Z historie řešení diofantických rovnic: od Diofanta k Mihăilescovi

Martin Klazar
Katedra aplikované matematiky, MFF UK, Praha

Přehled

1. Co je diofantická rovnice. Kdo byl Diofantos.
2. Fermatova poslední věta a abc domněnka.
3. Catalanův problém. Kdo je P. Mihăilescu.
4. Desátý Hilbertův problém.
5. C. Runge, A. Thue, Th. Skolem, C. L. Siegel,
A. Baker, G. Faltings.

1. Co je diofantická rovnice. Kdo byl Diofantos.

Diofantická rovnice:

$$P(x_1, x_2, \ldots, x_n) = 0 \ ,$$

$P \in \mathbf{Z}[x_1, \ldots, x_n]$ je polynom a řešení $x_i \in \mathbf{Z}$ (celá čísla). *Variace:* soustavy rovnic, exponenciální funkce místo polynomů, $x_i \in \mathbf{Q}$ a další obory. *Motivace:* vztahy mezi výrazy vytvořenými z celých čísel pomocí aritmetických operací $+$ a $\times$. *Zkoumané otázky:*

- existence řešení
- (ne)konečnost počtu řešení
- efektivní nalezení řešení

Příklad. *Pythagorejské trojice (PT):* hledáme trojici čísel $x, y, z \in \mathbf{Z}$, že

$$x^2 + y^2 = z^2 \ .$$

Triviální PT: $0^2 + (-2015)^2 = 2015^2, \ldots$ — $xyz = 0$.
Netriviální PT: $(-24)^2 + 10^2 = (-26)^2, \ldots$ — $xyz \neq 0$.
Primitivní PT: $x, y, z > 0$, $(x, y) = \mathrm{NSD}(x, y) = 1$, x je liché a y sudé. Každá netriviální PT se lehce převede na primitivní.

Věta. *x, y, z je primitivní PT* $\iff$ $x = a^2 - b^2$, $y = 2ab$, $z = a^2 + b^2$, *kde* $a > b > 0$, $(a, b) = 1$ *a mají různou paritu* $(a, b \in \mathbf{Z})$.

Důkaz. Implikace $\Leftarrow$ je jasná. $\Rightarrow$: $x^2 + y^2 = z^2$ dává

$$\left(\frac{y}{2}\right)^2 = \frac{z+x}{2} \cdot \frac{z-x}{2} =: u \cdot v \ ,$$

kde $u, v \in \mathbf{N} = \{1, 2, \ldots\}$ a $(u, v) = 1$. Tedy $u = a^2$, $v = b^2$, $y = 2ab$, $x = a^2 - b^2$, $z = a^2 + b^2$ a a, b mají uvedené vlastnosti. □

Našli jsme ∞ mnoho různých netriviálních PT, dokonce jsme je všechny popsali. Použili jsme **Základní větu aritmetiky (ZVA)** — každé $n \in \mathbf{N}$ má jediný rozklad $n = \prod_{i=1}^{k} p_i^{a_i}$, kde $a_i \in \mathbf{N}$ a $p_1 < p_2 < \cdots < p_k$ jsou prvočísla — a to tak, že ze ZVA plyne

$$u, v, c \in \mathbf{N}, (u, v) = 1, uv = c^2 \Rightarrow u = a^2, v = b^2 \, .$$

ZVA poprvé přesně formuloval a dokázal až *C. F. Gauss (1777-1855)* v Disquisitiones Arithmeticae v r. 1801. Vzorec pro PT x, y, z již u *Eukleida (cca -300)*, Základy, kniha X, tvrzení XXIX. Prvně se objevují ale o 1500 let dříve.

Plimpton 322. Klínopisná tabulka z Babylonu (dnešní jižní Irák), č. 322 v Plimptonově sbírce na Kolumbijské univerzitě, z r. cca -1800, autor neznámý písař či učitel.

Na 15 řádcích uvádí složky y, z PT v šedesátkové soustavě, např. $y = 5 : 19 = 319, z = 8 : 01 = 481$ nebo $y = 1 : 22 : 41 = 4961, z = 2 : 16 : 01 = 8161$.

