Zadání cvičení pro 4. týden: 12.3.-16.3.

Ve čtvrtém týdnu se budeme věnovat různým aspektům řešení (systémů) kongruencí, včetně tzv. Čínské zbytkové věty a distribuované zbytkové aritmetice. V případě potřeby ještě dokončete koncepty příklady z minula (primitivní kořeny, redukované systémy zbytků). Důraz prozím dejte na nejjednodušší systémy lineárních kongruencí, protože ty by se mohly objevit už ve vnitropísemce příští pondělí 19.3.

Příklad. *(první část 10.33)*
Určete primitivní kořen modulo 41.

Poznámka. Analyzujte, které řády je skutečně třeba sledovat – zjistíte, že stačí a je nutné, aby zároveň a^8 i a^{20} nebyly kongruentní s jedničkou. Poprvé vyjde u šestky.

Příklad. *Spočtěte nějaké jednoduché lineárních kongruence, např.* $130x \equiv 150 \pmod{232}$.

Poznámka. Výsledek je $x = 19 \pmod{116}$. Řešte pomocí Bezouta i elementárními úpravami s využitím $232 = 8 \cdot 29$.

Příklad. *(10.36-8)*
Vyřešte soustavy kongruencí

$$\begin{aligned} x &\equiv 7 \pmod{27} \\ x &\equiv -3 \pmod{11} \end{aligned} \qquad \begin{aligned} x &\equiv 1 \pmod{10} \\ x &\equiv 5 \pmod{18} \\ x &\equiv -4 \pmod{25} \end{aligned}$$

Poznámka. Připomeňte čínskou zbytkovou větu a z ní plynoucí obecné řešení pro po dvou nesoudělné moduly. Ukažte přímou metodu dosazování, fungující vždy.

Příklad. *(10.42)*
Řešte kongruenci $23\,941x \equiv 915 \pmod{3564}$.

Poznámka. Uveďte jako příklad poukazující na distribuovanou modulární aritmetiku, ke které se vrátíme ještě příště. (Určitě teď nebude v písemce.)