2-DESCENT ON ELLIPTIC CURVES AND RATIONAL POINTS ON CERTAIN KUMMER SURFACES

Alexei Skorobogatov and Sir Peter Swinnerton-Dyer

1. *Introduction.* In this paper we are primarily concerned with elliptic curves E defined over an algebraic number field k which have all their 2-division points defined over k. In §2 we remind the reader of the current machinery for finding the 2-Selmer group of E, including the refinements recently introduced in [4]; this section also establishes our notation. In §3 we introduce further refinements to this process; the main result here is Lemma 3, which leads up to Theorem 2. This shows that under suitable conditions the bilinear functions introduced in [4] are not merely symmetric but alternating; we expect this result to be useful in other contexts as well as in the present one. In §4 we prove a lemma about the effect of twisting on the parity of the rank of the 2-Selmer group of E which we shall need in §6.

In §§5 and 6 we address the question which actually gave rise to this whole investigation. The study of rational points on pencils of curves of genus 1 has already been applied to prove the existence of rational points on certain K3 surfaces (see [4], pp. 585, 626 and [17]). However the proof of those results depended both on the finiteness of the relevant Tate-Shafarevich groups and on Schinzel's Hypothesis. The first of those hypotheses is widely regarded as a respectable one to assume, but that is much less true of the second. The first paper about such pencils which did not depend on Schinzel's Hypothesis was [18], but there the underlying surfaces were only Del Pezzo. In §§5 and 6 we consider a family (1) of K3 surfaces quite different from that in [17], for which we can again exhibit sufficient conditions for the Hasse principle to hold. To prove this we still need the finiteness of the relevant Tate-Shafarevich groups, but we do not need Schinzel's Hypothesis. The possibility of doing this for the surfaces (1) was suggested to us some five years ago by Colliot-Thélène, but at that time neither he nor we foresaw the difficulties involved.

The K3 surfaces studied here have the form

$$Z^2 = f^{(1)}(X)f^{(2)}(Y) \tag{1}$$

where the $f^{(s)}$ are quartic polynomials defined over k, having no repeated roots. In order to simplify the definition of the set of bad places for (1), we shall assume that we are given $f^{(1)}$ and $f^{(2)}$ separately, rather than merely their product. Geometrically, surfaces (1) can be described as Kummer surfaces attached to products of two elliptic curves. In order to prove that solubility of (1) in k_v for each place v of k implies solubility in k, we expect to need further conditions on the surface (1) — not least because of the likely existence of non-trivial Brauer-Manin obstructions. It is not absurd to hope that these are the only obstructions to the Hasse principle for surfaces (1). But with our present fragmentary understanding of Brauer-Manin obstructions for K3 surfaces, it would be unrealistic to try to prove this. What the reader can reasonably ask for is as follows. Clearly a proof of the solubility of (1) under certain extra conditions implies indirectly that under these extra conditions there is no Brauer-Manin obstruction. But we should also exhibit a direct proof that the extra conditions imply that those parts of the Brauer-Manin obstruction which we know how to describe are trivial, and this direct proof should actually make use of all the extra conditions. In other words, we should show (and do show in the appendix to this paper) that though the extra conditions may be too strong, they are not outrageously too strong.

In §6, but not in §5, one of the further conditions which we impose is that the Jacobians $E^{(1)}$ and $E^{(2)}$ respectively of the curves

$$D^{(1)}:\, U^2 = f^{(1)}(X) \quad \text{and} \quad D^{(2)}:\, V^2 = f^{(2)}(Y) \tag{2}$$

have all their 2-division points defined over k. It is well known that the Jacobian of $z^2 = f(x)$, where f is a quartic polynomial with no repeated roots, is given by $v^2 = g(u)$ where g is the resolvent cubic of f. (See [1]; a short proof is given in Appendix A of [13]. Explicitly, the cubic resolvent of $f(x) = ax^4 + cx^2 + dx + e$ is $g(u) = u^3 - 27Iu - 27J$ where $I = 12ae + c^2$ and $J = 72ace - 27ad^2 - 2c^3$.) Thus if k_s is the least splitting field of $f^{(s)}$ over k the conditions that the $E^{(s)}$ have all their 2-division points defined over k can also be expressed as follows: $\mathrm{Gal}(k_s/k) \subset V_4$ for each s, where V_4 is the subgroup of order 4 of the alternating group A_4.

An elliptic curve with rational 2-division points can be written in the form

$$E:\; Y^2 = (X - c_1)(X - c_2)(X - c_3), \tag{3}$$

where without loss of generality we can assume that the c_i are integers. The twist of E by an element b in k^* is

$$E_b:\; Y^2 = (X - bc_1)(X - bc_2)(X - bc_3), \tag{4}$$

where we can require b and the bc_i to be integers. An equivalent form, probably more common in the literature, is

$$V^2 = b(U - c_1)(U - c_2)(U - c_3).$$

Similarly, if $D : y^2 = f(x)$ is a 2-covering of E then D_b will denote its twist $y^2 = bf(x)$, which is a 2-covering of E_b.

The primes of bad reduction for E are those which divide

$$R = 2(c_1 - c_2)(c_2 - c_3)(c_3 - c_1); \tag{5}$$

the additional bad primes for E_b are those which divide b to an odd power.

Our investigation of (1) falls naturally into two parts. The hypothesis that (1) is everywhere locally soluble is equivalent to the assertion that for each place v of k there exists a_v in k_v^* such that both the equations

$$U^2 = a_v f^{(1)}(X) \quad \text{and} \quad V^2 = a_v f^{(2)}(Y)$$

are soluble in k_v. However for (1) to be soluble in k there must exist a in k^* such that both the equations

$$U^2 = af^{(1)}(X) \quad \text{and} \quad V^2 = af^{(2)}(Y) \tag{6}$$

are soluble in each k_v. (These curves are $D_a^{(1)}$ and $D_a^{(2)}$ respectively, and their Jacobians are $E_a^{(1)}$ and $E_a^{(2)}$.) For the existence of a to follow from that of the a_v is a local-to-global assertion, and the obstruction to it is the Brauer-Manin obstruction given by the quaternion algebras $(c, f^{(1)}(X))$, where c is an element of k^* whose image in the k-algebra $k[X]/(f^{(1)}(X)) \otimes_k k[Y]/(f^{(2)}(Y))$ is a square. This step is a particular case of a general set-up discussed in §5 (see Theorem 3 and its Corollary), culminating in Lemma 6. If both Jacobians have rational 2-torsion then the classes of these quaternion algebras come from $\operatorname{Br} k$ and hence produce no Brauer-Manin obstruction; this is proved in Lemma 7.

Because we have to consider the equations (6) as a varies, we need information about the effect of twisting on the 2-Selmer group. The result which we need in §6 is a special case of stronger and more general results due to Kramer [8]; for ease of reference it is stated in §4. We recall that the elements of the 2-Selmer group of E can be written as triples $m = (m_1, m_2, m_3)$ where the m_i are in k^*/k^{*2} and $m_1 m_2 m_3 = 1$. A detailed exposition of this can be found at (7). We denote the triple associated with $D_a^{(s)}$ by $m^{(s)} = (m_1^{(s)}, m_2^{(s)}, m_3^{(s)})$. We shall assume that neither of the $m^{(s)}$ is $(1, 1, 1)$; for if for example $m^{(1)} = (1, 1, 1)$ then we could choose any value of Y and (1) would become an elliptic curve with rational 2-torsion, which would therefore have finite solutions.

Once we have proved that there does exist a such that (6) is soluble in each k_v, the methods which we use are similar to those used in [18]; the key idea was first introduced in [15] and [4]. What we do is to modify the value of a which appears in (6) so that the 2-Selmer groups of the two $E_a^{(s)}$ both have order 8; the order cannot be less than 8 because the 2-Selmer group of $E_a^{(s)}$ contains $D_a^{(s)}$ and the curves corresponding to the 2-division points, and after Lemma 8 and the assumption that neither $m^{(s)}$ is $(1, 1, 1)$, these are all distinct. Hence the order of that part of each Tate-Shafarevich group which is killed by 2 must be at most 2, and it cannot be equal to 2 because of the assumed finiteness of the Tate-Shafarevich group and the known properties of the Cassels-Tate skew-symmetric form. Thus the image of $D_a^{(s)}$ in the Tate-Shafarevich group is zero, and $D_a^{(s)}$ must therefore be soluble.

This process, which constitutes the proof of the solubility of (1) under suitable conditions, is best described as an algorithm. To make it work we need further conditions on the $f^{(s)}$. One of these we call Condition E. It is analogous to Condition D on page 583 of [4] and Conditions D and E of other previous papers; see for example pages 521 and 525 of [16]. Like them it is related to the Brauer-Manin condition. (Condition E is weaker than Condition D; it is essentially arithmetical, whereas Condition D can be written in purely algebraic form.) In [18] Condition E appears as Condition 5 (p. 905, see also Thm. 3); in Thm. 1 of [18] it is replaced by a condition which is simpler but not unreasonably stronger. In the present paper no such replacement for Condition E seems to be feasible. In [18] there is also nothing corresponding to Conditions Z_1 and Z_2 below.

We shall need several sets of bad places of k. In the definitions which follow, an *even* prime will be one which divides 2 and an *odd* prime will be one which does not divide 2.

- $\mathcal{S}^0$, which depends only on k, consists of the infinite places, the even primes, and a set of generators for the ideal class group of k.
- $\mathcal{S}(E)$ is obtained from $\mathcal{S}^0$ by adjoining the odd primes of bad reduction for the elliptic curve E.

- $\mathcal{S}(D^{(s)})$, $s = 1, 2$, is obtained from $\mathcal{S}(E^{(s)})$, where $E^{(s)}$ is the Jacobian of $D^{(s)}$, by adjoining the primes at which some $m_i^{(s)}$ is not a unit.
- $\mathcal{S}(D^{(1)}, D^{(2)}) = \mathcal{S}(D^{(1)}) \cup \mathcal{S}(D^{(2)})$. This set can be regarded as the set of bad places for the surface (1).
- $\mathcal{S}_c = \mathcal{S}_c(D^{(1)}, D^{(2)})$ for any c in k^* is obtained from $\mathcal{S}(D^{(1)}, D^{(2)})$ by adjoining those primes for which c is not a unit.
- $\mathcal{B}$ will always denote a finite set of places such that $\mathcal{B} \supset \mathcal{S}^0$. We often write $\mathcal{B}$ as the disjoint union of two sets $\mathcal{B}'$ and $\mathcal{B}''$, in which case we shall require that $\mathcal{B}' \supset \mathcal{S}^0$.

Let $\mathcal{M}$ be the set of triples m each of whose components m_i lies in the subgroup of k^*/k^{*2} generated by the $m_i^{(s)}$ for $s = 1, 2$ and $i = 1, 2, 3$; see (39) for a cohomological interpretation of $\mathcal{M}$. The reason for introducing $\mathcal{M}$ is that it consists of those 2-coverings which cannot be rendered insoluble by twisting by an element c of k^* which is in k_v^{*2} for every place v in $\mathcal{S}(D^{(1)}, D^{(2)})$ and which does not render insoluble either of the $D_c^{(s)}$. Condition E is as follows:

> For every place v in $\mathcal{S}(D^{(1)}, D^{(2)})$ there exists $a_v \in k_v^*$ with the following property: for each v both $D_{a_v}^{(1)}$ and $D_{a_v}^{(2)}$ are soluble in k_v, but for each $s = 1, 2$ and for each $m \in \mathcal{M} \setminus \{(1, 1, 1), m^{(s)}\}$ there exists w in $\mathcal{S}(D^{(1)}, D^{(2)})$ such that the 2-covering of $E_{a_w}^{(s)}$ given by m is not soluble in k_w.

In Theorem 4 of the appendix we show that Condition E implies the triviality of the algebraic Brauer-Manin obstruction for (1).

Conditions Z_1 and Z_2 were originally invented because we were unable to prove Theorem 1 without postulating some such properties; they are stronger than we need, but weaker conditions of the same kind would lead to further complications in the arguments in §6. We have subsequently observed that they imply that the 2-component of the transcendental Brauer-Manin obstruction is trivial; see Theorem 5 of the appendix. Condition Z_1 is as follows, where the $c_i^{(s)}$ are defined by writing the curves $E^{(s)}$ in the form (3).

> For some permutation i, j, k of $1, 2, 3$ there exist odd primes $\mathfrak{p}_{ij}^{(1)}$, $\mathfrak{p}_{ik}^{(1)}$ not in $\mathcal{S}(D^{(2)})$ such that the elements of the triple $m^{(1)}$ are

units at $\mathfrak{p}_{ij}^{(1)}$ and $\mathfrak{p}_{ik}^{(1)}$, and

$$\mathfrak{p}_{ij}^{(1)} \| (c_i^{(1)} - c_j^{(1)}) \text{ and } (c_i^{(1)} - c_k^{(1)}), (c_j^{(1)} - c_k^{(1)}) \text{ are units at } \mathfrak{p}_{ij}^{(1)},$$
$$\mathfrak{p}_{ik}^{(1)} \| (c_i^{(1)} - c_k^{(1)}) \text{ and } (c_i^{(1)} - c_j^{(1)}), (c_j^{(1)} - c_k^{(1)}) \text{ are units at } \mathfrak{p}_{ik}^{(1)}.$$

Condition Z_2 is obtained from Condition Z_1 by interchanging 1 and 2.

Theorem 1 *Suppose that* (1) *is everywhere locally soluble, that the* 2*-division points of* $E^{(1)}$ *and* $E^{(2)}$ *are defined over* k*, and that Conditions E,* Z_1 *and* Z_2 *hold. If the relevant Tate-Shafarevich groups are finite,* (1) *is soluble in* k*.*

It is noteworthy that the surfaces studied in [17] are fibred by pencils of curves of genus 1, and that we study the surfaces (1) by lifting them to threefolds which are fibred by pencils of products of two curves of genus 1. These facts are fundamental to the approach in both papers; but they do raise the question whether it is only in the presence of such fibrations that there exist reasonably simple sufficient conditions for the Hasse principle to hold for families of K3 surfaces.

We are indebted to Jean-Louis Colliot-Thélène and to the referee for a large number of valuable comments, in particular to Jean-Louis Colliot-Thélène for communicating to us an argument that lead us to Theorem 3. We are grateful to David Harari, Jan Nekovář and Olivier Wittenberg for useful discussions. The research reported in §3 was begun at a conference at the American Institute of Mathematics at Palo Alto. We are grateful to that Institute for its hospitality.

2. *Preliminaries.* We start by summarizing the standard theory of 2-descents on the elliptic curve (3). The notation introduced in this section will be used, with minor exceptions, throughout the paper. In the notation of (3), to any triple $m = (m_1, m_2, m_3)$ of elements of k^* with $m_1 m_2 m_3 = 1$ we associate the 2-covering E^m of E given by

$$m_i Y_i^2 = X - c_i \text{ for } i = 1, 2, 3 \quad \text{and} \quad Y = Y_1 Y_2 Y_3. \tag{7}$$

Twisting E^m does not alter the value of m; that is, $(E^m)_b = (E_b)^m$.

We ought to treat the m_i as elements of k^*/k^{*2} since the group of triples m is really a way of describing $H^1(k, E[2])$; treating the m_i as elements of k^* is convenient but involves some abuse of notation. In particular, the valuations $v_{\mathfrak{p}}(m_i)$ for primes $\mathfrak{p}$ of k really take values in $\mathbf{Z}/2$. We shall say that m is a *unit* at $\mathfrak{p}$ if all the $v_{\mathfrak{p}}(m_i)$ are even. There is an isomorphism between the $\mathbf{F}_2$-vector space of all 2-coverings of E and the group of triples m, the addition of two 2-coverings corresponding to componentwise multiplication of the triples m. The 2-coverings associated with the 2-division points are given by the triples

$$\begin{aligned} &((c_1-c_2)(c_1-c_3), c_1-c_2, c_1-c_3) \quad \text{for} \quad (c_1,0),\\ &(c_2-c_1, (c_2-c_3)(c_2-c_1), c_2-c_3) \quad \text{for} \quad (c_2,0), \qquad (8)\\ &(c_3-c_1, c_3-c_2, (c_3-c_1)(c_3-c_2)) \quad \text{for} \quad (c_3,0). \end{aligned}$$

For every finite set $\mathcal{B} \supset \mathcal{S}^0$ of places of k we shall as usual denote by $\mathfrak{o}^*_{\mathcal{B}}$ the group consisting of the elements of k^* which are units outside $\mathcal{B}$. We now define various sets, each of which is a vector space over $\mathbf{F}_2$. Write

$$X_{\mathcal{B}} = \mathfrak{o}^*_{\mathcal{B}}/\mathfrak{o}^{*2}_{\mathcal{B}}, \quad Y_v = k^*_v/k^{*2}_v, \quad Y_{\mathcal{B}} = \bigoplus\nolimits_{v\in\mathcal{B}} Y_v,$$

with a convention for $V_{\mathcal{B}}, T_{\mathcal{B}}, W_{\mathcal{B}}$ and $K_{\mathcal{B}}$ similar to that for $Y_{\mathcal{B}}$, where V, T, W and K will be defined shortly; but note that the spaces $\mathfrak{o}^*_{\mathcal{B}}$ and $X_{\mathcal{B}}$ do not follow this convention, nor does $U_{\mathcal{B}}$ which will be defined later. If n is the order of $\mathcal{B}$ then $X_{\mathcal{B}}$ has dimension n by Dirichlet's unit theorem, and $Y_{\mathcal{B}}$ has dimension $2n$ because Y_v contains $4/|2|_v$ elements. It is known from class field theory that $X_{\mathcal{B}} \to Y_{\mathcal{B}}$ is injective. Write

$$V_v = Y_v \oplus Y_v, \quad V_{\mathcal{B}} = \bigoplus\nolimits_{v\in\mathcal{B}} V_v = Y_{\mathcal{B}} \oplus Y_{\mathcal{B}}.$$

It is customary to identify the group of triples m with $(k^*/k^{*2})^2$, though this identification is not canonical and has the disadvantage of destroying the symmetry. This accounts for the way in which $V_{\mathcal{B}}$ and its subspaces are defined; but we shall almost always write elements of $V_{\mathcal{B}}$ as triples, the product of whose three components is 1.

