2. vnitrosemestrální práce MB104, 10. 4. 2017
skupina B

Příklad 1. (4b.) Vyřešte soustavu konguruencí

$$\begin{aligned} 13x &\equiv 120 \pmod 5 \\ 8x &\equiv 6 \pmod{14} \\ 4x &\equiv 5 \pmod{23} \end{aligned}$$

Řešení. $x = 805k - 85$. Správný modul 1b (vykrácení druhé kongruence), vyřešení kongruencí dosazováním postupně, v sumě: 0.5, 2.0, 4b. Nebo vyřešení kongruencí každé zvlášť 0.5, 0.5, 1.0b.

Příklad 2. (4b.) Veřejný klíč Honzy pro šifru RSA je $(119, 7)$. Zachytili jste jemu určenou zprávu 9. Dešifrujte ji.

Řešení. $119 = 7 \times 17$, $\varphi(119) = 96$, 0.5b, $7^{-1} \equiv 55 \pmod{96}$ (1.5b), $9^{55} \equiv 9^7 \equiv 2 \pmod{119}$ (2b). Správný postup s num. chybou 3b, s více num. chybami 2.5b.

Příklad 2. (2b.) Určete všechny primitivní kořeny modulo 10.

Řešení. 3,7 (po 0.5). Nutno vyloučit ostatní čísla 1b.