A NEW APPROACH TO MINIMISING BINARY QUARTICS AND TERNARY CUBICS

TOM FISHER

Abstract. We prove a theorem on the minimisation of genus one curves, generalising work of Birch and Swinnerton-Dyer [3], Cremona and Serf [5], [13] and Cremona and Stoll [6], [7]. The advantage of our approach over earlier methods is that we do not need to treat residue characteristics 2 and 3 as special cases. This work has applications to descent calculations on elliptic curves and to the study of the Tate-Shafarevich group.

1. Invariants

Let C be a smooth curve of genus one defined over a field K, and let D be a K-rational divisor on C of degree $n \geq 2$. We write $[D]$ for the linear equivalence class of D.

1.1. **Binary quartics.** If $n = 2$ then we pick $x, y \in K(C)$ such that $\mathcal{L}(D)$ and $\mathcal{L}(2D)$ have bases $1, x$ and $1, x, x^2, y$. The 9 elements $1, x, x^2, y, x^3, xy, x^4, x^2y, y^2$ in the 8 dimensional vector space $\mathcal{L}(4D)$ satisfy a linear dependence relation. Furthermore the coefficient of y^2 is non-zero. We deduce that the pair $(C, [D])$ has an equation

$$y^2 + (\alpha_0 x^2 + \alpha_1 x + \alpha_2)y = ax^4 + bx^3 + cx^2 + dx + e. \tag{1}$$

If $\mathrm{char}\,(K) \neq 2$ then we may complete the square so that $\alpha_0 = \alpha_1 = \alpha_2 = 0$. The classical invariants of the binary quartic

$$f(x, z) = ax^4 + bx^3z + cx^2z^2 + dxz^3 + ez^4$$

are

$$\begin{aligned} I &= 12ae - 3bd + c^2, \\ J &= 72ace - 27ad^2 - 27b^2e + 9bcd - 2c^3. \end{aligned}$$

We define the invariants c_4 and c_6 of (1) by taking $c_4 = 2^4 I$ and $c_6 = 2^5 J$ in the case $\alpha_0 = \alpha_1 = \alpha_2 = 0$. We then extend to the general case by demanding that c_4 and c_6 are preserved by all changes of co-ordinates of the form $y \mapsto y + r_0x^2 + r_1x + r_2$. In addition we put $\Delta = (c_4^3 - c_6^2)/1728$. We find that c_4, c_6 and Δ are primitive integer coefficient polynomials

Date: 12th May 2006.

in the indeterminates $\alpha_0, \alpha_1, \alpha_2, a, b, c, d, e$. This enables us define the invariants c_4, c_6 and Δ in arbitrary characteristic. Moreover if we put

$$(\alpha_0, \alpha_1, \alpha_2, a, b, c, d, e) = (0, a_1, a_3, 0, 1, a_2, a_4, a_6)$$

then our expressions for c_4, c_6 and Δ reduce to the standard formulae for an elliptic curve in Weierstrass form (recalled in §4.1). It is convenient to rewrite (1) as a homogeneous equation of degree 4, where x, z, y are assigned degrees $1, 1, 2$.

$$(2) \quad y^2 + (\alpha_0 x^2 + \alpha_1 xz + \alpha_2 z^2)y = ax^4 + bx^3 z + cx^2 z^2 + dxz^3 + ez^4.$$

By abuse of terminology we refer to (2) as a binary quartic.

1.2. **Ternary cubics.** If $n = 3$ then we pick a basis x, y, z for $\mathcal{L}(D)$. Writing down 10 elements in the 9 dimensional vector space $\mathcal{L}(3D)$ we deduce that $(C, [D])$ is defined by a ternary cubic

$$\begin{aligned} F(x, y, z) \;\; = \;\; & ax^3 + by^3 + cz^3 + a_2 x^2 y + a_3 x^2 z \\ & + b_1 xy^2 + b_3 y^2 z + c_1 xz^2 + c_2 yz^2 + mxyz. \end{aligned}$$

The Hessian of the ternary cubic $F(x_1, x_2, x_3)$ is

$$H(x_1, x_2, x_3) = -1/2 \times \det \left(\frac{\partial^2 F}{\partial x_i \partial x_j} \right)_{i,j=1}^{3}.$$

The factor $-1/2$, although not standard, is a convenient choice. The Hessian of any linear combination of F and H again belongs to the pencil spanned by F and H. Following [8], [12], the invariants c_4 and c_6 are determined by the relation

$$H(\lambda F + \mu H) = 3(c_4 \lambda^2 \mu + 2c_6 \lambda \mu^2 + c_4^2 \mu^3)F + (\lambda^3 - 3c_4 \lambda \mu^2 - 2c_6 \mu^3)H.$$

In addition we put $\Delta = (c_4^3 - c_6^2)/1728$. We find that c_4, c_6 and Δ are primitive integer coefficient polynomials in the indeterminates $a, b, c, a_2, a_3, b_1, b_3, c_1, c_2, m$. This enables us to define the invariants c_4, c_6 and Δ in arbitrary characteristic. Moreover if we put

$$(a, b, c, a_2, a_3, b_1, b_3, c_1, c_2, m) = (-1, 0, -a_6, 0, -a_2, 0, 1, -a_4, a_3, a_1)$$

then our expressions for c_4, c_6 and Δ reduce to the standard formulae for an elliptic curve in Weierstrass form (recalled in §4.1).

1.3. **Computing the Jacobian.** It was observed by Weil [16] that the invariants of a binary quartic may be used to compute its Jacobian. The generalisation to ternary cubics may be found in [1].

Theorem 1.1. *Let c_4, c_6 and Δ be the invariants of a binary quartic, respectively a ternary cubic.*
(a) The binary quartic, respectively ternary cubic, defines a smooth curve of genus one if and only if $\Delta \neq 0$.
(b) If $\mathrm{char}\,(K) \neq 2, 3$ *then the Jacobian has Weierstrass equation*

$$y^2 = x^3 - 27c_4x - 54c_6. \tag{3}$$

Notice that (3) has invariants 6^4c_4, 6^6c_6 and $6^{12}\Delta$. As pointed out in [2] these formulae for the Jacobian can be improved by minimising at 2 and 3. We give details in Appendix A.

1.4. **Equivalence of models.**

Definition 1.2. We say that a pair of binary quartics, respectively ternary cubics, are *equivalent* if they arise from the same pair $(C, [D])$.

More concretely, binary quartics are equivalent if they are related by making a substitution of the form

$$\begin{aligned} x &= \alpha x' + \beta z' \\ z &= \gamma x' + \delta z' \\ y &= \mu^{-1}y' + r_0x'^2 + r_1x'z' + r_2z'^2 \end{aligned}$$

and then multiplying through by μ^2. This transformation is denoted $[\mu, r, A]$ where $r = (r_0, r_1, r_2)$ and

$$A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}.$$

Similarly, ternary cubics are equivalent if they are related by making a substitution of the form

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = A \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix}$$

and then multiplying through by μ. This transformation is denoted $[\mu, A]$. In both cases we put $\lambda = \mu \det A$ and find $c_4' = \lambda^4 c_4$, $c_6' = \lambda^6 c_6$ and $\Delta' = \lambda^{12}\Delta$.

2. Statement of global results

Let E be an elliptic curve defined over a number field K with ring of integers $\mathcal{O}_K$ and class number h_K. We write $[n]$ for the multiplication-by-n map on E.

Definition 2.1. An n-covering of E is a smooth curve of genus one C defined over K equipped with a morphism $\pi : C \to E$ defined over K, such that $\pi = [n] \circ \psi$ for some isomorphism $\psi : C \simeq E$ defined over $\overline{K}$.

Giving C the structure of n-covering of its Jacobian is equivalent to specifying a K-rational divisor class $[D]$ on C of degree n. Indeed given an n-covering $\pi : C \to E$ with $\pi = [n] \circ \psi$ we put $D = \psi^*(n.0_E)$. Conversely given D we define $\pi : C \to \mathrm{Pic}^0 C = E; P \mapsto [n.P - D]$. We say that an n-covering has trivial obstruction if it is possible to represent the given divisor class by a K-rational divisor D. In the cases $n = 2, 3$ this is the condition for the n-covering to have an equation of the form described in §1.

