Pavel Kraemer

Zákon reciprocity v teorii čísel

In: Jindřich Bečvář (editor); Eduard Fuchs (editor): Člověk-umění-matematika. Sborník přednášek z letních škol Historie matematiky. (Czech). Praha: Prometheus, 1996. pp. 178–186.

Persistent URL: http://dml.cz/dmlcz/400558

CARL FRIEDRICH GAUSS

(1777 – 1855)

ZÁKON RECIPROCITY V TEORII ČÍSEL

PAVEL KRAEMER

Matematika je královnou všech věd
a teorie čísel
je královnou matematiky.
K. F. Gauss

Historický úvod.

Již od dob Pythagorových byli lidé fascinováni světem přirozených čísel. Viděli, že v něm panuje jistý řád a jisté zákony. Na rozdíl od geometrie byly ovšem tyto zákony hlouběji skryty a proto se lidé zpočátku museli spokojit s útržkovitými znalostmi. Hledaly se různé pythagorejské trojúhelníky, objevovala se nová dokonalá čísla, zkoumala se dělitelnost čísel.

To však duchu řeckých filosofů, toužícím po obecném, nemohlo stačit. A tak se objevují první obecná tvrzení. Snad nejdůležitějším pro teorii čísel je věta o nekonečném počtu prvočísel, která je dokázána v Eukleidových *Základech*. Řekové rovněž znali obecný postup pro řešení lineárních diofantovských rovnic, který dodnes nese Eukleidovo jméno. Snad by toho Řekové objevili více, kdyby se jejich zrak neodvrátil od aritmetiky ke geometrii, kdyby pokračovali v té linii, kterou započal Pythagoras.

Řeckou aritmetiku se podařilo vzkřísit až ve 3. století n. l. Diofantovi z Alexandrie. Diofantos zkoumal mimo jiné problém rozkladu čísel na čtverce. Jeho spisy podnítily Pierra de Fermata, zakladatele moderní teorie čísel, aby se hlouběji zabýval touto problematikou. Fermat se ptal, jaká prvočísla se dají napsat jako součet dvou nebo více čtverců, popř. jako součet čtverce a daného násobku jiného čtverce. Podívejme se na některá tvrzení, ke kterým dospěl.

Věty o součtu čtverců.

Liché prvočíslo je součtem dvou čtverců právě tehdy, když je tvaru $4n + 1$.
Liché prvočíslo je součtem čtverce a dvojnásobku čtverce právě tehdy, když je tvaru $8n + 1$ nebo $8n + 3$.
Liché prvočíslo různé od tří je součtem čtverce a trojnásobku čtverce právě tehdy, když je tvaru $3n + 1$.
Liché prvočíslo různé od pěti je součtem čtverce a pětinásobku čtverce právě tehdy, když je tvaru $20n + 1$ nebo $20n + 9$.

O tom, zda tato tvrzení Fermat také dokázal, žádné svědectví nemáme. Je to však přinejmenším pravděpodobné, neboť Fermat prohlásil, že důkazy má. A na rozdíl od mnoha matematiků své doby Fermat přesně věděl, co je a co není matematický důkaz. To, že skoro žádné důkazy nepublikoval, nás nesmí překvapit. V té době bylo dosti obecným zvykem publikovat dosažené výsledky bez jejich odvození.[1]

[1] Podrobný rozbor této problematiky je možno najít ve Weilově knize [8]. Weil se zde mimo jiné snaží naznačit, jak asi mohly vypadat Fermatovy důkazy těchto tvrzení.

K tomu, aby liché prvočíslo, které nedělí číslo n, bylo vyjádřitelné formou $x^2 + ny^2$, je nutné, aby p bylo dělitelem této formy, tzn. aby $p \mid x^2 + ny^2$ pro nějaká nesoudělná x, y. Je-li tomu tak, říkáme, že $-n$ je *kvadratický zbytek* (mod p). K tomu, abychom dokázali Fermatova tvrzení, je tedy především třeba vědět, pro jaká p je -1 resp. -2 resp. -3 resp. -5 *kvadratický zbytek* (mod p).[2] Na tyto otázky nám dává vyčerpávající odpověď tzv. *kvadratický zákon reciprocity*. Z tohoto zákona vyplývá, že takováto p jsou členy jistých aritmetických posloupností o diferenci n nebo $4n$. Jak jsme viděli, pro některá malá n tyto posloupnosti nalezl už Fermat.[3] Dříve než vyslovíme kvadratický zákon reciprocity, seznámíme se s některými základními vlastnostmi kvadratických zbytků.

