ACTA ARITHMETICA
156.2 (2012)

Density of rational points on elliptic surfaces

by

Ronald van Luijk (Leiden)

1. Introduction. Logan, McKinnon, and the author proved the following theorem in [8].

Theorem 1.1. *Let V be a diagonal quartic surface in $\mathbb{P}^3_{\mathbb{Q}}$, given by $ax^4 + by^4 + cz^4 + dw^4 = 0$ for some coefficients $a, b, c, d \in \mathbb{Q}^*$ whose product $abcd$ is a square. If V contains a rational point $P = [x_0 : y_0 : z_0 : w_0]$ with $x_0y_0z_0w_0 \neq 0$ that is not contained in one of the 48 lines on V, then the set $V(\mathbb{Q})$ of rational points on V is Zariski dense in V, as well as dense in the real-analytic topology on $V(\mathbb{R})$.*

The proof relies on the two elliptic fibrations that exist generically on diagonal quartic surfaces whose coefficients have square product. Swinnerton-Dyer [14] then showed that in much higher generality, namely for any K3 surface V over $\mathbb{Q}$ with at least two elliptic fibrations, there exists an explicitly computable Zariski closed subset $Z \subsetneq V$ such that if V contains a rational point outside Z, then $V(\mathbb{Q})$ is Zariski dense in V; he mentions that similar arguments work over any number field. Here, and in the remainder of the present paper, *explicitly computable* means that there is an algorithm that takes as input equations for both the surface V and the two fibrations, and that gives as output equations for the closed subset Z. In that same paper [14], Swinnerton-Dyer produces some nice results about density of $V(\mathbb{Q})$ in the real-analytic and p-adic topologies as well. He also gives a cleaner proof of Theorem 1.1, based on explicit formulas taken from [15].

Inspired by Swinnerton-Dyer's generalization, we similarly generalize another result from [8], namely a version of Theorem 1.1 over number fields that is in some sense uniform over finite extensions. The only topology we deal with is the Zariski topology. The main tools are essentially the same as the ones in [8]. Those were phrased differently from Swinnerton-Dyer's [14] in the sense that where the paper [8] uses an endomorphism $\alpha\colon F \to F$ of

2010 *Mathematics Subject Classification*: 14G05, 14J27.
Key words and phrases: rational points, density, elliptic surfaces, elliptic fibrations.

DOI: 10.4064/aa156-2-6

a genus-one curve F, Swinnerton-Dyer uses instead the associated covering $\chi\colon F \to J(F)$, $P \mapsto (P) - (\alpha(P))$, of the Jacobian $J(F)$ of F, so that $\alpha(P)$ is the translation of P by $-\chi(P)$. In the present paper we will use both of the equivalent points of view. Arguments similar to ours are also used by Bogomolov and Tschinkel [2, 3], and Harris and Tschinkel [6] in the setting of potential density.

2. Setting and main theorems. Let k be a number field and let $\overline{k}$ be an algebraic closure of k. Let V be a smooth projective surface over k. For $i = 1, 2$, let $f_i\colon V \to C_i$ be an elliptic fibration over k to a curve C_i, and let $\mathcal{V}_i$ be the generic fiber of f_i. We do not assume that the fibrations have a section, nor that they be minimal. We *do assume* that the fibrations are different in the sense that no fiber of f_1 is algebraically equivalent to a fiber of f_2; this is equivalent to the irreducible fibers of either one of the fibrations being horizontal curves with respect to the other fibration.

Remark 2.1. Note that surfaces of Kodaira dimension 1 admit a unique elliptic fibration [1, Proposition IX.3], while those of Kodaira dimension 2 do not admit any. This means that our results are constrained to surfaces of Kodaira dimension -1 and 0. For those of Kodaira dimension -1, in particular for rational surfaces, there are also other techniques available for proving density of rational points. Also for abelian varieties, which have Kodaira dimension 0, several advanced techniques exist. This means that the most interesting surfaces to apply our results to are K3 surfaces and Enriques surfaces.

