

VISUALISING SHA[2] IN ABELIAN SURFACES

NILS BRUIN

ABSTRACT. Given an elliptic curve E_1 over a number field K and an element s in its 2-Selmer group, we give two different ways to construct infinitely many Abelian surfaces A such that the homogeneous space representing s occurs as a fibre of A over another elliptic curve E_2 . We show that by comparing the 2-Selmer groups of E_1 , E_2 and A , we can obtain information about $\text{III}(E_1/K)[2]$ and we give examples where we use this to obtain a sharp bound on the Mordell-Weil rank of an elliptic curve.

As a tool, we give a precise description of the m -Selmer group of an Abelian surface A that is m -isogenous to a product of elliptic curves $E_1 \times E_2$.

One of the constructions can be applied iteratively to obtain information about $\text{III}(E_1/K)[2^n]$. We give an example where we use this iterated application to exhibit an element of order 4 in $\text{III}(E_1/\mathbb{Q})$.

1. INTRODUCTION

The Mordell-Weil theorem states that the rational points on an elliptic curve E over a number field K form a finitely generated commutative group. Given $m \in \mathbb{Z}$ with $m \geq 2$, there is an in-principle effectively computable object—the m -Selmer group $S^{(m)}(E/K)$ —that provides an upper bound on the free rank of $E(K)$, the m -Selmer rank of E/K . This bound is not sharp in general. The m -torsion of the Shafarevich-Tate group, $\text{III}(E/K)[m]$, measures the failure of the m -Selmer rank to provide a sharp bound on the rank of $E(K)$. If $\text{III}(E/K)[m]$ has no elements of order m , then the Selmer rank equals the rank of $E(K)$.

Suppose E_1 and E_2 are elliptic curves over a number field K with $E_1[m] \simeq E_2[m]$. We write $\Delta := E_1[m] \simeq E_2[m]$. One can construct an Abelian surface $A = E_1 \times E_2 / \Delta_E$, where $\Delta_E \subset \Delta \times \Delta \subset E_1 \times E_2$ is the anti-diagonal in $\Delta \times \Delta \simeq E_1[m] \times E_2[m]$. We investigate how $\text{III}(E_1/K)[m]$ and $\text{III}(E_2/K)[m]$ are related to $\text{III}(A/K)[m]$. In particular, we prove

Theorem 1.1. *Let E_1 be an elliptic curve over a number field K . Let $\xi \in \text{III}(E_1/K)[2]$. There are infinitely many explicitly constructible elliptic curves E_2 , not isomorphic over \overline{K} , such that ξ is in the kernel of the natural map $\text{III}(E_1/K)[2] \rightarrow \text{III}(A/K)[2]$.*

Received by the editor February 2, 2002 and, in revised form, September 13, 2002.

2000 *Mathematics Subject Classification.* Primary 11G05; Secondary 14G05, 14K15.

Key words and phrases. Visualisation, Shafarevich-Tate group, elliptic curve, two-descent, Mordell-Weil group.

The research in this paper was funded by the Pacific Institute for the Mathematical Sciences, Simon Fraser University, the University of British Columbia, and the School of Mathematics of the University of Sydney.

A nonconstructive proof of the existence of A can be found in [18]. In fact, the proof there applies to any $\xi \in H^1(K, E[2])$.

One obvious choice is to take E_2 to be a quadratic twist of E_1 . Suppose that E_2 is the twist of E_1 by $d \in K^*$. Then E_2 is isomorphic to E_1 over $K(\sqrt{d})$ and the Abelian surface A is the Weil restriction of E_1 with respect to $K(\sqrt{d})/K$.

Theorem 1.2. *Let E be an elliptic curve over a number field K . Let $\xi \in \text{III}(E/K)[2]$. There are infinitely many explicitly constructible quadratic extensions $K(\sqrt{d})/K$ such that ξ is in the kernel of $\text{III}(E/K)[2] \rightarrow \text{III}(E/K(\sqrt{d})[2])$.*

A nonconstructive proof that any $\xi \in \text{III}(E/\mathbb{Q})[m]$, with $m \geq 2$, is visualised in an Abelian variety of dimension at most m can be found in [1]. We can use Theorem 1.2 to get an explicit version of this fact for $m = 2^n$ and an arbitrary base field.

Corollary 1.3. *Let E be an elliptic curve over a number field K . Let $\xi \in \text{III}(E/K)[2^n]$. Then there is an explicitly constructible 2^n -dimensional Abelian variety A over K with a nonconstant map $E \rightarrow A$ such that ξ vanishes under the natural map $H^1(K, E) \rightarrow H^1(K, A)$.*

Proof. Let $K_0 = K$ and $\xi_0 = \xi$. By Theorem 1.2, there is a quadratic extension K_1 of K such that $2^{(n-1)}\xi_0 \in \text{III}(E/K_0)[2]$ vanishes in $\text{III}(E/K_1)$. Consequently, the image ξ_1 of ξ_0 in $\text{III}(E/K_1)$ satisfies $\xi_1 \in \text{III}(E/K_1)[2^{n-1}]$. We repeat this construction for $i = 0, 1, \dots$ to obtain a quadratic extension K_i of K_{i-1} such that the image ξ_i of ξ_{i-1} in $\text{III}(E/K_i)$ satisfies $2^{n-i}\xi_i = 0$. It follows that $\xi_n = 0$ in $\text{III}(E/K_n)$.

Let $A = \mathfrak{R}_{K_n/K}E$ be the Weil restriction of scalars in the sense of [3, §7.6]. Then A is a 2^n -dimensional Abelian variety, and there is a nonconstant morphism $E \rightarrow A$. By Shapiro’s lemma ([2, Proposition 2]) we have, canonically, $H^1(K_n, E) \simeq H^1(K, A)$, and the image of ξ under $H^1(K, E) \rightarrow H^1(K, A)$ is indeed trivial. \square

For the proofs of Theorems 1.1 and 1.2, we analyse the cohomology of nonsimple Abelian surfaces. In particular, let K be a number field and let A be an Abelian surface over K with a degree m isogeny $\varphi : A \rightarrow E_1 \times E_2$ to a product of elliptic curves E_1 and E_2 . We show that the Selmer groups satisfy the equalities

$$\begin{aligned} S^{(\varphi)}(A/K) &= S^{(m)}(E_1/K) + S^{(m)}(E_2/K), \\ S^{(\hat{\varphi})}(E_1 \times E_2/K) &= S^{(m)}(E_1/K) \cap S^{(m)}(E_2/K). \end{aligned}$$

As a motivation and an illustration, we consider a simple example that illustrates both theorems and shows how the constructions can be applied to exhibit nontrivial elements in $\text{III}(E/K)[2]$.

Consider the elliptic curve over \mathbb{Q} given by

$$E_1 : y^2 = x^3 - 22x^2 + 21x + 1.$$

From the 2-Selmer group of E_1/\mathbb{Q} , we see that $\text{rk}E_1(\mathbb{Q}) \leq 4$. A simple computation shows that $\langle (0, 1), (1, 1) \rangle \subset E_1(\mathbb{Q})$ forms a free subgroup of rank 2. An analytic rank computation and a 3-descent (see [21]) yield convincing evidence that the rank of E_1 really is 2, which means that $\text{III}(E_1/\mathbb{Q})[2] \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Proposition 1.4. $\text{rk}E_1(\mathbb{Q}) = 2$.

Proof 1. Consider

$$E_2 : 2y_2^2 = x^3 - 22x^2 + 21x + 1.$$

The group $\langle (1/2, 7/4), (1/8, 41/32) \rangle \subset E_2(\mathbb{Q})$ is free of rank 2, so $\text{rk}E_2(\mathbb{Q}) \geq 2$. From the 2-Selmer group of E_2/\mathbb{Q} we deduce that $\text{rk}E_2(\mathbb{Q}) \leq 4$. From

$$\text{rk}E_1(\mathbb{Q}(\sqrt{2})) = \text{rk}E_1(\mathbb{Q}) + \text{rk}E_2(\mathbb{Q}),$$

it follows that $\text{rk}E_1(\mathbb{Q}(\sqrt{2})) \geq 4$. From the 2-Selmer group of $E_1/\mathbb{Q}(\sqrt{2})$, we also find 4 as an upper bound for $\text{rk}E_1(\mathbb{Q}(\sqrt{2}))$. Consequently, we have $\text{rk}E_1(\mathbb{Q}) = \text{rk}E_2(\mathbb{Q}) = 2$. \square

Proof 2. Consider the smooth complete curve corresponding to the affine model

$$C : y_1^2 = -y_0^6 - 19y_0^4 + 20y_0^2 + 1.$$

Let

$$E_2 : v^2 = u^3 + 20u^2 - 19u - 1.$$

The curve C of genus 2 covers E_1 by $(y_0, y_1) \mapsto (x, y_1) = (-y_0^2 + 1, y_1)$ and E_2 by $(y_0, y_1) \mapsto (u, v) = (1/y_0^2, y_1/y_0^3)$. It follows that Jac_C is isogenous to $E_1 \times E_2$ and that

$$\text{rkJac}_C(\mathbb{Q}) = \text{rk}E_1(\mathbb{Q}) + \text{rk}E_2(\mathbb{Q}).$$

From $\langle (1, 1), (2, 7), (5, 23) \rangle \subset E_2(\mathbb{Q})$ and the 2-Selmer group of E_2/\mathbb{Q} , we deduce that $\text{rk}E_2(\mathbb{Q}) = 3$. A 2-descent on Jac_C/\mathbb{Q} yields $\text{rkJac}_C(\mathbb{Q}) = 5$, so it follows that $\text{rk}E_1(\mathbb{Q}) = 2$. \square

Both proofs make use of essentially the same construction. We find an elliptic curve E_2 and an Abelian surface A isogenous to $E_1 \times E_2$. Using a 2-descent we show that the rank of $A(\mathbb{Q})$ is smaller than the sum of the rank bounds we get from a 2-descent on E_1 and E_2 separately. In this article we analyse when this construction may yield nontrivial results and we give an explicit construction for E_2 .

