze přistoupiti k důkazu věty základní:

Positivní celé číslo lze jediným způsobem rozložiti v součin positivních prvočinitelů.

Předpokládejme, že by pro celé číslo a platily rozklady

$$a = p_1, p_2 \cdots p_\nu$$

a zároveň

$$a = q_1, q_2 \cdots q_n,$$

kdež $p_1, p_2, \ldots p_\nu$ a $q_1, q_2, \ldots q_n$ jsou dvě řady rovných neb nerovných prvočísel. Pak jest a, neboli součin $p_1, p_2, \ldots p_\nu$ dělitelný q_n a to by nebylo dle věty 3. možno, kdyby byla všechna p různá od q_n. Můžeme předpokládati, že jest na př. $p_\nu = q_n$ a nalezneme podobným úsudkem, že $p_{\nu-1} = q_{n-1}$ atd. Jest tedy $\nu = n$ a lze klásti $p_1 = q_1$, $p_2 = q_2, \ldots p_\nu = q_n$. Ostatně platí věta základní pro čísla a prvočinitele s libovolným

znaménkem, pokládáme-li takové dva rozklady za v podstatě stejné, při nichž se činitelé liší jen znaménkem.

Zmiňme se ještě krátce o důležitém symbolu, který byl zaveden Gaussem do číselné theorie. Aby se vyjádřilo, že celé číslo a jest dělitelno celým číslem m, nezáleží-li dále na hodnotě podílu $\frac{a}{m}$, píše se symbolicky

$$a \equiv 0 \ (mod\ m)$$

(a kongruentní s nullou modulo m neb dle modulu m).

Je-li rozdíl $a - b$ dvou celých čísel a, b dělitelný m, tedy $a - b \equiv 0 \ (mod\ m)$, píše se $a \equiv b \ (mod\ m)$. Tato kongruence vyjadřuje totéž jako rovnice $a = b + qm$, kdež q značí jisté číslo celistvé.

Z definice kongruence plynou okamžitě tyto důsledky, jichž důkazy neuvádíme, poněvadž je lze snadno provésti:

I. Je-li

$$a \equiv b \ (mod\ m),$$
$$a \equiv c \ (mod\ m),$$

jest

$$b \equiv c \ (mod\ m).$$

II. Je-li

$$a \equiv b \ (mod\ m),$$
$$c \equiv d \ (mod\ m),$$

jest

$$a \pm c \equiv b \pm d \ (mod\ m),$$
$$ac \equiv bd \ (mod\ m).$$

III. Je-li celé číslo n nesoudělné s m, plyne z kongruence

$$an \equiv bn \ (mod\ m)$$

kongruence nová

$$a \equiv b \ (mod\ m).$$

§ 2.

Obrátíme se nyní k uvažování čísel tvaru $a + bi$, kdež a, b jsou libovolná čísla racionálná a $i = \sqrt{-1}$. Čísla ta zavedl do číselné theorie Gauss, nazývaje je čísly komplexními. Lze o nich říci, že tvoří těleso, a to těleso označíme $R(i)$.

Neboť značí-li

$$\alpha = a_1 + b_1 i, \qquad \beta = a_2 + b_2 i$$

libovolná dvě taková čísla, náleží i jich součet, rozdíl, součin a podíl, t. j. čísla

$$\alpha \pm \beta = (a_1 \pm a_2) + (b_1 \pm b_2)\, i$$
$$\alpha\beta = (a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1)\, i$$
$$\frac{\alpha}{\beta} = \frac{a_1 a_2 + b_1 b_2}{a_2^2 + b_2^2} + \frac{a_2 b_1 - a_1 b_2}{a_2^2 + b_2^2}\, i$$

témuž systému $R(i)$.

Toto těleso $R(i)$, které obsahuje v sobě všechna čísla racionálná, jest speciálním případem tělesa druhého stupně (kvadratického tělesa), poněvadž všechna jeho čísla vzniknou opětovaným užíváním čtyř základních početních operací z čísla i, kteréž jest kořenem rovnice kvadratické s racionálnými koefficienty $x^2 + 1 = 0$. Tato rovnice má za druhý kořen $-i$. Číslo $\alpha' = a - bi$, které vzniká z čísla $\alpha = a + bi$ tím, že změníme i v $-i$, nazývá se sdružené (konjugované) s α. Pak jest α číslo sdružené s α'. Značí-li čárka přechod k číslu konjugovanému, platí, jak snadno lze dokázati, rovnice

$$(\alpha \pm \beta)' = \alpha' \pm \beta',$$
$$(\alpha\beta)' = \alpha'\beta',$$
$$\left(\frac{\alpha}{\beta}\right)' = \frac{\alpha'}{\beta'}.$$

Normou čísla α nazývá se součin obou čísel sdružených $\alpha\alpha'$ a označíme ji $n(\alpha)$, tak že

$$n(\alpha) = \alpha\alpha' = (a + bi)(a - bi) = a^2 + b^2.$$

Z toho plyne, že norma jest vždy positivní racionálné číslo, které $= 0$, jen když $a = b = 0$, tedy $\alpha = 0$.

Poněvadž $(\alpha\beta)' = \alpha'\beta'$ jest $(\alpha\beta)(\alpha\beta)' = (\alpha\alpha')(\beta\beta')$, tudíž

$$n(\alpha\beta) = n(\alpha)\, n(\beta).$$

Norma součinu jest rovna součinu norem obou činitelů.

