# Matematika v 20. a 21. století

Evropský sociální fond
Investujeme do vaší budoucnosti

Alena Šolcová
FIT ČVUT v Praze
2014

OPP A
PRA HA
PRA GUE
PRA GA
PRA G
EVROPSKÁ UNIE

# Poznámky k matematice 19. století

- 1812 – 1821 - Gauss, Bolzano, Cauchy – základy teorie konvergence řad
- 1812 – Pierre S. Laplace, 1827 – Simon Poisson – důkazy prvních limitních vět v teorii pravděpodobnosti
- 1820 – 1824 – Ch. Babbage – práce na počítacím stroji – funkcionální rovnice
- 1816 – W. Bessel – Besselovy funkce
- 1828 – August F. Moebius – *„Barycentrický kalkul“*
- 1828 – Niels Abel - Abelovo kriterium pro konvergenci řady, řešení rovnice 5. stupně
- 1830 – 1832 – Galois – teorie grup
- 1832 – Janos Bolyai – neekleidovská geometrie *„Appendix“*
- 1833 – 1834 – W. R. Hamilton – rozvoj variačního počtu, kvaterniony
- 1844 – Grassmann – *„Ausdehnugslehre“* – lineární algebra

# Poznámky k matematice 19. století - 2

- 1858 – Arthur Cayley – teorie matic
- 1869 – Karl Weierstrass – teorie funkcí komplexní proměnné
- 1872 – Sophus Lie - Lieovy grupy – spojitost a algebra
- 1873 – Charles Hermite – transcendentnost čísla e
- 1874 – Georg Cantor – nespočetnost množiny reálných čísel
- 1883 – 1887 – Georg Cantor – vznik teorie množin
- 1890 – Giusseppe Peano – axiomy přirozených čísel
- 1899 – David Hilbert *„Základy geometrie“*, souvislost mezi algebrou a geometrii

# David Hilbert a problémy pro 20. století

- Paříž, Sorbona - 8. srpna roku 1900
  2. mezinárodní kongres matematiků

➢ David Hilbert, profesor univerzity v Göttingen, formuloval 23 problémů pro 20. století

- 1902 – Úplný seznam 23 problémů zveřejněn v článku v Bulletinu Americké matematické společnosti.

Poznámka: 1. matematický kongres se konal v roce 1893 v Zürichu.

# Od hypotézy kontinua

1. Hypotéza kontinua – problém řešen do r. 1963

Hilbert v r. 1900 rozdělil problém na dvě otázky:

a) Existuje transfinitní číslo*) mezi spočetnou množinou a kontinuem?

b) Může být číselné kontinuum dobře uspořádanou množinou?

Axiom výběru – Ernst Zermelo (1871–1956)

Nezávislost axiomu výběru na teorii množin – Paul Cohen

2. Bezespornost axiomů aritmetiky – Kurt Gödel – Bez aritmetiky nelze dokázat bezespornost jiných teorií.

*) přesněji: transfinitní kardinál

# Další Hilbertovy problémy

8. Riemannova hypotéza – Dosud nevyřešena.
10. Najděte algoritmus k určení, zda daná polynomická rovnice s celými koeficienty má celočíselné řešení.

    Vyřešen 1970. – Matijasevičova věta – Takový algoritmus neexistuje.
18. Keplerova hypotéza o uspořádání koulí a jejich hustotě – 1998, Thomas Hales – 74%

    Počítačová podpora.
23. Další vývoj variačního počtu – Zatím stále otevřené téma.