The phenomenon used in the first proof was already observed in [19] and the phenomenon used in the second proof was already observed in [16].

2. SELMER GROUPS

2.1. Abstract definition of the Selmer group. In this section we recall the abstract definition of the Selmer group associated to an isogeny between Abelian varieties. We review the relation of the size of Selmer groups to the rank of an Abelian variety over a number field. Given isogenies φ and $\hat{\varphi}$ such that $\varphi \circ \hat{\varphi}$ is multiplication-by- m , we indicate how one can use the full multiplication-by- m Selmer group to improve the rank bound obtained from the φ - and $\hat{\varphi}$ -Selmer groups.

Consider two Abelian varieties A and B of equal dimension over a field K of characteristic 0 and a finite morphism (an *isogeny*) $\varphi : A \rightarrow B$. Let $\Delta = \ker \varphi$. Galois-cohomology yields

$$0 \rightarrow B(K)/\varphi A(K) \rightarrow H^1(K, \Delta) \rightarrow H^1(K, A).$$

If K is a number field, then we can approximate the image of $B(K)/\varphi A(K)$ in $H^1(K, \Delta)$ by determining the elements of $H^1(K, \Delta)$ that are in the image everywhere locally. This constitutes the φ -Selmer group of A over K . The following

diagram with exact rows illustrates the definition. The products are taken over all primes p of K .

$$\begin{array}{ccccccc}
 0 & \longrightarrow & B(K)/\varphi A(K) & \longrightarrow & H^1(K, \Delta) & \longrightarrow & H^1(K, A) \\
 & & \downarrow & & \downarrow & & \downarrow \\
 0 & \longrightarrow & \prod_p B(K_p)/\varphi A(K_p) & \longrightarrow & \prod_p H^1(K_p, \Delta) & \longrightarrow & \prod_p H^1(K_p, A)
 \end{array}$$

The φ -Selmer group of A over K is defined to be the subgroup of $H^1(K, \Delta)$ consisting of cocycles that map to elements in $\prod_p H^1(K_p, \Delta)$ that have a pre-image in $\prod_p B(K_p)/\varphi A(K_p)$. It is defined by the exact sequence

$$0 \rightarrow S^{(\varphi)}(A/K) \rightarrow H^1(K, \Delta) \rightarrow \prod_p H^1(K_p, A).$$

The Selmer group contains $B(K)/\varphi A(K)$ and therefore provides a bound on its size. Unfortunately, there may be 1-cocycles of A that are trivial everywhere locally (i.e., they are mapped to a coboundary under $H^1(K, A) \rightarrow H^1(K_p, A)$ for all primes p of K), but are not coboundaries themselves. They form the *Shafarevich-Tate group*

$$0 \rightarrow \text{III}(A/K) \rightarrow H^1(K, A) \rightarrow \prod_p H^1(K_p, A).$$

The subgroup of everywhere locally trivial cocycle classes that are in the kernel of $H^1(K, A) \rightarrow H^1(K, B)$ measures the failure of $S^{(\varphi)}(A/K)$ to bound $B(K)/\varphi A(K)$ sharply:

$$0 \rightarrow B(K)/\varphi A(K) \rightarrow S^{(\varphi)}(A/K) \rightarrow \text{III}(A/K)[\varphi] \rightarrow 0.$$

Although, from the description given here, it is not clear that either $S^{(\varphi)}(A/K)$ or $\text{III}(A/K)[\varphi]$ are effectively computable, we will see shortly that the Selmer group is finite and effectively computable in the situations we are interested in. First we explain why φ -Selmer groups help in computing the rank of $A(K)$.

First suppose that φ is multiplication by m , so that $B = A$. By the Mordell-Weil theorem we know that $A(K) \simeq \mathbb{Z}^r \times A(K)_{\text{tors}}$, where $A(K)_{\text{tors}} \subset A(K)$ is the finite subgroup of elements of finite order. Consequently,

$$A(K)/mA(K) = (\mathbb{Z}/m\mathbb{Z})^r \times A(K)_{\text{tors}}/mA(K)_{\text{tors}}.$$

Since the group $A(K)_{\text{tors}}$ is generally relatively easy to compute, one can deduce the free rank r from the size of $A(K)/mA(K)$.

We have $\#A(K)_{\text{tors}}/mA(K)_{\text{tors}} = \#A[m](K)$. For an isogeny $\varphi : A \rightarrow B$ such that $\hat{\varphi}\varphi = m$ with m prime, we define, analogous to the fact that $m^{\text{rk}A(K)}\#A[m](K) = \#A(K)/mA(K)$, the number $s =: \text{rk}S^{(\varphi)}(A/K)$ by $m^s\#A[\varphi](K) = \#S^{(\varphi)}(A/K)$. This definition allows us to state the relation between the rank of an Abelian variety and its m -Selmer group concisely.

Proposition 2.1. *Let A be an Abelian variety over a number field K , and let p be a prime number. Then $\text{rk}A(K) \leq \text{rk}S^{(p)}(A/K)$ and equality holds precisely if $\#\text{III}(A/K)[p] = 1$.*

Selmer groups of other isogenies also give information about the rank by combining them with the Selmer group of dual isogeny.

Lemma 2.2. *Let $\varphi : A \rightarrow B$ be an isogeny of Abelian varieties over a field K such that $\#B(K)/\varphi A(K)$ and $\#A(K)/\hat{\varphi}B(K)$ are finite groups. Suppose that $\varphi\hat{\varphi} = m$. Then*

$$\frac{\#A(K)/mA(K)}{\#A[m](K)} = \frac{\#B(K)/\varphi A(K)}{\#A[\varphi](K)} \frac{\#A(K)/\hat{\varphi}B(K)}{\#B[\hat{\varphi}](K)}.$$

Proof. Consider the exact sequence of finite groups

$$\begin{aligned} 0 \rightarrow A[\varphi](K) \rightarrow A[m](K) \rightarrow B[\hat{\varphi}](K) \\ \rightarrow B(K)/\varphi A(K) \rightarrow A(K)/mA(K) \rightarrow A(K)/\hat{\varphi}B(K) \rightarrow 0. \quad \square \end{aligned}$$

Corollary 2.3. *Let $\varphi : A \rightarrow B$ be an isogeny of Abelian varieties over a number field K such that $\hat{\varphi}\varphi = p$ for some prime p . Then*

$$\text{rk}A(K) \leq \text{rk}S^{(\varphi)}(A/K) + \text{rk}S^{(\hat{\varphi})}(B/K),$$

and equality holds precisely if $\#\text{III}(A/K)[\varphi] = \#\text{III}(B/K)[\hat{\varphi}] = 1$.

2.2. Two-Selmer groups of elliptic curves. In this section we give two alternative descriptions of $H^1(K, E[2])$ and the map $E(K)/2E(K) \rightarrow H^1(K, E[2])$, which we will use in Sections 4 and 5.

To find $S^{(2)}(E/K) \subset H^1(K, E[2])$, one needs some further nontrivial computations; see for instance [25].

We consider an elliptic curve

$$E : y^2 = x^3 + a_2x^2 + a_4x + a_6 = F(x)$$

over a field K of characteristic 0. First we describe $H^1(K, E[2])$. We write $M_K = K[x]/(F(x))$ and let $\theta \in M$ denote the residue class of x ; i.e., $F(\theta) = 0$. We write M_K^* for the multiplicative group of the algebra M_K , $M_K^{*2} \subset M_K^*$ for the squares, and $M'_K \subset M_K^*$ for the kernel of $M_K^* \xrightarrow{N_{M_K/K}} K^*/K^{*2}$.

