Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 58 (2012)

Artikel: Some bounds on the coefficients of covering curves
Autor: Fisher, Tom
DOI: https://doi.org/10.5169/seals-323248

L'Enseignement Mathématique (2) 58 (2012), 99–124

SOME BOUNDS ON THE COEFFICIENTS OF COVERING CURVES

by Tom FISHER

ABSTRACT. We compute bounds on the coefficients of the equations defining everywhere locally soluble n-coverings of elliptic curves over the rationals for $n = 2, 3, 4$. Our proofs use recent work of the author with Cremona and Stoll on the minimisation of genus one curves, together with standard results from the geometry of numbers. We use the same methods to give a criterion (satisfied by only a finite number of "small" elliptic curves) for ruling out the existence of elements of order 3 in the Tate-Shafarevich group.

1. INTRODUCTION

Let $E/\mathbf{Q}$ be an elliptic curve and $n \geq 2$ an integer. The *Selmer group* $S^{(n)}(E/\mathbf{Q})$ parametrises the everywhere locally soluble n-coverings $\pi\colon C \to E$. By global class field theory the curve C admits a $\mathbf{Q}$-rational divisor of degree n and hence can be written as either a double cover of $\mathbf{P}^1$ (case $n = 2$) or a genus one normal curve $C \subset \mathbf{P}^{n-1}$ (case $n \geq 3$). The aim of a descent calculation is to compute the Selmer group $S^{(n)}(E/\mathbf{Q})$ as an abelian group and to represent its elements by equations for the covering curves C. In view of the short exact sequence

$$0 \to E(\mathbf{Q})/nE(\mathbf{Q}) \to S^{(n)}(E/\mathbf{Q}) \to Ш(E/\mathbf{Q})[n] \to 0 \tag{1.1}$$

this gives information about both the *Mordell-Weil group* $E(\mathbf{Q})$ and the *Tate-Shafarevich group* $Ш(E/\mathbf{Q})$. Indeed the covering curves can be used either to help search for points of infinite order in $E(\mathbf{Q})$ or to exhibit explicit elements of $Ш(E/\mathbf{Q})$.

There are two different approaches to explicit 2-descent on an elliptic curve. The *number field method* computes $S^{(2)}(E/\mathbf{Q})$ as a subgroup of $L^\times/(L^\times)^2$ where L is a product of number fields. The Selmer group elements are then converted to binary quartics using a method that relies on an explicit version of

the Hasse principle for conics. In contrast the *invariant theory method* bounds the coefficients of the required binary quartics, and then uses these bounds to make an exhaustive search. The invariant theory method was used by Birch and Swinnerton-Dyer in their pioneering computer calculations [BSD] and subsequently developed by Cremona in his program `mwrank`. The development of computer algebra packages able to compute the class group and units of number fields has since made the number field method equally suitable for computation.

The number field method has been generalised to p-descent (see [DSS], [SS], [CFO]) and is practical for $p = 3$ (and $p = 5$ in small examples). The method relies on an explicit version of the local-to-global principle for the p-torsion of the Brauer group of $\mathbf{Q}$. The number field method also extends to 4-descent and 8-descent, as described in [MSS], [Wo], [S]. The invariant theory method in the case $n = 3$ was investigated in [DS], but does not appear to generalise in any practical way to $n > 2$.

The equations defining an n-covering C of E depend on a choice of co-ordinates on $\mathbf{P}^{n-1}$. It is obviously desirable to make a change of co-ordinates so that the equations have small integer coefficients. In practice this is achieved by the combination of two techniques, termed *minimisation* and *reduction*. In the minimisation stage spurious prime factors are removed from a suitably defined discriminant. In the reduction stage an integer unimodular change of co-ordinates is made to further reduce the size of the coefficients (without changing the discriminant). Minimisation and reduction are important for both the number field and invariant theory methods. In the number field method the equations computed typically have very large coefficients, and we need to minimise and reduce to get sensible answers. In the invariant theory method minimisation and reduction are used at the outset to obtain the bounds upon which the method relies.

In joint work with Cremona and Stoll [CFS] the author has described efficient algorithms for minimising and reducing n-coverings for $n = 2, 3, 4$. (The work on minimisation applies over an arbitrary local field.) It has been found in numerical examples that elements of the Tate-Shafarevich group typically have quite small coefficients and that the size of the coefficients tends to decrease with n. In this paper we give some theoretical support for these observations. In fact we give bounds on the coefficients depending only on the naive height of E. In principle this generalises the invariant theory method to $n = 3, 4$ although the result is certainly not a practical algorithm. In view of this we concentrate on giving a single bound for all the coefficients and do not keep track of certain implied constants. Thus our treatment in the cases $n = 2, 3$ differs from that in [BSD], [DS].

In the cases $n = 2, 3, 4$ we represent Selmer group elements by equations of the following form.

DEFINITION 1.1. A *genus one model* of degree $n \in \{2, 3, 4\}$ is

(i) if $n = 2$, a *binary quartic*, i.e. a homogeneous polynomial of degree 4 in 2 variables,

(ii) if $n = 3$, a *ternary cubic*, i.e. a homogeneous polynomial of degree 3 in 3 variables,

(iii) if $n = 4$, a *quadric intersection*, i.e. a pair of homogeneous polynomials of degree 2 in 4 variables.

Although in [F3] we also defined genus one models of degree 5, it will be understood in this paper that all genus one models are of degrees 2, 3 or 4. Since the theory in [F3] relies on the space of all genus one models being an affine space, it is far from clear what the appropriate definition of genus one model would be for curves of degree $n > 5$.

We recall that the *minimal discriminant* of an elliptic curve $E/\mathbf{Q}$ is

$$\Delta_E = (c_4^3 - c_6^2)/1728\,,$$

where c_4 and c_6 are the usual quantities associated to a globally minimal Weierstrass equation for E. In Theorem 1.2 below we instead work with the *naive height* of E which we define as

$$H_E = \max(|c_4|^{1/4}, |c_6|^{1/6})\,.$$

We write $\|\Phi\|_\infty$ for the maximum of the absolute values of the coefficients of a genus one model Φ. The notation $f \ll g$ should be understood to mean that $f \leq cg$ for some absolute constant $c > 0$.

THEOREM 1.2. *Let $E/\mathbf{Q}$ be an elliptic curve and let $n \in \{2, 3, 4\}$.*

(a) *Each $\xi \in S^{(n)}(E/\mathbf{Q})$ can be represented by a genus one model Φ with integer coefficients and*

$$\|\Phi\|_\infty \ll H_E^6\,.$$

(b) *If ξ is non-zero in $S^{(n)}(E/\mathbf{Q})$ then this bound may be improved to*

$$\|\Phi\|_\infty \ll H_E^4\,.$$

(c) *If the image of ξ in $Ш(E/\mathbf{Q})$ has exact order n then*

$$\|\Phi\|_\infty \ll H_E^{6-n}.$$

We remark that Theorem 1.2(a) gives a proof that $S^{(n)}(E/\mathbf{Q})$ is finite, and hence by (1.1) a proof of the weak Mordell-Weil theorem for $n = 2, 3, 4$. This proof differs from the usual proofs in that we work entirely over the rationals, i.e. we do not need to make any field extensions.

The formulae in Lemmas 3.11 and 3.12 of [CFS] suggest that the exponents of H_E in Theorem 1.2(a) and (b) might be best possible. We suspect that the exponent of H_E in Theorem 1.2(c) is also best possible in view of the models

$$\begin{aligned} n &= 2 \qquad & y^2 &= \lambda_0 x^4 + x^2 z^2 + \lambda_1 z^4 \\ n &= 3 \qquad & \lambda_0 x_0^3 &+ \lambda_1 x_1^3 + \lambda_2 x_2^3 - x_0 x_1 x_2 = 0 \\ n &= 4 \qquad & &\begin{cases} \lambda_0 x_0^2 + x_1 x_3 - \lambda_2 x_2^2 = 0 \\ \lambda_1 x_1^2 + x_0 x_2 - \lambda_3 x_3^2 = 0 \end{cases} \end{aligned}$$

that arise in the context of descent by cyclic isogeny (see [F1, §1.2] for the cases $n = 3, 4$).

We expect that Theorem 1.2 generalises to the case $n = 5$. (See [F3] for the definition of a genus one model of degree 5.)

In favourable circumstances, the geometry of numbers can be used to construct a rational point on a smooth plane cubic. We turn this into a criterion for ruling out the existence of elements of order 3 in the Tate-Shafarevich group.

THEOREM 1.3. *Let E be an elliptic curve over $\mathbf{Q}$ with j-invariant j and minimal discriminant Δ_E. Let*

$$B = \min\{|x| : x \in \mathbf{C} \text{ a root of } (X - 3^3)(X - 3^5)^3 + jX^3 = 0\}.$$

If $|\Delta_E| < \frac{1}{64}B^3$ then $Ш(E/\mathbf{Q})[3] = 0$.

Since B is bounded as a function of j this theorem applies to only finitely many elliptic curves. In fact $B \leq 3^4(2\sqrt{3} - 3)$ and so every elliptic curve satisfying the condition of the theorem has conductor less than 1000. Searching in Cremona's tables [C] we find there are exactly 92 such curves. Their ranks are distributed as follows

rank	0	1	2
# curves	49	41	2

There is no difficulty in verifying by 3-descent (see [SS]) that each of these curves has $Ш(E/\mathbf{Q})[3] = 0$. The interest of Theorem 1.3 instead lies in its method of proof, and in the hope that similar criteria might be found for ruling out elements of order n in $Ш(E/\mathbf{Q})$ for other integers n.

