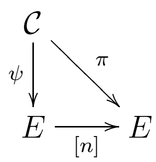
LOCAL SOLUBILITY AND HEIGHT BOUNDS FOR COVERINGS OF ELLIPTIC CURVES

T.A. FISHER AND G.F. SILLS

Abstract. We study genus one curves that arise as 2-, 3- and 4-coverings of elliptic curves. We describe efficient algorithms for testing local solubility and modify the classical formulae for the covering maps so that they work in all characteristics. These ingredients are then combined to give explicit bounds relating the height of a rational point on one of the covering curves to the height of its image on the elliptic curve. We use our results to improve the existing methods for searching for rational points on elliptic curves.

1. Introduction

Let E be an elliptic curve over a number field K. An n-covering of E is smooth curve of genus one $\mathcal{C}$ together with a morphism $\pi : \mathcal{C} \to E$, with $\mathcal{C}$ and π both defined over K, such that the diagram



commutes for some isomorphism $\psi : \mathcal{C} \cong E$ defined over $\overline{K}$. An n-descent calculation computes equations for the everywhere locally soluble n-coverings of E. Finding rational points on these n-coverings can assist in computing generators for the Mordell-Weil group $E(K)$. Indeed if $\mathcal{C}(K)$ is non-empty then $\pi(\mathcal{C}(K))$ is a coset of $nE(K)$ in $E(K)$.

Suppose that $\mathcal{C}$ is everywhere locally soluble, i.e. $\mathcal{C}(K_v) \neq \emptyset$ for all places v of K. By [Ca, Proof of Theorem 1.3] there exists a K-rational divisor D on $\mathcal{C}$ with $D \sim \psi^*(n.\mathcal{O})$, where $\mathcal{O}$ is the identity on E. The complete linear system $|D|$ defines a morphism $\mathcal{C} \to \mathbb{P}^{n-1}$. If $n = 2$ then $\mathcal{C} \to \mathbb{P}^1$ is a double cover ramified at 4 points. If $n \geq 3$ then $\mathcal{C} \subset \mathbb{P}^{n-1}$ is a genus one normal curve of degree n. The map $\pi : \mathcal{C} \to E$ may be recovered as $P \mapsto [nP - D] \in \mathrm{Pic}^0(\mathcal{C}) = E$ where D is now the hyperplane section on $\mathcal{C}$. In the cases $n = 2, 3, 4$ equations for $\mathcal{C}$ take the form of a binary quartic, ternary cubic or quadric intersection. The Jacobian elliptic

Date: 12th October 2010.

curve E and covering map π are then given by formulae from classical invariant theory as surveyed in [AKM^{3}P].

It is expected that points on $\mathcal{C}(K)$ will be smaller (and hence easier to find) than their images in $E(K)$. This statement is made precise using the theory of heights. Let h be the logarithmic height on $\mathcal{C}$ relative to the hyperplane section D, and h_E the x-coordinate logarithmic height on E. Then as pointed out in [Sto] there exist constants B_1 and B_2 such that

$$B_1 \le h(P) - \frac{1}{2n} h_E(\pi P) \le B_2 \tag{1.1}$$

for all $P \in \mathcal{C}(K)$. To prove this one first notes that since $n^2.\mathcal{O} \sim [n]^*\mathcal{O}$ we have $2nD \sim \pi^*(2.\mathcal{O})$. The existence of bounds B_1 and B_2 then follows by standard results about heights; see for example [HS, Theorem B.3.2].

We restrict to $n = 2, 3$ or 4. In these cases n-descent has been implemented in the computer algebra system Magma [BCP] at least over $K = \mathbb{Q}$. The algorithms for 3-descent are described in [SS], [CFOSS] and those for 4-descent in [MSS], [W]. In Sections 2, 3 and 4 we

- describe algorithms for testing whether $\mathcal{C}(K_v) \neq \emptyset$,
- modify the formulae for the covering map $\pi : \mathcal{C} \to E$ so that they work in all characteristics, and
- compute explicit bounds B_1 and B_2 in (1.1).

Recent work on higher descents and on computing the Cassels-Tate pairing (see [Cre], [Don], [F4], [Sta]) relies on being able to efficiently compute local points. This prompted us to improve the local solubility tests currently implemented in Magma. The material in Section 2 should however contain few surprises for experts. The main reason for including it here is as a preliminary to our work on height bounds. The latter is also the motivation for the formulae in Section 3, although these too may be of independent interest.

It is possible to compute bounds B_1 and B_2 in (1.1) using elimination theory. However this method gives rather poor results. Instead we compute our bounds as sums of local contributions. This generalises work of Siksek [Si2] who considered the case where π is multiplication-by-2 on E. As he observes it is worth putting some effort into obtaining good bounds, as this can significantly reduce the size of the region we end up searching. We give some examples in Section 5.

The bounds B_1 and B_2 depend on our choice of equations for $\mathcal{C}$ and E. Let us take $K = \mathbb{Q}$. For E we take the global minimal Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1.2}$$

with $a_1, a_3 \in \{0, 1\}$ and $a_2 \in \{0, \pm 1\}$. For $\mathcal{C}$ we take an equation that is minimised and reduced as described in [CFS]. Roughly speaking one expects that minimising improves the bounds at the finite places, and reducing improves the bounds at the infinite places. However there can be more than one choice of minimisation. We find that the bounds can vary significantly between these choices. In Section 5 we include an example where these ideas allow us to improve the search for rational points on $\mathcal{C}$ (and hence on E).

1.1. **Genus one models.** The following notation is recalled from [CFS], [F1]. We call the equations defining an n-covering (where $n = 2, 3$ or 4) a *genus one model*. More precisely we make the following definition.

Definition 1.1. Let R be any ring.

(i) A *genus one model of degree* 2 over R is a generalised binary quartic
$$y^2 + P(x_1, x_2)y = Q(x_1, x_2),$$
sometimes abbreviated (P, Q), where P and Q are homogeneous forms of degree 2 and 4 with coefficients in R. A transformation of genus one models is given by $y \leftarrow \mu^{-1}y + r_0x_1^2 + r_1x_1x_2 + r_2x_2^2$ for some $\mu \in R^\times$ and $r = (r_0, r_1, r_2) \in R^3$, followed by $x_j \leftarrow \sum n_{ij}x_i$ for some $N = (n_{ij}) \in \mathrm{GL}_2(R)$. We write $\mathcal{G}_2(R)$ for the group of all such transformations $g = [\mu, r, N]$ and define $\det g = \mu \det N$.

(ii) A *genus one model of degree* 3 over R is a ternary cubic $U \in R[x_1, x_2, x_3]$. A transformation of genus one models is given by multiplying the cubic through by $\mu \in R^\times$, followed by $x_j \leftarrow \sum n_{ij}x_i$ for some $N = (n_{ij}) \in \mathrm{GL}_3(R)$. We write $\mathcal{G}_3(R)$ for the group of all such transformations $g = [\mu, N]$ and define $\det g = \mu \det N$.

(iii) A *genus one model of degree* 4 over R is a quadric intersection, i.e. a pair of homogeneous polynomials $Q_1, Q_2 \in R[x_1, \ldots, x_4]$ of degree 2. A transformation of quadric intersections is given by $Q_i \leftarrow \sum m_{ij}Q_j$ for some $M = (m_{ij}) \in \mathrm{GL}_2(R)$ and $x_j \leftarrow \sum n_{ij}x_i$ for some $N = (n_{ij}) \in \mathrm{GL}_4(R)$. We write $\mathcal{G}_4(R)$ for the group of all such transformations $g = [M, N]$ and define $\det g = \det M \det N$.

We say that genus one models are *R-equivalent* if they are in the same orbit for the action of $\mathcal{G}_n(R)$. Notice that by our conventions the action of $\mathcal{G}_n(R)$ on the space of genus one models is a left action.

An invariant of weight k is a polynomial F in the coefficients of a genus one model such that $F \circ g = (\det g)^k F$ for all $g \in \mathcal{G}_n$. Let c_4, c_6 and $\Delta = (c_4^3 - c_6^2)/1728$ be the classical invariants of weights 4, 6 and 12. We fix the scaling of these invariants as described in [CFS], [F1], i.e so that the models $y^2 + x_1x_2y = 0$, $x_1x_2x_3 = 0$ and $x_1x_2 = x_3x_4 = 0$ have invariants $c_4 = 1$ and $c_6 = -1$. For example the binary quartic $y^2 = ax^4 + bx^3z + cx^2z^2 + dxz^3 + ez^4$ has invariants
$$\begin{aligned} c_4 &= 2^4(12ae - 3bd + c^2) \\ c_6 &= 2^5(72ace - 27ad^2 - 27b^2e + 9bcd - 2c^3). \end{aligned}$$

A genus one model Φ over a field K is *non-singular* if the variety $\mathcal{C}_\Phi$ it defines is a smooth curve of genus one, and K-*soluble* if $\mathcal{C}_\Phi(K) \neq \emptyset$. It is shown in [F1] that Φ is non-singular if and only if $\Delta(\Phi) \neq 0$. Moreover if $\mathrm{char}(K) \neq 2, 3$ then (by an observation originally due to Weil in the cases $n = 2, 3$) the Jacobian elliptic curve $E = \mathrm{Jac}(\mathcal{C}_\Phi)$ has Weierstrass equation

$$y^2 = x^3 - 27c_4(\Phi)x - 54c_6(\Phi). \tag{1.3}$$

Functions for computing with genus one models, their transformations and invariants have been contributed to Magma [BCP] by the first author.

2. Testing for local solubility

Let K be a finite extension of $\mathbb{Q}_p$ with ring of integers $\mathcal{O}_K$, maximal ideal $\pi\mathcal{O}_K$, residue field k and normalised discrete valuation $v : K^\times \to \mathbb{Z}$. Reduction mod π will be denoted $x \mapsto \widetilde{x}$. If f is a polynomial with coefficients in K then we write $v(f)$ for the minimum valuation of a coefficient.

Let Φ be a non-singular genus one model over K of degree $n \in \{2, 3, 4\}$. In this section we give algorithms for deciding whether Φ is K-soluble. Our algorithm in the case $n = 2$ is essentially the same as that in [BSD], [Bru], [Cr], [MSS] and is included only for completeness. The cases $n = 3, 4$ can also be handled by the general method for complete intersections described in [Bru]. However this general method involves looping over all k-points on the reduction, and is therefore inefficient when k is large. We overcome this problem by making use of the geometry of singular genus one models. We have contributed our algorithms (over $K = \mathbb{Q}_p$) to Magma [BCP], and from the next release (Version 2.17) they will be called by default when equations of the relevant form are passed to `IsLocallySoluble`.

The basic algorithms are listed in Section 2.1. They depend on methods for deciding whether there are any smooth k-points on the reduction (see Section 2.2) and for finding all non-regular k-points (see Section 2.3). It is clear by Hensel's lemma that when an answer is returned then that answer is correct. If the algorithms failed to terminate then from the resulting infinite sequence of transformation we could construct a singular point on the original curve. Thus our assumption that Φ is non-singular ensures that the algorithms terminate. We omit the details since we give an alternative proof in Section 4.4.

In practice we first replace Φ by a *minimal model*, i.e. a K-equivalent model over $\mathcal{O}_K$ with $v(\Delta(\Phi))$ minimal. Algorithms for doing this are described in [CFS]. Let $E = \mathrm{Jac}(\mathcal{C}_\Phi)$ be the Jacobian elliptic curve and Δ_E its minimal discriminant. Then $v(\Delta(\Phi)) = v(\Delta_E) + 12\ell$ where ℓ is a non-negative integer called the *level* of Φ. Notice that applying a transformation $g \in \mathcal{G}_n(K)$ changes the level by $v(\det g)$. In [CFS] it is shown that the minimal level is 0 if and only if $\mathcal{C}_\Phi(K^{\mathrm{nr}}) \neq \emptyset$ where K^{nr} is the maximal unramified extension of K. Therefore our local solubility tests are only needed for models of level 0. This extra hypothesis will be useful in Section 2.3.

We mention as an aside that if the Tamagawa number $c(E)$ is coprime to n then a further simplification is possible. Indeed by the following lemma we have $\mathcal{C}_\Phi(K) \neq \emptyset$ if and only if $\mathcal{C}_\Phi(K^{\mathrm{nr}}) \neq \emptyset$, and so the algorithms in [CFS] already give a test for local solubility.

Lemma 2.1. *The restriction map $H^1(K, E) \to H^1(K^{\mathrm{nr}}, E)$ has kernel of order $c(E)$.*

Proof: By [M, Proposition 3.8] and the inflation-restriction exact sequence the kernel is isomorphic to $H^1(k, \Phi_E)$ where Φ_E is the component group of the Néron model of E. Since Φ_E is finite and $c(E) = \#\Phi_E(k)$ the result follows by the exact sequence

$$0 \longrightarrow H^0(k, \Phi_E) \longrightarrow \Phi_E \stackrel{1-\mathrm{Frob}}{\longrightarrow} \Phi_E \longrightarrow H^1(k, \Phi_E) \longrightarrow 0.$$

□

2.1. **Algorithms.** Let Φ be a non-singular genus one model over K of degree $n \in \{2, 3, 4\}$. Our algorithms for deciding whether $\mathcal{C}_\Phi(K) \neq \emptyset$ start by making two simplifications. First by clearing denominators we may assume that Φ is defined over $\mathcal{O}_K$. Then by calling the algorithm n times (with the co-ordinates permuted) it suffices to look for points on a standard affine piece with co-ordinates in $\mathcal{O}_K$. We remark that if $\mathrm{char}(k) \neq 2$ then the first algorithm simplifies in the obvious way by completing the square.

Algorithm 2.2. `IsLocallySoluble(h,g)`
`INPUT:` Polynomials $h(x), g(x) \in \mathcal{O}_K[x]$ with $\deg(h) \leq 2$ and $\deg(g) \leq 4$.
`OUTPUT: TRUE/FALSE` (solubility of $y^2 + h(x)y = g(x)$ for $x, y \in \mathcal{O}_K$)

(i) Make a substitution $y \leftarrow y + r_0x^2 + r_1x + r_2$ (with $r_i \in \mathcal{O}_K$) so that if possible $v(h) \geq 1$ and $v(g) \geq 1$. If now $v(h) \geq 1$ and $v(g) \geq 2$ then replace h and g by $\pi^{-1}h$ and $\pi^{-2}g$ and repeat Step (i).

(ii) Consider the affine curve
$$\Gamma = \{y^2 + \widetilde{h}(x)y = \widetilde{g}(x)\} \subset \mathbb{A}^2_k.$$
If there are smooth k-points on Γ then return `TRUE`.

(iii) Find all non-regular k-points on Γ. These are the singular points $(\widetilde{u}, \widetilde{v})$ on Γ with the property that for some (and hence all) lifts $u, v \in \mathcal{O}_K$ of $\widetilde{u}, \widetilde{v} \in k$ we have $v^2 + h(u)v \equiv g(u) \pmod{\pi^2}$.

(iv) For each non-regular k-point $(\widetilde{u}, \widetilde{v})$ on Γ lift $\widetilde{u} \in k$ to $u \in \mathcal{O}_K$ and put $h_1(x) = h(u + \pi x)$, $g_1(x) = g(u + \pi x)$. If `IsLocallySoluble(h1,g1)` then return `TRUE`.

(v) Return `FALSE`.

Algorithm 2.3. `IsLocallySoluble(g)`
`INPUT:` A polynomial $g(x,y) \in \mathcal{O}_K[x,y]$ of total degree ≤ 3.
`OUTPUT: TRUE/FALSE` (solubility of $g(x,y) = 0$ for $x, y \in \mathcal{O}_K$)

(i) Divide g by $\pi^{v(g)}$ so that now $v(g) = 0$.
(ii) Consider the affine curve
$$\Gamma = \{\widetilde{g}(x,y) = 0\} \subset \mathbb{A}^2_k.$$
If there are smooth k-points on Γ then return `TRUE`.
(iii) Find all non-regular k-points on Γ. These are the singular points $(\widetilde{u}, \widetilde{v})$ on Γ with the property that for some (and hence all) lifts $u, v \in \mathcal{O}_K$ of $\widetilde{u}, \widetilde{v} \in k$ we have $g(u,v) \equiv 0 \pmod{\pi^2}$.
(iv) For each non-regular k-point $(\widetilde{u}, \widetilde{v})$ on Γ lift $\widetilde{u}, \widetilde{v} \in k$ to $u, v \in \mathcal{O}_K$ and put $g_1(x,y) = g(u + \pi x, v + \pi y)$. If `IsLocallySoluble(g1)` then return `TRUE`.
(v) Return `FALSE`.

