

Fermatův odkaz

Alena Šolcová

▶ **To cite this version:**

Alena Šolcová. Fermatův odkaz. Cahiers du CEFRES, 2002, Matematik Pierre de Fermat, 28, pp.173-202. halshs-01245666

HAL Id: halshs-01245666
https://shs.hal.science/halshs-01245666

Submitted on 17 Dec 2015

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Cahiers du CEFRES
N° 28, Matematik Pierre de Fermat
Alena Šolcová, Michal Křížek, Georges Mink (Ed.)

Alena ŠOLCOVÁ
Fermatův odkaz

Référence électronique / electronic reference :
Jean Dhombres, « Fermatův odkaz », Cahiers du CEFRES. N° 28, Matematik Pierre de Fermat (ed. Alena Šolcová, Michal Křížek, Georges Mink).
Mis en ligne en / published on : mai 2010 / may 2010
URL : http://www.cefres.cz/pdf/c28/solcova_2002_fermatuv_odkaz.pdf
Editeur / publisher : CEFRES USR 3138 CNRS-MAEE
http://www.cefres.cz

Ce document a été généré par l'éditeur.
© CEFRES USR 3138 CNRS-MAEE



Fermatův odkaz

Alena Šolcová[*], Praha

1. Kdy se vlastně Fermat narodil?

Zájem o životní data a osudy Pierra de Fermata vzrostl v roce 1995, kdy Andrew Wiles dokázal Velkou Fermatovu větu. Ještě v 19. století najdeme o Fermatovi v encyklopediích jen velmi skromné zprávy. Často se pouze uvádí jen to, že Pierre de Fermat byl právník žijící v Toulouse. O jeho matematických zájmech a výsledcích nacházíme jen stručné zmínky. Proto je dodnes v jeho životopise tolik nejasností a nepřesností. Všimněme si např. údaje o roku Fermatova narození na podstavci jeho sochy v Beaumont-de-Lomagne (viz obr. 1) a na pamětní desce (viz obr. 2) umístěné na jeho rodném domě v témže městě (viz obr. 3). Oba zdroje uvádějí rok 1601. Jiný údaj najdeme v Capitolu v Toulouse na sousoší Fermat a múza (viz obr. 4 a 6). V dolní části této sochy jsou Fermatova životní data vymezena takto: 1595–1665 (viz obr. 5). Deska umístěná v muzeu v budově augustiniánského kláštera v Toulouse zase uvádí, že se Fermat dožil 57 let, což odpovídá roku narození ≈ 1607 nebo 1608.



Obr. 1. Podstavec sochy Pierra de Fermata v Beaumont-de-Lomagne.

[*] Autorka děkuje Heleně Holovské a Jakubu Šolcovi za řadu užitečných připomínek a Pavlu Křížkovi za poskytnuté fotografie.



Obr. 2. Pamětní deska na Fermatově rodném domě, Beaumont-de-Lomagne.

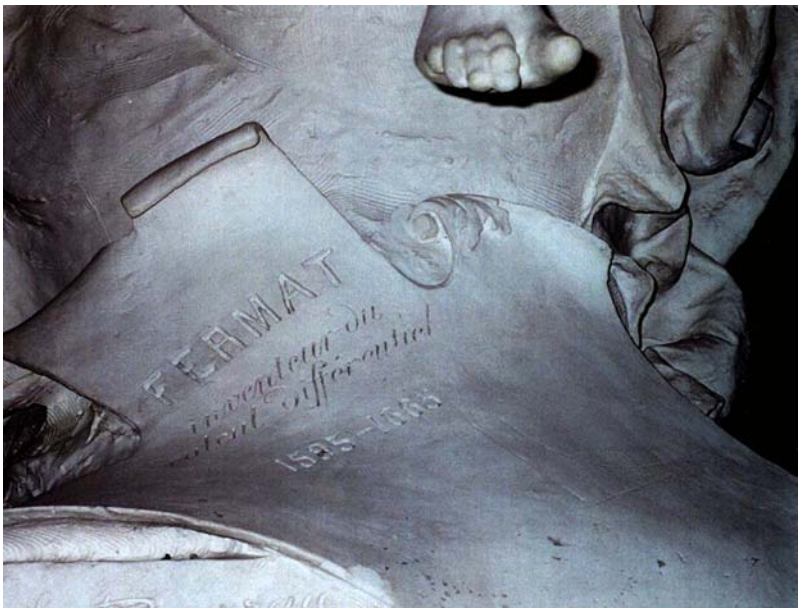


Obr. 3. Vstup do rodného domu Pierra de Fermata.

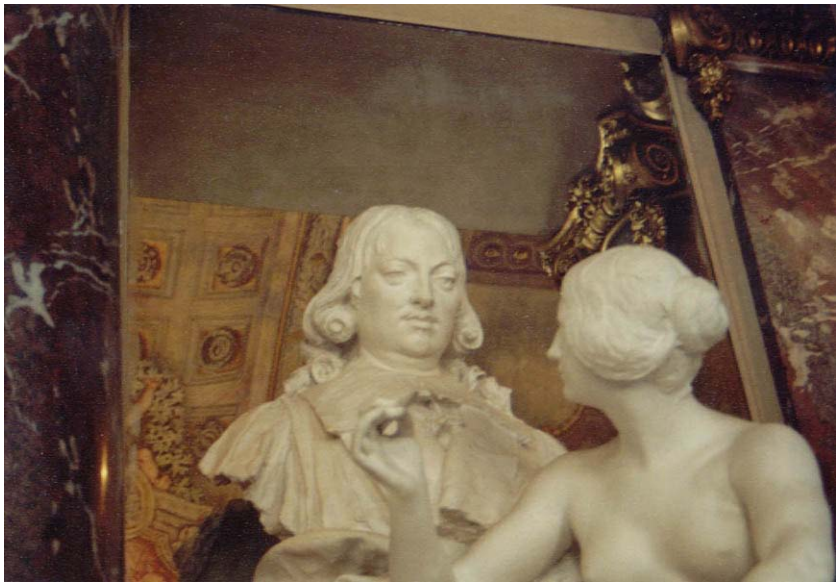
Profesor Klaus Barner z univerzity v Kasselu se v práci [Barner, 2000] zabýval problémem, kdy se matematik Pierre de Fermat skutečně narodil. Dospěl k názoru, že dítě Dominika Fermata, které bylo v roce 1601 pokřtěno Pierre, nebylo totožné s budoucím právníkem a matematikem. Matka tohoto dítěte, Françoise Cazenove, zemřela již v roce 1603 a otec Dominique se mezi lety 1603–1607 znovu oženil. Mezi pěti dětmi, které se mu v tomto druhém manželství se šlechtičnou Claire de Long narodily, by měl být i proslulý matematik Pierre. Zápisy o křtech z let 1607–1611 jsou ale nenávratně ztraceny. Klaus Barner se domnívá, že Fermatův syn Samuel označil otcův věk v době úmrtí – 57 let – na desce v augustiniánském klášteře správně. Deska byla zhotovena jen deset let po Fermatově smrti, roku 1675. Zda se někdy podaří prokázat tuto pozoruhodnou hypotézu a určit, kdo byla skutečná Fermatova matka a kdy se vlastně Pierre de Fermat narodil, zůstává otázkou. Důležitější je však to, co Fermat v matematice dokázal a k jakým výsledkům dospěl.