Let $U_{\mathcal{B}}$ be the image of $X_{\mathcal{B}} \oplus X_{\mathcal{B}}$ in $V_{\mathcal{B}}$. Thus $\dim U_{\mathcal{B}} = \frac{1}{2}\dim V_{\mathcal{B}} = 2n$. Define the non-degenerate alternating bilinear form $e_{\mathcal{B}}$ on $V_{\mathcal{B}}$ by

$$e_{\mathcal{B}} = \sum\nolimits_{v\in\mathcal{B}} e_v \quad \text{where} \quad e_v((a,b),(c,d)) = (a,d)_v + (b,c)_v, \qquad (9)$$

the factors on the right being additive Hilbert symbols. If we write elements of $V_{\mathcal{B}}$ as triples $m = (m_1, m_2, m_3)$ with $m_1m_2m_3 = 1$ and the m_i in $Y_{\mathcal{B}}$, then

$$e_v(m', m'') = (m'_1, m''_1)_v + (m'_2, m''_2)_v + (m'_3, m''_3)_v \qquad (10)$$

in an obvious notation. If we identify V_v with $H^1(k_v, E[2])$ then the bilinear form e_v is induced by the Weil pairing $E[2] \times E[2] \to \mathbf{F}_2$.

The Hilbert product formula shows that $U_{\mathcal{B}}$ is isotropic with respect to $e_{\mathcal{B}}$, and comparison of dimensions shows that it is maximal isotropic in $V_{\mathcal{B}}$. Let T_v be the image of $(\mathfrak{o}_v^*/\mathfrak{o}_v^{*2})^2$ in V_v, where $\mathfrak{o}_v$ is the ring of integers of k_v, and let W_v be the image of $E(k_v)$ in V_v under the Kummer map

$$P = (X, Y) \mapsto (X - c_1, X - c_2, X - c_3) \tag{11}$$

in the notation of (3). Tate has shown that W_v is a maximal isotropic subspace of V_v for the alternating form e_v, and $W_v = T_v$ if v is not an infinite place, an even prime or an odd prime of bad reduction for E. A 2-covering of E is soluble in k_v if and only if the corresponding point of V_v is in W_v.

Provided that $\mathcal{B} \supset \mathcal{S}(E)$, a 2-covering of E is soluble in k_v for all v not in $\mathcal{B}$ if and only if the corresponding point of $(k^*/k^{*2})^2$ is in $U_{\mathcal{B}}$. Hence in this case the 2-Selmer group of E can be identified with $U_{\mathcal{B}} \cap W_{\mathcal{B}}$. Since $U_{\mathcal{B}}$ and $W_{\mathcal{B}}$ are both maximal isotropic in $V_{\mathcal{B}}$, $U_{\mathcal{B}} \cap W_{\mathcal{B}}$ is both the left and the right kernel of the bilinear map $U_{\mathcal{B}} \times W_{\mathcal{B}} \to \mathbf{F}_2$ induced by $e_{\mathcal{B}}$.

So far this is traditional folklore, first systematically described by Tate. The next step was introduced in [4]. For any $\mathcal{B} \supset \mathcal{S}(E)$ we construct inside each V_v a maximal isotropic subspace K_v such that $V_{\mathcal{B}} = U_{\mathcal{B}} \oplus K_{\mathcal{B}}$. Let $t_{\mathcal{B}} : V_{\mathcal{B}} \to U_{\mathcal{B}}$ be the projection along $K_{\mathcal{B}}$ and write

$$U'_{\mathcal{B}} = U_{\mathcal{B}} \cap (W_{\mathcal{B}} + K_{\mathcal{B}}), \quad W'_{\mathcal{B}} = W_{\mathcal{B}}/(W_{\mathcal{B}} \cap K_{\mathcal{B}}) = \bigoplus\nolimits_{v \in \mathcal{B}} W'_v$$

where $W'_v = W_v/(W_v \cap K_v)$. The map $t_{\mathcal{B}}$ induces an isomorphism

$$\tau_{\mathcal{B}} : W'_{\mathcal{B}} \to U'_{\mathcal{B}}$$

and the bilinear function $e_{\mathcal{B}}$ induces a bilinear function

$$e'_{\mathcal{B}} : U'_{\mathcal{B}} \times W'_{\mathcal{B}} \to \mathbf{F}_2.$$

(An explicit description of $\tau_{\mathcal{B}}^{-1}$ will be given in the proof of Lemma 3.) The bilinear functions $U'_{\mathcal{B}} \times U'_{\mathcal{B}} \to \mathbf{F}_2$ and $W'_{\mathcal{B}} \times W'_{\mathcal{B}} \to \mathbf{F}_2$ defined respectively by

$$\theta^\flat_{\mathcal{B}}(u'_1, u'_2) = e'_{\mathcal{B}}(u'_1, \tau_{\mathcal{B}}^{-1}(u'_2)) \quad \text{and} \quad \theta^\sharp_{\mathcal{B}}(w'_1, w'_2) = e'_{\mathcal{B}}(\tau_{\mathcal{B}} w'_1, w'_2) \tag{12}$$

are symmetric. (For the proof, see [4] or [16].) We have $\theta^\sharp_{\mathcal{B}}(w'_1, w'_2) = \theta^\flat_{\mathcal{B}}(\tau_{\mathcal{B}} w'_1, \tau_{\mathcal{B}} w'_2)$.

If $\mathcal{B} \supset \mathcal{S}(E)$ the 2-Selmer group of E is isomorphic to both the left and the right kernel of $e'_{\mathcal{B}}$, and hence also to the kernels of the two maps (12). We have now two descriptions of the 2-Selmer group — one as $U_{\mathcal{B}} \cap W_{\mathcal{B}}$, which can be identified with the kernel of $e_{\mathcal{B}}$ restricted to $U_{\mathcal{B}} \times W_{\mathcal{B}}$, and the other as either kernel of $e'_{\mathcal{B}}$. These are essentially the same. For $U'_{\mathcal{B}}$ is orthogonal to $W_{\mathcal{B}} \cap K_{\mathcal{B}}$, so that $e'_{\mathcal{B}}$ induces a map $U'_{\mathcal{B}} \times W_{\mathcal{B}} \mapsto \mathbf{F}_2$ whose left kernel is the same as the left kernel of $e'_{\mathcal{B}}$. This is contained in the left kernel of $e_{\mathcal{B}}$ acting on $U_{\mathcal{B}} \times W_{\mathcal{B}}$; and these two left kernels have the same order, so they must be equal. In particular the left kernel of $e'_{\mathcal{B}}$ can be identified with $U_{\mathcal{B}} \cap W_{\mathcal{B}}$.

3. *Refining the* 2*-descent process.* In [4] there is considerable freedom in choosing the K_v, and this raises three obvious questions:

- Is there a canonical choice of the K_v?
- How small can we make U' and W'?
- Can we ensure that the functions (12) are not merely symmetric but alternating?

The answer to the first question appears to be negative, even after we have fixed the decomposition of the V_v in Lemma 1. Since $U'_{\mathcal{B}} \supset U_{\mathcal{B}} \cap W_{\mathcal{B}}$, the best possible response to the second question would be to achieve $U'_{\mathcal{B}} = U_{\mathcal{B}} \cap W_{\mathcal{B}}$; we shall do this by satisfying the requirement

$$W_{\mathcal{B}} = (U_{\mathcal{B}} \cap W_{\mathcal{B}}) \oplus (K_{\mathcal{B}} \cap W_{\mathcal{B}}) \tag{13}$$

which is stronger. For suppose that (13) holds; then

$$W_{\mathcal{B}} + K_{\mathcal{B}} = (U_{\mathcal{B}} \cap W_{\mathcal{B}}) + K_{\mathcal{B}}$$

and it follows immediately that

$$U'_{\mathcal{B}} = U_{\mathcal{B}} \cap (W_{\mathcal{B}} + K_{\mathcal{B}}) = U_{\mathcal{B}} \cap W_{\mathcal{B}}. \tag{14}$$

The proof that (13) implies (14) makes no assumptions about $\mathcal{B}$ other than $\mathcal{B} \supset \mathcal{S}(E)$; we shall use this fact with $\mathcal{B}'$ instead of $\mathcal{B}$ in the proof of Lemma 3. Since the 2-Selmer group is $U_{\mathcal{B}} \cap W_{\mathcal{B}}$ and can be identified with the left and right kernels of each of the functions (12), these functions vanish identically and are therefore alternating. However in the proof of Theorem 2 below we shall need to consider other recipes for choosing the K_v, for which (13) does not hold but we can still prove that the functions (12) are alternating.

The construction of the K_v in this paper depends on two vector space lemmas, whose setting generalizes the structure described in §2. We have stated Lemma 2 in a more general form than we need for the applications, so that the notation makes it easier to use Lemma 1. In doing this we follow [4], but Lemma 2 is considerably more powerful than the corresponding result there or in [16]; however Lemma 1 can already be found in [16].

Lemma 1 *Let ψ be a non-degenerate alternating bilinear form on a finite dimensional $\mathbf{F}_2$-vector space V, and let W be a maximal isotropic subspace of V. Then V can be expressed as a direct sum $\oplus V_i$ of mutually orthogonal subspaces, each of dimension 2, such that the restriction of ψ to any V_i is non-degenerate, each $V_i \cap W$ has dimension 1 and W is the direct sum of the $V_i \cap W$.*

Proof The existence of ψ shows that dim V is even; so let dim $V = 2n$ with $n > 1$, the case $n = 1$ being trivial. It is enough to show that if w_1 is a non-trivial element of W then w_1 lies in a subspace V_1 satisfying the conditions of the lemma, and that if V' is the orthogonal complement of V_1 in V then $\dim(V' \cap W) = n - 1$; for we can then complete the proof by induction on n. For this, choose x_1 in V not orthogonal to w_1. Let V_1 be the vector space generated by w_1 and x_1 and let V' be its orthogonal complement in V. Thus $\dim(V_1 \cap W) = 1$ and the restriction of ψ to V_1 is non-degenerate, because V_1 is not isotropic. Now $V' \cap W$ is the subspace of W orthogonal to x_1; so $\dim(V' \cap W) \geq n - 1$. On the other hand, w_1 is not in $V' \cap W$; so $\dim(V' \cap W) \leq n - 1$. □

Lemma 2 *Let the V_i be n vector spaces over $\mathbf{F}_2$, each equipped with a non-degenerate additive alternating bilinear form ψ_i with values in $\mathbf{F}_2$. Denote by ψ the sum of the ψ_i, which is a non-degenerate bilinear form on $V = \oplus V_i$. For each i let W_i be maximal isotropic in V_i, and let U be maximal isotropic in V with respect to ψ. Then there exist maximal isotropic subspaces $K_i \subset V_i$ such that $V = U \oplus K$ and*

$$W = (U \cap W) \oplus (K \cap W) \tag{15}$$

where $W = \oplus W_i$ and $K = \oplus K_i$. Moreover $U \cap (W + K) = U \cap W$.

Suppose also that there are functions ϕ_i on V_i with values in $\mathbf{F}_2$ which satisfy

$$\phi_i(\xi+\eta) = \phi_i(\xi) + \phi_i(\eta) + \psi_i(\xi,\eta) \tag{16}$$

for any ξ, η in V_i, and let ϕ on V be the sum of the ϕ_i. Assume that ϕ is trivial on U and ϕ_i is trivial on W_i. Then the K_i can be so chosen that in addition ϕ_i is trivial on K_i and therefore ϕ is trivial on K.

Proof We consider first the special case in which every V_i has dimension 2 and therefore every W_i has dimension 1. Let I be maximal among those subsets of $\{1,\dots,n\}$ for which $U \cap W_I$ is trivial, and let J be the complement of I. For $i \in I$ we choose $K_i = W_i$; this will automatically ensure that ϕ_i is trivial on K_i and that $U + \oplus_{i\in I} K_i$ is a direct sum. For any $j \in J$ the maximality of I shows that $U \cap (W_I + W_j)$ is nontrivial, whence $W_j \subset U \oplus W_I$ because W_j is one-dimensional; so $U \oplus W_I \supset W$. Choose each K_j so that $V_j = W_j \oplus K_j$ and suppose that $u + \sum w_i = \sum k_j$ is in $(U \oplus W_I) \cap K_J$. If for $\ell \in J$ we write the nontrivial element w_ℓ of W_ℓ as $w_\ell = u' + \sum w'_i$ in $U \oplus W_I$ then

$$\begin{aligned}\psi(k_\ell, w_\ell) =& \psi(\sum k_j, w_\ell) = \psi(u, w_\ell) = \psi(u, \sum w'_i) \\ &= \psi(\sum k_j - \sum w_i, \sum w'_i) = 0;\end{aligned}$$

so $k_\ell = 0$. Since this is true for each ℓ, $(U \oplus W_I) + K_J$ is a direct sum. By comparison of dimensions $V = U \oplus K$. Again $K \cap W = W_I$, so that

$$(U \cap W) \oplus (K \cap W) = (U \cap W) \oplus W_I = (U \oplus W_I) \cap W = W.$$

It only remains to show that if the ϕ_i exist then we can choose the K_j for $j \in J$ so that ϕ_j vanishes on K_j. Let β_j be the nontrivial element of W_j, and let α'_j and $\alpha''_j = \alpha'_j + \beta_j$ be the elements of $V_j \setminus W_j$. Since $\phi_j(\beta_j) = 0$ it follows from (16) and the non-degeneracy of ψ_j that

$$\phi_j(\alpha'_j) + \phi_j(\alpha''_j) = \psi_j(\alpha'_j, \beta_j) = 1;$$

we now generate K_j by whichever of α'_j and α''_j satisfies $\phi_j(\alpha_j) = 0$.

To deduce the lemma in general, we use Lemma 1 to decompose each V_i as the direct sum of mutually orthogonal subspaces V_{ij} of dimension 2, on each of which the bilinear form ψ_i is non-degenerate and each of which meets W_i in a subspace W_{ij} of dimension 1. By what we have already proved, we can find spaces K_{ij} having (with respect to this finer decomposition) all the properties stated in the lemma. Now take K_i to be the sum of the K_{ij}. □

We now revert to the notation of §2. Let $\mathcal{B}_1 \subset \mathcal{B}$ and let $\mathbf{V}_{\mathcal{B}_1}$ be a vector subspace of $V_{\mathcal{B}_1}$. There are two (and sometimes three) vector spaces in $V_{\mathcal{B}}$ which we can naturally associate with $\mathbf{V}_{\mathcal{B}_1}$, and we need a notation which distinguishes them. One, which we shall denote again by $\mathbf{V}_{\mathcal{B}_1}$, is simply $\mathbf{V}_{\mathcal{B}_1} \oplus \{0\}$ where $\{0\}$ is the trivial vector subspace of $V_{\mathcal{B}\setminus\mathcal{B}_1}$. A second is $\mathbf{V}_{\mathcal{B}_1} \oplus V_{\mathcal{B}\setminus\mathcal{B}_1}$; this is $\imath^*\mathbf{V}_{\mathcal{B}_1}$ where $\imath : V_{\mathcal{B}} \to V_{\mathcal{B}_1}$ is the projection map. The third can only be defined when $\mathbf{V}_{\mathcal{B}_1} \subset U_{\mathcal{B}_1}$. Now the pull-back of $\mathbf{V}_{\mathcal{B}_1}$ under the injection $X_{\mathcal{B}_1} \times X_{\mathcal{B}_1} \hookrightarrow V_{\mathcal{B}_1}$ is a vector subspace of $X_{\mathcal{B}} \times X_{\mathcal{B}}$, so its image in $V_{\mathcal{B}}$ is a vector space which we call $\jmath_*\mathbf{V}_{\mathcal{B}_1} \subset U_{\mathcal{B}}$. This construction induces a natural isomorphism $\mathbf{V}_{\mathcal{B}_1} \to \jmath_*\mathbf{V}_{\mathcal{B}_1}$, and we shall frequently identify these two spaces. If $\mathbf{V}_{\mathcal{B}_1} \subset U'_{\mathcal{B}_1}$ and $K_{\mathcal{B}\setminus\mathcal{B}_1} = T_{\mathcal{B}\setminus\mathcal{B}_1}$ then $\jmath_*\mathbf{V}_{\mathcal{B}_1} \subset U'_{\mathcal{B}}$; in this case the image of $\jmath_*\mathbf{V}_{\mathcal{B}_1}$ under $\tau_{\mathcal{B}}^{-1}$ lies in $W'_{\mathcal{B}_1} \oplus \{0\} \subset W'_{\mathcal{B}}$, which we identify with $W'_{\mathcal{B}_1}$, and the diagram

$$\begin{tikzcd}
\jmath_*\mathbf{V}_{\mathcal{B}_1} \arrow[r, hook] & \jmath_*U'_{\mathcal{B}_1} \arrow[r] & W'_{\mathcal{B}_1} \\
\mathbf{V}_{\mathcal{B}_1} \arrow[r, hook] \arrow[u] & U'_{\mathcal{B}_1} \arrow[r] \arrow[u] & W'_{\mathcal{B}_1} \arrow[u, equal]
\end{tikzcd}$$

commutes, where $U'_{\mathcal{B}_1} \to W'_{\mathcal{B}_1}$ is $\tau_{\mathcal{B}_1}^{-1}$.