Geometrické odvození vzorce pro PT

Rovnice pro PT je $(x/z)^2+(y/z)^2 = 1$, tedy hledáme $\mathbf{Q}^2 \cap C$ pro kružnici $C: \ x^2 + y^2 = 1$. Nechť ℓ je přímka jdoucí bodem $(0, 1) \in C$, ne rovnoběžná s osou x, $(t, 0)$ je průsečík ℓ a osy x, α je druhý průsečík ℓ a C. *Pak $t \mapsto \alpha$ je bijekce mezi $\mathbf{Q}$ a $(\mathbf{Q}^2 \cap C) \setminus \{(0, 1)\}$.* Máme $\ell: \ x = (1 - y)t$, z čehož se spočte

$$\alpha = \left(\frac{2t}{t^2 + 1}, \ \frac{t^2 - 1}{t^2 + 1} \right) = \left(\frac{2ab}{a^2 + b^2}, \ \frac{a^2 - b^2}{a^2 + b^2} \right), \ t = a/b \in \mathbf{Q}$$

— $\ell \cap C \leftrightarrow (1 - y)^2 t^2 + y^2 = 1 \leftrightarrow (t^2 + 1)y^2 - 2t^2 y + t^2 - 1 = 0$, tedy y-ová souř. průsečíku α je $[(t^2 - 1)/(t^2 + 1)]/1$ (*F. Viète (1540–1603)* a jeho vzorce).

Obrázek:

Diofantos ($\Delta\iota o\varphi\alpha\nu\tau o\zeta$) z Alexandrie (201–215 až 289–299) byl starořecký (správně: římský) matematik, autor řady knih nazvaných Aritmetika, mnohé z nichž se nedochovaly. Jako první užíval algebraický symbolismus a značení. Řešení po něm později nazvaných rovnic uvažoval ve $\mathbf{Q}$ (v $\mathbf{Z}$ systematicky až Fermat). *Metrodorus (5. st.)* uvádí ve sbírce rébusů a hříček Diofantův věk jako řešení (diofantické?) rovnice

$$x = \frac{x}{6} + \frac{x}{12} + \frac{x}{7} + 5 + \frac{x}{2} + 4$$

($1/6$ života chlapectví, $1/12$ mládí, po $1/7$ se oženil, po 5 letech přišel syn, jenž, žel, se dožil jen $1/2$ věku otce, 4 roky po něm odešel i D.) — $x = 84$ (nelze ověřit z jiného zdroje).

Vydání překladu Diofantovy Aritmetiky do latiny v r. 1621, které pořídil *Claude Gaspard Bachet de Mézirac (1581–1638)*, se proslavilo marginálními poznámkami *P. de Fermat*. (Bachetova, nesprávně Bezoutova, identita praví

$$a, b \in \mathbf{Z}, (a, b) = 1 \;\Rightarrow\; \exists c, d \in \mathbf{Z} : \;\; ca + db = 1 \; .)$$

Nejslavnější z nich je jistě

Fermatova poslední věta (FPV). Když $x, y, z, n \in \mathbf{N}$, tak

$$x^n + y^n = z^n \;\Rightarrow\; n \leq 2$$

(pro $n = 2$ máme PT). Podíváme se na ni v následující kapitole.

2. Fermatova poslední věta a abc domněnka.

Pierre de Fermat (1601/7–1665): právník, člen místního parlamentu v Toulouse, amatérský matematik, teorie čísel, FPV, základy matem. analýzy, optika.

FPV. $x, y, z, n \in \mathbf{N}$, $x^n + y^n = z^n \Rightarrow n \leq 2$.

Věta (Fermat). *FPV pro* $n = 4$*:* $x, y, z \in \mathbf{Z}$*,*

$$x^4 + y^4 = z^4 \;\Rightarrow\; xy = 0\,.$$

Důkaz. Fermatova poznámka v Diofantově Aritmetice, pomocí metody nekonečného sestupu. Výsledek zmiňuje v září 1636 v dopisu *M. Mersennovi (1588–1648)* pro *Sainte-Croix*. □

Částečné výsledky k FPV. *L. Euler (1707–1783):* $n = 3$; *S. Germainová (1776–1831):* $x, y, z \in \mathbf{Z}, x^p + y^p = z^p, 2p + 1 = q \Rightarrow p \,|\, xyz$; exponent $n = 5$ vyřešili

A. M. Legendre (1752–1833) (debakl s portrétem) r. 1830 a *P. Dirichlet (1805–1859)* r. 1828; *G. Lamé (1795–1870)* v r. 1839: $n = 7$; *E. Kummer (1810–1893)* v r. 1847: FPV platí pro $n = p$, když p nedělí ani jeden čitatel zlomků $B_2, B_4, \ldots, B_{n-3}$, kde $x/(e^x - 1) = \sum_{n \geq 0} B_n x^n/n!$ (platí pro $p \leq 100$, $p \neq 37, 59, 67$); *G. Terjanian* v r. 1977: $x, y, z \in \mathbf{Z}, x^{2p} + y^{2p} = z^{2p} \Rightarrow 2p \,|\, x$ nebo $2p \,|\, y$ (elementární důkaz!).