We are ready to state our main theorem.

Theorem 2.2. *Let E be an elliptic curve defined over a number field K, with $\mathcal{O}_K$-coefficient Weierstrass equation*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{4}$$

(i) Assume $(h_K, 2) = 1$. If C is an everywhere locally soluble 2-covering of E, then C has an $\mathcal{O}_K$-coefficient equation

$$y^2 + (\alpha_0x^2 + \alpha_1x + \alpha_2)y = ax^4 + bx^3 + cx^2 + dx + e \tag{5}$$

with the same invariants c_4, c_6 and Δ as (4).
(ii) Assume $(h_K, 3) = 1$. If C is an everywhere locally soluble 3-covering of E, then C has an $\mathcal{O}_K$-coefficient equation

$$ax^3+by^3+cz^3+a_2x^2y+a_3x^2z+b_1xy^2+b_3y^2z+c_1xz^2+c_2yz^2+mxyz = 0$$

with the same invariants c_4, c_6 and Δ as (4).

We give examples in Appendix B to show that the hypothesis on the class number cannot be removed.

Theorem 2.2 is most fruitfully applied in conjunction with the standard techniques for computing local and (where possible) global minimal Weierstrass equations. In the case $K = \mathbb{Q}$ we refer to [4, §3.2]. For K a general number field one should consult the original papers of Kraus, Connell, Laska and Tate cited there. Tate's algorithm, which provides more detailed local information, is also described in [15]. A discussion of the passage from local to global in this context may be found in [14, Chapter VIII,§8].

Remark 2.3. By completing the square, Theorem 2.2(i) implies a weaker version where $\alpha_0 = \alpha_1 = \alpha_2 = 0$, but the binary quartic (5) has invariants 2^4c_4, 2^6c_6, $2^{12}\Delta$ for c_4, c_6, Δ the invariants of (4).

Remark 2.4. Theorem 2.2 constructs a model for C with exactly the same invariants as (4). If our models for C and E have invariants c_4', c_6', Δ' and c_4, c_6, Δ, then an apparently weaker version would give that Δ' divides Δ in $\mathcal{O}_K$. In fact the full result may be deduced from this. Indeed Theorem 1.1 gives $c_4' = \lambda^4c_4$, $c_6' = \lambda^6c_6$ and $\Delta' = \lambda^{12}\Delta$ for some

$\lambda \in K^\times$. So once we know $\lambda^{-1} \in \mathcal{O}_K$, we can reduce to the case $\lambda = 1$ by rescaling, say, the x co-ordinate of our model for C.

We recall a standard definition.

Definition 2.5. Let E be an elliptic curve defined over a number field K. The minimal discriminant $\mathcal{D}_{E/K}$ is the integral ideal of K generated by all the $\Delta(a_1, a_2, a_3, a_4, a_6)$ as

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

ranges over all $\mathcal{O}_K$-coefficient Weierstrass equations for E.

The minimal discriminant $\mathcal{D}_{C/K}$ of a 2-covering or 3-covering C with trivial obstruction is defined in an entirely analogous manner. The proof of Theorem 2.2 also gives

Theorem 2.6. *Let E be an elliptic curve defined over a number field K. Let C be a 2-covering or 3-covering of E with trivial obstruction.*
(i) There is an integral ideal $\mathfrak{l}$ of K such that $\mathcal{D}_{C/K} = \mathfrak{l}^{12}\mathcal{D}_{E/K}$.
(ii) If C is everywhere locally soluble then $\mathfrak{l} = 1$.

Remark 2.7. We suspect it may be possible to give a general definition of the minimal discriminant of a genus one curve C that agrees with our definitions in the case C is equipped with a K-rational divisor D of degree $n = 1, 2$ or 3. Theorem 2.6(ii) would then be a special case of the statement that if two genus one curves are everywhere locally isomorphic then they have the same minimal discriminant.

In order to compare Theorem 2.2 with earlier work on minimisation we combine it with Kraus' conditions for the existence of a Weierstrass equation with given invariants. In the case $K = \mathbb{Q}$ these state:

Theorem 2.8. *Let c_4, c_6 be integers such that $\Delta = (c_4^3 - c_6^2)/1728$ is a non-zero integer. Then there exists an integer coefficient Weierstrass equation with invariants c_4 and c_6, if and only if*
(i) $\mathrm{ord}_3(c_6) \neq 2$, *and*
(ii) either $c_6 \equiv -1 \pmod 4$, *or* $\mathrm{ord}_2(c_4) \geq 4$ *and* $c_6 \equiv 0, 8 \pmod{32}$.

Proof: This is [9, Proposition 2]. In fact the necessity of these conditions is immediate from Tate's formulaire, *i.e.* (8) and (9). □

Theorem 2.8 may be used to determine whether a given integer coefficient Weierstrass equation is minimal. Indeed a Weierstrass equation with invariants c_4 and c_6 is minimal at p if and only if $p^{-4}c_4$ and $p^{-6}c_6$ fail to satisfy Kraus' conditions.

Definition 2.9. An integer coefficient binary quartic, respectively ternary cubic, with invariants c_4 and c_6 is *p-reducible* if it is equivalent to an integer coefficient binary quartic, respectively ternary cubic, with invariants $p^{-4}c_4$ and $p^{-6}c_6$.

Theorems 2.6 and 2.8 have the following corollary.

Corollary 2.10. *Let c_4 and c_6 be integers such that $\Delta = (c_4^3 - c_6^2)/1728$ is non-zero. The following conditions are necessary and sufficient for every integer coefficient p-adically soluble binary quartic, respectively ternary cubic, with invariants c_4 and c_6 to be p-reducible.*

$$\begin{array}{ll} p \geq 5 & p^4 \,|\, c_4 \text{ and } p^6 \,|\, c_6, \\ p = 3 & \text{either } 3^5 \,|\, c_4 \text{ and } 3^9 \,|\, c_6, \text{ or } 3^4 \,||\, c_4,\ 3^6 \,||\, c_6 \text{ and } 3^{12} \,|\, \Delta, \\ p = 2 & \text{either } 2^8 \,|\, c_4,\ 2^9 \,|\, c_6 \text{ and } 2^{-9}c_6 \equiv 0, 1 \pmod 4, \\ & \quad \text{or } 2^4 \,||\, c_4,\ 2^6 \,||\, c_6,\ 2^{12} \,|\, \Delta \text{ and } 2^{-6}c_6 \equiv -1 \pmod 4. \end{array}$$

The analogue of Corollary 2.10 for binary quartics without the cross terms (i.e. putting $\alpha_0 = \alpha_1 = \alpha_2 = 0$) is established by Cremona and Stoll [6, Appendix A] based on earlier work of Birch and Swinnerton-Dyer [3, Lemmas 3,4,5], [4, Proposition 3.6.1]. Their result is identical to ours at all primes $p \neq 2$, but is changed beyond recognition at $p = 2$. The method of Birch and Swinnerton-Dyer has been extended to quadratic number fields by Cremona and Serf [5], [13]. In the case of ternary cubics, Corollary 2.10 is a theorem of Cremona and Stoll [7], although the details of their work in the case $p = 2$ have yet to be written down.

The method of Birch and Swinnerton-Dyer, and its generalisations cited above, require an analysis of a large number of tedious (yet elementary) special cases, especially when dealing with the primes $p = 2, 3$. As observed by Cremona and Stoll [6], [7] the results for $p \geq 5$ generalise immediately to an arbitrary number field. In contrast for $p = 2, 3$ it seems necessary to treat each possible value of the absolute ramification index as a new special case.