Kvadratické zbytky.

Nejprve uvedeme klasickou definici kvadratického zbytku, která je, jak lze snadno nahlédnout, ekvivalentní s naší předchozí definicí.

Definice. Buď p liché prvočíslo, které nedělí celé číslo a. Existuje-li celé číslo x takové, že $a \equiv x^2 \pmod{p}$, říkáme, že a je *kvadratickým zbytkem* (mod p), a píšeme $\left(\frac{a}{p}\right) = +1$. V opačném případě je a *kvadratickým nezbytkem* (mod p), a píšeme $\left(\frac{a}{p}\right) = -1$.

Důležité pro počítání s kvadratickými zbytky je tzv.

Eulerovo kritérium. $\left(\frac{a}{p}\right) \equiv a^{p-1} \pmod{p}$

Důkaz. Je známo (tzv. *Malá Fermatova věta*), že $a^{p-1} \equiv 1 \pmod{p}$. Takže

$$0 \equiv a^{p-1} - 1 \equiv (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \pmod{p} .$$

1) Je-li $\left(\frac{a}{p}\right) = 1$, pak $a \equiv x^2 \pmod{p}$. Umocníme-li tuto kongruenci na $\frac{p-1}{2}$, dostaneme $a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod{p}$.
Je vidět, že zbytků (mod p) je přesně $\frac{p-1}{2}$ — jsou to čísla $1^1, 2^2, \cdots, (\frac{p-1}{2})^2$ a tato čísla dávají různé zbytky (mod p) .
2) Je-li $\left(\frac{a}{p}\right) = -1$, pak neplatí $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, neboť $a^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p}$ má právě $\frac{p-1}{2}$ řešení. Podle předchozího jich má totiž alespoň $\frac{p-1}{2}$, více než $\frac{p-1}{2}$ jich však mít nemůže, neboť v tělese všech zbytků (mod p) má každý polynom nad tímto tělesem nanejvýš tolik kořenů, kolik je jeho stupeň.[4] Tudíž $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$. □

---

[2] Pro $n = -1, -2, -3$ je otázka, zda liché p je tvaru $x^2 + ny^2$, ekvivalentní s otázkou, zda p je dělitelem této formy. Obecně tyto dvě otázky ekvivalentní nejsou. Dá se elementárně dokázat, že je-li možné v okruhu celých čísel tělesa $Q[\sqrt{-n}]$ zavést dělení se zbytkem, pak ekvivalence platí. Takových kvadratických těles (říkáme jim eukleidovská) je však pouze konečně mnoho.

[3] Viz předchozí poznámka.

[4] Důkaz probíhá obdobně jako pro těleso komplexních čísel.

Důsledek. *Jsou-li a, b celá čísla nesoudělná s p, pak* $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Nyní již můžeme vyslovit

Kvadratický zákon reciprocity. *Jsou-li p, q lichá prvočísla, je*

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

Doplňující věty k zákonu reciprocity. [5]

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

Nyní již můžeme ospravedlnit naše tvrzení o tom, že prvočísla, která jsou děliteli formy $x^2 + ny^2$, jsou obsažena v jistých aritmetických posloupnostech. Pro jednoduchost budeme předpokládat, že n je liché prvočíslo. Máme totiž

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

Protože první dva činitelé závisí jen na zbytku $p \pmod 4$ a poslední činitel závisí jen na zbytku $p \pmod n$, závisí celý výraz pouze na tom, jaký zbytek dává $p \pmod{4n}$. Tedy to, zda je p dělitelem formy $x^2 + ny^2$, závisí pouze na tom, do jaké posloupnosti o diferenci $4n$ prvočíslo p patří.