Obr. 4. Fermat a múza, Capitole, Toulouse.



Obr. 5. Detail nohy sousoší Fermat a múza s životními daty Pierra de Fermata (1595–1695).



Obr. 6. Fermat a múza (detail), Capitole, Toulouse.



Obr. 7. Capitole v Toulouse.

2. Fermatova metoda nekonečného sestupu

V tomto odstavci si přiblížíme jeden ze znamenitých Fermatových objevů – metodu nekonečného sestupu, která je blízká principu matematické indukce. Opírá se o vlastnost, že množina přirozených čísel $N = \{1, 2, 3, \ldots\}$ je dobře uspořádaná, což znamená, že libovolná její neprázdná podmnožina má nejmenší prvek. Podobnou vlastnost nemá ani množina celých čísel, ani množina racionálních či reálných čísel.

Fermatova metoda nekonečného sestupu je založena na následující větě.

Věta 1. *Nechť M je podmnožina množiny přirozených čísel N a nechť pro libovolné $m \in M$ existuje $n \in M$ tak, že $n < m$. Potom je množina M prázdná.*

D ů k a z. Předpokládejme naopak, že M je neprázdná. Protože je množina přirozených čísel N dobře uspořádaná, existuje nejmenší prvek m množiny M. Pak ale podle předpokladu věty existuje prvek $n \in M$, který je menší než m, což je spor s minimalitou m. Tedy M je prázdná množina. □

Věta 1 se používá k důkazům neexistence přirozených čísel jistých vlastností. Její užitečnost si ukážeme na důkazu tvrzení (viz věta 4.) týkajícího se pythagorejských trojúhelníků. Tímto tvrzením se zabýval Pierre de Fermat kolem roku 1640. Nejprve si ale připomeňme dvě známé věty.

Věta 2. *Nechť a, b, c jsou délky stran trojúhelníka. Pak je tento trojúhelník pravoúhlý s přeponou délky c právě tehdy, když platí*

$$a^2 + b^2 = c^2.$$

Implikace $\Rightarrow$ je známá Pythagorova věta. Obrácená implikace $\Leftarrow$, která je z praktického hlediska mnohem důležitější, se v řadě učebnic bohužel opomíjí. Například to, že volba $a = 3$, $b = 4$ a $c = 5$ dává pravoúhlý trojúhelník, vůbec neplyne z Pythagorovy věty, ale z věty 2!

Nechť pro uspořádanou trojici (a, b, c) přirozených čísel platí $a^2 + b^2 = c^2$. Pak se tato trojice nazývá *pythagorejská* a příslušný pravoúhlý trojúhelník z věty 2 se nazývá *pythagorejský*. Je-li (a, b, c) pythagorejská trojice, pak zřejmě (b, a, c) je také pythagorejská trojice. Jestliže navíc a, b, c nemají společného dělitele $d > 1$, pak se (a, b, c) nazývá *primitivní pythagorejská trojice.*

Následující věta je uvedena v Diophantově Aritmetice, jejíž latinská verze byla publikována v roce 1621.

Věta 3. *Trojice* (a, b, c) *přirozených čísel je primitivní pythagorejská trojice právě tehdy, když existují nesoudělná přirozená čísla* $m > n$, *z nichž jedno je sudé a druhé liché, tak, že buď*

(1) $$a = m^2 - n^2, \quad b = 2mn, \quad c = m^2 + n^2,$$

anebo

$$a = 2mn, \quad b = m^2 - n^2, \quad c = m^2 + n^2.$$

Čísla m *a* n *jsou určena jednoznačně.*

D ů k a z . Nechť (a, b, c) je primitivní pythagorejská trojice. Pak jen nejvýše jedno z těchto čísel může být sudé. Předpokládejme na okamžik, že a i b jsou obě lichá. Pak a^2 i b^2 jsou o jedničku větší než nějaký násobek 4, protože $(2j+1)^2 = 4j^2 + 4j + 1$. Tedy $a^2 + b^2$ je o 2 větší než nějaký násobek 4. Odtud ale plyne, že druhá mocnina c^2 je dělitelná 2, ale není dělitelná 4, což není možné. Proto právě jedno z čísel a nebo b musí být sudé. Bez újmy na obecnosti můžeme tedy předpokládat, že $b = 2k$ a že čísla a a c jsou lichá. Potom

$$k^2 = \frac{c^2 - a^2}{4} = \frac{c+a}{2}\,\frac{c-a}{2}.$$

Jelikož a a c jsou lichá, jsou čísla $(c + a)/2$ a $(c - a)/2$ přirozená. Musí být navíc nesoudělná, protože každý jejich společný dělitel dělí jejich součet (což je c) i jejich rozdíl (což je a) a o těchto číslech jsme předpokládali, že jsou nesoudělná.

Každé prvočíslo p, které dělí $(c - a)/2$, také dělí k^2, a proto i p^2 dělí k^2. Jelikož p nedělí $(c + a)/2$, musí p^2 dělit $(c - a)/2$. Rozklad $(c - a)/2$ na prvočísla má tedy jen sudé exponenty, což znamená, že číslo $(c - a)/2$ je čtverec. Podobně zjistíme, že $(c + a)/2$ je rovněž čtverec. Můžeme tedy psát

$$\frac{c+a}{2} = m^2 \qquad \text{a} \qquad \frac{c-a}{2} = n^2.$$

Vidíme, že čísla m a n jsou nesoudělná, jsou určena jednoznačně a $m > n$. Jelikož $c = m^2 + n^2$ je liché, jedno z čísel m a n musí být liché a druhé sudé. Dále vidíme, že $a = m^2 - n^2$, a tudíž $b = \sqrt{c^2 - a^2} = 2mn$.

