Homework 10 in Advanced Methods of Cryptography - Proposal for Solution -

Prof. Dr. Rudolf Mathar, Michael Reyer, Henning Maier
24.01.2014

Solution to Exercise 30.

Prove Euler's criterion: Let $p > 2$ be prime, then

$$c \in \mathbb{Z}_p^* \text{ is a quadratic residue (QR) modulo } p \Leftrightarrow c^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

„⇒“ c is QR modulo p with Definition 9.1 it follows

$$\exists\, x \in \mathbb{Z}_p^* : x^2 \equiv c \pmod{p} \Rightarrow c^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod{p},$$

where the last congruence follows from Fermat's Theorem.

„⇐“ $c^{\frac{p-1}{2}} \equiv 1 \pmod{p} \Rightarrow c \in \mathbb{Z}_p^*$ as c has an inverse modulo p.
Let y be a primitive element (PE), i.e., y is a generator of $\mathbb{Z}_p^*$. Note that there exists a PE with respect to Theorem 7.2 a).

$$\begin{aligned}
&\Rightarrow \exists\, j : c \equiv y^j \pmod{p} \\
&\Rightarrow c^{\frac{p-1}{2}} \equiv (y^j)^{\frac{p-1}{2}} \equiv 1 \pmod{p} \\
&\Rightarrow p-1 \mid j(p-1)/2 \Rightarrow j \text{ must be even} \\
&\Rightarrow \exists\, x \in \mathbb{Z}_p^* : x \equiv y^{\frac{j}{2}} \pmod{p} \\
&\Rightarrow x^2 \equiv y^j \equiv c \pmod{p} \\
&\Rightarrow c \text{ is QR modulo } p
\end{aligned}$$