London Mathematical Society ISSN 1461–1570

MINIMAL MODELS FOR 2-COVERINGS OF ELLIPTIC CURVES

MICHAEL STOLL AND JOHN E. CREMONA

Abstract

This paper concerns the existence and algorithmic determination of minimal models for curves of genus 1, given by equations of the form $y^2 = Q(x)$ where $Q(x)$ has degree 4. These models are used in the method of 2-descent for computing the rank of an elliptic curve. Our results are complete for unramified extensions of $\mathbb{Q}_2$ and $\mathbb{Q}_3$ and for all p-adic fields for $p \geqslant 5$. Our primary motivation is to complete the results of Birch and Swinnerton-Dyer [**2**], which are incomplete in the case of $\mathbb{Q}_2$. Our results in this case (when applied to 2-coverings of elliptic curves over $\mathbb{Q}$) yield substantial improvements in the running times of the 2-descent algorithm implemented in the program `mwrank` [**5**]. The paper ends with a section on implementation and examples, and an appendix gives constructive proofs in sufficient detail to be used for implementation.

1. *Introduction*

The method of descent has been used since classical times for studying the arithmetic of elliptic curves. More recently, explicit algorithms for determining the Mordell-Weil and Selmer groups of elliptic curves over the rational field $\mathbb{Q}$, general number fields, and other global fields, have been developed. One of the best such general algorithms for arbitrary elliptic curves over $\mathbb{Q}$ is the 2-descent algorithm described by Birch and Swinnerton-Dyer in [**2**], which was used by them to determine the ranks of many elliptic curves in the work which led up to their famous (and still unproved) conjectures. A description of this algorithm, which is implemented in the second author's program `mwrank` (see [**5**]), may be found in [**3**].

In the 2-descent algorithm (over $\mathbb{Q}$), one embeds $E(\mathbb{Q})/2E(\mathbb{Q})$ into the 2-Selmer group $S^2(E/\mathbb{Q})$ of the elliptic curve E. Elements of S^2 are represented by plane quartic curves of the form $Y^2 = g(X)$, where $g(X)$ is a quartic polynomial whose classical invariants I, J (defined below) are related to the usual c_4 and c_6 invariants of the elliptic curve. In [**2**], an analysis of the minimal integral models for such 2-coverings was made for elliptic curves over $\mathbb{Q}$. This is a local question: for each odd prime p, there is a unique minimal pair (I_0, J_0) such that every integral quartic of the above form which represents a p-adically soluble 2-covering of E is isomorphic to one with this minimal pair of invariants. For primes $p > 3$ the minimality condition is simply that either $v_p(I) < 4$ or $v_p(J) < 6$, while for $p = 3$ there is a slightly more complicated condition, equivalent to the condition that $I = c_4$ and $J = 2c_6$ where (c_4, c_6) are the invariants of a p-minimal integral model for E over $\mathbb{Z}$.

Received 14th May 2002*; published ??*.
1991 Mathematics Subject Classification 11G05, 11G07, 14G20, 14Q05

The situation at the prime 2 is more complicated: the result given in [**2**, Lemma 5] is that, for a fixed elliptic curve E over $\mathbb{Q}$, the 2-adically minimal quartics defining 2-coverings of E may have either one or two different pairs of invariants (I, J): a basic or "small" pair (I_0, J_0), and in some cases, also the "large" pair $(I, J) = (2^4 I_0, 2^6 J_0)$. Sufficient conditions on (I_0, J_0) are given under which no large quartics are required, in the sense that any large quartics are equivalent (in a sense to be defined below) to small ones and hence redundant. However, these conditions are not necessary, so this result is not best possible, and one of our aims was to find best possible conditions. We solve the local problem of 2-adic minimality, increasing the number of cases in which large quartics can be eliminated by local considerations (see Lemma 6.1 and the table preceding it). Of course, it may (and often does) happen that there are no global (integer) quartics with the larger invariants, as this existence cannot be completely determined by purely local considerations.

The practical consequences of our results are to reduce the running time of the 2-descent program `mwrank` for many elliptic curves. In [**3**, p.92], we said

> It would appear that rational points in $E(\mathbb{Q})$ whose quartics have the larger pair of invariants lie in certain components of the 2-adic locus $E(\mathbb{Q}_2)$. Further study of this would be very useful, since if the search for quartics with the larger pair of invariants could be eliminated or curtailed, it could result in a major saving of time in the algorithm.

The program carries out a search for quartics with given invariants for each relevant pair (I, J), and clearly we do not want to waste time searching a large region for large quartics if there are none (or only redundant ones). Implementing our optimal criteria for the non-existence of large quartics is simple, and has a dramatic effect on the running time for the curves to which it applies (see Section 7 for details).

Secondly, when both small and large quartics exist, we had noticed (after much experience of running `mwrank` on many curves) that the elements of the 2-Selmer group which are represented by small quartics appear to form a subgroup, of index 1, 2 or 4. Our second goal was to prove that this is indeed the case, which we do (see Theorem 5.2 below). We define a group homomorphism from $E(\mathbb{Q}_2)$ to $(\mathbb{Z}/2\mathbb{Z})^2$ whose kernel, which obviously contains $2E(\mathbb{Q}_2)$, consists precisely of the points associated to small quartics, from which the result follows. Again, there are practical consequences of this in the implementation: details and examples will be given below. For example, if we know from the start that the local index is 2, then we may stop the search for further large quartics as soon as one is found. Examples may again be found below in Section 7.

In this paper we start by working over a general p-adic field, i.e. a finite field extension of the field of p-adic numbers $\mathbb{Q}_p$. Although we prove little new for $\mathbb{Q}_p$ itself when $p > 2$, we are interested in carrying out explicit 2-descents over general number fields, so we also wish to consider extensions of $\mathbb{Q}_p$ for general p. Many results carry over easily to unramified extensions. Some results of this nature were obtained by Serf in her thesis [**8**] (see also [**6**]).

In the next section, we introduce some terminology and state basic results about minimality of quartics. Some proofs are relegated to the appendix, since we wish to give them in sufficient detail to to be implementable as algorithms. Sections 3 and 4 concern the connection with elliptic curves, including a characterization of "small" quartics over a local field K which is an unramified extension of $\mathbb{Q}_2$. The case of $\mathbb{Q}_2$ itself in then considered in some more detail. In the final section, implications for the global situation and practical consequences are examined, together with examples computed using `mwrank`. Some of the more technical results, which are necessary for implementation purposes, are given in the Appendices.

Some of the material in Sections 2 and 3 is reminiscent of sections 2–4 of [**1**]; however, in [**1**] the case of additive reduction is not covered, and in the other cases it is not clear that our results can easily be deduced from those of [**1**].

This work was partially supported by a Visiting Fellowship from the Engineering and Physical Sciences Research Council of the UK.

2. *Basics*

Let K be a p-adic field, i.e. a finite extension of $\mathbb{Q}_p$, with ring of integers $\mathcal{O}_K$. The normalized (additive) valuation of K will be denoted v_K. We denote the ramification index of $K/\mathbb{Q}_p$ by e_K and the residue class degree by f_K. We choose a uniformizer π_K, for example $\pi_K = p$ when $e_K = 1$. The residue field is then $k = \mathcal{O}_K/\pi_K\mathcal{O}_K$.

We consider binary quartic forms ('quartics' for short)

$$Q(x,z) = a\,x^4 + b\,x^3z + c\,x^2z^2 + d\,xz^3 + e\,z^4$$

with coefficients $a, b, c, d, e \in K$. We will use the shorthand $Q = (a, b, c, d, e)$. There are the following well-known invariants:

$$\begin{aligned} I(Q) &= 12\,ae - 3\,bd + c^2; \\ J(Q) &= 72\,ace + 9\,bcd - 27\,ad^2 - 27\,b^2e - 2\,c^3; \\ \Delta(Q) &= \operatorname{disc}(Q) = \tfrac{1}{27}(4\,I^3 - J^2). \end{aligned}$$

Throughout this paper, we will tacitly assume that all quartics Q are nondegenerate, i.e. that $\Delta(Q) \neq 0$.

Definition 2.1.

(a) Two quartics Q and Q' will be called *K-equivalent* if there is a matrix $A = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{GL}(2,K)$ and some $\varepsilon \in K^\times$ such that

$$Q' = \varepsilon^2 Q \cdot A = \varepsilon^2 Q(\alpha x + \beta z, \gamma x + \delta z)\,.$$

Note that the invariants of Q and of Q' are then related by

$$I(Q') = \varepsilon^4 \det(A)^4 I(Q)\,, \quad J(Q') = \varepsilon^6 \det(A)^6 J(Q)\,, \quad \Delta(Q') = \varepsilon^{12} \det(A)^{12} \Delta(Q).$$

(b) A quartic Q is called *K-soluble* if there exist elements $\xi, \zeta \in K$, not both zero, such that $Q(\xi,\zeta)$ is a square in K.

(c) A quartic Q is called *K-trivial* if there exist elements $\xi, \zeta \in K$, not both zero, such that $Q(\xi,\zeta) = 0$.

Both the latter properties are compatible with K-equivalence. The pair of invariants (I, J) of an equivalence class is well-defined up to the action of $K^\times$, given by $(I, J) \mapsto (\varepsilon^4 I, \varepsilon^6 J)$ for $\varepsilon \in K^\times$. The unique class of trivial quartics with invariants I, J is represented by the quartic $(0, 1, 0, -27I, -27J)$: to see this, take the root to be $(\xi, \zeta) = (0, 1)$, so $e = 0$, and apply the transformation $\left(\begin{smallmatrix} 0 & 9d \\ 1 & -3c \end{smallmatrix}\right)$ with $\varepsilon = (3d)^{-1}$.

Provided that $\Delta(Q) \neq 0$, the affine equation $y^2 = Q(x, 1)$ defines a curve $\mathcal{C}_Q$ of genus 1 over K. This curve[1] has a K-rational point, and hence is an elliptic curve defined over K,

[1] or rather, its nonsingular projective model

if and only if Q is K-soluble. Whether soluble or not, the Jacobian of $\mathcal{C}_Q$ is the elliptic curve $E = E_{I,J}$ with equation

$$E_{I,J}: \quad y^2 = x^3 - 27Ix - 27J$$

where I and J are the invariants of Q, and there is a map $\phi : \mathcal{C}_Q \to E_{I,J}$ of degree 4 defined over K making the following diagram commute:

$$\begin{tikzcd} E \arrow[r, "{[2]}"] & E \\ \mathcal{C}_Q \arrow[u, "\theta"] \arrow[ur, "\phi"'] & \end{tikzcd} \tag{1}$$

Here, $[2]$ denotes the multiplication-by-2 map on E, and the vertical map θ is an isomorphism defined over an extension field $K(\alpha)$ where α is a root of Q. Such a diagram is known as a 2-*covering* of E.

