Andrea Bandini

3-Selmer groups for curves $y^2 = x^3 + a$


Persistent URL: [http://dml.cz/dmlcz/128267](http://dml.cz/dmlcz/128267)

---

**Terms of use:**

© Institute of Mathematics AS CR, 2008

Institute of Mathematics of the Czech Academy of Sciences provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these Terms of use.
3-SELMER GROUPS FOR CURVES $y^2 = x^3 + a$

ANDREA BANDINI, Cosenza

(Received March 2, 2006)

Abstract. We explicitly perform some steps of a 3-descent algorithm for the curves $y^2 = x^3 + a$, $a$ a nonzero integer. In general this will enable us to bound the order of the 3-Selmer group of such curves.

Keywords: elliptic curves, Selmer groups

MSC 2000: 11G05

1. Introduction

Let $E$ be an elliptic curve defined over $\mathbb{Q}$, with complex multiplication given by the ring of integers $O_F$ of a quadratic imaginary field $F$. Some results of K. Rubin ([4], [5] and others) point out the necessity of computing explicitly the $p$-part of the Tate-Shafarevich group for some “exceptional” primes, which always include those dividing $\#O_F^\times$, in order to verify the whole Birch and Swinnerton-Dyer conjecture for such curves.

The exact sequence

$$0 \to E(\mathbb{Q})/pE(\mathbb{Q}) \to \text{Sel}^{(p)}(E/\mathbb{Q}) \to \text{III}(E/\mathbb{Q})[p] \to 0$$

shows the importance of computing the middle term (the $p$-Selmer group) to bound (and, in many cases, compute exactly) both the rank of $E$ and the order of the $p$-part of the Tate-Shafarevich group III($E/\mathbb{Q}$).

Recently an algorithm to perform a $p$-descent has been described by E. Schaefer and M. Stoll in [7]. It relies on number field computations (like computing $S$-units for a finite set of primes $S$) which are quite accessible at least for the prime $p = 3$.

In this paper we consider curves $E_a : y^2 = x^3 + a$ with $a \in \mathbb{Z} - \{0\}$. They describe all elliptic curves defined over $\mathbb{Q}$ admitting complex multiplication by the ring of
integers of \( \mathbb{Q}(\sqrt{-3})\), and this is the only case in which 3 divides \( \#O^*_F \). Such curves have been studied, for example, in [6], [11] and [12], so many results on their Selmer groups are already known. The aim of this paper is to present a combination of the algorithms of [1] and [7] which provides a nice and rather easy approach to the problem. To simplify the computations we shall perform a descent via isogenies as described for example in [13] and [1].

2. Notation and definitions

Let \( E_a : y^2 = x^3 + a \) with \( a \in \mathbb{Z} - \{0\} \) be an elliptic curve and, to have a minimal Weierstrass equation, assume that no 6th power divides \( a \). Let \( E_{a^2} : y^2 = x^3 + a^2 \) where

\[
\alpha^2 = \begin{cases} 
-27a & \text{if } 27 \text{ does not divide } a, \\
-\frac{1}{27}a & \text{otherwise.}
\end{cases}
\]

Notation. The (rather unconventional) choice of writing \( \alpha^2 \) has been made to lighten the notation in the rest of the paper, since its square root \( \alpha \) will appear quite often. Let \( m \in \mathbb{Z} - \{0\} \), then, in what follows, we fix the convention

\[
\sqrt{m} = \begin{cases} 
\text{the unique positive root} & \text{if } m > 0, \\
i\sqrt{|m|} & \text{if } m < 0.
\end{cases}
\]

There are isogenies \( \varphi : E_a \to E_{a^2} \) and \( \psi : E_{a^2} \to E_a \) such that \( \text{Ker } \varphi = E_a[\varphi] = \{O, (0, \sqrt{a}), (0, -\sqrt{a})\} \subset E_a[3], \psi \varphi = [3] \) on \( E_a \) and \( \varphi \psi = [3] \) on \( E_{a^2} \) (explicit formulas in [1] and [13]). From now on we will simply write \( E \) and \( E' \) for \( E_a \) and \( E_{a^2} \) respectively.

Let \( G = \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \) and, for any prime \( p \), let \( G_p \) be the decomposition group of \( p \) in \( G \). The cohomology of the exact sequence

\[
0 \to E[\varphi] \to E(\overline{\mathbb{Q}}) \xrightarrow{\varphi} E'(\overline{\mathbb{Q}}) \to 0
\]
gives a commutative diagram

\[
\begin{array}{cccccc}
0 & \to & E'(\overline{\mathbb{Q}})/\varphi E(\overline{\mathbb{Q}}) & \to & H^1(G, E[\varphi]) & \to & H^1(G, E(\overline{\mathbb{Q}})) \\
& & \downarrow \text{res}_p & & \downarrow \text{res}_p & & \\
0 & \to & E'(\mathbb{Q}_p)/\varphi E(\mathbb{Q}_p) & \to & H^1(G_p, E[\varphi]) & \to & H^1(G_p, E(\overline{\mathbb{Q}}_p))
\end{array}
\]

where \( \text{res}_p \) is the usual restriction map. Then the \( \varphi \)-Selmer group is defined to be the set

\[
\text{Sel}^{(\varphi)}(E/\mathbb{Q}) = \{ \beta \in H^1(G, E[\varphi]) : \text{res}_p(\beta) \in \text{Im } (E'(\mathbb{Q}_p)/\varphi E(\mathbb{Q}_p)) \ \forall p \}.
\]
The Tate-Shafarevich group $\text{III}(E/\mathbb{Q})$ fits into the exact sequence

$$0 \to E'(\mathbb{Q})/\varphi E(\mathbb{Q}) \to \text{Sel}^{(\varphi)}(E/\mathbb{Q}) \to \text{III}(E/\mathbb{Q})[\varphi] \to 0.$$ 

Following the same path as in [1, Section 3] we let $K = \mathbb{Q}(\sqrt{-3a}) = \mathbb{Q}(\alpha)$ and $G_K = \text{Gal}(\overline{\mathbb{Q}}/K)$. Via the inflation-restriction sequence and the isomorphism

$$H^1(G_K, E[\varphi]) \simeq H^1(G_K, \mu_3) \simeq K^*/K_3^*$$

we get an injective map

$$\delta: E'(\mathbb{Q})/\varphi E(\mathbb{Q}) \hookrightarrow K^*/K_3^*$$

which extends to local fields $\mathbb{Q}_p$ and to their maximal unramified extensions $\mathbb{Q}_p^{\text{unr}}$ as well. We have a commutative diagram

$$\begin{array}{ccc}
E'(\mathbb{Q})/\varphi E(\mathbb{Q}) & \xrightarrow{\delta} & K^*/K_3^* \\
\downarrow & & \downarrow \\
E'(\mathbb{Q}_p)/\varphi E(\mathbb{Q}_p) & \xrightarrow{\delta_p} & \mathbb{Q}_p(\alpha)^*/\mathbb{Q}_p(\alpha)_3^* \\
\downarrow & & \downarrow \\
E'(\mathbb{Q}_p^{\text{unr}})/\varphi E(\mathbb{Q}_p^{\text{unr}}) & \xrightarrow{\delta_p^{\text{unr}}} & \mathbb{Q}_p^{\text{unr}}(\alpha)^*/\mathbb{Q}_p^{\text{unr}}(\alpha)_3^*
\end{array}$$

where all the horizontal maps are injective.

