Prvočíselné vzorce

Víťa Kala

Prvočísla jsou jedním ze základních pojmů teorie čísel. Hodnoty prvních několika naznačují, že se jejich rozmístění mezi přirozenými čísly nevyznačuje žádnou jednoduchou zákonitostí. Nabízí se tedy otázka, zda jsou prvočísla rozmístěna zcela nahodile, anebo zda je možné jejich hodnoty vyjádřit nějakou jednoduchou funkcí. Poměrně dobrou funkcí je třeba $x^2 - x + 41$, nabývající pro všechna $x \in \{-39, -38, \ldots, 39, 40\}$ prvočíselných hodnot. Je ale jasné, že pro $x = 41$ její hodnota prvočíslem není, také pro $x = -40$ je $x^2 - x + 41 = 41^2$.

Tímto problémem se zabývali mnozí slavní matematici – například Pierre de Fermat se domníval, že všechna čísla tvaru $F_n = 2^{2^n} + 1$ jsou prvočísla. Je totiž $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ a $F_4 = 65537$, což jsou všechno prvočísla, ale $F_5 = 4294967297 = 641 \cdot 6700417$. Čísla F_n se nazývají Fermatova čísla; zajímavostí je, že dosud nebylo objeveno žádné další Fermatovo prvočíslo.

Prvočíselným vzorcem budeme rozumět libovolnou funkci, která pro všechna přirozená čísla nabývá prvočíselných hodnot. Už víme, že $2^{2^n} + 1$ není prvočíselným vzorcem; na přednášce dokážeme, že mnohé další funkce nejsou prvočíselnými vzorci, ale také si jeden předvedeme.

Během přednášky budeme používat některých známých tvrzení z teorie čísel, s nimiž se můžeš seznámit na mé přednášce o teorii čísel.

Mnohočleny

Lemma. *Ať je $P(x)$ mnohočlen s celočíselnými koeficienty a ať jsou a a b celá čísla. Pak $(a-b)|(P(a)-P(b))$ a $P(a)|P(a+bP(a))$.*

Věta. *Buď $P(x)$ nekonstantní polynom s celočíselnými koeficienty. Pak $P(x)$ není prvočíselným vzorcem.*

Dále se budeme zabývat lineárními dvojčleny. O nich vypovídá mimo jiné známá Dirichletova věta, kterou ale nebudeme dokazovat. Její důkaz je totiž značně neelementární a složitý.

Věta. (Dirichletova) *Mějme lineární dvojčlen $P(x) = ax + b$, kde $a \in \mathbb{N}$, $b \in \mathbb{Z}$ a $(a, b) = 1$. Potom je $P(x)$ prvočíslo pro nekonečně mnoho hodnot x.*

Definice. *Mějme polynom $P(x)$ s celočíselnými koeficienty. Množinu*

$$\{x; x \in \mathbb{N}, \forall n \in \mathbb{N}\, \forall k \in \mathbb{Z}\backslash 0 : x \neq n + kP(n)\}$$

nazýváme netriviálním definičním oborem $P(x)$; obdobně množina

$$\{x; x \in \mathbb{N}, \exists n \in \mathbb{N}\, \exists k \in \mathbb{Z}\backslash 0 : x = n + kP(n)\}$$

sluje triviální definiční obor. Hodnotu mnohočlenu v bodě z (ne)triviálního definičního oboru nazýváme (ne)triviální hodnotou polynomu.[2]

Z výše uvedeného lemmatu vyplývá, že mezi triviálními hodnotami libovolného nekonstantního mnohočlenu je nekonečně mnoho složených čísel. Nabízí se tedy otázka, jak je tomu s hodnotami v netriviálních bodech. Tu pro lineární dvojčleny záhy zodpovíme, k důkazu ale budeme potřebovat několik pojmů.

Definice. *Ať je n přirozené číslo. Celé číslo p nazveme prvočíslem v $\mathbb{Z}_n$ právě tehdy, když má kongruence $ab \equiv p \pmod n$, kde a a b jsou celá čísla, pouze taková řešení, že $a \equiv 1 \pmod n$ nebo $b \equiv 1 \pmod n$.*

Věta. *Buď n přirozené číslo. Číslo $p \in \{0, 1, \ldots, n-1\}$ je prvočíslem v $\mathbb{Z}_n$ právě v těchto případech:*

a) $n = 1$ a $p = 0$,
b) $n = 2$ a $p = 1$,
c) $n = 3$ a $p = 2$,
d) $n = 4$ a $p = 3$,
e) $n = 6$ a $p = 5$.

Věta. *Mějme nekonstantní lineární polynom $P(x)$ s celočíselnými koeficienty. Jeho netriviální definiční obor je konečný právě tehdy, když je hodnota dvojčlenu pro nějaké přirozené číslo rovna ± 1 nebo je $P(x) = 4x - 4u - 2$ pro nějaké přirozené u.*

Věta. *Ať je $P(x)$ nekonstantní lineární dvojčlen s celočíselnými koeficienty, nabývající nekonečně mnoha netriviálních hodnot. Jeho všechny hodnoty v netriviálních bodech jsou prvočísla tehdy a jen tehdy, když nastává nějaký z následujících případů:*

a) $P(x) = x + 1$,
b) $P(x) = 2x + 1$,
c) $P(x) = 3x - 1$,
d) $P(x) = 4x - 1$,
e) $P(x) = 6x - 1$.

[2] Pojmy netriviální a triviální definiční obor a hodnota jsem si vymyslel jen pro účely hrátek s prvočíselnými vzorci, nejde tedy o žádné běžné názvy, které bys mohl jen tak používat třeba v MO a očekávat, že je opravující budou znát.

Fungující prvočíselný vzorec

Záhy si už nějaký prvočíselný vzorec předvedeme, napřed ale pár užitečných označení: p_n budeme značit n-té prvočíslo (tedy $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, ...) a $\Pi(n)$ bude počet prvočísel nepřevyšujících n ($\Pi(1) = 0$, $\Pi(2) = 1$, $\Pi(3) = \Pi(4) = 2$, $\Pi(5) = \Pi(6) = 3$, ...). Pak zřejmě platí $\Pi(p_n) = n$. Taky se nám bude hodit, že $p_n < 4^n$, což na přednášce samozřejmě dokážeme.

Nyní tedy přichází slibovaná věta, jež dokonce představuje přímo vzorec pro výpočet n-tého prvočísla (i když je bohužel prakticky zcela nepoužitelná :-().

Věta. *Mějme přirozené číslo n. Označme*

$$f(n) = \left\lfloor \cos^2 \pi \frac{(n-1)! + 1}{n} \right\rfloor \quad \text{a} \quad g(n) = 1 - \left\lfloor \frac{1}{x+1} \right\rfloor .$$

Pak je

$$p_n = 1 + \sum_{m=1}^{4^n} g\left(\left\lfloor \frac{n}{\sum_{k=1}^{m} f(k)} \right\rfloor \right) .$$