
FRANCESCO SICA, Mount Allison University–AceCrypt, 67 York Street, Sackville, NB, E4L 1E6
Exploring a New Factoring Algorithm

I would like to highlight the principal features of a new factoring algorithm still in preparation. In particular, I believe that this algorithm runs in subexponential time. However, unlike previous leading subexponential-time factoring algorithms related to the Quadratic Sieve, this one does not use “Fermat-type” equalities.

Rather, to factor x , it finds a nontrivial relation between $O(x^\epsilon)$ values of a carefully chosen multiplicative function related to $\sigma(n) = \sum_{d|n} d$. L -functions come to the rescue in finding this relation and the functional equation plays a crucial role.