# A counterexample to a conjecture of Selmer

Tom Fisher

6 November 2002

**Abstract**

We present a counterexample to a conjecture cited by Cassels [CaI] and attributed to Selmer. The issues raised have been given new significance by the recent work of Heath-Brown [HB] and Swinnerton-Dyer [SwD] on the arithmetic of diagonal cubic surfaces.

## 1 Introduction

Let $E$ be an elliptic curve over a number field $k$, with complex multiplication by $\mathbf{Z}[\omega]$ where $\omega$ is a primitive cube root of unity. Let $K = k(\omega)$, so that $[K:k] = 1$ or $2$ according as $\omega \in k$ or $\omega \notin k$. In his work on cubic surfaces, Heath-Brown [HB] makes implicit use of

**Theorem 1.1** *If $[K:k] = 2$ and the Tate-Shafarevich group $Ш(E/k)$ is finite, then the order of $Ш(E/K)[\sqrt{-3}]$ is a perfect square.*

We explain how this result follows from the work of Cassels [CaIV], and give an example to show that the condition $[K:k]=2$ is necessary.

For the application to cubic surfaces, we only need a special case of the theorem, namely that $Ш(E/K)[\sqrt{-3}]$ cannot have order 3. This result, still conditional on the finiteness of the Tate-Shafarevich group, has already appeared in [BF] and [SwD]. In fact Swinnerton-Dyer [SwD] vastly generalises Heath-Brown's results. In the case $[K:k]=2$ he proves the Hasse principle for diagonal cubic 3-folds over $k$, conditional only on the finiteness of the Tate-Shafarevich group for elliptic curves over $k$. The condition $[K:k]=2$ is unnatural, and conjecturally should not appear. However, the counterexample presented in this article suggests that, if we are to follow the methods of Heath-Brown and Swinnerton-Dyer, then this condition on $k$ is unavoidable.

In §2 we recall how it is possible to pass between the fields $k$ and $K$. Then in §3 we give a modern treatment of the descent by 3-isogeny studied by Selmer [S1] and Cassels [CaI]. In §§4,5 we recall how the conjectures of Selmer may be deduced from properties of the Cassels-Tate pairing. This culminates in a proof of Theorem 1.1. Finally in §6 we present our new example.

# 2 Decomposition into Galois eigenspaces

Let $E$ be an elliptic curve over $k$ with complex multiplication by $\mathbf{Z}[\omega]$. The isogeny $[\sqrt{-3}] : E \to E$ is defined over $K = k(\omega)$. But the kernel $E[\sqrt{-3}]$ is defined over $k$. It follows that there is a 3-isogeny $\phi : E \to \widetilde{E}$ defined over $k$ with $E[\sqrt{-3}] = E[\phi]$. Here $\widetilde{E}$ is a second elliptic curve defined over $k$, which we immediately recognise as the $-3$-twist of $E$. The dual isogeny $\widehat{\phi} : \widetilde{E} \to E$ satisfies $\phi \circ \widehat{\phi} = [3]$ and $\widehat{\phi} \circ \phi = [3]$. Our notation for the Selmer groups and Tate-Shafarevich groups follows [Sil, Chapter X].

**Lemma 2.1** *If* $[K : k] = 2$ *then the exact sequence*

$$0 \longrightarrow E(K)/\sqrt{-3}E(K) \longrightarrow S^{(\sqrt{-3})}(E/K) \longrightarrow \text{Ш}(E/K)[\sqrt{-3}] \longrightarrow 0 \qquad (1)$$

*is the direct sum of the exact sequences*

$$0 \longrightarrow \widetilde{E}(k)/\phi E(k) \longrightarrow S^{(\phi)}(E/k) \longrightarrow \text{Ш}(E/k)[\phi] \longrightarrow 0 \qquad (2)$$

*and*

$$0 \longrightarrow E(k)/\widehat{\phi}\widetilde{E}(k) \longrightarrow S^{(\widehat{\phi})}(\widetilde{E}/k) \longrightarrow \text{Ш}(\widetilde{E}/k)[\widehat{\phi}] \longrightarrow 0. \qquad (3)$$

*Proof.* Since arguments of this type have already appeared in [BF], [N], [SwD] and presumably countless other places in the literature, we will not dwell on the proof. Suffice to say that we decompose (1) into eigenspaces for the action of $\mathrm{Gal}(K/k)$, and then use the inflation-restriction exact sequence to identify these eigenspaces as (2) and (3). The observation that $[K : k] = 2$ is prime to $\deg \phi = 3$ is crucial throughout the proof. □

**Remark 2.2** Each term of the exact sequence (1) is a $\mathbf{Z}/3\mathbf{Z}$-vector space with an action of $\mathrm{Gal}(K/k)$. So each term is a direct sum of the Galois modules $\mathbf{Z}/3\mathbf{Z}$ and $\mu_3$. If we replace $E$ by $\widetilde{E}$ in (1) then we obtain the same exact sequence of abelian groups, but as Galois modules the summands $\mathbf{Z}/3\mathbf{Z}$ and $\mu_3$ are interchanged.