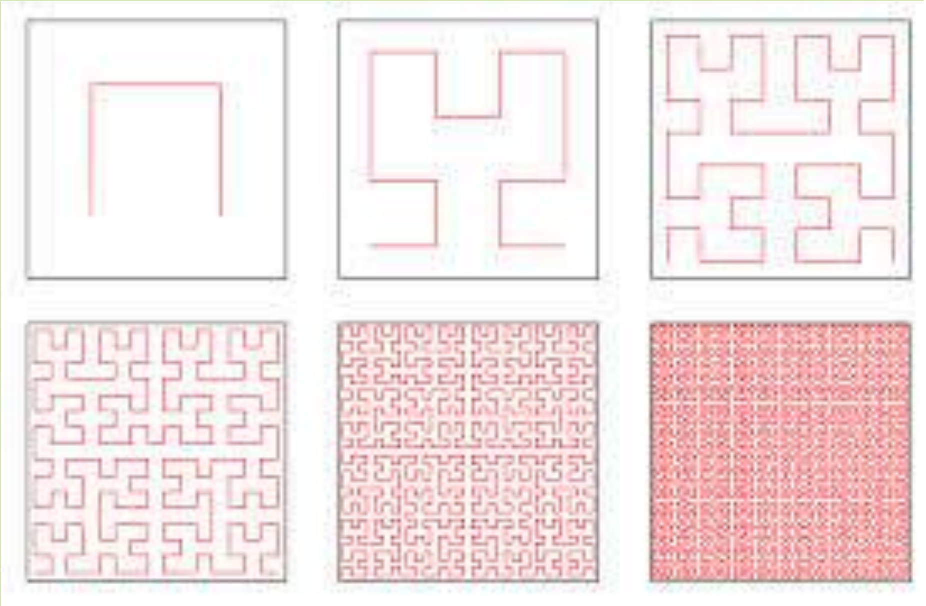
# Hilbertovy Základy geometrie

- 1899 – Grundlagen der Geometrie – přeloženy do mnoha jazyků.
- Hilbert jako zakladatel axiomatické školy měl vliv na formalizaci algebry a analýzy.
- Zajímal se o všechny aspekty čisté matematiky:

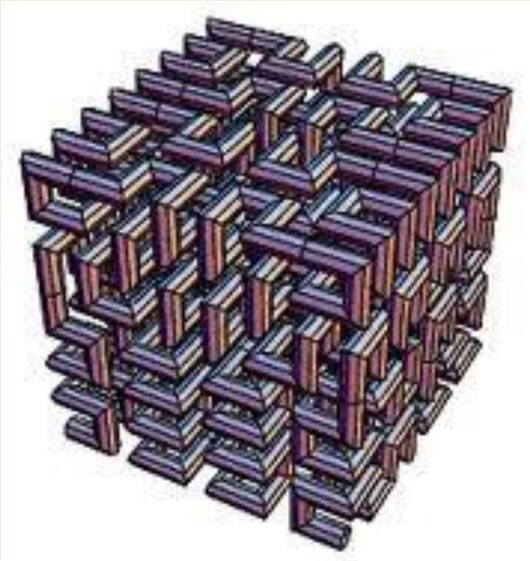
  např. zavedl pojem prostoru – Hilbertova, později Banachův prostor … nebo se zabýval vyplňováním prostoru křivkami … etc.