Our proof of Theorem 2.2 avoids all these special cases, and so gives a more general result. Nonetheless the old approach retains the following advantages:

- It gives efficient algorithms for minimising binary quartics and ternary cubics. This is useful in the number field method for 2-descent and 3-descent, where we obtain binary quartics and ternary cubics that initially have very large coefficients. An algorithm for minimising based on the proof of Theorem 2.2 would need to begin by finding explicit local solutions. It is therefore unlikely to be more efficient than the existing methods.

- In the invariant theory method for 2-descent (introduced in [3] and improved by Cremona in his program `mwrank`) it is more efficient to search for binary quartics without the cross terms. See [6] for a detailed discussion.
- As pointed out by Cremona and Stoll [6], [7] the hypothesis of local solubility may be weakened to that of solubility over an unramified extension of each local field. It is not clear how to match this result using our methods.

It has long been known that Theorem 2.2 is false if one does not make the hypothesis that C is everywhere locally soluble. Our favourite examples are given by the curves

$$\begin{array}{lll} C_a: & y^2 = ax^4 + a^3 & \Delta = 2^{12}a^{12} \\ C_a: & x^3 + ay^3 + a^2z^3 = 0 & \Delta = -3^9a^{12}. \end{array} \tag{6}$$

One finds that for $p \geq 5$ a prime, C_p has Jacobian C_1, yet C_p is not p-reducible. Indeed if C_p were p-reducible then one would obtain a model with good reduction at p. It would follow that $C_p(\mathbb{Q}_p) \neq \emptyset$ which, upon inspection of (6), is plainly not the case.

It is easy to show that the converse of Theorem 2.6(ii) is false. For example the binary quartic $y^2 = 3x^4 + x^2z^2 - z^4$ has discriminant $\Delta = 2^8.3.13^2$ yet is 2-adically insoluble. Similarly the ternary cubic $x^3 + 2y^3 + 5z^3 = 0$ has discriminant $\Delta = -2^4.3^9.5^4$ yet is 3-adically insoluble.

In a sequel to this paper we plan to generalise Theorem 2.2 to n-coverings of elliptic curves. The proof will be by induction on n starting from the case $n = 3$ considered here. The case $n = 4$ should be compared with Womack's algorithm [17] for minimising a pair of homogeneous quadratics in 4 variables.

It is clear that the models obtained in Theorem 2.2 are far from unique. An interesting problem would be to determine the number of integral equivalence classes of solutions. Here we say that two models are integrally equivalent if, in the notation of §1.4, they are related by an integer coefficient transformation with λ a unit.

3. The passage from local to global

Let K be a finite extension of $\mathbb{Q}_p$ with ring of integers $\mathcal{O}_K$. Theorem 2.2 has the following local analogue.

Theorem 3.1. *Let E be an elliptic curve defined over K. Let c_4, c_6 and Δ be the invariants of an $\mathcal{O}_K$-coefficient Weierstrass equation for E. Then*

(i) Every soluble 2-covering C of E has an $\mathcal{O}_K$-coefficient equation

$$y^2 + (\alpha_0 x^2 + \alpha_1 x + \alpha_2)y = ax^4 + bx^3 + cx^2 + dx + e$$

with invariants c_4, c_6 and Δ.
(ii) Every soluble 3-covering C of E has an $\mathcal{O}_K$-coefficient equation

$$ax^3+by^3+cz^3+a_2x^2y+a_3x^2z+b_1xy^2+b_3y^2z+c_1xz^2+c_2yz^2+mxyz = 0$$

with invariants c_4, c_6 and Δ.

We give the proof of Theorem 3.1 in §4. First we show how to deduce Theorems 2.2 and 2.6 from Theorem 3.1.

Proof of Theorem 2.6: Let $n = 2$ or 3. We recall that E is an elliptic curve defined over a number field K, and that C is an n-covering of E with trivial obstruction. We fix a prime $\mathfrak{p}$ of K and put $\gamma_\mathfrak{p} = \mathrm{ord}_\mathfrak{p}(\mathcal{D}_{C/K})$, $\varepsilon_\mathfrak{p} = \mathrm{ord}_\mathfrak{p}(\mathcal{D}_{E/K})$. We aim to show
(i) $\gamma_\mathfrak{p} = \varepsilon_\mathfrak{p} + 12m$ for some integer $m \geq 0$, and
(ii) if $C(K_\mathfrak{p}) \neq \emptyset$ them $m = 0$.
We choose an $\mathcal{O}_K$-coefficient model for C whose discriminant Δ_C satisfies $\mathrm{ord}_\mathfrak{p}(\Delta_C) = \gamma_\mathfrak{p}$, and an $\mathcal{O}_K$-coefficient Weierstrass equation for E whose discriminant Δ_E satisfies $\mathrm{ord}_\mathfrak{p}(\Delta_E) = \varepsilon_\mathfrak{p}$.

To prove (i) we use the formulae of Appendix A to construct an $\mathcal{O}_K$-coefficient model for E with discriminant Δ_C. (Notice that for $\mathfrak{p} \nmid 6$ it suffices to use Theorem 1.1.) Thus $\varepsilon_\mathfrak{p} \leq \gamma_\mathfrak{p}$. Moreover $\Delta_C = \lambda^{12}\Delta_E$ for some $\lambda \in K^\times$. Putting $m = \mathrm{ord}_\mathfrak{p}(\lambda)$ gives $\gamma_\mathfrak{p} = \varepsilon_\mathfrak{p} + 12m$ as required.

To prove (ii) we use Theorem 3.1 to construct an $\mathcal{O}_\mathfrak{p}$-coefficient model for C with discriminant Δ_E. In the notation of §1.4 this new model is related to the old by a transformation $[\mu_\mathfrak{p}, r_\mathfrak{p}, A_\mathfrak{p}]$, respectively $[\mu_\mathfrak{p}, A_\mathfrak{p}]$. For $t \in K_\mathfrak{p}^\times$ the following transformations are identical:

$$\begin{array}{lrcl} n = 2 & [\mu_\mathfrak{p}, r_\mathfrak{p}, A_\mathfrak{p}] & = & [t^{-2}\mu_\mathfrak{p}, t^2 r_\mathfrak{p}, tA_\mathfrak{p}] \\ n = 3 & [\mu_\mathfrak{p}, A_\mathfrak{p}] & = & [t^{-3}\mu_\mathfrak{p}, tA_\mathfrak{p}]. \end{array} \tag{7}$$

We may therefore assume that $r_\mathfrak{p} \in \mathcal{O}_\mathfrak{p}^3$ and $A_\mathfrak{p} \in \mathrm{Mat}_n(\mathcal{O}_\mathfrak{p})$. We approximate $r_\mathfrak{p}$ by a vector $r \in \mathcal{O}_K^3$ and $A_\mathfrak{p}$ by a matrix $A \in \mathrm{Mat}_n(\mathcal{O}_K)$. Since we can find a finite set of primes, not containing $\mathfrak{p}$, that generates the class group, there exists $\mu \in K^\times$ with $\mathrm{ord}_\mathfrak{p}(\mu) = \mathrm{ord}_\mathfrak{p}(\mu_\mathfrak{p})$ yet $\mathrm{ord}_{\mathfrak{p}'}(\mu) \geq 0$ for all $\mathfrak{p}' \neq \mathfrak{p}$. Finally the transformation $[\mu, r, A]$, respectively $[\mu, A]$, gives a new $\mathcal{O}_K$-coefficient model for C whose discriminant Δ satisfies $\mathrm{ord}_\mathfrak{p}(\Delta) = \varepsilon_\mathfrak{p}$. Thus $\gamma_\mathfrak{p} \leq \varepsilon_\mathfrak{p}$ as required. □

Before proceeding with the proof of Theorem 2.2 we need two lemmas on strong approximation. For $A = (a_{ij}) \in \mathrm{Mat}_n(K_\mathfrak{p})$ we put $||A||_\mathfrak{p} = \max_{1 \leq i,j \leq n} ||a_{ij}||_\mathfrak{p}$.