Věta (A. Wiles a R. Taylor, 1995). *FPV platí, tedy*

$$x, y, z, n \in \mathbf{N}, x^n + y^n = z^n \Rightarrow n \leq 2 \,.$$

Poznámky. Důkaz pomocí eliptických křivek, první verze obsahovala mezeru (proto Taylor). Jeho délka je 129 stran (A. W., *Ann. Math.*, 141 (1995) 443–551 a R. T. and A. W., *Ann. Math.*, 141 (1995) 553–572).

Důkaz *Feitovy–Thompsonovy věty* (neexistuje nekomutativní jednoduchá grupa lichého řádu) má 255 stran (W. F. and J. T., *Pacific J. Math.* 13 (1963) 775–1029). Formalizovaný důkaz F.-T. věty v systému Coq byl proveden (naprogramován) po šestiletém úsilí v r. 2012 skupinou vedenou *G. Gonthierem*. A co FPV, nyní *Wilesova-Taylorova věta*? Podle expertů není zatím formalizovaný důkaz v dohledu — W.-T. důkaz je na mnohem vyšší úrovni abstrakce než F.-T. věta.

Je W.-T. důkaz v rámci ZFC (Zermelova–Fraenkelova teorie množin s axiomem výběru)? Jak je, prý nikoli: algebr. geometrie $\rightsquigarrow$ Grothendieckova universa $\rightsquigarrow$ nedosažitelné kardinály. Lze je ale (snad) z důkazu eliminovat, viz *C. McLarty* (*Bull. Symb. Logic* 16 (2010) 359–377).

Následují dva slajdy s úplným důkazem Fermatovy poslední věty ... pro polynomy

Pro polynom $a \in \mathbf{C}[x]$ jako $r(a)$, radikál a, označíme počet jeho kořenů bez násobností. Patrně $r(a^n b) = r(ab)$ a $r(a) \leq \deg a$.

Věta (W. Stothers, 1981; R. C. Mason, 1984). *Když $a, b, c \in \mathbf{C}[x]$, kde $(a, b) = 1$ a některý z a, b, c není konstantní, pak*

$$a + b = c \;\Rightarrow\; \deg a, \deg b, \deg c \leq r(abc) - 1 \,.$$

Důkaz. Nechť $a(x) = \alpha \prod (x - \alpha_i)^{a_i}$ atd. Z $(a/c)'/(b/c)' = -1$ máme $[(a/c)'/(a/c)] \,/\, [(b/c)'/(b/c)] = -b/a$ a

$$\frac{S}{S} \cdot \frac{\sum a_i/(x - \alpha_i) - \sum c_i/(x - \gamma_i)}{\sum b_i/(x - \beta_i) - \sum c_i/(x - \gamma_i)} = -\frac{b}{a} \,,$$

kde $S = \prod (x - \alpha_i)(x - \beta_i)(x - \gamma_i)$ má $\deg S = r(abc)$. Tedy $r(abc) - 1 \geq \deg b, \deg a$ a totéž pro $\deg c$. □

Důsledek (FPV pro polynomy). *Když* $n \in \mathbf{N}$, $a, b, c \in \mathbf{C}[x]$, *kde* $(a, b) = 1$ *a některý z* a, b, c *není konstantní, pak*

$$a^n + b^n = c^n \;\Rightarrow\; n \leq 2$$

(pro $n = 2$ *to opět řeší polynomiální PT).*

Důkaz. S.-M. věta pro $a^n + b^n = c^n$ dává tři nerovnosti $n \deg a, n \deg b, n \deg c \leq r(a^n b^n c^n) - 1 \leq \deg a + \deg b + \deg c - 1$, jejichž sečtení vede na

$$n(\deg a + \deg b + \deg c) \leq 3(\deg a + \deg b + \deg c) - 3$$

a $n < 3$. □

Jak totéž udělat v okruhu $\mathbf{Z}$ místo $\mathbf{C}[x]$? Pro nenulové $a \in \mathbf{Z}$ označíme $r(a) = \prod_{p \mid a} p$ (v prvočíselném rozkladu $|a|$ zapomeneme násobnosti). Opět $r(a^n b) = r(ab)$ a $r(a) \leq |a|$.

abc domněnka (D. Masser a J. Oesterlé, 1985). *Když* $a, b, c \in \mathbf{Z}$ *a* $(a, b) = 1$, *pak pro každé* $\epsilon > 0$ *platí*

$$a + b = c \;\Rightarrow\; |a|, |b|, |c| \ll_\epsilon r(abc)^{1+\epsilon}$$

(zde $\ll_\epsilon \ldots$ *znamená* $< C(\epsilon)|\ldots|$, $C(\epsilon) > 0$*).*

Důsledek abcd (skoro FPV). *Když* $n, a, b, c \in \mathbf{N}$, *pak*

$$a^n + b^n = c^n \;\Rightarrow\; n \leq n_0\,.$$

Důkaz je shodný s polynomiálním případem.

