A PARAMETRIZED SET OF EXPLICIT ELEMENTS OF $\text{Ш}(\mathbf{E}/\mathbb{Q})[\mathbf{3}]$

Steven R. Groen
Department of Mathematics, University of Warwick, Coventry, United Kingdom.
steven.groen@warwick.ac.uk

Jaap Top
Bernoulli Institute, University of Groningen, Groningen, the Netherlands.
j.top@rug.nl

Received: 4/12/22, Revised: 9/5/22, Accepted: 11/20/22, Published: 12/16/22

Abstract

In this paper a set of elliptic curves E with explicit elements of order 3 in their Tate-Shafarevich group is constructed. First, the theory of descent by 3-isogeny is reviewed, including explicit equations for homogeneous spaces representing the elements in the associated Selmer group. For the main result, elliptic curves admitting a rational 2-isogeny as well as a rational 3-isogeny are constructed. Using elementary 2-isogeny descent, it is shown that our curves have rank zero. A result of Cassels then shows that the Selmer group of the 3-isogeny is non-trivial. As a consequence one obtains in a very simple way explicit examples of plane cubics over $\mathbb{Q}$ that have a point everywhere locally, but not globally.

1. Introduction

In this article, we consider elliptic curves defined over $\mathbb{Q}$ that admit a rational isogeny of degree 3. As is well known (see, for instance, [20, Theorem X.4.2]) such an isogeny $\psi\colon E \to \bar{E}$ gives rise to an exact sequence of $\mathbb{F}_3$-vector spaces

$$0 \to \bar{E}(\mathbb{Q})/\psi(E(\mathbb{Q})) \to \mathrm{Sel}^{(\psi)}(E/\mathbb{Q}) \to \text{Ш}(E/\mathbb{Q})[\psi] \to 0.$$

The elements of $\mathrm{Sel}^{(\psi)}(E/\mathbb{Q})$ are represented by genus-1 curves called *homogeneous spaces*. As a preparation for our main result, section 2 presents explicit equations for these curves. The fact that they come from the Selmer group means they have points everywhere locally. A global point on such a curve gives rise to a point on $\bar{E}(\mathbb{Q})/\psi(E(\mathbb{Q}))$. Section 2 is the "*Descent via Three-Isogeny*" analogue of the classical "*Descent via Two-Isogeny*" described in [20, Proposition X.4.9]. Although most of this is known to experts and parts of it can be found in the literature ([1], [7, Section 8.4], [8], [12], [23]), we are convinced our short and complete exposition is useful.

In section 3 the main result of the paper is presented: it combines and compares the two simplest types of descent, namely a 2-isogeny descent and a 3-isogeny descent. We construct an explicit set of elliptic curves defined over $\mathbb{Q}$ (and admitting both a rational 2-isogeny and a rational 3-isogeny) with elements of order 3 in their Tate-Shafarevich group. Concretely, we prove the following theorem.

Theorem 1. *Let h be a positive integer such that $h \equiv 3 \bmod 8$ and moreover h, $h-2$, $h-6$ and $h-8$ are prime numbers. Define*

$$E_h\colon y^2 = x^3 - 216(x - h(h-6)^2)^2.$$

Then E_h has the following properties:

1. *E_h has a rational 2-isogeny ϕ and a rational 3-isogeny ψ (see section 3.1).*
2. *$E_{h,tors}(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$ (see section 3.1).*
3. *Using 2-isogeny descent one concludes that $E_h(\mathbb{Q})$ has rank zero (see section 3.2).*
4. *$\#\mathrm{Sel}^{(\psi)}(E_h/\mathbb{Q}) = 9$; this gives rise to 9 pairwise distinct elements in the group $\text{Ш}(E_h/\mathbb{Q})[3]$ (see section 3.3).*

By section 2, this yields explicit cubics violating the Hasse principle. For example

$$C^h\colon 3w^2z + 2z^3 + w^3 + 6wz^2 + 2(h-2)^2(h-8) = 12z^2 - 6w^2$$

has a point over every completion of $\mathbb{Q}$, but not over $\mathbb{Q}$ itself.

Schinzel's hypothesis H ([17]) predicts as a specific case that

$$S = \{h \in \mathbb{Z} \ : \ h \equiv 3 \bmod 8 \text{ and } h,\ h-2,\ h-6,\ h-8 \text{ prime}\}$$

is infinite and hence that this set yields infinitely many examples as above.

An infinite family of genus 1 curves violating the Hasse principle and related to Ш[3] is already given in [16], using the Brauer-Manin obstruction to show the non-existence of rational points (the earliest examples coming from Ш[3] seem to be those from Selmer's paper [19]). In [3] it is shown that in fact a positive proportion of plane cubics fail the Hasse principle. Furthermore, it is a classic result ([5], [1], [13]) that the 3-torsion in Tate-Shafarevich groups of elliptic curves over $\mathbb{Q}$ gets arbitrarily large. In contrast with our result, apart from [16] and [3] the papers cited here discuss elliptic curves admitting a rational point of order 3. The method of comparing 2- and 3-isogeny descents we used is very natural, yet we are not aware of an earlier text presenting examples in this way.

2. Homogeneous Spaces Corresponding to a Rational 3-Isogeny

In order to construct explicit counterexamples to the Hasse principle in section 3, this section reviews via Galois cohomology the descent coming from a rational 3-isogeny ψ. This builds up to Theorem 2, giving explicit equations for the homogeneous spaces in $\mathrm{WC}(E/\mathbb{Q})$ coming from ψ. As already stated, our aim is to provide a description for 3-isogeny descent comparable to what is done for 2-isogenies in [20, Proposition X.4.9].

2.1. Elliptic Curves with a Rational 3-Isogeny

Let E be an elliptic curve over $\mathbb{Q}$ with a Galois invariant subgroup T of size 3. The quotient map $\psi\colon E \to E/T =: \bar{E}$ is a rational 3-isogeny. By, for example, [20, Proposition III.4.12], every rational 3-isogeny between elliptic curves is obtained in this way. Following [23], one distinguishes the cases $j_E = 0$ and $j_E \neq 0$ to obtain explicit descriptions for these curves and maps. The nice discussion of 3-isogeny descent in [7, Section 8.4] avoids this distinction by using equations $y^2 = x^3 + d(ax+b)^2$ (but different from our text, it does not discuss the Galois cohomological derivation of various maps, nor the form of various homogeneous spaces).

