Institut f. Analysis und Zahlentheorie

Zahlentheoretisches Kolloquium

Freitag, 13. 4. 2018, 14:00 Uhr

Seminarraum Analysis-Zahlentheorie (NT02008), Kopernikusgasse 24/II

Reducing integer factorization to modular tetration

Markus Hittmeir

(Universität Salzburg)

Abstract. Let $a, k \in \mathbb{N}$. For the $k-1$-th iterate of the exponential function $x \mapsto a^x$, also known as tetration, we write

$$ {}^{k}a := a^{a^{\cdot^{\cdot^{\cdot^{a}}}}}. $$

In this talk, we show how an efficient algorithm for tetration modulo natural numbers N may be used to factorize N. In particular, we prove that the problem of computing the squarefree part of integers is deterministically polynomial-time reducible to modular tetration.

R.Tichy