Fermatovy marginálie

In: Karel Lepka (author): Historie Fermatových kvocientů (Fermat – Lerch). (Czech). Praha: Prometheus, 2000. pp. 74–89.

Persistent URL: http://dml.cz/dmlcz/401891

Kapitola 6

Fermatovy marginálie

V této kapitole se stručně zmíníme o řeckém matematikovi Diofantovi z Alexandrie a uvedeme některé Fermatovy poznámky, které zapsal na okraje Bachetova vydání Aritmetiky z roku 1621. Budeme si všímat poznámek týkajících se rozkladu čísla na součet dvou čtverců a samozřejmě poznámky, která je dnes známa jako Velká Fermatova věta.

6.1 Diofantos z Alexandrie

O životě tohoto významného matematika „stříbrného věku řecké matematiky" máme dnes velmi málo údajů. Uvádí se, že žil ve 3. století po Kristu. Z jeho díla se zachovaly dva tituly, a sice *Aritmetika* a *O číslech mnohoúhelníkových*. Nutno však podotknout, že obě tato díla se nezachovala úplná. Z třinácti knih Aritmetiky, o nichž se Diofantos zmiňuje v předmluvě k tomuto dílu, se zachovalo pouze šest, navíc konec druhé knihy je ztracen.[1] Pokud Diofantos v Aritmetice mluví o teoreticko číselných předpokladech, obyčejně odkazuje na svoje *Porismata*. Není známo, zda to byla samostatná kniha, či zda Porismata byla součástí Aritmetiky. V každém případě se nezachoval žádný Diofantův číselně teoretický důkaz.

Zatímco u řeckých matematiků klasického a helénistického období můžeme mluvit o geometrizaci všech částí matematiky, dílo Diofantovo představuje vyvrcholení návratu k aritmetizaci matematiky. Tuto tendenci můžeme pozorovat u alexandrijských matematiků v prvním a druhém století po Kristu, jako byl například Herón z Alexandrie. Za druhý zdroj Diofantova díla nutno považovat řešení neurčitých rovnic. O této disciplíně se ze starověku zachovalo velmi málo zpráv. Jak ukazuje tzv. *Plimptonská tabulka č. 322*, Babylóňané uměli řešit neurčitou rovnici

$$X^2 + Y^2 = Z^2.$$

[1] V osmdesátých letech byly objeveny další čtyři knihy, ty však v době Fermatově nebyly známy, proto se o nich nebudeme podrobněji zmiňovat.

Řešení této rovnice má rovněž Eukleides ve svých em Základech (Kniha 10, tvrzení 29). Eukleides ukázal (Základy, Kniha 2, tvrzení 9) jak najít všechna řešení, tzv. *Pellovy rovnice*

$$aX^2 + 1 = Y^2$$

pro $a = 2$, známe-li nejmenší řešení této rovnice.

Aritmetika je sbírka úloh (zachovalo se jich celkem 189), každá z nich je vyřešena. Má-li nějaká úloha více způsobů řešení, jsou všechny uvedeny. Na první pohled se zdá, že Aritmetika není teoretickým dílem. V antické matematice však bylo běžné, že metody řešení nebyly formulovány obecným způsobem odděleným od úloh, ale jsou uváděny na konkrétních příkladech. Diofantos se držel této tradice a i když své úlohy formuluje obecně, řešení demonstruje na konkrétním příkladu. Obecné řešení však lze z těchto ukázek odvodit. Řešením úloh jsou vždy kladná racionální čísla. Diofantovým největším přínosem jsou jeho metody řešení neurčitých rovnic.

První kniha je rozdělena na dvě části. V první definuje Diofantos základní pojmy. Udává, že všechna čísla se skládají z určitého počtu jednotek, přičemž tento počet lze zvyšovat do nekonečna. Zavádí také přirozené mocniny až do stupně šest. Pro tyto mocniny zavedl zavedl zvláštní symboly: Δ^γ pro druhou mocninu, K^γ pro třetí mocninu, $\Delta^\gamma\Delta$ pro čtvrtou mocninu, ΔK^γ pro pátou mocninu a konečně $K^\gamma K$ pro mocninu šestou. Neurčitý počet jednotek (neznámou) nazývá číslem ($\alpha\varrho\iota\theta\mu o\varsigma$) a označuje písmenem ς. Určitý a neměnný počet jednotek (koeficient) nazývá η $\mu o\nu\alpha\varsigma$ a označuje symbolem M^o. Dále jsou zavedeny převrácené hodnoty a pravidla pro násobení mocnin a jejich převrácených hodnot. Diofantos zavádí i záporná čísla (nedostatek) a pravidla pro jejich sčítání, násobení a dělení, nedává jim však žádný smysl. Nezavedl žádné speciální symboly pro operace sčítání a násobení, stejně tak neužívá žádný symbol, vyskytuje-li se neznámá ve vyšší mocnině. Pro druhou mocninu neurčité proměnné však zavedl symbol $\Box$. Všechny úlohy v této knize jsou určité. Úlohy 27 až 30 vedou na systém dvou rovnic o dvou neznámých, který je ekvivalentní kvadratické rovnici. Aby bylo řešení racionální, je třeba, aby diskriminant rovnice byl druhou mocninou přirozeného čísla. Diofantos tak činí bez zvláštního vysvětlování, což svědčí o tom, že metoda řešení kvadratické rovnice ve všech jejích podobách byla v té době dobře známa.

Úlohy druhé knihy již představují řešení neurčitých úloh. Prvních deset je ekvivalentní rovnicím tvaru

$$F_2(X < Y) = 0,$$

kde $F_2(X, Y)$ je mnohočlen 2. stupně s racionálními koeficienty. Na těchto úlohách Diofantos ukazuje svoji metodu. Diofantos rovněž bezpečně věděl, že má-li tato rovnice racionální řešení, má jich nekonečně mnoho, přičemž neznámé mohou být vyjádřeny jako racionální funkce jednoho parametru $X = \varphi(t)$, $Y = \psi(t)$. Ve druhé knize toto není explicitně uvedeno, v devatenácté úloze třetí knihy však uvádí: „Víme, že rozložení kvadrátu na dva kvadráty je možno provést nekonečně mnoha způsoby.“ Zbývající úlohy vedou na řešení systémů rovnic, které nejsou vyššího stupně než dva. V závěru druhé a na počátku třetí knihy se objevují zadání, která představují rozšíření už vyřešených úloh na větší počet neznámých.

Kniha třetí je vlastně pokračováním předešlé. Řeší se zde soustavy tří, čtyř i více rovnic, každá z nich je stupně nejvýš dva.

V knize čtvrté jsou řešeny neurčité rovnice třetího a čtvrtého stupně, úloha osmnáctá je dokonce stupně šest.

Nejobtížnější úlohy řeší kniha pátá, snad proto je zde text mnohdy vynechaný a nesrozumitelný, neboť ti, jenž ho přepisovali, mu nerozuměli. Právě Fermat ve svých poznámkách tento text na mnoha místech doplňuje a správným způsobem interpretuje. V této knize se objevuje nový typ úloh, kdy zadané číslo N je nutno vyjádřit jako sumu dvou, tří či čtyř kvadrátů, z nichž každý vyhovuje nějakým podmínkám. Pro řešení těchto úloh objevil Diofantos speciální algoritmus.

