FINDING RATIONAL POINTS ON ELLIPTIC CURVES USING 6-DESCENT AND 12-DESCENT

TOM FISHER

Abstract. We explain how recent work on 3-descent and 4-descent for elliptic curves over $\mathbb{Q}$ can be combined to search for generators of the Mordell-Weil group of large height. As an application we show that every elliptic curve of prime conductor in the Stein-Watkins database has rank at least as large as predicted by the conjecture of Birch and Swinnerton-Dyer.

1. Introduction

Let E be an elliptic curve over $\mathbb{Q}$. An n-descent calculation on E provides us with n-covering curves $\pi_\alpha : C_\alpha \to E$ for α running over a finite indexing set A, with the property that

$$\bigcup_{\alpha \in A} \pi_\alpha(C_\alpha(\mathbb{Q})) = E(\mathbb{Q}).$$

The usual choice of indexing set A is the n-Selmer group $S^{(n)}(E/\mathbb{Q})$ which sits in a short exact sequence

$$0 \to E(\mathbb{Q})/nE(\mathbb{Q}) \xrightarrow{\delta} S^{(n)}(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[n] \to 0.$$

Given $\alpha \in S^{(n)}(E/\mathbb{Q})$ there are two possibilities: either $\pi_\alpha(C_\alpha(\mathbb{Q}))$ is a coset of $nE(\mathbb{Q})$ in $E(\mathbb{Q})$, in which case α is the image of this coset by δ, or $C_\alpha(\mathbb{Q})$ is empty, in which case α maps to a non-trivial element of the Tate-Shafarevich group $Ш(E/\mathbb{Q})$.

It has long been known that n-descent can help in the search for generators of the Mordell-Weil group $E(\mathbb{Q})$. Indeed the theory of heights (see for example [12]) suggests that if we write our n-coverings as curves of degree n with small coefficients, then a point of (logarithmic) height h on $E(\mathbb{Q})$ should come from a point of height approximately $h/(2n)$ on $C_\alpha(\mathbb{Q})$ for suitable α. This is not a precise statement (the height is only bounded up to the addition of a constant whose behaviour with respect to n is unknown) but the idea seems to work well in practice.

We would therefore like to perform n-descent calculations for n as large as possible. Until recently n-descent has only been practical for

Date: 23rd November 2007.

general[1] elliptic curves in the case $n = 2$. Methods for 4-descent and 8-descent have been developed in the PhD theses of Siksek [18], Womack [24] and Stamminger [20]. Joint work of the author with Cremona, O'Neil, Simon and Stoll [5] has now made 3-descent practical, and in a few preliminary examples also 5-descent. The algorithms for 2-descent, 3-descent and 4-descent have been contributed to the computer algebra system Magma [15].

The natural question therefore arises as to how we can combine an m-covering and n-covering for m and n coprime to give an mn-covering. At the level of abelian groups it is trivial that

$$S^{(mn)}(E/\mathbb{Q}) \cong S^{(m)}(E/\mathbb{Q}) \times S^{(n)}(E/\mathbb{Q}).$$

However, if we are to represent the Selmer group elements as covering curves, then it is not so clear how one should proceed.

Suppose we are given an m-covering $\pi_m : C_m \to E$ and an n-covering $\pi_n : C_n \to E$. Then the curves C_m and C_n are torsors under E, and an mn-covering is given by

$$C_{mn} = \frac{C_m \times C_n}{E}$$

where we quotient out by the diagonal action of E. An alternative would be to take fibre product

$$C_{mn} = C_m \times_E C_n$$

with respect to the covering maps π_m and π_n. As far as we can see, neither of these constructions is suitable for practical computation. We have therefore taken a different approach based on representations of the Heisenberg group.

Unfortunately our approach does not work for arbitrary coprime integers m and n, but only when each of m and n is plus or minus a square modulo the other. This includes the case of consecutive integers. In this case, we specify an embedding of E in $\mathbb{P}(\mathrm{Mat}_{n,n+1})$ as a curve of degree $n(n+1)$, in such a way that when E acts on itself by translation, the n-torsion points act as left multiplication by $n \times n$ matrices, and the $(n+1)$-torsion points act as right multiplication by $(n+1) \times (n+1)$ matrices. We can then twist E by a pair of cocycles taking values in $E[n]$ and $E[n+1]$ to obtain the required $n(n+1)$-covering $C_{n(n+1)}$ as a curve in $\mathbb{P}(\mathrm{Mat}_{n,n+1})$. Moreover, it turns out that the covering map $C_{n(n+1)} \to C_{n+1}$ is defined by the $n \times n$ minors.

[1] *i.e.* we make no assumption on the Galois module structure of $E[n]$.

We give a precise statement of these results in §2. We employ two different methods of proof. The first, described in §3, uses representations of the Heisenberg group, and leads to results for arbitrary n. The second, described in §§4,5, uses the invariant theory of binary quartics and ternary cubics, and gives practical formulae specific to 6-descent and 12-descent.

In §6 we give some details of our implementation of 6-descent and 12-descent in Magma. Using 12-descent, we now expect to be able to find rational points on an elliptic curve over $\mathbb{Q}$ up to logarithmic height 600 (provided the coefficients of the original elliptic curve are not too large). The main bottleneck comes in the 3-descent, where we must compute the class group and units of each number field generated by the co-ordinates of a 3-torsion point of E. (There is usually just one such field, and it has degree 8.) Fortunately, since our final answer comes in the form of a rational point, there is no need to perform these intermediate calculations rigorously.

Stein and Watkins [21] have constructed a database of elliptic curves that is expected to contain most elliptic curves over $\mathbb{Q}$ of prime conductor N with $N < 10^{10}$. We are able to show that every curve in their database (of prime conductor) has rank at least as large as predicted by the conjecture of Birch and Swinnerton-Dyer. Prior to our involvement, this had been reduced by Cremona and Watkins to a list of 35 curves of analytic rank 2 for which one generator of small height (less than 34) was known, but a second generator of large height (greater than 220) remained to be found. In each case we were able to find the second generator using either 6-descent or 12-descent.

We give two numerical examples in §7. In the first we use 6-descent to find a pair of non-zero integers x and y for which both

$$x^2 - 809xy + y^2 \quad \text{and} \quad x^2 + 809xy + y^2$$

are squares. We find that the smallest solution is given by x and y with 534 and 537 decimal digits respectively. Our second example is the last in the list of 35 curves mentioned above. In this case we use 12-descent to find a generator of height 642.63.

Acknowledgments

I would like to thank Steve Donnelly for sharing his initial thoughts on this problem, and Mark Watkins for suggesting suitable test data, including the examples in §7. All computer calculations in support of this work were performed using Magma [15].

2. Computing twists

Let k be a field of characteristic zero, with algebraic closure $\overline{k}$. We fix an elliptic curve E over k with identity $\mathcal{O}$. Let $n \geq 2$ be an integer. A base diagram $[E \to \mathbb{P}^{n-1}]$ of level n is a morphism defined over k determined by the complete linear system $|n.\mathcal{O}|$. Thus any two base diagrams differ by an element of $\mathrm{PGL}_n(k)$.

More generally we consider diagrams $[C \to S]$ where C is a torsor under E and S is a variety (both defined over k) and the map $C \to S$ is a morphism defined over k. Two such diagrams $[\phi_1 : C_1 \to S_1]$ and $[\phi_2 : C_2 \to S_2]$ are isomorphic if there is an isomorphism of torsors $\alpha : C_1 \cong C_2$ and an isomorphism of varieties $\beta : S_1 \cong S_2$ satisfying $\phi_2 \circ \alpha = \beta \circ \phi_1$. We define a Brauer-Severi diagram $[C \to S]$ to be a twist of the base diagram. Then S is a Brauer-Severi variety, and the morphism $C \to S$ is that determined by a complete linear system $|D|$, where the divisor D is linearly equivalent to all its Galois conjugates, but need not itself be defined over k.

We recall from [5, Paper I, §1.3] that the Brauer-Severi diagrams are parametrised, as twists of a fixed base diagram, by the Galois cohomology group $H^1(k, E[n])$. Moreover there is an obstruction map

$$\mathrm{Ob}_n : H^1(k, E[n]) \to \mathrm{Br}(k)[n]$$

taking the class of $[C \to S]$ to the class of $[S]$. In general this map is not a group homomorphism. We are interested in the elements of $H^1(k, E[n])$ with trivial obstruction, equivalently those that are represented by diagrams of the form $[\phi_n : C \to \mathbb{P}^{n-1}]$. With the convention that points of $\mathbb{P}^{n-1}$ are written as column vectors, we define the "character" associated to ϕ_n to be the unique morphism of k-group schemes $\chi_n : E[n] \to \mathrm{PGL}_n$ such that

$$\phi_n(T + P) = \chi_n(T)\phi_n(P)$$

for all $T \in E[n](\overline{k})$ and $P \in C(\overline{k})$.

In §3 we use representations of the Heisenberg group to prove

Theorem 2.1. *Let m and n be coprime integers satisfying*

$$u^2 n \equiv \pm 1 \pmod{m} \quad \text{and} \quad v^2 m \equiv \pm 1 \pmod{n}, \tag{1}$$

for some integers u and v. Let χ_m, χ_n and χ_{mn} be the characters associated to base diagrams of level m, n and mn. Then there is a morphism of k-group schemes

$$\Xi : \mathrm{PGL}_m \times \mathrm{PGL}_n \to \mathrm{PGL}_{mn}$$

such that

$$\Xi(\chi_m(S), \chi_n(T)) = \chi_{mn}(uS + vT)$$

for all $S \in E[m](\overline{k})$ and $T \in E[n](\overline{k})$.

Let $[C \to \mathbb{P}^{n-1}]$ be a twist of the base diagram $[E \to \mathbb{P}^{n-1}]$. By definition this means that there is a commutative diagram

$$\begin{tikzcd} C \arrow[r] \arrow[d, "\alpha"'] & \mathbb{P}^{n-1} \arrow[d, "\beta"] \\ E \arrow[r] & \mathbb{P}^{n-1} \end{tikzcd}$$

where α and β are isomorphisms defined over $\overline{k}$. We say that the matrix $B_n \in \mathrm{PGL}_n(\overline{k})$ representing β is a flex matrix for $[C \to \mathbb{P}^{n-1}]$. In §6.2 we give some algorithms for computing flex matrices, starting from equations for C. Conversely, it is clear that we can recover equations for C from a flex matrix (by starting with equations for E and making the relevant substitution).

Our next result explains how Theorem 2.1 is used to construct an mn-covering from an m-covering and an n-covering.

Proposition 2.2. *In the setting of Theorem 2.1, suppose that $\xi \in H^1(k, E[m])$ and $\eta \in H^1(k, E[n])$ are represented by Brauer-Severi diagrams $[C_m \to \mathbb{P}^{m-1}]$ and $[C_n \to \mathbb{P}^{n-1}]$ with flex matrices B_m and B_n. Then $u\xi + v\eta \in H^1(k, E[mn])$ is represented by a Brauer-Severi diagram $[C_{mn} \to \mathbb{P}^{mn-1}]$ with flex matrix $B_{mn} = \Xi(B_m, B_n)$.*

PROOF: Let $\sigma \in \mathrm{Gal}(\overline{k}/k)$. Since $\sigma(B_m)B_m^{-1} = \chi_m(\xi_\sigma)$, $\sigma(B_n)B_n^{-1} = \chi_n(\eta_\sigma)$ and Ξ is defined over k, we have

$$\begin{aligned} \sigma(B_{mn})B_{mn}^{-1} &= \Xi(\sigma(B_m)B_m^{-1}, \sigma(B_n)B_n^{-1}) \\ &= \Xi(\chi_m(\xi_\sigma), \chi_n(\eta_\sigma)) \\ &= \chi_{mn}(u\xi_\sigma + v\eta_\sigma). \end{aligned}$$

Thus B_{mn} represents a change of co-ordinates on $\mathbb{P}^{mn-1}$ taking E to a curve C_{mn} defined over k. Then $[C_{mn} \to \mathbb{P}^{mn-1}]$ is the twist of $[E \to \mathbb{P}^{mn-1}]$ by $u\xi + v\eta \in H^1(k, E[mn])$. $\square$

Remark 2.3. The proposition shows that if ξ and η have trivial obstruction, then so does $u\xi + v\eta$. In fact, standard properties of the obstruction map (see [5, Paper I], [17], [25]) already show that

$$\mathrm{Ob}_{mn}(u\xi + v\eta) = u^2 n\, \mathrm{Ob}_m(\xi) + v^2 m\, \mathrm{Ob}_n(\eta) \tag{2}$$

for m and n coprime. Interestingly, the hypothesis (1) of Theorem 2.1 is that the coefficients on the right hand side of (2) are ± 1.

We are mainly interested in the case m and n are consecutive integers. We can therefore either take $u = v = 1$ in Theorem 2.1, or use the refined version of the theorem we give next.

