Množina prvočísel

Def (Prvočíslo): Prvočíslem na množině $\mathbb{N}$ nazveme každé $p \in \mathbb{N}$, $p \geq 2$ právě když:

$$\forall a,b \in \mathbb{N}: \quad p = a \cdot b \Rightarrow (a=1 \vee b=1).$$

Množinu všech prvočísel označme $\mathbb{P}$.

Pozn. V definici prvočísla bychom místo použitého požadavku mohli použít: $\forall a \in \mathbb{N}: a \mid p \Rightarrow (a=1 \vee a=p)$.

Věta: Každé $n \in \mathbb{N}$, $n \geq 2$, je buď prvočíslo, nebo je součinem prvočísel.

Důkaz: Použijeme silnou indukci:

1.) Pro $n=2$ je tvrzení věty pravdivé, neboť 2 je prvočíslo.

2.) Indukční krok. Předpokládejme, že každé $k \in \{2,\dots,n-1\}$ je buď prvočíslo, nebo součin prvočísel. Mohou nastat 2 možnosti:

α) n je prvočíslo

β) n není prvočíslo $\Rightarrow \exists a,b \in \mathbb{N}: p = a \cdot b \wedge (a>1 \wedge b>1)$

$\Rightarrow$ podle indukčního předpokladu musí být a,b prvočísla, nebo součiny prvočísel (neboť $a,b \in \{2,\dots,n-1\}$).

$\Rightarrow n$ je buď prvočíslo, nebo součin prvočísel. □

Věta (Euklidova prvočíselná): Prvočísel je nekonečně mnoho.

Důkaz: Sporem. Předpokládejme, že $p_1 < p_2 < \dots < p_n$ je konečná posloupnost všech prvočísel.

$k = p_1 \cdot p_2 \cdot \dots \cdot p_n + 1 > p_n$ proto k není prvočíslo, ale číslo složené - je dělitelné některým z čísel $p_1, \dots, p_n$, řekněme prvočíslem p_i.
Proto $\frac{k}{p_i} \in \mathbb{Z}$, ale:

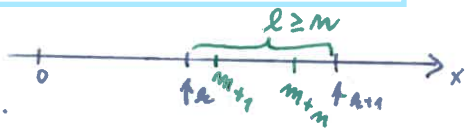
$$\frac{k}{p_i} = \underbrace{\frac{p_1 p_2 \cdots p_i \cdots p_n}{p_i}}_{\in \mathbb{N}} + \underbrace{\frac{1}{p_i}}_{\in (0,1)} \notin \mathbb{Z} \Rightarrow \text{Spor!}$$

□

⇒ Prvočísel je z hlediska náhledu „hodně." Ukážeme ale, že na číselné ose jsou libovolně široké intervaly, kde nejsou prvočísla ⇒ „je jich málo."

Věta: Nechť $p_1 < p_2 < \dots$ je posloupnost všech prvočísel. Potom
$\forall n \in \mathbb{N}\ \exists k \in \mathbb{N}: \quad p_{k+1} - p_k \geq n.$

Důkaz: Pro libovolné dané $n \in \mathbb{N}$ označme $m = (n+1)! + 1$.



$m+1 = (n+1)! + 2 = 2 \cdot \left(\frac{(n+1)!}{2} + 1\right)$ ⇒ $m+1$ je složené!
($1 < k_1 \in \mathbb{Z}$)

$m+2 = (n+1)! + 3 = 3 \left(\frac{(n+1)!}{3} + 1\right)$ ⇒ $m+2$ je složené!
($1 < k_2 \in \mathbb{Z}$)

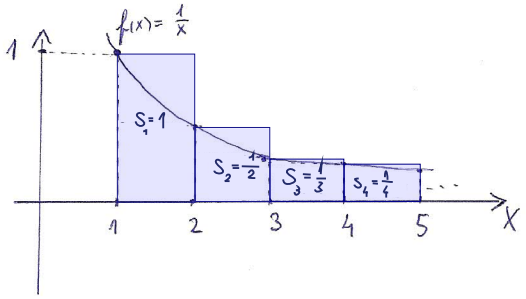
$\vdots$

$m+n = (n+1)! + n+1 = (n+1)\,(n! + 1)$ ⇒ $m+n$ je složené!

