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

THREE-DESCENT AND THE BIRCH AND SWINNERTON-DYER CONJECTURE

ANDREA BANDINI

ABSTRACT. We give a three-descent procedure to bound and, in some cases, compute the three-part of the Selmer and Tate-Shafarevich group of the curves $y^2 = x^3 + a$, a a nonzero integer. This enables us to verify the whole Birch and Swinnerton-Dyer conjecture for some of such curves.

1. Introduction. Let E be an elliptic curve defined over $\mathbf{Q}$ with complex multiplication by the ring of integers O_F of a quadratic imaginary field F. Let $Ш(E/\mathbf{Q})$ be the Tate-Shafarevich group of E over $\mathbf{Q}$. The Birch and Swinnerton-Dyer conjecture (first formulation [**1**], 1965, refined in [**5**], 1982) relates the rank of $E(\mathbf{Q})$ and the order of $Ш(E/\mathbf{Q})$ to the behavior of a certain L-function, associated with E, at 1.

The first major step towards a proof of the conjecture was made by Coates and Wiles in 1977 in two papers ([**3, 4**]) in which they proved that for an elliptic curve E with complex multiplication

$$\operatorname{rank} E(\mathbf{Q}) \geq 1 \Longrightarrow L(E_{/\mathbf{Q}}, 1) = 0.$$

Later Rubin in a series of papers ([**7, 8** and many others]) proved, among other important results, that if $\operatorname{rank} E(\mathbf{Q}) = 0$ then the conjecture holds up to primes dividing $\#O_F^*$.

In this paper we deal with curves $E_a : y^2 = x^3 + a$ with $a \in \mathbf{Z} - \{0\}$ which admit complex multiplication by the ring of integers of $\mathbf{Q}(\sqrt{-3})$. This is the only case in which 3 divides $\#O_F^*$ and our goal is to bound or, in some cases, compute exactly the order of the three-part of the Tate-Shafarevich group of such curves.

In Section 2 we shall give precise definitions for the groups we are interested in and fix notations for the rest of the paper.

Received by the editors on February 9, 2001, and in revised form on June 14, 2001.

In Section 3 we shall define a number field K and describe a descent procedure to embed the three-part of the Selmer group of E_a into a subgroup of $K^*/(K^*)^3$ (Theorem 3.6). The three-rank of such a subgroup turns out to be always finite and easy to bound (Lemma 3.4).

In Section 4 we shall give some applications for the three-descent. In some special cases we will be able to compute exactly the three-part of the Selmer and Tate-Shafarevich groups and, with the help of Rubin's results, we will verify the whole conjecture for some curves of the form $y^2 = x^3 + b^3$.

2. Definitions and notations. Let E, E' be elliptic curves defined over $\mathbf{Q}$ with an isogeny φ of odd degree defined between them. Consider the exact sequence

$$0 \longrightarrow E[\varphi] \longrightarrow E(\overline{\mathbf{Q}}) \xrightarrow{\varphi} E'(\overline{\mathbf{Q}}) \longrightarrow 0$$

where $\overline{\mathbf{Q}}$ is an algebraic closure of $\mathbf{Q}$.

Taking cohomology with respect to the group $G = \mathrm{Gal}\,(\overline{\mathbf{Q}}/\mathbf{Q})$ and doing the same with local fields, one obtains the diagram

$$\begin{array}{ccccccc}
0 & \longrightarrow & E'(\mathbf{Q})/\varphi E(\mathbf{Q}) & \longrightarrow & H^1(G, E[\varphi]) & \longrightarrow & H^1(G, E(\overline{\mathbf{Q}})) \\
 & & \downarrow & & \downarrow{\scriptstyle \mathrm{res}_p} & & \downarrow{\scriptstyle \mathrm{res}_p} \\
0 & \longrightarrow & E'(\mathbf{Q}_p)/\varphi E(\mathbf{Q}_p) & \longrightarrow & H^1(G_p, E[\varphi]) & \longrightarrow & H^1(G_p, E(\overline{\mathbf{Q}_p}))
\end{array}$$

where $G_p = \mathrm{Gal}\,(\overline{\mathbf{Q}_p}/\mathbf{Q}_p)$ and res_p is the usual restriction map.