# 3 Computation of Selmer groups

Let $k$ be a number field. Let $T[a_0, a_1, a_2]$ be the diagonal plane cubic

$$a_0 x_0^3 + a_1 x_1^3 + a_2 x_2^3 = 0 \tag{4}$$

where $a_0, a_1, a_2 \in k^*/k^{*3}$. Let $E_A$ be the elliptic curve $T[A, 1, 1]$ with identity element $0 = (0 : 1 : -1)$. It is well known [St] that $E_A$ has Weierstrass equation $y^2 = x^3 - 432A^2$. An alternative proof of the following lemma may be found in [CaL, §18].

**Lemma 3.1** *The diagonal plane cubic $T[a_0, a_1, a_2]$ is a smooth curve of genus 1 with Jacobian $E_A$ where $A = a_0 a_1 a_2$.*

*Proof.* There is an isomorphism $T[a_0, a_1, a_2] \simeq E_A$ defined over $k(\sqrt[3]{\alpha})$ where $\alpha = a_1 a_2^2$. It is given by

$$\psi : (x_0 : x_1 : x_2) \mapsto (a_2 x_0 : \alpha^{2/3} x_1 : \alpha^{1/3} a_2 x_2).$$

The cocycle $\sigma(\psi)\psi^{-1}$ takes values in the subgroup $\mu_3 \subset \mathrm{Aut}(E_A)$ generated by $x_i \mapsto \omega^i x_i$. But since $\mu_3$ acts on $E_A$ without fixed points, this action belongs to the translation subgroup of $\mathrm{Aut}(E_A)$. It follows that $T[a_0, a_1, a_2]$ is a torsor under $E_A$ and that $E_A$ is the Jacobian of $T[a_0, a_1, a_2]$. $\square$

Temporarily working over $K = k(\omega)$ we note that $E_A$ has complex multiplication by $\mathbf{Z}[\omega]$ where $\omega : (x_0 : x_1 : x_2) \mapsto (\omega x_0 : x_1 : x_2)$ and that $E_A[1 - \omega] = E_A[\sqrt{-3}]$ is generated by $(0 : \omega : -\omega^2)$. So as in §2 there is a map $\phi$ which gives an exact sequence of Galois modules

$$0 \longrightarrow \mu_3 \longrightarrow E_A \xrightarrow{\phi} \widetilde{E}_A \longrightarrow 0$$

where $\widetilde{E}_A$ is the $-3$-twist of $E_A$. Taking Galois cohomology we obtain an exact sequence

$$0 \longrightarrow \widetilde{E}_A(k)/\phi E_A(k) \xrightarrow{\delta} k^*/k^{*3} \longrightarrow H^1(k, E_A)[\phi] \longrightarrow 0. \tag{5}$$

The group $H^1(k, E_A)$ parametrises the torsors under $E_A$. We write $C_{A,\alpha}$ for the torsor under $E_A$ described by $\alpha \in k^*/k^{*3}$. The proof of Lemma 3.1 shows that

$$T[a_0, a_1, a_2] \simeq C_{A,\alpha} \qquad \text{for } A = \prod a_\nu \text{ and } \alpha = \prod a_\nu^\nu \tag{6}$$

where the products are over $\nu \in \mathbf{Z}/3\mathbf{Z}$. Since $T[a_0,a_1,a_2] \simeq T[a_1,a_2,a_0]$ it is clear that $A \in \operatorname{im}\delta$. If $\widetilde{E}_A$ has Weierstrass equation $Y^2Z = -4AX^3 + Z^3$ then the 3-covering map $T[a_0,a_1,a_2] \to \widetilde{E}_A$ is given by

$$(x_0 : x_1 : x_2) \mapsto (x_0x_1x_2 : a_1x_1^3 - a_2x_2^3 : a_0x_0^3).$$

The Selmer group attached to $\phi$ is

$$S^{(\phi)}(E_A/k) = \{\, \alpha \in k^*/k^{*3} \mid C_{A,\alpha}(k_{\mathfrak{p}}) \neq \emptyset \text{ for all primes } \mathfrak{p} \,\}.$$

Since $\deg\phi = 3$ is odd we have ignored the infinite places. We write $\delta_{\mathfrak{p}}$ for the local connecting map obtained when we apply (5) to the local field $k_{\mathfrak{p}}$. Then the condition $C_{A,\alpha}(k_{\mathfrak{p}}) \neq \emptyset$ may also be written $\alpha \in \operatorname{im}\delta_{\mathfrak{p}}$. Using (6) to give equations for $C_{A,\alpha}$ it is easy to prove

