THE OPEN BOOK SERIES 1

ANTS X
Proceedings of the Tenth
Algorithmic Number Theory Symposium

Explicit 5-descent on elliptic curves

Tom Fisher

msp

THE OPEN BOOK SERIES **1** (2013)
Tenth Algorithmic Number Theory Symposium
dx.doi.org/10.2140/obs.2013.1.395

Explicit 5-descent on elliptic curves

Tom Fisher

We compute equations for genus-one curves representing nontrivial elements of order 5 in the Tate-Shafarevich group of an elliptic curve. We explain how to write the equations in terms of Pfaffians and give examples for elliptic curves over the rationals both with and without a rational 5-isogeny.

1. Introduction

An explicit descent calculation on an elliptic curve E over a number field K computes the Selmer group (attached to some isogeny) and represents its elements by giving equations for the corresponding covering curves. These curves may be used to help search for generators of the Mordell-Weil group $E(K)$ or to exhibit nontrivial elements of the Tate-Shafarevich group $Ш(E/K)$.

Let C be a smooth curve of genus one representing an element of order n in $Ш(E/K)$. Cassels [8] showed that C admits a K-rational divisor D of degree n. So for $n \geq 3$ we may embed $C \subset \mathbb{P}^{n-1}$ by the complete linear system $|D|$. The result is called a *genus-one normal curve of degree* n. For $n \geq 4$ it is well known (see for example [19; 29]) that the homogeneous ideal of such a curve is generated by a vector space of quadrics of dimension $n(n-3)/2$.

The equations for a genus-one normal curve of degree 5 may conveniently be written as the 4×4 Pfaffians of a 5×5 alternating matrix of linear forms. Over the complex numbers this is a classical fact. In general it is a consequence of the Buchsbaum-Eisenbud structure theorem [7; 6] for Gorenstein ideals of codimension 3. In Section 4 we explain how to compute these matrices of linear forms.

The author has been compiling [22] a list of explicit elements of $Ш(E/\mathbb{Q})[5]$ for elliptic curves $E/\mathbb{Q}$ of small conductor (taken from the Cremona database [10; 11]). The equations are computed using either descent by 5-isogeny, full 5-descent, or visibility. We give details of the first two of these methods in Sections 5 and 6,

MSC2010: primary 11G05; secondary 14H52, 14H25.
Keywords: elliptic curves, descent, Selmer groups, Pfaffians.

expanding on the treatments in [17] and [12; 13; 14]. Our use of visibility is described in [20].

2. Background on descent

Let $\phi : E \to E'$ be an isogeny of elliptic curves over K. A *ϕ-covering* of E' is a pair (C, π) where C is a smooth curve of genus one and $\pi : C \to E'$ is a morphism (both defined over K) such that the diagram

$$\begin{tikzcd} C \arrow[d, "\psi"'] \arrow[dr, "\pi"] & \\ E \arrow[r, "\phi"'] & E' \end{tikzcd}$$

commutes for some isomorphism $\psi : C \to E$ defined over $\overline{K}$.

We write $H^i(K, -)$ as a shorthand for $H^i(\mathrm{Gal}(\overline{K}/K), -)$. Taking Galois cohomology of the short exact sequence of $\mathrm{Gal}(\overline{K}/K)$-modules

$$0 \longrightarrow E[\phi] \longrightarrow E \xrightarrow{\phi} E' \longrightarrow 0$$

gives a long exact sequence of abelian groups

$$\cdots \longrightarrow E(K) \xrightarrow{\phi} E'(K) \xrightarrow{\delta} H^1(K, E[\phi]) \longrightarrow H^1(K, E) \longrightarrow \cdots . \qquad (1)$$

The group $H^1(K, E[\phi])$ parametrises the ϕ-coverings of E', up to isomorphism over K. The subgroup of everywhere locally soluble coverings is the *ϕ-Selmer group* $S^{(\phi)}(E/K)$. Likewise the group $H^1(K, E)$ parametrises the torsors (or principal homogeneous spaces) under E, up to isomorphism over K. The subgroup of everywhere locally soluble torsors is the *Tate-Shafarevich group* Ш(E/K). There is then an exact sequence

$$0 \longrightarrow E'(K)/\phi E(K) \xrightarrow{\delta} S^{(\phi)}(E/K) \longrightarrow Ш(E/K)[\phi_*] \longrightarrow 0$$

where $\phi_* :$ Ш$(E/K) \to$ Ш(E'/K) is the map induced by ϕ.

There are two natural ways to construct a rational divisor class on C. Let m be the smallest positive integer such that $E[\phi] \subset E[m]$. Then $D = \psi^*(m \cdot 0_E)$ and $D' = \pi^*(0_{E'})$ are divisors on C of degrees m and $n = \deg \phi$, respectively. A calculation shows that D is linearly equivalent to all its Galois conjugates, whereas D' is already defined over K. For each $\sigma \in \mathrm{Gal}(\overline{K}/K)$ we pick $h_\sigma \in \overline{K}(C)^\times$ with $\mathrm{div}(h_\sigma) = \sigma D - D$. There is then an obstruction map (see [26; 30; 12])

$$\mathrm{Ob} : H^1(K, E[\phi]) \longrightarrow \mathrm{Br}(K) = H^2(K, \overline{K}^\times)$$

that sends the ϕ-covering (C,π) to the class of the 2-cocycle $(\sigma,\tau)\mapsto\sigma(h_\tau)h_\sigma/h_{\sigma\tau}$. Since $H^1(K,\overline{K}(C)^\times)=0$ it follows that D is linearly equivalent to a K-rational divisor if and only if (C,π) has trivial obstruction.

If $\#(E[\phi]\cap E[2])=1$ or 4 then the elements of $E[\phi]$ sum to 0_E, in which case $\phi^*(0_{E'})\sim n\cdot 0_E$ and $D'\sim(n/m)D$.

In this paper we are interested in the following two cases, where we may write C as a genus-one normal curve of degree 5 with hyperplane section D:

(i) ϕ is an isogeny of degree 5 and $(C,\pi)\in H^1(K,E[\phi])$.

(ii) ϕ is multiplication-by-5 on E and $(C,\pi)\in S^{(5)}(E/K)$.

The obstruction is trivial in both cases. In the first case this is because $D\sim D'$, whereas in the second case the proof (which we follow in our calculations) uses the local-to-global principle for the Brauer group.

3. Pfaffians

We recall some basic facts about Pfaffians. Let $A=(a_{ij})$ be an $n\times n$ alternating matrix. If $n=2m$ is even then the *Pfaffian* of A is

$$\operatorname{pf}(A)=\frac{1}{2^m m!}\sum_{\sigma\in S_n}\operatorname{sign}(\sigma)\prod_{i=1}^{m}a_{\sigma(2i-1)\sigma(2i)}. \tag{2}$$

Standard calculations (see [3, §5]) show that $\operatorname{pf}(PAP^T)=\det(P)\operatorname{pf}(A)$ and that $\det(A)=\operatorname{pf}(A)^2$. Since $\det(A)$ in an integer coefficient polynomial in the entries of A, the same must be true of $\operatorname{pf}(A)$. This is used to define the Pfaffian over an arbitrary ring.