We write $\mathbb{P}(\mathrm{Mat}_{a,b})$ for the projective space of dimension $ab-1$ formed from the vector space of $a \times b$ matrices. Taking $n \times n$ minors defines a rational map

$$\mu : \mathbb{P}(\mathrm{Mat}_{n,n+1}) \dashrightarrow \mathbb{P}^n ; \quad A \mapsto (\ldots : (-1)^i \det(A^{\{i\}}) : \ldots)$$

where $A^{\{i\}}$ is A with the ith column deleted. The following refinement of Theorem 2.1 is proved alongside the original theorem in §3.

Theorem 2.4. *Let $[\phi_n : E \to \mathbb{P}^{n-1}]$ and $[\phi_{n+1} : E \to \mathbb{P}^n]$ be base diagrams of levels n and $n+1$, with associated characters χ_n and χ_{n+1}. Then there is a base diagram*

$$[\phi_{n,n+1} : E \to \mathbb{P}(\mathrm{Mat}_{n,n+1})]$$

of level $n(n+1)$, with associated character $\chi_{n,n+1}$ given by

$$\chi_{n,n+1}(S+T) : A \mapsto \chi_n(S) A \chi_{n+1}(T)$$

for all $S \in E[n](\overline{k})$ and $T \in E[n+1](\overline{k})$. Moreover if $[n] : E \to E$ is the multiplication-by-n map then the diagram

$$\begin{tikzcd} E \arrow[r, "\phi_{n,n+1}"] \arrow[d, "{[n]}"'] & \mathbb{P}(\mathrm{Mat}_{n,n+1}) \arrow[d, dashed, "\mu"] \\ E \arrow[r, "\phi_{n+1}"] & \mathbb{P}^n . \end{tikzcd}$$

commutes.

We obtain equations for an $n(n+1)$-covering from an n-covering and an $(n+1)$-covering, by first finding the base diagram $\phi_{n,n+1}$ of Theorem 2.4, and then twisting by the flex matrices B_n and B_{n+1}. These twists may be performed one after the other. In fact twisting by B_n first gives the following generalisation of Theorem 2.4.

Theorem 2.5. *Let $[\phi_n : C \xrightarrow{|D|} \mathbb{P}^{n-1}]$ be a Brauer-Severi diagram and $[\phi_{n+1} : E \to \mathbb{P}^n]$ a base diagram, of levels n and $n+1$, with associated characters χ_n and χ_{n+1}. Then there is a Brauer-Severi diagram*

$$[\phi_{n,n+1} : C \xrightarrow{|(n+1)D|} \mathbb{P}(\mathrm{Mat}_{n,n+1})]$$

of level $n(n+1)$, with associated character $\chi_{n,n+1}$ given by

$$\chi_{n,n+1}(S+T) : A \mapsto \chi_n(S) A \chi_{n+1}(T)$$

for all $S \in E[n](\overline{k})$ and $T \in E[n+1](\overline{k})$. Moreover if $\pi : C \to E$ is the n-covering map then the diagram

$$\begin{tikzcd} C \arrow[r, "\phi_{n,n+1}"] \arrow[d, "\pi"'] & \mathbb{P}(\mathrm{Mat}_{n,n+1}) \arrow[d, dashed, "\mu"] \\ E \arrow[r, "\phi_{n+1}"] & \mathbb{P}^n \end{tikzcd}$$

commutes.

Proof: Theorem 2.4 is the special case where $(C, [D]) = (E, [n.\mathcal{O}])$. We twist by B_n to obtain the general result. □

The advantage of using Theorem 2.5 (instead of Theorem 2.4) is that we then only need to twist by B_{n+1} (rather than both B_n and B_{n+1}) to obtain the desired $n(n+1)$-covering. In §5 we use invariant theory to give an alternative proof of Theorem 2.5 in the cases $n = 2, 3$. In particular we obtain explicit formulae for $\phi_{2,3}$ and $\phi_{3,4}$ which we then use in our implementations of 6-descent and 12-descent.

3. The Heisenberg group

We continue to work over a field k of characteristic 0. Let E be an elliptic curve with identity $\mathcal{O}$, and $n \geq 2$ an integer. We recall that if D is a divisor on E of degree n then the Riemann-Roch space $\mathcal{L}(D)$ has dimension n. Let $V_n = \mathcal{L}(n.\mathcal{O})^*$. Then there is a "co-ordinate free" base diagram $[E \to \mathbb{P}(V_n)]$ with associated character $\chi_n : E[n] \to \mathrm{PGL}(V_n)$.

Definition 3.1. (i) The theta group Θ_n is the inverse image of $\chi_n(E[n])$ in $\mathrm{GL}(V_n)$. It sits in a commutative diagram of k-group schemes with exact rows:

$$\begin{tikzcd} 0 \arrow[r] & \mathbb{G}_m \arrow[r] \arrow[d, equal] & \Theta_n \arrow[r] \arrow[d] & E[n] \arrow[r] \arrow[d, "\chi_n"] & 0 \\ 0 \arrow[r] & \mathbb{G}_m \arrow[r] & \mathrm{GL}(V_n) \arrow[r] & \mathrm{PGL}(V_n) \arrow[r] & 0. \end{tikzcd}$$

(ii) The Heisenberg group H_n is the inverse image of $\chi_n(E[n])$ in $\mathrm{SL}(V_n)$. It sits in a commutative diagram of k-group schemes with exact rows:

$$\begin{tikzcd} 0 \arrow[r] & \mu_n \arrow[r] \arrow[d, equal] & H_n \arrow[r] \arrow[d] & E[n] \arrow[r] \arrow[d, "\chi_n"] & 0 \\ 0 \arrow[r] & \mu_n \arrow[r] & \mathrm{SL}(V_n) \arrow[r] & \mathrm{PGL}(V_n) \arrow[r] & 0. \end{tikzcd}$$

Remark 3.2. It is well known (see e.g. [13]) that over $k = \overline{k}$ we may choose a basis for V_n such that Θ_n is generated by

$$\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & \zeta_n & 0 & \cdots & 0 \\ 0 & 0 & \zeta_n^2 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & \zeta_n^{n-1} \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix},$$

and the scalar matrices. (Here $\zeta_n \in k$ is a primitive nth root of unity.) In particular, taking commutators in Θ_n defines a non-degenerate pairing $e_n : E[n] \times E[n] \to \mu_n$, which turns out to be the Weil pairing.

The group $H_n(\overline{k})$ is a non-abelian group of order n^3 with centre $\mu_n(\overline{k})$.

Definition 3.3. A representation $\rho : H_n(\overline{k}) \to \mathrm{GL}_d(\overline{k})$ has central character $[r]$ if $\rho(\zeta) = \zeta^r I_d$ for all $\zeta \in \mu_n(\overline{k})$.

Lemma 3.4. *Let r be an integer coprime to n. Then*
(i) Every representation of $H_n(\overline{k})$ with central character $[r]$ is a direct sum of irreducible n-dimensional representations.
(ii) Up to equivalence, there is a unique n-dimensional representation of $H_n(\overline{k})$ with central character $[r]$.

PROOF: Let ρ be a representation of $H_n(\overline{k})$ with central character $[r]$. If $\sigma, \tau \in H_n(\overline{k})$ lift $S, T \in E[n](\overline{k})$ then $\rho(\sigma)\rho(\tau)\rho(\sigma)^{-1} = e_n(S,T)^r \rho(\tau)$ and so $\mathrm{Tr}(\rho(\tau)) = e_n(S,T)^r \,\mathrm{Tr}(\rho(\tau))$. Since r is coprime to n, the character of ρ vanishes outside the centre of $H_n(\overline{k})$. Then orthogonality relations in the character table show that ρ is irreducible if and only if it has dimension n. This proves (i) and the uniqueness in (ii). Existence is clear in the case $r = 1$. In general we take the rth tensor power and apply (i). $\square$

To prove Theorem 2.1 we need to construct a morphism Ξ that is defined over k. We therefore study representations $\rho : H_n(\overline{k}) \to \mathrm{GL}_d(\overline{k})$ that are Galois equivariant, equivalently those that induce a morphism of k-group schemes $H_n \to \mathrm{GL}_d$. We call these representations of H_n.

By construction, V_n is an n-dimensional representation of H_n with central character [1]. So by Lemma 3.4(i) it is irreducible. We might hope to construct other irreducible n-dimensional representations of H_n by any one of the following standard methods.

(i) Take a subspace or quotient of a tensor power of V_n.
(ii) Replace V_n by one of its Galois conjugates.
(iii) Precompose $\rho : H_n \to \mathrm{GL}(V_n)$ with an automorphism of H_n.

We see no way of using (i) in the proof of Theorem 2.1, other than in the case of $V_n^* = \wedge^{n-1} V_n$. (The problem is that there is no analogue of Lemma 3.4(i) with H_n replaced by GL_n.) Our restriction to Galois equivariant representations rules out the use of (ii).

To use (iii) we must first describe the (Galois equivariant) automorphisms of H_n. Each automorphism of H_n induces an automorphism of $E[n]$. We may identify $\mathrm{Aut}(E[n])$ as the centraliser of the image of Galois in $\mathrm{Aut}_{\overline{k}}(E[n]) \cong \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. So in general the only automorphisms of $E[n]$ are the maps $T \mapsto aT$ for $a \in (\mathbb{Z}/n\mathbb{Z})^\times$. We show that each of these maps lifts to an automorphism of H_n. (Without our insistence on Galois equivariance, this would be trivial.)

Lemma 3.5. *For each $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ there is a morphism of k-group schemes $\psi_a : H_n \to H_n$ making the diagram*

$$\begin{tikzcd} 0 \arrow[r] & \mu_n \arrow[r] \arrow[d, "a^2"] & H_n \arrow[r] \arrow[d, "\psi_a"] & E[n] \arrow[r] \arrow[d, "a"] & 0 \\ 0 \arrow[r] & \mu_n \arrow[r] & H_n \arrow[r] & E[n] \arrow[r] & 0 \end{tikzcd}$$

commute.

Proof: The $[-1]$-map on E lifts to a matrix $\iota \in \mathrm{GL}_n(k)$. Conjugation by ι gives the map ψ_{-1}. In general we first define

$$\lambda : H_n \to \mu_n\,; \quad h \mapsto \iota h \iota^{-1} h$$

and then put

$$\psi_a : H_n \to H_n\,; \quad h \mapsto \lambda(h)^{a(a-1)/2} h^a.$$

Since $\lambda(xy) = xy(\iota x \iota^{-1})(\iota y \iota^{-1}) = \lambda(x)\lambda(y)xyx^{-1}y^{-1}$ for all $x, y \in H_n$, it is easy to check that ψ_a is a group homomorphism. Galois equivariance is clear from the construction. □

Let $V_n^{(a)}$ be the representation of H_n given by

$$H_n \times V_n \to V_n\,; \quad (h, v) \mapsto \psi_a(h)v.$$

It is an irreducible n-dimensional representation of H_n with central character $[a^2]$. Taking these representations and their duals we obtain all the representations of Lemma 3.4(ii) with $r \equiv \pm a^2 \pmod{n}$.

We write $\tau_P : E \to E$ for translation by $P \in E(\overline{k})$. We recall from [16, §23], (see also [5, Paper I]), that the theta group Θ_n may be described as pairs

$$\Theta_n(\overline{k}) = \{\, (f, T) \in \overline{k}(E)^\times \times E[n](\overline{k}) \mid \mathrm{div}(f) = \tau_T^*(n.\mathcal{O}) - n.\mathcal{O} \,\}$$

with group law

$$(f,S) * (g,T) = ((\tau_T^* f)g, S+T). \tag{3}$$

There is a natural action of Θ_n on $V_{nN}^* = \mathcal{L}(nN.\mathcal{O})$ given by

$$(f,T) : \ h \mapsto \tau_{-T}^*(h/f^N). \tag{4}$$

We use this notation to relate the Heisenberg groups H_n for different levels n.

Proposition 3.6. *Let m and n be coprime integers. Then there is an isomorphism of k-group schemes*

$$\begin{array}{rcl} H_m \times H_n & \cong & H_{mn} \\ ((f,S),(g,T)) & \mapsto & (f^n,S) * (g^m,T). \end{array}$$

For the proof we need two lemmas.

Lemma 3.7. *Let $M_T \in \Theta_n(\overline{k})$ be a lift of $T \in E[n](\overline{k})$. If T has exact order r then*

$$\det(M_T) = (-1)^{n(n-1)/r} M_T^n.$$

Proof: By Remark 3.2 we know that M_T is similar to

$$\lambda \, \mathrm{Diag}(1, \zeta_r, \ldots, \zeta_r^{n-1})$$

for some $\lambda \in \overline{k}^\times$ and ζ_r a primitive rth root of unity. Then $\det(M_T) = \zeta_r^{n(n-1)/2} M_T^n = (-1)^{n(n-1)/r} M_T^n$ as required. □

Lemma 3.8. *Let N be a positive integer. Then there is a commutative diagram of k-group schemes*

$$\begin{array}{ccc} \Theta_n & \xrightarrow{\alpha} & \Theta_{nN} \\ \Big\downarrow{\scriptstyle \det} & & \Big\downarrow{\scriptstyle \det} \\ \mathbb{G}_m & \xrightarrow{N^2} & \mathbb{G}_m. \end{array}$$

where $\alpha : (f,T) \mapsto (f^N, T)$.

