UNIVERZITA PALACKÉHO V OLOMOUCI
PŘÍRODOVĚDECKÁ FAKULTA
KATEDRA ALGEBRY A GEOMETRIE

BAKALÁŘSKÁ PRÁCE

Čísla ve tvaru součtů druhých mocnin

Vedoucí bakalářské práce:
Mgr. Michal Botur, Ph.D.
Rok odevzdání: 2011

Vypracoval:
Petr Uřičář
DISMAT, III. ročník

Prohlášení

Prohlašuji, že jsem tuto bakalářskou práci zpracoval samostatně pod vedením pana Mgr. Michala Botura, Ph.D. a že jsem v seznamu literatury uvedl všechny použité zdroje.

V Olomouci dne 9. srpna 2011

Poděkování

Rád bych na tomto místě poděkoval vedoucímu své bakakářské práce panu Mgr. Michalu Boturovi, Ph.D. za trpělivost a cenné rady, které mi pomohly k dokončení této práce.

Obsah

Úvod

Problém existence a určení takových přirozených čísel n, které je možné vyjádřit jako součet dvou druhých mocnin přirozených (nezáporných) čísel, tj. ve tvaru $n = x^2 + y^2$ pro některá $x, y \in \mathbb{N}$, je nedílnou součástí teorie čísel. Pro tato čísla bylo už v minulosti vysloveno a dokázáno hned několik velice zajímavých výsledků.

Lze tato čísla nějak charakterizovat? Pro uvedení do problematiky se můžeme podívat na několik prvních přirozených čísel.

$$1 = 1^2 + 0^2$$
$$2 = 1^2 + 1^2$$
$$3 = ??$$
$$4 = 2^2 + 0^2$$
$$5 = 2^2 + 1^2$$
$$6 = ??$$
$$7 = ??$$
$$8 = 2^2 + 2^2$$

Jak je patrné, ne všechna čísla lze tímto způsobem vyjádřit.

Hlavním cílem této práce je tedy zaměřit se na nejdůležitější známá fakta o těchto číslech, jejich vlastnostech a zabývat se existencí a případnými možnostmi nalezení jejich reprezentace ve tvaru součtu čtverců.

1 Čísla ve tvaru součtu čtverců

V této kapitole charakterizujeme čísla, která lze vyjádřit jako součet druhých mocnin přirozených čísel.

1.1 Prvočísla

Pokud je p prvočíslo, pak množina $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ společně s operacemi sčítání a násobení modulo p tvoří konečné těleso.

Lemma 1.1. *Nechť p je prvočíslo. Potom $0^2, 1^2, 2^2, \ldots, \lfloor \frac{p}{2} \rfloor^2$ tvoří různé prvky tělesa $\mathbb{Z}_p$.*

Důkaz. Je-li $x^2 \equiv y^2 \pmod{p}$, pak $(x-y)(x+y) \equiv 0 \pmod{p}$, a tedy $x \equiv y \pmod{p}$ nebo $x \equiv -y \pmod{p}$. □

Lemma 1.2. *Nechť p je prvočíslo. Potom rovnice $s^2 \equiv -1 \pmod{p}$ má pro $p = 4m+1$ dvě řešení $s \in \{1, 2, \ldots, p-1\}$, pro $p = 2$ jedno řešení a žádné řešení pro $p = 4m+3$.*

Důkaz. V případě $p = 2$ je zřejmě jediným řešením $s = 1$. Je-li $p \neq 2$, definujme na množině $\{1, 2, \ldots, p-1\}$ ekvivalenci E, jejíž třídy rozkladu jsou

$$[x]_E = \{x, -x, \overline{x}, -\overline{x}\},$$

kde $-x$ je inverzní prvek vzhledem ke sčítání, $\overline{x}$ je inverzní prvek vzhledem k násobení a $-\overline{x}$ je inverzní prvek k $\overline{x}$ vzhledem ke sčítání v tělese $\mathbb{Z}_p$. Tyto prvky jsou pro každé $x \in \mathbb{Z}_p$ určeny jednoznačně, a E tedy tvoří rozklad množiny $\{1, 2, \ldots, p-1\}$.

Podívejme se detailněji na tyto třídy. Jelikož $x \not\equiv -x \pmod{p}$ pro lichá p, uvažujme pouze následující dva možné případy.

Prvním případem je

$$x \equiv \overline{x} \pmod{p}. \tag{1}$$

Vynásobením obou stran výrazem x dostaneme rovnici $x^2 \equiv 1 \pmod{p}$, která má podle Lemmatu 1.1 dvě řešení, $x_1 = 1$ a $x_2 = p - 1$. Protože $x_1 \equiv -x_2 \pmod{p}$, odpovídá těmto dvěma řešením v ekvivalenci E jediná třída, a to $\{1, p-1\}$. Tato situace nastane pro každé liché prvočíslo p.

Druhým možným případem je

$$x \equiv -\overline{x} \pmod{p}. \tag{2}$$

Obdobně, vynásobením výrazem x dostaneme $x^2 \equiv -1 \pmod{p}$. Uvažujme dále, že řešením této rovnice, pokud existují, jsou $x_1 = x$ a $x_2 = p - x$. Podobně jako v prvním případě, odpovídá těmto řešením jediná třída ekvivalence E, třída $\{x, p - x\}$.

Ekvivalence E má tedy alespoň jednu a zároveň maximálně dvě třídy, které mají 2 prvky, a třídy, které mají 4 různé prvky.

Nechť $p = 4m + 3$, pak má množina $\{1, 2, \ldots, p - 1\}$ $4m + 2$ prvků. Jelikož situace v případě (1) nastane pro každé prvočíslo $p \neq 2$, nemůže nastat (2) a rovnice $s^2 \equiv -1 \pmod{p}$ nemá řešení.

Pro $p = 4m + 1$ má množina $\{1, 2, \ldots, p - 1\}$ $4m$ prvků. Protože jiná situace než v případech (1) a (2) nastat nemůže, existuje třída $\{x, p-x\}$, jejíž prvky jsou řešením $s^2 \equiv -1 \pmod{p}$. □

Věta 1.1. *Žádné přirozené číslo n ve tvaru $n = 4m+3$ nelze vyjádřit jako součet čtverců.*

Důkaz. Pro každé přirozené číslo n platí:

$$n^2 \equiv \begin{cases} 0 \pmod{4} & \text{pro } n = 2k \\ 1 \pmod{4} & \text{pro } n = 2k + 1 \end{cases}$$

Z toho vyplývá, že každé přirozené číslo $n = x^2 + y^2$ je kongruentní s $0, 1$ nebo $2 \pmod{4}$. □

Definice 1.1. Nechť $f \neq id$ je zobrazení na množině M. Řekneme, že f je involuce (involutorní zobrazení), jestliže $f \circ f = id$, tj. $f(f(x)) = x$ pro každé $x \in M$.

Věta 1.2. *Každé prvočíslo p ve tvaru $p = 4m + 1$ je součtem čtverců.*

Důkaz. Důkaz je založen na třech involucích a jejich pevných bodech. Nechť je $p = 4m + 1$ prvočíslo. Uvažujme nyní množinu S definovanou způsobem

$$S = \{(x, y, z) \in \mathbb{Z}^3 \mid 4xy + z^2 = p, \quad x, y > 0\}.$$

Tato množina je jistě neprázdná a vzhledem k tomu, že $x, y > 0$, také konečná. Jelikož p je prvočíslo, je $z \neq 0$.

Nyní zavedeme první involuci $f : S \longrightarrow S$ definovanou předpisem

$$f((x, y, z)) = (y, x, -z). \tag{3}$$

Lze snadno nahlédnout, že takto definované zobrazení je involuce na S, protože $(y, x, -z) \in S$ a $f(f((x, y, z))) = f((y, x, -z)) = (x, y, z)$. Navíc f nemá na S žádný pevný bod, jelikož $(x, y, 0) \notin S$.

Dále definujme podmnožiny T, U množiny S a podívejme se na chování zobrazení f na prvcích těchto množin. Nechť platí

$$T = \{(x, y, z) \in S \mid z > 0\}.$$

Pro každý prvek $(x, y, z) \in T$ platí, že $f((x, y, z)) = (y, x, -z) \notin T$, protože $-z < 0$, ale prvek $(y, x, -z) \in S$. Zobrazení f tedy zobrazuje množinu T na množinu $S \setminus T$ a naopak. Pak ale $|S| = 2|T|$.