Podobně platí pro podíly rovnice

$$n\left(\frac{\alpha}{\beta}\right) = \frac{n(\alpha)}{n(\beta)}.$$

Číslo komplexní $\alpha = a + bi$ s číslem sdruženým $\alpha' = a - bi$ jsou kořeny kvadratické rovnice s racionálnými koefficienty

$$x^2 - 2ax + a^2 + b^2 = 0.$$

Aby rovnice tato měla za koefficienty čísla celá a při x^2 koefficient 1, musí býti a i b čísla celá. Pak nazývá se $\alpha = a + bi$ komplexním číslem celistvým, jinak, není-li α kořenem podobné rovnice, je-li tedy jedno z čísel a, b neb obě číslem lomeným, nazývá se i α číslem lomeným. Celá čísla racionálná tvoří část systému celých čísel komplexních a každé celé číslo komplexní, je-li zároveň racionálné, jest nutně celým číslem racionálným.

Celá čísla komplexní reprodukují se sčítáním, odčítáním a násobením. Podobně jako při číslech racionálných zavedeme i zde pojem dělitelnosti.

Celé číslo α jest dělitelno celým číslem δ, je-li $\frac{\alpha}{\delta}$ opět číslem celým. Jest patrno ihned, že platí i zde věty označené *a*), *b*) v § 1. Je-li $\alpha = a + bi$ celé číslo, jest norma $n(\alpha) = a^2 + b^2$ číslo přirozené (t. j. positivní, racionálné celé číslo). Poněvadž i číslo sdružené $\alpha' = a - bi$ jest celým, jest norma $n(\alpha)$ číslem α dělitelna.

Z věty o normě součinu plyne ihned:

Je-li celé číslo α dělitelno celým číslem β, jest $n(\alpha)$ dělitelno $n(\beta)$.

Jednotkou nazývá se celé číslo ε, které jest dělitelem čísla 1 a tedy i všech celých čísel; dle věty předešlé musí býti $n(\varepsilon)$ obsaženo v $n(1)$, t. j. v 1, musí tedy býti $n(\varepsilon) = 1$, a naopak, je-li $n(\varepsilon) = 1$, bude číslo ε jednotkou. Položíme-li $\varepsilon = x + iy$, bude $n(\varepsilon) = x^2 + y^2 = 1$, kdež x a y jsou celá čísla racionálná. Z toho plyne, že musí býti buď $x^2 = 1$ a $y = 0$, neb $x = 0$ a $y^2 = 1$. Tak obdržíme čtyři jednotky ± 1, $\pm i$.

Je-li číslo ε i jeho reciproká hodnota $\frac{1}{\varepsilon}$ číslem celým, jest ε nutně jednotkou. Jest totiž

$$n(\varepsilon)\, n\left(\frac{1}{\varepsilon}\right) = n(1) = 1$$

a poněvadž jak $n(\varepsilon)$, tak $n\left(\frac{1}{\varepsilon}\right)$ jsou čísla přirozená, jest $n(\varepsilon) = 1$, tedy skutečně ε jednotkou.

Čísla, jichž podíl jest jednotkou, nazývají se associovaná. Jsou vždy čtyři spolu associovaná čísla $\pm \alpha$, $\pm \alpha i$, která při všech otázkách, týkajících se dělitelnosti, chovají se stejně, tak že je můžeme pokládati za v podstatě stejná. Je-li totiž celé číslo α dělitelno celým číslem β, jsou také čísla s α associovaná dělitelna β a čísly s β associovanými.

Celé číslo komplexní π, které má za dělitele pouze 1, π a čísla s nimi associovaná nazývá se prvočíslem.

I pro čísla komplexní platí věta o jednoznačné rozložitelnosti. Důkaz se provede opět pomocí Euklidova algorithmu. K tomu cíli dokažme si nejprve větu: *Jsou-li α a β dvě libovolná čísla komplexní, existuje vždy celé číslo komplexní $\varkappa$ té vlastnosti, že* $n(\alpha - \beta\varkappa) \leqq \frac{1}{2} n(\beta)$.

Položme $\frac{\alpha}{\beta} = K + Li$ a nechť jest k celé číslo racionálné ležící nejblíže K, tak že $| K - k | \leqq \frac{1}{2}$ a l celé číslo ležící nejblíže L, tedy $| L - l | \leqq \frac{1}{2}$, dále pak $\varkappa = k + li$. Ježto

$$\frac{\alpha}{\beta} - \varkappa = (K - k) + (L - l)\, i,$$

bude

$$n\left(\frac{\alpha}{\beta} - \varkappa\right) = (K - k)^2 + (L - l)^2 \leqq \frac{1}{4} + \frac{1}{4} \leqq \frac{1}{2}$$

a tedy skutečně

$$n(\alpha - \beta\varkappa) \leqq \frac{1}{2} n(\beta).$$

Buďtež nyní dána dvě celá čísla komplexní α a β. Určeme celé číslo komplexní $\varkappa$ tak, aby

$$n(\alpha - \beta\varkappa) \leqq \frac{1}{2} n(\beta)$$

a položme

$$\alpha - \beta\varkappa = \varrho,$$

tak že

$$n(\varrho) \leqq \frac{1}{2} n(\beta).$$

Dále určeme celé číslo $\varkappa_1$ tak, aby

$$n(\beta - \varrho\varkappa_1) \leqq \frac{1}{2} n(\varrho)$$

a položme

$$\beta - \varrho\varkappa_1 = \varrho_1,$$

tedy

$$n(\varrho_1) \leqq \frac{1}{2} n(\varrho).$$

Postupujíce podobně dále, dostaneme řadu rovnic

$$\begin{aligned}
\alpha &= \varkappa\beta + \varrho \\
\beta &= \varkappa_1\varrho + \varrho_1 \\
\varrho &= \varkappa_2\varrho + \varrho_2 \\
&\cdots\cdots\cdots \\
\varrho_{n-3} &= \varkappa_{n-1}\varrho_{n-2} + \varrho_{n-1} \\
\varrho_{n-2} &= \varkappa_n\varrho_{n-1} + \varrho_n.
\end{aligned}$$