Definition 2.1. The Selmer group of E, relative to φ, is

$$S^{(\varphi)}(E/\mathbf{Q}) = \{x \in H^1(G, E[\varphi]) : \\ \mathrm{res}_p(x) \in \mathrm{Im}\,(E'(\mathbf{Q}_p)/\varphi E(\mathbf{Q}_p)) \text{ for all } p\}.$$

The *Tate-Shafarevich group of* E is

$$Ш(E/\mathbf{Q}) = \{x \in H^1(G, E(\overline{\mathbf{Q}})) : \mathrm{res}_p(x) = 0 \text{ for all } p\}.$$

These groups fit into the exact sequence

$$0 \longrightarrow E'(\mathbf{Q})/\varphi E(\mathbf{Q}) \longrightarrow S^{(\varphi)}(E/\mathbf{Q}) \longrightarrow Ш(E/\mathbf{Q})[\varphi] \longrightarrow 0.$$

Now assume that E admits complex multiplication by O_F, the ring of integers of an imaginary quadratic field F. Let $L(E_{/\mathbf{Q}}, s)$ be the L-function associated to E and let $\Omega \in \mathbf{C}^*$ be an O_F generator of the period lattice of a minimal model of E.

Theorem 2.2. *Assume* $L(E_{/\mathbf{Q}}, 1) \neq 0$. *Then* $\operatorname{rank} E(\mathbf{Q}) = 0$ *and, for any prime* p *not dividing* $\#O_F^*$, *one has*

$$\#E(F)\frac{L(E_{/\mathbf{Q}}, 1)}{\Omega} \not\equiv 0 \pmod{p} \Longrightarrow Ш(E/\mathbf{Q})[p] = 0.$$

Proof. See [**7**, p. 528]. □

As a consequence we see that the computation of the three-part of the Tate-Shafarevich group becomes crucial for the verification of the whole conjecture if 3 divides $\#O_F^*$. This happens if and only if $F = \mathbf{Q}(\sqrt{-3})$, i.e., only for the curves of the form $E_a : y^2 = x^3 + a$ with $a \neq 0$, and we restrict our attention to them from now on.

Some curves of this type have been studied before. For example, Stephens in [**15**] considers the case $a = -2^4 3^3 D^2$ with $D \in \mathbf{Z} - \{0\}$ square-free. With the help of Theorem 2.2 and of a formula by Schaefer (see Section 4) we are able to go a bit further in the verification of the conjecture.

3. The 3-descent. Let a be a nonzero integer not divisible by any sixth power, and let E_a be the elliptic curve given by the minimal Weierstrass equation $y^2 = x^3 + a$. Such a curve $E_a = E$ has discriminant $\Delta(E) = -2^4 3^3 a^2$, j-invariant $j(E) = 0$ and has complex multiplication by the ring of integers of $\mathbf{Q}(\sqrt{-3})$.

It is easy to see that the 3-torsion subgroup of E contains the cyclic subgroup $C = \{O, (0, \sqrt{a}), (0, -\sqrt{a})\}$, which is invariant under the action of $\operatorname{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Then a curve E' and an isogeny $\varphi : E \to E'$ exist, both defined over $\mathbf{Q}$, such that $\operatorname{Ker}(\varphi) = C$.

Explicitly (see [**17**, p. 306]) we have

$$E' : \eta^2 = \xi^3 - 27a \quad \text{and} \quad \varphi(x, y) = \left(\frac{y^2 + 3a}{x^2}, \frac{y(x^3 - 8a)}{x^3}\right).$$

The same remarks also hold for E' and $C' = \{O, (0, \sqrt{-27a}), (0, -\sqrt{-27a})\}$ so the dual isogeny $\psi : E' \to E$, such that $\psi\varphi = [3]$ on E and $\varphi\psi = [3]$ on E', is defined over $\mathbf{Q}$ as well.

Remark 3.1. Note that if 27 divides a, then the Weierstrass equation for E' is not minimal. In that case we shall define

$$E' : \eta^2 = \xi^3 - \frac{a}{27}$$

and analogous small modifications are needed for φ and ψ.

Our goal is to embed the Selmer group $S^{(\varphi)}(E/\mathbf{Q})$ into a more understandable group which we shall soon describe. We start with some Galois cohomology to build a commutative diagram which will simplify our task.

Consider the exact sequence

$$0 \longrightarrow C \longrightarrow E(\overline{\mathbf{Q}}) \xrightarrow{\varphi} E'(\overline{\mathbf{Q}}) \longrightarrow 0.$$

Let K be a quadratic extension of $\mathbf{Q}$. Let $G = \mathrm{Gal}\,(\overline{\mathbf{Q}}/\mathbf{Q})$ and $G_K = \mathrm{Gal}\,(\overline{\mathbf{Q}}/K)$. Taking G-cohomology and using the inflation-restriction sequence, where $[K : \mathbf{Q}] = 2$ yields $H^1(\mathrm{Gal}\,(K/\mathbf{Q}), C^{G_K}) = 0$, one gets injections

$$E'(\mathbf{Q})/\varphi E(\mathbf{Q}) \hookrightarrow H^1(G, C) \hookrightarrow H^1(G_K, C).$$

There are two natural choices for K depending on the action we want on C.