# Vyplňování prostoru křivkami

- Hilbertova křivka – 1891

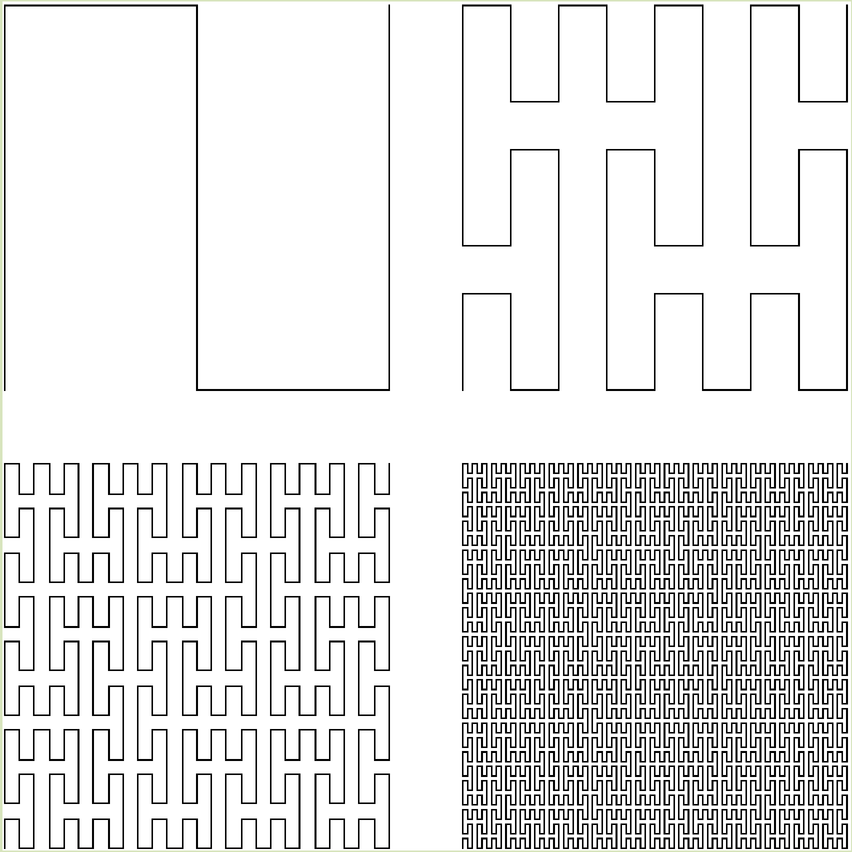


Hilbertova křivka ve 3D



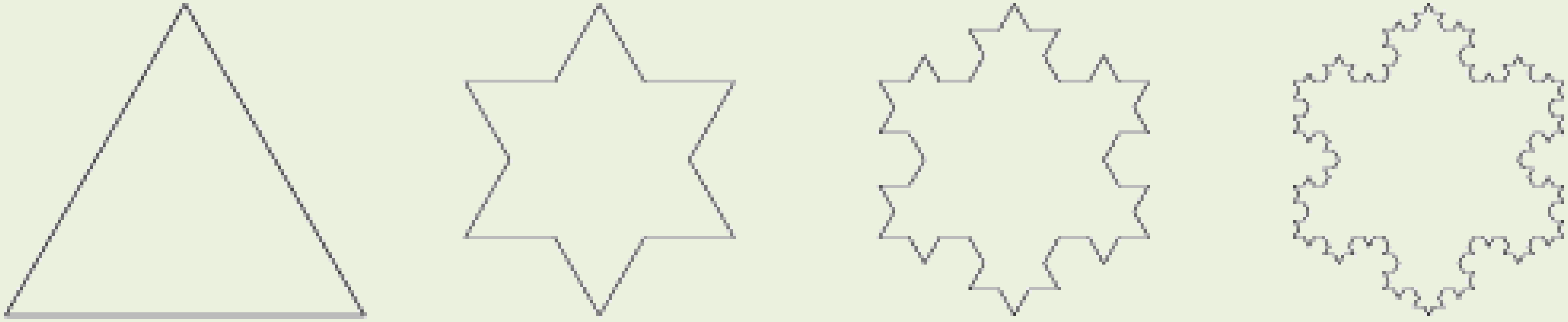
# Giusseppe Peano

- Peanova křivka – první varianta

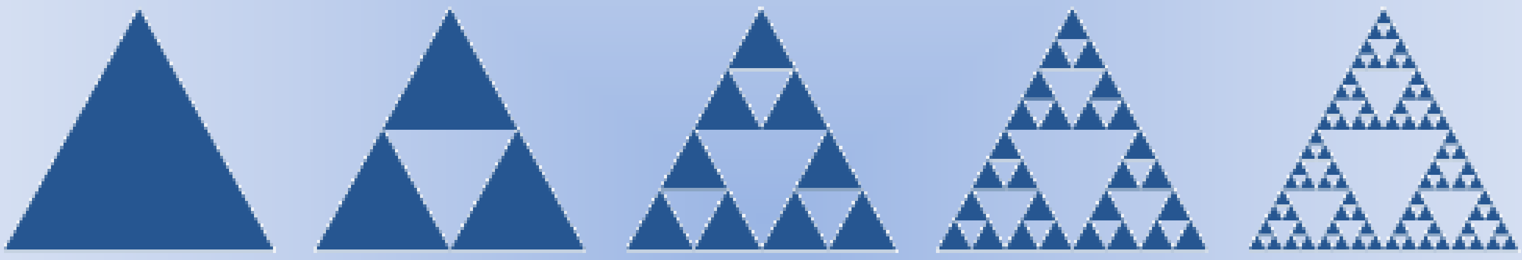


# Kochova křivka

- Helge von Koch (1870 – 1924), profesor ve Stockholmu v roce 1904:
- Navrhl křivku založenou na rovnostranném trojúhelníku a třetění jeho stran:



# Sierpińskiho síto



Wacław Franciszek Sierpiński (1882 – 1969),
polský matematik,
věnoval se teorii čísel, teorii množin a topologii.

# Nové definice integrálu

- Archimedés, Kepler, Newton, Leibniz, Riemann.

- Henri Lebesgue, 1904 – Základní integrál pro řešení diferenciálních rovnic (umí přeskočit singularity).

  Riemannův integrál „naležato“

  Nejdříve se definují integrály po částech konstantních funkcí, tzv. jednoduchých. Integrál pak je limita posloupnosti integrálů konvergujících jednoduchých funkcí.

  Funkce i množiny jsou tzv. měřitelné a neměřitelné.

  Lebesgueův integrál je def. pouze pro měřitelné.

  Jiná definice L-int. vychází ze zavedení míry množiny.

  Integrál Dirichletovy funkce existuje a je roven nule.
- Oskar Perron, 1912 – nový typ integrálu, komplikovaný
- Jaroslav Kurzweil 1957 – integrál neabsolutně konvergentní. Kurzweil našel velmi elegantní definici. Teorii K-int. rozpracoval Ralph Henstock. Později dokázáno, že je ekvivalentní Perronovu integrálu.
- atd.

# Co je matematika?

- Ve 20. století se změnil pohled na to, co je matematika?
  - Je to aritmetika? Věda spojená s čísly?