Let $S$ be a finite set of finite primes of $O_K$ (the ring of integers of $K$) and define

$$H(S) = \{ \beta \in K^*/K_3^* : v_p(\beta) \equiv 0 \pmod{3} \ \forall \ p \not\in S \},$$

where $v_p$ is the $p$-adic valuation. For any such set $S$ let $S(\mathbb{Q})$ be the set of primes in $\mathbb{Z}$ lying below the primes in $S$.

Exploring the above diagram in [1] we proved (Theorem 3.6 there)

**Theorem 2.1.** \text{Sel}^{(\varphi)}(E/\mathbb{Q}) embeds in $H(S_1)$ with

$$S_1 = \{ p : p \ | \ p, \ p \text{ of bad reduction for } E \text{ and } E'(\mathbb{Q}_p)/\varphi E(\mathbb{Q}_p) \neq 0 \}.$$ 

This, with an easy bound on $\dim_{\mathbb{F}_3} H(S_1)$, was used to give bounds for $\text{Sel}^{(\varphi)}(E/\mathbb{Q})$, $\text{Sel}^{(\psi)}(E'/\mathbb{Q})$ and $\text{III}(E/\mathbb{Q})[3]$ and to show their triviality in some particular cases.
In [7] the authors describe a general algorithm for $p$-descent on elliptic curves which, applied to our case, gives exactly the same embeddings $\delta$ and $\delta_p$ (in their notation $D$ is $\mathbb{Q}(\alpha)$ and $k \circ \omega \circ \delta_\theta$ is our $\delta$). For any prime $p$ and any elliptic curve $\tilde{E}$ let $c_{\tilde{E},p} = \# \tilde{E}(\mathbb{Q}_p)/\tilde{E}_0(\mathbb{Q}_p)$ be the Tamagawa number. Let

$$S_2 = \{3\} \cup \{p: 3 | c_{E,p} \text{ or } 3 | c_{E',p}\},$$

which is a finite set of primes, and let

$$K(S_2) = \{\beta \in K^*/K^*: \beta \text{ is unramified outside } S_2\}$$

where $\beta$ is called unramified outside $S_2$ if $K(\sqrt[3]{\beta})/K$ is unramified at all primes of $O_K$ lying above the primes not in $S_2$ (including infinite ones). One has an embedding $\text{Sel}^{(\varphi)}(E/\mathbb{Q}) \hookrightarrow K(S_2)$ (see [7, Proposition 3.2 and Section 5]). Going through the algorithm (in particular Sections 3 and 5 of [7]) one finds a way to compute explicitly the function $\delta$ and a description of $\text{Sel}^{(\varphi)}(E/\mathbb{Q})$:

$$\text{Sel}^{(\varphi)}(E/\mathbb{Q}) \simeq \{\beta \in K(S_2): N_{K/\mathbb{Q}}(\beta) \in \mathbb{Q}^*3 \text{ and } \text{res}_p(\beta) \in \delta_p(E'(\mathbb{Q}_p)/\varphi E(\mathbb{Q}_p)) \forall p \in S_2\}$$

which is computable once one knows a basis for the $S_2$-units and the $S_2$-class group of $K$. Such bases are not always easy to find and, in the next section, we will only perform the computation of $\delta_p(E'(\mathbb{Q}_p)/\varphi E(\mathbb{Q}_p))$ for any $p \in S_2$. Then we will go back to our set $H(S_1)$ with this new information to see how the set $S_1$ can sometimes be made a little smaller.

**Notation.** Note that the set $S_1$ (and the, still to be defined, set $S'_1$) contains primes in $K$ while $S_2$ is a set of primes in $\mathbb{Q}$. We decided to maintain this notation to be coherent with the main references [1] and [7], hoping that no confusion will arise from it.

### 3. The 3-descent

First we need to determine the set $S_2$ and this can be done by Tate’s algorithm ([10, IV, Section 9]). For the curve $E$: $y^2 = x^3 + a$ (which has complex multiplication by the ring of integers of $\mathbb{Q}(\sqrt{-3})$) one has $3 | c_{E,p}$ if and only if the curve is of reduction type IV or IV*. Then

- for $p = 2$ one has $3 | c_{E,2} \iff v_2(a) = 0, 2$ and $a \in \mathbb{Q}_2^*2$;
- for $p \geq 5$ one has $3 | c_{E,p} \iff v_p(a) = 2, 4$ and $a \in \mathbb{Q}_p^*2$,}
where \( v_p \) is the \( p \)-adic valuation (we recall that we are assuming \( 0 \leq v_p(a) < 6 \) for any \( p \) and \( 3 \) need not be checked because \( 3 \in S_2 \) in any case). The same has to be done for \( E' : y^2 = x^3 + \alpha^2 \). Finally, one gets

\[
S_2 = \{3\} \cup \{ p : v_p(4a) = 2, 4 \text{ and } a \in \mathbb{Q}_p^* \text{ or } v_p(4a) = 2, 4 \text{ and } -3a \in \mathbb{Q}_p^* \}.
\]

Now we can go on computing \( \delta_p(E' / \phi E) \) for any \( p \in S_2 \).

### 3.1. Computing generators of \( E'(\mathbb{Q}_p) / \phi E(\mathbb{Q}_p) \)

In this section and in the next one we will consider only primes \( p \in S_2 \).

The size of \( E'(\mathbb{Q}_p) / \phi E(\mathbb{Q}_p) \) (see also [6, Lemme 1.9 and Lemme 1.10]) is given by the formulas

\[
\#E'(\mathbb{Q}_p) / \phi E(\mathbb{Q}_p) = \#E(\mathbb{Q}_p)[\phi] \cdot \frac{c_{E',p}}{c_{E,p}} \text{ if } p \neq 3;
\]

\[
\#E'(\mathbb{Q}_3) / \phi E(\mathbb{Q}_3) = \gamma \cdot \#E(\mathbb{Q}_3)[\phi] \cdot \frac{c_{E',3}}{c_{E,3}}
\]

(see [8, Lemma 3.8]) where \( \gamma \) is the norm of the leading coefficient of the power series representation of \( \phi \). Direct computations lead to

**Proposition 3.1.** For \( p \in S_2 \) one finds

\[
\#E'(\mathbb{Q}_p) / \phi E(\mathbb{Q}_p) = \begin{cases} 3 & \text{if } -3a \in \mathbb{Q}_p^*, \\ 1 & \text{otherwise,} \end{cases}
\]

while \( #E'(\mathbb{Q}_3) / \phi E(\mathbb{Q}_3) \) 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 \( a/27 \equiv 2, 4 \pmod{9} \);
2. 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 \( a/27 \equiv 1, 5, 7, 8 \pmod{9} \),
   - or \( v_3(a) = 4 \),
   - or \( v_3(a) = 5 \) and \( a/243 \equiv 1 \pmod{3} \);
3. if \( a \equiv 7 \pmod{9} \),
   - or \( v_3(a) = 5 \) and \( a/243 \equiv 2 \pmod{3} \).
Remark 3.2. More details on this computation can be found in [1, Theorem 4.1]. In that paper there is an error for $p = 2$ and $v_2(a) = 4$ because in that case $c_{E,2} = c_{E',2} = 1$, so

$$\#E'(\mathbb{Q}_p)/\varphi E(\mathbb{Q}_p) = \begin{cases} 3 & \text{if } a \in \mathbb{Q}_p^* \setminus \{1\}, \\ 1 & \text{otherwise.} \end{cases}$$

Since $E$ has good reduction at $2$ for $v_2(a) = 4$ and $a \in \mathbb{Q}_p^*$, one has that if $v_2(a) = 4$ then the primes dividing $2$ are not in the set $S_1$ of Theorem 2.1. Anyway, the other data are correct and we are only interested in those because if $v_2(a) = 4$ then $2 \notin S_2$.

