MATHEMATICS OF COMPUTATION
VOLUME 64, NUMBER 211
JULY 1995, PAGES 1251–1265

# ON A CLASS OF ELLIPTIC CURVES WITH RANK AT MOST TWO

H. E. ROSE

ABSTRACT. In this note we consider the elliptic curves $y^2 = x^3 + px$ defined over $\mathbb{Q}$ for primes $p$ satisfying $p \equiv 1 \pmod 8$, and review some of their properties. We then compute and list (in the supplement) their ranks, and give, when the rank is positive, the generators of the group of rational points and Mordell-Weil lattice invariant $\tau$ for all primes $p < 50000$ of the form $m^2 + 64n^2$.

## 1. INTRODUCTION

Considerable progress has been made in the study of elliptic curves defined over the rational field $\mathbb{Q}$, but many questions remain unanswered. For example, formulas for, or even estimates of, the rank of many of these curves have not been found. Hence, it is of interest to study properties of particular classes of curves in the hope that some of these questions can be answered in these cases.

In this paper we shall consider the class of elliptic curves

$$C_p : y^2 = x^3 + px,$$

defined over the rational field $\mathbb{Q}$ and where $p$ is a prime. Let $r(C_p)$ denote the rank of this curve, that is the number of independent infinite-order generators of the (Mordell-Weil) group of rational points on this curve. It is known that

$$\text{if } p \equiv 7 \text{ or } 11 \pmod{16}, \quad \text{then } r(C_p) = 0;$$
$$\text{if } p \equiv 3, 5, 13 \text{ or } 15 \pmod{16}, \quad \text{then } r(C_p) = 0 \text{ or } 1; \text{ and}$$
$$\text{if } p \equiv 1 \text{ or } 9 \pmod{16}, \quad \text{then } r(C_p) = 0, 1 \text{ or } 2,$$

see Silverman [8, p. 311]. Bremner and Cassels [1] and Bremner [2] have considered the class of curves $C_p$ for primes $p \equiv 5 \pmod 8$; they showed that $r(C_p) = 1$ for $p < 20000$ and conjectured that this holds for all primes in their class. Here we shall consider the third case above, that is the curves $C_p$ where $p \equiv 1 \pmod 8$. The rank can be zero or two, and it is conjectured that it cannot equal one. We give some evidence in support of this; also this conjecture is a consequence of the full Birch and Swinnerton-Dyer conjecture, in particular it holds when the corresponding Shafarevich-Tate group is finite.

Received by the editor January 19, 1994 and, in revised form, June 28, 1994.
1991 *Mathematics Subject Classification.* Primary 11G05, 11D25; Secondary 14H52.
*Key words and phrases.* Elliptic curve, rank.

For primes $p \equiv 1 \pmod 4$, Gauss showed that 2 is a quartic residue modulo $p$ if and only if $p$ can be expressed as a sum of squares $p = x^2 + y^2$ where $8 \mid y$. We shall call a prime with this property a *G-prime* in this paper; it is necessarily congruent to 1 (mod 8). We can easily show that $r(C_p) = 0$ if $p \equiv 1 \pmod 8$ and $p$ is not a G-prime, see §2. The converse is only partially true. There are 625 G-primes less than 50000, in 366 cases the rank of the corresponding curve is two, examples are

$$73, 89, 113, 233, \ldots, 49801;$$

whilst in the remaining 259 cases the rank is zero, with examples [1]

$$257, 577, 1097, 1201, \ldots, 49633.$$

In §2 we reduce the question of finding rational points on $C_p$ to the problem of solving one or more of three simple quartic equations (numbered (I), (II) and (III)) in rational integers. These three quartic equations correspond to the three 'principal homogeneous spaces' for $C_p$; see Silverman [8, Chapter 10]. In §3 we give algorithms which generate solutions to one of these equations provided solutions for the remaining two are known; this provides an elementary example of the operation of the Weil-Châtelet group for the curve. This also provides another derivation of the rank estimates quoted above. In §4 we discuss briefly the problem of showing that the rank of our curves cannot be one. Finally, in §5, we describe the computations that have been undertaken to calculate the ranks of our curves for all G-primes less than 50000. The supplement gives the basic data from which the infinite-order generators of the corresponding groups can be constructed, the values of $\tau$ for the Mordell-Weil lattice (see final section of this paper), and values of the $L$-functions when these groups are finite.

In a forthcoming paper further computations will be presented. This will include evaluations of the second derivatives of the $L$-functions at $s = 1$ for the rank-two curves $C_p$ listed in the supplement (thus giving further data in support of the full Birch and Swinnerton-Dyer conjecture) and evaluations of the $L$-functions for non G-primes. Also, all of these computations will be extended to primes $p < 100000$. For example, the order of the Shafarevich-Tate group Ш for the curve $C_{50177}$ is 256, and 50177 is the first G-prime larger than 50000 for which the rank of the corresponding elliptic curve $C_p$ is zero.

## 2. Preliminaries

We shall study the elliptic curves

$$y^2 = x^3 + px \quad \text{for primes} \quad p \equiv 1 \pmod 8. \tag{1}$$

The group of rational points on (1) will be denoted $C_p(\mathbb{Q})$, which we shall usually abbreviate to $C_p$. Clearly, the point $(0, 0) \in C_p$ and has order two. Except for this point and the neutral element, a point belonging to $C_p$ has the form $(u/s^2, v/s^3)$, where $u$, $v$ and $s$ are nonzero integers, and $(u, s) =$

[1] There is a possible connection here with real quadratic fields. If $\mathrm{cl}(p)$ denotes the class number of the field $\mathbb{Q}(\sqrt{p})$, then, for G-primes less than 1097, $r(C_p) = 2$ if and only if $\mathrm{cl}(p) = 1$. It is unclear whether this is a coincidence or not; it is false when $p = 1097$ and for some larger primes.