Proof: It is clear from (3) that α is a group homomorphism. Now let $x \in \Theta_n$ and assume n is odd. Using Lemma 3.7 we compute

$$\det(\alpha(x)) = \alpha(x)^{nN} = \alpha(\det x)^N = (\det x)^{N^2}.$$

The calculation for n even is similar. □

Proof of Proposition 3.6: Let (f,S) and (g,T) be elements of $\Theta_m(\overline{k})$ and $\Theta_n(\overline{k})$. The commutator of (f^n,S) and (g^m,T) in $\Theta_{mn}(\overline{k})$

is both an mth root of unity and an nth root of unity, and therefore trivial. So there is a morphism of k-group schemes

$$\begin{array}{rcl} \Theta_m \times \Theta_n & \to & \Theta_{mn} \\ ((f,S),(g,T)) & \mapsto & (f^n,S) * (g^m,T). \end{array}$$

By Lemma 3.8 we can restrict to a map $H_m \times H_n \to H_{mn}$. Since m and n are coprime, this restriction is clearly an isomorphism. □

We recall that H_n acts on $\mathcal{L}(nN.\mathcal{O})$ as specified in (4).

Lemma 3.9. *The H_n-invariant subspace of $\mathcal{L}(nN.\mathcal{O})$ is trivial unless n divides N, in which case it has dimension N/n.*

Proof: By Lemma 3.8 there is a group homomorphism $H_n(\overline{k}) \to H_{nN}(\overline{k})$ given by $(f,T) \mapsto (f^N,T)$. By the proof of Lemma 3.4 the character of $\mathcal{L}(nN.\mathcal{O})$ is trivial outside the centre of $H_{nN}(\overline{k})$. The same is therefore true when $\mathcal{L}(nN.\mathcal{O})$ is viewed as a representation of $H_n(\overline{k})$. We are done by the orthogonality relations in the character table. □

Proposition 3.10. *Let m and n be coprime integers. Suppose that $n \equiv a^2 \pmod{m}$ and $m \equiv b^2 \pmod{n}$ for some integers a and b. Then there is a k-isomorphism of H_{mn}-representations*

$$\pi : V_m^{(a)} \otimes V_n^{(b)} \cong V_{mn}.$$

Proof: We recall that $V_m^{(a)}$ is an irreducible H_m-representation with central character $[a^2]$. Likewise $V_n^{(b)}$ is an irreducible H_n-representation with central character $[b^2]$. Then Proposition 3.6 makes $V_m^{(a)} \otimes V_n^{(b)}$ an irreducible H_{mn}-representation with central character $[1]$. Indeed $(\zeta_m,\zeta_n) \in H_m \times H_n$ acts on $V_m^{(a)} \otimes V_n^{(b)}$ as $\zeta_m^{a^2}\zeta_n^{b^2}$ and on V_{mn} as $\zeta_m^n\zeta_n^m$. The required isomorphism π exists by Lemma 3.4(ii). Finally, since we work with Galois equivariant representations, we can choose an isomorphism π that is defined over k. □

Proof of Theorem 2.1: We first treat the case $u^2n \equiv 1 \pmod{m}$ and $v^2m \equiv 1 \pmod{n}$. Let a and b be inverses for u and v modulo m and n respectively. Then the map $\pi : V_m \otimes V_n \to V_{mn}$ constructed in Proposition 3.10 satisfies

$$\pi(\psi_a(f,S)v_m \otimes \psi_b(g,T)v_n) = ((f^n,S) * (g^m,T))\pi(v_m \otimes v_n)$$

for all $(f,S) \in H_m$, $(g,T) \in H_n$, $v_m \in V_m$, $v_n \in V_n$. Passing to $\mathbb{P}(V_{mn})$ we obtain

$$\pi(\chi_m(aS)v_m \otimes \chi_n(bT)v_n) = \chi_{mn}(S+T)\pi(v_m \otimes v_n).$$

Hence

$$\pi \circ (\chi_m(aS) \boxtimes \chi_n(bT)) = \chi_{mn}(S+T) \circ \pi$$

where

$$\boxtimes : \mathrm{PGL}(V_m) \times \mathrm{PGL}(V_n) \to \mathrm{PGL}(V_m \otimes V_n)$$

is the natural map. The theorem now holds on defining

$$\begin{array}{rcl} \Xi : \mathrm{PGL}(V_m) \times \mathrm{PGL}(V_n) & \to & \mathrm{PGL}(V_{mn}) \\ (\alpha, \beta) & \mapsto & \pi \circ (\alpha \boxtimes \beta) \circ \pi^{-1}. \end{array}$$

In general, if $u^2 n \equiv -1 \pmod m$ or $v^2 m \equiv -1 \pmod n$ then we replace $V_m^{(a)}$ or $V_n^{(b)}$ by its dual in Proposition 3.10, and the proof carries through as before. □

Next we prove our refined version of the theorem in the case m and n are consecutive integers.

Proof of Theorem 2.4: The analogue of Proposition 3.10 gives a k-isomorphism of $H_{n(n+1)}$-modules

$$\pi : V_n \otimes V_{n+1}^* \cong V_{n(n+1)}.$$

Hence there is a base diagram

$$\phi_{n,n+1} : E \to \mathbb{P}(V_n \otimes V_{n+1}^*) \tag{5}$$

with associated character

$$\chi_{n,n+1}(S+T) = \chi_n(S) \boxtimes \chi_{n+1}(T)^*.$$

Picking bases for V_n and V_{n+1}, we identify $\mathbb{P}(V_n) = \mathbb{P}^{n-1}$, $\mathbb{P}(V_{n+1}) = \mathbb{P}^n$ and $\mathbb{P}(V_n \otimes V_{n+1}^*) = \mathbb{P}(\mathrm{Mat}_{n,n+1})$. Then $\chi_{n,n+1}$ is given by

$$\chi_{n,n+1}(S+T) : A \mapsto \chi_n(S) A \chi_{n+1}(\pm T)$$

where the sign $\pm$ is immaterial by the case $a = -1$ of Lemma 3.5. This proves the first statement of Theorem 2.4.

The base diagram (5) is given by a matrix $\mathfrak{A} \in \mathrm{Mat}_{n,n+1}(k(E))$ whose entries are a basis for $\mathcal{L}(n(n+1).\mathcal{O})$. Let r be the rank of this matrix. Then the $r \times r$ minors define a morphism

$$\Phi : E \to \mathbb{P}(\wedge^r V_{n+1}^*)$$

with the property that $\Phi \circ \tau_S = \Phi$ for all $S \in E[n](\overline{k})$. Hence Φ factors through $[n] : E \to E$. Therefore $n^2 \mid \deg(\Phi^* H)$ where H is the hyperplane section on $\mathbb{P}(\wedge^r V_{n+1}^*)$. Since $\deg(\Phi^* H) = rn(n+1)$ it follows that $r = n$. Thus there is a commutative diagram

$$\begin{tikzcd} E \arrow[r, "\phi_{n,n+1}"] \arrow[d, "{[n]}"'] & \mathbb{P}(V_n \otimes V_{n+1}^*) \arrow[d, dashed, "\mu"] \\ E \arrow[r, "\gamma"] & \mathbb{P}(V_{n+1}) \end{tikzcd}$$

where the pull back of the hyperplane section by γ has degree $n+1$. We must show that $\gamma = \phi_{n+1}$.

It is easy to see that γ shares with ϕ_{n+1} the property

$$\gamma(T + P) = \chi_{n+1}(T)\gamma(P)$$

for all $T \in E[n+1](\overline{k})$ and $P \in E(\overline{k})$. Since V_{n+1} is an irreducible representation of H_{n+1} the image of γ spans $\mathbb{P}(V_{n+1})$. So γ is an embedding by a complete linear system.

By Lemma 3.9 the subspace of $\mathcal{L}(n^2(n+1).\mathcal{O})$ fixed by H_n has dimension $n+1$. Since the $n \times n$ minors of $\mathfrak{A}$ are linearly independent they are a basis for this space. We show in Proposition 3.11 that if $g \in \overline{k}(E)^\times$ with

$$\operatorname{div}(g) = (n+1)[n]^*\mathcal{O} - n^2(n+1).\mathcal{O}$$

then g is fixed by H_n. Hence we may assume that the first $n \times n$ minor of $\mathfrak{A}$, viewed as a homogeneous form of degree n in the co-ordinate ring of $\mathbb{P}(V_n \otimes V_{n+1}^*)$, meets E with divisor $(n+1)[n]^*\mathcal{O}$. Then $(n+1).\mathcal{O}$ is the pull back of a hyperplane section by γ, and hence γ is a base diagram of level $n+1$.

Since γ and ϕ_{n+1} are base diagrams of level $n+1$ they can only differ by an element of $\mathrm{PGL}(V_{n+1})$. But they also have the same character χ_{n+1}. Since the image of χ_{n+1} is its own centraliser in $\mathrm{PGL}(V_{n+1})$, it follows that $\gamma = \phi_{n+1}$ as required. $\square$

Let $\sigma : \operatorname{Div}(E) \to E$ be the summation map. An unexpected difficulty in the proof of Theorem 2.5 is showing that, if D is a hyperplane section for the image of γ, then $\sigma(D) = \mathcal{O}$. (Comparing pull backs via $\mu \circ \phi_{n,n+1}$ and $\gamma \circ [n]$ only gives that $\sigma(D)$ is an n-torsion point.) We appeal to the case $N = n+1$ of the following proposition.

Proposition 3.11. *Let $g \in \overline{k}(E)^\times$ with $\operatorname{div}(g) = [n]^*\mathcal{O} - n^2.\mathcal{O}$. Then g^N is fixed by the natural action of H_n on $\mathcal{L}(n^2 N.\mathcal{O})$.*

For the proof we need two lemmas.

Lemma 3.12. *Let $T \in E(\overline{k})$ be a point of exact order n. Let $f \in \overline{k}(E)^\times$ with $\mathrm{div}(f) = n.T - n.\mathcal{O}$. If $S \in E(\overline{k})$ with $2S = T$ and $nS \neq \mathcal{O}$ then*

$$\prod_{i=0}^{n-1} f(S + iT) = f(S)^n.$$

Proof: The rational function $P \mapsto f(P)f(T - P)$ has trivial divisor and is therefore constant. Hence for any integer i,

$$f(S + iT)f(S - iT) = f(S)^2.$$

We are immediately done in the case n is odd. In the case n is even it remains to show that $f(S) = f(S + T_2)$ where $T_2 = \frac{n}{2}T \in E[2](\overline{k})$. Let $x \in \overline{k}(E)^\times$ with $\mathrm{div}(x) = 2.T_2 - 2.\mathcal{O}$. Then comparing divisors gives

$$\prod_{i=0}^{(n-2)/2} \tau_{-iT}^* f = c x^{n/2}$$

for some constant $c \in \overline{k}^\times$. Evaluating each side at $\pm S$ we deduce

$$\frac{f(S + T_2)}{f(S)} = \left(\frac{x(-S)}{x(S)}\right)^{n/2} = 1.$$

□

Lemma 3.13. *Let $T \in E(\overline{k})$ be a point of exact order n. Let $f, g \in \overline{k}(E)^\times$ with $\mathrm{div}(f) = n.T - n.\mathcal{O}$ and $\mathrm{div}(g) = [n]^*\mathcal{O} - n^2.\mathcal{O}$. Then*
(i) The pair $(f, -T)$ belongs to H_n if and only if $\prod_{i=0}^{n-1} \tau_{iT}^* f = (-1)^{n-1}$.
(ii) If f satisfies (i) then $\frac{g}{\tau_{-T}^* g} = f^n$.

Proof: (i) By Lemma 3.7 the pair $(f, -T)$ belongs to H_n if and only if $(f, -T)^n = (-1)^{n-1}$. By the group law (3) this is equivalent to the stated condition.
(ii) Each side has divisor $n^2.T - n^2.\mathcal{O}$. So it suffices to check equality at $S \in E(\overline{k})$ with $2S = T$ and $nS \neq \mathcal{O}$. Since g has a pole of order $n^2 - 1$ at $\mathcal{O}$, we deduce $[-1]^*g = (-1)^{n-1}g$. So the left hand side evaluated at S is $(-1)^{n-1}$. By (i) and Lemma 3.12 we also get $(-1)^{n-1}$ on the right hand side. □

Proof of Proposition 3.11: If $(f, -T) \in H_n$ then

$$(f, -T)g^N = \tau_T^*(g^N / f^{nN}) = g^N$$

where for the first equality we use (4), and for the second equality we use Lemma 3.13. □

4. Invariant Theory

We recall some classical invariant theory of binary quartics and ternary cubics, as surveyed in [1]. We then add to this theory by introducing what we call "covariant columns". These are used in §5 to give formulae for $\phi_{2,3}$ and $\phi_{3,4}$. In this section we give a complete classification of the covariant columns. This is more that we need in §5, but serves to explain where our formulae come from.