From here until the end of this section we require that $\mathcal{B} \supset \mathcal{S}(E)$. Let $\mathcal{B}$ be the disjoint union of the sets $\mathcal{B}' \supset \mathcal{S}^0$ and $\mathcal{B}''$, and replace ψ_i by e_v. It is not easy to make use of the construction of the K_v given in the proof of Lemma 2. In what follows, we shall therefore usually apply Lemma 2 to $\mathcal{B}'$ rather than $\mathcal{B}$, and we shall use a simpler but less powerful recipe for choosing K_v when v is in $\mathcal{B}''$. The new recipe does not yield (13), but we shall see in Theorem 2 that it does still make $\theta^\flat_{\mathcal{B}}$ alternating. The first part of Lemma 2, which does not involve the ϕ_i, gives the following result.

Lemma 3 *In the notation of §2, we can take $K_v = T_v$ for all v in $\mathcal{B}''$, and we can choose the K_v for v in $\mathcal{B}'$ so that*

$$W_{\mathcal{B}'} = (U_{\mathcal{B}'} \cap W_{\mathcal{B}'}) \oplus (K_{\mathcal{B}'} \cap W_{\mathcal{B}'}) \subset V_{\mathcal{B}'}, \tag{17}$$

which implies $U'_{\mathcal{B}'} = U_{\mathcal{B}'} \cap W_{\mathcal{B}'}$. Moreover

$$U'_{\mathcal{B}} = \jmath_*U'_{\mathcal{B}'} \oplus \tau_{\mathcal{B}}W'_{\mathcal{B}''} = \jmath_*U'_{\mathcal{B}'} \oplus \left(\oplus_{\mathsf{q}\in\mathcal{B}''}\tau_{\mathcal{B}}W'_{\mathsf{q}}\right) \subset V_{\mathcal{B}}, \tag{18}$$

and the restriction of $\theta^\flat_{\mathcal{B}}$ to $\jmath_*U'_{\mathcal{B}'}$ is trivial.

Proof For $\mathcal{B} = \mathcal{B}'$ this follows from Lemma 2. In the general case, let the K_v for v in $\mathcal{B}'$ be those already constructed for $\mathcal{B} = \mathcal{B}'$ and let $K_v = T_v$ for v in $\mathcal{B}''$. By dimension count, to prove that $V_{\mathcal{B}} = U_{\mathcal{B}} \oplus K_{\mathcal{B}}$ it is enough to prove that $K_{\mathcal{B}} \cap U_{\mathcal{B}}$ is trivial. But if $\sigma = (\sigma_1, \sigma_2, \sigma_3)$ is an element of $K_{\mathcal{B}} \cap U_{\mathcal{B}}$ then the σ_i must be units at $\mathfrak{p}$ for any $\mathfrak{p}$ in $\mathcal{B}''$; so σ belongs to the image of $U_{\mathcal{B}'}$ in $V_{\mathcal{B}} = V_{\mathcal{B}'} \oplus V_{\mathcal{B}''}$. Hence the projection onto $V_{\mathcal{B}'}$ of σ lies in $K_{\mathcal{B}'} \cap U_{\mathcal{B}'}$, which is trivial; so each σ_i is trivial and $K_{\mathcal{B}} \cap U_{\mathcal{B}}$ is indeed trivial. As we noted after (14), the assertion that $U'_{\mathcal{B}'} = U_{\mathcal{B}'} \cap W_{\mathcal{B}'}$ follows from (17). Again

$$\dim U'_{\mathcal{B}} = \dim W'_{\mathcal{B}} = \dim W'_{\mathcal{B}'} + \dim W'_{\mathcal{B}''} = \dim U'_{\mathcal{B}'} + \dim W'_{\mathcal{B}''}. \tag{19}$$

Consider the map

$$U'_{\mathcal{B}} \hookrightarrow V_{\mathcal{B}} = W_{\mathcal{B}} + K_{\mathcal{B}} \to W'_{\mathcal{B}} = W'_{\mathcal{B}'} \oplus W'_{\mathcal{B}''} \to W'_{\mathcal{B}''}, \tag{20}$$

where the second map is projection along $K_{\mathcal{B}}$, since $W'_{\mathcal{B}} = W_{\mathcal{B}}/(W_{\mathcal{B}} \cap K_{\mathcal{B}})$. Suppose that u is in the kernel of the map (20). Because the map $U'_{\mathcal{B}} \to W'_{\mathcal{B}}$ which is a factor of (20) is the isomorphism $\tau_{\mathcal{B}}^{-1}$ and $K_{\mathcal{B}''} = T_{\mathcal{B}''}$, this implies that u is in $\jmath_* U_{\mathcal{B}'}$ and therefore in $\jmath_* U_{\mathcal{B}'} \cap U'_{\mathcal{B}} = \jmath_* U'_{\mathcal{B}'}$. The relation (19) now shows that the map (20) is onto and its kernel is precisely $\jmath_* U'_{\mathcal{B}'}$.

For use later, it is convenient to calculate $\tau_{\mathcal{B}}^{-1} u$ for any u in $U'_{\mathcal{B}}$, though for the proof of Lemma 3 we only need to do this for u in $\jmath_* U'_{\mathcal{B}'}$. To obtain $\tau_{\mathcal{B}}^{-1} u$ we project u to an element u_v of V_v for each v in $\mathcal{B}$ and then add to each u_v whatever element of K_v is needed for the sum to lie in W_v; this sum is then projected into W'_v. If u is in $\jmath_* U'_{\mathcal{B}'}$ then u_v is in W_v for each v in $\mathcal{B}'$, by the sentence before (19), and in $T_v = K_v$ for each v in $\mathcal{B}''$. So the component of $\tau_{\mathcal{B}}^{-1} u$ in W'_v for v in $\mathcal{B}'$ is just the coset of $W_v \cap K_v$ containing u_v; and the component of $\tau_{\mathcal{B}}^{-1} u$ in W'_v for v in $\mathcal{B}''$ is trivial. To compute the first function (12) we add an element of $K_{\mathcal{B}}$ to u'_2 in such a way as to obtain an element w_2 of $W_{\mathcal{B}}$, and we then evaluate

$$\theta^\flat_{\mathcal{B}}(u'_1, u'_2) = e_{\mathcal{B}}(u'_1, w_2) = e_{\mathcal{B}'}(u'_1, w_2) + e_{\mathcal{B}''}(u'_1, w_2).$$

If u'_1 and u'_2 are both in $\jmath_* U'_{\mathcal{B}'}$ then the first summand on the right vanishes because $U'_{\mathcal{B}'} \subset W_{\mathcal{B}'}$ and $e_{\mathcal{B}'}$ is trivial on $W_{\mathcal{B}'} \times W_{\mathcal{B}'}$, and the second summand on the right vanishes because the projection of w_2 on $V_{\mathcal{B}''}$ is trivial. □

The map $\tau_{\mathcal{B}}^{-1} : W'_{\mathcal{B}} \to U'_{\mathcal{B}}$ depends on the choice of $\mathcal{B}'$ and of the K_v, and so does the composite map $W_{\mathcal{B}} \to W'_{\mathcal{B}} \to U'_{\mathcal{B}} \to U_{\mathcal{B}}$. Lemma 3 enables us to write the matrix representing $\theta^\sharp$ or $\theta^\flat$ in the form $\begin{pmatrix} 0 & * \\ * & * \end{pmatrix}$, and we already know that this matrix is symmetric. In Theorem 2 we obtain sufficient conditions for the matrix to be alternating; this result is useful primarily because alternating matrices have even rank. Our main application of Theorem 2 is to twisted curves E_b where $\mathcal{B}'$ contains $\mathcal{S}(E)$ and the primes in $\mathcal{B}''$ are bad only because they divide b. But it costs nothing to prove a slightly more general result.

For the rest of this paper, we always choose the K_v in accordance with the recipe in Lemma 3. When we apply the second paragraph of Lemma 2, we replace i by v and ψ_i by e_v; and for (m_1, m_2, m_3) in V_v where $v \in \mathcal{B}'$ we take $\phi_v((m_1, m_2, m_3))$ to be any one of the three expressions

$$(m_i(c_i - c_j)(c_i - c_k), m_j(c_j - c_i)(c_j - c_k))_v, \tag{21}$$

which can easily be seen to be equal. The significance of ϕ_v is as follows. The antipodal involution $(X, Y) \mapsto (X, -Y)$ on (3) determines an involution on the 2-covering E^m; in the notation of (7) this involution reverses the signs of Y_1, Y_2, Y_3. The quotient of E^m by this involution is a smooth projective curve C^m of genus 0, which is given by

$$(c_2 - c_3)m_1Y_1^2 + (c_3 - c_1)m_2Y_2^2 + (c_1 - c_2)m_3Y_3^2 = 0; \tag{22}$$

and $\phi_v(m)$ is just the class $[C^m]$ as an element of Br k_v. We must check that these ϕ_v satisfy the conditions of Lemma 2. Straightforward calculation, starting from (21) and using the bilinearity of the Hilbert symbol, shows that if we write $\xi = (\xi_1, \xi_2, \xi_3)$ and $\eta = (\eta_1, \eta_2, \eta_3)$ then

$$\begin{aligned}\phi_v(\xi + \eta) + &\phi_v(\xi) + \phi_v(\eta) = (\xi_1, \eta_2)_v + (\eta_1, \xi_2)_v \\ &+ ((c_1 - c_2)(c_1 - c_3), (c_2 - c_1)(c_2 - c_3))_v.\end{aligned}$$

Here the sum of the first two terms on the right is $e_v(\xi, \eta)$, and the third term vanishes because the sum of its two arguments is $(c_1 - c_2)^2$. The triviality of ϕ on $U_{\mathcal{B}'}$ follows from the Hilbert product formula, and the triviality on W_v follows from the fact that for $m \in W_v$ the conic C^m has a k_v-point, whence $[C^m] = 0$. Alternatively, we can argue as follows. It follows from (22) that

$$\begin{aligned}(c_2 - c_1)(c_2 - c_3)m_2(m_1Y_1)^2 + (c_1 - c_2)(c_1 - c_3)m_1(m_2Y_2)^2 \\ = m_1m_2m_3((c_1 - c_2)Y_3)^2.\end{aligned}$$

If the 2-covering (7) is soluble, then since $m_1m_2m_3 = 1$ this implies

$$((c_1 - c_2)(c_1 - c_3)m_1, (c_2 - c_1)(c_2 - c_3)m_2)_v = 0, \tag{23}$$

which is just the result that we need.

Theorem 2 *Suppose that $\mathcal{B} \supset \mathcal{S}(E)$ is the disjoint union of $\mathcal{B}' \supset \mathcal{S}^0$ and $\mathcal{B}''$. Suppose that for each $\mathfrak{q}$ in $\mathcal{B}''$ all the $v_{\mathfrak{q}}(c_i - c_j)$ have the same parity. Choose the K_v as in Lemma* 3 *so that in particular*

$$W_{\mathcal{B}'} = (U_{\mathcal{B}'} \cap W_{\mathcal{B}'}) \oplus (K_{\mathcal{B}'} \cap W_{\mathcal{B}'}) \tag{24}$$

and $K_v = T_v$ for all v in $\mathcal{B}''$. Then $\theta^\flat_{\mathcal{B}}$ is alternating on $U'_{\mathcal{B}}$.

Proof For v in $\mathcal{B}'$, ϕ_v vanishes on K_v because the K_v have been chosen as in Lemma 2. For $\mathfrak{p}$ in $\mathcal{B}''$ and m in $K_{\mathfrak{p}} = T_{\mathfrak{p}}$ the m_i are units at $\mathfrak{p}$. Hence (22) has good reduction at $\mathfrak{p}$ because the $v_{\mathfrak{p}}(c_i - c_j)$ are all congruent mod 2; so $\phi_{\mathfrak{p}}$ again vanishes on $K_{\mathfrak{p}}$. Thus $\phi_{\mathcal{B}}(k) = 0$ for all k in K.

Now let u be in $U'_{\mathcal{B}}$; thus $u = w + k$ with w in $W_{\mathcal{B}}$ and k in $K_{\mathcal{B}}$, and $\tau_{\mathcal{B}}^{-1}u$ is the image of w in $W'_{\mathcal{B}}$. Now

$$\theta^\flat_{\mathcal{B}}(u,u) = e'_{\mathcal{B}}(u, \tau_{\mathcal{B}}^{-1}u) = e_{\mathcal{B}}(u,w) = \phi_{\mathcal{B}}(u) + \phi_{\mathcal{B}}(w) + \phi_{\mathcal{B}}(u-w)$$

where the right hand equality is (16). The Hilbert product formula, applied for example to (21), shows that $\phi_{\mathcal{B}}(u) = 0$. If m is in W_v then E^m is soluble in k_v and hence so is C^m; so $\phi_v(m) = [C^m] = 0$. This proves that $\phi_{\mathcal{B}}(w) = 0$; finally $u - w = k$ and we have already shown that $\phi_{\mathcal{B}}(k) = 0$. □

For later use we need detailed information about $W_{\mathfrak{q}}$ for odd $\mathfrak{q}$ in $\mathcal{B}$. The following lemma provides a complete dictionary, though in what follows we shall only use part of it. (Unfortunately it does not seem possible to use the corresponding information when v is an infinite place, nor even to describe it when v comes from an even prime; indeed the result over **Q** for the prime 2 is already extremely intricate.) In the statement and proof of the following lemma $a_1 \sim a_2$ will mean that a_1/a_2 is in $k_{\mathfrak{q}}^{*2}$, and classes will mean classes in $k_{\mathfrak{q}}^*/k_{\mathfrak{q}}^{*2}$.

Lemma 4 *Let $\mathfrak{q}$ be an odd prime.*

If $\mathfrak{q}$ divides all the $c_i - c_j$ to the same even power, then $W_{\mathfrak{q}} = (\mathfrak{o}_{\mathfrak{q}}^*/\mathfrak{o}_{\mathfrak{q}}^{*2})^2$.

If $\mathfrak{q}$ divides all the $c_i - c_j$ to the same odd power, then $W_{\mathfrak{q}}$ consists of the classes of

$$(1,1,1) \text{ and the three triples } (8). \tag{25}$$

Now suppose that $\mathfrak{q}$ does not divide all the $c_i - c_j$ to the same power. After renumbering, let

$$v(c_1 - c_2) > v(c_1 - c_3) = v(c_2 - c_3). \tag{26}$$

Denote by η the class of $c_1 - c_2$, by ϵ the class of $c_1 - c_3$ (which by (26) *is the same as the class of $c_2 - c_3$), and by ν the class of quadratic non-residues* mod $\mathfrak{q}$. *If $v(\epsilon)$ is odd then $W_\mathfrak{q}$ consists of the classes of*

$$(1,1,1),\ (\eta\epsilon,\eta,\epsilon),\ (-\eta,-\eta\epsilon,\epsilon),\ (-\epsilon,-\epsilon,1). \tag{27}$$

If $v(\eta)$ is odd and $v(\epsilon)$ even then $W_\mathfrak{q}$ consists of the classes of

$$(1,1,1),\ (\eta\epsilon,\eta,\epsilon),\ (\nu,\nu,1),\ (\nu\eta\epsilon,\nu\eta,\epsilon). \tag{28}$$

If $v(\eta)$ and $v(\epsilon)$ are both even and $\epsilon \sim \nu$ then $W_\mathfrak{q}$ consists of the classes of

$$(1,1,1),\ (\nu,\nu,1),\ (\nu,1,\nu),\ (1,\nu,\nu). \tag{29}$$

If $v(\eta)$ and $v(\epsilon)$ are both even and $\epsilon \sim 1$ then $W_\mathfrak{q}$ consists of the classes of

$$(1,1,1),\ (\nu,\nu,1),\ (\pi,\pi,1),\ (\pi\nu,\pi\nu,1) \tag{30}$$

where π is a uniformizing variable for $\mathfrak{q}$.

Proof Since $W_\mathfrak{q}$ is maximal isotropic in $V_\mathfrak{q}$ and $\mathfrak{q}$ is odd, $W_\mathfrak{q}$ contains exactly four elements. Hence it is enough to show in each case that the elements exhibited induce distinct elements of $V_\mathfrak{q}$ and lie in $W_\mathfrak{q}$; and the first of these statements is always obvious. If the $c_i - c_j$ are all divisible by the same even power of $\mathfrak{q}$ we can rescale the equation (3) so that $\mathfrak{q}$ becomes a prime of good reduction, and the assertion is then well-known. The three expressions (8) are all in $W_\mathfrak{q}$; this proves the assertions in the lemma whenever $v(\epsilon)$ is odd, and also shows that the second expression (28) is in $W_\mathfrak{q}$. If $v(\epsilon)$ is even we can find ξ in $\mathfrak{o}_\mathfrak{q}^*$ such that $\xi \sim \nu(c_1 - c_3)$ and $1 + \xi \sim c_1 - c_3$. Indeed, the conic $(c_1 - c_3)X_1^2 = \nu(c_1 - c_3)X_2^2 + 1$ has good reduction, and so is solvable in $\mathfrak{o}_\mathfrak{q}$ by Hensel's lemma. Moreover, we can arrange that X_2 is in $\mathfrak{o}_\mathfrak{q}^*$; then we choose $\xi = \nu(c_1 - c_3)X_2^2$. Now take $X = c_1 + \xi(c_1 - c_3)$ in (11), so that

$$Y^2 = \xi(1+\xi)(c_1 - c_3)^2\{(c_1 - c_2) + \xi(c_1 - c_3)\} \sim (c_1 - c_3)^3\xi^2(1+\xi)$$

is in k^{*2}; thus $(\nu,\nu,1)$ is in $W_\mathfrak{q}$, which completes the proof of (28). The same argument also shows that $(\nu,\nu,1)$ is in $W_\mathfrak{q}$ under the hypotheses of (29). One of the last two triples (29) is an expression (8), and this completes the proof of (29). Finally, under the hypotheses of (30) the same argument as before shows that $(\nu,\nu,1)$ is in $W_\mathfrak{q}$. Since now $v(\eta) > v(\epsilon) + 1$, we can take

$$X = c_1 + \pi(c_1 - c_3) \quad \text{or} \quad X = c_1 + \nu\pi(c_1 - c_3)$$

and this shows that the last two elements of (30) are also in $W_{\mathfrak{q}}$. □

Remark When the smallest $v(c_i - c_j)$ is odd, E has additive reduction. When all the $v(c_i - c_j)$ are equal to the same even number E has good reduction. All the other cases correspond to multiplicative reduction.

