ACTA ARITHMETICA
105.2 (2002)

A formula for the Selmer group of a rational three-isogeny

by

Matt DeLong (Upland, IN)

1. Introduction. We study elliptic curves which admit a rational 3-isogeny. Such an elliptic curve, $E/\mathbb{Q}$, has a subgroup $T \subset E(\overline{\mathbb{Q}})$ of order 3 defined over $\mathbb{Q}$. We may suppose that E is given by the equation $y^2 = x^3 + ax^2 + cx + d$, and by a change of coordinates, we may assume that T is generated by the point $(0, \sqrt{d})$. Using the explicit addition law found in [6], we find that this point has order 3 precisely when $c^2 = 4ad$. If $c \neq 0$, then the equation of the curve can be written as $y^2 = x^3 + a(x-b)^2$.

In [8] Top gave an inequality relating the rank of the Mordell–Weil group over $\mathbb{Q}$ of an elliptic curve of the form $y^2 = x^3 + a(x-b)^2$ to the 3-ranks of the quadratic number fields $\mathbb{Q}(\sqrt{a})$ and $\mathbb{Q}(\sqrt{-3a})$, denoted $r_3(a)$ and $r_3(-3a)$ respectively. Here we expand on the work of Top to give a formula for the dimension of the Selmer group of the 3-isogeny from the elliptic curve given by the equation $y^2 = x^3 + a(x-b)^2$ to the isogenous curve given by $y^2 = x^3 - 27a(x-(4a+27b))^2$. The formula relates the dimension of this Selmer group to $r_3(a)$ and $r_3(-3a)$ as well as the cardinalities of certain sets of primes dividing a and $4a + 27b$. In addition, we calculate via a formula of Cassels [1] the difference between the dimensions of the Selmer groups of the isogeny and its dual. This provides a useful check on the main result.

If $c = 0$, then the equation of the curve can be written as $y^2 = x^3 + d$. We extend the work found in [4] and study elliptic curves of this latter form in [2].

2. The work of Top. Let E be the elliptic curve defined over $\mathbb{Q}$ given by the equation $E : y^2 = x^3 + a(x-b)^2$ with $a, b \in \mathbb{Z}$ such that $a, b,$ and $4a+27b$ are non-zero. Up to an isomorphism over $\mathbb{Q}$, we may assume that a is square-free, and we do so throughout. This curve admits a rational 3-isogeny. We denote this isogeny and its dual by ψ and ψ' respectively.

In [8] Top gave an injection of the Selmer group of ψ, denoted by S^{ψ}, into a group related to the class group of $\mathbb{Q}(\sqrt{-3a})$, and used this to bound

2000 *Mathematics Subject Classification*: Primary 11G05.

the dimension of the Selmer group. He similarly bounded the dimension of the Selmer group $S^{\psi'}$, and so deduced the following theorem concerning the rank of an elliptic curve of the form $E : y^2 = x^3 + a(x-b)^2$.

THEOREM 2.1 (Top). *Denote by $E_{a,b}/\mathbb{Q}$ the elliptic curve which is given by the equation $y^2 = x^3 + a(x-b)^2$ with $a, b \in \mathbb{Z}$, $a \neq 0$, $b \neq 0$, $4a+27b \neq 0$. Assume that*

(1) *$a \equiv 2$ or $11 \pmod{12}$ and*
(2) *a is square-free.*

Write s for the number of primes $p \geq 5$ such that $p \mid b$ and $\left(\frac{a}{p}\right) = 1$. Similarly, write t for the number of primes $p \geq 5$ such that $p \mid (4a + 27b)$ and $\left(\frac{-3a}{p}\right) = 1$. Then

$$\operatorname{rank} E_{a,b}(\mathbb{Q}) \leq r_3(a) + r_3(-3a) + s + t + 1.$$

REMARK 2.2. The first condition of the theorem is really two separate conditions. Condition (1a), $a \equiv 2$ or $3 \pmod 4$, ensures that, so far as the calculations concerning the Selmer group are concerned, the prime $p = 2$ behaves like a good prime ([1]). Condition (1b), $a \equiv 2 \pmod 3$, ensures that the prime $p = 3$ also behaves like a good prime.

The result of Top's theorem is an inequality for two reasons. The first reason is the unfortunate presence of the Tate–Shafarevich group. This problem will not be dealt with here. The second reason that Top's theorem gives an inequality is that he merely bounds the dimension of the Selmer groups by formulating the dimensions of the groups into which he injects S^{ψ} and $S^{\psi'}$. Here we make explicit the added restrictions necessary to determine the images of the Selmer groups in the groups considered by Top.

Because the primes 2 and 3 create special problems, the general result will actually be stated for a generalized Selmer group which avoids these primes. The generalized Selmer group will agree with the standard Selmer group when certain congruence conditions are placed on the parameter a, and these conditions will be stated explicitly.

3. An exact sequence. Let $E : y^2 = x^3 + a(x-b)^2$ be the elliptic curve considered above. Such an elliptic curve has a rational subgroup T of order 3 generated by the point $(0, b\sqrt{a})$. Dividing by this subgroup yields another elliptic curve $E' : y^2 = x^3 - 27a(x-4a-27b)^2$, which has a rational subgroup T' of order 3 generated by $(0, 3(4a+27b)\sqrt{-3a})$. Let $\psi : E \to E'$ be the quotient map. Its dual, $\psi' : E' \to E$, results from division by T'.

([1]) Top gives condition (1a) as $a \equiv 3 \pmod 4$ and $b \equiv 1 \pmod 2$ (or $a \equiv 1 \pmod 2$ and $b \equiv 2 \pmod 4$), but an application of Tate's algorithm shows that the correct condition is given above.

