Od prvočísel po Riemannovu hypotézu

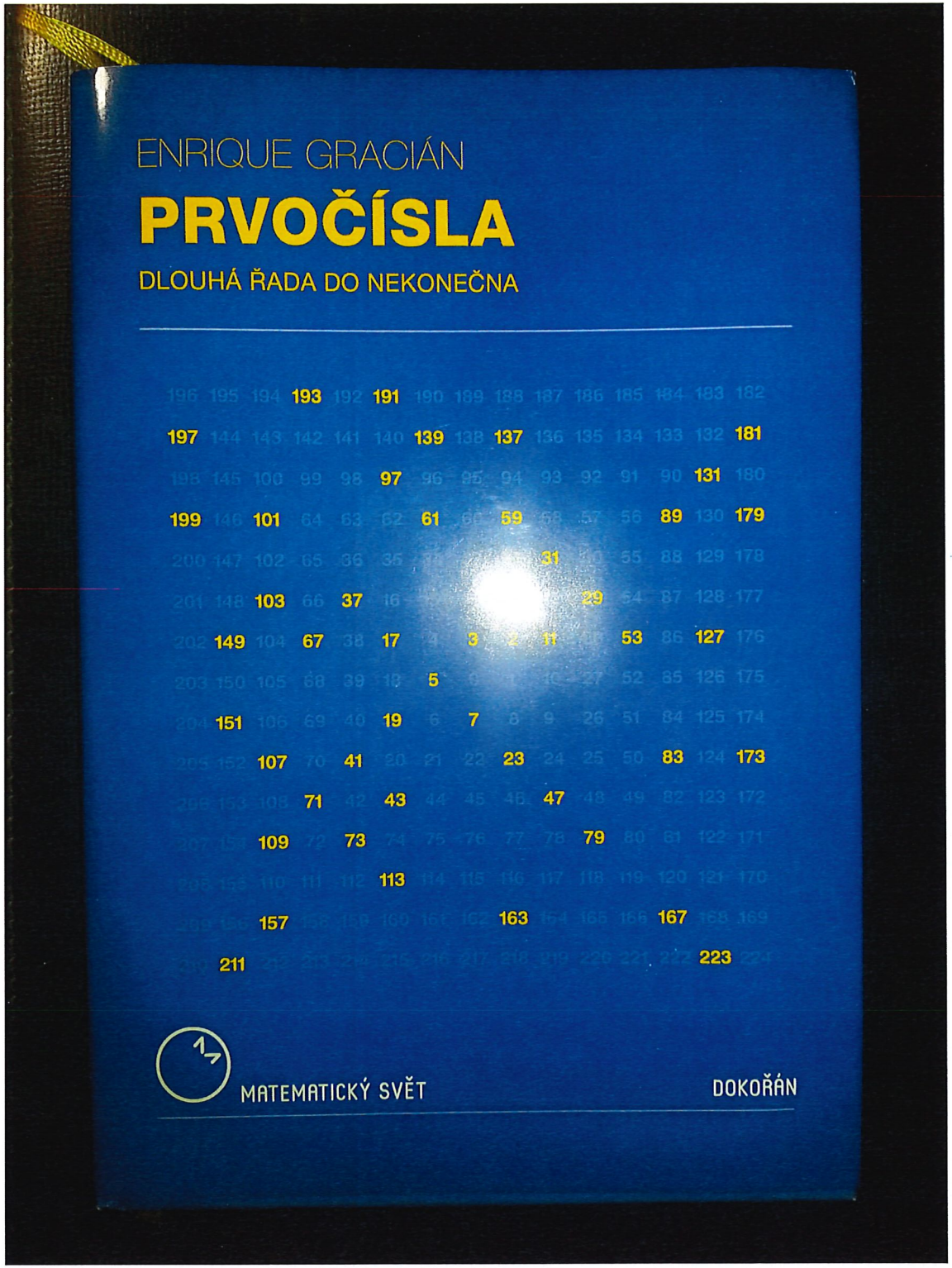
Pavel Drábek

katedra matematiky FAV ZČU

MOTTO (E. GRACIÁN: Prvočísla, dlouhá řada do nekonečna)

Prvočísla jsou nevychovaná banda: objevují se, kdy je napadne, bez předchozího varování, zjevně chaoticky, aniž by vyhovovala jakékoli zákonitosti.

Nejhorší je, že je nemůžeme ignorovat - jsou nepostradatelná pro aritmetiku a pro matematiku obecně.


ENRIQUE GRACIÁN
PRVOČÍSLA
DLOUHÁ ŘADA DO NEKONEČNA
MATEMATICKÝ SVĚT
DOKOŘÁN

Základní věta aritmetiky:

"Každé přirozené číslo větší než 1 lze vyjádřit jednoznačně jako součin prvočísel."