Důsledek abcd (Rothova věta z r. 1955). *Je-li* $\alpha \in \mathbf{R}$ *iracionální algebraické číslo, pak*

$$\left|\alpha - \frac{p}{q}\right| \gg_{\alpha,\epsilon} \frac{1}{q^{2+\epsilon}}$$

pro každé $\epsilon > 0$ *a* $p/q \in \mathbf{Q}$.

V srpnu v roce 2012 ohlásil japonský matematik *Shinichi Mochizuki (1969)* (Ph.D. v r. 1992 pod vedením *G. Faltingse*) důkaz abc domněnky za pomoci „Inter-Universal Teichmüller theory“. Včetně prerekvizit má asi 1500∼2000 stran (vlastní autorovo vyjádření). Březen 2015: lze říci, že „the jury is still out“ ohledně platnosti Mochizukiho důkazu.

3. Catalanův problém. Kdo je P. Mihăilescu.

Eugène Charles Catalan (1814–1894): francouzský a belgický matematik, nar. v Brugách. Studoval v Paříži a v Châlons-sur-Marne. Ph.D. v r. 1841 na Pařížské univerzitě, vedoucí *J. Liouville*. Účastnil se revoluce v r. 1848. Prof. na Univerzitě v Liège, kde zemřel. Catalanova čísla: $\frac{1}{n+1}\binom{2n}{n}$. Řetězové zlomky, kombinatorika, minimální plochy (E. Catalan dokázal, že rovina a helikoida jsou jediné minimální přímkové plochy).

Domněnka (E. Catalan, 1844). *Jediná dvě po sobě jdoucí čísla v množině ryzích mocnin*

$$RM = \{a^b \mid a, b \in \mathbf{N}\backslash\{1\}\}$$

jsou 8 *a* 9. *Ekvivalentně:* $3^2 - 2^3 = 1$ *je jediné netriviální řešení diofantické rovnice* $x^m - y^n = 1$.

Částečné výsledky. *L. Euler v 18. st.:* $m = 2, n = 3$; *V.-A. Lebesgue (1791–1875) v r. 1850:* $n = 2$; *Chao Ko v r. 1965:* $m = 2$; *J. Cassels (1922) v r. 1960:* $x^p - y^q = 1$, $x, y \in \mathbf{N} \Rightarrow p \,|\, y$ a $q \,|\, x$; *R. Tijdeman (1943) v r. 1976:* efektivně konečně mnoho řešení (metoda *A. Bakera*).
Preda Mihăilescu (1955): rumunsko-německý matematik, nar. v Bukurešti. Z Rumunska odešel v 18 letech, studoval matematiku a informatiku v Curychu. Ph.D. na ETH v Curychu v r. 1997 u *E. Englera* a *H. Lenstry*. Působil v Paderbornu, 2005– prof. na Georg-Augustově univerzitě v Göttingen. Numerická matematika a TČ.
Věta (P. Mihăilescu, 2002). *Catalanova d. platí:*

$$x, y, m, n \in \mathbf{N}\backslash\{1\},\ x^m - y^n = 1 \ \Rightarrow\ x = n = 3,\ m = y = 2\,.$$

Domněnka. $n, n+2 \in RM \Rightarrow n = 5^2, n+2 = 3^3$?

4. Desátý Hilbertův problém.

Na prvním Mezinárodním kongresu matematiků v Paříži v r. 1900 se *D. Hilbert (1862–1943)* zeptal:

Desátý Hilbertův problém (D. Hilbert, 1900). *Je řešitelnost diofantických rovnic*

$$P(x_1, x_2, \ldots, x_n) = 0$$

($P \in \mathbf{Z}[x_1, \ldots, x_n]$, $x_i \in \mathbf{Z}$) algoritmicky rozhodnutelná?

