Yann Bugeaud; Maurice Mignotte
Catalanova domněnka dokázána

*Pokroky matematiky, fyziky a astronomie*, Vol. 50 (2005), No. 4, 280--285

Persistent URL: http://dml.cz/dmlcz/141281

# Catalanova domněnka dokázána

*Yann Bugeaud a Maurice Mignotte, Strasbourg*

## 1. Úvod

V roce 1844 E. Catalan[1]) zaslal L. von Crellemu, zakladateli a vydavateli prestižního matematického časopisu *Journal für die reine und angewandte Mathematik*, následující sdělení, které bylo vzápětí v časopise uveřejněno:

> *Je vous prie, Monsieur, de bien vouloir énoncer, dans votre recueil, le théorème suivant, que je crois vrai, bien que je n'aie pas encore réussi à le démontrer complètement: d'autres seront peut-être plus heureux:*
>
> *Deux nombres entiers consécutifs, autres que* 8 *et* 9*, ne peuvent être des puissances exactes; autrement dit: l'équation* $x^m - y^n = 1$*, dans laquelle les inconnues sont entières et positives, n'admet qu'une seule solution.*

Stručně řečeno, Catalanova otázka zní: Existují po sobě jdoucí kladná celá čísla kromě 8 a 9, která jsou obě mocninami? Tato otázka je ekvivalentní *Catalanově rovnici*

$$x^m - y^n = 1, \quad \text{kde} \quad m, n, x, y \geqq 2, \tag{1}$$

která je předmětem Ribenboimovy knihy [14].

Rovnici (1) vyřešil v roce 2002 Preda Mihăilescu: jediné kladné řešení[2]) je $9 - 8 = 3^2 - 2^3 = 1$. Jeho důkaz, i když není tak náročný jako Wilesův důkaz Velké Fermatovy věty, nemůžeme zde pro jeho obtížnost ani uvést, ani naznačit. Omezíme se jen na stručný historický přehled obsahující všechny podstatné příspěvky k problému. Náš závěrečný seznam literatury není zdaleka úplný.

Je zřejmé, že (1) stačí vyřešit jen pro prvočíselné hodnoty exponentů $m$ a $n$. Dále budeme proto vždy uvažovat ekvivalentní problém

$$x^p - y^q = 1, \quad \text{kde } p \text{ a } q \text{ jsou prvočísla a } x, y \geqq 2. \tag{2}$$

[1]) Pozn. překl.: Belgický matematik Eugène Catalan (1814–1894) měl to štěstí, že kromě Catalanovy domněnky byla po něm nazvána i posloupnost Catalanových čísel $c_n = 1, 2, 5, 14, 42, \ldots$, $c_n = \frac{1}{n+1}\binom{2n}{n}$, která se objevuje v mnoha enumerativních problémech.

[2]) Pozn. překl.: Řešeními rovnic se v tomto textu vždy rozumějí řešení v celých číslech.

Prof. Dr. Y. Bugeaud (1971) a Prof. Dr. M. Mignotte (1946) působí na Univerzitě Louise Pasteura ve Štrasburku (Centre de Calcul de l'Esplanade, 7, rue René Descartes, 67084 Strasbourg, France); e-mail: bugeaud@math.u-strasbg.fr, mignotte@math.u-strasbg.fr

Z anglického rukopisu přeložil Martin Klazar.

## 2. Případ, kdy $p$ nebo $q$ je sudé

V roce 1738 L. Euler ukázal, že jediné řešení rovnice $x^2 - y^3 = 1$ je $x = 3$ a $y = 2$, to jest $9 - 8 = 1$. I když jsou dnes známy různé důkazy tohoto výsledku, žádný z nich není snadný. V roce 1850 V. A. Lebesgue [8] dosáhl prvního významného pokroku v Catalanově problému.

**Věta** (V. A. Lebesgue, 1850)**.** *Diofantická rovnice*

$$x^p - y^2 = 1 \tag{3}$$

*nemá řešení v celých číslech $x$, $y$, $p$, kde $y \neq 0$ a $p$ je prvočíslo.*

V důkazu věty pracoval V. A. Lebesgue s okruhem Gaussových celých čísel $\mathbf{Z}[i]$.

Rovnice $x^2 - y^q = 1$ je však mnohem obtížnější než (3). Vyřešil ji až v roce 1965 Ko Chao v článku [6] a jeho důkaz je velmi rafinovaný.

**Věta** (Ko Chao, 1965)**.** *Diofantická rovnice*

$$x^2 - y^q = 1$$

*má v kladných celých číslech $x$, $y$, $q$, kde $q$ je prvočíslo, jediné řešení $x = 3$, $y = 2$, $q = 3$.*

Dále proto budeme předpokládat, že neznámá prvočísla $p$ a $q$ v (2) jsou obě lichá.