Consider the fields $K = \mathbb{Q}(\sqrt{-3a})$ and $K' = \mathbb{Q}(\sqrt{a})$. Following the notational conventions of Top, let S denote the set of all split primes of $K/\mathbb{Q}$. Write N for the map induced by the norm map, $N : K^*/K^{*3} \to \mathbb{Q}^*/\mathbb{Q}^{*3}$. For a set of primes $p_1, \ldots, p_t \in \mathbb{Z}$ which all split in K, write

$$(1) \quad H(p_1, \ldots, p_t) := \{x \in \ker N : 3 \,|\, v_{\mathfrak{p}}(x) \text{ for all } \mathfrak{p} \in S \text{ not lying over any } p_1, \ldots, p_t\}.$$

Likewise let S', N', and H' be the corresponding objects for the field K'.

Top showed that S^{ψ} injects into $H(P)$ and $S^{\psi'}$ injects into $H(P')$, where

$$(2) \quad P = \left\{\text{integer primes } p \geq 5 \text{ such that } p \,|\, (4a + 27b) \text{ and } \left(\frac{-3a}{p}\right) = 1\right\},$$

$$(3) \quad P' = \left\{\text{integer primes } p \geq 5 \text{ such that } p \,|\, b \text{ and } \left(\frac{a}{p}\right) = 1\right\}.$$

We use a well known exact sequence to extend these facts. The following lemma will be our key tool. Its proof is a standard but tedious diagram chase.

LEMMA 3.1. *For any sequence of homomorphisms of abelian groups* $A \xrightarrow{f} B \xrightarrow{g} C$, *we obtain the following exact sequence*:

$$0 \to \ker f \to \ker(g \circ f) \to \ker g \to \operatorname{cok} f \to \operatorname{cok}(g \circ f) \to \operatorname{cok} g \to 0.$$

For every prime $p \in \mathbb{Q}$ including $p = \infty$, we have the following commutative diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & E'(\mathbb{Q})/\psi E(\mathbb{Q}) & \longrightarrow & H^1(\mathbb{Q}, T) & \longrightarrow & H^1(\mathbb{Q}, E)_{\psi} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & E'(\mathbb{Q}_p)/\psi E(\mathbb{Q}_p) & \longrightarrow & H^1(\mathbb{Q}_p, T) & \longrightarrow & H^1(\mathbb{Q}_p, E)_{\psi} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & E'(\mathbb{Q}_p^{\mathrm{un}})/\psi E(\mathbb{Q}_p^{\mathrm{un}}) & \longrightarrow & H^1(\mathbb{Q}_p^{\mathrm{un}}, T) & \longrightarrow & H^1(\mathbb{Q}_p^{\mathrm{un}}, E)_{\psi} & \longrightarrow & 0
\end{array}$$

The commutative diagram is usually considered where the second and third rows are taken as the direct sum over all primes p. When we write $\bigoplus_p$ with no conditions on p, we mean that the sum is to be taken over all primes. We also consider the diagram with second and third rows taken as the direct sum over all primes $p \neq 2, 3$. This allows us to avoid special problems which occur for these primes.

The portion of the diagram to which we apply Lemma 3.1 is

$$(4) \qquad H^1(\mathbb{Q}, T) \to \bigoplus_p H^1(\mathbb{Q}_p, E)_{\psi} \to \bigoplus_p H^1(\mathbb{Q}_p^{\mathrm{un}}, E)_{\psi}.$$

Recall that S^{ψ} is defined to be the kernel of the first map. Also note that $H^1(\mathbb{R}, E)$ is of order dividing 2. Since the order of $H^1(\mathbb{R}, E)_{\psi}$ divides both 2 and 3, the group must be trivial. Therefore, when considering the above diagram we may restrict our attention to the finite primes.

We use the following notational convention.

DEFINITION 3.2. The *generalized Selmer group* is the kernel of

$$H^1(\mathbb{Q}, T) \to \bigoplus_{p \neq 2,3} H^1(\mathbb{Q}_p, E)_{\psi}.$$

It will be denoted by S_g^{ψ}.

Since we are interested in the dimension of the Selmer group, the following easy lemma will also be useful. We will apply this lemma to the exact sequence given in Lemma 3.1.

LEMMA 3.3. *If* $0 \to V_1 \to V_2 \to \ldots \to V_n \to 0$ *is an exact sequence of finite-dimensional vector spaces, then*

$$\dim V_1 - \dim V_2 + \dim V_3 - \ldots + (-1)^{n-1} \dim V_n = 0.$$

To avoid confusion in what follows, we remark that throughout we frequently identify the Selmer groups S^{ψ} and $S^{\psi'}$ with their images in $H(P)$ and $H(P')$ respectively.

4. The middle kernel of the sequence. We first analyze the kernel of $H^1(\mathbb{Q}, T) \to \bigoplus_p H^1(\mathbb{Q}_p^{\mathrm{un}}, E)_{\psi}$.

PROPOSITION 4.1. *The kernel of* $H^1(\mathbb{Q}, T) \to \bigoplus_{p \neq 2,3} H^1(\mathbb{Q}_p^{\mathrm{un}}, E)_{\psi}$ *is* $H(P)$, *where* $P = \{$*primes* $p \geq 5$ *such that* $p \,|\, (4a + 27b)$ *and* $\left(\frac{-3a}{p}\right) = 1\}$.

Proof. In this proof $p \neq 2, 3$ is a prime. In [8], Top demonstrated that $H^1(\mathbb{Q}, T)$ is isomorphic to $\ker N$, where $K = \mathbb{Q}(\sqrt{-3a})$ and $N : K^*/K^{*3} \to \mathbb{Q}^*/\mathbb{Q}^{*3}$. The isomorphism is well-determined up to sign, depending on the choice of a generator for $T(\overline{\mathbb{Q}})$. Now $x \in \ker N$ implies that $3 \,|\, v_p(N(x))$ for all p. If we let $\mathfrak{p}$ denote a prime lying over p, then

$$v_p(N(x)) = \begin{cases} v_{\mathfrak{p}}(x) & \text{if } p \text{ ramifies in } K, \\ 2v_{\mathfrak{p}}(x) & \text{if } p \text{ inert in } K, \end{cases} \tag{5}$$

implies that $3 \,|\, v_{\mathfrak{p}}(x)$ for non-split p.