Rovnic těch jest konečný počet a v poslední z nich bude buď $\varrho_n = 0$ neb $n(\varrho_n) = 1$, tedy ϱ_n jednotkou. To plyne z toho, že normy čísel $\beta, \varrho, \varrho_1, \ldots \varrho_{n-1}, \varrho_n$ tvoří posloupnost čísel klesajících kladných a musí nutně skončiti buď $\varrho_n = 0$ neb $n(\varrho_n) = 1$.

Z napsané řady rovnic můžeme odvoditi tytéž důsledky, jako jsme učinili při číslech racionálných. Je-li ϱ_n jednotkou, jsou α, β čísla nesoudělná, je-li $\varrho_n = 0$, jsou společní dělitelé čísel α, β dělitelé čísla ϱ_{n-1} a číslo ϱ_{n-1} samo. Číslo toto, dle analogie z theorií čísel racionálných nazveme největší společnou měrou.

Z platnosti Euklidova algorithmu plyne však, že platí pro čísla komplexní i věty, označené 1. 2. 3. 4. v § 1. a tedy také věta základní:

Každé celé číslo komplexní lze rozložiti v podstatě jediným způsobem v součin prvočinitelů, pokládáme-li za podstatně stejné takové dva rozklady, které se liší pouze tak, že místo prvočinitelů rozkladu jednoho jsou v druhém prvočinitelé associovaní.

Kongruenci definujeme při číslech komplexních stejně jako jsme to učinili při číslech racionálných: $\alpha \equiv 0 \pmod{\mu}$, je-li celé číslo α dělitelno celým číslem μ, $\alpha \equiv \beta \pmod{\mu}$, je-li $\alpha - \beta \equiv 0 \pmod{\mu}$. I zde platí věty I., II., III. Jest patrno, že místo μ lze psáti kterékoliv z čísel associovaných.

Poznámka*). Není nesnadné určiti všechna prvočísla z tělesa $R(i)$. Existuje samozřejmě nekonečně mnoho přirozených čísel, která daným komplexním prvočíslem π jsou dělitelna: jedním z nich jest na př. $n(\pi)$. Nejmenší z těchto čísel musí býti přirozeným prvočíslem p. Neboť p jest nutně různé od 1, sic by bylo π jednotkou a p také nesmí se dáti rozložiti v součin dvou přirozených čísel, sic by π jakožto prvočíslo musilo v jednom z těchto faktorů, který jest $< p$, býti obsaženo, což jest proti předpokladu o p. Každé komplexní prvočíslo π jest tedy dělitelem určitého přirozeného prvočísla p a hledání prvočísel v tělese $R(i)$ převedeno tak na hledání dělitelů z $R(i)$ přirozených prvočísel p. $n(\pi)$ jest nutně dělitelem $n(p) = p^2$ a tedy jest $n(\pi) = p$ neb $= p^2$. Je-li $n(\pi) = p$, nazývá se prvočíslo π stupně prvního, je-li $n(\pi) = p^2$, jest π prvočíslem stupně druhého. V prvém případě jest $p = \pi\pi' = n(\pi)$ součinem dvou sdružených prvočísel stupně prvního, poněvadž, je-li π prvočíslem, jest jím také π'. V druhém případě jest $p = \pi\varepsilon$, $n(\varepsilon) = 1$, tak že jest p associováno s π a tedy také samo komplexním prvočíslem druhého stupně. Jedná se nyní o to, rozhodnouti, kdy který případ nastane. V prvém případě, kdy $p = \pi\pi'$, vidíme, že, klademe-li $\pi = r + si$, bude $p = r^2 + s^2$, tak že lze p rozložiti v součet dvou čtverců.

Čtverec sudého čísla jest kongruentní s 0, lichého s 1 $\pmod{4}$, může tedy býti součet dvou čtverců $\equiv 0$, 1 neb 2 $\pmod{4}$, nikoliv však $\equiv 3 \pmod{4}$. Vidíme tedy, že pro $p \equiv 3 \pmod{4}$ musí jistě nastati případ druhý, tak že platí věta:

Každé přirozené prvočíslo p tvaru $4n + 3$ jest komplexním prvočíslem druhého stupně.

---

*) Věty obsažené v této poznámce, jichž porozumění vyžaduje některé znalosti z číselné theorie, uvádíme pouze k vůli úplnosti; v následujícím nebudeme jich potřebovati.

Pro 2 platí

$$2 = n(1 - i) = n(1 + i) = (1 + i)(1 - i) = i(1 - i)^2 = -i(1 + i)^2.$$

Číslo 2 *jest associováno se čtvercem prvočísla prvního stupně* $1 + i$ *neb* $1 - i$.