4. *An effect of twisting.* For $b \in k^*$ let E_b be the quadratic twist (4) of an elliptic curve E with equation (3), and let d_b be the rank of the 2-Selmer group of E_b. We now address a special case of the problem of the variation of the parity of d_b with b.

Lemma 5 *Let $\mathfrak{q}$ be an odd prime in $\mathcal{S}(E)$ such that*

$$v_{\mathfrak{q}}(c_1 - c_2) > 0, \quad v_{\mathfrak{q}}(c_1 - c_3) = v_{\mathfrak{q}}(c_2 - c_3) = 0.$$

Let b, c in k^* be such that $b \in k_v^{*2}$ for all v in $\mathcal{S}(E)$ other than $\mathfrak{q}$, b is a quadratic non-residue at $\mathfrak{q}$, and c is a unit at $\mathfrak{q}$. Then d_c and d_{cb} have opposite parities.

Proof Equation (4) shows that without loss of generality we can assume $c = 1$. The parity of $d_b + d_1$ is that of the rank of the 2-Selmer group of E over $k(\sqrt{b})$ ([10], Lemma 1.2, which uses the skew-symmetric Cassels-Tate form, but not the conjectural finiteness of the Tate–Shafarevich groups). By Thm. 1 of [8] this rank has the same parity as the (finite) sum of th $i_v = \dim W_v/(W_v \cap W_v^{(b)})$, where $W_v^{(b)}$ is the image of $E_b(k_v)$ in V_v (see [8], (11) and Prop. 7). In our case if $v \neq \mathfrak{q}$ is in $\mathcal{S}(E)$ then E and E_b are isomorphic over k_v, and hence $i_v = 0$. The reduction of E at $\mathfrak{q}$ is multiplicative and $k(\sqrt{b})/k$ is inert, thus $i_{\mathfrak{q}} = 1$ by the formulae on p. 128 of [8]. If $v \notin \mathcal{S}(E)$ is a prime dividing b to an odd power, then the reduction of E at v is good and $k(\sqrt{b})/k$ is ramified; in this case $i_v = 0$ by Prop. 3 of [8]. If both E and E_b have good reduction at v, then $W_v = W_v^{(b)}$, so that $i_v = 0$. Alternatively, dim $W_v \cap W_v^{(b)}$ in all these cases can be easily found from Lemma 4. □

5. *The local-to-global step and the vertical obstruction.* Let k be a field of characteristic 0 with algebraic closure $\overline{k}$; $\Gamma = \mathrm{Gal}\,(\overline{k}/k)$. Let X and Y be smooth projective varieties over k, and $\pi : Y \to X$ a *ramified* double covering. For an irreducible divisor $D \subset X$ we write $\mathrm{val}_D : k(X)^* \to \mathbf{Z}$ for the corresponding valuation, and write k_D for the algebraic closure of k in the function field $k(D)$. Choose $f \in k(X)$ such that $k(Y) = k(X)(\sqrt{f})$. Define a separable k-algebra L as the direct sum of k_D such that $\mathrm{val}_D(f)$ is

odd; L is well defined since f is unique up to multiplication by an element of $k(X)^{*2}$.

Let $\mathcal{Y}$ be the quotient of $Y \times_k \mathbf{G}_m$ by $\mu_2 = \{\pm 1\}$ acting on $\mathbf{G}_m$ by multiplication and on Y as the Galois group of the covering $Y \to X$. The generic fibre of $\mathcal{Y} \to X$ is a $k(X)$-torsor under $\mathbf{G}_m$; it is trivial by Hilbert's theorem 90. Hence $\mathcal{Y}$ is birationally equivalent to $X \times_k \mathbf{P}^1_k$ over X. If t is a multiplicative coordinate on $\mathbf{G}_m$, then $\mathcal{Y}$ is given by the equation $y^2 = tf$. The fibres of the natural map $\mathcal{Y} \to \mathbf{P}^1_k$ are the quadratic twists Y_a of Y, for all $a \in k^*$. By Hironaka's theorem there exists a smooth compactification $\mathcal{Y} \subset \mathcal{X}$ such that the following diagram commutes:

$$\begin{tikzcd}
\mathcal{Y} \arrow[r, hook] \arrow[d] & \mathcal{X} \arrow[d, "p"'] \\
\mathbf{G}_m \arrow[r, hook] & \mathbf{P}^1_k
\end{tikzcd}$$

We refer the reader to §1 of [5] for a convenient survey of the basic properties of the Brauer group. By definition the vertical Brauer group $\mathrm{Br}_{\mathrm{vert}}\mathcal{X}$ attached to the morphism $p : \mathcal{X} \to \mathbf{P}^1_k$ is the intersection of $p^*\mathrm{Br}\, k(\mathbf{P}^1_k) = p^*\mathrm{Br}\, k(t)$ and $\mathrm{Br}\,\mathcal{X}$ in $\mathrm{Br}\, k(\mathcal{X})$. The commutative diagram

$$\begin{tikzcd}
\mathrm{Br}\, k(X) \arrow[r, hook] & \mathrm{Br}\, k(X \times_k \mathbf{P}^1_k) \arrow[r, phantom, "="] & \mathrm{Br}\, k(\mathcal{X}) \\
\mathrm{Br}\, X \arrow[u, phantom, "\cup"] \arrow[r, phantom, "="] & \mathrm{Br}\,(X \times_k \mathbf{P}^1_k) \arrow[u, phantom, "\cup"] \arrow[r, phantom, "="] & \mathrm{Br}\,\mathcal{X} \arrow[u, phantom, "\cup"]
\end{tikzcd}$$

shows that $\mathrm{Br}\, X$ is naturally isomorphic to $\mathrm{Br}\,\mathcal{X}$. Thus we can consider $\mathrm{Br}_{\mathrm{vert}}\mathcal{X}$ as a subgroup of $\mathrm{Br}\, X$. Recall the standard notation

$$\mathrm{Br}_0 X = \mathrm{Im}[\mathrm{Br}\, k \to \mathrm{Br}\, X], \quad \mathrm{Br}_1 X = \mathrm{Ker}\,[\mathrm{Br}\, X \to \mathrm{Br}\, \overline{X}].$$

Theorem 3 *In the above notation* $\mathrm{Br}_{\mathrm{vert}}\mathcal{X}/\mathrm{Br}_0 X$ *consists of the classes of quaternion algebras* (c, f)*, where* c *belongs to the finite group* $\mathrm{Ker}\,[k^*/k^{*2} \to L^*/L^{*2}]$*.*

The theorem also holds for π unramified provided that c ranges over all of k^*/k^{*2}.

Proof By the definition of $\mathcal{Y}$ the base change $\mathbf{G}_m \to \mathbf{G}_m$, $t \mapsto t^2$, turns $\mathcal{Y} \to \mathbf{G}_m$ into $Y \times_k \mathbf{G}_m \to \mathbf{G}_m$. Hence the base change $f : \mathbf{P}^1_k \to \mathbf{P}^1_k$ given by $t = z^2$ turns $p : \mathcal{X} \to \mathbf{P}^1_k$ into $p' : \mathcal{X}' \to \mathbf{P}^1_k$, where $\mathcal{X}'$ is birationally equivalent to $Y \times_k \mathbf{P}^1_k$ over $\mathbf{P}^1_k$. We have an obvious commutative diagram:

$$\begin{tikzcd}
\mathrm{Br}\, k(z) \arrow[r, "p'^*"] & \mathrm{Br}\, k(\mathcal{X}') & \supset & \mathrm{Br}\, \mathcal{X}' & = & \mathrm{Br}\,(Y \times_k \mathbf{P}^1_k) & = & \mathrm{Br}\, Y \\
\mathrm{Br}\, k(t) \arrow[r, "p^*"] \arrow[u, "f^*"] & \mathrm{Br}\, k(\mathcal{X}) \arrow[u] & \supset & \mathrm{Br}\, \mathcal{X} \arrow[u] & & & &
\end{tikzcd}$$

Let $\mathcal{A} \in \mathrm{Br}\, k(t)$ be such that $p^*\mathcal{A} \in \mathrm{Br}\, \mathcal{X}$. Since the fibres of $\mathcal{Y} \to \mathbf{G}_m$ are geometrically irreducible, $\mathcal{A}$ can be ramified only at 0 and ∞. On the other hand, we have $p'^* f^* \mathcal{A} \in \mathrm{Br}\, \mathcal{X}' = \mathrm{Br}\,(Y \times_k \mathbf{P}^1_k)$. Since the fibres of the projection $Y \times_k \mathbf{P}^1_k \to \mathbf{P}^1_k$ are geometrically irreducible, $f^*\mathcal{A}$ is an unramified element of $\mathrm{Br}\, k(z)$, hence $f^*\mathcal{A} \in \mathrm{Br}\, \mathbf{P}^1_k = \mathrm{Br}\, k$. The covering $f : \mathbf{P}^1_k \to \mathbf{P}^1_k$ is ramified only at 0 and ∞, with ramification index 2, hence the equal residues of $\mathcal{A}$ at 0 and ∞ are the classes in k^*/k^{*2} of some $c \in k^*$. It follows that up to an element of $\mathrm{Br}\, k$ we have $\mathcal{A} = (c, t)$ (see [5], §1.2). The natural injection $\mathrm{Br}\, k(X) \to \mathrm{Br}\, k(\mathcal{X})$ sends (c, f) to $(c, f) = (c, t)$, since $tf \in k(\mathcal{X})^{*2}$. This map restricted to $\mathrm{Br}\, X$ is an isomorphism onto $\mathrm{Br}\, \mathcal{X}$, hence $(c, t) \in \mathrm{Br}\, \mathcal{X}$ if and only if $(c, f) \in \mathrm{Br}\, X$. The purity theorem of Grothendieck ([6], II, Thm. 6.1, see also [5], Thm. 1.3.2) gives the following exact sequence

$$0 \to \mathrm{Br}\, X \to \mathrm{Br}\, k(X) \xrightarrow{\mathrm{res}} \oplus H^1(k(D), \mathbf{Q}/\mathbf{Z})$$

where the sum is over all irreducible divisors $D \subset X$. If $\mathrm{val}_D(f)$ is even then $\mathrm{res}_D((c, f)) = 0$; if $\mathrm{val}_D(f)$ is odd, then $\mathrm{res}_D((c, f))$ is the class of c in $k_D^*/k_D^{*2} \subset k(D)^*/k(D)^{*2} = H^1(k(D), \frac{1}{2}\mathbf{Z}/\mathbf{Z}) \subset H^1(k(D), \mathbf{Q}/\mathbf{Z})$ (see [5], Prop. 1.1.3). This shows that $(c, f) \in \mathrm{Br}\, X = \mathrm{Br}\, \mathcal{X}$ precisely when c goes to zero in L^*/L^{*2}. □

Now assume that k is a number field, and X has points in all completions of k.

Lemma 6 (i) *The obstruction related to* $\mathrm{Br}_{\mathrm{vert}}\mathcal{X}$*, which we call the vertical Brauer-Manin obstruction, vanishes if and only if for each place v of k there exists $a_v \in k_v^*$ such that $Y_{a_v}(k_v)$ is non-empty and*

$$\sum_v \mathrm{inv}_v((c, a_v)) = 0 \textit{ for all } c \in \mathrm{Ker}\,[k^*/k^{*2} \to L^*/L^{*2}]. \tag{31}$$

(ii) *Let $\{a_v\}$ be a family satisfying the conditions of* (i)*, and let $\mathcal{B}$ be a finite set of places of k. Then there exists $a \in k^*$ arbitrarily close to a_v for each $v \in \mathcal{B}$, and in particular with $a/a_v \in k_v^{*2}$, such that for each place v of k the set $Y_a(k_v)$ is non-empty.*

Proof (i) The vertical obstruction vanishes if and only if there exists $\{P_v\}$ in $\prod_v \mathcal{X}(k_v)$ such that $\sum_v \mathrm{inv}_v(\mathcal{A}(P_v)) = 0$ for all $\mathcal{A} \in \mathrm{Br}_{\mathrm{vert}}\mathcal{X}$. Theorem 3 shows that the quotient of $\mathrm{Br}_{\mathrm{vert}}\mathcal{X}$ by the image of $\mathrm{Br}\, k$ is finite; and for fixed $\mathcal{A}$ the function $\mathrm{inv}_v(\mathcal{A}(P_v))$ with values in $\mathbf{Q}/\mathbf{Z}$ is locally constant. Thus for each v we can find Q_v in a small neighbourhood of P_v in $\mathcal{X}(k_v)$ such that $p(Q_v) \in \mathbf{G}_m$ and $\mathrm{inv}_v(\mathcal{A}(Q_v)) = \mathrm{inv}_v(\mathcal{A}(P_v))$ for all $\mathcal{A}$ in $\mathrm{Br}_{\,vert}\mathcal{X}$. Let $a_v \in k_v^*$ be the coordinate of $p(Q_v)$. Now (i) follows from Theorem 3.

(ii) See the proof of Theorem A of [2], which uses torsors and strong approximation. Alternatively, if L contains a factor which is an abelian extension of k we can apply Theorem 2.2.1(a) of [3] to an appropriate model $\mathcal{X}$ (this theorem uses Dirichlet's theorem on primes in an arithmetic progression). For both theorems it is essential that at most two geometric fibres of p are degenerate. □

Similar results were obtained by David Harari by a different method (unpublished).

We now consider a particular case of the above set-up. In the rest of this section $f^{(1)}(x_1)$ and $f^{(2)}(x_2)$ will be any separable quartic polynomials. We remind the reader that the curves $D^{(s)}$, $s = 1, 2$, are defined by $y_s^2 = f^{(s)}(x_s)$, and that $E^{(s)}$ is the Jacobian of $D^{(s)}$. Let Y be the blowing-up of the sixteen points of $D^{(1)} \times D^{(2)}$ given by $x_1 = x_2 = 0$, and let X be the minimal desingularization of the quotient of $D^{(1)} \times D^{(2)}$ by the involution which changes the signs of y_1 and y_2. This involution extends to Y and defines a double covering $\pi : Y \to X$ ramified at the sixteen exceptional curves. We can choose either of $f^{(1)}$ and $f^{(2)}$ as our function f. For $s = 1, 2$ let L_s be the separable k-algebra $k[x]/(f^{(s)}(x))$; then $L = L_1 \otimes_k L_2$.

Lemma 7 (i) *Suppose that the group* $\mathrm{Ker}[k^*/k^{*2} \to L^*/L^{*2}]$ *is generated by* $\mathrm{Ker}[k^*/k^{*2} \to L_1^*/L_1^{*2}]$ *and* $\mathrm{Ker}[k^*/k^{*2} \to L_2^*/L_2^{*2}]$. *Then* $\mathrm{Br}_{\mathrm{vert}}\mathcal{X} = \mathrm{Br}_0 X$.

(ii) *The condition of* (i) *is satisfied when each* $f^{(i)}$ *is irreducible with a biquadratic splitting field or is the product of two irreducible quadratic polynomials.*

(iii) *Let k be a number field. Suppose that X has points in all completions of k, and each $E^{(s)}$ has all its 2-division points in k. Let $\mathcal{B}$ be a finite set of places of k and for each v in $\mathcal{B}$ let a_v in k_v^* be such that each $D_{a_v}^{(s)}(k_v)$ is non-empty. Then there exists a in k^* arbitrarily close to a_v for each v in $\mathcal{B}$ such that for each place v of k neither of the $D_a^{(s)}(k_v)$ is empty.*

Proof (i) The quaternion algebra $(c, f) = (c, f^{(s)}(x_s))$ with $c \in \mathrm{Ker}\,[k^*/k^{*2} \to L_s^*/L_s^{*2}]$ is in $\mathrm{Br}\,\mathcal{X}$ and belongs to the image of $\mathrm{Br}\, k(x_s)$; and $k(x_s) \subset k(\mathcal{X})$.

The algebra $(c, f^{(s)}(x))$ is unramified away from the closed points of $\mathbf{A}^1_k$ given by the monic irreducible factors $P(x)$ of $f^{(s)}(x)$. The residue at $P(x) = 0$ is the class of c in $H^1(k_P, \mathbf{Z}/2) = k_P^*/k_P^{*2}$, where $k_P = k[x]/(P(x))$. Since $L_s = \oplus_P k_P$ where the sum is taken over all irreducible monic $P(x)$ dividing $f^{(s)}(x)$, we have $L_s^*/L_s^{*2} = \oplus_P k_P^*/k_P^{*2}$. Hence $(c, f^{(s)}(x))$ is unramified everywhere on $\mathbf{A}^1_k$. It is also unramified at infinity since the degree of $f^{(s)}$ is even. Thus $(c, f^{(s)}(x))$ represents an element of $\mathrm{Br}\,\mathbf{P}^1_k = \mathrm{Br}\,k$.

(ii) In this case L is a direct sum of composita of factors of L_1 and L_2. All these fields are pluriquadratic extensions of k, and the statement follows at once.