Například $24 = 2.2.2.3 = 2^3.3$

Interpretace:

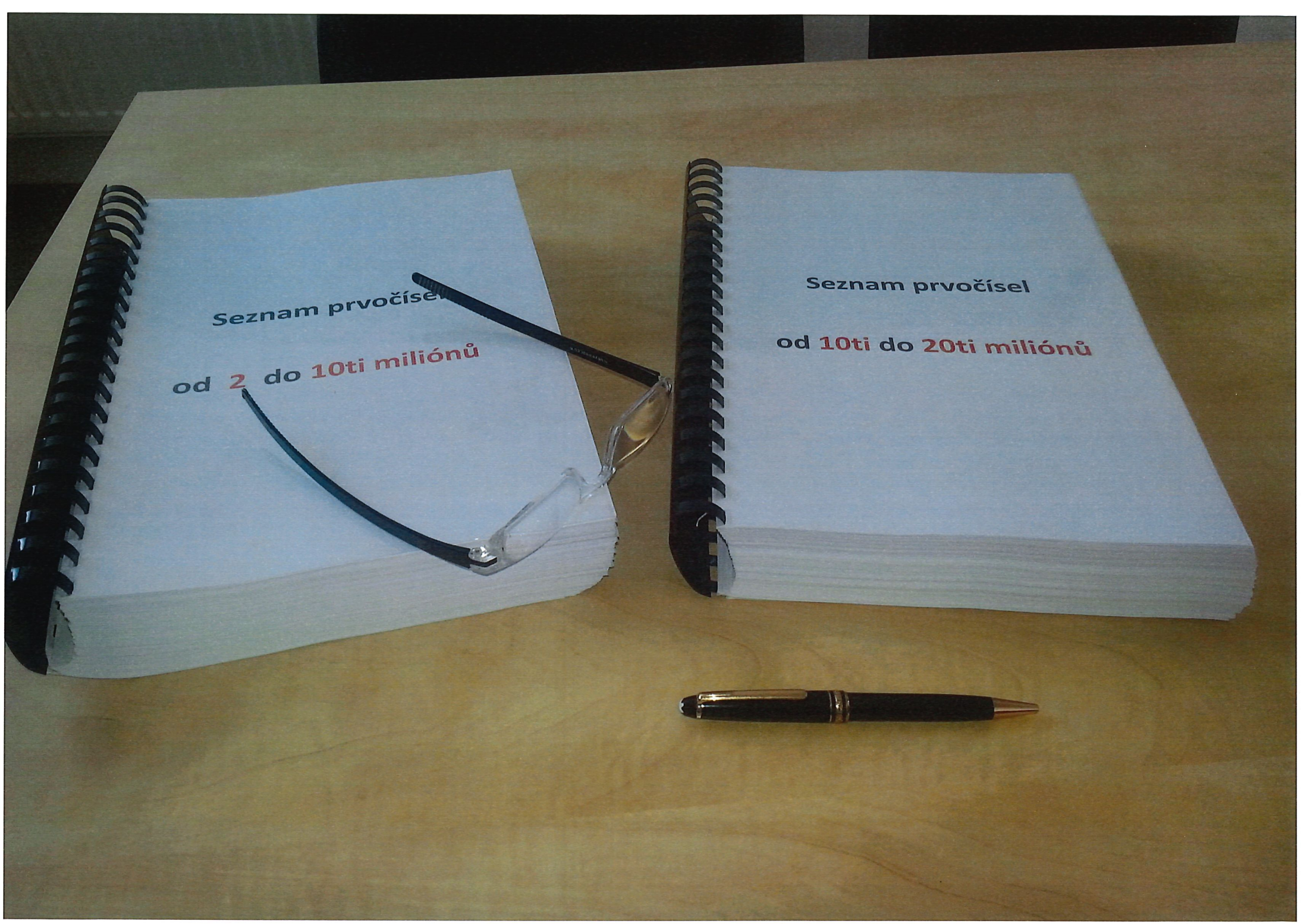
- DNA čísla 24 tvoří posloupnost genů 2^3 a 3
- 2 a 3 jsou atomy, které tvoří molekulu 24

Je jich nekonečně mnoho (Eukleides, asi 325–260)

Sporem: $p_1, p_2, \dots, p_n$ všechna prvočísla

$\forall i = 1, \dots, n \quad p_1 p_2 \cdots p_n + 1 > p_i$

$\left.\begin{array}{l} \exists j \in \{1, \dots, n\} \quad p_j \mid p_1 p_2 \cdots p_n + 1 \\ \text{zároveň } p_j \mid p_1 p_2 \cdots p_n \end{array}\right\} \Rightarrow p_j \mid 1$ ↯


Seznam prvočísel
od 2 do 10ti miliónů
Seznam prvočísel
od 10ti do 20ti miliónů

Mezery mezi prvočísly "jakkoli dlouhé"

$1 \times 2 \times 3 \times 4 \times 5 \oplus 2 = 122$ dělitelné 2

$1 \times 2 \times 3 \times 4 \times 5 \oplus 3 = 123$ 3

$1 \times 2 \times 3 \times 4 \times 5 \oplus 4 = 124$ 4

$1 \times 2 \times 3 \times 4 \times 5 \oplus 5 = 125$ 5

$\underbrace{5!+2, 5!+3, 5!+4, 5!+5}_{4 \text{ čísla}}$ nejsou prvočísla

$\underbrace{101!+2, 101!+3, \ldots, 101!+101}_{100 \text{ čísel}}$ — " —

$\underbrace{(n+1)!+2, (n+1)!+3, \ldots, (n+1)!+n+1}_{n \text{ čísel}}$ — " —

Joseph Louis Francois Bertrand (1822–1900)