Jedná se ještě o přirozená prvočísla p tvaru $4n + 1$. O těch lze dokázati, že pro ně nastává případ první. Uvážíme-li, že v tomto případě $p = r^2 + s^2$, vidíme, že jedná se o větu z theorie kvadratických forem, že prvočíslo tvaru $4n + 1$ jest součtem dvou čtverců. Bez této theorie lze to dokázati takto:

Podobně jako při číslech racionálných platí i při číslech komplexních věta, že kongruence

$$f(x) \equiv 0 \ (mod\ \pi),$$

kdež $f(x)$ jest racionálná celistvá funkce stupně m s koefficienty z $R(i)$ a π prvočíslo z $R(i)$, má nanejvýš m nekongruentních kořenů. Avšak kongruence $p - 1^{ho}$ stupně $x^{p-1} \equiv 1 \ (mod\ p)$ má dle věty Fermatovy nekongruentní kořeny $1, 2, 3, \ldots p - 1$ a je-li $p = 4n + 1$, ještě kořen i, tedy celkem p kořenů, z čehož plyne, že p nemůže býti v tělese $R(i)$ prvočíslem. Prvočinitelé π, π', v něž se p rozpadá, nemohou býti associováni, neboť z $\pi = \pm \pi'$ neb $\pi = \pm i\pi'$ by plynulo buď $r = 0$ neb $s = 0$ neb $r^2 = -s^2$, což jest nemožno. Platí tedy věta:

Přirozené prvočíslo p *tvaru* $4n + 1$ *rozpadá se v tělese* $R(i)$ *v součin dvou konjugovaných, neassociovaných prvočísel stupně prvého.*

Z této věty plyne bezprostředně:

Prvočíslo p *tvaru* $4n + 1$ *lze vždy a to pouze jediným způsobem rozložiti v součet dvou čtverců* $r^2 + s^2$ *(nehledíme-li na znamení při* r *a* s*).* Jest to věta, vyslovená Fermatem a dokázaná Eulerem.

§ 3.

Obrátíme se nyní ke Kummerovu důkazu pro $n = 4$.

Značí-li α, β, γ *celá čísla z tělesa* $R(i)$, *z nichž žádné není rovno nulle, není splněna nikdy rovnice*

$$\alpha^4 + \beta^4 = \gamma^2. \qquad (1)$$

O číslech α, β, γ můžeme předpokládati, že jsou nesoudělná. Kdyby totiž měla jistého společného dělitele, mohli bychom obdržeti krácením z rovnice (1) rovnici téhož tvaru, kdež α, β, γ jsou čísla nesoudělná

Položme

$$\lambda = 1 + i.$$

Pak bude

$$n(\lambda) = 2, \qquad 2 = -i\lambda^2.$$

Ukážeme nejprve, že, mají-li vyhovovati rovnici (1) tři celá čísla nesoudělná α, β, γ vesměs různá od 0, musí býti jedno z čísel α, β dělitelno λ.

Číslo $\alpha = a + bi$ lze psáti ve tvaru

$$\alpha = a - b + b(1 + i) = a - b + b\lambda.$$

Není-li α dělitelno λ, nesmí býti $a - b$ dělitelno λ, tedy, poněvadž jest to číslo racionálné, nesmí býti $a - b$ dělitelno 2. Musí tedy býti buď a liché, b sudé, pak jest

$$a) \qquad \alpha \equiv 1 \,(mod\ 2),$$

neb a sudé, b liché, pak jest

$$a) \qquad \alpha \equiv i \,(mod\ 2).$$

Z kongruencí a) odvodíme *)

$$b) \qquad \alpha^2 \equiv \pm 1 \,(mod\ 4), \text{ neboli } (mod\ \lambda^4)$$

a dále

$$c) \qquad \alpha^4 \equiv 1 \,(mod\ 8), \text{ neboli } (mod\ \lambda^6).$$

Není-li ani β dělitelno λ, bude podobně

$$\beta^4 \equiv 1 \,(mod\ \lambda^6),$$

tedy

$$\alpha^4 + \beta^4 \equiv 2 \,(mod\ \lambda^6)$$

a na základě rovnice (1)

$$\gamma^2 \equiv 2 \,(mod\ \lambda^6),$$

neboli

$$\gamma^2 - 2 \equiv 0 \,(mod\ \lambda^6). \qquad (2)$$

*) Zde jakož i v následujícím tím způsobem, že kongruenci napíšeme jako rovnici, na př. kongruenci $\alpha \equiv i \,(mod\ 2)$ píšme $\alpha = i + 2\varkappa$, kdež $\varkappa$ jest celé číslo. Z toho plyne $\alpha^2 = -1 + 4\varkappa i + 4\varkappa^2$, neboli $\alpha^2 = -1 + 4(\varkappa i + \varkappa^2)$, což psáno jako kongruence $\alpha^2 \equiv -1 \,(mod\ 4)$.

Rozdíl $\gamma^2 - 2 = \gamma^2 + i\lambda^2$ nemůže býti dělitelný λ^2, jen když bude γ dělitelno λ, ne však vyšší mocností λ. Položíme-li $\gamma = \lambda\gamma_1$, bude γ_1 nedělitelné λ a

$$\gamma^2 - 2 = \lambda^2\gamma_1^2 + i\lambda^2 = \lambda^2(\gamma_1^2 + i).$$

Plynula by tedy z rovnice (2) kongruence

$$\gamma_1^2 + i \equiv 0 \ (mod\ \lambda^4),$$

která jest nemožná, poněvadž pro celé číslo nedělitelné λ platí dle *b*) jedna z kongruencí $\gamma_1^2 \equiv \pm 1 \ (mod\ \lambda^4)$.