Všechny úlohy šesté knihy se týkají pravoúhlých trojúhelníků s racionálními stranami $X^2+Y^2 = Z^2$. Jsou zde uvedeny doplňující podmínky týkající se plochy, součtu plochy a délky jedné strany atd. Jinými slovy je zadána ještě nějaká funkce $f(X, Y, Z) = 0$. Právě Fermatovy poznámky k řešením úloh této knihy tvoří poměrně velkou část jeho díla z teorie čísel. Fermat měl při studiu této knihy patrně dost času a navíc na okrajích bylo dost místa, takže nám zde zanechal jediný kompletní důkaz z teorie čísel.

6.2 Rozklad čísla na součet dvou čtverců

O nejznámější marginálii, kterou dnes známe jako Velká Fermatova věta, bude pojednáno později, proto se zmíníme o dalších, které představují nejdůležitější Fermatovy výsledky z teorie čísel. Podívejme se podrobněji na další Fermatovo důležité tvrzení z teorie čísel, které můžeme formulovat do následující věty:

Věta 6.1 *Dané prvočíslo p lze rozložit jediným způsobem na součet dvou kvadrátů právě tehdy, když je tvaru $4k + 1$ nebo $p = 2$.*

Úloha 19 třetí knihy zní: *Najít taková čtyři čísla, aby druhá mocnina součtu všech čtyř čísel zůstala druhou mocninou, jestliže k ní přičteme nebo od ní odečteme každé z těchto čtyř čísel.*

Diofantos řeší tuto úlohu následujícím způsobem: Protože v každém pravoúhlém trojúhelníku druhá mocnina přepony zůstane druhou mocninou, přičteme-li k ní či odečteme-li od ní dvojnásobek součinu odvěsen, budu nejprve hledat čtyři pravoúhlé trojúhelníky, které mají stejnou přeponu. Tato úloha je shodná s úlohou o rozložení nějakého kvadrátu na součet dvou kvadrátů, a to čtyřmi způsoby, přičemž víme, že rozložení kvadrátu na součet dvou kvadrátů lze provést nekonečně mnoha způsoby.

Nyní vezmeme dva pravoúhlé trojúhelníky z nejmenších čísel, jako například 3, 4, 5 a 5, 12, 13 a strany každého z nich vynásobíme přeponou druhého. První trojúhelník bude mít strany 39, 52, 65 a druhý 25, 60, 65. Jsou to pravoúhlé trojúhelníky, které mají stejnou přeponu.

Podle své podstaty se číslo 65 rozkládá na součet dvou čtverců dvěma způsoby, jmenovitě 49 plus 16 a 64 plus 1. Je to proto, že 65 je součin 5 a 13 a každé z těchto čísel se rozkládá na součet dvou čtverců. Nyní pro čísla 49 a 16 naleznu strany, které jsou 7 a 4 na základě těchto čísel sestrojím pravoúhlý trojúhelník, který

bude mít strany 33, 56, 65. Stejně tak číslům 64 a 1 odpovídají odvěsny 8 a 1 a sestrojím trojúhelník o stranách 16, 63 a 65.

Tímto způsobem obdržíme čtyři pravoúhlé trojúhelníky se stejnými přeponami. Vrátíme-li se k původní úloze, jako součet těchto čtyř čísel beru $65x$, každé z těchto čísel v x^2, vzatých tolikrát, kolik je druhá mocnina plochy, jmenovitě první $4056x^2$, druhé $3000x^2$, třetí $3696x^2$ a čtvrté $2016x^2$. Součet těchto čtyř čísel $12768x^2$ je roven $65x$, číslo x je rovno $\frac{65}{12768}$. K podmínkám: první číslo bude 17136600, druhé 12675000 takových dílů, třetí 15615600 takových dílů, čtvrté 8517600 a jmenovatel bude roven 163021824.

V této úloze hledáme řešení neurčité rovnice

$$(X_1 + X_2 + X_3 + X_4)^2 \pm X_i = \square \qquad i = 1, 2, 3, 4.$$

Při řešení této úlohy Diofantos nejprve přichází k pravoúhlým trojúhelníkům s racionálními stranami, přesněji řeší neurčitou rovnici

$$X^2 + Y^2 = Z^2$$

v oboru celých čísel. Řešení této rovnice je, jak bude dokázáno později,

$$Z = p^2 + q^2, \qquad Y = 2pq, \qquad X = p^2 - q^2,$$

kde $p > q$ a čísla p, q mají opačnou paritu. Diofantos toto řešení nikde neuvádí, neboť je považuje za všeobecně známé.

Diofantos také věděl, že jsou-li a, b, c strany pravoúhlého trojúhelníka, je $c^2 \pm 2ab = \square$. Hledá proto celé číslo N, které lze vyjádřit jako součet dvou čtverců čtyřmi různými způsoby. Proto bere dva pravoúhlé trojúhelníky v „nejmenších číslech“, tedy trojúhelníky, jejichž strany jsou celá nesoudělná čísla a tvrdí, že součin jejich přepon, tedy 65, lze vyjádřit jako součet dvou čtverců dvěma různými způsoby. Toto tvrzení je důsledek následujícího vzorce, který je dnes také znám jako Viètovy identity

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2 = (ad + bc)^2 + (ac - bd)^2.$$

To, že Diofantos tuto formuli znal, svědčí jeho slova, že číslo 65 je podle jeho podstaty možno rozložit na součet dvou čtverců dvěma způsoby, protože 65 je součin 5 a 13 a každé z těchto čísel lze vyjádřit jako součet dvou čtverců. Stejně tak věděl, že číslo 65 je přeponou čtyř pravoúhlých trojúhelníků s celočíselnými stranami, jinými slovy druhá mocnina čísla, které lze rozložit dvěma různými způsoby na součet dvou kvadrátů se dá rozložit na součet čtyř kvadrátů čtyřmi různými způsoby.

Fermatova poznámka k této úloze je poměrně dlouhá a svědčí o tom, že se Fermat v této problematice velmi dobře orientoval: *Prvočíslo, které převyšuje o jedničku násobek čtyř, je pouze v jednom případě přeponou pravoúhlého trojúhelníka, jeho kvadrát ve dvou případech, krychle ve třech, bikvadrát ve čtyřech a tak dále až do nekonečna.*

Totéž prvočíslo a jeho kvadrát lze pouze jedním způsobem vyjádřit jako součet dvou kvadrátů, jeho krychli a bikvadrát dvěma, pátou a šestou mocninu čtyřmi a tak dále až do nekonečna.

Vynásobíme-li prvočíslo, které lze vyjádřit jako součet dvou čtverců, jiným takovým prvočíslem, potom lze tento součin rozložit na součet dvou čtverců dvěma způsoby. Bude-li násobitel kvadrát druhého čísla, potom lze tento součin třemi způsoby rozložit na součet dvou čtverců. Bude-li násobitel třetí mocninou druhého čísla, potom lze rozložení součinu na součet dvou čtverců provést čtyřmi způsoby a tak dále až do nekonečna.