Remark 3.3. From the definitions of $S_1$ and $S_2$ and Proposition 3.1 it is easy to see that $S_1(\mathbb{Q}) \subseteq S_2$.

Now we compute generators for the nontrivial cases.

3.1.1. Case 1: $p \neq 3$

The group $E'(\mathbb{Q}_p)/\varphi E(\mathbb{Q}_p)$ is nontrivial when $-3a \in \mathbb{Q}_p^2$; so $E'(\mathbb{Q}_p)[\psi] = \{O, (0, \alpha), (0, -\alpha)\}$ (remember that $\alpha^2 = -27a$ or $-a/27$). We have $(0, \alpha) = \varphi((\sqrt[3]{-4a}, \sqrt[3]{-3a}) + E[\alpha])$. We are considering $p \in S_2$ so $v_p(4a) = 2, 4$ and $-4a$ is not a cube in $\mathbb{Q}_p$. Hence $(0, \alpha) \notin \varphi E(\mathbb{Q}_p)$ and, in this case,

$$E'(\mathbb{Q}_p)/\varphi E(\mathbb{Q}_p) = \langle (0, \alpha) \rangle.$$ 

3.1.2. Case 2: $p = 3$

In general, we look for points in $E'(\mathbb{Q}_3)$ with first coordinate as small as possible or for particular points like the 3-torsion point $(\sqrt[3]{-4a}, \sqrt[3]{-3a})$. Then we have to check that such points are not in $\varphi E(\mathbb{Q}_3)$ with the explicit formula for $\varphi$ (but see also Remark 3.4). Moreover, when $\#E'(\mathbb{Q}_3)/\varphi E(\mathbb{Q}_3) = 9$, we shall also need to check the independence of the generators we found.

For example, consider the case $v_3(a) = 4$ with $\alpha^2 = -a/27$. Obviously $(1, \sqrt[3]{1 + \alpha^2}) \in E'(\mathbb{Q}_3)$ and one looks for a solution of

$$\varphi(x, y) = \left(\frac{y^2 + 3a}{9x^2}, \frac{y(x^3 - 8a)}{27x^3}\right) = (1, \sqrt[3]{1 + \alpha^2}) \quad \text{with } (x, y) \in E(\mathbb{Q}_3).$$

However,

$$\frac{y^2 + 3a}{9x^2} = 1 \iff x^3 + 4a = 9x^2 \iff x^2(x - 9) = -4a.$$ 

This yields $v_3(x^2(x - 9)) = 4$, which is not satisfied by any $x \in \mathbb{Q}_3$. Hence $(1, \sqrt[3]{1 + \alpha^2}) \notin \varphi E(\mathbb{Q}_3)$ and it is a generator of $E'(\mathbb{Q}_3)/\varphi E(\mathbb{Q}_3)$ in this case. In
general, \( E'(\mathbb{Q}_3)/\varphi E(\mathbb{Q}_3) \) can be generated by

\[
(0, \alpha) \text{ if } v_3(a) = 1 \text{ and } a/3 \equiv 2 \pmod{3},
\]

or \( v_3(a) = 3 \) and \( a/27 \equiv 5, 8 \pmod{9} \);

\[
(1, \sqrt{1 + \alpha^2}) \text{ if } a \equiv 1, 4 \pmod{9},
\]

or \( v_3(a) = 4 \),

or \( v_3(a) = 5 \) and \( a/243 \equiv 1 \pmod{3} \);

\[
(-1, \sqrt{\alpha^2 - 1}) \text{ if } v_3(a) = 3 \text{ and } a/27 \equiv 1, 7 \pmod{9};
\]

\[
(-3, \sqrt{\alpha^2 - 27}) \text{ if } a \equiv 5 \pmod{9};
\]

\[
(0, \alpha), (1, \sqrt{1 + \alpha^2}) \text{ if } v_3(a) = 5 \text{ and } a/243 \equiv 2 \pmod{3};
\]

\[
(1, \sqrt{1 + \alpha^2}), (\sqrt{-4\alpha^2}, \sqrt{-3\alpha^2}) \text{ if } a \equiv 7 \pmod{9}.
\]

**Remark 3.4.** For the next step we are going to compute the image of these points in \( \mathbb{Q}_3(\alpha)^*/\mathbb{Q}_3(\alpha)^3 \) via the map \( \delta_3 \). Since this map is injective it suffices to check that \( \delta_3(R) \notin \mathbb{Q}_3(\alpha)^* \) (which usually is quite easy) to know that \( R \notin \varphi E(\mathbb{Q}_3) \). For the same reason the independence of the generators for the cases \( a \equiv 7 \pmod{9} \) and \( v_3(a) = 5 \), \( a/243 \equiv 2 \pmod{3} \) can be checked by verifying the independence of their images.

### 3.2. Computing \( \delta_p(E'(\mathbb{Q}_p)/\varphi E(\mathbb{Q}_p)) \)

We start with the explicit description of the map \( \delta \) (see [7, Section 3] and [3, Section 2]). Let \( P = (0, \alpha) \) and consider the map on the points of \( E' \) given by \( f(x, y) = y - \alpha \). Its divisor is \( 3P - 3O \) and it satisfies

\[
f \circ \varphi(x, y) = \begin{cases} 
\left( \frac{y - \sqrt{-3a}}{x} \right)^3 & \text{if } 27 \nmid a, \\
\left( \frac{y - \sqrt{-3a}}{3x} \right)^3 & \text{if } 27 \mid a,
\end{cases} \quad \forall (x, y) \in E.
\]

For any \( R \in E'(\mathbb{Q}) \) let \( \sum_{i=1}^{n} P_i - \sum_{i=1}^{n} Q_i \) be a \( \mathbb{Q} \)-defined divisor which is linearly equivalent to \( R - O \) and whose support avoids \( E'[\psi] \). Then \( \delta \) is equivalent to the function \( F \) defined on divisors of degree 0

\[
\delta: E'(\mathbb{Q})/\varphi E(\mathbb{Q}) \hookrightarrow \mathbb{Q}(\alpha)^*/\mathbb{Q}(\alpha)^3,
\]

\[
\delta(R) = F(R - O) \overset{\text{def}}{=} \prod_{i=1}^{n} f(P_i) / \prod_{i=1}^{n} f(Q_i).
\]
Since \( f \circ \varphi \) is a cube, for any \( R \notin E'[3] \) we simply have \( F(R - O) = f(R) \). For \( R \in E'[3] \) we have to find a linearly equivalent divisor as described in [3, Section 2] and then apply \( f \) to it.