Historický vývoj.

Kvadratický zákon reciprocity byl objeven v letech 1744 až 1746 Leonhardem Eulerem. Euler, vědom si jeho důležitosti, se pokoušel o důkaz; jeho snaha však nebyla korunována úspěchem. Eulerovy výsledky byly publikovány až roku 1783, a tak upadla tato věta na dlouhou dobu v zapomnění.

Roku 1785 Legendre znovu objevil kvadratický zákon reciprocity a podal neúplný důkaz. Neúplnost důkazu spočívala v tom, že Legendre využíval skutečnosti, že v každé aritmetické posloupnosti existuje nekonečně mnoho prvočísel.[6] Tuto velice hlubokou větu dokázal až Dirichlet metodami algebraické teorie čísel.[7]

Dne 8. 4. 1796 podal osmnáctiletý Gauss první úplný důkaz kvadratického zákona reciprocity. Zveřejnil ho roku 1801 ve svém epochálním díle *Disquisitiones Mathematicae*. Důkaz je naprosto elementární, využívá velmi důmyslně matematickou indukci. O svém objevu Gauss píše:

---

[5] Obě tvrzení byla v pozměněné formě známa už Fermatovi – jsou totiž triviálními důsledky prvních dvou Fermatových vět o součtu čtverců, které jsme si uvedli na začátku. První bylo dokázáno Eulerem, druhé Lagrangem.

[6] Rozumí se tím, pochopitelně, posloupnosti $an + b$, kde a, b jsou celá nesoudělná čísla.

[7] I když Dirichlet využíval nástrojů matematické analýzy, nejedná se ještě o analytickou teorii čísel, neboť nejsou používány metody teorie funkcí.

Větu jsem zcela samostatně objevil roku 1795, v době, kdy jsem neměl nejmenší ponětí o tom, co bylo ve vyšší aritmetice již dosaženo. Neměl jsem sebemenší literární pomůcky. Celý rok mě tato věta mučila a vzdorovala nejhouževnatějším pokusům, až jsem konečně dospěl k důkazu uvedenému ve čtvrté části onoho díla.

O dva měsíce později přivedlo Gausse studium teorie kvadratických forem podnícené četbou děl Lagrangeových a Legendreových k druhému důkazu tohoto zákona, který sice není elementární, ale dává více nahlédnout do podstaty problému a *důvodu* jeho platnosti. Týž rok nalezl další dva důkazy využívající vyšší kongruence a teorie kruhových těles.

O pět let později podal pátý, velmi elegantní důkaz využívající vlastností tzv. Gaussových součtů.

Roku 1807 objevil Gauss tzv. Gaussovo lemma dovolující dokázat kvadratický zákon reciprocity způsobem běžným v učebnicích elementární teorie čísel. Tento důkaz je asi nejjednodušší; nepodařilo se ho však zobecnit na vyšší zákony reciprocity.[8]

Během svého života podal Gauss celkem osm důkazů. Následovaly desítky dalších. Cauchy, Jacobi, Eisenstein, Liouville, Kummer ..., ti všichni považovali za užitečné dokázat tento zákon nějakým novým způsobem. O tom, jak velký význam přikládal Gauss zákonu reciprocity, se můžeme poučit z jeho vlastních slov:

Tato základní věta o kvadratických zbytcích, kterou je nutno počítat mezi nejvyšší pravdy vyšší aritmetiky, byla snadno objevena induktivní cestou, ale její důkaz byl neobyčejně obtížný. V tomto odvětví matematiky se často stává, že se badateli samy zjevují jednoduché zákonitosti, ale jejich důkazy jsou velmi hluboko skryty a mohou být vyneseny na světlo úplně jiným způsobem, než se očekávalo. Dále se nezřídka stává, že poté, co byla nalezena cesta k důkazu, otvírají se další cesty, které vedou k témuž cíli — některé kratší a přímější, jiné jsou jakoby vedlejším důsledkem různých principů, o jejichž souvislosti se studovaným problémem jsme předtím neměli tušení. Tyto podivuhodné souvislosti mezi skrytými pravdami propůjčují těmto úvahám zvláštní půvab; zasluhují si být proto důkladně prozkoumány a zdůvodněny, nebot jejich studiem získáváme nové prostředky k obohacení věd.