If K is a number field and E an elliptic curve defined over K, then elements of the 2-Selmer group $S^2(E/K)$ are represented by 2-coverings, and hence by such curves $\mathcal{C}_Q$, with $Q(x, 1) \in K[x]$, which are K_v-soluble for all completions K_v of K. Such a global quartic is then *everywhere locally soluble*, or *ELS* for short. Note that since the Hasse principle fails for curves of genus 1, ELS quartics may not be globally soluble (over K). The process of 2-descent on an elliptic curve E involves the computation of its 2-Selmer group, and one way to do this is therefore to find all equivalence classes of ELS quartics with the appropriate invariants.

In general, over any field of characteristic neither 2 nor 3, we have a bijection between $E(K)/2E(K)$ (with $E = E_{I,J}$) and the set of equivalence classes of soluble quartics over K with invariants I, J. For future reference we now make this bijection explicit: for proofs, see [**4**]. A point $(\xi, \eta) \in E_{I,J}(K)$ maps to the class of the quartic $(1, 0, -6\xi, 8\eta, 108I - 3\xi^2)$, which has rational points at infinity and invariants $2^4 3^4 I$ and $2^6 3^6 J$.

Conversely, given a soluble quartic $Q = (a, b, c, d, e)$, we may assume (applying a suitable unimodular substitution) that the rational point is at infinity, so that the leading coefficient a is a square; then the corresponding point on $E_{I,J}$ is

$$(\xi, \eta) = \left(3\frac{3b^2 - 8ac}{4a}, 27\frac{b^3 + 8a^2d - 4abc}{8a^{3/2}}\right).$$

See [**4**] or [**3**] for the general formula, given an arbitrary rational point on $\mathcal{C}_Q$.

In this correspondence, the trivial coset $2E(K)$ corresponds to the class of trivial quartics.

Later on, we will be interested mainly in an elliptic curve E, which we will assume to be in the form $y^2 = x^3 + A\,x + B$, and its 2-coverings. In this case, the correspondence is as follows.

Proposition 2.2. *Let K be an arbitrary field of characteristic neither 2 nor 3, and let $E : y^2 = x^3 + A\,x + B$ be an elliptic curve over K. Then there is a map*

$$Q_E : E(K)/2E(K) \longrightarrow K\text{-equivalence classes of quartics}$$

given by mapping the class of a point $(\xi, \eta) \in E(K)$ to the class of the quartic $Q = (1, 0, -6\xi, 8\eta, -3\xi^2 - 4A)$. The map Q_E is injective, and the image consists exactly of the K-soluble K-equivalence classes of quartics with invariants $(I, J) = (-3\,A, (-3)^3\,B)$

(modulo the action of $K^\times$ on (I, J)). The image of the zero element under Q_E is the trivial equivalence class of quartics, containing $(0, 1, 0, A, B)$.

We will also use Q_E to denote the induced map from $E(K)$ to classes of quartics.

We now return to the case where K is a local field.

Definition 2.3. We define the *level* of a quartic Q to be the integer

$$\operatorname{level}(Q) = \lfloor \min\{v_K(I)/4, v_K(J)/6\} \rfloor.$$

In each K-equivalence class of quartics, there are certainly forms with coefficients in $\mathcal{O}_K$ (replace Q by $\varepsilon^2 Q$ for suitable ε); these integral forms have non-negative level. We call an integral form Q *K-minimal* if it satisfies $\operatorname{level}(Q) \leqslant \operatorname{level}(Q')$ for all equivalent integral forms Q'; otherwise we call Q *K-nonminimal*.

Clearly each class of forms has minimal elements. We will be concerned with determining the level of K-minimal quartics. From the formulae given in Definition 2.1, we have (in the notation used there)

$$\operatorname{level}(Q') = \operatorname{level}(Q) + v_K(\varepsilon \det(A)). \tag{2}$$

Integral forms of level 0 are clearly minimal, but the converse is false in general, as we will see.

3. *Levels of minimal soluble quartics*

Our goal in this section is to prove the following result.

Theorem 3.1. *Over a p-adic local field K, all soluble minimal integral quartic forms Q have level satisfying*

$$\operatorname{level}(Q) \begin{cases} = 0 & \text{if } p \geqslant 5; \\ \leqslant \lfloor (1+e_K)/2 \rfloor & \text{if } p = 3; \\ \leqslant e_K & \text{if } p = 2. \end{cases}$$

In particular, if K is unramified then $\operatorname{level}(Q) \leqslant 1$.

PROOF: By Prop. 2.2, every such quartic Q belongs to a class $Q_E(\xi, \eta)$ for some elliptic curve E over K and some point $(\xi, \eta) \in E(K)$. If this point is integral (i.e., we have $\xi, \eta \in \mathcal{O}_K$), then the given representative quartic Q' is also integral (and vice versa). We can choose E to be given by an equation $y^2 = x^3 + Ax + B$ with $0 \leqslant \min\{3v_K(A), 2v_K(B)\} < 12$. Then, since $I(Q') = -3 \cdot 2^4 A$ and $J(Q') = (-3)^3 \cdot 2^6 B$, it follows that $\operatorname{level}(Q') = 0$ for $p \geqslant 5$, $\operatorname{level}(Q') \leqslant \lfloor (1 + e_K)/2 \rfloor$ for $p = 3$, and $\operatorname{level}(Q') = e_K$ for $p = 2$. Since the level of the minimal forms within an equivalence class is uniquely determined, this proves the theorem for quartics in classes that are images of integral points as above.

Hence it only remains to prove the theorem for the images of non-integral points. These points (together with the zero of the group law) make up the kernel of reduction of our model for E. We will use the customary notation $E^1(K)$ for this kernel of reduction, and more generally, $E^n(K)$ for the nth kernel of reduction, consisting of the $(\xi, \eta) \in E(K)$ such that $v_K(\xi) \leqslant -2n$, $v_K(\eta) \leqslant -3n$, together with $0 \in E(K)$. (Caution: If $p = 2$ or

$p = 3$, our model for E is not necessarily minimal, and therefore our $E^n(K)$ may differ from the usual definition.) Now it is a well-known fact that $E^1(K)$ is isomorphic to the $\pi_K \mathcal{O}_K$-points of a certain formal group; in particular, $E^1(K)$ is an $\mathcal{O}_K$-module. Since $2 \in \mathcal{O}_K^\times$ when p is odd, all quartics corresponding to non-integral points are trivial in this case. The remaining case follows from the following result. $\square$

Proposition 3.2. *Let K be a 2-adic local field and let $E : y^2 = x^3 + A\,x + B$ with $0 \leqslant \min\{3v_K(A), 2v_K(B)\} < 12$ be an elliptic curve over K. Then the image of $E^n(K)$ under Q_E consists of classes of level at most $\max\{e_K - n, 0\}$, and is just the trivial class when $n > e_K$.*

PROOF: The points in $E^1(K)$ are parametrized by $\pi_K \mathcal{O}_K$ in the following way.

$$\pi_K \mathcal{O}_K \ni t \longmapsto P(t) = (t^{-2} f(t), t^{-3} f(t)) \in E^1(K)\,,$$

where

$$f(t) = 1 - A\,t^4 - B\,t^6 \pm \cdots = 1 + t^4 f_1(t)$$

is a power series with coefficients in $\mathcal{O}_K$, see [**7**, Prop. VII.2.2]. The quartic representing $Q_E(P(t))$ is then given by

$$Q_1(x, z) = (1, 0, -6t^{-2} f(t), 8t^{-3} f(t), -3t^{-4} f(t)^2 - 4A)\,.$$

Let $n = v_K(t) \geqslant 1$. We scale:

$$Q_2(x, z) = Q_1(x, tz) = (1, 0, -6f(t), 8f(t), -3f(t)^2 - 4t^4 A)$$

and shift:

$$Q_3(x, z) = Q_2(x + z, z) = (1, 4, -6t^4 f_1(t), -4t^4 f_1(t), -4t^6 f_2(t) - 3t^8 f_1(t)^2)\,,$$

where we have set $f_1(t) = -A + t^2 f_2(t)$. The valuations of the coefficients are

$$(\,= 0,\ = 2e_K,\ \geqslant 4n + e_K,\ \geqslant 4n + 2e_K,\ \geqslant \min\{6n + 2e_K, 8n\})\,.$$

If $n > e_K$, then the Newton polygon of Q_3 has a vertex at $x^3 z$, hence Q_3 splits off a linear factor over K, and the class of Q_3 is the trivial class (this implies $P(t) \in 2E(K)$). In particular, the image of $P(t)$ has level 0 in this case.

If $n = e_K$, we can scale to get an integral quartic $Q_4(x, z) = Q_3(x, z/4)$ of level 0, hence $Q_E(P(t))$ has level 0.

In the remaining case, $1 \leqslant n < e_K$, we have $2e_K > 2n$, $4n+e_K > 4n$, $4n+2e_K > 6n$, therefore we can scale to get an integral quartic $Q_5(x, z) = Q_3(x, z/t^2)$ of level $e_K - n$. $\square$

Note that it is possible to have classes of level e_K in the image when $p = 2$. For example, if there is a point (ξ, η) with $v_K(\xi) = 1$ (and $v_K(-3\xi^2 - 4A) < 4$ if $e_K = 1$), then the quartic representing its image is minimal by Lemma 5.1 below, and the class has level e_K. This means that the above result is best possible.

4. *Criteria for minimality*

In this section, we derive criteria for when a given integral quartic (usually supposed to be K-soluble) over a p-adic local field K is minimal. Though parts of the results given here follow from Theorem 3.1 or arguments similar to those used for its proof, we will provide alternative proofs here that are constructive and can be turned into an algorithm for minimizing a given quartic.

Definition 4.1. The *valuation* of a quartic $Q = (a, b, c, d, e)$ over a p-adic local field K is defined to be

$$v_K(Q) = \min\{v_K(a), v_K(b), v_K(c), v_K(d), v_K(e)\} .$$

Note that we always have $v_K(Q) \leqslant 2 \operatorname{level}(Q)$.

We denote by K^{nr} the maximal unramified extension of K.

We begin with the simplest case.

Proposition 4.2. *Let K be a p-adic field where $p \geqslant 5$ and let Q be an integral quartic over K.*

(1) If $v_K(Q) \geqslant 2$, then Q is K-nonminimal.

(2) If $\operatorname{level}(Q) = 0$, then Q is K-minimal.

(3) If $\operatorname{level}(Q) = 1$ and $v_K(Q) = 0$, then Q is K-nonminimal.

(4) If $\operatorname{level}(Q) = 1$ and $v_K(Q) = 1$, then Q is K-nonminimal if it is K^{nr}-soluble.

(5) If $\operatorname{level}(Q) \geqslant 2$, then Q is K-nonminimal.

In particular, a K-soluble integral quartic is K-minimal if and only if it has level 0.