Algorithm 2.4. `IsLocallySoluble(g1,g2)`
`INPUT:` Polynomials $g_1, g_2 \in \mathcal{O}_K[x,y,z]$ of total degree ≤ 2.
`OUTPUT: TRUE/FALSE` (solubility of $g_1(x,y,z) = g_2(x,y,z) = 0$ for $x, y, z \in \mathcal{O}_K$)

(i) Replace g_1 and g_2 by linear combinations so that $\widetilde{g}_1$ and $\widetilde{g}_2$ are linearly independent over k. If $\widetilde{g}_1$ and $\widetilde{g}_2$ have a common linear factor then make a change of coordinates so that this factor is x. Then replace $g_i(x,y,z)$ by $\pi^{-1} g_i(\pi x, y, z)$ for $i = 1, 2$ and repeat Step (i).
(ii) Consider the affine curve
$$\Gamma = \{\widetilde{g}_1(x,y,z) = \widetilde{g}_2(x,y,z) = 0\} \subset \mathbb{A}^3_k.$$
If there are smooth k-points on Γ then return `TRUE`.
(iii) Find all non-regular k-points on Γ. These are the points $(\widetilde{u}, \widetilde{v}, \widetilde{w})$ on Γ that are singular on $\{\widetilde{g} = 0\}$ for some $g = \lambda g_1 + \mu g_2$ (where $\lambda, \mu \in \mathcal{O}_K$ not both divisible by π) with the property that for some (and hence all) lifts $u, v, w \in \mathcal{O}_K$ of $\widetilde{u}, \widetilde{v}, \widetilde{w} \in k$ we have $g(u,v,w) \equiv 0 \pmod{\pi^2}$.
(iv) For each non-regular k-point $(\widetilde{u}, \widetilde{v}, \widetilde{w})$ on Γ lift $\widetilde{u}, \widetilde{v}, \widetilde{w} \in k$ to $u, v, w \in \mathcal{O}_K$ and put
$$h_i(x,y,z) = g_i(u + \pi x, v + \pi y, w + \pi z)$$
for $i = 1, 2$. If `IsLocallySoluble(h1,h2)` then return `TRUE`.
(v) Return `FALSE`.

Remark 2.5. The algorithms may be adapted to return a certificate in the case Φ is locally soluble. This certificate takes the form of a transformation of genus one models g such that $g\Phi$ has smooth k-points on its reduction. A smooth k-point on the reduction is easily found (e.g. by intersecting with random hyperplanes). We may then use Hensel's lemma to compute a local point to any desired precision. This is the second returned argument of Magma's `IsLocallySoluble`.

2.2. **Testing for smooth points.** We show how to decide whether a genus one model defined over a finite field k has any smooth k-points. For small k there is no difficulty in looping over all k-points and testing to see which if any are smooth. For larger k this can be rather inefficient.

First we recall the classification of singular genus one models over an algebraically closed field $\mathbb{K}$. Notice that we are only interested in models that define a curve.

Lemma 2.6. *The* $\mathrm{GL}_2(\mathbb{K})$*-orbits of singular binary quartics have the following representatives.*

	binary quartic	*geometric description*
A_1	$y^2 = x^3z + x^2z^2$	*a rational nodal curve*
A_2	$y^2 = x^2z^2$	*two rational curves*
B_1	$y^2 = x^3z$	*a rational cuspidal curve*
B_2	$y^2 = x^4$	*two rational curves*
D	$y^2 = 0$	*a double line*

Proof: These cases correspond to the number and multiplicity of the repeated roots of the binary quartic. □

Lemma 2.7. *Assume char*$(\mathbb{K}) \neq 3$*. Then the* $\mathrm{GL}_3(\mathbb{K})$*-orbits of non-zero singular ternary cubics have the following representatives.*

	ternary cubic	*geometric description*
A_1	$xyz - y^3 - z^3$	*a rational nodal cubic*
A_2	$xyz - y^3$	*a conic and a line*
A_3	xyz	*three lines*
B_1	$y^2z - x^3$	*a rational cuspidal cubic*
B_2	$x^2y - y^2z$	*a conic and a line*
B_3	$x^2y - xy^2$	*three lines*
C	x^2y	*a line and a double line*
D	x^3	*a triple line*

Proof: This is standard. See for example [Dol, Section 10.3]. □

Lemma 2.8. *Assume char*$(\mathbb{K}) \neq 2$. *Then the* $\mathrm{GL}_2(\mathbb{K}) \times \mathrm{GL}_4(\mathbb{K})$*-orbits of quadric intersections* (Q_1, Q_2)*, with* Q_1 *and* Q_2 *coprime, have the following representatives. (The final column relates to Lemma 2.13 below.)*

	quadric intersection	*geometric description*	*Segre symbol*	m
A_1	$x_1x_3 - x_2^2 - x_4^2,\ x_2x_4 - x_3^2$	*a rational nodal quartic*	[112]	0
A_2	$x_1x_3 - x_2^2,\ x_2x_4 - x_3^2$	*a twisted cubic and a line*	[22]	0
A_3	$x_1x_4 - x_2^2 - x_3^2,\ x_2x_3$	*two conics*	[11(11)]	1
A_4	$x_1x_3 - x_2^2,\ x_2x_4$	*a conic and two lines*	[2(11)]	1
A_5	$x_1x_3,\ x_2x_4$	*four lines*	[(11)(11)]	2
B_1	$x_1x_4 - x_2^2,\ x_2x_4 - x_3^2$	*a rational cuspidal quartic*	[13]	0
B_2	$x_1x_4 - x_2x_3,\ x_2x_4 - x_3^2$	*a twisted cubic and a line*	[4]	0
B_3	$x_1x_3 + x_1x_4 - x_2^2,\ x_3x_4$	*two conics*	[1(21)]	1
B_4	$x_1x_3 - x_2^2 + x_2x_4,\ x_3x_4$	*a conic and two lines*	[(31)]	1
B_5	$x_2x_3 - x_3x_4,\ x_2x_4 - x_3x_4$	*four lines*	[111]	3
C_1	$x_2x_3 - x_3x_4,\ x_2x_4 - x_3x_4$	*a conic and a double line*	[1{3}]	1
C_2	$x_1x_3 + x_2x_4,\ x_1x_4$	*two lines and a double line*	[(22)]	1
C_3	$x_2x_3 - x_2x_4,\ x_3x_4$	*two lines and a double line*	[12]	2
C_4	$x_2x_3 - x_4^2,\ x_3x_4$	*a line and a triple line*	[3]	1
D_1	$x_1^2 - x_2x_3,\ x_4^2$	*a double conic*	[1(111)]	$-$
D_2	$x_1x_4 + x_2x_3,\ x_4^2$	*two double lines*	[(211)]	$-$
D_3	$x_2x_3,\ x_4^2$	*two double lines*	[1(11)]	$-$
D_4	$x_2x_4 - x_3^2,\ x_4^2$	*a quadruple line*	[(21)]	$-$
D_5	$x_3^2,\ x_4^2$	*a quadruple line*	[11]	$-$

Proof: The classification (at least over $\mathbb{K} = \mathbb{C}$) is due to Segre. See for example [Bro], [DLLP], [HP]. □

Remark 2.9. The restrictions on the characteristic of $\mathbb{K}$ in Lemmas 2.7 and 2.8 are necessary. For example if $\mathrm{char}(\mathbb{K}) = 3$ then the cuspidal cubics $y^2z = x^3 + \lambda x^2 y$ are inequivalent for $\lambda = 0$ and $\lambda \neq 0$. Likewise if $\mathrm{char}(\mathbb{K}) = 2$ then the cuspidal quadric intersections $x_1x_4 + \lambda x_2x_3 - x_2^2 = x_2x_4 - x_3^2 = 0$ are inequivalent for $\lambda = 0$ and $\lambda \neq 0$.

Figures 1, 2 and 3 illustrate the classifications in Lemmas 2.6, 2.7 and 2.8.

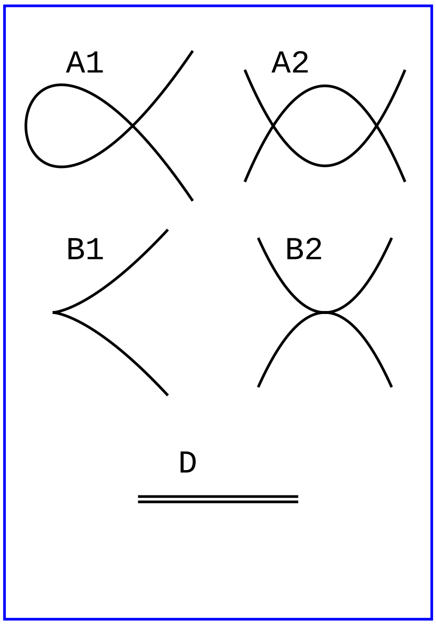


Figure 1

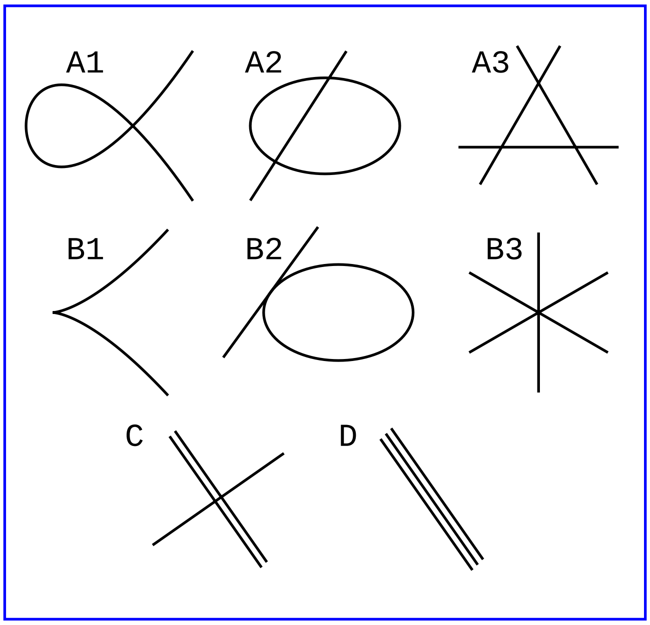


Figure 2

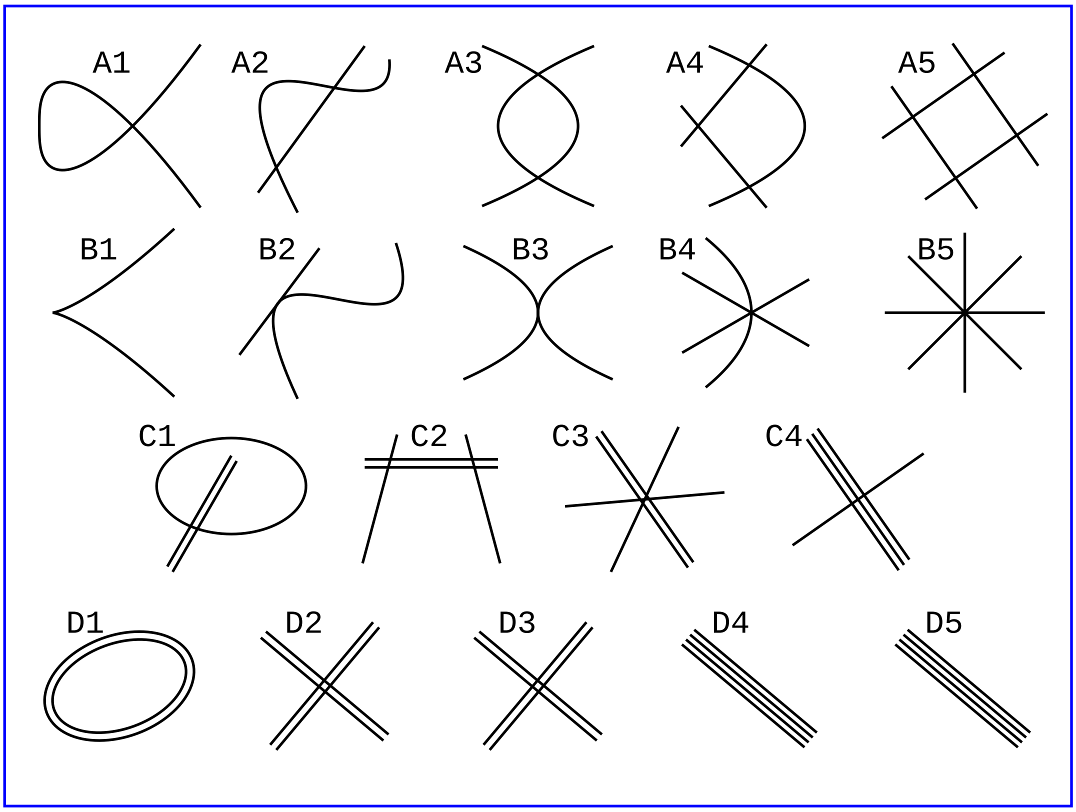


Figure 3

Let Φ be a genus one model over a finite field k. To decide whether there are any smooth k-points on $\mathcal{C}_\Phi$ we employ the following lemmas.

Remark 2.10. The algorithms in Section 2.1 in fact ask whether there are any smooth k-points on some affine piece Γ of $\mathcal{C}_\Phi$. It can happen that all the smooth k-points lie on the hyperplane at infinity, either because k is small or because all relevant components are contained in that hyperplane. In terms of our original task of deciding K-solubility this simply means that we find a point sooner than expected.

In the case $n = 2$ we assume $\mathrm{char}(k) \neq 2$. In particular we may complete the square so that our models are given by binary quartics.

Lemma 2.11. *Assume* $\mathrm{char}(k) \neq 2$ *and let* $F \in k[x, z]$ *be a binary quartic.*

(i) *If* F *is identically zero then* $\mathcal{C}_F$ *has no smooth* k*-points.*
(ii) *If* F *is non-zero, but factors as* $F(x, z) = \alpha G(x, z)^2$*, then* $\mathcal{C}_F$ *has a smooth* k*-point if and only if* $\alpha \in (k^\times)^2$*.*
(iii) *In all other cases* $\mathcal{C}_F$ *has a smooth* k*-point.*

Proof: This is clear by Lemma 2.6. □

We write $\overline{k}$ for the algebraic closure of k.

Lemma 2.12. *Let* $U \in k[x, y, z]$ *be a non-zero ternary cubic.*

(i) *If* U *factors over* $\overline{k}$ *as a product of linear forms then* $\mathcal{C}_U$ *has a smooth* k*-point if and only if one of these linear forms is defined over* k *and is not a repeated factor.*
(ii) *In all other cases* $\mathcal{C}_U$ *has a smooth* k*-point.*

Proof: This is clear by Lemma 2.7. □

Now let $\Phi = (Q_1, Q_2)$ be a model of degree 4. It is clear that if there is a rank 1 quadric in the pencil

$$\{\lambda Q_1 + \mu Q_2 \mid (\lambda : \mu) \in \mathbb{P}^1(\overline{k})\} \tag{2.1}$$

then $\mathcal{C}_\Phi$ has no smooth k-points.

Lemma 2.13. *Assume* $\mathrm{char}(k) \neq 2$ *and let* $\Phi = (Q_1, Q_2)$ *be a quadric intersection over* k *with* Q_1 *and* Q_2 *coprime. Suppose the pencil (2.1) over* $\overline{k}$ *contains no rank* 1 *quadrics and exactly* m *rank* 2 *quadrics.*

(i) *If* $m = 0$ *then* $\mathcal{C}_\Phi$ *has a smooth* k*-point.*
(ii) *If* $m = 1$ *then* $\mathcal{C}_\Phi$ *has a smooth* k*-point if and only if the rank* 2 *quadric in the pencil factors over* k*.*
(iii) *If* $m \geq 2$ *then* $\mathcal{C}_\Phi$ *is (set-theoretically) a union of lines.*

PROOF: This follows from the classification in Lemma 2.8. (The integer m is recorded in the statement of the lemma. It is replaced by a dash in cases where there is a rank 1 quadric.) □

It remains to test for smooth k-points in the case $\mathcal{C}_\Phi$ is a union of lines. Let A and B be the 4 by 4 symmetric matrices corresponding to Q_1 and Q_2. Let M be the generic 4 by 4 skew-symmetric matrix. The *Fano scheme* is the subscheme of $\mathbb{P}^5$ defined by the vanishing of the Pfaffian of M and all entries of the matrices MAM and MBM. The points of the Fano scheme correspond to the lines on the quadric intersection. In particular the Fano scheme is zero-dimensional.