Důkaz kvadratického zákona reciprocity.

Uvedeme důkaz kvadratického zákona reciprocity, který využívá Gaussovy součty. Tento důkaz zde uvádíme proto, že existuje podobný důkaz pro kubický či bikvadratický případ.[9] Gauss začal používat tyto součty roku 1796 pro eukleidovskou konstrukci pravidelného sedmnáctiúhelníku. Jsou velmi jednoduchým a přitom velmi mocným prostředkem k řešení mnoha číselně teoretických problémů.

[8] Zobecněním této metody se Gaussovi podařilo určit bikvadratický charakter čísla 2, tj. zjistit, pro jaká p je číslo 2 bikvadratickým zbytkem.

[9] V kubickém, resp. bikvadratickém případě je ovšem díky jistým technickým komplikacím příslušný důkaz mnohem delší.

Definice. Gaussovým součtem, který přísluší prvočíslu p, rozumíme součet $S(p) = \sum_{i=1}^{p-1} \left(\frac{i}{p}\right)\varepsilon^i$, kde ε je primitivní p-tá odmocnina z jedné.[10]

Hodnotu Gaussova součtu lze přesně spočítat; k našemu důkazu stačí znát jeho druhou mocninu.[11]

Věta.

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

Důkaz.

$$S(p)^2 = \left(\sum_{i=1}^{p-1}\left(\frac{i}{p}\right)\varepsilon^i\right)\left(\sum_{k=1}^{p-1}\left(\frac{k}{p}\right)\varepsilon^k\right) = \sum_{1\le i,k\le p-1}\left(\frac{ik}{p}\right)\varepsilon^{i+k}$$

Je-li i pevné a probíhá-li k redukovaný systém zbytků (mod p), probíhá též ik redukovaný systém zbytků (mod p). Můžeme proto místo k psát ik :

$$\begin{aligned} S(p)^2 &= \sum_{1\le i,k\le p-1}\left(\frac{i^2k}{p}\right)\varepsilon^{i+ik} = \sum_{1\le i,k\le p-1}\left(\frac{k}{p}\right)\varepsilon^{i(1+k)} = \\ &= \sum_{k=1}^{p-1}\left(\frac{k}{p}\right)\left(\sum_{i=1}^{p-1}\varepsilon^{i(1+k)}\right) = \sum_{k=1}^{p-2}\left(\frac{k}{p}\right)\left(\sum_{i=1}^{p-1}\varepsilon^{i(1+k)}\right) + \left(\frac{-1}{p}\right)\sum_{i=1}^{p-1}\varepsilon^0 = \\ &= \sum_{k=1}^{p-2}\left(\frac{k}{p}\right)\left(\sum_{l=1}^{p-1}\varepsilon^l\right) + \left(\frac{-1}{p}\right)(p-1) = \sum_{k=1}^{p-2}\left(\frac{k}{p}\right)(-1) + \left(\frac{-1}{p}\right)p - \\ &- \left(\frac{-1}{p}\right) = \left(\frac{-1}{p}\right)p - \sum_{k=1}^{p-1}\left(\frac{k}{p}\right) = \left(\frac{-1}{p}\right)p\,, \end{aligned}$$

neboť zbytků je stejně jako nezbytků. Během důkazu jsme použili identitu $1 + \sum_{i=1}^{p-1}\varepsilon^i = 0$ pro součet kořenů rovnice $x^p - 1 = 0$. □

Lemma. *Je-li q prvočíslo různé od p, pak platí*

$$S(p,q) = \sum_{i=1}^{p-1}\left(\frac{i}{p}\right)\varepsilon^{iq} = \left(\frac{q}{p}\right)S(p)\,. \tag{2}$$

Důkaz.

$$\sum_{i=1}^{p-1}\left(\frac{i}{p}\right)\varepsilon^{iq} = \left(\frac{q}{p}\right)\sum_{i=1}^{p-1}\left(\frac{q}{p}\right)\left(\frac{i}{p}\right)\varepsilon^{iq} = \left(\frac{q}{p}\right)\sum_{i=1}^{p-1}\left(\frac{qi}{p}\right)\varepsilon^{iq} =$$

[10] To znamená, že $\varepsilon^p = 1$ a přitom $\varepsilon \neq 1$.

