Der Wissenschaftsfonds.

Institut f. Analysis und Zahlentheorie

Zahlentheoretisches Kolloquium

Freitag, 2. 6. 2017, 13 Uhr

SR Analysis-Zahlentheorie (NT02008), Kopernikusgasse 24, 2.Stock

A babystep-giantstep method for faster deterministic integer factorization

MARKUS HITTMEIR

(Universität Salzburg)

Abstract. In 1977, Volker Strassen presented a deterministic and rigorous algorithm for solving the problem to compute the prime factorization of natural numbers N. His method is based on fast polynomial arithmetic techniques and runs in time $\widetilde{O}(N^{1/4})$, which has been state of the art for the last forty years. In this talk, we discuss the core ideas for improving the bound by a superpolynomial factor. The runtime complexity of our algorithm is of the form

$$\widetilde{O}\left(N^{1/4}\exp(-C\log N/\log\log N)\right).$$

R.Tichy