ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 24, Number 3, Summer 1994

ON THE EQUATION $Y^2 = (X + p)(X^2 + p^2)$

ROEL J. STROEKER AND JAAP TOP

ABSTRACT. In this paper the family of elliptic curves over $\mathbf{Q}$ given by the equation $y^2 = (x + p)(x^2 + p^2)$ is studied. It is shown that for p a prime number $\equiv \pm 3 \bmod 8$, the only rational solution to the equation given here is the one with $y = 0$. The same is true for $p = 2$. Standard conjectures predict that the rank of the group of rational points is odd for all other primes p. A lot of numerical evidence in support of this is given. We show that the rank is bounded by 3 in general for prime numbers p. Moreover, this bound can only be attained for certain special prime numbers $p \equiv 1 \bmod 16$. Examples of such rank 3 curves are given. Lastly, for certain primes $p \equiv 9 \bmod 16$ nontrivial elements in the Shafarevich group of the elliptic curve are constructed. In the literature one finds similar investigations of elliptic curves with complex multiplication. It may be interesting to note that the curves considered here do not admit complex multiplication.

1. Introduction. Let p be a prime number. Throughout this paper $E_p/\mathbf{Q}$ will denote the elliptic curve given by the equation $y^2 = (x+p)(x^2+p^2)$. The change of variable $x = \xi - p$ yields another model $y^2 = \xi(\xi^2 - 2p\xi + 2p^2)$ for E_p. This paper is devoted to the study of the finitely generated abelian group $E_p(\mathbf{Q})$ consisting of the $\mathbf{Q}$-rational points on E_p. The torsion subgroup of $E_p(\mathbf{Q})$ is given by

Proposition 1.1. *$E_p(\mathbf{Q})_{\text{tor}} \cong \mathbf{Z}/2\mathbf{Z}$, with the $\mathbf{Q}$-rational point having $y = 0$ as a generator.*

Proof. If $l \in \mathbf{Z}$, $l \geq 5$ is a prime where E_p has good reduction (i.e., $l \neq 2$ and $l \neq p$), then the homomorphism 'reduction modulo l' : $E_p(\mathbf{Q})_{\text{tor}} \to E_p(\mathbf{F}_l)$ is known to be injective [**12**, p. 176]. Now for $l = 5, 7, 11$ and $p \neq 5, 7, 11$, respectively, $E_p(\mathbf{F}_l)$ consists of 6 ± 2, respectively 8 ± 2, respectively 12 ± 4, points; the sign depending on whether p is a square modulo l or not. From this, it follows that the torsion subgroup of $E_p(\mathbf{Q})$ has order at most 2. Since it always contains a point of order 2 the proposition follows. □

Received by the editor on July 2, 1993.

The L-series $L(E_p, s)$ is the complex function defined for $\mathrm{Re}\,(s) > 3/2$ by the Euler product

$$L(E_p, s) = \prod_{l \neq 2, l \neq p} \frac{1}{1 - a_l l^{-s} + l^{1-2s}}$$

in which a_l is defined by $1 - a_l + l = \#E_p(\mathbf{F}_l)$. In general, not much is known about the L-series of an elliptic curve. For the curves $E_p/\mathbf{Q}$, however, one has

Proposition 1.2. *The curves $E_p/\mathbf{Q}$ are modular elliptic curves of conductor $N = 128p^2$ for $p > 2$, respectively $N = 128$ for $p = 2$. In particular, $L(E_p, s)$ extends to a holomorphic function on all of $\mathbf{C}$ and satisfies a functional equation*

$$(2\pi)^{-s}\Gamma(s)L(E_p, s) = \pm N^{1-s}(2\pi)^{s-2}\Gamma(2-s)L(E_p, 2-s).$$

Here the sign ± 1 is $+1$ for $p = 2$ and for $p \equiv \pm 3 \bmod 8$; it is -1 for $p \equiv \pm 1 \bmod 8$.

Proof. Write $E_\pm$ for the elliptic curves of conductor 128 given by $y^2 = x^3 \pm 2x^2 + 2x$. Combining a theorem of Ogg [**11**]—who found all elliptic curves over $\mathbf{Q}$ of 2-power conductor—with Honda and Miyawaki's complete table [**8**] of all modular forms of weight 2, trivial character and level a power of 2, it follows that E_+ and E_- and E_2 are modular. Moreover, the curve E_2 is isomorphic over $\mathbf{Q}$ to the curve listed $128G$ in Table 1 of [**2**, pp. 81–113]. From Table 3 of [**2** pp. 116–122], one concludes that the functional equation of $L(E_2, s)$ indeed has a $+$-sign. So from now on, we may and will assume $p > 2$.

From the fact that E_p and E_+ are isomorphic over $\mathbf{Q}(\sqrt{-p})$ (and similarly E_p and E_- over $\mathbf{Q}(\sqrt{p})$), one deduces that $L(E_p, s) = L(E_+, s, \chi)$ in case $p \equiv 3 \bmod 4$, while for $p \equiv 1 \bmod 4$, the equality $L(E_p, s) = L(E_-, s, \chi)$ holds. Here χ is the unique quadratic Dirichlet character of conductor p, and $L(s, \chi)$ denotes the L-series $\sum \chi(n)a_n n^{-s}$ in case $L(s) = \sum a_n n^{-s}$. Using, e.g., [**9**, p. 127], it follows that E_p is modular too. Furthermore, the sign of its functional equation is obtained by multiplying the sign in $L(E_\pm, s)$ by $\chi(-128)$, as explained in [**2**, pp. 7–9].

Now E_+ is $\mathbf{Q}$-isomorphic to the curve listed $128A$ in [**2**], which has sign $+1$ in its functional equation. Similarly, $E_- \cong 128C$, which has a sign -1. From this, the proposition easily follows. □

The conjectures of Birch and Swinnerton-Dyer predict that the rank of the group $E(\mathbf{Q})$ of rational points on an elliptic curve $E/\mathbf{Q}$ equals the order of vanishing at $s = 1$ of $L(E, s)$. In our particular case this means that the rank of $E_p(\mathbf{Q})$ should be odd if $p \equiv \pm 1 \bmod 8$ and even, otherwise. Part of this will be proven in Section 3 below.

Theorem 1.3. *For $p = 2$ and for $p \equiv \pm 3 \bmod 8$ one has rank $E_p(\mathbf{Q}) = 0$.*

The case $p = 2$ can be read off from [**2**, Table 1]. We will ignore it in the remainder of this paper.

As discussed above, in the remaining case $p \equiv \pm 1 \bmod 8$, the Birch and Swinnerton-Dyer conjectures would imply

Conjecture 1.4. *The equation $y^2 = (x+p)(x^2+p^2)$ has infinitely many rational solutions for every prime number $p \equiv \pm 1 \bmod 8$.*

It is quite feasible that the case $p \equiv -1 \bmod 8$ of this conjecture can be settled using Heegner points on the modular curve $X_0(128)$, as explained in [**1**]. This method is known to work precisely when the derivative $L'(E_p, 1) \neq 0$, by the Gross and Zagier theorem [**7**]. An indication that this nonvanishing should be the case is given by

Theorem 1.5. $\operatorname{rank} E_p(\mathbf{Q}) \leq 1$ *for $p \equiv -1 \bmod 8$.*

We will prove this in Section 3.

If $p \equiv 1 \bmod 8$, the conjecture may be a lot harder. To state our results for this case, note that $\sqrt{-1}$ exists in $\mathbf{F}_p$ for these primes. Also, since $(1+\sqrt{-1})(1-\sqrt{-1}) = 2$ is a square in $\mathbf{F}_p$, the Legendre symbol $((1+\sqrt{-1})/p)$ does not depend on the choice of $\sqrt{-1} \in \mathbf{F}_p$.

Theorem 1.6. *For a prime* $p \equiv 1 \bmod 8$ *one has* $\operatorname{rank} E_p(\mathbf{Q}) \leq 1$, *unless* $p \equiv 1 \bmod 16$ *and* $((1+\sqrt{-1})/p) = 1$. *If each one of these latter conditions holds, then* $\operatorname{rank} E_p(\mathbf{Q}) \leq 3$. *The case* $\operatorname{rank} E_p(\mathbf{Q}) = 3$ *really occurs*; *examples are furnished by* $p = 337$ *and* $p = 1201$.

The proof of this is given in Sections 4 and 7 below.

2. Selmer groups corresponding to 2-isogenies. In this section the classical Selmer and Shafarevich groups which play a role in rank calculations are reviewed. Using these notions we will be able to state the results mentioned in the previous section in a more precise form.

