ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 40, Number 6, 2010

COMPACT REPRESENTATION OF QUADRATIC INTEGERS AND INTEGER POINTS ON SOME ELLIPTIC CURVES

FILIP NAJMAN

1. Introduction. Let $\mathbf{Q}(\sqrt{d})$ be a real quadratic field. Following [**17**] we define a *compact representation* of an algebraic number $\beta \in \mathbf{Q}(\sqrt{d})$ to be

$$\beta = \prod_{j=1}^{k} \left(\frac{\alpha_j}{d_j} \right)^{2^{k-j}}, \tag{1}$$

where $d_j \in \mathbf{Z}$, $\alpha_j = (a_j + b_j\sqrt{d})/2 \in \mathbf{Q}(\sqrt{d})$, $a_j, b_j \in \mathbf{Z}$, $j = 1, \ldots, k$. Bounds on k, α and d_j are given in [**17**], and all depend polynomially on $\log d$. Compact representations are used to store the fundamental unit of the quadratic order O_K. The reason for doing this is that, as is shown in [**15**], there is an infinite set of quadratic orders, such that the binary length of the fundamental unit is exponential in $\log d$. This makes it impossible to create an algorithm for solving the Pell equation with complexity less than exponential. Compact representations are polynomial in $\log d$, and allow faster algorithms for solving the Pell equation.

This representation is a extension of a compact representation as defined in [**2**] from algebraic integers to all elements of $\mathbf{Q}^*(\sqrt{d})$. It is often useful to do modular arithmetic on compact representations, for example for determining the solvability of certain Diophantine equations, as seen in [**14**]. We present an algorithm for computing the value of a quadratic integer represented by a compact representation as defined in [**17**]. In [**2, 14**] there are algorithms for doing modular arithmetic on compact representations as defined in [**2**], but to our knowledge there are no algorithms for doing modular arithmetic on compact representations as defined in [**17**]. The main problem is that the [**2**] representation requires that the partial products

$$\gamma_j = \alpha_j \prod_{i=1}^{j-1} \left(\frac{\alpha_i}{d_i} \right)^{2^{j-i}} \tag{2}$$

Received by the editors on June 11, 2008, and in revised form on June 30, 2008.
DOI:10.1216/RMJ-2010-40-6-1979