Bertrandův postulát:

$$\forall n \geq 1 \quad \exists p \text{ (prvočíslo)} : \quad n < p \leq 2n$$

Joseph Bertrand	1845	ověřil platnost	$\forall n < 3\,000\,000$
Pafnuty Chebyshev (1821–1894)	1850	1. známý důkaz	
.....			
Srinivasa Ramanujan (1887–1920)			
.....			
Paul Erdös (1913–1996)	1932	(jako 1. článek v 19ti letech)	

Prvočíselná dvojčata

oddělená pouze jedním sudým číslem (které je vždy dělitelné 3)

V první stovce čísel nalezneme následující páry prvočísel, mezi nimiž leží pouze jedno číslo:

$(3,5)$, $(5,7)$, $(11,13)$, $(17,19)$, $(29,31)$, $(41,43)$, $(59,61)$ a $(71,73)$.

Tyto dvojice se nazývají „prvočíselná dvojčata“ nebo prostě jen „dvojčata“. Dvojčata mohou být popsána předpisem $(p, p+2)$, kde p je prvočíslo. Seznam všech prvočíselných dvojčat v první tisícovce čísel vypadá následovně:

$(3,5)$,	$(5,7)$,	$(11,13)$,	$(17,19)$,	$(29,31)$,
$(41,43)$,	$(59,61)$,	$(71,73)$,	$(101,103)$,	$(107,109)$,
$(137,139)$,	$(149,151)$,	$(179,181)$,	$(191,193)$,	$(197,199)$,
$(227,229)$,	$(239,241)$,	$(269,271)$,	$(281,283)$,	$(311,313)$,
$(347,349)$,	$(419,421)$,	$(431,433)$,	$(461,463)$,	$(521,523)$,
$(569,571)$,	$(599,601)$,	$(617,619)$,	$(641,643)$,	$(659,661)$,
$(809,811)$,	$(821,823)$,	$(827,829)$,	$(857,859)$,	$(881,883)$.

Největší známá dvojčata (objevená v roce 2016) jsou tvořena čísly

$2\,996\,863\,034\,895 \times 2^{1\,290\,000} - 1$ a $2\,996\,863\,034\,895 \times 2^{1\,290\,000} + 1$,

která mají 388 342 číslic!

Hypotéza o prvočíselných dvojčatech

Je jich nekonečně mnoho?

Alphonse de Polignac (1817-1890)

1849: $\forall$ celé číslo C existuje nekonečně mnoho párů prvočísel, která jsou od sebe oddělena $2C-1$ složenými čísly

($C = 1 \rightarrow$ hypotéza o prvočíselných dvojčatech)

Viggo Brun 1919 :

(1885 – 1978)

$$\sum_{p;\,p+2\in\mathbb{P}} \left(\frac{1}{p}+\frac{1}{p+2}\right) = \left(\frac{1}{3}+\frac{1}{5}\right)+\left(\frac{1}{5}+\frac{1}{7}\right)+$$

$$+\left(\frac{1}{11}+\frac{1}{13}\right)+\ldots = B_2$$

Brunova konstanta

Crandall, Pomerance : $B_2 \in (1.83,\ 2.347)$

! $\sum_{p\in\mathbb{P}} \frac{1}{p} = +\infty$

Edmund Landau (1877 – 1938)

Mezinárodní kongres matematiků 1912

1. Goldbachova hypotéza.

   Každé sudé číslo větší než 2 lze vyjádřit jako součet dvou prvočísel.

2. Hypotéza o prvočíselných dvojčatech.

3. Legendrova hypotéza.

   $\forall n \in \mathbb{N} \; \exists p \text{ (prvočíslo)} : n^2 < p < (n+1)^2$

4. $\exists$ nekonečně mnoho prvočísel p tvaru $p = n^2 + 1$ pro nějaké $n \in \mathbb{N}$.

Christian Goldbach (1690-1764)

18.11.1752 dopis Eulerovi (1707-1783)

$4 = 2+2,\ 6 = 3+3,\ 8 = 3+5,\ 10 = 3+7,$

$12 = 5+7,\ 14 = 3+11$

.....

Euler 16.12.1752 → dopis C.G. ověřil pro čísla do 1000

3.4.1753 → ověřil do 2500

.....

dnes ověřeno do 2 bilionů

?

Slabá Goldbachova hypotéza:

Každé liché číslo větší než 5 může být vyjádřeno jako součet tří prvočísel.

Goldbachova hypotéza ⇒ slabá Goldbachova hypotéza

Každé sudé číslo větší než 4 je součet 2 prvočísel ⇒
⇒ přičtením 3 ke každému takovému sudému číslu dostaneme liché číslo větší než 7, které je součtem 3 prvočísel a pokryjeme všechna lichá čísla větší než 7.

Navíc $7 = 2+2+3$.

Důkazy slabé Goldbachovy hypotézy:

Ivan Matveevich Vinogradov (1891 - 1983)

1937: dokázal pro všechna "dostatečně velká" liché čísla (žádný odhad pro "dost. velké"!)