Note that the curves E_p we study are equipped with a rational point of order 2. A general procedure for finding the rank of such a curve over $\mathbf{Q}$ was given by Tate in his 1961 Haverford lectures; it is recalled by various authors, e.g., [**6**], [**12**, pp. 301–302]. We will briefly describe this method and indicate the cohomological interpretation of the basic homomorphism to $\mathbf{Q}^*/\mathbf{Q}^{*2}$ which it involves.

Suppose $E/\mathbf{Q}$ is an elliptic curve given by an equation $y^2 = x(x^2 + ax + b)$ with $a, b \in \mathbf{Z}$. Translation over the point $(0,0)$ gives rise to an involution on the function field $\mathbf{Q}(E)$. Denote this translation by

$$(\xi, \eta) = (x, y) + (0, 0).$$

The field of functions which are invariant under the involution is generated by

$$X = \xi + x + a = \frac{y^2}{x^2} \quad \text{and} \quad Y = -y - \eta = y\left(\frac{b - x^2}{x^2}\right),$$

which satisfy $Y^2 = X(X^2 - 2aX + a^2 - 4b)$. Denote the curve defined by the latter equation by E' (compare [**12**, p. 74]). The morphism $\psi : E \to E'$, given by: $(x, y) \mapsto (X, Y)$, defines homomorphisms $E(K) \to E'(K)$ for every field $K \supset \mathbf{Q}$. These homomorphisms will also be denoted by ψ; they have kernel $\mathbf{Z}/2\mathbf{Z}$, generated by (0,0). Repeating the process, one obtains $\psi' : E' \to E'' \cong E$. The compositions $\psi\psi'$ and $\psi'\psi$ define multiplication by 2 on E' and E, respectively.

A formula for the rank of $E(\mathbf{Q})$ can be obtained using the exact sequence

$$0 \to \frac{\langle(0,0)\rangle}{\langle(0,0)\rangle \cap \psi E(\mathbf{Q})} \to E'(\mathbf{Q})/\psi E(\mathbf{Q}) \xrightarrow{\psi'} E(\mathbf{Q})/2E(\mathbf{Q}) \\ \to E(\mathbf{Q})/\psi' E'(\mathbf{Q}) \to 0.$$

One has $(0,0) \in \psi E(\mathbf{Q})$ precisely when $\dim_{\mathbf{F}_2} E(\mathbf{Q})[2] = 2$, hence

$$\dim_{\mathbf{F}_2} \langle(0,0)\rangle / \langle(0,0)\rangle \cap \psi E(\mathbf{Q}) = 2 - \dim_{\mathbf{F}_2} E(\mathbf{Q})[2].$$

Since $\dim_{\mathbf{F}_2} E(\mathbf{Q})/2E(\mathbf{Q}) = \operatorname{rank} E(\mathbf{Q}) + \dim_{\mathbf{F}_2} E(\mathbf{Q})[2]$, it follows that

$$\operatorname{rank} E(\mathbf{Q}) = \dim_{\mathbf{F}_2} E(\mathbf{Q})/\psi' E'(\mathbf{Q}) + \dim_{\mathbf{F}_2} E'(\mathbf{Q})/\psi E(\mathbf{Q}) - 2.$$

What remains is to study a group like $E(\mathbf{Q})/\psi' E'(\mathbf{Q})$. As explained in the texts quoted above, this injects into $\mathbf{Q}^*/\mathbf{Q}^{*2}$; the injection is induced from $E(\mathbf{Q}) \to \mathbf{Q}^*/\mathbf{Q}^{*2}$ as follows: $(x,y) \mapsto x\mathbf{Q}^{*2}$ if $x \neq 0$, $(0,0) \mapsto b\mathbf{Q}^{*2}$. One can explain the existence of this map using Galois cohomology. The basic facts about this needed here can be found in [**12**, Appendix B].

Write $G = \operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. The short exact sequence of G-modules

$$0 \to \mathbf{Z}/2\mathbf{Z} \to E'(\overline{\mathbf{Q}}) \xrightarrow{\psi'} E(\overline{\mathbf{Q}}) \to 0$$

gives rise to a long exact sequence of Galois cohomology groups

$$\cdots \to E'(\mathbf{Q}) \xrightarrow{\psi'} E(\mathbf{Q}) \xrightarrow{\delta} H^1(G, \mathbf{Z}/2\mathbf{Z}) \to \cdots .$$

Here the homomorphism δ maps a point $P \in E(\mathbf{Q})$ to the homomorphism $\delta(P) : G \to \mathbf{Z}/2\mathbf{Z}$ defined as follows. Fix $\tilde{P} \in E'(\overline{\mathbf{Q}})$ such that $\psi'\tilde{P} = P$. Then for $\sigma \in G$ one has $\delta(P)(\sigma) = \sigma(\tilde{P}) - \tilde{P} \in \operatorname{Ker}\psi' \cong \mathbf{Z}/2\mathbf{Z}$. It is well known that $H^1(G, \mathbf{Z}/2\mathbf{Z}) \cong \mathbf{Q}^*/\mathbf{Q}^{*2}$, with $x\mathbf{Q}^{*2}$ corresponding to $\sigma \mapsto \sigma(y)/y \in \langle\pm 1\rangle \cong \mathbf{Z}/2\mathbf{Z}$, where $y \in \overline{\mathbf{Q}}$ satisfying $y^2 = x$. Now take $P = (x,y) \in E(\mathbf{Q})$, and fix $(\alpha,\beta) \in E'(\overline{\mathbf{Q}})$ with $\psi'(\alpha,\beta) = P$. If we assume for a moment that P is not of the form $(x,0)$ for an $x \neq 0$, this means that $\beta = y \cdot 8\alpha^2/(a^2 - 4b - \alpha^2)$ and $\alpha^2 - (2a+4x)\alpha + a^2 - 4b = 0$. Hence, for $\sigma \in G$ one has $\delta(P)(\sigma) = 0$

precisely when $\sigma(\alpha) = \alpha$, which is the case if and only if the square roots of the discriminant of the quadratic equation which α satisfies, are fixed by σ. Hence

$$\delta(P)(\sigma) = 0 \Longleftrightarrow \sigma(\sqrt{x^2 + ax + b}) = \sqrt{x^2 + ax + b}.$$

It follows that $\delta(0,0)(\sigma) = 0$ precisely when $\sigma(\sqrt{b}) = \sqrt{b}$ and, because $x(x^2 + ax + b) = y^2$ is always a square, $\delta(x,y)(\sigma) = 0$ if and only if $\sigma(\sqrt{x}) = \sqrt{x}$ (for $x \neq 0$, $y \neq 0$). In the remaining case $P = (x, 0)$ with $x \neq 0$ one has $\alpha = a + 2x$ and $\beta^2 = x \cdot 4\alpha^2$. Hence again $\delta(x,0)(\sigma) = 0$ precisely when $\sigma(\sqrt{x}) = \sqrt{x}$. Thus, the map to $\mathbf{Q}^*/\mathbf{Q}^{*2}$ given in terms of Galois cohomology here coincides with the map described by Tate and others.

Since any $(x,y) \in E(\mathbf{Q})$ different from (0,0) can be written as

$$(x,y) = \left(d\frac{m^2}{e^2}, d\frac{nm}{e^3}\right)$$

in which $d, n, m, e \in \mathbf{Z}$, $d \mid b$, $m \neq 0 \neq e$, $\gcd(n,e) = \gcd(n,m) = \gcd(m,e) = 1$ and $n^2 = dm^4 + am^2e^2 + (b/d)e^4$, one concludes that the image in $\mathbf{Q}^*/\mathbf{Q}^{*2}$ is in the subgroup generated by all divisors of b.

Let v be a place of $\mathbf{Q}$ (finite or infinite). The above discussion about the map to $\mathbf{Q}^*/\mathbf{Q}^{*2}$ remains valid if one replaces $\mathbf{Q}$ by $\mathbf{Q}_v$ everywhere. In particular, for v corresponding to a finite prime l the image of $E(\mathbf{Q}_l)/\psi' E'(\mathbf{Q}_l)$ in $\mathbf{Q}_l^*/\mathbf{Q}_l^{*2}$ is among the classes $d\mathbf{Q}_l^{*2}$ for which $d \in \mathbf{Z}_l$ and $d \mid b$. The inclusion $\mathbf{Q} \subset \mathbf{Q}_v$ leads to a commutative diagram

$$\begin{array}{ccc} E(\mathbf{Q})/\psi' E'(\mathbf{Q}) & \xhookrightarrow{\delta} & \mathbf{Q}^*/\mathbf{Q}^{*2} \\ \downarrow & & \downarrow \\ E(\mathbf{Q}_v)/\psi' E'(\mathbf{Q}_v) & \xhookrightarrow{\delta_v} & \mathbf{Q}_v^*/\mathbf{Q}_v^{*2}. \end{array}$$

The ψ'-Selmer group is defined as

$$S[\psi'] := \bigcap_{\text{all } v} \beta_v^{-1} \text{ (image of } \delta_v).$$

Clearly $S[\psi']$ is generated by classes $d\mathbf{Q}^{*2}$ with $d \mid b$, so in particular it is a finite group. By definition $E(\mathbf{Q})/\psi' E'(\mathbf{Q})$ injects into it; the

cokernel of this injection is called the ψ'-Shafarevich group. We denote it by $ь[\psi']$. Hence

$$0 \to E(\mathbf{Q})/\psi' E'(\mathbf{Q}) \to S[\psi'] \to ь[\psi'] \to 0$$

is exact.