First we consider the primes that ramify in K. Let $\widetilde{K}_{\mathfrak{p}}$ denote the maximal unramified extension of $K_{\mathfrak{p}}$. We have

$$H^1(\mathbb{Q}_p^{\mathrm{un}}, T) \cong \ker(Nm : \widetilde{K}_{\mathfrak{p}}^*/\widetilde{K}_{\mathfrak{p}}^{*3} \to \mathbb{Q}_p^{\mathrm{un}*}/\mathbb{Q}_p^{\mathrm{un}*3}), \tag{6}$$

where $\widetilde{K}_{\mathfrak{p}}^*/\widetilde{K}_{\mathfrak{p}}^{*3} \cong \mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Q}_p^{\mathrm{un}*}/\mathbb{Q}_p^{\mathrm{un}*3} \cong \mathbb{Z}/3\mathbb{Z}$. Since $v_p(N(x)) = v_{\mathfrak{p}}(x)$, the norm map commutes with the identity map on $\mathbb{Z}/3\mathbb{Z}$. Therefore, $H^1(\mathbb{Q}_p^{\mathrm{un}}, T) = 0$, and so $H^1(\mathbb{Q}, T) \to H^1(\mathbb{Q}_p^{\mathrm{un}}, T)$ is the zero map.

If p is not ramified, then $T \cong \mu_3$ over $\mathbb{Q}_p^{\mathrm{un}}$. Therefore, $\widetilde{K}_{\mathfrak{p}} = \mathbb{Q}_p^{\mathrm{un}}$, and so $H^1(\mathbb{Q}_p^{\mathrm{un}}, T) \cong \mathbb{Q}_p^{\mathrm{un}*}/\mathbb{Q}_p^{\mathrm{un}*3} \cong \mathbb{Z}/3\mathbb{Z}$.

If we identify $H^1(\mathbb{Q}, T)$ with $\ker N$, it follows that for p unramified, $x \in H^1(\mathbb{Q}, T)$ has $3 \mid v_{\mathfrak{p}}(x)$ if and only if it maps to the identity in $H^1(\mathbb{Q}_p^{\mathrm{un}}, T)$. So if p is inert, then $H^1(\mathbb{Q}, T) \to H^1(\mathbb{Q}_p^{\mathrm{un}}, T)$ is the zero map by (5).

Finally we treat the split primes. By definition the elements of $H(P)$ map to the identity in $H^1(\mathbb{Q}_p^{\mathrm{un}}, T)$ for all split primes $p \notin P$. Following the argument analogous to case 2 of page 310 of Top [8], we can show that $E'(\mathbb{Q}_p^{\mathrm{un}})/\psi E(\mathbb{Q}_p^{\mathrm{un}}) \cong \mathbb{Z}/3\mathbb{Z}$ for $p \in P$, in virtue of the following commutative diagram with exact rows and columns:

$$\begin{array}{ccccc}
0 & \longrightarrow & 0 & \longrightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow \\
E_0(\mathbb{Q}_p^{\mathrm{un}}) & \longrightarrow & E_0'(\mathbb{Q}_p^{\mathrm{un}}) & \longrightarrow & E_0'(\mathbb{Q}_p^{\mathrm{un}})/\psi E_0(\mathbb{Q}_p^{\mathrm{un}}) \\
\downarrow & & \downarrow & & \downarrow \\
E(\mathbb{Q}_p^{\mathrm{un}}) & \longrightarrow & E'(\mathbb{Q}_p^{\mathrm{un}}) & \longrightarrow & E'(\mathbb{Q}_p^{\mathrm{un}})/\psi E(\mathbb{Q}_p^{\mathrm{un}}) \\
\downarrow & & \downarrow & & \downarrow \\
\mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/3n\mathbb{Z} & \longrightarrow & \mathbb{Z}/3\mathbb{Z} \\
\downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & 0 & \longrightarrow & 0
\end{array}$$

The second-to-last row comes from Tate's algorithm, which shows that if $p^n \parallel (4a+27b)$, then the reduction for E is type I_n, while the reduction for E' is type I_{3n}. Since $E_0'(\mathbb{Q}_p^{\mathrm{un}})/\psi E_0(\mathbb{Q}_p^{\mathrm{un}}) = 0$, we have $E'(\mathbb{Q}_p^{\mathrm{un}})/\psi E(\mathbb{Q}_p^{\mathrm{un}}) \cong \mathbb{Z}/3\mathbb{Z}$.

Thus, the exactness of

$$0 \to E'(\mathbb{Q}_p^{\mathrm{un}})/\psi E(\mathbb{Q}_p^{\mathrm{un}}) \to H^1(\mathbb{Q}_p^{\mathrm{un}}, T) \to H^1(\mathbb{Q}_p^{\mathrm{un}}, E)_\psi \to 0 \tag{7}$$

implies that $H^1(\mathbb{Q}_p^{\mathrm{un}}, E)_\psi = 0$ for $p \in P$. Therefore, $H(P)$ is contained in the kernel of $H^1(\mathbb{Q}, T) \to \bigoplus_{p \neq 2,3} H^1(\mathbb{Q}_p^{\mathrm{un}}, E)_\psi$.

For the split primes at which E, E' have good reduction, $E'(\mathbb{Q}_p^{\mathrm{un}})/\psi E(\mathbb{Q}_p^{\mathrm{un}})$ is the trivial group. The remaining split primes are those that divide b. Using the argument analogous to case 2 of page 311 of Top [8], we can show that $E'(\mathbb{Q}_p^{\mathrm{un}})/\psi E(\mathbb{Q}_p^{\mathrm{un}}) = 0$ for these primes as well. As before, we have a commutative diagram:

$$\begin{array}{ccccc}
0 & \longrightarrow & 0 & \longrightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow \\
E_0(\mathbb{Q}_p^{\mathrm{un}}) & \longrightarrow & E_0'(\mathbb{Q}_p^{\mathrm{un}}) & \longrightarrow & E_0'(\mathbb{Q}_p^{\mathrm{un}})/\psi E_0(\mathbb{Q}_p^{\mathrm{un}}) \\
\downarrow & & \downarrow & & \downarrow \\
E(\mathbb{Q}_p^{\mathrm{un}}) & \longrightarrow & E'(\mathbb{Q}_p^{\mathrm{un}}) & \longrightarrow & E'(\mathbb{Q}_p^{\mathrm{un}})/\psi E(\mathbb{Q}_p^{\mathrm{un}}) \\
\downarrow & & \downarrow & & \downarrow \\
\mathbb{Z}/3n\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} & \longrightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & 0 & \longrightarrow & 0
\end{array}$$

