1. domácí úloha z MIN401, jaro 2024

Příklad 1. Martin řešil rovnici $x \cdot 5^x \equiv 3 \pmod{17}$.

(1) **Najděte** jedno řešení této rovnice. Martin jej hledal následovně. Protože je zjevně $3 = 3 \cdot 1$, zkusil hledat x splňující

$$x \equiv 3 \pmod{17}$$
$$5^x \equiv 1 \pmod{17}.$$

U druhé kongruence se vám může hodit, že 5 je primitivní kořen modulo 17.

(2) Toto řešení x není zbytková třída modulo 17 (to třeba znamená, že když x je řešení, tak $x + 17$ řešením být nemusí), ale modulo vhodné m. **Najděte** takové m.

(3) **Určete** počet řešení původní kogruence (modulo m), tato další řešení hledat nemusíte! Doporučený postup: Určete počet způsobů, jak rozložit $3 \equiv a \cdot b \pmod{17}$ (kolik existuje pro dané a příslušných b?) a určete, pro která z těchto a, b má soustava

$$x \equiv a \pmod{17}$$
$$5^x \equiv b \pmod{17}$$

řešení a kolik jich je modulo m. Využijte, že 5 je primitivní kořen modulo 17.

Příklad 2. Zbytek x se nazývá idempotent modulo n, jestliže $x^2 \equiv x \pmod{n}$. Příkladem idempotentů jsou 0 a 1. Z přednášky víme, že pro prvočíselný modul už žádné další neexistují (kvadratická rovnice má maximálně dvě řešení).

a) **Najděte** zbylé dva idempotenty y a z modulo $m = 11 \cdot 19$, přičemž je asi dosti výhodné „řešit“ rovnici prvně zvlášť modulo 11 a modulo 19 a pak dát tyto výsledky dohromady.

b) Studujte celočíselné lineární kombinace $x = k \cdot y + l \cdot z$ idempotentů y a z z předchozího bodu a zejména jejich zbytky modulo 11 a 19 a **ukažte**, jak lze takto **pomocí** y a z snadno napsat řešení soustavy kongruencí

$$x \equiv a \pmod{11}$$
$$x \equiv b \pmod{19}$$