PROOF: The proof of [**2**, Lemma 3] for $\mathbb{Q}_p$ goes over unchanged to arbitrary extensions of $\mathbb{Q}_p$ for $p \geqslant 5$. See Prop. A.3 in Appendix A for details. This proof may easily be turned into an algorithm for reducing quartics for which $v_K(I) \geqslant 4$ and $v_K(J) \geqslant 6$; all we need to be able to do is to locate multiple roots of quartics with coefficients in the finite field $\mathcal{O}_K/\pi\mathcal{O}_K$. □

Note that the solubility assumption in part (4) is necessary, as shown by the example $Q = (\pi, 0, 0, 0, \pi^3)$, which is of level 1 and K-minimal by Lemma 5.1 below.

The next complicated case is when the residue characteristic is 3.

Proposition 4.3. *Let K be an unramified* 3*-adic field. Then an integral quartic which is K^{nr}-soluble is K-nonminimal if and only if* either $v_K(I) \geqslant 5$ *and* $v_K(J) \geqslant 9$, or $v_K(I) = 4$, $v_K(J) = 6$ *and* $v_K(\Delta) \geqslant 12$. *In particular, minimal quartics have level* 0 *or* 1.

PROOF: For $K = \mathbb{Q}_3$, this is [**2**, Lemma 4], though the proof was omitted there. See Appendix A, Prop. A.4 for a proof, which only uses $v_K(3) = 1$, and so applies to unramified extensions of $\mathbb{Q}_3$.

The last statement also follows from Theorem 3.1, since $e_K = 1$. □

In the unramified 3-adic case, the minimal level depends only on the invariants, and is at most 1. In the ramified case ($e_K = v_K(3) \geqslant 2$) we have the following generalization.

Proposition 4.4. *Let K be a* 3*-adic field with ramification degree $e_K \geqslant 1$. Let Q be an integral K-soluble quartic with invariants I, J. Assume that Q is K-nonminimal. Then one of the following conditions holds:*

1. $v_K(I) = 2i + 4$ *and* $v_K(J) = 3i + 6$, *for some* $i \in \mathbb{Z}$ *with* $0 \leqslant i < e_K/2$;
2. $v_K(I) \geqslant e_K + 4$, *and* $v_K(J) = 3i + 6$ *for some* $i \in \mathbb{Z}$ *with* $e_K/2 \leqslant i < e_K$;
3. $v_K(I) \geqslant e_K + 4$ *and* $v_K(J) \geqslant 3e_K + 6$.

Condition (3) *is always sufficient for nonminimality.*

When $e_K = 1$, condition (1) *is also sufficient, provided also that* $v_K(\Delta) \geqslant 12$. *(Condition* (2) *does not occur.)*

When $e_K = 2$, condition (1) *is sufficient provided also that $v_K(\Delta) \geqslant 12$, and condition* (2) *is sufficient provided also that $v_K(\Delta) \geqslant 15$.*

PROOF: For the necessity, it is an easy exercise to show that an integral quartic with $i = v_K(c)$ has invariants satisfying *either* $v_K(I) = 2i$ and $v_K(J) = 3i$ for some i with $0 \leqslant i < e_K/2$; *or* $v_K(I) \geqslant e_K$ and $v_K(J) = 3i$ for some i with $e_K/2 \leqslant i < e_K$; *or* $v_K(I) \geqslant e_K$ and $v_K(J) \geqslant 3e_K$. Since any nonminimal quartic has valuations of (I, J) that are by a multiple of $(4, 6)$ larger than those of a minimal one, necessity follows.

When $e_K = 1$, the sufficiency has already been proved; for $e_K = 2$, see [**8**, pp. 193–200]. The method of proof used in [**8**], and in Appendix A in the unramified case, becomes exceedingly tedious when there are many cases to consider. Sufficiency of the third condition follows (though non-constructively) from a consideration of the map Q_E on integral points, since the representative quartic Q has $v_K(I(Q)) < e_k + 4$ or $v_K(J(Q)) < 3e_k + 6$. □

Finally, we consider the hardest case of 2-adic fields, where the minimal level cannot be determined from the invariants alone, even for an unramified 2-adic field such as $\mathbb{Q}_2$. Over $\mathbb{Q}_2$, the best previously known result which depends only on the invariants is Lemma 5 of [**2**], which states that (over $K = \mathbb{Q}_2$), if $v_K(I) \geqslant 6$, $v_K(J) \geqslant 9$, and $v_K(8I + J) \geqslant 10$, then every K-soluble quartic with invariants (I, J) is nonminimal. This result was extended to quadratic extensions of $\mathbb{Q}_2$ in [**8**], where fairly strong conditions were stated which are satisfied by minimal quartics over $\mathbb{Q}_2$ with level 1. In Section 6 below, we improve the result of [**2**] (compare Lemma 6.1).

The following result is best possible in the unramified 2-adic case. We express it in as invariant a way as possible, namely invariant under $\mathrm{SL}(2, \mathcal{O}_K)$.

Proposition 4.5. *Let K be an unramified 2-adic field. Then an integral quartic Q which is K^{nr}-soluble is K-minimal if and only if* either *it has level* 0*,* or *it has level* 1 *and satisfies one of the following conditions.*

1. *$v(Q) = 1$, and $\frac{1}{2}Q$ has a quadruple root modulo* 2 *and no root modulo* 8*;*
2. *$v(Q) = 0$, and Q has a quadruple root modulo* 4 *and no root modulo* 16*.*

In particular, if $v(I) \geqslant 6$, $v(J) \geqslant 9$ and $v(8I + J) \geqslant 10$ then Q is nonminimal; as a special case, quartics of level at least 2 *are nonminimal.*

The condition above can be explained as follows: $Q_1 = 2^{-v(Q)}Q$ has a unique multiple root modulo 2, which has multiplicity at least 3 (this follows from the vanishing of $I(Q_1)$ and $J(Q_1)$ modulo 2 for forms of level 1). If the multiplicity is only 3, then the form is nonminimal, while if the multiplicity is 4 then minimality depends on the valuation of the constant term after shifting the multiple root to $0 \bmod 2$.

An alternative formulation of the result is as follows. *An integral and soluble quartic of level* 1 *is minimal if and only if it is* $\mathrm{SL}(2, \mathcal{O}_K)$*-equivalent to a quartic (a, b, c, d, e) with $v_K(a) \leqslant 1$, $v_K(b), v_K(c), v_K(d) \geqslant 2$ and $2 \leqslant v_K(e) \leqslant 3$.* Compare Lemma 5.1 below.

PROOF: We give the details in Appendix A, Prop. A.5, again in a form which may be used as part of an algorithm for minimizing quartics over $\mathbb{Z}$. □

We do not have a best possible result on minimality of quartics for general 2-adic fields, but at least we know by Theorem 3.1 that the level of a K-minimal K-soluble quartic is at most e_K.

REMARK: Over an unramified 2-adic field, we may consider more general equations of soluble 2-covering curves, of the form

$$Y^2 + P(X)Y = Q(X),$$

where Q is a quartic and $\deg(P) \leqslant 2$. Every soluble 2-covering of an elliptic curve over K has such an equation of level 0 (with an obvious extension of the definition of level to such equations). However, we have found the use of such equations less convenient for computations. The situation is similar to that of minimal Weierstrass models for elliptic curves over 2-adic fields, where equations of the form $Y^2 =$ cubic do not suffice.

5. *Characterization of small quartics when $K/\mathbb{Q}_2$ is unramified*

In this section, we restrict to the case where $p = 2$, and K is an *unramified* extension of $\mathbb{Q}_2$. Let E be an elliptic curve over K as above. The image of Q_E consists of classes of quartics of levels 0 and (possibly) 1: we call a class in the image of Q_E *small* if its level is zero and *large* otherwise.

The following Lemma is also used in the proof of Prop. 4.5, see Appendix A. The "only if" direction of the Lemma was proved (for $\mathbb{Q}_2$) in [**8**], but there is no proof there for the "if" direction. We remedy that here. One corollary is that the algorithm for reducing quartics over $\mathbb{Q}_2$ which is implicit in [**8**] and implemented in the second author's program `mwrank` (see [**3**]) is always guaranteed to produce a minimal integral quartic equivalent to a given one. We only need this result when K is a 2-adic field, but we state and prove it for general p-adic fields.

Lemma 5.1. *Let $Q = (a, b, c, d, e)$ be an integral quartic over a p-adic field K such that*

$$v_K(a) \leqslant 1, \quad v_K(b) \geqslant 2, \quad v_K(c) \geqslant 2, \quad v_K(d) \geqslant 3, \quad v_K(e) \geqslant 2\,.$$

Then Q is K-minimal if and only if $v_K(e) \leqslant 3$.

PROOF: If $v_K(e) \geqslant 4$, then we can scale Q to get $Q_1(x, z) = Q(x, z/\pi_K)$, which is still integral and has smaller invariants, so Q is nonminimal in this case.

So suppose now that $v_K(e) \leqslant 3$. If Q were nonminimal, there would be a matrix $A = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right) \in \mathrm{GL}(2, K)$ and an $\varepsilon \in K^\times$ with $v_K(\varepsilon) + v_K(\det A) \leqslant -1$ (compare (2)) such that

$$Q_1(x, z) = (a_1, b_1, c_1, d_1, e_1) = \varepsilon^2 Q(\alpha x + \beta z, \gamma x + \delta z)$$

is integral. By changing (ε, A) into $(\pi_K^{-2n}\varepsilon, \pi_K^n A)$ for a suitable $n \in \mathbb{Z}$, we can assume that A has integral entries not all divisible by π_K. Then we have $v_K(\varepsilon) \leqslant -1 - v_K(\det A) \leqslant -1$. We observe that

$$\begin{aligned} \varepsilon^{-2} a_1 &= Q(\alpha, \gamma) = a\alpha^4 + b\alpha^3\gamma + c\alpha^2\gamma^2 + d\alpha\gamma^3 + e\gamma^4, \\ \varepsilon^{-2} e_1 &= Q(\beta, \delta) = a\beta^4 + b\beta^3\delta + c\beta^2\delta^2 + d\beta\delta^3 + e\delta^4. \end{aligned}$$

The first of these equations implies (considering the valuations of the various terms) that $v_K(\alpha) \geqslant 1$. Similarly, we get from the second equation that $v_K(\beta) \geqslant 1$. This implies $v_K(\det A) \geqslant 1$ and therefore $v_K(\varepsilon) \leqslant -2$. Looking at the two equations again, we see that we must now have both $v_K(\gamma) \geqslant 1$ and $v_K(\delta) \geqslant 1$, contradicting our choice of the matrix A. Hence Q must be minimal. □

We wish to characterize the points of $E(K)$ whose image is small. This characterization will finally lead to the following result, which then can be used to improve the `mwrank` program.