Zvolíme-li $p_k = \max \{ p_i \in \mathbb{P} \mid p_i \leq m \}$, pak $p_{k+1} > m+n \geq p_k + n$

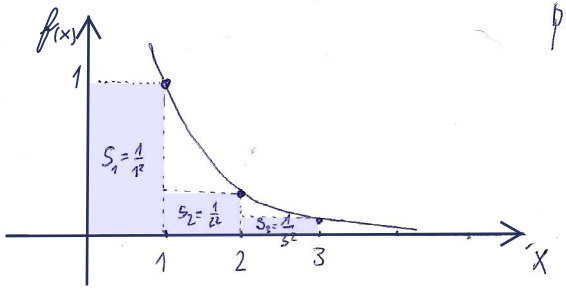
□

1.) $\sum_{n \in \mathbb{N}} \frac{1}{n} = \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \dots$ = součet posloupnosti převrácených hodnot všech přirozených čísel.



$$\sum_{i=1}^{\infty} S_i \geq \int_1^{\infty} \frac{1}{x}\,dx = [\ln x]_1^{\infty} = \lim_{x \to \infty} (\ln x - \ln 1) = \infty$$

2.) $\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} \dots$ = součet posloupnosti převrácených hodnot druhých mocnin přirozených čísel



$$\sum_{i=1}^{\infty} S_i = 1 + \sum_{i=2}^{\infty} S_i \leq 1 + \int_1^{\infty} \frac{1}{x^2}\,dx = 1 + \left[-\frac{1}{x}\right]_1^{\infty} = 1 + 1 < \infty$$

⇒ Srovnání těchto sum ukazuje, že druhých mocnin je v jistém smyslu méně, než všech ostatních přirozených čísel – a to podstatně „méně" – jelikož je vynecháme, pak součet převrácených hodnot rostoucích přirozených čísel diverguje; součet převrácených hodnot druhých mocnin konverguje.

3.) $\sum_{p \in \mathbb{P}} \frac{1}{p} = ?$ Konverguje, nebo diverguje?

Věta: Nechť $\{p_i\}_{i=1}^{\infty}$ je rostoucí posloupnost všech prvočísel. Potom platí:

$$\sum_{i=1}^{\infty} \frac{1}{p_i} = +\infty$$

Důkaz: Sporem. Předpokládejme, že $\sum_{i=1}^{\infty} \frac{1}{p_i} = c \in \mathbb{R}$. Potom

$$\forall \varepsilon > 0 \; \exists k \in \mathbb{N} : \sum_{i=k+1}^{\infty} \frac{1}{p_i} < \varepsilon$$

(Pozn. z mat. analýzy: u konvergentní řady vždy musíme najít libovolně malý „zbytek řady".) $\Rightarrow \exists k \in \mathbb{N} : \sum_{i=k+1}^{\infty} \frac{1}{p_i} < \frac{1}{2}$ (*)

Označme $k_n = 1 + n \cdot \underbrace{p_1 p_2 \cdots p_k}_{\text{„}P=\text{konst.}} = 1 + n \cdot P$.

Jak vidno, $\forall n \in \mathbb{N}$, číslo k_n není dělitelné žádným z prvočísel $p_1, p_2, \dots, p_k$. Tj. rozklad k_n na prvočísla má tvar:

$$k_n = p_{k+1}^{\beta_{k+1}(n)} \, p_{k+2}^{\beta_{k+2}(n)} \cdots p_{\alpha(n)}^{\beta_{\alpha(n)}(n)},$$

kde $\alpha(n) \in \mathbb{N}$, $\alpha(n) \geq k+1$ i $\beta_i(n) \in \mathbb{N}_0$ pro $i \in \{k+1, \dots, \alpha(n)\}$.