**Lemma 3.2** *Let $k$ be a number field, and let $\mathfrak{p}$ be a prime not dividing 3. Let $\mathfrak{o}_{\mathfrak{p}}$ denote the ring of integers of $k_{\mathfrak{p}}$. Then*

$$\operatorname{im}\delta_{\mathfrak{p}} = \begin{cases} \mathfrak{o}_{\mathfrak{p}}^*/\mathfrak{o}_{\mathfrak{p}}^{*3} & \text{if } \operatorname{ord}_{\mathfrak{p}}(A) \equiv 0 \pmod 3 \\ \langle A \rangle & \text{if } \operatorname{ord}_{\mathfrak{p}}(A) \not\equiv 0 \pmod 3. \end{cases}$$

If $\mathfrak{p}$ divides 3 the situation is more complicated, although we still have

$$\operatorname{im}\delta_{\mathfrak{p}} \subset \mathfrak{o}_{\mathfrak{p}}^*/\mathfrak{o}_{\mathfrak{p}}^{*3} \quad \text{if } \operatorname{ord}_{\mathfrak{p}}(A) \equiv 0 \pmod 3. \tag{7}$$

If $\omega \in k_{\mathfrak{p}}$ then Tate local duality tells us that $\operatorname{im}\delta_{\mathfrak{p}}$ is a maximal isotropic subspace with respect to the Hilbert norm residue symbol

$$k_{\mathfrak{p}}^*/k_{\mathfrak{p}}^{*3} \times k_{\mathfrak{p}}^*/k_{\mathfrak{p}}^{*3} \to \mu_3. \tag{8}$$

The next lemma treats the case $k = \mathbf{Q}(\omega)$. This field has ring of integers $\mathbf{Z}[\omega]$ and class number 1. The unique prime above 3 is $\pi = \omega - \omega^2$.

**Lemma 3.3** *Let $A \in \mathbf{Z}[\omega]$ be non-zero and cube-free. Then*

$$\operatorname{im}\delta_{\pi} = \begin{cases} \langle\, A, (1-A)/(1+A) \,\rangle & \text{if } \operatorname{ord}_{\pi}(A) \neq 0 \\ \langle\, A, 1-\pi^3 \,\rangle & \text{if } \operatorname{ord}_{\pi}(A) = 0 \text{ and } A^2 \not\equiv \pm 1 \ (\pi^3) \\ \langle\, \omega(1+3a), 1-\pi^3 \,\rangle & \text{if } A = \pm(1+a\pi^3) \text{ for some } a \in \mathbf{Z}[\omega]. \end{cases}$$

*Proof.* We recall [CF, Exercise 2.13] that $k_\pi^*/k_\pi^{*3}$ has basis $\pi, \omega, 1-\pi^2, 1-\pi^3$ and that these elements define a filtration compatible with the pairing (8). By Tate local duality it follows that $\operatorname{im}\delta_\pi$ has order 9. So to prove the lemma it suffices to prove the inclusions $\supset$. As always $A \in \operatorname{im}\delta_\pi$, whereas (7) and Tate local duality tell us that $1-\pi^3 \in \operatorname{im}\delta_\pi$. There is at most one more element to find.
(i) Suppose $\operatorname{ord}_\pi(A) \neq 0$. If $\alpha$ satisfies $\alpha - \alpha^{-1} = A$ then $T[A, \alpha, \alpha^{-1}]$ is soluble. Splitting into the cases $\operatorname{ord}_\pi(A) = 1$ or $2$ we find

$$4A/(1-A^2) \equiv A \pmod{\pi^4}.$$

So $\alpha = (1-A)/(1+A)$ provides a solution mod $\pi^4$.
(ii) Suppose $A = 1 + a\pi^3$ for some $a \in \mathbf{Z}[\omega]$. If $\alpha$ satisfies $A + \alpha + \alpha^{-1} = 0$ then $T[A, \alpha, \alpha^{-1}]$ is soluble. In view of the identity

$$(1+\pi^3 a) + \omega(1+3a) + \omega^2(1-3a) = 0$$

we see that $\alpha = \omega(1+3a)$ provides a solution mod $\pi^4$. □

# 4 Selmer's conjectures

In this section we take $k = \mathbf{Q}$, so that $K = \mathbf{Q}(\omega)$. We consider the elliptic curves $E_A$ and $\widetilde{E}_A$ over $\mathbf{Q}$ where $A \geq 2$ is a cube-free integer.

**Lemma 4.1** *If $A \geq 3$ then the torsion subgroups are*

$$E_A(\mathbf{Q})_{\text{tors}} = 0 \quad \text{and} \quad \widetilde{E}_A(\mathbf{Q})_{\text{tors}} \simeq \mathbf{Z}/3\mathbf{Z}.$$

*Proof.* See [St, §6] or [K, Chapter 1, Problem 7]. □

Lemma 2.1 gives a decomposition into $\operatorname{Gal}(K/\mathbf{Q})$-eigenspaces

$$S^{(\sqrt{-3})}(E_A/K) \simeq S^{(\phi)}(E_A/\mathbf{Q}) \oplus S^{(\widehat{\phi})}(\widetilde{E}_A/\mathbf{Q}). \tag{9}$$

The following examples were found by Selmer [S1], [S2].

