Důkazové metody v teorii čísel

Michal „Kenny“ Rolínek

Abstrakt. Příspěvek nejen ukazuje klasická tvrzení z elementární teorie čísel, ale především ukazuje obvyklé postupy při jejich používání, a to převážně na úlohách olympiádního typu. Dohromady obsahuje 45 příkladů, z nichž 6 je přímo z mezinárodních olympiád a mnoho dalších je převzato z prestižních domácích či zahraničních soutěží.

Teorie čísel je patrně nejrozsáhlejší a též i nejobtížnější oblast olympiádnické matematiky. Získat v ní orientaci je o mnoho náročnější než například u geometrie, neboť mnoho běžných úvah působí v první chvíli velmi nezvykle. Tato přednáška má za cíl počáteční nedůvěru překonat a pomoci získat vhled i do temných zákoutí této královské disciplíny.

Úmluva. Všechny proměnné v dalším textu jsou z oboru celých čísel, nebude-li řečeno jinak.

Základy dělitelnosti

Tvrzení. (Zásadní!) *Pro dělitelnost zavádíme symbol $a \mid b$, který čteme „a dělí b“. Platí pro něj následující tvrzení.*

(i) *Pokud je p prvočíslo, pak platí implikace $p \mid ab \Rightarrow p \mid a \vee p \mid b$.*
(ii) *Pokud $d \mid a, d \mid b$, pak $d \mid ka + lb$.*
(iii) *Pokud $a \mid b$, pak $|a| \leq |b|$ (často dokonce $2|a| \leq |b|$ atd.).*

Tvrzení. *Nechť a, b jsou celá čísla. Jejich největší společný dělitel d značíme (a, b) a platí, že d je nejmenší nezáporné číslo, které lze zapsat ve tvaru $ka + lb$, kde k a l jsou celá čísla. Též platí $(a - b, b) = (a, b)$, díky čemuž lze (a, b) snadno vypočítat (tento postup se nazývá Euklidův algoritmus).*

Definice. Nejmenší společný násobek přirozených čísel a, b budeme značit $[a, b]$.

Definice. Čísla a, b nazveme nesoudělná, pokud $(a, b) = 1$.

Příklad 1. Čísla a, b jsou nesoudělná. Rozhodněte, co víte o soudělnosti následujících dvojic čísel.

(i) $a + b, ab$
(ii) $a^2 + b^2, ab$
(iii) $a + b, a - b$
(iv) $a^3, (a + 1)^5$

Klíčová slova. Malá Fermatova věta, Čínská zbytková věta, kongruence, dělitelnost, p-valuace, řád prvku, teorie čísel

Příklad 2. Nalezněte všechna přirozená čísla, kterými lze krátit některý ze zlomků tvaru

$$\frac{3p-q}{5p+2q},$$

kde p a q jsou nesoudělná celá čísla. (Školní kolo MO 2008)

Příklad 3. Ukažte, že zlomek

$$\frac{21n+4}{14n+3}$$

je v základním tvaru pro každé $n \in \mathbb{N}$. (IMO 1959)

Příklad 4. Určete všechna celá kladná čísla m, n taková, že n dělí $2m-1$ a zároveň m dělí $2n-1$. (Krajské kolo MO 2009)

Příklad 5. Pro přirozená čísla a, b, c platí

$$a+b+c \mid abc.$$

Ukažte, že $a+b+c$ je složené číslo.

Příklad 6. Pro která celá čísla n je výraz

$$\frac{n^3-3}{n-3}$$

celočíselný. (Náboj 2007)

Příklad 7. Zjistěte, pro která přirozená čísla a, b je hodnota podílu

$$\frac{b^2+ab+a+b-1}{a^2+ab+1}$$

rovna celému číslu. (Celostátní kolo MO 2008)

Příklad 8. Ukažte, že pokud je p takové liché prvočíslo, že i $2p+1$ je prvočíslo, pak existují právě čtyři přirozená čísla k taková, že

$$2p+k \mid 2p+k^2.$$

(Variace na celostátní kolo MO 2008)

Příklad 9. Najděte všechny dvojice přirozených čísel x, y takové, že

$$\frac{xy^2}{x+y}$$

je prvočíslo. (Domácí kolo MO 2008)

Rozklady, rozklady, rozklady!

