Homework 3 in Cryptography II

Prof. Dr. Rudolf Mathar, Peter Schwabe

03.05.2007

Exercise 7.
Let $p > 2$ be prime and let $\left(\frac{a}{p}\right)$ be the Legendre-symbol. Prove the following:

(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 8.
Prove that Algorithm 8 from the lecture notes computes the Jacobi symbol $\left(\frac{a}{n}\right)$.

Hint: Use the law of quadratic reciprocity, which states that

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