EXAMPLE 1.4. Let E be the elliptic curve

$$y^2 + y = x^3 + x^2 - 2x\,.$$

Then $\Delta_E = 389$, $j = 2^{12}7^3/389$ and $\frac{1}{64}B^3 = 528.57930586\ldots$. Theorem 1.3 shows that $Ш(E/\mathbf{Q})[3] = 0$. In fact $E(\mathbf{Q}) \cong \mathbf{Z}^2$ and the (inverse pairs of) non-trivial elements of $S^{(3)}(E/\mathbf{Q}) \cong (\mathbf{Z}/3\mathbf{Z})^2$ are represented by the ternary cubics

$$\begin{aligned}
F_1(x,y,z) &= x^2z - xy^2 - 2xyz + xz^2 + y^2z + yz^2\\
F_2(x,y,z) &= x^2z - xy^2 + 2xyz - yz^2 - z^3\\
F_3(x,y,z) &= x^2y - xy^2 - xz^2 - y^2z - 2yz^2\\
F_4(x,y,z) &= x^2y + xy^2 - 2xyz + xz^2 - y^2z - yz^2\,.
\end{aligned}$$

2. BACKGROUND AND OVERVIEW

2.1 INVARIANTS OF GENUS ONE MODELS

We work over a field K of characteristic zero and write $\overline{K}$ for its algebraic closure. The space of genus one models of degree $n = 2,3,4$ is acted on by the group $\mathcal{G}_n$ defined as follows

$$\begin{aligned}
\mathcal{G}_2 &= \mathbf{G}_m \times \mathrm{GL}_2 \qquad & [\mu, N]\colon F &\mapsto \mu^2(F \circ N)\\
\mathcal{G}_3 &= \mathbf{G}_m \times \mathrm{GL}_3 \qquad & [\mu, N]\colon F &\mapsto \mu(F \circ N)\\
\mathcal{G}_4 &= \mathrm{GL}_2 \times \mathrm{GL}_4 \qquad & [M, N]\colon (Q_1, Q_2)^T &\mapsto M(Q_1 \circ N, Q_2 \circ N)^T\,.
\end{aligned}$$

Let $\det\colon \mathcal{G}_n \to \mathbf{G}_m$ be the character defined by $[\mu, N] \mapsto \mu \det N$, respectively $[M, N] \mapsto \det M \det N$. An *invariant of weight* k is a polynomial I in the coefficients of a genus one model satisfying

$$I(g\Phi) = \det(g)^k I(\Phi) \tag{2.1}$$

for all $g \in \mathcal{G}_n$. The action of the centre of $\mathcal{G}_n$ shows that I is homogeneous of degree $kn/(6-n)$. In each of the cases $n = 2,3,4$ the ring of invariants is generated by invariants c_4 and c_6 of weights 4 and 6. See [F3, §7], [CFS] for explicit formulae. We put $\Delta = (c_4^3 - c_6^2)/1728$. It is shown in [AKM], [F3] that Φ is *non-singular* (i.e. defines a smooth curve of genus one) if and only if $\Delta(\Phi) \neq 0$, and that the Jacobian elliptic curve is

$$y^2 = x^3 - 27c_4(\Phi)x - 54c_6(\Phi)\,. \tag{2.2}$$

DEFINITION 2.1. Genus one models Φ_1 and Φ_2 are *K-equivalent* if they are in the same orbit for the action of $\mathcal{G}_n(K)$. They are *properly K-equivalent* if $\Phi_2 = g\Phi_1$ for some $g \in \mathcal{G}_n(K)$ with $\det g = 1$.

LEMMA 2.2. *Non-singular genus one models Φ_1 and Φ_2 are properly $\bar{K}$-equivalent if and only if they have the same invariants, i.e. $c_4(\Phi_1) = c_4(\Phi_2)$ and $c_6(\Phi_1) = c_6(\Phi_2)$.*

Proof. The first implication is clear by (2.1). For the converse, we see by Propositions 4.6 and 4.7 in [F3] that every non-singular model is properly $\bar{K}$-equivalent to a model of the form

$$\begin{aligned} n &= 2 \qquad & y^2 &= x^3z + Axz^3 + Bz^4 \\ n &= 3 \qquad & y^2z &= x^3 + Axz^2 + Bz^3 \\ n &= 4 \qquad & x^2 - zt &= y^2 - xt - Axz - Bz^2 = 0\,. \end{aligned}$$

It then suffices to note that these "Weierstrass models" are uniquely determined by their invariants. In fact $c_4 = -48A$ and $c_6 = -864B$. □

A non-singular genus one model Φ defines both a smooth curve of genus one C and a regular 1-form ω on C. Writing F_i for the partial derivative of F with respect to x_i we have

$$\begin{aligned} n &= 2 \qquad & y^2 &= F(x_0, x_1) \qquad & \omega &= x_0^2 d(x_1/x_0)/2y \\ n &= 3 \qquad & F(x_0, x_1, x_2) &= 0 \qquad & \omega &= x_0^2 d(x_1/x_0)/F_2 \\ n &= 4 \qquad & F = G &= 0 \qquad & \omega &= x_0^2 d(x_1/x_0)/(F_2G_3 - F_3G_2)\,. \end{aligned}$$

It is shown in [F3, Proposition 5.19] that if $\Phi_2 = g\Phi_1$ and $\gamma\colon C_2 \to C_1$ is the morphism determined by g then

$$\gamma^*\omega_1 = (\det g)\,\omega_2\,. \tag{2.3}$$

2.2 GALOIS COHOMOLOGY

We consider pairs $(C \to S, \omega)$ where $C \to S$ is a morphism from a smooth curve of genus one C to a Brauer-Severi variety S, and ω is a regular 1-form on C. An *isomorphism* between $(C_1 \to S_1, \omega_1)$ and $(C_2 \to S_2, \omega_2)$ is a pair of isomorphisms $\phi\colon C_1 \cong C_2$ and $\psi\colon S_1 \cong S_2$ such that $\phi^*\omega_2 = \omega_1$ and the following diagram commutes

$$\begin{array}{ccc} C_1 & \longrightarrow & S_1 \\ {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle\psi} \\ C_2 & \longrightarrow & S_2 \end{array}$$

Let $n \geq 2$ be an integer. Let E/K be an elliptic curve with invariant differential ω_E. We map $E \to \mathbf{P}^{n-1}$ via the complete linear system $|n.0_E|$, i.e. we map $P \mapsto (f_0(P) : \ldots : f_{n-1}(P))$ where $f_0, \ldots, f_{n-1}$ are a basis for the Riemann-Roch space

$$\mathcal{L}(n.0_E) = \{f \in K(E)^\times \mid \operatorname{div}(f) + n.0_E \geq 0\} \cup \{0\}.$$

We recall that objects defined over K are called *twists* if they are isomorphic over $\overline{K}$.

LEMMA 2.3. *The twists of* $(E \to \mathbf{P}^{n-1}, \omega_E)$, *up to* K*-isomorphism, are parametrised by* $H^1(K, E[n])$.

Proof. This is [F2, Lemma 2.3]. □

The *obstruction map*, defined in [O], [CFO], is

$$\begin{aligned} \mathrm{Ob}\colon H^1(K, E[n]) &\to \mathrm{Br}(K) \\ (C \to S, \omega) &\mapsto [S]. \end{aligned}$$

In general this map is not a group homomorphism. Nonetheless we write ker(Ob) for the inverse image of the identity.

LEMMA 2.4. *Let* E/K *be an elliptic curve and let* $n \in \{2, 3, 4\}$. *Then the genus one models of degree* n *with the same invariants as a fixed Weierstrass equation for* E, *up to proper* K*-equivalence, are parametrised by* $\ker(\mathrm{Ob}) \subset H^1(K, E[n])$.

Proof. A non-singular genus one model Φ defines a smooth curve of genus one $C \to \mathbf{P}^{n-1}$ and a regular 1-form ω on C. Conversely, every twist $(C \to S, \omega)$ of $(E \to \mathbf{P}^{n-1}, \omega_E)$ with $S \cong \mathbf{P}^{n-1}$ arises in this way. Let Φ_E be a genus one model defining $(E \to \mathbf{P}^{n-1}, \omega_E)$. By (2.2) it has the same invariants as some Weierstrass equation for E. We see by (2.3) that Φ_1 and Φ_2 are properly equivalent if and only if they determine isomorphic pairs $(C_1 \to \mathbf{P}^{n-1}, \omega_1)$ and $(C_2 \to \mathbf{P}^{n-1}, \omega_2)$. Thus ker(Ob) parametrises the genus one models properly $\overline{K}$-equivalent to Φ_E, up to proper K-equivalence. By Lemma 2.2 the genus one models properly $\overline{K}$-equivalent to Φ_E are those with the same invariants as Φ_E. □

REMARK 2.5. The subset $\ker(\mathrm{Ob}) \subset H^1(K, E[n])$ contains the identity and is closed under taking inverses. A binary quartic represents the identity

if and only if it has a K-rational root. A ternary cubic, respectively quadric intersection, represents the identity if and only if it has a K-rational point of inflection, respectively hyperosculating point.