1. $K = \mathbf{Q}(\sqrt{a})$: trivial action (see [**10**]) which yields

$$H^1(G_K, C) \simeq \mathrm{Hom}\,(G_K, \mathbf{Z}/3\mathbf{Z}).$$

2. $K = \mathbf{Q}(\sqrt{-3a})$: action by inversion (see [**17**]) which gives

$$H^1(G_K, C) \simeq H^1(G_K, \mu_3) \simeq K^*/(K^*)^3$$

where the last isomorphism holds by Hilbert Theorem 90.

The first one has been described by Satgé in [**10**] so we are going to focus on the second and our results will be complementary to the ones of that paper.

From now on, let $K = \mathbf{Q}(\sqrt{-3a})$. We have obtained an embedding

$$\delta : E'(\mathbf{Q})/\varphi E(\mathbf{Q}) \hookrightarrow K^*/(K^*)^3$$

which can be extended to local fields as well. Let p be a prime in $\mathbf{Q}$ and let $\mathfrak{p}$ be a prime of K lying above p. Then, with the same procedure, we find

$$\delta_{\mathfrak{p}} : E'(\mathbf{Q}_p)/\varphi E(\mathbf{Q}_p) \hookrightarrow K_{\mathfrak{p}}^*/(K_{\mathfrak{p}}^*)^3.$$

Considering the maximal abelian unramified extensions of $\mathbf{Q}_p$ and $K_{\mathfrak{p}}$, we can build the following diagram

$$\begin{array}{ccc} E'(\mathbf{Q})/\varphi E(\mathbf{Q}) & \xrightarrow{\delta} & K^*/(K^*)^3 \\ \downarrow{\scriptstyle \nu_{\mathfrak{p}}} & & \downarrow{\scriptstyle \gamma_{\mathfrak{p}}} \\ E'(\mathbf{Q}_p)/\varphi E(\mathbf{Q}_p) & \xrightarrow{\delta_{\mathfrak{p}}} & K_{\mathfrak{p}}^*/(K_{\mathfrak{p}}^*)^3 \\ \downarrow{\scriptstyle \nu_{\mathfrak{p}}^{un}} & & \downarrow{\scriptstyle \gamma_{\mathfrak{p}}^{un}} \\ E'(\mathbf{Q}_p^{un})/\varphi E(\mathbf{Q}_p^{un}) & \xrightarrow{\delta_{\mathfrak{p}}^{un}} & K_{\mathfrak{p}}^{un*}/(K_{\mathfrak{p}}^{un*})^3 \end{array} \tag{1}$$

which holds for any $\mathfrak{p}$ dividing p and where all the horizontal maps are injective.

Remark 3.2. Note that the definition of $S^{(\varphi)}(E/\mathbf{Q})$ given in Definition 2.1 can be reformulated as follows

$$S^{(\varphi)}(E/\mathbf{Q}) = \{\alpha \in K^*/(K^*)^3 \text{ s.t. } \gamma_{\mathfrak{p}}(\alpha) \in \operatorname{Im}\delta_{\mathfrak{p}} \text{ for any } \mathfrak{p}\}$$

in the language of the diagram above.

To go on we need to define the set in which we want to embed $S^{(\varphi)}(E/\mathbf{Q})$.

Definition 3.3. Let O_K be the ring of integers of K, and let S be a finite set of finite primes of O_K. We define

$$H(S) = \{x \in K^*/(K^*)^3 : v_{\mathfrak{p}}(x) \equiv 0 \pmod 3 \text{ for any } \mathfrak{p} \notin S\}.$$

Lemma 3.4. *Let S be as above, let $r_3(K)$ be the 3-rank of the ideal class group of K, and let U_K be the group of units of O_K. Then*

$$\dim_{\mathbf{F}_3} H(S) \leq r_3(K) + \dim_{\mathbf{F}_3} U_K/U_K^3 + \#S.$$

Proof. Let O_S be the ring of S-integers in O_K. Taking the 3-part in the exact sequence on ideles one has

$$0 \longrightarrow O_S^*/(O_S^*)^3 \longrightarrow H(S) \longrightarrow \mathrm{Cl}\,(O_S)[3]$$

where $\mathrm{Cl}\,(O_S)$ is a quotient of the ideal class group of K. Dirichlet's theorem on $\mathrm{rank}\,(O_S^*)$ immediately yields the desired estimate for $\dim_{\mathbf{F}_3} H(S)$. □