Dále nechť

$$U = \{(x, y, z) \in S \mid x - y + z > 0\}.$$

Pro každý prvek $(x, y, z) \in U$ platí, že $f((x, y, z)) = (y, x, -z) \notin U$, protože $y - x - z = -(x - y + z) < 0$, ale prvek $(y, x, -z) \in S$. Dále nechť $x - y + z = 0$, potom $z = y - x$ a $p = 4xy + (y - x)^2 = (y + x)^2$, což je spor s předpokladem,

že p je prvočíslo. Tedy $x - y + z \neq 0$. Zobrazení f tedy zobrazuje množinu U na množinu $S \setminus U$ a naopak. Pak ale $|S| = 2|U|$.

Porovnáním výsledků dostáváme $|S| = 2|T| = 2|U|$, z čehož vyplývá, že množiny T a U mají stejný počet prvků.

Nyní zavedeme druhou involuci $g : U \longrightarrow U$ definovanou předpisem

$$g((x, y, z)) = (x - y + z, y, 2y - z)\,. \tag{4}$$

Ověříme, že zobrazení g je správně definované. Jelikož $(x, y, z) \in U$, pak

$$\begin{aligned} x - y + z &> 0\,, \\ y &> 0\,, \\ 4(x - y + z)y + (2y - z)^2 &= 4xy + z^2\,, \end{aligned}$$

a tedy $g((x, y, z)) \in S$. Dále jelikož $(x - y + z) - y + (2y - z) = x > 0$, tak také $g((x, y, z)) \in U$.

Zobrazení g je involuce, protože

$$\begin{aligned} g(g((x, y, z))) &= g((x - y + z, y, 2y - z)) \\ &= (x - y + z - y + 2y - z, y, 2y - 2y + z) \\ &= (x, y, z)\,. \end{aligned}$$

Nakonec ukažme, že g má na U právě jeden pevný bod.

Platí, že (x, y, z) je pevný bod (tj. $g((x, y, z)) = (x, y, z)$), právě tehdy když

$$\begin{aligned} x - y + z &= x\,, \\ y &= y\,, \\ 2y - z &= z\,. \end{aligned}$$

Snadno ověříme, že toto je ekvivalentní s $y = z$. Jelikož $p = 4xy + z^2$ je prvočíslo ve tvaru $4m + 1$, je jediným bodem (x, y, z), pro který platí $y = z$, bod $(m, 1, 1)$, který je tedy jediným pevným bodem involuce g. Jestliže má ale g na konečné

množině U právě jeden pevný bod, pak má množina U lichý počet prvků, a tím pádem má lichý počet prvků i množina T.

Třetí involuci $h : T \longrightarrow T$ definujme předpisem

$$h((x, y, z)) = (y, x, z)\,. \tag{5}$$

Snadno lze vidět, že $h((x, y, z)) \in T$ a že h je involuce. Podle předchozího má množina T lichý počet prvků a je konečná. Pak má ale involuce h alespoň jeden pevný bod $(x, y, z) \in T$, pro který platí, že $x = y$. Z toho plyne, že $p = (2x)^2 + z^2$, a tedy $p = 4m + 1$ je součtem čtverců. □

Poznámka 1.1. Ve skutečnosti je až na pořadí toto vyjádření jediné. Důkaz tohoto tvrzení provedeme později.

Prvočísla tedy můžeme rozdělit do třech tříd. Prvočíslo $p = 2$, které je součtem čtverců, třída prvočísel ve tvaru $4m + 3$, která nelze vyjádřit jako součet čtverců, a prvočísla ve tvaru $4m + 1$, pro která toto vyjádření existuje.

1.2 Složená čísla

Lemma 1.3. *Nechť jsou přirozená čísla m a n součty čtverců. Pak je součtem čtverců i jejich součin mn.*

Důkaz. Jelikož jsou přirozená čísla m, n součty dvou čtverců, lze je psát ve tvaru $m = x_1^2 + y_1^2$, $n = x_2^2 + y_2^2$. Potom platí

$$\begin{aligned} mn &= (x_1^2 + y_1^2)(x_2^2 + y_2^2) \\ &= (x_1x_2)^2 + (y_1y_2)^2 + (x_1y_2)^2 + (y_1x_2)^2 - 2x_1x_2y_1y_2 + 2x_1x_2y_1y_2 \\ &= (x_1x_2 - y_1y_2)^2 + (x_1y_2 + y_1x_2)^2\,. \end{aligned}$$

Tedy $mn = x^2 + y^2$, kde $x = |x_1x_2 - y_1y_2|$ a $y = x_1y_2 + y_1x_2$, je součtem čtverců. □

Věta 1.3. *Nechť $n = x^2 + y^2$ je součet čtverců a p je prvočíslo ve tvaru $4m + 3$. Jestliže $p \mid n$, pak $p \mid x$ a zároveň $p \mid y$.*

Důkaz. Předpokládejme, že platí opak. Tedy $p \mid n$ a zároveň platí, že $p \nmid x$ nebo $p \nmid y$. Uvažujme například, že p nedělí x. Potom tedy $x \not\equiv 0 \pmod{p}$ a existuje $\overline{x}$ takové, že $x\overline{x} \equiv 1 \pmod{p}$. Vynásobením obou stran rovnice $x^2+y^2 \equiv 0 \pmod{p}$ výrazem $\overline{x}^2$ dostaneme $1+(\overline{x}y)^2 \equiv 0 \pmod{p}$, což je rovnice $(\overline{x}y)^2 \equiv -1 \pmod{p}$, která podle Lemmatu 1.2 nemá pro $p = 4m + 3$ řešení, což je spor. Tedy $p \mid x$ (analogicky $p \mid y$). □

Důsledek 1.1. *Nechť prvočíslo $p = 4m + 3$ je dělitelem čísla $n = x^2 + y^2$. Pak je také p^2 dělitelem čísla n a číslo $\dfrac{n}{p^2}$ je opět součtem čtverců.*

Důkaz. Z předchozí věty plyne $p \mid x$ a $p \mid y$, a tedy $\dfrac{n}{p^2} = \left(\dfrac{x}{p}\right)^2 + \left(\dfrac{y}{p}\right)^2$. □

Na základě předchozích vět můžeme na závěr vyslovit hlavní výsledek této části, jímž je nutná a postačující podmínka pro vyjádření přirozeného čísla jako součtu dvou čtverců.

Věta 1.4. *Přirozené číslo n je součtem dvou čtverců, právě tehdy když se v jeho prvočíselném rozkladu vyskytují všechny členy tvaru $4m + 3$ se sudou mocninou.*

Důkaz. Každý prvočíselný rozklad přirozeného čísla $n \geq 2$ lze psát ve tvaru

$$n = 2^{\alpha} p_1^{\alpha_1} \cdots p_k^{\alpha_k} q_1^{\beta_1} \cdots q_l^{\beta_l},$$

kde $p_i \equiv 1 \pmod{4}$ a $q_j \equiv 3 \pmod{4}$ jsou prvočísla a $\alpha, \alpha_i, \beta_j$ jsou nezáporná celá čísla.

Čísla $1 = 1^2 + 0^2$ a $2 = 1^2 + 1^2$ jsou součty čtverců. Každý člen p_i je podle Věty 1.2 součtem čtverců. Nechť $\beta_j = 2\gamma_j$ pro každé $j \in \{1, \ldots, l\}$, kde γ_j je nějaké nezáporné celé číslo. Potom každý člen $q_j^2 = 0^2 + q_j^2$ je součtem čtverců. Užitím emmatu 1.3 dostáváme jednu část tvrzení.

Nechť $n = x^2+y^2$ je součtem čtverců a $p = 4m+3$ je libovolný prvočinitel čísla n. Podle Důsledku 1.1 tedy $p^2 \mid n$ a číslo $\dfrac{n}{p^2} = \left(\dfrac{x}{p}\right)^2 + \left(\dfrac{y}{p}\right)^2$ lze opět vyjádřit jako součet čtverců. Stejný postup je možné opakovat pro všechny další případné prvočinitele čísla $\dfrac{n}{p^2}$ ve tvaru $4m + 3$. □

2 Počet způsobů vyjádření

V této kapitole se zaměřme na počet způsobů vyjádření čísla jako součtu dvou čtverců, neboli na počet všech neuspořádaných dvojic $(x, y) \in \mathbb{N}_0^2$, pro které platí $n = x^2 + y^2$. Vidíme například, že číslo $50 = 1^2 + 7^2 = 5^2 + 5^2$ lze vyjádřit dvěma způsoby.

Pro další účely této části textu zavedeme následující označení.

