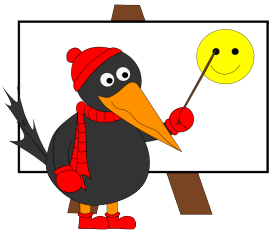
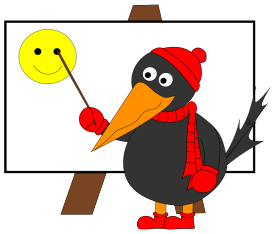


Pomocný text

Prvočísla



Prvočísla mají mezi přirozenými čísly své výsadní postavení nejen pro numerology, ale i pro matematiky. Než se pustíme do zkoumání jejich vlastností, ujasněme si tři pojmy:

Definice 1. *Nechť a, b jsou přirozená čísla. Řekneme, že a dělí b (a je dělitelem b), pokud existuje přirozené číslo c takové, že $ac = b$. Tuto skutečnost zapisujeme $a \mid b$.*

Definice 2. *Prvočíslem rozumíme takové přirozené číslo, které má právě dva různé dělitele (1 a samo sebe).*

Zejména odtud plyne, že číslo 1 za prvočíslo nelze považovat.

Z definic plyne, že každé přirozené číslo n je buď prvočíslo, nebo jej lze napsat jako součin dvou čísel různých od jedné. Každé z těchto čísel je buď prvočíslo, nebo jej lze opět rozepsat jako součin, a tak dále. Protože tím rozepisováním dostáváme n jako součin čím dál menších čísel, nemůže toto rozepisování trvat nekonečně dlouho. Nakonec dostaneme n jako součin prvočísel. *Základní věta aritmetiky* říká, že takový součin existuje jednoznačně. Abychom to dokázali, budeme potřebovat pojem největší společný dělitel a jednu pomocnou větu.

Definice 3. *Nechť a, b, d jsou přirozená čísla taková, že $d \mid a$, $d \mid b$ a pro každé číslo c splňující $c \mid a$ a $c \mid b$ platí $d \mid c$. Pak číslo d nazveme největším společným dělitelem čísel a, b, píšeme $d = (a, b)$.*

Věta 1. *Nechť a, b, c jsou přirozená čísla taková, že $a \mid bc$ a navíc $(a, b) = 1$. Pak $a \mid c$.*

Tuto větu nyní použijme k důkazu jednoznačnosti rozkladu. Předpokládejme, že pro různá prvočísla $p_1, p_2, \ldots, p_n$ platí $p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n} = p_1^{f_1} p_2^{f_2} \cdots p_n^{f_n}$ a přitom pro nějaké prvočíslo jsou exponenty na levé a pravé straně různé, BÚNO[1] $e_1 > f_1$. Po vydělení $p_1^{f_1}$ dostáváme $p_1^{e_1 - f_1} p_2^{e_2} \cdots p_n^{e_n} = p_2^{f_2} \cdots p_n^{f_n}$. Zřejmě p_1 dělí levou stranu, musí dělit i pravou. Protože je nesoudělné s každým p_j, kde $j > 1$, dostáváme dle základní věty aritmetiky, že musí dělit $p_2^{f_2 - 1} \cdots p_n^{f_n}$. Opakovanou aplikací této věty můžeme součin, který má p_1 dělit, stále zmenšovat, až dostaneme $p_1 \mid 1$, což je spor. Není těžké dokázat, že ze základní věty aritmetiky plyne zmíněná pomocná věta, proto jsou obě tvrzení zaměnitelná.

Jednoznačnosti rozkladu na součin se využívá v mnoha úlohách.

[1] Bez Újmy Na Obecnosti

Úloha 1. *Najděte všechny dvojice prvočísel p, q takových, že $p^2 - 2q^2 = 1$.*

Řešení 1. *Zde je nejjednodušší rovnici přepsat jako $2q^2 = p^2 - 1$, což dá po úpravě $2q^2 = (p-1)(p+1)$. Z jednoznačnosti rozkladu na součin víme, že levou stranu lze zapsat jako součin dvou čísel pouze třemi způsoby: $1 \cdot 2q^2$, $2 \cdot q^2$, $q \cdot 2q$. První by znamenal $p - 1 = 1$, $p + 1 = 2q^2$, tedy $p = 2$, což vede na neceločíselné q. Druhý dává $p - 1 = 2$, $q^2 = p + 1$, tedy $p = 3$ a $q = 2$. Poslední vede na $p - 1 = q$, $p + 1 = 2q$, výsledek stejný jako předchozí. Jediná možnost je $p = 3$, $q = 2$.*

Asi nejslavnější důkaz týkající se prvočísel je Eukleidův důkaz, že jich je nekonečně mnoho. Předpokládal pro spor, že je prvočísel konečně mnoho. Pak uvážil jejich součin zvětšený o jedničku. Ten nemohl ve svém rozkladu na součin prvočísel obsahovat žádné z existujících prvočísel (pak by se dva násobky toho prvočísla lišily o 1, což nelze). Musí tedy obsahovat nějaké jiné prvočíslo, a to je spor s tím, že původní součin byl vytvořen ze všech. Analogicky se dá dokázat, že prvočísel tvaru $4k + 3$ je nekonečně mnoho. Předpokládáme, že jich je konečně mnoho, všechny vynásobíme mezi sebou a k výsledku přičteme 2 nebo 4 tak, aby součet dával zbytek 3 po dělení čtyřmi. Snadno nahlédneme, že součet nemůže být součinem prvočísel tvaru $4k+1$, musí být proto dělitelný nějakým prvočíslem tvaru $4k+3$, které nebylo mezi původními, což je opět spor. Toto tvrzení se dá zobecnit.

Věta 2 (Dirichletova)**.** *Pokud jsou a, b nesoudělná čísla, je prvočísel tvaru $ak + b$ nekonečně mnoho.*

Důkaz je však nesrovnatelně těžší, než ve výše uvedeném speciálním případě.

Víme sice, že je prvočísel v této posloupnosti nekonečně mnoho, ale neznáme žádný algoritmus, jak je rychle hledat. Přesto máme určité nutné a dostatečné podmínky, aby číslo bylo prvočíslem.

Věta 3 (Wilsonova)**.** *Číslo p je prvočíslo právě tehdy, když $p \mid ((p-1)! + 1)$.*

Věta 4 (Malá[2] Fermatova)**.** *Pokud je číslo p prvočíslo, pak pro všechna a nesoudělná s p platí $p \mid a^{p-1} - 1$.*

Druhá z vět se při hledání prvočísel používá – vyzkoušením několika malých a lze prvočíselnost s jistotou vyvrátit, nebo s velkou pravděpodobností potvrdit. Jsou známy i algoritmy, které o čísle p efektivně [3]) zjistí, jestli jde o prvočíslo, ale i ty jsou dost pomalé.

Tvrzení tvaru $p \mid u - v$, kde u, v jsou nějaká čísla nebo výrazy, se nazývají kongruence. V řešení úloh o prvočíslech (a z teorie čísel obecně) se dají často využít. O kongruencích jsme psali v loňském povídání ke třetí sérii, proto tentokrát odkážeme čtenáře na náš webový archiv.

[2] Existuje i Velká Fermatova věta, která říká, že pro žádné $n > 2$ neexistuje trojice přirozených čísel x, y, z splňující $x^n + y^n = z^n$. Zatímco důkaz Malé Fermatovy věty je na pár řádků, důkaz té velké má více než 100 stran.

[3] Počet kroků algoritmu je pro nějaká k a l menší než $kn^6 \ln^l n$, kde n je délka čísla.