Leonard Euler (1707–1783), Ben Green (1977) a Terry Tao (1975): Prvočísla před třemi sty lety a dnes

Martin Klazar (KAM MFF UK Praha)

- Co jsou prvočísla
- Kdo byl L. Euler
- Euler a prvočísla
- Moderní použití prvočísel
- Kdo jsou B. Green a T. Tao
- Greenova-Taova věta o prvočíslech

Co jsou prvočísla – atomy multiplikativního světa čísel

1, 2, 3, 4, 5, 6, ... +, $\dot{\times}$ – aritm. operace

1

$50 = 15 \cdot 10 = 3 \cdot 5 \cdot 10 = \underbrace{3 \cdot 5 \cdot 2 \cdot 5}$

$= \underbrace{2 \cdot 3 \cdot 5^2}$

prvočísla – nedají se dál rozložit (dělitelné jen 1 a sebe samou)

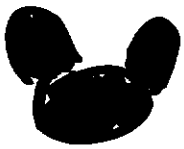
$\mathcal{P} = 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, \ldots$

Chemické prvky: rovněž dále (chemicky) nedělitelné atomy

Prvky: H vodík, He helium, Li lithium, Be beryllium, B bor, C uhlík, N dusík, O kyslík, F fluor, Ne neon, ...

H_2O (voda) $\sim 2^2 \cdot 19 = 76$

1. prvek, 8. prvek, 1. prvočíslo, 8. prvočíslo



NaCl (kuchyňská sůl) $\sim 31 \cdot 59 = 1829$

11. prvek, 17. prvek, 11. prvoč., 17. prvoč.

Mendělejevova tabulka prvků má (října 2006) 117 prvků (Ununoctium – 118. prvek) objeven v říjnu 2006 v Dubně u Moskvy

Množina prvočísel je nekonečná

- Euklides (Základy, kniha IX, propozice 20)

(~~[illegible]~~ Alexandrie, 3. st. př. n. l.)

Důkaz (∞-sti počtu prvočísel)

Sporem. Nechť $p_1, p_2, \dots, p_r$ jsou všechna prvočísla. Uvaž číslo $č = p_1 p_2 \cdots p_r + 1$. To je dělitelné nějakým prvočíslem p. Kdyby $p = p_1$, pak by p dělilo 1 $(= č - p_1 p_2 \cdots p_r)$ – nelze. Stejně tak nelze $p = p_2, \dots, p = p_r$. Takže p je nové prvočíslo, různé od $p_1, \dots, p_r$. Spor.

Příklad $č = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031$

$30031 = 59 \cdot 509$, nová prvočísla 59 a 509.

Základní věta aritmetiky

Rozklad na prvočísla je jednoznačný (až na pořadí činitelů).

Takže si můžeme být jisti, že

$$(450 =)\ 2 \cdot 3^2 \cdot 5^2 \neq 2^6 \cdot 7\ (= 448)$$

$$\neq 3 \cdot 151\ (= 453)$$

z VA, tj. jednoznačnost rozkladu na „prvočísla" (nerozložitelné prvky), obecně neplatí v jiných strukturách. Například v $\mathbb{Z}[\sqrt{-5}]$ = čísla tvaru $a + b\sqrt{-5}$, kde a, b jsou celá (např. $3 - 2\sqrt{-5}$, 0, 6, $17 + 5\sqrt{-5}$, ...) má 6 dva různé rozklady na „prvočísla": $\underbrace{2 \cdot 3} = 6$.

$$\underbrace{(1+\sqrt{-5})\cdot(1-\sqrt{-5})} = 1^2 - (\sqrt{-5})^2 = 1-(-5) = 6.$$

Leonard Euler (1707–1783)

- největší matematik všech dob (vedle Gausse)
- rovněž mechanika, fyzika, astronomie, technika
- (866)
- více než 850 pojednání, viz The Euler Archive

www.math.dartmouth.edu/~euler

- narodil se 15.4.1707 v Basileji ve Švýcarsku v rodině pastora
- studuje na Un. v Basileji, u Johanna Bernoulliho
- 1727 odjíždí do St. Petersburgu (Petrohradu)

1. petrohradské období 1727–41

- 1733 přebírá stolici matematiky po D. Bernoulliim, žení se a kupuje dům.
- 1735, suma $1/1^2 + 1/2^2 + 1/3^2 + \dots = \pi^2/6$, mezinárodní reputace
- 1738 slepne na pravé oko
- 1741 polit. krize v Rusku, odjíždí do Berlína (Friedrich II)

berlínské období 1741–66

- 1762 Kateřina II carevnou, snaží se získat E. zpět (1771 – slepne úplně)
- 1766 vrací se do St. Petersburgu

2. petrohradské období 1766–83

- umírá 18.9.1783 v St. P.

