Institut f. Analysis und Zahlentheorie

Zahlentheoretisches Kolloquium

Freitag, 29. 4. 2016, ab 14:00 Uhr

SR NT02008, Kopernikusgasse 24/2.Stock

14:00: **Markus Hittmeir**, (Univ. Salzburg)
A Computational Aspect of Rational Residuosity

Abstract. Let $k \in$, $p \in$ and $a \in$ such that $p \nmid a$. We consider a generalization of Legendre's symbol, the so called rational power residue symbol

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

Let $N = pq$ be a semiprime number with large prime factors p and q, $p \neq q$. The security of the RSA cryptosystem relies on the difficulty to compute p and q in the case that only N is known. 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 will show that an efficient algorithm for computing this generalized Jacobi symbol would allow the efficient computation of the 2-adic valuations $\nu_2(p-1)$ and $\nu_2(q-1)$ and, hence, of the first few bits of p and q. We will also discuss the problem raised by this result, namely finding a reciprocity law for $\left(\frac{a}{N}\right)_{2^k}$.

14:45: **Bruno Martin**, (Univ. du Littoral Côte d'Opale)
On prime numbers with an average sum of digits

Abstract: Let $q \geq 2$ be an integer and $\mathcal{E}$ be the set of prime numbers p whose the sum of digits in base q is equal to $\left\lfloor \frac{q-1}{2} \frac{\log p}{\log q} \right\rfloor$. We prove that for every irrational number β, the sequence $(\beta p)_{p \in \mathcal{E}}$ is uniformly distributed modulo 1.

This is a joint work with Christian Mauduit and Jo&quot;el Rivat (Université d'Aix-Marseille).

R.Tichy, P.Grabner