$(v, s) = 1$. We have

$$(2) \qquad (u/s^2, v/s^3) + (0, 0) = (ps^2/u, psv/u^2) \in C_p,$$

and so $u = r^2$, for some $r$, and $r \mid v$; or $u = pr_1^2$, for some $r_1$, and $pr_1 \mid v$. *We shall assume from now on that the first case always holds.* Therefore, with the exception of the neutral point and the point $(0, 0)$, a typical point on $C_p$ has the form

$$(3) \qquad (r^2/s^2, rt/s^3) \quad \text{with} \quad (r, s) = (t, s) = 1 \quad \text{and} \quad rst \neq 0.$$

[For each such point a second point on $C_p$ is always given by (2), and vice versa.] Using this assumption, we can write equation (1), cancelling $r^2/s^6$, in the form

$$(4) \qquad r^4 + ps^4 = t^2$$

with $r, s$ and $t$ as in (3). Note this implies $(r, t) = 1$. As $p \equiv 1 \pmod 8$, $r$ and $s$ have different parities, and $t$ is odd; we shall consider these cases separately. This equation has been discussed previously in Mordell [5].

*Case* 1. Equation (4) has the form $16r^4 + ps^4 = t^2$ and $s$ is odd.

Rewriting this, we have $ps^4 = (t - 4r^2)(t + 4r^2)$. Now $t - 4r^2$ and $t + 4r^2$ cannot have a common factor, and so each is a fourth power or $p$ times a fourth power. Eliminating $t$ and renaming the variables ($r \to t$ and $s \to rs$) we obtain two possibilities for equation (4) in this case:

(I) $r^4 - ps^4 = -8t^2$ with $(r, s) = (s, t) = (t, r) = 1$ and $r, s$ odd,

or

(II) $r^4 - ps^4 = 8t^2$ with $(r, s) = (s, t) = (t, r) = 1$ and $r, s$ odd.

We can impose a restriction on $p$ as follows. If either of (I) or (II) is soluble, and if $q$ (a prime) divides $t$, then $r^4 \equiv ps^4 \pmod q$, and so the Legendre symbol $(p/q) = (q/p) = 1$ by quadratic reciprocity; this gives $(t/p) = 1$. Therefore, we can find an integer $u$ satisfying $u^2 \equiv t \pmod p$, and then we have $\mp 8u^4 \equiv r^4 \pmod p$, with the upper sign for (I) and the lower sign for (II). As $p \equiv 1 \pmod 8$, $-1$ is a quartic residue modulo $p$, and so 2 must also be a quartic residue modulo $p$ (that is, $p$ is a G-prime) and both (I) and (II) are insoluble if this is not so.

*Case* 2. Equation (4) has the form $r^4 + 16ps^4 = t^2$ and $r$ is odd.

Arguing as above, we obtain four subcases, with $s = s_1 s_2$ and $(s_1, s_2) = 1$:

$$\begin{aligned} t - r^2 &= 2s_1^4 & t + r^2 &= 8ps_2^4, \\ t - r^2 &= 2ps_1^4 & t + r^2 &= 8s_2^4, \\ t - r^2 &= 8s_1^4 & t + r^2 &= 2ps_2^4, \\ t - r^2 &= 8ps_1^4 & t + r^2 &= 2s_2^4. \end{aligned}$$

The first two subcases are impossible because $r$ is odd. The fourth subcase gives

$$r^2 = s_2^4 - 4ps_1^4, \qquad t = s_2^4 + 4ps_1^4, \tag{5}$$

and so $(s_2^2 - r)(s_2^2 + r) = 4ps_1^4$. As in Case 1, this gives $s_1 = uv$, $(u, v) = 1$, and

$$s_2^2 + r = 2u^4, \quad s_2^2 - r = 2pv^4, \quad \text{or}$$
$$s_2^2 + r = 2pv^4, \quad s_2^2 - r = 2u^4.$$

If the first pair of equations apply, then $s_2^2 = u^4 + pv^4$ and $r = u^4 - pv^4$, and the corresponding point on $C_p$, that is $(r^2/4s^2, rt/8s^3) = 2(u^2/v^2, s_2u/v^3)$, is a double point. Similarly, if the second pair apply, then the point is $2(u^2/v^2, -s_2u/v^3)$, another double point. Hence, as we are mainly concerned with the generators of $C_p$, we may exclude the fourth subcase completely. Eliminating $t$ from the third subcase, we find that $s_1$ is even and so, relabelling the variables ($r \to t$, $s_1 \to 2r$ and $s_2 \to s$), we obtain the third possibility for equation (4):

(III) $64r^4 - ps^4 = -t^2$ with $(r, s) = (s, t) = (t, r) = 1$ and $s, t$ odd.

Gauss's result mentioned in the introduction states that '2 is a quartic residue modulo $p$ if and only if $p$ can be expressed in the form $x^2 + 64y^2$'. The proof of this classic result can easily be adapted to show that if equation (III) is soluble, then 2 is a quartic residue modulo $p$, and so $p$ is a G-prime.

Hence, we need to consider the three equations (I), (II) and (III); they are the three principal homogeneous spaces for $C_p$ (see Silverman [8, Chapter 10]). For (I) or (II) the corresponding point on the curve $C_p$ is

$$(4t^2/r^2s^2, t(r^4 + ps^4)/r^3s^3) \quad \text{with } r \text{ and } s \text{ odd}, \tag{6}$$

and for equation (III) the corresponding point is

$$(t^2/16r^2s^2, t(64r^4 + ps^4)/64r^3s^3) \quad \text{with } s \text{ and } t \text{ odd}. \tag{7}$$

In each case $p$ must be a G-prime for a solution to exist. Further, by Gauss's result, quadratic reciprocity, and the usual descent arguments, we see that, corresponding to the cases (I), (II) and (III) above, $p$ can be expressed by three distinct quadratic forms as follows:

$$p = a^2 + 8b^2 = c^2 - 8d^2 = 64e^2 + f^2. \tag{8}$$

Note that these may provide solutions to (I), (II) or (III) directly. If $a$ is a square, then (I) has the solution $r = \sqrt{a}, s = 1, t = b$; similarly if $c$ is a square, (II) is soluble, and if $e$ is a square, (III) is soluble. We shall see later that generators of the group $C_p$, when they exist, are given by solutions of (I) and (II) using (6).

