ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 32, Number 3, Fall 2002

ON THE COMPUTATION OF MORDELL-WEIL AND 2-SELMER GROUPS OF ELLIPTIC CURVES

J.E. CREMONA

1. Introduction. Let E be an elliptic curve defined over $\mathbf{Q}$. In this note, we present related methods to do the following tasks:

1. Prove that a given finite set of points in the Mordell-Weil group $E(\mathbf{Q})$ is independent;
2. Make the group law in the 2-Selmer group $S^2(E/\mathbf{Q})$ explicit, and hence show that a given finite set of elements in $S^2(E/\mathbf{Q})$ is independent.

The first provides an alternative to computing the height-pairing matrix of the given set of points and shows that its determinant is nonzero. While that is easily done, for curves of large rank it requires some delicate consideration of precision in order to be sure of the result. The method here, by contrast, involves only "discrete" computations: finding roots of cubics and evaluating quadratic characters modulo primes. The method was also described by Silverman in [**6**], attributed there to Brumer and me. In fact, Brumer described the method to me in 1996 and it was apparently used by him and Kramer in verifying the examples in [**2**], though the method is not explicitly mentioned there; so the method goes back to 1975 at least. We give it here as it is closely related to, and leads to, our second section where we apply similar ideas to 2-Selmer groups. We illustrate the method with the Martin-McMillen curve which has 23 independent points.

The second problem arises when doing explicit 2-descents on elliptic curves with no 2-torsion, as implemented in our program `mwrank`. Following the method set out in [**1**], we represent elements of the Selmer group $S^2(E/\mathbf{Q})$ by quartics $g(X) \in \mathbf{Z}[X]$ such that the genus 1 curve $Y^2 = g(X)$ is a 2-covering of E. These quartics are found by a finite search procedure. In [**1**], the resulting set of (equivalence classes of) quartics is treated as a set without making explicit its structure as an

Received by the editors on September 15, 2000, and in revised form on November 30, 2000.

Copyright ©2002 Rocky Mountain Mathematics Consortium