In terms of these groups, the results we have obtained about the curves E_p can be stated as follows.

Theorem 2.1. *Using the notations introduced above, one has for the curves* E_p:

i) *If* $p \equiv \pm 3 \bmod 8$, *then* $S[\psi] \cong S[\psi'] \cong \mathbf{Z}/2\mathbf{Z}$ *and* $ь[\psi] \cong ь[\psi'] \cong (0)$,

ii) *If* $p \equiv 7 \bmod 8$ *and also if* $p \equiv 1 \bmod 8$ *and* $((1+\sqrt{-1})/p) = -1$, *then* $S[\psi] \cong (\mathbf{Z}/2\mathbf{Z})^2$, $S[\psi'] \cong \mathbf{Z}/2\mathbf{Z}$ *and* $ь[\psi'] \cong (0)$,

iii) *In the remaining case where* $p \equiv 1 \bmod 8$ *and* $((1+\sqrt{-1})/p) = 1$, *the Selmer groups are* $S[\psi] \cong (\mathbf{Z}/2\mathbf{Z})^3$ *and* $S[\psi'] \cong (\mathbf{Z}/2\mathbf{Z})^2$.

Moreover, if $p \equiv 9 \bmod 16$, *then* $ь[\psi] \cong (\mathbf{Z}/2\mathbf{Z})^2$.

Clearly Theorems 1.3, 1.5 and 1.6 follow easily from the above one using the formula:

$$\operatorname{rank} E_p(\mathbf{Q}) = \dim_{\mathbf{F}_2} S[\psi] + \dim_{\mathbf{F}_2} S[\psi'] - \dim_{\mathbf{F}_2} ь[\psi] - \dim_{\mathbf{F}_2} ь[\psi'] - 2.$$

3. Selmer group computations. In this section the statements about the Selmer groups $S[\psi]$ and $S[\psi']$ of Theorem 2.1 are proven. By definition,

$$\begin{aligned} S[\psi'] = \{ & d\mathbf{Q}^{*2}; d \in \mathbf{Z}, d \mid 2p^2 \text{ and } n^2 = dm^4 - 2pm^2e^2 + (2p^2/d)e^4 \\ & \text{has solutions } n, m \neq 0, e \neq 0 \text{ in } \mathbf{R} \\ & \text{and (pairwise coprime) in } Z_l \text{ for every } l\} \cup \{2\mathbf{Q}^{*2}\} \end{aligned}$$

and

$$\begin{aligned} S[\psi] = \{ & d\mathbf{Q}^{*2}; d \in \mathbf{Z}, d \mid 4p^2 \text{ and } n^2 = dm^4 + 4pm^2e^2 - (4p^2/d)e^4 \\ & \text{has solutions } n, m \neq 0, e \neq 0 \text{ in } \mathbf{R} \\ & \text{and (pairwise coprime) in } Z_l \text{ for every } l\} \cup \{-\mathbf{Q}^{*2}\}. \end{aligned}$$

Considering solvability in real numbers, it follows that

$$\{\mathbf{Q}^{*2}, 2\mathbf{Q}^{*2}\} \subset S[\psi'] \subset \{\mathbf{Q}^{*2}, 2\mathbf{Q}^{*2}, p\mathbf{Q}^{*2}, 2p\mathbf{Q}^{*2}\}$$

and

$$\{\pm\mathbf{Q}^{*2}\} \subset S[\psi] \subset \{\pm\mathbf{Q}^{*2}, \pm 2\mathbf{Q}^{*2}, \pm p\mathbf{Q}^{*2}, \pm 2p\mathbf{Q}^{*2}\}.$$

Moreover, the equations under investigation define double covers of the projective line ramified at the zeros of certain binary forms of degree 4. It is trivially checked that these zeros are simple in every characteristic $l \neq 2, p$. Hence, the equations define curves of genus 1 over $\mathbf{F}_l$. Such curves have an $\mathbf{F}_l$-rational point (compare, e.g., [**12**, p. 320, 10.6]). Using Hensel's lemma, such a point can be lifted to a point over $\mathbf{Q}_l$, and it yields a solution to the equation of the desired kind. It follows that one only needs to consider the equations 2-adically and p-adically.

First, we will study $S[\psi']$. Since this group already contains $2\mathbf{Q}^{*2}$ it suffices to check whether or not $p\mathbf{Q}^{*2}$ belongs to $S[\psi']$. The corresponding equation is

$$n^2 = pm^4 - 2pm^2e^2 + 2pe^4.$$

Considering this modulo 2 and then modulo 8 it follows that a necessary condition for solvability over $\mathbf{Z}_2$ in coprime n, m, e is that $p \equiv 1 \bmod 8$. Assuming $p \equiv 1 \bmod 8$, of course $m = e = 1$ yields a solution over $\mathbf{Z}_2$ as desired. With the same condition on p, a solution sought over $\mathbf{Z}_p$ necessarily has $e \in \mathbf{Z}_p^*$. Hence after dividing through by e^4, one has to consider

$$n^2 = pm^4 - 2pm^2 + 2p.$$

Clearly one needs that $X^4 - 2X^2 + 2 = (X^2 - 1)^2 + 1$ has a zero in $\mathbf{F}_p$, which means $((1+\sqrt{-1}/p) = 1$. Lifting such a zero to $\mathbf{Z}_p$ one concludes that this condition is also sufficient. This proves that $\dim_{\mathbf{F}_2} S[\psi'] = 2$ precisely when $p \equiv 1 \bmod 8$ and $((1 + \sqrt{-1})/p) = 1$.

In case $\dim_{\mathbf{F}_2} S[\psi'] = 1$ the group $S[\psi']$ is generated by the image of the point $(0, 0) \in E_p(\mathbf{Q})$, which implies $ь[\psi' = (0)$.

Next, consider $S[\psi]$. Now one has to deal with equations

$$n^2 = dm^4 + 4pm^2e^2 - fe^4,$$

where $df = 4p^2$. Analogous to the case above it can be checked that for $p \equiv \pm 3 \bmod 8$ one finds $S[\psi] = \{\pm\mathbf{Q}^{*2}\}$ and $ь[\psi] = (0)$.

We now assume $p \equiv \pm 1 \bmod 8$ and we study $p\mathbf{Q}^{*2}$. Depending on the choice $d = p$ or $d = 4p$, the corresponding equation is either

$$n^2 = pm^4 + 4pm^2e^2 - 4pe^4$$

or

$$n^2 = 4pm^4 + 4pm^2e^2 - pe^4.$$

In both cases one obtains a 2-adic solution by taking $m = e = 1$. Considering the first of these equations $n^2 = pm^4 + 4pm^2e^2 - 4pe^4$ over $\mathbf{Z}_p$, we conclude that it is solvable in coprime integers precisely when $n^2 = p(m^4 + 4m^2 - 4)$ has solutions in $\mathbf{Z}_p$. Such solutions exist for $p \equiv -1 \bmod 8$, as one of the zeros of $X^2 + 4X - 4$ is a square in $\mathbf{Z}_p$ in this case. In case $p \equiv 1 \bmod 8$, either both zeros $2(-1 \pm \sqrt{2})$ are squares, or none of them is. Since $(1+\sqrt{2})(1+\sqrt{-1}) = (1+\zeta_8)^2$ for an eighth root of unity ζ_8 which is in $\mathbf{Z}_p$ for $p \equiv 1 \bmod 8$, this means solutions exist precisely when $((1+\sqrt{-1})/p) = 1$. So $p\mathbf{Q}^{*2} \in S[\psi]$ if and only if either $p \equiv -1 \bmod 8$ or $p \equiv 1 \bmod 8$ and $((1+\sqrt{-1})/p) = 1$.

Similar and in fact easier arguments show that for $p \equiv -1 \bmod 8$, none of $2\mathbf{Q}^{*2}$, $2p\mathbf{Q}^{*2}$ belongs to $S[\psi]$. Hence $S[\psi] = \{\pm\mathbf{Q}^{*2}, \pm p\mathbf{Q}^{*2}\}$ in this case.