  - Věda o strukturách?
  - Obor, který pomocí výpočtů nebo manipulací se symboly řeší nějaké problémy?

    Takto vnímali svůj obor před 150 lety samotní matematikové.
- Již v polovině 19. století došlo ke změně, přímo revoluční:

# Co je matematika? - 2

- Göttingen:

  Bernhard Riemann, Pierre Lejeune Dirichlet, Richard Dedekind
- Podle jejich představy v matematice nejde o provádění výpočtů a hledání odpovědí,

  ale o formulace a porozumění abstraktním koncepcím a vztahům.

  Nalezli odpověď na to:

  „Co je jádrem oboru a co patří mezi pomocné dovednosti?“

  Důraz je přesunut z provádění na porozumění!
- Chybná interpretace „Hnutí za novou matematiku“ v 60. letech 20. století ve školách.

  („Zapomeňte na počítání a soustřeďte pouze na koncepci.“ Po několika letech tyto myšlenky ve školních osnovách opuštěny.)

# Dirichlet

- *„Myslet koncepčně!“* (*„Denken in Begriffen!“*)

  motto mladé generace matematiků

- Matematické pojmy již nebyly považovány za cosi daného formulemi, ale za nosiče koncepčních vlastností.
- Důkaz se stal procesem koncepční logické dedukce, nebyla to jen manipulace s pojmy v rámci daných pravidel.

# Pojem funkce podle Dirichleta

- Před Dirichletem: vzorec $y = x^2 + 3x - 5$ je předpis, jak získat z daného čísla $x$ nové číslo $y$.
- Dirichlet:

*„Zapomeňme na vzorec a soustřeďme se na funkci samotnou.“*

- *Funkce je cokoli, co přiřadí danému číslu číslo nové. K jejímu popisu není třeba matematické formule. Ani se nemusíme omezovat na čísla.* (Též pojem „zobrazení“.)