Taking Galois cohomology of the short exact sequence $0 \to E[2] \to E[4] \to E[2] \to 0$ gives an exact sequence

$$E(K)[2] \longrightarrow H^1(K, E[2]) \xrightarrow{\iota_*} H^1(K, E[4]) \xrightarrow{[2]_*} H^1(K, E[2])\,.$$

LEMMA 2.6. *The maps ι_* and $[2]_*$ have the following interpretations.*

(i) *The binary quartic $F(x,z) = ax^4 + bx^3z + cx^2z^2 + dxz^3 + ez^4$ is mapped by ι_* to the quadric intersection*

$$x_0x_2 - x_1^2 = x_3^2 - ax_0^2 - bx_0x_1 - cx_1^2 - dx_1x_2 - ex_2^2 = 0\,. \tag{2.4}$$

(ii) *The quadric intersection (Q_1, Q_2) where $Q_i(\mathbf{x}) = \mathbf{x}^T A_i \mathbf{x}$ for $i = 1, 2$ is mapped by $[2]_*$ to the binary quartic*

$$F(x,z) = \det(A_1x + A_2z)\,.$$

Proof. (i) Let C_2 be the curve defined by $y^2 = F(x,z)$ and $C_4 \subset \mathbf{P}^3$ the curve defined by (2.4). Note that C_4 is the image of C_2 under the embedding

$$(x : y : z) \mapsto (x^2 : xz : z^2 : y)\,. \tag{2.5}$$

If C_2' is a double cover of $\mathbf{P}^1$ and C_4' a quadric intersection, and these are related in the same way as C_2 and C_4, then each isomorphism $(C_2 \to \mathbf{P}^1) \cong (C_2' \to \mathbf{P}^1)$ induces an isomorphism $(C_4 \to \mathbf{P}^3) \cong (C_4' \to \mathbf{P}^3)$ compatible with the embeddings (2.5). Hence twisting $(C_2 \to \mathbf{P}^1)$ by $\xi \in H^1(K, E[2])$ has the effect of twisting $(C_4 \to \mathbf{P}^3)$ by $\iota_*\xi \in H^1(K, E[4])$.

(ii) Let C_4 be the curve $Q_1 = Q_2 = 0$ and C_2 the curve $y^2 = F(x,z)$. Weil [We, Chapter II, Appendix III] constructs a morphism $\omega\colon C_4 \times C_4 \to C_2$ with the property that

$$\omega(P,Q) = \omega(P',Q') \iff P + Q \sim P' + Q'\,,$$

where $\sim$ denotes linear equivalence of divisors. For fixed $P \in C_4$ the map $Q \mapsto \omega(P,Q)$ induces a map on Jacobians that is independent of the choice of P. This map is an isomorphism and we use it to identify the Jacobians of C_4 and C_2. Then $P \mapsto \omega(P,P)$ is a morphism that induces multiplication-by-2 on the Jacobians. Explicit formulae for this covering map are given in [AKM], [MSS]. If C_4' and C_2' are related in the same way

as C_4 and C_2 then each isomorphism $(C_4 \to \mathbf{P}^3) \cong (C_4' \to \mathbf{P}^3)$ induces an isomorphism $(C_2 \to \mathbf{P}^1) \cong (C_2' \to \mathbf{P}^1)$ compatible with the covering maps. Hence twisting $(C_4 \to \mathbf{P}^3)$ by $\xi \in H^1(K, E[4])$ has the effect of twisting $(C_2 \to \mathbf{P}^1)$ by $[2]_*\xi \in H^1(K, E[2])$. □

2.3 Minimisation and reduction

We quote the following result on minimisation.

PROPOSITION 2.7. *Let $n \in \{2,3,4\}$. Let C be an everywhere locally soluble n-covering of an elliptic curve $E/\mathbf{Q}$. Let c_4 and c_6 be the invariants of a minimal Weierstrass equation for E. Then C can be defined by an integer coefficient genus one model with invariants c_4 and c_6, except in the case $n = 2$ where it may only be possible to find a model with invariants 2^4c_4 and 2^6c_6.*

Proof. This is [CFS, Theorem 1.1]. In [CFS] we gave a more general definition of genus one model of degree 2. The models considered here are obtained by completing the square. This has the effect of multiplying the invariants c_4 and c_6 by 2^4 and 2^6. □

Our treatment of reduction differs from that in [CFS]. In that paper our goal was to find a practical algorithm for reducing, whereas here we are interested in bounding coefficients. We recall that a genus one model Φ is non-singular if it defines a smooth curve of genus one, equivalently $\Delta(\Phi) \neq 0$. We say that Φ is *real* if it has real coefficients. In Section 3 we prove

PROPOSITION 2.8. *Let $n \in \{2,3,4\}$. Let Φ be a non-singular real genus one model of degree n with invariants c_4 and c_6. Then Φ is properly $\mathbf{R}$-equivalent to a genus one model Φ' with $\|\Phi'\|_\infty \ll H^{(6-n)/n}$ where $H = \max(|c_4|^{1/4}, |c_6|^{1/6})$.*

Since c_4 and c_6 are polynomials of degrees $4n/(6-n)$ and $6n/(6-n)$ the exponent of H in Proposition 2.8 is best possible. Combining the last two propositions we immediately deduce

THEOREM 2.9. *Let $n \in \{2,3,4\}$. Let C be an everywhere locally soluble n-covering of an elliptic curve $E/\mathbf{Q}$. Then C can be defined by an integer coefficient genus one model that is properly $\mathbf{R}$-equivalent to a genus one model Φ' with $\|\Phi'\|_\infty \ll H_E^{(6-n)/n}$.*

We write $\|x\| = (\sum x_i^2)^{1/2}$ for the usual Euclidean norm. In Section 4 we use the geometry of numbers to deduce Theorem 1.2 from Theorem 2.9. The key fact here is

LEMMA 2.10 (Minkowski). *Let $\Lambda \subset \mathbf{R}^n$ be a rank n lattice with covolume 1. Then there are linearly independent vectors $v_1, \dots, v_n \in \Lambda$ with $\prod_{i=1}^n \|v_i\| \le \gamma_n^{n/2}$ where γ_n^n is Hermite's constant.*

Proof. See for example [PZ, p. 197]. In fact for $n \le 4$ we can take $v_1, \dots, v_n$ a basis for Λ. □

The exact value of Hermite's constant is known for $n \le 8$.

n	1	2	3	4	5	6	7	8
γ_n^n	1	4/3	2	4	8	64/3	64	256

We use Lemma 2.10 to give upper bounds on all of the $\|v_i\|$. For this we need lower bounds on some of the $\|v_i\|$. The hypotheses in parts (a), (b) and (c) of Theorem 1.2 are used to give successively better lower bounds, and hence successively better upper bounds.

3. NORMAL FORMS FOR GENUS ONE MODELS OVER THE REALS

In this section we prove Proposition 2.8.

LEMMA 3.1. *Let $E/\mathbf{R}$ be an elliptic curve and $n \ge 2$ an integer.*

(i) *If n is odd or $\Delta_E < 0$ then $H^1(\mathbf{R}, E[n]) = 0$.*

(ii) *If n is even and $\Delta_E > 0$ then $H^1(\mathbf{R}, E[n]) \cong (\mathbf{Z}/2\mathbf{Z})^2$ and the obstruction map $H^1(\mathbf{R}, E[n]) \to \mathrm{Br}(\mathbf{R})$ has kernel of size 3.*

Proof. We recall that $E[n] \cong (\mathbf{Z}/n\mathbf{Z})^2$ has a basis S, T with $S \in E(\mathbf{R})$ and

$$\sigma(T) = \begin{cases} -T & \text{if } \Delta_E > 0 \\ S - T & \text{if } \Delta_E < 0 \end{cases},$$

where σ denotes complex conjugation. It is easy to compute $H^1(\mathbf{R}, E[n])$ using the rule

$$H^1(\mathbf{R}, A) = \frac{\{a \in A : a + \sigma(a) = 0\}}{\{b - \sigma(b) : b \in A\}}.$$

Now suppose n is even and $\Delta_E > 0$. Then $E(\mathbf{R}) \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{R}/\mathbf{Z}$ and the exact sequence

$$0 \to E(\mathbf{R})/nE(\mathbf{R}) \to H^1(\mathbf{R}, E[n]) \to H^1(\mathbf{R}, E)[n] \to 0$$

shows that ker(Ob) has size at least 2. Let $(\ ,\ )$ be the *Tate pairing*

$$H^1(\mathbf{R}, E[n]) \times H^1(\mathbf{R}, E[n]) \to \mathrm{Br}(\mathbf{R})$$

defined by the Weil pairing and cup product. It is shown in [O], [Z] that

$$(\xi, \eta) = \mathrm{Ob}(\xi + \eta) - \mathrm{Ob}(\xi) - \mathrm{Ob}(\eta)$$

for all $\xi, \eta \in H^1(\mathbf{R}, E[n])$. Since the Tate pairing is non-degenerate, the obstruction map is not linear, and hence ker(Ob) has size 3. □

Let $E/\mathbf{R}$ be an elliptic curve and let c_4 and c_6 be the invariants of a fixed Weierstrass equation. Lemma 2.4 identifies the proper $\mathbf{R}$-equivalence classes of genus one models with invariants c_4 and c_6 with $\ker(\mathrm{Ob}) \subset H^1(\mathbf{R}, E[n])$. Our strategy for proving Proposition 2.8 is therefore the following. According as we are in case (i) or (ii) of Lemma 3.1 we exhibit either 1 or 3 real genus one models with the given invariants. In case (ii) we then check that these models are not equivalent over the reals.

3.1 Binary quartics

As suggested in Lemma 3.1 we split into cases according to the sign of the discriminant.

