Základní věty z teorie čísel

Martin Čech

Abstrakt. Příspěvek obsahuje základní poznatky z teorie čísel včetně Malé Fermatovy, Wilsonovy a Eulerovy věty. Dále obsahuje několik úloh na jejich používání v praxi.

Úmluva. Nebude-li řečeno jinak, všechny níže uvedené proměnné jsou z oboru celých čísel.

Na přednášce si ukážeme základní metody používané při řešení úloh z teorie čísel, které se vyskytují v různých olympiádách a dalších matematických soutěžích. Neobejdeme se však bez nejnutnější teorie.

Trocha teorie

Definice. Řekneme, že číslo a je *dělitelem* čísla b, pokud existuje číslo k takové, že platí $k \cdot a = b$. Tuto skutečnost zapisujeme $a \mid b$.

Cvičení. Rozmyslete si, že pro nenulová čísla a, b, c, d platí:

(1) $1 \mid a$,
(2) $a \mid a$,
(3) $a \mid 0$,
(4) pokud $a \mid b$ a $b \mid c$, potom $a \mid c$,
(5) pokud $a \mid b$ a $a \mid c$, potom $a \mid kb + lc$ pro libovolná čísla k, l,
(6) pokud $a \mid b$ a $c \mid d$, potom $ac \mid bd$,
(7) pokud $a \mid b$, potom $|a| \leq |b|$ (speciálně pokud navíc $b \mid a$, potom $|a| = |b|$).

Tvrzení. (Dělení se zbytkem) *Pro každá dvě čísla m a n existuje právě jedna dvojice nezáporných celých čísel k a r takových, že $r < m$ a $n = km + r$. Říkáme, že číslo n dává po dělení m zbytek r.*

Definice. (Kongruence) Říkáme, že čísla a, b jsou *kongruentní modulo d*, pokud dávají po dělení číslem d stejný zbytek (tj. pokud $d \mid a - b$). Tuto skutečnost zapisujeme $a \equiv b \pmod{d}$.

Cvičení. Rozmyslete si, že platí následující základní vlastnosti kongruencí:

(1) $a \equiv 0 \pmod{m}$ právě tehdy, když $m \mid a$,

(2) pokud $a \equiv b \pmod m$, potom $a + k \equiv b + k \pmod m$ a $ak \equiv bk \pmod m$ pro libovolné k,
(3) pokud $a \equiv b \pmod m$ a $b \equiv c \pmod m$, potom $a \equiv c \pmod m$,
(4) pokud $a \equiv b \pmod m$ a $c \equiv d \pmod m$, potom $a + c \equiv b + d \pmod m$ a $ac \equiv bd \pmod m$.

Definice. Přirozená čísla, která mají právě dva kladné dělitele, nazýváme *prvočísla.*

Definice. Je-li p prvočíslo, množinu čísel $0, 1, ..., p-1$ nazýváme *množinou zbytků modulo p.*

Prvočísla hrají zásadní roli v teorii čísel, hlavně díky následujícím tvrzením:

Tvrzení. *Jestliže $p \mid ab$, kde p je prvočíslo, potom $p \mid a$ nebo $p \mid b$.*

Tvrzení. (Prvočíselný rozklad) *Každé přirozené číslo lze jednoznačně až na pořadí činitelů vyjádřit jako součin prvočísel.*

Tvrzení. *Prvočísel je nekonečně mnoho.*

Před slibovanými větami přichází důležité tvrzení, které bude hrát zásadní roli v jejich důkazech.

Tvrzení. (Stěžejní) *Je-li p prvočíslo a a číslo, které není dělitelné p, potom*

$$\{a \pmod p, 2a \pmod p, ..., (p-1)a \pmod p, pa \pmod p\},$$

kde zápis $b \pmod p$ znamená zbytek b po dělení p, je množinou zbytků modulo p.

Předchozí tvrzení říká, že když počítáme modulo prvočíslo p, můžeme dělit libovolným nenulovým číslem (kde nenulovým myslíme nenulovým modulo p, tedy nedělitelným p).

Nyní přicházejí slibované věty:

Věta. (Malá Fermatova věta) *Je-li p prvočíslo a a číslo nedělitelné p, potom*

$$a^{p-1} \equiv 1 \pmod p.$$

Pro její důkaz stačí vynásobit všech $p-1$ kongruencí z předchozího tvrzení.