Lemma 2.14. *Assume* $\text{char}(k) \neq 2$ *and let* Φ *be a quadric intersection such that* $\mathcal{C}_\Phi$ *is (set-theoretically) a union of lines. Then* $\mathcal{C}_\Phi$ *has a smooth* k*-point if and only if the Fano scheme has a smooth* k*-point.*

PROOF: It suffices to show that a line has multiplicity one if and only if it corresponds to a smooth point on the Fano scheme. We checked this using the classification in Lemma 2.8. □

Remark 2.15. Assume $\text{char}(k) \neq 2, 3$. Then one way to test whether a binary quartic F is the square of a polynomial over $\overline{k}$ is to test whether F and its Hessian (which is again a binary quartic) are linearly dependent. Likewise if Φ is a genus one model of degree 3 or 4 and $\mathcal{C}_\Phi$ is a curve then $\mathcal{C}_\Phi$ is a union of lines if and only if Φ and its Hessian are linearly dependent. For the definition of the Hessian in the case $n = 4$ see [F3].

2.3. **Finding the non-regular points.** We keep the notation for local fields introduced at the start of Section 2. In particular K is a finite extension of $\mathbb{Q}_p$ with ring of integers $\mathcal{O}_K$ and residue field k.

We show how to find the k-rational non-regular points on the reduction of a genus one model over K. (See the algorithms of Section 2.1 for the definition of a non-regular point.) If k is small or the singular locus is zero-dimensional then there is no difficulty in looping over all singular points on the reduction and testing to see which if any are non-regular. For larger k this can be rather inefficient. Instead we employ the following lemmas.

Recall that by the results in [CFS] we may assume that our models have level 0 and so in particular are minimal. Notice also that, taking into account the transformations in Step (i) that immediately follow each recursion, the algorithms in Section 2.1 never increase the level.

Lemma 2.16. *Assume* $\text{char}(k) \neq 2$ *and let* $y^2 = F(x, z)$ *be a minimal binary quartic over* K*. Then the non-regular points are some (but not necessarily all) of the roots of* $F_1(x, z) \equiv 0 \pmod{\pi}$ *where* $F_1 = \pi^{-v(F)} F$.

Proof: Since F is minimal we have $v(F) = 0$ or 1. The rest is clear. □

Lemma 2.17. *Let $F(x, y, z)$ be a minimal ternary cubic over K. If the singular locus of the reduction has positive dimension then by a change of co-ordinates we may assume that*

$$F(x, y, z) = f_0x^3 + f_1(y, z)x^2 + \pi f_2(y, z)x + \pi f_3(y, z)$$

where the f_i are binary forms of degree i. There are then at most 3 non-regular points and these are the roots of $x \equiv f_3(y, z) \equiv 0 \pmod{\pi}$.

Proof: Since F is minimal we have $v(F) = 0$ and $v(f_3) = 0$. The rest is clear. □

Assume $\mathrm{char}(k) \neq 2$ and consider the quadric intersection $\mathbf{x}^T A\mathbf{x} = \mathbf{x}^T B\mathbf{x} = 0$ where $A = (a_{ij})$ and $B = (b_{ij})$ are 4 by 4 symmetric matrices over $\mathcal{O}_K$. Then $(1 : 0 : 0 : 0)$ is a non-regular point on the reduction if and only if, after using a matrix in $\mathrm{GL}_2(\mathcal{O}_K)$ to replace A and B by suitable linear combinations, we have $\pi^2 \mid a_{11}$, $\pi \mid a_{12}, a_{13}, a_{14}$ and $\pi \mid b_{11}$.

Lemma 2.18. *Assume $\mathrm{char}(k) \neq 2$ and let $Q_1 = Q_2 = 0$ be a minimal quadric intersection over K. We write A and B for the 4 by 4 symmetric matrices corresponding to Q_1 and Q_2 and put $F(x, z) = \det(Ax + Bz)$. (If $Q_1 = Q_2 = 0$ has level 0 then the so-called doubling $y^2 = F(x, z)$ is again minimal.)*

(i) *Suppose $(x : z) = (1 : 0)$ is a non-regular point on $y^2 = F(x, z)$ and let $s = 4 - \mathrm{rank}\,\widetilde{A}$. By a change of co-ordinates we may assume*

$$A = \begin{pmatrix} \pi A_1 & \pi A_2 \\ \pi A_2^T & A_3 \end{pmatrix} \qquad B = \begin{pmatrix} B_1 & B_2 \\ B_2^T & B_3 \end{pmatrix} \tag{2.2}$$

where A_1 and B_1 are s by s matrices. Let q_1 and q_2 be the quadratic forms corresponding to A_1 and B_1. Then there are at most 4 solutions to

$$q_1(x_1, \ldots, x_s) \equiv q_2(x_1, \ldots, x_s) \equiv x_{s+1} \equiv \ldots \equiv x_4 \equiv 0 \pmod{\pi}$$

and each of these is a non-regular point on $Q_1 = Q_2 = 0$.

(ii) *If we loop over all non-regular points on $y^2 = F(x, z)$, moving each to $(x : z) = (1 : 0)$ in turn, then all non-regular points on $Q_1 = Q_2 = 0$ arise as described in (i).*

Proof: (i) Since $Q_1 = Q_2 = 0$ is minimal we have $s \leq 3$. If $s = 2$ then the binary quadratic forms q_1 and q_2 cannot both vanish mod π as this would contradict minimality. Likewise if $s = 3$ then q_1 and q_2 are ternary quadratic forms with no common factor. So by Bezout's theorem there are at most 4 solutions.
(ii) Suppose $(1 : 0 : 0 : 0)$ is a non-regular point. If we replace Q_1 and Q_2 by suitable linear combinations then A and B are given by (2.2) with $s = 1$ and

$A_1 \equiv B_1 \equiv 0 \pmod{\pi}$. It follows that $\det(Ax+Bz) = ax^4 + bx^3z + \ldots$ with $\pi^2 \mid a$ and $\pi \mid b$. Then $(1:0)$ is a non-regular point on $y^2 = F(x,z)$. □

Remark 2.19. These lemmas show that for a model of level 0 the number of non-regular points is bounded independent of the size of the residue field. This has the interpretation that the $\mathcal{O}_K$-scheme defined by the model is normal. Alternative proofs (taking a more geometric approach in the case $n = 4$) are given in [Sa].

2.4. **Real solubility.** A section on testing local solubility would be incomplete without some discussion of the real place. However we have nothing new to add. For models of degree 3 and for models of degree 2 and 4 with negative discriminant real solubility is automatic. A binary quartic with positive discriminant has either 0 or 4 real roots, and in the former case is soluble over the reals if and only if the leading coefficient is positive. For real solubility of quadric intersections we refer to [Si1, Chapter 6].

3. Covering maps

Let Φ be a non-singular genus one model over a field K with $\mathrm{char}(K) \neq 2, 3$. The starting point for this section is the survey article [AKM^{3}P] that gives formulae for the covering map $\pi : \mathcal{C}_\Phi \to E$ where E is the Jacobian elliptic curve with Weierstrass equation (1.3). The formulae are given by covariants coming from classical invariant theory.

Our height bounds in Section 4 will be computed as sums of local contributions. To compute the correct contributions at primes dividing 2 and 3 we modify the formulae in [AKM^{3}P]. The first step is to give a Weierstrass equation for the Jacobian

$$y^2 + a_1(\Phi)xy + a_3(\Phi)y = x^3 + a_2(\Phi)x^2 + a_4(\Phi)x + a_6(\Phi) \tag{3.1}$$

that works in all characteristics. This is accomplished in [ARVT], [CFS], where the a-invariants a_1, a_2, a_3, a_4, a_6 are obtained from c_4 and c_6 by working back through the formulae

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \qquad b_4 = 2a_4 + a_1a_3, \qquad b_6 = a_3^2 + 4a_6, \\ c_4 &= b_2^2 - 24b_4, \qquad c_6 = -b_2^3 + 36b_2b_4 - 216b_6. \end{aligned} \tag{3.2}$$

We recall formulae for the a-invariants below. It is important to note however that they are not invariants in the sense of Section 1.1. Likewise our modified formulae for the covering maps will not be covariants. Nonetheless we still need to understand how they change under transformations of genus one models.

3.1. **Generalised binary quartics.** We recall that a genus one model of degree 2 is a generalised binary quartic $y^2 + P(x_1, x_2)y = Q(x_1, x_2)$ where

$$P(x_1, x_2) = lx_1^2 + mx_1x_2 + nx_2^2$$
$$Q(x_1, x_2) = ax_1^4 + bx_1^3x_2 + cx_1^2x_2^2 + dx_1x_2^3 + ex_2^4.$$

Let $g = \frac{1}{4}P^2 + Q$ be the binary quartic obtained by completing the square. It has covariants $h = \frac{1}{3}(g_{12}^2 - g_{11}g_{22})$ and $k = \frac{1}{12}(g_2h_1 - g_1h_2)$ where the subscripts denote partial derivatives. In [CFS] the a-invariants of (P, Q) are defined as

$$\begin{aligned}
a_1 &= m \\
a_2 &= -ln + c \\
a_3 &= ld + nb \\
a_4 &= -l^2e - lnc - n^2a - 4ae + bd \\
a_6 &= -l^2ce + lmbe - lnbd - m^2ae + mnad - n^2ac - 4ace + ad^2 + b^2e.
\end{aligned}$$

The b-invariants b_2, b_4, b_6 and c-invariants c_4, c_6 are then given by (3.2). We put $F = 4g = P^2 + 4Q$ and

$$\begin{aligned}
Z &= 2y + P \\
X &= \tfrac{1}{3}(h - b_2g) \\
Y &= k - \tfrac{1}{2}a_1XZ - \tfrac{1}{2}a_3FZ.
\end{aligned}$$

Lemma 3.1. *(i) Z, X, Y have coefficients in $\mathbb{Z}[l, m, n, a, b, c, d, e]$.*
(ii) Let (P, Q) be a non-singular generalised binary quartic defined over K. Then $E = \operatorname{Jac} \mathcal{C}_{(P,Q)}$ has Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

and the 2-covering map $\mathcal{C}_{(P,Q)} \to E$ is given by $(x_1 : x_2 : y) \mapsto (X/Z^2, Y/Z^3)$.

Proof: (i) A direct calculation.
(ii) The formula for E is recalled from [CFS]. The classical syzygy

$$27k^2 = h^3 - 3c_4g^2h - 2c_6g^3$$

becomes

$$\begin{aligned}
Y^2 + a_1XYZ + a_3YZF = X^3 + a_2X^2F + a_4XF^2 + a_6F^3 \\
- (a_1X + a_3F)^2(y^2 + Py - Q).
\end{aligned}$$

Since $F \equiv Z^2 \mod (y^2 + Py - Q)$ this gives the required map. □

For use in later sections we put $F_2 = F = P^2 + 4Q$ and $G_2 = X$. Explicitly

$$\begin{aligned}
F_2 &= (l^2+4a)x_1^4 + (2lm+4b)x_1^3x_2 + (2ln+m^2+4c)x_1^2x_2^2 + (2mn+4d)x_1x_2^3 \\
&\quad + (n^2+4e)x_2^4, \\
G_2 &= (-l^2c + lmb - m^2a - 4ac + b^2)x_1^4 + (-2l^2d + 2lnb - 4mna - 8ad)x_1^3x_2 \\
&\quad + (-4l^2e - lmd + 2lnc - mnb - 4n^2a - 16ae - 2bd)x_1^2x_2^2 \\
&\quad + (-4lme + 2lnd - 2n^2b - 8be)x_1x_2^3 + (-m^2e + mnd - n^2c - 4ce + d^2)x_2^4.
\end{aligned}$$

In [S] these polynomials were denoted $4G$ and $\widetilde{G}$. We describe how they change under transformations of genus one models.

Lemma 3.2. *(i) If $(P', Q') = [\mu, (r_0, r_1, r_2), I_2](P, Q)$ then*

$$\begin{aligned}
F_2'(x,z) &= \mu^2 F_2(x,z) \\
G_2'(x,z) &= \mu^4(G_2(x,z) + (lr_2 + 2r_0r_2 + nr_0)F_2(x,z)).
\end{aligned}$$

(ii) If $(P', Q') = [1, 0, \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)](P, Q)$ then

$$\begin{aligned}
F_2'(x,z) &= F_2(\alpha x + \gamma z, \beta x + \delta z) \\
G_2'(x,z) &= (\alpha\delta - \beta\gamma)^2 G_2(\alpha x + \gamma z, \beta x + \delta z) - \lambda F_2(\alpha x + \gamma z, \beta x + \delta z)
\end{aligned}$$

where $\lambda = 2\alpha^2\gamma^2 a + \alpha\gamma(\alpha\delta + \beta\gamma)b + 2\alpha\beta\gamma\delta c + \beta\delta(\alpha\delta + \beta\gamma)d + 2\beta^2\delta^2 e$.

Proof: A direct calculation. $\square$

3.2. **Ternary cubics.** A genus one model of degree 3 is a ternary cubic

$$\begin{aligned}
U(x_1, x_2, x_3) = ax_1^3 + bx_2^3 + cx_3^3 + fx_2^2x_3 + gx_3^2x_1 + hx_1^2x_2& \\
+ ix_2x_3^2 + jx_3x_1^2 + kx_1x_2^2 + mx_1x_2x_3&.
\end{aligned}$$

It has Hessian $H = -(1/2)\det(U_{ij})$ and covariants

$$\Theta = (1/3)\begin{vmatrix} U_{11} & U_{12} & U_{13} & H_1 \\ U_{21} & U_{22} & U_{23} & H_2 \\ U_{31} & U_{32} & U_{33} & H_3 \\ H_1 & H_2 & H_3 & 0 \end{vmatrix}, \qquad J = (1/18)\begin{vmatrix} U_1 & U_2 & U_3 \\ H_1 & H_2 & H_3 \\ \Theta_1 & \Theta_2 & \Theta_3 \end{vmatrix},$$

where the subscripts denote partial derivatives. In [ARVT], [CFS] the a-invariants of U are defined as

$$\begin{aligned} a_1 &= m \\ a_2 &= -(fj + gk + hi) \\ a_3 &= 9abc - afi - bgj - chk - fgh - ijk \\ a_4 &= -3(abgi + acfk + bchj) + af^2g + ai^2k + bg^2h + bij^2 \\ &\qquad + cfh^2 + cjk^2 + fgjk + fhij + ghik \\ a_6 &= -27a^2b^2c^2 + 9abc(afi + bgj + chk) + \ldots + abcm^3. \end{aligned}$$

The b-invariants b_2, b_4, b_6 and c-invariants c_4, c_6 are then given by (3.2). We put $b_8 = (b_2b_6 - b_4^2)/4$ and

$$\begin{aligned} Z &= \tfrac{1}{4}(H + b_2U) \\ X &= \tfrac{1}{192}(\Theta - 16b_2Z^2 - 12b_2^2ZU + b_2^3U^2) \\ Y &= \tfrac{1}{2}(\tfrac{1}{384}J - (a_1XZ + a_3Z^3 + a_3XU + a_1b_6ZU^2 + a_1b_8U^3)). \end{aligned}$$

Lemma 3.3. *(i) Z, X, Y have coefficients in $\mathbb{Z}[a, b, c, f, g, h, i, j, k, m]$.*
(ii) Let U be a non-singular ternary cubic defined over K. Then $E = \operatorname{Jac}\mathcal{C}_U$ has Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

and the 3-covering map $\mathcal{C}_U \to E$ is given by $(x_1 : x_2 : x_3) \mapsto (X/Z^2, Y/Z^3)$.

Proof: (i) A direct calculation.
(ii) The formula for E is recalled from [ARVT], [CFS]. The classical syzygy

$$\begin{aligned} 12J^2 = \Theta^3 &- 3c_4\Theta H^4 - 2c_6H^6 - 9c_4\Theta^2HU + 12c_6\Theta H^3U + 21c_4^2H^5U \\ &+ 6c_6\Theta^2U^2 + 9c_4^2\Theta H^2U^2 - 72c_4c_6H^4U^2 - 24c_4c_6\Theta HU^3 \\ &+ (27c_4^3 + 64c_6^2)H^3U^3 + 9c_4^3\Theta U^4 - 48c_4^2c_6H^2U^4 + 9c_4^4HU^5 \end{aligned}$$

becomes

$$\begin{aligned} Y^2 + a_1XYZ + a_3YZ^3 &= X^3 + a_2X^2Z^2 + a_4XZ^4 + a_6Z^6 \\ &- a_3XYU + (4a_1a_3 + 9a_4)X^2ZU + \gamma_1XZ^3U + \gamma_2Z^5U - (7a_3^2 + 27a_6)X^2U^2 \\ &- (a_1a_3^2 + 4a_1a_6)YZU^2 + \gamma_3XZ^2U^2 + \gamma_4Z^4U^2 + \gamma_5YU^3 + \gamma_6XZU^3 \\ &+ \gamma_7Z^3U^3 + \gamma_8XU^4 + \gamma_9Z^2U^4 + \gamma_{10}ZU^5 + \gamma_{11}U^6 \end{aligned}$$

where the γ_i are certain polynomials in $\mathbb{Z}[a_1, a_2, a_3, a_4, a_6]$. This gives the required formula for the 3-covering map. □

For use in later sections we put $F_3 = Z^2$ and $G_3 = X$. We describe how these polynomials change under transformations of genus one models.