Přirozená čísla mají z hlediska násobení velmi zajímavou strukturu. Všechna jsou postavena ze základních kamenů, kterým se říká prvočísla. Při řešení úloh bývá často klíčové si prvočíselné rozklady představovat a umět s nimi pracovat. Například budeme-li dokazovat, že $a = b$, často bude výhodnější ukázat, že mají ve svých rozkladech všechna prvočísla ve stejných mocninách. Podobně pak můžeme ukazovat, že $a \mid b$ atd.

Tvrzení. *Každé přirozené číslo lze jednoznačně rozložit na součin prvočísel nebo jejich mocnin.*

Definice. Buď n přirozené číslo. Pak je pro každé prvočíslo p jednoznačně určený exponent v prvočíselném rozkladu čísla n. Tento exponent budeme označovat $v_p(n)$ a říkat mu p-valuace čísla n. Pokud $(p, n) = 1$ je $v_p(n) = 0$.

Tvrzení. *Pro libovolná přirozená čísla a, b platí*

(i) $v_p(ab) = v_p(a) + v_p(b)$
(ii) $v_p(a + b) \geq \min\{v_p(a), v_p(b)\}$
(iii) *Pokud* $v_p(a) \neq v_p(b)$, *pak dokonce* $v_p(a + b) = \min\{v_p(a), v_p(b)\}$.
(iv) $v_p((a, b)) = \min\{v_p(a), v_p(b)\}$
(v) $v_p([a, b]) = \max\{v_p(a), v_p(b)\}$

Příklad 10. Ukažte, že platí $(a, b) \cdot [a, b] = ab$.

Příklad 11. Dokažte, že pro libovolná přirozená čísla a, b, c platí

$$\frac{[a, b, c]^2}{[a, b] \cdot [b, c] \cdot [c, a]} = \frac{(a, b, c)^2}{(a, b) \cdot (b, c) \cdot (c, a)}.$$

(USAMO 1972)

Příklad 12. Přirozená čísla a, b, c, d splňují $ab = cd$. Ukažte, že platí

$$(a, c) \cdot (a, d) = a \cdot (a, b, c, d).$$

(Polská MO, Mecz 2009)

Příklad 13. Nechť $a_1, a_2, \ldots, a_k, b_1, b_2, \ldots b_k$ jsou přirozená čísla, která splňují $(a_i, b_i) = 1$ pro každé $i \in \{1, 2, \ldots, k\}$. Dále buď $m = [b_1, b_2, \ldots, b_k]$. Ukažte, že platí

$$\left(\frac{a_1 m}{b_1}, \frac{a_2 m}{b_2}, \ldots, \frac{a_k m}{b_k}\right) = (a_1, a_2, \ldots, a_k).$$

(IMO shortlist 1974)

Příklad 14. Na tabuli jsou napsána přirozená čísla $a_1, a_2, \ldots a_n$. V jednom kroku vybereme dvě čísla a_i, a_j taková, že $i < j$ a po řadě je nahradíme čísly

$(a_i, a_j), [a_i, a_j]$. Ukažte, že po konečném počtu kroků dospějeme do stavu, který takto už nepůjde změnit. (Putnam 2009)

Finta na faktoriály

Nejlépe využijeme vlastnosti p-valuací při manipulaci s dělitelností faktoriálů a kombinačních čísel. Většinu práce za nás odvede následující tvrzení.

Tvrzení. *Buď n přirozené číslo. Pak platí*

$$v_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots = \frac{n - s_p(n)}{p-1},$$

kde $s_p(n)$ je ciferný součet čísla n zapsaného v soustavě o základu p.

Příklad 15. Určete kolika nulami končí číslo 2010!.

Příklad 16. Ukažte, že $n!$ není dělitelné 2^n pro žádné přirozené číslo n.