The second-to-last row comes from Tate's algorithm, which shows that if $p^n \,\|\, b$, then the reduction for E is type I_{3n}, while the reduction for E' is type I_n. Thus we have an isomorphism $E_0'(\mathbb{Q}_p^{\mathrm{un}})/\psi E_0(\mathbb{Q}_p^{\mathrm{un}}) \cong E'(\mathbb{Q}_p^{\mathrm{un}})/\psi E(\mathbb{Q}_p^{\mathrm{un}})$. Since the former quotient is zero, so is the latter.

Thus, for the split primes $p \notin P$, the exactness of (7) implies that an element of $H^1(\mathbb{Q}, T)$ will map to the identity in $H^1(\mathbb{Q}_p^{\mathrm{un}}, E)_\psi$ if and only if it maps to the identity in $H^1(\mathbb{Q}_p^{\mathrm{un}}, T)$. Therefore, the kernel of $H^1(\mathbb{Q}, T) \to \bigoplus_{p\neq 2,3} H^1(\mathbb{Q}_p^{\mathrm{un}}, E)_\psi$ is precisely $H(P)$. ∎

If we wish a result for the standard Selmer group, we must put conditions on a to make things work correctly at $p = 2, 3$.

Proposition 4.2. *The kernel of* $H^1(\mathbb{Q}, T) \to \bigoplus_{p\neq 3} H^1(\mathbb{Q}_p^{\mathrm{un}}, E)_\psi$ *is* $H(P)$, *when* $a \equiv 2$ *or* $3 \pmod 4$.

Proof. If $a \equiv 2$ or $3 \pmod 4$, then 2 ramifies in K, so by the argument in the previous proof, $H^1(\mathbb{Q}, T) \to H^1(\mathbb{Q}_2^{\mathrm{un}}, T)$ is the zero map. ∎

Definition 4.3. Denote by $H(P)_r$ the subset of $H(P)$ represented by elements x such that $x \in \widetilde{K}_{\mathfrak{p}}^{*3}$ for a choice of $\mathfrak{p} \mid 3$.

Proposition 4.4. *When* $a \equiv 2$ *or* $3 \pmod 4$ *and* $3 \nmid a$, *the kernel of the map* $H^1(\mathbb{Q}, T) \to \bigoplus_p H^1(\mathbb{Q}_p^{\mathrm{un}}, E)_\psi$ *is* $H(P)_r$.

Proof. The condition that $3 \nmid a$ implies that 3 ramifies in K. As in the previous proposition, we have

$$H^1(\mathbb{Q}_3^{\mathrm{un}}, T) \cong \ker(Nm : \widetilde{K}_{\mathfrak{p}}^*/\widetilde{K}_{\mathfrak{p}}^{*3} \to \mathbb{Q}_3^{\mathrm{un}*}/\mathbb{Q}_3^{\mathrm{un}*3}). \tag{8}$$

Using Tate's algorithm [7], we find that E' has reduction of type $\mathrm{I}_{v_3(b)}$, and E has reduction of type $\mathrm{I}_{3v_3(b)}$. Therefore, $E'(\mathbb{Q}_p^{\mathrm{un}})/\psi E(\mathbb{Q}_p^{\mathrm{un}}) = 0$, and so the kernel of $H^1(\mathbb{Q}, T) \to H^1(\mathbb{Q}_3^{\mathrm{un}}, E)_\psi$ is the same as the kernel of $H^1(\mathbb{Q}, T) \to H^1(\mathbb{Q}_3^{\mathrm{un}}, T)$. Using the explicit description of $H^1(\mathbb{Q}_3^{\mathrm{un}}, T)$ and the previ-

ous propositions, we find that the kernel of $H^1(\mathbb{Q},T) \to \bigoplus_p H^1(\mathbb{Q}_p^{\mathrm{un}},E)_\psi$ is $H(P)_r$. ∎

Combining Proposition 4.4 with Lemma 3.1, we obtain Top's result that S^ψ maps into $H(P)$. Since we are interested in the dimension of S^ψ, we would like to know the dimension of $H(P)$. The following proposition gives a formula for the dimension of this vector space.

Denote the elements of the set P by $p_1,\dots,p_t$. By definition, these primes split in the field $K=\mathbb{Q}(\sqrt{-3a})$. Choose a set of primes of K, $\{\mathfrak{p}_1,\dots,\mathfrak{p}_t\}$, so that $\mathfrak{p}_i \mid p_i$.

PROPOSITION 4.5. *Let* $V=\{(i_1,\dots,i_t)\in(\mathbb{Z}/3\mathbb{Z})^t$ *be such that* $\mathfrak{p}_1^{i_1}\dots\mathfrak{p}_t^{i_t} \in Cl(K)^3\}$. *Then*

$$\dim_{\mathbb{F}_3} H(P) = r_3(-3a) + \dim_{\mathbb{F}_3} V + \dim_{\mathbb{F}_3} U/U^3,$$

where U *denotes the units in the ring of integers of* K.

Proof. Define the map Θ by

$$\Theta : H(P) \to (\mathbb{Z}/3\mathbb{Z})^t, \tag{9}$$

$$x \mapsto \bigoplus_{i=1}^{t} v_{\mathfrak{p}_i}(x) \pmod 3, \tag{10}$$

where $\mathfrak{p}_i \subseteq \mathcal{O}_K$ is one of the primes lying over p_i. Suppose $x \in \ker\Theta$. It is easy to see that the ideal of K generated by x must be a cube. Therefore the dimension of $\ker\Theta$ is $r_3(-3a)+\dim_{\mathbb{F}_3} U/U^3$.