Nechť naopak $m > n$ jsou nesoudělná přirozená čísla, z nichž jedno je liché a druhé sudé. Položme nejprve

$$a = m^2 - n^2, \quad b = 2mn, \quad c = m^2 + n^2.$$

Pak zřejmě a a c jsou lichá, b je sudé a

$$a^2 + b^2 = (m^2 - n^2)^2 + (2mn)^2 = (m^2 + n^2)^2 = c^2 .$$

Tudíž (a, b, c) je pythagorejská trojice. Kdyby čísla a, b, c byla všechna dělitelná nějakým lichým prvočíslem p, pak by také čísla $c + a = 2m^2$ a $c - a = 2n^2$ byla dělitelná p, což je ve sporu s tím, že m a n jsou nesoudělná. Odtud plyne, že (a, b, c) je primitivní pythagorejská trojice.

Případ, kdy a je sudé a b je liché, lze vyšetřit analogicky. □

Poznamenejme ještě, že pro přirozené číslo d dávají volby

$$a = d(m^2 - n^2), \quad b = d(2mn), \quad c = d(m^2 + n^2) ,$$

a

$$a = d(2mn), \quad b = d(m^2 - n^2), \quad c = d(m^2 + n^2)$$

všechny pythagorejské trojice.

Obsah pythagorejského trojúhelníka

(2) $$P = \frac{ab}{2}$$

je vždy přirozené číslo, protože a nebo b ve větě 3 je sudé. Věty 1 a 3 nyní použijeme k důkazu následujícího *Fermatova tvrzení*.

Věta 4. *Neexistuje pythagorejský trojúhelník, jehož obsah je čtvercem přirozeného čísla.*

D ů k a z . Předpokládejme naopak, že existují $a, b, c \in N$ tak, že $a^2 + b^2 = c^2$ a že obsah P pythagorejského trojúhelníka je čtvercem nějakého přirozeného čísla. Lze předpokládat, že (a, b, c) je primitivní pythagorejská trojice. Kdyby tomu tak nebylo, pak bychom položili $a' = a / d$, $b' = b / d$ a $c' = c / d$, kde d je největší společný dělitel čísel a, b, c. Trojice (a', b', c') by pak opět byla pythagorejská a obsah příslušného pythagorejského trojúhelníka by byl opět čtvercem, jak plyne z (2). Podle věty 3 je právě jedno z čísel a a b sudé; bez újmy na obecnosti můžeme předpokládat, že sudé je b. Existují tedy nesoudělná přirozená čísla $m > n$ tak, že platí (1). Proto jsou po dvojicích nesoudělná také čísla m, n, $m + n$ a $m - n$.

Obsah uvažovaného pythagorejského trojúhelníka podle (1) a (2) je

(3) $$P = mn(m + n)(m - n) .$$

Protože P je čtverec, musí být čtverce i jednotliví činitelé v (3), tj. existují $u, v, k, l \in N$ tak, že

(4) $$m = u^2, \quad n = v^2, \quad m + n = u^2 + v^2 = k^2, \quad m - n = u^2 - v^2 = l^2 .$$

Sečtením a odečtením dvou posledních rovnic dostaneme

(5) $2m = 2u^2 = k^2 + l^2, \quad 2n = 2v^2 = k^2 - l^2 = (k+l)(k-l).$

Protože předpokládáme, že $a = m^2 - n^2$ je liché (viz (1)), čísla $k^2 = m+n$ a $l^2 = m-n$ ze vztahu (4) jsou rovněž lichá. Tedy k a l jsou také lichá čísla.

Nechť j je největší společný dělitel čísel $k + l$ a $k-l$. Zřejmě $j \geq 2$, protože $k + l$ a $k-l$ jsou čísla sudá. Vidíme, že j dělí (beze zbytku) $2k$ i $2l$. Čili j^2 dělí $4(k^2 + l^2) = 8m$ i $4(k^2 - l^2) = 8n$. Protože čísla m a n jsou nesoudělná, je $j \leq 2$. Čísla $k + l$ a $k-l$ tedy nemají kromě 2 žádného společného dělitele. Proto podle (5) existují $r \in N$ a sudé číslo $s \in N$ tak, že buď

$$k+l = 2r^2 \qquad \text{a} \qquad k-l = s^2,$$

anebo

$$k+l = s^2 \qquad \text{a} \qquad k-l = 2r^2.$$

Odtud a z (5) dostaneme

$$(r^2)^2 + \left(\frac{s^2}{2}\right)^2 = \left(\frac{k+l}{2}\right)^2 + \left(\frac{k-l}{2}\right)^2 = \frac{k^2+l^2}{2} = u^2.$$

Vidíme, že trojice $(r^2, s^2/2, u)$ je novou pythagorejskou trojicí. Obsah odpovídajícího trojúhelníka je $P' = r^2 s^2 / 4$, což je zřejmě čtverec přirozeného čísla, neboť s je sudé. Obsah P' je však menší než obsah P, tj.

$$P' = \frac{r^2 s^2}{4} = \frac{k^2 - l^2}{8} < k^2 < u^2 v^2 k^2 l^2 = P,$$

kde poslední rovnost plyne z (3) a (4).

Ověřili jsme tak předpoklady věty 1 pro množinu

$$M = \{P \in N \mid \exists\, a,b,c,i \in N\colon\ P = i^2 = \frac{ab}{2},\ a^2 + b^2 = c^2\},$$

kde symbol $\exists$ označuje existenční kvantifikátor. M je tedy prázdná množina. □

Fermat použil *metodu nekonečného sestupu* i při důkazu dalších tvrzení, např. k důkazu Velké Fermatovy věty pro exponent 4.

3. Malá Fermatova věta

V roce 1640 vyslovil Fermat následující větu (viz [Fletcher, 1989, 1991]) a přitom snad ani netušil, jaké obrovské uplatnění bude mít o více než 300 let později. Označme písmeny n.s.d. nejmenšího společného dělitele přirozených čísel z N.