Theorem 5.2. *The set of elements of $E(K)/2E(K)$ that map to small classes is a subgroup, and its index can be determined explicitly. When $K = \mathbb{Q}_2$, the index is at most 4.*

The first step is to get some criterion in terms of (the coordinates of) a point $P \in E(K)$ for when its image under Q_E is small. We already know by Theorem 3.1 that the levels of the classes in the image are either 0 or 1, and by Proposition 3.2 that the image of $E^1(K)$ consists of small classes. We can therefore restrict our attention to points with integral coordinates. For the following, we need some more notation.

Definition 5.3. We denote by t the automorphism of K such that $t(\xi)^2 \equiv \xi \bmod 2$ for all $\xi \in \mathcal{O}_K$. We denote by u the map $K \ni \xi \mapsto (\xi - t(\xi)^2)/2 \in K$; note that u maps $\mathcal{O}_K$ into itself. If $K = \mathbb{Q}_2$, then t is simply the identity.

Lemma 5.4. *t and u have the following properties.*

(1) t is additive and multiplicative and preserves the valuation.

(2) For all $\xi, \eta \in K$:

$$u(\xi + \eta) = u(\xi) + u(\eta) - t(\xi\eta) \qquad \textit{and} \qquad u(-\xi) = u(\xi) - \xi\,.$$

(3) For all $\xi, \eta \in K$:

$$u(\xi\eta) = \xi u(\eta) + \eta u(\xi) - 2u(\xi)u(\eta)\,.$$

(4) For all $\xi, \eta \in \mathcal{O}_K$ and all $n \geqslant 0$:

$$\xi \equiv \eta \bmod 2^{n+1} \Longrightarrow u(\xi) \equiv u(\eta) \bmod 2^n\,.$$

(5) For all $\xi, \eta \in \mathcal{O}_K$:

$$u(\xi + 2\eta) \equiv u(\xi) + \eta \bmod 2\,.$$

(6) For all $\xi \in \mathcal{O}_K$:

$$u(\xi) \equiv 0 \bmod 2 \iff \xi \textit{ is a square mod 4}\,.$$

PROOF: Easy. □

Now we can formulate our criterion.

Lemma 5.5. *Let $P = (\xi, \eta) \in E(K) \setminus E^1(K)$ be an integral point. Then $Q_E(P)$ is small if and only if*

$$v_K\big(u(\xi)^2 - A + 2t(\xi)(\eta - t(\xi)^3 - t(\xi)u(\xi))\big) \geqslant 2\,,$$

or equivalently, if and only if

$$u(\xi) \equiv t(A) \bmod 2 \qquad \textit{and} \qquad B\xi \equiv u(A)^2 \bmod 2\,.$$

PROOF: The quartic representing the class $Q_E(P)$ is given as

$$Q_1(x, z) = (1, 0, -6\xi, 8\eta, -3\xi^2 - 4A)\,,$$

which has level 1. We do a shift:

$$\begin{aligned} Q_2(x,z) &= Q_1(x+t(\xi)z,z) \\ &= \Big(1, 4t(\xi), -12u(\xi), 8(\eta - t(\xi)^3 - 3t(\xi)u(\xi)), \\ &\qquad -4\big(A + 3u(\xi)^2 - 2t(\xi)(\eta - t(\xi)^3 - 3t(\xi)^2u(\xi))\big)\Big)\,. \end{aligned}$$

To this quartic, we can apply Lemma 5.1. It tells us that Q_2 is nonminimal (and hence the class is small) if and only if the valuation of its z^4 term is at least 4; this proves the first claim. To see the equivalence, note first that a necessary condition is that $u(\xi)^2 \equiv A \bmod 2$; this is equivalent to $u(\xi) \equiv t(A) \bmod 2$. If this condition holds, it follows that $u(\xi)^2 \equiv t(A)^2 \bmod 4$, hence $u(\xi)^2 - A \equiv 2u(A) \bmod 4$. In this case, the first condition is equivalent with (mod 2)

$$\begin{aligned} 0 &\equiv u(A) + t(\xi)(\eta - t(\xi)^3 - t(\xi)u(\xi)) \\ &\equiv u(A) + t(\xi(\eta^2 - \xi^3 - A\xi)) \\ &\equiv t(u(A)^2 + B\xi)\,, \end{aligned}$$

and since t is an automorphism, this is equivalent to $B\xi \equiv u(A)^2 \bmod 2$. □

We now proceed to show that the points mapping to small classes form a subgroup. We need a little lemma.

Lemma 5.6. *Suppose $P_1, P_2, P_3 \in E(K)$ are three points such that $P_1+P_2+P_3 = 0$ and such that $P_3 \in E^1(K)$, but $P_1, P_2 \in E(K) \setminus E^1(K)$. Let $P_j = (\xi_j, \eta_j)$ for $j = 1, 2, 3$. Then we have $\xi_1 \equiv \xi_2 \bmod 4$.*

PROOF: ξ_j and η_j are integral for $j = 1, 2$, while $\xi_3 = \xi/4^n$ with ξ a unit and $n \geqslant 1$. Set $\lambda = (\eta_2 - \eta_1)/(\xi_2 - \xi_1) = (\eta_3 - \eta_1)/(\xi_3 - \xi_1) = 2^{-n}\epsilon$ with ϵ a unit; now

$$2^n(\eta_2 - \eta_1) = \epsilon(\xi_2 - \xi_1)$$

so (since $n > 0$) $\xi_2 \equiv \xi_1 \bmod 2$. Hence $\eta_2 \equiv \eta_1 \bmod 2$ (from the equation for E, since squaring is an automorphism modulo 2), hence $\xi_2 \equiv \xi_1 \bmod 4$ from the previous equation again. □

Since $\pi_K = 2$, the residue field is $k = \mathcal{O}_K/2\mathcal{O}_K$.

Proposition 5.7. *The map $\tilde\Phi : E(K) \longrightarrow k \times k$, defined as follows,*

$$\tilde\Phi : \begin{cases} E^1(K) \ni P & \longmapsto \quad (0,0) \\ E(K) \setminus E^1(K) \ni (\xi,\eta) & \longmapsto \quad (u(\xi)^2 + A, B\xi + u(A)^2 + (u(\xi)^2 + A)\xi^2) \end{cases}$$

is a homomorphism. It therefore induces a homomorphism

$$\Phi : E(K)/(2E(K) + E^1(K)) \longrightarrow k \times k\,.$$

The kernel of Φ consists exactly of those points that map under Q_E to small classes of quartics.

PROOF: Take three points $P_1, P_2, P_3 \in E(K)$ such that $P_1 + P_2 + P_3 = 0$. We have to show that $\tilde\Phi(P_1) + \tilde\Phi(P_2) + \tilde\Phi(P_3) = 0$.

Suppose first that two of the points are in $E^1(K)$. Then so must be the third, and $\tilde\Phi(P_j) = 0$ for $j = 1, 2, 3$.

If exactly one of the points, P_3 say, is in $E^1(K)$, then by Lemma 5.6, the x-coordinates of P_1 and P_2 are congruent mod 4. Hence $\tilde\Phi(P_1) = \tilde\Phi(P_2)$ and so $\tilde\Phi(P_1) + \tilde\Phi(P_2) +$

$\tilde{\Phi}(P_3) = 0$ as required (note that $\tilde{\Phi}(\xi, \eta)$ only depends on $\xi \bmod 4$ if the point is integral, compare Lemma 5.4, (4)).

Finally suppose that all three points are in $E(K) \setminus E^1(K)$. Then P_1, P_2, P_3 lie on a line of equation $y = \lambda x + \mu$ with λ and μ integral. Writing $P_j = (\xi_j, \eta_j)$, we have the relations

$$\xi_1 + \xi_2 + \xi_3 = \lambda^2, \quad \xi_1\xi_2 + \xi_2\xi_3 + \xi_3\xi_1 = A - 2\lambda\mu, \quad \xi_1\xi_2\xi_3 = \mu^2 - B\,. \tag{3}$$

Apply u to the first equation and use Lemma 5.4 to get (mod 2)

$$\begin{aligned} 0 &\equiv u(\lambda^2) = u(\xi_1 + \xi_2 + \xi_3) \\ &\equiv u(\xi_1) + u(\xi_2) + u(\xi_3) + t(\xi_1\xi_2 + \xi_2\xi_3 + \xi_3\xi_1) \\ &\equiv u(\xi_1) + u(\xi_2) + u(\xi_3) + t(A)\,, \end{aligned}$$

so that we have

$$u(\xi_1) + u(\xi_2) + u(\xi_3) \equiv t(A) \bmod 2\,. \tag{4}$$

Square both sides to get

$$\sum_{j=1}^{3} (u(\xi_j)^2 + A) \equiv 0 \bmod 2\,;$$

this shows that the first component of $\tilde{\Phi}$ is a homomorphism.

Now apply u to the second equation in (3) (and use Lemma 5.4 again) to get (again mod 2)

$$\begin{aligned} u(A) + \lambda\mu &\equiv u(A - 2\lambda\mu) = u(\xi_1\xi_2 + \xi_2\xi_3 + \xi_3\xi_1) \\ &\equiv \xi_1(u(\xi_2) + u(\xi_3)) + \xi_2(u(\xi_3) + u(\xi_1)) + \xi_3(u(\xi_1) + u(\xi_2)) \\ &\qquad + t(\xi_1\xi_2\xi_3)t(\xi_1 + \xi_2 + \xi_3) \\ &\overset{\text{use (4)}}{\equiv} \xi_1(u(\xi_1) + t(A)) + \xi_2(u(\xi_2) + t(A)) + \xi_3(u(\xi_3) + t(A)) \\ &\qquad + t(\lambda^2\mu^2) + t((\xi_1 + \xi_2 + \xi_3)B) \\ &\equiv \lambda\mu + \sum_{j=1}^{3} \bigl(\xi_j(u(\xi_j) + t(A)) + t(B\xi_j)\bigr)\,. \end{aligned}$$

Squaring this, we finally get

$$\sum_{j=1}^{3} \bigl(B\xi_j + u(A)^2 + (u(\xi_j)^2 + A)\xi_j^2\bigr) \equiv 0 \bmod 2\,;$$

this shows that also the second component of $\tilde{\Phi}$ is a homomorphism.

The assertion that $\tilde{\Phi}$ induces the homomorphism Φ is clear.

Finally, the last assertion follows immediately from Lemma 5.5 and the fact that points in $E^1(K)$ map to small classes of quartics. □

The practical aspect of this result is that we can find the subgroup of $E(K)$ mapping to small classes by applying the map Φ to a set of representatives of $E(K)/(2E(K) + E^1(K))$. This is easily done for any given elliptic curve. In the special case $K = \mathbb{Q}_2$, a very explicit description is given below in Section 6.

We also see that this subgroup has index at most $\#k^2 = 4^{f_K}$ in $E(K)$. This information is only interesting when $K = \mathbb{Q}_2$, however (bounding the index by 4 in this case), since we always have $\#E(K)/2E(K) \leqslant 2^{2+f_K}$.