LEMMA 3.2. *Let $E/\mathbf{R}$ be an elliptic curve with positive discriminant. We fix a Weierstrass equation*

$$y^2 = (x - e_1)(x - e_2)(x - e_3)\,, \tag{3.1}$$

where $e_1, e_2, e_3 \in \mathbf{R}$. Then every real binary quartic with the same invariants as (3.1) *is properly $\mathbf{R}$-equivalent to exactly one of F_1, F_2, F_3 where*

$$F_i(x, z) = a_i(x^4 + z^4) + 2b_i x^2 z^2$$

and for i, j, k a cyclic permutation of $1, 2, 3$ we put

$$a_i = (e_i - e_j)/4\,, \qquad b_i = (e_i + e_j - 2e_k)/4\,.$$

Proof. A direct calculation shows that the quartics $F_i(x,z)$ have the same invariants as (3.1). Let r,s,t be the permutation of $1,2,3$ with $e_r < e_s < e_t$. Since

$$4F_i(x,z) = (e_i - e_j)(x^2 - z^2)^2 + 4(e_i - e_k)x^2z^2$$

it is clear that $F_r(x,z) < 0$ and $F_t(x,z) > 0$ for all $(x : z) \in \mathbf{P}^1(\mathbf{R})$, whereas $F_s(x,z) = 0$ has 4 roots in $\mathbf{P}^1(\mathbf{R})$. Hence the $F_i(x,z)$ are not equivalent over the reals. □

The analogous result for negative discriminants is the following.

LEMMA 3.3. *Let $E/\mathbf{R}$ be an elliptic curve with negative discriminant. We fix a Weierstrass equation*

$$y^2 = (x - e_1)(x - e_2)(x - e_3)\,, \tag{3.2}$$

where $e_1, e_2 \in \mathbf{C}$ are complex conjugates and $e_3 \in \mathbf{R}$. Then every real binary quartic with the same invariants as (3.2) *is properly $\mathbf{R}$-equivalent to*

$$F(x,z) = a(x^4 - z^4) + 2bx^2z^2\,,$$

where

$$a = (e_1 - e_2)/4i\,, \qquad b = (e_1 + e_2 - 2e_3)/4\,.$$

Proof. A direct calculation shows that the quartic $F(x,z)$ has the same invariants as (3.2). □

The proof of Proposition 2.8 in the case $n = 2$ is completed by the following trivial lemma.

LEMMA 3.4. *Let e_1, e_2, e_3 be the roots of $f(x) = x^3 - 27c_4x - 54c_6$. Then $\max(|e_1|, |e_2|, |e_3|) \ll H^2$ where $H = \max(|c_4|^{1/4}, |c_6|^{1/6})$.*

Proof. Since $f(e_i) = 0$ we have $|e_i|^3 \ll \max(|c_4e_i|, |c_6|)$. The result is immediate. □

3.2 RECALL OF ANALYTIC FORMULAE

Before proceeding with the proof of Proposition 2.8 in the cases $n = 3, 4$ we recall some standard analytic formulae. For $\tau \in \mathfrak{H} = \{z \in \mathbf{C} : \mathrm{Im}(z) > 0\}$ and $\alpha \in \mathbf{Q}$ we write $q^\alpha = e^{2\pi i\alpha\tau}$. The *Dedekind η-function*

$$\eta(\tau) = q^{1/24}\prod_{n\geq 1}(1 - q^n) \tag{3.3}$$

satisfies the functional equation

$$\eta(-1/\tau) = \sqrt{\tfrac{\tau}{i}}\eta(\tau)\,. \tag{3.4}$$

A useful formula in this context is the *Jacobi triple product identity*

$$\prod_{n\geq 1}(1-q^{2n})(1-q^{2n-1}z)(1-q^{2n-1}z^{-1}) = \sum_{n\in\mathbf{Z}}(-1)^n q^{n^2}z^n. \tag{3.5}$$

The spaces of modular forms of level 1 and weight $k = 4, 6$ are spanned by the *Eisenstein series*

$$E_4(\tau) = 1 + 240\sum_{n\geq 1}\sigma_3(n)q^n\,, \qquad E_6(\tau) = 1 - 504\sum_{n\geq 1}\sigma_5(n)q^n\,,$$

where $\sigma_m(n) = \sum_{d|n} d^m$. The *discriminant modular form* is

$$\Delta(\tau) = \eta(\tau)^{24} = (E_4(\tau)^3 - E_6(\tau)^2)/1728\,.$$

The Eisenstein series E_4 and E_6 are related to the invariants c_4 and c_6 as described in the following well-known lemma (see, for example, [C, p.45]).

LEMMA 3.5. *Let E be an elliptic curve over $\mathbf{C}$ with Weierstrass equation*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\,. \tag{3.6}$$

Let Λ be the period lattice obtained by integrating $dx/(2y + a_1x + a_3)$. If we choose a basis ω_1, ω_2 for Λ so that $\tau = \omega_2/\omega_1 \in \mathfrak{H}$ then the invariants c_4 and c_6 of the Weierstrass equation (3.6) *are given by $c_k = (\frac{2\pi}{\omega_1})^k E_k(\tau)$.*

Proof. The *Weierstrass $\wp$-function*

$$\wp(z) = \frac{1}{z^2} + \sum_{0\neq\lambda\in\Lambda}\Big(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2}\Big)$$

satisfies the equation

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3\,, \tag{3.7}$$

where $g_2 = 60G_4(\Lambda)$, $g_3 = 140G_6(\Lambda)$. Moreover for $k \geq 4$ we have

$$G_k(\Lambda) = \sum_{0\neq\lambda\in\Lambda}\frac{1}{\lambda^k} = \frac{2\zeta(k)}{\omega_1^k}E_k(\tau)\,.$$

Hence $g_2 = \frac{1}{12}(\frac{2\pi}{\omega_1})^4 E_4(\tau)$ and $g_3 = \frac{1}{216}(\frac{2\pi}{\omega_1})^6 E_6(\tau)$. The uniformisation map ϕ with $\phi^*(dx/(2y + a_1x + a_3)) = dz$ is given by

$$\begin{aligned}\phi\colon \mathbf{C}/\Lambda &\to E(\mathbf{C})\\ z &\mapsto \big(\wp(z) - \tfrac{1}{12}b_2\,,\ \tfrac{1}{2}\wp'(z) - a_1(\wp(z) - \tfrac{1}{12}b_2) - a_3\big)\,,\end{aligned}$$

where $b_2 = a_1^2 + 4a_2$. A calculation comparing (3.6) and (3.7) now shows that $c_4 = 12g_2$ and $c_6 = 216g_3$. □

3.3 Ternary cubics

Differentiating the Jacobi triple product identity (3.5) with respect to z and putting $z = q$ we obtain

$$\eta(\tau)^3 = \sum_{n\in\mathbf{Z}} (-1)^n n q^{(2n+1)^2/8} = q^{1/8} \prod_{n\geq 1} (1-q^n)^3 . \tag{3.8}$$

LEMMA 3.6. *For $k = 4, 6$ we have*

$$E_k(\tau) = f_k(\eta(\tfrac{\tau}{3})^3, \sqrt{27}\eta(3\tau)^3)/\eta(\tau)^k ,$$

where

$$f_4(a,b) = a^4 + \tfrac{4}{\sqrt{3}} a^3 b + 2a^2 b^2 + \tfrac{4}{\sqrt{3}} ab^3 + b^4$$
$$f_6(a,b) = a^6 + 2\sqrt{3}a^5 b + 5a^4 b^2 - 5a^2 b^4 - 2\sqrt{3}ab^5 - b^6 .$$

Proof. Let $F_k(\tau) = f_k(\eta(\frac{\tau}{3})^3, \sqrt{27}\eta(3\tau)^3)/\eta(\tau)^k$. It is easily seen that the q-expansions of $F_4(\tau)$ and $F_6(\tau)$ each have leading term 1.

Let $\zeta_n = e^{2\pi i/n}$. By (3.8) we have

$$\begin{aligned}
\eta(\tfrac{\tau}{3})^3 - \zeta_{24}^{-1}\eta(\tfrac{\tau+1}{3})^3 &= (1-\zeta_3) \sum_{n\equiv 1 \bmod 3} (-1)^n n q^{(2n+1)^2/24} \\
&= (1-\zeta_3) \sum_{n\in\mathbf{Z}} (-1)^{3n+1} (3n+1) q^{3(2n+1)^2/8} \\
&= 3(\zeta_3 - 1)\eta(3\tau)^3 .
\end{aligned}$$

Hence

$$\frac{\eta(\frac{\tau+1}{3})^3}{\eta(\tau+1)} = \frac{\eta(\frac{\tau}{3})^3}{\eta(\tau)} + \sqrt{27} i \zeta_3^2 \frac{\eta(3\tau)^3}{\eta(\tau)} . \tag{3.9}$$

It is readily verified that

$$f_k(a + i\zeta_3^2 b, \zeta_3 b) = f_k(a,b) .$$

Hence $F_k(\tau+1) = F_k(\tau)$. A straightforward calculation using the functional equation (3.4) shows that $F_k(-1/\tau) = \tau^k F_k(\tau)$. Since the space of modular forms of level 1 and weight $k = 4, 6$ is 1-dimensional it follows that $E_k = F_k$. □

