Zbytky a mocnění

Kuba Svoboda

Abstrakt. Příspěvek obsahuje návod na řešení olympiádní teorie čísel pomocí kongruencí a také uvádí základní věty z teorie čísel, malou Fermatovu větu, Wilsonovu větu a Eulerovu větu. Je zde také spousta příkladů na procvičení.

Úmluva. Není-li řečeno jinak, pracujeme s celými čísly.

Definice. Skutečnost, že $a = b \cdot k$, tedy a je násobek b, můžeme vyjádřit jako $b \mid a$ a říkáme b dělí a.

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

Definice. Množinu čísel nazýváme úplnou sadou zbytků modulo n, pokud každý zbytek modulo n je kongruentní s alespoň jedním prvkem z množiny.

Tvrzení. $\{0, 1, \ldots, p-1\} = \{a \cdot 0, a \cdot 1, \ldots, a \cdot (p-1)\}$, *pro* $a \not\equiv 0 \pmod{p}$

Věta. (Malá Fermatova) *Buď p prvočíslo a a číslo s ním nesoudělné, potom*

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

Věta. (Wilsonova) *Buď p prvočíslo, potom*

$$(p-1)! \equiv -1 \pmod{p}.$$

Věta. (Eulerova) *Buď a nesoudělné s n a $\varphi(n)$ počet čísel menších než n nesoudělných s n. Potom*

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

Úlohy

Úloha 1. Najděte pro $n > 1$ a celočíselné x všechna řešení $(n-1)! \equiv x \pmod{n}$.

Úloha 2. Vyšetřete, jak se chová $\binom{p-1}{a}$ modulo p pro všechna možná a.

Úloha 3. Nechť $P(x) = 5x^{13} + 13x^5 + 9ax$. Najdi nejmenší a takové, že $P(x)$ je dělitelné 65 pro každé x. (Irsko 2000)

Úloha 4. Najdi všechna kladná n, pro která je $n! + 5$ čtverec.

Úloha 5. Nechť $p > 5$ je prvočíslo a číslo n je tvořeno $p - 1$ jedničkami v soustavě o základu $p + 6$. Dokažte, že $p \mid a$.

Úloha 6. Najdi všechna prvočísla p a q taková, že $p + q = (p - q)^3$.

(Rusko 2001)

Úloha 7. Dokažte, že existují právě tři nejvýše n-ciferná přirozená čísla a taková, že

$$a^2 \equiv a \pmod{10^n}.$$

(MKS 24–5–5)

Úloha 8. Ukaž, že pro různá prvočísla p a q platí

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

Úloha 9. Zjisti, pro která přirozená n platí, že $n \mid 3^{n!} - 2^{n!}$. (MKS 17–7–4)

Úloha 10. Uvažujme posloupnost $a_1, a_2, \dots$ definovanou vztahem $a_n = 6^n + 3^n + 2^n - 1$. Určete všechna přirozená čísla, která jsou nesoudělná s každým členem této posloupnosti. (IMO 2005)

Úloha 11. Dokaž, že pro každé x a každé y, z, w liché platí $17 \mid x^{y^{z^w}} - x^{y^z}$.

(Irsko 2005)

Úloha 12. Pro liché prvočíslo p dokažte

$$1^{p-2} + 2^{p-2} + \cdots + \left(\frac{p-1}{2}\right)^{p-2} \equiv \frac{2-2^p}{p} \pmod{p}.$$

(iKS 2012–N3)

Úloha 13. Dokaž, že pro každé sudé přirozené n platí, že $n^2 - 1$ dělí $2^{n!} - 1$.

Úloha 14. Dokažte, že pokud je $4^n + 2^n + 1$ prvočíslo, potom je n mocnina trojky.

Úloha 15. Určete hodnotu výrazu $1 \cdot 2^{-1} + 2 \cdot 3^{-1} + \cdots + (p-2) \cdot (p-1)^{-1} \pmod{p}$ pro libovolné p. (MKS 24–5–7)

Úloha 16. Můžeme najít přirozené číslo n dělitelné právě 2015 prvočíselnými děliteli takové, že $n \mid 2^n + 1$? (IMO 2000)

Úloha 17. Dokaž, že 2005^{2005} je součet dvou čtverců, ale ne součet dvou třetích mocnin.

(Irsko 2005)

Úloha 18. Definujme $a_1 = 2$, $a_n = 2^{a_{n-1}}$. Dokažte, že pro všechna $n > 1$ platí $n \mid a_n - a_{n-1}$. (iKS 2012–N5)

Úloha 19. Nechť je a liché přirozené číslo. Dokaž, že $a^{2^n} + 2^{2^n}$ a $a^{2^m} + 2^{2^m}$ jsou pro všechna přirozená $n \neq m$ nesoudělná.