Množina prvočísel

Množinu všech prvočísel budeme označovat $\mathbb{P}$. Nejprve jednoduše dokážeme, že prvočísel je nekonečně mnoho.

Věta (Euklidova prvočíselná): Prvočísel je nekonečně mnoho.

Důkaz: Nechť $p_1 < p_2 < \dots$ je posloupnost prvočísel. Sporem dokážeme, že je nekonečná.

Předpokládejme, že $p_1 < p_2 < \dots < p_n$ jsou všechna prvočísla. Každé číslo větší než p_n je tedy číslem složeným.

$\Rightarrow k = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1 \quad /:p_i$ je číslo složené $\Rightarrow$ je dělitelné některým z prvočísel $p_1, p_2, \dots, p_n$ – označme jej p_i $\Rightarrow \frac{k}{p_i} \in \mathbb{Z}$

ale $\underbrace{p_1 p_2 \cdots p_{i-1} p_{i+1} \cdots p_n}_{\in \mathbb{Z}} + \underbrace{\frac{1}{p_i}}_{\in (0, \frac{1}{2}\rangle} \notin \mathbb{Z}$ spor!

$\square$

Dokážeme, že na číselné ose nalezneme libovolně velké „díry" mezi prvočísly.

Věta: Nechť $p_1 < p_2 < \dots$ je posloupnost všech prvočísel. Pro každé $n \in \mathbb{N}$ existuje $k \in \mathbb{N}$ takové, že

$$p_{k+1} - p_k \geq n.$$

Důkaz: Vezměme libovolné $n \in \mathbb{N}$ a označme $m = (n+1)! + 1$

$\Rightarrow m+1 = (n+1)! + 2 = 2\left(\frac{(n+1)!}{2} + 1\right) = 2 \cdot k_1$, kde $k_1 \in \mathbb{Z}, k_1 > 1 \Rightarrow m+1$ je složené

$m+2 = (n+1)! + 3 = 3\left(\frac{(n+1)!}{3} + 1\right) = 3 \cdot k_2$, kde $k_2 \in \mathbb{Z}, k_2 > 1 \Rightarrow m+2$ je složené

$\vdots$

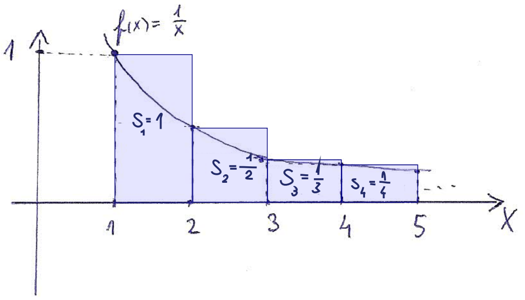
$m+n = (n+1)! + n+1 = (n+1)(n! + 1) = (n+1) \cdot k_n$, kde $k_n \in \mathbb{Z}, k_n > 1 \Rightarrow m+n$ je složené

$\Rightarrow$ našli jsme n po sobě jdoucích čísel, která jsou složená $\Rightarrow$

označíme-li p_k nejbližší ~~větší~~ menší (nebo rovné) prvočíslo k číslu m $\Rightarrow p_k + n \leq p_{k+1}$

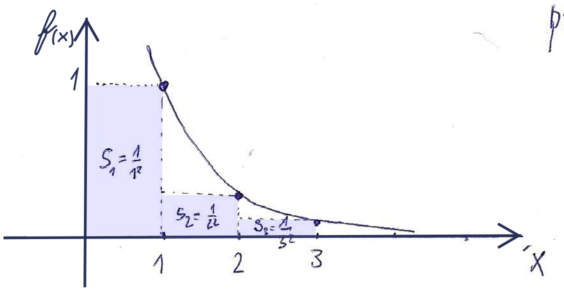
$\square$

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.



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

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



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

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

3.) $\sum_{p_i \in P} \frac{1}{p_i} = ?$ 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

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

(Poznatek 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 $k_n = 1 + n \cdot \overbrace{p_1 p_2 \cdots p_k}^{\text{„}P = \text{konst.}} = 1 + n \cdot P$.

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 $n = 1, 2, \dots, r$ jsou navzájem různá a $\frac{1}{k_n}$ je jistě některým ze členů součtu:

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

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

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

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

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

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

$\square$

Př: Existují prvočísla, která jsou prvky aritmetické posloupnosti $\{3k+2\}_{k=0}^{\infty}$?

2 5 8 11 14 17 20 23 26 29 32 35 38 .....

Př: Existují prvočísla, která jsou prvky aritmetické posloupnosti $\{6k+10\}_{k=0}^{\infty}$?

10 16 22 28 34 40 46 52 58 64 ....

$6k+10 = 3\cdot 2k + 5\cdot 2 = 2\,(3k+5)$ $\Rightarrow$ Každý prvek posloupnosti je složené číslo.

Poznámka: Prvočíslo nemůže být prvkem posloupnosti $\{ak+b\}_{k=1}^{\infty}$, $a,b \in \mathbb{N}$ kde $\gcd(a,b) = d > 1$.

Důkaz: $d \mid a \wedge d \mid b \Rightarrow$ $ak+b = da_1k + db_1 = \underbrace{d}_{>1}\underbrace{(a_1k+b_1)}_{\geq 2}$

Problém: Mějme posloupnost $\{ak+b\}_{k\in\mathbb{Z}}$, kde $a,b\in\mathbb{N}$, $\gcd(a,b)=1$. Jsou prvky této posloupnosti nějaká prvočísla? Pokud ano, je jich konečně, nebo nekonečně mnoho?