LEMMA 3.7. *Let $E/\mathbf{R}$ be an elliptic curve with Weierstrass equation*

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 . \tag{3.10}$$

Let $\Lambda = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$ be the period lattice obtained by integrating $dx/(2y + a_1 x + a_3)$. We may assume that $\omega_1 \in \mathbf{R}_{>0}$ and $\tau = \omega_2/\omega_1 \in \mathfrak{H}$

with $\mathrm{Re}(\tau) \in \{0, 3/2\}$. *Then every real ternary cubic with the same invariants as* (3.10) *is properly* $\mathbf{R}$*-equivalent to*

$$F(x, y, z) = a(x^3 + y^3 + z^3) - 3(a + \sqrt{3}b)xyz\ ,$$

where

$$a = \frac{1}{\sqrt{27}}\left(\frac{2\pi}{\omega_1}\right)\frac{\eta(\tau/3)^3}{\eta(\tau)}\ , \qquad b = \left(\frac{2\pi}{\omega_1}\right)\frac{\eta(3\tau)^3}{\eta(\tau)}\ .$$

Proof. Since $\mathrm{Re}(\tau) \in \{0, 3/2\}$ it is clear that $q^{1/3}$ is real, and hence a and b are real. For $k = 4, 6$ we compute

$$c_k(F) = 3^{3k/2} f_k(a, b) = (\tfrac{2\pi}{\omega_1})^k f_k\big(\eta(\tfrac{\tau}{3})^3, \sqrt{27}\eta(3\tau)^3\big)/\eta(\tau)^k = (\tfrac{2\pi}{\omega_1})^k E_k(\tau)\,.$$

It follows by Lemma 3.5 that F has the same invariants as (3.10). □

The proof of Proposition 2.8 in the case $n = 3$ is completed by

LEMMA 3.8. *For* $\tau \in \mathfrak{H}$ *with* $\mathrm{Re}(\tau) \in \{0, 3/2\}$ *we have*

$$\max\left(\left|\frac{\eta(\tau/3)^3}{\eta(\tau)}\right|, \left|\frac{\eta(3\tau)^3}{\eta(\tau)}\right|\right) \ll \max(|E_4(\tau)|^{1/4}, |E_6(\tau)|^{1/6})\,. \tag{3.11}$$

Proof. The functional equation (3.4) shows we are free to replace τ by $-1/\tau$. Likewise (3.9) shows we may replace τ by $\tau + 1$. So if the bound holds on some subset of $\mathfrak{H}$, then it will hold on any $\mathrm{SL}_2(\mathbf{Z})$-translate of that subset (possibly with a different implied constant).

We only need to establish the bound for $\mathrm{Im}(\tau)$ large and $\mathrm{Im}(\tau)$ small, since the result will then follow by a compactness argument. (Note that E_4 and E_6 have no common zeros in $\mathfrak{H}$.) As $\mathrm{Im}(\tau) \to \infty$ we have $q \to 0$ and the result is clear. By the action of $\mathrm{SL}_2(\mathbf{Z})$ this implies the result for $\mathrm{Im}(\tau)$ small. □

3.4 QUADRIC INTERSECTIONS

Putting $z = -q, \pm 1$ in the Jacobi triple product identity (3.5) we obtain functions

$$\begin{aligned}
\theta_2(\tau) &= \sum_{n\in\mathbf{Z}} q^{(2n+1)^2/4} = 2q^{1/4}\prod_{n=1}^{\infty}(1 - q^{2n})(1 + q^{2n})^2 \\
\theta_3(\tau) &= \sum_{n\in\mathbf{Z}} q^{n^2} = \prod_{n=1}^{\infty}(1 - q^{2n})(1 + q^{2n-1})^2 \qquad (3.12)\\
\theta_4(\tau) &= \sum_{n\in\mathbf{Z}} (-1)^n q^{n^2} = \prod_{n=1}^{\infty}(1 - q^{2n})(1 - q^{2n-1})^2\,.
\end{aligned}$$

LEMMA 3.9. *For* $k = 4, 6$ *we have*

$$E_k(\tau) = f_k(\theta_2(\tau), \theta_3(\tau)) = (\tfrac{1}{2i})^k f_k(\theta_3(\tfrac{\tau}{4}), \theta_4(\tfrac{\tau}{4}))\,,$$

where

$$f_4(a,b) = a^8 + 14a^4b^4 + b^8$$
$$f_6(a,b) = a^{12} - 33a^8b^4 - 33a^4b^8 + b^{12}\,.$$

Proof. Let $F_k(\tau) = f_k(\theta_2(\tau), \theta_3(\tau))$. It is clear that $F_4(\tau)$ and $F_6(\tau)$ are power series in q with constant term 1. So to prove the first equality it suffices to show that $F_k(-1/\tau) = \tau^k F_k(\tau)$ for $k = 4, 6$.

The expressions for the $\theta_j(\tau)$ as products allow us to rewrite them in terms of the Dedekind η-function:

$$\theta_2(\tau) = 2\frac{\eta(4\tau)^2}{\eta(2\tau)}\,, \qquad \theta_3(\tau) = \frac{\eta(2\tau)^5}{\eta(\tau)^2\eta(4\tau)^2}\,, \qquad \theta_4(\tau) = \frac{\eta(\tau)^2}{\eta(2\tau)}\,.$$

By the functional equation (3.4) and the expressions for the $\theta_j(\tau)$ as sums, we deduce

$$\begin{aligned} \theta_2(-1/\tau) &= \sqrt{\tfrac{\tau}{2i}}\theta_4(\tfrac{\tau}{4}) = \sqrt{\tfrac{\tau}{2i}}(-\theta_2(\tau) + \theta_3(\tau)) \\ \theta_3(-1/\tau) &= \sqrt{\tfrac{\tau}{2i}}\theta_3(\tfrac{\tau}{4}) = \sqrt{\tfrac{\tau}{2i}}(\theta_2(\tau) + \theta_3(\tau))\,. \end{aligned} \tag{3.13}$$

It is readily verified that

$$f_k(-a+b, a+b) = (2i)^k f_k(a,b)\,.$$

Hence

$$\begin{aligned} F_k(-1/\tau) &= f_k(\theta_2(-1/\tau), \theta_3(-1/\tau)) \\ &= (\tfrac{\tau}{2i})^k f_k(-\theta_2(\tau) + \theta_3(\tau), \theta_2(\tau) + \theta_3(\tau)) = \tau^k F_k(\tau)\,. \end{aligned}$$

Since the space of modular forms of level 1 and weight $k = 4, 6$ is 1-dimensional it follows that $E_k = F_k$. The second expression for E_k is obtained by replacing τ by $-1/\tau$ and using (3.13). □

As suggested in Lemma 3.1 we split into cases according to the sign of the discriminant.

LEMMA 3.10. *Let* $E/\mathbf{R}$ *be an elliptic curve with positive discriminant and with Weierstrass equation*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\,. \tag{3.14}$$

Let $\Lambda = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$ *be the period lattice obtained by integrating* $dx/(2y + a_1x + a_3)$. *We may assume that* $\omega_1 \in \mathbf{R}_{>0}$ *and* $\tau = \omega_2/\omega_1 \in \mathfrak{H}$ *with* $\mathrm{Re}(\tau) = 0$. *Then every real quadric intersection with the same invariants as* (3.14) *is properly* $\mathbf{R}$*-equivalent to exactly one of* (Q_1, Q_2), (Q_1', Q_2'), (Q_1'', Q_2'') *where*

$$Q_1 = a(x_0^2 + x_2^2) - 2bx_1x_3 \qquad Q_1' = a(x_0^2 - x_2^2) - 2bx_1x_3$$
$$Q_2 = a(x_1^2 + x_3^2) - 2bx_0x_2 \qquad Q_2' = a(x_1^2 - x_3^2) - 2bx_0x_2$$

$$Q_1'' = b(x_0^2 + x_2^2) - 2ax_1x_3$$
$$Q_2'' = b(x_1^2 + x_3^2) - 2ax_0x_2$$

and

$$a = \tfrac{1}{2}\sqrt{\frac{\pi}{\omega_1}}\theta_4(\tau/4)\,, \qquad b = \tfrac{1}{2}\sqrt{\frac{\pi}{\omega_1}}\theta_3(\tau/4)\,.$$

Proof. In the notation of Lemma 3.9 all three quadric intersections have invariants $2^8 f_4(a,b)$ and $-2^{12} f_6(a,b)$. For $k = 4, 6$ we compute

$$(4i)^k f_k(a,b) = (\tfrac{i\pi}{\omega_1})^k f_k(\theta_4(\tfrac{\tau}{4}), \theta_3(\tfrac{\tau}{4})) = (\tfrac{2\pi}{\omega_1})^k E_k(\tau)\,.$$

It follows by Lemma 3.5 that these quadric intersections have the same invariants as (3.14). It remains to show that they are pairwise inequivalent over the reals.

Since $\mathrm{Re}(\tau) = 0$ we have $q > 0$ and hence $b > a > 0$. We put $c = \sqrt[4]{b^4 - a^4}$. Then $Q_1 = Q_2 = 0$ has real point (in fact a hyperosculating point)

$$(x_0 : x_1 : x_2 : x_3) = (\sqrt{b^2 + c^2} : \sqrt{ab} : \sqrt{b^2 - c^2} : \sqrt{ab})\,.$$

Rather more obviously $Q_1' = Q_2' = 0$ has real point

$$(x_0 : x_1 : x_2 : x_3) = (\sqrt{2b/a} : 1 : 0 : 1)\,.$$

On the other hand, since the quadratic form

$$Q_1'' + Q_2'' = \tfrac{b-a}{2}\left((x_0 + x_2)^2 + (x_1 + x_3)^2\right) + \tfrac{a+b}{2}\left((x_0 - x_2)^2 + (x_1 - x_3)^2\right)$$

is positive definite, there are no real solutions to $Q_1'' = Q_2'' = 0$.