Lemma 3.2. *Let S be a finite set of primes of K. Suppose given $A_{\mathfrak{p}} \in \mathrm{SL}_n(\mathcal{O}_{\mathfrak{p}})$ for all $\mathfrak{p} \in S$ and let $\varepsilon > 0$. Then there exists $A \in \mathrm{SL}_n(\mathcal{O}_K)$ such that $||A - A_{\mathfrak{p}}||_{\mathfrak{p}} < \varepsilon$ for all $\mathfrak{p} \in S$.*

PROOF: Let E_{ij} be the $n \times n$ matrix with entry 1 in the (i,j)-th place, and zeros elsewhere. Using the identities

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

and

$$\begin{pmatrix} 1 & 0 \\ -\alpha^{-1} & 1 \end{pmatrix} \begin{pmatrix} 1 & \alpha - 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & \alpha^{-1} - 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix}$$

one can show (via row and column operations) that $\mathrm{SL}_n(\mathcal{O}_{\mathfrak{p}})$ is generated by the matrices $I_n + \lambda E_{ij}$ for $\lambda \in \mathcal{O}_{\mathfrak{p}}$ and $i \neq j$. So it suffices to treat the case $A_{\mathfrak{p}} = I_n + \lambda_{\mathfrak{p}} E_{ij}$ with $\lambda_{\mathfrak{p}} = 0$ for all but one prime $\mathfrak{p}$ in S. We are done by the Chinese Remainder Theorem. □

Lemma 3.3. *Let S be a finite set of primes of K and let $\delta \in \mathcal{O}_K$. Suppose given $A_{\mathfrak{p}} \in \mathrm{Mat}_n(\mathcal{O}_{\mathfrak{p}})$ with $\det(A_{\mathfrak{p}}) = \delta$ for all $\mathfrak{p} \in S$ and let $\varepsilon > 0$. Then there exists $A \in \mathrm{Mat}_n(\mathcal{O}_K)$ with $\det(A) = \delta$ such that $||A - A_{\mathfrak{p}}||_{\mathfrak{p}} < \varepsilon$ for all $\mathfrak{p} \in S$.*

PROOF: By Lemma 3.2 it suffices to treat the case where each local matrix $A_{\mathfrak{p}}$ is diagonal. We must choose $A = (a_{ij})$. Let $b \in \mathcal{O}_K$ be an S-unit which is $\mathfrak{p}$-adically small for all $\mathfrak{p} \in S$. (This is possible by the finiteness of the class group.) We set $a_{i\,i+1} = b$ for all $1 \leq i \leq n-1$. We then use the Chinese Remainder Theorem to choose diagonal entries for our matrix A that are $\mathfrak{p}$-adically close to the diagonal entries of $A_{\mathfrak{p}}$ for all $\mathfrak{p} \in S$. We put

$$a_{n1} \;=\; (-1)^n (\textstyle\prod_{i=1}^n a_{ii} - \delta)/b^{n-1}.$$

Setting all remaining entries zero gives the required matrix A. □

PROOF OF THEOREM 2.2: Let $n = 2$ or 3. We recall that E is an elliptic curve defined over a number field K, and C is an everywhere locally soluble n-covering of E. In particular C has trivial obstruction everywhere locally. It is shown in [11] that the obstruction takes values in the Brauer group. So by global class field theory, C has trivial obstruction. (This is the only stage in the proof where we use the hypothesis of local solubility at the infinite places. This is only an issue for $n = 2$.) Thus C is represented by a binary quartic or a ternary cubic. We use the transformations of §1.4 to find such a model with $\mathcal{O}_K$-coefficients.

Let Δ_C and Δ_E be the discriminants of our models for C and E. By Theorem 1.1 we have $\Delta_C = \lambda^{12}\Delta_E$ for some $\lambda \in K^\times$. Let S be a finite set of primes containing a set of generators for the class group, and all primes $\mathfrak{p}$ with $\mathrm{ord}_\mathfrak{p}(\lambda) \neq 0$. Theorem 3.1 tells us that for each $\mathfrak{p} \in S$ our model for C is equivalent to an $\mathcal{O}_\mathfrak{p}$-coefficient model with discriminant Δ_E. In the notation of §1.4 the equivalence is given by a transformation $[\mu_\mathfrak{p}, r_\mathfrak{p}, A_\mathfrak{p}]$, respectively $[\mu_\mathfrak{p}, A_\mathfrak{p}]$, with $\mu_\mathfrak{p} \in K_\mathfrak{p}^\times$, $r_\mathfrak{p} \in K_\mathfrak{p}^3$ and $A_\mathfrak{p} \in \mathrm{GL}_n(K_\mathfrak{p})$. We are free to make adjustments of the form (7). Not only does this allow us to assume that $r_\mathfrak{p} \in \mathcal{O}_\mathfrak{p}^3$ and $A_\mathfrak{p} \in \mathrm{Mat}_n(\mathcal{O}_\mathfrak{p})$ for all $\mathfrak{p} \in S$, but also, since $(h_K, n) = 1$, we can find $\mu \in K^\times$ with

$$\mathrm{ord}_\mathfrak{p}(\mu) \;=\; \begin{cases} \mathrm{ord}_\mathfrak{p}(\mu_\mathfrak{p}) & \text{for } \mathfrak{p} \in S, \\ 0 & \text{for } \mathfrak{p} \notin S. \end{cases}$$

Our local transformations are now of the form $[\mu, r_\mathfrak{p}, A_\mathfrak{p}]$, respectively $[\mu, A_\mathfrak{p}]$ with $r_\mathfrak{p} \in \mathcal{O}_\mathfrak{p}^3$ and $A_\mathfrak{p} \in \mathrm{Mat}_n(\mathcal{O}_\mathfrak{p})$.

Let $\lambda_\mathfrak{p} = \mu \det A_\mathfrak{p}$. Since $\Delta_C = \lambda_\mathfrak{p}^{12}\Delta_E$ it follows that $\lambda/\lambda_\mathfrak{p}$ is a root of unity. Making adjustments to $r_\mathfrak{p}$ and $A_\mathfrak{p}$ (say, by rescaling the x co-ordinate on our local model) we may suppose that $\lambda = \lambda_\mathfrak{p}$ for all $\mathfrak{p} \in S$. We put $\delta = \lambda\mu^{-1}$. Then $\det A_\mathfrak{p} = \delta$ for all $\mathfrak{p} \in S$, and moreover $\delta \in \mathcal{O}_K$. We use Lemma 3.3 to construct a matrix $A \in \mathrm{Mat}_n(\mathcal{O}_K)$ with determinant δ that is $\mathfrak{p}$-adically close to $A_\mathfrak{p}$ for all $\mathfrak{p} \in S$. In the case $n = 2$ we also approximate the $r_\mathfrak{p}$ for $\mathfrak{p} \in S$ by a vector $r \in \mathcal{O}_K^3$. Finally the transformation $[\mu, r, A]$, respectively $[\mu, A]$, gives a new $\mathcal{O}_K$-coefficient model for C with discriminant Δ_E. We are done by Remark 2.4. □

4. Proof of local results

We work over a local field K, complete with respect to a discrete valuation $\mathrm{ord} : K^\times \to \mathbb{Z}$. We write R for the ring of integers and π for a uniformiser. The residue field is $k = R/\pi R$. We make no restriction on the characteristic of k (or for that matter K).

4.1. **Weierstrass equations.** We recall some standard facts about elliptic curves and Weierstrass equations, many of which we have been using already. The formulae are taken from [14, Chapter III].

Definition 4.1. An elliptic curve $(E, 0)$ defined over K is a smooth curve of genus one defined over K equipped with a rational point $0 \in E(K)$.