Liu Ming-Chit a Wang Tian-Ze 2002:

dostatečně velké: $n > e^{3100} \sim 2.10^{1346}$

(komp. prověřit do 10^{20}!)

Harald Andrés Helfgott 2013: dokázat pro $n > 5$!

Generování prvočísel

Eratosthenes z Kyrény (273 – 194) síto

~~1~~ ② ③ ~~4~~ ⑤ ~~6~~ ⑦ ~~8~~ ~~9~~ ~~10~~ 11 ..... 97 ~~98~~ ~~99~~ ~~100~~

$\sqrt{N}$

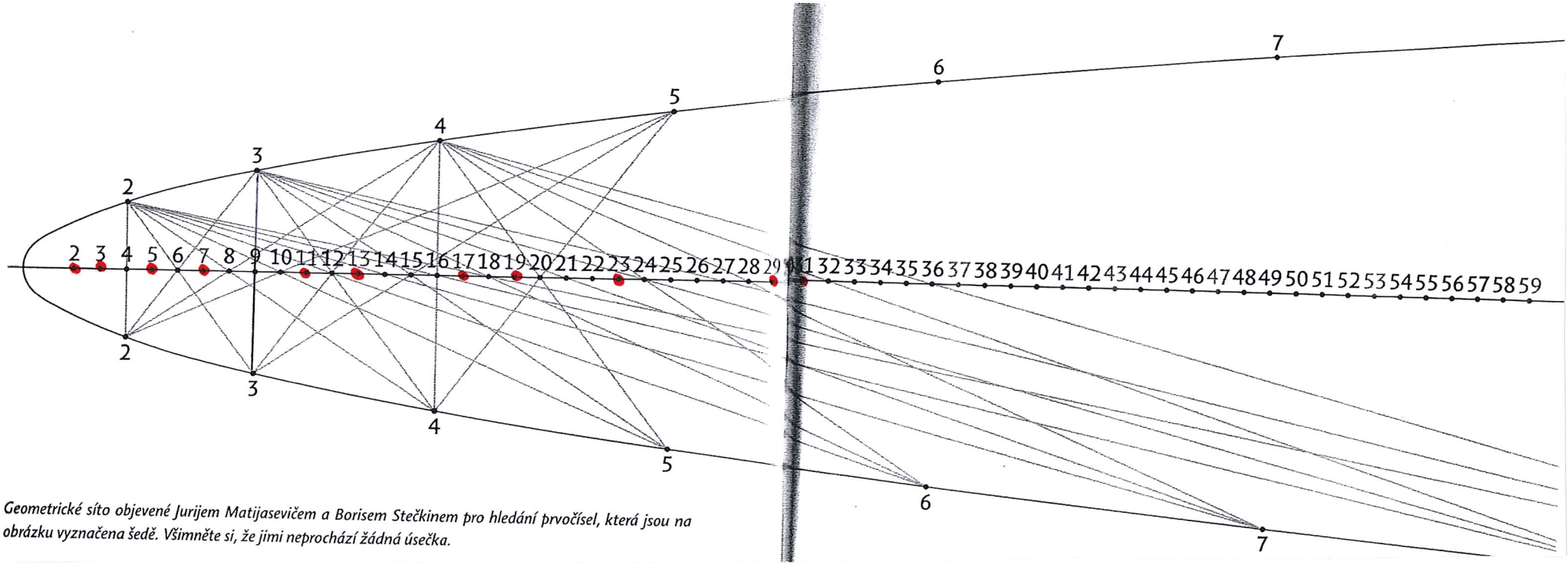
N

Geometrické síto:

Juraj Matijasevič (1947 – ?)

Boris Steckin (1920 – 1995)

Geometrické síto



Geometrické síto objevené Jurijem Matijasevičem a Borisem Stečkinem pro hledání prvočísel, která jsou na obrázku vyznačena šedě. Všimněte si, že jimi neprochází žádná úsečka.

Speciální prvočísla

Marin Mersenne (1588 - 1648)

(spolužák René Descart)

Harmonie Universelle 1636 - základy chromatických stupnic

Cogitata physico-mathematica 1644:

" Mezi všemi prvočísly p od 2 do 257 je $2^p - 1$ prvočíslem $\Leftrightarrow$ p je jedním z čísel

2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257

$2^{257} - 1$ má 77 číslic !

$\underbrace{2^p - 1 \text{ prvočíslo}}_{A} \Rightarrow \underbrace{p \text{ je prvočíslo}}_{B}$

non B $\Rightarrow$ non A : p není prvočíslo $\Rightarrow \exists a, b : p = ab \Rightarrow$

$2^p - 1 = 2^{ab} - 1 = (2^a)^b - 1 =$

$= \underbrace{(2^a - 1)}_{\alpha}\underbrace{(2^{a(b-1)} + 2^{a(b-2)} + \dots + 1)}_{\beta}$

$A \not\Rightarrow B$!

$2^{11} - 1$ není prvočíslo !