$s_k(n)\ldots$ funkce, jejíž hodnotou je 1, pokud $n = kx^2$ pro některé $x \in \mathbb{N}_0$, jinak $s_k(n) = 0$

$r_2(n)\ldots$ počet uspořádaných dvojic $(x, y) \in \mathbb{Z}^2$ splňujících $n = x^2 + y^2$

$R_2(n)\ldots$ počet neuspořádaných dvojic $(x, y) \in \mathbb{N}_0^2$ splňujících $n = x^2 + y^2$

$d_k(n)\ldots$ počet všech dělitelů čísla n ve tvaru $4m + k$

Jako motivaci pro nalezení počtu způsobů těchto reprezentací uvažujme následující situaci. Vezmeme nekonečný součet ve tvaru $(1 + q + q^4 + q^9 + q^{16} + \cdots)$ a umocníme jej na druhou[1]. Tedy

$$\left(\sum_{n\geq 0} q^{n^2}\right)^2 = (1 + q + q^4 + q^9 + q^{16} + \cdots)^2$$
$$= \sum_{k\geq 0,\, l\geq 0} q^{(k^2+l^2)} = \sum_{n\geq 0} a(n)q^n\,.$$

Potom koeficient $a(n)$ u takto naznačeného součinu je součtem počtu všech uspořádaných dvojic $(x, y) \in \mathbb{N}_0^2$ splňujících $n = x^2 + y^2$. Poslední sumu můžeme také vyjádřit jako

$$\sum_{k\geq 0,\, l\geq 0} q^{(k^2+l^2)} = \sum_{k\geq 0} q^{2k^2} + 2\sum_{k>l\geq 0} q^{(k^2+l^2)}$$
$$= \sum_{n\geq 0} s_2(n)q^n + 2\sum_{n\geq 0} b(n)q^n\,,$$

[1]Všechny symboly Σ a Π v této kapitole jsou užity pro formální vyjádření nekonečných součtů a součinů. Všechny rovnosti mezi těmito vyjádřeními jsou ve smyslu rovností koeficientů u stejných mocnin.

kde koeficient $b(n)$ udává počet všech dvojic $(x, y) \in \mathbb{N}_0^2$, pro které platí $x > y$ a $x^2 + y^2 = n$. Můžeme tedy prozatím vyjádřit $R_2(n)$ jako

$$R_2(n) = s_2(n) + b(n) \tag{6}$$

2.1 Jacobiho věta o součtu dvou čtverců

Nyní se podívejme na funkci $r_2(n)$. Použitím naprosto stejné úvahy můžeme psát

$$\left(\sum_{-\infty}^{\infty} q^{n^2}\right)^2 = \sum_{n\geq 0} r_2(n) q^n \,.$$

Vhodnou úpravou výrazu na levé straně získáme poměrně zajímavý vztah pro vyjádření $r_2(n)$. Tento vztah je známý též jako Jacobiho věta o součtu dvou čtverců, která je společně s dalšími důsledky hlavním tématem [3] a [4]. Před vyslovením této věty ještě ale uveďme identitu, kterou využijeme v jejím důkazu.

Věta 2.1. *(Jacobiho třísoučinová identita [2])*

$$\prod_{n\geq 1} (1 + aq^{2n-1})(1 + a^{-1}q^{2n-1})(1 - q^{2n}) = \sum_{-\infty}^{\infty} a^n q^{n^2} \,.$$

Důkaz. viz. [2] str. 333. □

Věta 2.2. *(Jacobiho věta o součtu dvou čtverců)*

Počet všech způsobů vyjádření přirozeného čísla n ve tvaru součtu dvou čtverců je roven čtyřnásobku rozdílu mezi počtem dělitelů čísla n ve tvaru $4m+1$ a počtem dělitelů n ve tvaru $4m + 3$, tedy

$$r_2(n) = 4\big(d_1(n) - d_3(n)\big) \,.$$

Důkaz. Dosadíme-li do Jacobiho identity z předchozí věty $a = -a^2 q$ a následně $q^2 = q$, dostaneme

$$\prod_{n\geq 1} (1 - a^2 q^n)(1 - a^{-2} q^{n-1})(1 - q^n) = \sum_{-\infty}^{\infty} (-1)^n a^{2n} q^{\frac{n^2+n}{2}} \,.$$

[2] volný překlad anglického názvu Jacobi's triple product identity

Úpravou levé strany a následným vynásobením obou stran číslem a získáme

$$(a-a^{-1})\prod_{n\geq 1}(1-a^2q^n)(1-a^{-2}q^n)(1-q^n)=\sum_{-\infty}^{\infty}(-1)^n a^{2n+1}q^{\frac{n^2+n}{2}}$$

a dalšími úpravami pravé strany a opětovným užitím Jacobiho identity převedeme na tvar

$$\begin{aligned}\sum_{-\infty}^{\infty}(-1)^n a^{2n+1}q^{\frac{n^2+n}{2}} &= \sum_{-\infty}^{\infty}a^{4n+1}q^{2n^2+n}-\sum_{-\infty}^{\infty}a^{4n-1}q^{2n^2-n}\\ &= a\sum_{-\infty}^{\infty}\left(a^4q\right)^n\left(q^2\right)^{n^2}-a^{-1}\sum_{-\infty}^{\infty}\left(a^4q^{-1}\right)^n\left(q^2\right)^{n^2}\\ &= a\prod_{n\geq 1}(1+a^4q^{4n-1})(1+a^{-4}q^{4n-3})(1-q^{4n})\\ &\quad -a^{-1}\prod_{n\geq 1}(1+a^4q^{4n-3})(1+a^{-4}q^{4n-1})(1-q^{4n})\,.\end{aligned}$$

Pro zjednodušení označme

$$\begin{aligned}P_n &= (1+a^4q^{4n-1})(1+a^{-4}q^{4n-3})(1-q^{4n})\,,\\ Q_n &= (1+a^4q^{4n-3})(1+a^{-4}q^{4n-1})(1-q^{4n})\,.\end{aligned}$$

Získali jsme tedy

$$(a-a^{-1})\prod_{n\geq 1}(1-a^2q^n)(1-a^{-2}q^n)(1-q^n)=a\prod_{n\geq 1}P_n-a^{-1}\prod_{n\geq 1}Q_n\,. \qquad (7)$$

Derivací levé strany podle a a následným dosazením $a=1$ dostaneme

$$2\prod_{n\geq 1}(1-q^n)^3$$

a s využitím vztahu pro derivaci součinu

$$\Big(\prod_{n\geq 1}f_n\Big)'=\Big(\prod_{n\geq 1}f_n\Big)\sum_{n\geq 1}\frac{f_n'}{f_n}$$

zderivujeme také pravou stranu podle a. Tedy

$$\begin{aligned}\Big(a\prod_{n\geq 1}P_n\Big)' &= \prod_{n\geq 1}P_n + a\Big(\prod_{n\geq 1}P_n\Big)' \\ &= \prod_{n\geq 1}P_n + a\Big(\prod_{n\geq 1}P_n\Big)\sum_{n\geq 1}\frac{P_n'}{P_n} \\ &= \Big(\prod_{n\geq 1}P_n\Big)\left(1 + a\sum_{n\geq 1}\frac{P_n'}{P_n}\right)\end{aligned}$$

a analogicky

$$\begin{aligned}\Big(-a^{-1}\prod_{n\geq 1}Q_n\Big)' &= a^{-2}\prod_{n\geq 1}Q_n - a^{-1}\Big(\prod_{n\geq 1}Q_n\Big)' \\ &= a^{-2}\prod_{n\geq 1}Q_n - a^{-1}\Big(\prod_{n\geq 1}Q_n\Big)\sum_{n\geq 1}\frac{Q_n'}{Q_n} \\ &= \Big(\prod_{n\geq 1}Q_n\Big)\left(a^{-2} - a^{-1}\sum_{n\geq 1}\frac{Q_n'}{Q_n}\right),\end{aligned}$$

kde pro P_n'/P_n a Q_n'/Q_n platí

$$\begin{aligned}\frac{P_n'}{P_n} &= \frac{4a^3q^{4n-1}}{1+a^4q^{4n-1}} - \frac{4a^{-5}q^{4n-3}}{1+a^{-4}q^{4n-3}}\,, \\ \frac{Q_n'}{Q_n} &= \frac{4a^3q^{4n-3}}{1+a^4q^{4n-3}} - \frac{4a^{-5}q^{4n-1}}{1+a^{-4}q^{4n-1}}\,.\end{aligned}$$