We choose $x, y \in K(E)$ such that $\mathcal{L}(2.0)$ and $\mathcal{L}(3.0)$ have bases $1, x$ and $1, x, y$. Then the 7 elements $1, x, y, x^2, xy, x^3, y^2$ in the 6 dimensional vector space $\mathcal{L}(6.0)$ satisfy a linear dependence relation. Furthermore the coefficients of x^3 and y^2 are non-zero. Rescaling x and y we deduce that $(E, 0)$ has a Weierstrass equation

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

Following Tate's formulaire we define

$$\begin{array}{rcl} b_2 & = & a_1^2 + 4a_2 \\ b_4 & = & 2a_4 + a_1a_3 \\ b_6 & = & a_3^2 + 4a_6 \\ b_8 & = & a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \end{array} \tag{8}$$

and

$$\begin{array}{rcl} c_4 & = & b_2^2 - 24b_4 \\ c_6 & = & -b_2^3 + 36b_2b_4 - 216b_6 \\ \Delta & = & -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6. \end{array} \tag{9}$$

As noted in §1 these formulae for c_4, c_6 and Δ may also be obtained by specialising the invariants for a binary quartic or ternary cubic.

Definition 4.2. A Weierstrass equation for $(E, 0)$ is minimal if $\mathrm{ord}(\Delta)$ is minimal subject to the condition $a_1, a_2, a_3, a_4, a_6 \in R$.

Any two Weierstrass equations for $(E, 0)$ are related by making a substitution of the form

$$\begin{array}{rcl} x & = & u^2x' + r \\ y & = & u^3y' + u^2sx' + t \end{array}$$

and then dividing through by u^6. This transformation is denoted $[u; r, s, t]$. The coefficients a_i' of the new Weierstrass equation are related to the coefficients a_i of the old via

$$\begin{array}{rcl} ua_1' & = & a_1 + 2s \\ u^2a_2' & = & a_2 - sa_1 + 3r - s^2 \\ u^3a_3' & = & a_3 + ra_1 + 2t \\ u^4a_4' & = & a_4 - sa_3 + 2ra_2 - (rs + t)a_1 + 3r^2 - 2st \\ u^6a_6' & = & a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1. \end{array} \tag{10}$$

The associated quantities (8) and (9) are transformed by

$$\begin{array}{rcl} u^2b_2' & = & b_2 + 12r \\ u^4b_4' & = & b_4 + rb_2 + 6r^2 \\ u^6b_6' & = & b_6 + 2rb_4 + r^2b_2 + 4r^3 \\ u^8b_8' & = & b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4 \end{array} \tag{11}$$

and $u^4c_4' = c_4$, $u^6c_6' = c_6$, $u^{12}\Delta' = \Delta$.

4.2. **Generalised Weierstrass equations.** We generalise the standard definitions recalled in the last subsection.

Definition 4.3. A generalised elliptic curve $(E, 0, 0')$ defined over K is a smooth curve of genus one defined over K equipped with an ordered pair of rational points $0, 0' \in E(K)$. The possibility $0 = 0'$ is allowed.

We choose $x, y \in K(E)$ such that $\mathcal{L}(0 + 0')$ and $\mathcal{L}(2.0 + 0')$ have bases $1, x$ and $1, x, y$. Then the 8 elements $1, x, y, x^2, xy, x^3, y^2, x^2y$ in the 7 dimensional vector space $\mathcal{L}(4.0+3.0')$ satisfy a linear dependence relation. Furthermore the coefficient of y^2 is non-zero. We deduce that $(E, 0, 0')$ has a generalised Weierstrass equation

$$y^2 + \alpha_1 xy + \alpha_3 y = \xi x^2 y + \eta x^3 + \alpha_2 x^2 + \alpha_4 x + \alpha_6.$$

The invariants c_4, c_6 and Δ are defined as polynomials in ξ, η, α_1, α_2, α_3, α_4, α_6 by specialising the invariants for a ternary cubic.

Definition 4.4. A generalised Weierstrass equation for $(E, 0, 0')$ is minimal if $\mathrm{ord}(\Delta)$ is minimal subject to the condition ξ, η, α_1, α_2, α_3, α_4, $\alpha_6 \in R$.

Any two generalised Weierstrass equations for $(E, 0, 0')$ are related by making a substitution of the form

$$\begin{aligned} x &= v^2 w x' + \rho \\ y &= v^3 w^2 y' + v^2 w \sigma x' + \tau \end{aligned}$$

and then dividing through by $v^6 w^4$. This transformation is denoted $[v, w; \rho, \sigma, \tau]$. The coefficients of the new generalised Weierstrass equation are related to the old via

$$\begin{aligned} v^{-1}\xi' &= \xi \\ w\eta' &= \eta + \sigma\xi \\ vwa_1' &= \alpha_1 - 2\rho\xi + 2\sigma \\ v^2w^2\alpha_2' &= \alpha_2 + (2\rho\sigma + \tau)\xi - \sigma\alpha_1 + 3\rho\eta - \sigma^2 \\ v^3w^2\alpha_3' &= \alpha_3 - \rho^2\xi + \rho\alpha_1 + 2\tau \\ v^4w^3\alpha_4' &= \alpha_4 + \rho(\rho\sigma + 2\tau)\xi - \sigma\alpha_3 + 2\rho\alpha_2 - (\rho\sigma + \tau)\alpha_1 + 3\rho^2\eta - 2\sigma\tau \\ v^6w^4\alpha_6' &= \alpha_6 + \rho^2\tau\xi + \rho\alpha_4 + \rho^2\alpha_2 + \rho^3\eta - \tau\alpha_3 - \tau^2 - \rho\tau\alpha_1. \end{aligned}$$

We have arranged that if $\xi = 0$, $\eta = 1$, $\alpha_i = a_i$ and

$$[v, w; \rho, \sigma, \tau] = [u, 1; r, s, t]$$

then these formalae reduce to those recalled in §4.1.

Proposition 4.5. *Let $(E, 0, 0')$ have generalised Weierstrass equation*

$$y^2 + \alpha_1 xy + \alpha_3 y = \xi x^2 y + \eta x^3 + \alpha_2 x^2 + \alpha_4 x + \alpha_6. \tag{12}$$

Then $(E, 0)$ has Weierstrass equation

$$Y^2 + a_1 XY + a_3 Y = X^3 + a_2 X^2 + a_4 X + a_6 \tag{13}$$

where

$$\begin{array}{rcl} a_1 &=& \alpha_1 \\ a_2 &=& \alpha_2 + \xi\alpha_3 \\ a_3 &=& \eta\alpha_3 - \xi\alpha_4 \\ a_4 &=& \eta\alpha_4 + \xi\alpha_2\alpha_3 - \xi^2\alpha_6 \\ a_6 &=& \eta^2\alpha_6 - \xi\eta\alpha_1\alpha_6 + \xi\eta\alpha_3\alpha_4 - \xi^2\alpha_2\alpha_6. \end{array} \tag{14}$$

Moreover the generalised Weierstrass equation (12) and its associated Weierstrass equation (13) have the same invariants c_4, c_6 and Δ.

PROOF: The required isomorphism is given by

$$\begin{array}{rcl} X &=& \eta x + \xi y \\ Y &=& \eta y + \xi(-\alpha_1 y + \xi xy + \eta x^2 + \alpha_2 x + \alpha_4). \end{array}$$

The statement concerning invariants is proved by direct calculation. An alternative proof is given by specialising the formulae of Artin, Rodriguez-Villegas and Tate recalled in Appendix A. □

Lemma 4.6. *If we transform the generalised Weierstrass equation (12) by $[v, w; \rho, \sigma, \tau]$ then the associated Weierstrass equation (13) is transformed by $[u; r, s, t]$ where*

$$\begin{array}{rcl} u &=& vw \\ r &=& \rho\eta + \tau\xi \\ s &=& \sigma - \rho\xi \\ t &=& \tau\eta - 2\rho^2\xi\eta + (\rho\sigma\alpha_1 - \rho\alpha_2 + \sigma\alpha_3 + 2\sigma\tau)\xi - \rho(\rho\sigma + \tau)\xi^2. \end{array} \tag{15}$$

PROOF: A direct calculation. □

4.3. **An algorithm for minimising.** We continue to write R for the ring of integers of K. It is clear that every generalised Weierstrass equation is equivalent to one with coefficients in R.