The following lemma gives a calculation for $\operatorname{im}\Theta$. Lemma 3.3 then gives the desired equality. ∎

LEMMA 4.6. *The image of* Θ *is the vector space* V.

Proof. If $(i_1,\dots,i_t)\in\operatorname{im}\Theta$, then there is an $x\in H(P)$ with the ideal factorization $(x)=\mathfrak{p}_1^{i_1}(\overline{\mathfrak{p}}_1)^{k_1}\dots\mathfrak{p}_t^{i_t}(\overline{\mathfrak{p}}_t)^{k_t}\mathfrak{b}^3$ for some $\mathfrak{b}\subseteq\mathcal{O}_K$ where $k_j = 0$, 1, or 2 according as $i_j = 0$, 2, or 1. Since the p_i split, we have an equality of ideals $(p_1^{i_1}\dots p_t^{i_t}) = \mathfrak{p}_1^{i_1}(\overline{\mathfrak{p}}_1)^{i_1}\dots\mathfrak{p}_t^{i_t}(\overline{\mathfrak{p}}_t)^{i_t}$. Because $i_j+k_j\equiv 0 \pmod 3$, multiplying the ideal equality by the factorization for (x) gives $(p_i^{i_1}\dots p_t^{i_t}x) = \mathfrak{p}_1^{2i_1}\dots\mathfrak{p}_t^{2i_t}\mathfrak{a}^3$ for a different ideal $\mathfrak{a}$. Squaring both sides gives $(y)=\mathfrak{p}_1^{i_1}\dots\mathfrak{p}_t^{i_t}\mathfrak{c}^3$ for still another ideal $\mathfrak{c}$, where $y=p_1^{2i_1}\dots p_t^{2i_t}x^2$. This implies that $\mathfrak{p}_1^{i_1}\dots\mathfrak{p}_t^{i_t} \sim (\mathfrak{c}^{-1})^3$ in $Cl(K)$, or in other words $(i_1,\dots,i_t)\in V$.

On the other hand, if $(i_1,\dots,i_t)\in V$, then there is a $y\in K$ with the property that $(y)=\mathfrak{p}_1^{i_1}\dots\mathfrak{p}_t^{i_t}\mathfrak{b}^3$. Multiplying by the ideal $(p_1^{i_1}\dots p_t^{i_t}) = \mathfrak{p}_1^{i_1}(\overline{\mathfrak{p}}_1)^{i_1}\dots\mathfrak{p}_t^{i_t}(\overline{\mathfrak{p}}_t)^{i_t}$ and squaring yields $(x)\mathfrak{p}_1^{i_1}(\overline{\mathfrak{p}}_1)^{2i_1}\dots\mathfrak{p}_t^{i_t}(\overline{\mathfrak{p}}_t)^{2i_t}\mathfrak{a}^3$ for some ideal $\mathfrak{a}$, where $x=p_1^{2i_1}\dots p_t^{2i_t}y^2$. The element x satisfies the conditions to be in $H(P)$, and $\Theta(x)=(i_1,\dots,i_t)$. ∎

REMARK 4.7. Since the dimension of V is clearly at most t, Proposition 4.5 implies Lemma 3 of [8], in which Top gives an inequality for the dimension of $H(P)$.

REMARK 4.8. *A priori* to determine if the vector $(i_1, \ldots, i_t)$ is in the image of Θ, one must search for any $x \in K^*$ with the proper ideal factorization. The factorization specifies only what must happen at the primes lying over $p_1, \ldots, p_t$. Thus, the vector will be in the image if any one of the infinitely many allowed prime factorization gives a principal ideal. Lemma 4.6 replaces this infinite search with the test of a single ideal $\mathfrak{p}_1^{i_1} \ldots \mathfrak{p}_t^{i_t}$.

5. The last kernel of the sequence. Let $E : y^2 = x^3 + a(x-b)^2$ be the usual elliptic curve without congruence conditions on a or b. In the fundamental exact sequence with which we work, the third group is the kernel of the map

$$\bigoplus_p H^1(\mathbb{Q}_p, E)_\psi \to \bigoplus_p H^1(\mathbb{Q}_p^{\mathrm{un}}, E)_\psi. \tag{11}$$

We analyze this kernel by first considering the kernel of a single factor of this map.

Let $G = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$, and $I = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p^{\mathrm{un}})$. By the inflation-restriction sequence,

$$0 \to H^1(G/I, E(\mathbb{Q}_p^{\mathrm{un}})) \to H^1(\mathbb{Q}_p, E) \to H^1(\mathbb{Q}_p^{\mathrm{un}}, E)^{G/I} \to \ldots \tag{12}$$

Furthermore, Milne shows in Proposition I.3.8 of [3] that

$$H^1(G/I, E(\mathbb{Q}_p^{\mathrm{un}})) \cong H^1(\widehat{\mathbb{Z}}, \pi_0(\overline{E})), \tag{13}$$

where $\pi_0(\overline{E}) = E(\mathbb{Q}_p^{\mathrm{un}})/E_0(\mathbb{Q}_p^{\mathrm{un}})$, and $\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{un}}/\mathbb{Q}_p)$ is canonically identified with $\widehat{\mathbb{Z}}$. Taking ψ-kernels of all the cohomology groups and putting together the factors for each p, we find that $H(P)$ maps into $\bigoplus_p H^1(\widehat{\mathbb{Z}}, \pi_0(\overline{E}))_\psi$ in our exact sequence.

PROPOSITION 5.1. *The kernel of*

$$\bigoplus_{p \neq 2,3} H^1(\mathbb{Q}_p, E)_\psi \to \bigoplus_{p \neq 2,3} H^1(\mathbb{Q}_p^{\mathrm{un}}, E)_\psi$$

is $\bigoplus_{p \in P'} H^1(\widehat{\mathbb{Z}}, \pi_0(\overline{E}))_\psi \cong (\mathbb{Z}/3\mathbb{Z})^{\#P'}$ *where* P' *is the set of primes* $\left\{p \geq 5 \text{ such that } p \mid b \text{ and } \left(\frac{a}{p}\right) = 1\right\}$. *Moreover, if* $a \equiv 2$ *or* $11 \pmod{12}$, *then this is also the kernel of* $\bigoplus_p H^1(\mathbb{Q}_p, E)_\psi \to \bigoplus_p H^1(\mathbb{Q}_p^{\mathrm{un}}, E)_\psi$.