Malá Fermatova věta: *Nechť p je prvočíslo a* $n \in N$. *Pak platí implikace*

$$\text{n.s.d.}(n, p) = 1 \quad \Rightarrow \quad n^{p-1} \equiv 1 \pmod{p}. \qquad (1)$$

Tato věta je asi nejpoužívanějším nástrojem v teorii čísel. Lze ji užít např. k důkazu toho, že číslo je složené, aniž bychom znali některého jeho netriviálního dělitele. Pokud totiž kongruence v (1) neplatí pro nějaké $n \in N$, pak jistě není p prvočíslo.



Obr. 8. Kolej Pierra de Fermata v Toulouse.

Později zavedl Leonhard Euler funkci

$$\varphi(q) = \text{card}\{\, r \in \{1, 2, \ldots, q\} \mid \text{n.s.d.}(r, q) = 1\},$$

tzv. *Eulerovu funkci*, kde card označuje počet prvků, a zobecnil Malou Fermatovu větu takto:

Fermatova–Eulerova věta: *Nechť* $n, q \in N$. *Pak platí ekvivalence*

$$\text{n.s.d.}(n, q) = 1 \;\Leftrightarrow\; n^{\varphi(q)} \equiv 1 \pmod{q}.$$

Tato věta se používá např. v kryptografické metodě RSA[*] k důkazu toho, že zašifrovaná zpráva je po dešifrování shodná s původní zprávou. Metoda RSA našla široké uplatnění ve vojenství a bankovnictví k přenosu tajných a jiných důvěrných zpráv. Je na ní založen i digitální podpis, který nedávno schválil náš parlament a který hraje důležitou roli při projektování počítačových systémů. Brání například systém proti nežádoucím vstupům a manipulacím, ochraňuje data před „nepovolanými čtenáři", před falzifikací a zabezpečuje rozličné soubory před jejich destrukcí. Podrobněji se s metodou RSA můžete seznámit např. v článku [Křížek].

4. Velká Fermatova věta

Fermat by jistě ocenil, že jedna z jeho hypotéz bude nazvána **Velkou Fermatovou větou[†]:**

Pro přirozené číslo $n > 2$ *nemá rovnice*

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

žádné řešení pro přirozená čísla x, y *a* z.

Metody, které použil Wiles k jejímu důkazu, jsou vysvětleny např. v knize [Hellegouarch] nebo v článku [Nekovář].

Podle známé Fermatovy poznámky, kterou Fermat učinil při četbě Diofantovy Aritmetiky, se zdálo, že důkaz neexistence řešení bude snadný. Přesto zaměstnával řadu matematiků přes více než 350 let. Fermat sám dokázal větu pro $n = 4$ a Leonhard Euler pro $n = 3$. Velký zájem o její vyřešení vzbudila Wolfskehlova cena založená roku 1908 Paulem Wolfskehlem, německým lékařem, jehož koníčkem byla matematika. Andrew Wiles z princetonské university našel způsob, jak Fermatovu větu dokázat (viz [Wiles]). Později v roce 1995 společně s Richardem Taylorem zveřejnil její úplný důkaz (viz [Taylor, Wiles]). Metodu, kterou autoři použili, Fermat znát nemohl, neboť řada pojmů nebyla tehdy ještě zavedena (modulární formy, eliptické křivky, grupy). Wiles za svůj významný objev získal stříbrnou plaketu, kterou převzal na univerzitě v Berkeley v roce 1998. Udělení Fieldsovy medaile bránil Wilesův věk, neboť mu bylo již více než 40 let.

---

[*] Metoda RSA byla nazvána podle počátečních písmen autorů článku [Rivest, Shamir, Adleman], v němž je popsán šifrovací a dešifrovací algoritmus výpočtu a vysvětlena podstata metody RSA. Matematický princip metody RSA objevili již dříve W. Diffie a M. Hellman a popsali jej v článku [Diffie, Hellman, 1996].

[†] Více o Velké Fermatově větě viz stejnojmenný článek G. Terjaniana v tomto svazku.

Jako mnoho jiných se pokoušel také dokázat Velkou Fermatovu větu Andrew Beal. Hledal jednodušší důkaz než vytvořili Wiles společně s Taylorem. Společně s Danielem Mauldinem z University of North Texas vyhlásili cenu 50 000 $ za důkaz zobecněné Velké Fermatovy věty (viz [Mauldin]).

Bealova hypotéza: *Rovnice* $x^k + y^m = z^n$ *nemá žádné řešení pro pro přirozená čísla k, m, n větší než 2 a vzájemně nesoudělná přirozená čísla x, y, z .*

Původní Fermatova hypotéza říká, že součet dvou *n*-tých mocnin přirozených čísel nemůže být roven *n*-té mocnině jiného přirozeného čísla pro $n > 2$. Beal se zabýval případem, kdy obecně nejsou všechny exponenty stejné. Vidíme např., že $17^4 + 34^4 = 17^5$. Tedy sčítanci na levé straně jsou umocněni na týž exponent a rovnají se číslu umocněnému na jinou mocninu. Proto se v Bealově hypotéze předpokládá, že čísla x, y a z nemají společného dělitele.

Věnujme se nyní případům, kdy sčítanci jsou vzájemně nesoudělná čísla a exponenty vzájemně různé a větší než 1. Jsou to např.:

$$1^k + 2^3 = 3^2 \quad (k > 3),$$
$$2^5 + 7^2 = 3^4,$$
$$7^3 + 13^2 = 2^9,$$
$$2^7 + 17^3 = 71^2,$$
$$3^5 + 11^4 = 122^2,$$
$$17^7 + 76271^3 = 21063928^2,$$
$$1414^3 + 2213459^2 = 65^7,$$
$$9262^3 + 15312283^2 = 113^7,$$
$$43^8 + 96222^3 = 30042907^2,$$
$$33^8 + 1549034^2 = 15613^3.$$

Povšimněme si, že ve všech uvedených případech se vyskytuje exponent 2.

hypotéza je zobecněním Velké Fermatovy věty. Bude-li někdy rozřešena, podobné slávy jako její speciální případ již patrně nedosáhne.

V literatuře se také občas setkáváme s termínem Fermatova funkce. Podle jedné definice je *Fermatova funkce f(n)* pro *n* přirozené nejmenší absolutní hodnota výrazu

[2] Andrew Beal je zakladatel, majitel a předseda Bealovy banky, největší místní banky v Dallasu. Založil též společnost Beal Aerospace, která se věnuje navrhování a konstrukci další generace raket pro satelity Země.

$$F_n(x, y, z) = x^n + y^n - z^n,$$

kde *x*, *y*, *z* jsou navzájem různá přirozená čísla.