Mersenn 2, 3, 5, 7, 13, 17, 19, 31, ~~67~~, 127, ~~257~~
(bez důkazu)

Leonhard Euler (1707 - 1783):

cca 1744 (100 let po Mersennovi) dokázal, že
$2^{31}-1$ je prvočíslo

1947: 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127

"Mersennova prvočísla"
2^p-1

Velká známá prvočísla jsou právě Mersennova p.

k 14.4. 2014 bylo známo jen 47 M.p., největší
$2^{43\,112\,609}-1$ má ≈ 13.000.000 číslic

K 20. 1. 2016 bylo nalezeno 49. Mersen-

novo prvočíslo ~~(největší známé prvočíslo)~~:

$$2^{74.207.281} - 1.$$

Toto prvočíslo má

22.338.618 číslic !

K 16. 12. 2017 bylo nalezeno 50. Mersen-
novo prvočíslo

$$2^{77\,232\,917} - 1.$$

Toto prvočíslo má

23 249 425 cifer.

Speciální prvočísla

Pierre de Fermat (1601 – 1665)

"Velká Fermatova věta": $\forall n > 2 \; \nexists$ přir. čísla $x, y, z : x^n + y^n = z^n$
(Andrew Wiles 1995)

"Malá Fermatova věta"

$\forall p$ prvočíslo $\forall a \in \mathbb{N}$: $a^p - a$ je dělitelné p

Indukce:

I. $a = 2$: $2^p - 2 = (1+1)^p - 2 =$

$= 1 + \binom{p}{1} + \binom{p}{2} + \ldots + \binom{p}{p-1} + 1 - 2 =$

$= \underbrace{p} + \underbrace{\frac{p(p-1)}{2}} + \ldots + \underbrace{p}$

každý sčítanec dělitelný p

II. Nechť $a^p - a$ je dělitelné $p \overset{?}{\Longrightarrow} (a+1)^p - (a+1)$ je dělit. p

$$(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \ldots + \binom{p}{p-1}a + 1$$

$$\underbrace{(a+1)^p - a^p - 1}_{} = \underbrace{\binom{p}{1}}a^{p-1} + \underbrace{\binom{p}{2}}a^{p-2} + \ldots + \underbrace{\binom{p}{p-1}}a$$

p dělí všechny sčítance

p dělí levou stranu $\Longleftarrow$ p dělí pravou stranu

p dělí levé $a^p - a$ (předpoklad)

$\Downarrow$

p dělí

$$\left[(a+1)^p - a^p - 1\right] + a^p - a = (a+1)^p - (a+1). \quad \text{QED}$$

1. důkaz: EULER 1736

Malá Fermatova věta jako test prvočíselnosti.

Není třeba rozkládat na prvočinitele!

Příklad. $p = 9$, $a = 2$ $\Rightarrow$ $2^9 - 2 = 510$ není dělitelné 9 $\Rightarrow$ 9 NENÍ PRVOČÍSLO!

JE DŮLEŽITÉ PRO VELKÁ p.

Malá Fermatova věta: podmínka nutná!

Příklad. $p = 341 \; (= 11 \times 31)$, $a = 2$ $\Rightarrow$ $2^{341} - 2$ je dělitelné 341

$\Rightarrow$ neplatnost tzv. čínské hypotézy (400 př. n. l.)

$2^p - 2$ dělitelné p $\Leftrightarrow$ p je prvočíslo

Fermatova čísla $F_n = 2^{2^n} + 1$

$F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65\,537$

Fermatova domněnka: $\forall n$ je F_n prvočíslo

$F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 4.294.067.297$

Euler 1732: $4.294.067.297 = 641 \times 6.700.417$

Do roku 2010 byla faktorizována $F_0, F_1, F_2, F_3, F_4, F_{11}$

$n \geq 12$ F_n je prvočíslo?

$\exists$ takové n?

kolik jich je?

je jich co málo?

Hustota rozložení prvočísel

Johann Carl Friedrich Gauss (1777 – 1855)

součet aritmetické řady

ve 14 letech: „Prvočísla menší než a (≈ ∞) a/La."

