Čínská zbytková věta

Lucien Šíma

Abstrakt. Na přednášce si ukážeme Čínskou zbytkovou větou a demonstrujeme její využití na několika olympiádních příkladech.

Pohádka

Generál Koňadra by rád zjistil, kolik má vojáků. Svým bystrým okem odhadne, že jich zřejmě nebude více než 210. Jelikož je líný vojáky počítat, nařídí jim, aby se rozdělili do skupin. Když je rozdělil do skupin po dvou či po třech, zbyl jeden osamocený voják. Když je rozdělil do skupin po pěti či po sedmi, zbyli nerozdělení tři vojáci. Po snadných úvahách mu došlo, kolik vojáků má.

Soustava kongruencí

Označme si x počet vojáků. Generál se vlastně snažil vyřešit následující soustavu kongruencí:

$$\begin{aligned} x &\equiv 1 \pmod 2,\\ x &\equiv 1 \pmod 3,\\ x &\equiv 3 \pmod 5,\\ x &\equiv 3 \pmod 7. \end{aligned}$$

Je možné vždy najít nějaké řešení pro libovolný počet kongruencí? Kolik takových řešení bude? Odpovědí na tyto otázky je následující věta.

Věta. (Čínská zbytková věta) *Nechť $n_1, \dots, n_k \in \mathbb{N}$ jsou po dvou nesoudělná čísla a $r_1, \dots, r_k \in \mathbb{N}$. Pak soustava kongruencí*

$$\begin{aligned} x &\equiv r_1 \pmod{n_1},\\ x &\equiv r_2 \pmod{n_2},\\ &\dots\\ x &\equiv r_k \pmod{n_k}, \end{aligned}$$

má právě jedno řešení x takové, že $0 \le x < n_1 \cdot \ldots \cdot n_k$.

Příklady

Příklad 1. Zjistěte poslední tři číslice čísla 249^{19}.

Příklad 2. Dokažte, že pro každé $n \in \mathbb{N}$ existuje n-tice po sobě jdoucích čísel takových, že pro každé z nich existuje prvočíslo $p \in \mathbb{N}$, že $p^2 \mid n$.

Příklad 3. Dokažte, že pro každé $n \in \mathbb{N}$ existuje n-tice po sobě jdoucích složených čísel.

Příklad 4. Jsou dána čísla $a_1, \ldots, a_n$. Dokažte, že existuje K $\in \mathbb{N}$ takové, že $K \cdot a_i$ je mocnina pro každé $i \in (1, \ldots, n)$.

Příklad 5. Dokažte, že pro každé $n \in \mathbb{N}$ existuje n-tice přirozených čísel takových, že součet libovolného počtu z nich je mocnina.

Příklad 6. Zkonstruujte nekonečnou rostoucí posloupnost a_n takovou, že pro každé $k \in \mathbb{N}$ obsahuje posloupnost $a_n + k$ pouze konečně mnoho prvočísel.
(Česká MO 1997)

Příklad 7. Dokažte, že pro každé $n \in \mathbb{N}$ existuje n-tice po dvou nesoudělných čísel $k_1, \ldots, k_n > 1$ taková, že $k_1 \cdot k_2 \cdot \ldots \cdot k_n - 1$ je součin dvou po sobě jdoucích přirozených čísel. (USAMO 2008)

Příklad 8. Dokažte, že pro každé $n \in \mathbb{N}$ existují $a, b \in \mathbb{N}$ takové, že $n \mid 4a^2 + 9b^2 - 1$.

Příklad 9. Mřížový bod v rovině nazveme *neviditelný*, pokud se na úsečce spojující jej s počátkem nachází další mřížový bod. Dokažte, že pro každé $n \in \mathbb{N}$ existuje čtverec o rozměrech $n \times n$ se stranami rovnoběžnými s osami, jehož n^2 mřížových bodů je neviditelných. (Taiwan 2012)

Příklad 10. Rozhodněte, zda existuje posloupnost, která obsahuje každé přirozené číslo právě jednou, a pro každé k $\in \mathbb{N}$ platí, že $k \mid a_1 + a_2 + \cdots + a_k$.
(Ruská MO 1995)

Příklad 11. Dokažte, že pro každá dvě různá prvočísla p, q platí, že: $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.

Příklad 12. Nechť $f : \mathbb{N} \to \mathbb{N}$ je funkce splňující:

(1) $\mathrm{NSD}(f(m), f(n)) = 1 \Leftrightarrow \mathrm{NSD}(m, n) = 1$,
(2) $n \leq f(n) \leq n + 2017$ pro každé $n \in \mathbb{N}$.

Dokažte, že pro každé $n \in \mathbb{N}$ a prvočíslo p platí, že $p \mid f(n)$ implikuje $p \mid n$.
(TSTST 2012/3)

Návody

1. $1000 = 8 \cdot 125$

2. Zvolte si libovolných n prvočísel.

3. Zvolte si libovolných $2n$ prvočísel.

4. Koukněte se na prvočíselné rozklady čísel v n-tici a doplňte je na mocninu.

5. Uvědomte si, že se jedná o důsledek příkladu 4.

6. Pro každé k zvolte prvočíslo p_k, které bude dělit všechny členy $a_n + k$ až na konečně mnoho.

8. Použijte rozklad n na prvočinitele.

9. Chceme, aby souřadnice všech těchto bodů byly soudělné. Zvolme n^2 prvočísel a nalezněme souřadnice levého dolního bodu $[x, y]$, aby tomu tak bylo.

10. Zkonstruujte jí rekurzivně. Přidávejte členy po dvou.

11. Použijte Malou Fermatovu větu.

12. Hint není. Přece jenom to má být nejtěžší úloha, ne?

Literatura a zdroje

[1] Titu Andrescu, Dorin Andrica: *Number Theory*, Springer, 2009.
[2] David Hruška: *Čínská zbytková věta*, Uhelná Příbram, 2014.
[3] Evan Chen: *The Chinese Remainder Theorem*, *web.evanchen.cc/handouts/CRT/CRT.pdf*