Čínská zbytková věta

David Hruška

Abstrakt. Na přednášce si dokážeme Čínskou zbytkovou větu a vyřešíme s ní několik těžších úloh vyskytujících se například v MO.

Pohádka na dobrou ... vlastně na úvod

Jeden čínský generál pořádal vojenskou přehlídku, na kterou se měl dostavit sám velký císař. Aby se císaři přehlídka líbila, rozhodl se generál, že budou vojáci pochodovat v pravidelném (obdélníkovém) zástupu. Když je ale nechal seřadit do sedmistupu, jeden voják přebýval. Generálovi se zdálo škoda toho vojáka zastřelit, nechal tedy vojáky nastoupit do osmistupu. Bohužel to zase nevyšlo – dva vojáci zbyli. Pro devítistup zbylo vojáků šest. To už se generál rozzlobil a řekl si, že se raději podívá, kolika vojákům to vlastně velí. Nemohl si ale vzpomenout, kam si to číslo napsal, pouze si pamatoval, že jich bylo méně než 500. Poradíte mu?

Soustavy kongruencí

Úmluva. Číslem myslíme přirozené číslo, není-li řečeno jinak. Největší společný dělitel čísel a, b značíme (a, b). *Mocninou* myslíme číslo tvaru n^k pro $k > 1$.

Jistě jste odhalili, že generál z pohádky potřeboval vyřešit soustavu kongruencí

$$\begin{aligned} x &\equiv 1 \pmod 7, \\ x &\equiv 2 \pmod 8, \\ x &\equiv 6 \pmod 9. \end{aligned}$$

Občas se to může hodit i nám, proto se podíváme na to, kdy a jak je to možné.

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

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

má právě jedno řešení x takové, že $0 \leq x < n_1 \cdot n_2 \cdots n_k$.

Poznámka. (O soudělnosti modulů) Bez podmínky o nesoudělnosti je soustava řešitelná právě tehdy, když pro každá $1 \leq i, j \leq n$ platí $r_i \equiv r_j \pmod{(n_i, n_j)}$.

Cvičení. Předchozí věta nám zaručuje existenci nějakého řešení. Jak jej ale najít? Dořešte úlohu z pohádky.

Úlohy

Úloha 1. Je dáno přirozené číslo n. Ukažte, že existuje n po sobě jdoucích čísel takových, že každé z nich je dělitelné alespoň dvěma různými prvočísly.

Úloha 2. Rozhodněte, zda existuje nekonečná množina $K \subset \mathbb{N}$ taková, že kdykoliv p je prvočíslo a $k \in K$, pak $p^2 + k$ je složené.

Úloha 3. Jsou dána čísla $a_1, \ldots, a_n$. Dokažte, že existuje $M \in \mathbb{N}$ takové, že pro každé $1 \leq i \leq n$ je $M \cdot a_i$ mocnina.

Úloha 4. Dokažte, že existuje 2014 po sobě jdoucích čísel, z nichž žádné není mocninou.

Úloha 5. Dokažte, že existuje číslo n takové, že pro libovolné celé číslo k nemá číslo $k^2 + k + n$ žádného prvočíselného dělitele menšího než 2008. (ČPS 2008)

Úloha 6. Rozhodněte, zda existuje posloupnost obsahující každé přirozené číslo právě jednou taková, aby součet jejích prvních k členů byl dělitelný k, kdykoliv $k \in \mathbb{N}$. (Ruská MO 1995)

Úloha 7. Dokažte, že každý zbytek modulo liché $n \geq 3$ lze vyjádřit jako součet nebo rozdíl dvou zbytků modulo n nesoudělných s n.

Úloha 8. Ukažte, že existuje nekonečná rostoucí posloupnost přirozených čísel a_n taková, že kdykoliv $k \geq 0$, pak posloupnost $b_n = k + a_n$ obsahuje jen konečně mnoho prvočísel. (Česká MO 1997)

Úloha 9. Nechť $n \in \mathbb{N}$ a $a_1, \ldots, a_k$ $(k \geq 2)$ jsou navzájem různá celá čísla z množiny $\{1, \ldots, n\}$ taková, že pro každé $i = 1, \ldots, k-1$ je číslo $a_i(a_{i+1} - 1)$ dělitelné n. Dokažte, že číslo $a_k(a_1 - 1)$ není dělitelné n. (IMO 2009)

Úloha 10. Mřížový bod v rovině nazveme *neviditelným*, pokud úsečka, která jej spojuje s počátkem, obsahuje nějaký další mřížový bod. Dokažte, že existuje čtverec se stranami rovnoběžnými s osami a rozměry 100×100 tak, že všechny jeho mřížové body jsou neviditelné.

Úloha 11. Najděte všechna přirozená n taková, že existují čísla $b_1, \ldots, b_n$, která nejsou všechna stejná, tak, že pro každé k je $(b_1 + k)(b_2 + k) \cdots (b_n + k)$ mocnina.

Úloha 12. Nechť $P(x)$ je polynom s celočíselnými koeficienty. Čísla $a_1, \ldots, a_n$ mají tu vlastnost, že pro každé $x \in \mathbb{N}$ je existuje $i \in \{1, \ldots, n\}$ tak, že $a_i \mid P(x)$. Dokažte,

že pak existuje $j \in \{1, \ldots, n\}$ takové, že pro každé $x \in \mathbb{N}$ platí $a_j \mid P(x)$.
(St. Petersburg MO)

Úloha 13. Ukažte, že existuje přirozené číslo k takové, že $k \cdot 2^n + 1$ je složené pro každé $n \in \mathbb{N}$.

Literatura a zdroje

[1] Michal „Kenny“ Rolínek: *Důkazové metody v teorii čísel*. Domaslav, 2010.
[2] Titu Andrescu, Dorin Andrica: *Number Theory*. Springer, 2009.
[3] *http://www.problems.ru*