Lemma 3.5. *For any $\mathfrak{p}$ of O_K not dividing 3 and $x \in K^*/(K^*)^3$*

$$v_{\mathfrak{p}}(x) \equiv 0 \pmod 3 \Longleftrightarrow \gamma_{\mathfrak{p}}^{un}\gamma_{\mathfrak{p}}(x) = 1.$$

Proof. $v_{\mathfrak{p}}(x) \equiv 0 \pmod 3 \Leftrightarrow \gamma_{\mathfrak{p}}(x)$ is trivial or a unit in $K_{\mathfrak{p}}^*/(K_{\mathfrak{p}}^*)^3$. This happens if and only if $K_{\mathfrak{p}}(\sqrt[3]{x})$ is $K_{\mathfrak{p}}$ itself or the cubic unramified extension of $K_{\mathfrak{p}}$, i.e., if and only if $x \in (K_{\mathfrak{p}}^{un*})^3$ or, which is the same, $\gamma_{\mathfrak{p}}^{un}\gamma_{\mathfrak{p}}(x) = 1$. □

Our final step consists in minimizing $\#S$, the number of "exceptional" primes, in order to find a sharper bound for $\dim_{\mathbf{F}_3} S^{(\varphi)}(E/\mathbf{Q})$.

Theorem 3.6. *$S^{(\varphi)}(E/\mathbf{Q})$ embeds into $H(S)$ with*

$$S = \{\mathfrak{p} : \mathfrak{p}|p,\ p \text{ is of bad reduction for } E, \#E'(\mathbf{Q}_p)/\varphi E(\mathbf{Q}_p) \neq 1\}.$$

Proof. We distinguish two cases for the primes of $\mathbf{Q}$.

1. *Primes of good reduction.* Let p be a prime of good reduction for E, i.e., $p \neq 2, 3$ and p does not divide a. Then the reduction mod p

map gives a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E_1(\mathbf{Q}_p^{un}) & \longrightarrow & E(\mathbf{Q}_p^{un}) & \xrightarrow{\mathrm{mod}p} & E(\overline{\mathbf{F}}_p) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle\varphi} & & \downarrow{\scriptstyle\varphi} & & \downarrow{\scriptstyle\varphi} & & \\ 0 & \longrightarrow & E_1'(\mathbf{Q}_p^{un}) & \longrightarrow & E'(\mathbf{Q}_p^{un}) & \xrightarrow{\mathrm{mod}p} & E'(\overline{\mathbf{F}}_p) & \longrightarrow & 0 \end{array}$$

where the right and left vertical arrows are surjective (the left one because $\varphi\psi = [3]$ and this is an isomorphism on $E_1'(\mathbf{Q}_p^{un})$ by [**13**]).

Therefore $E'(\mathbf{Q}_p^{un})/\varphi E(\mathbf{Q}_p^{un}) = 0$ and $\operatorname{Im}\delta_{\mathfrak{p}} \subseteq \operatorname{Ker}\gamma_{\mathfrak{p}}^{un}$. By Remark 3.2 and Lemma 3.5, one has

$$S^{(\varphi)}(E/\mathbf{Q}) \hookrightarrow H \text{ (primes of } K \text{ lying over primes of bad reduction).}$$

2. *Primes of bad reduction.* Diagram (1) clearly shows that if $E'(\mathbf{Q}_p)/\varphi E(\mathbf{Q}_p) = 0$, then

$$S^{(\varphi)}(E/\mathbf{Q}) \hookrightarrow \{x \in K^*/(K^*)^3 \text{ s.t. } v_{\mathfrak{p}}(x) \equiv 0 \pmod 3 \text{ for any } \mathfrak{p}|p\}.$$

Hence such $\mathfrak{p}$'s can be erased from the exceptional set, thus giving the desired embedding for $S^{(\varphi)}(E/\mathbf{Q})$. □

4. Applications to the Birch and Swinnerton-Dyer conjecture. To give examples and compute some explicit cases our main tool will be a formula proved by Schaefer ([**12**, Lemma 3.8]) which states

$$\#E'(\mathbf{Q}_p)/\varphi E(\mathbf{Q}_p) = \frac{|\varphi'(0)|_p^{-1}\#E(\mathbf{Q}_p)[\varphi]\#E'(\mathbf{Q}_p)/E_0'(\mathbf{Q}_p)}{\#E(\mathbf{Q}_p)/E_0(\mathbf{Q}_p)}$$

where $|\varphi'(0)|_p$ is the p-adic normalized absolute value of the first derivative of the power series expansion of φ evaluated at 0 (see [**13**]).

