

## 6. cvičení z MIN401 – kvadratické zbytky, Legendrovy a Jacobiho symboly

**Příklad 1:** Pomocí Rabinova kryptosystému s veřejným klíčem  $n = 713$  a soukromým klíčem  $p = 23$  a  $q = 31$  zašifrujte zprávu  $M = 327$  a ukažte, jak ji pak dešifrovat.

**Příklad 2:** Vyřešte následující kongruence:

(i)  $x^2 \equiv 1 \pmod{30}$ ,

(ii)  $x^3 + x + 3 \equiv 0 \pmod{25}$ ,

(iii)  $5x^2 + x + 8 \equiv 0 \pmod{11}$ ,

(iv)  $x^3 \equiv 2 \pmod{23}$ .

**Příklad 3:** Spočítejte následující Legendreův nebo Jacobiho symbol

$$\left(\frac{101}{1987}\right), \quad \left(\frac{-35}{97}\right), \quad \left(\frac{-23}{85}\right).$$

**Příklad 4:** [Odjinud, 10.67, 10.68] Rozhodněte, zda následující kongruence mají řešení:

(i)  $x^2 \equiv 5 \pmod{227}$ ,

(ii)  $x^2 \equiv 5 \pmod{229}$ ,

(iii)  $x^2 \equiv 38 \pmod{65}$ ,

(iv)  $x^2 - 23 \equiv 0 \pmod{77}$ .