Theorem 2.4 ([7], [8, Chapter 15]). *Let K be a field of characteristic 0, and let E and M_K be as above. Then*

$$H^1(K, E[2]) \simeq M'_K/M_K^{*2}.$$

Under this isomorphism, the map

$$\mu : E(K)/2E(K) \rightarrow H^1(K, E[2])$$

is induced by

$$\begin{aligned} E(K) &\rightarrow M_K^*, \\ (x, y) &\mapsto x - \theta \quad \text{if } F(x) \neq 0. \end{aligned}$$

To facilitate the evaluation of the map μ , we use the following lemma, which can be proved by a straightforward computation.

Lemma 2.5. *Let $E : y^2 = x^3 + a_2x^2 + a_4x + a_6 = F(x)$ be an elliptic curve over a field K , and let θ be a root of $F(x)$ in $K[x]/F(x)$. Let $e_1, e_2 \in E(K)$ and $e_3 := e_1 + e_2$. Then*

$$(x(e_1) - \theta)(x(e_2) - \theta)(x(e_3) - \theta) = C(e_1, e_2)^2,$$

where $C(e_1, e_2)$ is a symmetric algebraic function of e_1, e_2 .

Corollary 2.6. *Let $E : y^2 = x^3 + a_2x^2 + a_4x + a_6 = F(x)$ be an elliptic curve over a field K and let L be a separable quadratic extension of K , with $\sigma : L \rightarrow L$ conjugation over K . Then the following diagram commutes.*

$$\begin{CD} E(L) @>\mu>> M'_L/M_L^{*2} \\ @V e \mapsto e + \sigma e VV @VV N_{M_L/M_K} V \\ E(K) @>\mu>> M'_K/M_K^{*2} \end{CD}$$

Proof. The only possible obstruction to the commutativity of this diagram is that $M_L^{*2} \cap M_K^*$ may be larger than M_K^{*2} . However, using Lemma 2.5, we see that, for e such that $C(e, \sigma e)$ is well defined and nonzero, $\mu(e + \sigma e)\mu(e)\mu(\sigma e) = C(e, \sigma e)^2$, where $C(e, \sigma e)$ is σ -invariant and therefore in M_K^* . For the special e such that $C(e, \sigma e)$ has a pole or a zero, one can verify the statement separately, which we will leave to the reader. □

An alternative interpretation of $H^1(K, E[2])$ can be obtained by considering unramified covers of E with a certain Galois-group. First we review some terminology. Let $\pi : D \rightarrow C$ be a nonconstant morphism of smooth complete absolutely irreducible curves over K such that $\#\text{Aut}_{\overline{K}}(D/C) = \text{deg } \varphi$, i.e., a *Galois cover*. We say that $\pi' : D' \rightarrow C$ is a *twist* of $D \xrightarrow{\pi} C$ if there is an isomorphism $\psi : D \rightarrow D'$ over \overline{K} such that $\pi = \pi' \circ \psi$. If ψ is already defined over K , then $D \xrightarrow{\pi} C$ and $D' \xrightarrow{\pi'} C$ are considered the same.

Theorem 2.7 ([23]). *Let $\pi : D \rightarrow C$ be a Galois cover over a number field K . Then*

$$H^1(K, \text{Aut}_{\overline{K}}(D/C)) \simeq \{ \text{Twists of } D \xrightarrow{\pi} C \}$$

as pointed sets with $\text{Gal}(\overline{K}/K)$ -action.

In particular, $H^1(K, E[2]) \simeq \{ \text{Twists of } E \xrightarrow{2} E \}$. Given an element $\delta \in M'_K$, we can find the corresponding cover of E explicitly. We refer to it as T_δ to distinguish it from the representation as an element of M'_K/M_K^{*2} . First, we fix a representation of M_K over K . Let $\{1, \theta, \alpha\}$ be a basis of M_K as a K -vector space. If $F(x)$ is irreducible over K , then one can take $\alpha = \theta^2$. We find a model of T_δ by composing $T_\delta \rightarrow E$ with $E \xrightarrow{x} \mathbb{P}^1$. A heuristic motivation for the construction below is that if $P \in E(K)$ with $\mu(P) = \delta$, then T_δ should have a rational point above P , so in the composed cover $T_\delta \rightarrow \mathbb{P}^1$ we have a rational point above $x(P)$.

If $\mu(P) = \delta$, then there are $u_0, u_1, u_2 \in K$ such that

$$x(P) - \theta = \delta(u_0 + \theta u_1 + \alpha u_2)^2.$$

We expand the right-hand side with respect to the K -basis of M_K . Let

$$Q_{\delta,i}(u_0, u_1, u_2) \in K[u_0, u_1, u_2]$$

be the quadratic forms so that

$$\delta(u_0 + \theta u_1 + \alpha u_2)^2 = Q_{\delta,0}(u_0, u_1, u_2) + \theta Q_{\delta,1}(u_0, u_1, u_2) + \alpha Q_{\delta,2}(u_0, u_1, u_2).$$

We find that $Q_{\delta,0}(u_0, u_1, u_2) = x(P)$, $Q_{\delta,1}(u_0, u_1, u_2) = -1$ and $Q_{\delta,2} = 0$.

Independent of whether there exists a point $P \in E(K)$ with $\mu(P) = \delta$, we take u_0, u_1, u_2 to be variables and define the $Q_{\delta,i}$ as above. Using these forms, we define

two projective varieties over K . Let

$$\begin{aligned} L_\delta &: Q_{\delta,2}(u_0, u_1, u_2) = 0, \\ T_\delta &: Q_{\delta,2}(u_0, u_1, u_2) = 0 \text{ and } Q_{\delta,1}(u_0, u_1, u_2) = -u_3^2. \end{aligned}$$

Note that the map $(u_0 : u_1 : u_2 : u_3) \mapsto (u_0 : u_1 : u_2)$ induces a degree 2 cover $T_\delta \rightarrow L_\delta$. This cover is ramified at the points where $u_3 = 0$. Consequently, the ramification locus lies above those $(u_0 : u_1 : u_2)$ satisfying $Q_{\delta,1}(u_0, u_1, u_2) = Q_{\delta,2}(u_0, u_1, u_2) = 0$. On both L_δ and T_δ we define the function

$$x(u_0, u_1, u_2) = -\frac{Q_{\delta,0}(u_0, u_1, u_2)}{Q_{\delta,1}(u_0, u_1, u_2)}.$$

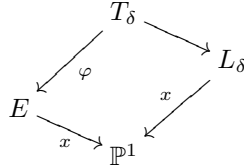
Since $\delta \in M'_K$, we can choose $d \in K^*$ such that $d^2 = N_{M_K/K}(\delta)$. On T_δ , we define

$$y_d(u_0, u_1, u_2) = \frac{d}{u_3} N_{M_K[u_0, u_1, u_2]/K[u_0, u_1, u_2]}(u_0 + \theta u_1 + \alpha u_2).$$

We find that T_δ covers E by

$$\begin{aligned} \varphi_\delta : \quad T_\delta &\quad \rightarrow \quad E \\ (u_0 : u_1 : u_2 : u_3) &\mapsto (x(u_0, u_1, u_2), y_d(u_0, u_1, u_2, u_3)). \end{aligned}$$

The defined varieties are in fact connected curves and they fit in the following diagram.



We see that $T_\delta = E \times_{\mathbb{P}^1} L_\delta$. One can check that $T_\delta \rightarrow E$ is unramified. Consequently, $\text{genus}(T_\delta) = 1$. Furthermore, $T_\delta \rightarrow L_\delta$ is ramified at four geometric points, so $\text{genus}(L_\delta) = 0$. We have $\delta \in S^{(2)}(E/K)$ precisely if $T_\delta(K_p)$ is nonempty for all primes p of K . Consequently, $L_\delta(K_p)$ is also nonempty for all primes p of K , and by the Hasse-Minkowski theorem we have $L_\delta \simeq \mathbb{P}^1$. Choose a parametrisation $t \mapsto (u_0(t), u_1(t), u_2(t))$ of L_δ . This yields a model

$$T_\delta : u_3^2 = R(t) = -Q_{\delta,1}(u_0(t), u_1(t), u_2(t)).$$

We recover the description of $S^{(2)}(E/K)$ as a set of classes of quartics that have a point everywhere locally, as used in some formulations of the 2-descent method for elliptic curves over \mathbb{Q} ([24], [12], [11]).

Proposition 2.8. *Let E, K, M'_K , and T_δ be defined as above. The isomorphism*

$$H^1(K, E[2]) \rightarrow \text{Twists}(E \xrightarrow{2} E)$$

is induced by

$$\begin{aligned} M'_K &\rightarrow \{ \text{Covers of } E \}, \\ \delta &\mapsto T_\delta. \end{aligned}$$

3. NONSIMPLE ABELIAN SURFACES

In this section we consider an Abelian surface A , isogenous to the product of two elliptic curves E_1 and E_2 . Although in Sections 4 and 5 we will only be considering 2-isogenies, the results in this section are valid for any m -isogeny where $m \geq 2$.