For later use we have the following consequences of the equations (8):

$$(a/p) = (b/p) = (c/p) = (d/p) = (e/p) = (f/p) = 1, \tag{9}$$

$$a \equiv 1 \text{ or } 7 \pmod 8 \quad \text{and} \quad c \equiv 1 \text{ or } 3 \pmod 8. \tag{10}$$

For (9), we have by (8), $a^2 \equiv p \pmod{b}$, and so, by quadratic reciprocity, $(b/p) = 1$. Further, as both $-1$ and 2 are quartic residues modulo $p$, we can find an integer $n$ to satisfy $n^4 \equiv -8 \pmod{p}$ which, using (8) again, gives $(nb)^4 \equiv a^2b^2 \pmod{p}$ and $(\pm ab/p) = 1$ for some choice of the sign. But $p \equiv 1 \pmod{8}$, and so $(a/p) = 1$ follows by the first result. For (10), we have by (8) and as $a$ is odd, $(2p/a) = 1$, and so $(2/a) = 1$ by (9). Therefore, $a \equiv \pm 1 \pmod{8}$ follows using the properties of the Jacobi symbol. The remaining parts of (9) and (10) are proved similarly.

## 3. Two points known

In this section we show that if two of the equations (I), (II) or (III) are soluble, then the third is also soluble. We shall also give a characterization of the general solutions of each of these three equations. These provide an illustration of the operation of the Weil-Châtelet group of $C_p$, see Silverman [8, Chapter 10].

First we consider the case when a solution $\{r_1, s_1, t_1\}$ of equation (I) corresponding to the point $P_1$ on the curve $C_p$, and a solution $\{r_2, s_2, t_2\}$ of equation (II) corresponding to $P_2$ on $C_p$, are known. In this case we shall describe an algorithm which gives *two* solutions to equation (III); these solutions correspond to the points $P_1 + P_2$ and $P_1 - P_2$ on $C_p$. We may assume that $(r_1, s_1, t_1) = (r_2, s_2, t_2) = 1$.

We shall work with the following expressions:

$$
\begin{aligned}
&A = r_1s_1t_2 + r_2s_2t_1, && B = r_1s_1t_2 - r_2s_2t_1,\\
&C = (r_1^2r_2^2 - ps_1^2s_2^2)/8, && D = r_1^2s_2^2 + r_2^2s_1^2,\\
&K = r_2s_2t_2(r_1^4 + ps_1^4) - r_1s_1t_1(r_2^4 + ps_2^4),\\
&L = r_2s_2t_2(r_1^4 + ps_1^4) + r_1s_1t_1(r_2^4 + ps_2^4).
\end{aligned}
\tag{11}
$$

A number of identities exist between these expressions; they are given in the following lemmas. The most important is

**Lemma 1.** *The equation $AB = CD$ holds.*

*Proof.* We have

$$
\begin{aligned}
8AB &= 8t_2^2r_1^2s_1^2 - 8t_1^2r_2^2s_2^2\\
&= (r_2^4 - ps_2^4)r_1^2s_1^2 + (r_1^4 - ps_1^4)r_2^2s_2^2 \qquad \text{by (I) and (II)}\\
&= r_1^2r_2^2(r_1^2s_2^2 + r_2^2s_1^2) - ps_1^2s_2^2(r_1^2s_2^2 + r_2^2s_1^2) = 8CD. \qquad \square
\end{aligned}
$$

**Lemma 2.** *Let $U = r_1^2r_2^2 + ps_1^2s_2^2$ and $V = r_2^2s_1^2 - r_1^2s_2^2$. Then*

(i) $KL = AB(U^2 - pV^2)$,
(ii) $4(A^2 + B^2) = UV$,
(iii) $L^2 - K^2 = (A^2 - B^2)(64C^2 + pD^2)$.

*Proof.* (i) We have, using the identity

$$x^3 + 3x^2y - 3xy^2 - y^3 = (x - y)(x^2 + 4xy + y^2)$$

in the fourth line,

$$\begin{aligned}
8KL &= 8t_2^2r_2^2s_2^2(r_1^4 + ps_1^4)^2 - 8t_1^2r_1^2s_1^2(r_2^4 + ps_2^4)^2 \\
&= (r_2^4 - ps_2^4)r_2^2s_2^2(r_1^4 + ps_1^4)^2 + (r_1^4 - ps_1^4)r_1^2s_1^2(r_2^4 + ps_2^4)^2 \\
&= D[r_1^6r_2^6 + 3pr_1^4r_2^4s_1^2s_2^2 - 3p^2r_1^2r_2^2s_1^4s_2^4 \\
&\qquad - p^3s_1^6s_2^6 - p(r_1^2r_2^2 - ps_1^2s_2^2)(r_2^4s_1^4 + r_1^4s_2^4)] \\
&= 8DC[r_1^4r_2^4 + 4pr_1^2r_2^2s_1^2s_2^2 + p^2s_1^4s_2^4 - p(r_2^4s_1^4 + r_1^4s_2^4)] \\
&= 8AB(U^2 - pV^2)
\end{aligned}$$

by Lemma 1. Propositions (ii) and (iii) follow in a similar manner. □

**Lemma 3.** *The integers* $C, D, r_1, \ldots, t_2$ *satisfy the following congruence properties:*

(i) $r_1, r_2, s_1, s_2$ *are odd and* $C \in \mathbb{Z}$,
(ii) $p \nmid r_1r_2s_1s_2$ *and* $p \nmid C$,
(iii) $2 \parallel D$ *and* $t_1 \equiv t_2 \pmod 2$,
(iv) $2 \mid A$, $2 \mid B$, *and* $2 \mid C$.

*Proof.* Parts (i) and (ii) follow from our assumptions that $(r_1, s_1, t_1) = (r_2, s_2, t_2) = 1$. For (iii) and (iv), $D$ is even by (i) but, as $D$ is a sum of squares, $4 \mid D$ would contradict (i). Secondly, if $t_1$ and $t_2$ have different parities, then both $A$ and $B$ are odd, but this conflicts with the evenness of $D$ by Lemma 1, and so (iii) follows. Consequently, both $A$ and $B$ are even, and the evenness of $C$ follows by Lemma 1. □

**Definition.** Let the coordinates (see (6) and (7)) of the points $P_1, P_2, P_1 + P_2$ and $P_1 - P_2$ be denoted by $(x_1, y_1), (x_2, y_2), (x_{12}, y_{12})$ and $(x_{21}, y_{21})$, respectively.