**Example 4.2** Let $A = 60$. Lemmas 3.2 and 3.3 tell us that

$$S^{(\sqrt{-3})}(E_{60}/K) \simeq \langle 2, 3, 5 \rangle \subset K^*/K^{*3}.$$

Then (9) gives $S^{(\phi)}(E_{60}/\mathbf{Q}) \simeq (\mathbf{Z}/3\mathbf{Z})^3$ and $S^{(\widehat{\phi})}(\widetilde{E}_{60}/\mathbf{Q}) = 0$. But a 2-descent [CaL, §15], [Cr] shows that $E_{60}(\mathbf{Q})$ has rank 0. We deduce

$$Ш(E_{60}/\mathbf{Q})[3] \simeq (\mathbf{Z}/3\mathbf{Z})^2.$$

**Example 4.3** Let $A = 473$. Lemmas 3.2 and 3.3 tell us that

$$S^{(\sqrt{-3})}(E_{473}/K) \simeq \langle 11, 1-6\omega, 1-6\omega^2 \rangle \subset K^*/K^{*3}.$$

Then (9) gives $S^{(\phi)}(E_{473}/\mathbf{Q}) \simeq (\mathbf{Z}/3\mathbf{Z})^2$ and $S^{(\widehat{\phi})}(\widetilde{E}_{473}/\mathbf{Q}) \simeq \mathbf{Z}/3\mathbf{Z}$. But a 2-descent [S2], [Cr] shows that $E_{473}(\mathbf{Q})$ has rank 0. We deduce

$$Ш(E_{473}/\mathbf{Q})[\phi] \simeq \mathbf{Z}/3\mathbf{Z} \quad \text{and} \quad Ш(\widetilde{E}_{473}/\mathbf{Q})[\widehat{\phi}] \simeq \mathbf{Z}/3\mathbf{Z}.$$

**Remark 4.4** According to the formulae and tables of Stephens [St], the above examples have $L(E_A, 1) \neq 0$. So the claims $\operatorname{rank} E_A(\mathbf{Q}) = 0$ could equally be deduced from the work of Coates-Wiles [CW].

Example 4.2 tells us that each of the curves

$$\begin{array}{rrcl} T[3,4,5]: & 3x_0^3 + 4x_1^3 + 5x_2^3 & = & 0 \\ T[1,3,20]: & x_0^3 + 3x_1^3 + 20x_2^3 & = & 0 \\ T[1,4,15]: & x_0^3 + 4x_1^3 + 15x_2^3 & = & 0 \\ T[1,5,12]: & x_0^3 + 5x_1^3 + 12x_2^3 & = & 0 \end{array} \tag{10}$$

is a counterexample to the Hasse Principle for smooth curves of genus 1 defined over $\mathbf{Q}$. Selmer proves this without the need for a 2-descent. Instead he shows that the equations (10) are insoluble over $\mathbf{Q}$ by writing them as norm equations. As Cassels explains [CaI, §11] this is equivalent to performing a second descent, *i.e.* computing the middle group in

$$\widetilde{E}_A(\mathbf{Q})/\phi E_A(\mathbf{Q}) \subset \widehat{\phi} S^{(3)}(\widetilde{E}_A/\mathbf{Q}) \subset S^{(\phi)}(E_A/\mathbf{Q}). \tag{11}$$

In fact Selmer's calculations suffice to show that $Ш(E_{60}/\mathbf{Q})(3) \simeq (\mathbf{Z}/3\mathbf{Z})^2$. In other words $Ш(E_{60}/\mathbf{Q})$ does not contain an element of order 9. More recent work of Rubin [M] improves this to $Ш(E_{60}/\mathbf{Q}) \simeq (\mathbf{Z}/3\mathbf{Z})^2$.

Selmer also gave practical methods for computing the two right hand groups in

$$E_A(\mathbf{Q})/\widehat{\phi}\widetilde{E}_A(\mathbf{Q}) \subset \phi S^{(3)}(E_A/\mathbf{Q}) \subset S^{(\widehat{\phi})}(\widetilde{E}_A/\mathbf{Q}). \tag{12}$$

Following Stephens [St] we write $g_1+1$, $\lambda_1'+1$, $\lambda_1+1$ for the dimensions of the $\mathbf{Z}/3\mathbf{Z}$-vector spaces (11) and $g_2$, $\lambda_2'$, $\lambda_2$ for the dimensions of the $\mathbf{Z}/3\mathbf{Z}$-vector spaces (12). Trivially we have $0 \le g_1 \le \lambda_1' \le \lambda_1$, $0 \le g_2 \le \lambda_2' \le \lambda_2$ and $\operatorname{rank} E_A(\mathbf{Q}) = g_1 + g_2$. Based on a large amount of numerical evidence, Selmer [S3] made the following