In the remaining case $p \equiv 1 \bmod 8$ considering $2p\mathbf{Q}^{*2}$ reduces to the equation $n^2 = 2p(m^4+2m^2-1)$. A 2-adic solution is provided by $m = 1$, and a p-adic one exists precisely when $((1+\sqrt{-1})/p) = 1$ by the same argument as above. The element $2\mathbf{Q}^{*2}$ is treated similarly: $m = e = 1$ yields both a 2-adic and a p-adic solution of $n^2 = 2m^4+4pm^2e^2-2p^2e^4$. Hence, for $p \equiv 1 \bmod 8$ one concludes that $S[\psi] = \{\pm\mathbf{Q}^{*2}, \pm 2\mathbf{Q}^{*2}\}$ in case $((1+\sqrt{-1})/p) = -1$, and $S[\psi] = \{\pm\mathbf{Q}^{*2}, \pm 2\mathbf{Q}^{*2}, \pm p\mathbf{Q}^{*2}, \pm 2p\mathbf{Q}^{*2}\}$ otherwise.

This concludes the proof of all assertions of Theorem 2.1 about the Selmer groups $S[\psi]$ and $S[\psi']$.

4. Nontrivial Shafarevich groups. Denote by E'_p the elliptic curve which over $\mathbf{Q}$ is 2-isogenous to E_p. So E'_p can be given by the equation $y^2 = x(x^2 + 4px - 4p^2)$, and we have that $\psi : E_p \to E'_p$ is of degree 2. In this section it is assumed throughout that $p \equiv 1 \bmod 8$ and $((1+\sqrt{-1})/p) = 1$. As is explained above, under these conditions one obtains a short exact sequence

$$0 \to E'_p(\mathbf{Q})/\psi E_p(\mathbf{Q}) \to \{\pm\mathbf{Q}^{*2}, \pm 2\mathbf{Q}^{*2}, \pm p\mathbf{Q}^{*2}, \pm 2p\mathbf{Q}^{*2}\} \to Ш[\psi] \to 0.$$

Since the point $(0,0) \in E'_p(\mathbf{Q})$ provides a nontrivial element of the group on the left, clearly $\dim_{\mathbf{F}_2} Ш[\psi] \leq 2$. The aim of this section is to prove that under the additional assumption $p \equiv 9 \bmod 16$ this upper bound is attained, i.e., $Ш[\psi] \cong (\mathbf{Z}/2\mathbf{Z})^2$. This is equivalent to the statement that the equations $n^2 = dm^4 + 4pm^2e^2 - (4p^2/d)e^4$, for $d = 2, 2p^2, p, 2p, 4p$ have no solutions in pairwise coprime integers $n, m \neq 0$, $e \neq 0$ (although they have such solutions everywhere locally).

The following proposition will turn out to be very useful.

Proposition 4.1. *Let $p \equiv 1 \bmod 8$ be a prime number satisfying $((1+\sqrt{-1})/p) = 1$. Denote by $\pi, \bar{\pi}$ conjugate elements in $\mathbf{Z}[\sqrt{2}]$ such that $\pi\bar{\pi} = \pm p$. Then the following statements are equivalent*:

i) $p \equiv 9 \bmod 16$,

ii) *π is not a square modulo $\bar{\pi}$*,

iii) *$\sqrt{2}$ is not a square in $\mathbf{F}_p$*.

Proof. Details of the proof can be easily extracted from Stevenhagen's recent paper [**14**, Section 2]. The equivalence of the first and third statement is in fact trivial using $\pm\sqrt{2} = \zeta_8 + \zeta_8^7 = \zeta_8(1 - \zeta_8^2)$ for a primitive eighth root of unity ζ_8. To see the equivalence with the second statement, note that, as we saw in the previous section, the conditions imply that $1+\sqrt{2}$ is a square in $\mathbf{F}_p$. Using class field theory, one now easily translates the condition '$\sqrt{2}$ is a square in $\mathbf{F}_p$' into the statement that a cyclic extension of $\mathbf{Q}(\sqrt{2p})$ of degree 8 exists which is unramified at all finite primes. From this, one deduces the equivalence of the second and the third statement. □

Although we will not need this, it may be interesting to remark that the same paper [**14**] shows that the primes p satisfying the conditions and the equivalent statements in the proposition above are precisely the ones that can be represented by the form $x^2 + 32y^2$ but not by $x^2 + 64y^2$.

We will now consider the five relevant equations separately. First, suppose pairwise coprime $n, m \neq 0$, $e \neq 0$ exist in $\mathbf{Z}$ satisfying $n^2 = 2m^4 + 4pm^2e^2 - 2p^2e^4$. Then n is even, $n = 2N$, say, and

factoring over $\mathbf{Z}[\sqrt{2}]$ yields

$$2N^2 = (m^2 + (1+\sqrt{2})pe^2)(m^2 + (1-\sqrt{2})pe^2).$$

The two factors on the right have greatest common divisor $(\sqrt{2})$; hence, one concludes

$$m^2 + (1+\sqrt{2})pe^2 = \varepsilon\sqrt{2}n_1^2$$

for some $\varepsilon \in \mathbf{Z}[\sqrt{2}]^*$ and $n_1 \in \mathbf{Z}[\sqrt{2}]$. Reducing this modulo a prime $\pi \mid p$, it follows that $\sqrt{2}$ has to be a square modulo p. Hence, by Proposition 4.1 above, a solution can only exist when $p \equiv 1 \bmod 16$. The equation $n^2 = 2p^2m^4 + 4pm^2e^2 - 2e^4$ is dealt with completely analogously.

Next we study

$$n^2 = 2pm^4 + 4pm^2e^2 - 2pe^4.$$

Now n has to be of the form $2pN$ and we arrive at

$$2pN^2 = (m^2 + (1+\sqrt{2})e^2)(m^2 + (1-\sqrt{2})e^2).$$

As before, the assumptions imply that the two factors on the righthand side have gcd $(\sqrt{2})$, and hence one obtains a system

$$\begin{aligned} m^2 + (1+\sqrt{2})e^2 &= \sqrt{2}\pi n_1^2 \\ m^2 + (1-\sqrt{2})e^2 &= -\sqrt{2}\bar{\pi}\bar{n}_1^2, \end{aligned}$$

in which $\pi\bar{\pi} = -p$ and $n_1 \in \mathbf{Z}[\sqrt{2}]$. Taking the difference of these expressions and reducing modulo π reveals that $\bar{\pi}$ must be a square modulo π, so again no solutions can exist for $p \equiv 9 \bmod 16$.

Finally, consider $n^2 = pm^4 + 4pm^2e^2 - 4pe^4$. Reasoning as in the cases above leads to the system

$$\begin{aligned} m^2 + 2(1+\sqrt{2})e^2 &= \pi n_1^2 \\ m^2 + 2(1-\sqrt{2})e^2 &= \bar{\pi}\bar{n}_1^2, \end{aligned}$$

in which $\pi\bar{\pi} = p$ and $n_1^2\bar{n}_1^2 = N^2 = n^2/p^2$. It follows that $\pi, \bar{\pi} > 0$. Considering the system over $\mathbf{Z}_2[\sqrt{2}]$, one checks that if a solution as desired exists, then π and $\bar{\pi}$ have to be squares. But in that case the

prime over 2 in the field $\mathbf{Q}(\sqrt{2})$ splits completely in the totally real field $\mathbf{Q}(\sqrt{2}, \sqrt{\pi}, \sqrt{\bar{\pi}})$. Using the arguments from [**14**, pp. 3–6], we conclude that the strict class number of $\mathbf{Q}(\sqrt{2p})$ is divisible by 8, and hence $\sqrt{2}$ is a square in $\mathbf{F}_p$. By Proposition 4.1 this shows that a solution can exist only if $p \equiv 1 \bmod 16$. Exactly the same argument works for $n^2 = 4pm^4 + 4pm^2e^2 - pe^4$.

This proves our claim about $ь[\psi]$ and hence finishes the proof of Theorem 2.1.

5. Constructing generators, computational preliminaries. In this section we set up the machinery needed for the explicit calculation of the rank of the Mordell-Weil group $E_p(\mathbf{Q})$ and the construction of a set of generators for this group. These calculations have been carried out for prime numbers $p \equiv \pm 1 \bmod 8$ in the range $p < 300$. In fact, for primes $p \equiv -1 \bmod 8$ in this range, we also checked that $L'(E_p, 1) \neq 0$, which shows that rank $= 1$ (see the lines following Conjecture 1.4). The numerical data obtained have been collected into two tables, one for the case $p \equiv -1 \bmod 8$, the other for $p \equiv +1 \bmod 8$, and evidently fully support Conjecture 1.4. Often the excellent Apecs[1] program by Ian Connell has been very helpful.