Let $m > 1$ be an integer, and let E_1 and E_2 be elliptic curves over a field K of characteristic 0 with $E_1[m] \simeq E_2[m]$ as group schemes over K . We write $\Delta := E_1[m] \simeq E_2[m]$ and $\Delta_E \subset E_1[m] \times E_2[m]$ for the anti-diagonal embedding. Let $A := (E_1 \times E_2)/\Delta_E$.

We have $p^* : E_1 \rightarrow A$ induced by $P \mapsto (P, 0) \in E_1 \times E_2$ and $q^* : E_2 \rightarrow A$ induced by $Q \mapsto (0, Q) \in E_1 \times E_2$. Note that $\Delta \subset (E_1 \times E_2)[m]$, so the multiplication-by- m map on $E_1 \times E_2$ factors through A . This factorisation induces the maps $p_* : A \rightarrow E_1 \times E_2 \rightarrow E_1$ and $q_* : A \rightarrow E_1 \times E_2 \rightarrow E_2$. It is straightforward to check that $p_* \circ p^* = m|_{E_1}$ and $q_* \circ q^* = m|_{E_2}$.

$$\begin{array}{ccccccc}
 & & & & 0 & & \\
 & & & & \downarrow & & \\
 & & & & \Delta_A & & \\
 & & & & \downarrow & & \\
 0 & \longrightarrow & \Delta_E & \longrightarrow & E_1 \times E_2 & \xrightarrow{p^*+q^*} & A \longrightarrow 0 \\
 & & & & \searrow^m & & \downarrow^{p_* \times q_*} \\
 & & & & & & E_1 \times E_2 \\
 & & & & & & \downarrow \\
 & & & & & & 0
 \end{array}$$

It follows that the isogeny $p_* \times q_* : A \rightarrow E_1 \times E_2$ is dual to $p^* + q^* : E_1 \times E_2 \rightarrow A$ and that its kernel Δ_A fits in the short exact sequence

$$0 \rightarrow \Delta_E \rightarrow (E_1 \times E_2)[m] \rightarrow \Delta_A \rightarrow 0$$

and, since $(E_1 \times E_2)[m] \simeq \Delta \times \Delta$, that $\Delta_A \simeq \Delta$.

Here and further, for a field K , we write \overline{K} for the separable closure of K and $\text{Gal}(K)$ for the automorphism group of \overline{K} over K .

Theorem 3.1. *Let E_1 and E_2 be elliptic curves over a field K of characteristic 0 with isomorphic m -torsion $E_1[m] = \Delta = E_2[m]$. Let $A = (E_1 \times E_2)/\Delta_E$, where Δ_E is the anti-diagonal embedding of Δ in $E_1[m] \times E_2[m]$ and $\mu_1 : E_1 \rightarrow H^1(K, \Delta)$ and $\mu_2 : E_2 \rightarrow H^1(K, \Delta)$. Then*

- (a) $\mu_1 \circ p_* = -\mu_2 \circ q_*$.
- (b) *The sequence*

$$E_1 \times E_2(K) \xrightarrow{p^*+q^*} A(K) \xrightarrow{\frac{\mu_1 p_*}{\mu_2 q_*}} H^1(K, \Delta)$$

is exact.

- (c) *Let $\mu_1 + \mu_2 : E_1(K) \times E_2(K) \rightarrow H^1(K, \Delta)$ denote the map $(e_1, e_2) \rightarrow \mu_1(e_1) + \mu_2(e_2)$. The sequence*

$$A(K) \xrightarrow{p_* \times q_*} E_1 \times E_2(K) \xrightarrow{\mu_1 + \mu_2} H^1(K, \Delta)$$

is exact.

Proof. (a) Let $a \in A(K)$, and put $\delta_1 = \mu_1 p_*(a)$ and $\delta_2 = \mu_2 q_*(a)$. By definition of μ_1 , there is a point $e_1 \in E_1(\overline{K})$ such that $me_1 = p_*(a)$ and for any $\sigma \in \text{Gal}(K)$, we have $\sigma e_1 = e_1 + \delta_1(\sigma)$. Similarly, there is a point $e_2 \in E_2(\overline{K})$ with $me_2 = q_*(a)$ and $\sigma e_2 = e_2 + \delta_2(\sigma)$.

Since $p_* \circ (p^* \times q^*) = m|_{E_1}$ and $q_* \circ (p^* \times q^*) = m|_{E_2}$, we see that $p^*(e_1) + q^*(e_2) - a = T \in \Delta_A(\overline{K})$. It follows that $\sigma T - T = p^*\delta_1(\sigma) + q^*\delta_2(\sigma)$. Using the identifications $E_1[m] = \Delta = E_2[m]$ via p^* and q^* , we see that $\delta_1 + \delta_2$ is a 1-coboundary.

(b) It is immediate that $\mu_1 p_* \circ (p^* + q^*) = \mu_1 \circ m|_{E_1} = 0$. On the other hand, if $a \in A(K)$ with $\mu_1 p_*(a) = 0$, then we can apply the same construction as in (a), but now we can choose $e_1 \in E_1(K)$ and $e_2 \in E_2(K)$. It follows that $p^*(e_1) + q^*(e_2) - a = T \in \Delta_A(K)$, so $(p^* + q^*)(e_1 - T, e_2) = a$.

(c) Using (a), we see that $(\mu_1 + \mu_2) \circ (p_* \times q_*) = 0$. To obtain exactness, consider $e_1 \in E_1(K)$ and $e_2 \in E_2(K)$ with $\mu_1(e_1) = -\mu_2(e_2)$. There are points $e_3 \in E_1(\overline{K})$ and $e_4 \in E_2(\overline{K})$ such that $me_3 = e_1$, $me_4 = e_2$, and there is a point $T \in \Delta(\overline{K})$ such that $p^*(\sigma e_3 - e_3) + q^*(\sigma e_4 - e_4) = \sigma T - T$ for all $\sigma \in \text{Gal}(K)$. It follows that $a = p^*(e_3) + q^*(e_4) - T$ satisfies $\sigma a - a = 0$, so $a \in A(K)$ and $p_*(a) = e_1$ and $q_*(a) = e_2$. \square

Corollary 3.2. *Let E_1 and E_2 be elliptic curves over a number field K with $\Delta := E_1[m] \simeq E_2[m]$. Let $p^* + q^* : E_1 \times E_2 \rightarrow A = (E_1 \times E_2)/\Delta$ and let $p_* \times q_* : A \rightarrow E_1 \times E_2$ be the dual isogeny. Then*

- (a) $S^{(p_* \times q_*)}(A/K) = S^{(m)}(E_1/K) + S^{(m)}(E_2/K)$,
- (b) $S^{(p^* + q^*)}((E_1 \times E_2)/K) = S^{(m)}(E_1/K) \cap S^{(m)}(E_2/K)$.

Proof. For all places p of K , apply Theorem 3.1 to the completion K_p of K and use the definition of the Selmer group. \square

From Corollary 3.2, and the fact that $m|_{E_1}$, $m|_{E_2}$, $p^* + q^*$, and $p_* \times q_*$ all have kernels isomorphic to Δ , it follows that for m prime

$$\text{rk}S^{(p_* \times q_*)}(A/K) + \text{rk}S^{(p^* + q^*)}((E_1 \times E_2)/K) = \text{rk}S^{(m)}(E_1/K) + \text{rk}S^{(m)}(E_2/K).$$

Furthermore, it is immediate that

$$S^{(m)}((E_1 \times E_2)/K) = S^{(m)}(E_1/K) \times S^{(m)}(E_2/K),$$

so descents via $m|_{E_1 \times E_2}$, the dual isogenies $m|_{E_1} \times 1|_{E_2}$ and $1|_{E_1} \times m|_{E_2}$, and the dual isogenies $p^* + q^*$ and $p_* \times q_*$ all give rise to the same bound on $\text{rk}(E_1 \times E_2)(K) = \text{rk}E_1(K) + \text{rk}E_2(K)$.