Z tohoto lze snadno stanovit, kolika způsoby může být dané číslo přeponou pravoúhlého trojúhelníka. Je třeba vzít všechna prvočísla, která o jedničku převyšují násobek čtyř, které jsou obsaženy v daném čísle, například 5, 13, 17. Obsahuje-li dané číslo mocniny těchto prvočinitelů, je třeba vzít exponenty těchto prvočinitelů. Nechť například dané číslo obsahuje 5 ve třetí mocnině, 13 ve druhé mocnině a 17 v mocnině první. V tom případě je nutné vzít exponenty všech těchto prvočinitelů, konkrétně pro číslo 5 exponent 3, pro číslo 13 exponent 2 a pro číslo 17 exponent jedna. Dále je třeba tyto exponenty, o nichž byla řeč, uspořádat, například 3, 2, 1.

Je třeba vynásobit první druhým, zdvojnásobit a přičíst součet prvního a druhého, obdržíme 17. Dále vynásobíme 17 třetím exponentem, zdvojnásobíme a přičteme součet 17 a třetího exponentu, čímž obdržíme 52. V tomto případě bude dané číslo přeponou 52 různých pravoúhlých trojúhelníků. Metoda se nezmění pro jakýkoliv počet prvočinitelů a jakékoliv exponenty.

Jiná prvočísla, která nepřevyšují o jedničku násobek čtyř, stejně tak jako jejich mocniny, nic k hledanému číslu nepřičítávají a nic od něho neodečítají.

Najít číslo, které bude přeponou pravoúhlého trojúhelníka tolikrát, kolikrát si přejeme. Nechť je třeba najít číslo, které bude přeponou sedmi různých pravoúhlých trojúhelníků.

Dané číslo 7 zdvojnásobíme, obdržíme 14. Přidáme jedničku, dostaneme 15. Vezmeme všechny prvočíselné dělitele 15, což jsou 3 a 5. Odečteme od každého jedničku a bereme polovinu zbytků, dostaneme 1 a 2, jmenovitě vynásobíme jeden kvadrátem druhého. Tak dostaneme číslo, vyhovující podmínce, aby obsahovalo pouze prvočísla o jedničku převyšovaly násobek čtyř. Na základě toho je snadné najít nejmenší číslo, které by bylo přeponou pravoúhlého trojúhelníka tolikrát, kolikrát je třeba.

Najít číslo, které lze rozložit na součet dvou kvadrátů tolikrát, kolikrát se požaduje. Nechť požadujeme rozložit dané číslo deseti způsoby. Dvojnásobek desítky je dvacet. Vezmeme prvočinitele, což jsou čísla 2, 2, 5. Od každého odečteme jedničku, dostaneme 1, 1, 4. Znamená to, že musíme vzít tři prvočísla, která převyšují o jedničku násobek čtyř, například čísla 5, 13, 17. Z jednoho z nich vezmeme kvadráto-kvadrát a ten vynásobíme ostatními dvěma. Tak dostaneme číslo, které se rozkládá na součet dvou kvadrátů deseti způsoby.

Z druhé strany tato metoda umožňuje najít, kolika způsoby se dané číslo rozkládá na součet kvadrátů.

Nechť je dané číslo 325. Jeho prvočíselní dělitelé, kteří převyšují o jedničku násobek čtyř budou 5, 13, přičemž poslední je jednou a první v druhé mocnině. Vezmeme exponenty 2 a 1. Sečteme jejich násobek a součet, což dává 5, přičteme jedničku a vezmeme polovinu, což je 3. To znamená, že dané číslo je možno rozložit na součet dvou kvadrátů třemi způsoby.

Dostaneme-li tři exponenty, například 2, 2, 1, proces bude následující. Součin dvou prvních, sečtený s jejich sumou, bude 8. Vynásobíme toto číslo třetím a připočteme součet činitelů, dostaneme 17. Nakonec přičteme jedničku, což dá 18, polovina tohoto čísla je 9. Tolika způsoby lze rozdělit toto číslo na součet dvou kvadrátů. Je-li poslední číslo, z něhož je nutné vzít polovinu, liché, musíme od něho odečíst jedničku a vzít polovinu zbytku.

Je možné ještě zadat následující otázku: Najít celé číslo, jehož součet se zadaným celým číslem bude druhá mocnina a na druhé straně bude přeponou pravoúhlého trojúhelníka tolikrát, kolikrát je požadováno.

Tato otázka je těžká. Je-li například třeba najít číslo, které bude dvakrát přeponou pravoúhlého trojúhelníka a při připočtení 2 dává kvadrát, potom číslo 2023 vyhovuje podmínce, ale existuje nekonečně mnoho jiných, jako 3362 atd.

Fermatovo tvrzení, že každé prvočíslo tvaru $4k+1$ lze rozložit jediným způsobem na součet dvou čtverců, hraje velmi důležitou roli v teorii čísel. Fermat neuvádí jeho důkaz, ten však není příliš obtížný.

Předpokládejme nejprve, že dané prvočíslo lze vyjádřit jako součet dvou kvadrátů, tedy $p = a^2 + b^2$. Je zřejmé, že čísla a a b nemohou být sudá, neboť součet jejich druhých mocnin by byl dělitelný čtyřmi. Jsou-li obě lichá, je $a^2 + b^2 \equiv 2 \pmod 4$ a tedy $p = 2$. Konečně je-li například a liché a b sudé, je $p \equiv 1 \pmod 4$.

Naopak $2 = 1^2 + 1^2$. Dále budeme předpokládat, že $p \equiv 1 \pmod 4$. Z teorie kvadratických zbytků plyne, že číslo -1 je kvadratický zbytek všech prvočísel tvaru $4k+1$. Existuje tedy číslo x splňující podmínku $1 \leq x \leq p-1$ takové, že platí $x^2 + 1 \equiv 0 \pmod p$, tedy $x^2 + 1 = mp$, kde $1 \leq m \leq p-1$. Množina všech čísel m, splňujících podmínku $1 \leq m \leq p-1$ a $mp = x^2 + y^2$ je neprázdná. Označme m_0 nejmenší z těchto čísel. Je-li $m_0 = 1$, potom prvočíslo p je suma dvou čtverců.

Předpokládejme naopak, že $m_0 > 1$. ísla x a y napíšeme ve tvaru

$$x = cm_0 + x_1 \quad \text{a} \quad y = dm_0 + y_1,$$

kde c a d jsou celá čísla a

$$-\frac{m_0}{2} < x_1, y_1 \leq \frac{m_0}{2}.$$

Je zřejmé, že alespoň jedno z čísel x_1 a y_1 je různé od nuly. V opačném případě ${m_0}^2 | x^2 + y^2 = m_0 p$, tedy $m_0 | p$ a tudíž $m_0 = p$, což nelze. Je tedy

$$0 < {x_1}^2 + {y_1}^2 \leq \frac{{m_0}^2}{4} + \frac{{m_0}^2}{4} = \frac{{m_0}^2}{2} < {m_0}^2$$

a

$${x_1}^2 + {y_1}^2 \equiv x^2 + y^2 \pmod{m_0}.$$

Je tedy $x^2 + y^2 = m_0 m'$, přičemž platí $1 \leq m' < m_0$. Odsud plyne

$${m_0}^2 m' p = (x^2 + y^2)({x_1}^2 + {y_1}^2) = (xx_1 + yy_1)^2 + (xy_1 - yx_1)^2.$$

Na druhé straně platí

$$xx_1 + yy_1 = x(x - cm_0) + y(y - dm_0) = (x^2 + y^2) - m_0(c + yd) = m_0 t,$$

$$xy_1 - yx_1 = x(y - dm_0) - y(x - cm_0) = -m_0(xd - yc) = m_0 u,$$

kde t, u jsou celá čísla. Je tudíž $m'p = t^2 + u^2$ a $1 \leq m' < m_0$. To je však spor s předpokladem, že m_0 je nejmenší z čísel m, proto je $m_0 = 1$.