Theorem 4.7. *A generalised Weierstrass equation with coefficients in R is minimal if and only if its associated Weierstrass equation is minimal.*

PROOF: It is clear from Proposition 4.5 that if a generalised Weierstrass equation is not minimal then its associated Weierstrass equation is not minimal. Explicitly if the generalised Weierstrass equation is minimised by a transformation $[v, w; \rho, \sigma, \tau]$ then its associated Weierstrass equation is minimised by $[u; r, s, t]$ where u, r, s, t are given by (15).

To prove the theorem we give an algorithm for minimising a generalised Weierstrass equation, subject only to the hypothesis that the associated Weierstrass equation is not minimal. The basic idea is as follows. By hypothesis there is a transformation $[1; r, s, t]$ which when

applied to the associated Weierstrass equation gives $\pi^i \,|\, a_i$ for all i. We hope to solve (15) for ρ, σ, τ. If successful, we apply the transformation $[1, 1; \rho, \sigma, \tau]$ to our generalised Weierstrass equation, and thus reduce to the case $\pi^i \mid a_i$ for all i. With a bit of luck we can then use (14) to show that the α_i are divisible by certain powers of π. Finally we minimise using either $[\pi, 1; 0, 0, 0]$ or $[1, \pi; 0, 0, 0]$.

In practice our algorithm is a hybrid of the above sketch and the first few steps of Tate's algorithm: see [15].

Step 1. If $\pi \,|\, \xi$ and $\pi \,|\, \eta$ then we repeatedly apply the transformation $[\pi^{-1}, \pi; 0, 0, 0]$ until either ξ or η is a unit.

Step 2. By hypothesis $\pi \,|\, \Delta$. So the reduction mod π of our generalised Weierstrass equation has a singular point. By Step 1 either $\pi \nmid \xi$ or $\pi \nmid \eta$. So the points at infinity on the reduction are smooth. Making a transformation of the form $[1, 1; \rho, 0, \tau]$ we may suppose that the singular point is $(x, y) = (0, 0)$. Then $\pi \mid \alpha_3, \alpha_4, \alpha_6$. By (14) we also have $\pi \,|\, a_3, a_4, a_6$.

Step 3. By hypothesis $\pi \,|\, c_4 = b_2^2 - 24b_4$. But by Step 1 we already have $\pi \,|\, b_4 = 2a_4 + a_1a_3$. Therefore $\pi \,|\, b_2$ where

$$b_2 = a_1^2 + 4a_2 = \alpha_1^2 + 4\alpha_2 + 4\xi\alpha_3.$$

Since $\pi \,|\, \alpha_3$ we deduce $\pi \,|\, (\alpha_1^2 + 4\alpha_2)$. Making a transformation of the form $[1, 1; 0, \sigma, 0]$ we may assume that $\pi \,|\, \alpha_i$ for all i. By (14) we also have $\pi \,|\, a_i$ for all i.

Step 4. By hypothesis there is a transformation $[1; r, s, t]$ for which the transformed quantities a_i' satisfy $\pi^i \,|\, a_i'$ for all i. Since we already have $\pi \,|\, a_i$ for all i it follows by (10) that

$$\pi \,|\, 2s, \quad \pi \,|\, (3r - s^2), \quad \pi \,|\, 2t, \quad \pi \,|\, (3r^2 - 2st), \quad \pi \,|\, (r^3 - t^2).$$

From these we deduce $\pi \,|\, r, s, t$. (Recall that we make no assumption on the characteristic of k.)

The algorithm now splits into two cases.

Case $\pi \nmid \eta$. Making a transformation $[1, \eta; 0, 0, 0]$ we may assume that $\eta = 1$. Let r, s, t be as in Step 4. We solve for ρ, σ, τ satisfying

$$\begin{aligned} r &= \rho + \xi\tau \\ s &= \sigma - \xi\rho \\ t &= \tau - 2\xi\rho^2 + \xi(\alpha_1\rho\sigma - \alpha_2\rho + \alpha_3\sigma + 2\sigma\tau) - \xi^2\rho(\rho\sigma + \tau). \end{aligned} \tag{16}$$

To do this we set $(\rho_1, \sigma_1, \tau_1) = (r, s, t)$ and recursively define

$$\begin{aligned}\rho_n &= r - \xi\tau_{n-1}\\ \sigma_n &= s + \xi\rho_n\\ \tau_n &= t + 2\xi\rho_n^2 - \xi(\alpha_1\rho_n\sigma_n - \alpha_2\rho_n + \alpha_3\sigma_n + 2\sigma_n\tau_n)\\ &\qquad + \xi^2\rho_n(\rho_n\sigma_n + \tau_n).\end{aligned}$$

Since $\pi \,|\, r, s, t$ and $\pi \,|\, \alpha_1, \alpha_2, \alpha_3$ it follows by induction that

$$\begin{aligned}\rho_{n+1} &\equiv \rho_n \pmod{\pi^n}\\ \sigma_{n+1} &\equiv \sigma_n \pmod{\pi^n}\\ \tau_{n+1} &\equiv \tau_n \pmod{\pi^{n+1}}.\end{aligned}$$

Since K is complete[1] the sequences ρ_n, σ_n, τ_n converge to $\rho, \sigma, \tau \in R$, a solution to (16). We apply the transformation $[1, 1; \rho, \sigma, \tau]$ and hence reduce to the case $\pi^i \,|\, a_i$ for all i. Since $\pi \,|\, \rho, \sigma, \tau$ we still have $\pi \nmid \eta$ and $\pi \,|\, \alpha_i$ for all i. We now use (14) to show that $\pi^2 \,|\, \alpha_6$ since $\pi^2 \,|\, a_6$, then $\pi^2 \,|\, \alpha_4$ since $\pi^2 \,|\, a_4$, then $\pi^2 \,|\, \alpha_3$ since $\pi^2 \,|\, a_3$, and so on. In the end we get $\pi^i \,|\, \alpha_i$ for all i. We can then minimise using the transformation $[\pi, 1; 0, 0, 0]$.

Case $\pi \,|\, \eta$. By Step 1 we have $\pi \nmid \xi$. Making a transformation $[\xi^{-1}, 1; 0, 0, 0]$ we may assume that $\xi = 1$. Let r, s, t be as in Step 4. Since

$$a_4' = a_4 - sa_3 + 2ra_2 - (rs + t)a_1 + 3r^2 - 2st$$

we have $\pi^2 \,|\, a_4$. Then using (14) we obtain $\pi^2 \,|\, \alpha_6$ and $\pi^3 \,|\, a_6$. Since

$$\begin{aligned}a_3' &= a_3 + ra_1 + 2t\\ a_6' &= a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1\end{aligned}$$

it follows that $\pi^2 \,|\, t$.

We apply the transformation $[1, 1; 0, s, r]$ to our generalised Weierstrass equation. After this transformation we still have $\pi \,|\, \eta$ and $\pi \,|\, \alpha_i$ for all i. According to Lemma 4.6 the associated Weierstrass equation is transformed by $[1; r, s, t']$ where $t' = r\eta + s\alpha_3 + 2rs$. Since $t \equiv t' \equiv 0 \pmod{\pi^2}$ it follows by (10) and (11) that

$$\pi \,|\, a_1, \quad \pi^2 \,|\, a_2, a_3, \quad \pi^3 \,|\, a_4, \quad \pi^4 \,|\, a_6$$

and $\pi^i \,|\, b_i$ for all i. Using (14) we obtain $\pi^2 \,|\, \alpha_4, \alpha_6$ and then

$$\pi^2 \,|\, (\alpha_2 + \alpha_3), \quad \pi^3 \,|\, (\alpha_2\alpha_3 - \alpha_6), \quad \pi^4 \,|\, \alpha_2\alpha_6.$$

From these we deduce

$$\pi \,|\, \alpha_1, \quad \pi^2 \,|\, \alpha_2, \alpha_3, \alpha_4, \quad \pi^3 \,|\, \alpha_6.$$

[1] In fact an approximate solution to (16) would suffice, so we don't really need that K is complete.