In this section k will be a field with $\mathrm{char}\,(k) \neq 2, 3$.

4.1. **Binary quartics.** We study the invariants and covariants of the binary quartic

$$U(x_1, x_2) = ax_1^4 + bx_1^3x_2 + cx_1^2x_2^2 + dx_1x_2^3 + ex_2^4.$$

For a polynomial $F \in k[x_1, x_2]$ and matrix $g \in \mathrm{GL}_2(k)$ we write

$$(F \circ g)(x_1, x_2) \quad = \quad F(g_{11}x_1 + g_{12}x_2, g_{21}x_1 + g_{22}x_2)$$

Thus $(F \circ g)(\mathbf{x}) = F(g\mathbf{x})$ where $\mathbf{x}$ is the column vector $(x_1, x_2)^T$.

Definition 4.1. A covariant $F = F(U; \mathbf{x})$ of order m, degree d and weight p, is a homogeneous polynomial of degree m in x_1, x_2, whose coefficients are homogeneous polynomials of degree d in the coefficients of the binary quartic U, such that

$$F(U \circ g; \mathbf{x}) = (\det g)^p F(U; g\mathbf{x})$$

for all $g \in \mathrm{GL}_2(\overline{k})$.

By considering g a scalar matrix, it is clear that the order m, degree d and weight p of a covariant are related by $4d = 2p + m$. It is well known that the ring of invariants (an invariant is a covariant of order 0) is generated by c_4 and c_6 where

$$\begin{aligned} c_4 &= 2^4(12ae - 3bd + c^2) \\ c_6 &= 2^5(72ace - 27ad^2 - 27b^2e + 9bcd - 2c^3). \end{aligned}$$

Moreover, the ring of covariants is generated by c_4, c_6, U, H and J, where

$$H(x_1, x_2) \quad = \quad \tfrac{1}{3} \det \left(\frac{\partial^2 U}{\partial x_i \partial x_j} \right)_{i,j=1,2}$$

and

$$J(x_1, x_2) \quad = \quad \frac{1}{12} \frac{\partial(U,H)}{\partial(x_1,x_2)} \;, \tag{6}$$

subject only to the relation

$$27J^2 = -H^3 + 3c_4HU^2 - 2c_6U^3. \tag{7}$$

Since c_4, c_6, U, H and J have weights 4, 6, 0, 2 and 3 we deduce

Lemma 4.2. *Every covariant of odd weight is divisible by J.*

We now define what we call a "covariant column".

Definition 4.3. A covariant column $\mathbf{v} = \mathbf{v}(U; \mathbf{x})$ of order m, degree d and weight p, is a column vector $\mathbf{v} = (v_1, v_2)^T$ of degree m homogeneous polynomials in x_1, x_2, whose coefficients are homogeneous polynomials of degree d in the coefficients of the binary quartic U, such that

$$\mathbf{v}(U \circ g; \mathbf{x}) = (\det g)^p g^{-1} \mathbf{v}(U; g\mathbf{x})$$

for all $g \in \mathrm{GL}_2(\overline{k})$.

By considering g a scalar matrix, it is clear that the order m, degree d and weight p of a covariant column are related by $4d = 2p+m-1$. The column vector $\mathbf{x}$ itself is a covariant column of order 1, degree 0 and weight 0. The proof of the following lemma is entirely straightforward, and so will be omitted.

Lemma 4.4. *(i) If F is a covariant of order m, degree d and weight p then $\partial F = (-\frac{\partial F}{\partial x_2}, \frac{\partial F}{\partial x_1})^T$ is a covariant column of order $m-1$, degree d and weight $p+1$,*
(ii) If $\mathbf{v}_1$ and $\mathbf{v}_2$ are covariant columns of orders m_1, m_2, degrees d_1, d_2 and weights p_1, p_2, then the determinant $[\mathbf{v}_1, \mathbf{v}_2]$ is a covariant of order $m_1 + m_2$, degree $d_1 + d_2$ and weight $p_1 + p_2 - 1$.

For F a covariant of order m we have $[\mathbf{x}, \partial F] = mF$.

Theorem 4.5. *(i) The covariant columns of even weight form a free $k[c_4, c_6, U, H]$-module of rank 2 with basis $\mathbf{x}$, ∂J.*
(ii) The covariant columns of odd weight form a free $k[c_4, c_6, U, H]$-module of rank 2 with basis ∂U, ∂H.

PROOF: (i) Since $[\mathbf{x}, \partial J] = 6J \neq 0$, we can write any covariant column as $\mathbf{v} = F_1 \mathbf{x} + F_2 \partial J$ for some rational functions F_1 and F_2. Then $[\mathbf{v}, \partial J] = 6JF_1$ is a covariant of odd weight. It follows by Lemma 4.2 that F_1 is a covariant. The same argument shows that F_2 is a covariant.
(ii) Since we can rewrite (6) as $[\partial U, \partial H] = 12J$, the proof carries over exactly as in case (i). □

Corollary 4.6. *The covariant columns form a module over the ring of covariants, generated by $\mathbf{x}$, ∂U, ∂H, ∂J, subject only to the relations*

$$\begin{aligned}
3J\mathbf{x} &= H\partial U - U\partial H \\
18J\partial J &= 2(c_4 UH - c_6 U^2)\partial U + (c_4 U^2 - H^2)\partial H \\
9J\partial U &= (c_4 U^2 - H^2)\mathbf{x} + 6U\partial J \\
9J\partial H &= 2(c_6 U^2 - c_4 UH)\mathbf{x} + 6H\partial J
\end{aligned}$$

PROOF: It only remains to describe the action of multiplication by J. The first relation is obtained by applying the proof of Theorem 4.5(ii) to $\mathbf{v} = J\mathbf{x}$, and the second is obtained by differentiating the syzygy (7). We take linear combinations, and use the syzygy once more to obtain the final two relations. $\square$

4.2. **Ternary cubics.** We study the invariants and covariants of the ternary cubic

$$U(x_1, x_2, x_3) = ax_1^3 + bx_2^3 + cx_3^3 + \ldots + mx_1x_2x_3.$$

For a polynomial $F \in k[x_1, x_2, x_3]$ and matrix $g \in \mathrm{GL}_3(k)$ we write $(F \circ g)(\mathbf{x}) = F(g\mathbf{x})$ where $\mathbf{x}$ is the column vector $(x_1, x_2, x_3)^T$. The definition of a covariant is exactly analogous to that in the case of a binary quartic. By considering g a scalar matrix, it is clear that the order m, degree d and weight p of a covariant are related by $3d = 3p+m$.

The Hessian is a covariant of order 3, degree 3 and weight 2 given by

$$H(x_1, x_2, x_3) \quad = \quad -\tfrac{1}{2} \det \left(\frac{\partial U}{\partial x_i \partial x_j} \right)_{i,j=1,2,3}.$$

There are invariants c_4 and c_6 such that

$$H(\lambda U + \mu H) = 3(c_4\lambda^2\mu + 2c_6\lambda\mu^2 + c_4^2\mu^3)U + (\lambda^3 - 3c_4\lambda\mu^2 - 2c_6\mu^3)H,$$

and it is well known that these generate the ring of invariants.

If $Q_1(\mathbf{x})$ and $Q_2(\mathbf{x})$ are ternary quadrics, with corresponding 3×3 symmetric matrices A_1 and A_2, *i.e.*

$$Q_1(\mathbf{x}) \quad = \quad \tfrac{1}{2}\mathbf{x}^T A_1 \mathbf{x} \quad \text{and} \quad Q_2(\mathbf{x}) \quad = \quad \tfrac{1}{2}\mathbf{x}^T A_2 \mathbf{x},$$

then we write $\{Q_1, Q_2\}$ for the 3×3 symmetric matrix satisfying

$$\mathrm{adj}(A_1 + tA_2) = \mathrm{adj}(A_1) + t\{Q_1, Q_2\} + t^2 \,\mathrm{adj}(A_2).$$

We can then define a symmetric matrix of quadrics

$$M \quad = \quad \textstyle\sum_{i,j=1}^3 \left\{ \frac{\partial U}{\partial x_i}, \frac{\partial H}{\partial x_j} \right\} x_i x_j$$

and covariants

$$\begin{aligned} \Theta(x_1, x_2, x_3) \quad &= \quad \textstyle\sum_{r,s=1}^3 M_{rs} \frac{\partial U}{\partial x_r} \frac{\partial H}{\partial x_s} \\ J(x_1, x_2, x_3) \quad &= \quad \frac{1}{3} \frac{\partial(U,H,\Theta)}{\partial(x_1,x_2,x_3)}. \end{aligned} \tag{8}$$

Again it is well known that the ring of covariants is generated by c_4, c_6, U, H, Θ and J subject only to a relation which reduces mod U to

$$J^2 \equiv \Theta^3 - 27c_4\Theta H^4 - 54c_6H^6 \pmod{U}. \tag{9}$$

Since c_4, c_6, U, H, Θ and J have weights 4, 6, 0, 2, 6 and 9 we deduce

Lemma 4.7. *Every covariant of odd weight is divisible by J.*

Our definition of a covariant column is exactly analogous to that in the case of a binary quartic. However we now also need to work with "contravariant columns".

Definition 4.8. A covariant column, respectively contravariant column, $\mathbf{v} = \mathbf{v}(U; \mathbf{x})$ of order m, degree d and weight p, is a column vector $\mathbf{v} = (v_1, v_2, v_3)^T$ of degree m homogeneous polynomials in x_1, x_2, x_3, whose coefficients are homogeneous polynomials of degree d in the coefficients of the ternary cubic U, such that

$$\mathbf{v}(U \circ g; \mathbf{x}) = (\det g)^p g^{-1} \mathbf{v}(U; g\mathbf{x}),$$

respectively

$$\mathbf{v}(U \circ g; \mathbf{x}) = (\det g)^p g^T \mathbf{v}(U; g\mathbf{x}),$$

for all $g \in \mathrm{GL}_3(\overline{k})$.

By considering g a scalar matrix, it is clear that the order m, degree d and weight p of a covariant column, respectively contravariant column, are related by $3d = 3p + m - 1$, respectively $3d = 3p + m + 1$. The column vector $\mathbf{x}$ itself is a covariant column of order 1, degree 0 and weight 0. The proof of the following lemma is entirely straightforward, and so will be omitted.

Lemma 4.9. *(i) If F is a covariant of order m, degree d and weight p then $\nabla F = (\frac{\partial F}{\partial x_1}, \frac{\partial F}{\partial x_2}, \frac{\partial F}{\partial x_3})^T$ is a contravariant column of order $m-1$, degree d and weight p.*
(ii) Let $\mathbf{v}_1$ and $\mathbf{v}_2$ be covariant or contravariant columns of orders m_1, m_2, degrees d_1, d_2 and weights p_1, p_2. Then

1. *If $\mathbf{v}_1$ is a covariant column, and $\mathbf{v}_2$ a contravariant column then the dot product $\mathbf{v}_1 \cdot \mathbf{v}_2$ is a covariant of order $m_1 + m_2$, degree $d_1 + d_2$ and weight $p_1 + p_2$.*
2. *If $\mathbf{v}_1$ and $\mathbf{v}_2$ are covariant columns then the cross product $\mathbf{v}_1 \times \mathbf{v}_2$ is a contravariant column of order $m_1 + m_2$, degree $d_1 + d_2$ and weight $p_1 + p_2 - 1$.*
3. *If $\mathbf{v}_1$ and $\mathbf{v}_2$ are contravariant columns then the cross product $\mathbf{v}_1 \times \mathbf{v}_2$ is a covariant column of order $m_1 + m_2$, degree $d_1 + d_2$ and weight $p_1 + p_2 + 1$.*

(iii) If $\mathbf{v}$ is a contravariant column of order m, degree d and weight p, then $M\mathbf{v}$ is covariant column of order $m + 2$, degree $d + 4$ and weight $p + 4$.

For F a covariant of order m we have $\mathbf{x}.\nabla F = mF$. The determinant of the three vectors $\mathbf{v}_1$, $\mathbf{v}_2$, $\mathbf{v}_3$ will be denoted

$$[\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3] \;=\; (\mathbf{v}_1 \times \mathbf{v}_2) \cdot \mathbf{v}_3 \;=\; \mathbf{v}_1 \cdot (\mathbf{v}_2 \times \mathbf{v}_3).$$

We define contravariant columns $\mathbf{u} = \nabla U$, $\mathbf{h} = \nabla H$, $\mathbf{t} = \nabla \Theta$ and covariant columns $\mathbf{e} = M\mathbf{u}$ and $\mathbf{f} = M\mathbf{h}$.

