3. cvičení z MB154, podzim 2021

Příklad 1. Vyřešte kongruenci $74x \equiv 22 \pmod{168}$.

Bylo by fajn diskutovat řešení modulo 84 (tak to vyjde), pak také modulo 168.

Příklad 2. Vyřešte soustavu kongruencí

$$x \equiv 10 \pmod{25}$$
$$x \equiv 6 \pmod{11}.$$

Já to vysvětlím jak převedením na společný modul a počítání tam – prvně naivně "vypsáním" všech řešení první i druhé rovnice a porovnáním, pak modifikací Eukleidova algoritmu. Na závěr skrz parametrické vyjadření jedné rovnice a dosazení do druhé rovnice.

Příklad 3. Vyřešte soustavu kongruencí

$$x \equiv 1 \pmod{15}$$
$$x \equiv 4 \pmod{21}$$
$$x \equiv 6 \pmod{25}.$$

Tady už bych to dělal jen dosazováním parametrického tvaru.

Příklad 4. Najděte primitivní kořen modulo 53 (případně aspoň modulo 19 při nedostatku času). Poté popište *všechny* primitivní kořeny modulo 53.

Studenti nebudou vědět, co to znamená, tak to vysvětlete zatím jen modulo prvočíslo (opakování mocnin by jim mělo být intuitivně jasné, to lze snadno upřesnit Fermatovou větou; Eulerovu větu zatím nezmiňovat, nebudou umět Eulerovu funkci, té se věnujte jen, pokud zbude čas).

Příklad 5. Určete $\varphi(10)$, $\varphi(100)$, $\varphi(1000)$, $\varphi(256)$.

Příklad 6. Nalezněte všechna $m \in \mathbb{N}$ taková, že $\varphi(m) = 38$, resp. $\varphi(m) = 16$.

To by měly být hodnoty, pro které to jde rozumně a netechnicky, s využitím $p \mid m \Rightarrow p - 1 \mid \varphi(m)$, což dává výrazné omezení na možné dělitele $p \mid m$.