  *Funkcí může být jakýkoli předpis, který uvažuje objekty určitého typu a přiřazuje jim objekty obecně jiného typu.*

- Př. Pravidlo, které přiřadí každému státu hlavní město.

# Vlastnosti abstraktních funkcí

- Př. Funkce je prostá, sudá, lichá, … další vlastnosti
- Je $y = x^2$ prostá? Je y = sin *x* sudá funkce?

- „Epsílon–delta gymnastika“

  August Cauchy, Karl Weierstrass

- Riemann definoval komplexní funkci pomocí jejích diferenciálních vlastností

➢ 1859 – Riemann: *O počtu prvočísel ležících pod danou hodnotou* – snaha porozumět struktuře prvočísel.

# Riemannův dopis Weierstrassovi

O Riemannově hypotéze:

„Jistě by bylo žádoucí získat precizní důkaz toho tvrzení;

po několika zběžných marných pokusech to ale zatím dávám stranou, protože se zdá, že můj další výzkum se bez toho obejde."

# Vlastnosti prvočísel

- Kolik je prvočísel? Eukleidés …
- Jaká je jejich hustota?

Prvočíselná věta

$D_N = P(N)/N \quad = 1/\ln(N)$

Gauss - hypotéza
Hadamard – důkaz 1896
Vallée de Poussin

| $N$ | 10 | 100 | 1000 | 10000 | 100000 | 1000000 |
|---|---|---|---|---|---|---|
| $D_N$ | 0,5 | 0,24 | 0,168 | 0,123 | 0,096 | 0,078 |

- Problém prvočíselných dvojčat?

  Zda existuje nekonečně mnoho prvočíselných dvojic lišících se o dvě: 11 a 13, 17 a 19, …. V 21. století se hledají mezi čísly s více než 50 000 ciframi.

- Goldbachova domněnka? 1742 – Každé sudé číslo větší než 2 je součtem právě dvou prvočísel. Potvrzeno do $2x\ 10^{17}$ v roce 2004. Stále otevřený problém.

# Problémy pro 21. století

Clayův matematický institut / 24. května 2000

– Millenium Prize Problems – $ 1 000 000

1. P versus NP - rychlost algoritmů

   polynomiální - nedeterministicky polynomiální časová složitost algoritmů

2. Hodgeova domněnka
3. Poincaréova hypotéza (dokázána – Grigorij Perelman)
4. Riemannova hypotéza – kořeny funkce „dzéta“ a rozložení prvočísel
5. Yang-Millsova teorie a hypotéza hmotnostních rozdílů
6. Navier-Stokesovy rovnice – existence řešení
7. Birchova a Swinerton-Dyerova domněnka – Kdy rovnice nemá řešení?

# P versus NP - rychlost algoritmů

- Jak efektivně mohou počítat počítače?
- polynomiální - nedeterministicky polynomiální časová složitost algoritmů
- Stephen Cook (*1939) testoval Goldbachovu domněnku, přestal studovat elektroinženýrství v Michiganu.
  Přestoupil na studium matematiky (informatika ještě nebyla samostatná disciplína).
  Chtěl studovat algebru.
  Ocitl se na Harvardově univerzitě pod vlivem logika Wanga a seznámil se s prací Michaela Rabina o teorii složitosti.

