**1897 1. mezinárodní matematický kongres Curych**

6. 8. – 12. 8. 1900 2. kongres Paříž (226 účastníků – 90 Francie, 25 Německo, 17 USA, 15 Itálie atd.)

**Předseda H. Poincaré (1854 – 1912), čestný předseda Ch. Hermite (1822 – 1901).**

**6 sekcí:**
1. **Aritmetika a algebra (předseda D. Hilbert (1862 – 1943), tajemník É. Cartan (1869 – 1951))**
2. **Analýza (Paul Painlévé (1863 – 1933), J. Hadamard (1865 – 1963))**
3. **Geometrie (J. Darboux (1842 – 1917))**
4. **Mechanika a matematická fyzika**
5. **Historie matematiky**
6. **Výuka a metodologie matematiky**

**8. 8. 1900 Hilbertova přednáška Matematické problémy**

**„…Síla badatele se uplatňuje při řešení problémů: nachází nové metody, nová hlediska, objevuje širší a svobodnější horizonty.**
**… Zmiňme se ještě krátce o tom, které jsou všeobecné požadavky, které je právem třeba klást na řešení jakéhokoliv matematického problému. Především mám na mysli požadavek, abychom se mohli přesvědčit o správnosti odpovědi konečným počtem logických závěrů, a to na základě konečného počtu předpokladů, které vyplývají z podstaty úlohy a musí být v každém případě přesně formulovány.**
**… požadavek přesnosti, který se v matematice stal už pří-**

**slovečným, odpovídá obecné filozofické potřebě našeho rozumu.**
**… Tato podivuhodná skutečnost (spolu s jinými filozofickými důvody) nás vede k přesvědčení, které určitě sdílí každý matematik – které však nicméně až dosud nikdo nepotvrdil důkazem – k přesvědčení o tom, že každý matematický problém je možno tak či onak rozhodnout; buďto v tom smyslu, že bude ukázána nemožnost rozřešení problému a spolu s tím dokázána nutnost nezdaru všech pokusů o jeho řešení.**
**… Toto přesvědčení o rozhodnutelnosti každého matematického problému je pro nás silnou pobídkou v průběhu naší práce; slyšíme v sobě neustálé volání: Zde je problém, hledej řešení. Můžeš ho najít pomocí čistého myšlení, protože v matematice neexistuje (nepoznatelné) Ignorabimus.**

**Diofantická rovnice**

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

**kde P je polynom s celočíselnými koeficienty. Řešením této rovnice je každá n-tice celých čísel, která tento polynom anuluje.**

**Již EUKLEIDES (3. stol. př. Kr.) například našel všechna řešení rovnice**

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

**DIOFANTOS (3. stol.) řešil rovnice 2. stupně ve 2 proměnných.**

**Velká Fermatova věta.**

**1768 LAGRANGE (1736 – 1813): vyřešil obecně problém rovnic 2. stupně ve dvou proměnných.**

**HILBERT: Buď dána diofantická rovnice s libovolnými neznámými a s celočíselnými koeficienty. Je třeba najít metodu, která by umožnila po konečném počtu operací rozhodnout, má-li tato rovnice řešení v celých číslech.**

**1900 Alex THUE (1863 – 1922) Buď f(x) polynom s celočíselnými koeficienty, jehož všechny sčítance jsou stupně alespoň třetího a který není součinem dvou nebo více polynomů stupně alespoň prvního. Pak rovnice**

$$f(x,y) = c \text{ , } c \text{ celé}$$

**nemůže mít nekonečně mnoho celočíselných řešení.**

**Z jeho řešení však nebylo možno najít interval, v němž řešení leží, ani z něho neplynul algoritmus pro nalezení těchto řešení. Tento algoritmus nalezl v r. 1966 Alan BAKER (*1939).**

**1938 nalezl řešení jistého speciálního typu Thoralf Albert SKOLEM (1887 – 1963).Skolem**

**Až do vybudování teorie algoritmů byly hledány metody řešení alespoň jistých typů diofantických rovnic. Nepodařilo se však vyřešit ani nejjednodušší typ – rovnice ve dvou proměnných. (Rovnice s jednou proměnnou lze řešit snadno – plyne to z tzv. BEZOUTOVY věty – Etienne BEZOUT (1730 – 1783) .)**

**Polovina třicátých let – teorie algoritmů Alan Mattison TURING (1912 – 1954), Alonzo CHURCH (1903 -- 1995).**

**Podezření, že problém nemá řešení.**
**Poznámka: Můžeme se omezit na řešení v přirozených číslech – plyne z Lagrangeovy věty.**