Dosazením $a = 1$ do derivace pravé strany vztahu (7) tak získáme

$$\begin{aligned}\Big(a\prod_{n\geq 1}P_n - a^{-1}\prod_{n\geq 1}Q_n\Big)'_{a=1} &= T_n\left(1 + 4\sum_{n\geq 1}\left(\frac{q^{4n-1}}{1+q^{4n-1}} - \frac{q^{4n-3}}{1+q^{4n-3}}\right)\right) \\ &\quad + T_n\left(1 - 4\sum_{n\geq 1}\left(\frac{q^{4n-3}}{1+q^{4n-3}} - \frac{q^{4n-1}}{1+q^{4n-1}}\right)\right) \\ &= 2T_n\left(1 + 4\sum_{n\geq 1}\left(\frac{q^{4n-1}}{1+q^{4n-1}} - \frac{q^{4n-3}}{1+q^{4n-3}}\right)\right),\end{aligned}$$

kde

$$T_n = \prod_{n\geq 1}(1+q^{4n-1})(1+q^{4n-3})(1-q^{4n})$$

a celkově tedy dostáváme

$$\prod_{n\geq 1}(1-q^n)^3 = T_n\left(1+4\sum_{n\geq 1}\left(\frac{q^{4n-1}}{1+q^{4n-1}}-\frac{q^{4n-3}}{1+q^{4n-3}}\right)\right).$$

Nyní podělíme obě strany poslední rovnosti výrazem

$$\begin{aligned}\prod_{n\geq 1}(1+q^n)^2(1-q^n) &= \prod_{n\geq 1}(1+q^n)(1-q^{2n})\\ &= \prod_{n\geq 1}(1+q^{2n-1})(1+q^{2n})(1-q^{2n})\\ &= \prod_{n\geq 1}(1+q^{2n-1})(1-q^{4n})\\ &= \prod_{n\geq 1}(1+q^{4n-1})(1+q^{4n-3})(1-q^{4n})\\ &= T_n\end{aligned}$$

a obdržíme vztah

$$\prod_{n\geq 1}\left(\frac{1-q^n}{1+q^n}\right)^2 = 1+4\sum_{n\geq 1}\left(\frac{q^{4n-1}}{1+q^{4n-1}}-\frac{q^{4n-3}}{1+q^{4n-3}}\right). \tag{8}$$

Vezměmě nyní opět Jacobiho identitu, dosaďme $a=-1$ a dostaneme tak

$$\begin{aligned}\sum_{-\infty}^{\infty}(-1)^n q^{n^2} &= \prod_{n\geq 1}(1-q^{2n-1})^2(1-q^{2n})\\ &= \prod_{n\geq 1}\frac{(1-q^{2n-1})^2(1-q^{2n})^2}{1-q^{2n}}\\ &= \prod_{n\geq 1}\frac{(1-q^n)^2}{1-q^{2n}}\\ &= \prod_{n\geq 1}\frac{1-q^n}{1+q^n}.\end{aligned}$$

Nyní můžeme psát

$$\left(\sum_{-\infty}^{\infty}(-1)^n q^{n^2}\right)^2 = \prod_{n\geq 1}\left(\frac{1-q^n}{1+q^n}\right)^2 = 1+4\sum_{n\geq 1}\left(\frac{q^{4n-1}}{1+q^{4n-1}}-\frac{q^{4n-3}}{1+q^{4n-3}}\right)$$

a položíme-li $q = -q$, přepíšeme na

$$\left(\sum_{-\infty}^{\infty} q^{n^2}\right)^2 = 1 + 4\sum_{n\geq 1}\left(\frac{q^{4n-3}}{1-q^{4n-3}} - \frac{q^{4n-1}}{1-q^{4n-1}}\right). \tag{9}$$

S využitím vztahu

$$\frac{1}{(1-q)} = \sum_{l\geq 0} q^l$$

upravíme členy v závorce na pravé straně na

$$\frac{q^{4n-3}}{1-q^{4n-3}} = q^{4n-3}\sum_{l\geq 0}\left(q^{4n-3}\right)^l = \sum_{l\geq 1} q^{l(4n-3)}$$
$$\frac{q^{4n-1}}{1-q^{4n-1}} = \sum_{l\geq 1} q^{l(4n-1)}$$

Pro přehlednost dalšího kroku, nahraďme index n v sumě písmenem k a posloupností úprav pravé strany (9) dostaneme

$$\begin{aligned}
1 + 4\sum_{k\geq 1}\left(\frac{q^{4k-3}}{1-q^{4k-3}} - \frac{q^{4k-1}}{1-q^{4k-1}}\right) &= 1 + 4\sum_{k\geq 1}\left(\sum_{l\geq 1} q^{l(4k-3)} - \sum_{l\geq 1} q^{l(4k-1)}\right) \\
&= 1 + 4\sum_{k\geq 0}\left(\sum_{l\geq 1} q^{l(4k+1)} - \sum_{l\geq 1} q^{l(4k+3)}\right) \\
&= 1 + 4\sum_{k\geq 0,\, l\geq 1}\left(q^{l(4k+1)} - q^{l(4k+3)}\right).
\end{aligned}$$

Při bližším pohledu na poslední sumu vidíme, že koeficient u členu $q^n,\ n \geq 1$, je tvořen rozdílem součtu počtu dělitelů čísla n tvaru $4m+1$ a součtu počtu dělitelů n tvaru $4m + 3$. Tedy

$$\left(\sum_{-\infty}^{\infty} q^{n^2}\right)^2 = 1 + 4\sum_{n\geq 1}\Big(d_1(n) - d_3(n)\Big)q^n$$

a porovnáním koeficientů u stejných mocnin dostáváme tvrzení. □

Poznámka 2.1. Věta platí pro $n \geq 1$. Je-li $n = 0$, definujme $r_2(n) = 1$.

2.1.1 Důsledky Jacobiho věty

Důsledek 2.1. *Prvočíslo ve tvaru $p = 4m + 1$ lze až na pořadí vyjádřit jediným způsobem jako součet druhých mocnin přirozených čísel.*

Důkaz. Prvočíslo $p = 4m + 1$ má pouze 2 triviální dělitele, 1 a p. Potom ale $d_1(p) = 2$ a $d_3(p) = 0$, a podle předchozí věty je tedy celkem 8 uspořádaných dvojic $(x, y) \in \mathbb{Z}^2$, pro které platí $x^2 + y^2 = p$. Jelikož je p prvočíslo, je $x, y \neq 0$ a $|x| \neq |y|$. Jsou to tedy dvojice $(\pm x, \pm y)$ a $(\pm y, \pm x)$ pro některé $x, y \in \mathbb{N}$. □

Věta 2.3. *Nechť $n = 2^\alpha p_1^{\alpha_1} \cdots p_k^{\alpha_k} q_1^{\beta_1} \cdots q_l^{\beta_l}$ je přirozené číslo a $p_i \equiv 1 \pmod 4$, $q_j \equiv 3 \pmod 4$ jsou různá prvočísla. Je-li n součet dvou čtverců, pak platí*

1. $r_2(n) = r_2(p_1^{\alpha_1} \cdots p_k^{\alpha_k})$
2. $r_2(n) = 4(\alpha_1 + 1) \cdots (\alpha_k + 1)$

Důkaz. Nejprve ukažme, že $r_2(2^\alpha w) = r_2(w)$. Toto plyne okamžitě z Věty 2.2, jelikož vynásobíme-li každý dělitel čísla w číslem 2^α, nezískáme žádný další dělitel ve tvaru $4m + 1$, respektive $4m + 3$.

1. Jelikož je n součet čtverců, pak podle Věty 1.4 je β_j sudé pro všechna $j \in \{1, \ldots, l\}$ a dělitelé $q_j^{\beta_j}$ jsou $1, q_j, q_j^2, \ldots, q_j^{\beta_j}$, z nichž $\frac{\beta_j}{2} + 1$ je tvaru $4m + 1$ a $\frac{\beta_j}{2}$ tvaru $4m + 3$. Platnost ukážeme matematickou indukcí vzhledem k l.