Příklad 17. Dokažte, že platí

$$v_p\left(\binom{m}{n}\right) = \frac{v_p(n) + v_p(m-n) - v_p(m)}{p-1}.$$

Příklad 18. Buď p libovolné prvočíslo. Najděte všechna přirozená čísla n taková, že p dělí $\binom{n}{k}$ pro každé $k \in \{1, 2, \ldots, n-1\}$. (PraSe 26-Myšmaš)

Příklad 19. Pro každé přirozené číslo platí

$$(n+1) \cdot \left[\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{n}\right] = [1, 2, \ldots, n+1].$$

Dokažte. (Rumunsko TST 1990)

Příklad 20. Nalezněte nejvyšší mocninu dvojky, která dělí

$$\binom{2^{n+1}}{2^n} - \binom{2^n}{2^{n-1}}.$$

(IMO shortlist 2007)

Zbytky a jejich chování

Definice. Skutečnost, že $p \mid a - b$ budeme značit $a \equiv b \pmod{p}$ a říkat a je kongruentní s b modulo p.

Tvrzení. *Kongruence o stejném modulu lze sčítat, odečítat a násobit.*

Definice. Buď p prvočíslo. Množinu $\{0, 1, \ldots, p-1\}$ budeme nazývat úplnou sadou zbytků.

Tvrzení. *Nenulovým násobkem úplné sady zbytků je úplná sada zbytků. Násobkem máme na mysli množinu* $\{0, k, 2k, \ldots, k(p-1)\}$.

Tvrzení. („Zbytky lze dělit!“) *Buď p prvočíslo a $a \in \mathbb{Z}$ takové, že $(a, p) = 1$. Pak právě jedno existuje $b \in \mathbb{Z}, 0 < b < p$, že $ab \equiv 1 \pmod{p}$.*

Příklad 21. Nalezněte všechny dvojice prvočísel p, q takové, že $p + q = (p - q)^3$. (Ruská MO 2001)

Příklad 22. Ukažte, že každé prvočíslo má nekonečně mnoho násobků, jejichž posledních 10 cifer je různých.

Tvrzení. (Čínská zbytková věta) *Nechť $m_1, m_2, \ldots m_k$ jsou po dvou nesoudělná čísla. Pak soustava kongruencí*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_k \pmod{m_k} \end{aligned}$$

má právě jedno řešení modulo $m_1 m_2 \ldots m_k$.

Příklad 23. 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.

Příklad 24. Nechť n je kladné celé číslo 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)

Příklad 25. Je dáno přirozené číslo n. Ukažte, že existuje n po sobě jdoucích čísel takových, že každé z nich je dělitelné alespoň dvěma různými prvočísly.

Příklad 26. Dokažte, že existuje přirozené číslo n takové, že pro libovolné celé číslo k nemá číslo $k^2 + k + n$ žádného prvočíselného dělitele menšího než 2008. (Mezinárodní střetnutí česko-slovensko-polské 2008)

Příklad 27. 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)

Příklad 28. 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)

Příklad 29. Ukažte, že existuje přirozené číslo k takové, že $k \cdot 2^n + 1$ je složené pro každé $n \in \mathbb{N}$.

Umocňování a Malá Fermatova věta

Nejtěžší úlohy z teorie čísel jsou ty, v nichž se dělitelnost míchá s umocňováním a sčítáním. Krom trošky potřebné teorie o tom, jak se čísla při umocňování chovají, je potřeba hlavně celková orientace a nadhled. Ukažme si, oč jde.

Tvrzení. (Malá Fermatova) *Buď p prvočíslo a n číslo s ním nesoudělné. Pak* $n^{p-1} \equiv 1 \pmod{p}$.

Tvrzení. *Buď p prvočíslo a n číslo s ním nesoudělné. Pak existuje nejmenší přirozené číslo r takové, že* $n^r \equiv 1 \pmod{p}$. *Všechna ostatní čísla s touto vlastností jsou jeho násobky. Číslo r pak budeme nazývat řádem prvku n modulo p a značit* $r = ord_p(n)$.

Tvrzení. *Pokud* $n^a \equiv 1 \pmod{p}$ *a zároveň* $n^b \equiv 1 \pmod{p}$, *pak též* $n^{(a,b)} \equiv 1 \pmod{p}$.