Nechť $p = a^2 + b^2$. Snadno se ukáže, že platí

$$p^2 = (a^2 + b^2)^2 = (2ab)^2 + (a^2 - b^2)^2,$$

jinými slovy čísla p a p^2 jsou přeponou pouze jednoho pravoúhlého trojúhelníka. Použitím této identity i identit Viètových lze dokázat, že čísla p^3 a p^4 jsou přeponami dvou pravoúhlých trojúhelníků atd.

Je-li p přeponou pravoúhlého trojúhelníka, potom rovnice $p^2 = x^2 + y^2$ má jediné řešení, a sice $x = 2ab$ a $y = a^2 - b^2$. Je-li p^n přeponou pravoúhlého trojúhelníka, potom rovnice $p^{2n} = x^2 + y^2$ má podle předcházející úvahy n řešení.

Jsou-li p a q jsou prvočísla tvaru $4k + 1$, potom je $p = a^2 + b^2$, $q = c^2 + d^2$. Součin těchto čísel lze vyjádřit pomocí identity (6. 1.) a obdržíme

$$pq = (a^2 + b^2)(c^2 + d^2) = (ad \pm bc)^2 + (ac \mp bd)^2$$

Odsud plyne, že součin pq lze rozložit na součet dvou čtverců dvěma různými způsoby. Pro součin pq^2 obdržíme

$$pq^2 = (a^2 + b^2)(c^2 + d^2) = \begin{cases} a^2(c^2 + d^2)^2 + b^2(c^2 + d^2)^2 \\ (a^2 + b^2)[(2cd)^2 + (c^2 - d^2)^2] \end{cases} .$$

Výraz $(a^2 + b^2)[(2cd)^2 + (c^2 - d^2)^2]$ lze rozložit na součet dvou čtverců dvěma způsoby, součin pq^2 se rozkládá celkem třemi způsoby. Analogicky lze postupovat pro součin pq^n, takže tento lze rozložit na součet dvou kvadrátů celkem $n + 1$ způsoby.

Nechť N je dané číslo. Ptáme se, v kolika různých pravoúhlých trojúhelnících je toto číslo přeponou. Je zřejmé, že tento počet mohou ovlivnit pouze ti prvočinitelé čísla N, které lze vyjádřit jako součet dvou čtverců. Fermat uvádí příklad, kdy $N = N_1 p^a q^b r^c$, kde N_1 je součin prvočinitelů tvaru $4k - 1$ a čísla p, q a r jsou tvaru $4k + 1$. Dle jeho návodu počet pravoúhlých trojúhelníků je $n = (2ab + a + b)2c + (2ab + a + b) + c$. Provedeme-li naznačené úkony, máme $n = 4abc + 2ab + 2ac + 2bc + a + b + c$ a tuto rovnost lze jednoduchou úvahou napsat ve tvaru

$$n = \frac{1}{2}[(2a + 1)(2b + 1)(2c + 1) - 1].$$

Uvědomíme-li si, že prvočíslo p^a je přeponou právě $n = \frac{1}{2}[(2a + 1) - 1] = a$ pravoúhlých trojúhelníků, je zřejmé, jakým způsobem Fermat uvažoval. Tuto formuli lze rozšířit na libovolný počet prvočinitelů.

Známe-li naopak číslo n, lze tuto rovnost upravit na tvar

$$(2a + 1)(2b + 1) \ldots (2c + 1) = 2n + 1.$$

Protože $2n + 1$ je liché číslo, lze je rozložit na součin m lichých prvočinitelů $x, y, \ldots z$. Odsud plyne, že $a = \frac{x-1}{2}$, $b = \frac{y-1}{2}$, atd. Vezmeme-li postupně prvních m prvočísel tvaru $4k + 1$ a čísla $a, b, \ldots c$ uspořádáme sestupně, je

$$N = p^a q^b \ldots r^c$$

nejmenší číslo, které je přeponou n pravoúhlých trojúhelníků.

Je-li $N = p^a q^b \dots r^c$, kde $p, q, \dots r$ jsou prvočísla tvaru $4k+1$, potom lze toto číslo rozložit na součet dvou čtverců n způsoby, přičemž

$$n = \frac{1}{2}[(a+1)(b+1)\dots(c+1)]$$

způsoby. Nalezení čísla N je zřejmé, včetně jeho minimalizace.

V deváté úloze páté knihy dává Diofantos tuto úlohu: *Rozložit jednotku na dva zlomky a přičíst ke každému z nich dané číslo tak, abychom dostali čtverec. Dané číslo nesmí být liché, (jeho dvojnásobek, zvětšený o jedničku nesmí být dělitelný prvočíslem, jenž po přičtení jedničky je dělitelné čtyřmi).*

Tato úloha je ekvivalentní systému rovnic

$$\begin{aligned} X_1 + X_2 &= 1 \\ X_1 + a &= {Y_1}^2 \\ X_2 + a &= {Y_2}^2 \end{aligned}$$

Jednoduchou úpravou se z těchto rovnic obdrží podmínka $2a+1 = {Y_1}^2 + {Y_2}^2$. číslo tvaru $2a+1$ nelze vždy vyjádřit jako součet dvou čtverců, což zřejmě Diofantos věděl a proto klade dodatečná omezení pro číslo a. První komentátoři a překladatelé Arimetiky neuměli ztracený text doplnit, doplnění v závorce pochází až od P. Tanneryho. Podívejme se, jak řešil úlohu Diofantos.

Předpokládám, že se ke každému zlomku připočítává 6 a dostane se kvadrát. Jelikož chceme rozložit jednotku, přičíst ke každé části 6 a obdržet kvadrát, znamená to, že součet kvadrátů je roven 13. Tedy je nutno rozložit 13 na dva čtverce, každý z nich bude větší než 6.

Rozložím-li 13 na dva kvadráty, jejichž rozdíl je menší než jednička, našel jsem řešení úlohy. Vezmu-li polovinu z 13 obdržím $6\frac{1}{2}$, hledám jakou druhou mocninu zlomku je nutné přičíst k $6\frac{1}{2}$ abych dostal druhou mocninu. Vše vynásobím čtyřmi, potom budu hledat, jakou druhou mocninu zlomku je nutné přičíst k 26, abychom obdrželi kvadrát. Nechť tento přičítaný zlomek je $\frac{1}{x^2}$, potom $26 + \frac{1}{x^2} = \square$.

Vynásobím-li vše x^2, obdržím $26x^2 + 1 = \square$. Nechť číslo na pravé straně je rovno $5x+1$, potom $\square = 25x^2 + 10x + 1$ a x je rovno 10, x^2 je 100 a $\frac{1}{x^2}$ je $\frac{1}{100}$. V tomto případě k 26 je nutné přidat $\frac{1}{100}$ a $\frac{1}{400}$ k $6\frac{1}{2}$, což dává čtverec o straně $\frac{51}{20}$. Tímto způsobem je tedy nutné rozložit 13 na dva čtverce tak, aby strana každého z nich byla blízká $\frac{51}{20}$. Budu hledat co musím odečíst od tří a přičíst ke 2, abych dostal $\frac{51}{20}$.