Theorem 4.10. *(i) The covariant columns, respectively contravariant columns, of even weight form a free* $k[c_4, c_6, U, H, \Theta]$*-module of rank* 3 *with basis* $\mathbf{x}$, $\mathbf{e}$, $\mathbf{f}$, *respectively* $\mathbf{u}$, $\mathbf{h}$, $\mathbf{t}$.
(ii) The covariant columns, respectively contravariant columns, of odd weight form a free $k[c_4, c_6, U, H, \Theta]$*-module of rank* 3 *with basis* $\mathbf{u} \times \mathbf{h}$, $\mathbf{u} \times \mathbf{t}$, $\mathbf{h} \times \mathbf{t}$, *respectively* $\mathbf{x} \times \mathbf{e}$, $\mathbf{x} \times \mathbf{f}$, $\mathbf{e} \times \mathbf{f}$.

Proof: (i) Since $[\mathbf{x}, \mathbf{e}, \mathbf{f}] = -2J \neq 0$, we can write any covariant column as $\mathbf{v} = F_1\mathbf{x} + F_2\mathbf{e} + F_3\mathbf{f}$ for some rational functions F_1, F_2, F_3. Then $[\mathbf{v}, \mathbf{e}, \mathbf{f}] = -2JF_1$ is a covariant of odd weight. It follows by Lemma 4.7 that F_1 is a covariant, and likewise for F_2 and F_3. The case of a contravariant column is similar, since we can rewrite (8) as $[\mathbf{u}, \mathbf{h}, \mathbf{t}] = 3J$.
(ii) Since $[\mathbf{u} \times \mathbf{h}, \mathbf{u} \times \mathbf{t}, \mathbf{h} \times \mathbf{t}] = [\mathbf{u}, \mathbf{h}, \mathbf{t}]^2 = 9J^2 \neq 0$, we can write any covariant column as $\mathbf{v} = F_1(\mathbf{u} \times \mathbf{h}) + F_2(\mathbf{u} \times \mathbf{t}) + F_3(\mathbf{h} \times \mathbf{t})$ for some rational functions F_1, F_2, F_3. Then $\mathbf{v} \cdot \mathbf{t} = 3JF_1$ is a covariant of odd weight. It follows by Lemma 4.7 that F_1 is a covariant, and likewise for F_2 and F_3. The case of a contravariant column is similar. □

Corollary 4.11. *(i) The covariant columns are generated as a module over the ring of covariants by* $\mathbf{x}$, $\mathbf{e}$, $\mathbf{f}$, $\mathbf{u} \times \mathbf{h}$, $\mathbf{u} \times \mathbf{t}$ *and* $\mathbf{h} \times \mathbf{t}$.
(ii) The contravariant columns are generated as a module over the ring of covariants by $\mathbf{u}$, $\mathbf{h}$, $\mathbf{t}$, $\mathbf{x} \times \mathbf{e}$, $\mathbf{x} \times \mathbf{f}$ *and* $\mathbf{e} \times \mathbf{f}$.

As in the case of binary quartics, there is no difficulty in finding the relations (describing the effect of multiplication by J). Since these relations are somewhat messy, we instead record the identities

$$\mathbf{x} \cdot \mathbf{u} = 3U, \quad \mathbf{x} \cdot \mathbf{h} = 3H, \quad \mathbf{x} \cdot \mathbf{t} = 6\Theta, \quad \mathbf{e} \cdot \mathbf{h} = \mathbf{f} \cdot \mathbf{u} = \Theta$$

and

$$\begin{aligned}
\mathbf{e} \cdot \mathbf{u} &= 3(H^2 - 3c_4U^2) \\
\mathbf{f} \cdot \mathbf{h} &= 3(3c_4H^2 - 8c_6UH + 3c_4^2U^2) \\
\mathbf{e} \cdot \mathbf{t} &= 12(3c_4H^3 - c_4U\Theta - 12c_6UH^2 + 9c_4^2U^2H) \\
\mathbf{f} \cdot \mathbf{t} &= 12(c_4H\Theta - 3c_6H^3 - 3c_6U\Theta + 9c_4^2UH^2 - 3c_4c_6U^2H - 9c_4^3U^3)
\end{aligned}$$

from which the relations may be recovered by following the proof of Theorem 4.10.

5. Covariant matrices

We use the invariant theory of binary quartics and ternary cubics to given an alternative proof of Theorem 2.5 in the cases $n = 2, 3$.

5.1. **The case** $n = 2$**.** A binary quartic $U \in k[x_1, x_2]$ is non-singular if its discriminant $\Delta = (c_4^3 - c_6^2)/1728$ is non-zero. We write $\mathbb{P}(1, 1, 2)$ for the weighted projective space where the co-ordinates x_1, x_2, y are assigned degrees 1, 1, 2.

Proposition 5.1. *Let $U \in k[x_1, x_2]$ be a non-singular binary quartic with invariants $c_4, c_6 \in k$ and covariants $H, J \in k[x_1, x_2]$. Then*
(i) The equation $y^2 = U(x_1, x_2)$ defines a smooth curve of genus one $C_2 \subset \mathbb{P}(1, 1, 2)$.
(ii) The Jacobian E of C_2 has Weierstrass equation
$$Y^2Z = X^3 - 27c_4XZ^2 - 54c_6Z^3.$$
(iii) The 2-covering map $\pi : C_2 \to E$ is given by
$$(Z : X : Y) = (yU(x_1, x_2) : -3yH(x_1, x_2) : 27J(x_1, x_2)).$$
(iv) Let $\phi_3 : E \to \mathbb{P}^2$ be the natural inclusion. Then the Brauer-Severi diagrams $\phi_2 : C_2 \to \mathbb{P}^1$; $(x_1 : x_2 : y) \mapsto (x_1 : x_2)$ and $\phi_{2,3} : C_2 \to \mathbb{P}(\mathrm{Mat}_{2,3})$; $(x_1 : x_2 : y) \mapsto A_{2,3}$, where
$$A_{2,3} = \begin{pmatrix} -9\frac{\partial H}{\partial x_2} & -3\frac{\partial U}{\partial x_2} & x_1y \\ 9\frac{\partial H}{\partial x_1} & 3\frac{\partial U}{\partial x_1} & x_2y \end{pmatrix},$$
satisfy the conclusions of Theorem 2.5.

Proof: Statements (i)–(iii) are well known: see [1], [23].
(iv) Let D be the hyperplane section for $\phi_2 : C \to \mathbb{P}^1$. Then $\mathcal{L}(3D)$ has basis x_1^3, $x_1^2x_2$, $x_1x_2^2$, x_2^3, x_1y, x_2y. We write the entries of $A_{2,3}$ as linear combinations of these basis elements, and arrange the coefficients in a 6×6 matrix. The determinant of this matrix is $2^2 3^8 \Delta$. Hence $\phi_{2,3} : C_2 \to \mathbb{P}(\mathrm{Mat}_{2,3})$ is an embedding by the complete linear system $|3D|$.

In the notation of §4.1 we have $A_{2,3} = (9\partial H, 3\partial U, y\mathbf{x})$. The 2×2 minors of this matrix are
$$\begin{pmatrix} -3y[\mathbf{x}, \partial U] \\ 9y[\mathbf{x}, \partial H] \\ -27[\partial U, \partial H] \end{pmatrix} = 12 \begin{pmatrix} -yU \\ 3yH \\ -27J \end{pmatrix}$$
So the final statement of Theorem 2.5 is immediate from (iii).

It remains to show that $S \in E[2](\overline{k})$, respectively $T \in E[3](\overline{k})$, acts on the image of $\phi_{2,3}$ as left multiplication by $\chi_2(S)$, respectively right multiplication by $\chi_3(T)$.

The statement for $S \in E[2](\overline{k})$ follows formally from the covariance of the columns of $A_{2,3}$. Indeed, writing $A_{2,3} = (\mathbf{a}_1, \mathbf{a}_2, y\mathbf{a}_3)$, where the $\mathbf{a}_i$ are covariant columns, Definition 4.3 gives

$$\mathbf{a}_i(U \circ g; \mathbf{x}) = g^{-1}\mathbf{a}_i(U, g\mathbf{x})$$

for all $g \in \mathrm{SL}_2(\overline{k})$. So if $g \in \mathrm{SL}_2(\overline{k})$ is a lift of $\chi_2(S)$ then $U \circ g = U$ and

$$g\,\phi_{2,3}(\mathbf{x} : y) = \phi_{2,3}(g\,\mathbf{x} : y)$$

as required.

We deduce the statement for $T \in E[3](\overline{k})$ from the parts of Theorem 2.5 already established. To this end, let M_S and M_T be endomorphisms of $\mathrm{Mat}_{2,3}(\overline{k})$ lifting $\chi_{2,3}(S)$ and $\chi_{2,3}(T)$ respectively. We have shown that M_S is left multiplication by a 2×2 matrix. Accordingly we view $\mathrm{Mat}_{2,3}(\overline{k})$ as an H_2-module via left multiplication. (In this proof we write H_n as a shorthand for $H_n(\overline{k})$.) Since 2 and 3 are coprime, the commutator of M_S and M_T is trivial. Hence M_T is an endomorphism of $\mathrm{Mat}_{2,3}(\overline{k})$ as an H_2-module. Since the standard representation V_2 of H_2 is irreducible, it follows by Schur's lemma that M_T belongs to

$$\mathrm{End}_{H_2}(\mathrm{Mat}_{2,3}(\overline{k})) \cong \mathrm{End}_{H_2}(V_2 \oplus V_2 \oplus V_2) \cong \mathrm{Mat}_3(\overline{k}).$$

Thus M_T is right multiplication by a 3×3 matrix. Let $\psi(T)$ be the image of this matrix in $\mathrm{PGL}_3(\overline{k})$. It remains to show that the characters $\chi_3 : E[3] \to \mathrm{PGL}_3$ and $\psi : E[3] \to \mathrm{PGL}_3$ are equal. Recalling that $\phi_3 \circ \pi = \mu \circ \phi_{2,3}$, we take $P \in C_2(\overline{k})$ and compute

$$\begin{array}{rrcl} & \phi_3(\pi(P+T)) & = & \mu(\phi_{2,3}(P+T)) \\ \Longrightarrow & \phi_3(\pi(P)+2T) & = & \mu(\phi_{2,3}(P)\psi(T)) \\ \Longrightarrow & \chi_3(T)^{-1}\phi_3(\pi(P)) & = & \psi(T)^{-1}\mu(\phi_{2,3}(P)). \end{array}$$

Hence $\chi_3 = \psi$ as required. □

5.2. **The case $n = 3$.** A ternary cubic $U \in k[x_1, x_2, x_3]$ is non-singular if its discriminant $\Delta = (c_4^3 - c_6^2)/1728$ is non-zero. The covariant columns $\mathbf{e}$, $\mathbf{f}$ and contravariant columns $\mathbf{u}$, $\mathbf{h}$ were defined in §4.2.

Proposition 5.2. *Let $U \in k[x_1, x_2, x_3]$ be a non-singular ternary cubic with invariants $c_4, c_6 \in k$ and covariants $H, \Theta, J \in k[x_1, x_2, x_3]$. Then*
(i) The equation $U(x_1, x_2, x_3) = 0$ defines a smooth curve of genus one $C_3 \subset \mathbb{P}^2$.
(ii) The Jacobian E of C_3 has Weierstrass equation

$$Y^2Z = X^3 - 27c_4XZ^2 - 54c_6Z^3.$$

(iii) The 3-covering map $\pi : C_3 \to E$ is given by

$$(Z : X : Y) = (H^3 : \Theta H : J).$$

(iv) Let $\phi_4 : E \to \mathbb{P}^3$; $(Z : X : Y) \mapsto (Z^2 : XZ : YZ : X^2)$. *Then the Brauer-Severi diagrams* $\phi_3 : C_3 \to \mathbb{P}^2$ *and* $\phi_{3,4} : C_3 \to \mathbb{P}(\mathrm{Mat}_{3,4})$; $(x_1 : x_2 : x_3) \mapsto A_{3,4}$, *where*

$$A_{3,4} = \begin{pmatrix} -3\mathbf{f} + 9c_4 H\mathbf{x} & \mathbf{e} & \frac{2}{3}(\mathbf{u} \times \mathbf{h}) & -\frac{1}{3}H\mathbf{x} \end{pmatrix},$$

satisfy the conclusions of Theorem 2.5.

Proof: Statements (i)–(iii) are well known: see [1].
(iv) By Theorem 4.10 the covariant columns of order 4 form a free $k[c_4, c_6]$-module with basis

$$U\mathbf{x}, \quad H\mathbf{x}, \quad \mathbf{e}, \quad \mathbf{f}, \quad \mathbf{u} \times \mathbf{h}. \tag{10}$$

The entries of these columns give us 15 ternary quartics. We arrange the coefficients of these quartics in a 15×15 matrix, and find that the determinant is $2^{42}3^{12}\Delta^5$. (The calculation is made easier if we first put U in Hesse normal form:

$$U(x_1, x_2, x_3) = a(x_1^3 + x_2^3 + x_3^3) + bx_1x_2x_3.)$$

Let D the hyperplane section for $\phi_3 : C_3 \to \mathbb{P}^2$. Since the only ternary quartics vanishing on C_3 are the entries of $U\mathbf{x}$, the above calculation shows that $\phi_{3,4} : C_3 \to \mathbb{P}(\mathrm{Mat}_{3,4})$ is an embedding by the complete linear system $|4D|$.