The next two lemmas give expressions for $x_{12}, \ldots, y_{21}$.

**Lemma 4.** *We have* $x_{12} = K^2/16A^2B^2$, $x_{21} = L^2/16A^2B^2$.

*Proof.* The line through the points $(x_1, y_1)$ and $(x_2, y_2)$ has equation

$$(x_2 - x_1)y = (y_2 - y_1)x + y_1x_2 - x_1y_2.$$

If we let $r_1r_2s_1s_2 = Z$, then

$$\begin{aligned}
x_2 - x_1 &= 4AB/Z^2, \\
y_1x_2 - x_1y_2 &= 4t_1t_2K/Z^3, \\
y_2 - y_1 &= [r_1^3s_1^3t_2(r_2^4 + ps_2^4) - r_2^3s_2^3t_1(r_1^4 + ps_1^4)]/Z^3,
\end{aligned}$$

and our equation for the line becomes

$$4ABZy = [r_1^3s_1^3t_2(r_2^4 + ps_2^4) - r_2^3s_2^3t_1(r_1^4 + ps_1^4)]x + 4t_1t_2K. \tag{12}$$

Squaring both sides of this equation and replacing $y^2$ by $x^3 + px$, we obtain a cubic in $x$ whose roots are $x_1$, $x_2$ and $x_{12}$, viz:

$$(r_1^2 s_1^2 x - 4t_1^2)(r_2^2 s_2^2 x - 4t_2^2)(16A^2B^2x - K^2) = 0,$$

and the result follows. An exactly similar argument gives the value of $x_{21}$. □

**Lemma 5.** *We have*

$$\text{(i)} \qquad y_{12} = [K(64A^2C^2 + pB^2D^2)]/64A^3B^3,$$

$$\text{(ii)} \qquad y_{21} = -[L(64B^2C^2 + pA^2D^2)]/64A^3B^3.$$

*Proof.* By Lemma 4, (i) follows by substituting the value of $x_{12}$ in (12) and collecting terms, and (ii) follows similarly. □

**Theorem 1.** *We have*

$$\text{(i)} \qquad -K^2 = 64A^2C^2 - pB^2D^2,$$

$$\text{(ii)} \qquad -L^2 = 64B^2C^2 - pA^2D^2.$$

*Proof.* (i) As $(x_{12}, y_{12})$ is a point on $C_p$, we have, by Lemmas 4 and 5, and dividing by $K^2/(4AB)^6$,

$$(64A^2C^2 + pB^2D^2)^2 = K^4 + 256pA^4B^4 = K^4 + 256pA^2B^2C^2D^2$$

by Lemma 1. Hence,

$$\pm K^2 = 64A^2C^2 - pB^2D^2. \tag{13}$$

To evaluate the sign, suppose $2^t \parallel B$; then by Lemmas 1 and 3 we have $2^{2t+2} \parallel pB^2D^2$ and $2^{2t+6} \mid 64A^2C^2$. Hence, $2^{2t+2} \parallel K^2$, which shows that $\pm K^2/2^{2t+2}$ and $-pB^2D^2/2^{2t+2}$ are odd integers congruent modulo 8. Therefore, the only possible sign in (13) is minus, and (i) follows. The proof of (ii) is similar. □

This theorem provides an algorithm for solving equation (III) in §2 as follows: In (i) of Theorem 1 cancel the common factors of $K$, $AC$ and $BD$ (or of $L$, $BC$ and $AD$ in part (ii)); then $AC$ and $BD$ become squares (and similarly for $BC$ and $AD$), thus providing the required solutions. To justify this, we consider first the case when $A$, $B$, $C$ and $D$ have a common factor.

**Lemma 6.** *If $q$ divides $A$, $B$, $C$ and $D$, then $q^2$ divides both $K$ and $L$.*

*Proof.* By Lemmas 1 and 3 we note that 2 divides $A$, $B$, $C$ and $D$, no higher power of 2 has this property, and, by definition, 4 divides both $K$ and $L$. Hence, as $p \nmid q$, we may assume that $q$ is coprime to both 2 and $p$.

Secondly, with $U$ and $V$ as given in Lemma 2, we have $U^2 + pV^2 = 64C^2 + pD^2$, and so $q^2 \mid U^2 + pV^2$ and, by Lemma 2, $q^2 \mid UV$. Together, these show that $q \mid U$ and $q \mid V$. Hence, by Lemma 2 again, we see that $q^4 \mid KL$ and $q^4 \mid L^2 - K^2$, and the lemma follows. □

Now let $q^{u_1} \parallel A$, $q^{u_2} \parallel B$, $q^{u_3} \parallel C$ and $q^{u_4} \parallel D$. By Lemma 7 we may assume that one of $u_1$, $u_2$, $u_3$ or $u_4$ is zero. So, for the first case, suppose $u_1$ is zero, and then (by Lemma 1) $u_2 = u_3 + u_4$. This gives $q^{u_3} \parallel AC$, $q^{u_3+2u_4} \parallel BD$, $q^{2u_3+u_4} \parallel BC$, and $q^{u_4} \parallel AD$. Hence, the factor $q^{2u_3}$ can be cancelled from both sides of equation (i) in Theorem 1. Now the only occurrence of

$q$ in this equation is: $q^{4u_4}$ in the prime factorization of $B^2D^2$. Similarly, in equation (ii), $q^{2u_4}$ can be cancelled throughout, leaving the factor $q^{4u_3}$ in $B^2C^2$. The cases when $u_2$, $u_3$ or $u_4$ are zero can be dealt with similarly. If this process is carried out on all primes dividing $AB$, then, via Theorem 1, two solutions of equation (III) are given by this algorithm.