The Selmer group $S^{(m)}(A/K)$ may yield different information. The map $p_* \times q_* : A[m] \rightarrow \Delta$ induces a homomorphism N that fits in the following commutative diagram with exact rows.

$$\begin{array}{ccccc} A(K) & \xrightarrow{m} & A(K) & \xrightarrow{\nu} & H^1(K, A[m]) \\ \downarrow p_* \times q_* & & \parallel & & \downarrow N \\ E_1 \times E_2(K) & \xrightarrow{p^* + q^*} & A(K) & \xrightarrow{\mu_1 p_*} & H^1(K, \Delta) \end{array}$$

This allows us to obtain a sharper bound on $\#A(K)/(p^*E_1(K) + q^*E_2(K))$. Furthermore, using that $\mu_1 p_*(A(K)) = N\nu(A(K)) = \mu_2 q_*(A(K))$, we find that $N\nu(A(K)) = \mu_1(E_1(K)) = \mu_2(E_2(K))$. Consequently,

Lemma 3.3. *Let $A, E_1,$ and E_2 be as defined above over a number field $K,$ with $N : H^1(K, A[m]) \rightarrow H^1(K, \Delta).$ Then*

$$\mu_1(E_1(K)) \cap \mu_2(E_2(K)) \subset S^{(m)}(E_1/K) \cap S^{(m)}(E_2/K) \cap NS^{(m)}(A/K).$$

Now we analyse when Lemma 3.3 may provide a strictly sharper bound than $S^{(p^*+q^*)}((E_1 \times E_2)/K).$ This only applies if $\text{III}(E_1/K)[m]$ or $\text{III}(E_2/K)[m]$ is nontrivial. Suppose that $\delta \in H^1(K, \Delta)$ represents a cocycle with a nontrivial image under $H^1(K, \Delta) \rightarrow H^1(K, E_1),$ but which is trivial in $H^1(K_p, E_1)$ for any place p of $K.$ If we combine the Galois-cohomology of $E_1 \xrightarrow{m} E_1, E_2 \xrightarrow{m} E_2,$ and $0 \rightarrow E_1 \xrightarrow{p^*} A \xrightarrow{q^*} E_2 \rightarrow 0,$ we obtain the following commutative diagram with exact rows and columns.

$$\begin{array}{ccccccc}
 & & & & E_2(K) & \xrightarrow{q^*} & A(K) \\
 & & & & \downarrow m & & \downarrow q_* \\
 & & & & E_2(K) & \xlongequal{\quad} & E_2(K) \\
 & & & & \downarrow \mu_2 & & \downarrow \\
 E_1(K) & \xrightarrow{m} & E_1(K) & \xrightarrow{\mu_1} & H^1(K, \Delta) & \longrightarrow & H^1(K, E_1) \\
 p_* \downarrow & & \parallel & & \downarrow & & \downarrow \\
 A(K) & \xrightarrow{p_*} & E_1(K) & \longrightarrow & H^1(K, E_2) & \longrightarrow & H^1(K, A)
 \end{array}$$

If δ does not vanish in $H^1(K, A),$ it leads to a nontrivial element in

$$\text{III}(A/K)[p_* \times q_*] \subset \text{III}(A/K)[m].$$

The space $H^1(K, E_1)$ is isomorphic to the set of principally homogeneous spaces of E_1 over K (see [23, Theorem X.3.6]). As such the map $E_2(K) \rightarrow H^1(K, E_1)$ corresponds to $q_*^{-1};$ i.e., takes the fibre of $q_* : A \rightarrow E_2$ over a rational point on $E_2.$ Following [13], we say that an element of $H^1(K, E_1)$ that occurs as such a fibre is *visualised* in $A.$ We formulate this observation as a corollary.

Corollary 3.4. *A cocycle $\xi \in H^1(K, E_1)$ vanishes in $H^1(K, A)$ precisely if ξ is in the image of $E_2(K).$*

We see that a necessary condition for Lemma 3.3 to yield an improved rank bound is that some nontrivial elements of $\text{III}(E_1/K)[m] \subset H^1(K, E_1)$ occur as fibres of A over $E_2(K).$

4. QUADRATIC WEIL RESTRICTIONS OF ELLIPTIC CURVES

In this section, we interpret Theorem 1.2 in terms of the construction explained in Section 3 and we give a proof. Informally, the idea is the following. Recall from Section 2.2 that an element $\delta \in H^1(K, E[2])$ is in the image of $E(K)/2E(K),$ and therefore maps to 0 in $H^1(K, E)$ precisely if a curve T_δ has a K -rational point. One obvious way to force a rational point on T_δ is by extension of the base field. As is noted in that same section, if $\delta \in S^{(2)}(E/K),$ then T_δ has a model $u_3^2 = R(t),$ where $R(t)$ is a quartic polynomial. For any value $t_0 \in K$ and $L := K(\sqrt{R(t_0)}),$ the set $T_\delta(L)$ is nonempty. By taking the *Weil restriction of scalars* $A = \mathfrak{R}_{L/K}E,$ we find ourselves in the situation of Section 3 with $m = 2.$ We make this explicit.

Let K be a field of characteristic 0. Consider the elliptic curves

$$\begin{aligned} E_1 : \quad y_1^2 &= x^3 + a_2x^2 + a_4x + a_6 = F(x), \\ E_2 : \quad dy_2^2 &= x^3 + a_2x^2 + a_4x + a_6 \end{aligned}$$

over K , where $d \in K^*$ is not a square. Let $L = K(\sqrt{d})$. As curves over L , we have $E_1 \simeq E_2$ by $(x, y_1) = (x, \sqrt{d}y_2)$. We write $E(L)$ for $E_1(L) \simeq E_2(L)$. We will use the model of E_1 for E , but the reader should note that the construction is essentially symmetric in E_1 and E_2 .

Obviously, $\Delta = E_1[2] \simeq E_2[2]$ as a K -Galois module. Applying Theorem 2.4, we find that the maps $E_i(K)/2E_i(K) \rightarrow H^1(K, \Delta)$ are induced by

$$\begin{array}{ccc} \mu_1 : E_1(K) & \rightarrow & M'_K \\ (x, y_1) & \mapsto & (x - \theta) \end{array} \quad \begin{array}{ccc} \mu_2 : E_2(K) & \rightarrow & M'_K \\ (x, y_2) & \mapsto & d(x - \theta) \end{array} .$$

We consider the Weil restriction $A = \mathfrak{R}_{L/K}E$ in the sense of [3, §7.6]. It will suffice for our purposes to describe $A(\overline{K})$ as a $\text{Gal}(\overline{K})$ -module. We define $A(\overline{K}) = E_1(\overline{K}) \times E_1(\overline{K})$ as a set, but with a twisted Galois action. For $\sigma \in \text{Gal}(\overline{K})$ and $(e_1, e_2) \in A(\overline{K})$, we define

$$\sigma(e_1, e_2) = \begin{cases} (\sigma e_1, \sigma e_2) & \text{if } \sigma \in \text{Gal}(L) \subset \text{Gal}(\overline{K}), \\ (\sigma e_2, \sigma e_1) & \text{otherwise.} \end{cases}$$

Let $\sigma \in \text{Gal}(\overline{K}) \setminus \text{Gal}(L)$. It is straightforward to check that $E(L) \simeq A(K)$ via $e \mapsto (e, \sigma e)$. We identify $E_2(\overline{K})$ with $E_1(\overline{K})$ via $(x, y_1) = (x, \sqrt{d}y_2)$. Under this identification, we have

$$E_2(K) = \{e \in E_1(\overline{K}) : e = -\sigma e \text{ for } \sigma \in \text{Gal}(\overline{K}) \setminus \text{Gal}(L)\}.$$

As maps between Galois modules, we obtain

$$\begin{array}{ccc} p^* : E_1(\overline{K}) & \rightarrow & A(\overline{K}) \\ e & \mapsto & (e, e) \end{array} \quad \begin{array}{ccc} q^* : E_1(\overline{K}) & \rightarrow & A(\overline{K}) \\ e & \mapsto & (e, -e), \end{array}$$

$$\begin{array}{ccc} p_* : A(\overline{K}) & \rightarrow & E_1(\overline{K}) \\ (e_1, e_2) & \mapsto & e_1 + e_2 \end{array} \quad \begin{array}{ccc} q_* : A(\overline{K}) & \rightarrow & E_1(\overline{K}) \\ (e_1, e_2) & \mapsto & e_1 - e_2. \end{array}$$

It is straightforward to check that this places us in the situation of Section 3 with $m = 2$.

By Shapiro’s lemma and Theorem 2.4, we have $H^1(K, A[2]) = H^1(L, E_1[2]) = M'_L/M_L^*$. We write $\nu : A(K)/2A(K) \rightarrow M'_L/M_L^*$ for the corresponding map, where we use $A(K) \simeq E(L)$ and the map $\text{res}_L^K \mu_1 : E_1(L) \rightarrow M'_L$.

The obvious map $N = N_{M_L/M_K} : M_L^* \rightarrow M_K^*$ completes the explicit description of the ingredients of Corollary 3.2 and Lemma 3.3, as the following lemma shows.

Lemma 4.1. *With the definitions above,*

$$\mu_1 p_* = N\nu = \mu_2 q_*.$$

Proof. We prove the first equality. The second follows by symmetry. Suppose $a \in A(K)$ and let $e \in E(L)$ be the corresponding point. Then $\mu_1 p_*(a) = \mu_1(e + \sigma e)$, where $\sigma \in \text{Gal}(\overline{K})$ acts nontrivially on L . By Corollary 2.6, this equals $N\nu(a)$. \square

Proof of Theorem 1.2. Let $\delta \in S^{(2)}$ be a cocycle representing ξ . Recall from Section 2.2 that L_δ is a curve of genus 0 with points everywhere locally. Consequently, L_δ is isomorphic to \mathbb{P}^1 and has infinitely many rational points. Each point lifts to a quadratic point on the genus 1 curve T_δ . Thus $T_\delta(L)$ is nonempty for some

quadratic extension of K . Since the number of L -rational points of T_δ of height bounded by B is at most logarithmic in B and the number of K -rational points on L of height bounded by B is polynomial in B , we see that this construction leads to infinitely many distinct quadratic extensions L of K .