[11] Známe-li druhou mocninu nějakého čísla, známe toto číslo až na znaménko. Právě určení znaménka Gaussova součtu je kamenem úrazu. Sám Gauss toto znaménko hledal několik let. Nakonec ho, zřejmě inspirován některými identitami z teorie eliptických funkcí, našel.

$$= \left(\frac{q}{p}\right) \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \varepsilon^k = \left(\frac{q}{p}\right) S(p) \quad \square$$

Přistupme nyní k vlastnímu důkazu. Bez újmy na obecnosti budeme předpokládat, že $q > p$. Umocníme-li (1) na $\frac{q+1}{2}$ a odečteme-li od výsledku (2) vynásobenou součtem $S(p)$, dostaneme

$$S(p)^{q+1} - S(p)S(p,q) = (-1)^{\frac{1}{2}(p-1)\frac{1}{2}(q+1)} p^{\frac{1}{2}(q+1)} - \left(\frac{q}{p}\right) S(p)^2 \; ; \qquad (3)$$

dosadíme-li sem hodnotu $S(p)^2 = (-1)^{\frac{1}{2}(p-1)} p$, dostaneme

$$S(p)\,(S(p)^q - S(p,q)) = (-1)^{\frac{1}{2}(p-1)} p \left((-1)^{\frac{1}{2}(p-1)\frac{1}{2}(q-1)} p^{\frac{1}{2}(q-1)} - \left(\frac{q}{p}\right) \right) \qquad (4)$$

Pro stručnost označme levou stranu jako Λ. Roznásobíme-li $S(p)^q$ podle multinomické věty, dostaneme jednotlivé sčítance Gaussova součtu umocněné na q, a spoustu dalších členů dělitelných q.

$$S(p)^q = \sum_{i=1}^{p-1} \left(\frac{i}{p}\right)^q \varepsilon^{qi} + q\beta = S(p,q) + q\beta \; ,$$

kde β je celočíselný polynom v ε. Proto $\Lambda = qS(p)\beta$, tedy

$$\Lambda = q(A + B\varepsilon + C\varepsilon^2 + \ldots + K\varepsilon^{p-1}) \; ,$$

kde $A, B, C, \ldots, K$ jsou celá čísla. Naším cílem je ukázat, že q dělí pravou stranu rovnosti (4). Na první pohled vypadá, že je to zřejmé, neboť q dělí levou stranu, tj. Λ. To jsme však zatím nedokázali, neboť v předchozí rovnosti jde o dělitelnost v okruhu $Z[\varepsilon]$, což není totéž. Nicméně tato obtíž se dá jednoduše obejít. Stačí si uvědomit, že vůbec nezáleží na tom, kterou z primitivních odmocnin ε jsme vzali. Stejně tak bychom mohli vzít kteroukoli z ostatních primitivních kořenů $\varepsilon^2, \varepsilon^3 \ldots \varepsilon^{p-1}$. Dostali bychom tyto rovnice:

$$\begin{aligned}
\Lambda &= q(A + B\varepsilon + C\varepsilon^2 + \ldots + K\varepsilon^{p-1}) \\
\Lambda &= q(A + B\varepsilon^2 + C\varepsilon^{2\cdot 2} + \ldots + K\varepsilon^{(p-1)\cdot 2}) \\
&\ldots\ldots\ldots\ldots\ldots\ldots \\
\Lambda &= q(A + B\varepsilon^{p-1} + C\varepsilon^{2\cdot(p-1)} + \ldots + K\varepsilon^{(p-1)(p-1)})
\end{aligned}$$

Sečteme-li těchto $p-1$ rovnic, dostaneme

$$(p-1)\Lambda = q\,((p-1)A - B - C - \ldots - K) \; .$$

Proto $q|(p-1)\Lambda$, z čehož vzhledem k předpokladu $q > p$ plyne, že q dělí pravou stranu rovnosti (4). Tedy

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

Upravíme-li podle Eulerova kritéria, dostaneme

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

z čehož už plyne dokazované tvrzení. $\square$

Vyšší zákony reciprocity.