Věta. (Wilsonova věta) *Číslo p je prvočíslo právě tehdy, když*

$$1 \cdot 2 \cdots (p-2) \cdot (p-1) = (p-1)! \equiv -1 \pmod p.$$

Vyzbrojeni těmito větami se už můžeme vrhnout na řešení úloh!

Úlohy

Úloha 1. Je-li p prvočíslo, dokažte, že $p \mid ab^p - ba^p$ pro všechna čísla a, b.

Úloha 2. Buď p prvočíslo a n takové číslo, že $p \mid 4n^2+1$. Dokažte, že potom $p \equiv 1 \pmod 4$.

Výsledek předchozí úlohy se dá použít k dokázání existence nekonečně mnoha prvočísel tvaru $4k+1$. Stačí pro spor předpokládat jejich konečné množství a vzít za n jejich součin.

Úloha 3. Buďte $A = \{a_1, a_2, \ldots, a_{101}\}$ a $B = \{b_1, b_2, \ldots, b_{101}\}$ množiny všech přirozených čísel od 0 do 100 (v libovolném pořadí). Může i $C = \{a_1 b_1 \pmod{101}, a_2 b_2 \pmod{101}, \ldots, a_{101} b_{101} \pmod{101}\}$ obsahovat všechna přirozená čísla od 0 do 100?

Úloha 4. Mějme danou posloupnost $a_n = 2^n + 3^n + 6^n - 1$. Najděte všechna přirozená čísla, která jsou nesoudělná s každým členem této posloupnosti.

(IMO 2005)

Zobecnění Malé Fermatovy věty

Malá Fermatova věta se dá použít, pouze pokud počítáme modulo prvočísla. V této kapitolce si ukážeme, že se dá zobecnit i pro složená čísla.

Definice. Čísla a, b nazýváme *nesoudělná*, pokud žádné prvočíslo nedělí obě z nich (tj. pokud jediný jejich společný dělitel je 1). Pro přirozené číslo n značí $\varphi(n)$ počet nezáporných čísel menších než n, která jsou s n nesoudělná.

Všimněte si, že je-li n prvočíslo, potom $\varphi(n) = n-1$. Budeme nyní postupovat podobně jako při důkazu Malé Fermatovy věty. Nejprve si ukážeme tvrzení obdobné stěžejnímu tvrzení z předchozí kapitoly, ze kterého potom obdobně dokážeme zobecnění Malé Fermatovy věty.

Tvrzení. *Je-li n přirozené číslo, $A = \{a_1, \ldots, a_{\varphi(n)}\}$ je množina nezáporných čísel menších než n, která jsou s n nesoudělná, a $a \in A$, potom $\{aa_1 \pmod n, aa_2 \pmod n, \ldots, aa_{\varphi(n)} \pmod n\} = A$.*

Po vynásobení $\varphi(n)$ kongruencí z předchozího tvrzení dostaneme:

Věta. (Eulerova věta) *Je-li n přirozené číslo a a přirozené číslo nesoudělné s n, potom*

$$a^{\varphi(n)} \equiv 1 \pmod n.$$

Nyní přicházejí další úlohy na procvičení:

Úloha 5. Najděte všechna přirozená čísla n taková, že $n \mid 3^{n!} - 2^{n!}$.

(MKS, 17. ročník)

Úloha 6. Ukažte, že pro každá dvě nesoudělná přirozená čísla a, b existují přirozená čísla m, n taková, že $a^n + b^m \equiv 1 \pmod{ab}$.

Úloha 7. Mějme dánu posloupnost $a_n = na+b$, kde a, b jsou nesoudělná přirozená čísla. Dokažte, že kdykoliv dostanete nekonečnou podmnožinu členů posloupnosti a_n a přirozené číslo N, umíte najít alespoň N prvků této podmnožiny, jejichž součin je člen posloupnosti a_n.

Zdroje a literatura

[1] *http://www.artofproblemsolving.com/Resources/Papers/SatoNT.pdf*
[2] Andreescu, T., Andrica, D. a Feng, Z.; *104 Number Theory Problems*