A Computational Aspect of Rational Residuosity

Markus HITTMEIR
University of Salzburg

Let $k \in \mathbb{N}$, $a \in \mathbb{Z}$ and p be prime such that $p \nmid a$. We consider a generalization of Legendre's symbol, the so called rational power residue symbol

$$\left(\frac{a}{p}\right)_{2^k} := \begin{cases} 1, & \text{if there is } x \in \mathbb{Z} \text{ such that } x^{2^k} \equiv a \mod p, \\ -1 & \text{else.} \end{cases}$$

Let $N = pq$ be a semiprime number with prime factors p and q, $p \neq q$. For $\gcd(N, a) = 1$, we define

$$\left(\frac{a}{N}\right)_{2^k} := \left(\frac{a}{p}\right)_{2^k} \cdot \left(\frac{a}{q}\right)_{2^k}.$$

In this talk, we describe several properties of this symbol and discuss applications to computational and cryptographical problems.

In particular, we show that an efficient algorithm for computing $\left(\frac{a}{N}\right)_4$ allows to efficiently solve the Quadratic Residuosity Problem modulo semiprime numbers N satisfying $N \equiv 3 \mod 4$.