Pfaffians, just like determinants, may be expanded along a row. We write $A^{\{i,j\}}$ for the matrix obtained from A by deleting the i-th and j-th rows and columns. It may be shown using (2) that

$$\operatorname{pf}(A)=\sum_{j=2}^{n}(-1)^j a_{1j}\operatorname{pf}(A^{\{1,j\}}).$$

For example, in the 4×4 case we have

$$\operatorname{pf}\begin{pmatrix}0 & a_{12} & a_{13} & a_{14}\\ & 0 & a_{23} & a_{24}\\ & - & 0 & a_{34}\\ & & & 0\end{pmatrix}=a_{12}a_{34}-a_{13}a_{24}+a_{14}a_{23}.$$

Definition 3.1. Let A be an $n\times n$ alternating matrix with n odd. The *row vector of submaximal Pfaffians of* A is $\operatorname{Pf}(A)=(p_1,\dots,p_n)$, where $p_i=(-1)^i\operatorname{pf}(A^{\{i\}})$ and $A^{\{i\}}$ is the matrix obtained by deleting the i-th row and column of A.

Lemma 3.2. *If A is an $n \times n$ alternating matrix with n odd then*

(i) $\mathrm{Pf}(A)A = 0$,

(ii) $\mathrm{Pf}(PAP^T) = \mathrm{Pf}(A)\,\mathrm{adj}(P)$,

(iii) $\mathrm{adj}(A) = \mathrm{Pf}(A)^T\,\mathrm{Pf}(A)$.

Proof. Since we only need the case $n = 5$ (which may be checked by a generic computation) we omit the proof. □

4. Computing genus-one models

A *genus-one model* (of degree 5) is a 5×5 alternating matrix of linear forms in variables $x_1, \dots, x_5$. We write $X_5(K)$ for the space of all genus-one models with coefficients in a field K, and $C_\Phi \subset \mathbb{P}^4$ for the subscheme defined by the 4×4 Pfaffians of $\Phi \in X_5(K)$.

Theorem 4.1. *Let $C \subset \mathbb{P}^4$ be a genus-one normal curve of degree 5 defined over a field K.*

(i) *There exists $\Phi \in X_5(K)$ such that $C = C_\Phi$.*

(ii) *If $\Phi_1, \Phi_2 \in X_5(K)$ with $C = C_{\Phi_1} = C_{\Phi_2}$ then there exist $A \in \mathrm{GL}_5(K)$ and $\mu \in K^\times$ such that $\Phi_2 = \mu A \Phi_1 A^T$.*

Theorem 4.1 is a consequence of the Buchsbaum-Eisenbud structure theorem [7; 6] for Gorenstein ideals of codimension 3. In this section we give a simplified form of the proof and use it to give explicit algorithms for computing Φ and A. These algorithms are needed in our work [19; 20] on the invariant theory of genus-one models.

Example 4.2. Let E be the elliptic curve $y^2 = x^3 + ax + b$. For any $n \geq 3$ we may embed E into $\mathbb{P}^{n-1}$ via the complete linear system $|n \cdot 0_E|$ to give a genus-one normal curve of degree n. If $n = 5$ then the embedding is given by

$$(x_1 : \cdots : x_5) = (1 : x : y : x^2 : xy)$$

and the image is defined by the 4×4 Pfaffians of

$$\begin{pmatrix} 0 & bx_1 & x_5 & x_4 + ax_1 & -x_3 \\ & 0 & -x_4 & -x_3 & x_2 \\ & & 0 & -x_2 & 0 \\ & - & & 0 & -x_1 \\ & & & & 0 \end{pmatrix}.$$

(Since the homogeneous ideal is generated by a 5-dimensional space of quadrics, it suffices to check that the 4×4 Pfaffians are linearly independent and that they vanish on E.)

Let $R = K[x_1, \dots, x_n] = \bigoplus_{d \geq 0} R_d$ be the polynomial ring with its usual grading by degree. Let $R_+ = \bigoplus_{d \geq 1} R_d$ be the irrelevant ideal.

Definition 4.3. Let M be a finitely generated graded R-module. A *graded free resolution* of M is a complex of graded free R-modules

$$F_\bullet : \quad 0 \longrightarrow F_s \xrightarrow{\varphi_s} F_{s-1} \longrightarrow \cdots \longrightarrow F_2 \xrightarrow{\varphi_2} F_1 \xrightarrow{\varphi_1} F_0 \longrightarrow 0$$

that is exact at all terms except F_0, where we have $F_0/\operatorname{im}(\varphi_1) \cong M$. The resolution $F_\bullet$ is *minimal* if $\phi_i(F_i) \subset R_+ F_{i-1}$ for all i.

We shall need the following two facts.

Lemma 4.4. *Let $F_\bullet$ be a minimal graded free resolution of M. Then any graded free resolution of M is a direct sum of $F_\bullet$ and a trivial complex. In particular, $F_\bullet$ is unique up to isomorphism.*

Proof. See [16, §20.1] or [33, §7]. □

Lemma 4.5 (Buchsbaum-Eisenbud acyclicity criterion). *The complex $F_\bullet$ is acyclic (that is, exact at all terms except F_0) if and only if for all $1 \leq i \leq s$,*

$$\operatorname{rank} F_i = \operatorname{rank} \varphi_i + \operatorname{rank} \varphi_{i+1},$$

and the ideal generated by the $r_i \times r_i$ minors of φ_i (where $r_i = \operatorname{rank} \varphi_i$) has codimension at least i.

Proof. See [5, Theorem 1.4.13] or [16, Theorem 20.9]. We use here that R is Cohen-Macaulay, so that the codimension (also called height) of an ideal is the same as the grade (also called depth). □

We follow the convention that maps of graded R-modules preserve the degree. Let $R(d)$ be R as a graded module over itself with degrees shifted by d, that is, $R(d)_e = R_{d+e}$. We use the same notation for maps of R-modules and the matrices that represent them (with respect to the standard bases).

Theorem 4.6. *Let $C \subset \mathbb{P}^4$ be a genus-one normal curve of degree 5 with homogeneous ideal $I = I(C) \subset R = K[x_1, \dots, x_5]$.*

(i) *The minimal graded free resolution of R/I takes the form*

$$0 \longrightarrow R(-5) \xrightarrow{Q^T} R(-3)^5 \xrightarrow{\Phi} R(-2)^5 \xrightarrow{P} R \longrightarrow 0. \tag{3}$$

(*This means that $P = (p_1, \dots, p_5)$ and $Q = (q_1, \dots, q_5)$ are vectors of quadrics and Φ is a 5×5 matrix of linear forms.*)

(ii) *The K-vector space*

$$\{B \in \operatorname{Mat}_5(K) \mid \Phi B \text{ is alternating}\}$$

is 1-dimensional and contains a nonsingular matrix.

(iii) *If* Φ *is alternating then* P *and* Q *are scalar multiples of* $\mathrm{Pf}(\Phi)$.