Since the image of Q_E consists exactly of the equivalence classes of soluble 2-coverings of E, we can define a map Ψ from soluble quartics with invariants corresponding to E to $k \times k$ by first applying the inverse of Q_E. A formula for $\Psi(Q)$ involving the x-coordinate of a K-rational point on the corresponding 2-covering can easily be derived; it appears, however, that it is not possible to give a formula just in terms of the coefficients of Q.

6. *The case* $K = \mathbb{Q}_2$

The most important case for practical application is when $K = \mathbb{Q}_2$. Our results can then be used to improve the algorithm behind the `mwrank` program, see [**3**]. We give examples to illustrate the improvement in running time in the next section.

When $K = \mathbb{Q}_2$, the formulae in our results can be simplified by observing that t is simply the identity and that we have $u(\xi) \equiv 0 \bmod 2$ for $\xi \equiv 0, 1 \bmod 4$ and $u(\xi) \equiv 1 \bmod 2$ for $\xi \equiv 2, 3 \bmod 4$. This leads to the following table of values of Φ. Each entry corresponds to given residues of A mod 4, B mod 2 and ξ mod 4.

		$\xi \equiv 0$	$\xi \equiv 1$	$\xi \equiv 2$	$\xi \equiv 3$
B even	$A \equiv 0$	$(0,0)$	$(0,0)$	$(1,0)$	$(1,1)$
	$A \equiv 1$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,0)$
	$A \equiv 2$	$(0,1)$	$(0,1)$	$(1,1)$	$(1,0)$
	$A \equiv 3$	$(1,1)$	$(1,0)$	$(0,1)$	$(0,1)$
B odd	$A \equiv 0$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,0)$
	$A \equiv 1$	$(1,0)$	$(1,0)$	$(0,0)$	$(0,1)$
	$A \equiv 2$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,1)$
	$A \equiv 3$	$(1,1)$	$(1,1)$	$(0,1)$	$(0,0)$

If we take into account the residue class of B mod 4, then we can exclude certain residue classes for ξ, since the right hand side of the curve equation is a non-square mod 4. In the following table, each entry corresponds to given residues of A and B mod 4 and lists the residue classes mod 4 such that a point $(\xi, \eta) \in E(\mathbb{Q}_2)$ with ξ in one of these residue classes has non-trivial image under Φ (or, equivalently, maps to a large class of quartics under $\mathbb{Q}_E$).

	$A \equiv 0$	$A \equiv 1$	$A \equiv 2$	$A \equiv 3$
$B \equiv 0$	2	$\underline{0}$	$0, 2, \mathbf{3}$	$\underline{0}, 1, 3$
$B \equiv 1$	$2, \underline{3}$	$\mathbf{0}$	$\mathit{0, 2}$	$\mathbf{0}, 1$
$B \equiv 2$	$\mathbf{3}$	1	$\mathbf{1}$	$\underline{2}$
$B \equiv 3$	$\underline{1}$	$\mathit{1, 3}$	$\underline{3}$	$\mathbf{2}$

The entries in boldface stand for residue classes that always contain the x-coordinate of some point in $E(\mathbb{Q}_2)$ because $\xi^3 + A\xi + B$ can always be made to be $\equiv 1 \bmod 8$. The entries in italics stand for pairs of residue classes such that exactly one of them gives rise to a point in this way (depending on A and $B \bmod 8$). The underlined entries indicate residue classes that contain a 2-torsion point. (When A is odd and B is even, then there is a zero of $\xi^3 + A\xi + B$ with $\xi \equiv B \bmod 4$, as can be seen from the Newton polygon. When A is even and B is odd, then we can apply the same argument after shifting ξ by 1; this gives a zero $\xi \equiv A + B + 2 \bmod 4$.)

We proceed to show that when $A \equiv 2$ or 3 and $B \equiv 0$ mod 4, there is a point with ξ-coordinate of the same parity as A. This then implies that Φ is surjective. Consider first the case $A \equiv 2$. Then the Newton polygon of $f(\xi) = \xi^3 + A\xi + B$ has a length 1 segment of slope $\geqslant 1$, hence f has a zero $\xi \in 2\mathbb{Z}_2$. In the other case, $A \equiv 3$: if $A + B + 1 \equiv 0 \bmod 8$ then we shift ξ by 1 to get the same situation as before, so that f has a zero $\xi \in 1 + 2\mathbb{Z}_2$; if $A + B + 1 \equiv 4 \bmod 8$ then one can see that for some $\xi \in 1 + 4\mathbb{Z}_2$ we have $f(\xi) \equiv 4 \bmod 32$, so that $f(\xi)$ is a square.

Collecting this information (and taking into account the values of Φ taken on the various residue classes), we get the following table for the possible values of the size of the image of Φ, or the index in $E(\mathbb{Q}_2)$ of the subgroup corresponding to small quartics.

	$A \equiv 0$	$A \equiv 1$	$A \equiv 2$	$A \equiv 3$
$B \equiv 0$	$1, 2$	2	4	4
$B \equiv 1$	2	2	2	2
$B \equiv 2$	2	$1, 2$	2	2
$B \equiv 3$	2	2	2	2

In the two cases where it is possible to have no large quartics, namely A is a square mod 4 and $B \equiv 2A \bmod 4$, we have to check whether the curve has a point in the specified residue class. This can easily be done by a recursive procedure that tests whether $\xi^3 + A\xi + B$ is a square or not if this can be decided on the current knowledge about ξ. If this cannot be decided, the current residue class for ξ is split into two residue classes modulo the next higher power of 2. In Appendix B we discuss this further, and give a more efficient non-recursive algorithm for determining the index in these two cases. Here we can give a more specific result, improving on an old result due to Birch and Swinnerton-Dyer [**2**] (their result covers the case $A, B \equiv 0 \bmod 4$ and $16 \mid 2A + B$). The following Lemma allows us to determine the index precisely in three quarters of the ambiguous cases.

Lemma 6.1.

(a) *Suppose that* $A \equiv B \equiv 0 \bmod 4$.
  - *(1)* *If* $2A + B \equiv 0$ *or* $4 \bmod 16$*, then there are no large classes of quartics (i.e., the image of* Φ *is trivial);*
  - *(2)* *if* $(A, B) \equiv (0, 8), (0, 12), (8, 8)$ *or* $(8, 12) \bmod 16$*, then there are large classes of quartics (i.e.,* Φ *is non-trivial);*

(b) *Suppose that* $A \equiv 1$*,* $B \equiv 2 \bmod 4$.
  - *(1)* *If* $A + B \equiv 7$ *or* $11 \bmod 16$*, then there are no large classes of quartics (i.e., the image of* Φ *is trivial);*
  - *(2)* *if* $(A, B) \equiv (1, 14), (5, 14), (9, 6)$ *or* $(13, 6) \bmod 16$*, then there are large classes of quartics (i.e.,* Φ *is non-trivial);*

PROOF: (a). In case (1), we have to show that $E(\mathbb{Q}_2)$ contains no integral points with x-coordinate $\xi \equiv 2 \bmod 4$. For such a ξ, we have

$$\xi^3 + A\xi + B \equiv 8 + 2A + B \bmod 16\,.$$

Since $8 + 2A + B \equiv 8$ or $12 \bmod 16$, this cannot be a square.

In case (2), we have to show that $E(\mathbb{Q}_2)$ contains an integral point with x-coordinate $\xi \equiv 2 \bmod 4$. In the cases $(A, B) \equiv (0, 12), (8, 12)$, one may check that either $f(2)$ or $f(-2)$ is a square, where $f(x) = x^3 + Ax + B$. In the cases $(A, B) \equiv (0, 8), (8, 8)$, the Newton polygon for $g(x) = f(4x + 2)$ shows that $g(x)$ has an integral root.

(b). Similarly, in case (1), we have to show that there is no integral point with $\xi \equiv 1 \bmod 4$. For such a ξ, we have

$$\xi^3 + A\xi + B \equiv 1 + A + B \bmod 16 \,.$$

(Write $\xi = 1 + 4\xi_1$ and note that $3 + A \equiv 0 \bmod 4$ to see this.) Since $1 + A + B \equiv 8$ or 12 mod 16, this cannot be a square.

In case (2), when $(A, B) \equiv (5, 14), (13, 6) \bmod 16$, one may check that either $f(1)$ or $f(5)$ is a square. If $(A, B) \equiv (1, 14), (9, 6) \bmod 16$ then the Newton polygon of $g(x) = f(4x + 1)$ shows that there is an integral root, provided that $A + B \equiv 31 \bmod 32$. Finally, when $(A, B) \equiv (1, 14), (9, 6) \bmod 16$ and $A + B \equiv 15 \bmod 32$, one may check that one of the values $g(\pm 1)$, $g(\pm 3)$ is a square. □

Using this Lemma, together with the algorithm of Appendix B for the cases where the Lemma does not apply, we increase significantly the number of cases where large quartics do not have to be considered in a systematic enumeration of all the equivalence classes, compared with [**2**]. This has a significant effect on the average running time of the 2-descent algorithm over $\mathbb{Q}$. It does not seem possible to determine the image of Φ completely in all cases, simply in terms of 2-adic congruence conditions on the coefficients A and B; on the other hand, the algorithm in Appendix B resolves the ambiguity quickly for any given curve.

7. *Implementation and examples*

We conclude with some remarks about the practical consequences of our results, particularly those of the preceding section, for the two-descent algorithm implemented in our freely-available program `mwrank` [**5**]. For more details of the algorithm, see [**3**].

We determine the Selmer group of an elliptic curve E by finding quartics which represent all two-coverings of E. In general we have to search first for "small" quartics, and then for "large" quartics, in the sense defined above. The search for large quartics takes considerably longer, since the search regions are larger, though we can speed up the large search by imposing congruence conditions on the coefficients of large quartics which ensure that we only find those which are $\mathbb{Q}$-minimal (not equivalent to small ones).

Define the "local index" of a curve $E/\mathbb{Q}$ to be the order of the image of the map Φ defined above, which is the index $[E(\mathbb{Q}_2) : \ker(\Phi)]$. Elements of $E(\mathbb{Q})$ in $\ker(\Phi)$ are associated to small quartics. Define the "global index" to be the index $[E(\mathbb{Q}) : E(\mathbb{Q}) \cap \ker(\Phi)]$. Then the local index is 1, 2 or 4 and may be determined by the results of the previous section, invoking Lemma 6.1 or the algorithm of Appendix B when necessary. We need to search for large quartics if and only if the local index is greater than 1, and we find any if and only if the global index is greater than 1.

Exact knowledge of the local index allows us to reduce the number of cases in which large quartics need to be considered at all. Previously `mwrank` used the result from [**2**], which only applies when $A \equiv B \equiv 0 \bmod 4$ and $2A + B \equiv 0 \bmod 16$. This is one of the cases in Lemma 6.1(a)(1). Hence by the use of Lemma 6.1, we may increase by a factor of 4 the proportion of curves for which we do not need to consider large quartics. This change to the algorithm reduced the running time of `mwrank` on our test data (see below) by around 65%.