It is not hard to see that $|\varphi'(0)|_p^{-1} = 1$ if $p \neq 3$ and

$$|\varphi'(0)|_3^{-1} = \begin{cases} 3 & \text{if 27 divides } a \\ 1 & \text{otherwise} \end{cases}$$

by Remark 3.1.

Moreover, $E(\mathbf{Q}_p)[\varphi] = C \cap E(\mathbf{Q}_p)$, so

$$\#E(\mathbf{Q}_p)[\varphi] = \begin{cases} 3 & \text{if } a \text{ is a square in } \mathbf{Q}_p \\ 1 & \text{otherwise.} \end{cases}$$

The remaining terms can be computed with Tate's algorithm ([**16, 14**], or for the results [**10**]). For p of bad reduction different from 3 one has

$$E(\mathbf{Q}_p)/E_0(\mathbf{Q}_p) \text{ is } \begin{cases} \text{equal to } 3 & \text{if } a \text{ is a square in } \mathbf{Q}_p \\ \text{prime with } 3 & \text{otherwise.} \end{cases}$$

Finally $E(\mathbf{Q}_3)/E_0(\mathbf{Q}_3)$ has order 3 in the following cases

i) $v_3(a) = 2$ and $a/9 \equiv 1 \pmod 3$;

ii) $v_3(a) = 3$ and $a/27 \equiv 2, 4 \pmod 9$;

iii) $v_3(a) = 4$ and $a/81 \equiv 1 \pmod 3$

and is prime with 3 in all the other cases.

Similar computations can be done for $E'(\mathbf{Q}_p)/E'_0(\mathbf{Q}_p)$ substituting a with $-27a$, or $-a/27$.

An immediate application is the following

Theorem 4.1. *Let $a = \prod_{p|a} p^{v_p(a)} > 0$ with $1 \leq v_p(a) < 6$ and a not a square. Then $S^{(\varphi)}(E/\mathbf{Q}) = 0$ if the following conditions are verified*

1) $r_3(\mathbf{Q}(\sqrt{-3a})) = 0$;

2) *for p of bad reduction but $p \neq 2, 3$, $v_p(a) \equiv 1 \pmod 2$,*
or $v_p(a) \equiv 0 \pmod 2$ and $-27a/p^{v_p(a)}$ is not a square mod p;

3) $v_2(a) \equiv 1 \pmod 2$,
or $v_2(a) \equiv 0 \pmod 2$ and $a/2^{v_2(a)} \equiv 1, 3, 7 \pmod 8$;

4) $a \equiv 2, 8 \pmod 9$, *or $v_3(a) = 1$ and $a/3 \equiv 1 \pmod 3$,*
or $v_3(a) = 2$, or $v_3(a) = 3$ and $a/27 \equiv 2, 4 \pmod 9$.

Proof. We give the explicit computations for the easy case of p of bad reduction different from 2 and 3.

If $v_p(a) \equiv 1 \pmod 2$, then all the quantities involved are prime with 3 so $E'(\mathbf{Q}_p)/\varphi E(\mathbf{Q}_p) = 0$.

If $v_p(a) \equiv 0 \pmod 2$ then the contributions of $E(\mathbf{Q}_p)[\varphi]$ and $E(\mathbf{Q}_p)/E_0(\mathbf{Q}_p)$ compensate and we are left with $E'(\mathbf{Q}_p)/E'_0(\mathbf{Q}_p)$ which gives

$$\#E'(\mathbf{Q}_p)/\varphi E(\mathbf{Q}_p) = \begin{cases} 3 & \text{if } -27a/p^{v_p(a)} \text{ is a square mod } p \\ 1 & \text{otherwise.} \end{cases}$$

Note that this holds also in the case $27 \mid a$ because $-27a$ and $-a/27$ differ by a square.

In the same way one computes the cases $p = 2, 3$ using the formulas above.

$\#E'(\mathbf{Q}_2)/\varphi E(\mathbf{Q}_2)$ is equal to

- 1 if $v_2(a) \equiv 1 \pmod 2$,
  or $v_2(a) \equiv 0 \pmod 2$ and $a/2^{v_2(a)} \equiv 1, 3, 7 \pmod 8$;
- 3 if $v_2(a) \equiv 0 \pmod 2$ and $a/2^{v_2(a)} \equiv 5 \pmod 8$.