Proof. The conclusions of the theorem are unchanged if we extend our field K, so we may assume K is algebraically closed. Then C is an elliptic curve, and up to translation any two divisors on C of the same degree are linearly equivalent. So we may change coordinates on $\mathbb{P}^4$ so that $C = C_\Phi$ where Φ is as given in Example 4.2. (If K has characteristic 2 or 3, we use the more general formula in [19, §6].) By Lemma 3.2(i) there is a complex

$$0 \longrightarrow R(-5) \xrightarrow{P^T} R(-3)^5 \xrightarrow{\Phi} R(-2)^5 \xrightarrow{P} R \longrightarrow 0 \tag{4}$$

with $P = \mathrm{Pf}(\Phi)$. Since P is not identically zero we have $\mathrm{rank}(\Phi) = 4$ and $\mathrm{rank}(P) = 1$. By Lemma 3.2(iii) the ideals generated by the 4×4 Pfaffians of Φ and the 4×4 minors of Φ have the same radical. Since $C \subset \mathbb{P}^4$ has codimension 3, the conditions of Lemma 4.5 are satisfied and so (4) is the minimal graded free resolution of R/I. This proves (i) and shows by Lemma 4.4 that for any resolution (3) there exist $A_1, A_2 \in \mathrm{GL}_5(K)$ such that $A_1 \Phi A_2$ is alternating. Replacing Φ by $\Phi A_2 A_1^{-T}$ we may assume for the proof of (ii) that Φ is alternating.

Suppose that both Φ and ΦB are alternating for some $B \in \mathrm{Mat}_5(K)$. Then $P\Phi = P\Phi B = 0$ and $\Phi P^T = \Phi B P^T = 0$. Since the sequence (3) is exact it follows that P^T and BP^T are scalar multiples of Q^T. Therefore B is a scalar matrix. This proves (ii). To prove (iii) we apply the same argument starting with the identity $\mathrm{Pf}(\Phi)\Phi = 0$. □

Theorem 4.6 not only proves Theorem 4.1(i) but gives the following algorithm for computing a genus-one model Φ with $C = C_\Phi$. We start with a basis $p_1, \dots, p_5$ for the space of quadrics vanishing on C. We then solve by linear algebra for a matrix Ψ whose columns are a basis for the space of all 5-tuples of linear forms $(\ell_1, \dots, \ell_5) \in R^5$ satisfying $\sum_{i=1}^5 \ell_i p_i = 0$. Finally we take $\Phi = \Psi B$ where $B \in \mathrm{Mat}_5(K)$ is any nonzero matrix satisfying $\Psi B = -B^T \Psi^T$.

To prove Theorem 4.1(ii) we put $P_1 = \mathrm{Pf}(\Phi_1)$ and $P_2 = \mathrm{Pf}(\Phi_2)$, and note that by Lemma 4.4 there is an isomorphism of complexes

$$\begin{tikzcd}
0 \arrow[r] & R(-5) \arrow[r, "P_1^T"] \arrow[d, "\mu"] & R(-3)^5 \arrow[r, "\Phi_1"] \arrow[d, "A^{-T}"] & R(-2)^5 \arrow[r, "P_1"] \arrow[d, "B^T"] & R \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & R(-5) \arrow[r, "P_2^T"] & R(-3)^5 \arrow[r, "\Phi_2"] & R(-2)^5 \arrow[r, "P_2"] & R \arrow[r] & 0
\end{tikzcd}$$

for some $A, B \in \mathrm{GL}_5(K)$ and $\mu \in K^\times$. Commutativity of this diagram gives $P_1^T = \mu A^T P_2^T = B P_2^T$ and $\Phi_2 = B^T \Phi_1 A^T$. Since the entries of P_2 are linearly independent it follows that $B = \mu A^T$, and so $\Phi_2 = \mu A \Phi_1 A^T$, as required. The proof shows that $A \in \mathrm{GL}_5(K)$ is uniquely determined up to scalars by the condition $\mathrm{Pf}(\Phi_1) \propto \mathrm{Pf}(\Phi_2) A$. This observation (which also follows by Lemma 3.2(ii)) gives a convenient way to compute A. If K is algebraically closed then we may scale A so that $\mu = 1$. With this convention A is unique up to sign.

5. Descent by isogeny

We return to working over a number field K. Let $\phi : E \to E'$ be a cyclic isogeny of degree n and let $\widehat{\phi} : E' \to E$ be its dual isogeny. If (C, π) is a ϕ-covering of E' then $(C, \widehat{\phi} \circ \pi)$ is an n-covering of E. In general not all n-coverings of E arise in this way. Instead, an upper bound for the rank is obtained by computing both $S^{(\phi)}(E/K)$ and $S^{(\widehat{\phi})}(E'/K)$.

Since the Weil pairing $E[\phi] \times E'[\widehat{\phi}] \to \mu_n$ is nondegenerate, the action of Galois on $E[\phi]$, $E'[\widehat{\phi}]$, and μ_n is described by three characters

$$\chi^{-1}\omega, \chi, \omega : \mathrm{Gal}(\overline{K}/K) \to (\mathbb{Z}/n\mathbb{Z})^\times.$$

Let $L = K(E'[\widehat{\phi}])$ be the fixed field of the kernel of χ, and let $G = \mathrm{Gal}(L/K)$. If n is prime then $[L : K]$ divides $n-1$ and so is coprime to n. By the inflation-restriction exact sequence we have

$$H^1(K, E[\phi]) \cong H^1(L, E[\phi])^G.$$

Since $H^1(L, E[\phi]) \cong H^1(L, \mu_n) \cong L^\times/(L^\times)^n$ it follows (by keeping track of the G-actions) that $H^1(K, E[\phi]) \cong (L^\times/(L^\times)^n)^\chi$, where, if A is a G-module, we write

$$A^\chi = \{a \in A \mid \sigma(a) = a^{\chi(\sigma)} \text{ for all } \sigma \in G\}.$$

There is an analogue of the exact sequence (1) obtained by replacing K by its completion K_v. Let δ_v be the connecting map in this exact sequence. The Selmer group attached to ϕ is

$$S^{(\phi)}(E/K) = \{\theta \in H^1(K, E[\phi]) \mid \mathrm{res}_v(\theta) \in \mathrm{im}\, \delta_v \text{ for all places } v\}$$

where $\mathrm{res}_v : H^1(K, E[\phi]) \to H^1(K_v, E[\phi])$ is the restriction map. Assuming we can compute the groups

$$L(\mathcal{S}, n) = \{\theta \in L^\times/(L^\times)^n \mid v_{\mathfrak{p}}(\theta) \equiv 0 \bmod n \text{ for all } \mathfrak{p} \notin \mathcal{S}\}$$

for $\mathcal{S}$ a finite set of primes, the problem of computing the Selmer group reduces to that of computing the images of the local connecting maps δ_v. Since we give equations for the covering curves, the images of the δ_v may be computed by working out conditions for these curves to be locally soluble. See for example [17; 18; 9]. Alternatively, as described for example in [23; 28], the images of the δ_v may be computed as the cokernels of the maps $\phi : E(K_v) \to E'(K_v)$.

