Čínská zbytková věta

Matěj Doležálek

Abstrakt. Ukážeme si, jak se koukat na úlohy modulo více různých čísel naráz, jak tyto pohledy skládat dohromady, a hlavně k čemu je to všechno dobré. Dokážeme Čínskou zbytkovou větu a procvičíme dva hlavní způsoby jejího použití: vyrábění čísel s hromadou dobrých vlastností v konstrukčních úlohách a lámání problému na více menších kousků v důkazových úlohách.

Definice. Celá čísla a, b nazveme nesoudělná, pokud mezi přirozenými čísly nemají jiného společného dělitele než 1.

Tvrzení. (Bézoutova identita) *Jsou-li a, b nesoudělná celá čísla, pak existují celá x, y splňující $ax + by = 1$.*

Důkaz. Rozšířený Eukleidův algoritmus.

Tvrzení. *Pokud $a \mid bc$ a zároveň jsou a, c nesoudělná, pak už i $a \mid b$.*

Tvrzení. *Nechť jsou a, b nesoudělná a platí $a \mid c$, $b \mid c$. Potom platí i $ab \mid c$.*

Definice. Říkáme, že a, b jsou *kongruentní modulo m*, pokud $m \mid a - b$. Tento vztah značíme $a \equiv b \pmod{m}$.

Jinak řečeno: a, b jsou kongruentní modulo m, pokud po dělení číslem m dávají stejný zbytek.

Cvičení. (speciální případ zbytkovky) Jsou-li $m_1, \ldots, m_k$ po dvou nesoudělná a platí $x \equiv a \pmod{m_i}$ pro $i = 1, \ldots, k$, pak už i $x \equiv a \pmod{M}$, kde $M = m_1 \cdots m_k$.

Věta. (Čínská zbytková) *Buďte dána po dvou nesoudělná přirozená $m_1, \ldots, m_k$ a libovolná celá čísla $a_1, \ldots, a_k$. Potom existuje celé číslo x splňující*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

a všechna taková x jsou si navzájem kongruentní modulo $M = m_1 \cdots m_k$.

Cvičení. Mějme celá čísla $b_1, \ldots, b_k$ splňující $b_i \equiv \left(\frac{M}{m_i}\right)^{-1} \pmod{m_i}$ pro každé i. Potom pro $c_i = \frac{M}{m_i} \cdot b_i$ platí $c_i \equiv 1 \pmod{m_i}$ a $c_i \equiv 0 \pmod{m_j}$ pro $j \neq i$. Následně lze v Čínské zbytkové větě spočíst x jako $x = a_1c_1 + \cdots + a_kc_k$.

Příklad. Jan Žižka si chtěl po velké bitvě, do které vyslal 1200 bojovníků, rychle spočítat ztráty. Nechal si proto přeživší bojovníky nastoupit postupně po třech, pěti, sedmi a jedenácti. Nejprve mu zbyli dva bojovníci, poté dvakrát po třech bojovnících a nakonec jich zbylo deset. Kolik bojovníků tedy přežilo?

Použití Čínské zbytkové věty jde rozlišit na dva hlavní přístupy. V jednom si pro nějaká čísla poručíme vlastnosti, které jsou v úloze užitečné, a zbytkovka zařídí jejich existenci. V druhém si vezmeme k srdci to, že (s jistými omezeními) kongruence platí modulo M, právě když platí modulo jednotlivá m_i. Formálně sice v obou případech děláme totéž, ale jedná o dvě různé strategie, kterými lze úlohy řešit.

Čínská zbytková věta umožňuje celočíselné proměnné poručit libovolné množství modulárních podmínek, dokud jsou příslušná modula vzájemně nesoudělná. Tu a tam se hodí umět tímto způsobem vyčarovat nejen tak ledajaké číslo, ale dokonce prvočíslo. K tomu lze užít následující kanón – poznamenejme, že jeho důkaz daleko přesahuje možnosti běžných olympiádních nástrojů.