(iii) We are in the situation of (ii), thus we have the conclusion of (i). Since the vertical Brauer–Manin obstruction vanishes, (31) holds for any family $\{a_v\}$ such that $D^{(s)}_{a_v}(k_v)$ is not empty. Now the statement follows from Lemma 6(ii). □

Note that the condition in (i) of this lemma is not always satisfied. Indeed, $\mathrm{Ker}[k^*/k^{*2} \to L^*/L^{*2}]$ consists of the classes of those a in k^* such that $L \supset k(\sqrt{a})$. Hence it is enough to show that there exist extensions k_1 and k_2, both of degree 4, such that each of them contains the same quadratic extension k_0 of k and no other subextension, but the compositum $K = k_1k_2$ also contains a different quadratic extension of k. To construct such an example we start with a Galois extension K/k with Galois group D_4, the dihedral group of order 8 generated by (1234) and (13). Let H_1 and H_2 be the subgroups of D_4 generated by (13) and (24) respectively, and let k_1 and k_2 be the fixed fields of H_1 and H_2 respectively; then $K = k_1k_2$. The fields L with $K \supset L \supset k$ correspond to the subgroups $G = \mathrm{Gal}(K/L) \subset D_4$, and $L \subset k_i$ if and only if $G \supset H_i = \mathrm{Gal}(K/k_i)$. The subgroups of index 2 in D_4 are $G_1 = \langle(1234)\rangle$, $G_2 = \langle(12)(34), (13)(24)\rangle$ and $G_3 = \langle(13)(24)\rangle$; and G_3 contains both H_i, whereas G_1 and G_2 contain neither H_i. Hence there are three quadratic extensions of k contained in K, but only one of them is contained in either of the k_i.

Corollary *Assume that the surface* (1) *is everywhere locally soluble and Condition E holds. Then there exists $a \in k^*$ such that for $s = 1, 2$ the* 2-*covering of $E^{(s)}_a$ given by $m \in \mathcal{M}$ is everywhere locally soluble if and only if $m = (1, 1, 1)$ or $m = m^{(s)}$.*

Proof Condition E gives us $a_v \in k_v^*$ for every place v of bad reduction of (1). By Lemma 7(iii) we can find $a \in k^*$ such that $a/a_v \in k^{*2}$ for all these places, and such that both curves $D_a^{(s)}$ are everywhere locally soluble. However, the 2-covering of $E_a^{(s)}$ given by $m \in \mathcal{M}$ other than $(1,1,1)$ or $m^{(s)}$ is not soluble at the place w provided by Condition E. $\square$

The proof of Lemma 7(iii) is not constructive. But for any particular pair $f^{(1)}, f^{(2)}$ defined over k, regardless of whether it satisfies the conditions of Lemma 7(ii) or (iii), the search for a suitable a, and therefore the decision whether such an a exists, is finite. The argument is as follows. Let ψ be the natural map $k^* \to \prod_{\mathcal{S}}(k_v^*/k_v^{*2})$ where $\mathcal{S} = \mathcal{S}(D^{(1)}, D^{(2)})$, and for any a in k^*/k^{*2} decompose the ideal (a) as $\mathfrak{a}'\mathfrak{a}''$ where $\mathfrak{a}'$ is a product of ideals in $\mathcal{S}$ and $\mathfrak{a}''$ is a product of ideals outside $\mathcal{S}$; here $\mathfrak{a}'$ and $\mathfrak{a}''$ are really ideals modulo squares of ideals. Suppose we choose one of the finitely many values of $\psi(a)$ for which both $D_a^{(s)}$ are locally soluble at each place in $\mathcal{S}$; this in particular determines $\mathfrak{a}'$. Let $\mathfrak{p}$ be a prime with $v_{\mathfrak{p}}(\mathfrak{a}'')$ odd; then $f^{(s)}(X) = 0$ must be soluble in $k_{\mathfrak{p}}$ for $D_a^{(s)}$ to be soluble in $k_{\mathfrak{p}}$. The only other condition which we need to impose on $\mathfrak{a}''$ is that $\mathfrak{a}'\mathfrak{a}''$ is principal and can be written as (a) with $\psi(a)$ having the chosen value. For given $\mathfrak{a}'$ the question whether there exists an $\mathfrak{a}''$ satisfying these conditions is decidable.

6. *Proof of Theorem* 1. We need to impose some extra constraints on the value of a given by the Corollary to Lemma 7. Once we have chosen a, the twists $E_c^{(s)}$ which will appear in this section will all be such that c/a is a unit at each prime in $\mathcal{S}_a = \mathcal{S}_a(D^{(1)}, D^{(2)})$. The first additional property in Lemma 8 ensures that Conditions Z_1 and Z_2 hold for all those $D_c^{(s)}$ and not merely for the $D^{(s)}$. The second additional property ensures that for each s the three triples (8) are distinct from each other, from $(1,1,1)$ and from $m^{(s)}$; we have already required each $m^{(s)}$ to be distinct from $(1,1,1)$. Recall that the $m^{(s)}$ are units outside $\mathcal{S}_a$.

Lemma 8 *Assume that the surface* (1) *is everywhere locally soluble and Condition E holds. Then there exists $a \in k^*$ such that for $s = 1,2$ the 2-covering of $E_a^{(s)}$ given by $m \in \mathcal{M}$ is everywhere locally soluble if and only if $m = (1,1,1)$ or $m = m^{(s)}$. Moreover, we can arrange that in addition*

- *a is a unit at $\mathfrak{p}^{(s)}$ for each $\mathfrak{p}^{(s)}$ in Conditions Z_1 and Z_2,*
- *there is a prime ideal $\mathfrak{p}$ not in $\mathcal{S}(D^{(1)}, D^{(2)})$ such that $v_{\mathfrak{p}}(a)$ is odd.*

Proof Choose a as in the Corollary to Lemma 7. If the first additional property does not hold, suppose for example that some such $\mathfrak{p}^{(1)}$ does divide

a to an odd power, and let $\mathfrak{p}$ be a prime ideal not in $\mathcal{S}_a$ such that we can write $\mathfrak{p}/\mathfrak{p}^{(1)} = (b)$ where b is in k_v^{*2} for every v in $\mathcal{S}_a$ other than $\mathfrak{p}^{(1)}$. The solubility of $D_a^{(1)}$ at $\mathfrak{p}^{(1)}$ implies that we are in case (27) of Lemma 4 and therefore $m^{(1)}$ is in the class of $(1,1,1)$ because by hypothesis $m^{(1)}$ is a unit at $\mathfrak{p}^{(1)}$. Hence $D_{ab}^{(1)}$ is soluble at $\mathfrak{p}^{(1)}$. Similarly $D_a^{(2)}$ is in case (25) of Lemma 4, so that $m^{(2)}$ is in the class of $(1,1,1)$ and $D_{ab}^{(2)}$ is soluble at $\mathfrak{p}^{(1)}$. For any v in $\mathcal{S}_a$ other than $\mathfrak{p}^{(1)}$, $D_{ab}^{(s)}$ is isomorphic to $D_a^{(s)}$ over k_v and therefore soluble in k_v. The Hilbert product formula applied to each symbol $(m_i^{(s)}, b)$ shows that each $m_i^{(s)}$ is a square at $\mathfrak{p}$; thus the curves $D_{ab}^{(s)}$ are soluble at $\mathfrak{p}$. Since both curves $D_{ab}^{(s)}$ are everywhere locally soluble we can replace a by ab, and $\mathfrak{p}^{(1)}$ divides ab to an even power.

To satisfy the second condition we multiply a by π, where $\mathfrak{p} = (\pi)$ is a principal prime ideal such that π is in k_v^{*2} for every v in $\mathcal{S}_a$.

It remains to check that no 2-covering of $E_{ab}^{(s)}$ defined by a triple $m \neq (1,1,1)$, $m \neq m^{(s)}$, is everywhere locally soluble. By Corollary to Lemma 7 the 2-covering of $E_a^{(s)}$ is insoluble at some prime $v \in \mathcal{S}_a$, and $v \neq \mathfrak{p}^{(1)}$ since each $m_i^{(s)}$ is a square at $\mathfrak{p}^{(1)}$. Now $E_{ab}^{(s)}$ and $E_a^{(s)}$ are isomorphic over k_v, so that their 2-coverings given by m are both soluble or both insoluble. □

We denote the rank of the 2-Selmer group of $E_a^{(s)}$ by $d_a^{(s)}$. From now on a has the fixed value given by Lemma 8; thus $\mathcal{S}_a$ is also fixed. At later stages the constant actually used for the twisting will be denoted by c, and to change the twisting we shall replace c by cb where b will be a unit at every prime in $\mathcal{S}_c$. As was noted in §1, the components m_i of a triple m are really elements of k^*/k^{*2}, though it is convenient to represent them as elements of k^*; so $v_{\mathfrak{q}}(m_i)$ for any prime $\mathfrak{q}$ is really an element of $\mathbf{Z}/2$.

We express the proof of Theorem 1 as an algorithm for choosing a value of c such that every $D_c^{(s)}$ is everywhere locally soluble and each $d_c^{(s)} = 3$. The reader to whom algorithms are repellent can choose that value of c satisfying the conditions of Lemma 8 for which the pair $d_c^{(1)}, d_c^{(2)}$ is minimal under the lexicographic ordering. The arguments which follow then enable him or her to obtain a contradiction unless $d_c^{(1)} = d_c^{(2)} = 3$. Of course recasting the argument in this form renders it non-constructive.

Define the *restricted* 2-*Selmer group* of $E_c^{(s)}$ to be the subgroup of the 2-Selmer group consisting of those triples which are units outside $\mathcal{S}_a$. The restricted 2-Selmer group contains $D_c^{(s)}$ and the trivial element $E_c^{(s)}$. In the first stage of the algorithm, which is Lemma 9(i), we reduce the restricted

2-Selmer group of each $E_c^{(s)}$ for this value of c to these two elements. In the second stage we reduce $d^{(1)}$ to 3, possibly at the price of increasing $d^{(2)}$; and in the third stage we reduce $d^{(2)}$ to 3 while preserving $d^{(1)} = 3$.

Lemma 9(ii) will show that the twistings involved in these stages leave the restricted 2-Selmer groups of the two $E^{(s)}$ unchanged. For at each step the change in the twisting will be given either by the Corollary to Lemma 10 or by Lemma 12. In the former case it will satisfy the conditions of Lemma 9(ii); in the latter case it will be the compositum of a twisting which obviously does not change the restricted 2-Selmer groups and a twisting which satisfies the conditions of Lemma 9(ii). Indeed Lemma 9(ii) has been tailored to these applications.

Lemma 9 *Let a satisfy the conclusions of Lemma 8.*

(i) *We can choose b in k^* so that b is a unit at each prime in $\mathcal{S}_a$ and for $s = 1, 2$ the restricted 2-Selmer group of $E_{ab}^{(s)}$ consists of $E_{ab}^{(s)}$ and $D_{ab}^{(s)}$.*

(ii) *Let c, c' be such that c/a is a unit at each prime in $\mathcal{S}_a$ and*

- *c'/c is a unit at each prime in $\mathcal{S}_c$,*
- *c'/c is in k_v^{*2} for each v in $\mathcal{S}_a$ other than possibly the $\mathfrak{p}^{(1)}$ and $\mathfrak{p}^{(2)}$ of Conditions Z_1 and Z_2,*
- *every $m_i^{(s)}$ is in $k_{\mathfrak{q}}^{*2}$ for all $\mathfrak{q}$ at which c'/c is not a unit.*

Then c'/a is a unit at each prime in $\mathcal{S}_a$. Moreover, if the restricted 2-Selmer group of $E_c^{(s)}$ consists of $E_c^{(s)}$ and $D_c^{(s)}$ then the restricted 2-Selmer group of $E_{c'}^{(s)}$ consists of $E_{c'}^{(s)}$ and $D_{c'}^{(s)}$.

Proof Suppose that m is a triple which is a unit outside $\mathcal{S}_a$ but which is not in the $\mathcal{M}$ defined in Condition E in §1. By the Tchebotarev density theorem we can choose a prime $\mathfrak{p}$ not in $\mathcal{S}_a$ which splits completely in the field obtained by adjoining the square roots of all the $m_i^{(s)}$ to k, but does not split completely in the field obtained by also adjoining the square roots of the m_i. For such a $\mathfrak{p}$ all the $m_i^{(s)}$ for either s are in $k_{\mathfrak{p}}^{*2}$ but not all the m_i are in $k_{\mathfrak{p}}^{*2}$. Using Dirichlet's theorem on primes in arithmetic progression, choose a further prime $\mathfrak{p}' \neq \mathfrak{p}$ not in $\mathcal{S}_a$ such that $\mathfrak{p}\mathfrak{p}' = (x)$ for some x in k^* which is in k_v^{*2} for every v in $\mathcal{S}_a$. The Hilbert product formula applied to each symbol $(m_i^{(s)}, x)$ shows that each $m_i^{(s)}$ is a square at $\mathfrak{p}'$. Choose $\mathfrak{p}, \mathfrak{p}', x$ for each $m \in U_{\mathcal{S}_a} \setminus \mathcal{M}$, with all the $\mathfrak{p}, \mathfrak{p}'$ distinct, and let b be the product of all the factors x. For each of $s = 1, 2$ the curves $D_a^{(s)}$ and $D_{ab}^{(s)}$ are isomorphic over k_v for all $v \in \mathcal{S}_a$. This and the fact that each $m_i^{(s)}$ is a square at $\mathfrak{p}$ and $\mathfrak{p}'$ imply that the curves $D_{ab}^{(s)}$ are everywhere locally soluble. The 2-covering of $E_{ab}^{(s)}$ associated with m is locally insoluble at $\mathfrak{p}$ because we are in the case (25) of Lemma 4; here the m_i are units at $\mathfrak{p}$ and not all squares at $\mathfrak{p}$, whereas the components of the triples (8) are not all units at $\mathfrak{p}$. Hence the restricted Selmer group of $E_{ab}^{(s)}$ is contained in $\mathcal{M}$. But if $m \in \mathcal{M} \setminus \{(1,1,1), m^{(s)}\}$ then Condition E implies that the corresponding 2-covering of $E_a^{(s)}$ is not locally soluble in k_w for some $w \in \mathcal{S}_a$. Hence neither is the 2-covering of $E_{ab}^{(s)}$ corresponding to m, because b is in k_w^{*2} and therefore the 2-coverings of $E_a^{(s)}$ and $E_{ab}^{(s)}$ corresponding to m are isomorphic over k_w. So the restricted 2-Selmer group of $E_{ab}^{(s)}$ consists of $E_{ab}^{(s)}$ and $D_{ab}^{(s)}$. This proves (i).

The first conclusion in (ii) is obvious because $\mathcal{S}_c \supset \mathcal{S}_a$. Now $D_{c'}^{(s)}$ is isomorphic to $D_c^{(s)}$ in k_v for each v in $\mathcal{S}_a$ except possibly for the $\mathfrak{p}^{(1)}$ and $\mathfrak{p}^{(2)}$, and therefore is locally soluble at such v. For $\mathfrak{p}_{12}^{(1)}$ for example, $D^{(1)}$ is in case (28) of Lemma 4, so that the local solubility of $D_c^{(1)}$ implies that $m_3^{(1)}$ is locally a square, which implies the local solubility of $D_{c'}^{(1)}$; and $D_{c'}^{(2)}$ is locally soluble because $\mathfrak{p}_{12}^{(1)}$ is a prime of good reduction for $E_{c'}^{(2)}$ at which $m^{(2)}$ is a unit. Again, $D_{c'}^{(s)}$ is locally soluble for each $\mathfrak{q}$ for which c'/a is not a unit, by case (25) of Lemma 4; here we must consider separately the case when c is a unit at $\mathfrak{q}$ (when solubility follows from the third condition in the Lemma) and when c is not a unit at $\mathfrak{q}$ (when solubility of $D_{c'}^{(s)}$ follows from solubility of $D_c^{(s)}$). Hence $D_{c'}^{(s)}$ is everywhere locally soluble. For any triple m in $\mathcal{M}$ other than $m^{(s)}$ or $(1,1,1)$, arguments like those in the first half of this paragraph show that if the 2-covering corresponding to m for $E_{c'}^{(s)}$ is everywhere locally soluble, so is that corresponding to m for $E_c^{(s)}$; and this we know is false. Finally, if m is in $U_{\mathcal{S}_a} \setminus \mathcal{M}$ then the associated 2-covering of $E_c^{(s)}$ is locally insoluble at a prime $\mathfrak{p}$ which is not in $\mathcal{S}_a$ and must therefore divide c/a; so by case (25) of Lemma 4 not all the m_i are in $k_{\mathfrak{p}}^{*2}$ and therefore the 2-covering of $E_{c'}^{(s)}$ corresponding to m is also not locally soluble at $\mathfrak{p}$. □

We now take ab, with the b of Lemma 9(i), to be the initial value of c; subject to what is said in the proof of Lemma 12, all subsequent changes of c will satisfy the conditions of Lemma 9, so that the restricted 2-Selmer group of $E_c^{(s)}$ will continue to consist of $E_c^{(s)}$ and $D_c^{(s)}$. To prove Theorem 1 it is enough to show that we can modify a so as to satisfy the additional condition that both $d_a^{(s)}$ are equal to 3; for in that case each $D_a^{(s)}$ must be soluble in k, for reasons given in the Introduction.

At each step we have to consider the two curves $E_c^{(s)}$ for some c which has already been chosen, and we further twist these curves by some b which is prime to c. Here b and c, like a, are really elements of k^*/k^{*2}. At the end of the step we replace c by cb, which will be the new twisting constant. Thus $\mathcal{S}_c$ changes as the algorithm proceeds, but $\mathcal{S}_a$ is fixed.