In the case $j_E = 0$, one gives E by

$$E\colon y^2 = x^3 + A$$

(here T is generated by a point with $x = 0$), and the isogeny ψ up to possibly multiplication by -1 is

$$\begin{aligned}\psi : (x,y) &\mapsto \left(\frac{y^2+3A}{x^2}\,,\ \frac{y(x^3-8A)}{x^3}\right),\\ \bar{E} : \eta^2 &= \xi^3 - 27A.\end{aligned}$$

For brevity, we introduce the notation $\bar{A} := -27A$.

In the case $j_E \neq 0$, one gives E by

$$E\colon y^2 = x^3 + A(x-B)^2.$$

Again T is generated by a point with $x = 0$, and (up to ± 1) here ψ is given by

$$\begin{aligned}\psi : (x,y) &\mapsto \left(\frac{3(6y^2+6AB^2-3x^3-2Ax^2)}{x^2}\,,\ \frac{27y(8AB^2-x^3-4ABx)}{x^3}\right), \qquad (1)\\ \bar{E} : \eta^2 &= \xi^3 - 27A(\xi - 4A - 27B)^2.\end{aligned}$$

For brevity, we introduce $\bar{B} := 4A + 27B$.

By $\hat{\psi}\colon \bar{E} \to E$ we will denote the dual isogeny of ψ, such that $\hat{\psi}\circ\psi = [3]$.

2.2. Galois Cohomology

For any field K, let $G_K = \mathrm{Gal}(K^{\mathrm{sep}}/K)$ be its absolute Galois group. The isogeny ψ described above yields an exact sequence

$$0 \longrightarrow E[\psi] \longrightarrow E \xrightarrow{\psi} \bar{E} \longrightarrow 0 \tag{2}$$

of $G_{\mathbb{Q}}$-modules. Taking $G_{\mathbb{Q}}$ invariants yields a long sequence of Galois cohomology

$$0 \longrightarrow E(\mathbb{Q})[\psi] \longrightarrow E(\mathbb{Q}) \xrightarrow{\psi} \bar{E}(\mathbb{Q}) \xrightarrow{\delta} H^1(G_{\mathbb{Q}}, E[\psi]) \longrightarrow H^1(G_{\mathbb{Q}}, E) \xrightarrow{\psi_*} H^1(G_{\mathbb{Q}}, \bar{E}),$$

which is shortened to

$$0 \to \bar{E}(\mathbb{Q})/\psi(E(\mathbb{Q})) \xrightarrow{\delta} H^1(G_{\mathbb{Q}}, E[\psi]) \longrightarrow H^1(G_{\mathbb{Q}}, E)[\psi_*] \to 0. \tag{3}$$

Recall that a *homogeneous space* (also called a torsor) of $E/\mathbb{Q}$ is a smooth curve $C/\mathbb{Q}$ with a simply transitive action $E \times C \to C$. By [20, Theorem X.3.6], elements of $H^1(G_{\mathbb{Q}}, E)$ are in bijection with $\mathbb{Q}$-isomorphism classes of homogeneous spaces. Hence the set of $\mathbb{Q}$-isomorphism classes of homogenous spaces inherits the structure of a group, called the Weil-Châtelet group $\mathrm{WC}(E/\mathbb{Q}) \cong H^1(G_{\mathbb{Q}}, E)$. In this section we explicitly describe the homogeneous spaces coming from a certain subgroup of $H^1(G_{\mathbb{Q}}, E)$.

Localizing (3) gives the commutative diagram with exact rows

$$\begin{array}{ccccc} \bar{E}(\mathbb{Q})/\psi(E(\mathbb{Q})) & \xhookrightarrow{\delta} & H^1(G_{\mathbb{Q}}, E[\psi]) & \twoheadrightarrow & \mathrm{WC}(E/\mathbb{Q})[\psi] \\ \downarrow & & \downarrow & & \downarrow \\ \prod_{v \in M_{\mathbb{Q}}} \bar{E}(\mathbb{Q}_v)/\psi(E(\mathbb{Q}_v)) & \xhookrightarrow{\delta} & \prod_{v \in M_{\mathbb{Q}}} H^1(\mathrm{Gal}(\bar{\mathbb{Q}}_v/\mathbb{Q}_v), E[\psi]) & \twoheadrightarrow & \prod_{v \in M_{\mathbb{Q}}} \mathrm{WC}(E/\mathbb{Q}_v)[\psi]. \end{array} \tag{4}$$

This allows one to define Selmer groups and Tate-Shafarevich groups, recalled here.

Definition 1. The *ψ-Selmer group* of E over $\mathbb{Q}$, denoted $\mathrm{Sel}^{(\psi)}(E/\mathbb{Q})$, is defined as the kernel of the composite map $H^1(G_{\mathbb{Q}}, E[\psi]) \to \prod_{v \in M_{\mathbb{Q}}} \mathrm{WC}(E/\mathbb{Q}_v)[\psi]$ in the diagram (4).

Definition 2. The *Tate-Shafarevich group* of E over $\mathbb{Q}$, denoted $\text{Ш}(E/\mathbb{Q})$, is the kernel of the localization map $\mathrm{WC}(E/\mathbb{Q}) \to \prod_{v \in M_{\mathbb{Q}}} \mathrm{WC}(E/\mathbb{Q}_v)$.

From (4) one infers the exact sequence

$$0 \to \bar{E}(\mathbb{Q})/\psi(E(\mathbb{Q})) \to \mathrm{Sel}^{(\psi)}(E/\mathbb{Q}) \to \text{Ш}(E/\mathbb{Q})[\psi] \to 0.$$

2.3. Explicit Equations for Homogeneous Spaces

Define $L := \mathbb{Q}[T]/(T^2 - \bar{A})$ and denote $\bar{\tau} := T \bmod (T^2 - \bar{A}) \in L$. The points in $\bar{E}[\hat{\psi}]$ have coordinates in any field obtained as the image of L under an algebra homomorphism.