Nechť $l = 1$. Jelikož všechny dělitelé $p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ jsou tvaru $4m + 1$, pak pro $p_1^{\alpha_1} \cdots p_k^{\alpha_k} q_1^{\beta_1}$ platí

$$d_1(p_1^{\alpha_1} \cdots p_k^{\alpha_k} q_1^{\beta_1}) = d_1(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) \left(\frac{\beta_1}{2} + 1 \right),$$
$$d_3(p_1^{\alpha_1} \cdots p_k^{\alpha_k} q_1^{\beta_1}) = d_1(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) \left(\frac{\beta_1}{2} \right),$$

a tedy

$$r_2(p_1^{\alpha_1} \cdots p_k^{\alpha_k} q_1^{\beta_1}) = 4d_1(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = r_2(p_1^{\alpha_1} \cdots p_k^{\alpha_k}).$$

Nechť pro $l - 1$ platí

$$r_2(p_1^{\alpha_1} \cdots p_k^{\alpha_k} q_1^{\beta_1}, \cdots, q_{l-1}^{\beta_{l-1}}) = r_2(p_1^{\alpha_1} \cdots p_k^{\alpha_k}),$$

potom

$$\begin{aligned} d_1(p_1^{\alpha_1}\cdots p_k^{\alpha_k}q_1^{\beta_1}\cdots q_l^{\beta_l}) &= d_1(p_1^{\alpha_1}\cdots p_k^{\alpha_k}q_1^{\beta_1}\cdots q_{l-1}^{\beta_{l-1}})\left(\frac{\beta_l}{2}+1\right) \\ &\quad + d_3(p_1^{\alpha_1}\cdots p_k^{\alpha_k}q_1^{\beta_1}\cdots q_{l-1}^{\beta_{l-1}})\left(\frac{\beta_l}{2}\right), \\ d_3(p_1^{\alpha_1}\cdots p_k^{\alpha_k}q_1^{\beta_1}\cdots q_l^{\beta_l}) &= d_1(p_1^{\alpha_1}\cdots p_k^{\alpha_k}q_1^{\beta_1}\cdots q_{l-1}^{\beta_{l-1}})\left(\frac{\beta_l}{2}\right) \\ &\quad + d_3(p_1^{\alpha_1}\cdots p_k^{\alpha_k}q_1^{\beta_1}\cdots q_{l-1}^{\beta_{l-1}})\left(\frac{\beta_l}{2}+1\right), \end{aligned}$$

a tedy

$$\begin{aligned} r_2(p_1^{\alpha_1}\cdots p_k^{\alpha_k}q_1^{\beta_1}\cdots q_l^{\beta_l}) &= 4d_1(p_1^{\alpha_1}\cdots p_k^{\alpha_k}q_1^{\beta_1}\cdots q_{l-1}^{\beta_{l-1}}) \\ &\quad - 4d_3(p_1^{\alpha_1}\cdots p_k^{\alpha_k}q_1^{\beta_1}\cdots q_{l-1}^{\beta_{l-1}}) \\ &= r_2(p_1^{\alpha_1}\cdots p_k^{\alpha_k}q_1^{\beta_1}\cdots q_{l-1}^{\beta_{l-1}}) \\ &= r_2(p_1^{\alpha_1}\cdots p_k^{\alpha_k}). \end{aligned}$$

2. Opět ukážeme platnost tvrzení matematickou indukcí vzhledem ke k. Všechny dělitelé $p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ jsou tvaru $4m+1$ a děliteli $p_i^{\alpha_i}$ jsou $1, p_i, p_i^2, \ldots, p_i^{\alpha_i}$.

Je-li $k=1$, pak $d_1(p_1^{\alpha_1}) = (\alpha_1+1)$ a tedy

$$r_2(p_1^{\alpha_1}) = 4(\alpha_1+1).$$

Nechť pro $k-1$ platí

$$r_2(p_1^{\alpha_1}\cdots p_{k-1}^{\alpha_{k-1}}) = 4(\alpha_1+1)\cdots(\alpha_{k-1}+1),$$

potom

$$\begin{aligned} d_1(p_1^{\alpha_1}\cdots p_k^{\alpha_k}) &= d_1(p_1^{\alpha_1}\cdots p_{k-1}^{\alpha_{k-1}})(\alpha_k+1) \\ &= (\alpha_1+1)\cdots(\alpha_k+1), \end{aligned}$$

a tedy

$$r_2(p_1^{\alpha_1}\cdots p_k^{\alpha_k}) = 4(\alpha_1+1)\cdots(\alpha_k+1).$$

□

Věta 2.4. *Nechť* $n = 2^{\alpha} p_1^{\alpha_1} \cdots p_k^{\alpha_k} q_1^{\beta_1} \cdots q_l^{\beta_l}$ *je přirozené číslo a* $p_i \equiv 1 \pmod 4$, $q_j \equiv 3 \pmod 4$ *jsou různá prvočísla. Pak pro počet všech způsobů vyjádření čísla* n *ve tvaru součtu dvou čtverců platí*

$$r_2(n) = 2\left(1 - (-1)^{(\beta_1+1)\cdots(\beta_l+1)}\right)(\alpha_1+1)\cdots(\alpha_k+1)\,.$$

Důkaz. Je-li n součet dvou čtverců, dostaneme 2. část věty 2.3. Není-li n součet dvou čtverců, je alespoň jedno β_j liché, a tedy $r_2(n) = 0$. □

Poznámka 2.2. Hodnota $r_2(n)$ nezáleží na hodnotách $p_1, \ldots, p_k, q_1, \ldots, q_l$, ale pouze na jejich mocninách.

Vraťme se nyní opět k funkci $R_2(n)$ a pokusme se najít její zajímavější vyjádření než ve vztahu (6). Podívejme se, zdali existuje nějaká souvislost tohoto vyjádření s funkcí $r_2(n)$.

Můžeme psát

$$\begin{aligned}
\left(\sum_{-\infty}^{\infty} q^{n^2}\right)^2 &= \left(1 + 2\sum_{n\geq 1} q^{n^2}\right)^2 = \left(2\sum_{n\geq 0} q^{n^2} - 1\right)^2 \\
&= 4\left(\sum_{n\geq 0} q^{n^2}\right)^2 - 4\sum_{n\geq 0} q^{n^2} + 1 \\
&= 4\sum_{n\geq 0} a(n)q^n - 4\sum_{n\geq 0} s_1(n)q^n + 1 \\
&= 1 + 4\sum_{n\geq 1}\big(a(n) - s_1(n)\big)q^n \\
&= 1 + 4\sum_{n\geq 1}\big(s_2(n) + 2b(n) - s_1(n)\big)q^n\,.
\end{aligned}$$

Podle věty 2.2 ale také platí

$$\left(\sum_{-\infty}^{\infty} q^{n^2}\right)^2 = 1 + \sum_{n\geq 1} r_2(n)q^n\,,$$

a porovnáme-li koeficienty u stejných mocnin, dostaneme pro $n \geq 1$

$$r_2(n) = 4\big(s_2(n) + 2b(n) - s_1(n)\big)\,.$$

Nyní využijeme vztahu (6) a dosazením a upravením získáme

$$R_2(n) = \frac{r_2(n) + 4\big(s_1(n) + s_2(n)\big)}{8}\,. \tag{10}$$

Podíváme-li se na funkční hodnoty funkcí $s_1(n)$ a $s_2(n)$, zjistíme, že pro $n \geq 1$ jsou buď obě nulové, nebo je-li $s_1(n) = 1$, je $s_2(n) = 0$, respektive naopak. Toto platí, jelikož kdyby platilo $x^2 = 2y^2$ pro nějaká $x, y \in \mathbb{N}$, pak $|\frac{x}{y}| = \sqrt{2}$, což je spor, jelikož $\sqrt{2}$ není racionální číslo. Součet $s_1(n) + s_2(n)$ je tedy 0 nebo 1.

Vztah (10) můžeme také napsat jako

$$R_2(n) = \frac{d_1(n) - d_3(n) + s_1(n) + s_2(n)}{2}\,,$$

a protože $R_2(n)$ je nezáporné celé číslo, je $d_1(n) - d_3(n) + s_1(n) + s_2(n)$ sudé. Potom tedy pro každé $n \geq 1$ platí

$$R_2(n) = \left\lceil \frac{d_1(n) - d_3(n)}{2} \right\rceil = \left\lceil \frac{r_2(n)}{8} \right\rceil\,. \tag{11}$$

2.2 Nejmenší čísla s vlastností $r_2(n), R_2(n)$

Pro $s \geq 1$ označme $N_s = \{n \in \mathbb{N} \mid r_2(n) = s\}$. Potom podle Věty 2.3 je každý prvek množiny N_s ve tvaru

$$n = 2^{\alpha} p_1^{\alpha_1} \cdots p_k^{\alpha_k} q_1^{2\beta_1} \cdots q_l^{2\beta_l}\,,$$

kde $p_i \equiv 1 \pmod 4$ a $q_j \equiv 3 \pmod 4$ jsou různá prvočísla a pro $\alpha_1, \ldots, \alpha_k$ platí, že $4(\alpha_1 + 1) \cdots (\alpha_k + 1) = s$.