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

$$\sum_{\substack{p\in\mathbb{P} \\ p=ak+b,\ k\in\mathbb{Z}}} \frac{1}{p} = \infty$$

$$\left(\sum_{\substack{p\in\mathbb{P} \\ p=ak+b \\ p\leq X}} \frac{1}{p} = \frac{1}{\varphi(a)} \log\log X + \underset{\substack{\uparrow \\ \text{konst. závislá na } a,b}}{A(a,b)} + O\left(\frac{1}{\log x}\right) \right)$$

$\Rightarrow$ V každé posloupnosti $\{ak+b\}_{k=1}^{\infty}$ je nekonečně mnoho prvočísel $\Leftrightarrow \gcd(a,b)=1$

Př: Dokažte, že existuje nekonečně mnoho prvočísel ve tvaru $4n-1$, kde $n \in \mathbb{N}$.

Důkaz: Sporem. Předpokládejme, že existuje jen konečný počet prvočísel ve tvaru $4n-1$, kde $n \in \mathbb{N}$ a p je největší z nich. Nechť

$$N = 2^2 \cdot \underbrace{3 \cdot 5 \cdot \ldots \cdot p}_{n_0} - 1$$

Součin všech prvočísel ve tvaru $2n-1$, tzn. všechna lichá prvočísla $\leq p$

$\Rightarrow$ (*) $N = 4 \cdot n_0 - 1$ $\Rightarrow$ N podle předpokladu není prvočíslo, protože $N > p$

Žádné prvočíslo $\leq p$ nedělí N (jinak by dělilo i jedničku, což je spor!) $\Rightarrow$

$\Rightarrow$ Všechny prvočíselné dělitelé čísla N jsou větší než p $\Rightarrow$ Všichni prvočíselní dělitelé N mají tvar $4n+1$.

$$(4n_1+1)(4n_2+1) = 16n_1n_2 + 4n_1 + 4n_2 + 1 = 4n+1$$

$\Rightarrow$ Součin čísel ve tvaru $4n+1$ je opět číslo ve tvaru $4n+1$. $\Rightarrow$

$\Rightarrow$ ~~Součin všech ve~~ Číslo N, které je součinem prvočísel ve tvaru $4n+1$ je ve tvaru $4n+1$. Ale to je spor s (*) !

Číslo N nemůže mít současně tvar $4n+1$ a také $4n_0-1$!

$$\left(\begin{aligned} 4n+1 &= 4n_0 - 1 \\ 4n &= 4n_0 - 2 \\ n &= n_0 - \tfrac{2}{4} \\ n &= n_0 - \tfrac{1}{2} \\ &\text{ale } n_0 \in \mathbb{N} \wedge n \in \mathbb{N} \text{ !!!} \end{aligned}\right)$$

$\square$

Čebyšev dokázal platnost nerovností:

$$\boxed{\frac{x}{\ln x}\left(c_1 + o(1)\right) \le \pi(x) \le \frac{x}{\ln x}\left(c_2 + o(1)\right)}\ \text{, kde}$$

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

$$c_1 = \ln\left(2^{\frac{1}{2}} 3^{\frac{1}{3}} 5^{\frac{1}{5}} 30^{-\frac{1}{30}}\right) \approx 0{,}92129 \quad \text{a} \quad c_2 = \frac{6}{5} c_1 \doteq 1{,}105\,55$$

Zajímavým důsledkem těchto nerovností je:

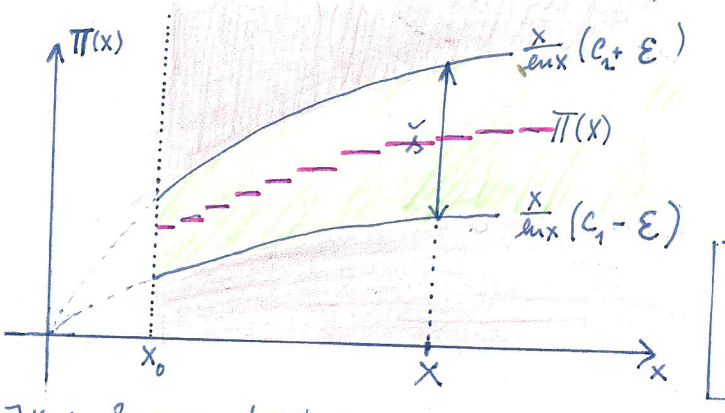
$$\lim_{x\to\infty} \frac{\pi(2x)}{\pi(x)} \ge \lim_{x\to\infty} \frac{\frac{2x}{\ln(2x)}\left(c_1 + o(1)\right)}{\frac{x}{\ln x}\left(c_2 + o(1)\right)} = \frac{2c_1}{c_2} \lim_{x\to\infty} \frac{\ln x}{\ln(2x)} \overset{l'H}{=} \frac{2c_1}{c_2} \lim_{x\to\infty} \frac{\frac{1}{x}}{\frac{1}{2x}\cdot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

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



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

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

$$\boxed{\check{s} = \lim_{x\to\infty} \underbrace{\frac{x}{\ln x}}_{\to\infty} \left(\underbrace{c_2 - c_1}_{\to 0} + \underbrace{o(1)}_{\to 0}\right) = \infty}$$

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	9 592	8 686	1,10
10^6	78 498	72 382	1,08

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

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 Vallé Poussin nezávisle na sobě) metodami komplexní matematické analýzy. Důkaz metodami teorie čísel podal v roce 1949 Atle Selberg a Paul Erdös.