ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 25, Number 4, Fall 1995

INFINITE DESCENT ON ELLIPTIC CURVES

SAMIR SIKSEK

Dedicated to my parents

ABSTRACT. We present an algorithm for computing an upper bound for the difference of the logarithmic height and the canonical height on elliptic curves. Moreover, a new method for performing the infinite descent on elliptic curves is given, using ideas from the geometry of numbers. These algorithms are practical and are demonstrated by a few examples.

1. Introduction. Recently there has been much interest in the computation of Mordell-Weil groups of elliptic curves, both for specific families of curves (such as in [**3, 4, 25**]), and in the development of new algorithms for computing the Mordell-Weil group (see, for example, [**11**]). Not only is this an interesting problem in itself, but it is also an essential ingredient for the popular algorithm for calculating the integral points on elliptic curves using elliptic logarithms (see any of [**12, 23, 24, 26**]).

Let E be an elliptic curve defined over a number field K. The computation of the Mordell-Weil group naturally falls into two parts:

(1) The 2-descent. Here, with some luck, a basis for $E(K)/2E(K)$ is computed.

(2) The infinite descent. This is the name given to the process by which, given a basis for $E(K)/mE(K)$ for some $m \geq 2$, we can obtain a basis for $E(K)$.

Over the rationals, the best (unconditional) algorithm known to me for the 2-descent is the one given in [**1**] and in [**9**, pp. 68–76]. This has recently been (re-)implemented by J. Cremona as the program `mwrank`. For most curves of reasonably small discriminant `mwrank` can calculate $E(\mathbf{Q})/2E(\mathbf{Q})$ in a very short time. In contrast to this, the method

Received by the editors on February 18, 1995.
1991 *Mathematics Subject Classification.* Primary 11G05, Secondary 11Y16.
Key words and phrases. Elliptic curves, Diophantine equations, computational number theory, Mordell-Weil group.
The author's research was funded by a studentship from the SERC/EPSRC.