We shall illustrate this algorithm with the prime 11969. We have (see (8))

$$11969 = 81^2 + 8 \times 26^2 = 113^2 - 8 \times 10^2 = 65^2 + 64 \times 11^2.$$

Now 81 is a square, and so we have a solution to equation (I) given by: $r_1 = 9, s_1 = 1, t_1 = 26$. Secondly, although 113 is not a square, we have $(113 + 10\sqrt{8})(3 + \sqrt{8})^2 = 2401 + 848\sqrt{8}$ (using the identity $3^2 - 8 \times 1^2 = 1$), and so equation (II) has the solution: $r_2 = 49, s_2 = 1, t_2 = 848$. Substituting these values in (11), we obtain

$$A = 8906 = 2 \times 61 \times 73, \qquad B = 6358 = 2 \times 11 \times 17^2,$$
$$C = 22814 = 2 \times 11 \times 17 \times 61, \qquad D = 2842 = 2 \times 17 \times 73,$$
$$K = 4 \times 5 \times 11 \times 17 \times 73 \times 2131, \qquad L = 4 \times 5 \times 17 \times 61 \times 102301.$$

Now $AC = 61^2 \times 4 \times 11 \times 17 \times 73$ and $BD = 17^2 \times 4 \times 11 \times 17 \times 73$. Hence, we can cancel the factor $(4 \times 11 \times 17 \times 73)^2$ from (11) and we obtain the following solution of (III):

$$-10655^2 = 64 \times 61^4 - 11969 \times 17^4.$$

Similarly, $BC = 11^2 \times 17^2 \times 4 \times 17 \times 61$ and $AD = 73^2 \times 4 \times 17 \times 61$, and so the second solution is

$$-511505^2 = 64 \times 187^4 - 11969 \times 73^4.$$

**Further algorithms.** An exactly similar algorithm to the above exists when solutions of (I) and (III) are known, or when solutions to (II) and (III) are known. Suppose $\{r_1, s_1, t_1\}$ is a solution to (III) corresponding to the point $Q_1 = (x_1', y_1')$ on the curve $C_p$ with $(r_1, s_1, t_1) = 1$, and $\{r_2, s_2, t_2\}$ is a solution to (I) [or (II)] corresponding to the point $Q_2 = (x_2', y_2')$ on the curve $C_p$ with $(r_2, s_2, t_2) = 1$. Following the procedure above, we define

$$A' = 8r_1s_1t_2 + r_2s_2t_1, \qquad B' = 8r_1s_1t_2 - r_2s_2t_1, \tag{14}$$
$$C' = 8r_1^2r_2^2 \pm ps_1^2s_2^2, \qquad D' = 8r_1^2s_2^2 \mp r_2^2s_1^2,$$

where the upper signs apply when $\{r_2, s_2, t_2\}$ is a solution to (I), and the lower signs apply when equation (II) is the given one. As in Lemma 1, it is a simple matter to show that $A'B' = C'D'$. Also, we define $K'$ and $L'$ by

$$K' = r_1s_1t_1(r_2^4 + ps_2^4) - r_2s_2t_2(64r_1^4 + ps_1^4),$$
$$L' = r_1s_1t_1(r_2^4 + ps_2^4) + r_2s_2t_2(64r_1^4 + ps_1^4),$$

and if $Q_1 + Q_2 = (x'_{12}, y'_{12})$ and $Q_1 - Q_2 = (x'_{21}, y'_{21})$, then

$$x'_{12} = 4K'^2/A'^2B'^2, \qquad y'_{12} = K'(A'^2C'^2 + pB'^2D'^2)/A'^3B'^3,$$
$$x'_{21} = 4L'^2/A'^2B'^2, \qquad y'_{21} = -L'(B'^2C'^2 + pA'^2D'^2)/A'^3B'^3.$$

Corresponding to Theorem 1 we have

**Theorem 2.** *There holds*

$$\text{(i)} \qquad \pm 8K'^2 = A'^2C'^2 - pB'^2D'^2,$$
$$\text{(ii)} \qquad \pm 8L'^2 = B'^2C'^2 - pA'^2D'^2,$$

*where the upper signs apply if* $\{r_2, s_2, t_2\}$ *is a solution to equation* (I), *and the lower signs apply when a solution to equation* (II) *is given.*

*Proof.* See the proof of Theorem 1. □

The algorithm described above also applies here. In (i) of Theorem 2 we cancel the common factors of $K'$, $A'C'$ and $B'D'$, and the resulting expressions provide solutions to (II) [or (I)] as $A'C'$ and $B'C'$ are then squares. Note that we obtain *two* solutions corresponding to the points $Q_1 + Q_2$ and $Q_1 - Q_2$. Therefore, if $Q_1 = P_1 + P_2$ and $Q_2 = P_1$, our new solutions to equation (II) [or (I)] given by Theorem 2 correspond to the points $P_2$ and $2P_1 + P_2$ on $C_p$.

We shall show now that this is always the case. If we have a solution to one of our equations $(*)$ (where $(*)$ is (I), (II) or (III)), with corresponding point $P \in C_p$, then, for all points $R \in C_p$, there is another solution to $(*)$ corresponding to the point $P + 2R$, and all solutions of $(*)$ are generated in this way.

**Theorem 3.** *Suppose we are given a nontrivial solution to equation* (I), (II) *or* (III) *corresponding to the point* $P \in C_p$; *then this equation has infinitely many solutions, and the corresponding points on* $C_p$ *have the form* $P + 2R$, *where* $R$ *is an arbitrary point on* $C_p$.

*Note.* We are not assuming that the points $P$ and $R$ are of the same type.

