Prof. Dr. Rudolf Mathar, Jose Calvo, Markus Rothe

Tutorial 1

Friday, October 30, 2015

Problem 1. *(Euler's criterion)* Prove Euler's criterion (Proposition 9.2): Let $p > 2$ be prime, then

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

Problem 2. *(calculating the basis)* Given $a^{13} \equiv 17 \mod 31$, calculate the basis a.