For example, consider \( R = (\sqrt[3]{-4\alpha^2}, \sqrt[3]{-3\alpha^2}) \in E'[3] \) (the computation for \( R = (0, \alpha) \) is similar and easier). Take \( -R = (\sqrt[3]{-4\alpha^2}, -\sqrt[3]{3\alpha^2}) \) and let \( T = (0, 0) \). Let

\[
r: y = -\frac{\sqrt[3]{-3\alpha^2}}{\sqrt[3]{-4\alpha^2}} \cdot x \text{ def } b x
\]

be the line through \( -R \) and \( T \) which does not pass through any other 3-torsion point. Let \( -R, P_1 = (x_1, bx_1) \) and \( P_2 = (x_2, bx_2) \) be the points of intersection of \( r \) with \( E' \). Take any \( c \in \mathbb{Q} \) which is not the \( x \)-coordinate of any 3-torsion point of \( E' \) and let \( Q_1 = (c, \sqrt[3]{c^3 + \alpha^2}), Q_2 = (c, -\sqrt[3]{c^3 + \alpha^2}) \in E' \). Then \( R - O \) is linearly equivalent to \( P_1 + P_2 - Q_1 - Q_2 \) and, since \( f(Q_1)f(Q_2) \) is always a cube, we can compute

\[
\delta(R) = F(R - O) \equiv f(P_1)f(P_2) \pmod{\mathbb{Q}(\alpha)^*^3} \\
\equiv -\alpha^2 + ab(x_1 + x_2) - b^2x_1x_2 \pmod{\mathbb{Q}(\alpha)^*^3}.
\]

From the equations for \( r \cap E' \) one has that \( x_1 \) and \( x_2 \) are the zeros of \( x^2 - (\alpha^2/\sqrt[3]{16\alpha^4})x - \alpha^2/\sqrt[3]{-4\alpha^2} \). Hence, substituting \( b, x_1 + x_2 \) and \( x_1x_2 \), one finds

\[
F(R - O) \equiv -\frac{\alpha^2}{4} + \frac{\alpha\sqrt[3]{-3\alpha^2}}{4} \pmod{\mathbb{Q}(\alpha)^*^3}.
\]

Now, since \( R \) is among the generators we choose only for \( a \equiv 7 \pmod{9} \), one can substitute \( \alpha^2 = -27a \) to get

\[
F(R - O) \equiv \frac{27a}{4}(1 + \sqrt[3]{-3}) \equiv 2a(1 + \sqrt[3]{-3}) \pmod{\mathbb{Q}(\alpha)^*^3}.
\]

To conclude, as \( p \) varies in \( S_2 \) we have only five points involved among the generators of \( E'(\mathbb{Q}_p)/\varphi E(\mathbb{Q}_p) \), and their images are

- \( \delta_p(0, \alpha) \equiv 4a \pmod{\mathbb{Q}_p(\alpha)^*^3} \);
- \( \delta_3(1, \sqrt[3]{1 + \alpha^2}) = \sqrt[3]{1 + \alpha^2} - \alpha \);
- \( \delta_3(-1, \sqrt[3]{\alpha^2 - 1}) = \sqrt[3]{\alpha^2 - 1} - \alpha \);
- \( \delta_3(-3, \sqrt[3]{\alpha^2 - 27}) = \sqrt[3]{\alpha^2 - 27} - \alpha \);
- \( \delta_3(\sqrt[3]{-4\alpha^2}, \sqrt[3]{-3\alpha^2}) \equiv 2a(1 + \sqrt[3]{-3}) \pmod{\mathbb{Q}_3(\alpha)^*^3} \).

With these values it is easy to check the independence of the generators as indicated in Remark 3.4. We recall that (by [7, Section 5]) one has

\[
\text{Sel}^{(\varphi)}(E/\mathbb{Q}) \simeq \{ \beta \in K(S_2): N_{K/\mathbb{Q}}(\beta) \in \mathbb{Q}^*^3 \text{ and } \\
\text{res}_p(\beta) \in \delta_p(E'(\mathbb{Q}_p)/\varphi E(\mathbb{Q}_p)) \forall p \in S_2 \}.
\]

436
3.3. A new set $S'_1$

We recall the definition of the set $H(S)$ where $S$ is a finite set of (finite) primes of $O_K$,

$$H(S) = \{ \beta \in K^*/K^{*3} : v_p(\beta) \equiv 0 \pmod{3} \forall p \notin S \}.$$ 

For any such set $S$ let $S(\mathbb{Q})$ be the set of primes of $\mathbb{Z}$ lying below the primes in $S$. Consider the embedding $\text{Sel}(\varphi)(E/\mathbb{Q}) \hookrightarrow H(S_1)$, where

$$S_1 = \{ p : p \mid p, p \text{ of bad reduction for } E \text{ and } E'(\mathbb{Q}_p)/\varphi E(\mathbb{Q}_p) \neq 0 \}$$

described in Theorem 2.1.

Using the condition $\text{res}_p(\beta) \in \delta_p(E'(\mathbb{Q}_p)/\varphi E(\mathbb{Q}_p))$ and the computations done so far we are going to define a new set of primes $S'_1 \subseteq S_1$ (the difference will concern only primes dividing 3) and an embedding $\text{Sel}(\varphi)(E/\mathbb{Q}) \hookrightarrow H(S'_1)$. Such an embedding is sufficient to prove $\text{Sel}(\varphi)(E/\mathbb{Q}) = 0$ in some cases and can be useful to reduce the computations on $S_2$-units of $K$ to the minimum by considering elements in $H(S'_1) \cap K(S_2)$ (as suggested in [7]) where now one has $S'_1(\mathbb{Q}) \subseteq S_1(\mathbb{Q}) \subseteq S_2$ (see Remark 3.3).

**Theorem 3.5.** Let $S'_1(\mathbb{Q})$ be the set described by

- $3 \neq p \in S'_1(\mathbb{Q}) \iff v_p(4a) = 2, 4 \text{ and } -3a \in \mathbb{Q}_p^{*2}$;
- $3 \in S'_1(\mathbb{Q}) \iff v_3(a) = 1 \text{ and } a/3 \equiv 2 \pmod{3}, \text{ or } v_3(a) = 5 \text{ and } a/243 \equiv 2 \pmod{3},$

and let $S'_1 = \{ p : p \mid p, p \in S'_1(\mathbb{Q}) \}$.

Then there is an embedding $\text{Sel}(\varphi)(E/\mathbb{Q}) \hookrightarrow H(S'_1)$.

**Proof.** We take $\beta \in K^*/K^{*3}$ and check that $\text{res}_p(\beta) \in \text{Im} \delta_p$ yields $v_p(\beta) \equiv 0 \pmod{3}$ for all primes $p$ dividing $p \notin S'_1(\mathbb{Q})$. The conditions on $p \neq 3$ are equivalent to $p$ being of bad reduction and $E'(\mathbb{Q}_p)/\varphi E(\mathbb{Q}_p) \neq 0$, so the main difference from Theorem 2.1 concerns the prime 3. We briefly recall the arguments for the other primes and then focus on $p = 3$.