In case L is a field, one has $E[\psi] \cong \mu_3$ as G_L-modules. Since $\#E[\psi]^{G_L}$ divides 3 and hence is coprime to $\#\mathrm{Gal}(L/\mathbb{Q})$, all cohomology groups $H^k(\mathrm{Gal}(L/\mathbb{Q}), E[\psi]^{G_L})$ are trivial. Therefore (using the inflation - restriction exact sequence, as is done in [23, Section 4]) the restriction $H^1(G_\mathbb{Q}, E[\psi]) \to H^1(G_L, E[\psi])^{\mathrm{Gal}(L/\mathbb{Q})}$ is an isomorphism. Combining this with Hilbert's Theorem 90 and writing $\mathrm{Ker}(N_{L/\mathbb{Q}}) := \mathrm{Ker}\left(N_{L/\mathbb{Q}} \colon L^\times/{L^\times}^3 \to \mathbb{Q}^\times/{\mathbb{Q}^\times}^3\right)$ gives

$$H^1(G_\mathbb{Q}, E[\psi]) \cong H^1(G_L, E[\psi])^{\mathrm{Gal}(L/\mathbb{Q})} \cong H^1(G_L, \mu_3)^{\mathrm{Gal}(L/\mathbb{Q})} \cong \mathrm{Ker}(N_{L/\mathbb{Q}}).$$

Under this sequence of isomorphisms, (3) becomes

$$0 \longrightarrow \bar{E}(\mathbb{Q})/\psi(E(\mathbb{Q})) \xrightarrow{\ \delta\ } \mathrm{Ker}(N_{L/\mathbb{Q}}) \longrightarrow \mathrm{WC}(E/\mathbb{Q})[\psi] \longrightarrow 0. \tag{5}$$

In case L is *not* a field one has $L \cong \mathbb{Q} \times \mathbb{Q}$. Under this identification the norm map $N_{L/\mathbb{Q}} \colon L^\times/{L^\times}^3 \to \mathbb{Q}^\times/{\mathbb{Q}^\times}^3$ yields multiplication $\mathbb{Q}^\times/{\mathbb{Q}^\times}^3 \times \mathbb{Q}^\times/{\mathbb{Q}^\times}^3 \to \mathbb{Q}^\times/{\mathbb{Q}^\times}^3$. In particular, its kernel $\mathrm{Ker}(N_{L/\mathbb{Q}})$ is isomorphic to $\mathbb{Q}^\times/{\mathbb{Q}^\times}^3$. Since in the present situation $E[\psi] \cong \mu_3$ as $G_\mathbb{Q}$-modules, one obtains in an analogous but simpler way as above again $H^1(G_\mathbb{Q}, E[\psi]) \cong \mathrm{Ker}(N_{L/\mathbb{Q}})$ and therefore also the sequence (5).

The following lemma describes the connecting homomorphism δ in terms of the equations presented in Section 2.1.

Lemma 1. *Let E be given by $y^2 = x^3 + A$. The map $\delta \colon \bar{E}(\mathbb{Q})/\psi(E(\mathbb{Q})) \to L^\times/{L^\times}^3$ is given by*

$$\delta \colon P + \psi(E(\mathbb{Q})) \mapsto \begin{cases} 1 \cdot {L^\times}^3 & \text{if } P = O, \\ (\eta + \bar{\tau}) \cdot {L^\times}^3 & \text{if } P = (\xi, \eta) \text{ with } \xi \neq 0, \\ (2A^2, 4A)^{\pm 1} \in \left(\mathbb{Q}^\times/{\mathbb{Q}^\times}^3\right)^{\oplus 2} & \text{if } P = (0, \pm\sqrt{\bar{A}}). \end{cases}$$

For E given by $y^2 = x^3 + A(x - B)^2$, the connecting homomorphism takes the form

$$\delta \colon P + \psi(E(\mathbb{Q})) \mapsto \begin{cases} 1 \cdot {L^\times}^3 & \text{if } P = O, \\ (\eta + (\xi - \bar{B})\bar{\tau}) \cdot {L^\times}^3 & \text{if } P = (\xi, \eta) \text{ with } \xi \neq 0, \\ (2\bar{B}^2 A, 4\bar{B}A^2) \in \left(\mathbb{Q}^\times/{\mathbb{Q}^\times}^3\right)^{\oplus 2} & \text{if } P = (0, \pm\sqrt{\bar{A}} \cdot \bar{B}). \end{cases}$$

Proof. The map $\delta \colon \bar{E}(\mathbb{Q})/\psi(\mathbb{Q}) \to H^1(G_\mathbb{Q}, E[\psi])$ sends the class of P in the group $\bar{E}(\mathbb{Q})/\psi(E(\mathbb{Q}))$ to the cocycle $\sigma \mapsto Q^\sigma - Q$, where $\psi(Q) = P$. One finishes the proof by a direct computation using the definition of ψ and Hilbert's Theorem 90. See also [20, Exercise 10.1] or [7, §8.4.4]. □

In case L is a field, write M_L for the set of primes (finite and infinite) of L. Let $S \subset M_L$ denote a finite set containing all infinite primes of L. We define

$$L(S,3) := \{t \in L^\times/L^{\times 3} \ : \ v(t) \equiv 0 \bmod 3 \ \forall v \in M_L \setminus S\}$$
$$L(S,3)^* := \{t \in L(S,3) \ : \ N_{L/\mathbb{Q}}(t) \in \mathbb{Q}^{\times 3}\}.$$

Let $S_{E,\psi} \subset M_L$ denote the set of bad primes of E, together with the primes dividing 3 (which is the degree of ψ), and the infinite primes of L. It is well-known (see, for instance, [20, Corollary X.4.4]) that $\mathrm{im}(\delta)$ is contained in $L(S_{E,\psi},3)$. This implies that $\mathrm{im}(\delta)$ is finite, which is essentially the weak Mordell-Weil theorem. Note that it is immediate from the equations (without using Galois cohomology) that $\mathrm{im}(\delta)$ is contained in the kernel of the norm map.

To adapt the above to the situation where L is not a field (so $\bar{A}$ is a non-zero square), one considers in that case any of the two projections $\pi\colon L^\times/L^{\times 3} \to \mathbb{Q}^\times/\mathbb{Q}^{\times 3}$ and defines, for $S \subset M_{\mathbb{Q}}$ containing the infinite prime of $\mathbb{Q}$, the group

$$L(S,3) := \{t \in L^\times/L^{\times 3} \ : \ v(\pi(t)) \equiv 0 \bmod 3 \ \forall v \in M_{\mathbb{Q}} \setminus S\}.$$

The subgroup $L(S,3)^*$ is defined exactly as before. With $S_{E,\psi} \subset M_{\mathbb{Q}}$ the set of bad primes for E together with 3 and ∞, again the image of δ is contained in $L(S_{E,\psi},3)^*$.

Lemma 2. *Suppose L is a field and $t \in L(S,3)^*$. If $v \in S$ is a finite place with the property that $v(t) \bmod 3 \not\equiv 0$, then v is either a split prime of $L/\mathbb{Q}$ or a non-principal ramified prime.*

Proof. Suppose $v \in S$ corresponds to an inert or a principal ramified prime, which we write as $\mathfrak{p} = \alpha\mathcal{O}_L$. Then $N_{L/\mathbb{Q}}(\alpha) \in \{\pm p, \pm p^2\}$ for a prime number p. If $v(t) \bmod 3 \not\equiv 0$, then any $\tau \in L^\times$ representing t has a norm containing the prime p to a power that is not $0 \bmod 3$. This violates the definition of $L(S,3)^*$. □

We now give explicit equations for the homogeneous space corresponding to such t.