**Conjecture 4.5** *Let $A \ge 2$ be a cube-free integer. Let $E_A$ be the elliptic curve $x^3+y^3=Az^3$ defined over $\mathbf{Q}$. Then*
**Weak form.** *The second descent excludes an even number of generators, i.e. $\lambda_1 \equiv \lambda_1' \pmod 2$ and $\lambda_2 \equiv \lambda_2' \pmod 2$.*
**Strong form.** *The number of generators of infinite order for $E_A(\mathbf{Q})$ is an even number less than what is indicated by the first descent, i.e. $\lambda_1+\lambda_2 \equiv g_1+g_2 \pmod 2$.*

For $A = 473$, Selmer found $\lambda_1 = \lambda_1' = \lambda_2 = \lambda_2' = 1$ yet $g_1 = g_2 = 0$. He was thus aware of the need to combine the contributions from $\phi$ and $\widehat{\phi}$ in the strong form of his conjecture.

**Remark 4.6** In Heath-Brown's notation [HB] we have

$$r(A) = \operatorname{rank} E_A(\mathbf{Q}) = g_1 + g_2 \quad \text{and} \quad s(A) = \lambda_1 + \lambda_2.$$

By (9) the order of $S^{(\sqrt{-3})}(E_A/K)$ is $3^{s(A)+1}$ and in fact it is this relation that Heath-Brown uses to define $s(A)$. Naturally he writes the strong form of Selmer's conjecture as $r(A) \equiv s(A) \pmod 2$.

Now let $k$ be any number field. Conjecture 4.5 is equivalent to the case $k = \mathbf{Q}$ of the following

**Conjecture 4.7** *Let $A \in k^*$ not a perfect cube. Let $E_A$ be the elliptic curve $x^3+y^3=Az^3$ defined over $k$. Then*
**Weak form.** *The subgroup $\widehat{\phi}(\text{Ш}(\widetilde{E}_A/k)[3]) \subset \text{Ш}(E_A/k)[\phi]$ has index a perfect square. The same is true for $\phi(\text{Ш}(E_A/k)[3]) \subset \text{Ш}(\widetilde{E}_A/k)[\widehat{\phi}]$.*
**Strong form.** *The order of $\text{Ш}(E_A/k)[\phi]$ multiplied by the order of $\text{Ш}(\widetilde{E}_A/k)[\widehat{\phi}]$ is a perfect square.*

In the next section we recall how Conjecture 4.7 follows from the work of Cassels, the strong form being conditional on the finiteness of $\text{Ш}(E_A/k)$.

# 5 The Cassels-Tate pairing

Let $E$ be an elliptic curve over a number field $k$. For $\phi : E \to E'$ an isogeny of elliptic curves over $k$ we shall write $\widehat{\phi} : E' \to E$ for the dual isogeny. Cassels [CaIV] defines an alternating bilinear pairing

$$\langle\ ,\ \rangle : Ш(E/k) \times Ш(E/k) \to \mathbf{Q}/\mathbf{Z} \tag{13}$$

with the following non-degeneracy property.

**Theorem 5.1** *Let $\phi : E \to E'$ be an isogeny of elliptic curves over $k$. Then $x \in Ш(E/k)$ belongs to the image of $\widehat{\phi} : Ш(E'/k) \to Ш(E/k)$ if and only if $\langle x, y\rangle = 0$ for all $y \in Ш(E/k)[\phi]$.*

*Proof.* This was proved by Cassels [CaIV] in the case $\phi = [m]$ for $m$ a rational integer. The general case follows by his methods and is explained in [F]. □

The pairing was later generalised to abelian varieties by Tate, and so is known as the Cassels-Tate pairing. The most striking applications in the case of elliptic curves come from the following easy lemma.

**Lemma 5.2** *If a finite abelian group admits a non-degenerate alternating bilinear pairing, then its order must be a perfect square.*

The weak form of Conjecture 4.7 is a special case of

**Corollary 5.3** *Let $\phi : E \to E'$ be an $m$-isogeny of elliptic curves over $k$. Then the subgroup $\widehat{\phi}(Ш(E'/k)[m]) \subset Ш(E/k)[\phi]$ has index a perfect square.*

*Proof.* According to Theorem 5.1 the pairing (13) restricted to $Ш(E/k)[\phi]$ has kernel $\widehat{\phi}(Ш(E'/k)[m])$. We are done by Lemma 5.2. □

Let us assume that $Ш(E/k)$ is finite. So by Theorem 5.1 and Lemma 5.2 the order of $Ш(E/k)$ is a perfect square. If $\phi : E \to E'$ is an isogeny of elliptic curves over $k$ then the same conclusions will hold for $E'$. We define

$$\langle\ ,\ \rangle_\phi : Ш(E/k) \times Ш(E'/k) \to \mathbf{Q}/\mathbf{Z}\,; \quad (x, y) \mapsto \langle \phi x, y\rangle = \langle x, \widehat{\phi} y\rangle \tag{14}$$

where the equality on the right is [CaVIII, Theorem 1.2]. The strong form of Conjecture 4.7 is a special case of