Pro první dvě hodnoty máme

$$f(1) = 0,$$
$$f(2) = 0 \text{ (pythagorejské trojice).}$$

Hodnoty pro $n > 2$ jsou zřejmě nenulové, protože platí Velká Fermatova věta.

Odtud pro $n = 3$ plyne, že $f(3) = 1$, protože $\left| 6^3 + 8^3 - 9^3 \right| = 1$.
Pro $n = 5$ zatím pouze víme, že $f(5) \leq 12$, protože $13^5 + 16^5 - 17^5 = 12$. Existuje hypotéza, že platí

$$f(n) < 3^n - 2^n - 1 \text{ pro } n > 5.$$

Se jménem Fermata jsou také spojeny plochy $F_n(x, y, z) = 0$ v trojrozměrném prostoru, kde $F_n(x, y, z) = x^n + y^n - z^n$, n je přirozené číslo a *x*, *y*, *z* jsou reálná čísla. Každá taková plocha zřejmě prochází bodem (0, 0, 0) a pro $n > 2$ žádná z ploch neprochází žádným mřížovým bodem, jehož souřadnicemi jsou přirozená čísla.

Studiem Fermatových polynomů se zabývá např. článek [Horanam].

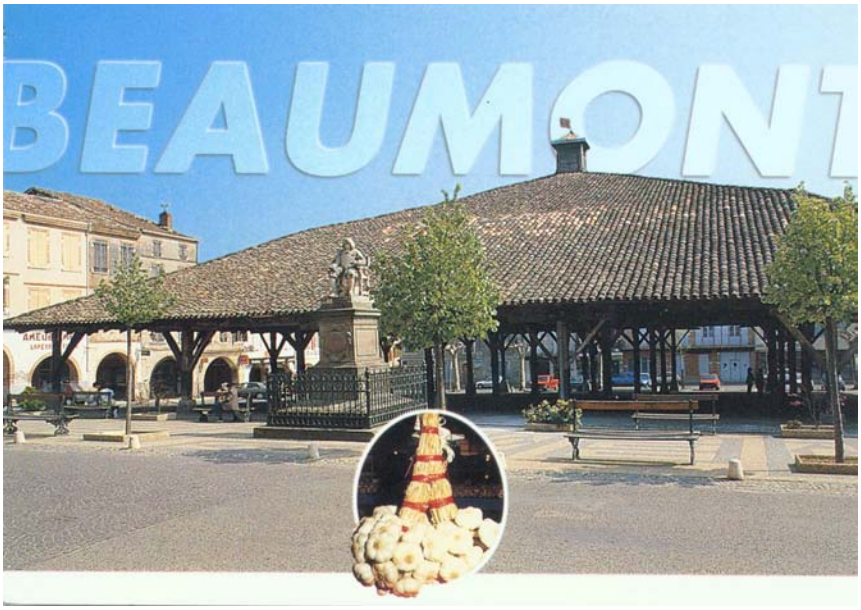
5. Fermatovy křivky

Fermatova první práce o analytické geometrii *Ad locos planos et solidos isagoge* zůstala v rukopise až do roku 1679, kdy ji Fermatův syn Samuel zahrnul do spisu *Varia opera*. V práci o tečnách a kvadraturách, která byla dokončena v roce 1636, definuje Fermat analyticky řadu nových křivek. Křivky zapsané dnes ve tvaru

$$x^m \cdot y^n = a,$$
$$y^n = ax^m,$$
$$r^n = a\theta$$

jsou známy jako *Fermatovy hyperboly, paraboly a spirály* (viz např. [Šolcová]).

Fermat se speciálně věnoval studiu kubické křivky (1666) dodnes spojované se jménem matematičky Marie Gaetany Agnesi (1718–1799), v angličtině „*witch of Agnesi*“ – *čarodějka z Agnesi*.* Její kartézská rovnice je $y\left(x^2+a^2\right)=a^3$. Konstrukci a tvar křivky lze nalézt např. na webovské stránce [w3].



Obr. 9. Náměstí s tržištěm, Beaumont–de–Lomagne. V popředí je Fermatova socha.

Při studiu křivek postupují Fermat a Descartes rozdílným způsobem: Tam, kde Descartes ve své *Géométrii* začíná se studiem „geometrických míst“, a pak nalézá rovnici, Fermat nejprve sestaví rovnici, a potom studuje „geometrická místa“, která rovnice popisuje. Fermatova práce je napsána ve Viètově symbolice, a proto působí archaicky ve srovnání s moderní symbolikou Descartovou. Kartézská rovina by se také mohla jmenovat Fermatova rovina, protože právě ve Fermatově uvažování lze již pozorovat souřadnicový přístup.

Fermat rozhodně překonal Descarta v metodě pro vyhledávání maxim a minim funkcí. Pierre-Simon de Laplace (1749–1827) považoval Fermata za skutečného objevitele diferenciálního počtu. Více o Fermatově příspěvku ke vzniku diferenciálního a integrálního počtu viz [Mahoney], popř. [Šolcová].

Descartes vyhrál bitvu,

* Historie této křivky je poněkud barvitá. Původní název *versaria* pro ni zvolil italský matematik Guido Grandi (1703). Souvisí s její konstrukcí a znamená „otáčející se v libovolném směru“. Časem dostalo slovo *versaria* jiný význam – znamenalo ženu, která nevěří v Boha. Do angličtiny pak bylo přeloženo jako *witch* – čarodějka.

nikoliv však válku.

6. Fermatova čísla

Fermat jistě neočekával, že se mnoho matematiků bude dodnes zabývat hledáním prvočíselných rozkladů Fermatových čísel $F_m = 2^{2^m} + 1$ pro $m = 0, 1, 2, \ldots$. Mylně předpokládal, že všechna čísla tohoto tvaru jsou prvočísla. Právě tato Fermatova chybná hypotéza stále inspiruje matematiky k objevování nových metod a k provádění velkého množství výpočtů při studiu vlastností Fermatových čísel. Řadu překvapujících tvrzení i s důkazy najde čtenář v monografii [Křížek, Luca, Somer].

Poslední zpráva o novém výsledku je z 3. července 2002 (viz tab. 1):

News Flash!

On July 3, 2002, Jim Fougeron discovered

the following new factor

of a Fermat number: $13308899 \cdot 2^{3723} + 1$ divides F_{57233}.

Tab. 1.