We take $n = 5$ and split into the cases where χ has order 1, 2 or 4. If χ is trivial then $E[\phi] \cong \mu_5$ and $E'[\widehat{\phi}] \cong \mathbb{Z}/5\mathbb{Z}$ as Galois modules. We recall from [17] that $E \cong C_\lambda$ and $E' \cong D_\lambda$ for some $\lambda \in K$, where C_λ and D_λ are the curves given by

$$\begin{aligned} C_\lambda: &\quad y^2 + (1-\lambda)xy - \lambda y = x^3 - \lambda x^2 + a_4 x + a_6, \\ D_\lambda: &\quad y^2 + (1-\lambda)xy - \lambda y = x^3 - \lambda x^2, \end{aligned} \tag{5}$$

where $a_4 = -5\lambda(\lambda^2 + 2\lambda - 1)$ and $a_6 = -\lambda(\lambda^4 + 10\lambda^3 - 5\lambda^2 + 15\lambda - 1)$.

Theorem 5.1. *If $\lambda_0, \dots, \lambda_4$ are elements of K such that*

$$\lambda = \prod_{i=0}^{4} \lambda_i \quad \textit{and} \quad \theta \equiv \prod_{i=0}^{4} \lambda_i^i \mod (K^\times)^5, \tag{6}$$

then the ϕ-covering of D_λ corresponding to $\theta \in K^\times/(K^\times)^5$ is defined by the 4×4 *Pfaffians of*

$$\begin{pmatrix} 0 & \lambda_1 x_1 & x_2 & -x_3 & -\lambda_4 x_4 \\ & 0 & \lambda_3 x_3 & x_4 & -x_0 \\ & & 0 & \lambda_0 x_0 & x_1 \\ & - & & 0 & \lambda_2 x_2 \\ & & & & 0 \end{pmatrix}.$$

Proof. See [17, Proposition 2.12]. The analogue of this result for cyclic isogenies of degrees 3 and 4 is given in [18, §1.2]. □

Example 5.2. Taking $K = \mathbb{Q}$ and $(\lambda_0, \dots, \lambda_4) = (1, 1, 2, 3, 5)$ gives an element of order 5 in Ш$(C_{30}/\mathbb{Q})$.

If χ is a quadratic character then E and E' are the quadratic twists by χ of C_λ and D_λ for some $\lambda \in K$. We write $L = K(\sqrt{d})$.

Theorem 5.3. *If r and s are elements of K, not both zero, then the ϕ-covering of E' corresponding to $\theta = (r + s\sqrt{d})/(r - s\sqrt{d}) \in (L^\times/(L^\times)^5)^\chi$ is defined by the* 4×4 *Pfaffians of*

$$\begin{pmatrix} 0 & \lambda x_0 & d(x_2 - x_4) & -x_1 + x_3 & -x_3 \\ & 0 & -x_1 - x_3 & x_2 + x_4 & x_4 \\ & & 0 & (r^2 - s^2 d)x_0 & r x_1 + s d x_2 \\ & - & & 0 & s x_1 + r x_2 \\ & & & & 0 \end{pmatrix}.$$

Proof. Let $\alpha = r + s\sqrt{d}$ and $\alpha' = r - s\sqrt{d}$. We apply Theorem 5.1 over L with

$$(\lambda_0, \dots, \lambda_4) = (\lambda/(\alpha\alpha'), \alpha, 1, 1, \alpha').$$

We then substitute $x_0 \leftarrow -(r^2 - s^2 d)x_0$ and

$$(x_1, \dots, x_4) \leftarrow (x_1 + \sqrt{d}x_2, x_3 + \sqrt{d}x_4, x_3 - \sqrt{d}x_4, x_1 - \sqrt{d}x_2)$$

to give a curve defined over K. Since $[L:K]$ and $\deg\phi$ are coprime to one another, the restriction map $H^1(K, E[\phi]) \to H^1(L, E[\phi])$ is injective. Since the curve we have found and the curve we are looking for are isomorphic over L, they must therefore be isomorphic over K. □

Example 5.4. Taking $K = \mathbb{Q}$ and $\lambda = 11$, $d = 5$, $r = s = 1$ gives an element of order 5 in Ш$(E/\mathbb{Q})$ where E is the elliptic curve 275b3 in Cremona's tables [10; 11].

Remark 5.5. The curve in Theorem 5.1 is defined by the 5 quadrics

$$\lambda_i x_i^2 + x_{i-1}x_{i+1} - \lambda_{i-2}\lambda_{i+2}x_{i-2}x_{i+2} = 0$$

where the subscripts are read modulo 5. If $\lambda_i' = -\lambda_{2i}/(\lambda_{2i-2}\lambda_{2i+2})$ then the curves defined by $\lambda_0, \dots, \lambda_4$ and $\lambda_0', \dots, \lambda_4'$ are isomorphic via

$$(x_0 : \cdots : x_4) \mapsto (x_0 : x_2 : x_4 : x_1 : x_3).$$

Taking Jacobians it follows that $C_\lambda \cong C_{-1/\lambda}$. Alternatively this last statement may be checked using the Weierstrass equations (5).

Now suppose χ has order 4. Let σ be the generator of $\mathrm{Gal}(L/K)$ with $\chi(\sigma) = 2$. Then E and E' are isomorphic over L to C_λ and D_λ for some $\lambda \in L$ satisfying $\sigma(\lambda) = -1/\lambda$.

Theorem 5.6. *If $\alpha \in L^\times$ then the ϕ-covering of E' corresponding to*

$$\theta = \alpha^4\sigma(\alpha)^2\sigma^2(\alpha)\sigma^3(\alpha)^3 \in (L^\times/(L^\times)^5)^\chi \tag{7}$$

is isomorphic over L to the curve in Theorem 5.1 with

$$(\lambda_0, \dots, \lambda_4) = \left(\lambda\sigma(\alpha)\sigma^3(\alpha), \frac{\alpha}{\lambda\sigma(\alpha)\sigma^3(\alpha)}, \frac{\lambda\sigma(\alpha)}{\alpha}, \frac{\lambda\sigma^3(\alpha)}{\sigma^2(\alpha)}, \frac{\sigma^2(\alpha)}{\lambda\sigma(\alpha)\sigma^3(\alpha)}\right).$$

Moreover a model for this curve over K is obtained by substituting

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} \leftarrow \begin{pmatrix} \beta_1 & \beta_2 & \beta_3 & \beta_4 \\ \sigma(\beta_1) & \sigma(\beta_2) & \sigma(\beta_3) & \sigma(\beta_4) \\ \sigma^3(\beta_1) & \sigma^3(\beta_2) & \sigma^3(\beta_3) & \sigma^3(\beta_4) \\ \sigma^2(\beta_1) & \sigma^2(\beta_2) & \sigma^2(\beta_3) & \sigma^2(\beta_4) \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}$$

where $\beta_1, \dots, \beta_4$ is a basis for L over K.

Proof. The first part is clear since we have chosen $\lambda_0, \dots, \lambda_4$ to satisfy (6). We have also arranged that $\sigma(\lambda_i) = -\lambda_{2i}/(\lambda_{2i-2}\lambda_{2i+2})$. The second part then follows by Remark 5.5. □

Remark 5.7. Since $\rho = 4 + 2\sigma + \sigma^2 + 3\sigma^3 \in \mathbb{F}_5[G]$ is an idempotent satisfying $\sigma\rho = 2\rho$, every element of $(L^\times/(L^\times)^5)^\chi$ is of the form (7).