$\pi(x)$ počet prvočísel menších než x

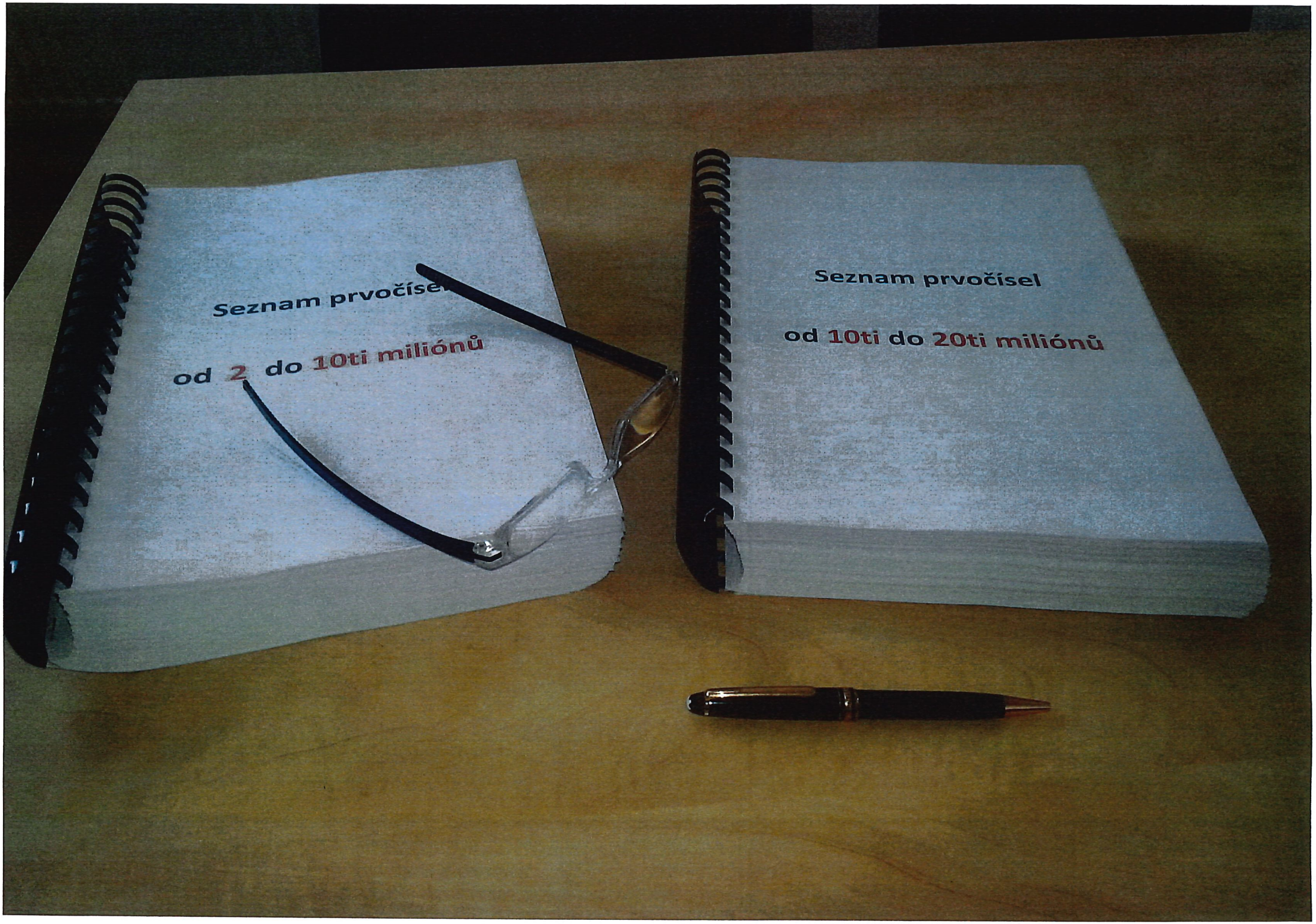
Příklad: $\pi(10) = 4$, $\pi(15) = 6$

Gaussova poznámka:

$$\pi(x) \sim \frac{x}{\ln x}, \quad x \to \infty$$

nebo:

$$\frac{x}{\pi(x)} \sim \ln x, \quad x \to \infty$$


Seznam prvočísel
od 2 do 10ti miliónů
Seznam prvočísel
od 10ti do 20ti miliónů

Prvočíselná věta: $\pi(x) \sim \frac{x}{\ln x}$, $x \to \infty$

(Gaussova domněnka)

⇓

Pravděpodobnost, že N je prvočíslo $\sim \frac{1}{\ln N}$

N-té prvočíslo je $\sim \frac{N}{\ln N}$

Důkaz 1896: Jacques Hadamard (1865–1963)

a nezávisle

Charles Jean de la Vallée Poussin (1866–1962)

Basilejský problém.

Jacob Bernoulli (1654 – 1705)

Johann Bernoulli (1667 – 1748)

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \dots$$

Jacob : součet je konečný ≤ 2

Euler : $\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$

$$\zeta(x) = \sum_{n=1}^{\infty} \frac{1}{n^x}$$

$\zeta(2)$ ... Basilejský problém

Každé n rozložíme na prvočinitele. Např. $360 = 2^3 \times 3^2 \times 5$, t.j.

$$\frac{1}{360^x} = \left(\frac{1}{2^3}\right)^x \cdot \left(\frac{1}{3^2}\right)^x \cdot \left(\frac{1}{5^1}\right)^x$$

Totéž s každým členem $\Rightarrow$

$$\zeta(x) = \frac{1}{1^x} + \frac{1}{2^x} + \ldots + \frac{1}{n^x} + \ldots =$$

$$= \left(1 + \frac{1}{2^x} + \frac{1}{4^x} + \frac{1}{8^x} + \ldots\right)\left(1 + \frac{1}{3^x} + \frac{1}{9^x} + \frac{1}{27^x} + \ldots\right)\ldots$$

$$\underbrace{\left(1 + \frac{1}{p^x} + \frac{1}{(p^2)^x} + \frac{1}{(p^3)^x} + \ldots\right)}_{\text{geometrická řada } \frac{1}{1-\frac{1}{p^x}}}\ldots = \prod_p \frac{1}{1-\frac{1}{p^x}}$$