For example, consider the curve $Y^2 = X^3 + 20$ with $(A, B) = (0, 20)$, so that $2A + B \equiv 4 \bmod 16$. The rank is 0. There are no non-trivial small quartics. Using the old criterion, we search for large quartics, and find two, though they are not $\mathbb{Q}_2$-soluble. Of course, for such a small example both versions of the algorithm are very fast, taking only a fraction of a second to run. For a similar larger example, take $(A, B) = (0, 16000004)$, where the curve again has rank 0. There are no small quartics. The old algorithm finds two (equivalent) large quartics which are not $\mathbb{Q}_2$-soluble; the running time is 45 seconds. The new algorithm only searches for small quartics, and takes just 7 seconds.

The curve with $(A, B) = (40004, 40004)$ has local index 1. (Here, Lemma 6.1 does not apply, since $2A + B \equiv 12 \bmod 16$, so we have to use the algorithm of Appendix B.) Searching only for small quartics we find the Selmer rank to be 1 after only 1.6 seconds, while the fruitless search for large quartics takes a further 7.5 seconds. (In this example, we have excluded the time taken to find a $\mathbb{Q}$-rational point on the one locally soluble quartic found, which is $(41, -36, -474, 1282, -982)$, since there are no such points of small height, so that in fact this search for points will dominate the running time if we wish to establish (unconditionally) that the rank is 1.)

Next, when the local index is determined to be 2, and we must search for large quartics, we may stop the search for large quartics as soon as we find one which is $\mathbb{Q}$-soluble (or just ELS, in case we are only interested in finding the Selmer group). In many cases a large quartic is found early on in the search, so that this eliminates most of the time previously spent on the large search. The situation here is entirely analogous to that which occurs when E has positive discriminant, so that $E(\mathbb{R})$ has two real components: the analogous strategy is detailed in [**3**, p.93].

For example, consider the curve $Y^2 = X^3 + X^2 - 3405X + 15280204$, where the local index and global index are both 2. The rank is 8, with a contribution of 7 from small quartics. In the search region for large quartics, the leading coefficient a satisfies either $0 < a \leqslant 859$ or $0 > a \geqslant -562$. The original algorithm searches this whole region, despite quickly finding a suitable quartic with $a = 1$, namely $(1, 0, -66116, 9253784, -364263500)$, and takes 36 seconds. The improved algorithm stops after finding this large quartic, and delivers the same result in under 5 seconds.

When the local index is 4 the situation is slightly more complicated. We can stop the search for large quartics once a second one (which is $\mathbb{Q}$-soluble or ELS) is found, *provided* that the second one is independent of the first one modulo the “small” subgroup. Our implementation takes account of this. Of course, the global index may be less than 4, in which case there is no reduction in running time. To illustrate the possibilities we consider the following curves, which all have local index 4: (1) $(A, B) = (2, 4)$ has global index 4 also: the rank is 2 and all comes from large quartics; (2) $(A, B) = (3, 8)$ has global index 2; the rank is 1, coming from a large quartic; (3) $(A, B) = (2, 8)$ has global index 1; the rank is 0, and there are no non-trivial $\mathbb{Q}$-soluble quartics at all.

To estimate the average expected gain from implementing the results of the previous section to “typical” curves is not straightforward. For curves for which the Birch–Swinnerton-Dyer criterion already applies, or for which the global index is strictly less than the local index, there is no change at all. (There is also no change for curves with rational 2-torsion, where a different descent strategy is used.) We measured the time taken for `mwrank` to process our standard test list of curves which are, in a sense, “typical”. In the list we have the following 474 curves, all with no rational 2-torsion: all 401 curves with conductor $N < 400$ and no 2-torsion, up to isogeny; all 18 rank 2 curves with conductor $N < 1000$, up to isogeny; and a miscellaneous collection of 10 rank 3 curves, 10 rank 4 curves, 5 rank 5 curves, 6 rank 6 curves, 21 rank 7 curves and 3 rank 8 curves. (These curves, together with the curves of conductor $N < 400$ with rational 2-torsion, form the test data now distributed with `mwrank`.)

The local index is 1 for 400 of these curves (which hence have global index 1 also), of which 169 satisfy the Birch–Swinnerton-Dyer condition for non-existence of large quartics while the remaining 231 require Lemma 6.1 or its refinement. The other 74 curves have local index 2, of which 13 have global index 1, and 61 have global index 2. (No curves in this list have local index 4). Overall, 231 curves out of 474 (or 48.7% of relevant cases) benefit from the exact computation of the 2-adic index. Of the 74 cases where the local index is greater than 1, 61 (or 82.4%) benefit from the early exit strategy.

We give here the time taken to process these curves with our algorithm, which in all cases determines the rank unconditionally, and also finds rational points generating $E(\mathbb{Q})/2E(\mathbb{Q})$, which therefore generate a subgroup of $E(\mathbb{Q})$ of finite, odd index. To see how the successive refinements to the algorithm affect the running time, we give times for four versions: (1) using only the Birch–Swinnerton-Dyer criteria; (2) using Lemma 6.1 but no early exit when the index is greater than 1; (3) using the refinement to Lemma 6.1 to determine the exact local index in all cases, but still with no early exit; and (4) as for (3), but with early exit during the search for large quartics when the global index reaches the local index. All these times are based on our development version of the `mwrank` code, using NTL with `gmp` integer arithmetic, compiled with GCC 2.8.1, running on a DEC alpha EV6.

Method	1	2	3	4
Time for all	$529s$	$189s$	$187s$	$108s$
Time for 174A1	$232s$	$31s$	$31s$	$31s$
Time without 174A1	$297s$	$158s$	$156s$	$77s$

From this table we see that Lemma 6.1 by itself gives a significant time-saving, as does the early exit strategy. The identification of curves of local index 1 in cases not covered by Lemma 6.1 is less significant (though it was the least simple to implement). The variation in times for the curves in this list is quite considerable, even amongst the curves of conductor under 400, all but one of which has rank 0 or 1. By far the most time-consuming is the curve with standard code 174A1 and Weierstrass coefficients $[1, 0, 1, -7705, 1226492]$, for which the the local index is 1 by Lemma 6.1(b).

Appendix A

We collect here proofs of some of the results of Section 4. Some of these may be found in [**2**], though many (and in some cases all) of the details are omitted there. The proofs we give may easily be turned into algorithms for minimizing a given quartic over a local field, or over a number field. In the latter case, we can minimize simultaneously at all primes provided that the relevant primes are principal: for example, if the field has class number 1.

In the following, K will again be a fixed p-adic field. We omit the subscript K in order to simplify notation, so for example $\pi = \pi_K$ and $v = v_K$. Recall the notation $v(Q) = \min\{v(a), v(b), v(c), v(d), v(e)\}$ for quartics $Q = (a, b, c, d, e)$ over K.

We begin with two lemmas. The first one gives conditions in terms of the valuations of the coefficients that imply nonminimality. The second one will serve to eliminate part of the cases in the results proved below, but is also of interest in itself.

Lemma A.1. *Let $Q = (a, b, c, d, e)$ be an integral quartic over K. Then Q is K-nonminimal in any one of the following cases.*

1. $v(a) \geqslant 0$, $v(b) \geqslant 1$, $v(c) \geqslant 2$, $v(d) \geqslant 3$, $v(e) \geqslant 4$.
2. $v(a) \geqslant 0$, $v(b) \geqslant 0$, $v(c) \geqslant 2$, $v(d) \geqslant 4$, $v(e) \geqslant 6$.
3. $v(Q) \geqslant 2$.

PROOF: The following K-equivalent quartics are integral and of lower level in each case. 1. $Q(x, \pi^{-1}z)$. 2. $\pi^2\, Q(x, \pi^{-2}z)$. 3. $\pi^{-2}\, Q(x, z)$. □

Lemma A.2. *Suppose the residue characteristic p is not 3. Let Q be an integral quartic over K, and set $Q_1 = \pi^{-v(Q)}Q$. If $\mathrm{level}(Q) \geqslant 1$ and Q is K-minimal, then Q_1 has a quadruple root, when reduced modulo π. (The root may be at infinity, in the sense that $Q_1(x, z) \equiv ez^4 \bmod \pi$).*

PROOF: We use $a_1, b_1, \ldots, I_1, J_1$ for the quantities associated to Q_1. If $v(Q) = 2$, then Q is K-nonminimal by Lemma A.1, so we either have $v(Q) = 0$ or $v(Q) = 1$. In both cases, $v(I_1) \geqslant 2$ and $v(J_1) \geqslant 3$.

The vanishing of I_1 and J_1 mod π implies that Q_1 has a root of multiplicity at least three mod π. We therefore have to show that Q is nonminimal when the multiplicity is exactly three.

By a suitable transformation in $\mathrm{SL}(2, \mathcal{O})$ (this preserves integrality and the level), we can achieve that the triple root is at zero (mod π) and that the remaining root is at infinity (mod π). This means that (in obvious notation) $v(a_1, b_1, c_1, d_1, e_1) \geqslant (1, 0, 1, 1, 1)$ with $v(b_1) = 0$.

Applying $\left(\begin{smallmatrix} 1 & \alpha \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{SL}(2, \mathcal{O})$, where $\alpha \in \pi\mathcal{O}_K$ satisfies the congruence $3b_1\alpha \equiv -c \bmod \pi^2$, we can achieve that additionally $v(c_1) \geqslant 2$. Considering the valuations of the various terms making up I and J, we deduce from $v(I_1) \geqslant 2$ that $v(d_1) \geqslant 2$ and then from $v(J_1) \geqslant 3$ that $v(e_1) \geqslant 3$. If $v(Q) = 1$, this means $v(a, b, c, d, e) \geqslant (2, 1, 3, 3, 4)$, which shows non-minimality by Lemma A.1, part 1. If $v(Q) = 0$, we have $v(I) \geqslant 4$ and $v(J) \geqslant 6$, from which we conclude $v(d) \geqslant 4$ and $v(e) \geqslant 6$. We then have $v(a, b, c, d, e) \geqslant (1, 0, 2, 4, 6)$, so Q is nonminimal by Lemma A.1, part 2. □

Now we proceed with the proofs of the results in Section 4.

Proposition A.3. *Let K be a p-adic field where $p \geqslant 5$ and let Q be an integral quartic over K.*

(1) If $v(Q) \geqslant 2$, then Q is K-nonminimal.

(2) If $\mathrm{level}(Q) = 0$, then Q is K-minimal.

(3) If $\mathrm{level}(Q) = 1$ and $v(Q) = 0$, then Q is K-nonminimal.

(4) If $\mathrm{level}(Q) = 1$ and $v(Q) = 1$, then Q is K-nonminimal if it is K^{nr}-soluble.

(5) If $\mathrm{level}(Q) \geqslant 2$, then Q is K-nonminimal.