A direct calculation (carried out for U in Hesse normal form) shows that the 3×3 minors of $A_{3,4}$ are

$$\begin{aligned}
\mu_1 &= 2H^4 - 6c_4U^2H^2 - \tfrac{2}{3}UH\Theta \\
\mu_2 &= 2\Theta H^2 - 18c_4^2U^3H - 18c_4UH^3 + 48c_6U^2H^2 \\
\mu_3 &= 2JH \\
\mu_4 &= 2\Theta^2 + 162c_4^3U^4 - 54c_4^2U^2H^2 - 432c_4c_6U^3H \\
&\qquad\qquad\qquad - 18c_4UH\Theta + 144c_6UH^3.
\end{aligned}$$

The final statement of Theorem 2.5 follows since by (iii) the composition $\phi_4 \circ \pi$ is given by

$$(x_1 : x_2 : x_3) \mapsto (H^4 : \Theta H^2 : JH : \Theta^2).$$

The remainder of the proof now carries through exactly as in the case $n = 2$. □

6. Computations

Let E be an elliptic curve over $\mathbb{Q}$. We use 6-descent and 12-descent to assist in the search for generators of $E(\mathbb{Q})$ of large height. The method is of greatest interest when $E(\mathbb{Q})$ has rank at least 2, or E has large conductor, *i.e.* in those cases where we cannot use Heegner points. In this section we give some details of our implementation in the computer algebra system Magma [15]. Further remarks accompany the numerical examples in §7.

6.1. **The method in outline.** We begin by using the existing functions in Magma to compute n-coverings for $n = 2, 3, 4$.

- The Magma function `TwoDescent`, takes as input a Weierstrass equation for E, and returns a list of $2^s - 1$ binary quartics representing the non-zero elements of the 2-Selmer group $S^{(2)}(E/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^s$.
- The Magma function `ThreeDescent`, written by Stoll, Donnelly and the author, takes as input a Weierstrass equation for E, and returns a list of $(3^t - 1)/2$ ternary cubics representing the non-zero elements of the 3-Selmer group $S^{(3)}(E/\mathbb{Q}) \cong (\mathbb{Z}/3\mathbb{Z})^t$.
- The Magma function `FourDescent`, written by Womack and Watkins, takes as input a binary quartic representing a non-zero element $\alpha \in S^{(2)}(E/\mathbb{Q})$, and returns a list of pairs of quadrics in four variables, representing the elements of the 4-Selmer group in the fibre of $S^{(4)}(E/\mathbb{Q}) \to S^{(2)}(E/\mathbb{Q})$ above α.

Each element of the n-Selmer group is now represented by (equations for) a Brauer-Severi diagram $[C_n \to \mathbb{P}^{n-1}]$. The Selmer group elements may equally be viewed as n-coverings, where the covering maps $\pi : C_n \to E$ are computed using the classical formulae surveyed in [1]. (For $n = 2$, 3 we recalled these formulae in Propositions 5.1 and 5.2.) Replacing the covering map π by $[-1] \circ \pi$ corresponds to taking the inverse in the Selmer group. So in the cases $n = 3, 4$ each ternary cubic, respectively pair of quadrics, represents both a Selmer group element and its inverse.

Definition 6.1. Let $[C_n \to \mathbb{P}^{n-1}]$ be a Brauer-Severi diagram with hyperplane section D. A point $P \in C_n(\overline{k})$ is a flex if $n.P \sim D$.

The flex points of a 2-covering are the roots of the binary quartic. In the cases $n = 3, 4$ the flex points (also known as points of inflection, or hyperosculating points) are the intersections with $H = 0$, respectively $J = 0$, where H is the Hessian of a ternary cubic, and J is the covariant defined in [1, §3.3].

We recall that if $[C_n \to \mathbb{P}^{n-1}]$ is a Brauer-Severi diagram, then the morphism $C_n \to \mathbb{P}^{n-1}$ is that determined by a complete linear system of degree n. So if $n \geq 3$ then $C_n \to \mathbb{P}^{n-1}$ is an embedding. We identify C_n with its image, which is called a genus one normal curve of degree n. It is well known that if $n \geq 4$ then the homogeneous ideal $I(C_n)$ is generated by a vector space of quadrics of dimension $n(n-3)/2$.

The details of 6-descent are as follows. We start with a 2-covering $C_2 = \{y^2 = U_2(x_1, x_2)\}$ and a 3-covering $C_3 = \{U_3(x_1, x_2, x_3) = 0\}$, each defined over $\mathbb{Q}$. Since these are coverings of the same elliptic curve E, we may assume that U_2 and U_3 have the same invariants c_4 and c_6. Then E has Weierstrass equation

$$y^2 = x^3 - 27c_4x - 54c_6.$$

We compute a flex point on C_3 with co-ordinates in a number field, L say. Typically $[L : \mathbb{Q}] = 9$. Then Algorithm 6.3 finds a matrix $g \in \mathrm{GL}_3(L)$ with

$$(U_3 \circ g)(z, x, y) = \lambda(y^2z - x^3 + 27c_4xz^2 + 54c_6z^3)$$

for some $\lambda \in L^\times$. (In the notation of §2 we have $g = B_3^{-1}$.)

Next we let $\phi_{2,3} : C_2 \to \mathbb{P}(\mathrm{Mat}_{2,3})$ be the embedding defined in Proposition 5.1(iv). The image is a genus one normal curve of degree 6. We use linear algebra to compute a basis $Q_1, \ldots, Q_9$ for the space of quadrics vanishing on this curve. Writing these as polynomials in variables X_{ij} for $1 \le i \le 2$ and $1 \le j \le 3$, we make the substitution

$$\begin{pmatrix} X_{11} & X_{12} & X_{13} \\ X_{21} & X_{22} & X_{23} \end{pmatrix} = \begin{pmatrix} x_{11} & x_{12} & x_{13} \\ x_{21} & x_{22} & x_{23} \end{pmatrix} g.$$

The new quadrics have coefficients in L, but the vector space they span has a basis with coefficients in $\mathbb{Q}$. We compute an LLL-reduced basis for the intersection of this space with $\mathbb{Z}[x_{11}, \ldots, x_{23}]$. These are now the equations for a 6-covering $C_6 \subset \mathbb{P}(\mathrm{Mat}_{2,3})$. Moreover, by Theorem 2.5, the covering map $C_6 \to C_3$ is defined by the 2×2 minors, *i.e.*

$$\begin{pmatrix} x_{11} & x_{12} & x_{13} \\ x_{21} & x_{22} & x_{23} \end{pmatrix} \mapsto (x_{12}x_{23} - x_{22}x_{13} : x_{13}x_{21} - x_{23}x_{11} : x_{11}x_{22} - x_{21}x_{12}).$$

The details of 12-descent are similar. We start with a 3-covering $C_3 = \{U_3(x_1, x_2, x_3) = 0\}$ and a 4-covering $C_4 = \{Q_1 = Q_2 = 0\}$, each defined over $\mathbb{Q}$, and with the same invariants c_4 and c_6. We compute a flex point on C_4 with co-ordinates in a number field, L say. Typically $[L : \mathbb{Q}] = 16$. Then Algorithm 6.4 finds a matrix $g \in \mathrm{GL}_4(L)$ with

$$\langle Q_1 \circ g, Q_2 \circ g \rangle = \langle x_1x_4 - x_2^2, x_2x_4 - x_3^2 - 27c_4x_1x_2 - 54c_6x_1^2 \rangle.$$

Next we let $\phi_{3,4} : C_3 \to \mathbb{P}(\mathrm{Mat}_{3,4})$ be the embedding defined in Proposition 5.2(iv). The image is a genus one normal curve of degree 12. We use linear algebra to compute a basis $Q_1, \ldots, Q_{54}$ for the space of quadrics vanishing on this curve. As in the case of 6-descent, we then twist by $g \in \mathrm{GL}_4(L)$ to obtain equations for a 12-covering $C_{12} \subset \mathbb{P}(\mathrm{Mat}_{3,4})$. Moreover, by Theorem 2.5, the covering map $C_{12} \to C_4$ is defined by the 3×3 minors.

Unlike the case of 6-descent, we can combine a 3-covering and a 4-covering to give a 12-covering in two essentially different ways. This is because each of C_3 and C_4 represents both a Selmer group element and its inverse. It is important that we compute both 12-coverings, since in the case they are soluble, their rational points will cover $\pm P + 12E(\mathbb{Q})$ and $\pm 5P + 12E(\mathbb{Q})$ respectively. In practice the second 12-covering is obtained by switching the sign in the third column of the matrix defining $\phi_{3,4}$.

It remains to search for rational points on C_6 and C_{12}. We use the p-adic point searching method due independently to Elkies and Heath-Brown, as implemented by Watkins in the Magma function `PointSearch`. Descriptions may be found in [22] and [24, §2.9]. (Elkies' original paper [10] only considers real approximations.) The method first chooses an auxiliary prime p, whose size depends on the height bound set for the search. The points on the reduction of C mod p are then enumerated, and for each such point P_0 a lattice method variant of Hensel's lemma is used to search for rational points on C with reduction P_0. A variant of the method uses two primes. The method works particularly well for curves of high codimension as considered here.

Finally, our search for points is significantly improved if we "minimise" our equations for C_6 and C_{12} before running `PointSearch`. We give details in §6.3.

6.2. **Computing flex matrices.** Let $[C \to \mathbb{P}^{n-1}]$ be a Brauer-Severi diagram. To compute a flex matrix for C, as defined in §2, we first find a flex point P on C. We then follow an inductive procedure, based on the idea of projecting away from P. This method is a by-product of the standard procedures for putting an elliptic curve in Weierstrass form, as described in [3, §8]. We therefore simply list the algorithms used. Notice that we do not use the general Riemann-Roch machinery implemented in Magma, as this would be unnecessarily slow in our applications.

Algorithm 6.2. Let $U \in k[x_1, x_2]$ be a non-singular binary quartic with invariants c_4 and c_6. Given $(\alpha : \beta) \in \mathbb{P}^1(k)$ with $U(\alpha, \beta) = 0$ we compute $g \in \mathrm{GL}_2(k)$ with last column $(\alpha, \beta)^T$ satisfying

$$(U \circ g)(z, x) \;=\; \tfrac{1}{36}(\det g)^2(x^3 z - 27c_4 x z^3 - 54c_6 z^4).$$

(1) Choose any $g_1 \in \mathrm{GL}_2(k)$ with last column $(\alpha, \beta)^T$.
(2) Compute $(U \circ g_1)(z, x) = (\det g_1)^2(bx^3 z + cx^2 z^2 + \ldots)$ and put $g_2 = \begin{pmatrix} 36b & 0 \\ -12c & 1 \end{pmatrix}$.
(3) Return $g_1 g_2$.

Algorithm 6.3. Let $U \in k[x_1, x_2, x_3]$ be a non-singular ternary cubic with invariants c_4 and c_6. Given $(\alpha : \beta : \gamma) \in \mathbb{P}^2(k)$ a flex point on the curve $\{U = 0\}$ we compute $g \in \mathrm{GL}_3(k)$ with last column $(\alpha, \beta, \gamma)^T$ satisfying

$$(U \circ g)(z, x, y) \;=\; \tfrac{1}{6}(\det g)(y^2 z - x^3 + 27c_4 x z^2 + 54 c_6 z^3).$$

(1) Choose any $g_1 \in \mathrm{GL}_3(k)$ with last column $(\alpha, \beta, \gamma)^T$.
(2) Write $(U \circ g_1)(z, x, y) = (\det g_1)(f_1(z, x)y^2 + f_2(z, x)y + f_3(z, x))$ and let $\alpha, \beta \in k$ with $f_1(z, x) = \beta z - \alpha x$. Then run Algorithm 6.2 on $\frac{1}{4} f_2^2 - f_1 f_3$ to obtain $g \in \mathrm{GL}_2(k)$.
(3) Compute $p, q \in k$ with

$$\begin{aligned}(f_1 \circ g)(z, x) &= (\det g) z \\ (f_2 \circ g)(z, x) &= (\det g)(pz + qx)z\end{aligned}$$

and put $g_2 = \begin{pmatrix} \multicolumn{2}{c}{\multirow{2}{*}{$6g$}} & 0 \\ & & 0 \\ -3p & -3q & 1 \end{pmatrix}$.
(4) Return $g_1 g_2$.

In the case $n = 4$ the invariants are again described in [1]. We label them c_4 and c_6, with scalings as specified in [11].