**Corollary 5.4** *Let $\phi : E \to E'$ be an isogeny of elliptic curves over $k$. If $\text{Ш}(E/k)$ is finite then the order of $\text{Ш}(E/k)[\phi]$ multiplied by the order of $\text{Ш}(E'/k)[\widehat{\phi}]$ is a perfect square.*

*Proof.* According to Theorem 5.1 the left and right kernels of $\langle\ ,\ \rangle_\phi$ are $\text{Ш}(E/k)[\phi]$ and $\text{Ш}(E'/k)[\widehat{\phi}]$. We obtain a non-degenerate pairing

$$\text{Ш}(E/k)/\text{Ш}(E/k)[\phi] \times \text{Ш}(E'/k)/\text{Ш}(E'/k)[\widehat{\phi}] \to \mathbf{Q}/\mathbf{Z}.$$

We deduce that these quotients have the same order and are done since $\text{Ш}(E/k)$ and $\text{Ш}(E'/k)$ each have order a perfect square. □

Another well known consequence is

**Corollary 5.5** *Let $E$ be an elliptic curve over $k$ whose Tate-Shafarevich group is finite, and let $m$ be a rational integer. Then the order of $\text{Ш}(E/k)[m]$ is a perfect square.*

*Proof.* According to Theorem 5.1 the kernel of $\langle\ ,\ \rangle_m$ is $\text{Ш}(E/k)[m]$. We obtain a non-degenerate alternating pairing

$$\text{Ш}(E/k)/\text{Ш}(E/k)[m] \times \text{Ш}(E/k)/\text{Ш}(E/k)[m] \to \mathbf{Q}/\mathbf{Z}.$$

We apply Lemma 5.2 to this pairing and are done since $\text{Ш}(E/k)$ has order a perfect square. □

**Remark 5.6** We could equally deduce Corollary 5.4 from Corollaries 5.3 and 5.5.

*Proof of Theorem 1.1.* Let $E$ be an elliptic curve over $k$ with complex multiplication by $\mathbf{Z}[\omega]$ and suppose that $[K : k] = 2$. Lemma 2.1 tells us that

$$\text{Ш}(E/K)[\sqrt{-3}] \simeq \text{Ш}(E/k)[\phi] \oplus \text{Ш}(\widetilde{E}/k)[\widehat{\phi}].$$

Assuming $\text{Ш}(E/k)$ is finite, Corollary 5.4 shows that the group on the right has order a perfect square. So the group on the left has order a perfect square, and this is precisely the statement of Theorem 1.1. □

In the first of his celebrated series of papers, Cassels [CaI] defines a pairing $S^{(\sqrt{-3})}(E_A/K) \times S^{(\sqrt{-3})}(E_A/K) \to \mu_3$. It is of course a special case of the pairing (13). He uses it to prove the weak form of Conjecture 4.7 in the case $[K : k] = 1$. However in the introduction to the same paper he misquotes the strong form of Selmer's conjecture. The statement he gives is equivalent to

- If $[K:k]=1$ then the order of $Ш(E_A/K)[\sqrt{-3}]$ is a perfect square.

It is this statement to which we have found a counterexample. It is possible that Cassels was mislead by earlier work of Selmer at a time when he did not appreciate the need to combine the contributions from $\phi$ and $\widehat{\phi}$ in the strong form of his conjecture.

**Remark 5.7** It is tempting to try and prove Theorem 1.1 in the case $[K:k]=1$ by imitating the proof of Corollary 5.5. However the isogeny $[\sqrt{-3}]$ has dual $[-\sqrt{-3}]$ and this extra sign means that the pairing $\langle\ ,\ \rangle_{\sqrt{-3}}$ is symmetric rather than alternating. Lemma 5.2 does not apply.

# 6 A new example

In this section we take $K=\mathbf{Q}(\omega)$. Let $E_A$ be the elliptic curve $x^3+y^3=Az^3$. We aim to find $A\in K$ such that the order of $Ш(E_A/K)[\sqrt{-3}]$ is not a perfect square. As in Example 4.3 our method is to compare a 3-descent with a 2-descent. The form of the curves $E_A$ makes the 3-descent easy. We use the results of §3 to compute the Selmer group $S^{(\sqrt{-3})}(E_A/K)$. For the 2-descent we would like to use John Cremona's program `mwrank` [Cr]. But `mwrank` is written specifically for elliptic curves over $\mathbf{Q}$, whereas Theorem 1.1 tells us that there are no examples of the required form with $A^2\in\mathbf{Q}$. Fortunately we were able to use a program of Denis Simon [Si1], [Si2], written using `pari` [BBBCO], that extends Cremona's work on 2-descents to general number fields (in practice of degrees 1 to 5).