**Hierarchie: funkce – vyčíslitelná funkce – efektivně vyčíslitelná funkce.**

**Formalizací vznikl pojem rekurzivní funkce.**

**Chceme popsat jistou třídu funkcí zobrazujících $(N_0)^k$ do $N_0$ .**
**Jisté „jednoduché“ funkce zvolíme za základní. Budou to všechny konstantní funkce (později uvidíme, že stačí vzít jen funkci nulovou).**
**Dále sem zařadíme funkci následovníka – tj. funkci**

$$S(x) = x+1$$

**a spočetnou množinu „projektivních“ funkcí**

$$I_{m,n}(x_1, x_2, \dots, x_n) = x_m .$$

**Rekurzivní funkce je nyní každá funkce, kterou z těchto základních funkcí obdržíme tím, že na ně konečně mnohokrát aplikujeme operátory substituce, primitivní rekurze nebo minimalizace.**

**Operátor substituce $S_{m,n}$ je definován takto:**

**jsou-li dány funkce**

$$h(x_1, \dots, x_m),\ g_1(x_1, \dots, x_n),\ \dots,\ g_m(x_1, \dots, x_n),$$

**pak**

$$S_{m,n}(h,g_1, \dots, g_m) = h[g_1(x_1, \dots, x_n), \dots, g_m(x_1, \dots, x_n)] = f(x_1, \dots, x_n) .$$

**Těchto operátorů je zřejmě spočetně mnoho.**

**Spočetně mnoho je i operátorů primitivní rekurze $R_n$ .**

**Mějme funkce**

$$g(x_1, \dots, x_n) \text{ a } h(x_1, \dots, x_n, x_{n+1}, x_{n+2}) .$$

**Pak**

$$R_n(g,h) = f(x_1, \dots, x_{n+1}),$$

**kde**

$$f(x_1, \dots, x_n, 0) = g(x_1, \dots, x_n)$$
$$f(x_1, \dots, x_n, y+1) = h[x_1, \dots, x_n, y, f(x_1, \dots, x_n, y)] .$$

**Operátor minimalizace umožňuje přecházet od již sestrojené funkce $f(x_1, \dots, x_{n+1})$ k funkci $g(x_1, \dots, x_n)$ takto:**

**Předpokládejme, že pro každou n-tici $[x_1, \dots, x_n]$ existuje alespoň jedno $x_{n+1}$ takové, že $f(x_1, \dots, x_n, x_{n+1}) = 0$ . Pak $g(x_1, \dots, x_n)$ je nejmenší $x_{n+1}$ takové, že $f(x_1, \dots, x_n, x_{n+1}) = 0$ .**

**Každá rekurzívní funkce je efektivně vyčíslitelná.**

**Předpoklad:**

**Churchova téze: Efektivně vyčíslitelné funkce jsou právě všechny rekurzivní funkce.**

**Množina A nezáporných celých čísel se nazývá rekurzivní, jestliže její charakteristická funkce je rekurzivní. Množina se nazývá rekurzivně spočetná, je-li oborem hodnot nějaké rekurzivní funkce.**

**Věta: rekurzivní $\Rightarrow$ rekurzivně spočetná**

**Věta: Hromadný rozhodovací problém pro množinu A nezáporných celých čísel je algoritmicky řešitelný právě tehdy, když je A rekurzivní.**

**Příklady:**

- **je-li A množina všech prvočísel, je problém algoritmicky řešitelný**
- **rozhodnout, zda je formule výrokového kalkulu dokazatelná je algoritmicky řešitelné**
- **totéž pro formule predikátového kalkulu není algoritmicky řešitelné**

**Formulace Hilbertova problému: Existuje algoritmus, který by pro každou diofantickou rovnici rozhodl, zda má řešení?**

**Množina přirozených čísel se nazývá diofantická, jestliže její prvky jsou právě všechna řešení nějaké diofantické rovnice $P(y, u_1, \dots, u_m) = 0$ .**
**Například množina {0, 1, 4, 9, 16, …} je diofantická; příslušný polynom je $P(y, u) = y - u^2$ .**

**Věta: Aby byl 10. problém algoritmicky řešitelný, musí být každá diofantická množina rekurzivní.**

**Je tedy nutno dokázat toto tvrzení nebo najít alespoň jednu diofantickou množinu, která není rekurzivní.**

**Zobecnění diofantické množiny:**
**Množina $A \subseteq N^n$ je diofantická, jestliže existuje nějaká diofantická rovnice taková, že**

$$\left[y_1,\cdots,y_n\right]\in A \;\Leftrightarrow\; \left(\exists u_1,\cdots,u_m\right) P\left(y_1,\cdots,y_n,u_1,\cdots,u_m\right)=0.$$

**Příklady diofantických množin:**

**{[x, y, z]; z = x + y}, {[x, y, z]; z = xy} .**

**V další historii sehrála důležitou roli otázka:**

**Je množina $E = \{[x, y, z]; z = x^y\}$ diofantická?**

**Terminologie: například ternární predikát z = x + y je pravdivý například pro trojice [3, 2, 5] a [8, 6, 14] a nepravdivý například pro trojici [1,1,1].**

