5 Cvičení 5

5.1 Najděte všechna celá čísla x, pro která

$$\begin{aligned} x &\equiv 3 \,(\mathrm{mod}\, 11) \\ x &\equiv 4 \,(\mathrm{mod}\, 7) \\ x &\equiv 1 \,(\mathrm{mod}\, 5) \end{aligned} \tag{1}$$

5.2 V $\mathbb{Z}_{153}$ najděte všechna x, pro která platí

$$108\, x = 27.$$

5.3 Pro šifrování pomocí RSA je $N = 253$ a veřejný klíč $e = 9$.

a) Dopočítejte soukromý klíč d.

b) Pomocí soukromého klíče dešifrujte zprávu $y = 101$. (použijte pro umocňování Čínskou větu o zbytcích).

5.4 V $\mathbb{Z}_{11}$ najděte všechny invertibilní prvky. Jestliže $i \in \mathbb{Z}_{11}$ je invertibilní, určete $i^{-1} \in \mathbb{Z}_{11}$.

5.5 V $\mathbb{Z}_{14}$ je dána rovnice:

$$4(x+1) = 1 - 3tx$$

s parametrem t. Najděte všechny hodnoty parametru t, pro něž má rovnice jediné řešení. Pro každé takové t toto řešení spočítejte.