The details of the second stage are determined by how the choice of b at each step affects $E^{(1)}$, and those of the third stage are similarly determined by $E^{(2)}$; thus we can in many places drop the superfix (s), though this will not apply to the primes $\mathfrak{p}^{(s)}$ introduced in Conditions Z_1 and Z_2 in §1, nor to the $d^{(s)}$. Each of the second and third stages consists of several steps, each of which will be of one of two kinds. A step of the first kind will always be possible, and it will either strictly decrease $d^{(s)}$ or increase it by 1. In the latter case it will be followed by a step of the second kind, and this will decrease $d^{(s)}$ by 2. To fix ideas, we describe these steps as applied to $E^{(1)}$. We can assume that $d_c^{(1)} > 3$, because otherwise there is nothing to do. For the following lemma we note that if a triple m is not a unit at some prime $\mathfrak{q}$ then exactly two of its components are divisible to an odd power by $\mathfrak{q}$.

Lemma 10 *Assume that $d_c^{(1)} > 3$, and that the restricted 2-Selmer group of $E_c^{(1)}$ consists of $E_c^{(1)}$ and $D_c^{(1)}$. Then we can choose $\mathfrak{q}_0$ in $\mathcal{S}_c \setminus \mathcal{S}_a$ so that there is a triple u in the 2-Selmer group of $E_c^{(1)}$ which is a unit at $\mathfrak{q}_0$ but is not a unit for at least one of the two primes $\mathfrak{p}^{(1)}$ in Condition Z_1.*

Proof Since the 2-Selmer group of $E_c^{(1)}$ has dimension $d_c^{(1)} > 3$, it strictly contains the product of the restricted 2-Selmer group and the group of order 4 coming from the 2-division points; so we can choose an element u of the 2-Selmer group which is not in that product. Choose a prime $\mathfrak{q}_1$ in $\mathcal{S}_c \setminus \mathcal{S}_a$. After multiplying by one of the triples (8) if necessary, we can assume that u is a unit at $\mathfrak{q}_1$. If some component of u is divisible to an odd power by one of the two $\mathfrak{p}^{(1)}$, then we can choose $\mathfrak{q}_0 = \mathfrak{q}_1$ and the proof is complete. Suppose not; since u is not in the restricted 2-Selmer group, there exists $\mathfrak{q}_2$ in $\mathcal{S}_c \setminus \mathcal{S}_a$ which divides some component of u to an odd power. By multiplying u by one of the triples (8), we can get rid of the factors $\mathfrak{q}_2$ in the components of u. But each of the triples (8) has two components which are divisible to an odd power by each of the two $\mathfrak{p}^{(1)}$; so in this case we can take $\mathfrak{q}_0 = \mathfrak{q}_2$. □

The triples attached to the 2-division points of E_c are

$$\begin{aligned}u_c^{(1)} =&((c_1-c_2)(c_1-c_3), c(c_1-c_2), c(c_1-c_3)),\\ u_c^{(2)} =&(c(c_2-c_1), (c_2-c_1)(c_2-c_3), c(c_2-c_3)),\\ u_c^{(3)} =&(c(c_3-c_1), c(c_3-c_2), (c_3-c_1)(c_3-c_2)),\end{aligned}$$

and $u_c^{(1)}u_c^{(2)}u_c^{(3)}$ is trivial. Denote by $w_{\mathfrak{q}}^{(i)}$ the image of $u_c^{(i)}$ in $V_{\mathfrak{q}}$. Despite the notation, the $u_c^{(i)}$ and $w_{\mathfrak{q}}^{(i)}$ do depend on s. For $\mathfrak{q}$ in $\mathcal{S}_c \setminus \mathcal{S}_a$ any two of the $w_{\mathfrak{q}}^{(i)}$ form a base of $W_{\mathfrak{q}}$.

From now on we shall write $\mathcal{B} = \mathcal{S}_c$; this will be the $\mathcal{B}$ which we use in applying the results of §3. For an odd prime $\mathfrak{q}$ denote by $\chi(\cdot, \mathfrak{q})$ the quadratic character mod $\mathfrak{q}$ with values in $\mathbf{F}_2$. The following corollary implements a step of the first kind for the second stage.

Corollary *Let $\mathfrak{q}_0 \in \mathcal{B} \setminus \mathcal{S}_a$ and $\mathfrak{p}^{(1)}$ satisfy Lemma* 10*. Let $\mathfrak{p} = (\pi)$ be a principal prime ideal not in $\mathcal{B}$ such that $\chi(\pi, \mathfrak{p}^{(1)}) = \chi(\pi, \mathfrak{q}_0) = 1$ and π is in k_v^{*2} for all other v in $\mathcal{B}$. Then we have either*

(i) $d_{c\pi}^{(1)} < d_c^{(1)}$ *or*

(ii) $d_{c\pi}^{(1)} = d_c^{(1)} + 1$ *and the* 2*-Selmer group of $E_{c\pi}^{(1)}$ contains elements w_2, w_3 such that the image of w_i in $W_{\mathfrak{p}}$ is $w_{\mathfrak{p}}^{(i)}$ and its image in $W_{\mathfrak{q}_0}$ is trivial.*

Proof The existence of such π follows from Dirichlet's theorem on primes in arithmetic progression, or from the Tchebotarev density theorem. Replacing c by $c\pi$ alters W_v for $v = \mathfrak{p}^{(1)}$ and for $v = \mathfrak{q}_0$ but leaves it unchanged for all other v in $\mathcal{B}$. To check that both curves $D_{c\pi}^{(s)}$ are everywhere locally soluble we need to prove local solubility at $\mathfrak{p}^{(1)}$, $\mathfrak{q}_0$ and $\mathfrak{p}$. At $\mathfrak{p}^{(1)}$ both $m^{(s)}$ are units, and it follows from the case (28) of Lemma 4 that although $W_{\mathfrak{p}^{(1)}}$ is altered on replacing c by $c\pi$, the local solubility conditions at $\mathfrak{p}^{(1)}$ on the two $D^{(s)}$ are unaltered. Since $D_c^{(s)}$ is soluble in $k_{\mathfrak{q}_0}$, the components of both $m^{(s)}$ are in $k_{\mathfrak{q}_0}^{*2}$ by case (25) of Lemma 4. Thus $D_{c\pi}^{(s)}$ is also soluble in $k_{\mathfrak{q}_0}$. The components of both $m^{(s)}$ are in $k_{\mathfrak{p}}^{*2}$ by the Hilbert product formula applied to each $(m_i^{(s)}, \pi)$, since π is a square at all $v \in \mathcal{S}_a$ except $\mathfrak{p}^{(1)}$; thus $D_{c\pi}^{(s)}$ is soluble in $k_{\mathfrak{p}}$, by case (25) of Lemma 4 again.

Now we show that one of (i) or (ii) holds. In this paragraph and again in the proof of Lemma 11, for any $\mathcal{B}_0 \subset \mathcal{B} \cup \{\mathfrak{p}\}$ and any place v of k we shall denote by $U_{\mathcal{B}_0}(v)$ for E_c the vector space consisting of those triples in $U_{\mathcal{B}_0}$ for which the associated 2-covering is soluble in k_v; similarly $U_{\mathcal{B}_0}(\mathcal{B}^\sharp)$ for

E_c will consist of those triples in $U_{\mathcal{B}_0}$ which lie in $U_{\mathcal{B}_0}(v)$ for every v in $\mathcal{B}^\sharp$. Write $\mathcal{B}_1 = \mathcal{B} \setminus \{\mathfrak{q}_0\}$ and note that $U_{\mathcal{B}_1}(\mathfrak{q}_0)$ for E_c and for $E_{c\pi}$ are the same, because by case (25) of Lemma 4 each of them consists of those elements of $U_{\mathcal{B}_1}$ whose components are all in $k^{*2}_{\mathfrak{q}_0}$. Similarly $U_{\mathcal{B}_1}(\mathfrak{p})$ for $E_{c\pi}$ consists of those elements of $U_{\mathcal{B}_1}$ whose components are all in $k^{*2}_{\mathfrak{p}}$, and an element x of $\mathfrak{o}^*_{\mathcal{B}_1}$ is in $k^{*2}_{\mathfrak{p}}$ if and only if it is not divisible to an odd power by $\mathfrak{p}^{(1)}$, by the Hilbert product formula applied to (x, π). Hence $U_{\mathcal{B}_1}(\mathfrak{p}) = U_{\mathcal{B}_1 \setminus \{\mathfrak{p}^{(1)}\}}$ for $E_{c\pi}$. The local solubility condition at $\mathfrak{p}^{(1)}$ on triples which are units at $\mathfrak{p}^{(1)}$ is the same for $E_{c\pi}$ and E_c, by case (28) of Lemma 4, so $U_{\mathcal{B}_1}(\{\mathfrak{p}, \mathfrak{p}^{(1)}\})$ for $E_{c\pi}$ is equal to $U_{\mathcal{B}_1 \setminus \{\mathfrak{p}^{(1)}\}}(\mathfrak{p}^{(1)})$ for E_c. Thus $U_{\mathcal{B}_1}(\mathcal{B})$ for E_c contains $U_{\mathcal{B}_1}(\mathcal{B} \cup \{\mathfrak{p}\})$ for $E_{c\pi}$ as a proper subspace, because we have deleted the u of Lemma 10. The codimension of $U_{\mathcal{B}_1}(\mathcal{B} \cup \{\mathfrak{p}\})$ in $U_{\mathcal{B}_1 \cup \{\mathfrak{p}\}}(\mathcal{B} \cup \{\mathfrak{p}\})$ is at most 2, hence $d^{(1)}_{c\pi} < d^{(1)}_c + 2$. By Lemma 5 the parity of $d^{(1)}_{c\pi}$ is opposite to that of $d^{(1)}_c$. Hence either we have strictly decreased $d^{(1)}$ or we have increased $d^{(1)}$ by 1. In the latter case, the codimension just described must be equal to 2, and the existence of w_2, w_3 follows immediately. □

If we have decreased $d^{(1)}$ by 1, we have made progress. But if we have increased $d^{(1)}$ by 1, we show in the next few paragraphs how the existence of w_2, w_3 allows a step of the second kind, which will diminish $d^{(1)}$ by 2; thus by means of the two steps taken together we again make progress so far as the second stage is concerned. The second stage terminates when we reach the value $d^{(1)} = 3$. For the third stage we also have to ensure that this value of $d^{(1)}$ is not increased by the steps which we use to diminish $d^{(2)}$. For a step of the first kind we show this now; for a step of the second kind we do so in Lemma 13. To reduce confusion of notation, we state and prove the next lemma with $E^{(1)}$ and $E^{(2)}$ having the same roles as in Lemma 10 and its Corollary; in the application we shall reverse the roles of $E^{(1)}$ and $E^{(2)}$.

Lemma 11 *With the notation of Lemma* 10 *and its Corollary,* $d^{(2)}_{c\pi} = d^{(2)}_c$.

Proof Write $\mathcal{B}_2 = \mathcal{S}(E^{(2)}_c)$, the set of bad places for $E^{(2)}_c$; thus $\mathcal{B}_2$ does not contain any $\mathfrak{p}^{(1)}_{ij}$, and the only place v in $\mathcal{B}_2$ for which π is not in k^{*2}_v is $\mathfrak{q}_0$. Hence $U_{\mathcal{B}_2}(\mathfrak{p})$ for $E^{(2)}_{c\pi}$ is just $U_{\mathcal{B}_2 \setminus \{\mathfrak{q}_0\}}$. It follows that

$$U_{\mathcal{B}_2}(\mathcal{B}_2 \cup \{\mathfrak{p}\}) = U_{\mathcal{B}_2 \setminus \{\mathfrak{q}_0\}}(\mathcal{B}_2)$$

for $E^{(2)}_{c\pi}$. But the right hand side is the same for $E^{(2)}_{c\pi}$ and $E^{(2)}_c$; for these two curves can be identified in k_v for any v in $\mathcal{B}_2 \setminus \{\mathfrak{q}_0\}$, and the projection of

$m \in U_{\mathcal{B}_2 \setminus \{\mathfrak{q}_0\}}$ to $V_{\mathfrak{q}_0}$ is in $W_{\mathfrak{q}_0}$ if and only if the components of this projection are in $k_{\mathfrak{q}_0}^{*2}$. Moreover the left hand side has dimension $d_{c\pi}^{(2)} - 2$ because we have to take into account the existence of the $u_{c\pi}^{(i)}$, and similarly the right hand side for $E_c^{(2)}$ has dimension $d_c^{(2)} - 2$ because of the existence of the $u_c^{(i)}$. □

It is now convenient to work with $\theta^\sharp$ rather than $\theta^\flat$, where $\theta^\flat$ and $\theta^\sharp$ are the functions defined by (12). To simplify the notation, we shall henceforth write $\theta_c^\sharp$ for $\theta_{\mathcal{B}}^\sharp$; this will depend on the choice of the K_v.

We now describe a step of the second kind. In accordance with our conventions, we write c for $c\pi$, so that the new $\mathcal{B}$ is the union of the old $\mathcal{B}$ and $\{\mathfrak{p}\}$.

Lemma 12 *Suppose that we are in case* (ii) *of the Corollary to Lemma* 10. *Let $\mathfrak{p}' = (\pi')$ be a prime ideal not dividing c such that π' is a square at all $v \in \mathcal{B}$ except $\mathfrak{p}$ and perhaps $\mathfrak{q}_0$, and that $\chi(\pi', \mathfrak{p}) = 1$. Let $\mathfrak{q}_0' = \lambda \mathfrak{q}_0$ be a prime ideal not dividing $c\pi'$ such that $\chi(\lambda, \mathfrak{p}) = 1$, λ is a square at all $v \in \mathcal{B}$ except $\mathfrak{p}$ and $\mathfrak{q}_0$, and $\chi(\pi', \mathfrak{q}_0')$ has a pre-assigned value. Set $c' = c\lambda\pi'$. Then $d_{c'}^{(1)} = d_c^{(1)} - 2$.*

Proof As usual, the existence of π' and λ follows from Dirichlet's theorem. Which value we need to assign to $\chi(\pi', \mathfrak{q}_0')$ will only become evident in Lemma 13. The operation of going from c to $c\lambda$ in effect replaces $\mathfrak{q}_0$ by $\mathfrak{q}_0'$; since $\chi(\alpha, \mathfrak{q}_0') = \chi(\alpha, \mathfrak{q}_0)$ for any α which is a unit outside $\mathcal{S}_a$, this does not alter the two restricted 2-Selmer groups. Going from $c\lambda$ to c' also does not alter either of these groups, by Lemma 9(ii).

We take $\mathcal{B}' = \mathcal{S}_a$, $\mathcal{B}'' = \mathcal{B} \setminus \mathcal{B}'$ and keep the notation $\mathcal{B}_1 = \mathcal{B} \setminus \{\mathfrak{q}_0\}$. Then $W'_{\mathcal{B}}$ is the direct sum of the subspace of dimension 2 coming from the 2-division points and the space $W'_{\mathcal{B}_1} = \tau^{-1} U'_{\mathcal{B}'} \oplus W'_{\mathcal{B}'' \setminus \{\mathfrak{q}_0\}}$. The ranks of $\theta_c^\sharp$ and of its restriction to $W'_{\mathcal{B}_1}$ are equal. Let $\mathcal{K}_c$ be the kernel of this restriction; this is a vector space of dimension $d_c^{(1)} - 2$. Take a base for $\mathcal{K}_c$ whose last two elements are the w_2 and w_3 in (ii) of the Corollary to Lemma 10, in such a way that no $w_{\mathfrak{p}}^{(i)}$ is a factor of any element other than w_2 and w_3 of this base. The use of the 2-division points has already ensured that no $w_{\mathfrak{q}_0}^{(i)}$ is a factor of any element of the base. Now extend this base for $\mathcal{K}_c$ to a base for

$W'_{\mathcal{B}_1}$. The matrix which represents $\theta_c^\sharp$ with respect to this base has the form

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & A \end{pmatrix} \tag{32}$$

where A is nonsingular.

The set $\mathcal{B}$ for the curve $E_{c'}$ is $\mathcal{B}_1 \cup \{\mathfrak{q}'_0, \mathfrak{p}'\}$. Since c/c' is a square at all $v \in \mathcal{B}_1$, the spaces $W_{\mathcal{B}_1}$ and $K_{\mathcal{B}_1}$ and hence also $W'_{\mathcal{B}_1}$ and $U'_{\mathcal{B}_1}$ for the curves E_c and $E_{c'}$ can be identified. Now we extend our base for $W'_{\mathcal{B}_1}$ to a base for $W'_{\mathcal{B}_1 \cup \{\mathfrak{p}'\}}$ for the curve $E_{c'}$ by adjoining $w^{(2)}_{\mathfrak{p}'}$ and $w^{(3)}_{\mathfrak{p}'}$. This time we have ensured that no $w^{(i)}_{\mathfrak{q}'_0}$ is a factor of any element of the base. The matrix which represents the restriction of $\theta^\sharp_{c'}$ to $W'_{\mathcal{B}_1 \cup \{\mathfrak{p}'\}}$ with respect to our base has the form

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & A & * & * \\ 0 & 0 & 1 & * & 0 & * \\ 0 & 1 & 0 & * & * & 0 \end{pmatrix} \tag{33}$$

Indeed, the fact that c/c' is a square at all $v \in \mathcal{B}_1$ implies that the 4×4 submatrix in the top left hand corner of (33) is the same as (32). We have

$$\tau_{c'} w^{(2)}_{\mathfrak{p}'} = (\pi', 1, \pi') \text{ and } \tau_{c'} w^{(3)}_{\mathfrak{p}'} = (\pi', \pi', 1)$$

since π' is a square at all the places of $\mathcal{S}_a$. It follows that

$$\begin{aligned} \theta^\sharp_{c'}(w^{(2)}_{\mathfrak{p}'}, w_2) =& e'_{\mathcal{B}}((\pi', 1, \pi'), w_2) = 2\chi(\pi', \mathfrak{p}) = 0, \\ \theta^\sharp_{c'}(w^{(3)}_{\mathfrak{p}'}, w_2) =& e'_{\mathcal{B}}((\pi', \pi', 1), w_2) = \chi(\pi', \mathfrak{p}) = 1, \end{aligned}$$

which explains the last two elements in the second row of (33); and the calculations for the last two elements of the third row are similar. Each of the last two elements in the first row of (33) is a sum of terms $\chi(\pi', \mathfrak{a})$ where $\mathfrak{a}$ is in $\mathcal{B}_1 \setminus \{\mathfrak{p}\}$, and all such terms are 0.