Ekvivalentní vyjádření zeta funkce

$$\sum_{n=1}^{\infty} n^{-x} = \zeta(x) = \prod_{p} (1-p^{-x})^{-1}$$

$$\sum \frac{1}{n^x} \qquad \prod_{p} \frac{1}{1-\frac{1}{p^x}}$$

Eulerův součin

Riemannova funkce zeta

Důsledek: $x = 1 \Rightarrow \sum_{n=1}^{\infty} \frac{1}{n} = \prod_{p} (1-p^{-1})^{-1} = \infty \Rightarrow$

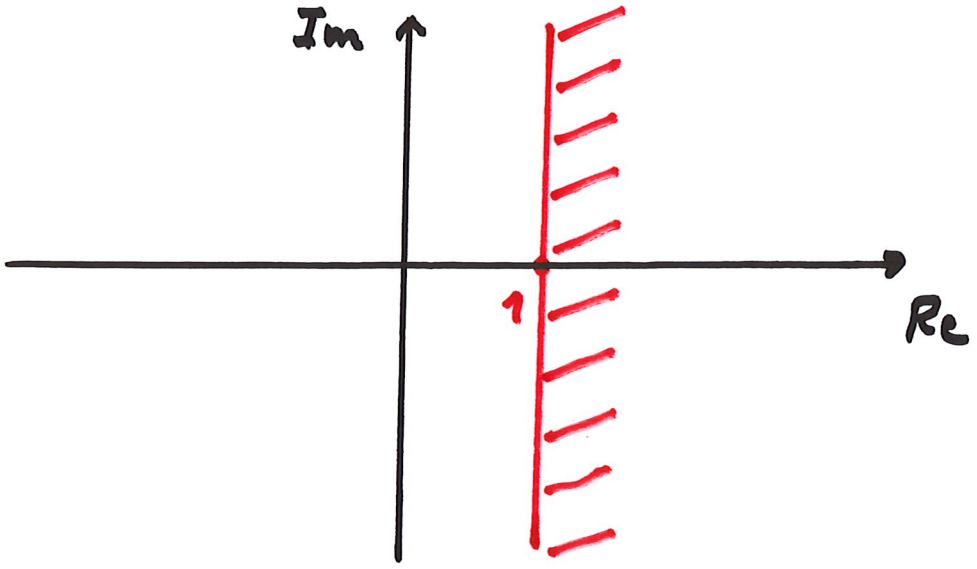
$\Rightarrow$ prvočísel je ∞ mnoho!

Bernhard Riemann (1826–1866)

Gaussova hypotéza a Eulerův součin

$$\zeta(x) = \sum_{n=1}^{\infty} \frac{1}{n^x} < \infty \quad , \quad x \in \mathbb{R}, \; x > 1$$

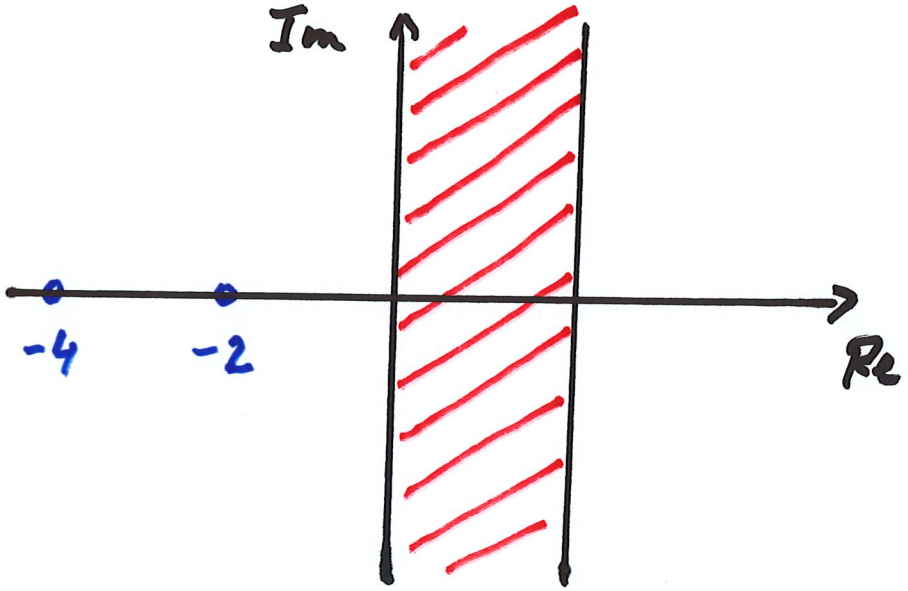
$x \in \mathbb{C}$ $\Rightarrow$ řada konverguje absolutně a lokálně stejnoměrně v polorovině $\mathrm{Re}\, x > 1$:



Riemann rozšířil funkci ζ do celé komplexní roviny $\mathbb{C}$ mimo bod 1 : analytické pokračování, které je meromorfní funkcí s jednoduchým pólem v bodě 1.