Euler a prvočísla

- brzy po příchodu do P. se seznámil s Ch. Goldbachem*), 177 dopisů mezi E. a G. v období 1729–64. G. inspiroval E. k výzkumům v teorii čísel.
- 1742 Goldbachův problém:

Každé sudé číslo (kromě 2) 4, 6, 8, 10, 12, ... je součtem 2 prvočísel; například

$12 = 7+5$, $20 = 13+7 = 3+17$, $32 = 19+13 = 3+29$

- dosud otevřený problém!

Fermatovy domněnky P. de Fermat (1601–1665)

1) Každé prvočíslo tvaru $4n+1$ je součet 2 čtverců; například $5 = 2^2+1^2$, $17 = 4^2+1^2$, $29 = 5^2+2^2$, $37 = 6^2+1^2$, $41 = 5^2+4^2$, ...

Dokázal Euler (Eneström – E 241 – Demonstratio theorematis Fermatiani ..., 1760)

---

*) Ch. G. (1690–1764), pruský matematik

2) Každé číslo tvaru $2^{2^n}+1$ je prvočíslo;

například $2^{2^0}+1 = 2^1+1 = \underline{3}$, $2^{2^1}+1 = \underline{5}$,

$2^{2^2}+1 = \underline{17}$, $2^{2^3}+1 = 2^8+1 = \underline{257}$, $2^{2^4}+1 = \underline{65537}$, ..

Vyvrátil Euler v 1. práci o teorii čísel

(E 26 - Observationes de theoremata quodam Fermatiano aliisque ad numeros primos spectantibus, 1732, 1738)

641 dělí $2^{2^5}+1$:

$2^{2^5}+1 = 4294967297 = 641 \cdot 6700417$.

- Je otevřený problém, zda existují další tzv. Fermatova prvočísla kromě kořejších pěti.

Gauss, Wantzel: Pravidelný n-úhelník lze sestrojit pravítkem a kružítkem $\iff n = 2^k \cdot p_1 \cdot p_2 \cdots p_r$, kde p_i jsou různá Fermatova prvočísla.

Např. 17-úhelník lze sestrojit ...

Dokonalá a spřátelená čísla

Číslo je <u>dokonalé</u>, je-li součtem svých vlastních dělitelů. Např. $6 = 1+2+3$

$28 = 1+2+4+7+14$

$496 =$

~~Euler~~ Euler dokázal, že <u>sudé</u> číslo je dokonalé $\Longleftrightarrow$ je tvaru $2^{n-1}(2^n-1)$, kde <u>2^n-1 je prvočíslo</u>. Je známo <u>44</u> dok. čísel. Je dosud otevřený problém, zda existují lichá dokonalá čísla.

Dvě čísla jsou <u>spřátelená</u>, je-li jedno součtem vlastních dělitelů druhého. Např. součet vl. dělitelů č. 220 je $1+2+4+5+10+11+20+22+44+55+110 = 284$ a součet vl. dělitelů č. 284 je $1+2+4+71+142 = 220$. Euler nalezl řadu dvojic spř. čísel (E 100 – De numeris amicabilibus, 1747)

Rozložení prvočísel

Víme, že prvočísel je nekonečně mnoho, ale jak hustě jsou mezi čísly 1, 2, 3, 4, ... rozložena?

Euler: $1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5}+\frac{1}{6}+\frac{1}{7}+\frac{1}{8}+\frac{1}{9}+\dots$

$$\text{„}=\text{"}\ \frac{1}{1-1/2}\cdot\frac{1}{1-1/3}\cdot\frac{1}{1-1/5}\cdot\frac{1}{1-1/7}\cdot\frac{1}{1-1/11}\cdots$$

přesněji, pro $\underbrace{s>1}$,

$$1+\frac{1}{2^s}+\frac{1}{3^s}+\frac{1}{4^s}+\dots=\frac{1}{1-1/2^s}\cdot\frac{1}{1-1/3^s}\cdot\frac{1}{1-1/5^s}\cdot\frac{1}{1-\frac{1}{7^s}}\cdots$$

$$(\zeta(s)=)\sum_{n=1}^{\infty}\frac{1}{n^s}=\prod_p\frac{1}{1-1/p^s}\quad(s>1)$$

– <u>Eulerova identita</u> (E72 – Variae observationes circa series infinitas, 1737)

$\rightsquigarrow$ Hadamard; Poussin (1896)

počet prvočísel $\leq x$ je $\doteq \frac{x}{\log x}$.