The rank of the matrix (33) is $4 + \dim A$. To see this, delete the first row and column; in the expansion of the resulting determinant any non-zero monomial must involve one non-zero factor from each row and column. In particular it must involve the 1s in the second and third rows and those in the second and third columns. So the value of the determinant which we are considering is $\det A \neq 0$. We conclude that the corank of (33), which is equal to $d_{c'}^{(1)} - 2$, is the corank of (32) minus 2. Hence $d_{c'}^{(1)} = d_c^{(1)} - 2$. □

Repeated use of steps of these two kinds implements the second stage. For the third stage we have also to ensure that a step of the second kind preserves $d^{(1)} = 3$; this is a weaker assertion than the one in Lemma 11, but it is adequate for our needs. As before, we state and prove the next lemma with $E^{(1)}$ and $E^{(2)}$ having the same roles as in Lemma 12; in the application the roles of $E^{(1)}$ and $E^{(2)}$ are reversed.

Lemma 13 *With the notation of Lemma* 12*, suppose that* $d_c^{(2)} = 3$*. Then there exists a value of* $\chi(\pi', \mathfrak{q}_0')$ *such that* $d_{c'}^{(2)} = 3$*.*

Proof In a notation corresponding to that of (33) the assumption $d_c^{(2)} = 3$ implies that $\mathcal{K}_c$ is generated by $m^{(2)}$. Thus the restricted matrix associated with $E_{c'}^{(2)}$ has the form

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & B & * & * \\ 0 & * & 0 & x \\ 0 & * & x & 0 \end{pmatrix} \tag{34}$$

where B is non-singular and does not depend on the $\mathfrak{q}_0'$ of Lemma 12. The reason for the zeros in the first row is that the 2-covering corresponding to $m^{(2)}$ is everywhere locally soluble. For the same reasons as in the previous proof we have $\tau_{c'} w_{\mathfrak{p}'}^{(2)} = (\pi', 1, \pi')$ and $\tau_{c'} w_{\mathfrak{p}'}^{(3)} = (\pi', \pi', 1)$; these elements do not depend on $\mathfrak{q}_0'$. Taking into account the symmetry of (34) this proves that the entries denoted by asterisks do not depend on $\mathfrak{q}_0'$. We have

$$x = \theta_{c'}^{\sharp}(w_{\mathfrak{p}'}^{(2)}, w_{\mathfrak{p}'}^{(3)}) = e_{\mathcal{B}}'((\pi', 1, \pi'), w_{\mathfrak{p}'}^{(3)}).$$

The only non-trivial term in the sum is that for $v = \mathfrak{p}'$, which is

$$e_{\mathfrak{p}'}((\pi', 1, \pi'), u_{c'}^{(3)}) = (\pi', c'(c_3 - c_2))_{\mathfrak{p}'} = (\pi', c'(c_3 - c_2))_{\mathfrak{q}_0'} + 1 = \chi(\pi', \mathfrak{q}_0') + 1.$$

Here the middle equality comes from the Hilbert product formula and the facts that π' is locally a square at all places in $\mathcal{B} \setminus \{\mathfrak{q}_0, \mathfrak{p}\}$, that c' is a unit at $\mathfrak{q}_0$ but not at $\mathfrak{p}$, and $\chi(\pi', \mathfrak{p}) = 1$. If we delete the first row and column of (34), the determinant of what is left is

$$-x^2 \det B + \text{ constant} = \chi(\pi', \mathfrak{q}_0') + \text{ constant},$$

where by 'constant' we mean something independent of the choice of $\mathfrak{q}_0'$. Here we have used the fact that in characteristic 2 the determinant of a symmetric matrix contains no non-symmetric terms. Since $\chi(\pi', \mathfrak{q}_0')$ played no part in the calculations of Lemma 12 for the curve $E^{(1)}$, we can ensure that (34) has corank 1 by suitable choice of $\chi(\pi', \mathfrak{q}_0')$. □

This completes the specification of the third stage, and so completes the proof of Theorem 1.

Appendix

In the first section of this appendix we show in Theorem 4, without assuming that the 2-division points of our elliptic curves are rational, that an appropriate generalization of Condition E implies the triviality of the algebraic part of the Brauer-Manin obstruction for X, the minimal projective desingularization of the surface (1). In the second section we prove that Conditions Z_1 and Z_2 imply that no element of exact order 2 in $\operatorname{Br} \overline{X}$ comes from $\operatorname{Br} X$. In particular, the transcendental Brauer-Manin obstruction defined by elements of the 2-primary torsion subgroup of $\operatorname{Br} X$ is trivial.

1. *Condition E and the algebraic Brauer-Manin obstruction.* Let k be a field of characteristic 0, $\Gamma = \operatorname{Gal}(\overline{k}/k)$. Let $E^{(1)}$ and $E^{(2)}$ be elliptic curves which are *not isogenous over* $\overline{k}$. Let

$$m = (m^{(1)}, m^{(2)}) \in H^1(k, E^{(1)}[2]) \oplus H^1(k, E^{(2)}[2]),$$

and let $D^{(s)}$ be the 2-covering of $E^{(s)}$ given by $m^{(s)}$, for $s = 1, 2$. Write $A = E^{(1)} \times E^{(2)}$, $D = D^{(1)} \times D^{(2)}$. The antipodal involution $\iota : x \mapsto -x$ on A commutes with the action of $A[2]$ by translations, hence there is a natural action of the k-group scheme $A[2] \times \mathbf{Z}/2$ on A. The antipodal involution acts on D, so that the corresponding twisted forms D_c are 2-coverings of quadratic twists A_c for $c \in k^*$. We consider Kummer surfaces X obtained by blowing-up the sixteen singular points of D/ι. These points correspond to the sixteen fixed points of ι on D. The fixed point set D^ι is a principal homogeneous space of $A[2]$ defined by m. In the notation of §5 we have $D^\iota = \operatorname{Spec}(L)$. Let $V = D \setminus D^\iota$ and $U = V/\iota$. Since $V \subset D$ is a complement to a finite set, the natural restriction maps $\operatorname{Pic} \overline{D} \to \operatorname{Pic} \overline{V}$ and $\operatorname{Br} D \to \operatorname{Br} V$ are isomorphisms (the last one by [6], II, Thm. 6.1, see also [5], Thm. 1.3.2).

We obtain the natural composed maps

$$\operatorname{Pic}\overline{X}\to\operatorname{Pic}\overline{U}\to\operatorname{Pic}\overline{V}=\operatorname{Pic}\overline{D},\quad \operatorname{Br}X\to\operatorname{Br}U\to\operatorname{Br}V=\operatorname{Br}D. \tag{35}$$

Since $E^{(1)}$ and $E^{(2)}$ are not isogenous over $\overline{k}$ we have an isomorphism of Galois modules $\operatorname{Pic}\overline{D}=\operatorname{Pic}\overline{D^{(1)}}\oplus\operatorname{Pic}\overline{D^{(2)}}$. Each Γ-module $\operatorname{Pic}\overline{D^{(s)}}$ fits into an exact sequence of Γ-modules

$$0\to E^{(s)}\to\operatorname{Pic}\overline{D^{(s)}}\to\mathbf{Z}\to 0;$$

here the third arrow is the degree map. Each Γ-module $(\operatorname{Pic}\overline{D^{(s)}})^\iota$ fits into an exact sequence of Γ-modules

$$0\to E^{(s)}[2]\to(\operatorname{Pic}\overline{D^{(s)}})^\iota\to\mathbf{Z}\to 0 \tag{36}$$

and $(\operatorname{Pic}\overline{D})^\iota=(\operatorname{Pic}\overline{D^{(1)}})^\iota\oplus(\operatorname{Pic}\overline{D^{(2)}})^\iota$. The class of this extension in $\operatorname{Ext}^1_k(\mathbf{Z},E^{(s)}[2])=H^1(k,E^{(s)}[2])$ is $m^{(s)}$; in other words, the differential sends $1\in\mathbf{Z}$ to $m^{(s)}\in H^1(k,E^{(s)}[2])$. This implies that

$$\begin{aligned}H^1(k,\operatorname{Pic}\overline{D^{(s)}}) &= H^1(k,E^{(s)})/\langle[D^{(s)}]\rangle,\\ H^1(k,(\operatorname{Pic}\overline{D^{(s)}})^\iota) &= H^1(k,E^{(s)}[2])/\langle m^{(s)}\rangle,\end{aligned}$$

where the class $[D^{(s)}]$ is the image of $m^{(s)}$ in $H^1(k,E^{(s)})$. Note that the submodule $(\operatorname{Pic}\overline{D^{(s)}})^\iota\subset\operatorname{Pic}\overline{D^{(s)}}$ is generated by the $\overline{k}$-points of $(D^{(s)})^\iota$.

Since X is a K3 surface the abelian group $\operatorname{Pic}\overline{X}$ is finitely generated and torsion free. Let F be the smallest extension of k such that $\operatorname{Gal}(\overline{k}/F)$ acts trivially on $\operatorname{Pic}\overline{X}$; then it also acts trivially on the $\overline{k}$-points of $(D^{(s)})^\iota$ for $s=1,2$. For a Γ-module M we write $H^1(F/k,M)$ for the kernel of the restriction map $H^1(k,M)\to H^1(F,M)$. Since $\operatorname{Pic}\overline{X}$ is a free abelian group and $H^1(\operatorname{Gal}(\overline{k}/F),\mathbf{Z})=0$ we have $H^1(k,\operatorname{Pic}\overline{X})=H^1(F/k,\operatorname{Pic}\overline{X})$. The map $\operatorname{Pic}\overline{X}\to\operatorname{Pic}\overline{D}$ factors through $(\operatorname{Pic}\overline{D})^\iota$, so that the maps (35) give rise to the following commutative diagram:

$$\begin{tikzcd}
\operatorname{Br}_1X/\operatorname{Br}_0X \arrow[rr] \arrow[d] & & \operatorname{Br}_1D/\operatorname{Br}_0D \arrow[d] \\
H^1(k,\operatorname{Pic}\overline{X}) \arrow[r] & \oplus H^1(F/k,E^{(s)}[2])/\langle m^{(s)}\rangle \arrow[r] & \oplus H^1(k,E^{(s)})/\langle[D^{(s)}]\rangle
\end{tikzcd} \tag{37}$$

where the direct sums are taken over $s=1,2$. Here the vertical maps come from the exact sequence

$$0\to\operatorname{Br}_1X/\operatorname{Br}_0X\to H^1(k,\operatorname{Pic}\overline{X})\to H^3(k,\overline{k}^*)\to H^3(X,\mathbf{G}_m) \tag{38}$$

provided by the spectral sequence $H^p(k, H^q(\overline{X}, \mathbf{G}_m)) \Rightarrow H^{p+q}(X, \mathbf{G}_m)$, and the similar sequence for D.

Let us now assume that k is a number field. We have $H^3(k, \overline{k}^*) = 0$ and also $H^3(k_v, \overline{k_v}^*) = 0$ for all completions k_v of k, so that the vertical maps in (37) are isomorphisms. Recall that $\mathcal{S}(D^{(1)}, D^{(2)})$ was defined in §1; it is the union of $\mathcal{S}^0$ and the set of places at which at least one of $D^{(1)}$ and $D^{(2)}$ has bad reduction. We now state a somewhat more general version of Condition E, which makes no assumptions about the 2-division points of the $E^{(s)}$:

> For every place $v \in \mathcal{S}(D^{(1)}, D^{(2)})$ there exists $a_v \in k_v^*$ such that
>
> (i) for each v we have $D^{(1)}_{a_v}(k_v) \neq \emptyset$ and $D^{(2)}_{a_v}(k_v) \neq \emptyset$;
>
> (ii) for each $s = 1, 2$ and each $m \in H^1(F/k, E^{(s)}[2]) \setminus \{0, m^{(s)}\}$ there exists w in $\mathcal{S}(D^{(1)}, D^{(2)})$ such that the 2-covering of $E^{(s)}_{a_w}$ given by m is not soluble in k_w;
>
> (iii) for all $c \in \mathrm{Ker}\,[k^*/k^{*2} \to L^*/L^{*2}]$ we have
>
> $$\sum_{v \in \mathcal{S}(D^{(1)}, D^{(2)})} \mathrm{inv}_v((c, a_v)) = 0.$$

In the case considered in the main body of the paper Γ acts trivially on $E^{(1)}[2]$ and $E^{(2)}[2]$. Then $m^{(s)} = (m_1^{(s)}, m_2^{(s)}, m_3^{(s)}) \in (k^*/k^{*2})^3$ with $m_1^{(s)} m_2^{(s)} m_3^{(s)} = 1$ and the field F is the extension of k obtained by adjoining to k the square roots of the $m_i^{(s)}$. A prime v not in $\mathcal{S}(E^{(1)}, E^{(2)})$ is a prime of good reduction of $D^{(1)}$ and $D^{(2)}$ if and only if F/k is unramified at v. We have

$$\mathcal{M} = H^1(F/k, E^{(s)}[2]) \tag{39}$$

for $s = 1, 2$. Condition E(iii) holds in this case by Lemma 7(iii) and its proof. Thus this Condition E reduces to the one given in §1 of the paper.

Theorem 4 *Let $E^{(1)}$ and $E^{(2)}$ be elliptic curves over a number field k, and let $D^{(1)}$ and $D^{(2)}$ be 2-coverings of $E^{(1)}$ and $E^{(2)}$ respectively. If $E^{(1)}$ and $E^{(2)}$ are not isogenous over $\overline{k}$ and Condition E holds, then the Kummer surface X associated to $D^{(1)} \times D^{(2)}$ has an adelic point satisfying the Brauer-Manin conditions given by* $\mathrm{Br}_1 X$.

Remark Conditions Z_1 and Z_2 imply that $E^{(1)}$ and $E^{(2)}$ are not isogenous over $\overline{k}$; see Theorem 5 below.

Proof $D^{(1)}$ and $D^{(2)}$ are curves of genus 1 with good reduction at v not in $\mathcal{S}(D^{(1)}, D^{(2)})$, so these curves have k_v-points. We set $a_v = 1$ for all such places v. Now the sum in Condition E(iii) extended to all places of k is 0, and so by Lemma 7(i) the vertical Brauer-Manin obstruction vanishes. By Lemma 7(ii) there exists $a \in k^*$ such that $a/a_v \in k_v^{*2}$ for $v \in \mathcal{S}(D^{(1)}, D^{(2)})$, the surface $D_a = D_a^{(1)} \times D_a^{(2)}$ has points in all completions of k, and Condition E(ii) holds with $E_a^{(s)}$ in place of $E_{a_w}^{(s)}$. In particular, $[D_a^{(s)}] \in H^1(k, E_a^{(s)})$ goes to zero in $H^1(k_v, E_a^{(s)})$ for all places v, $s = 1, 2$. Let $R = \oplus_{s=1,2} H^1(F/k, E^{(s)}[2])/\langle m^{(s)} \rangle$. The restriction from k to k_v now provides the following commutative diagram, where the products are taken over all places of k:

$$\begin{tikzcd}
 & \mathrm{Br}_1(D_a)/\mathrm{Br}\, k \arrow[r] \arrow[d, equal] & \prod_v \mathrm{Br}_1(D_a \times_k k_v)/\mathrm{Br}\, k_v \arrow[d, equal] \\
R \arrow[r] & \oplus_{s=1,2} H^1(k, E_a^{(s)})/\langle [D_a^{(s)}] \rangle \arrow[r] & \prod_v (\oplus_{s=1,2} H^1(k_v, E_a^{(s)}))
\end{tikzcd} \tag{40}$$

Condition E(ii) implies that the composition of the bottom arrows of (40) is injective.

For each $r \in R$, $r \neq 0$, we choose a place v such that the image r_v of r in $\oplus_{s=1,2} H^1(k_v, E_a^{(s)})$ is non-zero. The right kernel of the Tate pairing

$$(\cdot,\cdot)_v : \quad \oplus_{s=1,2} E_a^{(s)}(k_v) \quad \times \quad \oplus_{s=1,2} H^1(k_v, E_a^{(s)}) \quad \longrightarrow \quad \mathbf{Q}/\mathbf{Z}$$

is trivial, hence there exists $\alpha = \alpha(r)$ in $\oplus_{s=1,2} E_a^{(s)}(k_v)$ such that $(\alpha, r_v)_v \neq 0$. Define the character $\rho_r : R \to \mathbf{Z}/2$ by $\rho_r(x) = (\alpha, \mathrm{res}_{k,k_v}(x))_v$. Then $\rho_r(r) \neq 0$. We obtain $\#R-1$ characters ρ_r of R, not necessarily distinct, but such that the intersection of their kernels is trivial. Hence these characters generate $\mathrm{Hom}(R, \mathbf{Z}/2)$. Let $\delta(r) \in \prod_w (\oplus_{s=1,2} E_a^{(s)}(k_w))$ be such that $\delta(r)_v = \alpha$ and $\delta(r)_w = 0$ for $w \neq v$.