Example 5.8. Let E and E' be the 5-isogenous elliptic curves

$$\begin{aligned} E &= 23808c3: & y^2 &= x^3 - x^2 - 785949x - 271615419, \\ E' &= 23808c2: & y^2 &= x^3 - x^2 + 7651x + 676677. \end{aligned}$$

Then $L = \mathbb{Q}(\varepsilon)$ where $\varepsilon = \sqrt{2+\sqrt{2}}$. Moreover $\lambda = (49 + 41\sqrt{2})/31$ and $\sigma : \varepsilon \mapsto \varepsilon^3 - 3\varepsilon$. We take $\alpha = 1 + \varepsilon$ and $\beta_j = \varepsilon^{j-1}$ for $j = 1, \dots, 4$. After following the construction in Theorem 5.6, the algorithms for minimisation and reduction in [21] suggest the change of coordinates

$$\begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} \leftarrow \begin{pmatrix} 0 & 0 & 0 & 0 & 62 \\ 0 & 6 & -6 & 14 & 0 \\ 13 & -13 & -7 & -7 & 0 \\ 0 & 1 & -1 & -8 & 0 \\ -3 & 3 & 4 & 4 & 0 \end{pmatrix} \begin{pmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix}.$$

The result is $C \subset \mathbb{P}^4$ defined by the 4×4 Pfaffians of

$$\begin{pmatrix} 0 & x_0 - x_1 + x_3 + 4x_4 & x_1 - x_2 - x_4 & -x_2 - 2x_3 + 4x_4 & x_1 \\ & 0 & -x_2 - 4x_4 & x_1 - x_2 + x_4 & x_3 \\ & & 0 & x_0 - x_1 - x_3 - 4x_4 & x_2 \\ & - & & 0 & x_0 \\ & & & & 0 \end{pmatrix}.$$

Computing the invariants, as described in [19], and using Bruin's programs [4] to check local solubility, we find that C represents an element of $\text{Ш}(E/\mathbb{Q})[5]$. It is nontrivial since $E'(\mathbb{Q}) = 0$ and $\theta \notin (L^\times)^5$.

6. An example of full 5-descent

In this section we compute equations for an order-5 element in the Tate-Shafarevich group of the elliptic curve $E/\mathbb{Q}$:

$$6727a1: \quad y^2 + xy = x^3 - x^2 - 202951x - 34841040.$$

Since E has no rational 5-isogenies, our method is to use full 5-descent; that is, descent with respect to the multiplication-by-5 map on E. Further details of the calculation are given in a Magma [2] file available at this article's webpage.

Let $T = (x_T, y_T)$ be a nontrivial 5-torsion point on E. Then $L = \mathbb{Q}(T)$ is a number field of degree 24. Let σ_2 be the automorphism of L with $\sigma_2(T) = 2T$.

We shall write elements of L in terms of u and v where

$$v = -31(2y_T + x_T)/(x_T^2 + 480x_T + 87391)$$

and $u = v/\sigma_2(v)$. Explicitly, u has minimal polynomial

$$\begin{aligned} &X^{12} + 4X^{11} - 6X^{10} - 20X^9 + 15X^8 - 303X^7 \\ &\qquad + 323X^6 + 303X^5 + 15X^4 + 20X^3 - 6X^2 - 4X + 1 \end{aligned}$$

and v is a square root of

$$(2u^{11}+9u^{10}-8u^9-46u^8+10u^7-591u^6+343u^5+928u^4+331u^3+60u^2+8u-9)/3.$$

We recall from [15; 34] that there is an injective group homomorphism

$$H^1(\mathbb{Q}, E[5]) \to L^\times/(L^\times)^5$$

whose image is contained in the σ_2-eigenspace

$$\{x \in L^\times/(L^\times)^5 \mid \sigma_2(x) \equiv x^2 \bmod (L^\times)^5\}. \tag{8}$$

The primes of bad reduction for E are 7 and 31, with Tamagawa numbers $c_7 = 1$ and $c_{31} = 2$. Since the Tamagawa numbers are coprime to 5, we have $S^{(5)}(E/\mathbb{Q}) \subset L(\mathcal{S}, 5)$ where $\mathcal{S} = \{\mathfrak{p}_1, \mathfrak{p}_2\}$ is the set of primes of L above 5.

The number field L is too large for an unconditional computation of its class group and units. However according to PARI/GP [32] (which by default makes heuristic assumptions) the class number is 2. We also used PARI/GP to compute a set of fundamental units, and generators for the prime ideals $\mathfrak{p}_1$ and $\mathfrak{p}_2$. This gives a basis for $L(\mathcal{S}, 5) \cong (\mathbb{Z}/5\mathbb{Z})^{15}$. The intersection of $L(\mathcal{S}, 5)$ with the σ_2-eigenspace (8) is 3-dimensional. One of the nontrivial elements is $a = a'/294$, with

$$\begin{aligned} a' = (&4600u^{11}+8325u^{10}-72155u^9-50035u^8+289975u^7-1450795u^6 \\ &+4510595u^5-592350u^4-3962957u^3-1755928u^2-811953u-191035)v \\ &+(158985u^{11}+661975u^{10}-836070u^9-3280275u^8+1784950u^7 \\ &-48064875u^6+43645605u^5+52498690u^4+14516335u^3+7628705u^2 \\ &+310520u-311257). \end{aligned}$$

We have $(a) = \mathfrak{c}^5$ for some integral ideal $\mathfrak{c}$, and $a\sigma_2(a)^2 = b^5$ where $b = b'/294$ and

$$\begin{aligned} b' = (&452u^{11} + 1935u^{10} - 2186u^9 - 9743u^8 + 4070u^7 - 135379u^6 \\ &+ 108106u^5 + 172665u^4 + 54912u^3 + 14840u^2 - 4879u - 12762)v \\ &+ (-1983u^{11} - 9082u^{10} + 7240u^9 + 46137u^8 - 7149u^7 + 585937u^6 \\ &- 289205u^5 - 957562u^4 - 338134u^3 - 139997u^2 - 62943u + 7646). \end{aligned}$$

We recall some of the theory from [12; 13; 14]. Let E be an elliptic curve over a field K of characteristic 0. Let R be the K-algebra of all Galois-equivariant maps $E[n] \to \overline{K}$ and let $w : E[n] \to \overline{R}^\times = \mathrm{Map}(E[n], \overline{K}^\times)$ be the map induced by the Weil pairing e_n. If $\sigma \mapsto \xi_\sigma$ is a cocycle representing $\xi \in H^1(K, E[n])$ then by Hilbert's theorem 90 there exists $\gamma \in \overline{R}^\times$ with $\sigma(\gamma)/\gamma = w(\xi_\sigma)$ for all $\sigma \in \mathrm{Gal}(\overline{K}/K)$. We put $\alpha = \gamma^n$ and $\rho = \partial\gamma$ where

$$\partial : \overline{R}^\times \to (\overline{R} \otimes \overline{R})^\times = \mathrm{Map}(E[n] \times E[n], \overline{K}^\times)$$

is given by $(\partial z)(T_1, T_2) = z(T_1)z(T_2)/z(T_1 + T_2)$. Then according to [12, §3] there are group homomorphisms

$$\begin{aligned} w_1 &: H^1(K, E[n]) \to R^\times/(R^\times)^n, & \xi &\mapsto \alpha, \\ w_2 &: H^1(K, E[n]) \to (R \otimes R)^\times/\partial R^\times, & \xi &\mapsto \rho. \end{aligned}$$

The map w_1 is injective for n prime, whereas w_2 is always injective.