Lemma 3.4. *(i) If* $U' = [\mu, I_3]U$ *then* $F_3' = \mu^6 F_3$ *and* $G_3' = \mu^8 G_3$.
(ii) If $U' = [1, N]U$ *and* $x_j = \sum n_{ij} x_i'$ *where* $N = (n_{ij})$ *then*

$$\begin{aligned} F_3'(x_1', x_2', x_3') &= ((\det N)^4 F_3 + \alpha Z U + \beta U^2)(x_1, x_2, x_3) \\ G_3'(x_1', x_2', x_3') &= ((\det N)^6 G_3 + \lambda F_3 + \gamma Z U + \delta U^2)(x_1, x_2, x_3) \end{aligned} \tag{3.3}$$

for some $\lambda, \alpha, \beta, \gamma, \delta \in \mathbb{Z}[n_{11}, n_{12}, \ldots, n_{33}, a, b, c, \ldots, m]$. *Moreover if* N *is diagonal then* $\lambda = 0$.

Proof: (i) This is clear.
(ii) Since H and Θ are covariants we have

$$\begin{aligned} H'(x_1', x_2', x_3') &= (\det N)^2 H(x_1, x_2, x_3) \\ \Theta'(x_1', x_2', x_3') &= (\det N)^6 \Theta(x_1, x_2, x_3). \end{aligned}$$

Let $\xi = \frac{1}{12}(b_2' - (\det N)^2 b_2)$. Then (3.3) holds with $\lambda = -(\det N)^4 \xi$ and

$$\begin{aligned} \alpha &= 6(\det N)^2 \xi, & \beta &= 9\xi^2, \\ \gamma &= -(\det N)^2 \xi (2b_2' - 9\xi), & \delta &= -3\xi^2(b_2' - 3\xi). \end{aligned}$$

A generic calculation shows that $b_2' \equiv (\det N)^2 b_2 \pmod{12}$. Moreover if N is diagonal then $b_2' = (\det N)^2 b_2$ and so in that case $\lambda = 0$. □

3.3. **Quadric intersections.** A genus one model of degree 4 is a pair of quadratic forms (Q_1, Q_2) in variables $x_1, \ldots, x_4$. We write

$$\begin{aligned} Q_1(x_1, \ldots, x_4) &= \sum_{i \le j} a_{ij} x_i x_j = \tfrac{1}{2} \sum_{i,j=1}^{4} A_{ij} x_i x_j \\ Q_2(x_1, \ldots, x_4) &= \sum_{i \le j} b_{ij} x_i x_j = \tfrac{1}{2} \sum_{i,j=1}^{4} B_{ij} x_i x_j \end{aligned}$$

where $A = (A_{ij})$ and $B = (B_{ij})$ are the matrices of second partial derivatives of Q_1 and Q_2. Let $Q_1^* = \sum_{i \le j} a_{ij}^* x_i x_j$ and $Q_2^* = \sum_{i \le j} b_{ij}^* x_i x_j$ be the quadrics whose matrices of second partial derivatives are $\operatorname{adj} A$ and $\operatorname{adj} B$. There are covariants

$$\begin{aligned} T_1 &= \sum_{i,j=1}^{4} \sum_{r \le s} b_{rs}^* (A_{ij} A_{rs} - A_{is} A_{jr}) x_i x_j \\ T_2 &= \sum_{i,j=1}^{4} \sum_{r \le s} a_{rs}^* (B_{ij} B_{rs} - B_{is} B_{jr}) x_i x_j \\ J &= (1/4) \frac{\partial(Q_1, Q_2, T_1, T_2)}{\partial(x_1, x_2, x_3, x_4)}. \end{aligned}$$

It is noted in [CFS] that if $\Gamma = \sum_{i \le j} c_{ij} x_i x_j$ is a quadric in 4 variables then

$$\det\left(\frac{\partial^2 \Gamma}{\partial x_i \partial x_j}\right) = \operatorname{pf}(\Gamma)^2 + 4\operatorname{rd}(\Gamma)$$

where $\operatorname{pf}(\Gamma) = c_{12}c_{34} + c_{13}c_{24} + c_{14}c_{23}$ and $\operatorname{rd}(\Gamma) \in \mathbb{Z}[c_{11}, c_{12}, \ldots, c_{44}]$. Writing $\operatorname{pf}(xQ_1 + zQ_2) = lx^2 + mxz + nz^2$ we put

$$Y = \tfrac{1}{2}\left(J - lT_1^2 + mT_1T_2 - nT_2^2 + mn(lT_1 + mT_2)Q_1 + lm(mT_1 + nT_2)Q_2 \right.$$
$$\left. + l^2n^3Q_1^2 + lmn(ln + m^2)Q_1Q_2 + l^3n^2Q_2^2\right).$$

Lemma 3.5. *(i) T_1, T_2, Y have coefficients in $\mathbb{Z}[a_{11}, a_{12}, \ldots, b_{44}]$.*
(ii) Let (Q_1, Q_2) be a non-singular quadric intersection defined over K. Then $(P, Q) = (\operatorname{pf}(xQ_1 + zQ_2), \operatorname{rd}(xQ_1 + zQ_2))$ is a non-singular generalised binary quartic and the 4-covering map $\mathcal{C}_{(Q_1,Q_2)} \to E = \operatorname{Jac}\mathcal{C}_{(Q_1,Q_2)}$ is the composite of

$$\mathcal{C}_{(Q_1,Q_2)} \to \mathcal{C}_{(P,Q)}\,; \quad (x_1 : \ldots : x_4) \mapsto (T_1 : -T_2 : Y)$$

and the 2-covering map $\mathcal{C}_{(P,Q)} \to E$.

PROOF: (i) A direct calculation.
(ii) The formula for (P, Q) is recalled from [CFS]. There is a classical syzygy satisfied by Q_1, Q_2, T_1, T_2, J and the coefficients of

$$F(x, z) = \det(Ax + Bz). \tag{3.4}$$

Setting $Q_1 = Q_2 = 0$ it reduces to $J^2 \equiv F(T_1, -T_2) \mod (Q_1, Q_2)$. We have $F = P^2 + 4Q$ and $2Y \equiv J - P(T_1, -T_2) \mod (Q_1, Q_2)$. Therefore

$$4(Y^2 + P(T_1, -T_2)Y - Q(T_1, -T_2)) = S_1Q_1 + S_2Q_2$$

for some S_1, S_2 in $\mathbb{Z}[a_{11}, a_{12}, \ldots, b_{44}][x_1, \ldots, x_4]$. Since the generic quadrics Q_1 and Q_2 are coprime mod 2 a similar identity holds without the factor of 4. Hence

$$Y^2 + P(T_1, -T_2)Y \equiv Q(T_1, -T_2) \mod (Q_1, Q_2)$$

as required. □

The a-invariants of (Q_1, Q_2) are defined to be the a-invariants of (P, Q). The transformations of genus one models defined in Section 1.1 have the following effect on (P, Q) and on T_1 and T_2.

Lemma 3.6. *If $(Q_1', Q_2') = [M, N](Q_1, Q_2)$ then $(P', Q') = [\det N, r, M](P, Q)$ for some $r = (r_0, r_1, r_2)$ where the r_i are integer coefficient polynomials in the entries of M and N and the coefficients of Q_1 and Q_2. Moreover if N is diagonal then $r = 0$.*

PROOF: If $N = I_4$ then the result is clear. So suppose $(Q_1', Q_2') = [I_2, N](Q_1, Q_2)$. We must show that

$$\begin{aligned} P'(x,z) &= (\det N)P(x,z) + 2r(x,z) \\ Q'(x,z) &= (\det N)^2 Q(x,z) - (\det N)P(x,z)r(x,z) - r(x,z)^2 \end{aligned}$$

for some $r(x,z) = r_0x^2 + r_1xz + r_2z^2$ where the r_i are integer coefficient polynomials in the entries of N and the coefficients of Q_1 and Q_2. But in characteristic 2 we recognise $P(x,z) = \mathrm{pf}(xQ_1 + zQ_2)$ as the Pfaffian of a skew-symmetric matrix. This gives the formula for P'. The formula for Q' follows since $P'^2 + 4Q' = (\det N)^2(P^2 + 4Q)$. Moreover if N is diagonal then $P'(x,z) = (\det N)P(x,z)$ and so in that case $r = 0$. □

Lemma 3.7. *(i) If* $(Q_1', Q_2') = [(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}), I_4](Q_1, Q_2)$ *then*

$$\begin{aligned} T_1' &= (\alpha\delta - \beta\gamma)^2(\delta T_1 + \gamma T_2) + \nu_1 Q_1 + \nu_2 Q_2 \\ T_2' &= (\alpha\delta - \beta\gamma)^2(\beta T_1 + \alpha T_2) + \nu_3 Q_1 + \nu_4 Q_2 \end{aligned} \tag{3.5}$$

where the ν_i *are integer coefficient polynomials in* $\alpha, \beta, \gamma, \delta$ *and the coefficients of* Q_1 *and* Q_2.
(ii) If $(Q_1', Q_2') = [I_2, N](Q_1, Q_2)$ *and* $x_j = \sum n_{ij}x_i'$ *where* $N = (n_{ij})$ *then*

$$T_i'(x_1', \ldots, x_4') = (\det N)^2 T_i(x_1, \ldots, x_4)$$

for $i = 1, 2$.

PROOF: (i) Let a, b, c, d, e be the coefficients of (3.4) and a', b', c', d', e' their analogues for (Q_1', Q_2'). Direct calculation shows that (3.5) holds with

$$\begin{aligned} \nu_1 &= \tfrac{1}{6}(\gamma c' + 3\alpha d' - (\alpha\delta - \beta\gamma)^2(\gamma c + 3\delta d)) \\ \nu_2 &= \tfrac{1}{6}(\delta c' + 3\beta d' - (\alpha\delta - \beta\gamma)^2(\delta c + 3\gamma b)) \\ \nu_3 &= \tfrac{1}{6}(\alpha c' + 3\gamma b' - (\alpha\delta - \beta\gamma)^2(\alpha c + 3\beta d)) \\ \nu_4 &= \tfrac{1}{6}(\beta c' + 3\delta b' - (\alpha\delta - \beta\gamma)^2(\beta c + 3\alpha b)). \end{aligned}$$

Writing a', b', c', d', e' as polynomials in $\alpha, \beta, \gamma, \delta, a, b, c, d, e$ we find that $\nu_1, \nu_2, \nu_3, \nu_4$ belong to $\mathbb{Z}[\alpha, \beta, \gamma, \delta, a, b, c, d, e]$. These formulae are related to the covariance of the Hessian as defined in [F3].
(ii) Let M_1 and M_2 be the matrices of second partial derivatives of T_1 and T_2. Direct calculation shows that

$$\mathrm{adj}(\mathrm{adj}(A)x + \mathrm{adj}(B)z) = a^2Ax^3 + aM_1x^2z + eM_2xz^2 + e^2Bz^3.$$

The covariance of T_1 and T_2 then follows from properties of the adjugate. □

For use in later sections we put $F_4 = F_2(T_1, -T_2)$ and $G_4 = G_2(T_1, -T_2)$ where F_2 and G_2 are the polynomials associated to the model (P, Q) in Lemma 3.5(ii).

3.4. **A geometric observation.** Let Φ be a genus one model of degree $n \in \{2, 3, 4\}$ over a field K. Let E be the (possibly singular) curve defined by the Weierstrass equation with coefficients the a-invariants of Φ. The formulae in the last three sections define a map $\pi : \mathcal{C}_\Phi \to E$. If Φ is non-singular then $\mathcal{C}_\Phi$ is a smooth curve of genus one, E is the Jacobian elliptic curve and π is the n-covering map. However to understand what happens at primes of bad reduction we are also interested in singular models.

The composite $\mathcal{C}_\Phi \xrightarrow{\pi} E \xrightarrow{x} \mathbb{P}^1$ is given by $(F_n : G_n)$ where F_n and G_n are the homogeneous polynomials of degree $2n$ associated to Φ.

Theorem 3.8. *Let Φ be a genus one model of degree $n \in \{2, 3, 4\}$ over a field K. Let $P \in \mathcal{C}_\Phi$ say $P = (x_1 : x_2 : y)$ or $(x_1 : \ldots : x_n)$. Then $F_n(x_1, \ldots, x_n) = G_n(x_1, \ldots, x_n) = 0$ if and only if P is singular or lies on a component of $\mathcal{C}_\Phi$ of degree at most $n - 2$.*

Proof: We split into the cases $n = 2, 3, 4$.
Case $\mathbf{n = 2}$. The generalised binary quartic

$$y^2 + (lx^2 + mxz + nz^2)y = ax^4 + bx^3z + cx^2z^2 + dxz^3 + ez^4.$$

has associated polynomials

$$\begin{aligned} F_2(x, z) &= (l^2 + 4a)x^4 + (2lm + 4b)x^3z + (2ln + m^2 + 4c)x^2z^2 + \ldots \\ G_2(x, z) &= (-l^2c + lmb - m^2a - 4ac + b^2)x^4 + \ldots \end{aligned}$$

By Lemma 3.2 we may assume that P is the point $(x : z : y) = (1 : 0 : 0)$ and so $a = 0$. Then $F_2(1, 0) = G_2(1, 0) = 0$ if and only if $l = b = 0$. This is the condition for P to be a singular point.
Case $\mathbf{n = 3}$. A genus one model of degree 3 is a ternary cubic

$$\begin{aligned} U(x_1, x_2, x_3) = ax_1^3 + bx_2^3 + cx_3^3 + fx_2^2x_3 + gx_3^2x_1 + hx_1^2x_2 \\ + ix_2x_3^2 + jx_3x_1^2 + kx_1x_2^2 + mx_1x_2x_3. \end{aligned}$$

By Lemma 3.4 we may assume that P is the point $(x_1 : x_2 : x_3) = (1 : 0 : 0)$ and $a = h = 0$. We compute

$$\begin{aligned} F_3(1, 0, 0) &= j^4k^2 \\ G_3(1, 0, 0) &= b^2j^6 - bj^5km + fj^5k^2. \end{aligned}$$

Thus $F_3(1, 0, 0) = G_3(1, 0, 0) = 0$ if and only if $j = 0$ or $b = k = 0$. These are the conditions that P is either a singular point or lies on a line.
Case $\mathbf{n = 4}$. By Lemmas 3.2, 3.6 and 3.7 we may assume that P is the point $(1 : 0 : 0 : 0)$ and $\Phi = (Q_1, Q_2)$ takes the form

$$\begin{aligned} Q_1(x_1, \ldots, x_4) &= \lambda x_1x_3 + q_1(x_2, x_3, x_4) \\ Q_2(x_1, \ldots, x_4) &= \mu x_1x_4 + q_2(x_2, x_3, x_4). \end{aligned}$$

We compute $T_1(1,0,0,0) = \lambda^2\mu^2 b_{22}$ and $T_2(1,0,0,0) = \lambda^2\mu^2 a_{22}$. If $\lambda\mu = 0$ or $a_{22} = b_{22} = 0$ then $F_4(P) = G_4(P) = 0$ and P is a either a singular point or lies on a line. Otherwise we may assume that $\lambda = \mu = b_{22} = 1$ and $a_{22} = 0$. Then P maps to the point $(x : z : y) = (1 : 0 : 0)$ on the generalised binary quartic

$$\begin{aligned} y^2 + (a_{24}x^2 + (a_{23} + b_{24})xz + b_{23}z^2)y = -(a_{23}a_{24} + a_{44})x^3z+ \\ - (a_{23}b_{24} + a_{24}b_{23} - a_{34} + b_{44})x^2z^2 - (a_{33} + b_{23}b_{24} - b_{34})xz^3 - b_{33}z^4. \end{aligned}$$

Our proof in the case $n = 2$ shows that $F_4(P) = G_4(P) = 0$ if and only if $a_{24} = a_{44} = 0$. This is the condition for some quadric in the pencil spanned by Q_1 and Q_2 (in fact it can only be Q_1) to factor as a product of two linear forms. It is therefore also the condition for P to lie on a conic. □

Remark 3.9. We suspect that some analogue of Theorem 3.8 holds for n-coverings more generally. However our method of proof, using invariant theory and explicit formulae, is unlikely to generalise to larger n.