$\#E'(\mathbf{Q}_3)/\varphi E(\mathbf{Q}_3)$ is equal to

- 1 if $a \equiv 2, 8 \pmod 9$,
  or $v_3(a) = 1$ and $a/3 \equiv 1 \pmod 3$,
  or $v_3(a) = 2$,
  or $v_3(a) = 3$ and $a/27 \equiv 2, 4 \pmod 9$;
- 3 if $a \equiv 1, 4, 5 \pmod 9$,
  or $v_3(a) = 1$ and $a/3 \equiv 2 \pmod 3$,
  or $v_3(a) = 3$ and $a/27 \not\equiv 2, 4 \pmod 9$,
  or $v_3(a) = 4$,
  or $v_3(a) = 5$ and $a/243 \equiv 1 \pmod 3$;
- 9 if $a \equiv 7 \pmod 9$,
  or $v_3(a) = 5$ and $a/243 \equiv 2 \pmod 3$.

By Theorem 3.6 and conditions 2, 3 and 4, we have

$$S^{(\varphi)}(E/\mathbf{Q}) \hookrightarrow H(\varnothing).$$

By Lemma 3.4, condition 1 and the fact that a is positive and not a square, one has $\dim_{\mathbf{F}_3} H(\varnothing) = 0$. □

Remark 4.2. In [**10**] there are similar conditions regarding the nullity of the rank of the same family of elliptic curves (Théorème 3.5). Obviously the fact that $S^{(\varphi)}(E/\mathbf{Q})$ is trivial does not imply that the rank is 0 (and vice versa). Moreover, our initial choice of the field K gives us conditions which are complementary to those of that paper. For example, Théorème 3.5 starts with the condition $a \equiv 5, 7 \pmod 9$.

An interesting case is given by the curves

$$E_{b^3} : y^2 = x^3 + b^3$$

with b a square-free integer. Such curves have a rational point of order 2, namely $P = (-b, 0)$, and it is possible to find the 2-part of the Selmer group by explicit computation (see [**13**]). Together with our procedure this might be useful to verify the full Birch and Swinnerton-Dyer conjecture in some cases.

For these curves the previous theorem translates into

Theorem 4.3. *Let $a = b^3$ with $b > 1$ square-free. Then $S^{(\varphi)}(E/\mathbf{Q}) = 0$ if the following conditions are verified*:

1) $r_3(\mathbf{Q}(\sqrt{-3b})) = 0$;

2) 2 *divides* b *or* $b \equiv 1, 3, 7 \pmod 8$;

3) $b \equiv 2, 5, 8 \pmod 9$.

4.1. Example 1: $S^{(\varphi)}(E/\mathbf{Q}) = 0$. In the following tables we give all the curves verifying the conditions of Theorems 4.1 or 4.3 for $2 \leq a \leq 102$ and $5 \leq b \leq 119$ (many computations were done using the APECS program). The first entry is a, or b, and the second is the rank of the curve $E : y^2 = x^3 + a$, or $y^2 = x^3 + b^3$. Once we know $\dim_{\mathbf{F}_3} S^{(\varphi)}(E/\mathbf{Q})$ we can compute $\dim_{\mathbf{F}_3} S^{(\psi)}(E'/\mathbf{Q})$ with a theorem by Cassels [**10**, Proposition 1.17], and this is our third entry. The fourth one is the order of the 3-part of the Tate-Shafarevich group. In four cases our procedure only gives an estimate. In these four cases, using the exact sequence of Section 2, it is easy to see that

$\dim_{\mathbf{F}_3} Ш(E/\mathbf{Q})[\psi] = 2$, but this is not enough to compute $Ш(E/\mathbf{Q})[3]$ exactly.

TABLE 1. $y^2 = x^3 + a$.

a	$\operatorname{rank}(E)$	$S^{(\psi)}(E')$	$Ш(E)$	a	$\operatorname{rank}(E)$	$S^{(\psi)}(E')$	$Ш(E)$
2	1	1	1	48	1	1	1
3	1	1	1	54	1	1	1
8	1	1	1	56	1	1	1
11	1	1	1	57	2	2	1
12	1	1	1	63	2	2	1
17	2	2	1	65	2	2	1
18	1	1	1	66	1	1	1
26	1	1	1	71	1	1	1
30	1	1	1	72	1	1	1
35	1	1	1	89	2	2	1
38	1	1	1	90	0	2	≤ 9
39	1	1	1	92	1	1	1
44	1	1	1	99	1	1	1
47	1	1	1	102	1	1	1

TABLE 2. $y^2 = x^3 + b^3$.

b	$\operatorname{rank}(E)$	$S^{(\psi)}(E')$	$Ш(E)$	b	$\operatorname{rank}(E)$	$S^{(\psi)}(E')$	$Ш(E)$
11	1	1	1	59	1	1	1
14	1	1	1	65	2	2	1
17	0	2	≤ 9	71	1	1	1
23	1	1	1	86	1	1	1
26	1	1	1	89	0	2	≤ 9
35	1	1	1	95	1	1	1
38	1	1	1	107	1	1	1
41	0	2	≤ 9	110	1	1	1
47	1	1	1	119	1	1	1

