ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 34, Number 1, Spring 2004

A NOTE ON THE CURVE $Y^2 = (X + p)(X^2 + p^2)$

ALLAN J. MACLEOD

ABSTRACT. It is shown that infinite order rational points, on the curves of the title, can be found for $p \equiv 7 \bmod 8$ by adapting a Heegner point computation used by Elkies for congruent numbers. It is possible to find points with extremely large height in a matter of minutes.

1. Introduction. In [**4**], Stroeker and Top present a detailed analysis of the family of elliptic curves

$$E_p : y^2 = (x + p)(x^2 + p^2) \tag{1}$$

with p prime. They show that the curve has rank 0 if $p = 2$ and $p \equiv \pm 3 \bmod 8$. On the basis of the Birch and Swinnerton-Dyer conjecture, they find that rank E_p is 1 if $p \equiv 7 \bmod 8$, and 1 or 3 if $p \equiv 1 \bmod 8$.

The later sections of the paper are devoted to the problem of constructing generators for the rank 1 or 3 curves. Numerical evidence is given to show that the heights of such generators can be quite large, especially for $p \equiv 7 \bmod 8$. The authors describe a descent procedure suitable for points with small heights but state that it failed for larger heights. They then describe a specialized descent provided by Bremner which they used for the difficult points. We quote the following statement "In the following lines we shall only give an outline, as the details are rather messy."

The present author performed the height calculations for a much larger set of p-values and found some enormous heights. For example, $p = 3167$ gives an estimated height of 511.3. It would be anticipated that even Bremner's method might struggle for such points.

In this note we wish to point out that we can apply a variant of the method used by Elkies [**1**] for the congruent number problem. This

Received by the editors on January 31, 2001, and in revised form on August 30, 2001.