HUGH WILLIAMS, University of Calgary

Compact Representations of Certain Algebraic Integers

Suppose we have a real quadratic number field of discriminant d. If we have a principal ideal I, it usually requires an exponential (in log d) amount of time to write out a generator of I in the conventional way. However, there exists a representation of this generator, called a compact representation, which can be written out in polynomial time. In this talk I discuss algorithms for finding compact representations of such a generator, when we are given an approximate value of the logarithm of the absolute value of it and an integral basis of I. I go on to point out several improvements that have been to algorithms used in the past.