Zbývá tudíž pouze předpoklad, že jedno z čísel α, β, na př. α jest dělitelno λ, čísla β, γ že však λ nejsou dělitelna. Položme $\alpha = \lambda^n\alpha_1$, kdež α_1 značí číslo nedělitelné λ a uvažujme hned rovnici obecnější

$$\beta^4 - \gamma^2 = \varepsilon\lambda^{4n}\alpha_1^4, \tag{3}$$

kdež ε značí libovolnou jednotku z tělesa $R(i)$. Pišme rovnici (3) ve tvaru

$$(\beta^2 + \gamma)(\beta^2 - \gamma) = \varepsilon\lambda^{4n}\alpha_1^4.$$

$\beta^2 + \gamma$ a $\beta^2 - \gamma$ nemohou míti společného dělitele vyjma λ^2, poněvadž by jich společný dělitel musil býti obsažen i v součtu $2\beta^2$ a rozdílu 2γ a čísla 2γ a $2\beta^2$ mají pouze společného dělitele $2 = -i\lambda^2$. Z jednoznačné rozložitelnosti v prvočinitele plyne pak, že platí buď rovnice

$$\begin{aligned} \beta^2 + \gamma &= \eta\lambda^{4n-2}\alpha'^4, \\ \beta^2 - \gamma &= \vartheta\lambda^2\beta'^4, \end{aligned} \tag{4}$$

neb

$$\begin{aligned} \beta^2 + \gamma &= \vartheta\lambda^2\beta'^4, \\ \beta^2 - \gamma &= \eta\lambda^{4n-2}\alpha'^4, \end{aligned}$$

kdež η, ϑ jsou jednotky a α', β' celá, λ nedělitelná čísla z tělesa $R(i)$. Poněvadž od jedné dvojice rovnic lze přejíti ke druhé tím, že píšeme $-\gamma$ místo γ, čímž se rovnice 1) nezmění, stačí uvažovati jen jednu z nich, na př. první.

Sečtěme rovnice (4) a dělme $\vartheta\lambda^2$. I obdržíme rovnici

$$\beta'^4 - \zeta\beta^2 = \varepsilon'\lambda^{4(n-1)}\alpha'^4, \tag{5}$$

kdež ζ a ε' značí jednotky.

V případě $n = 1$ má rovnice tato tvar

$$\beta'^4 - \zeta\beta^2 = \varepsilon'\alpha'^4.$$

Rovnice tato jest jistě nesplnitelná.

Jest totiž

$$\alpha'^4 \text{ a také } \beta'^4 \equiv 1 \pmod{\lambda} \text{ (na základě } c),$$
$$\beta^2 \equiv \pm 1 \pmod{\lambda} \text{ (na základě } b),$$
$$\zeta, \varepsilon' \equiv \pm 1, \pm i \pmod{\lambda}.$$

Výraz na levé straně $\beta'^4 - \zeta\beta^2$ jest pak $\equiv 0$ neb 2 neb $1 \pm i$, tedy vždy $\equiv 0 \pmod{\lambda}$, kdežto pravá strana jest $\equiv 1$ neb $\pm i$, což není $\equiv 0 \pmod{\lambda}$. Musí tedy býti nutně $n > 1$.

Uvažujme pak rovnici (5) jako kongruenci $\pmod{\lambda^4}$. I plyne z ní

$$\beta'^4 - \zeta\beta^2 \equiv 0 \pmod{\lambda^4},$$

a ježto dle b) a c)

$$\beta'^4 \equiv 1 \pmod{\lambda^4},$$
$$\beta^2 \equiv \pm 1 \pmod{\lambda^4},$$

bude

$$\zeta \equiv \pm 1 \pmod{\lambda^4} \text{ neboli } \pmod{4}.$$

Poněvadž z jednotek ± 1, $\pm i$ jen ± 1 vyhovují této kongruenci, jest nutně $\zeta = \pm 1$.

Položíme-li tedy v rovnici (5) dle toho, je-li $\zeta = +1$ neb -1, $\beta = \gamma'$, resp. $\beta = i\gamma'$, dostaneme rovnici

$$\beta'^4 - \gamma'^2 = \varepsilon'\lambda^{4(n-1)}\alpha'^4, \qquad (6)$$

která má týž tvar jako (3), jen že je v ní n o 1 menší.

Analogickým postupem bychom odvodili z (6) rovnici téhož tvaru jako (3), ale s n o 2 menším a tak bychom postupovali, až bychom přišli k rovnici, při níž $n = 1$, a ta je, jak již bylo řečeno, nemožná.

Tím správnost tvrzení, jež bylo dokázati, dokázána ve všech případech.

§ 4.

Theorii komplexních čísel $a + bi$ právě uvažovaných jest zcela analogická theorie čísel tvaru $a + b\xi$, kdež a, b značí čísla racionálná a $\zeta = \frac{-1 + \sqrt{-3}}{2}$ jest třetí kořen z jed-

notky. Čísla ta lze patrně také psáti ve tvaru $A + B\sqrt{-3}$ a lze o nich snadno dokázati, že tvoří těleso. To nazývá se tělesem třetích kořenů z jednotky a označíme je $R(\zeta)$ neb $R(\sqrt{-3})$, abychom připomněli, že vzniklo z tělesa čísel racionálných R adjunkcí čísla ζ neb $\sqrt{-3}$ (použitím racionálných operací na čísla z R a na ζ resp. $\sqrt{-3}$). Toto těleso jest jako $R(i)$ speciálním případem tělesa kvadratického. ježto ζ jest kořenem rovnice kvadratické s racionálnými koefficienty

$$x^2 + x + 1 = 0.$$

Druhý kořen této rovnice jest ζ^2.

Klademe-li místo ζ tento druhý kořen ζ^2 v čísle

$$\alpha = a + b\zeta = A + B\sqrt{-3},$$

obdržíme číslo s α konjugované

$$\alpha' = a + b\zeta^2 = A - B\sqrt{-3}.$$

Součin obou čísel konjugovaných nazývá se opět normou

$$n(\alpha) = n(\alpha') = a^2 - ab + b^2 = A^2 + 3B^2.$$

Jest to číslo kladné a jest $= 0$ jen když $\alpha = 0$.