Sestrojím dva čtverce: jeden se stranou $11x+2$, druhý se stranou $3-9x$. Součet těchto čtverců je $202x^2 + 13 - 10x = 13$, což dává $x = \frac{5}{101}$. Znamená to, že strana jednoho čtverce bude $\frac{257}{101}$ a druhého $\frac{258}{101}$.

A odečtu-li od každého z těchto čtverců 6, potom jedna část jedničky bude $\frac{5358}{10201}$ a druhá $\frac{4843}{10201}$ a je zřejmé, že každá z nich jsouce zvětšena o 6 je kvadrát.

Diofantovo řešení se velmi snadno pochopí, podíváme-li se na problém očima geometrie, i když je více než pravděpodobné, že Diofantos takto neuvažoval. Tuto úlohu lze totiž formulovat následujícím způsobem: Na kružnici k, která má rovnici $u^2 + v^2 = 13$ najít bod $P = [\alpha; \beta]$ takový, že jeho souřadnice jsou racionální čísla,

která splňují podmínky $\alpha^2 > 6$ a $\beta^2 > 6$. Nalezneme bod $A = [\frac{51}{20}; \frac{51}{20}]$, který leží vně kružnice a bod $B = [2; 3]$ ležící na kružnici. Přímka AB má parametrické rovnice $u = 2 + 11t$ a $v = 3 - 9t$ a její průsečík s kružnicí k je bod P.

Jak již bylo řečeno, text této úlohy byl neúplný a komentátoři Arimetiky včetně Bacheta tuto úlohu nepochopili. Jak ukazují Fermatovy poznámky k této úloze, Fermat se zde perfektně orientoval a ztracenou podmínku dokázal doplnit.

V první poznámce k této úloze Fermat uvádí: „číslo 21 nemůže být rozloženo na součet dvou druhých mocnin zlomků. Toto můžeme snadno dokázat. Obecně žádné číslo, jehož třetí část nemá třetinu, nemůže být rozloženo na součet dvou čtverců ani celých čísel, ani zlomků."

Druhá poznámka, kterou Fermat k této úloze učinil, zní: „Zde je jistá podmínka, která je vskutku obecná a dokáže vyloučit všechna nevyhovující čísla. Je nutné, aby dané číslo nebylo liché a aby dvojnásobek tohoto čísla zvětšený o jedničku po vydělení největší druhou mocninou v něm obsaženou, nebylo dělitelné prvočíslem, které je o jedničku menší než násobek čtyř."

Tato poznámka jasně dokazuje, že Fermat bezpečně věděl, že žádné číslo tvaru $4k - 1$ nemůže být rozloženo na součet dvou čtverců. Předpokládáme-li opak tohoto tvrzení, obdržíme

$$4k - 1 = x^2 + y^2,$$

kde x a y jsou celá čísla s opačnou paritou, např. x sudé a y liché. Potom

$$k = \left(\frac{x}{2}\right)^2 + \left(\frac{y^2 + 1}{4}\right).$$

Podle předpokladu je první sčítanec celé číslo, je tedy i druhý sčítanec celé číslo, tedy platí $y^2 + 1 = 4k'$. V tomto případě bychom však dostali $y^2 = 4k' - 1$, jenže žádná druhá mocnina nemůže být v tomto tvaru a dostáváme spor s původním předpokladem.

Pokud by platilo

$$4k - 1 = \left(\frac{x}{2}\right)^2 + \left(\frac{y}{2}\right)^2,$$

obdrželi bychom $z^2(4k - 1) = x^2 + y^2$. Bez újmy na obecnosti můžeme předpokládat, že $(x, z) = (y, z) = 1$. Za tohoto předpokladu, nemohou být čísla x, y, z současně sudá. Nechť tedy z je liché. Potom platí $z = 4k' + 1$ a tedy $(4k' + 1)(4k - 1) = x^2 + y^2 = 4k'' - 1$ a toto číslo nelze rozdělit na součet dvou kvadrátů. Vyšetříme případ z sudé. V tomto případě je $z^2 = 4k'$ a tudíž $4k'(4k - 1) = x^2 + y^2 = 4k''$. Jelikož x a y nemohou být současně sudé, musí být obě liché, tedy je $x^2 = 4m + 1$, $y^2 = 4n + 1$ a jejich součet je tvaru $4r + 2$, tedy opět spor.

Vrátíme-li se k Fermatově poznámce, potom číslo $2n+1$ nemůže být rozloženo na součet dvou kvadrátů je-li n liché, neboť $2(2n - 1) + 1 = 4n - 1$. Stejně tak nemůže být rozloženo na tento součet, je-li $2n + 1 = m^2(4n - 1)$.

6.3 Velká Fermatova věta

Nejznámější Fermatova Marginálie se týká úlohy 8 druhé knihy, která zní: *Zadaný kvadrát rozložit na dva kvadráty.*

Diofantos nabízí dva způsoby řešení. Nechť je třeba rozložit 16 na dva kvadráty. Nechť první je roven x^2, potom druhý bude $16 - x^2$, tudíž $16 - x^2$ je rovněž rovno kvadrátu. Vytvářím kvadrát z jistého množství x minus tolik jednotek, kolik se jich najde ve straně čtverce s obsahem 16, nechť je to $2x - 4$. Potom kvadrát tohoto čísla je roven $4x^2 + 16 - 16x$ a musí se rovněž rovnat $16 - x^2$. Připočtu k oběma stranám chybějící a odečtu podobné od podobných. Potom $5x^2$ je rovno $16x$ a x je rovno $\frac{16}{5}$. Jeden kvadrát je roven $\frac{256}{25}$ a druhý $\frac{144}{25}$, jejich součet je $\frac{400}{25}$ a x je rovno 16.

Jiný způsob: Nechť opět 16 je nutno rozložit na dva kvadráty. Vezmu opět jako x stranu jednoho čtverce a stranu druhého několik x minus tolik jednotek, kolik je strana děleného čtverce, nechť je to $2x - 4$. Máme tedy dva kvadráty; jeden je x^2 a druhý $4x^2 + 16 + -16x$. Požaduji, aby součet těchto čtverců byl 16. Je tedy $5x^2 + 16 - 16x$ rovno 16 a x je rovno $\frac{16}{5}$. Strana prvního čtverce je $\frac{16}{5}$, sám čtverec bude $\frac{256}{25}$. Strana druhého čtverce je $\frac{12}{5}$, sám čtverec bude $\frac{144}{25}$ a důkaz je zřejmý.

Tato úloha spočívá v řešení neurčité rovnice

$$x^2 + y^2 = z^2 \tag{6.1}$$

v oboru racionálních čísel. Trojice čísel, které tuto rovnici splňují, nazýváme *pythagorejská čísla*, (pythagorejské trojice či triplety). Jak dokládá tzv. *plimptonská tabulka* č. 322, (1900–1600 př. n. l.) nalézt takové trojice uměli už ve staré Babylonii.