Note that, given $t \in L_\delta(K)$, we can take $d = F(x(t))$. Then, $E^{(d)} : dy_2^2 = F(x)$ has a rational point over $x(t)$. Therefore, the fibre product $T_\delta^{(d)} = E^{(d)} \times_{\mathbb{P}^1} L_\delta$ has a rational point over $x(t)$ as well. Since, over $L = K(\sqrt{d})$, the curves E and $E^{(d)}$ are isomorphic, we see that $T_\delta(L) \simeq T_\delta^{(d)}(L)$ is nonempty.

5. BI-ELLIPTIC CURVES OF GENUS 2

The previous section shows that for an elliptic curve E over a number field K , any element of $\text{III}(E/K)[2]$ can be visualised in infinitely many distinct Abelian surfaces. The Abelian surfaces constructed there are all isomorphic to $E \times E$ over \overline{K} , however. In this section we prove Theorem 1.1; i.e., that we can insist on nonisomorphic surfaces over \overline{K} .

Let K be a field of characteristic 0 and consider

$$\begin{aligned} E_1 : \quad y_1^2 &= x^3 + a_2x^2 + a_4x + a_6 = F(x), \\ L_0 : \quad dy_0^2 &= x - a, \\ E_2 : \quad dy_2^2 &= (x - a)F(x). \end{aligned}$$

We consider these curves to be covers of the same \mathbb{P}^1 corresponding to x . The fibre product $C = E_1 \times_{\mathbb{P}^1} L_0 = E_2 \times_{\mathbb{P}^1} L_0$ is a curve of genus 2 with model

$$C : y_1^2 = F(dy_0^2 + a).$$

The curve C is a double cover of both E_1 and E_2 by

$$\begin{aligned} p : \quad C &\rightarrow E_1 \\ (y_0, y_1) &\mapsto (x, y_1) = (dy_0^2 + a, y_1), \\ q : \quad C &\rightarrow E_2 \\ (y_0, y_1) &\mapsto (x, y_2) = (dy_0^2 + a, y_0y_1). \end{aligned}$$

We write $\infty \in L_0$ and $\infty \in E_1$ for the unique points on L_0 and E_1 above $\infty \in \mathbb{P}^1$. Choosing an arbitrary but fixed labelling, we write $\infty^+, \infty^- \in C$ for the two points on C above $\infty \in L_0$. The points ∞^+ and ∞^- are rational or quadratic conjugate over K , depending on d being a square. The unique point on E_1 above $\infty \in \mathbb{P}^1$ is denoted by ∞ as well.

For a curve C over K , we represent an element of $A := \text{Jac}_C$ by the corresponding divisor class $[\sum_{i=1}^r n_i P_i]$, where $P_i \in C(\overline{K})$ and $n_i \in \mathbb{Z}$, with $n_1 + \dots + n_r = 0$. Since we only consider curves of genus 1 and 2, we have that any point in $\text{Jac}_C(K)$ can be represented by the class of a K -rational divisor, i.e. a $\text{Gal}(K)$ -stable formal linear combination of points in $C(\overline{K})$.

We identify E_1 with Jac_{E_1} via $e_1 \mapsto [e_1 - \infty]$ and E_2 with Jac_{E_2} via $e_2 \mapsto [e_2 - (a, 0)]$. The map p gives rise to maps between Abelian varieties

$$\begin{aligned} p_* : \quad \text{Jac}_C &\rightarrow E_1 \\ [\sum_{i=1}^r n_i P_i] &\mapsto \sum_{i=1}^r n_i p(P_i), \\ p^* : \quad E_1 &\rightarrow \text{Jac}_C \\ e &\mapsto \left[\sum_{P \in p^{-1}\{e\}} P - \infty^+ - \infty^- \right], \end{aligned}$$

and similarly for q . It is straightforward to check that these maps satisfy the assumptions in Section 3, and we adopt the notation from that section.

Let $\theta \in M_K = K[x]/F(x)$ be such that $F(\theta) = 0$. Using Theorem 2.4 we find

$$\begin{aligned} \mu_1 : E_1(K)/2E_1(K) &\rightarrow M'_K/M_K^{*2} \\ (x, y_1) &\mapsto (x - \theta) \quad \text{if } y_1 \neq 0, \end{aligned}$$

and by transforming E_2 into Weierstrass form

$$\begin{aligned} \mu_2 : E_2(K)/2E_2(K) &\rightarrow M'_K/M_K^{*2} \\ (x, y_1) &\mapsto \begin{cases} d(x - a)(a - \theta)F(a)(x - \theta) & \text{if } y_2 \neq 0, \\ dF(a)(a - \theta) & \text{if } x = \infty. \end{cases} \end{aligned}$$

Any point $a \in A(K)$ has a representative $a = [(y_{0,1}, y_{1,1}) + (y_{0,2}, y_{1,2}) - \infty^+ - \infty^-]$, where $(y_{0,1}, y_{1,1})$ and $(y_{0,2}, y_{1,2})$ are either rational points of C or quadratic conjugates. In fact this representative is unique if $a \neq 0$. Let $\mathcal{M}_K = K[y_0]/F(dy_0^2 + a)$ and let Θ be the class of y_0 in \mathcal{M}_K . Similar to the map μ we defined in Theorem 2.4, we define

$$\begin{aligned} \tilde{\nu} : A(K) &\rightarrow \mathcal{M}'_K/K^*\mathcal{M}_K^{*2} \\ a &\mapsto (y_{0,1} - \Theta)(y_{0,2} - \Theta). \end{aligned}$$

Unfortunately, the map $\tilde{\nu}$ does not completely correspond to $\nu : A(K) \rightarrow H^1(K, A[2])$. The kernel may be a little bigger.

Lemma 5.1 ([10], [25]). *With the definitions above, there is a map $H^1(K, A[2]) \rightarrow \mathcal{M}'_K/K^*\mathcal{M}_K^{*2}$ that makes the following diagram with exact row commutative.*

$$\begin{array}{ccc} A(K) & \xrightarrow{2} & A(K) \xrightarrow{\nu} H^1(K, A[2]) \\ & & \searrow \tilde{\nu} \quad \downarrow \\ & & \mathcal{M}'_K/K^*\mathcal{M}_K^{*2} \end{array}$$

For a number field K , we define the *fake Selmer group* $\tilde{S}^{(2)}(A/K)$ to be the image of $S^{(2)}(A/K)$ under this map $H^1(K, A[2]) \rightarrow \mathcal{M}'_K/K^*\mathcal{M}_K^{*2}$. This group is effectively computable (see [25]). Fortunately, the map $N : H^1(K, A[2]) \rightarrow H^1(K, \Delta)$ factors through $\mathcal{M}'_K/K^*\mathcal{M}_K^{*2}$. So for applying Lemma 3.3, knowing the fake Selmer group suffices.

Lemma 5.2. *With the definitions above, the identity*

$$\mu_1 p_* = N_{\mathcal{M}_K/M_K} \tilde{\nu} = \mu_2 q_*$$

holds.

Proof. We prove the first equality. The second follows by symmetry. Suppose $a = [(y_{0,1}, y_{1,1}) + (y_{0,2}, y_{1,2}) - \infty^+ - \infty^-] \in A(K)$. We have $p_*(a) = (x_1, y_{1,1}) + (x_2, y_{1,2}) \in E_1(K)$, where $x_1 = dy_{0,1}^2 + a$ and $x_2 = dy_{0,2}^2 + a$. Generically, by Corollary 2.6, we have

$$\mu_1 p_*(a) = (x_1 - \theta)(x_2 - \theta) = N_{\mathcal{M}_K/M_K} \tilde{\nu}(a).$$

The special points where the middle expression is singular can be tested separately. □

Proof of Theorem 1.1. Let $\delta \in H^1(K, E_1[2])$ be a cocycle mapping to ξ . Since T_δ , as defined in Section 2.2, has points everywhere locally, the subcover $L_\delta \simeq \mathbb{P}^1$. Take a rational point $t_0 \in L_\delta$.

For some $a \in K$ with $F(a) \neq 0$ and $d \in K^*$, we consider

$$E_2 : dy_2^2 = (x - a)F(x).$$

The cover of E_2 corresponding to $\delta \in H^1(K, E_2[2]) \simeq H^1(K, E_1[2])$ is $L_\delta \times_{\mathbb{P}^1} E_2$. If we choose $d = (x(t_0) - a)F(x(t_0))$, then this cover has a rational point above $x(t_0)$. We see that we are completely free in choosing a , which gives us infinitely many distinct curves E_2 over \overline{K} with the desired property.