Theorem 2. *Let $t \in L$ represent a class in $L(S_{E,\psi},3)^*$ and let $s \in \mathbb{Q}$ be the unique rational number with $N_{L/\mathbb{Q}}(t) = s^3$. The map $L(S_{E,\psi},3)^* \to \mathrm{WC}(E/\mathbb{Q})[\psi]$ in (5) sends $t \cdot L^{\times 3}$ to a homogeneous space C_t. An explicit affine equation for C_t in variables w and z is as follows:*

- *If E is given by $y^2 = x^3 + A$ and $\bar{A}$ is a square, then $C_t\colon t^2w^3 - 2t\sqrt{\bar{A}} = z^3$.*
- *If E if given by $y^2 = x^3 + A$ and $\bar{A}$ is not a square, write $t = u + v\sqrt{\bar{A}}$. Then we have*

$$C_t\colon 3uw^2z + \bar{A}uz^3 + vw^3 + 3\bar{A} = 1.$$

- *For $E\colon y^2 = x^3 + A(x-B)^2$ and $\bar{A}$ a square, we have $C_t\colon t^2w^3 - 2t(wz - \bar{B})\sqrt{\bar{A}} = z^3$.*
- *For $E\colon y^2 = x^3 + A(x-B)^2$ and $\bar{A}$ not a square, write $t = u + v\sqrt{\bar{A}}$. Then*

$$C_t\colon 3uw^2z + \bar{A}uz^3 + vw^3 + 3\bar{A}vwz^2 + \bar{B} = s(w^2 - \bar{A}z^2).$$

Proof. Assume that t comes from $P = (\xi, \eta)$ on $\bar{E}(\mathbb{Q})/\psi(E(\mathbb{Q}))$, so t equals the image of δ in Lemma 1 up to multiplication by a cube. For every case this yields a model of C_t.

In the first case, $t \in \mathrm{im}(\delta)$ implies $w^3t = \eta + \sqrt{\bar{A}}$ for some $w \in \mathbb{Q}$. The condition $P \in \bar{E}(\mathbb{Q})$ yields that $(w^3t - \sqrt{\bar{A}})^2 = \eta^2 = \xi^3 + \bar{A}$. Setting $z = \frac{\xi}{w}$ gives the equation of C_t.

The second case is similar, starting from $(w + z\sqrt{\bar{A}})^3(u + v\sqrt{\bar{A}}) = \eta + \sqrt{\bar{A}}$. Comparing coefficients of $\sqrt{\bar{A}}$ yields the equation of C_t. Here P is automatically on the curve by letting ξ^3 be the norm of the left-hand side (which is a cube).

For the third case, $t \in \mathrm{im}(\delta)$ implies $w^3t = \eta + \sqrt{\bar{A}}(\xi - \bar{B})$. Just like in the first case, the condition $P \in \bar{E}(\mathbb{Q})$ gives the equation for C_t.

In the fourth case, we have $(w + z\sqrt{\bar{A}})^3(u + v\sqrt{\bar{A}}) = \eta + \sqrt{\bar{A}}(\xi - \bar{B})$. Comparing coefficients of $\sqrt{\bar{A}}$ yields $3uw^2z + \bar{A}uz^3 + vw^3 + 3\bar{A}vwz^2 + B = \xi$. Now, observe that

$$\xi^3 = N_{L/\mathbb{Q}}(\eta + \sqrt{\bar{A}}(\xi - \bar{B})) = N_{L/\mathbb{Q}}((w + z\sqrt{\bar{A}})^3(u + v\sqrt{\bar{A}})) = s^3(w^2 - \bar{A}z^2)^3.$$

Substituting $\xi = s(w^2 - \bar{A}z^2)$ gives the equation for C_t. □

Remark 1. Theorem 3.1 and Theorem 4.1 of [8] also describe the homogeneous spaces of a rational 3-isogeny. Like in [7], the slightly different model $\bar{E}\colon y^2 = x^3 + D(ax+b)^2$ is used. Theorem 3.1 treats $\sqrt{D} \in \mathbb{Q}$, resulting in $uX^3 + \left(\frac{1}{u}\right)Y^3 + 2bZ^3 = 2aXYZ$. This is equivalent to our first case (if $a = 0$) and third case (if $a \neq 0$), via the change of variables $(X, Y, Z) := (w, -z, 1)$. Theorem 4.1 of [8] treats the case $\sqrt{D} \notin \mathbb{Q}$, corresponding to the second case (if $a = 0$) and fourth case (if $a \neq 0$) in Theorem 2. Introducing an extra variable for the cube root of $N_{L/\mathbb{Q}}(t)$ is avoided by writing $\mathrm{Gal}(L/\mathbb{Q}) = \langle\sigma\rangle$ and $t = v^2\sigma(v)$ (which is allowed because t is chosen up to cubes), such that $N_{L/\mathbb{Q}}(t) = (v\sigma(v))^3$. This yields a different, but equivalent model of the corresponding homogeneous space.

3. A Set of Explicit Elements of Order 3 in Tate-Shafarevich Groups

In this section we exhibit a set $\{E_h\}$ of elliptic curves with a rational 2-isogeny ϕ and a rational 3-isogeny ψ. By the well-known method of 2-isogeny descent we show that every E_h has rank zero. Then we show that the Selmer group $\mathrm{Sel}^{(\psi)}(E_h/\mathbb{Q})$ must contain at least 9 elements. The non-trivial ones are represented by homogeneous spaces (in fact plane cubics whose model is given by Theorem 2), that violate the Hasse principle. We guarantee the existence of elements in the ψ-Selmer group using the following result of Cassels ([6, Thm. 1.1], [14, Thm. 1], [9, § 7]).

Theorem 3. *Let $\phi : E/\mathbb{Q} \to E'/\mathbb{Q}$ be a rational isogeny and let $\hat{\phi} : E'/\mathbb{Q} \to E/\mathbb{Q}$ be its dual. Then the following relation between the corresponding Selmer groups holds ([6, Theorem 1.1]):*

$$\frac{\#\mathrm{Sel}^{(\hat{\phi})}(E'/\mathbb{Q})}{\#\mathrm{Sel}^{(\phi)}(E/\mathbb{Q})} = \frac{\#E'(\mathbb{Q})[\hat{\phi}]\Omega_E \prod_p c_{E,p}}{\#E(\mathbb{Q})[\phi]\Omega_{E'} \prod_p c_{E',p}},$$

where $\Omega_E := \int_{E(\mathbb{R})} \omega_E$ denotes the real period of E and $c_p := \#E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$ denotes the Tamagawa number of E at p.