Pro normu součinu a podílu platí

$$n(\alpha\beta) = n(\alpha)\, n(\beta)$$

$$n\left(\frac{\alpha}{\beta}\right) = \frac{n(\alpha)}{n(\beta)}.$$

Sdružená čísla α, α' jsou kořeny rovnice kvadratické s racionálnými koefficienty

$$x^2 + (b + 2a)\, x + a^2 - ab + b^2 = 0$$

neb

$$x^2 - 2A\, x + A^2 + 3B^2 = 0.$$

Aby v rovnicích těchto byl koefficient u x^2 roven 1 a ostatní koefficienty racionálná čísla celistvá, musí býti v prvé rovnici a, b čísla celá, ve druhé musí býti $A = \frac{m}{2}$, kdež m jest číslo celé a dále $B = \frac{n}{2}$, kdež n jest číslo celé takové,

že $m \equiv n \pmod 2$. Číslo α těmto podmínkám vyhovující nazývá se číslem celým, nevyhovuje-li jim, nazývá se číslem lomeným. Celá čísla racionálná tvoří část systému celých čísel z tělesa $R(\zeta)$ a každé celé číslo z $R(\zeta)$, je-li zároveň racionálné, jest nutně celým číslem racionálným.

Celá čísla tělesa $R(\zeta)$ reprodukují se sčítáním, odčítáním a násobením. Pojem dělitelnosti zavedeme jako dříve: Celé číslo α jest dělitelno celým číslem δ, je-li $\frac{\alpha}{\delta}$ číslem celým.

Norma celého čísla α, $n(\alpha) = a^2 - ab + b^2$ jest číslem přirozeným a jest číslem α dělitelna.

Je-li celé číslo α dělitelno celým číslem β, jest $n(\alpha)$ dělitelno $n(\beta)$. Jednotkami nazveme opět celá čísla obsažená v 1. Pro jednotku $\varepsilon = x + \zeta y$, musí býti $n(\varepsilon) = 1$, tedy

$$x^2 - xy + y^2 = 1.$$

Aby rovnice tato byla celými čísly x, y řešitelná, musí býti x, y buď čísla o stejném znaménku neb jedno z nich $= 0$, poněvadž by jinak všichni sčítanci byla kladná čísla. Píšeme-li nyní rovnici tu ve tvaru

$$(x - y)^2 + xy = 1,$$

vidíme, že jeden z obou kladných sčítanců musí býti $= 1$, druhý $= 0$.

I máme rovnice

I. $\quad x - y = 0, \quad xy = 1.$

II. $\quad x - y = \pm 1, \quad xy = 0.$

I. nám poskytují $x = y = \pm 1$,

II. nám poskytují buď $x = 0 \quad y = \pm 1$,

neb $y = 0 \quad x = \pm 1$.

Tak dostaneme těchto 6 jednotek

$$1, \; -1, \; \zeta, \; -\zeta, \; \zeta^2 = -1 - \zeta, \; -\zeta^2 = 1 + \zeta.$$

Čísla, jichž podíl jest jednotkou, nazývají se opět associovanými. V tělese $R(\zeta)$ jest vždy 6 spolu associovaných čísel $\pm \alpha$, $\pm \zeta\alpha$, $\pm \zeta^2\alpha$, která můžeme v otázkách týkajících se dělitelnosti pokládati za „v podstatě“ stejná.

Celé číslo π z $R(\zeta)$ nazývá se prvočíslem, má-li pouze dělitele 1, π a čísla s těmito čísly associovaná.

V tělese $R(\zeta)$ platí pro čísla celá opět věta v jednoznačné rozložitelnosti v prvočinitele. Jest totiž i v tělese $R(\zeta)$ možno prováděti Euklidův algorithm. Dokažme nejprve větu:

Jsou-li α a β dvě libovolná čísla z tělesa $R(\zeta)$, existuje vždy celé číslo $\varkappa$ z tělesa $R(\zeta)$ té vlastnosti, že

$$n(\alpha - \beta\varkappa) \leqq \frac{1}{2} n(\beta).$$

Položíme-li

$$\frac{\alpha}{\beta} = \frac{K + L\sqrt{-3}}{2},$$

a zvolíme-li za l celé číslo racionálné, ležící nejblíže L, tak že

$$|L - l| \leqq \frac{1}{2},$$

a za k celé číslo $\equiv l \pmod 2$, ležící nejblíže K (tedy z obou celých čísel sousedních, mezi nimiž leží K ono, které jest $\equiv l \pmod 2$), tak že

$$|K - k| \leqq 1,$$

bude $\varkappa = \frac{k + l\sqrt{-3}}{2}$ číslo celé té vlastnosti, že

$$n\left(\frac{\alpha}{\beta} - \varkappa\right) = n\left(\frac{(K-k) + (L-l)\sqrt{-3}}{2}\right)$$

$$= \frac{(K-k)^2 + 3(L-l)^2}{4} \leqq \frac{1}{4}\left(1 + \frac{3}{4}\right) < \frac{1}{2}$$

a tedy skutečně

$$n(\alpha - \beta\varkappa) \leqq \frac{1}{2} n(\beta).$$

Jsou-li dána dvě celá čísla z tělesa $R(\zeta)$, α a β, hledá se jich „největší společná míra“, t. j. onen dělitel čísel α, β, v němž jsou všichni společní dělitelé čísel α, β obsaženi zcela analogicky jako při číslech celých v tělese $R(i)$. Na základě Euklidova algorithmu dokáže se pak základní věta theorie dělitelnosti celých čísel v tělese $R(\zeta)$:

Každé celé číslo z tělesa $R(\zeta)$ lze rozložiti „podstatně" jediným způsobem v součin prvočinitelů. Při tom slovo „podstatně" značí, že rozklady, lišící se jen tím, že místo prvočinitelů rozkladu jednoho jsou v druhém prvočinitelé associovaní, nepokládáme za různé.