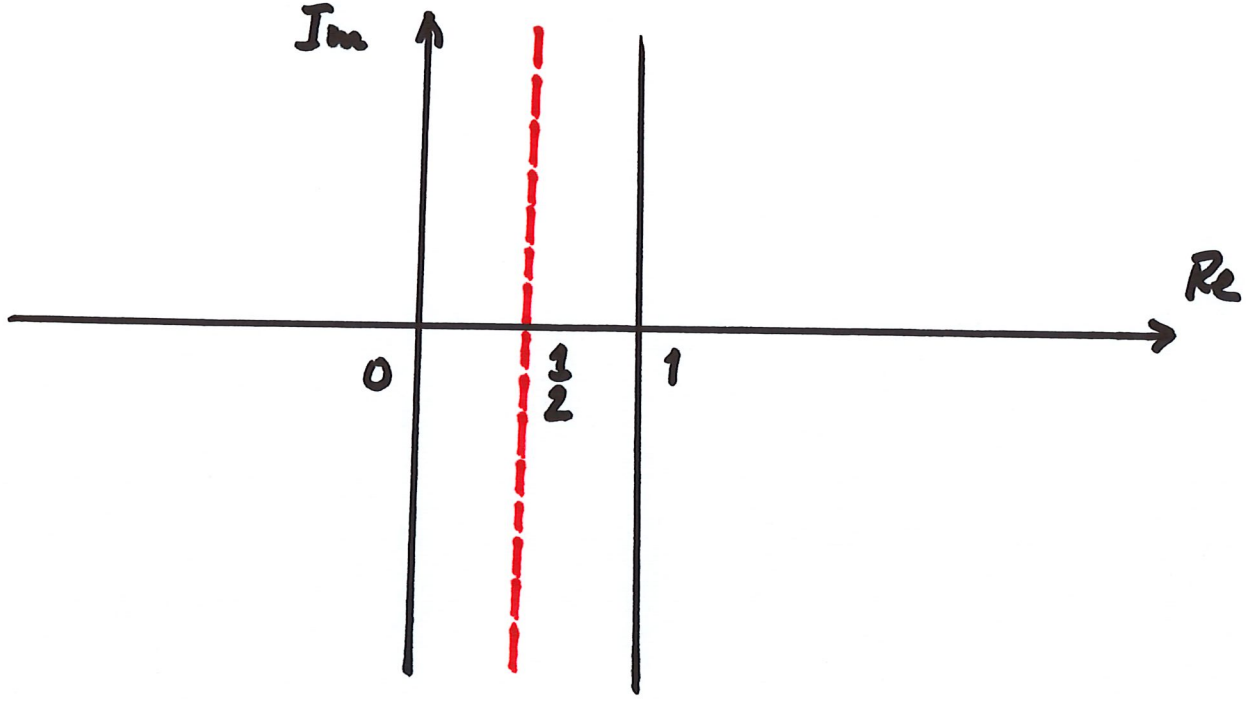
Nulové body : triviální (sudá záporná čísla)

netriviální (v kritickém pásu $0 < \mathrm{Re}\, x < 1$)



Riemannova hypotéza 1859:

Všechny netriviální nulové body funkce $\zeta(x)$ leží na kritické přímce $Re\, x = \frac{1}{2}$.



Godfrey Harold Hardy (1877 - 1947)

John Edensor Littlewood (1885 - 1977)

Na kritické přímce $\mathrm{Re}\, x = \frac{1}{2}$ leží nekonečně mnoho (netriviálních) nulových bodů funkce $f(x)$.

Souvislost nulových bodů ζ a rozložení prvočísel

$$\forall x \in \mathbb{C},\ \mathrm{Re}\, x = 1 \Rightarrow \zeta(x) \neq 0$$

$$\Downarrow$$

$$\pi(x) \sim \frac{x}{\ln x} \quad \text{neboli} \quad \lim_{x \to \infty} \frac{\pi(x) \ln x}{x} = 1$$

přesnější

$$\pi(x) \sim Li(x) = \int_2^x \frac{dt}{\ln t} \quad \text{neboli} \quad \lim_{x \to \infty} \frac{\pi(x)}{Li(x)} = 1$$

Víme-li, že $\zeta(x) \neq 0$ "více vlevo" od přímky $\mathrm{Re}\, x = 1$,
dostáváme odhad velikosti rozdílu $\pi(x) - Li(x)$:

Vallée Poussin 1896

$$\pi(x) = Li(x) + O\left(x e^{-c\sqrt{\ln x}}\right)$$

.....

I. M. Vinogradov, N. M. Korobov 1958

$$\pi(x) = Li(x) + O\left(x e^{-c \frac{\ln^{3/5} x}{(\ln \ln x)^{1/5}}}\right)$$

Riemannova hypotéza

$$\pi(x) = Li(x) + O(\sqrt{x}\ln x)$$

Literatura

Enrique Gracián: Prvočísla, dlouhá řada do nekonečna, Dokořán, Edice Matematický svět 1, 2017.

John Derbyshire: Posedlost prvočísly, Galileo, Academia, 2007.

Břetislav Novák: O osmém hilbertově problému, Pokroky matematiky, fyziky a astronomie, ročník 18, (1973), číslo 1, str. 9-17.

Břetislav Novák: Opět o Riemannově zeta funkci, Pokroky matematiky, fyziky a astronomie, ročník 38, (1993), číslo 1, str. 7-13.