4. Height bounds

Let E be an elliptic curve over a number field K. An n-descent calculation on E computes equations for the everywhere locally soluble n-coverings $\pi : \mathcal{C} \to E$. It is expected that a point $P \in \mathcal{C}(K)$ will have smaller height than its image in $E(K)$, and that therefore searching on the covering curves makes it easier to find generators for $E(K)$. Of course such an expectation can only be realised if our equations for $\mathcal{C}$ are given relative to some reasonably good choice of co-ordinates. In [CFS] it is explained (at least over $K = \mathbb{Q}$) how to make such choices of co-ordinates when $n = 2, 3$ or 4. We determine explicit height bounds in these cases.

4.1. **Local height bounds.** Let Φ be a non-singular genus one model of degree $n \in \{2, 3, 4\}$ over a number field K. Let M_K, respectively M_K^0, be the set of places, respectively finite places, of K. We write K_v for the completion of K at $v \in M_K$ and normalise the absolute values $|\cdot|_v$ on K_v so that the product formula holds. The height of a point $P = (x_1 : \ldots : x_n) \in \mathbb{P}^{n-1}(K)$ is

$$h(P) = \log \prod_{v \in M_K} \max(|x_1|_v, \ldots, |x_n|_v).$$

Let F_n and G_n be the polynomials associated to Φ as defined in Section 3. For $v \in M_K$ we define

$$\delta_v(\Phi) = \sup_{P \in \mathcal{C}_\Phi(K_v)} \frac{\max(|F_n(\mathbf{x})|_v, |G_n(\mathbf{x})|_v)}{\max(|x_1|_v, \ldots, |x_n|_v)^{2n}}$$

$$\varepsilon_v(\Phi) = \inf_{P \in \mathcal{C}_\Phi(K_v)} \frac{\max(|F_n(\mathbf{x})|_v, |G_n(\mathbf{x})|_v)}{\max(|x_1|_v, \ldots, |x_n|_v)^{2n}}$$

where $P = (x_1 : x_2 : y)$ or $(x_1 : \ldots : x_n)$. These definitions are independent of the scaling of the x_i since F_n and G_n are homogeneous of degree $2n$.

Theorem 4.1. *Let Φ be a non-singular genus one model over K.*

(i) *For any $v \in M_K$ we have $0 < \varepsilon_v(\Phi) \le \delta_v(\Phi) < \infty$.*
(ii) *If $v \in M_K^0$ and Φ is v-integral then $0 < \varepsilon_v(\Phi) \le \delta_v(\Phi) \le 1$.*
(iii) *If $v \in M_K^0$ and Φ has good reduction mod v then $\varepsilon_v(\Phi) = \delta_v(\Phi) = 1$.*
(iv) *Let h and h_E be the heights on $\mathcal{C}_\Phi$ and $E = \operatorname{Jac}(\mathcal{C}_\Phi)$ relative to $\mathcal{C}_\Phi \to \mathbb{P}^{n-1}$ and the Weierstrass equation (3.1). Let $\pi : \mathcal{C}_\Phi \to E$ be the covering map. Then for $P \in \mathcal{C}_\Phi(K)$ we have*

$$-\sum_v \log \delta_v(\Phi) \le 2nh(P) - h_E(\pi P) \le -\sum_v \log \varepsilon_v(\Phi). \tag{4.1}$$

Proof: (i) We are assuming that Φ is non-singular. So by Theorem 3.8 there does not exist $P \in \mathcal{C}_\Phi(K_v)$ with $F_n(P) = G_n(P) = 0$. Since $\mathcal{C}_\Phi(K_v)$ is compact it follows that $0 < \varepsilon_v(\Phi) \le \delta_v(\Phi) < \infty$.
(ii) Let $\mathcal{O}_v$ be the valuation ring of K_v. If Φ has coefficients in $\mathcal{O}_v$ then so do F_n and G_n. We scale the x_i so that $\max(|x_1|_v, \ldots, |x_n|_v) = 1$. Then $|F_n(\mathbf{x})|_v \le 1$ and $|G_n(\mathbf{x})|_v \le 1$. Hence $\delta_v(\Phi) \le 1$.
(iii) Again we scale the x_i so that $\max(|x_1|_v, \ldots, |x_n|_v) = 1$. Then by Theorem 3.8 applied to the reduction of Φ mod v we have $\max(|F_n(\mathbf{x})|_v, |G_n(\mathbf{x})|_v) = 1$. Hence $\varepsilon_v(\Phi) = \delta_v(\Phi) = 1$.
(iv) If $P \in \mathcal{C}_\Phi(K)$, say $P = (x_1 : x_2 : y)$ or $(x_1 : \ldots : x_n)$, then

$$h(P) = \log \prod_{v \in M_K} \max(|x_1|_v, \ldots, |x_n|_v)$$

and

$$h_E(\pi P) = \log \prod_{v \in M_K} \max(|F_n(\mathbf{x})|_v, |G_n(\mathbf{x})|_v).$$

Taking logs in the definitions of $\delta_v(\Phi)$ and $\varepsilon_v(\Phi)$ and summing over $v \in M_K$ gives the result. Notice that by (i) we are taking logs of positive numbers, and by (iii) the sums are finite. □

If $v \in M_K^0$ with uniformiser π_v then

$$\delta_v(\Phi) = |\pi_v|_v^{2\min A_v(\Phi)} \quad \text{and} \quad \varepsilon_v(\Phi) = |\pi_v|_v^{2\max A_v(\Phi)} \tag{4.2}$$

where $A_v(\Phi)$ is the set of *Tamagawa distances* defined and computed in the next two sections. An alternative description of the Tamagawa distances in Section 4.4 explains the choice of name. The computation of $\delta_v(\Phi)$ and $\varepsilon_v(\Phi)$ for v a real place is the subject of Section 4.5.

4.2. **Computing the Tamagawa distances.** Let K be a finite extension of $\mathbb{Q}_p$ with ring of integers $\mathcal{O}_K$, maximal ideal $\pi\mathcal{O}_K$, residue field k and normalised discrete valuation $v : K^\times \to \mathbb{Z}$. The corresponding absolute value is $|x| = c^{-v(x)}$ for some constant $c > 1$. Reduction mod π will be denoted $x \mapsto \widetilde{x}$.

Let Φ a non-singular genus one model over K of degree $n \in \{2, 3, 4\}$. Let F_n and G_n be the polynomials depending on Φ as defined in Section 3.

Definition 4.2. The set of *Tamagawa distances* $A = A(\Phi)$ is defined by

$$\left\{ \frac{\max(|F_n(\mathbf{x})|, |G_n(\mathbf{x})|)}{\max(|x_1|, \ldots, |x_n|)^{2n}} : P \in \mathcal{C}_\Phi(K) \right\} = \left\{ |\pi|^{2\alpha} : \alpha \in A(\Phi) \right\}.$$

where $P = (x_1 : x_2 : y)$ or $(x_1 : \ldots : x_n)$. In particular $\mathcal{C}_\Phi(K) \neq \emptyset$ if and only if $A(\Phi) \neq \emptyset$.

Definition 4.3. A transformation of genus one models $g \in \mathcal{G}_n(K)$ is *integral*, respectively *diagonal*, if it satisfies the following conditions.

n	g	integral	diagonal
2	$[\mu, r, N]$	$\mu \in \mathcal{O}_K^\times, r \in \mathcal{O}_K^3, N \in \mathrm{GL}_2(\mathcal{O}_K)$	$r = 0$ and N diagonal
3	$[\mu, N]$	$\mu \in \mathcal{O}_K^\times, N \in \mathrm{GL}_3(\mathcal{O}_K)$	N diagonal
4	$[M, N]$	$M \in \mathrm{GL}_2(\mathcal{O}_K), N \in \mathrm{GL}_4(\mathcal{O}_K)$	M and N diagonal.

The first part of the following theorem shows that if Φ and Φ' are $\mathcal{O}_K$-equivalent then they have the same set of Tamagawa distances. The second part describes the effect of a diagonal transformation that preserves the level.

Theorem 4.4. *Let Φ and Φ' be genus one models over $\mathcal{O}_K$ with $\Phi' = g\Phi$ for some $g \in \mathcal{G}_n(K)$, say $g = [\mu, r, N]$, $[\mu, N]$ or $[M, N]$. Let $P \in \mathcal{C}_\Phi(K)$, say $P = (x_1 : x_2 : y)$ or $(x_1 : \ldots : x_n)$, and $P' \in \mathcal{C}_{\Phi'}(K)$, say $P' = (x_1' : x_2' : y')$ or $(x_1' : \ldots : x_n')$, with $x_j = \sum n_{ij} x_i'$ where $N = (n_{ij})$. If either (i) g is integral or (ii) $\det g \in \mathcal{O}_K^\times$ and g is diagonal then*

$$\max(|F_n'(\mathbf{x}')|, |G_n'(\mathbf{x}')|) = |\det N|^{-2} \max(|F_n(\mathbf{x})|, |G_n(\mathbf{x})|).$$

Proof: Let $(r_2, s_2) = (2, 4)$, $(r_3, s_3) = (6, 8)$, $(r_4, s_4) = (12, 14)$. By Lemmas 3.2, 3.4, 3.6 and 3.7 we have

$$\begin{pmatrix} F_n'(x_1', \ldots, x_n') \\ G_n'(x_1', \ldots, x_n') \end{pmatrix} = (\det N)^{-2} \begin{pmatrix} (\det g)^{r_n} & 0 \\ \lambda & (\det g)^{s_n} \end{pmatrix} \begin{pmatrix} F_n(x_1, \ldots, x_n) \\ G_n(x_1, \ldots, x_n) \end{pmatrix}$$

for some $\lambda \in K$. These lemmas also show that (i) if g is integral then $\lambda \in \mathcal{O}_K$ and (ii) if g is diagonal then $\lambda = 0$. Taking absolute values gives the result. □

We use Theorems 3.8 and 4.4 to modify our local solubility algorithms in Section 2 to give algorithms for computing the set of Tamagawa distances. Our presentation differs from these earlier algorithms in that we do not restrict attention to (points whose reduction lies on) an affine piece until after the first iteration. For models of degrees 3 and 4 we use the subalgorithms in Section 4.3 to compute the contributions from lines and conics. The proof that our algorithms terminate (for Φ non-singular) is given in Section 4.4.

Algorithm 4.5. `TamagawaDistances(P,Q,Affine)`
`INPUT`: A generalised binary quartic $\Phi = (P, Q)$ over $\mathcal{O}_K$ and a boolean `Affine`.
`OUTPUT`: A finite set of non-negative integers A such that

$$\left\{ \frac{\max(|F_2(\mathbf{x})|, |G_2(\mathbf{x})|)}{\max(|x_1|, |x_2|)^4} : (x_1 : x_2 : y) \in \mathcal{C}_\Phi(K)^\dagger \right\} = \{|\pi|^{2\alpha} : \alpha \in A\}$$

where $\mathcal{C}_\Phi(K)^\dagger = \{P \in \mathcal{C}_\Phi(K) : \widetilde{P} \in \Gamma\}$ and Γ is the curve over k defined by

$$\begin{array}{ll} \{y^2 + \widetilde{P}(x_1, x_2)y = \widetilde{Q}(x_1, x_2)\} \subset \mathbb{P}(1, 1, 2) & \text{if } \texttt{Affine} = \texttt{FALSE} \\ \{y^2 + \widetilde{P}(x, 1)y = \widetilde{Q}(x, 1)\} \subset \mathbb{A}^2 & \text{if } \texttt{Affine} = \texttt{TRUE}. \end{array}$$

(i) Set $A = \emptyset$.
(ii) If there are smooth k-points on Γ then set $A = \{0\}$.
(iii) Find all non-regular k-points on Γ. Use an $\mathcal{O}_K$-transformation to move each such point to $(x_1 : x_2 : y) = (0 : 1 : 0)$. Then compute

$$A_1 = \texttt{TamagawaDistances}(\texttt{P1}, \texttt{Q1}, \texttt{TRUE})$$

where $P_1(x_1, x_2) = \pi^{-1}P(\pi x_1, x_2)$, $Q_1(x_1, x_2) = \pi^{-2}Q(\pi x_1, x_2)$, and set $A = A \cup \{\alpha + 1 : \alpha \in A_1\}$.
(iv) Return A.

Algorithm 4.6. `TamagawaDistances(U,Affine)`
`INPUT`: A ternary cubic $U \in \mathcal{O}_K[x, y, z]$ and a boolean `Affine`.
`OUTPUT`: A finite set of non-negative integers A such that

$$\left\{ \frac{\max(|F_3(\mathbf{x})|, |G_3(\mathbf{x})|)}{\max(|x_1|, |x_2|, |x_3|)^6} : (x_1 : x_2 : x_3) \in \mathcal{C}_U(K)^\dagger \right\} = \{|\pi|^{2\alpha} : \alpha \in A\}$$

where $\mathcal{C}_U(K)^\dagger = \{P \in \mathcal{C}_U(K) : \widetilde{P} \in \Gamma\}$ and Γ is the curve over k defined by

$$\begin{array}{ll} \{\widetilde{U}(x, y, z) = 0\} \subset \mathbb{P}^2 & \text{if } \texttt{Affine} = \texttt{FALSE} \\ \{\widetilde{U}(x, y, 1) = 0\} \subset \mathbb{A}^2 & \text{if } \texttt{Affine} = \texttt{TRUE}. \end{array}$$

(i) Set $A = \emptyset$.
(ii) If Γ contains an absolutely irreducible component of degree 2 or 3 then set $A = \{0\}$.

(iii) Find all k-rational lines that are components of Γ of multiplicity one. Compute the contribution α of each such line using Proposition 4.8 and put $A = A \cup \{\alpha\}$.

(iv) Find all non-regular k-points on Γ. Use a transformation in $\mathrm{GL}_3(\mathcal{O}_K)$ to move each such point to $(0:0:1)$. Then compute

$$A_1 = \texttt{TamagawaDistances}(\texttt{U1}, \texttt{TRUE})$$

where $U_1(x,y,z) = \pi^{-2} U(\pi x, \pi y, z)$ and set $A = A \cup \{\alpha + 2 : \alpha \in A_1\}$.

(v) Return A.

Algorithm 4.7. `TamagawaDistances(Q1,Q2,Affine)`
`INPUT`: A quadric intersection $\Phi = (Q_1, Q_2)$ over $\mathcal{O}_K$ and a boolean `Affine`.
`OUTPUT`: A finite set of non-negative integers A such that

$$\left\{ \frac{\max(|F_4(\mathbf{x})|, |G_4(\mathbf{x})|)}{\max(|x_1|, \ldots, |x_4|)^8} : (x_1 : \ldots : x_4) \in \mathcal{C}_\Phi(K)^\dagger \right\} = \{ |\pi|^{2\alpha} : \alpha \in A \}$$

where $\mathcal{C}_\Phi(K)^\dagger = \{ P \in \mathcal{C}_\Phi(K) : \widetilde{P} \in \Gamma \}$ and Γ is the curve over k defined by

$$\{ \widetilde{Q}_1(x_1, \ldots, x_4) = \widetilde{Q}_2(x_1, \ldots, x_4) = 0 \} \subset \mathbb{P}^3 \qquad \text{if } \texttt{Affine} = \texttt{FALSE}$$
$$\{ \widetilde{Q}_1(x,y,z,1) = \widetilde{Q}_2(x,y,z,1) = 0 \} \subset \mathbb{A}^3 \qquad \text{if } \texttt{Affine} = \texttt{TRUE}.$$

(i) Set $A = \emptyset$.

(ii) If Γ contains an absolutely irreducible component of degree 3 or 4 then set $A = \{0\}$.

(iii) Find all k-rational lines and conics that are components of Γ of multiplicity one. Compute the contribution α of each such component using Propositions 4.9 and 4.10 and put $A = A \cup \{\alpha\}$.

(iv) Find all non-regular k-points on Γ. Use a transformation in $\mathrm{GL}_4(\mathcal{O}_K)$ to move each such point to $(0:0:0:1)$ and a transformation in $\mathrm{GL}_2(\mathcal{O}_K)$ to arrange that $\frac{\partial Q_1}{\partial x_j}(0,0,0,1) \equiv 0 \pmod{\pi}$ for $1 \le j \le 4$ and $Q_1(0,0,0,1) \equiv 0 \pmod{\pi^2}$. Then compute

$$A_1 = \texttt{TamagawaDistances}(\texttt{Q1}', \texttt{Q2}', \texttt{TRUE})$$

where

$$Q_1'(x_1, \ldots, x_4) = \pi^{-2} Q_1(\pi x_1, \pi x_2, \pi x_3, x_4)$$
$$Q_2'(x_1, \ldots, x_4) = \pi^{-1} Q_2(\pi x_1, \pi x_2, \pi x_3, x_4)$$

and set $A = A \cup \{\alpha + 3 : \alpha \in A_1\}$.