**n-ární predikát $\tau(y_1, \dots, y_n)$ se nazývá diofantický, je-li množina**

$$\{[y_1, \dots, y_n]; \tau(y_1, \dots, y_n) \text{ je pravdivý}\}$$

**diofantická.**

**Příklady diofantických predikátů:**
**$\mu_1(x, y, z)$: $z = x^2 + y^2$ , $\mu_2(x, y)$: $x < y$ , $\mu_3(x, y)$: $x \leq y$ .**

**Binární predikát $\mu(x, y)$ se nazývá predikát exponenciálního růstu, jestliže z pravdivosti $\mu(x, y)$ vyplývá $y \leq x^x$ a přitom pro každé přirozené k existují čísla x,y taková, že $1 \leq x$ , $\mu(x, y)$ je pravdivý a $x^k < y$ .**

**Problém: existuje takový predikát?**

**1952 Julia Robinsonová: Pokud existuje alespoň jeden diofantický predikát exponenciálního růstu, je výše uvedená množina E diofantická.**

**1933**

**1941**

**1985**

**1961 Robinsonová, M. Davis, H. Putnam: Pokud je E diofantická, je každá rekurzivně spočetná množina diofantická.**

**Víme však, že existují rekurzivně spočetné množiny, které nejsou rekurzivní. Dokáže-li se tedy, že E je diofantická, existují diofantické množiny, které nejsou rekurzivní, takže 10. Hilbertův problém není řešitelný.**

**Podle Robinsonové však k tomu stačí najít alespoň jeden diofantický predikát exponenciálního růstu.**

**1970 J. V. MATIJASEVIČ: takový predikát existuje!**

**Označme $F_n$ n-té Fibonacciho číslo.**

$$\Phi(u,v): v = F_{2u} .$$

**$\Phi(u,v)$ je pravdivý pro dvojice (0, 0), (1, 1), (2, 3), (3, 8), (4,21), (5, 55), … .**

**Z vlastností Fibonacciho čísel poměrně snadno plyne, že $\Phi(u,v)$ je predikát exponenciálního růstu. Je však třeba ještě dokázat, že je diofantický.**

**Věta: $v = F_{2u}$ právě tehdy, když existují přirozená čísla $g, h, k, m, n, x, y, z$ taková, že platí následující vztahy:**

1. $u \leq v < m$
2. $m^2 - mz - z^2 = 1$
3. $g^2 - gh - h^2 = 1$
4. $m^2 \mid g$
5. $m \mid (n - 2)$
6. $(2h + g) \mid (n - 3)$
7. $x^2 - nxy + y^2 = 1$
8. $m \mid (x - u)$
9. $(2h + g) \mid (x - y)$

**Důsledek: $\Phi(u,v)$ je diofantický.**

## DODATEK

**1960 H. PUTNAM: Existuje takový polynom $Q(y_1, \ldots, y_k, z)$ pátého stupně s celočíselnými koeficienty, že každou rekurzivně spočetnou množinu M přirozených čísel lze získat jako množinu nezáporných hodnot polynomu**

**$Q(y_1, \ldots, y_k, a_M)$ , kde $a_M$ je konstanta, kterou lze efektivně vypočítat na základě znalosti rekurzivní funkce f takové, že $M = \{f(x); x \in N_0\}$ .**

**Důsledek: existuje polynom 5. stupně takový, že například všechna prvočísla jsou jeho nezápornými hodnotami.**

**Velká Fermatova věta.**

# Albert Thoralf Skolem

**Born: 23 May 1887 in Sandsvaer, Norway**
**Died: 23 March 1963 in Oslo, Norway**

Click the picture above
to see a larger version

Previous (Chronologically) Next Biographies Index

Previous (Alphabetically) Next Main index

**Thoralf Skolem** worked on Diophantine equations, mathematical logic, group theory, lattice theory and set theory. In 1912 he produced a description of a free distributive lattice. He made refinements to Zermelo's axiomatic set theory, publishing work in 1922 and 1929.

Skolem extended work by Löwenheim (1915) to give the Löwenheim- Skolem theorem, which states that if a theory has a model then it has a countable model. From 1933 he did pioneering work in metalogic and constructed a nonstandard model of arithmetic.

He also developed the theory of recursive functions as a means of avoiding the so-called paradoxes of the infinite.

**Article by:** *J J O'Connor* and *E F Robertson*

**Click on this link to see a list of the Glossary entries for this page**

**List of References** (6 books/articles)

**Mathematicians born in the same country**

**Other Web sites**

1. Nordic Journal of Philosophical Logic

Previous (Chronologically) Next Biographies Index

Previous (Alphabetically) Next Main index
History Topics Societies, honours, etc. Famous curves
Time lines Birthplace maps Chronology Search Form
Glossary index Quotations index Poster index
Mathematicians of the day Anniversaries for the year

---

JOC/EFR December 1996 School of Mathematics and Statistics
University of St Andrews, Scotland