Je zřejmé, že pokud x, y, z je pythagorejská trojice, je $kx, ky, kz; k \in \mathbb{N}^+$ také pythagorejská trojice. Jestliže $(x, y) = (y, z) = (x, z) = 1$, mluvíme o tzv. *primitivní* pythagorejské trojici. Dále ukážeme, jak nalézt libovolnou primitivní pythagorejskou trojici. Z vlastností sudých a lichých čísel plyne, že dvě čísla z této trojice jsou lichá a jedno sudé a že tím sudým číslem nemůže být číslo z. Nechť sudým číslem z trojice je číslo x. Potom lze psát

$$x^2 = z^2 - y^2 = (z + y)(z - y) \tag{6.2}$$

Jelikož součet resp. rozdíl dvou lichých čísel je číslo sudé, můžeme položit $x = 2u, z + y = 2v, z - y = 2w$ a dosazením do (6. 3) obdržíme

$$u^2 = vw, \qquad \text{přičemž } (v, w) = 1$$

Z věty o jednoznačnosti rozkladu celého čísla na prvočinitele plyne následující tvrzení:

Věta 6.2 *Nechť platí $u^2 = vw$ a $(v, w) = 1$. Potom čísla v, w jsou druhými mocninami.*

Platí tedy

$$z = v + w = p^2 + q^2, \quad y = v - w = p^2 - q^2, \quad x = 2pq, \quad p > q \tag{6.3}$$

a čísla p, q mají opačnou paritu.

Hledáme-li řešení rovnice v racionálních číslech, můžeme postupovat takto: Rovnici vydělíme číslem x a upravíme na tvar

$$1 = \left(\frac{z}{x}\right)^2 - \left(\frac{y}{x}\right)^2 = \left(\frac{z}{x} - \frac{y}{x}\right)\left(\frac{z}{x} + \frac{y}{x}\right).$$

Z tohoto tvaru je vidět, že oba činitelé jsou čísla převrácená a po jednoduché úpravě obdržíme

$$\frac{X}{Z} = \frac{2k}{k^2+1}, \qquad \frac{Y}{Z} = \frac{k^2-1}{k^2+1}$$

Volba $k = \frac{p}{q}$, $(p, q) = 1$ dává celočíselné řešení.

Diofantova volba $X = x$ a $Y = kx - a$, přičemž $k = 2$ je chápáno jako jeden z možných způsobů, $a = 4$ je pevně dané, vede právě k tomuto řešení.

Fermatova poznámka k této úloze zní: „Naopak je nemožné rozdělit krychli na dvě krychle, čtvrtou mocninu ve dvě čtvrté mocniny nebo obecně jakoukoliv mocninu vyšší než dvě ve dvě mocniny téhož stupně. Pro toto tvrzení jsem nalezl opravdu podivuhodný důkaz, ale tento okraj příliš úzký, aby zde mohl být napsán.“ Jinými slovy neurčitá (diofantická) rovnice

$$x^n + y^n = z^n \tag{6.4}$$

nemá pro $n > 2$ řešení v oboru kladných celých čísel. (Fermat, stejně jako Diofantos pracoval pouze s kladnými čísly.

Tato Fermatova poznámka, známá později jako *Velká Fermatova věta*, se stala patrně nejslavnějším problémem v dějinách matematiky a hledání Fermatova důkazu připomíná úsilí mnoha lidí o sestrojení perpetua mobile.

6.3.1 Případ $n = 4$

Fermat sám toto tvrzení uměl dokázat pro $n = 4$. K úloze 20 šesté knihy Aritmetiky připojil totiž následující poznámku: „Plocha pravoúhlého trojúhelníka, jehož strany jsou celá čísla, nemůže být druhá mocnina. Uvedu důkaz tohoto mnou objeveného tvrzení, které jsem objevil po vysilujícím a dlouhém přemýšlení. Tento způsob dokazování povede k nádherným úspěchům v aritmetice.

Kdyby plocha trojúhelníka byla kvadrátem, pak by existovaly dva bikvadráty, jejichž rozdíl by byl kvadrát, z čehož plyne, že by existovaly dva kvadráty, jejichž součet a rozdíl by byl kvadrát. To znamená, že by existovalo čtvercové číslo, jež by bylo rovno kvadrátu a udvojenému kvadrátu za podmínky, že kvadráty, z nichž je složeno, dají v součtu druhou mocninu. Je-li však čtvercové číslo sestaveno z kvadrátu a udvojeného kvadrátu, potom je jeho strana podobným způsobem sestavena z kvadrátu a udvojeného kvadrátu, což mohu snadno dokázat, a odsud plyne, že tato strana je součtem stran při pravém úhlu pravoúhlého trojúhelníka, jeden z těchto kvadrátů bude základnou a druhý udvojený výškou.

Znamená to, že tento pravoúhlý trojúhelník bude sestrojen ze dvou čtvercových čísel, jejichž součet a rozdíl jsou druhé mocniny. Je možné dokázat, že tyto dva kvadráty jsou menší než kvadráty původní, o nichž předpokládáme, že jejich

součet a rozdíl jsou druhé mocniny. Znamená to, že máme-li dva kvadráty, jejichž součet a rozdíl jsou opět kvadráty, potom existují celá čísla, jenž jsou také kvadráty stejných vlastností, ale jejich součet je menší prvního.

Touto úvahou obdržím druhý součet, který je menší než ten, který jsem získal z prvních čísel a tak do nekonečna budu nacházet celá čísla, která se neustále zmenšují. To je však nemožné, je-li dáno celé číslo, nemůže existovat nekonečně mnoho celých čísel, která jsou menší než toto číslo.

Úplný důkaz s podrobným objasněním nelze napsat na tyto úzké okraje.

Stejnou úvahou jsem našel a dokázal, že žádné trojúhelníkové číslo kromě jedničky není rovno bikvadrátu."

Tento popis důkazu, který nám Fermat zanechal, je brilantní ukázkou použití metody nekonečného sestupu. V pravoúhlém trojúhelníku platí $a^2 + b^2 = c^2$ a obsah tohoto trojúhelníka je $P = \frac{ab}{2} = s^2$. Platí

$$\begin{cases} (a+b)^2 = & c^2 + 4s^2 \\ (a-b)^2 = & c^2 - 4s^2 \end{cases}$$

Vynásobením těchto dvou rovnic obdržíme

$$(a^2 - b^2)^2 = c^4 - (2s)^4,$$

tedy rovnice

$$X^4 - Y^4 = Z^2$$

má netriviální řešení v oboru přirozených čísel. Nechť x, y, z jsou řešení této rovnice. Bez újmy na obecnosti lze předpokládat, že tato čísla jsou po dvou nesoudělná. Platí

$$z^2 = x^4 - y^4 = (x^2 + y^2)(x^2 - y^2).$$

Je-li $(x^2 + y^2, x^2 - y^2) = 1$, existují nesoudělná čísla k a l taková, že $x^2 + y^2 = k^2$ a $x^2 - y^2 = l^2$. Obě tato čísla musí být lichá, neboť platí $2x^2 = k^2 + l^2$. V tom případě existují kladná celá čísla $u = \frac{k+l}{2}$ a $v = \frac{k-l}{2}$ a $(u, v) = 1$, jelikož k a l jsou lichá.