Přední matematici 19. století se snažili zobecnit kvadratický zákon reciprocity na kongruence s vyššími exponenty. Podařilo se jim dokázat kubický a bikvadratický zákon reciprocity. Co se týče exponentů $n \geq 5$, byli už méně úspěšní. Abychom si ujasnili, o co vlastně šlo, podívejme se, jak to vypadá s kubickými zbytky. Budeme se řídit analogií s kvadratickými zbytky. Ukazuje se, že je třeba počítat v okruhu $Z[\rho]$, kde ρ je primitivní třetí odmocnina z jedné, tj. $\rho^3 = 1$, $\rho \neq 1$.

Definice. Nechť π je prvočíslo v $Z[\rho]$, $N(\pi) \neq 3$, π nedělí a.[12] Existuje-li číslo $x \in Z[\rho]$ takové, že $a \equiv x^3 \pmod{\pi}$, říkáme, že a je *kubickým zbytkem* (mod π), a píšeme $\left(\frac{a}{\pi}\right)_3 = +1$.

Z definice je jasné, že $\left(\frac{a^3}{\pi}\right)_3 = 1$. Analogicky jako v kvadratickém případě budeme požadovat, aby $\left(\frac{ab}{\pi}\right)_3 = \left(\frac{a}{\pi}\right)_3 \left(\frac{b}{\pi}\right)_3$. Speciálně $\left(\frac{a^3}{\pi}\right)_3 = \left(\frac{a}{\pi}\right)_3^3$, tedy $\left(\frac{a}{\pi}\right)_3^3 = 1$, tudíž $\left(\frac{a}{\pi}\right)_3 = \rho^i$, kde $i = 1$, nebo 2, nebo 3. Abychom zachovali multiplikativnost, budeme definovat kubický ekvivalent Legendreova symbolu pomocí obdoby Eulerova kritéria. Snadno se ukáže, že předkládaná definice je ve shodě s naší předchozí definicí.

Definice. Pro prvočíslo π takové, že $N(\pi) \neq 3$, definujme $\left(\frac{a}{\pi}\right)_3$ tak, aby platilo $\left(\frac{a}{\pi}\right)_3 \equiv a^{\frac{N(\pi)-1}{3}} \pmod{\pi}$.[13]

O tom, že je tato definice korektní, nás přesvědčí následující věta.

Malá Fermatova věta v okruhu $Z[\rho]$.

$$a^{N(\pi)-1} \equiv 1 \pmod{\pi}$$

Podobně jako v kvadratickém případě odsud plyne, že $a^{\frac{N(\pi)-1}{3}} \equiv \rho^i \pmod{\pi}$, kde $i = 1$, 2 nebo 3. Nyní již můžeme vyslovit

Kubický zákon reciprocity. *Jsou-li π, β primární*[14] *prvočísla v $Z[\rho]$, potom*

$$\left(\frac{\pi}{\beta}\right)_3 = \left(\frac{\beta}{\pi}\right)_3$$

Stručný vývoj vyšších zákonů reciprocity.

1750: V letech 1750–52 objevuje Euler několik zákonitostí vztahujících se k vyšším zákonům reciprocity.

[12] π je prvočíslo v $Z[\rho]$, když je nelze napsat jako součin dvou čísel z $Z[\rho]$ různých od jednotky. Jednotky jsou přitom ta čísla, jejichž norma je rovna jedné. V našem tělese máme šest jednotek: $\pm 1, \pm\rho, \pm\rho^2$.