## 3. Casselsova věta

Přirozený postup při řešení rovnice (2) je rozložit ji a přepsat ve tvaru

$$(x - 1)(x^{p-1} + x^{p-2} + \cdots + 1) = y^q.$$

Snadno se dokáže, že čísla $x - 1$ a $x^{p-1} + x^{p-2} + \cdots + 1$ jsou buď nesoudělná, nebo obě dělitelná prvočíslem $p$. V prvním případě hned plyne, že $x - 1$ i $x^{p-1} + x^{p-2} + \cdots + 1$ je $q$-tá mocnina. J. W. S. Cassels však v [3] ukázal, že první případ nemůže nastat.

**Věta** (J. W. S. Cassels, 1960)**.** *Má-li rovnice* (2) *řešení $(x, y, p, q)$, v němž je $pq$ liché, potom $p$ dělí $y$ a $q$ dělí $x$. Navíc existují celá čísla $a$, $b$, $u$, $v$ taková, že*

$$x - 1 = p^{q-1}a^q, \quad y + 1 = q^{p-1}b^p, \quad \sum_{i=1}^{p-1} x^i = pu^q, \quad \sum_{i=1}^{q-1} y^i = qv^p,$$

*kde $x = qbv$ a $y = pau$. Dále máme*

$$x \equiv 1 - p^{q-1} \pmod{q^2} \quad a \quad y \equiv q^{p-1} - 1 \pmod{p^2}.$$

Z Casselsovy věty se dají snadno odvodit dolní odhady pro velikost případných řešení Catalanovy rovnice. Tyto odhady jsou základním nástrojem v důkazech vět, které uvedeme v oddílech 5–7.

## 4. Tijdemanova věta

Bakerova teorie lineárních forem logaritmů algebraických čísel[3]) nalezla v oblasti diofantických rovnic mnoho důmyslných použití. Je například klíčovým nástrojem v důkazu faktu, že množina hodnot každého celočíselného polynomu $p(x)$ s alespoň třemi různými komplexními kořeny, kterých nabývá na celých číslech, obsahuje pouze konečně mnoho mocnin. Konkrétně, pro pevné $m \geqq 3$ má rovnice

$$x^m - 1 = y^n$$

jen konečně mnoho řešení $(x, y, n)$ s $n \geqq 2$ a lze explicitně spočítat horní odhad velikosti složek řešení. Platí dokonce i více: Je-li hodnota libovolné ze čtyř proměnných v rovnici (1) fixována, má rovnice ve zbývajících třech proměnných jen konečně mnoho řešení. Je překvapující, že lze jít ještě dále. V roce 1976 R. Tijdeman v [16] předvedl nádherné použití Bakerovy teorie, když dokázal konečnost počtu řešení rovnice (1).

**Věta** (R. Tijdeman, 1976)**.** *Catalanova rovnice* (1) *má pouze konečně mnoho řešení* $(x, y, m, n)$*. Navíc lze efektivně spočítat takovou konstantu* $C$*, že všechna řešení rovnice* (1) *splňují odhad* $\max\{|x|, |y|, m, n\} < C$*.*

Konstanta $C$ vypočítaná z odhadů lineárních forem logaritmů známých v té době vyšla velmi velká: M. Langevin v [7] provedl výpočty a získal odhady

$$\max\{m, n\} < 10^{106}, \quad \max\{x, y\} < \exp(\exp(\exp(\exp(700)))).$$

Tyto odhady na $x$ a $y$ nebyly samozřejmě nikdy použity. Od roku 1976 došlo v teorii lineárních forem logaritmů k pokroku a v roce 2000 byl v [11] dokázán odhad

$$\max\{m, n\} < 7{,}78 \times 10^{16}.$$

Další směr útoku na Catalanův problém, s nímž začal K. Inkeri, byl získat různá kritéria pro dvojice prvočísel $(p, q)$, která by ukazovala, že tyto dvojice nemohou být exponenty v řešení rovnice (2). Pokud by se to podařilo pro každou dvojici s $p$ a $q$ menšími než $7{,}78 \times 10^{16}$, byla by rovnice vyřešena!

## 5. Algebraická kritéria

Prvním matematikem, který nalezl algebraická kritéria pro Catalanovu rovnici, byl K. Inkeri. Dokázal dva výsledky, první v roce 1964 pro případ $p \equiv 3 \pmod 4$ a druhý

[3]) Pozn. překl.: Jde o dolní odhady veličiny $|\Lambda|$, kde $\Lambda = \sum \alpha_i \log \beta_i$ je konečný součet obsahující algebraická čísla $\alpha_i$, $\beta_i$ (tj. kořeny polynomů s racionálními koeficienty) a $\Lambda \neq 0$. Alan Baker (1939) za své fundamentální výsledky obdržel v roce 1970 Fieldsovu medaili.

v roce 1990 pro případ $p \equiv 1 \pmod 4$ (viz [4] a [5]). Následující věta je jejich kombinací.