Let $\mathrm{Ob} : H^1(K, E[n]) \to \mathrm{Br}(K)$ be the obstruction map as defined in Section 2.

Theorem 6.1. *Assume n is odd. Let $\xi \in H^1(K, E[n])$ and $\rho \in (R \otimes R)^\times$ with $w_2(\xi) = \rho\partial R^\times$. Let $A_\rho = (R, +, *_\rho)$ where the new multiplication $*_\rho$ is defined by*

$$z_1 *_\rho z_2 : T \mapsto \sum_{T_1+T_2=T} e_n(T_1, T_2)^{(n+1)/2}\rho(T_1, T_2)z_1(T_1)z_2(T_2).$$

Then A_ρ is a central simple algebra over K of dimension n^2 representing the class of $\mathrm{Ob}(\xi)$ *in* $\mathrm{Br}(K)$.

Proof. See [12, Lemma 3.11 and §4]. □

Returning to our numerical example, we write α and β for the elements $(1, a)$ and $(1, b)$ in the étale algebra $R = \mathbb{Q} \times L$. To compute ρ exactly (using $\partial\alpha = \rho^5$) we must extract a 5th root in a number field of degree $\frac{1}{2}\#\mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z}) = 240$. This would be the direct analogue of what we do for 3-descent (see [14, §8]), but is clearly not very promising. So instead we write $\rho = \partial\gamma$ and (fixing an embedding $\overline{\mathbb{Q}} \subset \mathbb{C}$) represent $\gamma \in \overline{R} = \mathrm{Map}(E[5], \overline{\mathbb{Q}})$ numerically. Since $\gamma^5 = \alpha$ there are at first sight 5^{25} possibilities for γ. We cut down to just 5^3 choices by requiring that

(i) $\gamma(T)\gamma(2T)^2 = \beta(T)$ for all $T \in E[5]$, and

(ii) $\gamma : E(\mathbb{C})[5] \to \mathbb{C}$ is $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$-equivariant.

To explain these conditions we recall that $\sigma(\gamma)/\gamma = w(\xi_\sigma)$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. From this it is easy to see that $T \mapsto \gamma(T)\gamma(2T)^2$ is Galois-equivariant. Since $\alpha(T)\alpha(2T)^2 = \beta(T)^5$, and there are no nontrivial fifth roots of unity in R, this proves (i). Let $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ be complex conjugation. (Recall that we fixed an embedding $\overline{\mathbb{Q}} \subset \mathbb{C}$.) Since $H^1(\mathbb{R}, E[5]) = 0$ we have $\tau(\gamma)/\gamma = w(\xi_\tau) = w(\tau(S) - S)$

for some $S \in E(\mathbb{C})[5]$. Dividing γ by $w(S)$ now gives (ii). Multiplying γ by $w(T)$ for $T \in E(\mathbb{R})[5]$ does not change $\rho = \partial\gamma$, so in fact we only need to loop over 5^2 choices for γ.

Let T_1, T_2 be a basis for $E[5](\mathbb{C})$ with $\overline{T}_1 = T_1, \overline{T}_2 = -T_2$. Then $\zeta = e_5(T_1, T_2)$ is a primitive fifth root of unity. We define

$$h(T_1) = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}, \quad h(T_2) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & \zeta & 0 & 0 & 0 \\ 0 & 0 & \zeta^2 & 0 & 0 \\ 0 & 0 & 0 & \zeta^3 & 0 \\ 0 & 0 & 0 & 0 & \zeta^4 \end{pmatrix},$$

and

$$h : E[5](\mathbb{C}) \to \mathrm{Mat}_5(\mathbb{C}), \quad h(rT_1 + sT_2) = \zeta^{-rs/2} h(T_1)^r h(T_2)^s,$$

where the exponent of ζ is read as an element of $\mathbb{Z}/5\mathbb{Z}$.

We compute the structure constants for A_ρ from the real trivialisation given in [14, §5], that is,

$$A_\rho \otimes \mathbb{R} \xrightarrow{\sim} \mathrm{Mat}_5(\mathbb{R}), \quad z \mapsto \sum_{T \in E[5]} \gamma(T) z(T) h(T).$$

As recommended there, we choose our $\mathbb{Q}$-basis for L to be a $\mathbb{Z}$-basis for $\mathfrak{c}^{-1}$ that is LLL-reduced with respect to the inner product

$$\langle z_1, z_2 \rangle = \sum_{0 \neq T \in E[5]} |\alpha(T)|^{2/5} z_1(T) \overline{z_2(T)}.$$

This makes the structure constants small integers, which are therefore easy to recognise from floating-point approximations. The incorrect choices of γ are quickly discarded since the structure constants do not in general turn out to be integers.

To record our final choice of γ we let T_1, T_2 be the basis for $E(\mathbb{C})[5]$ given (approximately) by

$$T_1 = (1996.32, -87675.66),$$
$$T_2 = (-643.55, 321.77 - 13079.33i).$$

Then γ is the fifth root of α given (approximately) by the following matrix, with entries $\gamma(rT_1 + sT_2)$ for $r, s = 0, \dots, 4$.

$$\begin{pmatrix} 1.00 & -3.96 + 0.90i & 1.39 - 4.05i & 1.39 + 4.05i & -3.96 - 0.90i \\ -0.92 & 5.87 - 2.18i & 2.39 + 1.96i & 2.39 - 1.96i & 5.87 + 2.18i \\ -2.20 & 4.41 + 3.00i & -3.56 - 4.19i & -3.56 + 4.19i & 4.41 - 3.00i \\ -2.12 & -7.13 - 4.33i & -0.29 + 3.75i & -0.29 - 3.75i & -7.13 + 4.33i \\ 4.44 & 0.14 - 0.12i & -0.96 - 0.48i & -0.96 + 0.48i & 0.14 + 0.12i \end{pmatrix}$$

Although our method for choosing a basis for L as a $\mathbb{Q}$-vector space works well on a computer, the basis vectors (which are elements of $\mathfrak{c}^{-1}$) are extremely messy to write down. To assist in recording some details of the calculation, we replace α and γ by their inverses. Our $\mathbb{Q}$-basis $u_1, \dots, u_{24}$ for L is now a $\mathbb{Z}$-basis for $\mathfrak{c}$. Its first two elements are $u_1 = u_1'/147$ and $u_2 = u_2'/294$, where

$$\begin{aligned} u_1' = 906u^{11} + 3697u^{10} - 5099u^9 - 18382u^8 + 11847u^7 - 274284u^6 \\ + 271264u^5 + 284304u^4 + 51522u^3 + 31261u^2 - 4247u - 3174 \end{aligned}$$

and

$$\begin{aligned} u_2' = (640u^{11} + 2621u^{10} - 3565u^9 - 13051u^8 + 8154u^7 - 193589u^6 \\ + 188894u^5 + 204155u^4 + 40745u^3 + 21338u^2 - 5548u - 2903)v \\ + (-221u^{11} - 943u^{10} + 1135u^9 + 4972u^8 - 2330u^7 + 65086u^6 \\ - 53197u^5 - 99488u^4 - 12061u^3 + 13094u^2 + 5473u + 4980). \end{aligned}$$