(v) Return A.

4.3. **Contributions from lines and conics.** Let Φ be a non-singular genus one model over $\mathcal{O}_K$. Suppose that the reduction of $\mathcal{C}_\Phi$ mod π contains a k-rational curve C as a component of multiplicity one. (The multiplicity one condition is equivalent to requiring that all but finitely many $\overline{k}$-points on C are smooth points on the reduction.) Theorem 3.8 shows that if C has degree $n-1$ or n then the points $P \in \mathcal{C}_\Phi(K)$ whose reduction is a smooth point on C contribute $\alpha = 0$ to the set of Tamagawa distances. In this section we determine the contributions in the remaining cases, namely when $n = 3$ and C is a line, and when $n = 4$ and C is a conic or line.

Proposition 4.8. *Let $U \in \mathcal{O}_K[x, y, z]$ be a non-singular ternary cubic whose reduction contains a k-rational line L as a component of multiplicity one. Then there is an integer α such that*

$$\frac{\max(|F_3(\mathbf{x})|, |G_3(\mathbf{x})|)}{\max(|x|, |y|, |z|)^6} = |\pi|^{2\alpha}$$

for all $(x : y : z) \in \mathcal{C}_U(K)$ whose reduction is a smooth point on L. Moreover if L is the line $\{x = 0\}$ then α may be computed as follows.

- (i) *Set $\alpha = 0$.*
- (ii) *Replace U by $\pi^{-1}U(\pi x, y, z)$ and let $\alpha = \alpha + 1$.*
- (iii) *Write $U(x, y, z) = f_0x^3 + f_1(y, z)x^2 + f_2(y, z)x + f_3(y, z)$ where the f_i are binary forms of degree i. If $\widetilde{f_2} \mid \widetilde{f_3}$ say*

$$f_3(y, z) \equiv (ay + bz)f_2(y, z) \pmod{\pi}$$

  for some $a, b \in \mathcal{O}_K$ then substitute $x \leftarrow x - ay - bz$ and go to Step (ii).
- (iv) *Return α.*

Proof: Writing

$$U(x, y, z) = f_0x^3 + f_1(y, z)x^2 + f_2(y, z)x + f_3(y, z)$$

we are given that $v(f_3) \geq 1$ and $v(f_2) = 0$. If $P = (u : v : w) \in \mathcal{C}_U(K)$ reduces to a smooth point on L then $u \equiv 0$ and $f_2(v, w) \not\equiv 0 \pmod{\pi}$. In Step (ii) we replace P by $(\pi^{-1}u : v : w)$. The increase of α by 1 is justified by Theorem 4.4(ii) with $[\mu, N] = [\pi^{-1}, \mathrm{Diag}(\pi, 1, 1)]$. After this transformation we still have $f_2(v, w) \not\equiv 0 \pmod{\pi}$ but now

$$U(x, y, z) \equiv f_2(y, z)x + f_3(y, z) \pmod{\pi}.$$

Hence P reduces to a smooth point on the rational curve parametrised by

$$(s : t) \mapsto (-\widetilde{f_3}(s, t) : s\widetilde{f_2}(s, t) : t\widetilde{f_2}(s, t))$$

If $\widetilde{f_2} \mid \widetilde{f_3}$ then this is a line and the substitution in Step (iii) moves the line to $\{x = 0\}$. We then return to Step (ii). Otherwise we have a curve of degree 2 or 3 and by Theorem 3.8 there is no further contribution to the Tamagawa distance.

We show in the next section that the algorithm terminates. □

Proposition 4.9. *Let $\Phi = (Q_1, Q_2)$ be a non-singular quadric intersection over $\mathcal{O}_K$ whose reduction contains a k-rational conic C as a component of multiplicity one. Then there is an integer α such that*

$$\frac{\max(|F_4(\mathbf{x})|, |G_4(\mathbf{x})|)}{\max(|x_1|, \dots, |x_4|)^8} = |\pi|^{2\alpha}$$

for all $(x_1 : \ldots : x_4) \in \mathcal{C}_\Phi(K)$ whose reduction is a smooth point on C. Moreover if C is contained in the plane $\{x_1 = 0\}$ then α may be computed as follows.

(i) *Set $\alpha = 0$.*
(ii) *Make a $\mathrm{GL}_2(\mathcal{O}_K)$-transformation so that $\widetilde{Q}_1$ vanishes on $\{x_1 = 0\}$. Replace (Q_1, Q_2) by $(\pi^{-1}Q_1(\pi x_1, x_2, x_3, x_4), Q_2(\pi x_1, x_2, x_3, x_4))$ and let $\alpha = \alpha + 1$.*
(iii) *Write $Q_i(x_1, \ldots, x_4) = \lambda_i x_1^2 + \ell_i(x_2, x_3, x_4)x_1 + q_i(x_2, x_3, x_4)$ for $i = 1, 2$. If $\widetilde{q_1}$ belongs to the ideal generated by $\widetilde{\ell_1}$ and $\widetilde{q_2}$ say*

$$q_1 \equiv (a_2x_2 + a_3x_3 + a_4x_4)\ell_1 + bq_2 \pmod{\pi}$$

for some $a_2, a_3, a_4, b \in \mathcal{O}_K$ then substitute $x_1 \leftarrow x_1 - (a_2x_2 + a_3x_3 + a_4x_4)$ and go to Step (ii).
(iv) *Return α.*

Proof: To simplify the notation in the proof we first make a substitution in x_2, x_3, x_4 so that the conic C is parametrised by $(s : t) \mapsto (0 : s^2 : st : t^2)$.

We write $Q_i = \lambda_i x_1^2 + \ell_i(x_2, x_3, x_4)x_1 + q_i(x_2, x_3, x_4)$ for $i = 1, 2$. After the $\mathrm{GL}_2(\mathcal{O}_K)$-transformation in Step (ii) we have $v(q_1) \geq 1$. We put

$$g(s, t) = \widetilde{\ell}_1(s^2, st, t^2).$$

By the Jacobian criterion $(0 : s^2 : st : t^2)$ is a smooth point on the reduction if and only if $g(s, t) \neq 0$. Our hypothesis that C has multiplicity one is therefore equivalent to the statement that g is not identically zero.

Suppose $P = (u_1 : \ldots : u_4)$ reduces to a smooth point on C. Then (assuming $u_1, \ldots, u_4$ belong to $\mathcal{O}_K$ but not all to $\pi\mathcal{O}_K$) we have $\ell_1(u_2, u_3, u_4) \not\equiv 0 \pmod{\pi}$. In Step (ii) we replace P by $(\pi^{-1}u_1 : u_2 : u_3 : u_4)$. The increase of α by 1 is justified by Theorem 4.4(ii) with $[M, N] = [\mathrm{Diag}(\pi^{-1}, 1), \mathrm{Diag}(\pi, 1, 1, 1)]$. This transformation changes neither ℓ_1 nor q_2 but we now have

$$\begin{aligned} Q_1(x_1, \ldots, x_4) &\equiv x_1\ell_1(x_2, x_3, x_4) + q_1(x_2, x_3, x_4) \pmod{\pi} \\ Q_2(x_1, \ldots, x_4) &\equiv \qquad\qquad\qquad\qquad\quad q_2(x_2, x_3, x_4) \pmod{\pi}. \end{aligned}$$

Hence P reduces to a smooth point on the rational curve parametrised by

$$(s : t) \mapsto (-f(s, t) : g(s, t)s^2 : g(s, t)st : g(s, t)t^2)$$

where $f(s,t) = \widetilde{q}_1(s^2, st, t^2)$. Since g is not identically zero this is a curve of degree 2, 3 or 4. If it has degree 2 then in Step (iii) we move it to lie in the plane $\{x_1 = 0\}$ and return to Step (ii). Otherwise we have a curve of degree 3 or 4 and by Theorem 3.8 there is no further contribution to the Tamagawa distance.

We show in the next section that the algorithm terminates. □

Proposition 4.10. *Let $\Phi = (Q_1, Q_2)$ be a non-singular quadric intersection over $\mathcal{O}_K$ whose reduction contains a k-rational line L as a component of multiplicity one. Then there is an integer α such that*

$$\frac{\max(|F_4(\mathbf{x})|, |G_4(\mathbf{x})|)}{\max(|x_1|, \dots, |x_4|)^8} = |\pi|^{2\alpha}$$

for all $(x_1 : \dots : x_4) \in \mathcal{C}_\Phi(K)$ whose reduction is a smooth point on L. Moreover if L is the line $\{x_1 = x_2 = 0\}$ then α may be computed as follows.

(i) *Set $\alpha = 0$.*

(ii) *Replace Q_i by $\pi^{-1} Q_i(\pi x_1, \pi x_2, x_3, x_4)$ for $i = 1, 2$ and let $\alpha = \alpha + 2$.*

(iii) *Write $Q_1 = \sum_{i \le j} a_{ij} x_i x_j$ and $Q_2 = \sum_{i \le j} b_{ij} x_i x_j$, and put*

$$C = \begin{pmatrix} a_{13} & a_{23} \\ b_{13} & b_{23} \end{pmatrix}, \qquad D = \begin{pmatrix} a_{14} & a_{24} \\ b_{14} & b_{24} \end{pmatrix}.$$

Then compute $g(s,t) = \det(s\widetilde{C} + t\widetilde{D})$ and

$$\begin{pmatrix} f_1(s,t) \\ f_2(s,t) \end{pmatrix} = \operatorname{adj}(s\widetilde{C} + t\widetilde{D}) \begin{pmatrix} \widetilde{Q}_1(0,0,s,t) \\ \widetilde{Q}_2(0,0,s,t) \end{pmatrix}.$$

(iv) *If g divides both f_1 and f_2 say*

$$f_1(s,t) = (\widetilde{\lambda}_1 s + \widetilde{\mu}_1 t) g(s,t)$$
$$f_2(s,t) = (\widetilde{\lambda}_2 s + \widetilde{\mu}_2 t) g(s,t)$$

for some $\lambda_1, \lambda_2, \mu_1, \mu_2 \in \mathcal{O}_K$ then substitute $x_3 \leftarrow x_3 + \lambda_1 x_1 + \lambda_2 x_2$ and $x_4 \leftarrow x_4 + \mu_1 x_1 + \mu_2 x_2$ and go to Step (ii).

(v) *If f_1, f_2 and g have a common linear factor then solve for a linear form $\ell \in \mathcal{O}_K[x_1, \dots, x_4]$ with*

$$\widetilde{\ell}(-f_1(s,t), -f_2(s,t), g(s,t)s, g(s,t)t) = 0.$$

Make a $\mathrm{GL}_4(\mathcal{O}_K)$-transformation so that $\ell = x_1$. Then run the algorithm of Proposition 4.9 on (Q_1, Q_2) and add the answer to α.

(vi) *Return α.*

PROOF: By the Jacobian criterion $(0:0:s:t)$ is a smooth point on the reduction if and only if $g(s,t) \neq 0$, where g is as defined in Step (iii). Our hypothesis that L has multiplicity one is therefore equivalent to the statement that g is not identically zero.

Suppose $P = (u_1 : \ldots : u_4) \in \mathcal{C}_\Phi(K)$ reduces to a smooth point on L. Then (assuming $u_1, \ldots, u_4$ belong to $\mathcal{O}_K$ but not all to $\pi\mathcal{O}_K$) we have $g(\widetilde{u}_3, \widetilde{u}_4) \neq 0$. In Step (ii) we replace P by $(\pi^{-1}u_1 : \pi^{-1}u_2 : u_3 : u_4)$. The increase in α by 2 is justified by Theorem 4.4(ii) with $[M, N] = [\mathrm{Diag}(\pi^{-1}, \pi^{-1}), \mathrm{Diag}(\pi, \pi, 1, 1)]$. Solving for the first two co-ordinates of $\widetilde{P}$ in terms of the last two we find it is a smooth point on the rational curve parametrised by

$$(s:t) \mapsto (-f_1(s,t) : -f_2(s,t) : g(s,t)s : g(s,t)t).$$

Since g is not identically zero this is a curve of degree 1, 2 or 3. These cases are treated in Steps (iv),(v) and (vi).

We show in the next section that the algorithm terminates. □

4.4. **Bounds on the Tamagawa distances.** We recall from Section 1.1 that the discriminant is a certain polynomial in the coefficients of a genus one model. In this section we bound the Tamagawa distances in terms of the valuation of the discriminant. In particular this proves that our algorithms terminate. We then give an alternative description of the Tamagawa distances.

Lemma 4.11. *Let $D = (d_{ij})$ be the 2 by 5 matrix over $\mathbb{Z}[l,m,n,a,b,c,d,e]$ whose entries are the coefficients of F_2 and G_2 as defined in Section 3.1. Then*

$$\Delta = -27m_{15}^2 + 4m_{14}m_{25} - m_{13}m_{35}$$

where $m_{ij} = d_{1i}d_{2j} - d_{1j}d_{2i}$.

PROOF: A direct calculation. □

Our algorithms for computing the Tamagawa distances (see Sections 4.2 and 4.3) only make transformations that preserve the level.

Definition 4.12. Let $g \in \mathcal{G}_n(K)$ be a transformation of genus one models of degree $n \in \{2,3,4\}$, say $g = [\mu, r, N], [\mu, N]$ or $[M, N]$. Then g is a transformation of *type* r with $0 < r < n$ if $\det(g) \in \mathcal{O}_K^\times$ and the Smith normal form of N is $\mathrm{Diag}(I_{n-r}, \pi I_r)$.

We establish the following bounds on the Tamagawa distances.

Theorem 4.13. *Let Φ be a genus one model over $\mathcal{O}_K$ of degree $n \in \{2,3,4\}$. Then the set of Tamagawa distances $A(\Phi)$ is bounded by*

$$\max A(\Phi) \le \begin{cases} \frac{1}{2}v(\Delta) & \text{if } n = 2 \\ v(\Delta) & \text{if } n = 3 \\ 2v(\Delta) & \text{if } n = 4 \end{cases}$$

where $\Delta = \Delta(\Phi)$. Moreover if $v(\Delta) = 1$ then $A(\Phi) = \{0\}$.

Proof: We split into the cases $n = 2, 3, 4$.
Case $\mathbf{n} = \mathbf{2}$. Let $y^2 + P(x,z)y = Q(x,z)$ be a generalised binary quartic with coefficients l, m, n and a, b, c, d, e. By Lemma 4.11 the discriminant Δ belongs to the ideal (n^2, nd, d^2, e) in $\mathbb{Z}[l, m, n, a, b, c, d, e]$. But if α is a Tamagawa distance then (P, Q) is $\mathcal{O}_K$-equivalent to a model with $\pi^\alpha \mid n, d$ and $\pi^{2\alpha} \mid e$. Hence $\pi^{2\alpha} \mid \Delta$ and $\alpha \le \frac{1}{2}v(\Delta)$.
Case $\mathbf{n} = \mathbf{3}$. We label the coefficients of our ternary cubic as

$$\begin{aligned} U(x_1, x_2, x_3) = ax_1^3 + bx_2^3 + cx_3^3 + fx_2^2x_3 + gx_3^2x_1 + hx_1^2x_2 \\ + ix_2x_3^2 + jx_3x_1^2 + kx_1x_2^2 + mx_1x_2x_3. \end{aligned}$$

Let $I_1 = (a, h, k, b)$ and $I_2 = (b, f, i, c)$ in $\mathbb{Z}[a, b, c, \ldots, m]$. We checked using Magma that the discriminant Δ belongs to $I_1 I_2^2$.

Let α be a Tamagawa distance. Then $\alpha = \alpha_1 + 2\alpha_2$ where Algorithm 4.6 performs α_r transformations of type r. The ternary cubic passed to the subalgorithm in Proposition 4.8 is $\mathcal{O}_K$-equivalent to one with $\pi^{\alpha_1} \mid a, h, k, b$ and $\pi^{\alpha_2} \mid b, f, i, c$. Since $\Delta \in I_1 I_2^2$ it follows that $\alpha = \alpha_1 + 2\alpha_2 \le v(\Delta)$. By symmetry we also have $\Delta \in I_1^2 I_2$ and so $\alpha_1, \alpha_2 \le \frac{1}{2}v(\Delta)$. In particular if $v(\Delta) = 0$ then $\alpha = 0$.
Case $\mathbf{n} = \mathbf{4}$. In Section 3.3 we saw that the quadric intersection (Q_1, Q_2) has the same discriminant as the generalised binary quartic

$$y^2 + \mathrm{pf}(xQ_1 + zQ_2)y = \mathrm{rd}(xQ_1 + zQ_2). \tag{4.3}$$

As usual we label the coefficients l, m, n and a, b, c, d, e. By Lemma 4.11 the discriminant Δ belongs to $J_1 J_2$ where $J_1 = (n^2, nd, d^2, e)$ and J_2 is the ideal generated by the 2×2 minors of D.

