

1125-11-2005

Jean-Francois Biasse*, 4202 E Fowler Ave, Tampa, FL 33620, and **Claus Fieker** and **Michael John Jacobson**. *Using lattice reduction to improve isogeny evaluation.*

We present novel algorithms for finding small relations and ideal factorizations in the ideal class group of an order in an imaginary quadratic field, where both the norms of the prime ideals and the size of the coefficients involved are bounded. We show how our methods can be used to improve the computation of large-degree isogenies and endomorphism rings of ordinary elliptic curves defined over finite fields. We obtain improved heuristic complexity results in almost all cases for these problems, and significantly improved performance in practice, especially in situations where the ideal class group can be computed in advance. (Received September 19, 2016)