3.1. The Elliptic Curves E_h

Recall the general form of an elliptic curve with a rational 3-isogeny and non-zero j-invariant:

$$E\colon y^2 = x^3 + A(x - B)^2.$$

We wish to use descent by 2-isogeny to show that E has rank zero, so we want to impose on the parameters A and B the condition that E admits a rational 2-isogeny. This is equivalent to the right-hand side polynomial having a rational root $x = c$. This implies $A = -\frac{c^3}{(c-B)^2}$. Multiplying by $(c - B)^6$, rescaling x and y and introducing $h := B$ yields

$$E\colon y^2 = x^3 - c^3(x - h(h - c)^2)^2.$$

We now make a strategic choice of c; we will later do arithmetic in $\mathbb{Q}(\bar{E}[\hat{\psi}]) = \mathbb{Q}(\sqrt{3c})$, so we pick $c = 6$ to land in the convenient number field $\mathbb{Q}(\sqrt{2})$. This gives the model of the curve we will use:

$$E_h\colon y^2 = x^3 - 216(x - h(h - 6)^2)^2. \tag{6}$$

We denote the rational 2-isogeny by $\phi\colon E_h \to E'_h$, and the rational 3-isogeny by $\psi\colon E_h \to \bar{E}_h$.

Remark 2. Viewing h as a variable, one can view $E_h/\mathbb{Q}(h)$ as the generic fiber of an elliptic surface $\mathcal{E} \to \mathbb{P}^1$ defined over $\mathbb{Q}$. This turns out to be a quadratic twist of Beauville's rational modular elliptic surface associated to the congruence subgroup $\Gamma_0(6)$. Indeed, Beauville in [2] describes this surface as the pencil of plane cubics given by

$$(x + y)(x + z)(y + z) + txyz = 0.$$

Using for instance the basepoint/section $(0:0:1)$ on the curves in this pencil, one readily obtains the Weierstrass equation

$$y^2 = x^3 + ((t+2)x + 4t)^2$$

for the latter surface. The Möbius transformation $h \mapsto t = -2h/(h-6)$ transforms this, after scaling, into

$$y^2 = x^3 + (6x + h(h-6)^2)^2$$

which is the quadratic twist over $\mathbb{Q}(h)(\sqrt{-6})/\mathbb{Q}(h)$ of E_h. As a consequence (see also [25, § 2.3.2] and No. 66 in the table of [15]), as an elliptic curve over the function field $\mathbb{Q}(h)$ one finds $E_h(\mathbb{Q}(h)) \cong \mathbb{Z}/2\mathbb{Z}$ and $E_h(\mathbb{Q}(h)(\sqrt{-6})) \cong \mathbb{Z}/6\mathbb{Z}$. In [18, p. 167 Table 8.3] another equation defining Beauville's example is presented.

We now consider values $h \in \mathbb{Z}$ and take $E = E_h/\mathbb{Q}$. In order to maintain some control over the local computations, we minimize the number of bad primes of E; we make sure that the discriminant

$$\Delta_E = -2^{10}3^9h^3(h-2)^2(h-6)^6(h-8)$$

has only 6 bad primes, by demanding that h, $h-2$, $h-6$ and $h-8$ are prime numbers. Note that this implies $h \equiv 4 \bmod 15$.

From reduction modulo 5, which we have rigged to be a good prime, and the fact that -6 and 2 are not squares (meaning the 3-torsion is not rational), it follows that the rational torsion subgroups of E_h, E'_h and $\bar{E}_h$ are isomorphic to $\mathbb{Z}/2\mathbb{Z}$, as claimed in Theorem 1.

In view of Theorem 3, we wish to manipulate the Tamagawa numbers such that $\prod_p c_{E,p} < \prod_p c_{\bar{E},p}$ and hence $\mathrm{Sel}^{(\psi)}(E/\mathbb{Q})$ grows. Using the algorithm in [22] one obtains the results described in Table 1.

	$h \equiv 1 \bmod 8$	$h \equiv 3 \bmod 8$	$h \equiv 5 \bmod 8$	$h \equiv 7 \bmod 8$
$p = 2$	Additive	Additive	Additive	Additive
$p = 3$	Additive	Additive	Additive	Additive
$p = h-8$	Split	Non-split	Non-split	Split
$p = h-6$	Non-split	Non-split	Split	Split
$p = h-2$	Split	Split	Non-split	Non-split
$p = h$	Split	Non-split	Non-split	Split
$\prod_p c_{E_h,p}$	48	16	48	144
$\prod_p c_{E'_h,p}$	48	16	48	144
$\prod_p c_{\bar{E}_h,p}$	144	48	16	48

Table 1: A table representing the local properties of E_h. 'Split' and 'non-split' refer to multiplicative reduction.

The cases $h \equiv 1, 3 \bmod 8$ are favorable in view of Theorem 3. In order to keep the local computations required for descent by 2-isogeny manageable, it helps to have small Tamagawa numbers, so we pick the case $h \equiv 3 \bmod 8$. Combining this with the earlier congruence relation $h \equiv 4 \bmod 15$ yields $h \equiv 19 \bmod 120$, which we assume from here on out.

3.2. Descent by 2-Isogeny

Let E_h be given by (6) with $h \equiv 3 \bmod 8$ and h, $h-2$, $h-6$ and $h-8$ primes. In order to apply the classical theory of 2-isogeny descent, we move the 2-torsion point to $(0,0)$. This yields the models

$$E_h\colon y^2 = x^3 + \left(18(h-6)^2 - 216\right)x^2 + 108(h-2)(h-6)^3 x \tag{7}$$
$$E'_h\colon Y^2 = X^3 + \left(432 - 36(h-6)^2\right)X^2 - 108h^3(h-8)X. \tag{8}$$

One verifies that both these models are globally minimal. The algorithm in [22] is needed to show that this model of E'_h is minimal at 2 (we have $\mathrm{ord}_2(\Delta_{E'_h}) = 14$), while in the other instances the computation of the discriminant suffices.

Lemma 3. $E'_h(\mathbb{Q})/\phi(E_h(\mathbb{Q})) = \{O, (0,0)\}$.