Let α be a Tamagawa distance. Then $\alpha = \alpha_1 + 2\alpha_2 + 3\alpha_3$ where Algorithm 4.7 performs α_3 transformations of type 3, then α_2 transformations of type 2 and then α_1 transformations of type 1. Notice that a transformation of type r has inverse of type $4-r$. The quadric intersection passed to the subalgorithm in Proposition 4.9 is both $\mathcal{O}_K$-equivalent to a model (Q_1, Q_2) with

$$Q_2(0, x_2, x_3, x_4) \equiv 0 \pmod{\pi^{\alpha_1}},$$

and $\mathcal{O}_K$-equivalent to a model (Q_1', Q_2') with

$$Q_1'(x_1, x_2, 0, 0) \equiv Q_2'(x_1, x_2, 0, 0) \equiv 0 \pmod{\pi^{\alpha_2}}.$$

We may therefore assume that $\pi^{\alpha_1} \mid n, d$ and $\pi^{2\alpha_1} \mid e$, and (using Lemma 3.6 to check the conclusion is unaffected by an $\mathcal{O}_K$-equivalence) that (4.3) is reducible mod π^{α_2}, i.e. there are binary quadratic forms t_1 and t_2 satisfying

$$\begin{aligned} \mathrm{pf}(xQ_1 + zQ_2) &\equiv t_1(x,z) + t_2(x,z) \pmod{\pi^{\alpha_2}} \\ \mathrm{rd}(xQ_1 + zQ_2) &\equiv -t_1(x,z)t_2(x,z) \pmod{\pi^{\alpha_2}}. \end{aligned}$$

This last condition implies that the 2 by 2 minors of the matrix D in Lemma 4.11 vanish mod π^{α_2}. Since $\Delta \in J_1 J_2$ it follows that $2\alpha_1 + \alpha_2 \le v(\Delta)$. The same argument gives $2\alpha_3 + \alpha_2 \le v(\Delta)$. Hence $\alpha = \frac{1}{2}(2\alpha_1 + \alpha_2) + \frac{3}{2}(2\alpha_3 + \alpha_2) \le 2v(\Delta)$. By Lemma 4.11 we also have $\Delta \in J_2^2$ and so $\alpha_1, \alpha_2, \alpha_3 \le \frac{1}{2}v(\Delta)$. In particular if $v(\Delta) = 0$ then $\alpha = 0$.

We have shown in the cases $n = 2, 3, 4$ that if $v(\Delta) = 1$ then $A(\Phi) \subset \{0\}$. To prove equality it remains to show that any such model is K-soluble. Since $v(\Delta) = 1$ we have $v(\Delta_E) = 1$ and so by Tate's algorithm the Tamagawa number $c(E)$ is also 1. By Lemma 2.1 it suffices to prove K^{nr}-solubility and this follows by the results in [CFS]. □

Corollary 4.14. *When the input is a non-singular genus one model the algorithms in Sections 2.1, 4.2 and 4.3 terminate.*

Proof: For the algorithms in Sections 4.2 and 4.3 this is immediate from our bounds on the Tamagawa distances. Taking into account the transformations in Step (i) that immediately follow each recursion, the algorithms in Section 2.1 never increase the level. So after finitely many iterations the level is preserved. Thereafter each iteration is a transformation of type $n-1$. By the proof of Theorem 4.13 the number of such iterations is bounded by $\frac{1}{2}v(\Delta)$. □

Remark 4.15. If we think of the algorithms as performing a tree search, then Theorem 4.13 bounds the depth of the search, and Section 2.3 (on non-regular points) bounds the breadth of the search. From both points of view it is clearly desirable that we first minimise our model using the algorithms in [CFS].

For the rest of this section we assume that Φ is K-soluble and of level 0. The set of Tamagawa distances $A(\Phi)$ has the following alternative interpretation. Let $\mathcal{N}$ be the set of all matrices N in $\mathrm{GL}_n(K)$ such that for some transformation $g = [\mu, r, N]$, $[\mu, N]$ or $[M, N]$ in $\mathcal{G}_n(K)$ the model $g\Phi$ is minimal (equivalently is integral of level 0). Let $\mathcal{N}_0 \subset \mathcal{N}$ be the subset where the reduction of $g\Phi$ defines a curve with a k-rational component of multiplicity one and degree $n-1$ or n. Let G be the subgroup of $\mathrm{GL}_n(K)$ generated by $\mathrm{GL}_n(\mathcal{O}_K)$ and the scalar matrices. Then

$$A(\Phi) = \{v(\det N_i) : 1 \le i \le m\}$$

where $N_1, \ldots, N_m$ are a set of representatives for $G \setminus \mathcal{N}_0$ scaled so that each N_i has entries in $\mathcal{O}_K$ not all in $\pi\mathcal{O}_K$.

Theorem 4.13 shows that the set $G \setminus \mathcal{N}_0$ is finite. Alternatively this follows by work of Sadek [Sa] who computes $\#(G\setminus\mathcal{N})$. If $n > 2$ then the same methods show that $\#(G \setminus \mathcal{N}_0)$ is the Tamagawa number $c(E)$ of $E = \mathrm{Jac}(\mathcal{C}_\Phi)$. This is still true when $n = 2$ if we adopt the convention that models of degree 2 whose reduction mod π have two k-rational components are counted twice.

It is natural to consider the graph with vertex set $G \setminus \mathcal{N}$ and (directed) edges corresponding to the transformations of types $1, 2, \ldots, n-1$. We recall that $c(E)$ is the number of k-rational components of the special fibre of the Néron model. For each such component there is a preferred vertex where the component is seen as a curve of degree $n-1$ or n. These vertices make up the set $G \setminus \mathcal{N}_0$. We may interpret $A(\Phi)$ as the set of distances (weighted by type) from the vertex corresponding to Φ to each of these special vertices. This explains why we call $A(\Phi)$ the set of Tamagawa distances.

These graphs are investigated further in [S] with particular attention given to the case $n = 4$ and E with multiplicative reduction. These investigations suggest that the bounds in Theorem 4.13 are best possible.

4.5. **Calculation at the infinite place.** Since our examples in Section 5 are over $K = \mathbb{Q}$ we will only consider real places. (If $n = 2$ then the complex places are already treated in [CPS].)

Let Φ be a non-singular genus one model over $\mathbb{R}$ of degree $n \in \{2, 3, 4\}$. We assume $\mathcal{C}_\Phi(\mathbb{R}) \neq \emptyset$. Let F_n and G_n be the polynomials associated to Φ as defined in Section 3 and let $r \in \mathbb{R}$. In this section we compute

$$\delta(\Phi, r) = \sup_{P \in \mathcal{C}_\Phi(\mathbb{R})} \frac{\max(|F_n(\mathbf{x})|, |rF_n(\mathbf{x}) + G_n(\mathbf{x})|)}{\max(|x_1|, \ldots, |x_n|)^{2n}}$$

$$\varepsilon(\Phi, r) = \inf_{P \in \mathcal{C}_\Phi(\mathbb{R})} \frac{\max(|F_n(\mathbf{x})|, |rF_n(\mathbf{x}) + G_n(\mathbf{x})|)}{\max(|x_1|, \ldots, |x_n|)^{2n}}$$

where $P = (x_1 : x_2 : y)$ or $(x_1 : \ldots : x_n)$. These definitions are slightly more general than those in Section 4.1 as previously we took $r = 0$.

Proposition 4.16. *We can compute $\delta(\Phi, r)$, respectively $\varepsilon(\Phi, r)$, by taking the maximum, respectively minimum, over all points $P \in \mathcal{C}_\Phi(\mathbb{R})$ satisfying one of the following conditions:*

(i) *$P = (x_1 : \ldots : x_n)$ with $x_i = \pm x_j$ for some $i \neq j$,*
(ii) *$F_n(P) = \pm(rF_n(P) + G_n(P))$,*
(iii) *$n = 2$ and $F_2(P) = 0$,*

(iv) *according as* $n = 2, 3, 4$,

$$\frac{\partial f}{\partial x_i}(P) = 0, \qquad \frac{\partial(U, f)}{\partial(x_i, x_j)}(P) = 0, \qquad \frac{\partial(Q_1, Q_2, f)}{\partial(x_i, x_j, x_k)}(P) = 0,$$

where $f = F_n$ *or* $rF_n + G_n$ *and* i, j, k *are distinct.*

Proof: Since $\mathcal{C}_\Phi(\mathbb{R})$ is non-empty we may identify it as the real locus of an elliptic curve. In particular it is isomorphic as a smooth real manifold to either one or two copies of the circle $\mathbb{R}/\mathbb{Z}$. We are asked to find the maxima and minima of a continuous real-valued function on this manifold. In (i) and (ii) we consider the points where this function is not differentiable, and in (iii) and (iv) we consider the points where its derivative vanishes. We recall by Theorem 3.8 that there are no points $P \in \mathcal{C}_\Phi$ with $F_n(P) = G_n(P) = 0$. Condition (iii) is needed since after completing the square $\mathcal{C}_\Phi$ has equation $y^2 = F_2(x_1, x_2)$. □

We check that the set of points P in Proposition 4.16 is finite. In case (i) it suffices to note (by Bezout's theorem) that $\mathcal{C}_\Phi$ has finite intersection with any hyperplane. In cases (ii) and (iii) we recall that $(F_n : G_n)$ defines a non-constant morphism $\mathcal{C}_\Phi \to \mathbb{P}^1$ and therefore has finite fibres. If there were infinitely many points P satisfying one of the conditions in case (iv) then (after permuting the co-ordinates if necessary) we would have

$$\lambda F_n + \mu G_n \equiv x_1^{2n} \pmod{I}$$

for some $(\lambda : \mu) \in \mathbb{P}^1(\mathbb{R})$, where $I = 0$, (U), (Q_1, Q_2) according as $n = 2, 3, 4$. In particular the form

$$\frac{\partial(F_2, G_2)}{\partial(x_1, x_2)} \quad \text{or} \quad \frac{\partial(U, F_3, G_3)}{\partial(x_1, x_2, x_3)} \quad \text{or} \quad \frac{\partial(Q_1, Q_2, F_4, G_4)}{\partial(x_1, x_2, x_3, x_4)}$$

would be divisible by x_1^{2n-1}. However the invariant theory in Section 3 shows that these forms meet $\mathcal{C}_\Phi$ in distinct points: namely $\pi^{-1}(E[2] \setminus \{0\})$ in the case $n = 2$ and $\pi^{-1}(E[2])$ in the cases $n = 3, 4$. This is the required contradiction.

Proposition 4.16 allows us to compute $\delta(\Phi, r)$ and $\varepsilon(\Phi, r)$ numerically. The case $n = 2$ is already covered in [Si2], [CPS]. See [S, Section 2.5] for a worked example. In the cases $n = 3, 4$ we use the Gröbner basis machinery in Magma. In Section 5 we consider models over $\mathbb{Q}$, so the Gröbner bases can be computed exactly.

5. Examples

5.1. **Explicit bounds.** Let $E/\mathbb{Q}$ be an elliptic curve with global minimal Weierstrass equation (1.2) and discriminant Δ_E. Let $\mathcal{C} = \mathcal{C}_\Phi$ be an n-covering of E, where Φ is a non-singular genus one model of degree $n \in \{2, 3, 4\}$. We assume that $\mathcal{C}(\mathbb{Q}_p) \neq \emptyset$ and Φ is minimal at all primes p. Therefore by [CFS, Theorem 3.4] we have $\Delta(\Phi) = \Delta_E$. In particular $\mathcal{C}$ and E have the same primes of bad reduction.

In Sections 4.2 and 4.3 we computed a finite set of integers $A_p = A_p(\Phi)$ at each bad prime p. The Weierstrass equations (1.2) and (3.1) are related by a substitution

$$x \leftarrow x + r \qquad y \leftarrow y + sx + t$$

for some $r, s, t \in \mathbb{Z}$. In Section 4.5 we computed the real contributions $\delta_\infty(\Phi, r)$ and $\varepsilon_\infty(\Phi, r)$. The height bounds B_1 and B_2 in (1.1) are now given by

$$B_1 = -(1/2n) \log \delta_\infty(\Phi, r) + (1/n) \sum_{p \mid \Delta_E} \min A_p(\Phi) \log p$$
$$B_2 = -(1/2n) \log \varepsilon_\infty(\Phi, r) + (1/n) \sum_{p \mid \Delta_E} \max A_p(\Phi) \log p$$

This follows from (4.1) and (4.2), except that in changing our choice of Weierstrass equation (from that given by the a-invariants to a standard one) we must replace G_n by $rF_n + G_n$. This makes no change at the finite places since $r \in \mathbb{Z}$.

By Theorem 4.13 we need only sum over primes p with $p^2 \mid \Delta_E$.

5.2. **A first example.** Let E be the elliptic curve $y^2 + y = x^3 - 41079x - 2440008$ labelled 120267g1 in [Cr]. The primes of bad reduction are $p = 3, 7, 23, 83$ with Kodaira symbols $\mathrm{I}_4^*, \mathrm{I}_4, \mathrm{I}_1, \mathrm{I}_3$ and Tamagawa numbers $4, 4, 1, 3$. The group $E(\mathbb{Q})$ is free of rank 2 generated by $(-106, 850)$ and $(-157, 373)$.

Among the coverings of E computed using n-descent for $n = 2, 3, 4$ we choose the following for illustration.

$$\mathcal{C}_2 : \quad y^2 + z^2 y = -5x^4 - 171x^3 z + 78x^2 z^2 + 216xz^3 - 106z^4$$
$$\mathcal{C}_3 : \quad 12x^2y - 9x^2z + 9xy^2 - 12xyz + 7y^3 + 10y^2z - 17yz^2 - 6z^3 = 0$$
$$\mathcal{C}_4 : \quad \left\{ \begin{array}{rcl} x_1x_2 + x_1x_3 + 3x_1x_4 + x_2x_3 - 4x_2x_4 + x_3^2 + 6x_3x_4 + 2x_4^2 & = & 0 \\ 3x_1x_3 + 3x_1x_4 - x_2^2 + x_2x_3 - 9x_3^2 + 4x_3x_4 + x_4^2 & = & 0 \end{array} \right.$$

The sets of Tamagawa distances A_p are as follows. We compute these as multisets so that, as a check on our calculations, the size of A_p is equal to the Tamagawa number. (See the comments at the end of Section 4.4.)

$n = 2$	$n = 3$	$n = 4$
$A_3 = \{0, 0, 1, 1\}$	$A_3 = \{2, 3, 3, 4\}$	$A_3 = \{2, 4, 6, 8\}$
$A_7 = \{0, 0, 1, 1\}$	$A_7 = \{1, 1, 1, 2\}$	$A_7 = \{1, 2, 3, 4\}$
$A_{23} = \{0\}$	$A_{23} = \{0\}$	$A_{23} = \{0\}$
$A_{83} = \{0, 0, 1\}$	$A_{83} = \{0, 1, 2\}$	$A_{83} = \{1, 2, 2\}$

Combining these with the contributions at the infinite place we obtain the following bounds on the height of $P_n \in \mathcal{C}_n(\mathbb{Q})$ mapping down to $P \in E(\mathbb{Q})$.

$$-3.06805 \leq h(P_2) - \tfrac{1}{4}h_E(P) \leq 1.21943$$
$$-2.80610 \leq h(P_3) - \tfrac{1}{6}h_E(P) \leq 2.44241$$
$$-3.08885 \leq h(P_4) - \tfrac{1}{8}h_E(P) \leq 2.48228$$

The curves $\mathcal{C}_n$ have many small rational points. We list a few of these together with their contributions to the Tamagawa distances (at $p = 3, 7, 83$) and the height difference $h(P) - \frac{1}{2n}h_E(\pi P)$.