Výpočty v této oblasti přinášejí v poslední době mnoho nových objevů (viz tab. 2):

Nedávno nalezení prvočinitelé F_m

Datum	Prvočinitel	Objevitel
11. dubna 2002	$1503975.2^{5533} + 1$ dělí F_{5531}	Gary Gostin
4. dubna 2002	$541664191 \cdot 2^{976} + 1$ dělí F_{971}	Dmitrij Komin
6. března 2002	$7619 \cdot 2^{50081} + 1$ dělí F_{50078}	Göran Axelsson
5. února 2002	$63 \cdot 2^{270094} + 1$ dělí F_{270091}	Tadashi Taura

Tab. 2.

Aktuální zpráva o Fermatových číslech F_m z 3. července 2002 říká (viz tab. 3) :

Prvočísla	m = 0, 1, 2, 3, 4
Složená úplně rozložená čísla	m = 5, 6, 7, 8 (každé dva dělitele), 9 (3 dělitelé), 10 (4 dělitelé), 11 (5 dělitelů)
Pět známých prvočíselných dělitelů	m = 12
Čtyři známí prvočíselní dělitelé	m = 13
Tři známí prvočíselní dělitelé	m = 15, 25
Dva známí prvočíselní dělitelé	m = 16, 18, 19, 27, 30, 36, 38, 52, 77, 147, 150, 284, 416
Jeden známý prvočíselný dělitel	m = 17, 21, 23, 26, 28, 29, 31, 32, 37, 39, 42, 43 a 166 hodnot m v intervalu $43 < m \leq 382447$
Složená Fermatova čísla, ale žádní známí dělitelé	m = 14, 20, 22, 24
Charakter čísel neznámý	m = 33, 34, 35, 40, 41, 44, 45, 46, 47, 49, 50, ...

Tab. 3.

K datu 18. září 2002 víme s jistotou, že alespoň 206 Fermatových čísel je složených (viz [w2]).

7. Počátky teorie pravděpodobnosti

Vášeň hráčů hazardních her přivedla matematiky k řešení úloh náležejících dnes do teorie pravděpodobnosti. Následující úlohu o rozdělení sázky řešil Fermat v korespondenci s Blaisem Pascalem.

> Dva hráči *A* a *B* hrají několik her o určitou částku *C*. Tuto částku dostane hráč, který vyhraje jako první *k* her. Hry jsou přerušeny ve chvíli, kdy jednomu z hráčů chybí do vítězství *l* her, druhému *m* her. Jak bude částka *C* spravedlivě mezi hráče rozdělena?

Zvolme např. $l = 2$ a $m = 3$. V tomto případě bude $k \geq 3$ libovolné. Fermat si uvědomil, že je třeba prověřit 16 níže uvedených možností:

aaaa, baaa, abaa, aaba, aaab, bbaa, abba, aabb, baba, abab, baab;
abbb, babb, bbab, bbba, bbbb,

kde *a*, resp. *b* znamená vítězství hráče *A*, resp. *B*. Odtud je již patrno, že částka *C* bude spravedlivě rozdělena v poměru 11 : 5.

Pascal ocenil Fermatovo řešení v dopise datovaném 29. července 1654 takto:

„Nyní již nepochybuji o tom, že jsem na správné cestě, když se moje výsledky shodují s Vašimi. Vidím, že pravda je na světě jen jedna, v Toulouse i v Paříži.“

I když byl Pascalův postup poněkud odlišný od Fermatova, oba dospěli ke stejnému výsledku. Oba tak učinili první kroky v rozvíjející se teorii pravděpodobnosti.

Fermat se pak snažil aplikovat pravděpodobnost v teorii čísel, ale to Pascala nezaujalo a Fermat pokračoval v korespondenci o dalších úlohách z pravděpodobnosti s Christianem Huygensem (viz [Mačák]).

8. Fermatův princip

V mnoha učebnicích fyziky se v kapitole o optice setkáme s *Fermatovým principem.*

Když se v roce 1650 jeden z Descartových žáků rozhodl shromáždit Descartovu korespondenci k vydání, obrátil se také s žádostí o pomoc k Fermatovi. Při této příležitosti se Fermat začal zabývat Descartovými optickými výklady. Odvodil, že se světlo pohybuje vzhledem k času vždy po nejkratší možné dráze. Dospěl k témuž principu, který popisuje lom světla při průchodu z jednoho optického prostředí do druhého jako Descartes, i když ne zcela správným postupem (podrobnosti viz [Andersen]):

$$\frac{\sin\alpha_1}{\sin\alpha_2} = \frac{v_1}{v_2},$$

kde α_1, α_2 jsou úhly dopadu a lomu a v_1, v_2 jsou rychlosti světla v daném prostředí.



Obr. 10. Fermatova busta, sál Henri-Martina, Capitole, Toulouse.

9. Závěr

Fermat užíval k důkazům postup blízký principu matematické indukce v dobře uspořádané množině pod názvem **metoda nekonečného sestupu**. Dobře si uvědomoval i platnost základní věty aritmetiky [Goldman], což mu umožnilo dokázat řadu zajímavých výsledků.

Fermat objevil vlastní **metodu rozkladu přirozených čísel**, která je efektivní, je-li N součin dvou přirozených čísel přibližně stejné velikosti. Tato faktorizační metoda nevyžaduje uchovávat v paměti počítače žádná prvočísla, jak je to nezbytné například u známého Eratosthenova síta.

Předpokládejme tedy, že N je složené. Je-li N čtverec, pak je rozklad ukončen. Jestliže N není čtverec, definujeme $a = \lfloor \sqrt{N} \rfloor + 1$, kde $\lfloor \sqrt{N} \rfloor$ označuje celou část $\sqrt{N}$, a položíme $x = a^2 - N$. Jestliže je to čtverec, jsme u konce, protože $N = \left(a + \sqrt{x}\right)\left(a - \sqrt{x}\right)$. Jinak vypočtěme další hodnotu

$$(a+1)^2 - N = a^2 + 2a + 1 - N = x + 2a + 1$$

a opět zjistíme, zda-li to je čtverec nebo ne. Jestliže ano, skončili jsme. Pokud ne, zvýšíme a o 2 atd. Po konečném počtu kroků najdeme rozklad na netriviální činitele (viz [Beran I, II]).