We consider all cube-free $A\in\mathbf{Z}[\omega]$ with $A^2\notin\mathbf{Q}$ and $\mathrm{Norm}(A)\le 150$. We ignore repeats of the form $\pm\sigma(A)$ for $\sigma\in\mathrm{Gal}(K/\mathbf{Q})$. In all 123 cases a calculation based on Lemmas 3.2 and 3.3 shows that $S^{(\sqrt{-3})}(E_A/K)$ is isomorphic to either $\mathbf{Z}/3\mathbf{Z}$ or $(\mathbf{Z}/3\mathbf{Z})^2$. In the 98 cases where $S^{(\sqrt{-3})}(E_A/K)\simeq\mathbf{Z}/3\mathbf{Z}$ it follows immediately that $\mathrm{rank}\,E_A(K)=0$. In the remaining 25 cases we run Simon's program. For 20 of these curves the program exhibits a point of infinite order. Since $E_A(K)$ has the structure of $\mathbf{Z}[\omega]$-module, we are able to deduce that $\mathrm{rank}\,E_A(K)=2$. The remaining 5 cases are

$$A=\pm(3+7\omega),\ \pm(9+\omega),\ \pm(12+5\omega),\ \pm(6+13\omega),\ \pm(13+7\omega)$$

and their Galois conjugates. In each case Simon's program reports that $\mathrm{rank}\,E_A(K)=0$. Reducing modulo some small primes we find $E_A(K)\simeq\mathbf{Z}/3\mathbf{Z}$.

Thus

$$Ш(E_A/K)[\sqrt{-3}] \simeq \mathbf{Z}/3\mathbf{Z}.$$

For the remainder of this article we restrict attention to the first of these examples, namely $A = 3 + 7\omega$, and give further details of the descent calculations involved. In particular we establish the counterexample of the title in a way that is independent of Simon's program.

We begin by checking the above computation of $S^{(\sqrt{-3})}(E_A/K)$ for $A = 3 + 7\omega$. Since $(A)$ is prime, Lemma 3.2 tells us that

$$S^{(\sqrt{-3})}(E_A/K) \subset \langle \omega, 3 + 7\omega \rangle. \tag{15}$$

We check the local conditions at the primes $(\pi)$ and $(A)$ above 3 and 37 respectively.

- Since $37 \equiv 1 \pmod 9$ we know that $\omega$ is a cube locally at $(A)$.
- Lemma 3.3 gives $\operatorname{im} \delta_\pi = \langle A, 1 - \pi^3 \rangle \subset K_\pi^*/K_\pi^{*3}$. Since $A = \omega - \pi^3$ it is clear that $\omega$ belongs to this subgroup.

It follows that equality holds in (15) as required.

Given the provisional nature of Simon's program we have taken the liberty of writing out the 2-descent for $A = 3+7\omega$ in the style of Cassels [CaL, p.72-73]. The curve $E_A$ has Weierstrass form

$$Y^2 = X^3 - 2^4 3^3 (3 + 7\omega)^2. \tag{16}$$

The 2-descent takes place over the field $L = K(\delta)$ where $\delta^3 = 4(3 + 7\omega)$. According to `pari` [BBBCO][1], $L$ has class number $h = 3$, and fundamental units

$$\begin{aligned} \eta_1 &= (-7 - 3\omega) + (-3 - 2\omega)\delta + (-2 + \omega)\delta^2/2 \\ \eta_2 &= (-7 - 3\omega) + (2 - \omega)\delta + (3 + 2\omega)\delta^2/2. \end{aligned}$$

Furthermore `pari` is able to certify these results, independent of any conjecture. We have chosen $\eta_1$ and $\eta_2$ to be $K$-conjugates. They have minimal polynomial

$$x^3 + (21 + 9\omega)x^2 + (102 - 165\omega)x - 1.$$

If $(X, Y) = (r/t^2, s/t^3)$ is a solution of (16), with fractions in lowest terms, then a common prime divisor of any two of

$$r - 3\delta^2 t^2, \quad r - 3\omega\delta^2 t^2, \quad r - 3\omega^2\delta^2 t^2$$

[1] These calculations were performed using Version 2.0.20 (beta)

must divide $2(1-\omega)(3+7\omega)$. Since $2,(1-\omega),(3+7\omega)$ ramify completely, $r-3\delta^2t^2$ must be a perfect ideal square. Since $h$ is odd it follows that $S^{(2)}(E/K)$ is a subgroup of $\langle -1,\eta_1,\eta_2\rangle \subset L^*/L^{*2}$. We claim that $S^{(2)}(E/K)$ is trivial. By considering norms from $L$ to $K$, it suffices to show that the equation

$$r-3\delta^2t^2=\eta\alpha^2 \quad \text{with } \eta=\eta_1,\eta_2 \text{ or } 1/(\eta_1\eta_2)$$

is insoluble for $r,t\in K$ and $\alpha\in L$. The action of $\mathrm{Gal}(L/K)$ shows that we need only consider the case $\eta=\eta_1$. Put $\alpha=u+v\delta+w\delta^2$. Equating coefficients of powers of $\delta$ we obtain

$$\begin{aligned} 0 &= (-3-2\omega)u^2+(-14-6\omega)uv+(-26-36\omega)v^2 \\ &\quad +(-52-72\omega)uw+(40-104\omega)vw+(-148\omega)w^2 \\ -3t^2 &= ((-2+\omega)/2)u^2+(-6-4\omega)uv+(-7-3\omega)v^2 \\ &\quad +(-14-6\omega)uw+(-52-72\omega)vw+(20-52\omega)w^2. \end{aligned}$$

