

**SUBEXPONENTIAL CLASS GROUP COMPUTATION IN QUADRATIC
ORDERS
(ABSTRACT)**

MICHAEL JOHN JACOBSON, JR.

In 1989, the first subexponential algorithm for computing the class group of an imaginary quadratic order was introduced by Hafner and McCurley. Their algorithm is based on an integer factorization algorithm due to Seysen, and is conditional on the truth of the Extended Riemann Hypothesis. Not long after, their result was generalized to arbitrary algebraic number fields by Buchmann. Efficient versions of these algorithms for imaginary quadratic orders and real quadratic orders were implemented by Düllmann and Cohen, Diaz y Diaz, and Olivier, which yielded a substantial improvement in the sizes of discriminants for which class groups and regulators could be computed.

In this thesis, we present a new algorithm for computing the class group and regulator of a quadratic order. Our algorithm is also based on an integer factorization algorithm, namely the multiple polynomial quadratic sieve. We describe how two important practical improvements of this factoring algorithm, self-initialization and the large prime variant, can be applied to class group computation. In addition, we describe a number of practical improvements related specifically to class group computation, such as methods for computing the Hermite normal form transformation matrix in conjunction with a modular Hermite normal form algorithm. Computational results are presented, which clearly demonstrate the efficiency of our algorithm.

As an application, we present algorithms for computing discrete logarithms in the class group and for principality testing, based on the work of Düllmann and Abel. We show how our idea of generating relations with sieving can be applied to improve the performance of these algorithms, and present computations illustrating this practical improvement.

We also present a number of quadratic orders with interesting mathematical properties whose class groups and regulators were computed with our algorithm. In particular, we present some imaginary quadratic orders which correspond to quadratic polynomials with high densities of prime values, and real quadratic orders which correspond to instances of Pell's equation with exceptionally large minimal solutions. These types of quadratic orders also represent worst-case and best-case inputs to our algorithm, and we discuss the performance of the algorithm on these inputs in relation to that on more average inputs.