Pozorování (Th. Skolem, 1934). Stačí se omezit na polynomy s $\deg P \leq 4$. Neboť $(P_1 = 0) \,\&\, \ldots \,\&\, (P_k = 0) \iff P_1^2 + \cdots + P_k^2 = 0$ a $x = x_1 x_2 \ldots x_k \iff (x = x_1 y_1) \,\&\, (y_1 = x_2 y_2) \,\&\, \ldots \,\&\, (y_{k-2} = x_{k-1} x_k)$.

Jurij Vladimirovič Matijasevič (1947): ruský matematik, nar. v Leningradu. 1980– laboratoř matem. logiky LOMI (Petrohrad). Informatika, TČ, matem. logika, kombinatorika.

Věta (Matijasevič, 1970). *Každé rekurzivně spočetné množině* $A \subset \mathbf{Z}$ *odpovídá polynom* $P \in \mathbf{Z}[x, x_1, \ldots, x_n]$, *že* $a \in A \iff \exists a_1, \ldots, a_k \in \mathbf{Z} : \ P(a, a_1, \ldots, a_k) = 0.$

Důsledek. *Protože existují rek. spočetné množiny s algoritmicky nerozhodnutelným náležením, je odpověď na otázku 10. H. problému negativní.*

Důsledek. *Existuje* $P \in \mathbf{Z}[x_1, \ldots, x_n]$, *že* $\{a \in \mathbf{N} \mid a = P(a_1, \ldots, a_n), a_i \in \mathbf{N}_0\} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots\}$.

Důkaz věty využívá výsledku *M. Davise (1928)*, *J. Robinsonové (1919–1985)* a *H. Putnama (1926)*, že stačí dokázat diofantovost exponenciály.

5. C. Runge, A. Thue, Th. Skolem, C. L. Siegel, A. Baker, G. Faltings.

Věty o konečnosti počtu řešení *celých tříd* diofantických rovnic, nejlépe *efektivní* konečnosti.

Carl Runge (1856–1927): německý matematik a fyzik (spektroskopie). Narodil se v Havaně (jeho otec tam byl dánským konzulem). Ph.D. v r. 1880 u *K. Weierstrasse* a *E. Kummera* v Berlíně, později působil v Göttingen. Rungeho–Kuttovy metody pro numerické řešení ODR. První konečný a efektivní výsledek o třídách diof. rovnic.

Nechť $0 \neq F \in \mathbf{Z}[x,y]$, $\deg_x F = m$, $\deg_y F = n$, $S = \{(i,j) \in \mathbf{N}_0^2 \mid a_{i,j} = [x^i y^j]F \neq 0\}$, ℓ je přímka $x/m + y/n = 1$ jdoucí body $(m,0)$, $(0,n)$ a $T = \ell \cap S$.

Věta (C. Runge, 1887). *Nechť $F \in \mathbf{Z}[x,y]$ je ireducibilní ve $\mathbf{Q}[x,y]$ a diofantická rovnice*

$$F(x,y) = 0$$

má nekonečně mnoho řešení $x, y \in \mathbf{Z}$. Pak
1. Žádný bod z S se nenachází nad přímkou ℓ (tudíž $(m,0), (0,n) \in T$).
2. ℓ-vedoucí část F splňuje $\sum_{(i,j)\in T} a_{i,j}x^i y^j = ap^k$, kde $0 \neq a \in \mathbf{Z}$, $k \in \mathbf{N}$ a $p \in \mathbf{Z}[x,y]$ je ireducibilní.
3. $F(x,y) = 0$, $x, y \in \mathbf{C}$ s x u ∞, určuje algebraickou (víceznačnou) funkci, jejíž všechny Puiseuxovy rozvoje jsou vzájemně konjugované.

To jest, porušuje se 1 nebo 2 nebo 3 $\Rightarrow$ $F(x,y) = 0$ má jen konečně mnoho řešení $x, y \in \mathbf{Z}$. Důkaz je efektivní! Větu však nelze použít třeba pro $x^3 - 2y^3 = 1$.

Důsledek. *Například každá rovnice tvaru*

$$y^n = (ax)^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \ ,$$

kde $a, a_i, n \in \mathbf{Z}$, $n \geq 2$, $a \neq 0$ *a* a_0 *není* d*-tá mocnina pro žádného dělitele* $d \geq 2$ *čísla* n*, má jen konečně mnoho řešení* $x, y \in \mathbf{Z}$.