In order to show that $\operatorname{rank} E_p(\mathbf{Q}) \geq 1$, it is clearly sufficient to find a point of infinite order. In principle–provided such a point exists of course–this should be possible by a straightforward computer search. However, the naive height of a generator may be very large indeed as is convincingly demonstrated by Bremner [**3**], Bremner and Buell [**4**] and Bremner and Cassels [**5**]. Thus, a simple-minded search by brute force does not always suffice. In the following lines the problem of 'uprooting' (independent) points of infinite order will be reduced to the construction of integral solutions to one or more systems of quadratic equations, conveniently chosen for the purpose of being subjected to a computer search.

Starting from the model

$$Y^2 = X(X^2 - 2pX + 2p^2), \tag{1}$$

where $p \equiv \pm 1 \bmod 8$ is prime, let (X, Y) on (1) be a generator of infinite order for $E_p(\mathbf{Q})$, assuming that such a point exists. Then $(X, Y) \neq (0, 0)$ is of the shape

$$X = R/S^2, \qquad Y = T/S^3$$

for integers R, S, and T with $\gcd(R,S) = \gcd(T,S) = 1$ and $R > 0$. Substitution into (1) yields

$$T^2 = R(R^2 - 2pRS^2 + 2p^2S^4). \tag{2}$$

From Proposition 1.1, we know that $(0,0)$ is the only nontrivial point of finite order, and it is easily seen that

$$(X', Y') := (X,Y) + (0,0) = \left(\frac{2p^2}{X}, -\frac{2p^2Y}{X^2}\right)$$

so that

$$X' = \frac{2p^2S^2}{R}, \quad \text{and} \quad Y' = -\frac{2p^2ST}{R^2}.$$

From (2) it follows that integers r and $d \in \{1, 2, p, 2p\}$ exist such that $R = dr^2$, and consequently

$$X = \frac{dr^2}{S^2}, \quad \text{and} \quad X' = \frac{2p^2S^2}{dr^2},$$

from which it is clear that of the four possible d-values only $d = 1$ and $d = p$ need separate consideration. Indeed, if $d = 2$, then $X' = (pS)^2/r^2$ and exchanging X' and X essentially gives the case $d = 1$. Likewise, $d = p$ and $d = 2p$ may be combined. Summarizing,

$$t^2 = dr^4 - 2pr^2S^2 + \frac{2p^2}{d}S^4, \tag{3}$$

where

$$R = dr^2, T = drt, d \in \{1, p\} \quad \text{and} \quad \gcd(r,S) = \gcd(t,S) = 1.$$

Observe that the signs of r, S, and t are immaterial. Further, it should be noted that both r and t are odd.

From (3), it is clear that $d \mid t$ because $d \mid p$. Writing $\tilde{p} := p/d$ and $\tilde{t} := t/d$, it follows that

$$\begin{aligned} d\tilde{t}^2 &= r^4 - 2\tilde{p}r^2S^2 + 2\tilde{p}^2S^4 = (r^2 - \tilde{p}S^2)^2 + \tilde{p}^2S^4 \\ &= (r^2 - (1-i)\tilde{p}S^2)(r^2 - (1+i)\tilde{p}S^2). \end{aligned} \tag{4}$$

If $p \equiv -1 \bmod 8$, then p remains prime in $\mathbf{Z}[i]$ and this forces $d \neq p$. Hence, we may always write $d = a^2 + b^2$ for suitable integers a and b. Because of the coprimality of r and S, and also of S and $\tilde{t}$, the above mentioned factorization in $\mathbf{Z}[i]$ implies

$$r^2 - (1-i)\tilde{p}S^2 = \varepsilon\pi^h(u+iv)^2,$$

where ε is a unit of $\mathbf{Z}[i]$, π is a prime divisor of p, $h \in \{0,1\}$, and u and v are coprime rational integers. It should be observed that minus signs can be absorbed into the square.

Equating coefficients of 1 and i in this equation yields after some rewriting,

$$\begin{aligned} r^2 &= (a'+b')(u^2-v^2) + 2uv(a'-b') \\ \tilde{p}S^2 &= b'(u^2-v^2) + 2a'uv, \end{aligned} \tag{5}$$

where

$$\begin{aligned} &(a',b') \in \{(1,0),(0,1),(p,0),(0,p)\} && \text{if } d = 1 \\ &(a',b') \in \{(a,b),(a,-b),(b,a),(b,-a)\} && \text{if } d = p = a^2+b^2 \\ & && \text{and } a > b > 0 \text{ minimal.} \end{aligned}$$

Also, in the same notation, $\tilde{t} = \sqrt{(a'^2+b'^2)/d}$.

From the preceding sections it is evident that the cases $p \equiv -1 \bmod 8$ and $p \equiv 1 \bmod 8$ differ substantially. It is not untimely to bring this difference into the picture.

6. Generators for small primes $p \equiv -1 \bmod 8$. The relations (6) of the following lemma are in most cases sufficient to obtain a point of infinite order by direct search.

Lemma 6.1. *Let (X,Y) as before. If $p \equiv -1 \bmod 8$ and $p = a^2 - 2b^2$ for integers a and b, then integers U, V, A, and B exist with $\gcd(U,V) = 1$, $\gcd(A,B) = 1$, and*

$$\begin{aligned} 2U^2 + V^2 &= a(A^2+2B^2) + 4bAB \\ V^2 &= b(A^2+2B^2) + 2aAB. \end{aligned} \tag{6}$$

If $(X,Y) = (R/S^2, T/S^3)$, *then*

$$R = p^2(A^2-2B^2)^2, \qquad S = 2UV, \quad \textit{and} \quad T = p^2(A^2-2B^2)(4U^4+V^4).$$

It suffices to consider the two cases $(a, \pm b)$ *where* $a > 0$ *and minimal, subject to* $p = a^2 - 2b^2$.

Proof. Recall that, by (4), $p \equiv -1 \bmod 8$ implies that $d = 1$. Of the four possible systems (5), two are impossible modulo 4, namely those for which $a' = 0$. In case $(a', b') = (1, 0)$, we'll show that the corresponding rational point (X, Y) cannot be a generator, as it is double another rational point. To be more precise, system (5) in this case is

$$\begin{aligned} r^2 &= u^2 - v^2 + 2uv \\ pS^2 &= 2uv, \end{aligned} \tag{7}$$

with $R = r^2$ and $t = u^2 + v^2$. From (7) it is obvious that S is even, and hence r must be odd. As t is odd, u and v have opposite parity, and clearly v is even. Also, p divides v, because otherwise $p \mid u$ and hence $r^2 + v^2 \equiv 0 \bmod p$. But then $p \mid v$ because $p \equiv -1 \bmod 8$, which contradicts the assumption. Factorization of the second equation of (7) yields

$$u = U^2, \qquad v = 2pV^2, \quad \text{and} \quad S = 2UV$$

for coprime integers U and V. The first equation of (7) reads, in terms of U and V,

$$\begin{aligned} r^2 &= (u+v)^2 - 2v^2 = (U^2 + 2pV^2)^2 - 8p^2V^4 \\ &= (U^2 + 2pV^2 + 2pV^2\sqrt{2})(U^2 + 2pV^2 - 2pV^2\sqrt{2}). \end{aligned}$$

Consequently,

$$U^2 + 2pV^2 + 2pV^2\sqrt{2} = \eta(A + B\sqrt{2})^2,$$

where $\eta \in \{1, 1+\sqrt{2}\}$ and A and B are relatively prime. As Norm $\eta = 1$, only $\eta = 1$ is feasible. Clearly, $B \neq 0$, otherwise S vanishes, which is impossible. Now define

$$X_0 = p\frac{A}{B}, \qquad Y_0 = p^2\frac{UV}{B^2}.$$

Then (X_0, Y_0) is a rational point on (1) and

$$X = \frac{r^2}{S^2} = \frac{(A^2 - 2B^2)^2}{4U^2V^2} = \frac{(X_0^2 - 2p^2)^2}{4Y_0^2}.$$

Hence $(X, Y) = 2(X_0, Y_0)$, and (X, Y) cannot be a generator. This only leaves $(a', b') = (p, 0)$. We proceed as before. Here (5) yields

$$\begin{aligned} r^2 &= p(u^2 - v^2 + 2uv) \\ S^2 &= 2uv. \end{aligned} \tag{8}$$