To an adelic point $\{P_v\}$ on D_a we associate the character $\chi \in \mathrm{Hom}(R, \mathbf{Z}/2)$ defined by $\chi(x) = \sum \mathrm{inv}_v(x(P_v))$ where the sum is taken over all places v of k. We can write $\chi = \sum_{r \in S} \rho_r$ for some $S \subset R \setminus \{0\}$. Consider the adelic point $\{Q_v\}$ on D_a which is the translation of $\{P_v\}$ by $\sum_{r \in S} \delta(r)$. For any $x \in R$ we have

$$\sum_v \mathrm{inv}_v(x(Q_v)) = \sum_v \mathrm{inv}_v(x(P_v)) - \sum_{r \in S} \sum_v (\delta(r)_v, \mathrm{res}_{k,k_v}(x))_v =$$
$$\chi(x) - \sum_{r \in S} \rho_r(x) = 0$$

where the first equality follows from Prop. 8(c) of [9]. The image of $\operatorname{Br}_1 X/\operatorname{Br}_0 X$ in $\operatorname{Br}_1(D_a)/\operatorname{Br} k$ factors through R, by (37). Hence the image of $\{Q_v\}$ on X is an adelic point satisfying all the Brauer-Manin conditions given by $\operatorname{Br}_1 X$. □

2. *Condition Z and the transcendental Brauer-Manin obstruction.* We retain the notation in the Introduction to the paper. In particular, $E^{(1)}$ and $E^{(2)}$ are elliptic curves with respective equations

$$z_1^2 = (x - c_1^{(1)})(x - c_2^{(1)})(x - c_3^{(1)}), \quad z_2^2 = (y - c_1^{(2)})(y - c_2^{(2)})(y - c_3^{(2)}).$$

Theorem 5 *Let k be a number field, and let X be the Kummer surface which is the minimal projective desingularization of* (1)*. If Conditions Z_1 and Z_2 hold, then $E^{(1)}$ and $E^{(2)}$ are not isogenous over $\overline{k}$, and the 2-primary torsion subgroup of* $\operatorname{Br} X$ *is contained in* $\operatorname{Br}_1 X$.

Proof Let K be the extension of k obtained by adjoining to k the square roots of -1 and the $m_i^{(s)}$. Conditions Z_1 and Z_2 imply that K/k is unramified at the four primes $\mathfrak{p}_{ij}^{(s)}$, $s = 1, 2$, of k introduced in these conditions. Hence there are primes of K over the $\mathfrak{p}_{ij}^{(s)}$ satisfying the same divisibility conditions as in Conditions Z_1 and Z_2. Thus Conditions Z_1 and Z_2 are still satisfied if we replace k by K. By permuting the $c_i^{(1)}$ and the $c_i^{(2)}$ we can assume without loss of generality that in Conditions Z_1 and Z_2 we have $i = 1$, $j = 2$ and $k = 3$. Note that $D^{(s)} \times_k K \simeq E^{(s)}$ for $s = 1, 2$. If we show that $E^{(1)}$ and $E^{(2)}$ are not isogenous over $\overline{k}$, then all the hypotheses of Theorem 6 below will be satisfied, so that Theorem 5 will follow from Theorem 6.

The modular invariant of the curve $y^2 = (x - c_1)(x - c_2)(x - c_3)$ is

$$j = 2^8 \frac{(c_1^2 + c_2^2 + c_3^2 - c_1c_2 - c_2c_3 - c_1c_3)^3}{(c_1 - c_2)^2(c_2 - c_3)^2(c_1 - c_3)^2}.$$

Let j_s be the modular invariant of $E^{(s)}$, $s = 1, 2$. Then the valuation of j_1 at $\mathfrak{p}_{ij}^{(1)}$ is -2, whereas the valuation of j_2 is positive or 0. Hence j_1 is not integral over the ring $\mathbf{Z}[j_2]$. By Thm. 2.6.3 of [12] the curves $E^{(1)}$ and $E^{(2)}$ are not isogenous over $\overline{k}$. □

Remark Since j_1 and j_2 are not algebraic integers, the curves $E^{(1)}$ and $E^{(2)}$ do not have complex multiplication. Another consequence of Conditions Z_1 and Z_2 is that all 2-primary torsion in $E^{(s)}(k)$, $s = 1, 2$, is 2-torsion. This easily follows from (8).

In the rest of this section k is a field of characteristic 0. Let Z be the Kummer surface obtained by blowing up the singular points of $(E^{(1)} \times E^{(2)})/\iota$. The surface $(E^{(1)} \times E^{(2)})/\iota$ is a double covering of $\mathbf{P}^1_k \times \mathbf{P}^1_k$ given by

$$z^2 = (x - c_1^{(1)})(x - c_2^{(1)})(x - c_3^{(1)})(y - c_1^{(2)})(y - c_2^{(2)})(y - c_3^{(2)}). \qquad (41)$$

The singular locus of this variety consists of the sixteen points with coordinates $x = c_1^{(1)}, c_2^{(1)}, c_3^{(1)}, c_4^{(1)}$ and $y = c_1^{(2)}, c_2^{(2)}, c_3^{(2)}, c_4^{(2)}$, where $c_4^{(1)} = c_4^{(2)} = \infty$. Let ℓ_{ij} be the rational curves on Z which are the inverse images of these points.

Lemma 14 *We have* $\mathrm{Br}_1 Z = \mathrm{Br}\, k$. *Let W be the complement in Z to the nine lines ℓ_{ij} with $i, j = 1, 2, 3$. Then* $\mathrm{Br}_1 W = \mathrm{Br}\, k$.

Proof By Prop. 2.3 of [7] the action of Γ on $\mathrm{Pic}\, \overline{Z}$ is trivial. Since $Z(k) \neq \emptyset$ the group $\mathrm{Br}_1 Z$ is the direct sum of $\mathrm{Br}\, k$ and $H^1(k, \mathrm{Pic}\, \overline{Z}) = 0$ which implies our first statement. The complement to the 0-dimensional closed set $(\overline{E^{(1)}} \times \overline{E^{(2)}})^\iota$ in $\overline{E^{(1)}} \times \overline{E^{(2)}}$ has no non-constant invertible regular functions. It maps to the complement to the union of all the sixteen lines ℓ_{ij} in $\overline{Z}$, which thus has the same property. Therefore, the larger open set $\overline{W}$ has no non-constant invertible regular functions. This implies that the kernel of the surjective map $\mathrm{Pic}\, \overline{Z} \to \mathrm{Pic}\, \overline{W}$ is the subgroup $\mathbf{Z}^9 \subset \mathrm{Pic}\, \overline{Z}$ freely generated by the classes of the nine lines. The abelian group $\mathrm{Pic}\, \overline{W} = \mathrm{Pic}\, \overline{Z}/\mathbf{Z}^9$ is torsion free, as follows, for example, from the well known structure of the Kummer lattice (see [11]). Since the action of Γ on $\mathrm{Pic}\, \overline{Z}$, and hence also on $\mathrm{Pic}\, \overline{W}$, is trivial, we have $H^1(k, \mathrm{Pic}\, \overline{W}) = 0$. We have $H^i(k, H^0(\overline{W}, \mathbf{G}_m)) = H^i(k, \overline{k}^*)$, $i \geq 0$, and this group injects into $H^i(W, \mathbf{G}_m)$ since W has k-points. Now our claim follows from the exact sequence (38) with X replaced by W. □

Lemma 15 *The quaternion algebras*

$$A_{ij} = ((x - c_i^{(1)})(x - c_3^{(1)}), (y - c_j^{(2)})(y - c_3^{(2)})),$$

where $i, j \in \{1, 2\}$, *belong to* $\mathrm{Br}\, W$.

Proof One shows that

$$\mathrm{div}((x - c_i^{(1)})(x - c_3^{(1)})) \equiv \sum_{j=1}^{4} (\ell_{ij} + \ell_{3j}) \bmod 2,$$

and similarly for $\mathrm{div}((y-c_j^{(2)})(y-c_3^{(2)}))$ (see [7], the displayed formula preceding (10)). The function $(y-c_j^{(2)})(y-c_3^{(2)})$ is the product of y^2 and $(1-c_j^{(2)}/y)(1-c_3^{(2)}/y)$, and the latter is regular at $y=\infty$ with value 1. A similar argument works for $(x-c_i^{(1)})(x-c_3^{(1)})$. Hence the algebras A_{ij} are unramified on W. □

Lemma 16 *The images of the A_{ij} in $\mathrm{Br}\,\overline{W}$ generate $(\mathrm{Br}\,\overline{Z})[2]\subset\mathrm{Br}\,\overline{W}$.*

Proof. It is easy to compute the residue of A_{ij} at ℓ_{mn}. It turns out to be represented by an element of k^*, so the corresponding class in $\overline{k}(\ell_{mn})^*/\overline{k}(\ell_{mn})^{*2}$ is trivial. Thus $A_{ij}\in\mathrm{Br}\,\overline{Z}$.

Let $\pi:\overline{Z}\to\mathbf{P}^1_{\overline{k}}$ be the map defined by $(x,y,z)\mapsto x$. The generic fibre $\mathcal{E}$ of π is the quadratic twist of the elliptic curve $E^{(2)}$ over the field $\overline{k}(x)$ by the class of $(x-c_1^{(1)})(x-c_2^{(1)})(x-c_3^{(1)})$ in $\overline{k}(x)^*/\overline{k}(x)^{*2}$, see (41). The inclusion of the generic fibre into $\overline{Z}$ defines a natural restriction map $\mathrm{Br}\,\overline{Z}\to\mathrm{Br}\,\mathcal{E}$. This map is injective by a general theorem of Grothendieck [6].

Every element of $(\mathrm{Br}\,\mathcal{E})[2]$ has the form

$$B_{a(x),b(x)}=(a(x),y-c_1^{(2)})+(b(x),y-c_2^{(2)}),$$

where $a(x)$ and $b(x)$ are square-free polynomials in $\overline{k}[x]$ (see [14], Exercise 2 on p. 91). Assume that $B_{a(x),b(x)}\in\mathrm{Br}\,\overline{Z}$. If $x-e$ for some $e\neq c_i^{(1)}$, $i=1,2,3$, divides $a(x)$, $b(x)$ or both, then the residue of $B_{a(x),b(x)}$ at the elliptic curve $E\subset\overline{Y}$ given by $x=e$ is the class of $y-c_1^{(2)}$, $y-c_2^{(2)}$ or $(y-c_1^{(2)})(y-c_2^{(2)})$ in $\overline{k}(E)^*/\overline{k}(E)^{*2}$. None of these three classes is trivial, and this contradicts the assumption that $B_{a(x),b(x)}$ is unramified on $\overline{Z}$. Therefore every element of $(\mathrm{Br}\,\overline{Z})[2]$ has the form $B_{a(x),b(x)}$ such that the only possible factors of $a(x)$ and $b(x)$ are $x-c_1^{(1)}$, $x-c_2^{(1)}$, $x-c_3^{(1)}$. We note that $\mathrm{Br}\,\overline{k}(x)=\mathrm{Br}\,\overline{k}(y)=0$ by Tsen's theorem, so that the elements of $\mathrm{Br}\,\overline{k}(Z)$ given by $(p(x),q(x))$ with $p(x),q(x)\in\overline{k}(x)^*$ are trivial. Using this fact and equation (41) it is straightforward to write the class of $B_{a(x),b(x)}$ in $\mathrm{Br}\,\overline{k}(Z)$ as a linear combination of the classes of A_{ij}, $i,j\in\{1,2\}$. Now lemma follows from the injectivity of the natural map $\mathrm{Br}\,\overline{Z}\to\mathrm{Br}\,\overline{k}(Z)$. □

Theorem 6 *Let k be a field of characteristic different from 2. Assume that $\sqrt{-1}\in k$, that $c_1^{(1)}-c_2^{(1)},c_1^{(1)}-c_3^{(1)},c_1^{(2)}-c_2^{(2)},c_1^{(2)}-c_3^{(2)}$ generate a subgroup of k^*/k^{*2} isomorphic to $(\mathbf{Z}/2)^4$ and that $E^{(1)}$ and $E^{(2)}$ are not isogenous over $\overline{k}$. Then the 2-primary torsion subgroup of $\mathrm{Br}\,Z$ is contained in $\mathrm{Br}_1 Z=\mathrm{Br}\,k$.*

Proof Suppose that the order of $\beta \in \mathrm{Br}\, Z$ is a power of 2, and the image of β in $\mathrm{Br}\, \overline{Z}$ is non-zero. Replacing β by an appropriate power we can assume that the order of its image in $\mathrm{Br}\, \overline{Z}$ is exactly 2. By Lemma 16 there exists a non-empty subset $S \subset \{(1,1),(1,2),(2,1),(2,2)\}$ such that the linear combination $\sum_{(i,j)\in S} A_{ij}$, which is an element of $\mathrm{Br}\, W$ by Lemma 15, has the same image in $\mathrm{Br}\, \overline{Z} \subset \mathrm{Br}\, \overline{W}$ as β. Considering $\beta - \sum_{(i,j)\in S} A_{ij}$ as an element of $\mathrm{Br}\, W$ we see that its image in $\mathrm{Br}\, \overline{W}$ is trivial, so that $\beta - \sum_{(i,j)\in S} A_{ij} \in \mathrm{Br}_1 W$. By Lemma 14 we can write

$$\beta = \sum_{(i,j)\in S} A_{ij} + \gamma,$$

where $\gamma \in \mathrm{Br}\, k$. Thus $\sum_{(i,j)\in S} A_{ij}$ is unramified everywhere on Z.

Let us now compute the residues of the A_{ij} at some of the lines ℓ_{mn}. We write $c^{(1)}_{ij} = c^{(1)}_i - c^{(1)}_j$, $c^{(2)}_{ij} = c^{(2)}_i - c^{(2)}_j$. Then the residues of A_{11}, A_{12}, A_{21}, A_{22} at ℓ_{11} are the classes of $c^{(1)}_{12}c^{(2)}_{12}$, $c^{(2)}_{12}c^{(2)}_{13}$, $c^{(1)}_{12}c^{(1)}_{13}$, 1 respectively in $k^*/k^{*2} \subset k(\ell_{11})^*/k(\ell_{11})^{*2}$. By the assumption in the theorem the only possibility is that S consists of the one element $(2,2)$. But the residue of A_{22} at ℓ_{12} is the class of $c^{(1)}_{12}c^{(1)}_{13}$, which shows that A_{22} is ramified at ℓ_{12}. This contradiction proves the theorem. □

References

[1] B.J.Birch and H.P.F.Swinnerton-Dyer, Notes on elliptic curves I, J. reine angew. Math. 212(1963), 7-25.

[2] J-L.Colliot-Thélène and A.N.Skorobogatov, Descent on fibrations over $\mathbf{P}^1_k$ revisited, Math. Proc. Camb. Phil. Soc. 128(2000), 383-393.

[3] J-L.Colliot-Thélène, A.N.Skorobogatov and Sir Peter Swinnerton-Dyer, Rational points and zero-cycles on fibred varieties: Schinzel's hypothesis and Salberger's device, J. reine angew. Math. 495(1998), 1-28.

[4] J-L.Colliot-Thélène, A.N.Skorobogatov and Sir Peter Swinnerton-Dyer, Hasse principle for pencils of curves of genus one whose Jacobians have rational 2-division points, Invent. Math. 134(1998), 579-650.

[5] J-L.Colliot-Thélène and Sir Peter Swinnerton-Dyer, Hasse principle and weak approximation for pencils of Severi–Brauer and similar varieties, J. reine angew. Math. 453(1994), 49-112.

[6] A.Grothendieck, Le groupe de Brauer, I, II, III, in *Dix exposés sur la cohomologie des schémas*, Adv. Stud. Pure Math. 3 (North-Holland, Amsterdam, 1968), 46-188.

[7] D.Harari and A.N.Skorobogatov, Non-abelian descent and the arithmetic of Enriques surfaces. Preprint, 2004.

[8] K.Kramer, Arithmetic of elliptic curves upon quadratic extension, Trans. Amer. Math. Soc. 264(1981), 121-135.

[9] Yu.I.Manin, Le groupe de Brauer-Grothendieck en géométrie diophantienne, in *Actes Congrès Int. Math. Nice* I (Gauthier-Villars, 1971), 401-411.

[10] P.Monsky, Generalizing the Birch-Stephens theorem, I, Modular curves, Math. Zeitschrift 221(1996), 415-420.

[11] V.V.Nikulin, Kummer surfaces. Izv. Akad. Nauk SSSR Ser. Mat. 39(1975), 278–293, 471. (Russian) English translation: Math. USSR Izv. 9(1975), 261-275.

[12] J.H.Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Math. 5 (Springer-Verlag, 1994).

[13] A.N.Skorobogatov, Beyond the Manin obstruction, Inv. Math. 135(1999), 399-424.

[14] A.N.Skorobogatov, *Torsors and rational points* (Cambridge University Press, 2001).

[15] Sir Peter Swinnerton-Dyer, Rational points on certain intersections of two quadrics, in *Abelian varieties* (ed. W.Barth, K.Hulek and H.Lange) (de Gruyter, Berlin, 1995), 273-292.

[16] Sir Peter Swinnerton-Dyer, Some applications of Schinzel's hypothesis to diophantine equations, in *Number theory in progress* (ed. K.Győry, H.Iwaniec and J.Urbanowicz) (Berlin, 1999), 503-530.

[17] Sir Peter Swinnerton-Dyer, Arithmetic of Diagonal Quartic Surfaces II, Proc. London Math. Soc. (3)80(2000), 513-544.

[18] Sir Peter Swinnerton-Dyer, The solubility of diagonal cubic surfaces, Ann. Sci. École Norm. Sup. (4)34(2001), 891-912.