*Proof.* We use the same method as in the previous two cases. We shall give the proof for equations (I) and (II); an exactly similar argument applies in the remaining cases. Suppose the point $P$ has coordinates $(4t^2/r^2s^2)$, $t(r^4 + ps^4)/r^3s^3$, where $\mp 8t^2 = r^4 - ps^4$, and $R$ has coordinates $(a^2/c^2, ab/c^3)$, where $b^2 = a^4 + pc^4$ (see (3) and (7)). The coordinates of $2R$ are

$$((a^4 - pc^4)^2/4a^2b^2c^2, (a^4 - pc^4)(a^8 + 6pa^4c^4 + p^2c^8)/8a^3b^3c^3),$$

and we may assume that $r$ and $s$ are odd, and $a$ and $c$ have different parities. Following the procedures above, we define

$$A'' = 4tabc + rs(a^4 - pc^4), \qquad B'' = 4tabc - rs(a^4 - pc^4),$$
$$C'' = \mp r^2b^2 + 2ps^2a^2c^2, \qquad D'' = 2r^2a^2c^2 \pm s^2b^2,$$
$$K'' = rst(a^8 + 6pa^4c^4 + p^2c^8) - abc(r^4 + ps^4)(a^4 - pc^4)/2,$$

where the upper [lower] signs apply when equation (I) [(II)] is being used.

**Lemma 7.** *We have* $A''B'' = C''D''$.

*Proof.* Using the equations $\mp 8t^2 = r^4 - ps^4$ and $b^2 = a^4 + pc^4$, we obtain

$$\begin{aligned} C''D'' &= \mp 2r^4a^2b^2c^2 - r^2s^2b^4 + 4pr^2s^2a^4c^4 \pm 2ps^4a^2b^2c^2 \\ &= \mp 2a^2b^2c^2(r^4 - ps^4) - r^2s^2(b^4 - 4pa^4c^4) = A''B''. \end{aligned}$$ □

Continuing the main proof, we see that the coordinates of the point $P + 2R$ are

$$(4K''^2/A''^2B''^2,\ K''(A''^2C''^2 + pB''^2D''^2)/A''^3B''^3),$$

and we have

$$\mp 8K''^2 = A''^2C''^2 - pB''^2D''^2.$$

We now cancel the common factors of $K''$, $A''C''$ and $B''D''$ in this equation, and the result is a new solution to equation (I) [or (II)]; the details follow exactly those given above for Lemmas 2 and 6. □

**Example.** Let $p = 73$ and let $P$ and $R$ be the generators of the group $C_p$ corresponding to equations (I) and (II), respectively. Hence, using the supplement table, (I), (3) and (4), we have $r = s = 1$, $t = 3$, $a = 2$, $b = 77$ and $c = 3$, and substituting these values in the above, we have

$$A'' = -353, \quad B'' = 17 \times 673, \quad C'' = -673, \quad D'' = 17 \times 353,$$
$$K'' = 353 \times 673 \times 873.$$

These values now give a new solution to equation (I) corresponding to the point $P + 2R$ [as $(353, 673) = 1$]:

$$1^4 - 73 \times 17^4 = -8 \times 873^2.$$

Finally, we prove the converse of Theorem 3; again the method of proof is very similar to that used in the above proofs.

**Theorem 4.** *If* $\{r_1, s_1, t_1\}$ *and* $\{r_2, s_2, t_2\}$ *are two solutions to one of the equations* (I), (II) *or* (III) *with corresponding points* $P_1$ *and* $P_2$, *then there is a point* $R \in C_p$ *with the property* $P_2 = P_1 + 2R$.

*Proof.* We give the proof for equation (I); the same argument applies in the remaining cases. As above, we define

$$\begin{aligned} A^* &= r_1s_1t_2 + r_2s_2t_1, & B^* &= r_1s_1t_2 - r_2s_2t_1, \\ C^* &= r_1^2r_2^2 + ps_1^2s_2^2, & D^* &= (r_1^2s_2^2 - r_2^2s_1^2)/8, \end{aligned}$$

$$\begin{aligned} K^* &= r_2s_2t_2(r_1^4 + ps_1^4) - r_1s_1t_1(r_2^4 + ps_2^4), \\ L^* &= r_2s_2t_2(r_1^4 + ps_1^4) + r_1s_1t_1(r_2^4 + ps_2^4). \end{aligned}$$

Repeating the arguments of Lemmas 1 to 6, we have

$$A^*B^* = C^*D^*,$$

the coordinates of $P_2 - P_1$ are

$$(L^{*2}/16A^{*2}B^{*2}, -L^*(B^{*2}C^{*2} - 64pA^{*2}D^{*2})/64A^{*3}B^{*3}),$$

and

$$L^{*2} = B^{*2}C^{*2} - 64pA^{*2}D^{*2}.$$

Note that we have a plus sign on the left-hand side of this last equation, as $2 \parallel C^*$ in this case; see the proof of Theorem 1. The result now follows using (5) of §2. □

## 4. One point known

In view of the results above a natural question to ask is: suppose we are given a solution to just one of our equations (I), (II) or (III); is there an algorithm which will generate solutions to the remaining two equations? This is a much harder problem; it is not definitely known that solutions exist, but we have the

**Conjecture.** If $p$ is a G-prime and the rank of the curve $C_p$ is not zero, then it equals 2.

Silverman [8], and others, have shown that this Conjecture is a consequence of the Shafarevich-Tate Conjecture, which states that the Shafarevich-Tate group Ш for $C_p$ is finite. Although some progress has been made on this second conjecture recently, it remains open at this time. The numerical evidence presented below shows that our conjecture is valid for all primes $p < 50000$. Also, this Conjecture can be replaced by the following apparently simpler question.

Suppose we have a solution $\{r, s, t\}$ to equation (I) [the argument is similar in the other two cases]. Then we can find solutions to equations (II) and (III) provided we can find a nontrivial simultaneous integer solution $\{x, y, z, w\}$ to the pair of equations

$$x^2 + 16txy - 8r^4y^2 = 8s^4z^2 + pw^2,$$
$$xy = zw.$$

Using (9) and (10), we can easily show that this pair of equations has common local solutions for all primes $q$. But this does not necessarily lead to simultaneous integer (global) solutions. We note that the second equation above is identical to that in Lemma 1; there it was the main link in the algorithm, here it seems to be the main stumbling block to progress; for further details see Rose [6].

## 5. Numerical data

Extensive computer searches have been undertaken to find the ranks and generators of the curves (1) for all G-primes $p < 50000$; the results are presented in the supplement. After some preliminary trials using a HP 28s calculator, the main searches were made using the package PARI/GP (developed by Cohen and his collaborators in Bordeaux, France) on a Sun 4. First, attempts were made to solve one or more of the equations (I), (II) and (III). If these failed to give solutions, then the value of the $L$-function for the curve at $s = 1$ was

calculated in order to prove that the rank was indeed zero, that is, (I), (II) and (III) are insoluble; see below.