# Stephen Cook

- Harvard – Berkeley, Kalifornie 4 roky – dodnes Toronto

*The Complexity of Theorem Proving Procedures*

(*Složitost procedur pro dokazování vět*)

Zavedl novou koncepci NP úplnost,
mocný nástroj pro analýzu výpočetních úloh

*„NP úplnost se mi jevila jako zajímavý nápad, ale neuvědomil jsem si její možný dopad.“*

Aplikace - Problém obchodního cestujícího

# Problém obchodního cestujícího (POC)

- 1930 – poprvé uvedl Karl Menger ve Vídni
- Vedl ke studiu obecných počítačových metod.
- POC  je počítačová úloha k nalezení optimální trasy.
- Teoretikové se však zabývají otázkou: S jakou efektivitou může počítač daný úkol vyřešit?
- Funkce časové složitosti: lineární, kvadratická, exponenciální …
- V 60. letech zavedena klasifikace NP. Nikdo zatím nedokázal, že třídy problémů P a NP splývají, ani že jde o různé třídy.
- Podle Cooka, 1971:

  NP problém je NP úplný, jestliže by objev polynomiální procedury vedoucí k jeho řešení znamenal, že kterýkoli jiný NP problém může být řešen polynomiálně.

# Birchova a Swinnerton-Dyerova domněnka

- Týká se matematických objektů – eliptické křivky, název eliptický je odvozen od toho, že se s nimi počítá při výpočtu obvodu elipsy.

$$y^2 = x^3 - ax + b$$

- Nalezení racionálních bodů jistých eliptických křivek a jejich počet.
- Henri Poincaré v roce 1901:

  Každé eliptické křivce můžeme přiřadit jistou grupu.

# Hodgeova domněnka

Každá harmonická diferenciální forma (jistého typu) nesingulární projektivní algebraické variety je racionální kombinací kohomologických tříd algebraických cyklů.

- Ukázka toho, že podstata moderní matematiky nedovoluje laikovi, aby ji náležitě ocenil.
- 1950 Mezinárodní matematický kongres v Cambridge

William Hodge (1903 – 1975) zabýval se teorií harmonických integrálů.

Založil Mezinárodní matematickou unii.

# Riemannova hypotéza

- Funkce $\zeta$ – „dzéta“
  $\zeta(s) = 1/1^s + 1/2^s + 1/3^s + 1/4^s + 1/5^s + \dots$ .

- Euler dokázal pro hodnotu 2: $\zeta(2) = \pi^2/6$,
  možnost výpočtu čísla π.

- Euler dokázal $\zeta(s) = \Pi\,[1/(1 - 1/p^s)]$
  pro libovolné *s* a přes všechna prvočísla *p*.
  Π – nekonečný součin
- Riemann:
  Hledal souvislost mezi komplexními kořeny funkce ζ -„dzéta“
  ve tvaru (½ + *b*i)
  a rozložením prvočísel.

# Riemannova hypotéza

- Kořeny Riemannovy fce: ζ (*n*) = 0 pro všechna záporná sudá celá čísla *n*.

Všechna ostatní komplexní čísla *z*,
splňující podmínku ζ(*z*) = 0,
kterých je nekonečně mnoho,
leží na kritické přímce Re (*z*) = ½.

- Důkaz - důsledky v bezpečnosti internetu, bankovní transakce apod.
- Většina matematiků věří, že Riemannova hypotéza platí.
- Souvislost matematiky s kvantovou fyzikou
  - Alain Connes.

# Umělá inteligence UI

- Artificial Intelligence AI – součást informatiky, která se zabývá tvorbou strojů majících rysy inteligentního chování
- Inteligence je shromažďování informací a jejich vyhodnocování – simulace učení strojem.
- 1955 – Předpověď rozvoje UI pro rok 1970:

Počítač bude

1. velmistrem v šachu.
2. Odhalí nová matematická tvrzení.
3. Porozumí přirozenému jazyku a bude schopen překládat.
4. Bude schopen komponovat hudbu na úrovni klasiků.

Některé z těchto představ se nenaplnily.

Alan Turing – řešil otázku, jak posuzovat inteligentní projevy stroje – 1950.

*Computing machinery and Inteligence*

# Různé přístupy k UI

- Neuronové sítě
- Genetické programování
- Expertní systémy
- Prohledávání stavového prostoru
- Dobývání znalostí
- Strojové učení

Matematika v GPS

Aplikace lineární algebry, statistiky, teorie grafů, kosmické geodézie atd.