Finally we claim that (Q_1, Q_2) and (Q_1', Q_2') are not equivalent over the reals. Let A_1, A_2 be the matrices of second partial derivatives of Q_1, Q_2 and likewise for Q_1', Q_2'. We compute

$$\det(xA_1 + zA_2) = -2^4(a^2x^2 - b^2z^2)(b^2x^2 - a^2z^2)$$
$$\det(xA_1' + zA_2') = 2^4(a^2x^2 + b^2z^2)(b^2x^2 + a^2z^2)\,.$$

The first of these quartics has four real roots, whereas the second has no real roots. This proves our claim $\square$

The analogous result for negative discriminants is the following.

LEMMA 3.11. *Let $E/\mathbf{R}$ be an elliptic curve with negative discriminant and with Weierstrass equation*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\,. \tag{3.15}$$

Let $\Lambda = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$ be the period lattice obtained by integrating $dx/(2y + a_1x + a_3)$. We may assume that $\omega_1 \in \mathbf{R}_{>0}$ and $\tau = \omega_2/\omega_1 \in \mathfrak{H}$ with $\mathrm{Re}(\tau) = 1/2$. Then every real quadric intersection with the same invariants as (3.15) *is properly $\mathbf{R}$-equivalent to (Q_1, Q_2) where*

$$Q_1 = a(x_0^2 - x_2^2) - 2bx_1x_3$$
$$Q_2 = a(x_1^2 - x_3^2) - b(x_0^2 + x_2)$$

and

$$a = \tfrac{1}{2}\sqrt{\frac{2\pi}{\omega_1}}\zeta_8^{-1}\theta_2(\tau)\,, \qquad b = \tfrac{1}{2}\sqrt{\frac{2\pi}{\omega_1}}\theta_3(\tau)\,.$$

Proof. Since $\mathrm{Re}(\tau) = 1/2$ it is clear from (3.12) that a and b are real. In the notation of Lemma 3.9 the quadric intersection (Q_1, Q_2) has invariants $2^8 f_4(\zeta_8 a, b)$ and $2^{12} f_6(\zeta_8 a, b)$. We compute

$$4^k f_k(\zeta_8 a, b) = (\tfrac{2\pi}{\omega_1})^k f_k(\theta_2(\tau), \theta_3(\tau)) = (\tfrac{2\pi}{\omega_1})^k E_k(\tau)\,.$$

It follows by Lemma 3.5 that (Q_1, Q_2) has the same invariants as (3.15). $\square$

The proof of Proposition 2.8 in the case $n = 4$ is completed by

LEMMA 3.12. *For $\tau \in \mathfrak{H}$ with $\mathrm{Re}(\tau) \in \{0, 1/2\}$ we have*

$$\max(|\theta_2(\tau)|, |\theta_3(\tau)|) \ll \max(|E_4(\tau)|^{1/8}, |E_6(\tau)|^{1/12}) \tag{3.16}$$

and

$$\max(|\theta_3(\tfrac{\tau}{4})|, |\theta_4(\tfrac{\tau}{4})|) \ll \max(|E_4(\tau)|^{1/8}, |E_6(\tau)|^{1/12})\,. \tag{3.17}$$

Proof. The first two equalities in (3.13) show that (3.16) is equivalent to (3.17) with τ replaced by $-1/\tau$. The second two equalities in (3.13) show that (3.16) and (3.17) are equivalent. It is clear from the definitions of θ_2 and θ_3 that we may replace τ by $\tau+1$. So if either bound holds on some subset of $\mathfrak{H}$ then both bounds hold on any $\mathrm{SL}_2(\mathbf{Z})$-translate of that subset (possibly with different implied constants).

We only need to establish the bounds for $\mathrm{Im}(\tau)$ large and $\mathrm{Im}(\tau)$ small, since the result will then follow by a compactness argument. (Note that E_4 and E_6 have no common zeros in $\mathfrak{H}$.) As $\mathrm{Im}(\tau)\to\infty$ we have $q\to 0$ and the result is clear. By the action of $\mathrm{SL}_2(\mathbf{Z})$ this implies the result for $\mathrm{Im}(\tau)$ small. □

4. Genus one models and the geometry of numbers

In this section we use the geometry of numbers to deduce Theorem 1.2 from Theorem 2.9.

4.1 Binary quartics

By Theorem 2.9 and Lemma 2.10 we have

Lemma 4.1. *Let C be an everywhere locally soluble 2-covering of an elliptic curve $E/\mathbf{Q}$. Then C can be defined by an integer coefficient binary quartic whose coefficient of $x^{4-j}z^j$ is bounded in absolute value by $A\mu_1^{4-j}\mu_2^j$ where $A\ll H_E^2$ and $\mu_1\mu_2\ll 1$.*

The binary quartic representing C is non-singular, i.e. it has no repeated roots in $\mathbf{P}^1(\overline{\mathbf{Q}})$. Under the hypothesis of Theorem 1.2(b) it has no $\mathbf{Q}$-rational root (see Remark 2.5). Since $n=2$ the bound claimed in Theorem 1.2(c) is the same as that in Theorem 1.2(b). The proof of Theorem 1.2 in the case $n=2$ is completed by

Lemma 4.2. *Let Φ be an integer coefficient binary quartic. Suppose that the coefficient of $x^{4-j}z^j$ is bounded in absolute value by $A\mu_1^{4-j}\mu_2^j$.*

(i) *If Φ has no repeated root in $\mathbf{P}^1(\mathbf{Q})$ then $\|\Phi\|_\infty\le A^3(\mu_1\mu_2)^6$.*

(ii) *If Φ has no root in $\mathbf{P}^1(\mathbf{Q})$ then $\|\Phi\|_\infty\le A^2(\mu_1\mu_2)^4$.*

Proof. Without loss of generality $\mu_1 \leq \mu_2$.

(i) If $A\mu_1^3\mu_2 < 1$ then Φ has no x^4 or x^3z terms and therefore a repeated root at $(1:0)$. By hypothesis this does not happen. Therefore $A\mu_1^3\mu_2 \geq 1$ and

$$\|\Phi\|_\infty \leq A\mu_2^4 \leq A^3(\mu_1\mu_2)^6.$$

(ii) If $A\mu_1^4 < 1$ then Φ has no x^4 term and therefore a root at $(1:0)$. By hypothesis this does not happen. Therefore $A\mu_1^4 \geq 1$ and

$$\|\Phi\|_\infty \leq A\mu_2^4 \leq A^2(\mu_1\mu_2)^4. \qquad \square$$

4.2 Ternary cubics

By Theorem 2.9 and Lemma 2.10 we have

LEMMA 4.3. *Let C be an everywhere locally soluble 3-covering of an elliptic curve $E/\mathbf{Q}$. Then C can be defined by an integer coefficient ternary whose coefficient of $x^iy^jz^k$ is bounded in absolute value by $A\mu_1^i\mu_2^j\mu_3^k$ where $A \ll H_E$ and $\mu_1\mu_2\mu_3 \ll 1$.*

The hypotheses of parts (b) and (c) of Theorem 1.2 are that C has no $\mathbf{Q}$-rational point of inflection, respectively that C has no $\mathbf{Q}$-rational point. The proof of Theorem 1.2 in the case $n = 3$ is completed by

LEMMA 4.4. *Let Φ be an integer coefficient ternary cubic defining a plane cubic curve $C \subset \mathbf{P}^2$. Suppose that the coefficient of $x^iy^jz^k$ is bounded in absolute value by $A\mu_1^i\mu_2^j\mu_3^k$.*

(i) *If C is non-singular then $\|\Phi\|_\infty \leq A^6(\mu_1\mu_2\mu_3)^6$.*

(ii) *If C is non-singular and has no $\mathbf{Q}$-rational point of inflection then $\|\Phi\|_\infty \leq A^4(\mu_1\mu_2\mu_3)^4$.*

(iii) *If C has no $\mathbf{Q}$-rational points then $\|\Phi\|_\infty \leq A^3(\mu_1\mu_2\mu_3)^3$.*

Proof. Without loss of generality $\mu_1 \leq \mu_2 \leq \mu_3$.

(i) If $A\mu_1^2\mu_3 < 1$ then Φ has no x^3, x^2y or x^2z terms and therefore C is singular at $(1:0:0)$. If $A\mu_2^3 < 1$ then Φ has no x^3, x^2y, xy^2, or y^3 terms. This would imply that C contains the line $z = 0$ and is therefore singular. Accordingly we have $A\mu_1^2\mu_3 \geq 1$ and $A\mu_2^3 \geq 1$. It follows by the identity

$$A\mu_3^3(A\mu_1^2\mu_3)^3(A\mu_2^3)^2 = A^6(\mu_1\mu_2\mu_3)^6$$

that $\|\Phi\|_\infty \leq A\mu_3^3 \leq A^6(\mu_1\mu_2\mu_3)^6$.

(ii) If $A\mu_1\mu_2^2 < 1$ then Φ has no x^3, x^2y or xy^2 terms and therefore C meets the line $z = 0$ with multiplicity at least 3. This would imply that either C is singular or that $(1 : 0 : 0)$ is a point of inflection. Accordingly we have $A\mu_1\mu_2^2 \geq 1$. Exactly as in the proof of (i) we have $A\mu_1^2\mu_3 \geq 1$. It follows by the identity

$$A\mu_3^3(A\mu_1\mu_2^2)^2A\mu_1^2\mu_3 = A^4(\mu_1\mu_2\mu_3)^4$$

that $\|\Phi\|_\infty \leq A\mu_3^3 \leq A^4(\mu_1\mu_2\mu_3)^4$.