Věta. (Dirichletova) *Nechť jsou a, n nesoudělná přirozená čísla. Potom existuje nekonečně mnoho prvočísel p splňujících $p \equiv a \pmod{n}$.*

Obecněji se Čínská zbytková věta často používá kombinováním s nějakým dalším modulárně zabarveným tvrzením. Hodit se proto může třeba následující:

Věta. (malá Fermatova) *Mějme celé číslo a a prvočíslo $p \nmid a$. Potom $a^{p-1} \equiv 1 \pmod{p}$.*

Konstrukce šikovných čísel

Úloha 1. Dokažte, že pro každé $n \in \mathbb{N}$ existuje n-tice po sobě jdoucích čísel, z nichž každé je dělitelné čtvercem nějakého přirozeného čísla většího než 1.

Úloha 2. Dokažte, že pro každé přirozené n existuje n po sobě jdoucích přirozených čísel, z nichž žádné není prvočíselná mocnina.

Úloha 3. Uvažujme v rovině mřížové body (a, b) s celočíselnými souřadnicemi. Bod (a, b) je *viditelný*, pokud jsou a, b nesoudělná celá čísla. Dokažte, že pro libovolné $n \in \mathbb{N}$ existuje čtverec $n \times n$ mřížových bodů, z nichž žádný není viditelný.

Úloha 4. Dokažte, že pro každé přirozené číslo k lze zvolit $2k$ navzájem různých přirozených čísel $a_1, \ldots, a_k, b_1, \ldots, b_k$ takových, že zlomky

$$\frac{a_1}{b_1}, \quad \frac{a_2}{b_2}, \quad \ldots, \quad \frac{a_k}{b_k}$$

jsou všechny v základním tvaru a tvoří aritmetickou posloupnost.

Úloha 5. Jsou dána celá čísla a, b taková, že pro všechna přirozená n platí

$$b^n + n \mid a^n + n.$$

Dokažte, že $a = b$. (ISL 2005 N6)

Úloha 6. Rozhodněte, zda lze přirozená čísla seřadit do posloupnosti $a_1, a_2, \ldots$ (přičemž každé přirozené číslo se vyskytne právě jednou) tak, aby pro každé přirozené n platilo $n \mid a_1 + \cdots + a_n$.

Úloha 7. Najděte všechny trojice přirozených čísel (a, b, c) takové, že pro každé přirozené n, které nemá žádného prvočíselného dělitele menšího než 2014, platí

$$n + c \mid a^n + b^n + n.$$

(ELMO SL 2014)

Úloha 8. Budiž $f : \mathbb{N} \to \mathbb{N}$ funkce splňující pro každá $a, b \in \mathbb{N}$:

(i) $f(a)$, $f(b)$ jsou nesoudělná, právě když a, b jsou nesoudělná.
(ii) $a \leq f(a) \leq a + 2012$.

Dokažte, že když prvočíslo p dělí $f(n)$, pak už i $p \mid n$. (USA TSTST 2012)

Úloha 9. Tabulka 2018×2018 je vydlážděna dominy 2×1. Dokažte, že lze do políček vepsat přirozená čísla tak, že:

(i) Součet dvou čísel na každém dominu je vždy stejný.
(ii) Libovolná dvě čísla, jejichž políčka sousedí stranou, jsou nesoudělná, právě pokud leží na stejném dominu. (PraSe 37–4p–8)

Rozkládání a skládání modul

Úloha 10. Jsou dána dvě různá kladná prvočísla p, q. Dokažte, že $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.

Úloha 11. Dokažte, že $4a^2 + 9b^2 \equiv 1 \pmod{n}$ má pro libovolné přirozené n řešení.

Úloha 12. Je dáno přirozené číslo n. Budiž A množina těch čísel $a \in \{1, 2, \ldots, n\}$, která splňují $a^2 \equiv a \pmod{n}$. Dokažte, že počet prvků A je mocnina dvojky. (PraSe 40–3s–1)

Úloha 13. Nechť $\varphi(n)$ značí počet čísel z množiny $\{1, \ldots, n\}$, která jsou nesoudělná s n. Vyjádřete $\varphi(n)$ pro n s prvočíselným rozkladem $p_1^{k_1} \cdots p_r^{k_r}$.

Úloha 14. Dokažte, že pro každé $n \in \mathbb{N}$ existuje n-tice po dvou nesoudělných čísel $k_1, \ldots, k_n > 1$ taková, že $k_1 \cdot k_2 \cdots k_n - 1$ je součin dvou po sobě jdoucích přirozených čísel. (USAMO 2008)

Úloha 15. Rozhodněte, zda existuje přirozené n takové, že pro libovolné celé číslo x nemá $x^2 + x + n$ žádného prvočíselného dělitele menšího než 2021.