The computations are easy: for example take $a = 17$. From the exact sequence for the Selmer group, we get

$$S^{(\varphi)}(E/\mathbf{Q}) = 0 \Longrightarrow E'(\mathbf{Q})/\varphi E(\mathbf{Q}) = Ш(E/\mathbf{Q})[\varphi] = 0$$

and Cassels' theorem yields $\dim_{\mathbf{F}_3} S^{(\psi)}(E'/\mathbf{Q}) = 2$. The sequence

$$0 \longrightarrow E'[\psi]/\varphi E[3] \longrightarrow E'/\varphi E \longrightarrow E/3E \longrightarrow E/\psi E' \longrightarrow 0$$

(where we omitted the $\mathbf{Q}$'s for aesthetic reasons) and the fact that $\operatorname{rank}(E) = 2$ yield

$$\dim_{\mathbf{F}_3} E(\mathbf{Q})/\psi E'(\mathbf{Q}) = 2.$$

Therefore $E(\mathbf{Q})/\psi E'(\mathbf{Q}) \simeq S^{(\psi)}(E'/\mathbf{Q}) \Longrightarrow Ш(E'/\mathbf{Q})[\psi] = 0$. Finally the exact sequence

$$0 \longrightarrow Ш(E/\mathbf{Q})[\varphi] \longrightarrow Ш(E/\mathbf{Q})[3] \longrightarrow Ш(E'/\mathbf{Q})[\psi],$$

shows that $Ш(E/\mathbf{Q})[3] = 0$.

4.2. Example 2: the Birch and Swinnerton-Dyer conjecture. Consider the curve $E : y^2 = x^3 + 39^3$ which has rank 0. Standard computational methods show that the predicted order of the Tate-Shafarevich group is 1 and that 2 is the only prime dividing

$$\#E(\mathbf{Q}(\sqrt{-3}))\,\frac{L(E_{/\mathbf{Q}}, 1)}{\Omega}.$$

Then by Theorem 2.2, $Ш(E/\mathbf{Q})[p] = 0$ for any $p \neq 2, 3$ and it suffices to compute the 2 and 3 Sylow subgroups to verify the conjecture.

The presence of a rational point $P = (-39, 0)$ of order 2 makes the computation of the Selmer groups quite easy for the prime 2. Following [**13**], one defines

$$\mathbf{Q}(S, 2) = \{\pm 1, \pm 2, \pm 3, \pm 13, \pm 6, \pm 26, \pm 39, \pm 78\}.$$

With Silverman's embedding for the 2-descent, one checks that

$$S^{(\lambda)}(E/\mathbf{Q}) \simeq \{1, -3\} \quad \text{and} \quad S^{(\nu)}(E''/\mathbf{Q}) \simeq \{1, 3\}$$

where $\lambda : E \to E''$ and $\nu : E'' \to E$ are rational isogenies such that $\nu\lambda = [2]$ on E. It follows that

$$\#Ш(E/\mathbf{Q})[\lambda] = 1 \quad \text{and} \quad \#Ш(E''/\mathbf{Q})[\nu] = 1.$$

Hence the sequence

$$0 \longrightarrow Ш(E/\mathbf{Q})[\lambda] \longrightarrow Ш(E/\mathbf{Q})[2] \longrightarrow Ш(E''/\mathbf{Q})[\nu]$$

yields $\#Ш(E/\mathbf{Q})[2] = 1$.

For the 3-part, Theorem 3.6 with $K = \mathbf{Q}(\sqrt{-13})$ shows that

$$S^{(\varphi)}(E/\mathbf{Q}) \hookrightarrow H(\{\mathfrak{p}\})$$

where $\mathfrak{p}$ is the only prime of K lying above 3. Therefore, $\dim_{\mathbf{F}_3} S^{(\varphi)}(E/\mathbf{Q}) \leq 1$ and Cassels' theorem yields $\dim_{\mathbf{F}_3} S^{(\varphi)} = \dim_{\mathbf{F}_3} S^{(\psi)}$. So, by now, we only get $1 \leq \#Ш(E/\mathbf{Q})[3] \leq 9$ which is not enough even if we know from another theorem of Cassels (see [**13**]) that this order has to be a square.