Proof. Following the classical descent by 2-isogeny in [20, Proposition X.4.9], there is an injective homomorphism

$$\begin{aligned}\alpha\colon E'_h(\mathbb{Q})/\phi(E(\mathbb{Q})) &\to \mathbb{Q}^\times/{\mathbb{Q}^\times}^2\\ (X,Y) &\mapsto X\cdot{\mathbb{Q}^\times}^2 \quad (\text{for } X \neq 0),\\ (0,0) &\mapsto -108h^3(h-8)\cdot{\mathbb{Q}^\times}^2 = -3h(h-8)\cdot{\mathbb{Q}^\times}^2.\end{aligned}$$

Hence

$$\langle -3h(h-8)\rangle \subseteq \mathrm{im}(\alpha) \subseteq \mathrm{Sel}^{(\phi)}(E/\mathbb{Q}) \subseteq \langle -1,2,3,h,h-2,h-6,h-8\rangle.$$

We prove that $\mathrm{Sel}^{(\phi)}(E/\mathbb{Q}) = \{1, -3h(h-8)\}$ by localizing to various primes.

Note that the square-free part of X has to divide $-108h^3(h-8)$ in order to yield a point $(X,Y) \in E'_h(\mathbb{Q})$ (see [21, page 86-87] for a more elaborate argumentation). This gives $\mathrm{im}(\alpha) \subseteq \langle -1,2,3,h,h-8\rangle$.

For any prime p, we let $\alpha_p : E'_h(\mathbb{Q}_p)/\phi(E(\mathbb{Q}_p)) \to \mathbb{Q}_p^\times/{\mathbb{Q}_p^\times}^2$ denote the localization of α at p. We first show that $E'_{h,1}(\mathbb{Q}_p)$ does not contribute. For odd p this is immediate as $p\mathbb{Z}_p/2p\mathbb{Z}_p \cong 0$. For $p = 2$, this is a straightforward calculation using the Laurent series in [20, page 118]. See also [24, Lemma 3.2.1] for a similar calculation.

First, we analyze

$$\alpha_2\colon E'_h(\mathbb{Q}_2)/\phi(E_h(\mathbb{Q}_2)) \to \mathbb{Q}_2^\times/{\mathbb{Q}_2^\times}^2 = \langle -1,5,2\rangle.$$

Using our computation of Tamagawa numbers and the minimality of the model, we infer $\#(E'(\mathbb{Q}_2)/E'_0(\mathbb{Q}_2)) = 2$ (note that to ease notation, here and once more below we removed the subscript h in E'_h). The reduction of (X,Y) is singular precisely when X is even, in which case it reduces to $(0,0)$. If X is odd, then so is Y and they satisfy the homogeneous equation

$$Y^2Z = X^3 + \left(432 - 36(h-6)^2\right) X^2Z - 108h^3(h-8)XZ^2,$$

implying

$$Z \equiv X + 4Z + 4X \equiv X \bmod 8.$$

Hence $X/Z = 1 \cdot {\mathbb{Q}_2^\times}^2$. Moreover, observe that

$$\alpha_2((0,0)) = -108h^3(h-8) \cdot {\mathbb{Q}_2^\times}^2 = 5{\mathbb{Q}_2^\times}^2,$$

and hence $\operatorname{im}(\alpha_2) = \langle 5 \rangle$. This gives the restriction $\operatorname{im}(\alpha) \subseteq \langle -3, -h, -(h-8) \rangle$.

Now consider the localized map

$$\alpha_3 : E'_h(\mathbb{Q}_3)/\phi(E_h(\mathbb{Q}_3)) \to \mathbb{Q}_3^\times/{\mathbb{Q}_3^\times}^2 = \langle -1, 3 \rangle.$$

Again we have computed $\#(E'(\mathbb{Q}_3)/E'_0(\mathbb{Q}_3)) = 2$. The point (X,Y) reduces to a singular point if and only if $3|X$, and otherwise $X \equiv 1 \bmod 3$. Moreover, $(0,0)$ is mapped to $-3h(h-8) \cdot {\mathbb{Q}_3^\times}^2 = 3{\mathbb{Q}_3^\times}^2$. We conclude that $\operatorname{im}(\alpha_3) = \langle 3 \rangle$, giving the restriction $\operatorname{im}(\alpha) \subseteq \langle 3h, -(h-8) \rangle$.

The final restriction comes from the localized map

$$\alpha_{h-2} : E'_h(\mathbb{Q}_{h-2})/\phi(E_h(\mathbb{Q}_{h-2})) \to \mathbb{Q}_{h-2}^\times/{\mathbb{Q}_{h-2}^\times}^2 = \langle -3, h-2 \rangle.$$

We see that $-3h(h-8) \cdot {\mathbb{Q}_{h-2}^\times}^2 = 36 \cdot {\mathbb{Q}_{h-2}^\times}^2 = 1 \cdot {\mathbb{Q}_{h-2}^\times}^2$. The algorithm in [22] shows that all points of $E'_h(\mathbb{Q}_{h-2})$ have good reduction. Over $\mathbb{F}_{h-2}$ the curve E'_h is given by

$$E'_h \colon Y^2 = X(X-72)^2.$$

Following [20, Proposition III.2.5], let $\gamma = \sqrt{72} \in \mathbb{F}_{h-2}$ be the slope of a tangent line at the node of $E'_h(\mathbb{F}_{h-2})$. The isomorphism

$$E'_{h,ns}(\mathbb{F}_{h-2}) \xrightarrow{\sim} \mathbb{F}_{h-2}^\times \quad : \quad (X,Y) \mapsto \frac{Y + \gamma(X-72)}{Y - \gamma(X-72)}$$

maps the point $(18, 27\gamma)$ to -3, which is not a square, so this point is not a multiple of 2. Finally, 18 is a square in $\mathbb{Q}_{h-2}$, so we infer $\operatorname{im}(\alpha_{h-2}) = \{1\}$. This gives the final restriction

$$\operatorname{im}(\alpha) = \operatorname{Sel}^{(\phi)}(E/\mathbb{Q}) = \{1, -3h(h-8)\}$$

and therefore

$$E'_h(E/\mathbb{Q})/\phi(E_h(\mathbb{Q})) = \{O, (0,0)\},$$

as desired. □

Lemma 4. $E_h(\mathbb{Q})/\hat{\phi}(E'_h(\mathbb{Q})) = \{O, (0,0)\}$.