Souvislost mezi Velkou Fermatovou větou a Fermatovými čísly plyne z následujícího tvrzení (viz [Křížek, Luca, Somer], s. 69):

Nechť p prvočíslo takové, že $p \mid F_m$. Pak platí

$$p^2 \mid F_m \Leftrightarrow 2^{p-1} \equiv 1 \left(\mathrm{mod}\, p^2\right) \text{ (Wieferichova kongruence).}$$

Když nějaké prvočíslo splňuje Wieferichovu kongruenci, pak také platí tzv. první případ Velké Fermatovy věty (viz [Skula]). Zatím jsou známa pouze dvě prvočísla, která splňují Wieferichovu kongruenci, $p = 1093$ a $p = 3511$. Byla objevena dlouho před možností použít počítače – Meissnerem (1913) a Beegerem (1922). Lze ale ukázat, že nedělí žádné F_m pro $m \leq 5$, neboť nemají obecný tvar dělitelů $2^{m+2}k+1$ Fermatových čísel.



Obr. 11. Socha Pierra de Fermata, detail, Beaumont-de-Lomagne.

Fourierova a Laplaceova transformace, které jsou široce užívané v technických aplikacích, předpokládají spojitá vstupní data. Při

použití výpočetní techniky musí být diskretizovány. Kromě diskrétní Fourierovy transformace a rychlé Fourierovy transformace se používá také **Fermatova digitální transformace** (Fermat Number Transform – FNT), která je jednodušší a rychlejší než rychlá Fourierova transformace. Diskrétní Fourierova transformace se počítá v komplexní aritmetice, zatímco Fermatova transformace se počítá v celočíselné aritmetice (více viz [Křížek, Luca, Somer], s. 167). Je to pěkná ukázka praktické aplikace Fermatových čísel. Jiným příkladem jsou generátory pseudonáhodných čísel nebo rychlé násobení v aritmetice modulo F_m.

Fermat formuloval řadu hypotéz, jejichž dokazování se věnovali matematici v dalších stoletích, např. **Fermatovu větu o součtu**:

Diofantická rovnice $y^3 = x^2 + 2$ *má celočíselné řešení pro* $y = 3,\ x \pm 5$ a žádné jiné.

Úlohu o **Fermatově bodu** *X*, který minimalizuje součet vzdáleností bodu *X* od všech vrcholů *A*, *B*, *C* ostroúhlého trojúhelníka *ABC*, navrhl Fermat Galileiovu žáku Evaristu Torricellimu (viz např. [Šolcová]); Torricelliho řešení pak publikoval v roce 1659 Viviani. Zobecněním této úlohy do *n* dimenzí je slavný **Fermatův–Weberův problém:** Nechť $S = \{p_1, \ldots, p_n\}$ je množina bodů v R^d. Pro každý bod $q \in R^d$ definujme jeho váhu takto:

$$w(q) = \sum_{i=1}^{n} d(q, p_i),$$

kde $d(x, y)$ označuje eukleidovskou vzdálenost mezi *x* a *y*. Fermatův–Weberův problém spočívá v nalezení bodu q_{opt}, pro který funkce *w* nabývá svého minima. Metoda rychlé aproximace těchto součtů je uvedena v článku [Bose, Maheswari, Morin] .

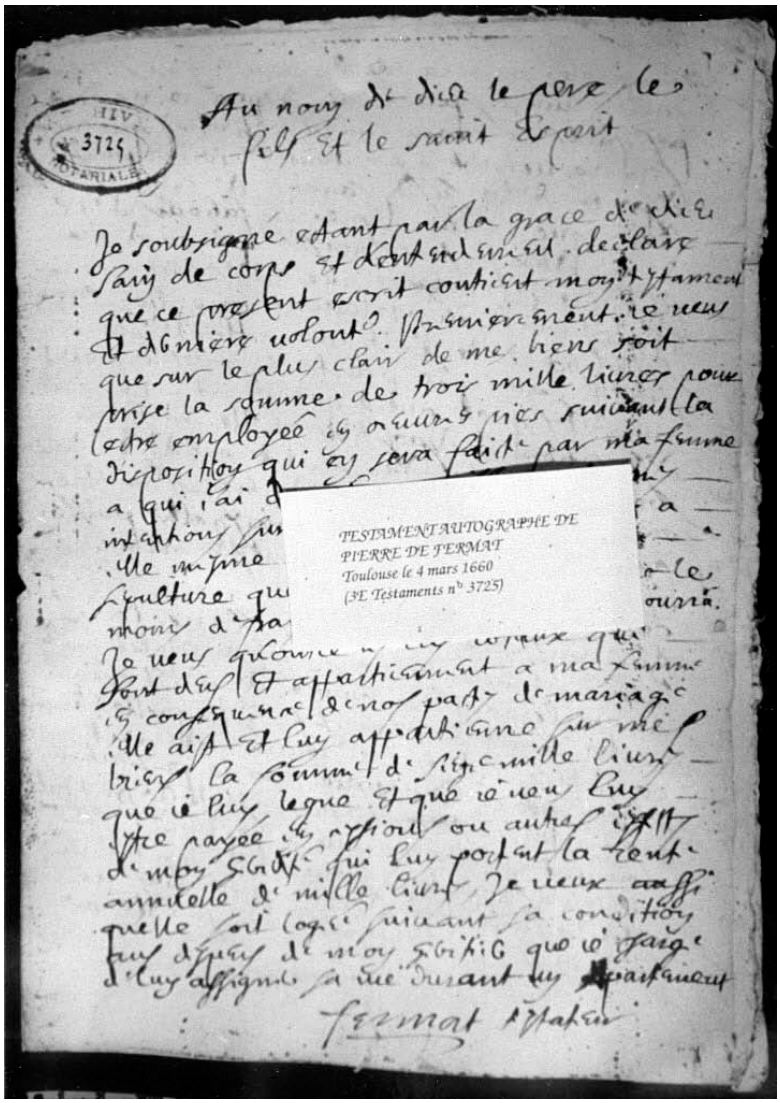
V roce 1638 Fermat usoudil, že každé přirozené číslo lze vyjádřit jako součet nejvýše tří trojúhelníkových čísel, čtyř čtvercových čísel, pěti pětiúhelníkových čísel a *n* čísel *n*-úhelníkových. Své tvrzení však nikdy nedokázal. **Fermatův problém mnohoúhelníkových čísel** zaujal mladého Carla Friedricha Gausse (1777-1855), který dokázal jeho speciální trojúhelníkový případ a tuto zprávu si zapsal do svého deníku 10. července 1796 takto:

$$** \quad \text{EYRHKA} \quad num = \Delta + \Delta + \Delta.$$

V roce 1812 dokázal August Cauchy obecný případ.