Clearly, $p \mid r$. Set $\tilde{r} := r/p$. Observe that S is even, that r and t are odd, and that u and v are coprime of opposite parity. Then

$$u^2 - v^2 + 2uv = p\tilde{r}^2 \equiv -1 \bmod 8,$$

and this implies that u is even and v is odd. By factorization of the second equation of (8), we may write

$$u = 2U^2, \qquad v = V^2, \quad \text{with} \quad \gcd(U, V) = 1,$$

so that $S = 2UV$. As $p \equiv -1 \bmod 8$, p can be written as $a^2 - 2b^2$. Choose $a > 0$, $b > 0$ and minimal. Rewriting the first equation of (8), we see that

$$(2U^2 + V^2 + V^2\sqrt{2})(2U^2 + V^2 - V^2\sqrt{2}) = (a + b\sqrt{2})(a - b\sqrt{2})\tilde{r}^2,$$

and as the factors of the left-hand side are relatively prime in $\mathbf{Z}[\sqrt{2}]$, there exist coprime integers A and B such that

$$2U^2 + V^2 + V^2\sqrt{2} = \eta(\pm a \pm b\sqrt{2})(A + B\sqrt{2})^2,$$

where $\eta \in \{1, 1 + \sqrt{2}\}$. Taking norms, it follows that $\eta = 1 + \sqrt{2}$ is impossible. A little reflection on signs shows that

$$2U^2 + V^2 + V^2\sqrt{2} = (a' + b'\sqrt{2})(A + B\sqrt{2})^2, \tag{9}$$

with $(a', b') \in \{(a, b), (a, -b)\}$. Equating coefficients of 1 and $\sqrt{2}$ in (9) gives the desired relations. This completes the proof of the lemma. □

It is clear from their form that relations (6) are quite suitable for recovering all candidate generators below a given bound on the naive height. The computations have been carried out on a desktop computer for all $p \equiv -1 \bmod 8$ in the range $p < 300$. In some cases our analysis needs to go a little further, and occasionally we failed to find a point at all, even after a detailed analysis and much effort. However, we are most grateful to Andrew Bremner who succeeded where we failed. By considering Heegner points on $X_0(128)$ (see the lines following Conjecture 1.4), we calculate the canonical height of a rational point, which gives an indication as to what may be expected. In fact, we applied the Apecs package to calculate $L'(E_p, 1)$. By the Gross-Zagier theorem [**7**, Theorem 7.3], there exists a point $P \in E_p(\mathbf{Q})$ such that

$$\begin{aligned} L'(E_p,1)/2 &= \hat{h}(P)\int_{E_p(\mathbf{R})}\frac{dx}{2y} = \hat{h}(P)\int_0^\infty \frac{d\xi}{\sqrt{\xi^3-2p\xi^2+2p^2\xi}} \\ &= \hat{h}(P)\frac{1}{\sqrt{p}}\int_0^\infty \frac{d\xi}{\sqrt{\xi^3-2\xi^2+2\xi}} \\ &= \frac{\hat{h}(P)}{\sqrt{p}} \times 4.0364616539 \end{aligned} \tag{10}$$

and this clearly determines $\hat{h}(P)$. It should be noted here that the constant α appearing in the Gross-Zagier formula can be taken as the product over the primes l of the number of $\mathbf{F}_l$-rational components of multiplicity one in the special fiber at l of the Néron model, divided by the square of the order of the group of rational torsion points. For the curves E_p, one finds $\alpha = 2$ if $p \equiv 1 \bmod 4$ and $\alpha = 1$ if $p \equiv 3 \bmod 4$. It should also be remarked here that, contrary to Gross and Zagier, we take throughout this paper as canonical height the one associated to the divisor one times the origin on the elliptic curves. It is the computation of this height which is implemented in Apecs. The height used by Gross and Zagier is twice this one, and that accounts for the division by 2 in the formula (10) above.

Closely following [**3**], we tried a similar descent argument for the seemingly nontrivial cases $p = 47, 167, 223$. We only succeeded for $p = 47$ and Andrew Bremner completed the remaining cases. In the following lines we shall only give an outline, as the details are rather messy.

From (6) it is possible by standard factorization techniques to deduce the following systems

$$\begin{aligned} pC^2 + D^2 &= \pm q_1(x,y) \\ CD &= q_2(x,y), \end{aligned} \tag{11}$$

for integral C, D, x, y and quadratic forms q_1, q_2 with integral coefficients. So

$$(D + C\sqrt{p})^2 = \pm q_1(x,y) + 2q_2(x,y)\sqrt{p}$$

or

$$z^2 = \alpha x^2 + \beta xy + \gamma y^2, \tag{12}$$

with $\alpha, \beta, \gamma \in \mathbf{Z}[\sqrt{p}]$. The idea is to extend the solution domain from $\mathbf{Z}$ to $\mathbf{Z}[\sqrt{p}]$. Although it may be very hard to locate a solution of (11) in integers C, D, x, y, it should be considerably simpler to spot solutions of (12) with $x, y, z \in \mathbf{Z}[\sqrt{p}]$. If one is lucky enough to spot a solution with $x, y \in \mathbf{Z}$, that's the end of the search. This happened to us for $p = 47$. Otherwise, this $\mathbf{Z}[\sqrt{p}]$-solution may be used to rewrite (12) as

$$\mathcal{X}\,\mathcal{Y} = \delta\mathcal{Z}^{\,2}$$

for fixed $\delta \in \mathbf{Z}[\sqrt{p}]$. Here $\mathcal{X}, \mathcal{Y}$ and $\mathcal{Z}$ are linear forms in x, y, z with coefficients in the ring $\mathbf{Z}[\sqrt{p}]$. Also, as ideals, $\mathcal{X}$ and $\mathcal{Y}$ can have only finitely many common prime ideal divisors. Factorization of this equation in $\mathbf{Z}[\sqrt{p}]$ yields expressions for $\mathcal{X}, \mathcal{Y}$ and $\mathcal{Z}$ which, after substitution, give binary quadratic form expressions for x, y and z with coefficients in $\mathbf{Z}[\sqrt{p}]$. As x and y should be rational integers, equating coefficients finally produces a finite number of systems consisting of two quadratic forms in four variables with integral coefficients. To give an impression, for $p = 167$, with the $+$ sign in (11), and quadratic forms

$$q_1(x,y) = 128x^2 - 184xy - 80y^2, \quad \text{and} \quad q_2(x,y) = 5x^2 - 6xy - 3y^2,$$

the expressions for x, y and z are given by

$$\begin{aligned} \frac{4\lambda x\theta}{(13-\theta)^a\theta^c} &= (196+15\theta)PQ + (25+2\theta)\varepsilon^e P^2 - (230-18\theta)\varepsilon^{1-e}Q^2, \\ \frac{4\lambda y\theta}{(13-\theta)^a\theta^c} &= (142+11\theta)PQ + (13+\theta)\varepsilon^e P^2 + (14-\theta)\varepsilon^{1-e}Q^2, \\ \frac{4\lambda z\theta}{(13-\theta)^a\theta^c} &= (-334-26\theta)PQ + (167+13\theta)\varepsilon^e P^2 - (167-11\theta)\varepsilon^{1-e}Q^2. \end{aligned}$$

Here $\lambda = \pm 1$, $\theta = \sqrt{167}$, $a, c, e \in \{0, 1\}$, and $\varepsilon = 168 + 13\theta$, the fundamental unit of $\mathbf{Q}(\theta)$. These expressions lead to eight different systems of two quadratic forms in P_1, P_2, Q_1, Q_2, where $P = P_1 + P_2\theta$, and $Q = Q_1 + Q_2\theta$, and each of these systems has to be searched for solutions. It is to be expected that the P_i and the Q_i corresponding to a solution are considerably smaller than those of the original U, V, A, and B.

In fact, Andrew Bremner found a solution of the system given by $(a, c, e) = (1, 0, 0)$, namely, $P = -1799 + 55\theta$, $Q = -967 + 89\theta$. This gives $x = 17832$, $y = -20585$ and $C = 18159$, $D = 138835$ in (11). Actually, the A and B of (6) are quadratic forms in x and y, here with values

$$A = -x^2 - 14xy - y^2, \quad B = q_2(x, y) = 5x^2 - 6xy - 3y^2.$$

All this leads to the rather large point (X, Y) on (1) with

$$X = \frac{1223750552270914818975279949270624769697169}{90117809458871347332914539873740924200004},$$

$$Y = \frac{22607477070335947628171594726362668955323571768602072697642905595}{27053031601544792167639118831010043036717430417571870116350008}.$$

Once a point of infinite order has been found, it is not so difficult to decide whether we are dealing with a generator or not. Let P be such a point. First we check that neither P nor $P+$ (the point of order 2) can be written as twice a rational point (which is very unlikely anyway from the result—and the proof—of Lemma 6.1). So, if G is a generator and P is not, then $P = mG$ with m odd and $m \geq 3$. Consequently,

$$\hat{h}(G) = \frac{1}{m^2}\hat{h}(P) \leq \frac{1}{9}\hat{h}(P),$$

where $\hat{h}$ denotes the Néron-Tate height. Working out the relationship between $\hat{h}(G)$ and the naive height $h(G)$ as given in [**13**, Theorem 1.1] in case of our model (1), results in

$$\begin{aligned} \frac{1}{2}h(G) &\leq \hat{h}(G) + \frac{1}{2}\log p + 1.8389 \\ &\leq \frac{1}{9}\hat{h}(P) + \frac{1}{2}\log p + 1.8389. \end{aligned} \tag{13}$$

The value of $\hat{h}(P)$ can be calculated, and a direct search should give us either no point at all or a new candidate of smaller height. The results of these computations can be found in Table 1. All curves in this table have rank 1.