Proof. We make use of Theorem 3. Clearly $\#E'_h(\mathbb{Q})[\hat{\phi}] = \#E_h(\mathbb{Q})[\phi] = 2$. Furthermore, Table 1 shows $\prod_p c_{E_h,p} = \prod_p c_{E'_h,p} = 16$. For the real periods, we make use of [10, Lemma 7.4]:

$$\frac{\Omega_{E_h}}{\Omega_{E'_h}} = \frac{\#\ker(\phi\colon E_h(\mathbb{R}) \to E'_h(\mathbb{R}))}{\#\mathrm{coker}(\phi\colon E_h(\mathbb{R}) \to E'_h(\mathbb{R}))} \cdot \left| \frac{\omega_{E_h}}{\phi^*\omega_{E'_h}} \right|, \tag{9}$$

where ω_E denotes the invariant differential of a minimal model of an elliptic curve E. First we observe that

$$\#\ker(\phi\colon E_h(\mathbb{R}) \to E'_h(\mathbb{R})) = \#\mathrm{coker}(\phi\colon E_h(\mathbb{R}) \to E'_h(\mathbb{R})) = 2.$$

Recall that the models (7) and (8) are minimal. Using the explicit form of ϕ (see, for instance, [20, Proposition X.4.9]) and writing $a := 432 - 36(h-6)^2$ and $b := -108h^3(h-8)$, we compute

$$\begin{aligned} \phi^*\omega_{E'_h} = \phi^*\left(\frac{dX}{2Y}\right) &= \frac{d(x^{-2}(x^3 + ax^2 + bx))}{2y(bx^{-2} - 1)} \\ &= \frac{(1 - bx^{-2})dx}{2y(bx^{-2} - 1)} = -\omega_{E_h}. \end{aligned}$$

Thus (9) yields that $\Omega_{E_h} = \Omega_{E'_h}$. Now one applies Theorem 3 to infer that $\#\mathrm{Sel}^{(\phi)}(E_h/\mathbb{Q}) = \#\mathrm{Sel}^{(\hat{\phi})}(E'_h/\mathbb{Q}) = 2$, from which the result follows immediately. □

Corollary 1. *The Mordell-Weil groups $E_h(\mathbb{Q})$, $E'_h(\mathbb{Q})$ and $\bar{E}_h(\mathbb{Q})$ have rank zero.*

Proof. This is a consequence of the formula (see, for example, [21, page 91])

$$2^{\mathrm{rank}_{\mathbb{Q}}(E_h)} = \frac{\#\mathrm{im}(\alpha)\#\mathrm{im}(\alpha')}{4}.$$

Since E'_h and $\bar{E}_h$ are isogenous to E_h, these also have rank zero over $\mathbb{Q}$. □

3.3. Descent by 3-Isogeny

We now compute $\mathrm{Sel}^{(\psi)}(E/\mathbb{Q})$. Corollary 1 guarantees that $E_h(\mathbb{Q})$ has rank zero and our choice of Equation (6) shows that $E_h(\mathbb{Q})$ does not have 3-torsion. Thus non-zero elements of $\mathrm{Sel}^{(\psi)}(E_h/\mathbb{Q})$ cannot come from points on $\bar{E}_h(\mathbb{Q})/\phi(E(\mathbb{Q}))$.

Theorem 4. $\mathrm{Sel}^{(\psi)}(E/\mathbb{Q})$ *consists of* 9 *elements and is isomorphic to* $Ш(E_h/\mathbb{Q})[3]$.

Proof. The lower bound for $\#\mathrm{Sel}^{(\psi)}(E/\mathbb{Q})$ comes from Theorem 3. The only quantities yet unknown are the real periods of E and $\bar{E}$. We again use (9). Both the real kernel and the real cokernel of ψ are trivial, so we need only compute ω_{E_h} and $\psi^*\omega_{\bar{E}_h}$. A minimal model of $\bar{E}_h$ is given by $y^2 = x^3 + 8(3x-(h-2)(h-6)^2)^2$. Now write $A := 8$ and $B := (h-2)(h-6)^2$. The explicit form (1) of ψ then gives

$$\begin{aligned}\psi^*\omega_{\bar{E}_h} = \psi^*\left(\frac{d\xi}{2\eta}\right) &= \frac{d\left(3^{-3}x^{-2}(6y^2+6AB^2-3x^3-2Ax^2)\right)}{2\cdot 3^{-3}y(8AB^2-x^3-4ABx)x^{-3}}\\ &= \frac{x^3 d\left(x^{-2}(6\left(x^3+A(x-B)^2\right)+6AB^2-3x^3-2Ax^2)\right)}{2y(8AB^2-x^3-4ABx)}\\ &= \frac{x^3(3+12ABx^{-2}-24AB^2x^{-3})dx}{2y(8AB^2-x^3-4ABx)}\\ &= \frac{-3dx}{2y} = -3\omega_{E_h}.\end{aligned}$$

Equation (9) in the present situation reads

$$\frac{\Omega_{E_h}}{\Omega_{\bar{E}_h}} = \frac{1}{1}\cdot\frac{1}{3}$$

so Theorem 3 yields

$$\frac{\#\mathrm{Sel}^{(\hat{\psi})}(\bar{E}_h/\mathbb{Q})}{\#\mathrm{Sel}^{(\psi)}(E_h/\mathbb{Q})} = \frac{\#\bar{E}_h(\mathbb{Q})[\hat{\psi}]\Omega_{E_h}\prod_p c_{E_h,p}}{\#E_h(\mathbb{Q})[\psi]\Omega_{\bar{E}_h}\prod_p c_{\bar{E}_h,p}} = \frac{1\cdot 1\cdot 16}{1\cdot 3\cdot 48} = \frac{1}{9}.$$

As a consequence, $9|\#\mathrm{Sel}^{(\psi)}(E_h/\mathbb{Q})$.

An upper bound on $\#\mathrm{Sel}^{(\psi)}(E_h/\mathbb{Q})$ is obtained by arithmetic in $L = \mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\bar{E}_h[\hat{\psi}])$. We compute $L(S_{E,\psi},3)^*$, the elements of $L^\times/L^{\times 3}$ that only ramify at the bad primes and have cube norm. Recall that by Lemma 2 the inert primes and the principally ramified primes of $\mathcal{O}_L$ cannot contribute. The prime 2 is ramified in $\mathcal{O}_L = \mathbb{Z}[\sqrt{2}]$, a principal ideal domain. Since 2 is non-square in $\mathbb{F}_3$, $\mathbb{F}_h$, $\mathbb{F}_{h-6}$ and $\mathbb{F}_{h-8}$, these primes are inert. Only the prime $h-2 = (k+l\sqrt{2})(k-l\sqrt{2})$ is split. Thus $L(S_{E,\psi},3)^*$ is generated by $(k+l\sqrt{2})^2(k-l\sqrt{2})$ and the fundamental unit $1+\sqrt{2}$, but this gives $\#L(S_{E,\psi},3)^* = 9$. We conclude

$$9 \le \#\mathrm{Sel}^{(\psi)}(E/\mathbb{Q}) \le \#L(S_{E,\psi},3)^* \le 9.$$

Since $E_h(\mathbb{Q})$ and $\bar{E}_h(\mathbb{Q})$ have rank zero and no 3-torsion, $\bar{E}_h(\mathbb{Q})/\psi(E(\mathbb{Q}))$ is trivial. The exact sequence

$$0 \to \bar{E}_h(\mathbb{Q})/\psi(E_h(\mathbb{Q})) \to \mathrm{Sel}^{(\psi)}(E_h/\mathbb{Q}) \to Ш(E_h/\mathbb{Q})[\psi] \to 0$$

then implies $\mathrm{Sel}^{(\psi)}(E_h/\mathbb{Q}) \cong Ш(E_h/\mathbb{Q})[\psi]$. Finally, since $\mathrm{Sel}^{(\hat{\psi})}(E'_h/\mathbb{Q})$ is trivial by Theorem 3, we conclude $Ш(E_h/\mathbb{Q})[\psi] \cong Ш(E_h/\mathbb{Q})[3]$, which finishes the proof. □