$\Rightarrow \forall n \in \mathbb{N} \; \exists \alpha(n) \in \mathbb{N}, \alpha(n) \geq k+1 \; \exists m(n) = \beta_{k+1}(n) + \beta_{k+2}(n) + \dots + \beta_{\alpha(n)}^{(n)}$:

$\frac{1}{k_n}$ je jedním ze členů součtu

$$\left(\sum_{i=k+1}^{\alpha(n)} \frac{1}{p_i} \right)^{m(n)} = \left(\frac{1}{p_{k+1}} + \frac{1}{p_{k+2}} + \dots + \frac{1}{p_{\alpha(n)}} \right)^{m(n)}$$

Např. $k_n = p_{k+1}^2 \cdot p_{k+2}^0 \cdot p_{k+3}^1 \Rightarrow$

$$\left(\frac{1}{p_{k+1}} + \frac{1}{p_{k+2}} + \frac{1}{p_{k+3}} \right)\left(\frac{1}{p_{k+1}} + \frac{1}{p_{k+2}} + \frac{1}{p_{k+3}} \right)\left(\frac{1}{p_{k+1}} + \frac{1}{p_{k+2}} + \frac{1}{p_{k+3}} \right) =$$

$$= \dots + \frac{1}{p_{k+1}^2 \, p_{k+3}} + \dots .$$

Všimněme si, že čísla $k_n = 1 + nP$, kde $n = 1, 2, \dots$ jsou navzájem různá a $\frac{1}{k_n}$ je jistě některým ze členů součtu:

$$\sum_{m=1}^{\infty} \left(\sum_{i=k+1}^{\infty} \frac{1}{p_i} \right)^m \quad \Rightarrow$$

$\forall r \in \mathbb{N}$:

$$\sum_{n=1}^{r} \frac{1}{k_n} = \sum_{n=1}^{r} \frac{1}{1+nP} \leq \sum_{m=1}^{\infty} \left(\sum_{i=k+1}^{\infty} \frac{1}{p_i} \right)^m \overset{(*)}{\leq} \sum_{m=1}^{\infty} \left(\frac{1}{2} \right)^m =$$

$$= \frac{1}{2} \cdot \frac{1}{1-\frac{1}{2}} = 1$$

$\Rightarrow \sum_{n=1}^{\infty} \frac{1}{k_n} = \sum_{n=1}^{\infty} \frac{1}{1+nP}$ konverguje (na základě předpokladu), ale!:

$$\sum_{n=1}^{r} \frac{1}{1+nP} \geq \sum_{n=1}^{r} \frac{1}{n+nP} \geq \sum_{n=1}^{r} \frac{1}{n(1+P)} = \underbrace{\frac{1}{1+P}}_{\searrow 0} \underbrace{\sum_{n=1}^{r} \frac{1}{n}}_{\searrow +\infty} \Rightarrow \sum_{n=1}^{\infty} \frac{1}{k_n} = +\infty \Rightarrow \text{spor!}$$

□

Prvočísla v aritmetických posloupnostech

Př. Hledejte prvočísla v daných posloupnostech.

1) $\{3k+2\}_{k=1}^{\infty}$: (2) (5) 8 (11) 14 (17) 20 (23) 26 (29) 32 35 38 (41) ...

Kolik jich bude?

2) $\{6k+10\}_{k=1}^{\infty}$: 10 16 22 28 34 ... $6k+10 = \underset{\geq 1}{2}(\underset{\geq 1}{3k+5})$ ... není prvočíslo!

Tady žádné nebudou, protože $\gcd(6, 10) = 2 > 1$

Př. Dokažte, že existuje nekonečně mnoho prvočísel ve tvaru $p_k = 4n-1$, $n \in \mathbb{N}$ (tzn. $p_k \equiv 3 \pmod 4$).

Důkaz: Sporem. Předpokládejme, že p je největší prvočíslo ve tvaru $4n-1$.