Pokud $4 \mid s$, jsou tyto množiny zřejmě nekonečné. Podívejme se nyní, jak vypadají jejich nejmenší prvky, jinými slovy nejmenší čísla s vlastností $r_2(n) = s$.

Podle Věty 2.3 pro každé $n \in N_s$ platí $r_2(n) = r_2(p_1^{\alpha_1} \cdots p_k^{\alpha_k})$. Uvažujme dále, že $p_1, \ldots, p_k$ je posloupností k prvních prvočísel tvaru $4m + 1$ a množina $A = \{(\alpha_1, \ldots, \alpha_k) \in \mathbb{N}^k \mid \alpha_1 \geq \ldots \geq \alpha_k\}$ je množina všech řešení rovnice $4(\alpha_1+1) \cdots (\alpha_k+1) = s$. Potom nejmenší číslo s vlastností $r_2(n) = s$ je nejmenším prvkem množiny $\{p_1^{\alpha_1} \cdots p_k^{\alpha_k} \mid (\alpha_1, \ldots, \alpha_k) \in A\}$.

Obdobně pro $s \geq 1$ označme $M_s = \{n \in \mathbb{N} \mid R_2(n) = s\}$. S využitím vztahu (11) můžeme psát $M_s = N_{8s} \cup N_{8s-4}$.

Příklad 2.1. Najděte nejmenší číslo n, pro které platí $R_2(n) = 50$.

Hledáme tedy nejmenší prvek množiny $N_{400} \cup N_{396}$. Nejprve nalezneme všechny $(\alpha_1, \ldots, \alpha_k) \in \mathbb{N}^k, \alpha_1 \geq \ldots \geq \alpha_k$, pro které platí

$$4(\alpha_1 + 1) \cdots (\alpha_k + 1) = 400$$
$$4(\alpha_1 + 1) \cdots (\alpha_k + 1) = 396$$

a pro posloupnost $p_1, \ldots, p_k$ prvních k prvočísel tvaru $4m + 1$ určíme nejmenší z čísel $p_1^{\alpha_1} \cdots p_k^{\alpha_k}$.

$100 = 5 \cdot 5 \cdot 2 \cdot 2$	$(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = (4, 4, 1, 1)$	$5^4 \cdot 13^4 \cdot 17 \cdot 29$
$= 25 \cdot 2 \cdot 2$	$(\alpha_1, \alpha_2, \alpha_3) = (24, 1, 1)$	
$= 10 \cdot 5 \cdot 2$	$(\alpha_1, \alpha_2, \alpha_3) = (9, 4, 1)$	
$= 5 \cdot 5 \cdot 4$	$(\alpha_1, \alpha_2, \alpha_3) = (4, 4, 3)$	$5^4 \cdot 13^4 \cdot 17^3$
$= 50 \cdot 2$	$(\alpha_1, \alpha_2) = (49, 1)$	
$= 25 \cdot 4$	$(\alpha_1, \alpha_2) = (24, 3)$	
$= 20 \cdot 5$	$(\alpha_1, \alpha_2) = (19, 4)$	
$= 10 \cdot 10$	$(\alpha_1, \alpha_2) = (9, 9)$	
$= 100$	$(\alpha_1) = (99)$	
$99 = 11 \cdot 3 \cdot 3$	$(\alpha_1, \alpha_2, \alpha_3) = (10, 2, 2)$	
$= 11 \cdot 9$	$(\alpha_1, \alpha_2) = (10, 8)$	
$= 33 \cdot 3$	$(\alpha_1, \alpha_2) = (32, 2)$	
$= 99$	$(\alpha_1) = (98)$	

Porovnáme-li všechna čísla $p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, vidíme, že nejmenším z nich je číslo $5^4 \cdot 13^4 \cdot 17 \cdot 29$, a tedy nejmenším přirozeným číslem, pro které platí $R_2(n) = 50$, je $8\,800\,358\,125$.

3 Nalezení vyjádření

V předchozích kapitolách jsme se zabývali nutnými a postačujícími podmínkami, které čísla ve tvaru součtu druhých mocnin splňují, a počtem jejich různých reprezentací. Víme tedy, která čísla lze vyjádřit, a kolika způsoby. Nyní se nabízí otázka, zdali existuje nějaký efektivní způsob, kterým lze tato vyjádření nalézt.

3.1 Euklidův algoritmus

Euklidův algoritmus je algoritmus pro nalezení největšího společného dělitele (NSD), který je popsán např. v [5] na straně 11. Pro účely této kapitoly zmíníme pouze některé jeho vlastnosti, které využijeme v důkazu správnosti jeho užití k nalezení reprezentace přirozeného čísla jako součtu dvou čtverců.

Nechť $r_0 > r_1$. Uvažujme následující posloupnost rovnic, které popisují Euklidův algoritmus,

$$\begin{aligned}
r_0 &= q_1 r_1 + r_2 && r_1 > r_2 > 0\,,\\
r_1 &= q_2 r_2 + r_3 && r_2 > r_3 > 0\,,\\
&\vdots && \vdots\\
r_{n-2} &= q_{n-1} r_{n-1} + r_n && r_{n-1} > r_n > 0\,,\\
r_{n-1} &= q_n r_n && r_n = \mathrm{NSD}(r_0, r_1)\,.
\end{aligned}$$

Pak je posloupnost $r_0 = a, r_1 = b, r_2, \cdots, r_n$ posloupností zbytků Euklidova algoritmu s výchozími hodnotami a a b.

Pro posloupnost $\{r_i\}_0^n$ platí vztah

$$\begin{aligned}
r_0 &= a\,,\\
r_1 &= b\,,\\
r_i &= r_{i-2} - q_{i-1} r_{i-1} \qquad \text{pro } i \geq 2
\end{aligned} \tag{12}$$

a zpětným dosazením můžeme každé r_i vyjádřit jako lineární kombinaci vstupních

hodnot a a b. Tedy ve tvaru

$$r_i = s_i a + t_i b \tag{13}$$

pro jistá s_i a t_i.

Dosadíme-li (13) do vztahu pro r_i a porovnáme-li koeficienty u a a b, dostaneme stejné vztahy i pro posloupnosti $\{s_i\}_0^n$ a $\{t_i\}_0^n$.

$$\begin{aligned} s_0 &= 1 & t_0 &= 0 \\ s_1 &= 0 & t_1 &= 1 \\ s_i &= s_{i-2} - q_{i-1}s_{i-1} & t_i &= t_{i-2} - q_{i-1}t_{i-1} \qquad \text{pro } i \geq 2 \end{aligned}$$

Při bližším pohledu na posloupnost $\{t_i\}_0^n$ si můžeme všimnout některých vlastností.

1. Jelikož je $q_i \geq 1$ pro každé $i \in \{1, \ldots, n\}$, platí pro $i \geq 1$

$$\frac{t_i}{t_{i+1}} < 0$$

2. Je-li $q_1 \geq 2$, pak je posloupnost $\{|t_i|\}_0^n$ rostoucí. Jelikož pro $i \geq 1$ mají každé dva po sobě jdoucí členy opačná znaménka a $|t_i| > 0$, pak platí

$$|t_{i+1}| = |t_{i-1}| + q_i|t_i| \tag{14}$$

a jelikož $|t_2| = q_1 > |t_1|$, je pro každé i

$$|t_{i+1}| > |t_i|$$

Platí-li pro vstupní hodnoty a a b, že $\mathrm{NSD}(a, b) = 1$. Pak lze každý zbytek r_i vyjádřit ve tvaru $r_i = f(q_{i+1}, \ldots, q_n)$, kde funkce $f(q_1, \ldots, q_n)$ je ve tvaru součtu součinu $q_1 \cdots q_n$, a dále všech součinů, které vzniknou z $q_1 \cdots q_n$ vynecháním všech dvou po sobě jdoucích členů $q_i q_{i+1}$ a dále vynecháním všech takových členů z takto vzniklých součinů. V případě, že n je sudé, je vynechání všech po sobě jdoucích členů rovno 1. Například, $f(q_1, q_2, q_3, q_4) = q_1q_2q_3q_4 + q_1q_2 + q_1q_4 + q_3q_4 + 1$.