Remark. By letting $a \rightarrow \infty$, we get the construction from Section 4 as a limit of the construction in this section.

6. ALGORITHMIC CONSIDERATIONS

The fact that the constructions presented in Sections 4 and 5 are completely explicit and that the Selmer groups in Lemma 3.3 are effectively and often practically computable, suggests a probabilistic algorithm to prove nontriviality of $\text{III}(E/K)[2]$ for an elliptic curve E over a number field K .

Let $\delta \in M_K^*$ represent an element of $S^{(2)}(E/K)$ for which we suspect that $T_\delta(K)$ is empty, i.e., δ represents a nontrivial element in $\text{III}(E/K)[2]$.

- (1) Choose $t_0 \in L_\delta(K)$, and compute $x_0 = x(t_0)$.
- (2) Take $E_2 : dy_2 = F(x)$ or $E_2 : dy_2^2 = (x - a)F(x)$ such that E_2 has a rational point above x_0 .
- (3) Test if $\delta \in S^{(2)}(E/K) \cap S^{(2)}(E_2/K) \cap NS^{(2)}(A/K)$.
- (4) If this is the case, go to (1); otherwise, δ indeed represents a nontrivial element in $\text{III}(E/K)[2]$.

Of course, if T_δ has a rational point, then this algorithm will not terminate. Unfortunately, otherwise we cannot prove it will either. We cannot exclude that $\delta \notin NS^{(2)}(A/K)$. In practice, the procedure appears to have a rather high success rate, though.

Of course, if δ represents a nontrivial element of $2\text{III}(E/K)[4]$, then the algorithm will not terminate either. The image of δ in $\text{III}(A/K)[2]$ will indeed be trivial, but a class which corresponds to $\frac{1}{2}\delta$ will just map to a nontrivial element in $\text{III}(A/K)[2]$. However, if we have $A = \mathfrak{R}_{L/K}E$ as in Section 4, then $\text{III}(A/K)[2] \simeq \text{III}(E/L)[2]$. We can use the same algorithm to prove that the image of that class in $\text{III}(A/K)$ indeed is nontrivial. See Example 4 in Section 7.

Theoretically, this procedure is weaker than attempting a sequence of 2-power descents, as suggested in, e.g., [23, Proposition X.4.12]. The latter is guaranteed to work if $\text{III}(E/K)[2^r] = 0$ for some r . The procedure above needs that and then is still only probabilistic. See, e.g., Example 2 in Section 7.

For practical applications, this approach has the benefit that one computes 2-Selmer groups of an elliptic curve over a tower of quadratic extensions, rather than higher Selmer groups over a constant base field. See, for instance, [20] for 4-descents and [9] for second descents, that yield the same information as 4-descents. See also [22] for a complexity analysis of 2-descents and [15] and [21] for odd p -descents.

The computation of a 2-Selmer group of an elliptic curve over an arbitrary number field (although for higher degree fields is prohibitively laborious) is effectively

implemented in MAGMA [4] and KASH [14] using the routines for computing S -unit groups originally by Hess [17]. See [6] and [5]. Such an implementation is presently missing for higher 2-power Selmer groups.

7. EXAMPLES

We give some examples as an illustration of the practicality of the methods described in this article. Only a brief outline of the computations is given to show the reader what phenomena occur. For more detailed results, we refer the reader to [6], which contains a complete transcript of the MAGMA [4] sessions leading to the results presented here. If the reader has access to MAGMA, the software to repeat the computations is also included.

Example 1. Mutual visualisation. Consider the curve from Proposition 1.4. A computation shows

$$S^{(2)}(E_1/\mathbb{Q}) = \langle -\theta, 1 - \theta, 1 - 2\theta, 1 - 8\theta \rangle \quad \text{and} \quad \mu_1 \langle (0, 1), (1, 1) \rangle = \langle -\theta, 1 - \theta \rangle.$$

We suspect that $1 - 2\theta$ and $1 - 8\theta$ represent nontrivial elements in $\text{III}(E_1/\mathbb{Q})[2]$. If we follow the procedure above, we write down the curve $L_{1-2\theta}$, find a rational point t_0 on it, and compute $d = F(x(t_0))$. From computational considerations, it is desirable that d has a small square-free part. Instead of trying different t_0 to obtain such a d , we enumerate small x -coordinates and check if the point lifts to $L_{1-2\theta}$.

We find that $L_{1-2\theta}$ has a rational point above $x = \frac{1}{2}$ and that $L_{1-8\theta}$ has a rational point above $x = \frac{1}{8}$. Furthermore, $F(\frac{1}{2}) = 2(\frac{7}{4})^2$ and $F(\frac{1}{8}) = 2(\frac{41}{32})^2$, so if we take $d = 2$ in the construction of Section 4, both elements will be visualised in the Abelian surface A . In fact, we find

$$S^{(2)}(E_1/\mathbb{Q}(\sqrt{2})) = \langle -\theta, 1 - \theta, 1 - 2\theta, 1 - 8\theta \rangle,$$

so

$$NS^{(2)}(E_1/\mathbb{Q}(\sqrt{2})) = \langle 1 \rangle.$$

By Lemma 3.3, we see that $\mu_1(E_1(\mathbb{Q})) \cap \mu_2(E_2(\mathbb{Q})) = \langle 1 \rangle$. Since $\langle -\theta, 1 - \theta \rangle \subset \mu_1(E_1(\mathbb{Q}))$ and $\langle 1 - 2\theta, 1 - 8\theta \rangle \subset \mu_2(E_2(\mathbb{Q}))$, we see that equality must hold.

Example 2. Failed visualisation. In the previous example we were lucky that both elements of $\text{III}(E_1/\mathbb{Q})[2]$ were visualised simultaneously. This need not happen. For the same curve as above, consider $L_{(1-\theta)(1-2\theta)}$. It has a rational point above $\frac{-4}{11}$. Since $F(\frac{-4}{11}) = -11(\frac{113}{121})^2$, it follows that $(1 - \theta)(1 - 2\theta)$ is visualised in the surface constructed according to Section 4 with $d = -11$. As it turns out,

$$S^{(2)}(E_2/\mathbb{Q}) = \mu_2 E_2(\mathbb{Q}) = \langle (1 - \theta)(1 - 2\theta) \rangle$$

and

$$NS^{(2)}(E_1/\mathbb{Q}(\sqrt{-11})) = \langle (1 - \theta)(1 - 2\theta) \rangle.$$

While we know we have visualised a nontrivial element from $\text{III}(E_1/\mathbb{Q})[2]$ from the argument given above, we cannot conclude this from the data computed with $d = -11$.

Example 3. Visualisation using bi-elliptic curves of genus 2. The construction from Section 5 offers two degrees of freedom, giving enhanced flexibility. We again consider the curve $E_1 : y^2 = F(x) = x^3 - 22x^2 + 21x + 1$.

We pick two elements from $S^{(2)}(E/\mathbb{Q})$, say $\delta_1=1-2\theta$ and $\delta_2=-\theta(1-2\theta)(1-8\theta)$. We pick $x_1 = 1/2$ below $L_{\delta_1}(\mathbb{Q})$ and $x_2 = 9/10$ below $L_{\delta_2}(\mathbb{Q})$. We use the construction from Section 5 to obtain an Abelian surface $A = \text{Jac}_C$ in which both δ_1 and δ_2 are visualised. To this end, we determine $a, d \in \mathbb{Q}$ with $d \neq 0$ and $F(a) \neq 0$ such that both $d(x_1 - a)F(x_1)$ and $d(x_2 - a)F(x_2)$ are squares. A priori such a, d might not exist. In that case, one could choose other x_1 and x_2 and try again. While there is no guarantee that this procedure would yield success after finitely many steps, in practice it seems rather easy to find x_1, x_2, a, d with the desired properties. In our case $a = 1, d = -1$ works. Thus δ_1 and δ_2 are visualised in the Abelian surface $A = \text{Jac}_C$ where $C : y_1^2 = -y_0^6 - 19y_0^4 + 20y_0^2 + 1$. We have

$$S^{(2)}(E_1/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^4 \quad \text{and} \quad S^{(2)}(E_2/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^3,$$

with

$$S^{(2)}(E_1/\mathbb{Q}) \cap S^{(2)}(E_2/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^2.$$

Using Stoll’s routines [25] in MAGMA [4], we can compute the fake Selmer group $\tilde{S}^{(2)}(\text{Jac}_C/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^4$ and

$$NS^{(2)}(\text{Jac}_C/\mathbb{Q}) = \langle 21 - \theta \rangle.$$

Writing

$$E_2 : v^2 = u^3 + 20u^2 - 19u - 1, \text{ where } (u, v) = (1/y_0^2, y_1/y_0^3),$$

we find

$$\mu_2\langle(1, 1), (2, 7), (5, 23)\rangle = \langle-\theta(1 - 2\theta), -\theta(1 - 8\theta), 21 - \theta\rangle.$$

By Lemma 3.3, we see that $1 - 2\theta$ and $1 - 8\theta$ in $S^{(2)}(E_1/\mathbb{Q})$ are not in $\mu_1(E_1(\mathbb{Q}))$.