Máme $uv = \frac{k^2-l^2}{4}$, tedy $y^2 = 2uv$. Existují tedy celá kladná čísla m a n taková, že platí $u = 2m^2$ a $v = n^2$. Dále platí

$$u^2 + v^2 = \frac{(k+l)^2 + (k-l)^2}{4} = \frac{k^2 + l^2}{2} = x^2.$$

Protože čísla u, v, x tvoří pythagorejskou trojici, existují nesoudělná čísla a, b taková, že platí

$$\begin{cases} u = 2m^2 = 2ab \\ v = n^2 = a^2 - b^2 \\ x = a^2 + b^2 \end{cases}$$

a odsud plyne $m^2 = ab$. Potom opět čísla a a b jsou druhé mocniny a

$$n^2 = a^2 - b^2 = c^4 - d^4.$$

Trojice čísel (c, d, n) je také řešení rovnice a platí $0 < c < a < x$.

Je-li $(x^2+y^2, x^2-y^2) = 2$, jsou čísla x a y lichá, z je sudé. Potom je $x^4 = y^4 + z^2$, čísla x^2, y^2 a z tvoří pythagorejskou trojici, je tedy

$$x^2 = a^2 + b^2, \qquad y^2 = a^2 - b^2, \qquad z = 2ab.$$

Odsud plyne $x^2y^2 = a^4 - b^4$, přičemž platí $0 < a < x$.

Je-li tedy jistá trojice přirozených čísel řešením rovnice, potom z toho plyne, že existuje další trojice menší než uvažovaná, která je řešením této rovnice. To však podle metody nekonečného sestupu není možné.

Důsledkem těchto úvah je následující tvrzení:

Věta 6.3 *Rovnice $X^4 + Y^4 = Z^4$ nemá řešení v oboru celých čísel.*

Pokud by totiž platilo $x^4 + y^4 = z^4$, platilo by také $z^4 - y^4 = (x^2)^2$, což je spor s výše uvedenými závěry.

Je nutné si uvědomit, že tím je současně dokázána platnost této věty i pro libovolné číslo dělitelné 4. Skutečně, kdyby platilo $x^{4m} + y^{4m} = z^{4m}$, byla by čísla x^m, y^m, z^m řešením rovnice $x^4 + y^4 = z^4$, které však neexistuje. Navíc je třeba si uvědomit, že každé přirozené číslo $n > 2$, které není dělitelné číslem 4, musí být dělitelné nějakým prvočíslem $p > 2$. Abychom dokázali obecně Velkou Fermatovu větu, stačí ji dokázat pouze pro prvočísla.

6.3.2 Případ $n = 3$

.

Prvním matematikem, který se po Fermatově smrti věnoval tomuto problému byl *Leonhard Euler*, jenž v dopise Goldbachovi oznamuje, že našel řešení tohoto problému pro $n = 3$. Později se rozhodl ho uveřejnit v posledním oddíle své *Algebry*, když vypracoval novou techniku pro práci s kvadratickými iracionalitami a jejich použití v teorii binárních kvadratických forem.

Tento důkaz je poměrně dlouhý, proto uvedeme pouze hlavní myšlenky. Kompletní důkaz může čtenář najít v [Ed] či v [Ri3]. Nechť x, y, z jsou kladná celá čísla, po dvou nesoudělná, která vyhovují rovnici

$$x^3 + y^3 = z^3. \tag{6.5}$$

Je zřejmé, že právě jedno z čísel x, y, z musí být sudé, nechť je to z. Potom čísla $x + y$ a $x - y$ jsou sudá, tedy $x + y = 2a$, $x - y = 2b$ a odsud plyne, že $x = a + b$ a $y = a - b$. Dosadíme-li za x a y do (6. 6), obdržíme

$$z^3 = x^3 + y^3 = (x + y)(x^2 - xy + y^2) = 2a(a^2 + 3b^2).$$

ísla a a b mají opačnou paritu a jsou nesoudělná. Navíc můžeme předpokládat že jsou kladná a $x \neq y$. Platí-li tedy Velká Fermatova věta, musí existovat celá čísla a, b taková, že $(a, b) = 1$ a výraz $2a(a^2 + 3b)$ je třetí mocninou celého čísla.

Protože čísla $2a$ a a^2+3b^2 jsou bu nesoudělná, nebo mají společný dělitel rovný číslu 3, dělí se důkaz na dva případy. Uvažujme nejprve, že $(2a, a^2 + 3b^2) = 1$. V tomto případě číslo a není dělitelné třemi a z věty o jednoznačnosti rozkladu

čísla na prvočinitele plyne, že $2a = r^3$ a $a^2 + 3b^2 = s^3$, kde s je liché a není dělitelné 3. V tomto případě i číslo s musí být tvaru $s = u^2+3v^2$ a $a = u(u^2-9v^2)$, $b = 3v(u^2-v^2)$, přičemž v je liché, u je sudé a není dělitelné 3 a $(u, v) = 1$. Odsud plyne, že čísla $2u$, $u + 3v$ a $u - 3v$ jsou po dvou nesoudělná a z podmínky

$$r^3 = 2a = 2u(u - 3v)(u + 3v)$$

plyne

$$2u = n^3, \qquad u - 3v = l^3, \qquad u + 3v = m^3.$$

Současně však platí

$$l^3 + m^3 = n^3,$$

přičemž

$$|n^3| < 3|n^3| \leq |n^3(u^-9v^2)(a^2 + 3b^2)| = |2a(a^2 + 3b^2| = |z^3|.$$

Podle metody nekonečného sestupu v tomto případě nemá rovnice (6. 6) řešení v oboru přirozených čísel. Podobným způsobem lze vyřešit i případ, kdy $(2a, a^2 + 3b^2) = 3$.

Eulerův důkaz měl však mezeru, neboť je nutné dokázat pomocné tvrzení, že pro $s^3 = a^2 + 3b^2$ je $s = t^2 + 3u^2$. Přesný a kompletní důkaz podal až Landau v roce 1901.

Vzhledem k tomu, že Fermat pracoval s kvadratickými formami tvaru x^2+ay^2, je možné, že znal , alespoň v hrubých rysech, důkaz pro $n = 3$. Je zajímavé, že Fermat kromě své poznámky k osmé úloze druhé knihy Aritmetiky nikdy neuváděl toto tvrzení obecně, zatím co případy $n = 3$ a $n = 4$ zmiňuje několikrát. (Viz např. uvedený dopis Carcavimu). Mahoney se domnívá [Ma], že právě úspěch v těchto dvou případech mohl vést Fermata k zobecnění tohoto tvrzení a že právě metoda nekonečného sestupu by mohla být oním podivuhodným důkazem. Jestliže tomu tak skutečně bylo, pak se Fermat dopustil podobě nesprávného zobecnění jako v případě Fermatových čísel.