TABLE 1. $p \equiv -1 \bmod 8$. This table lists for each $p < 300$ a generator $P = (X, Y)$ on (1). $X = R/S^2$, $Y = T/S^3$, as in Lemma 6.1. a, b, A, B, U and V are the corresponding values in (6). $\hat{h}(P)$ is the canonical height of P.

p	a	b	A	B	U	V	$\hat{h}(P)$
7	3	1	1	0	1	1	1.0351
23	5	1	7	1	9	11	5.5477
31	7	-3	3	1	4	3	3.6811
47	7	1	601	429	948	2083	15.3624
71	11	5	15	22	57	115	9.6526
79	9	1	1	0	2	1	2.1851
103	11	-3	35	74	203	143	11.5133
127	15	-7	1	1	2	3	2.6877
151	13	-3	5	1	11	7	5.6515
167	13	1	4397281631	2521104765	8387017401	17896486351	47.3231
191	17	-7	69	148	516	85	13.1978
199	19	9	71	-164	553	295	13.4427
223	15	1	95977	25901	203854	291771	25.7153
239	17	5	3	58	198	199	11.6143
263	19	-7	5	4	9	19	6.0066
271	17	-3	11	2	28	19	7.5393

The actual heights in the cases $p = 167$ and $p = 223$ nicely correspond with the values found by means of (10), namely 47.3298 for $p = 167$ and 25.7213 for $p = 223$.

7. Generators for small primes $p \equiv 1 \bmod 8$. For $p \equiv 1 \bmod 8$ things are more complicated. Here we could also give complete information in a lemma, like we did for primes $p \equiv -1 \bmod 8$ in Lemma 6.1, but instead of two distinct cases we would have to consider a grand total of eight. As the derivation is very similar, especially for primes p which do not satisfy the extra conditions of Theorem 1.6, we refrain from giving all the details. In its place we work out the case $p = 337$

completely, so that we can prove the following

Theorem 7.1. *For $p = 337$, the Mordell-Weil group $E_p(\mathbf{Q})$ has rank three and $P_1 = (8425/9, 567845/27)$, $P_2 = (57121, 13571615)$, and $P_3 = (113569/25, 35547097/125)$ on (1) form a set of generators modulo torsion.*

Of course, the first assertion of Theorem 7.1 has been proven as soon as three independent rational points of infinite order have been produced. That turned out to be easy enough. To establish the second part, we need to do quite a bit more. But before we do that, we like to make a couple of remarks on the calculations we deliberately left out.

When checking a system (6) for solutions, one should observe that this system may be written as

$$\begin{aligned} 2(a-b)U^2 &= ((a-b)A + (2b-a)B)^2 + pB^2 \\ bV^2 &= (bA + aB)^2 - pB^2 \end{aligned}$$

so that both $a-b$ and b are quadratic residues modulo p. In our search for solutions of the relevant systems for primes $p \equiv 1 \bmod 8$, it paid off to first calculate Legendre symbols like (a/p), (b/p), $((a-b)/p)$, etc., where a and b satisfy one of the relations $p = a^2 \pm 2b^2$, and check a few relations between them, implied by these systems. For almost all p, we could at once eliminate most of the relevant systems in this way. Of course, these relations should be just another way of expressing the conditions on p laid down in Theorem 1.6, namely: $p \equiv 1 \bmod 16$ and $((1 + \sqrt{-1})/p) = 1$. The primes $p \equiv 1 \bmod 8$ in the range $p < 300$ satisfying these conditions are $p = 113$ and $p = 257$. Of these primes we can only prove that $\operatorname{rank} E_p(\mathbf{Q}) = 1$ or 3 by exhibiting a point of infinite order. Under the usual Taniyama/Weil/Birch/Swinnerton-Dyer assumptions as well as the Riemann hypothesis for the L-function, Apecs shows by using Mestre's technique (see [**10**]) for the computation of an upper bound for the rank, that rank $= 1$ in both cases. The next interesting value for p is 337. As we mentioned above, we'll show that rank $= 3$ for this prime. In Table 2 we list a generator for each p in the range $p < 300$ with two possible exceptions. All the points listed were obtained by direct search and submitted to the generator checking procedure of the previous section.

Proof of Theorem 7.1. Let O denote the zero of $E_{337}(\mathbf{Q})$ and let $P_0 = (0,0)$ be the generator of the torsion subgroup. It is easy to check that P_1, P_2 and P_3 are independent, and that the 16 points $O, P_0, P_1, P_0+P_1, P_2, P_0+P_2, P_3, P_0+P_3, P_1-P_2, P_0+P_1-P_2, P_1+P_3, P_0+P_1+P_3, P_2+P_3, P_0+P_2+P_3, P_1-P_2-P_3, P_0+P_1-P_2-P_3$ represent $E_{337}(\mathbf{Q})/2E_{337}(\mathbf{Q})$. The signs have been chosen in such a way that the maximal value of the canonical heights of these representatives is as small as possible. For any rational point $P = (X, Y)$ belonging to this set, we calculate that

$$\hat{h}(P) \leq 6.3026$$

so that by (13) it follows for the naive height that

$$h(P) \leq 2\hat{h}(P) + \log(337) + 3.6777 \leq 22.1030.$$

By Proposition 7.2 of [**13**], this means that the set of rational points on $E_{337}(\mathbf{Q})$ with naive height bounded from above by 22.1030 generates $E_{337}(\mathbf{Q})$. However, if $X = R/S^2$, then a search would have to include all integers R below $\exp(22.1030)$, which is roughly 4×10^9. It is obvious that such a search is out of the question; we are forced to do some descent work.

TABLE 2. $p \equiv 1 \bmod 8$. This table lists for each $p < 300$ a generator $P = (X, Y)$ on (1), with the possible exceptions $p = 113$ and $p = 257$. $X = R/S^2$, $Y = T/S^3$, $\hat{h}(P)$ is the canonical height of P.

p	R	S	T	$\hat{h}(P)$
17	49	3	1295	2.6873
41	369	2	5043	1.1288
73	5041	7	274415	4.3700
89	27804529	1071	665725746673	9.3923
97	693889	33	497854945	6.7237
113	12769	6	1085365	2.3735
137	11097	7	844605	2.2695
193	289	9	372385	5.0015
233	1144538368561	141993	6301490607105836975	14.7605
241	82369	17	20319887	5.8170
257	145902241	3675	58058888074039	8.3819
281	5.166529	93	8318454913	7.7647

From (5) we see that we have to deal with eight different cases. We distinguish between them by referring to Case (a', b') where a' and b' are replaced by the relevant values as in (5). Let $M^2 := \exp(22.1030)$. From now on, we'll assume that $P = (R/S^2, T/S^3)$ is a rational point on (1), with $R > 0$, not twice another rational point, and $\max(R, S^2) \leq M^2$. In each case we'll try to reduce the upper bounds for the search parameters to reasonable proportions.

Case $(1, 0)$. Exactly as we did in the proof of Lemma 6.1, it can be shown that the corresponding point is twice another rational point. Hence, we can drop this case.