For $i = 1, 2$, let $\alpha_i\colon V \dashrightarrow V$ be a rational map that respects f_i. Then the map α_i is well defined on all smooth fibers of f_i. Let $\alpha_i^\circ\colon \mathcal{V}_i \to \mathcal{V}_i$ be the restriction of α_i to the generic fiber $\mathcal{V}_i$. Let $J(\mathcal{V}_i)$ denote the Jacobian of $\mathcal{V}_i$ and let $\chi_i\colon \mathcal{V}_i \to J(\mathcal{V}_i)$ be the map that sends P to $(P) - (\alpha_i^\circ(P))$. We *assume* that the map χ_i is not constant for $i = 1, 2$. In other words, the restriction α_i° of α_i to the generic fiber $\mathcal{V}_i$ is not merely translation by an element of the Jacobian $J(\mathcal{V}_i)$. This is then automatically also the case for the restriction of α_i to all smooth fibers. Let M_i denote the degree of χ_i. In Remark 2.6 we will see that rational maps such as α_1 and α_2 always exist. Note that for $i = 1, 2$, the map α_i is allowed to be constant on the fibers of f_i, in which case f_i has a section and χ_i is an isomorphism.

Remark 2.2. Whenever we claim that an object associated to V, f_1, f_2, α_1, and α_2 is computable, we assume that these five are all given by polynomial equations. Examples of computable objects are $J(\mathcal{V}_i)$ and χ_i.

Definition 2.3. A *twist* of the quintuple $(V, f_1, f_2, \alpha_1, \alpha_2)$ is a quintuple $(W, g_1, g_2, \beta_1, \beta_2)$, where W is a variety and $\beta_i\colon W \dashrightarrow W$ is a rational map respecting the fibration $g_i\colon W \to D_i$ over a curve D_i for $i = 1, 2$, with all objects defined over k and such that over $\overline{k}$ there are isomorphisms $\psi_i\colon (D_i)_{\overline{k}} \to (C_i)_{\overline{k}}$ and $\varphi\colon W_{\overline{k}} \to V_{\overline{k}}$, making the diagrams

$$\begin{tikzcd}
& W_{\overline{k}} \arrow[rr, "g_i"] \arrow[dd, "\varphi"', "\cong"] & & (D_i)_{\overline{k}} \arrow[dd, "\psi_i"', "\cong"] \\
W_{\overline{k}} \arrow[ur, "\beta_i"] \arrow[rr, "g_i"] \arrow[dd, "\varphi"', "\cong"] & & (D_i)_{\overline{k}} \arrow[ur, equal] \arrow[dd, "\psi_i"', "\cong"] & \\
& V_{\overline{k}} \arrow[rr, "f_i"'] & & (C_i)_{\overline{k}} \\
V_{\overline{k}} \arrow[ur, "\alpha_i"'] \arrow[rr, "f_i"'] & & (C_i)_{\overline{k}} \arrow[ur, equal] &
\end{tikzcd}$$

commutative for $i = 1, 2$.

By abuse of language, when we talk about a twist (W, g_1, g_2) of (V, f_1, f_2), or even a twist W of V, we implicitly assume the existence of rational maps $\beta_1, \beta_2\colon W \dashrightarrow W$, as well as morphisms g_1, g_2 in the latter case, for which $(W, g_1, g_2, \beta_1, \beta_2)$ is a twist of $(V, f_1, f_2, \alpha_1, \alpha_2)$. If we talk about an isomorphism $\varphi\colon W_{\overline{k}} \to V_{\overline{k}}$ corresponding to a twist W of V, then we mean *some* isomorphism φ for which there also exist ψ_1 and ψ_2 as in Definition 2.3. Our first main result is the following.

Theorem 2.4. *For each integer d there exists an explicitly computable closed subset $Z \subsetneq V$ such that for each field extension K of k of degree at most d over $\mathbb{Q}$ and for each twist W of V, with corresponding isomorphism $\varphi\colon W_{\overline{k}} \to V_{\overline{k}}$, the set $W(K)$ is Zariski dense in W as soon as it contains any point outside $\varphi^{-1}(Z)$.*

Theorem 2.4 implies Swinnerton-Dyer's Theorem 1 in [14] mentioned above, and is stronger in the sense that it is uniform over all twists of V as well as over all finite extensions of bounded degree.