The method used to attempt to solve our equations is as follows. First consider equation (I). Note, by (10), we can choose the sign of $a$ so that $a \equiv 1 \pmod 8$. Rewriting (I) and using (8), we look for integers $x$ and $y$ to satisfy

$$(a^2 + 8b^2)(x^2 + 8y^2) = (ax \pm 8by)^2 + 8(ay \mp bx)^2 = r^4 + 8t^2 = ps^4;$$

that is, we look for $s$, $x$ and $y$ to satisfy

$$x^2 + 8y^2 = s^4, \qquad ax \pm 8by \text{ is a square, } r^2, \tag{15}$$

and then $t = ay \mp bx$. The equation in (15) has the parametric solution

$$x = (m^2 - 2n^2)^2 - 8m^2n^2, \quad y = 2mn(m^2 - 2n^2), \quad s = m^2 + 2n^2.$$

Hence, using (15), we try various integers $m$ and $n$ until we find a pair such that

$$a((m^2 - 2n^2)^2 - 8m^2n^2) + 16bmn(m^2 - 2n^2) \text{ is a square, } r^2, \tag{16}$$

and then the values of $s$ and $t$ are determined using the above. For equation (II) the left-hand side of (16) is replaced by $c((m^2 + 2n^2)^2 + 8m^2n^2) + 16dmn(m^2 + 2n^2)$ [if $c \equiv 3 \pmod 8$, put $3c \pm 8d$ for $c$ and $c \pm 3d$ for $d$, see (8) and (9)], and for equation (III) the left-hand side of (16) is replaced by $\pm e((m^2 - 4n^2)^2 - 16m^2n^2) + fmn(m^2 - 4n^2)$, where both signs must be considered.

The method can be extended in the following way. Multiplying (16) by $a$ and rewriting, we have

$$w^2 = 8pu^2 + av^2, \tag{17}$$

where

$$u = mn, \quad v = r \quad \text{and} \quad w = a(m^2 - 2n^2) + 8bmn. \tag{18}$$

Using (9) and (10), we can easily see that equation (17) is soluble by Legendre's Theorem. Hence, one way to solve (I) is to look for general solutions to (17) subject to the conditions (18). In practice we found the most efficient method was to use (16) directly. First we tried all values of $m$ and $n$ satisfying $0 < m < 500$ and odd, and $-250 < n < 250$. If this failed, using the first few primes $q$, we sieved out those values of $m$ and $n$ for which (16) is impossible modulo $q$, and then tried larger values of $m$ and $n$ to solve (16). For example, if $p \equiv 2 \pmod 5$ (generally the most intractable case), then $5 \mid r$ and so the left-hand side of (16) must be congruent to 25 modulo 100.

It is worth pointing out that, for each G-prime $p$ under consideration, in all cases where solutions to one of the equations (I), (II) or (III) were found, solutions to the remaining two equations were also found—the prime 41521 was by far the most refractory—that is, in all 366 cases where the rank of the corresponding curve is positive, it does, in fact, equal two. Also in all of these cases, at least one of the three equations has a 'small' solution; that is, one with $m$ and $n$ (in (16) or its replacements for equations (II) or (III)) less than 20, the 'worst' case (for primes less than 50000) being $p = 47497$, where, for equation (II), the smallest solution is given by $m = 7$ and $n = 18$. Note that

the smallest solutions of the two remaining equations can be very 'large', for example with the prime $p = 41521$. In this example the smallest solutions for equations (I) and (II) are given in the supplement (for (I) the solution is generated by $m = 156347$, $n = 41668$), but note that equation (III) has the solution 5, 1, 39 and the corresponding values of $m$ and $n$ in this case are 1 and 0, respectively.

Rubin [7], developing some work of Kolyvagin and others, has proved some parts of the Birch and Swinnerton-Dyer Conjecture. In particular he has shown that, if an elliptic curve has complex multiplication (our curves $C_p$ have complex multiplication in the field $\mathbb{Q}(i)$ of Gaussian numbers), and if the value of the $L$-function for the curve at the point $s = 1$ is nonzero, then the curve has only finitely many points defined over $\mathbb{Q}(i)$; and so the rank of the curve over $\mathbb{Q}$ is zero. We applied this to our numerical work. For those curves $C_p$ where we were unable to find solutions to equations (I), (II) or (III) after fairly short trials, we calculated the values at $s = 1$ of the corresponding $L$-functions. In all cases we found these values to be positive, and hence, by the result quoted above, the ranks are zero and no further trials were required. Following Buhler, Gross and Zagier [3], we used the following formula to calculate the $L$-function:

$$L(C_p, 1) = 2\sum_{n=1}^{\infty} \frac{a_p(n)}{n} \exp\left(\frac{-\pi n}{4p}\right),$$

where $a_p(q)$ is the trace of Frobenius for primes $q$, and it is extended to all positive integers in the usual way (see, for example, Cohen [4, p. 406]). [Note that the curve $C_p$ has conductor $64p^2$, and the factor 2 occurs because the sign of the functional equation is positive for all of our curves; this was calculated using the method given in Cohen [4, p. 406].] To keep the computations within reasonable time bounds, we replaced $\infty$ in the above sum by $16p$ and took the sum over those $n$ satisfying $n \equiv 1 \pmod 4$, because for all curves under consideration the coefficients $a_p(n)$ are zero otherwise. If we then divided the result by the product of the real period, the Tamagawa numbers (in all cases $c_p = 2$ and the remainder are all equal to 1), and the inverse of the square of the order of the torsion subgroup of $C_p$ ($= 1/4$ in all cases, see (2)) as required by the Birch and Swinnerton-Dyer Conjecture, we obtained in all cases a square integer to at least five decimal places. Hence, as a by-product of these calculations we obtained (assuming the validity of this conjecture) the values $S$ of the orders of the Shafarevich-Tate groups Ш. For all G-primes $p$ for which $r(C_p) = 0$ we found that $S = 16$ except in the following cases: $S = 64$ when $p$ is one of the following 28 primes:

| | | | | | | |
|---|---|---|---|---|---|---|
| 4937 | 12161 | 15017 | 25601 | 31337 | 33937 | 44497 |
| 10657 | 12697 | 18257 | 26497 | 31817 | 34297 | 47161 |
| 10937 | 13417 | 23857 | 28697 | 32297 | 35897 | 47657 |
| 11777 | 14897 | 25057 | 29761 | 33377 | 36857 | 47777 |

and $S = 144$ when $p$ is

21577, 28537, 30937.