PROOF: (1) This is Lemma A.1, part 3.

(2) This is clear, since an integral quartic cannot have negative level.

(3) Let $Q = (a, b, c, d, e)$. By Lemma A.2, we can suppose that $v(a, b, c, d, e) \geqslant (0, 1, 1, 1, 1)$ with $v(a) = 0$. Then the valuations of I and J imply that $v(e) \geqslant 2$ and then $v(d) \geqslant 2$. Next, the valuation of $6cI - J$ implies that $v(c) \geqslant 2$ (this observation is due to Serf, see [**8**, page 148]). Finally, the valuations of I and J imply in turn that $v(e) \geqslant 3$, $v(d) \geqslant 3$, $v(e) \geqslant 4$, and we may reduce the level by Lemma A.1, part 1.

(4) Let $Q_1 = \pi^{-1}Q$. Then Q_1 has modulo π either a triple or a quadruple root. If it has a triple root, then Q is K-nonminimal by Lemma A.2. So suppose Q_1 has a quadruple

root modulo π. Then we can suppose that $v(a,b,c,d,e) \geqslant (1,2,2,2,2)$ with $v(a) = 1$. From the invariants, we get $v(d) \geqslant 3$ and $v(e) \geqslant 3$. We claim that $v(e) \geqslant 4$. Otherwise $v(e) = 3$, and it is easily seen that $v(Q(x,z))$ is odd for all $(x,z) \in (K^{\mathrm{nr}})^2 \setminus \{0\}$, so Q is not K^{nr}-soluble, a contradiction. Hence $v(a,b,c,d,e) \geqslant (1,2,2,3,4)$, and the level can be reduced by Lemma A.1, part 1 again.

(5) If $v(Q) \geqslant 2$, this follows from part (1). Otherwise, set $Q_1 = \pi^{-v(Q)}Q$; then $\mathrm{level}(Q_1) \geqslant 1$ and $v(Q_1) = 0$, so Q_1 is K-nonminimal by part (3), and the level of Q can be reduced in the same way as for Q_1. □

Proposition A.4. *Let K be an unramified 3-adic field. Then an integral quartic which is K^{nr}-soluble is K-nonminimal if and only if* either $v_K(I) \geqslant 5$, $v_K(J) \geqslant 9$, or $v_K(I) = 4$, $v_K(J) = 6$ *and* $v_K(\Delta) \geqslant 12$.

PROOF: This is [**2**, Lemma 4]. In [**2**] the proof was omitted. The argument only uses $v_K(3) = 1$, so also applies to unramified extensions of $\mathbb{Q}_3$.

For the necessity, suppose first that $Q = (a,b,c,d,e)$ is minimal. Then $v(I) > 0 \iff v(c) > 0 \iff v(J) > 0$, and in this case $v(J) \geqslant 3$, so that either $v(I) = v(J) = 0$, or $v(I) \geqslant 1$ and $v(J) \geqslant 3$. In both cases, we also have $v(4I^3 - J^2) \geqslant 3$, since $4I^3 - J^2 = 27\Delta$. Since any nonminimal quartic in the same class has valuations of (I,J,Δ) that are larger by a multiple of $(4,6,12)$, the necessity of the given conditions follows.

The proof of sufficiency follows the same plan as for the preceding Proposition. We consider the cases $v(Q) = 0$ and $v(Q) = 1$ in turn, the case $v(Q) \geqslant 2$ being trivial.

Suppose that $v(Q) = 0$. After a suitable unimodular substitution we may suppose that the multiple root modulo 3 is at 0, and that if the multiplicity is exactly 3 then the second root is at ∞. In the multiplicity 3 case, we have $v(b) = 0$ while $v(a), v(c), v(d), v(e) > 0$. Now $v(J) \geqslant 6$ implies $v(c) \geqslant 2$ and $v(e) \geqslant 2$, then $v(I) \geqslant 4$ implies $v(d) \geqslant 3$, and then $v(J) \geqslant 6$ implies $v(e) \geqslant 3$.

Consider the case where $v(I) \geqslant 5$ and $v(J) \geqslant 9$. The condition $v(c) \geqslant 3$ can be achieved with the unimodular transformation $\left(\begin{smallmatrix}1 & 3t\\ 0 & 1\end{smallmatrix}\right)$, where $bt \equiv -c/9 \bmod 27$. If $v(I) \geqslant 5$ we then see that $v(d) \geqslant 4$, and then $v(J) \geqslant 9$ implies $v(e) \geqslant 6$, so we can reduce the level by Lemma A.1, part 2.

Suppose alternatively that $v(I) = 4$ and $v(J) = 6$. Now, for suitable t (satisfying $bt^3 \equiv -e/3^3 \bmod 3$) the transformation $\left(\begin{smallmatrix}1 & 3t\\ 0 & 1\end{smallmatrix}\right)$ gives $v(e) \geqslant 4$. Now we use the fact that $v(\Delta) \geqslant 12$ to deduce that $v(d) \geqslant 4$, for otherwise the expression for Δ contains a unique term $4b^3d^3$ of minimal valuation 9. Also $v(c) = 2$ (exactly), and $v(\Delta) \geqslant 12$ now implies that $v(e) \geqslant 6$. Thus we may reduce the level by Lemma A.1, part 2 again.

The case of a quadruple root may be handled in a similar way, leading to reduction by Lemma A.1, part 1.

Now suppose that $v(Q) = 1$; then $I_1 \equiv J_1 \equiv 0 \bmod 3$, so Q_1 has a root of multiplicity at least 3 modulo 3. Shifting this multiple root to 0, we may assume that $v(a) \geqslant 1$, $v(b) \geqslant 1$, $v(c) \geqslant 2$, $v(d) \geqslant 2$, $v(e) \geqslant 2$. In the triple root case, we may suppose (after shifting the other root to ∞) that $v(b) = 1$ and $v(a) \geqslant 2$. In the case where $v(I) \geqslant 5$ and $v(J) \geqslant 9$, we obtain in succession $v(c) \geqslant 3$, $v(d) \geqslant 3$ and finally $v(e) \geqslant 4$, so we may reduce the level by Lemma A.1, part 1. Now suppose that $v(I) = 4$, $v(J) = 6$ and $v(\Delta) \geqslant 12$. Then $v(c) = 2$ exactly, and considering the terms of Δ we obtain successively $v(d) \geqslant 3$ and $v(e) \geqslant 4$ as required. In the quadruple root case, we have $v(a) = 1$ while $v(b), v(c), v(d), v(e) \geqslant 2$. When $v(I) \geqslant 5$ and $v(J) \geqslant 9$, we obtain in succession $v(c) \geqslant 3$, $v(e) \geqslant 3$, $v(d) \geqslant 3$, and now $v(e) \geqslant 4$ since $v(e) = 3$ would contradict K^{nr}-solubility. When $v(I) = 4$, $v(J) = 6$ and $v(\Delta) \geqslant 12$, we have $v(c) = 2$, and then consideration of the terms of Δ gives $v(e) \geqslant 3$

and $v(d) \geqslant 3$; again, we must have $v(e) \geqslant 4$ for K^{nr}-solubility. In both cases we succeed in reducing the level by Lemma A.1, part 1 again. □

Proposition A.5. *Let K be an unramified 2-adic field. Then an integral quartic $Q = (a, b, c, d, e)$ which is K^{nr}-soluble is K-minimal if and only if* either *it has level* 0, or *it has level* 1 *and satisfies one of the following conditions.*

1. *$v(Q) = 1$, and $\frac{1}{2}Q$ has a quadruple root modulo 2 and no root modulo 8;*
2. *$v(Q) = 0$, and Q has a quadruple root modulo 4 and no root modulo 16.*

In particular, if $v(I) \geqslant 6$, $v(J) \geqslant 9$ and $v(8I + J) \geqslant 10$ then Q is nonminimal; as a special case, quartics of level at least 2 are nonminimal.

The last sentence is essentially the statement of [**2**, Lemma 5]. For an improvement, see Lemma 6.1.

PROOF: Obviously, we only have to consider the case $\mathrm{level}(Q) = 1$ and $v(Q) \leqslant 1$. Lemma 5.1 shows that the given conditions are sufficient, since after applying a suitable element of $\mathrm{SL}(2, \mathcal{O})$, we have $v(a) \leqslant 1$, $v(b), v(c) \geqslant 2$, $v(d) \geqslant 3$ and $2 \leqslant v(e) \leqslant 3$ ($v(d) \geqslant 3$ following from $v(d) \geqslant 2$ and the other conditions, since $v(J) \geqslant 6$). This lemma also gives us the necessity under the assumption that Q_1 has a quadruple root modulo 2, respectively, that Q has a quadruple root modulo 4. Lemma A.2 tells us that Q_1 must have a quadruple root modulo 2 in any case, disposing of the case $v(Q) = 1$ already. So we only have to show that a minimal quartic of level 1 with $v(Q) = 0$ has a quadruple root modulo 4.

Therefore we suppose that $v(Q) = 0$ and Q has a quadruple root mod 2, whence we can assume that $v(a) = 0$ while $v(b), v(c), v(d), v(e) \geqslant 1$. The valuations of J and I imply that $v(d) \geqslant 2$ and $v(c) \geqslant 2$ respectively. The assumption $v(e) = 1$ leads (by J) to $v(b) \geqslant 2$ and then to the contradiction $v(I) = 3$, so $v(e) \geqslant 2$ also. This means that modulo 4, Q has at least a triple root. If Q does not have a quadruple root modulo 4 then $v(b) = 1$, from which we deduce that $v(d) \geqslant 3$ and $v(e) \geqslant 4$, so Q is nonminimal by Lemma A.1, part 1.

The last statement can be proved along these lines by observing that the given conditions ensure that there has to be a root modulo 16 if there is a quadruple root modulo 4. We do not give the details here, since Lemma 6.1 contains this assertion as a special case anyway. □

Appendix B

We give here an algorithm for determining the size of the index in the two ambiguous cases from Section 6. Recall that the problem is to determine whether the curve $y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}_2$ has an integral point (x, y) with x in a certain residue class modulo 4, in two cases:

1. [Case 1] $A \equiv B \equiv 0 \bmod 4$, with $x \equiv 2 \bmod 4$;
2. [Case 2] $A \equiv 1$, $B \equiv 2 \bmod 4$, with $x \equiv 1 \bmod 4$.

Replacing x by $4x + 2$ or $4x + 1$ respectively, this amounts to determining whether the polynomials

$$(4x+2)^3 + 4a(4x+2) + 4b \quad \text{and} \quad (4x+1)^3 + (4a+1)(4x+1) + (4b+1)$$

(with $a, b \in \mathbb{Z}_2$) ever take on square values (including 0) for some $x \in \mathbb{Z}_2$.