For $i = 1, 2$, let the *j-map* $j_i\colon C_i \to \mathbb{P}^1$ be given by $j_i(t) = j(f_i^{-1}(t))$, the j-invariant of the (Jacobian of the) genus-one fiber $f_i^{-1}(t)$. If the map j_i is nonconstant, then we let d_i be its degree, otherwise we set $d_i = \infty$. If the j-maps j_1 and j_2 are both nonconstant, then there is a pseudo-uniform version of Theorem 2.4 over *all* finite extensions of k in the sense that for larger extensions, the closed subset Z only needs to be enlarged by a finite number of points. We will show the existence of a bound for this number that depends only on the field extension K, the degrees d_1 and d_2, and the degrees M_1 and M_2, but our methods do not allow such a bound to be computed explicitly, as it involves the number of K-rational points on certain modular curves (see Definition 3.11). More precisely, our second main result is the following.

Theorem 2.5. *Assume the j-maps j_1 and j_2 are nonconstant. Then there exists an explicitly computable closed subset $Z \subsetneq V$ such that for each finite extension K of k there is an integer n that depends only on K, such that for each twist W of V, with corresponding isomorphism $\varphi\colon W_{\overline{k}} \to V_{\overline{k}}$, the set $W(K)$ is Zariski dense in W as soon as it contains more than $n \cdot \min(d_1M_1, d_2M_2)$ points outside $\varphi^{-1}(Z)$.*

Remark 2.6. Note that by the Theorem of Riemann–Roch [7, Theorem IV.1.3], for any divisor D of degree 1 on a curve X of genus 1, there is a unique point R on X such that the prime divisor (R) is linearly equivalent to D; in other words, $\mathcal{O}_X(R)$ is isomorphic to the line bundle $\mathcal{O}_X(D)$. This can be used to construct examples of rational maps α_1 and α_2 as follows.

Take $i \in \{1, 2\}$ and a line bundle $\mathcal{L}_i$ on V or, more generally, a line bundle $\mathcal{L}_i$ on $V_{\overline{k}}$ whose isomorphism class is defined over k. Let m_i denote the degree of the restriction $(\mathcal{L}_i)_F$ of $\mathcal{L}_i$ to any smooth fiber F of f_i. Define $\alpha_i\colon V \dashrightarrow V$ by $\alpha_i(P) = R$ for the unique point R on the fiber $F = f_i^{-1}(f_i(P))$ of f_i through P for which $\mathcal{O}_F(R)$ is isomorphic to the degree-one bundle $(\mathcal{L}_i)_F \otimes \mathcal{O}_F((1-m_i)P)$. In this case also the Theorem of Riemann–Roch shows that the map α_i is well defined on the smooth fibers of f_i.

The map $\chi_i\colon \mathcal{V}_i \to J(\mathcal{V}_i)$ is in this case induced by the map $\mathcal{V}_i \to \operatorname{Pic}^0\mathcal{V}_i$, $P \mapsto \mathcal{O}_{\mathcal{V}_i}(m_iP) \otimes (\mathcal{L}_i)_{\mathcal{V}_i}^{-1}$, and is the m_i-covering of $J(\mathcal{V}_i)$ corresponding to what Swinnerton-Dyer calls ψ (see [14]). The assumption that the map χ_i not be constant is equivalent to m_i being nonzero. In this example the degree of χ_i equals $M_i = m_i^2$.

In fact, if the endomorphism ring of the generic fiber $\mathcal{V}_i$ is just $\mathbb{Z}$, then all rational maps respecting f_i are of this form. These rational maps are a direct generalization of the maps e_1 and e_2 used in [8], where we had $\mathcal{L}_1 = \mathcal{L}_2 = \mathcal{O}_V(1)$ and $m_1 = m_2 = 4$ (cf. [8, Remark 2.15]). Also on the diagonal quartic surface given by $x^4 + y^4 + z^4 - t^4 = 0$, studied by Elkies [4], where the product of the coefficients is not a square, there exist two elliptic fibrations whose fibers are intersections of two quadrics, so again we could take $\mathcal{L}_1 = \mathcal{L}_2 = \mathcal{O}_V(1)$ and $m_1 = m_2 = 4$.