Corollary 2. *Assume h is a positive integer that satisfies the following conditions:*

- $h \equiv 3 \bmod 8$.
- *h, $h-2$, $h-6$ and $h-8$ are prime numbers.*

Then the plane cubic

$$C^h_{1+\sqrt{2}}\colon 3w^2z + 2z^3 + w^3 + 6wz^2 + 2(h-2)^2(h-8) = 12z^2 - 6w^2$$

has a point over every completion of $\mathbb{Q}$, but not over $\mathbb{Q}$ itself.

Proof. The equation for $C^h_{1+\sqrt{2}}$ is an application of Theorem 2 with $t = 1+\sqrt{2}$. We use a minimal model of $\bar{E}_h$ with $\bar{A} = 72$ and $\bar{B} = (h-2)^2(h-8)/3$ to reduce the size of the coefficients. Theorem 4 asserts that these curves represent non-trivial elements of the Tate-Shafarevich group, meaning that they violate the Hasse principle. □

Observe that $h = 19$ satisfies the conditions, hence the homogeneous space

$$C^{19}_{1+\sqrt{2}}\colon 3w^2z + 2z^3 + w^3 + 6wz^2 + 6358 = 12z^2 - 6w^2$$

violates the Hasse principle. By Magma [4], the values $h < 120000$ (besides $h = 19$) that satisfy our conditions are:

$$3259, 5659, 15739, 21019, 55339, 67219, 69499, 79699, 88819, 99139, 116539, 119299.$$

Not surprisingly, the set $\{E_h\}$ gives a sparser set of elements of order 3 in a Tate-Shafarevich group than the list in [11]. An advantage is that the examples coming from $\{E_h\}$ are easy to generate; one only needs the congruence $h \equiv 3 \bmod 8$ and the primality of h, $h-2$, $h-6$ and $h-8$.

Acknowledgements. It is our pleasure to thank Steffen Müller and Damiano Testa for their interest in this work, and for valuable suggestions.

References

[1] N. Aoki, On the Tate–Shafarevich group of semistable elliptic curves with a rational 3-torsion, *Acta Arith.* **112** (2004), 209–227.

[2] A. Beauville, Les familles stables de courbes elliptiques sur $\mathbf{P}^1$ admettant quatre fibres singulières, *C. R. Math. Acad. Sci. Paris Sér. I* **294** (1982)(19), 657–660.

[3] M. Bhargava, A positive proportion of plane cubics fail the Hasse principle, 2014, preprint, http://arxiv.org/abs/1402.1131.

[4] W. Bosma, J. Cannon, and C. Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.* **24** (1997), 235–265.

[5] J. W. S. Cassels, Arithmetic on Curves of genus 1. VI. The Tate-Šafarevič group can be arbitrarily large, *J. Reine Angew. Math.* **214-215** (1964), 65–70.

[6] 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.

[7] H. Cohen, *Number theory. Vol. I. Tools and Diophantine equations*, vol. 239 of *Graduate Texts in Mathematics*, Springer-Verlag, New York, 2007.

[8] H. Cohen and F. Pazuki, Elementary 3-descent with a 3-isogeny, *Acta Arith.* **140** (2009), 369–404.

[9] M. DeLong, A formula for the Selmer group of a rational three-isogeny, *Acta Arith.* **105** (2002), 119–131.

[10] T. Dokchitser and V. Dokchitser, Local invariants of isogenous elliptic curves, *Trans. Amer. Math. Soc.* **367** (2015), 4339–4358.

[11] T. A. Fisher, Elements of order 3 in the Tate-Shafarevich group, online tables, https://www.dpmms.cam.ac.uk/~taf1000/g1data/order3.html.

[12] T. A. Fisher, Some examples of 5 and 7 descent for elliptic curves over **Q**, *J. Eur. Math. Soc. (JEMS)* **3** (2001), 169–201.

[13] T. A. Fisher, The Cassels–Tate pairing and the Platonic solids, *J. Number Theory* **98** (2003), 205–255.

[14] R. Kloosterman and E. F. Schaefer, Selmer groups of elliptic curves that can be arbitrarily large, *J. Number Theory* **99** (2003), 148–163.

[15] K. Oguiso and T. Shioda, The Mordell-Weil lattice of a rational elliptic surface, *Comment. Math. Univ. St. Pauli* **40** (1991), 83–99.

[16] B. Poonen, An explicit algebraic family of genus-one curves violating the Hasse principle, *J. Théor. Nombres Bordeaux* **13** (2001), 263–274.

[17] A. Schinzel and W. Sierpiński, Sur certaines hypothèses concernant les nombres premiers, *Acta Arith.* **4** (1958), 185–208.

[18] M. Schütt and T. Shioda, *Mordell-Weil Lattices*, vol. 70 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge.*, Springer-Verlag, New York, 2019.

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

[20] J. H. Silverman, *The Arithmetic of Elliptic Curves*, vol. 106 of *Graduate Texts in Mathematics*, Springer-Verlag, New York, 1986.

[21] J. H. Silverman and J. T. Tate, *Rational points on elliptic curves*, Springer-Verlag, Heidelberg New York Dordrecht London, 1992.

[22] J. T. Tate, Algorithm for determining the type of a singular fiber in an elliptic pencil, in B. Birch and W. Kuyk, editors, *Modular Functions of One Variable IV*, Springer-Verlag, Berlin Heidelberg, 1975, pp. 33–52.

[23] J. Top, Descent by 3-isogeny and 3-rank of quadratic fields, *Advances in Number Theory: The Proceedings of the Third Conference of the Canadian Number Theory Association* (1993), 303–317.

[24] J. Top, Fermat's 'primitive solutions' and some arithmetic of elliptic curves, *Indag. Math. (N.S.)* **4** (1993), 211–222.

[25] J. Top and N. Yui, Explicit equations of some elliptic modular surfaces, *Rocky Mountain J. Math.* **37** (2007), 663–687.