FRANCESCO SICA, University of Calgary, Dept. of Mathematics and Statistics, 2500 University Drive NW, Calgary, AB T2N 1N4

An Analytic Approach to Subexponential Factoring

I will highlight a polynomial-time reduction to translate the problem of factoring a product N of two primes into the computation of some multiple series with analytic coefficients. In particular, I conjecture that these series can be computed in $O\big(\exp(\log^\epsilon N)\big)$ bit operations for any $\epsilon > 0$, therefore providing a similar estimate for the inferred subexponential deterministic factoring algorithm. Unlike previous leading subexponential-time factoring algorithms related to the Quadratic Sieve, this one does not use "Fermat-type" equalities. It rather finds an approximation to the value of a carefully chosen multiplicative function related to the sum of divisors of N (hence its deterministic character). Analytic number theoretic techniques and especially the Riemann zeta function play here an essential role.