Na počest Fermata je také pojmenován **interaktivní algebraický počítačový systém** *Fermat* pro matematické experimentování (viz [w1]) podobající se známějšímu Matlabu, Maplu či Mathematice. *Fermat* vznikl jako projekt R. E. U. (Research Experiences for

Undergraduates) vedený Robertem H. Lewisem na Fordham University, Bronx N. Y., v roce 1986. Byl již použit ke studiu eliptických křivek, počítačových algoritmů a k numerické analýze. Umožňuje studium dynamických systémů. Hodí se i pro metodu RSA. Poskytuje také rozmanité grafické možnosti. V poslední době se rozvíjí jeho aplikace v lineární algebře a pro vyšetřování racionálních funkcí. Program má dvě verze: *QFermat* (pro *Q, Z* a konečná tělesa) a *FFermat* (pro reálná čísla a komplexní, typ float).



Obr. 12. Rukopis Fermatovy závěti s vlastnoručním podpisem, Toulouse, 4. března 1660. Závěť je uložena v Muzeu Pierra de Fermata, Beaumont-de-Lomagne.

Fermatova cena je vyhlašována každé dva roky Univerzitou Paula Sabatiera ve francouzském Toulouse. Je to ocenění pro jednoho nebo více matematiků za práce v oborech, v nichž Pierre de Fermat působil: variační metody, základy infinitezimálního počtu a pravděpodobnosti, analytická geometrie a teorie čísel. Mezi oceněnými je i Andrew Wiles (1995) a Richard Taylor (2001) za důkaz Velké Fermatovy věty.

Fermatovo jméno proniklo i do filatelie. Je např. vyryto na české známce věnované Světovému roku matematiky 2000 a na francouzské známce z roku 2001, kdy si připomínáme 400. výročí Fermatova narození.

Fermatova sláva přesahuje dokonce hranice planety Země. Jeho jméno nalezneme i na mapě Měsíce, kde je po něm pojmenován **kráter Fermat** o průměru 39 km v blízkosti pohoří Altaj.

Literatura

Andersen, K.: *The mathematical technique in Fermat's deduction of the law of refraction,* Historia Math. 10 (1983), 48-62.

Barner, K.: *How old did Fermat become?* Univ. Gesamthochschule Kassel, Fachbereich Mathematik/Informatik, preprint No. 17/00, 2000, 1-22.

Beran, L.: *Fermatova metoda rozkladu v retrospektivě,* Rozhledy mat.-fyz. 72 (1995), 113-115.

Beran, L.: *Fermatova metoda rozkladu ve vašich rukách*, Rozhledy mat.-fyz. 72 (1995), 277-283.

Bose, P., Maheswari, A., Morin, P.: *Fast approximations for sums of distances, clustering and the Fermat–Weber problem*, Carleton University, 2002.

Diffie, W., Hellman, M.: *New directions in cryptography*, IEEE Trans. Inform. Theory, IT – 22, 1976, 644-654.

Dunham, W.: *The mathematical universe. An alphabetical journey through the great proofs, problems, and personalities,* John Wiley & Sons, Inc. New York – Chichester – Brisbane – Toronto – Singapore, 1947.

Eves, H.: *An introduction to the history of mathematics,* 3rd ed., Holt, Rinehart and Winston, New York, 1969.

Fletcher, C. R.: *Fermat's theorem*, Historia Math. 16 (1989), 149-153.

Fletcher, C. R.: *A reconstruction of the Frénicle-Fermat correspondence of 1640,* Historia Math. 18 (1991), 344-351.

Goldman, J. R.: *The queen of mathematics. A historically motivated guide to number theory*, A. K. Peters, Welleslay, Massachusetts, 1998.

Hellegouarch, Y.: *Invitation to the mathematics of Fermat-Wiles*, Academic Press, London, 2002.

Horadam, A. F.: *A synthesis of certain polynomial sequences*, in: Appl. of Fibonacci Numbers, Vol. 6, Dordrecht, 1996, 215–229.

Indorato, L., Nastasi, P.: *The 1740 resolution of the Fermat–Descartes controversy*, Historia Math. 16 (1989), 137-148.

Křížek, M.: *Metoda RSA pro šifrování zpráv pomocí velkých prvočísel,* Rozhledy mat.-fyz. 75 (1998), 101-107.

Křížek, M., Luca, F., Somer, L.: *17 lectures on Fermat numbers: From number theory to geometry*, Springer-Verlag, New York, 2001.

Mačák, K.: *Počátky počtu pravděpodobnosti,* Prometheus, Praha, 1997.

Mahoney, M. S.: *The mathematical career of Pierre de Fermat (1601–1665)*, Princeton University Press, Princeton, New Jersey, 1973, 1994.

Mauldin, R. D.: *A generalization of Fermat's Last Theorem: The Beal conjecture and prize problem,* Notices Amer. Math. Soc., 44 (1997), 1436-1437, český překlad Pokroky mat. fyz. astronom. 43 (1998), 104-107.

Nekovář J.: *Modulární křivky a Fermatova věta. Modular curves and Fermat's Last Theorem*, Math. Bohem. 119 (1994), 1, 79-96.

Rivest R. L., Shamir A., Adleman L. M.: *A method for obtaining digital signatures and public key cryptosystems*, Comm. ACM 21 (1978), 120-126.

Singh, S.: *Fermat's Last Theorem* (v českém překladu *Velká Fermatova věta*), Fourth Estate, London (Academia, Praha) 1997, 2000.

Skula, L.: *Některé historické aspekty Fermatova problému*, Pokroky mat. fyz. astronom. **39** (1994), 318-330.

Šolcová, A.: *D'Artagnan mezi matematiky - pocta Pierru Fermatovi k 400. výročí narození,* Pokroky mat. fyz. astronom. 46 (2001), 286-298.

Taylor, R., Wiles, A.: *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. 141 (1995), 553-572.

Wiles, A.: *Modular elliptic curves and Fermat's Last Theorem*, Ann. of Math. 141 (1995), 443-551.

[w1] http://www.bway.net/~lewis

[w2] http://www.prothsearch.net/fermat.html

[w3] http://www.keypress.com/sketchpad/java_gsp/witch.html

Adresa: RNDr. Alena Šolcová, katedra matematiky, ČVUT Stavební fakulta, Thákurova 7, 166 29 Praha 6, e-mail: solcova@mbox.cesnet.cz