Algorithm 6.4. Let $Q_1, Q_2 \in k[x_1, x_2, x_3, x_4]$ be a pair of quadrics, with invariants c_4 and c_6. We suppose that $\{Q_1 = Q_2 = 0\}$ is a smooth curve of genus one. Given $(\alpha : \beta : \gamma : \delta) \in \mathbb{P}^3(k)$, a flex point on this curve, we compute $g \in \mathrm{GL}_4(k)$ with last column $(\alpha, \beta, \gamma, \delta)^T$ satisfying

$$\langle Q_1 \circ g, Q_2 \circ g \rangle = \langle x_1 x_4 - x_2^2, x_2 x_4 - x_3^2 - 27 c_4 x_1 x_2 - 54 c_6 x_1^2 \rangle.$$

(1) Choose any $g_1 \in \mathrm{GL}_4(k)$ with last column $(\alpha, \beta, \gamma, \delta)^T$.
(2) Write

$$\begin{aligned}Q_1 \circ g_1 &= \ell_1(x_1, x_2, x_3)x_4 + q_1(x_1, x_2, x_3) \\ Q_2 \circ g_1 &= \ell_2(x_1, x_2, x_3)x_4 + q_2(x_1, x_2, x_3)\end{aligned}$$

and let

$$\alpha = \begin{vmatrix} \ell_{12} & \ell_{13} \\ \ell_{22} & \ell_{23} \end{vmatrix}, \quad \beta = \begin{vmatrix} \ell_{13} & \ell_{11} \\ \ell_{23} & \ell_{21} \end{vmatrix}, \quad \gamma = \begin{vmatrix} \ell_{11} & \ell_{12} \\ \ell_{21} & \ell_{22} \end{vmatrix},$$

where $\ell_i = \sum \ell_{ij} x_j$. Then run Algorithm 6.3 on $(\det g_1)^{-1}(\ell_2 q_1 - \ell_1 q_2)$ to obtain $g \in \mathrm{GL}_3(k)$.
(3) Replace Q_1 and Q_2 by linear combinations (and update the ℓ_i and q_i of Step 2) so that $\ell_i \circ g = x_i$ for $i = 1, 2$.
(4) Compute $a, b, c \in k$ with

$$\begin{aligned}q_1 \circ g &= \tfrac{1}{6}(x_1(ax_1 + bx_2 + cx_3) - x_2^2) \\ q_2 \circ g &= \tfrac{1}{6}(x_2(ax_1 + bx_2 + cx_3) - x_3^2 - 27c_4 x_1 x_2 - 54 c_6 x_1^2)\end{aligned}$$

and put $g_2 = \begin{pmatrix} & & & 0 \\ & 6g & & 0 \\ & & & 0 \\ -a & -b & -c & 1 \end{pmatrix}$.

(5) Return $g_1 g_2$.

6.3. **Minimisation.** If an n-covering $\pi : C \to E$ is to be useful in the search for rational points on E, not only must we find explicit equations for $C \subset \mathbb{P}^{n-1}$, but we must also find a change of co-ordinates on $\mathbb{P}^{n-1}$ so that these equations have reasonably small coefficients. The task naturally falls into two parts which, following terminology introduced by Cremona, we call minimisation and reduction.

Minimisation is the task of removing as many prime factors as possible from a suitably defined discriminant. The most familiar example is that of minimising a Weierstrass equation. By reduction we mean the use of unimodular transformations to further decrease the size of the coefficients. The basic example is reduction of binary quadratic forms, or more generally lattice reduction. Thus minimisation is concerned with the finite places, and reduction with the infinite places. The need to perform reduction is our main reason for working over the rationals (instead of a more general number field).

The minimisation and reduction of 2-coverings has been studied in [2], [4], and [8]. The generalisations to 3-coverings and 4-coverings are described in [6] and [24]. These algorithms have been implemented in Magma, and are called by the functions `TwoDescent`, `ThreeDescent` and `FourDescent`. Hence in §6.1 we start with an n-covering and an $(n+1)$-covering both of which are already minimised and reduced. So it would not be unreasonable to hope that the $n(n+1)$-covering computed from them will automatically be minimised and reduced. Numerical examples suggest that this is true for reduction, but not for minimisation.

The following is a description of our current ad hoc approach to the minimisation of n-coverings for $n > 5$. Although this method works reasonably well in practice, there remains considerable room for both theoretical and practical improvements.

Let $C \subset \mathbb{P}^{n-1}$ be a genus one normal curve, defined over $\mathbb{Q}$, and of degree $n \geq 4$. We recall that the homogeneous ideal $I(C)$ in $\mathbb{Q}[x_1, \ldots, x_n]$ is generated by a vector space of quadrics of dimension $N = n(n-3)/2$. Then for $A \in \mathrm{GL}_N(\mathbb{Q})$ and $B \in \mathrm{GL}_n(\mathbb{Q})$ we define

$$[A, B](q_1, \ldots, q_N) \quad = \quad (\textstyle\sum_{i=1}^N a_{1i} q_i \circ B^T, \ldots, \sum_{i=1}^N a_{Ni} q_i \circ B^T).$$

Definition 6.5. (i) An integral model $(q_1, \ldots, q_N)$ for C is a tuple of quadrics in $\mathbb{Z}[x_1, \ldots, x_n]$ generating $I(C)$.

(ii) An integral model $(q_1, \ldots, q_N)$ is minimal at a prime p if whenever $A \in \mathrm{GL}_N(\mathbb{Q})$ and $B \in \mathrm{GL}_n(\mathbb{Q})$ with $[A, B](q_1, \ldots, q_N)$ integral, then

$$\mathrm{ord}_p(\det A) + (n-3)\,\mathrm{ord}_p(\det B) \geq 0.$$

(iii) An integral model is minimal if it is minimal at all primes p.

It is not even clear from our definition that minimal models exist, although in the cases $n = 4$, 5 this can be proved using the invariants defined in [1] and [11]. The condition in Definition 6.5(ii) is motivated by considering what happens when A and B are scalar matrices.

We attempt to minimise at p as follows. Let I_p be the ideal in $\mathbb{F}_p[x_1, \ldots, x_n]$ generated by the reductions of $q_1, \ldots, q_N \bmod p$. We compute the $\mathbb{F}_p$-vector space V_p of linear forms in the radical of I_p. By a unimodular change of co-ordinates we may suppose that $V_p = \langle x_1, \ldots, x_d \rangle$ for some $0 \leq d < n$. Then we put

$$B = \begin{pmatrix} pI_d & 0 \\ 0 & I_{n-d} \end{pmatrix}$$

and compute the index p^m of the lattice spanned by the $q_i \circ B$ in its saturation in $\mathbb{Z}[x_1, \ldots, x_n]$. We call the integer $m - (n-3)d$ the gain. If the gain is positive then we switch to the new quadrics and start over again. Otherwise we stick with the old quadrics. Sometimes it is worth trying other choices for the vector space V_p, for example the space of linear forms in one of the minimal primes containing I_p. There is no guarantee that these methods will produce a p-minimal model (and in general they do not).

The end result of our attempts at minimisation is a change of co-ordinates on $\mathbb{P}^{n-1}$. We run the LLL algorithm on the rows (or columns depending on conventions) of the change of basis matrix, before applying it to the original quadrics. This is to ensure that we do not throw away the fact our quadrics are already (close to being) reduced.

7. Numerical Examples

7.1. **An example of 6-descent.** The following problem falls into the class of problems discussed on pages 480-481 of [9].

> Given an integer $N > 2$, decide whether there are non-zero integers x and y such that both $x^2 + Nxy + y^2$ and $x^2 - Nxy + y^2$ are squares.

Elementary manipulations show that the problem is equivalent to deciding whether the elliptic curve

$$E_N : \quad y^2 = x(x + (N+2)^2)(x + (N-2)^2)$$

has positive rank[2]. MacLeod and Rathbun [14] have undertaken to find a solution for x and y (where one exists) for all $N < 1000$. The one case to elude them (as of November 2006) was $N = 809$, for which the rank is 1 and the generator is predicted[3] to have height 617.88. On the 2-isogenous curve

$$E'_N : \quad y^2 = x^3 + 2(N^2 + 12N + 4)x^2 + (N-2)^4 x$$

the predicted height is half this value, yet still beyond the range that can be found using 4-descent. The conductor of $E = E'_{809}$ is sufficiently large that a Heegner point calculation ran into difficulties (and for this reason the curve was reported to Magma as a bug).

We find a point of infinite order on E using 6-descent. The existing Magma functions for 2-descent and 3-descent give us a 2-covering

$$C_2 = \left\{ y^2 = 138546x_1^4 + 225978x_1^3x_2 + 435649x_1^2x_2^2 + 3884x_1x_2^3 + 183499x_2^4 \right\}$$

and a 3-covering

$$C_3 = \left\{ \begin{array}{lcl} 54x^3 - 84y^3 - 258z^3 + 144x^2y + 87x^2z - 350xy^2 & & \\ \qquad\qquad + 71y^2z - 1656xz^2 - 986yz^2 - 388xyz & = & 0 \end{array} \right\}.$$

To compute this 3-covering we had to find the class group and units for a number field of degree 8. This is by far the most time consuming part of the 6-descent calculation, taking a couple of hours, as compared to at most a couple of minutes for each of the other steps.

Following the method described in §6.1 we compute 9 quadrics defining a 6-covering $C_6 \subset \mathbb{P}(\mathrm{Mat}_{2,3})$. These are quadrics in 6 variables, labelled x_{ij} for $1 \le i \le 2$ and $1 \le j \le 3$. The coefficients are reasonably small integers, the largest in absolute value being 142.

Minimising (at the primes 2, 3, 809 and 811), as described in §6.3, suggests making the substitution

$$\begin{pmatrix} x_{11} \\ x_{12} \\ x_{13} \\ x_{21} \\ x_{22} \\ x_{23} \end{pmatrix} = \begin{pmatrix} -70 & 455 & 293 & 700 & -63 & 437 \\ 104 & 417 & -363 & 290 & 745 & -579 \\ -268 & -89 & 205 & -60 & 1223 & 817 \\ -320 & -335 & -839 & 386 & 147 & -311 \\ -318 & 411 & -123 & -696 & -405 & 561 \\ 284 & 59 & -523 & 226 & -15 & 1973 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{pmatrix}.$$

This decreases the size of the coefficients. More importantly, but as we will only see in hindsight, it also reduces the (naive) height of the

[2]The trivial solutions correspond to a subgroup $T \subset E_N(\mathbb{Q})$ with $T \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Since $\pm(N^2-4) \notin (\mathbb{Q}^*)^2$, the image of T under the 2-descent map $E_N(\mathbb{Q}) \to \mathbb{Q}^*/(\mathbb{Q}^*)^2 \times \mathbb{Q}^*/(\mathbb{Q}^*)^2$ has order 4. It follows that $E_N(\mathbb{Q})_{\mathrm{tors}} = T$.

[3]This estimate comes from the Birch–Swinnerton-Dyer conjecture, assuming that the Tate-Shafarevich group is trivial.

point we are looking for. The new quadrics are

$$\begin{array}{rcl}
q_1 & = & x_1x_4 + 2x_2x_3 + 2x_2x_4 - 2x_2x_5 - 2x_2x_6 + 2x_3^2 - 2x_3x_4 - 6x_3x_6 - x_4x_5 + 4x_4x_6 \\
 & & \quad -2x_5^2 + 5x_5x_6 + x_6^2 \\
q_2 & = & x_1x_2 + x_1x_3 - 2x_1x_4 + 3x_1x_5 - 4x_1x_6 - x_2^2 + 2x_2x_5 - 7x_2x_6 + x_3^2 - x_3x_4 + 4x_3x_5 \\
 & & \quad -2x_3x_6 + 5x_4^2 - 3x_4x_5 - 8x_4x_6 + x_5^2 + 2x_5x_6 - 6x_6^2 \\
q_3 & = & x_1^2 + x_1x_3 + 3x_1x_4 + 5x_1x_5 - 2x_1x_6 - 3x_2^2 + 5x_2x_3 + x_2x_4 - 4x_2x_5 - x_2x_6 + 2x_3^2 \\
 & & \quad +4x_3x_4 + 7x_3x_5 - 5x_3x_6 + 3x_4^2 - 5x_4x_6 - 2x_5x_6 - x_6^2 \\
q_4 & = & x_1^2 - 3x_1x_2 + 3x_1x_4 + x_1x_5 + 5x_1x_6 + 7x_2x_3 + 3x_2x_4 - 5x_2x_5 + 3x_2x_6 + 7x_3^2 \\
 & & \quad -2x_3x_4 - x_3x_5 + 7x_3x_6 - 5x_4^2 + x_4x_5 - x_5^2 - x_5x_6 \\
q_5 & = & 2x_1x_2 - x_1x_3 + x_1x_5 - 7x_1x_6 - x_2^2 - 6x_2x_3 - 2x_2x_4 + x_2x_5 - 8x_2x_6 - 2x_3^2 - 3x_3x_4 \\
 & & \quad -5x_3x_5 + 2x_4^2 + 3x_4x_6 + x_5^2 - 7x_5x_6 - x_6^2 \\
q_6 & = & x_1^2 + 3x_1x_2 + 5x_1x_3 - 3x_1x_4 - 2x_1x_5 + 2x_1x_6 + 2x_2^2 + 4x_2x_3 + x_2x_5 + 9x_2x_6 \\
 & & \quad -x_3^2 + 2x_3x_4 + 4x_3x_5 + 9x_4^2 + 6x_4x_5 + 5x_4x_6 - x_5^2 + 4x_6^2 \\
q_7 & = & x_1^2 + 2x_1x_2 + 3x_1x_3 - 3x_1x_4 + x_1x_6 - 6x_2^2 + 3x_2x_3 + 9x_2x_4 + x_2x_5 + 2x_2x_6 + 3x_3^2 \\
 & & \quad +x_3x_4 + 7x_3x_5 - x_3x_6 - 6x_4^2 - 2x_4x_5 - 6x_4x_6 + 3x_5^2 - x_5x_6 - x_6^2 \\
q_8 & = & x_1^2 - 2x_1x_2 + x_1x_3 - 2x_1x_4 + 3x_1x_5 + 2x_1x_6 - x_2x_3 - x_2x_4 + 3x_2x_5 - 8x_2x_6 \\
 & & \quad -x_3^2 + 7x_3x_4 + 8x_3x_5 + 12x_3x_6 + 4x_4^2 - 2x_4x_5 + 2x_4x_6 + 6x_5x_6 - 5x_6^2 \\
q_9 & = & x_1x_2 - 6x_1x_3 + 6x_1x_4 - 2x_1x_5 + 6x_1x_6 - x_2^2 + x_2x_3 - 5x_2x_4 - 2x_2x_5 - 2x_2x_6 \\
 & & \quad -7x_3^2 - 3x_3x_4 + 5x_3x_5 + x_3x_6 - 3x_4^2 + 10x_4x_5 + 5x_4x_6 - 4x_5^2 + 5x_5x_6 + 2x_6^2.
\end{array}$$