Příklad 30. Ukažte, že kdykoliv je p prvočíslo a a, b přirozená čísla, pak $p \mid ab^p - ba^p$.

Příklad 31. Ukažte, že pro různá prvočísla p, q platí

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}.$$

Příklad 32. Buď $p > 3$ prvočíslo. Pak ukažte, že

$$p \mid 2^{p-2} + 3^{p-2} + 6^{p-2} - 1.$$

(IMO 2005)

Příklad 33. Buď p prvočíslo tvaru $4k + 3$. Platí, že $p \mid a^2 + b^2$, kde $a, b \in \mathbb{N}$. Ukažte, že pak i $p \mid a, p \mid b$.

Příklad 34. Buď p prvočíslo tvaru $3k + 2$. Platí, že $p \mid a^2 + ab + b^2$, kde $a, b \in \mathbb{N}$. Ukažte, že pak i $p \mid a, p \mid b$.

Příklad 35. Ukažte, že

$$(n^a + 1, n^b + 1) \mid n^{(a,b)} + 1,$$

kde a, b, n jsou přirozená čísla.

Příklad 36. Buď p prvočíslo a q přirozený dělitel čísla $2^p - 1$. Ukažte, že $p \mid q - 1$.

Příklad 37. Buď p prvočíslo a n, q přirozená čísla taková, že $q \mid (n+1)^p - n^p$. Ukažte, že $p \mid q - 1$. (Výběrko 2007)

Příklad 38. Prvočíslo p dělí n-té Fermatovo číslo $2^{2^n}+1$. Ukažte, že $2^{n+1} \mid p-1$.

Příklad 39. Najděte všechny dvojice prvočísel p, q takové, že

$$p^2 + 1 \mid 2003^q + 1,$$
$$q^2 + 1 \mid 2003^p + 1.$$

(Gabriel Dospinescu)

Příklad 40. Nalezněte všechny trojice prvočísel p, q, r splňující soustavu dělitelností

$$p \mid q^r + 1,\ q \mid r^p + 1,\ r \mid p^q + 1.$$

(USA TST 2003)

Závěrečný náklep!

Nejobvyklejší metody jsou již probrány a nastal čas řešit ty nejobtížnější úlohy z olympiádní teorie čísel. Držte si klobouky!

Tvrzení. *Buď p liché prvočíslo a A, B přirozená čísla, která nejsou dělitelná p, a platí $p \mid A - B$. Pak pro každé přirozené n platí*

$$v_p(A^n - B^n) = v_p(n) + v_p(A - B).$$

Příklad 41. Buďte a, b, c přirozená čísla taková, že $c \mid a^c - b^c$. Ukažte, že pak $c \mid \frac{a^c - b^c}{a-b}$. (AMM)

Příklad 42. Ukažte, že pro každé přirozené n je číslo $n!$ dělitelem čísla

$$(2^n - 2^0)(2^n - 2^1)\dots(2^n - 2^{n-1}).$$

Příklad 43. Pro přirozená čísla a, b platí, že $a^n + n \mid b^n + n$ pro každé $n \in \mathbb{N}$. Ukažte, že $a = b$. (IMO shortlist 2005)

Příklad 44. Najděte všechna přirozená čísla, pro něž $n^2 \mid 2^n + 1$. (IMO 1990)

Příklad 45. Nechť p je prvočíslo. Dokažte, že existuje prvočíslo q takové, že pro žádné přirozené číslo n není $n^p - p$ dělitelné q. (IMO 2003)

Literatura a zdroje

[1] Titu Andreescu, Gabriel Dospinescu, *Problems from the Book*, XYZ Press, Texas, 2008.
[2] Razvan Gelca, Titu Andreescu, *Putnam and Beyond*, Springer, New York, 2007.
[3] Titu Andreescu, Dorin Andrica, Zuming Feng, *104 Number Theory Problems from USA IMO Training*, BirkHauser, Boston, 2007.
[4] J. Herman, R. Kučera, J. Šimša, *Metody řešení matematických úloh I*, MU, Brno, 2001.
[5] *http://www.mathlinks.ro*