Then R has basis $r_1, \dots, r_{25}$, where $r_1 = (1, 0)$ and $r_{i+1} = (0, u_i)$. Let $A_\rho = (R, +, *_\rho)$ with basis $\boldsymbol{a}_1, \dots, \boldsymbol{a}_{25}$ corresponding to $r_1, \dots, r_{25}$. Note that $\boldsymbol{a}_1$ is the identity. The structure constants turn out to be integers with maximum absolute value 448 and mean absolute value 22.65. As predicted by [14, Lemma 5.2] the order with basis the $\boldsymbol{a}_i$ has discriminant $5^{48} \cdot 7^{16} \cdot 31^{18} = 5^{25} \cdot \mathrm{Disc}(L)$. The basis vectors $\boldsymbol{a}_i$ have minimal polynomials

$$X - 1, \quad X^5 + 435X^3 + 7315X^2 + 835X + 32172, \\ X^5 - 390X^3 - 4885X^2 + 17560X + 1407822, \quad \dots$$

If $\alpha \in R^\times/(R^\times)^5$ corresponds to a Selmer group element, then by the local-to-global principle for the Brauer group we have $A_\rho \cong \mathrm{Mat}_5(\mathbb{Q})$. The problem of finding such an isomorphism (called a *trivialisation*) is addressed in [14; 24; 25]. By using Magma to compute a maximal order (and running LLL on the change of basis matrix) we found a basis with minimal polynomials

$$\begin{gathered} X^2, \quad X^2, \quad X^2, \quad X^4, \quad X^2, \quad X^3, \quad X^2, \quad X^3 - X, \\ X^5 - 2X^3 + X, \quad X^4 - X^2, \quad X^4 - X^2, \quad X^5 + X^3, \quad X^2, \\ X^4 - X^2, \quad X^3, \quad X^4 - 2X^2, \quad X^4 - X^2, \quad X^5 - X^3 + X^2 + X, \\ X^5 - X^3 - 4X^2 + 4X, \quad X^4 - 2X^2 - X, \quad X^4 + X^3 - X^2 - X, \\ X^5 - X^3, \quad X^5 - 2X^3, \quad X^5 - 5X^2 + X, \quad X^3 + X^2. \end{gathered}$$

Any reducible minimal polynomial gives a zero-divisor in A_ρ, and once we know a zero-divisor it is easy to find a trivialisation. In this way we found a trivialisation τ

that maps $\boldsymbol{a}_1 \mapsto I_5$ and

$$\boldsymbol{a}_2 \mapsto \begin{pmatrix} 13 & -5 & -20 & -20 & -15 \\ -40 & -22 & 40 & 20 & 10 \\ -20 & -35 & 3 & -15 & -15 \\ -15 & 0 & 30 & 13 & 0 \\ 15 & 15 & -10 & -5 & -7 \end{pmatrix}, \quad \boldsymbol{a}_3 \mapsto \begin{pmatrix} -12 & 5 & 0 & 10 & 5 \\ -30 & -42 & 35 & 5 & 0 \\ -50 & -35 & 38 & 20 & 5 \\ -110 & -50 & 65 & 8 & 5 \\ 45 & 45 & -30 & 0 & 8 \end{pmatrix}.$$

These calculations show that the element α of $R^\times/(R^\times)^5$ corresponds to an element of $H^1(\mathbb{Q}, E[5])$ with trivial obstruction. It may therefore be represented by a genus-one normal curve $C \subset \mathbb{P}^4$.

We compute equations for C using the "Hesse pencil method", as described in [12, §5.1]. Let $r_1^*, \dots, r_{25}^*$ be the basis for R with $\operatorname{Tr}_{R/\mathbb{Q}}(r_i r_j^*) = \delta_{ij}$. It is shown that

$$M = \sum_{i=1}^{25} r_i^* \tau(\boldsymbol{a}_i) \in \mathrm{GL}_5(R) = \mathrm{Map}_{\mathbb{Q}}(E[5], \mathrm{GL}_5(\overline{\mathbb{Q}}))$$

describes the action of $E[5]$ on $C \subset \mathbb{P}^4$. In [20, §12] we gave a practical method for computing all genus-one normal curves $C \subset \mathbb{P}^4$ that have Jacobian E and are invariant under the matrices M_T for $T \in E[5]$. As predicted by [12, Proposition 5.5] there is only one such curve defined over $\mathbb{Q}$. We use the algorithms for minimisation and reduction in [21] to make a final change of coordinates. In this example the model obtained is already minimal, whereas reduction suggests the change of coordinates

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} \leftarrow \begin{pmatrix} -1 & 2 & 1 & -2 & 1 \\ -1 & 1 & 1 & -1 & 1 \\ 1 & -1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix}.$$

The result is $C \subset \mathbb{P}^4$ defined by the 4×4 Pfaffians of

$$\begin{pmatrix} 0 & -x_1+x_2+x_3 & x_1+3x_2+x_4 & -2x_2+x_3+x_5 & 2x_2-2x_3+x_5 \\ & 0 & -x_1-x_2-x_3+x_5 & x_2-x_4+x_5 & -x_2+x_3+x_4 \\ & & 0 & -x_3+x_5 & -x_1+x_3-x_5 \\ & - & & 0 & x_4 \\ & & & & 0 \end{pmatrix}.$$

Computing the invariants, as described in [19], and using Bruin's programs [4] to check local solubility, we find that C represents an element of $\text{Ш}(E/\mathbb{Q})[5]$. It is nontrivial since $E(\mathbb{Q})/5E(\mathbb{Q}) = 0$ and $\alpha \notin (R^\times)^5$.

The theory in [12, §3] shows that if $M^5 = \alpha' I_5$ then $\alpha'/\alpha \in (R^\times)^5$. This is a condition we can check exactly. So even though we made use of floating-point approximations (and did not check at the outset that α is in the image of w_1, although methods for doing this are described in [15; 34]), we can be sure that C corresponds to our original choice of α.

Repeating for other choices of α, we found a subgroup of Ш$(E/\mathbb{Q})$ isomorphic to $(\mathbb{Z}/5\mathbb{Z})^2$. For these, and examples for other elliptic curves $E/\mathbb{Q}$ of small conductor, see [22]. The main difficulty in computing further examples is that the computation of class group and units is often prohibitively expensive.