If $E'(\mathbb{Q}_p)/\varphi E(\mathbb{Q}_p) = 0$ then $\text{Im} \delta_p$ is trivial and there is nothing to prove (this obviously holds for any prime).

If $p \neq 3$ the isogeny $\varphi$ and the reduction mod $p$ map give the diagram

$$
\begin{array}{c}
0 \longrightarrow E_1(\mathbb{Q}_p^{\text{unr}}) \longrightarrow E_0(\mathbb{Q}_p^{\text{unr}}) \overset{\text{mod } p}{\longrightarrow} E_{ns}(\mathbb{F}_p) \longrightarrow 0 \\
\downarrow \varphi \downarrow \varphi \downarrow \varphi \\
0 \longrightarrow E'_1(\mathbb{Q}_p^{\text{unr}}) \longrightarrow E'_0(\mathbb{Q}_p^{\text{unr}}) \overset{\text{mod } p}{\longrightarrow} E'_{ns}(\mathbb{F}_p) \longrightarrow 0
\end{array}
$$

437
where the right and left vertical arrows are surjective (see [9, VII, Section 2]), so
\[ E'_0(\mathbb{Q}_p^{unr})/\varphi E_0(\mathbb{Q}_p^{unr}) = 0. \]
Consider also diagram (1) in Section 2.

If \( p \) is of good reduction then \( E'(\mathbb{Q}_p^{unr})/\varphi E(\mathbb{Q}_p^{unr}) \simeq E'_0(\mathbb{Q}_p^{unr})/\varphi E_0(\mathbb{Q}_p^{unr}) = 0 \) and \( \text{Im} \delta^{\text{unr}}_p = 1 \). Hence if \( \text{res}_p(\beta) \in \text{Im} \delta_p \) then \( \beta \) is unramified at all primes dividing \( p \), i.e. \( v_p(\beta) \equiv 0 \pmod{3} \) for any \( p \mid p \).

If \( p \) is of bad reduction then, by Proposition 3.1, one has \( E'(\mathbb{Q}_p)/\varphi E(\mathbb{Q}_p) = 0 \) unless \(-3a \in \mathbb{Q}_p^2\).

For \( p = 3 \) we go back to the computations done for \( \text{Im} \delta_3 \) (Section 3.2) and check what comes out from the condition \( \text{res}_3(\beta) \in \text{Im} \delta_3 \). We are interested in the class of \( v_p(\beta) \) modulo 3 (for any prime \( p \mid 3 \)); namely we need it to be 0 to eliminate 3 from our new set \( S'_1(\mathbb{Q}) \) (i.e. to eliminate \( p \mid 3 \) from \( S'_1 \)). Since we are working modulo \( \mathbb{Q}_3(\alpha)^* \), it suffices to check the class of \( v_p(x) \) modulo 3 for any \( x \in \text{Im} \delta_3 \) and, more precisely, it is enough to do that for \( x = \delta_3(P) \) as \( P \) varies in a set of generators for \( E'(\mathbb{Q}_3)/\varphi E(\mathbb{Q}_3) \) (computed in Section 3.1.2). As an example take
\[ P = (1, \sqrt{1 + \alpha^2}) \] with \( \delta_3(P) = \sqrt{1 + \alpha^2} - \alpha \).

If \( a \equiv 1, 4, 7 \pmod{9} \) then \( \mathbb{Q}_3(\alpha) = \mathbb{Q}_3(\sqrt{-3}) \) is ramified at 3 with \( (3) = (\sqrt{-3})^2 = p^2 \) and \( \alpha^2 = -27a \). Therefore
\[ v_p(\sqrt{1 - 27a} - \sqrt{-27a}) = 0, \]
and so, if \( \langle P \rangle = E'(\mathbb{Q}_3)/\varphi E(\mathbb{Q}_3) \) (i.e. if \( a \not\equiv 7 \pmod{9} \)), we can eliminate 3 from our new set \( S'_1(\mathbb{Q}) \) (if \( a \equiv 7 \pmod{9} \) one has to check the other generator as well).

If \( v_3(a) = 4 \) then \( (3) = p^2 \) is again ramified in \( \mathbb{Q}_3(\alpha) \) with \( \alpha^2 = -a/27 \) and \( \alpha \in \mathbb{p} \). As above,
\[ v_p(\sqrt{1 - a/27} - \sqrt{-a/27}) = 0, \]
so 3 can be eliminated again.

If \( v_3(a) = 5 \) and \( a/243 \equiv 1 \pmod{3} \) then \( \mathbb{Q}_3(\alpha) = \mathbb{Q}_3(\sqrt{-1}) \) is unramified at 3 which remains prime and \( \alpha^2 = -a/27 \). Thus
\[ v_3(\sqrt{1 - a/27} - \sqrt{-a/27}) = 0 \]
and \( 3 \notin S'_1(\mathbb{Q}) \).

If \( v_3(a) = 5 \) and \( a/243 \equiv 2 \pmod{3} \) then \( \mathbb{Q}_3(\alpha) = \mathbb{Q}_3 \) and \( \alpha^2 = -a/27 \). Thus
\[ v_3(\sqrt{1 - a/27} - \sqrt{-a/27}) = 0 \]
but, in this case, to eliminate 3 there is still one generator to check.
The same thing can be checked for all the generators chosen except \( (0, \alpha) \). When \( (0, \alpha) \) is one of the generators one finds

\[
v_3(4a) \equiv \begin{cases} 
1 \pmod{3} & \text{if } v_3(a) = 1 \text{ and } a/3 \equiv 2 \pmod{3}, \\
0 \pmod{3} & \text{if } v_3(a) = 3 \text{ and } a/27 \equiv 5, 8 \pmod{9}, \\
2 \pmod{3} & \text{if } v_3(a) = 5 \text{ and } a/243 \equiv 2 \pmod{3},
\end{cases}
\]

and we have \( 3 \not\in S'_1(\mathbb{Q}) \) only for \( v_3(a) = 3 \) and \( a/27 \equiv 5, 8 \pmod{9} \) (note that for the same reason we could not eliminate the primes \( p \neq 3 \) of bad reduction having \( (0, \alpha) \) as a generator of \( E'(\mathbb{Q}_p)/\varphi E(\mathbb{Q}_p) \)). \( \square \)

**Remark 3.6.** It follows from the theorem that to have \( p \in S'_1(\mathbb{Q}) \) it is necessary (but not sufficient) to have \( \alpha \in \mathbb{Q}_p \), i.e. \( \mathbb{Q}_p(\alpha) = \mathbb{Q}_p \). So any \( p \in S'_1(\mathbb{Q}) \) splits in \( K = \mathbb{Q}(\alpha) \) and one gets \( \#S'_1 = 2 \cdot \#S'_1(\mathbb{Q}) \).

