ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 15, Number 2, Spring 1985

CONTINUED FRACTIONS AND NUMBER-THEORETIC COMPUTATIONS

HUGH C. WILLIAMS

Dedicated to the memory of E.G. Straus

ABSTRACT. The purpose of this mainly expository paper is to describe how continued fractions over $\mathcal{K} = \mathbf{Q}(\sqrt{D})$ can be used in the development of algorithms for solving computational problems in number theory. These problems include: the factoring problem, i. e., the determination of whether an ideal in $\mathcal{K}$ is principal; and the class group structure of $\mathcal{K}$. Some attention is also given to the extension of these methods to complex cubic fields.

1. Introduction. The purpose of this mainly (but not entirely) expository paper is to describe how continued fraction algorithms can be used to solve computational problems which arise in the study of real quadratic and complex cubic fields. Many of the recent results presented here are due to Shanks [**12**], [**13**], [**14**], [**15**], Lenstra [**5**], Schoof [**11**], and Williams, Dueck, Schmid [**22**]. They show that by using the fairly simple idea of 'distance', the usual algorithms for solving the type of problem discussed here (determination of the regulator, class number, class group structure, etc.) can be considerably improved. As this material is scattered about in several diverse places and is described in rather different ways, it was thought that a simple, unified approach to these results would be useful. Our presentation will stress the computational rather than the theoretic aspects of these ideas. For a more sophisticated description of the quadratic case see the work of Lenstra [**5**] and Schoof [**11**].

The material described here is pretty-well self-contained. We require only some well-known properties of ideals and lattices and these are reviewed in §2 and §3. In §4, §5, and §6 we show how continued fractions can be used to solve certain problems in real quadratic extensions and in §7 we describe some means by which the ideas developed here can be applied to the problem of factoring. Finally, in §8, §9, and §10

Received by the editors April 11, 1984.
Research supported by NSERC of Canada grant A7649 and by the I. W. Killam Foundation.