Poznámka. Určení prvočísel v tělese $R(\zeta)$ jest také zcela podobné určení prvočísel v $R(i)$. I zde jest každé prvočíslo π dělitelem jistého přirozeného prvočísla p a jest $n(\pi) = p$ neb p^2. Je-li $n(\pi) = p$, $p = \pi\pi'$, jest π prvočíslem prvního stupně, je-li $n(\pi) = p^2$ bude π prvočíslem stupně druhého a bude associováno s p.

V případě prvočísla prvního stupně $\pi = r + \zeta s$, jest $p = n(\pi) = r^2 - rs + s^2 = (r + s)^2 - 3rs$.

Není-li $p = 3$, nesmí býti tedy $r + s$ dělitelno třemi, tak že $r + s \equiv \pm 1 \pmod 3$, $(r + s)^2 \equiv 1 \pmod 3$ a $p \equiv 1 \pmod 3$. Poněvadž prvočísla (vyjma 3) mají buď tvar $6n + 1$ neb $6n + 5$, musí býti v případě prvočísla stupně prvního $\neq 3$ jistě $p \equiv 1 \pmod 6$.

Přirozená prvočísla tvaru $6n + 5$ jsou pak v $R(\zeta)$ prvočísly druhého stupně.

Pro 3 máme:

$$3 = n(1 - \zeta) = (1 - \zeta)(1 - \zeta^2) = -\zeta^2(1 - \zeta)^2,$$

tak že *3 jest associováno se čtvercem prvočísla $1 - \zeta$.*

O prvočíslech přirozených tvaru $6n + 1$ platí pak, že v tělese $R(\zeta)$ nejsou již prvočísly.

Plyne to z toho, že by kongruence $x^{p-1} \equiv 1 \pmod p$ měla více než $p - 1$ kořenů nekongruentních, totiž

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

Rozpadají se tudíž přirozená prvočísla tvaru $6n + 1$ v tělese $R(\zeta)$ v součin dvou konjugovaných činitelů. Činitelé ty nejsou spolu associovány.

§ 5.

Značí-li α, β, γ celá čísla z tělesa třetích kořenů z jednotky, z nichž žádné není rovno nulle, není splněna nikdy rovnice

$$\alpha^3 + \beta^3 + \gamma^3 = 0. \qquad (1)$$

V rovnici (1) můžeme samozřejmě pokládati α, β, γ za čísla nesoudělná.

Položme

$$\lambda = 1 - \zeta = \frac{3 - \sqrt{-3}}{2} = \sqrt{-3} \cdot \zeta^2,$$

tak že jest λ číslo associované s $\sqrt{-3}$; λ^2 jest associováno se 3.

Ukážeme nejprve, že, má-li býti rovnice (1) vůbec splněna, musí býti nutně jedno z čísel α, β, γ dělitelno λ.

Není-li číslo α dělitelno λ, pišme

$$\alpha = a + b\zeta = a + b - b(1 - \zeta) = a + b - b\lambda,$$

z čehož vidíme, že $a + b$ nesmí býti dělitelno λ a tedy, poněvadž jest to číslo racionálné, ani ne 3.

Bude tedy

$$a + b \equiv \pm 1 \pmod 3,$$

tak že

$$\alpha \equiv \pm 1 \pmod \lambda.$$

Z toho plyne (neboť 3 jsou dělitelny λ^2), že pro číslo α nedělitelné λ platí kongruence

$$\alpha^3 \equiv \pm 1 \pmod{\lambda^3}.$$

Nejsou-li β a γ dělitelná λ, jest podobně

$$\beta^3 \equiv \pm 1 \pmod{\lambda^3}$$
$$\gamma^3 \equiv \pm 1 \pmod{\lambda^3}.$$

Bylo by tedy

$$\alpha^3 + \beta^3 + \gamma^3 \equiv \pm 1, \ \pm 3 \pmod{\lambda^3},$$

a poněvadž ani ± 1, ani ± 3 není $\equiv 0 \pmod{\lambda^3}$, obdrželi bychom důsledek, který jest ve sporu s rovnicí (1), čímž nemožnost rovnice (1) pro případ, že žádné z čísel α, β, γ není λ dělitelno, dokázána.

Obraťme se nyní k předpokladu, že by jedno z čísel α, β, γ, na př. γ, bylo λ dělitelno. Položme $\gamma = \lambda^n \gamma_1$ a uvažujme hned rovnici obecnější

$$\alpha^3 + \beta^3 = \varepsilon \lambda^{3n} \gamma_1, \qquad (2)$$

kdež ε značí libovolnou jednotku tělesa $R(\zeta)$.

