Algebrou proti koronaviru 0

Dělitelnost & počítání modulo

Připomeňme si, že je-li $n \in \mathbb{N}$, pak pro celá čísla a, b definujeme $a \equiv b \pmod{n}$ právě tehdy, když $n \mid (a-b)$. Rychle se zjistí, že pro $a \equiv b \pmod{m}$ a $c \equiv d \pmod{m}$ platí $a \Box c \equiv b \Box d \pmod{m}$, kde $\Box$ je některá z operací $+, -, \cdot$.

1. Dokažte, že pro $a, b, c, m \in \mathbb{Z}$, $c, m \neq 0$ platí:

   (a) $a \equiv b \pmod{m} \Leftrightarrow ac \equiv bc \pmod{mc}$

   (b) jsou-li c a m nesoudělná, pak $a \equiv b \pmod{m} \Leftrightarrow ac \equiv bc \pmod{m}$

Předchozí tvrzení je užitečný nástroj k řešení následujících příkladů:

2. Vyřešte v celých číslech následující rovnice:

   (a) $x \equiv 2 \pmod{8}$ $[x = 2 + 8k; k \in \mathbb{Z}]$

   (b) $3x \equiv 2 \pmod{5}$ $[x = 4 + 5k; k \in \mathbb{Z}]$

   (c) $6x \equiv 2 \pmod{8}$ $[x = 3 + 4k; k \in \mathbb{Z}]$

   (d) $x^2 \equiv 36 \pmod{45}$ $[\{6, 9\} + 15k, k \in \mathbb{Z}]$

3. Ukažte, že $n^2 \equiv 1 \pmod{8}$ pro každé liché $n \in \mathbb{N}$.

4. Buď p prvočíslo. Najděte všechna řešení rovnice $x^2 \equiv 1 \pmod{p}$ a ukažte, že jsou opravdu všechna.

A pro odvážné několik zábavných a zcela dobrovolných příkladů navíc:

5.* Vyřešte v celých číslech $x^2 + 10x + 6 \equiv 0 \pmod{17}$. $[\{1, 6\} + 17k; k \in \mathbb{Z}]$

6.* Pomocí modulární aritmetiky odvoďte kritérium dělitelnosti pro

   (a) 9

   (b) 11

7.* Ukažte, že je-li $2^n - 1$ prvočíslo, je i $n \in \mathbb{N}$ prvočíslo. (Z dlouhé chvíle si můžete vyzkoušet, že $n = 11$ dokazuje, že obrácená implikace neplatí.)

8.* Ukažte, že století (pokud se nezmění kalendář) nikdy nebudou začínat středou, pátkem ani nedělí. (1. ledna 2001 bylo pondělí.)