Suppose the line bundles $\mathcal{L}_1$ and $\mathcal{L}_2$ induce rational maps α_1 and α_2 respectively. Also assume that for $i = 1, 2$ we have fibrations $g_i\colon W \to D_i$ of a variety W to a curve D_i and isomorphisms $\psi_i\colon (D_i)_{\overline{k}} \to (C_i)_{\overline{k}}$ and $\varphi\colon W_{\overline{k}} \to V_{\overline{k}}$, making the front face of the diagram of Definition 2.3 commutative. If for $i = 1, 2$, the isomorphism class of $\varphi^*(\mathcal{L}_i)$ is defined over k, then we can associate a rational map $\beta_i\colon W \dashrightarrow W$ to it to obtain a twist $(W, g_1, g_2, \beta_1, \beta_2)$ of $(V, f_1, f_2, \alpha_1, \alpha_2)$.

Of course there exist abelian surfaces containing only finitely many rational points over some number field. But there is no K3 surface over a number field that is known to contain only a finite, positive number of rational points. It may therefore be the case that Theorem 2.4 is true for K3 surfaces even if we take $Z = \emptyset$ (cf. Remark 2.1). An interesting family of examples in this context is given by the diagonal quartic surfaces of the form $x^4 - y^4 = t(z^4 - w^4)$ for some rational number $t \in \mathbb{Q}$. They contain a trivial point $[1 : 1 : 1 : 1]$, so Theorem 2.4 with $Z = \emptyset$ would imply that the set of rational points is dense. For all t with numerator and denominator at most 100 this has been verified using Theorem 1.1. This leads to the following conjecture.

Conjecture 2.7. *Every number can be written as the ratio of two differences of fourth powers.*

In the next section we will state and prove explicit versions of Theorem 2.4 and 2.5. Those also allow one to easily check whether a given point is contained in the mentioned subset Z.

3. Explicit subsets. The proofs of Theorems 2.4 and 2.5 rely on an explicit version of Merel's Theorem [10, Corollaire], which bounds the torsion subgroup of the Mordell–Weil group of any elliptic curve over a number field. Oesterlé sharpened Merel's original explicit bound on possible prime orders. He showed that if E is an elliptic curve over a number field K of degree d over $\mathbb{Q}$ and the Mordell–Weil group $E(K)$ contains a point of prime order p, then we have $p \leq (1 + 3^{d/2})^2$; Parent [12, Théorème 1.2] shows that if $E(K)$ contains a point of prime power order p^n with p prime, then we have

$$p^n \leq \begin{cases} 65(3^d - 1)(2d)^6 & (p \neq 2, 3), \\ 65(5^d - 1)(2d)^6 & (p = 3), \\ 129(3^d - 1)(3d)^6 & (p = 2). \end{cases} \tag{3.1}$$

This is summarized in the following theorem.

Theorem 3.1 (Merel, Oesterlé, Parent). *The torsion subgroup of an elliptic curve over a number field of degree at most d is isomorphic to a subgroup of $\mathbb{Z}/B\mathbb{Z} \times \mathbb{Z}/B\mathbb{Z}$ with*

$$B = \prod_{p \leq (1+3^{d/2})^2} p^{n_p}, \tag{3.2}$$

where the product ranges over primes p and where p^{n_p} is the largest power of p satisfying (3.1).

Definition 3.2. For $i = 1, 2$ and any positive integer r, we let $T_{i,r}$ denote the closure of the locus of all geometric points $P \in V$ for which the fiber $F = f_i^{-1}(f_i(P))$ is smooth and for which the divisor $(\alpha_i(P)) - (P)$ on F has exact order r in the Jacobian of F.

The map from the smooth fiber F mentioned in Definition 3.2 to its Jacobian, given by $P \mapsto (\alpha_i(P)) - (P)$, is nonconstant by assumption (in fact it is of degree M_i), so the divisor $(\alpha_i(P)) - (P)$ is only of order r for finitely many points P on F, and the set $T_{i,r}$ does not contain F. It follows that $T_{i,r}$ does not contain any irreducible components of fibers of f_i, so it equals the closure of the locus of all geometric points P on the generic fiber $\mathcal{V}_i$ for which the divisor class $\chi_i(P) \in J(\mathcal{V}_i)$ has order r. Hence, $T_{i,r} \subset V$ is the closure of the preimage of the (exact) r-torsion in $J(\mathcal{V}_i)$ under the map $\chi_i \colon \mathcal{V}_i \to J(\mathcal{V}_i)$. This shows that $T_{i,r}$ is computable.