**Věta** (K. Inkeri, 1964 a 1990)**.** *Má-li rovnice* $x^p - y^q = \pm 1$*, kde* $p$ *a* $q$ *jsou lichá prvočísla, řešení, pak*

$$p^{q-1} \equiv 1 \pmod{q^2} \quad \textit{nebo} \quad q \mid h(\mathbf{K}_p), \tag{4}$$

*kde* $h(\mathbf{K})$ *označuje počet tříd číselného tělesa* $\mathbf{K}$ *a kde*

$$\mathbf{K}_p = \begin{cases} \mathbf{Q}(\sqrt{-p}) & \textit{pro} \quad p \equiv 3 \pmod 4, \\ \mathbf{Q}(\mathrm{e}^{2\pi \mathrm{i}/p}) & \textit{pro} \quad p \equiv 1 \pmod 4. \end{cases}$$

Počet tříd je přirozené číslo přiřazené číselnému tělesu, které je dosti obtížné spočítat[4]). Například není známa jeho hodnota pro těleso $\mathbf{Q}(\mathrm{e}^{2\pi \mathrm{i}/p})$, pokud $p \geqq 71$. Inkeriho věta obsahuje dvě podmínky, které lze užít pro vyloučení exponentů $(p, q)$: kongruenční podmínku a podmínku dělitelnosti pro jistý počet tříd. Následně byla Inkeriho kritéria vylepšena M. Mignottem v [10] a W. Schwarzem [15], kterým se podařilo nahradit počet tříd $h$ v (4) *relativním počtem tříd*, obvykle označovaným $h^-$, který se dá snáze spočítat.

Poznamenejme, že Inkeriho kritéria i jejich zmíněná vylepšení se nedají použít pro dvojice prvočísel

$$(83, 4871), \quad (193, 4877) \quad \text{a} \quad (2903, 18787). \tag{5}$$

Tyto tři dvojice $(p, q)$ totiž splňují kongruence $q^{p-1} \equiv 1 \pmod{p^2}$ a $p^{q-1} \equiv 1 \pmod{q^2}$.

V dubnu 1999 nalezli Y. Bugeaud a G. Hanrot podstatně odlišné kritérium (viz [2]), když se jim podařilo odstranit z (4) kongruenční podmínku.

**Věta** (Y. Bugeaud a G. Hanrot, 1999)**.** *Má-li rovnice* $x^p - y^q = \pm 1$*, kde* $p$ *a* $q$ *jsou lichá prvočísla a* $p < q$*, řešení, pak*

$$q \mid h^-\big(\mathbf{Q}(\mathrm{e}^{2\pi \mathrm{i}/p})\big).$$

Toto kritérium umožňuje vyloučit dvojice uvedené v (5). Bohužel není symetrické v $p$ a $q$ (na rozdíl od Inkeriho kritéria) a není příliš užitečné pro velká $p$ (větší než, řekněme, $10^6$), protože relativní počet tříd není lehké spočítat.

[4]) Pozn. překl.: Číselné těleso $\mathbf{K}$ je komutativní těleso obsahující těleso racionálních čísel $\mathbf{Q}$, které jako vektorový prostor nad $\mathbf{Q}$ má konečnou dimenzi. Těleso $\mathbf{K}$ obsahuje okruh celých čísel $O_{\mathbf{K}}$ tělesa $\mathbf{K}$, který v něm hraje stejnou roli jako okruh celých čísel $\mathbf{Z}$ v $\mathbf{Q}$. Na množině ideálů okruhu $O_{\mathbf{K}}$ (přesněji řečeno na jejich ekvivalenčních třídách) se přirozeným způsobem zavede grupová struktura, *grupa tříd ideálů* $G$. Řád grupy $G$, která je konečná, je právě počet tříd $h(\mathbf{K})$. Toto číslo měří nejednoznačnost rozkladů na ireducibilní prvky v $O_{\mathbf{K}}$.

V září 1999 P. Mihăilescu eliminoval z (4) podmínku pro počet tříd (viz [12]).

**Věta** (P. Mihăilescu, 1999)**.** *Má-li rovnice* $x^p - y^q = \pm 1$*, kde* $p$ *a* $q$ *jsou lichá prvočísla, řešení, pak*

$$q^{p-1} \equiv 1 \pmod{p^2} \quad a \quad p^{q-1} \equiv 1 \pmod{q^2}.$$

Mihăilescův důkaz má asi dvě strany a sleduje Inkeriho postup, navíc ale pracuje velmi rafinovaně s tzv. Stickelbergerovým prvkem a s jeho pomocí vylučuje podmínku pro počet tříd.