(iii) If $A\mu_1^3 < 1$ then $(1 : 0 : 0)$ is a $\mathbf{Q}$-rational point on C. Therefore $A\mu_1^3 \geq 1$ and $\|\Phi\|_\infty \leq A\mu_3^3 \leq A^3(\mu_1\mu_2\mu_3)^3$. □

4.3 Quadric intersections

By Theorem 2.9 and Lemma 2.10 we have

Lemma 4.5. *Let C be an everywhere locally soluble 4-covering of an elliptic curve $E/\mathbf{Q}$. Then C can be defined by an integer coefficient quadric intersection (Q_1, Q_2) whose coefficient of x_jx_k in Q_i is bounded in absolute value by $A\lambda_i\mu_j\mu_k$, where $A \ll H_E^{1/2}$, $\lambda_1\lambda_2 \ll 1$ and $\mu_1\mu_2\mu_3\mu_4 \ll 1$.*

Suppose that $\operatorname{rank}(xQ_1 + zQ_2) < 4$ for some $(x : z) \in \mathbf{P}^1(\mathbf{Q})$. Then by Remark 2.5 and Lemma 2.6(ii) the element $\xi_4 \in H^1(\mathbf{Q}, E[4])$ corresponding to C satisfies $[2]_*\xi_4 = 0$. Hence $\xi_4 = \iota_*(\xi_2)$ for some $\xi_2 \in H^1(\mathbf{Q}, E[2])$. Since C is everywhere locally soluble ξ_2 has trivial obstruction, i.e. it is represented by a binary quartic. We can therefore represent C by a quadric intersection of the form specified in Lemma 2.6(i). In this case Theorem 1.2(b) follows from the result for $n = 2$. Since ξ_2 and ξ_4 have the same images in $Ш(E/\mathbf{Q})$ the hypothesis of Theorem 1.2(c) is not satisfied.

The proof of Theorem 1.2 in the case $n = 4$ is completed by

Lemma 4.6. *Let $\Phi = (Q_1, Q_2)$ be an integer coefficient quadric intersection defining a degree 4 curve $C \subset \mathbf{P}^3$. Suppose that the coefficient of x_jx_k in Q_i is bounded in absolute value by $A\lambda_i\mu_j\mu_k$.*

(i) *If C is non-singular then $\|\Phi\|_\infty \leq A^{12}(\lambda_1\lambda_2)^6(\mu_1\mu_2\mu_3\mu_4)^6$.*

(ii) *If C is non-singular and there are no $\mathbf{Q}$-rational singular quadrics in the pencil spanned by Q_1 and Q_2 then*

$$\|\Phi\|_\infty \leq A^8(\lambda_1\lambda_2)^4(\mu_1\mu_2\mu_3\mu_4)^4.$$

(iii) *If C has no $\mathbf{Q}$-rational points and there are no $\mathbf{Q}$-rational singular quadrics in the pencil spanned by Q_1 and Q_2 then*

$$\|\Phi\|_\infty \leq A^4(\lambda_1\lambda_2)^2(\mu_1\mu_2\mu_3\mu_4)^2.$$

Proof. Without loss of generality $\lambda_1 \leq \lambda_2$ and $\mu_1 \leq \mu_2 \leq \mu_3 \leq \mu_4$.

(i) We make the following observations:

- If $A\lambda_2\mu_1\mu_3 < 1$ then $(1:0:0:0)$ is a singular point on C.
- If $A\lambda_2\mu_2^2 < 1$ then C contains the line $\{x_3 = x_4 = 0\}$.
- If $A\lambda_1\mu_3^2 < 1$ then Q_1 has rank at most 2.
- If $A\lambda_1\mu_2\mu_4 < 1$ then Q_1 has rank at most 2.

We are given that C is non-singular, and so none of the above inequalities can hold. We further note that if both $A\lambda_2\mu_1^2 < 1$ and $A\lambda_1\mu_1\mu_4 < 1$ then $(1:0:0:0)$ is a singular point on C. We therefore split into the cases $A\lambda_2\mu_1^2 \geq 1$ and $A\lambda_1\mu_1\mu_4 \geq 1$. In the first case it follows by the identity

$$(A\lambda_2\mu_1^2)^2(A\lambda_2\mu_2^2)(A\lambda_1\mu_3^2)^2(A\lambda_1\mu_2\mu_4)^2(A\lambda_2\mu_4^2) = A^8(\lambda_1\lambda_2)^4(\mu_1\mu_2\mu_3\mu_4)^4$$

that $\|\Phi\|_\infty \leq A\lambda_2\mu_4^2 \leq A^8(\lambda_1\lambda_2)^4(\mu_1\mu_2\mu_3\mu_4)^4$. In the second case it follows by the identity

$$(A\lambda_2\mu_1\mu_3)^2(A\lambda_2\mu_2^2)^3(A\lambda_1\mu_3^2)^2(A\lambda_1\mu_1\mu_4)^4(A\lambda_2\mu_4^2) = A^{12}(\lambda_1\lambda_2)^6(\mu_1\mu_2\mu_3\mu_4)^6$$

that $\|\Phi\|_\infty \leq A\lambda_2\mu_4^2 \leq A^{12}(\lambda_1\lambda_2)^6(\mu_1\mu_2\mu_3\mu_4)^6$.

(ii) We replace the third and fourth observations in (i) by

- If $A\lambda_1\mu_2\mu_3 < 1$ then Q_1 has rank at most 3.
- If $A\lambda_1\mu_1\mu_4 < 1$ then Q_1 has rank at most 3.

It follows by the identity

$$(A\lambda_2\mu_1\mu_3)^2(A\lambda_2\mu_2^2)(A\lambda_1\mu_2\mu_3)^2(A\lambda_1\mu_1\mu_4)^2(A\lambda_2\mu_4^2) = A^8(\lambda_1\lambda_2)^4(\mu_1\mu_2\mu_3\mu_4)^4$$

that $\|\Phi\|_\infty \leq A\lambda_2\mu_4^2 \leq A^8(\lambda_1\lambda_2)^4(\mu_1\mu_2\mu_3\mu_4)^4$.

(iii) If $A\lambda_2\mu_1^2 < 1$ then $(1:0:0:0)$ is a $\mathbf{Q}$-rational point on C. Therefore $A\lambda_2\mu_1^2 \geq 1$. We have already seen in (ii) that $A\lambda_1\mu_2\mu_3 \geq 1$. It follows by the identity

$$(A\lambda_2\mu_1^2)(A\lambda_1\mu_2\mu_3)^2(A\lambda_2\mu_4^2) = A^4(\lambda_1\lambda_2)^2(\mu_1\mu_2\mu_3\mu_4)^2$$

that $\|\Phi\|_\infty \leq A\lambda_2\mu_4^2 \leq A^4(\lambda_1\lambda_2)^2(\mu_1\mu_2\mu_3\mu_4)^2$. □

5. A CRITERION FOR $Ш(E/\mathbf{Q})[3] = 0$

In this section we prove Theorem 1.3. We will need the following lemma whose proof is just an exercise in calculus.

LEMMA 5.1. *Let* $a, b \in \mathbf{R}$ *and put* $c = (a^2 + \sqrt{3}ab + b^2)^{1/2}$. *Let*

$$F(x, y, z) = a(x^3 + y^3 + z^3) - 3(a + \sqrt{3}b)xyz.$$

Then $|F(\mathbf{x})| \leq \max(|a|, |b|, |c|)\|\mathbf{x}\|^3$ *for all* $\mathbf{x} = (x, y, z) \in \mathbf{R}^3$.

Proof. Let (x, y, z) be a local maximum of F on the sphere $x^2+y^2+z^2 = 1$. Then we have

$$\operatorname{rank} \begin{pmatrix} F_x & F_y & F_z \\ x & y & z \end{pmatrix} \leq 1.$$

We compute

$$yF_x - xF_y = 3(x - y)(axy + (a + \sqrt{3}b)(x + y)z).$$

If x, y, z are distinct then $a + \sqrt{3}b = a$ or $-a/2$. In the first case we have $b = 0$ and $xy+yz+zx = 0$. But then $x+y+z = \pm 1$ and $F(x, y, z) = \pm a$. In the second case we have $xy = yz = zx$, and this contradicts that x, y, z are distinct.

If $x = y = z$ then $F(x, y, z) = \pm b$. So without loss of generality $x \neq y = z$. Then

$$axy + (a + \sqrt{3}b)(x + y)y = 0.$$

If $y = 0$ we get $F(x, y, z) = \pm a$. Otherwise

$$x = -(a + \sqrt{3}b)\xi$$
$$y = (2a + \sqrt{3}b)\xi$$

for some $\xi \in \mathbf{R}$. We compute

$$x^2 + y^2 + z^2 = 9\xi^2(a^2 + \tfrac{10}{9}\sqrt{3}ab + b^2)$$
$$F(x, y, z) = 27\xi^3(a^2 + \sqrt{3}ab + b^2)(a^2 + \tfrac{10}{9}\sqrt{3}ab + b^2).$$

Eliminating ξ gives

$$|F(x, y, z)| = \frac{a^2 + \sqrt{3}ab + b^2}{(a^2 + \frac{10}{9}\sqrt{3}ab + b^2)^{1/2}}.$$

If $ab \geq 0$ then $|F(x, y, z)| \leq |c|$. Otherwise if $|a| \geq |b|$ we have

$$(a^2 + \sqrt{3}ab + b^2)^2 - a^2(a^2 + \tfrac{10}{9}\sqrt{3}ab + b^2) = (\tfrac{2}{\sqrt{3}}a + b)^3 b \leq 0$$

and hence $|F(x, y, z)| \leq |a|$. The case $|b| \geq |a|$ is similar. □

Proof of Theorem 1.3. Let $E/\mathbf{Q}$ be an elliptic curve. We aim to show that (under suitable hypotheses) $Ш(E/\mathbf{Q})[3] = 0$. By (1.1) it is equivalent to show that every $\xi \in S^{(3)}(E/\mathbf{Q})$ maps to zero in $Ш(E/\mathbf{Q})$.