Since

$$a_6 = \eta^2\alpha_6 - \eta\alpha_1\alpha_6 + \eta\alpha_3\alpha_4 - \alpha_2\alpha_6$$

it follows that $\pi^5 \,|\, a_6$. Next using

$$\begin{aligned} b_6 &= a_3^2 + 4a_6 \\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \end{aligned}$$

we obtain first $\pi^3 \,|\, a_3$ and then $\pi^4 \,|\, a_4$. By (14) we also have $\pi^3 \,|\, \alpha_4$ and $\pi^4 \,|\, \alpha_6$. We can then minimise using the transformation $[1, \pi; 0, 0, 0]$. □

Recall that we defined the invariants of a generalised Weierstrass equation (12) as the invariants of the ternary cubic

$$y^2z + \alpha_1xyz + \alpha_3yz^2 - (\xi x^2y + \eta x^3 + \alpha_2x^2z + \alpha_4xz^2 + \alpha_6z^3) = 0. \tag{17}$$

A calculation reveals that these are the same as the invariants of the binary quartic

$$y^2 + (-\xi x^2 + \alpha_1xz + \alpha_3z^2)y = \eta x^3z + \alpha_2x^2z^2 + \alpha_4xz^3 + \alpha_6z^4. \tag{18}$$

Proof of Theorem 3.1: Let $n = 2$ or 3. We recall that E is an elliptic curve defined over K, with K a finite extension of $\mathbb{Q}_p$. We are given an $\mathcal{O}_K$-coefficient Weierstrass equation for E and a soluble n-covering C of E. The structure of n-covering determines a K-rational divisor class $[D]$ on C. For 0 a rational point on C the Riemann-Roch space $\mathcal{L}(D - (n-1).0)$ is 1-dimensional. Hence

$$D \sim (n-1).0 + 0'$$

where $0'$ is a rational point on C. By Theorem 4.7 the generalised elliptic curve $(C, 0, 0')$ has an $\mathcal{O}_K$-coefficient generalised Weierstrass equation with the same invariants as a minimal Weierstrass equation for E. Then (18) or (17) is a model for the pair $(C, [D])$ with discriminant dividing that of our original Weierstrass equation. We are done by the local analogue of Remark 2.4. □

Remark 4.8. More concretely, a soluble binary quartic, respectively ternary cubic, may be put in generalised Weierstrass form using (in the notation of §1.4) a transformation $[1, 0, A]$, respectively $[1, A]$. Indeed in the case $n = 2$ we move the rational point to $(x : z) = (1 : 0)$. The resulting binary quartic has no x^4 term and is therefore of the form (18). In the case $n = 3$ we move the rational point to $(x : y : z) = (0 : 1 : 0)$ and its tangent line to $z = 0$. The resulting ternary cubic has no terms y^3 or xy^2 and is therefore of the form (17).

Appendix A. Formulae for the Jacobian

In §1 we defined the invariants c_4, c_6 and Δ of a binary quartic, respectively a ternary cubic. We now attempt to "work back" through the formulae (8) and (9) in order to define quantities b_2, b_4, b_6, b_8 and a_1, a_2, a_3, a_4, a_6. In the case $n = 2$, we find

$$c_4 \equiv (\alpha_1^2 - 4\alpha_0\alpha_2 + 4c)^2 \pmod{24}.$$

We set $b_2 = \alpha_1^2 - 4\alpha_0\alpha_2 + 4c$ and solve for b_4, b_6, b_8 using (9). Next we set $a_1 = \alpha_1$ and $a_2 = -\alpha_0\alpha_2 + c$. It turns out that we can write $b_4 = \alpha_1 a_3 + 2a_4$ where a_3 and a_4 are polynomials not involving α_1. Putting $a_6 = (b_6 - a_3^2)/4$ we obtain

$$\begin{aligned}
a_1 &= \alpha_1 \\
a_2 &= c - \alpha_0\alpha_2 \\
a_3 &= \alpha_0 d + \alpha_2 b \\
a_4 &= -4ae + bd - (\alpha_0^2 e + \alpha_0\alpha_2 c + \alpha_2^2 a) \\
a_6 &= -4ace + ad^2 + b^2 e - (\alpha_0^2 ce + \alpha_1^2 ae + \alpha_2^2 ac + \alpha_0\alpha_2 bd) \\
&\quad + \alpha_0\alpha_1 be + \alpha_1\alpha_2 ad.
\end{aligned}$$

In the case $n = 3$, we find

$$c_4 \equiv (m^2 - 4(a_2c_2 + a_3b_3 + b_1c_1))^2 \pmod{24}.$$

We set $b_2 = m^2 - 4(a_2c_2 + a_3b_3 + b_1c_1)$ and solve for b_4, b_6, b_8 using (9). Next we set $a_1 = m$ and $a_2 = -(a_2c_2 + a_3b_3 + b_1c_1)$. It turns out that we can write $b_4 = ma_3 + 2a_4$ where a_3 and a_4 are polynomials not involving m. Putting $a_6 = (b_6 - a_3^2)/4$ we obtain

$$\begin{aligned}
a_1 &= m \\
a_2 &= -(a_2c_2 + a_3b_3 + b_1c_1) \\
a_3 &= 9abc - (ab_3c_2 + ba_3c_1 + ca_2b_1) - (a_2b_3c_1 + a_3b_1c_2) \\
a_4 &= -3(abc_1c_2 + acb_1b_3 + bca_2a_3) \\
&\quad + a(b_1c_2^2 + b_3^2c_1) + b(a_2c_1^2 + a_3^2c_2) + c(a_2^2b_3 + a_3b_1^2) \\
&\quad + a_2c_2a_3b_3 + b_1c_1a_2c_2 + a_3b_3b_1c_1 \\
a_6 &= -27a^2b^2c^2 + 9abc(ab_3c_2 + ca_2b_1 + ba_3c_1) + 3abc(a_2b_3c_1 + a_3b_1c_2) \\
&\quad - (a^2bc_2^3 + b^2ca_3^3 + c^2ab_1^3 + a^2cb_3^3 + b^2ac_1^3 + c^2ba_2^3) \\
&\quad + 2(abc_1c_2 + bca_2a_3 + cab_1b_3)(a_2c_2 + a_3b_3 + b_1c_1) \\
&\quad - 3(aba_3b_3c_1c_2 + bca_2a_3b_1c_1 + caa_2b_1b_3c_2) \\
&\quad - (b_1c_1 + a_2c_2)(ab_3^2c_1 + bc_2a_3^2) \\
&\quad - (c_2a_2 + a_3b_3)(bc_1^2a_2 + ca_3b_1^2) \\
&\quad - (a_3b_3 + b_1c_1)(ca_2^2b_3 + ab_1c_2^2) \\
&\quad - a_2a_3b_1b_3c_1c_2 - 3abc(a_2c_2 + a_3b_3 + b_1c_1)m \\
&\quad + (ab(a_3c_2^2 + b_3c_1^2) + bc(a_2^2c_1 + a_3^2b_1) + ac(a_2b_3^2 + b_1^2c_2))m \\
&\quad + (ab_1b_3c_1c_2 + ba_2a_3c_1c_2 + ca_2a_3b_1b_3)m \\
&\quad - (abc_1c_2 + bca_2a_3 + cab_1b_3)m^2 + abcm^3.
\end{aligned}$$

We record an immediate consequence.

Lemma A.1. *Let a_1, a_2, a_3, a_4, a_6 be the quantities associated to a binary quartic or ternary cubic, as defined above. Then the Weierstrass equation*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{19}$$

has the same invariants c_4, c_6 and Δ as the original binary quartic or ternary cubic.

These formulae, in the case of a ternary cubic, are due to Artin, Rodriguez-Villegas and Tate [2]. Moreover they show that (19) is a formula for the Jacobian that works in arbitrary characteristic. In characteristic different from 2 and 3 this is already clear from Theorem 1.1.

Appendix B. The class group

We give some examples to show that the hypothesis on the class number in Theorem 2.2 cannot be removed. First we need two lemmas.