For $i = 1, 2$, we let S_i denote the union of the singular fibers of f_i and for each integer x we set

$$T_i(x) = \bigcup_{1 \le r \le x} T_{i,r}.$$

It is not hard to prove Theorem 2.4 by showing that for any twist W of V with corresponding isomorphism $\varphi \colon W_{\overline{k}} \to V_{\overline{k}}$, and for any finite extension K of k of degree d over $\mathbb{Q}$, with B as in (3.2), the set $W(K)$ is dense in W as soon as it contains a point outside the set $\varphi^{-1}(S_1 \cup S_2 \cup T_1(B) \cup T_2(B))$. We will show in Proposition 3.8 that the same conclusion holds when we replace this set by a much smaller one. This stronger statement, however, requires a little more care to prove. Theorem 1.1 follows from a special case of the stronger version 3.8 and Remark 3.9.

To avoid having to choose a twist W of V in almost every statement of the remainder of this section, we now fix a twist $(W, g_1, g_2, \beta_1, \beta_2)$ of $(V, f_1, f_2, \alpha_1, \alpha_2)$, knowing that everything that will be proved for W, in fact holds for every twist. Let D_1 and D_2 be the base curves of the fibrations g_1 and g_2 respectively. Let $\psi_i \colon (D_i)_{\overline{k}} \to (C_i)_{\overline{k}}$, for $i = 1, 2$, and $\varphi \colon W_{\overline{k}} \to V_{\overline{k}}$ be isomorphisms making the diagrams of Definition 2.3 commute.

Condition 3.3. Let x be an integer and K an extension of k. For $i \in \{1, 2\}$, we say that a point $P \in W(K)$ satisfies $\Xi_i(x)$ if the fiber $F = g_i^{-1}(g_i(P))$ of g_i through P is smooth and the divisor class of $(\beta_i(P)) - (P)$ in the Jacobian of F has finite order exceeding x.

Definition 3.4. Suppose $i \in \{1, 2\}$ and let x be an integer. Then we let $Z_i(x)$ be the union of $T_i(x)$ and the singular points of singular fibers of f_i.

Lemma 3.5. *Suppose $i \in \{1, 2\}$, let K be any field extension of k, and let x be a positive integer. Suppose that $W(K)$ contains a point P outside $\varphi^{-1}(Z_i(x))$ that does not satisfy $\Xi_i(x)$. Let $F = g_i^{-1}(g_i(P))$ be the fiber of g_i through P and $C \subset F$ an irreducible component of F containing P. Then $C(K)$ is infinite.*

Proof. If F is a singular fiber, then P is a smooth point on F, so C is the unique component of F containing P, and therefore C is also defined over K; since the genus of C equals 0 in this case, we find that C is birational over K to $\mathbb{P}^1$, so $C(K)$ is infinite indeed. We may therefore assume that F is smooth, so we have $F = C$. As the fiber F has a K-point, it is isomorphic to its Jacobian $J = J(F)$, so it suffices to show that the divisor $D = (\beta_i(P)) - (P) \in J(K)$ has infinite order. This is a geometric statement, so we assume $(W, g_1, g_2, \beta_1, \beta_2) = (V, f_1, f_2, \alpha_1, \alpha_2)$ without loss of generality. The divisor D does not have order r in $J(K)$ for any integer $r \leq x$ per definition of $Z_i(x)$. It also does not have order r for any $r > x$ because P does not satisfy $\Xi_i(x)$, so we conclude that it has infinite order, which finishes the proof. ∎

An immediate consequence of Lemma 3.5 is the following lemma.

