A babystep-giantstep method for faster deterministic integer factorization

Abstract. The topic of this talk is the problem of computing the prime factorization of natural numbers. In practice, a large variety of probabilistic and heuristic methods is used for this task. However, none of these algorithms is efficient and the problem itself is assumed to be computationally hard. The difficulty of factoring large integers is fundamental for the security of several cryptographical systems, one of which is the public-key scheme RSA.

A more theoretical aspect of the integer factorization problem concerns deterministic algorithms and the rigorous analysis of their runtime complexity. In 1977, Volker Strassen presented such a method based on fast polynomial arithmetic techniques. The procedure computes the prime factorization of any natural number N 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

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