2. vnitrosemestrální práce MB104, 10. 4. 2015
skupina A

Příklad 1. (4b.) Vyřešte soustavu konguruencí

$$\begin{aligned} 17x &\equiv 91 \pmod 7 \\ 12x &\equiv 18 \pmod{15} \\ 3x &\equiv 7 \pmod{22} \end{aligned}$$

Řešení. $x = 770k + 259$. 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 $(143, 43)$. Zachytili jste jemu určenou zprávu 25. Dešifrujte ji.

Řešení. $143 = 11 \times 13$, $\varphi(143) = 120$, 0.5b, $43^{-1} \equiv 67 \pmod{120}$ (1.5b), $25^{67} \equiv 25^7 \equiv 64 \pmod{143}$ (2b). Správný postup s num. chybou 3b, s více num. chybami 2.5b.

Příklad 3. (2b.) Určete všechny primitivní kořeny modulo 14.

Řešení. 3,5 (po 0.5). Nutno vyloučit ostatní čísla 1b.