Proof. Top [8] gives the possible reduction types of E and E' for $p \geq 5$ to be I_0, II, I_n^*, and I_n. Using Tate's algorithm [7] we see that with $a \equiv 2$ or $3 \pmod 4$, the possible reduction types at $p = 2$ are II and I_n^*. We can

also calculate that E has reduction of type $\mathrm{I}_{3v_3(b)}$ at $p=3$, whenever $a \not\equiv 0 \pmod 3$.

First we deal with the cases $p \neq 3$. If the reduction is of type I_n^*, the Kodaira–Néron classification gives

$$\pi_0(\overline{E}) \cong \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \text{for } n \text{ even}, \\ \mathbb{Z}/4\mathbb{Z} & \text{for } n \text{ odd}. \end{cases} \tag{14}$$

Since $\psi \circ \psi'$ is multiplication by 3, $\ker \psi \subseteq \ker [3]$. Because $\pi_0(\overline{E})$ has no elements of order 3, its ψ-kernel is trivial. Therefore, $\psi : \pi_0(\overline{E}) \to \pi_0(\overline{E}')$ defines an isomorphism, which implies that $H^1(\widehat{\mathbb{Z}}, \pi_0(\overline{E}))_\psi$ is also 0.

If the reduction is of type I_0 or II, then $H^1(\widehat{\mathbb{Z}}, \pi_0(\overline{E}))_\psi = 0$, since $\pi_0(\overline{E}) = 0$.

Finally, if the reduction is of type I_n, then $\pi_0(\overline{E})$ is cyclic. The action of $\widehat{\mathbb{Z}}$ on $\pi_0(\overline{E})$ must preserve the structure, so $\widehat{\mathbb{Z}}$ must act as ± 1, as in Theorem 3.7 of [5]. Consider the short exact sequence

$$0 \to U \to \widehat{\mathbb{Z}} \to \{\pm 1\} \to 0, \tag{15}$$

where U is the kernel of the map sending an element of $\widehat{\mathbb{Z}}$ to its action. Then U acts trivially on $\pi_0(\overline{E})$. Using the inflation-restriction sequence, we obtain

$$\begin{aligned} 0 \to H^1(\{\pm 1\}, \pi_0(\overline{E})) &\to H^1(\widehat{\mathbb{Z}}, \pi_0(\overline{E})) \\ &\to H^1(U, \pi_0(\overline{E}))^{\{\pm 1\}} \to H^2(\{\pm 1\}, \pi_0(\overline{E})) \to \dots \end{aligned} \tag{16}$$

By counting, we find that both $H^1(\{\pm 1\}, \pi_0(\overline{E}))_\psi$ and $H^2(\{\pm 1\}, \pi_0(\overline{E}))_\psi$ are 0. Thus, by left exactness $H^1(\widehat{\mathbb{Z}}, \pi_0(\overline{E}))_\psi = H^1(U, \pi_0(\overline{E}))_\psi^{\{\pm 1\}}$.

Since U acts trivially and has a single topological generator, we find that

$$H^1(U, \pi_0(\overline{E}))^{\{\pm 1\}} \cong \mathrm{Hom}\,(U, \pi_0(\overline{E}))^{\{\pm 1\}} \cong \pi_0(\overline{E})^{\{\pm 1\}}. \tag{17}$$

Looking at ψ-kernels, we obtain

$$H^1(\widehat{\mathbb{Z}}, \pi_0(\overline{E}))_\psi \cong \pi_0(\overline{E})_\psi^{\{\pm 1\}}. \tag{18}$$

Top shows that, in the case of multiplicative reduction, $p \,|\, b$ implies that $\pi_0(\overline{E})_\psi \cong \mathbb{Z}/3\mathbb{Z}$ and $\pi_0(\overline{E})_\psi = 0$ otherwise. Because $\widehat{\mathbb{Z}}$ acts on $\pi_0(\overline{E})_\psi$ as it acts on $\pi_0(\overline{E})$, $H^1(\widehat{\mathbb{Z}}, \pi_0(\overline{E}))_\psi$ will give a copy of $\mathbb{Z}/3\mathbb{Z}$ when $\widehat{\mathbb{Z}}$ acts as $+1$, and the trivial group otherwise.

By IV.9.6 of [7], $\widehat{\mathbb{Z}}$ acts on $\pi_0(\overline{E})$ as $+1$ if E has split multiplicative reduction and as -1 if E has non-split multiplicative reduction. Since $p \,|\, b$, the reduced equation is $\widetilde{E} : \widetilde{y}^2 = \widetilde{x}^3 + a\widetilde{x}^2$. Thus, the reduction is split precisely when $\left(\frac{a}{p}\right) = 1$.

Finally, we consider the case $p = 3$. The condition that $a \equiv 2 \pmod 3$ implies that the splitting field of $T^2 - a$ over $\mathbb{F}_3$ strictly contains $\mathbb{F}_3$. Therefore, Tate's algorithm implies that $\widehat{\mathbb{Z}}$ acts as -1, and so $\pi_0(\overline{E})^{\{\pm 1\}}$ has order 1 or 2, which means that its ψ-kernel is trivial. ∎

6. A formula for S^ψ. By previous calculations, the generalized Selmer group fits into the exact sequence

$$0 \to S_g^\psi \to H(P) \to \bigoplus_{p\in P'} (\mathbb{Z}/3\mathbb{Z}) \to \dots, \tag{19}$$

where the sets P and P' are defined in Section 3. (Here the maps are those resulting from the identification of the cohomology groups with their images in $H(P)$ and $\bigoplus_{p\in P'}(\mathbb{Z}/3\mathbb{Z})$ as in Sections 4 and 5 respectively.) Therefore, S_g^ψ is isomorphic to the kernel of $H(P) \to \bigoplus_{p\in P'}(\mathbb{Z}/3\mathbb{Z})$. Moreover, if $a \equiv 2$ or $11 \pmod{12}$, then the standard Selmer group fits into the exact sequence

$$0 \to S^\psi \to H(P)_r \to \bigoplus_{p\in P'} (\mathbb{Z}/3\mathbb{Z}) \to \dots, \tag{20}$$

where $H(P)_r$ denotes the subset of $H(P)$ given in Proposition 4.4. Thus, $S^\psi \cong \ker(H(P)_r \to \bigoplus_{p\in P'}(\mathbb{Z}/3\mathbb{Z}))$.

