# Exercise 3 in Advanced Methods of Cryptography

Prof. Dr. Rudolf Mathar, Henning Maier, Markus Rothe

2014-11-07

**Problem 7.** *(properties of quadratic residues)* Let $p$ be prime, $g$ a primitive element modulo $p$ and $a, b \in \mathbb{Z}_p^*$. Show the following:

**a)** $a$ is a quadratic residue modulo $p$ if and only if there exists an even $i \in \mathbb{N}_0$ with $a \equiv g^i \mod p$.

**b)** If $p$ is odd, then exactly one half of the elements $x \in \mathbb{Z}_p^*$ are quadratic residues modulo $p$.

**c)** The product $a \cdot b$ is a quadratic residue modulo $p$ if and only if $a$ and $b$ are both either quadratic residues or quadratic non-residues modulo $p$.

**Problem 8.** *(coin flipping)* Consider the coin flipping protocol. Let $p > 2$ be prime.

**a)** Show that if $x \equiv -x \mod p$, then $x \equiv 0 \mod p$.

**b)** Suppose $x, y \not\equiv 0 \mod p$ and $x^2 \equiv y^2 \mod p^2$. Show that $x \equiv \pm y \mod p^2$.

**c)** Suppose Alice cheats when flipping coins over the telephone by choosing $p = q$. Show that Bob almost always loses if he trusts Alice.

**d)** Bob suspects that Alice has cheated. Why is it not wise for Alice to choose $n = p^2$ as the secret key? Can Bob discover her attempt to cheat? Can Bob use Alice' cheating as an advantage for himself?

**Problem 9.** *(Legendre symbol)* Let $\left(\frac{a}{p}\right)$ be the Legendre symbol, with $p > 2$ prime. 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 $a \equiv b \mod p$

**Problem 10.** *(Jacobi symbol)* Show that Algorithm 6 from the lecture notes computes the Jacobi symbol.

**Hint:** Use the following equations for any odd integers $n, m > 2$.

$$\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}} \cdot \left(\frac{n}{m}\right) \qquad \text{law of quadratic reciprocity}$$

$$\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$$