1. domácí úloha z MIN401, jaro 2024

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

a) **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.

b) 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.

c) **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.

Řešení.

a) Druhá rovnice je ekvivalentní $x \equiv 0 \pmod{16}$, díky tomu, že 5 je podle zadání primitivní kořen. Řešíme tedy soustavu

$$x \equiv 3 \pmod{17}$$
$$x \equiv 0 \pmod{16}$$

kde dosazením $x = 17t + 3$ do druhé kongruence dostáváme $t \equiv 13 \pmod{16}$, celkově pak $x \equiv 224 \pmod{272}$.

b) Výše jsme odvodili $m = 272$.

c) Při rozkladu $3 \equiv a \cdot b \pmod{17}$ bude, podobně jako v prvním bodě, soustava ze zadání ekvivalentní

$$x \equiv a \pmod{17}$$
$$x \equiv \log_{17} b \pmod{16}$$

a podle čínské zbytkové věty bude mít jediné řešení modulo $m = 272$. Přitom pro každé nenulové $a \pmod{17}$ existuje jediné $b \equiv 3 \cdot a^{-1} \pmod{17}$. Protože je rozkladů 16, a pro každý existuje jedno řešení, máme dohromady 16 řešení.

□

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

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

Řešení.

a) Protože modulo 11 i modulo 19 máme pouze dvě řešení 0 a 1, a tyto můžeme libovolně kombinovat, budou zbylí dva idempotenti řešeními soustav

$$y \equiv 1 \pmod{11} \qquad z \equiv 0 \pmod{11}$$
$$y \equiv 0 \pmod{19} \qquad z \equiv 1 \pmod{19}$$

Jejich vyřešením standardním způsobem dostaneme $y \equiv 133 \pmod{209}$ a $z \equiv 77 \pmod{209}$.

b) Z kongruencí pro y a z z prvního bodu dostáváme pro $x = k \cdot y + l \cdot z$ úpravou

$$x \equiv k \cdot 1 + l \cdot 0 \equiv k \pmod{11}$$
$$x \equiv k \cdot 0 + l \cdot 1 \equiv l \pmod{19}$$

Dostáváme tak $k \equiv a \pmod{11}$ a $l \equiv b \pmod{19}$ a řešením obecné soustavy kongruencí je tedy $x \equiv a \cdot 133 + b \cdot 77 \pmod{209}$.

□