Let us name the maps

$$\Phi : H(P) \to \bigoplus_{p\in P'} \mathbb{Z}/3\mathbb{Z}, \tag{21}$$

$$\widehat{\Phi} : H(P)_r \to \bigoplus_{p\in P'} \mathbb{Z}/3\mathbb{Z}. \tag{22}$$

THEOREM 6.1. *The dimension of the generalized Selmer group is*

$$\dim_{\mathbb{F}_3} S_g^\psi = r_3(-3a) + \dim_{\mathbb{F}_3} V + \dim_{\mathbb{F}_3} U_K/U_K^3 - \dim_{\mathbb{F}_3} \operatorname{im} \Phi,$$

where V is the vector space defined in Proposition 4.5.

Moreover, if $a \equiv 2$ or $11 \pmod{12}$, then the dimension of the Selmer group is

$$\dim_{\mathbb{F}_3} S^\psi = r_3(-3a) + \dim_{\mathbb{F}_3} V + \dim_{\mathbb{F}_3} U_K/U_K^3 - \dim_{\mathbb{F}_3} \operatorname{im} \widehat{\Phi} - \nu,$$

where ν is the codimension of $H(P)_r$ in $H(P)$.

Proof. Since $S_g^\psi = \ker \Phi$ and $S^\psi = \ker \widehat{\Phi}$, this follows immediately from Lemma 3.3 and Proposition 4.5. ∎

REMARK 6.2. We note that similar results for the Selmer group of ψ' follow, with the sets of primes P and P' trading roles. The only changes are in the proof of the analogue to Proposition 4.4, where we note that 3 is inert in $\mathbb{Q}(\sqrt{a})$ when $a \equiv 2 \pmod 3$, and in the proof of the analogue to Proposition 5.1, where we note that the possible reduction types for E' are the same as for E when $a \equiv 2 \pmod 3$.

7. Relating the Selmer groups of dual isogenies. In this section, we directly relate the dimension of the Selmer group S^ψ to the dimension of $S^{\psi'}$ using a formula of Cassels [1]. The formula is given by

$$\frac{\#S^{\psi}}{\#S^{\psi'}} = \frac{\#T(\mathbb{Q})}{\#T'(\mathbb{Q})} \cdot \frac{\alpha'}{\alpha} \prod_{p} \frac{c'_p}{c_p}, \tag{23}$$

where $\alpha = \int_{E(\mathbb{R})} \omega$ (resp. $\alpha' = \int_{E'(\mathbb{R})} \omega'$) for ω the canonical Néron differential of E (resp. ω' the canonical Néron differential of E'), c_p (resp. c'_p) is the number of connected components of the special fiber of the Néron model of E (resp. E'), and $T(\mathbb{Q})$ (resp. $T'(\mathbb{Q})$) is the group of points of the kernel of ψ (resp. ψ') which are defined over $\mathbb{Q}$. Since $T(\mathbb{Q})$ and $T'(\mathbb{Q})$ are trivial, to relate the dimensions of the Selmer groups we only need to find the reduction types and calculate the integrals of the canonical differentials. Throughout this section we consider only $a \equiv 2$ or $11 \pmod{12}$.

First we calculate c_3 and c'_3. By assumption 3 does not divide a, and therefore does not divide $4a + 27b$. Since

$$\Delta_E = -2^4 a^2 b^3 (4a + 27b), \tag{24}$$

we see that $v_3(\Delta_E) = 3v_3(b)$. Using Tate's algorithm for $p = 3$ we find that, since $3 \nmid b_2 = 4a$, the reduction is of type $\mathrm{I}_{3v_3(b)}$, and so $c_3 = 3v_3(b)$. On the other hand,

$$\Delta_{E'} = -2^4 3^{12} a^2 b (4a + 27b)^3. \tag{25}$$

Therefore the equation for E' is not minimal at $p = 3$. It becomes minimal at 3 after the change of variables

$$x = 3^2 x', \quad y = 3^3 y'. \tag{26}$$

The new discriminant is $2^4 a^2 b(4a+27b)^3$. An application of Tate's algorithm then yields that the reduction is of type $\mathrm{I}_{v_3(b)}$, and so $c'_3 = v_3(b)$.

Next we calculate c_p and c'_p for $p \neq 3$. For $p = 2$ Tate's Algorithm shows that $c_2 = c'_2$. For $p \geq 5$, Top [8] showed that the reduction is of type $\mathrm{I}_0, \mathrm{II},$ or I^*_n, and hence $c_p = c'_p$, unless either

$$p \nmid a \quad \text{and} \quad p \mid b \tag{27}$$

or

$$p \nmid a \quad \text{and} \quad p \mid (4a + 27b). \tag{28}$$

In the former case, $c_p = 3v_p(b)$ and $c'_p = v_p(b)$. In the latter case, $c_p = v_p(4a + 27b)$ and $c'_p = 3v_p(4a + 27b)$.

