Homework 4 in Advanced Methods of Cryptography

Prof. Dr. Rudolf Mathar, Henning Maier, Georg Bocherer

09.11.2010

Exercise 13. Let $p > 2$ be prime. Let $\left(\frac{a}{p}\right)$ be the Legendre symbol. Prove the following calculation rules.

(a) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

(b) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$

(c) $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$, if $a \equiv b \mod p$

Exercise 14. Show that Algorithm 6 from the lecture notes calculates the Jacobi symbol.
Hint: Use the following equations for any odd integers $n, m > 2$.

$$\begin{aligned} \left(\frac{m}{n}\right) &= (-1)^{\frac{m-1}{2}\frac{n-1}{2}} \cdot \left(\frac{n}{m}\right) \quad \text{law of quadratic reciprocity} \\ \left(\frac{2}{n}\right) &= (-1)^{\frac{n^2-1}{8}} \end{aligned}$$

Exercise 15. Prove Remark 9.9 (1): Show that for $a, b, n \in \mathbb{N}$, it holds for the Jacobi symbol $\left(\frac{ab}{n}\right)$ that

$$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right).$$