Modulární aritmetika

Matěj Doležálek

26. březen 2021

Základní vlastnosti

Definice. Řekneme, že a, b jsou *kongruentní modulo* m, pokud $m \mid a - b$. Značíme $a \equiv b \pmod{m}$.

Pokud $a \equiv c$ a zároveň $b \equiv d \pmod{m}$, pak i

$$a + b \equiv c + d \pmod{m}, \qquad ab \equiv cd \pmod{m}.$$

Pokud $ac \equiv bc \pmod{m}$, pak i $a \equiv b \pmod{\frac{m}{\mathrm{NSD}(m,c)}}$.

Úloha 1. Ukažte, že $2^{60} + 7^{30}$ je násobek třinácti.

Úloha 2. Jaký zbytek po dělení sedmnácti dává 13^{2020}?

Úloha 3. Nechť $S(a)$ značí ciferný součet a v desítkové soustavě. Potom $S(a) \equiv a \pmod{9}$.

Úloha 4. Je dáno přirozené číslo n nesoudělné s 10. Dokažte, že nějaké číslo zapsané (v desítkové soustavě) samými jedničkami je násobkem n.

Kvadratické zbytky

Definice. Číslo a nazveme kvadratickým (ne)zbytkem mod n, pokud (ne)jde vyjádřit jako $a \equiv x^2 \pmod{n}$.

Úloha 5. Najděte všechny dvojice přirozených čísel a, b, které splňují $a^2 = 1! + 2! + \cdots + b!$.

Úloha 6. 4042ciferné přirozené číslo n je zapsáno (v nějakém pořadí) 2021 nulami a 2021 jedničkami. Může n být druhou mocninou celého čísla?

Úloha 7. Pro která n lze tabulku $n \times n$ vyplnit čísly 1 až n^2 tak, aby součet v každém sloupci i v každém řádku byl dělitelný sedmi?

Úloha 8. Najděte všechna celočíselná řešení rovnice $x^4 + y^4 = z^4 + 4$.

Mocniny

Věta (malá Fermatova)**.** *Mějme prvočíslo p a číslo $a \not\equiv 0 \pmod{p}$. Pak $a^{p-1} \equiv 1 \pmod{p}$.*

Úloha 9. Jsou dána různá prvočísla p, q. Dokažte $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.

Úloha 10. Modulo prvočíslo $p = 4k + 3$ je -1 kvadratický nezbytek.

Úloha 11. Je dáno prvočíslo p. Dokažte, že existuje nekonečně mnoho přirozených čísel n takových, že $p \mid 2^n - n$.

Zdroje

[1] Karolína Kuchyňová: *Kongruence*, `https://prase.cz/library/KongruenceKK/KongruenceKK.pdf`

[2] Radovan Švarc: *Úvod do diofantických rovnic*, `https://prase.cz/library/DiofantickeRovniceRS/DiofantickeRovniceRS.pdf`

[3] Filip Čermák: *Zbytky a mocnění*, `https://prase.cz/library/ZbytkyFC/ZbytkyFC.pdf`