There is an exact sequence

\[
0 \to O^*_{K,S'_1}/(O^*_{K,S'_1})^3 \to H(S'_1) \to \text{Cl}(O_{K,S'_1})[3]
\]

(with \( S'_1 \)-units and the 3-torsion of the \( S'_1 \)-class group of \( K \)), which immediately yields the bound

\[
\dim_{\mathbb{F}_3} \text{Sel}^{(\varphi)}(E/\mathbb{Q}) \leq \dim_{\mathbb{F}_3} H(S'_1) \leq r_3(K) + \dim_{\mathbb{F}_3} O_K/O_K^3 + \#S'_1
\]

(where \( r_3(K) \) is the 3-rank of the ideal class group of \( K \), see [1, Lemma 3.4]). Moreover, the generators of \( \text{Sel}^{(\varphi)}(E/\mathbb{Q}) \) can be found using the generators of \( O^*_{K,S'_1} \) and of \( \text{Cl}(O_{K,S'_1}) \) (as suggested in [7] with \( S_2 \)) where now \( S'_1(\mathbb{Q}) \subseteq S_2 \).

4. **Examples**

We consider only the case \( a > 0 \) since all curves with \( a < 0 \) are then included among the \( E' \)'s. Moreover, once one knows \( \#\text{Sel}^{(\varphi)}(E/\mathbb{Q}) \), one can compute \( \#\text{Sel}^{(\psi)}(E'/\mathbb{Q}) \) by a theorem of Cassels (see [2] or [6, Proposition 1.17]). After that, the commutative diagram

\[
\begin{array}{cccc}
E'(\mathbb{Q})/\varphi E(\mathbb{Q}) & \to & \text{Sel}^{(\varphi)}(E/\mathbb{Q}) & \to & \text{III}(E/\mathbb{Q})[\varphi] \\
\downarrow & & \downarrow & & \downarrow \\
E(\mathbb{Q})/3E(\mathbb{Q}) & \to & \text{Sel}^{(3)}(E/\mathbb{Q}) & \to & \text{III}(E/\mathbb{Q})[3] \\
\downarrow & & \downarrow & & \downarrow \\
E(\mathbb{Q})/\psi E'(\mathbb{Q}) & \to & \text{Sel}^{(\psi)}(E'/\mathbb{Q}) & \to & \text{III}(E'/\mathbb{Q})[\psi]
\end{array}
\]
(see [7, Section 6]) can be used in several cases to compute the 3-Selmer group and the 3-part of the Tate-Shafarevich group of $E$. Note that for $a > 0$ one has

$$\dim_{\mathbb{F}_3} O^*_K/O^*_K \cdot 3 = \begin{cases} 1 & \text{if } a \text{ is a square}, \\ 0 & \text{otherwise}. \end{cases}$$

### 4.1. $S'_1(\mathbb{Q}) = \emptyset$ and $\text{Sel}(\phi)^*(E/\mathbb{Q}) = 0$

As a simple corollary of Theorem 3.5 and of the bounds on $\dim_{\mathbb{F}_3} H(S'_1)$ one has

**Corollary 4.1.** If the following conditions are satisfied:

i) $a$ is not a square;

ii) $3$ does not divide the order of the ideal class group of $\mathbb{Q}(\alpha)$;

iii) $S'_1(\mathbb{Q}) = \emptyset$;

then $\text{Sel}(\phi)^*(E/\mathbb{Q}) = 0$.

Writing down explicitly condition iii) one has that $S'_1(\mathbb{Q}) = \emptyset$ if and only if

- $v_2(a) \neq 0, 2$,
  - or $v_2(a) = 0, 2$ and $a/2^{v_2(a)} \not\equiv 5 \pmod{8}$;
- $v_3(a) \neq 1, 5$,
  - or $v_3(a) = 1$ and $a/3 \equiv 1 \pmod{3}$,
  - or $v_3(a) = 5$ and $a/243 \equiv 1 \pmod{3}$;
- for $p \geq 5$, $v_p(a) \neq 2, 4$,
  - or $v_p(a) = 2, 4$ and $-3a/p^{v_p(a)}$ is not a square mod $p$.

As a particular case consider $a = b^3$ when there is a rational 2-torsion point and it is quite easy to perform a 2-descent (for example see [9, X]). Only the prime 2 can be in $S'_1(\mathbb{Q})$ and this occurs if and only if $v_2(a) = 0$ and $-3a \equiv 1 \pmod{8}$, i.e. $a = b^3 \equiv 5 \pmod{8}$. Therefore

$$S'_1(\mathbb{Q}) = \begin{cases} \{2\} & \text{if } a \equiv 5 \pmod{8}, \\ \emptyset & \text{otherwise}. \end{cases}$$

Moreover, $a$ is not a square (we are assuming $v_p(a) < 6$ for any $p$ so $b$ is squarefree) and one has

**Corollary 4.2.** Let $a = b^3$. If $a \not\equiv 5 \pmod{8}$ then $\text{Sel}(\phi)^*(E/\mathbb{Q})$ embeds in $\text{Cl}(\mathbb{Q}(\alpha))[3]$. In particular, if $3$ does not divide the order of the ideal class group of $\mathbb{Q}(\alpha)$ then $\text{Sel}(\phi)^*(E/\mathbb{Q}) = 0$.

**Proof.** The hypotheses yield

$$\text{Sel}(\phi)^*(E/\mathbb{Q}) \hookrightarrow H(\emptyset) \hookrightarrow \text{Cl}(\mathbb{Q}(\alpha))[3].$$

□

440
We conclude this part with some remarks regarding the Tate-Shafarevich group (the group directly involved in the Birch and Swinnerton-Dyer conjecture).

In the case \( a = b^3 \) Cassels’ formula ([6, Proposition 1.17]) yields
\[
\dim_{\mathbb{F}_3} \operatorname{Sel}^{(\psi)}(E'/\mathbb{Q}) = \dim_{\mathbb{F}_3} \operatorname{Sel}^{(\varphi)}(E/\mathbb{Q}) + m + y_\infty(a)
\]
where
\[
m = \begin{cases} 
1 & \text{if } a \equiv 1 \pmod{8}, \\
0 & \text{if } a \equiv 0, 3 \pmod{4}, \\
-1 & \text{if } a \equiv 5 \pmod{8}
\end{cases}
\]
\((m \text{ depends only on the behaviour of the prime } 2 \text{ in } \mathbb{Q}(\alpha))\), and
\[
y_\infty(a) = \begin{cases} 
1 & \text{if } v_3(a) = 0, \\
0 & \text{otherwise.}
\end{cases}
\]

**Proposition 4.3.** Let \( a = b^3 \). Assume that 3 does not divide the order of the ideal class group of \( \mathbb{Q}(\alpha) \) and that \( \text{III}(E/\mathbb{Q}) \) is finite. If \( a \not\equiv 1, 5, 13, 17, 21 \pmod{24} \) then \( \text{III}(E/\mathbb{Q})[3] = 0 \).