Case $(0, 1)$. Substitution of the proper values for a', b', and p in the system (5) yields

$$\begin{aligned} r^2 &= u^2 - v^2 - 2uv \\ 337S^2 &= u^2 - v^2. \end{aligned} \tag{14}$$

Factorization of the first equation of (14) in $\mathbf{Z}[\sqrt{2}]$, observing that there is no loss of generality in taking $u - v > 0$, we get

$$u - v = U^2 + 2V^2, \qquad v = 2UV, \quad \text{with} \quad \gcd(U, V) = 1,$$

so that $r = |U^2 - 2V^2|$. Because of,

$$337S^2 = (U^2 + 2V^2)(U^2 + 2V^2 + 4UV),$$

there are two possibilities, depending on whether 337 divides $U^2 + 2V^2$ or not. Assume the former. Then coprime integers A and B can be found such that

$$\begin{aligned} 337A^2 &= U^2 + 2V^2 \\ B^2 &= U^2 + 2V^2 + 4UV. \end{aligned} \tag{15}$$

Note that $S = AB$. As $337 = 7^2 + 2 \cdot 12^2$, we may write the first equation of (15) as

$$(U + V\sqrt{-2})(U - V\sqrt{-2}) = (7 + 12\sqrt{-2})(7 - 12\sqrt{-2})A^2,$$

and hence

$$U + V\sqrt{-2} = \pm(7 \pm 12\sqrt{-2})(m + n\sqrt{-2})^2$$

for coprime integers m and n. The $\pm$ signs are independent. Then $A = m^2 + 2n^2$ and

$$\begin{aligned} \pm U &= 7(m^2 - 2n^2) \mp 48mn \\ \pm V &= 14mn \pm 12(m^2 - 2n^2), \end{aligned} \tag{16}$$

where the left-hand side signs correspond and those of the right-hand side also. Now we'll compute upper bounds for $|m|$ and $|n|$. From

$$\begin{aligned} \max((u-v)^2, (u+v)^2) &= |(u-v)^2 - (u+v)^2| + \min((u-v)^2, (u+v)^2) \\ &\le 4|uv| + |u^2 - v^2| = 2|337S^2 - r^2| + 337S^2 \\ &\le 1013M^2, \end{aligned}$$

(note that $R = r^2$) we deduce that

$$(m^2 + 2n^2)^2 = A^2 = \frac{|u - v|}{337} \le \frac{\sqrt{1013}M}{337} < 5954,$$

and consequently,

$$\max(|m|, |n|\sqrt{2}) < 9.$$

When 337 does not divide $U^2 + 2V^2$, we write $337 = 25^2 - 2 \cdot 12^2$ and we proceed as before. We get similar equations with upper bounds for the relevant parameters m and n that are only slightly larger.

Case $(337, 0)$. We considered this case in the proof of Lemma 6.1. The fact that $p \equiv 1 \bmod 8$ changes things, but only slightly. We find–compare with (6)–that

$$u = U^2, \qquad v = 2V^2, \qquad S = 2UV, \qquad r = \pm(A^2 - 2B^2),$$

so that the roles of u and v are interchanged. As

$$\begin{aligned} \max(u^2, v^2) &= |u^2 - v^2| + \min(u^2, v^2) \\ &\le |337\tilde{r}^2 - S^2| + \frac{S^2}{2} \\ &\le \frac{3S^2}{2} + \frac{R}{337} \le 1.503M^2 \end{aligned}$$

and

$$337(A^2+2B^2) = 25U^2 + 2(25\pm 24)V^2 \le 74\max(u,v),$$

we deduce that

$$\max(|A|, |B|\sqrt{2}) < 131.$$

Case $(0, 337)$. The case is similar to the previous one. From

$$u-v = U^2, \qquad u+v = V^2, \qquad S = UV \quad \text{with} \quad \gcd(U,V) = 1,$$

via

$$U^2 + V^2 + V^2\sqrt{2} = \sqrt{2}(25 \pm 12\sqrt{2})(A + B\sqrt{2})^2,$$

where A and B are relatively prime, we deduce by equating coefficients that

$$337(A^2+2B^2) = (25\pm 12)A^2 \mp B^2 \le \max(|u|, |v|)$$

and

$$\max(u^2, v^2) = |u^2 - v^2| + \min(u^2, v^2) \le S^2 + \frac{1}{2}|p\tilde{r}^2 - S^2|,$$

from which essentially the same upper bound is obtained as in the previous case. As the four remaining cases are very much alike, we shall only give the details of one of them. We have selected

Case $(16, 9)$. After rewriting (5) for $(a', b') = (16, 9)$ and $d = 337$, it is seen that

$$\begin{aligned} 32r^2 - 14S^2 &= 2\cdot 337(u^2 - v^2) \\ 9r^2 - 25S^2 &= -2\cdot 337uv, \end{aligned} \tag{17}$$

and also

$$(9u + 16v)^2 - 9S^2 = 337r^2.$$

Choose the sign of S such that $9u + 16v + 3S \equiv 0 \bmod 337$. Then

$$\begin{aligned} 9u + 16v + 3S &= \pm 2\cdot 3^e \cdot 337U^2, \\ 9u + 16v - 3S &= \pm 2\cdot 3^e \cdot V^2, \\ v &= \pm 2\cdot 3^e UV, \end{aligned}$$

where U and V are relatively prime, $e \in \{0,1\}$ and matching $\pm$ signs. Then

$$\pm 9u = 3^e((V-16U)^2 + 81U^2)$$

from which we deduce that $e = 0$, because $\gcd(u,v) = 1$. Put $A := U$ and $3B := V - 16U$. Recall that

$$R = 337r^2, \quad \text{and} \quad \max(R, S^2) < M^2 = \exp(22.1030),$$

so that (17) implies that

$$2 \cdot 337|u^2 - v^2| = |32r^2 - 14S^2| \leq \frac{32M^2}{337} + 14M^2 < 14.1M^2,$$
$$2.337|uv| = |9r^2 - 25S^2| \leq \frac{9M^2}{337} + 25M^2 < 25.1M^2.$$

Consequently,

$$\max(u^2, v^2) = |u^2 - v^2| + \min(u^2, v^2) < 0.06M^2,$$

so that finally

$$\max(|A|, |B|) \leq \sqrt{|u|} < 125.$$

The remaining search for rational points P with $h(P) < 22.1030$ is now rather straightforward. Choosing the upper bounds for the search parameters rather widely, 36 rational points (X, Y) with $Y > 0$ were found, only 11 of which satisfy the canonical height upper bound of 6.3026. Taking into account that in our search only points associated with $d = 1$ and $d = p$ are considered (see (3))–this means that of the two points P and $P + P_0$ only one is counted–and points doubling another one are neglected, we found precisely those points we expected to find.

This completes the proof of the theorem. □

As is mentioned in the statement of Theorem 1.6 above, another rank 3 example is provided by $p = 1201$. In fact, using, for instance, Section 2 above, one finds that on the model $y^2 = (x+p)(x^2+p^2)$ three points with $x = -2^3 \cdot 3p/5^2$, $x = 7 \cdot 43p/900$ and $x = 2^4 \cdot 3 \cdot 5^2 \cdot 769p/(13^2 37^2)$ generate a free subgroup of rank 3 of the group of rational points. A detailed search, like we did for $p = 337$, reveals that these points also form a set of generators for the full subgroup of rational points modulo torsion.

ENDNOTES

1. Apecs, an acronym for "arithmetic of plane elliptic curves," is a collection of procedures written in the Maple language; it also contains a catalog of the Antwerp IV curves of [**2**]. Here we used version 2.7.

REFERENCES

1. B.J. Birch, *Heegner points of elliptic curves*, Symp. Math. Inst. Alta Math. **15** (1975), 441–445.

2. B.J. Birch and W. Kuyk, *Modular functions of one variable* IV, Springer-Verlag LNM 476 (1975).

3. A. Bremner, *On the equation* $Y^2 = X(X^2 + p)$, in *Number theory and applications* (R.A. Mollin, ed.), Kluwer, Dordrecht, The Netherlands, 1989, 3–23.

4. A. Bremner and D. Buell, *Three points of great height on elliptic curves*, Math. Comp. **61** (1993), 111–115.

5. A. Bremner and J.W.S. Cassels, *On the equation* $Y^2 = X(X^2 + p)$, Math. Comp. **42** (1984), 257–264.

6. J. Coates, *Elliptic curves and Iwasawa theory*, in *Modular forms* (R.A. Rankin, ed.), Ellis Horwood, Chichester, 1984, 51–73.

7. B. Gross and D. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), 225–320.

8. T. Honda and I. Miyawaki, *Zeta-functions of elliptic curves of* 2*-power conductor*, J. Math. Soc. Japan **26** (1974), 362–373.

9. N. Koblitz, *Introduction to elliptic curves and modular forms*, Springer-Verlag, New York, 1984.

10. J.-F. Mestre, *Formules explicites et minorations de conducteurs de variétés algébriques*, Compositio Math. **58** (1986), 209–232.

11. A. Ogg, *Abelian curves of* 2*-power conductor*, Proc. Cambr. Phil. Soc. **62** (1966), 143–148.

12. J.H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, New York, 1986.

13. ———, *The difference between the Weil height and the canonical height on elliptic curves*, Math. Comp. **55** (1990), 723–743.

14. P. Stevenhagen, *Divisibility by* 2*-powers of certain quadratic class numbers*, J. Number Theory **43** (1993), 1–19.

Econometric Institute, Erasmus University, P.O. Box 1738, 3000 DR Rotterdam, The Netherlands

Department of Mathematics, University of Groningen, P.O. Box 800, 9700 AV Groningen, The Netherlands