Použití prvočísel

- prvočísla byla dlouho kanonickým příkladem čisté matematiky bez praktického využití
- základní prostředek a nástroj v <u>teorii čísel</u> pro studium vlastností čísel 1, 2, 3, 4, 5, 6, ...
- Gödel je použil pro kódování formulí a důkazů v logice ve své větě o neúplnosti.
- V 70-tých letech 20. st. byly objeveny kryptografické systémy s veřejným klíčem, založené na prvočíslech

RSA algoritmus (též C. Cocks, 1973, utajeno)

↑ R. Rivest
↑ A. Shamir
↑ L. Adleman

(1977)

RSA algoritmus (systém) je založen na tom, že:

p, q velká prvočísla $p, q \rightsquigarrow n = pq$ je lehké, ale je těžké zpátky rozložit $n \rightsquigarrow p, q$.

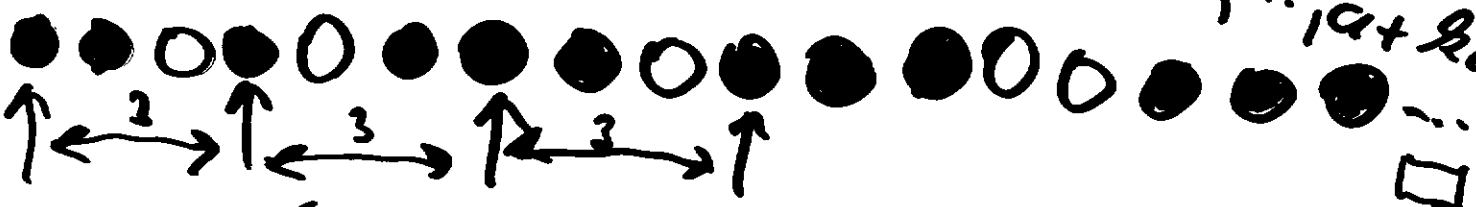
Greenova–Taova věta o prvočíslech

duben 2004 – B. Green a T. Tao umístili na preprintový server Arxiv cca 50-ti stránkový článek s důkazem věty:

Množina prvočísel $\{2, 3, 5, 7, 11, 13, \dots\}$ obsahuje libovolně dlouhé aritmetické posloupnosti.

aritm. posl. je např. $8, 13, 18, 23, 28$, protože $13-8 = 18-13 = 23-18 = 28-23$ $(=5)$, má délku 5.

obecná aritm. posl.: $a, a+d, a+2d, \dots, a+kd$.



jednobarevná A.P. délky 4 (s diferencí 2) barvy:

van der Waerdenova věta (cca 1927):
Jsou-li čísla 1, 2, 3, 4, ... obarvena konečným počtem barev (např. pěti, jako výše), vždy lze nalézt jednobarevnou A.P. libovolné délky.

Erdősova-Turánova domněnka (≐ 1936):
Vybereme-li z čísel 1, 2, 3, 4, ... jakoukoli podmnožinu X, která obsahuje alespoň 1% (0.1%, 0.01%, 0.001%, ...) všech čísel, potom X vždy musí obsahovat A.P. libovolné délky.

(X obsahuje alespoň 1% všech čísel $\Leftrightarrow$
$\Leftrightarrow \frac{|X \cap \{1,2,\dots,n\}|}{n} \geq 0.01$ pro nekonečně mnoho n)

Erdősovu-Turánovu domněnku dokázal v r. 1975 E. Szemerédi
(už před tím v r. 1955 K. Roth ji dokázal pro A.P. délky 3)

B. Green a T. Tao dokázali rozšířit Szemerédiho výsledek na X = množina prvočísel (která nemá Kladnou hustotu, obsahuje 0% všech čísel)

Např. 5, 11, 17, 23, 29 je A.P. délky pět složená z prvočísel.

Kdo jsou Ben Green a Terry Tao

Ben Green (nar. 1977) Bristol, UK

95–98 Trinity Coll., Cambridge

99–02 PhD, Cambridge; pak postdok
05–06 Un. of Bristol
06– Un. of Cambridge

Terence Tao, (nar. 1975) Adelaide, Austrálie

mezin. matem. olymp.
medaile na IMO: 1986 bronzová
1987 stříbrná
1988 zlatá

PhD Un. of Princeton, USA 1996
1999– prof. matematiky na UCLA
V r. 2006 – Fieldsova medaile na kongresu v Madridu.