**Proof.** The hypothesis on the ideal class group and \( a \not\equiv 5, 13, 21 \pmod{24} \) yield \( \operatorname{Sel}^{(\varphi)}(E/\mathbb{Q}) = 0 \). With the above formula it is easy to check that \( a \not\equiv 1, 17 \pmod{24} \) implies \( \dim_{\mathbb{F}_3} \operatorname{Sel}^{(\psi)}(E'/\mathbb{Q}) \leq 1 \). Therefore \( \#\text{III}(E'/\mathbb{Q})[\psi] \leq 3 \), which yields \( \#\text{III}(E/\mathbb{Q})[3] \leq 3 \). Since the order of the Tate-Shafarevich group has to be a square, by [9, X, Theorem 4.14], this implies \( \text{III}(E/\mathbb{Q})[3] = 0 \). \( \square \)

In the cases \( a \equiv 1, 17 \pmod{24} \) one still has \( \operatorname{Sel}^{(\varphi)}(E/\mathbb{Q}) = 0 \) but one finds \( \dim_{\mathbb{F}_3} \operatorname{Sel}^{(\psi)}(E'/\mathbb{Q}) = 2 \), so we can only say that \( \#\text{III}(E/\mathbb{Q})[3] \leq 9 \).

4.2. The case \( a = b^2 \) with \( S'_1(\mathbb{Q}) = \emptyset \)

If \( a \) is a square then \( K = \mathbb{Q}(\sqrt{-3a}) = \mathbb{Q}(\sqrt{-3}) \), \( r_3(K) = 0 \) and \( O_K^*/O_K^{*3} = \langle \zeta_3 \rangle \) where \( \zeta_3 = \frac{1}{2}(-1 + \sqrt{-3}) \) is a cube root of unity. Obviously \(-3a \not\in \mathbb{Q}_3^{*2} \) and \(-3a \not\in \mathbb{Q}_2^{*2} \), so \( 2, 3 \not\in S'_1(\mathbb{Q}) \). For primes \( p \geq 5 \) one has \(-3a \in \mathbb{Q}_p^{*2} \iff -3 \text{ is a square mod } p \), i.e., if and only if \( p \equiv 1 \pmod{3} \). Therefore
\[
S'_1(\mathbb{Q}) = \{ p \geq 5 : p \mid a \text{ and } p \equiv 1 \pmod{3} \}
\]
and \( S'_1(\mathbb{Q}) = \emptyset \) if and only if all primes \( p \geq 5 \) dividing \( a \) are \( \equiv 2 \pmod{3} \).

From now on we consider the case \( S'_1(\mathbb{Q}) = \emptyset \). From the exact sequence
\[
0 \to O_K^*/O_K^{*3} \to H(\emptyset) \to \text{Cl}(K)
\]
one gets \( \operatorname{Sel}^{(\varphi)}(E/\mathbb{Q}) \hookrightarrow H(\emptyset) \simeq \langle \zeta_3 \rangle \).

441
It suffices to check whether $\zeta_3 \in \delta_p(E'(\mathbb{Q}_p)/\varphi E(\mathbb{Q}_p))$ for all $p \in S_2$ to see whether $\text{Sel}(\varphi)(E/\mathbb{Q}) = 0$ or $\langle \zeta_3 \rangle$ (obviously $\zeta_3 \in \text{Ker} N_{K/\mathbb{Q}}$, so the first condition for $\text{Sel}(\varphi)(E/\mathbb{Q})$ is verified).

Since $a$ is a square we have $S_2 = \{3\} \cup \{p: v_p(4a) = 2, 4\}$ and we are assuming that $p \in S_2 - \{3\} \implies p \equiv 2 \pmod{3}$. In this situation it is not hard to check that $\text{Sel}(\varphi)(E/\mathbb{Q}) = 0$ for any $a \neq 16, 1296$.

**Corollary 4.4.** Assume $a = b^2$ is a square and $S_1' = \{Q\} = \emptyset$. If $S_2 \neq \{3\}$ then $\text{Sel}(\varphi)(E/\mathbb{Q}) = 0$.

**Proof.** Let $p \in S_2 - \{3\}$. Then $-3a \not\in \mathbb{Q}_p^{*2}$ yields $E'(\mathbb{Q}_p)/\varphi E(\mathbb{Q}_p) = 0$ and we need to check whether $\zeta_3 \in \mathbb{Q}_p(\sqrt{-3})^{*3}$ or not. Obviously $\zeta_3$ is a cube if and only if a primitive 9th root of unity $\zeta_9$ is in $\mathbb{Q}_p(\sqrt{-3})^{*}$ and this occurs only for primes $p$ such that $p \equiv 1 \pmod{9}$ or $p^2 \equiv 1 \pmod{9}$. Since we are assuming $p \equiv 2 \pmod{3}$ these conditions reduce to $p \equiv 8 \pmod{9}$.

Let $a = 3^{2t}p_1^{2e_1}\ldots p_n^{2e_n}$ with $0 \leq i \leq 2$ and $1 \leq e_j \leq 2$, then $p_j \equiv 8 \pmod{9}$ for any $j$ yields $a/3^{2t} \equiv 1 \pmod{9}$. Therefore (see Section 3.1.2)

- $i = 0 \implies E'(\mathbb{Q}_3)/\varphi E(\mathbb{Q}_3)$ is generated by $(1, \sqrt{1 + \alpha^2})$;
- $i = 1 \implies E'(\mathbb{Q}_3)/\varphi E(\mathbb{Q}_3) = 0$ (by Proposition 3.1);
- $i = 2 \implies E'(\mathbb{Q}_3)/\varphi E(\mathbb{Q}_3)$ is generated by $(1, \sqrt{1 + \alpha^2})$.

**Case 1:** $i = 0$. We need to see whether $\zeta_3$ or $\zeta_3^2$ are congruent to $\sqrt{1 - 27b^2} - \sqrt{-27b^2}$ modulo $\mathbb{Q}_3(\sqrt{-3})^{*3}$. As an example consider

$$\zeta_3 \equiv \sqrt{1 - 27b^2} - \sqrt{-27b^2} \pmod{\mathbb{Q}_3(\sqrt{-3})^{*3}},$$

which yields

$$4(-1 + \sqrt{-3})(\sqrt{1 - 27b^2} + \sqrt{-27b^2}) = (x + y\sqrt{-3})^3 \in \mathbb{Q}_3(\sqrt{-3})^{*3}. $$

One finds two equations

$$\begin{cases} -4\sqrt{1 - 27b^2} - 36|b| = x(x^2 - 9y^2), \\ 4\sqrt{1 - 27b^2} - 12|b| = 3y(x^2 - y^2). \end{cases} \quad (\ast)$$

Consider the 3-adic valuation $v_3$ and note that

$$v_3(-4\sqrt{1 - 27b^2} - 36|b|) = v_3(4\sqrt{1 - 27b^2} - 12|b|) = 0. $$

Hence

- if $v_3(x) > 0$, then $(\ast) \implies v_3(y) < -1 \implies (\ast)$ has no solutions;
if \( v_3(x) < 0 \), then \((*) \implies v_3(y) < -1 \implies (**)
has no solutions;
if \( v_3(x) = 0 \), then (**)
has no solutions.
The same can be done with \( \zeta_3^2 \), so, for \( i = 0 \), \( \zeta_3 \not\in \text{Sel}^{(\varphi)}(E/\mathbb{Q}) = 0 \).