Note the connection between the fact that in all cases $16 \mid S$ and the 4-descent described above, and that the structure of Ш is determined by the corresponding 2-descent and the Cassels pairing $\mathbb{Z}/\sqrt{S}\mathbb{Z} \times \mathbb{Z}/\sqrt{S}\mathbb{Z}$. Some authors have suggested that the value of $S$ increases, if only slowly, as the value of the conductor increases. In particular, if $S_p$ denotes the order of Ш for the elliptic curve $C_p$, then it is conjectured that for large $p$ the approximate value of $S_p$ is $p^{1/4\pm o(1)}$. Our data shows a fairly uniform spread through the range 1—50000 for the higher values of $S$, and so no conclusions can be drawn from our calculations. Owing to the computer time required, we did not calculate the orders $S$ of the groups Ш for those primes $p$ where $r(C_p) = 2$; this will be undertaken in the sequel.

Our calculations have established the values of $r(C_p)$ for all primes $p$ less than 50000 and congruent to 1 modulo 8. For the 629 non G-primes $q$, $r(C_q) = 0$ (see §2), and for the 625 G-primes $p$ the table in the supplement gives either the value of the $L$-function at $s = 1$ when $r(C_p) = 0$ (in 259 cases), or the values of $r$ and $s$ for equations (I) and (II) when $r(C_p) = 2$ from which the coordinates of the generators of the group $C_p$ can easily be calculated using (6) (366 cases in all). In some cases equations (I) or (II) have two distinct solutions where both $r$ and $s$ are roughly similar in size; in these cases the solution with the smaller value of $s$ was chosen. This was not checked in all cases.

Finally, at the referee's suggestion and after some discussions with John Cremona, we have included some data on the Mordell-Weil lattices of the rank-two curves. Suppose $P_1$ and $P_2$ generate $C_p$ modulo torsion (that is, $C_p$ is generated by $P_1$, $P_2$ and $(0, 0)$, see (2)). Let $\langle P_i, P_j \rangle$, for $i, j = 1$ or 2, denote the Néron-Tate height pairing and let $R_{C_p}$ denote the elliptic regulator of $C_p$, see Silverman [8, p. 232]. Over the complex field $\mathbb{C}$, the generators of the Mordell-Weil lattice $\Lambda$ for $C_p$ can be taken to be

$$\omega_1 = \sqrt[+]{\langle P_1, P_1 \rangle},$$

$$\omega_2 = (\langle P_1, P_2 \rangle + i\sqrt{R_{C_p}})/\sqrt[+]{\langle P_1, P_1 \rangle}.$$

Then the invariant $\tau$, a complex number in the upper half-plane, is defined by

$$\tau = \omega_2/\omega_1 = (\langle P_1, P_2 \rangle + i\sqrt{R_{C_p}})/\langle P_1, P_1 \rangle$$

modulo transformations by elements of $SL(2, \mathbb{Z})$. Once $\tau$ has been moved to the fundamental region of the group $SL(2, \mathbb{Z})$, it is independent of the choice of the generators $P_1$ and $P_2$ of $C_p$, and so provides information about the shape of the Mordell-Weil lattice $\Lambda$.

For each of the rank-2 curves discussed in this paper we computed (using PARI/GP) the value of $\tau$, and these values are given in the table in the supplement. In some cases, to obtain a value of $\tau$ in the fundamental region of $SL(2, \mathbb{Z})$, $\pm 1$ was added to the computed complex number; no other $SL(2, \mathbb{Z})$ transformation was required. In this region the values of $\tau$ for approximately half of the curves under consideration lie in a segment of the annular region bounded by the ellipses $375x^2 + y^2 = 100$ and $480x^2 + y^2 = 200$, and the lines $2x \pm 1 = 0$, where $x$ denotes the real part and $y$ the imaginary part. Only six values of $\tau$ lie below this region, and the remainder above. Also the

proportion of values of $\tau$ with positive or negative real part is approximately equal, and those with larger imaginary part tend to correspond with the larger values of the prime $p$.

## BIBLIOGRAPHY


1. A. Bremner and J. W. S. Cassels, *On the equation* $Y^2 = X(X^2 + p)$, Math. Comp. **42** (1984), 257–264.
2. A. Bremner, *On the equation* $Y^2 = X(X^2 + p)$, Number Theory and Applications (R. A. Mollin, ed.), Kluwer, Dordrecht, 1989, pp. 3–23.
3. J. Buhler, B. Gross, and D. Zagier, *On the conjecture of Birch and Swinnerton-Dyer for a curve of rank* 3, Math. Comp. **44** (1985), 473–481.
4. H. Cohen, *A course in computational algebraic number theory,* Springer, Berlin, 1993.
5. L. J. Mordell, *The diophantine equation* $x^4 + my^4 = z^2$, Quart. J. Math. (2) **18** (1967), 1–6.
6. H. E. Rose, *On a class of elliptic curves with rank at most two,* University of Bristol preprint, 1992.
7. K. Rubin, *The one-variable main conjecture for elliptic curves with complex multiplication, L*-functions and Arithmetic (J. Coates and M. J. Taylor, eds.), Cambridge Univ. Press, Cambridge, 1991.
8. J. H. Silverman, *The arithmetic of elliptic curves,* Springer, New York, 1986.


DEPARTMENT OF MATHEMATICS, UNIVERSITY OF BRISTOL, UNIVERSITY WALK, BRISTOL BS8 1TW, UNITED KINGDOM

*E-mail address*: h.e.rose@bris.ac.uk