Rovnici (2) můžeme psáti, rozložíme-li levou stranu v činitele, ve tvaru

$$(\alpha + \beta)\ (\alpha + \beta\xi)\ (\alpha + \beta\zeta^2) = \varepsilon\lambda^{3n}\gamma_1^3. \qquad (3)$$

Pravá strana jest dělitelná prvočíslem λ; musí tedy býti i na levé straně jeden činitel λ dělitelný. Poněvadž však činitelé ty jsou spolu kongruentní (*mod* λ), bude

$$\alpha + \beta \equiv \alpha + \beta\zeta \equiv \alpha + \beta\xi^2 \equiv 0 \ (mod\ \lambda). \qquad (4)$$

Ježto α, β jsou čísla nedělitelná λ, jsou $\equiv \pm 1$ (*mod* λ) a sice musí býti, aby splněny byly kongruence (4), buď

$$\alpha \equiv 1, \qquad \beta \equiv -1 \ (mod\ \lambda)$$

neb

$$\alpha \equiv -1, \qquad \beta \equiv 1 \ (mod\ \lambda).$$

Uvažujme dále jeden z těchto případů, na př. první (ke druhému bychom přišli, kdybychom zaměnili spolu α a β, což jest dovoleno, poněvadž se tím rovnice (2) nemění).

Můžeme psáti

$$\alpha = 1 + \lambda\mu, \quad \beta = -1 + \lambda\nu,$$

kdež μ, ν jsou čísla celá. Pak jest

$$\alpha + \beta = \lambda(\mu + \nu)$$
$$\alpha + \beta\zeta = \lambda(\mu + \nu + 1) - \lambda^2\nu$$
$$\alpha + \beta\zeta^2 = \lambda(\mu + \nu + 2) + \lambda^2(1 - 2\nu) + \lambda^3\nu.$$

Z čísel $\mu + \nu$, $\mu + \nu + 1$, $\mu + \nu + 2$ je jedno jistě dělitelno λ, bude tedy z čísel $\alpha + \beta$, $\alpha + \beta\zeta$, $\alpha + \beta\zeta^2$ jistě jedno dělitelno λ^2.

Vidíme tedy, že levá strana v rovnici (3) jest dělitelna aspoň λ^4, z čehož plyne ihned nemožnost rovnice (3) pro případ $n = 1$.

Předpokládejme tedy $n > 1$.

Poněvadž se rovnice (2) nemění, píšeme-li v ní $\beta\zeta$ neb $\beta\zeta^2$ místo β, lze změnou označení převésti $\alpha + \beta\zeta$ a $\alpha + \beta\zeta^2$ v $\alpha + \beta$. Stačí tedy uvažovati případ, kdy $\alpha + \beta$ jest dělitelno λ^2.

Kterékoliv dva faktory levé strany v rovnici (3) mohou míti za společnou míru jen λ. Uvažujme na př. $\alpha + \beta$ a $\alpha + \beta\zeta$.

Pak máme

$$(\alpha + \beta) - (\alpha + \beta\xi) = \beta\lambda,$$
$$\xi(\alpha + \beta) - (\alpha + \beta\xi) = -\alpha\lambda,$$

tak že společný činitel $\alpha + \beta$ a $\alpha + \beta\xi$ musí býti obsažen také v $\beta\lambda$ a $-\alpha\lambda$. Z toho plyne dále, že jen $\alpha + \beta$ jest dělitelno λ^2, $\alpha + \beta\xi$ a $\alpha + \beta\xi^2$ jsou dělitelna pouze λ.

Rovnici (3) nelze pak jinak vyhověti, než když položíme

$$\alpha + \beta = \eta_1 \lambda^{3n-2} \gamma'^3,$$
$$\alpha + \beta\xi = \eta_2 \lambda \alpha'^3,$$
$$\alpha + \beta\xi^2 = \eta_3 \lambda \beta'^3,$$

kdež η_1, η_2, η_3 jsou jednotky a α', β', γ' celá čísla z tělesa $R(\xi)$.

Vyloučíme-li z těchto rovnic α a β tím, že je násobíme po řadě 1, ξ, ξ^2 a sečteme, obdržíme

$$\eta_1 \lambda^{3n-2} \gamma'^3 + \eta_2 \xi \lambda \alpha'^3 + \eta_3 \xi^2 \lambda \beta'^3 = 0.$$

Dělme $\eta_2 \xi \lambda$. Tak obdržíme rovnici

$$\alpha'^3 + \vartheta \beta'^3 = \varepsilon' \lambda^{3(n-1)} \gamma'^3, \tag{5}$$

kdež ϑ a ε' jsou opět jednotky.

Poněvadž $n > 1$, jest

$$\alpha'^3 + \vartheta \beta'^3 \equiv 0 \ (mod\ \lambda^3).$$

Avšak pro čísla nedělitelná λ jest

$$\alpha'^3 \equiv \pm 1 \ (mod\ \lambda^3), \qquad \beta'^3 \equiv \pm 1 \ (mod\ \lambda^3),$$

tedy

$$\vartheta \equiv \pm 1 \ (mod\ \lambda^3)$$

a též

$$\vartheta \equiv \pm 1 \ (mod\ 3).$$

Z jednotek vyhovují pouze ± 1 této kongruenci, tak že $\vartheta = \pm 1$ a rovnice (5) nabude tvaru

$$\alpha'^3 + \beta'^3 = \varepsilon' \lambda^{3(n-1)} \gamma'^3, \tag{6}$$

píšeme-li, v případě, že $\vartheta = -1$, $-\beta'$ místo β'.

Rovnice (6) jest téhož typu jako (2), jen že jest v ní $n - 1$ místo n. Týmž způsobem, jako jsme přešli od rovnice (2) k rovnici (6), mohli bychom přejíti od rovnice (6) k rovnici téhož typu jako (2), kde by bylo n zmenšeno o 2 a tak podobně až k rovnici s $n = 1$, která, jak již podotknuto, jest nemožná.

Tím věta, vyřčená na počátku tohoto §, dokázána.