[13] $N(\pi)$ značí normu čísla π. Je-li $\pi = a + b\rho$, pak $N(\pi) = (a+b\rho)(a+b\rho^2) = a^2 - ab + b^2$.

[14] Prvočíslo $\pi = a + b\rho$ je primární, když $a \equiv 2 \pmod{3}$ a $b \equiv 0 \pmod{3}$. Pro $N(\pi) \neq 3$ je z šesti čísel $\pm\pi$, $\pm\pi\rho$, $\pm\pi\rho^2$ vždy právě jedno primární.

1805: Od tohoto roku studuje Gauss kubický a bikvadratický zákon reciprocity. Pokouší se o důkaz, ale marně.

1817: Gauss oznamuje, že se mu podařilo najít cestu, jak dokázat bikvadratický zákon reciprocity.

1828: Gauss publikuje svůj první článek o bikvadratických zbytcích. Dokazuje, že číslo 2 je bikvadratickým zbytkem prvočísel p takových, že $p = a^2+b^2$ a 8 dělí b. Důkaz tohoto tvrzení je velmi zdlouhavý.

1832: Gauss píše další článek, v němž používá komplexní čísla typu $a + bi$.

1827: Jacobi vyslovuje kubický zákon reciprocity. Používá čísla typu $a+b\sqrt{-3}$.

1837: Jacobi údajně přednesl na přednášce důkaz kubického zákona reciprocity.

1844: Eisenstein publikuje své důkazy kubického a bikvadratického zákona reciprocity. Jacobi ho obviňuje z plagiátství:
Tyto důkazy, známé z četných opisů mých přednášek, byly nedávno publikovány panem Eisensteinem.
Eisenstein je šokován a tvrdí, že nebyl ovlivněn ničím jiným než Gaussovými články. Jeho odpověď byla stručná:
Výzkumy pana Jacobiho mi byly naprosto neznámy. Považuji za zbytečné, rozvádět toto téma, neboť mé pozdější práce snadno dokazují nezávislost mých výzkumů.
Jacobi studuje zbytky pátého, osmého a dvanáctého stupně. Nedaří se mu dokázat nalezené zákonitosti. Eisensteinovy snahy zůstávají též bez úspěchu. Problém byl mimo jiné v tom, že věta o jednoznačném rozkladu prvočísel neplatí pro většinu kruhových těles.

1847: Kummerovi se podaří zformulovat zákon reciprocity pro ideální prvočísla.

1850: Eisenstein předkládá veřejnosti svůj zákon reciprocity, zahrnující i čísla složená. Tento zákon, obecnější než Kummerův, čekal na důkaz plných padesát let. Vděčíme za něj Furtwänglerovi.

1859: Kummer dokazuje zákon reciprocity pro ideální prvočísla.

1900: Jedním ze slavných Hilbertových problémů je úloha, dokázat zákon reciprocity pro obecná algebraická tělesa.

1928: Artin dokazuje po něm nazvaný všeobecný zákon reciprocity.

LITERATURA

[1] H. Edwards, *Fermat's Last Theorem. A Genetical Introduction to Algebraic Number Theory*, Springer-Verlag, New York, 1977.

[2] F. G. M. Eisenstein, *Mathematische Werke*, Bd. 1, 2, Chelsea, New York, 1975.

[3] C. F. Gauss, *Werke*, Bd. 1, 2, Göttingen–Leipzig–Berlin, 1870–1933.

[4] N. Koblitz (ed.), *Number Theory Related to Fermat's Last Theorem*, Birkhäuser, Boston-Basel-Stuttgart, 1983.

[5] H. Pieper, *Variationen über ein Zahlentheoretisches Thema von Carl Friedrich Gauss*, Birkhäuser, Basel, 1978.

[6] W. Scharlau, H. Opolka, *From Fermat to Minkowski*, Springer–Verlag, New York, 1985.

[7] H. J. Smith, *A Report on the Theory of Numbers*, Collected Mathematical Works, Clarendon Press, Oxford, 1894.

[8] A. Weil, *From Hammurapi to Legendre*, Birkhäuser, Basel, 1984.