Důkaz Rungeho věty je efektivní, konkrétně platí:

Věta (P. G. Walsh, 1995). *Nechť* $F \in \mathbf{Z}[x, y]$ *je ireducibilní ve* $\mathbf{Q}[x, y]$ *a porušuje jednu z podmínek 1–3 Rungeho věty,* $d = \max(m, n)$ *a* $h = \max |a_{i,j}|$. *Pak*

$$x, y \in \mathbf{Z}, F(x, y) = 0 \ \Rightarrow \ |x|, |y| < (2d)^{2d+18d^7} h^{12d^6} \ .$$

Axel Thue (1863–1922): norský matematik. Narozen v Tönsbergu, městečku u Oslofjordu. Profesor na Univerzitě v Kristianii (Oslo), 7 dětí, nutná další výuka na vojenské akademii. Teorie čísel a kombinatorika slov: Thueho–Morseovo slovo $011010011001\cdots \not\supset u^3$.

Věta (A. Thue, 1909). *Je-li* $\alpha \in \mathbf{R}$ *algebraické číslo stupně* $d \geq 2$*, pak*

$$|\alpha - p/q| \gg_{\alpha,\epsilon} q^{-d/2-1-\epsilon}$$

pro každé $\epsilon > 0$ *a* $p/q \in \mathbf{Q}$.

Věta (A. Thue, 1908). *Když je* $F \in \mathbf{Z}[x,y]$ *homogenní,* $\deg F \geq 3$ *a je ireducibilní v* $\mathbf{Z}[x,y]$*, pak má diofantická rovnice*

$$F(x,y) = m \in \mathbf{Z}$$

jen konečně mnoho řešení $x, y \in \mathbf{Z}$.

Thueho rovnice jsou rovnice popsané ve větě. Například

$$x^3 - 2y^3 = m$$

má pro každé $m \in \mathbf{Z}$ jen konečně mnoho řešení $x, y \in \mathbf{Z}$ (dokažte si to pro $m = 0$). Jak je ale nalézt? Thueho důkaz je bohužel *neefektivní* (neposkytuje algoritmus), dává jen odhad *počtu* řešení rovnice, nikoli jejich velikosti. A tak to zůstalo, skoro, až do Bakerových průlomů v 60-tých letech.

Příklad. Pellova rovnice

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

má nekonečně mnoho řešení: $(3+2\sqrt{2})^n = x_n + y_n\sqrt{2}$ dává řešení $(x_n, y_n)_{n\geq 1} = (3,2),\ (17,12),\ (99,70), \ldots$.

Věta (A. Thue, 1918). *Nechť* $a, b, \alpha, \beta, \gamma, n \in \mathbf{N}$, $n \geq 3$ *prvočíslo,* $a\alpha^n - b\beta^n = \gamma$,

$$(*)\ (4a\alpha^n)^{n-2} > \gamma^{2n-2} n^{n^2/(n-1)} (a\alpha^n / b\beta^n)^{2(n-1)^2/n}\ ,$$

$c > 0$, $r \in \mathbf{N}_0$ *splňují* $r \geq (\log c - \log K)/\log L$, *kde*

$$\begin{aligned} K &= \frac{n^{(n^2-4n+1)/(n-1)} b^{(n^2-n+1)/n} \beta^{(n-1)^2}}{2^{n+4} \gamma^{n-1} \alpha^{2n+1} a^{(n+1)/n}} \\ L &= LS/PS\ (\textit{v nerovnosti (*)}, > 1)\ . \end{aligned}$$

Potom každé řešení $p, q \in \mathbf{N}$ *nerovnosti* $|ap^n - bq^n| \leq c$ *splňuje*

$$p \leq \frac{nb\beta^{n-1}}{2\gamma} \left(\frac{4a\alpha^n}{\gamma^2 n^{n/(n-1)} (a\alpha^n / b\beta^n)^{(2n-2)/n}} \right)^r\ .$$

Smysl: má-li $f(x,y) = ax^n - by^n$ dosti malou hodnotu $f(\alpha,\beta) = \gamma$ splňující (*), lze efektivně odhadnout velikost všech řešení $x, y \in \mathbf{N}$ nerovnosti $|f(x,y)| \leq c$ a tedy efektivně vyřešit každou Thueho rovnici $f(x,y) = m$.

Důsledek. *Thueho věta třeba dává:* $x, y, c \in \mathbf{Z}$,

$$x^7 - 17y^7 = c \;\Rightarrow\; |x|, |y| \leq 693|c|^4 \,,$$

díky hodnotě $3^7 - 17 \cdot 2^7 = 11$.

Poznámky. V originálu je ve vzorci pro K chybně uvedena mocnina α^{2n}. Znehodnocuje to jeden z Thueho numerických příkladů a důkaz výsledku *S. Lubelskiho (1902–1941, zabit v Białystoku nebo KT Majdanek)* z r. 1935, že jediná řešení rovnice $x^4 - 15y^4 = 1$ jsou $\pm 1, 0$ a $\pm 2, \pm 1$, jenž se o Thueho větu opírá.

