
HUGH WILLIAMS, University of Calgary, Calgary, AB

Compact Representation of the Generator of a Principal Ideal

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 an algorithm for finding a compact representation when we are given an approximate value of the logarithm of the absolute value of a generator and an integral basis of I .