Označme $N = 4 \cdot \underbrace{3 \cdot 5 \cdot 7 \cdot \ldots \cdot p}_{\text{součin všech lichých prvočísel od 3 do } p} - 1 \quad (*)$ ⇒

N jistě není dělitelné žádným z prvočísel $2, 3, 5, \ldots, p$ (jinak spor $\mathbb{Z} \ni \frac{N}{p_i} = \frac{4 \cdot 3 \cdot 5 \cdot 7 \ldots p}{p_i} - \frac{1}{p_i} \notin \mathbb{Z}$) a samo také není prvočíslo, neboť $N = 4k-1 \wedge N > p$. Proto N je součinem prvočísel ve tvaru $4n+1$. Tzn.

$$N = q_1 \cdot \ldots \cdot q_m \quad \text{, kde } q_i \in \mathbb{P}, \; q_i \equiv 1 \pmod 4 \Rightarrow$$

$$N = q_1 \ldots q_m \equiv 1 \pmod 4$$

To je ale spor s (*) odkud plyne, že $N \equiv -1 \equiv 3 \pmod 4$. □

Jak je vidět na příkladu posloupnosti $\{6k+1\}_{k=1}^{\infty}$, má smysl hledat prvočísla v posloupnostech $\{mk+a\}_{k=1}^{\infty}$, kde $a, m \in \mathbb{N}$, pouze v případě, že $\gcd(m,a)=1$.

Dirichletova věta říká, že v takovém případě jich sám je nekonečně mnoho.

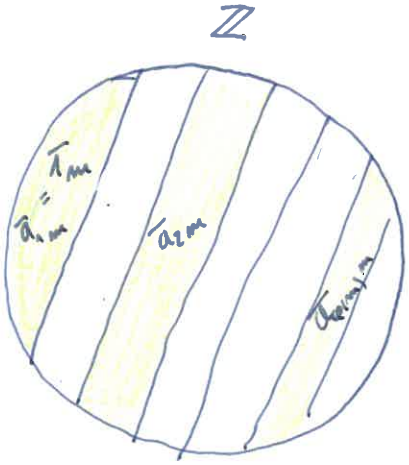
Věta (Dirichletova): Nechť $m \in \mathbb{N}$, $a \in \mathbb{Z}$, $\gcd(a,m)=1$. Potom

$$\sum_{\substack{p \in \mathbb{P} \\ p \equiv a \pmod m}} \frac{1}{p} = +\infty$$

Poznámka: Dirichletovu větu je možné formulovat i silněji:

$$\sum_{\substack{p \in \mathbb{P} \\ p \equiv a \pmod m \\ p \le X}} \frac{1}{p} = \underbrace{\frac{1}{\varphi(m)}}_{\text{Eulerova funkce}} \cdot \underbrace{\ln \ln X}_{\to \infty} + \underbrace{A(a,m)}_{\substack{\text{konstanta} \\ \text{závisející} \\ \text{na } a, m, \\ \text{ale ne na } X!}} + \underbrace{O\left(\frac{1}{\ln X}\right)}_{\to 0} \qquad (D)$$

„počet čísel z $\{1,\dots,m\}$ nesoudělných s m"



⇒ Vzhledem (D) říká, že v každé ze zbytkových tříd $\bar{a}_{1_m}, \bar{a}_{2_m}, \dots, \bar{a}_{\varphi(m)_m}$, kde $\gcd(a_i, m)=1$ je „téměř stejný" počet prvočísel $p \le X$ (pro „velké" x), neboť ve výrazu na pravé straně rovnosti se nevyskytuje a.

↑ je tu $\varphi(m)$ zbytkových tříd $\bar{a}_{1m}, \bar{a}_{2m}, \dots, \bar{a}_{\varphi(m),m}$ takových, že $\gcd(a_i, m)=1$

Čebyšev dokázal platnost nerovností:

$$\frac{x}{\ln x}\left(c_1+\sigma(1)\right) \le \pi(x) \le \frac{x}{\ln x}\left(c_2+\sigma(1)\right)$$

, kde

$$\pi(x) = \left|\{p\in\mathbb{P} \mid p\le x\}\right| \text{ pro } x\in\mathbb{R}^+.$$

$c_1 = \ln\left(2^{\frac{1}{2}}3^{\frac{1}{3}}5^{\frac{1}{5}}30^{-\frac{1}{30}}\right) \approx 0{,}92129$ a $c_2 = \frac{6}{5}c_1 \doteq 1{,}10555$

Zajímavým důsledkem těchto nerovností je:

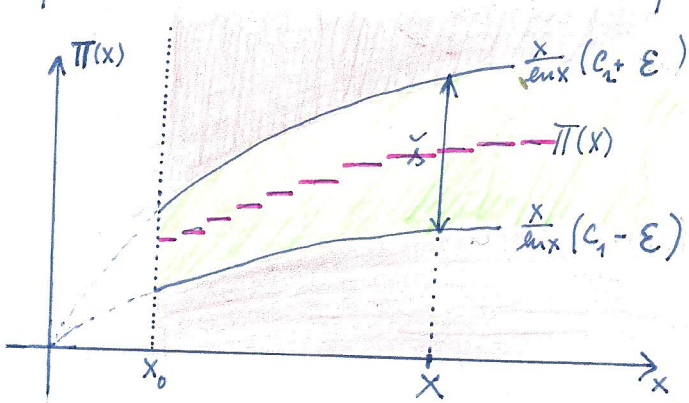
$$\lim_{x\to\infty}\frac{\pi(2x)}{\pi(x)} \ge \lim_{x\to\infty}\frac{\frac{2x}{\ln(2x)}\left(c_1+\sigma(1)\right)}{\frac{x}{\ln x}\left(c_2+\sigma(1)\right)} = \frac{2c_1}{c_2}\lim_{x\to\infty}\frac{\ln x}{\ln(2x)} \overset{l'H}{=} \frac{2c_1}{c_2}\lim_{x\to\infty}\frac{\frac{1}{x}}{\frac{1}{2x}\cdot 2} = \frac{2c_1}{c_2} = \frac{10}{6} > 1$$

$\Rightarrow$ Pro dostatečně velká x platí $\pi(2x) > \pi(x)$, to znamená, že mezi x a $2x$ existuje nějaké prvočíslo.

Věta (Bertrandův postulát): Pro každé $n\in\mathbb{N}$, $n>3$ existuje prvočíslo p splňující:

$$n < p < 2n-2$$

Poznámka: Ohraničení funkce $\pi(x)$: $\frac{x}{\ln x}(c_1+\sigma(1)) \le \pi(x) \le \frac{x}{\ln x}(c_2+\sigma(1))$ je „dobré" po stránce kvalitativní, ale ne po stránce kvantitativní (při $c_2\neq c_1$):



$\forall\varepsilon>0\ \exists x_0$: Pro $x>x_0$: $|\sigma(1)|<\varepsilon$

Šířka pásu, ve kterém je $\pi(x)$ „uvězněna" roste nade všechny meze:

$$š = \lim_{x\to\infty}\underbrace{\left(\frac{x}{\ln x}\right)}_{\to\infty}\left(\underbrace{c_2-c_1}_{\to 0}+\underbrace{\sigma(1)}_{\to 0}\right) = \infty$$

Prvočíselná věta

Pánové Johan Carl Friedrich Gauss a Adrien-Marie Legendre studovali tabulku hodnot funkcí $\pi(x)$ a $\frac{x}{\ln x}$ pro $x \leq 10^6$:

x	$\pi(x)$	$x/\ln x$	$\pi(x) / \frac{x}{\ln x}$
10	4	4,3	0,93
10^2	25	21,7	1,15
10^3	168	144,8	1,16
10^4	1 229	1086	1,13
10^5	9592	8686	1,10
10^6	78 498	72 382	1,08

a vyslovili hypotézu, že $\lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1$.

Čebyševův výsledek (viz dříve):

$$0,92129 + o(1) \leq \frac{\pi(x)}{\frac{x}{\ln x}} \leq 1,10555 + o(1) \qquad \text{(rok 1851)}$$

Tomu také nasvědčuje. Navíc dokázal, že zmíněná limita, pokud existuje, musí být rovna jedné. Její existenci se mu ale nepodařilo dokázat. Gauss-Legendrovu hypotézu - prvočíselnou větu - se podařilo dokázat až v roce 1896 (Jacques Salomon Hadamard a Charles-Jean Étienne Gustav Nicolas de la Vallée Poussin nezávisle na sobě) metodami komplexní matematické analýzy. Důkaz metodami teorie čísel podal v roce 1949 Atle Selberg a Paul Erdös.