References

[1] Wieb Bosma and John Cannon (eds.), *Discovering mathematics with Magma: Reducing the abstract to the concrete*, Algorithms and Computation in Mathematics, no. 19, Springer, Berlin, 2006. MR 2007h:00016

[2] 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. MR 1484478

[3] N. Bourbaki, *Algèbre. Chapitre* 9: *Formes sesquilinéaires et formes quadratiques*, Actualités Sci. Ind., no. 1272, Hermann, Paris, 1959, reprinted Springer, Berlin, 2007. MR 21 #6384

[4] Nils Bruin, *Some ternary Diophantine equations of signature* $(n, n, 2)$, in Bosma and Cannon [1], 2006, pp. 63–91. MR 2007m:11047

[5] Winfried Bruns and Jürgen Herzog, *Cohen-Macaulay rings*, Cambridge Studies in Advanced Mathematics, no. 39, Cambridge University Press, 1993. MR 95h:13020

[6] David A. Buchsbaum and David Eisenbud, *Algebra structures for finite free resolutions, and some structure theorems for ideals of codimension* 3, Amer. J. Math. **99** (1977), no. 3, 447–485. MR 56 #11983

[7] ———, *Gorenstein ideals of height* 3, Seminar D. Eisenbud/B. Singh/W. Vogel, vol. 2, Teubner-Texte zur Math., no. 48, Teubner, Leipzig, 1982, pp. 30–48. MR 84i:13017

[8] J. W. S. Cassels, *Arithmetic on curves of genus* 1*, IV: Proof of the Hauptvermutung*, J. Reine Angew. Math. **211** (1962), 95–112. MR 29 #1214

[9] Henri Cohen and Fabien Pazuki, *Elementary 3-descent with a 3-isogeny*, Acta Arith. **140** (2009), no. 4, 369–404. MR 2011h:11063

[10] J. E. Cremona, *Algorithms for modular elliptic curves*, 2nd ed., Cambridge University Press, 1997. MR 99e:11068

[11] ———, *Elliptic curve data*, 9999. http://homepages.warwick.ac.uk/staff/J.E.Cremona/ftp/data

[12] J. E. Cremona, T. A. Fisher, C. O'Neil, D. Simon, and M. Stoll, *Explicit n-descent on elliptic curves, I: Algebra*, J. Reine Angew. Math. **615** (2008), 121–155. MR 2009g:11067

[13] ———, *Explicit n-descent on elliptic curves, II: Geometry*, J. Reine Angew. Math. **632** (2009), 63–84. MR 2011d:11128

[14] ———, *Explicit n-descent on elliptic curves*, *III*: *Algorithms*, 2011, to appear in *Math. Comp.* arXiv 1107.3516 [math.NT]

[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] David Eisenbud, *Commutative algebra: With a view toward algebraic geometry*, Graduate Texts in Mathematics, no. 150, Springer, New York, 1995. MR 97a:13001

[17] Tom Fisher, *Some examples of 5 and 7 descent for elliptic curves over* $\mathbb{Q}$, J. Eur. Math. Soc. (JEMS) **3** (2001), no. 2, 169–201. MR 2002m:11045

[18] ———, *The Cassels-Tate pairing and the Platonic solids*, J. Number Theory **98** (2003), no. 1, 105–155. MR 2003k:11094

[19] ———, *The invariants of a genus one curve*, Proc. Lond. Math. Soc. (3) **97** (2008), no. 3, 753–782. MR 2009j:11087

[20] ———, *The Hessian of a genus one curve*, Proc. Lond. Math. Soc. (3) **104** (2012), no. 3, 613–648. MR 2900238

[21] ———, *Minimisation and reduction of 5-coverings of elliptic curves*, Algebra Number Theory **7** (2013), no. 5, 1179–1205.

[22] ———, *Elements of order 5 in the Tate-Shafarevich group*, 9999. http://www.dpmms.cam.ac.uk/~taf1000/g1data/order5.html

[23] E. V. Flynn and C. Grattoni, *Descent via isogeny on elliptic curves with large rational torsion subgroups*, J. Symbolic Comput. **43** (2008), no. 4, 293–303. MR 2009c:11080

[24] Gábor Ivanyos, Lajos Rónyai, and Josef Schicho, *Splitting full matrix algebras over algebraic number fields*, J. Algebra **354** (2012), 211–223. MR 2879232

[25] Ádám Lelkes, *Small zero divisors in maximal orders of* $M_n(\mathbf{Q})$, Scientific student conference, Budapest, 2011. http://www.math.bme.hu/~lelkesa/tdk.pdf

[26] Stephen Lichtenbaum, *The period-index problem for elliptic curves*, Amer. J. Math. **90** (1968), 1209–1223. MR 38 #5788

[27] E. Marchionna (ed.), *Questions on algebraic varieties: Lectures given at a Summer School of the Centro Internazionale Matematico Estivo (C.I.M.E.) held in Varenna (Como), Italy, September 7–17, 1969*, C.I.M.E. Summer Schools, no. 51, Berlin, Springer, 2011.

[28] Robert L. Miller and Michael Stoll, *Explicit isogeny descent on elliptic curves*, Math. Comp. **82** (2013), no. 281, 513–529. MR 2983034

[29] David Mumford, *Varieties defined by quadratic equations*, in Marchionna [27], 2011, pp. 29–100. MR 44 #209

[30] Catherine O'Neil, *The period-index obstruction for elliptic curves*, J. Number Theory **95** (2002), no. 2, 329–339, erratum: [31]. MR 2003f:11079

[31] ———, *Erratum to: "The period-index obstruction for elliptic curves"* [*J. Number Theory* **95** *(2002), no. 2, 329–339*], J. Number Theory **109** (2004), no. 2, 390. MR 2005g:11096

[32] The PARI Group, *PARI/GP*, 2012. http://pari.math.u-bordeaux.fr/

[33] Irena Peeva, *Graded syzygies*, Algebra and Applications, no. 14, Springer, London, 2011. MR 2011j:13015

[34] Edward F. Schaefer and Michael Stoll, *How to do a p-descent on an elliptic curve*, Trans. Amer. Math. Soc. **356** (2004), no. 3, 1209–1231. MR 2004g:11045

TOM FISHER: `T.A.Fisher@dpmms.cam.ac.uk`
*DPMMS, Centre for Mathematical Sciences, University of Cambridge, Wilberforce Road,
Cambridge CB3 0WB, United Kingdom*

msp

VOLUME EDITORS

Everett W. Howe
Center for Communications Research
4320 Westerra Court
San Diego, CA 92121-1969
United States

Kiran S. Kedlaya
Department of Mathematics
University of California, San Diego
9500 Gilman Drive #0112
La Jolla, CA 92093-0112

Front cover artwork based on a detail of
Chicano Legacy 40 Años ©2010 Mario Torero.

Electronic copies can be obtained free of charge from http://msp.org/obs/1 and printed copies can be ordered from MSP (contact@msp.org).

The Open Book Series is a trademark of Mathematical Sciences Publishers.

ISSN: 2329-9061 (print), 2329-907X (electronic)

ISBN: 978-1-935107-00-2 (print), 978-1-935107-01-9 (electronic)

First published 2013.

msp

MATHEMATICAL SCIENCES PUBLISHERS
798 Evans Hall #3840, c/o University of California, Berkeley CA 94720-3840
contact@msp.org **http://msp.org**

THE OPEN BOOK SERIES 1

Tenth Algorithmic Number Theory Symposium

The Algorithmic Number Theory Symposium (ANTS), held biennially since 1994, is the premier international forum for research in computational number theory. ANTS is devoted to algorithmic aspects of number theory, including elementary, algebraic, and analytic number theory, the geometry of numbers, arithmetic algebraic geometry, the theory of finite fields, and cryptography.

This volume is the proceedings of the tenth ANTS meeting, held July 9–13, 2012, at the University of California, San Diego. It includes revised and edited versions of the 25 refereed papers presented at the conference, together with extended abstracts of two of the five invited talks.

TABLE OF CONTENTS