Jelikož $|t_{i+1}| = q_i|t_i| + |t_{i-1}|$ a je-li $q_1 \geq 2$, pak $|t_i| > |t_{i-1}|$, a definujeme-li $t_{n+1} = t_{n-1} - q_n t_n$, je posloupnost $\{|t_i|\}_{n+1}^1$ posloupností zbytků Euklidova

algoritmu s výchozími hodnotami $|t_{n+1}|$ a $|t_n|$. Vidíme, že při aplikaci algoritmu s těmito hodnotami je posloupnost $\{q_i\}$ v obráceném pořadí. Protože $\mathrm{NSD}(|t_{n+1}|, |t_n|) = 1$, je $r_0 = f(q_1, \ldots, q_n) = f(q_n, \ldots, q_1) = |t_{n+1}|$.

3.2 Algoritmus nalezení vyjádření

Nechť p je prvočíslo tvaru $4k + 1$. Algoritmus nalezení reprezentace p jako součtu dvou čtverců sestává z následujících dvou kroků.

1. Nalezneme x takové, že $x^2 \equiv -1 \pmod{p}$.
2. Provedeme Euklidův algoritmus s výchozími hodnotami p a x. První dva zbytky menší než $\sqrt{p}$ jsou hledané hodnoty.

Podle Lemmatu 1.2 víme, že x, pro které je $x^2 \equiv -1 \pmod{p}$, existuje. Podívejme se nyní na to, jakým způsobem jej můžeme nalézt.

Definice 3.1. Nechť $a \in \mathbb{Z}$ a $n \in \mathbb{N}$. Řekneme, že a je kvadratickým zbytkem modulo n, jestliže existuje $k \in \mathbb{N}$ takové, že $k^2 \equiv a \pmod{n}$.

Věta 3.1. *(Eulerovo kritérium)*

Nechť $p > 2$ je prvočíslo, $a \in \mathbb{Z}$ a $\mathrm{NSD}(a, p) = 1$. Pak $x^2 \equiv a \pmod{p}$ má dvě řešení, právě tehdy když $a^{(p-1)/2} \equiv 1 \pmod{p}$, a žádné řešení, právě tehdy když $a^{(p-1)/2} \equiv -1 \pmod{p}$.

Důkaz. viz. [5] str. 101. □

Důsledek 3.1. *Nechť $p > 2$ je prvočíslo, $a \in \mathbb{Z}$ a $\mathrm{NSD}(a, p) = 1$. Pak a není kvadratický zbytek modulo p, právě tehdy když $a^{(p-1)/2} \equiv -1 \pmod{p}$.*

Důkaz. Plyne přímo z Definice 3.1 a Věty 3.1. □

Pro nalezení řešení rovnice $x^2 \equiv -1 \pmod{p}$ pro $p = 4m + 1$ tedy nejprve nalezneme $c \in \mathbb{N}$, které není kvadratickým zbytkem modulo p. Podle předchozího

důsledku je $c^{2m} \equiv -1 \pmod{p}$. Za c volíme prvočíselné hodnoty a testujeme splnění podmínky, dokud jej nenalezneme. Za x pak bereme $c^m \pmod{p}$.

Před samotným důkazem správnosti tohoto algoritmu si vyzkoušejme jeho užití na nějakém konkrétním příkladu.

Příklad 3.1. Najděte vyjádření prvočísla 1993 jako součet čtverců.

Číslo 1993 je ve tvaru $4m + 1$, kde $m = 498$. Podle předchozího zjistíme, že 5 není kvadratickým zbytkem modulo 1993, a tedy $x = 5^{498} \pmod{1993} = 834$, $\sqrt{1993} \sim 44.64$.

		zbytek
$p = 1993$	$x = 834$	325
834	325	184
325	184	141
184	141	*43
141	43	*12

Podle tabulky jsou hledaná čísla 43 a 12. Snadno se můžeme přesvědčit, že skutečně $43^2 + 12^2 = 1849 + 144 = 1993$.

3.2.1 Důkaz správnosti algoritmu

Důkaz. Uvažujme nejprve, že x je řešením rovnice $x^2 \equiv -1 \pmod{p}$, pro které platí $x < p - x$. Potom $\mathrm{NSD}(p, x) = 1$ a $p > 2x$, z čehož plyne $q_1 > 2$ a $|t_{n+1}| = p$. Ze vztahu (13) také dostaneme $t_i b \equiv r_i \pmod{a}$, a tedy $t_n x \equiv 1 \pmod{p}$. Vynásobíme-li obě strany této rovnice x, dostaneme $t_n \equiv -x \pmod{p}$. Jelikož $|t_n| < p$, je t_n buď $-x$, nebo $p - x$. Druhý případ není možný, jinak by byla posloupnost $\{t_i\}$ delší než $\{r_i\}$. Tedy $t_n = -x$. Posloupnost $\{|t_i|\}_{n+1}^{1}$ je tudíž také posloupností zbytků Euklidova algoritmu s výchozími hodnotami p a x, a tedy platí

$$|t_i| = r_{n+1-i}\,. \tag{15}$$

Navíc, jelikož $t_1 = 1$, $t_n = -x$ a posloupnost $\{t_i\}_1^n$ mění s každým členem znaménko, je n sudé.

Dosaďme nyní rovnost $|t_i| = r_{n+1-i}$ do vztahu (14) a dostaneme tak

$$r_{n-i} = r_{n+2-i} + q_i r_{n+1-i}\,. \tag{16}$$

Podle (12) platí také $r_i = r_{i-2} - q_{i-1}r_{i-1}$ a položíme-li $i = n + 2 - i$, dostaneme

$$r_{n-i} = r_{n+2-i} + q_{n+1-i} r_{n+1-i}\,. \tag{17}$$

Porovnáme-li rovnosti (16) a (17), vidíme, že $q_i = q_{n+1-i}$. Posloupnost $\{q_i\}_1^n$ je tedy symetrická kolem svého středu.

Ze vztahu (13) také plyne, že $t_i x \equiv r_i \pmod p$. Umocněním obou stran rovnice získáme $r_i^2 + t_i^2 \equiv 0 \pmod p$, což můžeme pomocí (15) upravit a přepsat na

$$r_i^2 + r_{n+1-i}^2 \equiv 0 \pmod p\,.$$

Speciálně pro $i = n/2$ pak na

$$r_{n/2}^2 + r_{n/2+1}^2 \equiv 0 \pmod p\,.$$

Nyní stačí jen ukázat, že $r_{n/2}$ je první zbytek menší než $\sqrt{p}$. Potom

$$s = r_{n/2}^2 + r_{n/2+1}^2 < 2p\,,$$

a protože $p \mid s$, dostaneme okamžitě $s = p$.

Zbytek $r_{n/2}$ můžeme vyjádřit pomocí funkce f jako $r_{n/2} = f(q_{n/2+1}, \ldots, q_n)$ a s využitím symetrie posloupnosti $\{q_i\}_1^n$ dostáváme

$$r_{n/2}^2 = f(q_1, \ldots, q_{n/2}) f(q_{n/2+1}, \ldots, q_n)\,,$$

kde každý člen tohoto součinu je obsažen i v $f(q_1, \ldots, q_n) = p$. Potom $r_{n/2}^2 \le p$, a tedy platí

$$r_{n/2} \le \sqrt{p}\,.$$

Jelikož je $r_{n/2} > r_{n/2+1}$, potom je $r_{n/2}^2 + r_{n/2+1}^2 < 2p$.

Dále ukážeme, že předchozí zbytek $r_{n/2-1}$ je větší než $\sqrt{p}$. Jako v předchozím případě vyjádříme $r_{n/2-1}$ pomocí funkce f jako $r_{n/2-1} = f(q_{n/2}, q_{n/2+1}, \ldots, q_n)$ a opět využijeme symetrie $\{q_i\}_1^n$. Tedy

$$r_{n/2-1}^2 = f(q_1, \ldots, q_{n/2+1}) f(q_{n/2}, q_{n/2+1}, \ldots, q_n)\,.$$

Každý člen $f(q_1, \ldots q_n) = p$ je obsažen v předešlém součinu, z čehož plyne, že $r_{n/2-1}^2 \geq p$, a tedy

$$r_{n/2-1} \geq \sqrt{p}\,.$$

Aplikujeme-li Euklidův algoritmus s výchozími hodnotami p a $p - x$, pak je posloupností zbytků $p, p-x, x, \ldots$, kde další členy jsou stejné jako v posloupnosti zbytků Euklidova algoritmu s hodnotami p a x. Získáme tedy stejné vyjádření čísla p jako součtu dvou čtverců. □

Poznámka 3.1. Důkaz nevyžaduje nutnost prvočíselnosti p, ale pouze existenci řešení rovnice $x^2 \equiv -1 \pmod{p}$.

3.3 Použití algoritmu pro složená čísla

Podívejme se nyní na existenci řešení rovnice $x^2 \equiv -1 \pmod{n}$ pro libovolnné přirozené číslo n.