The `PointSearch` function (see §6.1 for references) finds a solution

$$\begin{array}{rcl}
(x_1 : \ldots : x_6) & = & (7439932626 : -837815413 : -525136075 : \\
 & & \qquad 2262805710 : -3465232629 : -1122238333).
\end{array}$$

Mapping back to C_6 this point becomes

$$\begin{pmatrix} x_{11} & x_{12} & x_{13} \\ x_{21} & x_{22} & x_{23} \end{pmatrix} = \begin{pmatrix} 42664889066 & -110100049465 & -1219600972219 \\ -157741863480 & -574453039469 & 114558712088 \end{pmatrix}$$

The 2×2 minors are the co-ordinates of a point in $C_3(\mathbb{Q})$ which then maps down to a point $P \in E(\mathbb{Q})$ of canonical height 308.94. It is routine to check (using the bounds given in [7]) that P is a generator for the Mordell-Weil group modulo torsion.

The final values of x and y for which both $x^2 + 809xy + y^2$ and $x^2 - 809xy + y^2$ are squares may be found on the website [14]. They have 534 and 537 decimal digits respectively.

7.2. **An example of 12-descent.** As described in the introduction, Mark Watkins provided me with a list of 35 elliptic curves over $\mathbb{Q}$ of analytic rank 2 for which only one generator of the Mordell-Weil group was known. The Birch–Swinnerton-Dyer conjecture gives an estimate for the height of the supposed second generator. The curves were ordered by this estimated height. For the first 30 curves on the list, the estimated height was in the range 220 up to 370. The last 5 were as follows. We list the conductor N_E, the coefficients $a_1, \ldots, a_6$ of a minimal Weierstrass equation, and the canonical heights of the generators. (The last column was computed in hindsight.)

N_E	$[a_1, a_2, a_3, a_4, a_6]$	$\widehat{h}(P_1)$	$\widehat{h}(P_2)$
8423178259	$[0, -1, 1, -6286122, -6064183289]$	17.2636	442.070
4817824003	$[0, -1, 1, -91969194, -339447383999]$	15.4617	445.878
4353186907	$[1, 1, 0, -14176508, -20550712585]$	14.4505	488.336
5242805459	$[1, 1, 0, -5078887, -4407675042]$	2.9643	527.301
7800899941	$[0, 0, 1, -237882589, -1412186639384]$	5.3208	642.626

Each curve on the list is the only curve in its isogeny class, and so in particular has trivial torsion subgroup. According to Magma we have $S^{(3)}(E/\mathbb{Q}) \cong (\mathbb{Z}/3\mathbb{Z})^2$ and $S^{(4)}(E/\mathbb{Q}) \cong (\mathbb{Z}/4\mathbb{Z})^2$. Magma also returns 4 ternary cubics and 6 pairs of quadrics, representing the inverse pairs of elements of order n in $S^{(n)}(E/\mathbb{Q})$ for $n = 3, 4$. Following the method described in §6.1 we compute 48 different 12-coverings, each corresponding to an inverse pair of elements of order 12 in $S^{(12)}(E/\mathbb{Q}) \cong (\mathbb{Z}/12\mathbb{Z})^2$. Since $E(\mathbb{Q})$ has one generator of small height, we only needed to search on a few of these before a second independent generator was found.

We give brief details for the last curve on the list. In this case the first generator is

$$P_1 = (-2003564/15^2, -1691/15^3).$$

To compute a second independent generator we start with a 3-covering

$$C_3 = \left\{ \begin{array}{rcl} 13x^3 - 87y^3 - 142z^3 + 17x^2y + 28x^2z + 77xy^2 & & \\ - 187y^2z - 35xz^2 - 30yz^2 - 118xyz & = & 0 \end{array} \right\}$$

and a 4-covering

$$C_4 = \left\{ \begin{array}{rcl} x_1^2 + 3x_1x_2 + 13x_1x_4 - 2x_2^2 - 2x_2x_3 & & \\ + x_2x_4 - 6x_3^2 - 9x_3x_4 + 7x_4^2 & = & 0 \\ 3x_1^2 - 6x_1x_2 + 5x_1x_3 - 14x_1x_4 + 8x_2^2 & & \\ - 7x_2x_3 - 2x_2x_4 + 5x_3^2 + 6x_4^2 & = & 0 \end{array} \right\}.$$

Following the method described in §6.1 we compute 54 quadrics in 12 variables defining a 12-covering $C_{12} \subset \mathbb{P}(\mathrm{Mat}_{3,4})$. The coefficients are integers of absolute value at most 40. After minimising at the unique bad prime of E, the largest absolute value was 7. On this modified curve, `PointSearch` (see §6.1 for references) found a solution

$$(-38935814 : 66676907 : 35419393 : -17989378 : 14587909 : -9597188 : -41856515 : -6994528 : -103052506 : 12269644 : 11697462 : 25846956)$$

Mapping back to C_{12} this point becomes

$$\begin{pmatrix} -5858527466652 & -134738830676 & 992806781984 & -476555121265 \\ -5994121237 & 8026743882 & -211970353911 & 286395682995 \\ 303306392932 & -167866472332 & -273061778593 & 215669566507 \end{pmatrix}.$$

The 3×3 minors are the co-ordinates of a point in $C_4(\mathbb{Q})$ which then maps down to a point $P = (r/t^2, s/t^3) \in E(\mathbb{Q})$ of canonical height 651.86 where

$$
\begin{aligned}
t &= 19114217356093463705777747876066898415631548291608697\backslash\\
&\quad 40922807612824612875940389382477232533975065261036903\backslash\\
&\quad 1136244375962645684728831244647511\\
r &= 93385419996781156236208893304670769704360761931620474\backslash\\
&\quad 91160376652094516256058095438975234936485365750728672\backslash\\
&\quad 93638862617394747880602761519393543195699455909538302\backslash\\
&\quad 59168129312401737073248837456279406678810951156628252\backslash\\
&\quad 40211217008647003170248465787238475381689553329226658\backslash\\
&\quad 862657964535534165\\
s &= 21189601910515224224247520792578674272370041362778083\backslash\\
&\quad 56705954773720391166818153294963600750782215820469113\backslash\\
&\quad 74353930791392149260850703573807892173379962268109766\backslash\\
&\quad 98439592570904852474980215470887488235939468315716611\backslash\\
&\quad 87491555874815362407229178054307290009804071221273367\backslash\\
&\quad 65774805454336495291566121830488793684956520543942634\backslash\\
&\quad 32595140366259647660234205784539280961702449802725098\backslash\\
&\quad 96112530054586556368131586070462495535201464722076521 2
\end{aligned}
$$

A second generator of slightly smaller height is $P_2 = P + P_1$ with $\widehat{h}(P_2) = 642.63$. (In hindsight we could find P_2 directly by starting with different C_3 and C_4.) According to Magma the regulator of the subgroup generated by P_1 and P_2 is 3415.49, the non-zero value confirming that these points are independent. Again it is routine to check (using the bounds given in [7]) that P_1 and P_2 generate the Mordell-Weil group.

References

[1] S.Y. An, S.Y. Kim, D.C. Marshall, S.H. Marshall, W.G. McCallum and A.R. Perlis, Jacobians of genus one curves, *J. Number Theory* 90 (2001), no. 2, 304–315.

[2] B.J. Birch and H.P.F. Swinnerton-Dyer, Notes on elliptic curves I. *J. Reine Angew. Math.* **212** (1963), 7–25.

[3] J.W.S. Cassels, *Lectures on elliptic curves*, LMS Student Texts 24, Cambridge University Press, Cambridge, 1991.

[4] J.E. Cremona, Reduction of binary cubic and quartic forms, *LMS J. Comput. Math.* **2** (1999), 64–94 (electronic).

[5] J.E. Cremona, T.A. Fisher, C. O'Neil, D. Simon and M. Stoll, *Explicit n-descent on elliptic curves, I Algebra*, to appear *J. Reine Angew. Math.*, *II Geometry*, submitted for publication, *III Algorithms*, in preparation.

[6] J.E. Cremona, T.A. Fisher and M. Stoll, *Minimisation and reduction for 3- and 4-coverings of elliptic curves*, in preparation.
[7] J.E. Cremona, M. Prickett and S. Siksek, Height difference bounds for elliptic curves over number fields, *J. Number Theory* **116** (2006), no. 1, 42–68.
[8] J.E. Cremona and M. Stoll, Minimal models for 2-coverings of elliptic curves, *LMS J. Comput. Math.* **5** (2002), 220–243 (electronic).
[9] L.E. Dickson, *History of the theory of numbers, Vol. II: Diophantine analysis*, Chelsea Publishing Co., New York 1966.
[10] N.D. Elkies, Rational points near curves and small nonzero $|x^3 - y^2|$ via lattice reduction, *Algorithmic number theory* (Leiden, 2000), 33–63, Lecture Notes in Comput. Sci., 1838, Springer, Berlin, 2000.
[11] T.A. Fisher, *The invariants of a genus one curve*, preprint, available at `http://arxiv.org/abs/math/0610318`
[12] M. Hindry and J.H. Silverman, *Diophantine geometry*, Graduate Texts in Mathematics 201, Springer-Verlag, New York, 2000.
[13] K. Hulek, *Projective geometry of elliptic curves*, Astérisque No. 137 (1986).
[14] A.J. MacLeod, Elliptic curves in recreational number theory, website at `http://maths.paisley.ac.uk/allanm/ECRNT/Ecrnt.htm`
[15] MAGMA is described in W. Bosma, J. Cannon and C. Playoust, The Magma algebra system I: The user language, *J. Symbolic Comput.* 24, 235–265 (1997). The Magma home page is at `http://magma.maths.usyd.edu.au/magma/`
[16] D. Mumford, *Abelian varieties*, Oxford University Press, 1970.
[17] C. O'Neil, The period-index obstruction for elliptic curves, *J. Number Theory* 95 (2002), no. 2, 329–339.
[18] S. Siksek, *Descent on curve of genus* 1, PhD thesis, University of Exeter, 1995.
[19] J.H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics 106, Springer-Verlag, New York, 1992.
[20] S. Stamminger, *Explicit 8-descent on elliptic curves*, PhD thesis, International University Bremen, 2005.
[21] W.A. Stein and M. Watkins, A database of elliptic curves—first report, *Algorithmic number theory* (Sydney, 2002), 267–275, Lecture Notes in Comput. Sci., 2369, Springer, Berlin, 2002.
[22] M. Watkins, *Searching for points p-adically*, notes available from `http://www.maths.bris.ac.uk/~mamjw/papers/`
[23] A. Weil, Remarques sur un mémoire d'Hermite, *Arch. Math.* 5, (1954). 197–202.
[24] T. Womack, *Explicit descent on elliptic curves*, PhD thesis, University of Nottingham, 2003.
[25] Ju. G. Zarhin, Noncommutative cohomology and Mumford groups, *Math. Notes* **15** (1974), 241–244.

University of Cambridge, DPMMS, Centre for Mathematical Sciences, Wilberforce Road, Cambridge CB3 0WB, UK
E-mail address: `T.A.Fisher@dpmms.cam.ac.uk`