In this case we can solve this problem going into the details of the computations done so far. Tracing back the maps in cohomology which lead to the diagram in Section 3, one sees that

$$\delta_{\mathfrak{p}}(\xi, \eta) = (\eta + 13\sqrt{-13})(K_{\mathfrak{p}}^*)^3$$

(see [**11**, Theorem 1.2] or [**17**]). Note that $E' : \eta^2 = \xi^3 - 13^3$ and it is easy to see that, for any $(\xi, \eta) \in E'(\mathbf{Q}_3)$,

$$v_{\mathfrak{p}}(\eta + 13\sqrt{-13}) \equiv 0 \pmod 3.$$

Hence we can take $\mathfrak{p}$ out of our exceptional set and, by Lemma 3.5, we get

$$S^{(\varphi)}(E/\mathbf{Q}) \hookrightarrow H(\varnothing),$$

i.e.,

$$\dim_{\mathbf{F}_3} S^{(\varphi)}(E/\mathbf{Q}) = \dim_{\mathbf{F}_3} S^{(\psi)}(E'/\mathbf{Q}) = 0$$

and eventually $Ш(E/\mathbf{Q})[3] = 0$.

Therefore $\#Ш(E/\mathbf{Q}) = 1$ and the whole conjecture is verified. The same procedure can be used, for example, for $b = 66,\ 102,\ 111$. We only remark that, in the cases $b = 66,\ 111$, one finds

$$\#Ш(E/\mathbf{Q})[3] = 1 \quad \text{and} \quad \#Ш(E/\mathbf{Q})[2] = 4.$$

The expected size of $Ш(E/\mathbf{Q})$ is 4 in both cases but, to conclude, one needs to show that there are no elements of order 4 in $Ш(E/\mathbf{Q})[4]$ and this needs some more powerful techniques (see, for example, [**2**] or [**6**]).

Acknowledgments. This paper was prepared while I was attending the MRI's master class in algebraic geometry at Utrecht University. I would like to thank both these institutions for their support and hospitality. I am especially grateful to Jaap Top for many helpful discussions and suggestions.

REFERENCES

1. B. Birch and P. Swinnerton-Dyer, *Notes on elliptic curves* II, J. Reine Angew. Math. **218** (1965), 79–108.

2. J.W.S. Cassels, *Second descents for elliptic curves*, J. Reine Angew. Math. **494** (1998), 101–127.

3. J. Coates and A. Wiles, *On the conjecture of Birch and Swinnerton-Dyer*, Invent. Math. **39** (1977), 223–251.

4. ———, *On p-adic L-functions and elliptic units*, J. Austral. Math. Soc. Ser. A **26** (1978), 1–25.

5. B. Gross, *On the conjecture of Birch and Swinnerton-Dyer for elliptic curves with complex multiplication*, in *Number theory related to Fermat's last theorem* (N. Koblitz, ed.), Progr. Math., vol. 26, Birkhäuser, Boston, 1982, pp. 219–236.

6. J.R. Merriman, S. Siksek and N.P. Smart, *Explicit* 4*-descents on an elliptic curve*, Acta Arith. **77** (1996), 385–404.

7. K. Rubin, *Tate-Shafarevich groups and L-functions of elliptic curves with complex multiplication*, Invent. Math. **89** (1987), 527–560.

8. ———, *The "main conjecture" of Iwasawa theory for imaginary quadratic fields*, Invent. Math. **103** (1991), 25–68.

9. ———, *Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer*, in *Arithmetic theory of elliptic curves* (C. Viola, ed.), Lecture Notes in Math., vol. 1716, Springer-Verlag, New York, 1999, pp. 167–234.

10. P. Satgé, *Groupes de Selmer et corps cubique*, J. Number Theory **23** (1986), 294–317.

11. E.F. Schaefer, 2*-descent on the Jacobian of hyperelliptic curves*, J. Number Theory **51** (1995), 219–232.

12. ———, *Class groups and Selmer groups*, J. Number Theory **56** (1996), 79–114.

13. J.H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Math., vol. 106, Springer-Verlag, New York, 1986.

14. ———, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Math., vol. 151, Springer-Verlag, New York, 1994.

15. N.M. Stephens, *The diophantine equation* $X^3 + Y^3 = DZ^3$ *and the conjectures of Birch and Swinnerton-Dyer*, J. Reine Angew. Math. **231** (1968), 121–162.

16. J. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, in *Modular functions of one variable* IV (B.J. Birch and W. Kuyk, eds.), Lecture Notes in Math., vol. 476, Springer-Verlag, New York, 1975, pp. 33–52.

17. J. Top, *Descent by* 3*-isogeny and* 3*-rank of quadratic fields* in Advances in number theory, Proceedings of Conf. in Kingston (F.Q. Gouvea and N. Yui, eds.), Oxford Sci. Publ., New York, 1993, pp. 303–317.

Dipartimento di Matematica, Universitá di Pisa, via F. Buonarroti n. 2, 56127 Pisa, Italy
E-mail address: bandini@mail.dm.unipi.it