4. cvičení z MB154, podzim 2021

Příklad 1. Dořeště příklady z minula, v mém případě: Popište *všechny* primitivní kořeny modulo 53; Nalezněte všechna $m \in \mathbb{N}$ taková, že $\varphi(m) = 38$, resp. $\varphi(m) = 16$.

Příklad 2. Najděte poslední cifru čísla $3^{7^{11^5}}$. Určete poslední dvě cifry čísla 13^{2021}.

Příklad 3. Určete, pro která $n \in \mathbb{Z}$ platí

$$5^{3n+4} \equiv 8 \pmod{13}.$$

Určete, pro která $n \in \mathbb{Z}$ platí

$$5^{2^{3n+1}} \equiv -7 \pmod{22}.$$

Příklad 4. Rozhodněte, zda je 7 kvadratický zbytek modulo 13.

Příklad 5. Řešte kongruenci $3x^2 + x - 5 \equiv 0 \pmod{13}$.

Příklad 6. Řešte kongruence $x^2 - 3x - 10 \equiv 0 \pmod{49}$, $x^2 - 3x - 14 \equiv 0 \pmod{49}$.
V prvním případě úpravou vyjde $(x - 26)^2 \equiv 0$, ve druhém $(x - 24)(x - 28) \equiv 0$.

Příklad 7. Rozhodněte, zda je 58 kvadratický zbytek modulo 157.

Příklad 8. Rozhodněte, zda je 58 kvadratický zbytek modulo 163. Vyřešte kongruenci

$$x^2 \equiv 58 \pmod{163}.$$

Budu to osobně prezentovat tak, že to vynásobím $1 \equiv 58^{81} \equiv \left(\frac{58}{163}\right)$ (protože 58 je kvadratický zbytek) a pak celé odmocním. V případě dostatku času můžete zkusit vyřešit i předchozí příklad, kde ale $58^{78} \equiv \left(\frac{58}{157}\right)$ nepomůže a je potřeba místo toho $-1 \equiv 58^{39}$ (bohužel 58 není čtvrtá mocnina nebo tak něco) a ještě si pomůžete $-1 \equiv 2^{79} \equiv 4^{39}$ (prostě je potřeba najít nějaký kvadratický nezbytek, vyjde hned 2, takže 4 není čtvrtá mocnina a tedy jejich součin $4 \cdot 58$ je čtvrtá mocnina), dohromady tak $4x^2 \equiv 4 \cdot 58 \equiv (4 \cdot 58)^{40}$ a opět lze odmocnit: $x \equiv \pm 2^{-1} \cdot (4 \cdot 58)^{20}$.