	P	$p = 3$	$p = 7$	$p = 83$	$h(P) - \frac{1}{2n}h_E(\pi P)$
	$(1:1:3)$	0	1	0	-1.68305
	$(2:3:37)$	0	0	1	-0.30284
$n = 2$	$(6:-1:178)$	1	1	0	-1.08967
	$(27:-1:871)$	1	1	1	1.14846
	$(769:787:2143781)$	0	0	0	-2.63972
	$(1:0:0)$	4	1	0	-1.15212
	$(1:-1:-1)$	3	1	0	-2.16072
$n = 3$	$(2:-3:1)$	2	2	0	-1.74660
	$(2:18:15)$	4	2	2	1.96488
	$(1:-6:20)$	2	1	0	-2.38783
	$(1:0:0:0)$	4	2	1	-0.70073
	$(-2:5:2:7)$	2	4	1	-1.54491
$n = 4$	$(-3:3:1:8)$	6	3	1	-0.80265
	$(557:544:-134:470)$	2	2	1	-2.31493
	$(157397:2728:1502:-1438)$	8	3	2	1.99552

5.3. **Searching for generators of large height.** We give two examples. The first is an example where the generator was found by Michael Stoll using 4-descent (see [CFS, Section 7C]). The elliptic curve E in the second example is taken from a list of curves sent to us by Robert Miller. Although in both these examples the elliptic curve has rank 1, the conductor is large enough to make a Heegner point calculation difficult.

Example 5.1. Let $E/\mathbb{Q}$ be the elliptic curve $y^2 = x^3 + 7823$. An L-value computation shows that rank $E(\mathbb{Q}) = 1$ and the generator is predicted to have canonical height $h_1 = 77.61777\ldots$ (if we assume $\text{Ш}(E/\mathbb{Q})$ is trivial).

Using the implementations of 2-, 3- and 4-descent in Magma, together with minimisation and reduction, we obtain the following n-coverings of E.

$$\mathcal{C}_2: \quad y^2 + (x^2+z^2)y = -3x^4 + 28x^3z - 2x^2z^2 - 4xz^3 + 10z^4$$

$$\mathcal{C}_3: \quad x^3 + x^2y - 4x^2z - 8xyz + 8xz^2 + y^3 - 5y^2z - 7yz^2 + z^3 = 0$$

$$\mathcal{C}_4: \quad \begin{cases} 2x_1x_2 + x_1x_3 + x_1x_4 + x_2x_4 + x_3^2 - 2x_4^2 = 0 \\ x_1^2 + x_1x_3 - x_1x_4 + 2x_2^2 - x_2x_3 + 2x_2x_4 - x_3^2 - x_3x_4 + x_4^2 = 0 \end{cases}$$

At each of the bad primes $p = 2, 3, 7823$ the elliptic curve E has additive reduction with Kodaira symbol II. The finite primes make no contribution to our height bounds. If $P_n \in \mathcal{C}_n(\mathbb{Q})$ maps down to $P \in E(\mathbb{Q})$ then our bounds work out as

$$\begin{aligned} -1.94921 \le & h(P_2) - \tfrac{1}{4}h_E(P) \le -0.92414 \\ -2.91485 \le & h(P_3) - \tfrac{1}{6}h_E(P) \le -1.41177 \\ -3.66288 \le & h(P_4) - \tfrac{1}{8}h_E(P) \le -2.43592 \end{aligned}$$

The bounds established in [CPS] show that for $P \in E(\mathbb{Q})$ we have

$$-3.68143 \le h_E(P) - \widehat{h}_E(P) \le 0.74248$$

where $\widehat{h}_E$ is the canonical height. We write $P_n = (x_1 : x_2 : y)$, respectively $(x_1 : \ldots : x_n)$, where $x_1, \ldots, x_n$ are coprime integers. Taking $\widehat{h}_E(P) = h_1$ we therefore expect to find $P_n \in \mathcal{C}_n(\mathbb{Q})$ with $H_n = \max(|x_1|, \ldots, |x_n|)$ in the following ranges. For comparison we list the actual points P_n.

$$\begin{array}{ll} 15170781 \le H_2 \le 127792792 & P_2 = (10677130 : -42786483 : 5018494588774686) \\ 12185 \le H_3 \le 114492 & P_3 = (10445 : -32922 : 16423) \\ 265 \le H_4 \le 1570 & P_4 = (116 : 207 : 474 : -332) \end{array}$$

Example 5.1 makes precise the statement that searching on an n-covering to find a generator for $E(\mathbb{Q})$ becomes easier as n increases. For the actual searching we use the p-adic method due to Elkies [E] and Heath-Brown, as implemented in Magma by Watkins. This takes time $O(H)$, respectively $O(H^{2/3})$, to search for points of height up to H on a 3-covering, respectively 4-covering.

Example 5.2. Let E_0 be the elliptic curve $y^2 + xy + y = x^3 - x^2 - 2305x + 43447$, labelled 3850m1 in [Cr], and E the quadratic twist of E_0 by $d = -2351$. We fix a Weierstrass equation for E of the form (1.2). The primes of bad reduction are $p = 2, 5, 7, 11, 2351$ with Kodaira symbols $\mathrm{I}_1, \mathrm{II}^*, \mathrm{I}_2, \mathrm{I}_1, \mathrm{I}_0^*$ and Tamagawa numbers $1, 1, 2, 1, 2$. An L-value computation shows that rank $E(\mathbb{Q}) = 1$ and the generator is predicted to have canonical height $h_1 = 182.01408\ldots$ (if we assume $\text{Ш}(E/\mathbb{Q})$ is trivial). The torsion subgroup of $E(\mathbb{Q})$ is trivial.

Using 4-descent in Magma we obtain a 4-covering $\mathcal{C}_4$ of E with equations

$$3x_1^2 + 17x_1x_2 + x_1x_3 + 7x_1x_4 - 5x_2^2 + 11x_2x_3 + 6x_2x_4 + 5x_3^2 + 9x_4^2 = 0$$
$$10x_1^2 + 7x_1x_2 - x_1x_3 - x_1x_4 + 4x_2^2 - x_2x_3 - 13x_2x_4 + 14x_3^2 - 30x_3x_4 + 18x_4^2 = 0$$

The Tamagawa distances for this quadric intersection are $A_2 = A_{11} = \{0\}$, $A_5 = \{6\}$, $A_7 = \{1,1\}$ and $A_{2351} = \{4,4\}$. For $P_4 \in \mathcal{C}_4(\mathbb{Q})$ we obtain the bounds

$$0.65550 \le h(P_4) - \tfrac{1}{8}h_E(\pi P_4) \le 0.94857.$$

The bounds in [CPS] are now $-15.51194 \le h_E(P) - \widehat{h}_E(P) \le 8.73556$. We are therefore looking for $P_4 \in \mathcal{C}_4(\mathbb{Q})$ with

$$21.46827 \le h(P_4) \le 24.79228.$$

A direct search is not practical. However our computation of the Tamagawa distances at $p = 5$ and $p = 2351$ suggests replacing $\mathcal{C}_4$ by either $\mathcal{C}_4'$ with equations

$$3x_1^2 + 3x_1x_2 + 4x_1x_3 + 6x_1x_4 + 3x_2^2 - 3x_2x_3 + 2x_2x_4 + 6x_3^2 - 28x_3x_4 + 11x_4^2 = 0$$
$$4x_1^2 + x_1x_2 - 7x_1x_3 + 9x_1x_4 - 4x_2^2 - 8x_2x_3 + 38x_2x_4 + 31x_3^2 + 14x_3x_4 + 16x_4^2 = 0$$

or $\mathcal{C}_4''$ with equations

$$2x_1^2 + 4x_1x_2 + 10x_1x_3 + 3x_1x_4 - 3x_2^2 - 2x_2x_3 - 6x_2x_4 - 5x_3^2 - 10x_3x_4 - 21x_4^2 = 0$$
$$14x_1^2 + x_1x_2 + 11x_1x_3 - 11x_1x_4 + 2x_2^2 + 25x_2x_3 + 15x_2x_4 - 2x_3^2 - 24x_3x_4 + 12x_4^2 = 0.$$

Again we have reduced these models as described in [CFS]. We do not record the changes of co-ordinates used, since they may easily be recovered using the algorithm in [F2], as implemented in the Magma function `IsEquivalent`.

On $\mathcal{C}_4'$ and $\mathcal{C}_4''$ we have $A_2 = A_5 = A_{11} = \{0\}$, $A_7 = \{1,1\}$ and $A_{2351} = \{0,4\}$. So the only finite primes to contribute to our height bounds are $p = 7$ and $p = 2351$. Moreover if we are willing to search on both curves then the contributions at $p = 2351$ may be ignored. Suppose $P_4 \in \mathcal{C}_4(\mathbb{Q})$, corresponds to $P_4' \in \mathcal{C}_4'(\mathbb{Q})$ and $P_4'' \in \mathcal{C}_4''(\mathbb{Q})$, and maps down to $P \in E(\mathbb{Q})$. Then depending on the reductions of these points mod 2351, we have either

$$-9.65955 \le h(P_4') - \tfrac{1}{8}h_E(P) \le -9.29236 \tag{5.1}$$

or

$$-9.72818 \le h(P_4'') - \tfrac{1}{8}h_E(P) \le -9.35987. \tag{5.2}$$

Taking $\widehat{h}_E(P) = h_1$ it follows that either

$$11.15322 \le h(P_4') \le 14.55134 \quad \text{or} \quad 11.08459 \le h(P_4'') \le 14.48383.$$

If we are willing to search on only one of these curves then the upper bounds increase by $\log 2351 = 7.76259\ldots$.

Magma's `PointSearch` takes just a few seconds to find a point $P_4'' \in \mathcal{C}_4''(\mathbb{Q})$. We find the corresponding points $P_4 \in \mathcal{C}_4(\mathbb{Q})$ and $P_4' \in \mathcal{C}_4'(\mathbb{Q})$ by making the relevant changes of co-ordinates, and thus obtain

$$\begin{aligned} P_4 &= (-32083748086 : 42638879317 : 38411124781 : 22127244455) & h(P_4) &= 24.47603\ldots \\ P_4' &= (472320823 : 4111701909 : -2388802174 : -2139378517) & h(P_4') &= 22.13710\ldots \\ P_4'' &= (785047 : -840912 : 1542460 : -236990) & h(P_4'') &= 14.24888\ldots \end{aligned}$$

These points map down to $P = (u/w^2, v/w^3) \in E(\mathbb{Q})$ where

$$\begin{aligned} u &= 175728793690502532825333156071827234024273934992644702509442858 8\backslash \\ &\quad 4833392724486595115 \\ v &= 41250774324940490011744417755978803448069175034652424472575958 90\backslash \\ &\quad 8353083565737309347095830251104254424513602652951188 8663249 \\ w &= 3644365472926088194685733359379575 48482. \end{aligned}$$

If $P_0 \in E(\mathbb{Q})$ is a generator then (assuming we have carried out the 4-descent rigorously) it lifts to a rational point on $\mathcal{C}_4$. Combining our height bounds (5.1) and (5.2) with those in [CPS] it follows that

$$\widehat{h}_E(P_0) \geq 8 \times 9.29236 - 8.73556 = 65.60332.$$

Since $\widehat{h}_E(P) = 182.01408\ldots$ we deduce (without the need for any further searching) that P is a generator for $E(\mathbb{Q})$.

Example 5.2 shows the advantages of searching on several different models of the same curve. One strategy would be to search on $\prod_p c_p(E)$ models of each curve, so that only the contributions to our height bounds at the infinite place are relevant. (These contributions do not appear to vary greatly between the models, so long as we always reduce them.) However when $\prod_p c_p(E)$ is large then some compromise is needed and for this the graphs in [S] are useful. Alternatively it may be possible to adapt the p-adic point searching method to search on several models of the same curve simultaneously.

Acknowledgements

This article is based on the second author's PhD thesis. We would like to thank Mohammad Sadek for many useful discussions. All computer calculations in support of this work were performed using Magma [BCP].

References

[ARVT] M. Artin, F. Rodriguez-Villegas and J. Tate, On the Jacobians of plane cubics, *Adv. Math.* **198** (2005), no. 1, 366–382.

[AKM^{3}P] 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.

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

[BCP] W. Bosma, J. Cannon and C. Playoust, The MAGMA algebra system I: The user language, *J. Symb. Comb.* **24**, (1997) 235–265. (See also the MAGMA home page at `http://magma.maths.usyd.edu.au/magma/`.)

[Bro] T. Bromwich, *Quadratic forms and their classification by means of invariant-factors*, Reprint of the 1906 edition, Cambridge Tracts in Mathematics and Mathematical Physics, Hafner Publishing Co., New York, 1971.

[Bru] N. Bruin, Some ternary Diophantine equations of signature $(n, n, 2)$, *Discovering mathematics with Magma*, 63–91, Algorithms Comput. Math., 19, Springer, Berlin, 2006.

[Ca] J.W.S. Cassels, Arithmetic on curves of genus 1, IV. Proof of the Hauptvermutung, *J. Reine Angew. Math.* **211** 1962 95–112.

[Cr] J.E. Cremona, *Algorithms for modular elliptic curves*, Second edition, Cambridge University Press, Cambridge, 1997. (See also the tables at `http://www.warwick.ac.uk/staff/J.E.Cremona/ftp/data/`.)

[Cre] B.M. Creutz, *Explicit second p-descent on elliptic curves*, PhD thesis, Jacobs University Bremen, 2010.

[CFOSS] J.E. Cremona, T.A. Fisher, C. O'Neil, D. Simon and M. Stoll, Explicit n-descent on elliptic curves, I Algebra *J. reine angew. Math.* **615** (2008) 121-155; II Geometry *J. reine angew. Math.* **632** (2009), 63–84; *III Algorithms*, in preparation.

[CFS] J.E. Cremona, T.A. Fisher and M. Stoll, Minimisation and reduction of 2-, 3- and 4-coverings of elliptic curves, to appear in *Algebra & Number Theory*.

[CPS] 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.

[Dol] I. Dolgachev, Lectures on invariant theory, LMS Lecture Note Series, 296, CUP, Cambridge, 2003.

[Don] S. Donnelly, *Computing the Cassels-Tate pairing*, in preparation.

[DLLP] L. Dupont, D. Lazard, S. Lazard and S. Petitjean, Near-optimal parameterization of the intersection of quadrics, II. A classification of pencils, *J. Symbolic Comput.* **43** (2008), no. 3, 192–215.

[E] 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.

[F1] T.A. Fisher, The invariants of a genus one curve, *Proc. Lond. Math. Soc.* (3) 97 (2008), no. 3, 753–782.

[F2] T.A. Fisher, Some improvements to 4-descent on an elliptic curve, in *Algorithmic number theory*, A. van der Poorten, A. Stein (eds.), Lecture Notes in Comput. Sci., **5011**, Springer, 2008.

[F3] T.A. Fisher, *The Hessian of a genus one curve*, preprint.

[F4] T.A. Fisher, *Higher descents on an elliptic curve with a rational* 2*-torsion point*, in preparation.

[HS] M. Hindry and J.H. Silverman, *Diophantine geometry, An introduction*, Graduate Texts in Mathematics, **201**, Springer-Verlag, New York, 2000.

[HP] W.V.D. Hodge and D. Pedoe, *Methods of algebraic geometry*, Volume II, Reprint of the 1952 original, Cambridge University Press, Cambridge, 1994.

[M] J.S. Milne, *Arithmetic duality theorems*, Second edition, BookSurge, LLC, Charleston, SC, 2006.

[MSS] J. R. Merriman, S. Siksek and N. P. Smart, Explicit 4-descents on an elliptic curve. *Acta Arith.* **77** (1996), no. 4, 385–404.

[Sa] M.M. Sadek, *Models of genus one curves*, PhD thesis, University of Cambridge, 2009.

[SS] E.F. Schaefer, M. Stoll, How to do a p-descent on an elliptic curve, *Trans. Amer. Math. Soc.* **356 no. 3** (2004), 1209–1231

[Si1] S. Siksek, *Descent on curves of genus one*, PhD thesis, University of Exeter, 1995. `http://www.warwick.ac.uk/staff/S.Siksek/papers/phdnew.pdf`

[Si2] S. Siksek, Infinite descent on elliptic curves, *Rocky Mountain J. Math.* **25** (1995), no. 4, 1501–1538.

[S] G.F. Sills, *Height bounds for n-coverings*, PhD thesis, University of Cambridge, 2010.

[Sta] S. Stamminger, *Explicit 8-descent on elliptic curves*, PhD thesis, International University Bremen, 2005.

[Sto] M. Stoll, *Descent on elliptic curves*, lecture notes, `arXiv:math/0611694v1[math.NT]`

[W] T. Womack, *Explicit descent on elliptic curves*, PhD thesis, University of Nottingham, 2003. `http://www.warwick.ac.uk/staff/J.E.Cremona/`

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

University of Cambridge, DPMMS, Centre for Mathematical Sciences, Wilberforce Road, Cambridge CB3 0WB, UK
E-mail address: `gs300@cantab.net`