Example 4. Visualisation of 4-torsion. We consider the curve

$$E_1 : y_1^2 = x^3 - 162x^2 + x.$$

This is a model of the curve 1640G3 in [11]. Using a 4-isogeny, one can show that $E_1(\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z}$ and that $\text{III}(E_1/\mathbb{Q})[4] = (\mathbb{Z}/4\mathbb{Z})^2$. We use this curve to illustrate Corollary 1.3, which also applies to curves without any 2-power isogenies.

Let $E_2 : -y_2^2 = x^3 - 162x^2 + x$ and $K = \mathbb{Q}(i) = \mathbb{Q}(\sqrt{-1})$. We consider a subgroup $\langle g_1, \dots, g_8 \rangle \subset H^1(\mathbb{Q}, E[2])$, which contains both $S^{(2)}(E_1/K)$ and $S^{(2)}(E_2/K)$, corresponding to generators chosen by [6] based on [4]. Since we merely want to illustrate Corollary 1.3, we refer the reader to [6] for details and the definitions of the g_i . We find

$$\begin{aligned} S^{(2)}(E_1/\mathbb{Q}) &= \langle g_5, g_6, g_8 \rangle; & \mu_1(0, 0) &= g_5 + g_6 \\ S^{(2)}(E_2/\mathbb{Q}) &= \langle g_6, g_6 + g_8 \rangle &= \mu_2\langle(0, 0), (-9/4, 231/8)\rangle. \end{aligned}$$

In particular, the group $\langle g_6, g_8 \rangle \subset S^{(2)}(E_1/\mathbb{Q})$ is visualised in $\mathfrak{R}_{K/\mathbb{Q}}E_1$. However, we already know that this group represents $2\text{III}(E_1/\mathbb{Q})[4]$. Indeed, writing $\langle h_1, \dots, h_7 \rangle \subset H^1(K, E[2])$, we find

$$S^{(2)}(E_1/K) = \langle h_3, h_4, h_5 + h_6, h_7 \rangle; \text{res}_K^{\mathbb{Q}}\mu_1\langle(0, 0), (-9/4, 231/8i)\rangle = \langle h_4, h_3 \rangle$$

and

$$N_{K/\mathbb{Q}}S^{(2)}(E_1/K) = \langle g_6, g_8 \rangle.$$

Of course, $N_{K/\mathbb{Q}}h_3 = N_{K/\mathbb{Q}}h_4 = 0$.

As suggested in the proof of Corollary 1.3, we pick an element $h = h_4 + h_5 + h_6 \in S^{(2)}(E_1/K)$ such that $N_{K/\mathbb{Q}}h = g_8$ is suspected to represent a nontrivial element in $\text{III}(E/\mathbb{Q})[2]$. We choose

$$E_3 : (i - 2)y_3^2 = x^3 - 162x^2 + x,$$

such that under the map $\mu_3 : E_3(K) \rightarrow H^1(K, E[2])$ we have

$$\mu_3(0, 0) = h \in S^{(2)}(E_3/K).$$

Therefore, putting $L = K(\sqrt{i-2})$, the element $h \in S^{(2)}(E_1/K)$ is visualised in $\mathfrak{R}_{L/K}E_1$. Indeed, we find that

$$N_{L/K}S^{(2)}(E_1/L) = \langle h_4, h_3 + h_5 + h_6 \rangle.$$

Using Lemma 3.3, we find that $\text{res}_K^{\mathbb{Q}}\mu_1(E_1(K)) \cap \mu_3(E_3) \subset N_{L/K}S^{(2)}(E_1/L)$. In particular, it follows that

$$h_5 + h_6 + \langle h_3, h_4 \rangle \cap \text{res}_K^{\mathbb{Q}}\mu_1(E_1(K)) = \emptyset.$$

Since

$$h_5 + h_6 + \langle h_3, h_4 \rangle = \{h \in S^{(2)}(E_1/K) : N_{K/\mathbb{Q}}h = g_8\},$$

we see that $g_8 \notin \mu_1(E_1(\mathbb{Q}))$. It follows that g_8 indeed represents a nontrivial element in $\text{III}(E_1/\mathbb{Q})[2]$. We could give a similar argument for g_6 .

REFERENCES

1. Amod Agashe and William A. Stein, *Visibility of Shafarevich-Tate groups of abelian varieties*, <http://modular.fas.harvard.edu/papers/>, 2001. MR **2003h**:11070
2. M. F. Atiyah and C. T. C. Wall, *Cohomology of groups*, Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965), Thompson, Washington, D.C., 1967, pp. 94–115. MR **36**:2593
3. Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud, *Néron models*, Springer-Verlag, Berlin, 1990. MR **91i**:14034
4. Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993).
5. Nils Bruin, *Algae, a program for 2-Selmer groups of elliptic curves over number fields*, see <http://www.cecm.sfu.ca/~bruin/e11.shar>.
6. ———, *Transcript of computations*, available from <http://www.cecm.sfu.ca/~bruin/vissha>, 2002.
7. J. W. S. Cassels, *Diophantine equations with special reference to elliptic curves*, J. London Math. Soc. **41** (1966), 193–291. MR **33**:7299
8. ———, *Lectures on elliptic curves*, LMS-ST 24, University Press, Cambridge, 1991.
9. ———, *Second descents for elliptic curves*, J. Reine Angew. Math. **494** (1998), 101–127, Dedicated to Martin Kneser on the occasion of his 70th birthday. MR **99d**:11058
10. J. W. S. Cassels and E. V. Flynn, *Prolegomena to a middlebrow arithmetic of curves of genus 2*, LMS-LNS 230, Cambridge University Press, Cambridge, 1996. MR **97i**:11071
11. J. E. Cremona, *Algorithms for modular elliptic curves*, Cambridge University Press, 1992. MR **93m**:11053
12. ———, *Classical invariants and 2-descent on elliptic curves*, J. Symbolic Comput. **31** (2001), no. 1-2, 71–87, Computational algebra and number theory (Milwaukee, WI, 1996). MR **2002a**:11055
13. John E. Cremona and Barry Mazur, *Visualizing elements in the Shafarevich-Tate group*, Experiment. Math. **9** (2000), no. 1, 13–28. MR **2001g**:11083
14. M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner, M. Schörnig, and K. Wildanger, *KANT V4*, J. Symbolic Comput. **24** (1997), no. 3-4, 267–283, Available from <ftp://ftp.math.tu-berlin.de/pub/algebra/Kant/Kash>. MR **99g**:11150

15. Z. Djabri, Edward F. Schaefer, and N. P. Smart, *Computing the p -Selmer group of an elliptic curve*, Trans. Amer. Math. Soc. **352** (2000), no. 12, 5583–5597. MR **2001b**:11047
16. E. V. Flynn and J. Redmond, *Application of covering techniques to families of curves*, J. Number Theory **101** (2003), no. 2, 376–397.
17. Florian Heß, *Zur Klassengruppenberechnung in algebraischen Zahlkörpern*, Diplomarbeit, Technische Universität Berlin, 1996, available from <http://www.math.tu-berlin.de/~kant/publications/diplom/hess.ps.gz>.
18. Tomas Antonius Klenke, *Visualizing elements of order two in the Weil-Châtelet group*, in preparation, 2001.
19. Kenneth Kramer, *Arithmetic of elliptic curves upon quadratic extension*, Trans. Amer. Math. Soc. **264** (1981), no. 1, 121–135. MR **82g**:14028
20. J. R. Merriman, S. Siksek, and N. P. Smart, *Explicit 4-descents on an elliptic curve*, Acta Arith. **77** (1996), no. 4, 385–404. MR **97j**:11027
21. Edward F. Schaefer and Michael Stoll, *How to do a p -descent on an elliptic curve*, see <http://www.math.uni-duesseldorf.de/~stoll/papers/p-descent.dvi>.
22. S. Siksek and N. P. Smart, *On the complexity of computing the 2-Selmer group of an elliptic curve*, Glasgow Math. J. **39** (1997), no. 3, 251–257. MR **99b**:11061
23. Joseph H. Silverman, *The arithmetic of elliptic curves*, GTM 106, Springer-Verlag, 1986. MR **87g**:11070
24. Denis Simon, *Computing the ranks of elliptic curves over number fields*, to appear in LMS JCM. MR **2003g**:11060
25. Michael Stoll, *Implementing 2-descent for Jacobians of hyperelliptic curves*, Acta Arith. **98** (2001), no. 3, 245–277. MR **2002b**:11089

DEPARTMENT OF MATHEMATICS, SIMON FRASER UNIVERSITY, BURNABY, BRITISH COLUMBIA,
CANADA V5A 1S6

E-mail address: bruin@member.ams.org