Thoralf Skolem (1887–1963): norský matematik. Nejprve asistentem fyzika *K. Birkelanda*, v Súdánu pozorovali zvířetníkové světlo. Ph.D. v r. 1926 pod vedením *A. Thueho*. Působil v Bergenu a na Univerzitě v Oslo. Algebra, teorie svazů, matematická logika, průkopník teorie modelů (Löwenheimova–Skolemova věta, Skolemův paradox), diofantické rovnice, p-adické metody.

Věta (T. Skolem, 1933; K. Mahler, 1935; C. Lech, 1953). *K buď těleso s $\mathrm{char}(K) = 0$ a $(a_1, a_2, \dots) \subset K$ buď lin. rekur. posloupnost: existují $c_1, \dots, c_k \in K$, že pro každé $n > k$ je $a_n = \sum_{i=1}^{k} c_i a_{n-i}$. Pak existuje modul $m \in \mathbf{N}$, že pro $i = 1, 2, \dots, m$ každá z m množin*

$$Z_i := \{n \in \mathbf{N}_0 \mid a_{i+mn} = 0_K\} = \mathbf{N}_0 \quad \textit{nebo je konečná .}$$

Důkaz. Pomocí p-adických čísel, dosud neefektivní. □

Poznámky. $(1,0,1,0,1,0,\dots) \subset \mathbf{Q}$ daná rekurencí $a_n = a_{n-2}$ má $m = 2$, $Z_1 = \emptyset$ a $Z_2 = \mathbf{N}_0$. SML věta popisuje řešení $n \in \mathbf{N}$ exponenciální diofantické rovnice

$$a_n = \sum_{j=1}^{r} p_j(n)\alpha_j^n = 0,\ p_j \in \overline{K}[x], \alpha_j \in \overline{K}\ .$$

(Fibonacciova čísla $(f_n) = (1,1,2,3,5,8,13,\dots)$ mají $f_n = a\alpha^n + b\beta^n$, $a,b,\alpha,\beta \in \overline{\mathbf{Q}}$, $x^2 - x - 1 = (x-\alpha)(x-\beta)$.)

Skolemův problém. *Je přítomnost* 0 *v lin. rekur. posloupnostech* $(a_n) \subset \mathbf{Z}$ *algoritmicky rozhodnutelná?*

Algoritmus znám pouze pro rekurence $a_n = \sum_{i=1}^{k} c_i a_{n-i}$, $c_i \in \mathbf{Z}$, řádu $k \leq 4$. Viz preprint *Halava et al.*, Skolems problem ..., 2005 (kde se mimo jiné předkládá algoritmus pro rekurence řádu $k = 5$, důkaz je ale chybný).

Carl Ludwig Siegel (1896–1981): německý matematik. Narodil se v Berlíně. Pacifista, během 1. sv. války v psych. léčebně. Ph.D. 1920 pod vedením *E. Landau*. 1940-51 IAS Princeton, od r. 1951 Göttingen. Matematická analýza, nebeská mechanika a teorie čísel (transcendence, L-funkce, $\zeta(s)$, diofantické rovnice).

Věta (C. L. Siegel, 1929). *C buď geometricky ireducibilní hladká afinní křivka, definovaná nad číselným tělesem K. Když $\mathrm{rod}(C) \geq 1$ nebo má C alespoň 3 body v ∞, pak má C jen konečně mnoho bodů s K-celými souřadnicemi.*

Důkaz je neefektivní. Jednodušší důkaz podali *P. Corvaja (1967)* a *U. Zannier (1957)* v r. 2002.

Věta (C. L. Siegel, 1937). *Nechť* $a, b, c, d, n \in \mathbf{N}$, $n \geq 3$, $\lambda_n = 4n^n \prod_{p \mid n} p^{n/(p-1)}$. *Pak*

$$(ab)^{n/2-1} \geq \lambda_n c^{2n-2} \;\Rightarrow\; ax^n - by^n = c$$

má nejvýše jedno řešení $x, y \in \mathbf{N}$.

Např. jediné celočíselné řešení rovnic $33x^7 - 32y^7 = 1$ i $33x^{11} - 32y^{11} = 1$ je $x = y = 1$.