It is easy to write a general recursive procedure for determining whether a square-free polynomial $f(x) \in \mathbb{Z}_2[x]$ ever takes on square values. The answer is "yes" if $f(0)$ is a square, or if the Newton Polygon of f allows one to conclude that f has an integral root. Otherwise, set $c = f(0)$, $v = v(c)$ and $c_0 = c/2^v$, and let w be the minimum valuation of the non-constant coefficients of f. Then the answer is "no" if v is odd and $w > v$ (since then $v(f(x)) = v$ for all $x \in \mathbb{Z}_2$), or if v is even, $c_0 \equiv 3 \bmod 4$ and $w > v + 1$ (since then $v(f(x)) = v$ and $f(x)/2^v \equiv 3 \bmod 4$ for all x), or if v is even, $c_0 \equiv 5 \bmod 8$ and $w > v + 2$ similarly. If none of these cases occurs, we recursively consider the two polynomials $f(2x)$ and $f(2x + 1)$ in turn.

However, for the special cases of concern to us here, we found it to be faster to avoid the recursive branching with the following two special algorithms. In each case, by imposing congruence conditions on the parameters a, b we are able either to decide the answer, or to eliminate one parity for the variable x. The resulting procedures then have a simple loop instead of branching, and for square-free f we can bound the number of times the loop is executed in terms of the 2-adic valuation of its discriminant.

Case 1: $A \equiv B \equiv 0 \bmod 4$, *with* $x \equiv 2 \bmod 4$

Write $A = 4a$, $B = 4b$, and replace x by $4x + 2$. Then $f(x) = x^3 + Ax + B$ becomes $4g(x)$ where $g(x) = 16x^3 + 24x^2 + 4(a + 3)x + (2a + b + 2)$. For brevity, write $g = (16, 24, 4c, d)$ where $c = a + 3$ and $d = 2a + b + 2$. The following should be thought of as steps in an algorithm, so that the conditions we impose are cumulative; the variables c, d and the current polynomial g will change as we proceed.

1. If $d \equiv 2, 3 \bmod 4$, then return "no"; for $g(x) \equiv d \bmod 4$.
2. If $d \equiv 1 \bmod 4$, then return "yes" if either $c \equiv 1 \bmod 2$ or $d \equiv 1 \bmod 8$, otherwise return "no"; for $g(x) \equiv 4cx + d \bmod 8$.
3. [Now $d \equiv 0 \bmod 4$.] If $c \equiv 1 \bmod 2$, return "yes"; for the valuations of the coefficients are $4, 3, 2, \geqslant 2$, so the Newton Polygon shows that g has an integral root.
4. [Now also $c \equiv 0 \bmod 2$.] Divide c by 2 and d by 4, and divide the polynomial by 4, so that we are now considering $g = (4, 6, 2c, d)$. Set $a = b = 1$, so that $g = (4a, 4b + 2, 2c, d)$. The following steps should be repeated as necessary.
5. (*) If $c \equiv 1 \bmod 2$, then return "yes" if $d \equiv 0, 1 \bmod 4$, otherwise return "no". For $g(x) \equiv 2x(x + c) + d \equiv d \bmod 4$ so $d \equiv 2, 3 \bmod 4$ is impossible; $g(0) = d$ is a square if $d \equiv 1 \bmod 8$; $g(2) \equiv 4c + d \equiv 1 \bmod 8$ if $d \equiv 5 \bmod 8$; and the Newton Polygon gives an integral root if $d \equiv 0 \bmod 4$.
6. [Now $c \equiv 0 \bmod 2$.] If $d \equiv 1 \bmod 2$, then return "yes" if either $d \equiv 1 \bmod 8$ or $4(a + b) + 2c + d + 1 \equiv 0 \bmod 8$, otherwise return "no"; for $g(x)$ is odd, $g(2x) \equiv d \bmod 8$, and $g(2x + 1) \equiv 4(a + b) + 2c + d + 2 \bmod 8$.
7. [Now also $d \equiv 0 \bmod 2$.] If $d \equiv 0 \bmod 4$, then x must be even, since for odd x we have $g(x) \equiv 2 \bmod 4$. Now $g(2x)/4 = (8a, 4b + 2, c, d/4)$, so we set $(a, b, c, d) := (2a, b, c/2, d/4)$ and loop back to (*).
8. If $d \equiv 2 \bmod 4$, then x must be odd, since for even x we have $g(x) \equiv d \bmod 4$. Now $g(2x + 1)/4 = (8a, 12a + 4b + 2, 6a + 4b + c + 2, a + b + c/2 + (d + 2)/4)$, so we set $(a, b, c, d) := (2a, 3a + b, 3a + 2b + c/2 + 1, a + b + c/2 + (d + 2)/4)$ and loop back to (*).

Note that $7/8$ of the cases are decided before reaching the loop, with $9/16$ returning "no" and $5/16$ returning "yes"; of the $1/8$ of cases which reach the loop, $3/4$ are decided in the first pass, with half of these returning "no" and half returning "yes". This means that of those cases which reach the loop at all, half will return "no" and half "yes", so that overall we find that in $5/8$ of the cases the answer is "no" while in $3/8$ of the cases it is "yes".

We can bound the number of passes through the loop as follows, giving at the same time a proof that the above algorithm terminates when $f(x)$ is square-free. The simple observation is that each time we re-enter the loop (i.e., from the second time on we reach step 5), the valuation of $\mathrm{disc}(g)$ has been decreased by 2 in steps 7 or 8. (We have $\mathrm{disc}(g(ax)) = a^6 \mathrm{disc}(g(x))$, $\mathrm{disc}(ag(x)) = a^4 \mathrm{disc}(g(x))$ and $\mathrm{disc}(g(x+1)) = \mathrm{disc}(g(x))$.) Since at the end of step 4, $v(\mathrm{disc}(g)) = v(\mathrm{disc}(f)) - 4$, the number of passes through the loop is bounded by $v(\mathrm{disc}(f))/2 - 1$.

Case 2: $A \equiv 1$, $B \equiv 2 \bmod 4$, *with* $x \equiv 1 \bmod 4$

Write $A = 4a + 1$, $B = 4b + 2$, and replace x by $4x + 1$. Then $f(x) = x^3 + Ax + B$ becomes $4g(x)$ with $g = (16, 12, 4c, d)$ where $c = a + 1$ and $d = a + b + 1$.

1. If $d \equiv 2, 3 \bmod 4$, then return "no"; for $g(x) \equiv d \bmod 4$.
2. If $d \equiv 1 \bmod 4$, then return "yes" if either $c \equiv 0 \bmod 2$ or $d \equiv 1 \bmod 8$, otherwise return "no"; for $g(x) \equiv 4x(x + c) + d \bmod 8$.
3. [Now $d \equiv 0 \bmod 4$.] If $c \equiv 1 \bmod 2$, return "yes"; for if $d \equiv 0 \bmod 8$ then the valuations of the coefficients are $4, 2, 2, \geqslant 3$, so the Newton Polygon shows that g has an integral root, while if $d \equiv 4 \bmod 8$ then one of $g(0)$, $g(-c)$, $g(4)$, $g(3c)$ is a square, $d \equiv 4, 12, 20, 28 \bmod 32$ respectively.
4. [Now also $c \equiv 0 \bmod 2$.] Divide c by 2 and d by 4, and divide the polynomial by 4, so that we are now considering $g = (4, 3, 2c, d)$. Set $a = 1$, $b = 0$, so that $g = (4a, 3(4b + 1), 2c, d)$. The following steps should be repeated as necessary.
5. (*) Suppose that $c \equiv 1 \bmod 2$.
   - If $d \equiv 0 \bmod 4$, then return "yes"; for the Newton Polygon gives an integral root.
   - If $d \equiv 2 \bmod 4$, then return "no"; for $g(x) \equiv 2, 3 \bmod 4$.
   - If $d \equiv 1 \bmod 4$, then return "yes" if $d \equiv 1 \bmod 8$, else return "no"; for $g(2x + 1) \equiv 2 \bmod 4$, and $g(2x) \equiv d \bmod 8$.
   - If $d \equiv 3 \bmod 4$, then x must be odd since $g(2x) \equiv d \bmod 4$, so replace $g(x)$ by $g(2x+1)/4$: set $(a, b, c, d) := (2a, a+b, 3a+6b+(c+3)/2, a+3b+(c+1)/2+(d+1)/4)$, and loop back to (*).
6. Suppose that $c \equiv 0 \bmod 2$.
   - If $d \equiv 1 \bmod 4$, then return "yes"; for $g(2x) \equiv 4x^2 + d \bmod 8$, which is a square for $x = 0$ or $x = 1$.
   - If $d \equiv 3 \bmod 4$, then return "no"; for $g(x) \equiv 3x^2 + d \equiv 2, 3 \bmod 4$.
   - If $d \equiv 2 \bmod 4$, then return "yes" if $4(a+b)+2c+d+2 \equiv 0 \bmod 8$, else return "no"; for $g(2x) \equiv 2 \bmod 4$, while $g(2x + 1) \equiv 4(a + b) + 2c + d + 3 \bmod 8$.
   - If $d \equiv 0 \bmod 4$, then x must be even, since $g(2x + 1) \equiv 3 \bmod 4$, so replace $g(x)$ by $g(2x)/4$: set $(a, b, c, d) := (2a, b, c/2, d/4)$ and loop back to (*).

As in Case 1, one can show from the above algorithm that the result is "yes" in $3/8$ of the cases and "no" in the remaining $5/8$, and that the number of passes through the loop is again bounded by $v(\mathrm{disc}(f))/2 - 1$.

References

1. A. Brumer and K. Kramer: *The rank of elliptic curves*, Duke Math. J. **44**, 715–743 (1977).

2. B.J. Birch and H.P.F. Swinnerton-Dyer: *Notes on elliptic curves, I*, J. reine angew. Math. **212**, 7–25 (1963).

3. J.E. Cremona: *Algorithms for modular elliptic curves*, 2nd edition, Cambridge University Press (1997).

4. J.E. Cremona: *Classical invariants and 2-descent on elliptic curves*, Journal of Symbolic Computation **31**, 71–87 (2001).

5. J.E. Cremona: `mwrank` and other programs for elliptic curves over $\mathbb{Q}$ are available from
`http://www.maths.nott.ac.uk/personal/jec/ftp/progs`.

6. J.E. Cremona and P. Serf: *Computing the rank of elliptic curves over real quadratic fields of class number* 1, Math. Comp. **68** (1999), 1187–1200.

7. J.H. Silverman: *The arithmetic of elliptic curves*, Springer GTM 106 (1986).

8. P. Serf: *The rank of elliptic curves over real quadratic number fields of class number* 1, Thesis, Universität des Saarlandes, 1995.

Michael Stoll `m.stoll@iu-bremen.de`

School of Engineering and Science, International University Bremen,
P.O.Box 750561, 28725 Bremen, Germany

John E. Cremona `john.cremona@nottingham.ac.uk`

School of Mathematical Sciences, University of Nottingham, University Park,
Nottingham NG7 2RD, England