## 6. Dolní odhady pro exponenty

Díky předchozím kritériím se dají získat dolní odhady pro $\min\{p, q\}$. Výpočty probíhají následovně. Pro pevné $p$ uvažujeme systém rovnic $x^p - y^q = \pm 1$. S pomocí odhadů pro lineární formy logaritmů umíme dokázat, že pro $p > 3000$

$$q < 2{,}77p\big(\log(q/\log p) + 2{,}333\big)^2 \log p,$$

což nám dává dobrý horní odhad pro $q$, který označíme $Q(p)$. Pro $p$ menší než 3000 získáme podobné odhady. Pak, s použitím výsledků z oddílu 5, vyloučíme každou dvojici $(p, q)$, kde $q < Q(p)$. Po několika měsících výpočtů byl získán následující výsledek (viz [11]).

**Věta** (M. Mignotte, 2001)**.** *Rovnice* (2) *nemá řešení* $(x, y, p, q)$*, v němž je* $pq$ *liché a* $\min\{p, q\} < 10^7$.

Třebaže počítače jsou stále výkonnější a výkonnější, mezi dolními a horními odhady exponentů stále zůstává velká mezera. Pro úplné vyřešení Catalanovy rovnice byly zapotřebí nové nápady.

## 7. Konec příběhu

V dubnu 2002 Yuri Bilu rozeslal několika kolegům emailovou zprávu, v níž oznámil, že se P. Mihăilescovi podařilo úplně vyřešit Catalanovu rovnici, viz [13].

**Věta** (P. Mihăilescu, 2002)**.** *Jediným řešením Catalanovy rovnice je*

$$9 - 8 = 3^2 - 2^3 = 1.$$

Důkaz je založen na obtížných nástrojích z teorie kruhových těles [to jsou právě tělesa $\mathbf{Q}(\mathrm{e}^{2\pi\mathrm{i}/p})$ z oddílu 5]. Byl uveřejněn po 160 letech od Catalanova dopisu v témže německém časopise, v *Journal für die reine und angewandte Mathematik*. Čtenář může nahlédnout také do textu [1] ze *Seminaire Bourbaki*, který přednesl Yuri Bilu v listopadu 2002 v Paříži nebo do článku [9] od T. Metsänkyläho.

Na závěr zbývá otázka: existují jiné kladné mocniny než 25 a 27, které se liší o 2? Patrně ne, ale v současnosti není známo ani to, zda rovnice $x^m - y^n = 2$ má jen konečně mnoho (netriviálních) řešení!

L i t e r a t u r a


[1] Bilu, Yu.: *Catalan' conjecture (after Mihăilescu).* Sém. Bourbaki, 55 ème année, *909*, 2002/03, 24 s.

[2] Bugeaud, Y., Hanrot, G.: *Un noveau critère pour l'équation de Catalan.* Mathematika *47* (2000), 63–73.

[3] Cassels, J. W. S.: *On the equation $a^x - b^y = 1$, II.* Proc. Cambridge Philos. Soc. *56* (1960), 97–103.

[4] Inkeri, K.: *On Catalan's problem.* Acta Arith. *9* (1964), 285–290.

[5] Inkeri, K.: *On Catalan's conjecture.* J. Number Theory *34* (1990), 142–152.

[6] Ko Chao: *On the diophantine equation $x^2 = y^n + 1$, $xy \neq 0$.* Sci. Sinica *14* (1965), 457–460.

[7] Langevin, M.: *Quelques applications de nouveaux résultats de van der Poorten.* Sém. Delange-Pisot-Poitou, 1977/78, Paris, Exp. 4, 7 s.

[8] Lebesgue, V. A.: *Sur l'impossibilité en nombres entiers de l'équation $x^m = y^2 + 1$.* Nouv. Ann. Math. *9* (1850), 178–181.

[9] Metsänkylä, T.: *Catalan's conjecture: another old Diophantine problem solved.* Bull. Amer. Math. Soc. (N. S.) *41* (2004), 43–57.

[10] Mignotte, M.: *A criterion on Catalan equation.* J. Number Theory *52* (1995), 280–284.

[11] Mignotte, M.: *Catalan's equation just before 2000.* Number theory (Turku, 1999), 247–254, de Gruyter, Berlin 2001.

[12] Mihăilescu, P.: *A class number free criterion for Catalan's conjecture.* J. Number Theory *99* (2003), 225–231.

[13] Mihăilescu, P.: *Primary cyclotomic units and a proof of Catalan's conjecture.* J. Reine Angew. Math. *572* (2004), 167–195.

[14] Ribenboim, P.: *Catalan's conjecture.* Academic Press, Boston 1994.

[15] Schwarz, W.: *A note on Catalan equation.* Acta Arith. *72* (1995), 277–279.

[16] Tijdeman, R.: *On the equation of Catalan.* Acta Arith. *29* (1976), 197–209.