Předpokládejme, že Velká Fermatova věta neplatí pro nějaký exponent $n > 2$. Můžeme předpokládat, že n je liché prvočíslo a že existují celá čísla a, b, c taková, že platí $a^n + b^n = c^n$, přičemž c je sudé a zbývající čísla jsou lichá, $a \neq b$ a $(a, b, c) = 1$. Položme

$$x = \frac{c^n}{2}, \qquad y = \frac{a^n - b^n}{2}, \qquad z = \frac{abc^{n-2}}{2},$$

kde x, y, z jsou celá čísla, x je sudé. Potom je

$$x + y = a^n, \qquad x - y = b^n.$$

Odsud plyne

$$\frac{x^2 - y^2}{4x^2} = \left(\frac{ab}{c^2}\right)^n = \left(\frac{z}{x}\right)^n.$$

Dále platí

$$x(x^n - 4z^n) = x^{n-1}\left[x^2 - 4x^2\left(\frac{z}{x}\right)^n\right] = (x^{\frac{n-1}{2}}y)^2.$$

Nechť $d = (x, z)$, takže $d = \frac{c^{n-2}}{2}$, neboť $(ab, c) = 1$. Položme $x = dx'$, $z = dz'$, takže $(x', z') = 1$ a x' je sudé. Potom číslo $d^{n+1}x'(x'^n - 4z'^n)$ je druhá mocnina a tudíž existují celá čísla r a s taková, že platí

$$x' = r^2, \qquad x'^n - 4z'^n = s^2.$$

Je tedy

$$r^{2n} - s^2 = (r^n + s)(r^n - s) = 4z'^n.$$

Protože je $r \equiv s \pmod 2$, je $(r^n + s, r^n - s) = 2$ a

$$r^n + s = 2t^2, \qquad r^n - s = 2u^n.$$

Sečtením těchto dvou rovnic obdržíme $r^n = t^n + u^n$. Jelikož je

$$r^2 = x' = \frac{x}{d} = c^2,$$

je $r = c$ a metoda nekonečného sestupu se nedá pro tento případ použít.

Použití kvadratických forem však není jedinou možností jak dokázat Velkou Fermatovu větu pro $n = 3$. Uvažujme výrazy typu $v = a + b\sqrt{-3}$, $a, b \in \mathbb{Z}$. Snadno se dokáže, že součet, rozdíl a součin těchto výrazů je rovněž výraz tohoto typu a navíc platí $1 \cdot (a + b\sqrt{-3}) = (a + b\sqrt{-3})$. Řečeno slovy dnešní algebry, výrazy tohoto tvaru tvoří komutativní okruh s jedničkou. Euler jako první použil smělou myšlenku přenést zákony aritmetiky celých čísel na čísla tvaru $(a+b\sqrt{-3})$. Jinými slovy Euler byl první, kdo začal pracovat s komplexními čísly jako s čísly.

Rozložíme-li totiž výraz

$$p^2 + 3q^2 = (p + q\sqrt{-3})(p - q\sqrt{-3}),$$

lze dokázat, že k tomu, abychom našli třetí mocninu tvaru $p^2 + 3q^2$ stačí položit

$$p + q\sqrt{-3} = (a + b\sqrt{-3})^3.$$

6.3.3 Události roku 1847

Euler při řešení případu $n = 5$ neuspěl. Důkaz podal v roce 1825 *Dirichlet*, tento důkaz však byl neúplný, na což poukázal *Legendre*, který současně uvedl vlastní nezávislý a úplný důkaz. Dirichlet v roce 1828 svůj důkaz doplnil a o čtyři roky později se mu podařilo vyřešit případ $n = 14$. V roce 1839 dokázal platnost pro $n = 7$ *Lamé*. Tyto důkazy však byly čím dál tím složitější a případ od případu se značně lišily. Proto úsilí matematiků, kteří se zabývali tímto problémem, směřovalo k nalezení metody, která by Velkou Fermatovu větu řešila obecně.

Dne 1. března 1847 oznámil *Lamé* na zasedání Pařížské akademie, že našel obecný důkaz Velké Fermatovy věty. Lamé v podstatě zobecnil myšlenky důkazů pro $n = 3, 4, 5, 7$. Zavedl komplexní čísla a rozložil výraz $x^n + y^n$ na n lineárních činitelů

$$x^n + y^n = (x + y)(x + ry)(x + r^2y) \cdots (x + r^{n-1}y), \quad n \text{ liché}.$$

Komplexní číslo r musí splňovat podmínku $r^n = 1$. Jsou-li činitelé na pravé straně po dvou nesoudělní, musí každý z nich být n-tou mocninou a lze použít metodu nekonečného sestupu. Lamé tak místo s celými čísly pracoval se speciálními čísly tvaru

$$a_0 + a_1\zeta + \cdots + a_{\lambda-1}\zeta^{\lambda-1}, \quad a_0, a_1, \ldots, a_{\lambda-1} \in \mathbb{Z}.$$

Tato čísla tvoří kruhové těleso $Q(\zeta)$. Název kruhové těleso vznikl z toho, že mocniny čísla ζ znázorněné v komplexní rovině jsou vrcholy pravidelného n-úhelníka vepsaného jednotkové kružnici se středem v počátku. Podobnými úvahami se zabýval i *Cauchy*. Oba dva deponovali u Pařížské akademie zapečetěné obálky. [2] Lamého nadšení však nesdílel Liouville, který ve svém vystoupení poukázal na skutečnost, že Lamé mechanicky přenesl vlastnosti celých čísel na prvky tělesa $Q(\zeta)$. V okruhu celých čísel platí věta o jednoznačnosti rozkladu čísla na prvočinitele.

24. května zveřejnil Liouville dopis, ve kterém *Kummer* z Wroclavi píše, že pro $n = 37$ není tento rozklad jednoznačný a uvedená metoda se nedá obecně použít. Kummer dále píše, že tento nedostatek je možné odstranit zavedením nového typu komplexních čísel, které nazval *ideální komplexní čísla*. Nakonec uvedl, že výsledky této nové teorie byly předneseny na zasedání Berlínské akademie věd v roce 1846 a publikovány ve Zprávách této Akademie. V roce 1847 publikoval další dva články [Ku1], [Ku2], v nichž podává úplné vysvětlení své nové teorie. Kummerovy práce se staly základem nově vzniklé teorie ideálů obecného okruhu, která byla rozvinuta Dedekindem, Krullem, van der Waerdenem a dalšími význačnými matematiky.

I přes velký význam Kummerovy teorie se však nepodařilo obecně Fermatovu hypotézu dokázat, i když zejména v posledních letech, kdy byly do řešení tohoto problému zapojeny i nejvýkonnější počítače, s jejichž pomocí byla tato hypotéza ověřena pro všechna lichá čísla $< 4 \cdot 10^6$. Teprve v roce 1993 se podařilo tento problém, který více než 300 let odolával úsilí mnoha světových profesionálních i amatérských matematiků a který se několikrát stal i motorem pokroku v matematice, vyřešit. Dne 23. června 1993 přednesl britský matematik *Andrew Wiles* přednášku o vyřešení významné hypotézy japonského matematika Zutaki Taniyamy v aritmetické algebraické geometrii týkající se velké třídy eliptických křivek nad racionálními čísly. Jako důsledek odsud vyplývá nemožnost řešení rovnice (1) v oboru přirozených čísel. Tento důkaz je však daleko za hranicemi Fermatových možností, takže to, jaký důkaz měl Fermat na mysli, už asi zůstane navždy tajemstvím.

[2] Pokud někdo přišel na nový objev, který bylo nutno ještě dopracovat, mohl u Pařížské akademie uložit zapečetěnou obálku, kde popsal hlavní myšlenku svého objevu.