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.

allows us to calculate points on E_p, which have a very large height, in minutes.

2. Method. The method used is an application of the techniques used by Elkies, with the following specific differences.

Firstly, we use the transformations $y = wp\sqrt{-p}$ and $x = -pz$ to show that E_p is isomorphic to

$$E : w^2 = z^3 - z^2 + z - 1 \tag{2}$$

over the field $Q(\sqrt{-p})$. In this field, the prime 2 splits if $p \equiv 7 \bmod 8$, which we now assume.

The curve E is modular with rank 0 and conductor 128, so that

$$\phi(\tau) = \sum_{n=1}^{\infty} a_n q^n,$$

with $q = \exp(2\pi i\tau)$, is a modular form of weight 2 for $\Gamma_0(128)$.

To compute the a_i terms in the congruent number case, there is an expansion involving the Dedekind η function, but this does not occur in the current problem, so we must compute the coefficients directly from the elliptic curve E. This can be time-consuming for a large number of coefficients, but need only be done once. It should be noted that $a_i = 0$ for i even, so we only need to compute for odd i.

For each ideal class in $Q(\sqrt{-p})$, we have to compute a Heegner point, which can be done by manipulations of the underlying primitive quadratic forms. This is not as trivial as a reading of Elkies might suggest. The algorithmic paper of Stephens [**3**] also does not describe how to do the computation. There is, however, an excellent analysis and algorithm in the first chapter of Liverance's Ph.D. thesis [**2**].

We then need to evaluate the images of these Heegner points under the modular parametrization $X_0(128) \to E$, given by the formula

$$I(\tau) = \sum_{n=1}^{\infty} \frac{a_n}{n} q^n \tag{3}$$

with $q = \exp(2\pi i\tau)$. The following properties hold

$$I(\tau + 1/2) = -I(\tau), \quad I(-1/128\tau) + I(\tau) = 2I(i/\sqrt{128}) \tag{4}$$

the second of which means that we use (3) with τ if $|\tau| \geq 1/\sqrt{128}$, and with $-1/128\tau$ otherwise.

The remainder of the computations are identical to those described by Elkies.

3. Liverance's method. At the suggestion of the referee, we now describe the basic steps of the method given in Eric Liverance's thesis.

Let N be the conductor of the underlying elliptic curve, and let (A, B, C) denote a primitive quadratic form, representing an ideal class in $Q(\sqrt{-d})$.

Let ρ be an integer satisfying $\rho^2 \equiv \Delta \bmod 4N$, with Δ the discriminant of the quadratic field. If such an integer does not exist, neither do the Heegner points. For moderately sized conductors N, ρ can be found easily by a simple search.

The Heegner point for this class can be represented by an equivalent quadratic form (A', B', C') with $A' \equiv 0 \bmod N$ and $B' \equiv \rho \bmod 2N$.

We thus need to find an integer matrix

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$$

with determinant 1, such that

$$\begin{aligned} A' &= A\alpha^2 + B\alpha\gamma + C\gamma^2 \\ B' &= 2A\alpha\beta + B(\alpha\delta + \beta\gamma) + 2C\gamma\delta \\ C' &= A\beta^2 + B\beta\delta + C\delta^2 \end{aligned} \tag{5}$$

Liverance shows that, if α and γ satisfy

$$\begin{pmatrix} A & \frac{B+\rho}{2} \\ \frac{B-\rho}{2} & C \end{pmatrix} \begin{pmatrix} \alpha \\ \gamma \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \bmod N \tag{6}$$

then A' and B' satisfy the required congruences.

He shows that a solution exists with $\gcd(\alpha, \gamma) = 1$, which leads to easily finding β and δ. If N is of moderate size, a simple search procedure finds these values quickly.

From the quadratic form (A', B', C') we compute $I(\tau)$ with $\tau = (-B' + \sqrt{\Delta})/2A')$.

4. Results. The above method was initially programmed in UBASIC to allow easy algorithmic development and run on a variety of PCs. Obviously, as the projected height of a rational point increases, the required precision needs to increase which implies that the number of a_i values will need to increase.

To show that the method works we present the results for $p = 983$ and $p = 3167$, with all computations on a 500 MHz laptop. Initial computations, using the Birch and Swinnerton-Dyer conjecture, suggest the height of the generator for $p = 983$ is 180.9 (or 361.8 using the alternative height normalization), and that this is the largest height for $p < 1000$.

For $p = 983$, UBASIC was used with approximately 400 digits of precision and 90000 terms in the expansion (3). The resulting point has 158 digits in the numerator and 154 in the denominator, and took 231 secs to find. To present the results in a slightly more accessible form, we define $z = x + p$ so that E_p can be given in the form

$$y^2 = z(z^2 - 2pz + 2p^2).$$

For points on this curve we have $z = du^2/v^2$ with d squarefree and $d|2p$. We find $d = 2$ and

u =		3085	71914	43709	39902
33433	99991	88834	72641	67331	15053
73245	14611	90376	17889	71942	65438

v =		63	69985	26667	08251
29230	73741	10006	03633	98297	61221
87572	91823	10442	21945	71135	75137

For $p = 3167$, the precision limitations on complex numbers in UBASIC meant that the program failed. We wrote an equivalent code in Pari (the code is available upon request by e-mail to the author) and

ran it with 1500 digits of precision and 400000 terms in $I(\tau)$. The run took 10 hours and 1 minute to find the point with $d = 2$ and

u =			69	01613	10202	52680	42405
73517	04507	63661	42083	83406	42504	63908	40041
79732	68216	72661	23502	59096	15251	66074	00849
65335	84997	43546	70249	99551	51546	76605	89090
56942	40602	77475	94442	58760	98468	39122	68927
15778	61022	52820	20110	84837	62369	70802	35492

v =			2	02726	63074	73110	52096
03134	18523	58835	54466	14932	93926	35340	01680
89379	22475	30662	78033	19210	50588	56975	76843
83369	38746	35241	51903	40483	66031	49779	08497
60995	59565	56180	46331	68128	10248	79111	32631
56201	21667	96054	09502	91256	82388	75524	25031

Acknowledgments. The author would like to thank the referee for several very helpful comments, which have improved the presentation of the paper.

REFERENCES

1. N. Elkies, *Heegner point computations*, in *Algorithmic number theory* (L.M. Adleman and M.D. Huang, eds.), ANTS-1, Lecture Notes in Computer Science, vol. 877, 1994, pp. 122–133.

2. E. Liverance, *Heights of Heegner points in a family of elliptic curves*, Ph.D. Thesis, Univ. of Maryland, 1993.

3. N.M. Stephens, *Computation of rational points on elliptic curves using Heegner points*, in *Number theory and applications* (R.A. Mollin ed.), Kluwer, Dordrecht, 1989, pp. 205-214.

4. R.J. Stroeker and J. Top, *On the equation* $Y^2 = (X + p)(X^2 + p^2)$, Rocky Mountain J. Math. **24** (1994), 1135–1161.

Department of Mathematics and Statistics, University of Paisley, High St. Paisley, Scotland PA1 2BE.
E-mail address: macl-ms0@paisley.ac.uk