Úloha 16. Jsou dána přirozená čísla $a > b > c \geq 3$ splňující

$$a \mid bc + b + c, \qquad b \mid ca + c + a, \qquad c \mid ab + a + b.$$

Dokažte, že alespoň jedno z a, b, c je složené číslo.

Úloha 17. Jsou dána přirozená čísla $n, k \geq 2$ a k-tice po dvou různých čísel $a_1, \ldots, a_k$ z množiny $\{1, 2, \ldots, n\}$ taková, že $n \mid a_i(a_{i+1} - 1)$ pro $i = 1, \ldots, k-1$. Dokažte, že $n \nmid a_k(a_1 - 1)$. (IMO 2009/1)

Úloha 18. Pro konečnou množinu X přirozených čísel nechť $S(X)$ značí součet jejích prvků a $P(X)$ jejich součin. Dále uvažujme dvě konečné množiny přirozených čísel A, B takové, že $|A| = |B|$, $P(A) = P(B)$, ale $S(A) \neq S(B)$. Pokud pro každé $n \in A \cup B$ a jeho prvočíselného dělitele p platí $p^{36} \mid n$, ale $p^{37} \nmid n$, dokažte, že $|S(A) - S(B)| > 10^6$. (NIMO 2013)

Návody

1. Předepiš každému číslu čtvercového dělitele.

2. Předepiš každému číslu dva prvočíselné dělitele.

3. Poruč si pro každý bod hledaného čtverce prvočíslo, kterým mají být souřadnice soudělné.

4. Vezmi zkrácenou posloupnost $\frac{x+1}{N}, \ldots, \frac{x+k}{N}$ pro vhodná x, N. Jednotlivá b_i odliš zkrácenými prvočísly, a_i pak už odlišíš snadno.

5. Vyrob pro $a - b$ hodně prvočíselných dělitelů. Modula p a $p - 1$ jsou nesoudělná!

6. Přidávej členy po dvou – jeden zvol libovolně a jeden urči.

7. S pomocí kanónu ukaž, že $a + b - c$ má hodně prvočíselných dělitelů. Navol si zbytky v různých modulech dle libosti nejprve pro p, potom pro n.

8. Zkus nejdřív zapomenout na n, p a pomocí zbytkovky zkonstruovat takové x, že $f(x) = x$. Potom do výrobního procesu přidej $x \equiv 0 \pmod{p}$, $x \equiv 1 \pmod{n}$.

9. Vyplňuj na jednotlivá domina dvojice čísel $S \pm x_i$ podle šachovnicového obarvení. Kdekoliv má dvojice čísel být soudělná, zvol si na to zvláštní prvočíslo.

10. Podívej se zvlášť mod p a mod q.

11. Vyřeš modulo prvočíselné mocniny. Mocniny 2 a 3 jsou trochu výjimečné, ostatní jsou snadné.

12. Nejprve vyřeš prvočíselné mocniny.

13. Nejprve vyřeš prvočíselné mocniny.

14. Jen se chce, aby $x^2 + x + 1$ umělo mít hodně prvočíselných dělitelů. Pouprav důkaz existence nekonečně mnoha prvočísel.

15. Polynom $x^2 + x$ neumí modulo p nabývat všech možných hodnot – podle toho navol n mod p pro $p < 2021$.

16. Slož do modula abc.

17. Z předpokladu sporu dokaž, že buďto $a_i \equiv 0 \pmod{p^r}$ pro všechna i, nebo $\equiv 1$ pro všechna i.

18. Součin prvočísel p, pro něž $p - 1 \mid 36$. Když se místo malého Fermata použije Euler, lze odhad vylepšit až na asi $6 \cdot 10^7$.

Literatura a zdroje

[1] Lucien Šíma: *Čínská zbytková věta*, Meziměstí, 2017.
[2] Evan Chen: *The Chinese Remainder Theorem*, *https://web.evanchen.cc/handouts/CRT/CRT.pdf*.
[3] Fíla Čermák, Matěj Doležálek: *Teorie nejen čísel*, seriál MKS, 3. díl, 40. ročník.