Věta (C. L. Siegel, 1972). *Řešitelnost kvadratické diofantické rovnice*

$$F(x_1, x_2, \ldots, x_n) = 0$$

($F \in \mathbf{Z}[x_1, x_2, \ldots, x_n]$, $\deg F \leq 2$ *a* $x_i \in \mathbf{Z}$*) je algoritmicky rozhodnutelná.*

Alan Baker (1939): britský matematik, nar. v Londýně, FRS. Ph.D. v r. 1964 na Cambridgeské univerzitě pod vedením *H. Davenporta*. Fieldsova medaile v r. 1970 (efektivní výsledky v TČ). Prof. na Cambridgeské univerzitě. TČ (transcendence, diofantické rovnice).

Věta (A. Baker, 1964). $a, b, n \in \mathbf{N}$, $n \geq 3$, $7a/8 \leq b < a$, $n \mid a-b$, $\mu_n = \prod_{p \mid n} p^{1/(p-1)}$, $\lambda = 4b/\mu_n(a-b)^2 > 1$, $\kappa, c > 0$: $\lambda^\kappa = 2\mu_n(a+b)$ *a* $c = 1/2^{\kappa+3}(a+b)$. *Potom*

$$\left|p/q - (a/b)^{1/n}\right| > c/q^{1+\kappa}$$

pro každé $p, q \in \mathbf{N}$.

Např. $a = 128 = 2^7, b = 125 = 5^3$ a $n = 3$ dávají

Důsledek. $x, y, c \in \mathbf{Z}$,

$$x^3 - 2y^3 = c \Rightarrow |x|, |y| < (263000|c|)^{22} .$$

Věta (A. Baker, 1968). *Nechť* $\mu, \alpha_1, \alpha_2, \ldots, \alpha_n \in K$, *kde* K *je číselné těleso stupně* d, α_i *jsou vzájemně různé,* $n \geq 3$, $\mu \neq 0$ *a* $K = \mathbf{Q}(\alpha_1, \ldots, \alpha_n, \mu, \beta)$ *pro alg. číslo* β. *Pak pro* $x, y \in O_K$ *máme*

$$\prod_{i=1}^{n}(x - \alpha_i y) = \mu \;\Rightarrow\; h(x), h(y) < \exp\left((dH)^{(10d)^5}\right) \;.$$

Zde O_K *jsou* K*-celá čísla,* $h(x) = \max|$*konjugát* $x|$ *a* $H = \max|c|$, *kde* $c \in \mathbf{Z}$ *je koeficient definujících polynomů pro čísla* $\mu, \alpha_1, \ldots, \alpha_n, \beta$.

Důsledek. *Klasická Thueho rovnice* $F(x, y) = m$ *stupně* $d \geq 3$: *pro* $x, y \in \mathbf{Z}$ *máme*

$$F(x, y) = m \;\Rightarrow\; |x|, |y| < \exp\left((dH)^{(10d)^5}\right) \;,$$

kde H *je maximum abs. hodnoty koeficientu polynomu* $F(x, y) - m \in \mathbf{Z}[x, y]$.

Gerd Faltings (1954): německý matematik. Narozen v Gelsenkirchenu-Bueru (NSR). Ph.D. v r. 1978 na Univerzitě v Münsteru pod vedením *H.-J. Nastolda*. Fieldsova medaile v r. 1986 za důkaz Mordellovy domněnky. 1985–94 prof. na Princetonské univerzitě, od r. 1994 ředitel Ústavu Maxe Plancka pro matematiku v Bonnu. Aritmetická a algebraická geometrie.

Věta (G. Faltings, 1983). *Na geometricky ireducibilní hladké projektivní křivce rodu* ≥ 2*, definované nad číselným tělesem* K*, leží pouze konečně mnoho bodů se souřadnicemi v* K*.*

Důsledek. $x, y, z, n \in \mathbf{Z}$, $(x, y) = 1$, $n \geq 5$, $x^n + y^n = z^n \Rightarrow |x|, |y|, |z| < c$.

Původně domněnka *L. J. Mordella (1888–1972)* z r. 1922 pro případ $K = \mathbf{Q}$. Důkaz je neefektivní.

Další důkazy: *P. Vojta (1957)* (napsal prohlížeč xdvi) v r. 1991 a *E. Bombieri (1940)* též v r. 1991. Obdobu Mordellovy domněnky pro pole funkcí dokázal v r. 1965 *H. Grauert (1930–2011)*. Důkaz *Ju. Manina (1937)* z r. 1963 obsahoval mezeru, kterou odstranil *R. Coleman (1954–2014)* až v r. 1990.

Děkuji za pozornost!

(Za cenné poznámky během přednášky 3. března 2015 a po ní děkuji doc. A. Šolcové i dalším posluchačům.)