We now calculate the ratio α'/α. The explicit formula for the map ψ is given in [8] by

$$\begin{aligned} &\psi(x, y, z) \\ &= \left(9\left(2xy^2z + 2ab^2xz^3 - x^4 - \frac{2}{3}ax^3z\right), 27y(4abxz^2 - 8ab^2z^3 + x^3), x^3z\right). \end{aligned} \tag{29}$$

Therefore, using the quotient rule, we obtain $\psi^*\omega'' = \omega/3$, where ω is the invariant differential for the given Weierstrass equation for E and ω'' is the

invariant differential for the given Weierstrass equation for E'. Since the Weierstrass equation for E' is not minimal at $p = 3$, we use the change of variables (26), and calculate that

$$\omega'/3 = \omega''. \tag{30}$$

Therefore, we find that

$$\psi^*\omega' = \omega. \tag{31}$$

This relation and a little calculus gives

$$\alpha = \int_{E(\mathbb{R})} \omega = \int_{E(\mathbb{R})} \psi^*\omega' = \int_{\psi(E(\mathbb{R}))} \omega'. \tag{32}$$

The real loci of the curves E and E' are connected when b and $4a + 27b$ have the same sign, but the curves each have two connected components when b and $4a + 27b$ have opposite signs. It is easy to verify that the connected component of $E(\mathbb{R})$ containing infinity is a one-fold (resp. three-fold) cover of the connected component of $E'(\mathbb{R})$ containing infinity, when $a < 0$ (resp. $a > 0$). Likewise, if the second connected components are present, then the component not containing infinity of $E(\mathbb{R})$ is a one-fold (resp. three-fold) cover of the connected component of $E'(\mathbb{R})$ not containing infinity when $a < 0$ (resp. $a > 0$). Therefore,

$$\int_{\psi(E(\mathbb{R}))} \omega' = \begin{cases} \int_{E'(\mathbb{R})} \omega' & \text{if } a < 0, \\ 3\int_{E'(\mathbb{R})} \omega' & \text{if } a > 0. \end{cases} \tag{33}$$

Combining these results yields

$$\alpha = \begin{cases} \alpha' & \text{if } a < 0, \\ 3\alpha' & \text{if } a > 0. \end{cases} \tag{34}$$

The relationship (23) then gives us the following formula.

PROPOSITION 7.1. *The dimensions over* $\mathbb{F}_3$ *of the Selmer groups* S^ψ *and* $S^{\psi'}$ *are subject to the relation*

$$\dim_{\mathbb{F}_3} S^\psi - \dim_{\mathbb{F}_3} S^{\psi'} = A - B - \delta - \varepsilon,$$

where $A = \#\{p \mid p \geq 5,\ p \nmid a \text{ and } p \mid (4a + 27b)\}$, $B = \#\{p \mid p \geq 5,\ p \nmid a \text{ and } p \mid b\}$,

$$\delta = \begin{cases} 0 & \text{if } 3 \nmid b, \\ 1 & \text{if } 3 \mid b, \end{cases} \quad \text{and} \quad \varepsilon = \begin{cases} 0 & \text{if } a < 0, \\ 1 & \text{if } a > 0. \end{cases}$$

We can compare this to the results obtained by subtracting the dimensions of the Selmer groups obtained in the previous analysis. Using the formulas for the exact dimensions of the Selmer groups yields

$$\begin{aligned} &\dim_{\mathbb{F}_3} S^\psi - \dim_{\mathbb{F}_3} S^{\psi'} \\ &= r_3(-3a) - r_3(a) + \dim_{\mathbb{F}_3} V - \dim_{\mathbb{F}_3} V' - \dim_{\mathbb{F}_3} \widehat{\Phi} + \dim_{\mathbb{F}_3} \widehat{\Phi}' + \beta + \nu - \nu'. \end{aligned} \tag{35}$$

Here

$$\beta = \begin{cases} 1 & \text{if } a < 0, \\ -1 & \text{if } a > 0. \end{cases} \tag{36}$$

Note that Scholz's theorem implies that

$$r_3(-3a) - r_3(a) = \begin{cases} 0 \text{ or } -1 & \text{if } a < 0, \\ 0 \text{ or } 1 & \text{if } a > 0. \end{cases} \tag{37}$$

Also recall that V and Φ' are vector spaces of dimension at most

$$C = \#\left\{ p \geq 5 \;\middle|\; p \,|\, (4a + 27b) \text{ and } \left(\frac{-3a}{p}\right) = 1 \right\}, \tag{38}$$

and that V' and Φ are vector spaces of dimension at most

$$D = \#\left\{ p \geq 5 \;\middle|\; p \,|\, b \text{ and } \left(\frac{a}{p}\right) = 1 \right\}. \tag{39}$$

We note that, heuristically speaking, C is roughly $A/2$ and D is roughly $B/2$. Therefore, the differences obtained via the two methods are consistent. The difference obtained by utilizing the theorem of Cassels is more concrete and much easier to compute. However, appealing to this process only allows the calculation of the difference of the dimensions of the Selmer groups and not the sum. Finding an upper bound for the rank of the elliptic curves requires knowing the sum of the dimensions of the Selmer groups. Therefore, the lengthier analysis provides information not available through the duality theorem.

References

[1] J. W. S. Cassels, *On the conjectures of Birch and Swinnerton-Dyer*, J. Reine Angew. Math. 217 (1965), 180–199.

[2] M. DeLong, *Relating elliptic curves to three ranks of quadratic number fields*, PhD thesis, University of Michigan, 1998.

[3] J. S. Milne, *Arithmetic Duality Theorems*, Perspect. Math., Academic Press, Orlando, 1986.

[4] P. Satgé, *Groupes de Selmer et corps cubiques*, J. Number Theory 23 (1986), 294–317.

[5] E. F. Schaefer, *Class groups and Selmer groups*, ibid. 56 (1996), 79–114.

[6] J. Silverman, *The Arithmetic of Elliptic Curves*, Springer, New York, 1992.

[7] —, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer, New York, 1994.

[8] J. Top, *Descent by 3-isogeny and 3-rank of quadratic fields*, in: Advances in Number Theory, Oxford Univ. Press, 1993, 303–317.

Department of Mathematics
Taylor University
236 W. Reade ave.
Upland, IN 46989, U.S.A.
E-mail: mtdelong@tayloru.edu

Received on 25.6.1999
and in revised form on 22.4.2002 (3638)