On putting

$$\begin{aligned} u &= (-8+6\omega)e+(-6-34\omega)f+(-20+15\omega)g \\ v &= (-4-4\omega)e+(12+4\omega)f+(-10-11\omega)g \\ w &= (1-\omega)e+(1+4\omega)f+(2-2\omega)g \end{aligned}$$

in the first equation, it becomes

$$0=(3+7\omega)g^2-16ef.$$

Hence there are $m,n$ such that

$$e:f:g=m^2:(3+7\omega)n^2:4mn.$$

On substituting into the second equation, we get

$$\begin{aligned} -3t^2 &= 2(-1-4\omega)m^4+8(-4+3\omega)m^3n+4(21+12\omega)m^2n^2 \\ &\quad +8(4-3\omega)mn^3+2(-33-40\omega)n^4. \end{aligned}$$

But this is impossible in $K_2$. Hence $S^{(2)}(E_A/K)$ is trivial and $\operatorname{rank} E_A(K)=0$ as claimed.


# Acknowledgements

The author would like to thank Laura Basile, Alexei Skorobogatov and Sir Peter Swinnerton-Dyer for useful conversations.

# References


[BF] C.L. Basile and T.A. Fisher, Diagonal cubic equations in four variables with prime coefficients, *Rational points on algebraic varieties*, 1–12, Progr. Math., **199**, Birkhäuser, Basel, 2001.

[BBBCO] C. Batut, K. Belabas, D. Bernardi, H. Cohen and M. Olivier, `pari/gp`, a computer algebra package, `http://www.parigp-home.de`

[CaI] J.W.S. Cassels, Arithmetic on curves of genus 1, I. On a conjecture of Selmer, *J. Reine Angew. Math.* **202** (1959), 52–99.

[CaIV] J.W.S. Cassels, Arithmetic on curves of genus 1, IV. Proof of the Hauptvermutung, *J. Reine Angew. Math.* **211** (1962), 95–112.

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

[CaL] J.W.S. Cassels, *Lectures on elliptic curves*, LMSST **24**, Cambridge University Press, Cambridge, 1991.

[CF] J.W.S. Cassels and A. Fröhlich (Eds.), *Algebraic number theory*, Academic Press, London, 1967.

[CW] J. Coates and A. Wiles, On the conjecture of Birch and Swinnerton-Dyer. *Invent. Math.* **39** (1977), no. 3, 223–251.

[Cr] J.E. Cremona, `mwrank`, a program for performing 2-descent on elliptic curves over $\mathbf{Q}$,
`http://www.maths.nottingham.ac.uk/personal/jec/ftp/progs`

[F] T.A. Fisher, The Cassels-Tate pairing and the Platonic solids, to appear in *J. Number Theory.*

[HB] D.R. Heath-Brown, The solubility of diagonal cubic Diophantine equations, *Proc. London Math. Soc.* (3) **79** (1999), no. 2, 241–259.

[K] N. Koblitz, *Introduction to elliptic curves and modular forms*, GTM **97**. Springer-Verlag, New York, 1993.

[M] B. Mazur, On the passage from local to global in number theory. *Bull. Amer. Math. Soc.* **29** (1993), no. 1, 14–50.

[N] J. Nekovář, Class numbers of quadratic fields and Shimura's correspondence, *Math. Ann.* **287** (1990), no. 4, 577–594.

[S1] E.S. Selmer, The diophantine equation $ax^3 + by^3 + cz^3 = 0$, *Acta Math.* **85** (1951), 203–362.

[S2] E.S. Selmer, The diophantine equation $ax^3 + by^3 + cz^3 = 0$, completion of the tables, *Acta Math.* **92** (1954), 191–197.

[S3] E.S. Selmer, A conjecture concerning rational points on cubic curves, *Math. Scand.* **2** (1954), 49–54.

[Sil] J.H. Silverman, *The arithmetic of elliptic curves*, GTM **106**, Springer-Verlag, New York, 1986.

[Si1] D. Simon, Computing the rank of elliptic curves over number fields, *LMS J. Comput. Math.* **5** (2002), 7–17.

[Si2] D. Simon, `ell.gp`, a program for calculating the rank of elliptic curves over number fields, `http://www.math.unicaen.fr/~simon`

[St] 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.

[SwD] H.P.F. Swinnerton-Dyer, The solubility of diagonal cubic surfaces, *Ann. Sci. École Norm. Sup.* (4) **34** (2001), no. 6, 891–912.