Věta 3.2. *Nechť a, b a $m > 0$ jsou celá čísla a $d = \mathrm{NSD}(a, m)$. Pak rovnice*

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

má řešení, právě tehdy když $d \mid b$. Jestliže $d \mid b$, pak existuje d řešení.

Důkaz. viz. [5] str. 62. □

Věta 3.3. *(Čínská věta o zbytcích)*

Nechť $n_1, \ldots, n_r$ jsou přirozená čísla, pro která platí $\mathrm{NSD}(n_i, n_j) = 1$ *pro všechna $i \neq j$. Nechť $a_1, \ldots, a_r$ jsou libovolná celá čísla. Pak existuje x, které je řešením systému rovnic*

$$x \equiv a_i \pmod{n_i} \qquad i = 1, \ldots, r\,. \tag{18}$$

Důkaz. viz. [5] str. 64. □

Nechť $n = n_1 \cdots n_r$, $\mathrm{NSD}(n_i, n_j) = 1$ pro všechna $i \neq j$. Pak lze snadno ověřit že x ve tvaru

$$x \equiv \sum_{i=1}^{r} a_i b_i \frac{n}{n_i} \pmod{n}\,, \tag{19}$$

kde pro každé b_i platí

$$b_i \frac{n}{n_i} \equiv 1 \pmod{n_i}\,,$$

je řešením (18). Jelikož $\mathrm{NSD}(n/n_i, n_i) = 1$, pak podle Věty 3.2 pro každé $i \in \{1, \ldots, r\}$ takové řešení b_i existuje. Jelikož pro každé dvě řešení x_1, x_2 systému (18) platí $x_1 \equiv x_2 \pmod{n_i}$ pro každé i, pak také $x_1 \equiv x_2 \pmod{n}$ a tedy $x \pmod{n}$ je jediné řešení systému (18).

Nechť $n = n_1 \cdots n_r$, $\mathrm{NSD}(n_i, n_j) = 1$ pro všechna $i \neq j$ a nechť pro všechna n_i existují řešení a_i rovnic $s^2 \equiv -1 \pmod{n_i}$. Potom pro řešení (19) systému $x \equiv a_i \pmod{n_i}$ pro $i = 1, \ldots, r$ platí

$$\begin{aligned} x^2 &= n_1 k_1 - 1\,, \\ &\vdots \\ x^2 &= n_r k_r - 1\,, \end{aligned}$$

a jelikož pro každé $i \neq j$ je $\mathrm{NSD}(n_i, n_j) = 1$, platí

$$x^2 = n_1 \cdots n_r k - 1\,,$$

a tedy x je jedním řešením rovnice $x^2 \equiv -1 \pmod{n}$. Další řešení dostaneme řešením systému $x \equiv a_i \pmod{n_i}$ pro $i = 1, \ldots, r$ pro další kombinace řešení a_i

rovnic $s^2 \equiv -1 \pmod{n_i}$. Takto získaná řešení jsou různá, jinak by pro některé n_i platilo $x \equiv a_{i_1} \equiv a_{i_2} \pmod{n_i}$, kde a_{i_1}, a_{i_2} jsou dvě různá řešení $s^2 \equiv -1 \pmod{n_i}$, což není možné, jelikož tato řešení tvoří dvě různé třídy kongruence modulo n_i.

Věta 3.4. *Nechť a je libovolné celé číslo, $p > 2$ je prvočíslo a NSD$(a, p) = 1$. Pak pro $n \geq 1$ platí, že $x^2 \equiv a \pmod{p}$ má řešení, právě tehdy když $x^2 \equiv a \pmod{p^n}$ má řešení.*

Důkaz. viz. [7] str. 67. □

Uvažujme, že x je řešením rovnice $x^2 \equiv -1 \pmod{p^n}$, tedy $x^2 = bp^n - 1$. Pak pro řešení rovnice $y^2 \equiv -1 \pmod{p^{n+1}}$ platí $y \equiv x + zp^n \pmod{p^{n+1}}$, kde z je řešením $2xz \equiv -b \pmod{p}$.

$$\begin{aligned} y^2 &\equiv (x + zp^n)^2 \\ &\equiv bp^n - 1 + 2xzp^n \equiv (2xz + b)p^n - 1 \\ &\equiv -1 \pmod{p^{n+1}} \end{aligned}$$

Ukažme, že $p \nmid 2x$. Potom podle Věty 3.2 takové z exisutje. Z $x^2 \equiv -1 \pmod{p^n}$ plyne, že $x^2 \equiv -1 \pmod{p}$, a tedy $x \not\equiv 0 \pmod{p}$, neboli $p \nmid x$, z čehož dostáváme $p \nmid 2x$.

Podle důkazu Věty 3.4 uvedeného v [7] mají rovnice $x^2 \equiv -1 \pmod{p}$ a $x^2 \equiv -1 \pmod{p^n}$ stejný počet řešení.

Věta 3.5. *Nechť $f(x)$ je daný polynom s celočíselnými koeficienty. Pro přirozené číslo n označme $N(n)$ jako počet všech řešení rovnice $f(x) \equiv 0 \pmod{n}$. Jestliže $n = n_1 n_2$ a $\mathrm{NSD}(n_1, n_2) = 1$, pak $N(n) = N(n_1)N(n_2)$.*

Důkaz. viz. [5] str. 70. □

Nechť n je přirozené číslo. Nejprve pomocí výše uvedených vět rozhodneme, zdali existuje nějaké jeho vyjádření jako součtu dvou čtverců. Jestliže existuje,

pak je n ve tvaru

$$n = 2^{\alpha} p_1^{\alpha_1} \cdots p_k^{\alpha_k} q_1^{2\beta_1} \cdots q_l^{2\beta_l},$$

kde $p_i \equiv 1 \pmod 4$ a $q_i \equiv 3 \pmod 4$ jsou různá prvočísla. Dále označme

$$p = \begin{cases} 2p_1^{\alpha_1} \cdots p_k^{\alpha_k} & \text{pro liché } \alpha \\ p_1^{\alpha_1} \cdots p_k^{\alpha_k} & \text{pro sudé } \alpha \end{cases}$$

a $q^2 = n/p$. Pak podle Věty 2.3 a (11) platí $R_2(n) = R_2(p)$ a pro každé vyjádření $x^2 + y^2$ čísla p je $(qx)^2 + (qy)^2$ vyjádřením čísla n.

Pro každé $m = \dfrac{p}{d^2}$ nalezneme všechna řešení rovnice $s^2 \equiv -1 \pmod m$, která podle Lemmatu 1.2 a Vět 3.3 a 3.4 existují. Pro všechna řešení $s < \dfrac{m}{2}$ aplikujeme Euklidův algoritmus s výchozími hodnotami m a s. První dva zbytky menší než $\sqrt{m}$ jsou řešením $x^2 + y^2 = m$, respektive $(dqx)^2 + (dqy)^2 = n$.

Podle [5] kapitoly 3.6 tvoří takto nalezená řešení všechna vyjádření n jako součtu čtverců.

Závěr

V úvodní kapitole jsme ukázali, jak lze na základě prvočíselného rozkladu charakterizovat přirozená čísla ve tvaru součtu dvou čtverců. Poté jsme shrnuli dva způsoby, kterými lze určit počet dvou různých způsobů vyjádření těchto čísel. V poslední kapitole této práce jsme se zabývali existencí řešení rovnice $x^2 \equiv -1 \pmod{n}$ pro libovolné přirozené číslo n a využitím těchto řešení a vlastností Euklidova algoritmu pro nalezení těchto reprezentací.

Literatura

[1] M. Aigner, G.M. Zeigler, *Proofs from THE BOOK*, Springer, 2001.

[2] G.E. Andrews, *A simple proof of Jacobi's triple product identity*, Proceedings of the American Mathematical Society 16/2, 1965.

[3] M.D. Hirschhorn, *A simple proof of Jacobi's two-square theorem*, Amer. Math. Monthly 92, 1985.

[4] M.D. Hirschhorn, *Arithmetic consequences of Jacobi's two-squares theorem*, Ramanujan Journal 4, 2000.

[5] I. Niven, H.S. Zuckerman, H.L. Montgomery, *An Introduction to the Theory of Numbers, 5th edition*, Wiley, 1991.

[6] S. Wagon, *Editor's Corner: The Euclidean Algorithm Strikes Again*, Amer. Math. Monthly 97, 1990.

[7] D. Flath, *Introduction to Number Theory*, Wiley, 1989.