Let $\xi \in S^{(3)}(E/\mathbf{Q})$. Then ξ corresponds to an everywhere locally soluble 3-covering $\pi\colon C \to E$. Our aim is to show that $C(\mathbf{Q}) \neq \varnothing$. By Proposition 2.7 we know that C can be defined by an integer coefficient ternary cubic f with the same invariants as a minimal Weierstrass equation for E. We fix a minimal Weierstrass equation for E and let $\tau = \omega_2/\omega_1 \in \mathfrak{H}$ be as in Lemma 3.7. Then $f = F \circ g$ for some $g \in \mathrm{SL}_3(\mathbf{R})$ where

$$F(x,y,z) = a(x^3 + y^3 + z^3) - 3(a + \sqrt{3}b)xyz$$

and

$$a = \frac{1}{\sqrt{27}}\left(\frac{2\pi}{\omega_1}\right)\frac{\eta(\tau/3)^3}{\eta(\tau)}, \qquad b = \left(\frac{2\pi}{\omega_1}\right)\frac{\eta(3\tau)^3}{\eta(\tau)}.$$

Let $\gamma = a + i\zeta_3^2 b$ and $c = |\gamma| = (a^2 + \sqrt{3}ab + b^2)^{1/2}$. The lattice $\Lambda = g(\mathbf{Z}^3) \subset \mathbf{R}^3$ has covolume 1. Hence by Lemma 2.10 there exists $0 \neq \mathbf{x} \in \Lambda$ with $\|\mathbf{x}\|^3 \leq \sqrt{2}$. If $\max(|a|,|b|,|c|) < 1/\sqrt{2}$ then by Lemma 5.1 we have

$$|F(\mathbf{x})| \leq \max(|a|,|b|,|c|)\,\|\mathbf{x}\|^3 < 1.$$

Since $F(\mathbf{x}) = f(u,v,w)$ for some $u,v,w \in \mathbf{Z}$ it follows that $F(\mathbf{x}) = 0$. Hence $C(\mathbf{Q}) \neq \varnothing$ and ξ maps to zero in $Ш(E/\mathbf{Q})$.

It remains to show that the condition $\max(|a|,|b|,|c|) < 1/\sqrt{2}$ is equivalent to the hypothesis of the theorem. By (3.9) we have

$$\gamma = \frac{1}{\sqrt{27}}\left(\frac{2\pi}{\omega_1}\right)\frac{\eta(\frac{\tau+1}{3})^3}{\eta(\tau+1)}, \qquad \overline{\gamma} = \frac{1}{\sqrt{27}}\left(\frac{2\pi}{\omega_1}\right)\frac{\eta(\frac{\tau-1}{3})^3}{\eta(\tau-1)}.$$

We now put

$$\alpha_1(\tau) = -\eta(\tfrac{\tau}{3})^{12} \qquad \alpha_3(\tau) = \eta(\tfrac{\tau+1}{3})^{12}$$
$$\alpha_2(\tau) = -3^6\eta(3\tau)^{12} \qquad \alpha_4(\tau) = \eta(\tfrac{\tau-1}{3})^{12}$$

and claim that

$$\prod_{i=1}^{4}(X - \alpha_i(\tau)) = (X - 3^3\eta(\tau)^{12})(X - 3\eta(\tau)^{12})^3 + E_4(\tau)^3\eta(\tau)^{12}X. \tag{5.1}$$

It is routine to check using (3.3) and (3.4) that

$$\alpha_1(\tau+1) = -\alpha_3(\tau) \qquad \alpha_1(-1/\tau) = -\tau^6\alpha_2(\tau)$$
$$\alpha_2(\tau+1) = -\alpha_2(\tau) \qquad \alpha_2(-1/\tau) = -\tau^6\alpha_1(\tau)$$
$$\alpha_3(\tau+1) = -\alpha_4(\tau) \qquad \alpha_3(-1/\tau) = -\tau^6\alpha_4(\tau)$$
$$\alpha_4(\tau+1) = -\alpha_1(\tau) \qquad \alpha_4(-1/\tau) = -\tau^6\alpha_3(\tau).$$

Hence the square of each coefficient of the left hand side of (5.1) is a modular form of level 1. The claim is then proved by comparing the first few coefficients of the q-expansions. By Lemma 3.5 we have $\Delta_E = (\frac{2\pi}{\omega_1})^{12}\Delta(\tau)$ and $j = E_4(\tau)^3/\Delta(\tau)$. Finally we compute

$$\begin{aligned}
&\max(|a|,|b|,|c|) < \tfrac{1}{\sqrt{2}} \\
&\quad\iff \tfrac{1}{\sqrt{27}}(\tfrac{2\pi}{\omega_1}) \max\left(|\eta(\tfrac{\tau}{3})|^3, \sqrt{27}|\eta(3\tau)|^3, |\eta(\tfrac{\tau+1}{3})|^3\right) < \tfrac{1}{\sqrt{2}}|\eta(\tau)| \\
&\quad\iff 2^6|\Delta_E| \max\{|x|^3 : x \text{ a root of } (5.1)\} < 3^{18}|\eta(\tau)|^{36} \\
&\quad\iff 2^6|\Delta_E| \max\{|x|^3 : x \text{ a root of } (X-3^3)(X-3)^3 + jX = 0\} < 3^{18} \\
&\quad\iff 2^6|\Delta_E| < \min\{|x|^3 : x \text{ a root of } (X-3^3)(X-3^5)^3 + jX^3 = 0\}\,.
\end{aligned}$$

This final condition is the hypothesis of the theorem. □

REFERENCES

[AKM] AN, S.Y., 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), 304–315.

[BSD] BIRCH, B.J. and H.P.F. SWINNERTON-DYER. Notes on elliptic curves. I. *J. Reine Angew. Math. 212* (1963), 7–25.

[C] CREMONA, J.E. *Algorithms for Modular Elliptic Curves*. Second edition. Cambridge University Press, Cambridge, 1997. See also the on-line tables at http://www.warwick.ac.uk/staff/J.E.Cremona/ftp/data/

[CFO] CREMONA, J.E., 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; II. Geometry. *J. Reine Angew. Math. 632* (2009), 63–84; III. Algorithms. Preprint arXiv: 1107.3516v1 (2011).

[CFS] CREMONA, J.E., T.A. FISHER and M. STOLL. Minimisation and reduction of 2-, 3- and 4-coverings of elliptic curves. *Algebra Number Theory 4* (2010), 763–820.

[DSS] DJABRI, Z., E.F. SCHAEFER and N.P. SMART. Computing the p-Selmer group of an elliptic curve. *Trans. Amer. Math. Soc. 352* (2000), 5583–5597.

[DS] DJABRI, Z. and N.P. SMART. A comparison of direct and indirect methods for computing Selmer groups of an elliptic curve. In: *Algorithmic Number Theory* (Portland, OR, 1998), 502–513. Lecture Notes in Comput. Sci. *1423*. Springer, Berlin, 1998.

[F1] FISHER, T.A. The Cassels-Tate pairing and the Platonic solids. *J. Number Theory 98* (2003), 105–155.

[F2] —— Testing equivalence of ternary cubics. In: *Algorithmic Number Theory*, 333–345. Lecture Notes in Comput. Sci. *4076*. Springer, Berlin, 2006.

[F3] —— The invariants of a genus one curve. *Proc. Lond. Math. Soc. (3) 97* (2008), 753–782.

[MSS] MERRIMAN, J.R., S. SIKSEK and N.P. SMART. Explicit 4-descents on an elliptic curve. *Acta Arith. 77* (1996), 385–404.

[O] O'NEIL, C. The period-index obstruction for elliptic curves. *J. Number Theory 95* (2002), 329–339.

[PZ] POHST, M. and H. ZASSENHAUS. *Algorithmic Algebraic Number Theory*. Encyclopedia of Mathematics and its Applications *30*. Cambridge University Press, Cambridge, 1989.

[SS] SCHAEFER, E.F. and M. STOLL. How to do a p-descent on an elliptic curve. *Trans. Amer. Math. Soc. 356* (2004), 1209–1231.

[S] STAMMINGER, S. Explicit 8-descent on elliptic curves. Ph.D. thesis, International University Bremen, 2005.

[We] WEIL, A. *Number Theory*. An approach through history from Hammurapi to Legendre. Birkhäuser Boston, Inc., Boston, MA, 1984.

[Wo] WOMACK, T.O. Explicit descent on elliptic curves. Ph.D. thesis, University of Nottingham, 2003.

[Z] ZARHIN, JU.G. Noncommutative cohomology and Mumford groups. *Mat. Zametki 15* (1974), 415–419; English translation: *Math. Notes 15* (1974), 241–244.

(Reçu le 26 octobre 2010)

Tom Fisher

Department of Pure Mathematics and Mathematical Statistics
Centre for Mathematical Sciences
Wilberforce Road
Cambridge CB3 0WB
United Kingdom
e-mail: T.A.Fisher@dpmms.cam.ac.uk