**Case 2:** \( i = 1 \). Obviously \( \zeta_9 \not\in \mathbb{Q}_3(\sqrt{-3}) \), hence \( \zeta_3 \not\in \mathbb{Q}_3(\sqrt{-3})^{*3} \) and \( \zeta_3 \not\in \text{Sel}^{(\varphi)}(E/\mathbb{Q}) = 0 \) as well.

**Case 3:** \( i = 2 \). We have to check whether \( \zeta_3 \) or \( \zeta_3^2 \) are congruent to \( \sqrt{1 - \frac{1}{27} b^2 + \frac{1}{3} b \sqrt{-3}} \) modulo \( \mathbb{Q}_3(\sqrt{-3})^{*3} \). One can easily see, as in Case 1, that this does not hold, hence again \( \zeta_3 \not\in \text{Sel}^{(\varphi)}(E/\mathbb{Q}) = 0 \).

\[\delta_3(12, 36) \equiv 32(1 + \sqrt{-3}) \equiv \zeta_3^2 \pmod{\mathbb{Q}_3(\sqrt{-3})^{*3}}.\]

Hence \( \text{Sel}^{(\varphi)}(E/\mathbb{Q}) = \langle \zeta_3 \rangle \) and, moreover, \( (12, 36) \in E'(\mathbb{Q}) - \varphi E(\mathbb{Q}) \) implies

\[\#\text{III}(E/\mathbb{Q})[\varphi] = 0.\]

Cassels’ formula yields \( \text{Sel}^{(\psi)}(E'/\mathbb{Q}) = 0 \) as well, so

\[\text{III}(E'/\mathbb{Q})[\psi] = 0 \quad \text{and} \quad \text{III}(E/\mathbb{Q})[3] = 0.\]

• \( a = 144, \, v_3(a) = 2 \)

One has \( E'(\mathbb{Q}_3)/\varphi E(\mathbb{Q}_3) = 0 \) and \( \zeta_9 \not\in \mathbb{Q}_3(\sqrt{-3}) \implies \zeta_3 \not\in \text{Sel}^{(\varphi)}(E/\mathbb{Q}) = 0 \).

Cassels’ formula yields \( \#\text{Sel}^{(\psi)}(E'/\mathbb{Q}) = 3 \). Moreover, \( E' \) is \( y^2 = x^3 - 3888 \) and \( (0, 12) \in E(\mathbb{Q}) - \psi E'(\mathbb{Q}) \). The diagram then shows that \( \text{III}(E'/\mathbb{Q})[\psi] = 0 \), which yields \( \text{III}(E/\mathbb{Q})[3] = 0 \) as well.

• \( a = 1296, \, v_3(a) = 4 \)

Now \( E'(\mathbb{Q}_3)/\varphi E(\mathbb{Q}_3) \) is generated by \( (1, \sqrt{-47}) \) and one can check that

\[\delta_3(1, \sqrt{-47}) \equiv \zeta_3^2 \pmod{\mathbb{Q}_3(\sqrt{-3})^{*3}}.\]

Hence \( \text{Sel}^{(\varphi)}(E/\mathbb{Q}) = \langle \zeta_3 \rangle \) and Cassels’ formula yields \( \#\text{Sel}^{(\psi)}(E'/\mathbb{Q}) = 3 \) as well. To conclude the three descent for this case note that \( E' \) is \( y^2 = x^3 - 48 \), so \( E'(\mathbb{Q})[\psi] = 0 \),
\((4, 4) \in E'(\mathbb{Q}) - \varphi E(\mathbb{Q})\) and \((0, 36) \in E(\mathbb{Q}) - \psi E'(\mathbb{Q})\). Hence the diagram shows that

\[
\#E'(\mathbb{Q})/\varphi E(\mathbb{Q}) = \#E(\mathbb{Q})/\psi E'(\mathbb{Q}) = \#\text{Sel}(\varphi)(E/\mathbb{Q}) = \#\text{Sel}(\psi)(E'/\mathbb{Q}) = 3, \\
\text{III}(E'/\mathbb{Q})[\psi] = \text{III}(E/\mathbb{Q})[\varphi] = \text{III}(E/\mathbb{Q})[3] = 0.
\]

Note that for \(a = b^2 \neq 16\) one has \((0, b) \in E(\mathbb{Q}) - \psi E'(\mathbb{Q})\), so that \(#\text{Sel}(\psi)(E'/\mathbb{Q}) \geq 3\). Consequently, we have

**Corollary 4.5.** Let \(a = b^2 \neq 16\). Assume that \(\text{Sel}(\varphi)(E/\mathbb{Q}) = 0\) and that \(\text{III}(E/\mathbb{Q})\) is finite. If \(\dim_{F_3} \text{Sel}(\psi)(E'/\mathbb{Q}) = 0\) then \(\text{III}(E'/\mathbb{Q})[3] = 0\).

**Proof.** Since \(a \neq 16\), one has \(#E(\mathbb{Q})/\psi E'(\mathbb{Q}) \geq 3\). Therefore the hypotheses imply \(#\text{III}(E'/\mathbb{Q})[\psi] \leq 3\) and \(\text{III}(E/\mathbb{Q})[\varphi] = 0\). The diagram yields \(#\text{III}(E/\mathbb{Q})[3] \leq 3\) and, since this order has to be a square, eventually \(\text{III}(E/\mathbb{Q})[3] = 0\). \(\square\)

As examples we consider the case \(S'_1 = \emptyset\) and \(\text{Sel}(\varphi)(E/\mathbb{Q}) = 0\). Let \(n\) be the number of primes of bad reduction for \(E\) which are congruent to 2 (mod 3). In this case Cassel’s formula ([6, Proposition 1.17]) reads

\[
\dim_{F_3} \text{Sel}(\psi)(E'/\mathbb{Q}) = n - 1 + y_\infty(a) + y_3(a)
\]

where

\[
y_\infty(a) = \begin{cases} 
1 & \text{if } v_3(a) = 0, 2, \\
0 & \text{if } v_3(a) = 4
\end{cases}
\]

and

\[
y_3(a) = \begin{cases} 
1 & \text{if } v_3(a) = 2, 4, \\
0 & \text{if } a \equiv 1, 4 \pmod{9}, \\
-1 & \text{if } a \equiv 7 \pmod{9}.
\end{cases}
\]

This yields

\[
\dim_{F_3} \text{Sel}(\psi)(E'/\mathbb{Q}) = \begin{cases} 
n - 1 & \text{if } a \equiv 7 \pmod{9}, \\
n & \text{if } v_3(a) = 4, \\
n & \text{if } a \equiv 1, 4 \pmod{9}, \\
n + 1 & \text{if } v_3(a) = 2.
\end{cases}
\]

So the hypothesis in Corollary 4.5 can easily be verified by counting the number of primes dividing \(a\) (and checking their congruence classes modulo 9).

**Acknowledgement.** The author wishes to thank the anonymous referee for helpful comments which led to some corrections and improvements in the exposition.
References


Author’s address: A. Bandini, Dipartimento di Matematica, Università della Calabria, Via P. Bucci–Cubo 30B, 87036 Arcavacata di Rende (CS), Italy, e-mail: bandini@mat.unical.it.