Lemma B.1. *Let $[K : \mathbb{Q}_p] < \infty$ with $p \neq 2$. Let $[\mu, r, A]$ with $\mu \in K^\times, r \in K^3$ and $A \in \mathrm{GL}_2(K)$ be a transformation relating two $\mathcal{O}_K$-coefficient binary quartics with good reduction. Then*

$$\mathrm{ord}(\mu) \equiv \mathrm{ord}(\det A) \equiv 0 \pmod 2.$$

Proof: Since $p \neq 2$ we may assume the binary quartics have no cross terms (i.e. $\alpha_0 = \alpha_1 = \alpha_2 = 0$) and $r = 0$. Let $\pi \in K$ with $\mathrm{ord}(\pi) = 1$. Since both binary quartics have good reduction we have $\mathrm{ord}(\mu) = -\mathrm{ord}(\det A)$. So without loss of generality

$$[\mu, r, A] = [\pi^{-a-b}, 0, \begin{pmatrix} \pi^a & 0 \\ 0 & \pi^b \end{pmatrix}]$$

for some $a \geq b$. If $a > b$ then the first binary quartic has singular reduction above $(x : z) = (0 : 1)$. So $a = b$ and $\mathrm{ord}(\mu) \equiv \mathrm{ord}(\det A) \equiv 0 \pmod 2$. □

Lemma B.2. *Let $[K : \mathbb{Q}_p] < \infty$. Let $[\mu, A]$ with $\mu \in K^\times$ and $A \in \mathrm{GL}_3(K)$ be a transformation relating two $\mathcal{O}_K$-coefficient ternary cubics with good reduction. Then*

$$\mathrm{ord}(\mu) \equiv \mathrm{ord}(\det A) \equiv 0 \pmod 3.$$

PROOF: Let $\pi \in K$ with $\mathrm{ord}(\pi) = 1$. Since both ternary cubics have good reduction we have $\mathrm{ord}(\mu) = -\mathrm{ord}(\det A)$. So without loss of generality

$$[\mu, A] = [\pi^{-a-b-c}, \begin{pmatrix} \pi^a & 0 & 0 \\ 0 & \pi^b & 0 \\ 0 & 0 & \pi^c \end{pmatrix}]$$

for some $a \geq b \geq c$. If $b > c$ then the first ternary cubic has singular reduction at $(x : y : z) = (0 : 0 : 1)$. If $a > b = c$ then the reduction contains the line $x = 0$. So $a = b = c$ and $\mathrm{ord}(\mu) \equiv \mathrm{ord}(\det A) \equiv 0 \pmod 3$. □

Example B.3. Let $K = \mathbb{Q}(\sqrt{-35})$ and $\alpha = (-1 + \sqrt{-35})/2$. Let E be the elliptic curve with Weierstrass equation

$$y^2 = x^3 - 11x + 14$$

and C the 2-covering of E with equation

$$y^2 = \alpha(x^2 - \overline{\alpha}z^2)(x^2 - 2\overline{\alpha}z^2). \tag{20}$$

We have $\Delta_E = 2^9$ and $\Delta_C = 2^9 3^{12}$. The prime 3 factors in $\mathcal{O}_K$ as $(3) = \mathfrak{p}\overline{\mathfrak{p}}$ with $\mathfrak{p}^2 = (\alpha)$. We can minimise (20) locally at $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ by means of the transformations

$$[3^{-1}, 0, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}] \quad \text{and} \quad [1, 0, \begin{pmatrix} 1 & 0 \\ 0 & 3^{-1} \end{pmatrix}].$$

So if C has an $\mathcal{O}_K$-coefficient equation with the same invariants as E, then (20) and this new equation are related by $[\mu, r, A]$ with

$$\begin{aligned} \mathrm{ord}_{\mathfrak{p}}(\mu) &\equiv 1 \pmod 2 \\ \mathrm{ord}_{\overline{\mathfrak{p}}}(\mu) &\equiv 0 \pmod 2 \end{aligned}$$

and $\mathrm{ord}_{\mathfrak{q}}(\mu) \equiv 0 \pmod 2$ for all $\mathfrak{q} \nmid 2, 3$. Since 2 is inert in K and $h_K = 2$ it follows that $\mathfrak{p}$ is principal, which is a contradiction. Finally we note that $\alpha \in (K_2^*)^2$, so C is everywhere locally soluble.

Example B.4. Let $K = \mathbb{Q}(\sqrt{-23})$ and $\alpha = 2 + \sqrt{-23}$. Let E be the elliptic curve with Weierstrass equation

$$y^2 + y = x^3 + 2\sqrt{-23}x + 8 + 3\sqrt{-23}$$

and C the 3-covering of E with equation

$$3x^3 + \alpha(x^2y - xz^2 + 3y^2z) + \alpha^2 y^3 = 0. \tag{21}$$

We have $(\Delta_E) = \mathfrak{p}_1\mathfrak{p}_2$ and $\Delta_C = \alpha^{12}\Delta_E$ where $\mathfrak{p}_1 = (1 + 6\sqrt{-23})$ and $\mathfrak{p}_2 = (1527 + 446\sqrt{-23})$ are prime ideals. The prime 3 factors in $\mathcal{O}_K$

as $(3) = \mathfrak{p}\overline{\mathfrak{p}}$ with $\mathfrak{p}^3 = (\alpha)$. We can minimise (21) locally at $\mathfrak{p}$ by means of the transformation

$$[3^{-4}, \begin{pmatrix} 3 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}].$$

So if C has an $\mathcal{O}_K$-coefficient equation with the same invariants as E, then (21) and this new equation are related by $[\mu, A]$ with

$$\mathrm{ord}_{\mathfrak{p}}(\mu) \equiv 2 \pmod 3$$

and $\mathrm{ord}_{\mathfrak{q}}(\mu) \equiv 0 \pmod 3$ for all $\mathfrak{q} \neq \mathfrak{p}, \mathfrak{p}_1, \mathfrak{p}_2$. Since $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are principal and $h_K = 3$ it follows that $\mathfrak{p}$ is principal, which is a contradiction. Finally we note that C is globally soluble.

Acknowledgements

I would like to thank John Cremona and Michael Stoll for sharing many of their ideas on this topic. The computer calculations in support of this work were performed using Magma [10].

References

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

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

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

[4] J.E. Cremona, *Algorithms for modular elliptic curves*, Second edition, Cambridge University Press, Cambridge, 1997.

[5] J.E. Cremona and P. Serf, Computing the rank of elliptic curves over real quadratic number fields of class number 1, *Math. Comp.* **68** (1999), no. 227, 1187–1200.

[6] J.E. Cremona and M. Stoll, Minimal models for 2-coverings of elliptic curves, *LMS J. Comput. Math.* **5** (2002), 220–243.

[7] J.E. Cremona and M. Stoll, *Minimisation and reduction of ternary cubics*, in preparation.

[8] D. Hilbert, *Theory of algebraic invariants*, Cambridge University Press, Cambridge, 1993.

[9] A. Kraus, Quelques remarques à propos des invariants c_4, c_6 et Δ d'une courbe elliptique. *Acta Arith.* **54** (1989), no. 1, 75–80.

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

[11] C. O'Neil, The period-index obstruction for elliptic curves. *J. Number Theory* **95** (2002), no. 2, 329–339.

[12] G. Salmon, *A treatise on the higher plane curves*, Third edition, Hodges, Foster and Figgis, Dublin, 1879.
[13] P. Serf, *The rank of elliptic curves over real quadratic number fields of class number* 1, PhD thesis, Universität des Saarlandes, Saarbrücken, 1995.
[14] J.H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, Springer-Verlag, New York, 1986.
[15] J.H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics **151**, Springer-Verlag, New York, 1994.
[16] A. Weil, Remarques sur un mémoire d'Hermite, *Arch. Math.* **5** (1954), 197–202.
[17] T. Womack, *Explicit descent on elliptic curves*, PhD thesis, University of Nottingham, 2003.

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