Lemma 3.6. *Suppose $i \in \{1, 2\}$, let K be any field extension of k, and let x be a positive integer. Let $C \subset W$ be an irreducible horizontal curve with respect to g_i that is not contained in $\varphi^{-1}(T_i(x))$ and for which $C(K)$ is infinite. If only finitely many points in $W(K)$ satisfy $\Xi_i(x)$, then $W(K)$ is Zariski dense in W.*

Proof. The curve C intersects $\varphi^{-1}(T_i(x))$ and each fiber of g_i in only finitely many points. Therefore there are infinitely many smooth fibers containing a point in $C(K)$ and only finitely many of these points are contained in $\varphi^{-1}(T_i(x))$. If also only finitely many of these points satisfy $\Xi_i(x)$, then infinitely many smooth fibers remain with a K-rational point that is not contained in $\varphi^{-1}(T_i(x))$ and that does not satisfy $\Xi_i(x)$; since $\varphi^{-1}(T_i(x))$ and $\varphi^{-1}(Z_i(x))$ differ only in singular fibers, Lemma 3.5 implies that there are infinitely many fibers of g_i that contain infinitely many K-rational points, so $W(K)$ is Zariski dense. ∎

Definition 3.7. For any integer x we let $\mathcal{C}(x)$ denote the collection of all irreducible components of fibers of f_1 or f_2 that are contained in $(S_1 \cap S_2) \cup T_1(x) \cup T_2(x)$ and we set

$$Z_0(x) = \bigcup_{C \in \mathcal{C}(x)} C.$$

Note that $T_i(x)$ does not contain any components of fibers of f_i for $i = 1, 2$, so $\mathcal{C}(x)$ consists of irreducible curves that for both fibrations are contained in a singular fiber and of components of any fiber of f_1 that are contained in $T_2(x)$ or vice versa.

Proposition 3.8. *Let K be a finite extension of k of degree at most d over $\mathbb{Q}$ and let B be as in (3.2). If $W(K)$ contains a point outside $\varphi^{-1}(Z)$ for $Z = Z_0(B) \cup (Z_1(B) \cap Z_2(B))$, then $W(K)$ is dense in W.*

Proof. Suppose $P \in W(K)$ is a point outside $\varphi^{-1}(Z)$. Without loss of generality we assume that P is not contained in $\varphi^{-1}(Z_1(B))$. Let $F = g_1^{-1}(g_1(P))$ be the fiber of g_1 through P. Since no elliptic curve over K has a K-point of order larger than B by Theorem 3.1, we conclude from Lemma 3.5 that there is an irreducible component C of F containing P for which $C(K)$ is infinite. From $\varphi(P) \notin Z_0(B)$ we conclude that $\varphi(C)$ is not contained in $\mathcal{C}(B)$, so C is a horizontal curve with respect to g_2 and C is not contained in $\varphi^{-1}(T_2(B))$. Again by Theorem 3.1, no point of $W(K)$ satisfies $\Xi_2(B)$, so by Lemma 3.6, the set $W(K)$ is Zariski dense. ■

Proof of Theorem 2.4. Let B be as in (3.2). Then by Proposition 3.8 we may take $Z = Z_0(B) \cup (Z_1(B) \cap Z_2(B))$. ■

Remark 3.9. Mazur's Theorem (see [9]) gives a much stronger bound for the order of a rational torsion point on an elliptic curve over $\mathbb{Q}$ than Theorem 3.1. It implies that for the case $k = K = \mathbb{Q}$ and $d = 1$, we may replace B by 12 in Proposition 3.8 and the proof of Theorem 2.4.

In the special case of Theorem 1.1, it turns out that the Jacobian $J(\mathcal{V}_i)$ of the generic fiber $\mathcal{V}_i$ contains the full 2-torsion and that the image of the map $\chi_i \colon \mathcal{V}_i \to J(\mathcal{V}_i)$ is contained in $2J(\mathcal{V}_i)$; from the fact that this is then the case for all smooth fibers, one can deduce with Mazur's Theorem that B may in fact be replaced by 4 (see [8, Proposition 2.29]).

Recall that for any positive integer N, the curve $X_1(N)$ parametrizes pairs (E, P), up to isomorphism over the algebraic closure of the ground field, of an elliptic curve E and a point P of order N. The genus of $X_1(N)$ is at least 2 for $N = 13$ and $N \geq 16$ (see [11, p. 109]). Let $\gamma_N \colon X_1(N) \to \mathbb{A}_1(j)$ be the natural map to the j-line, sending (E, P) to $j(E)$.

Lemma 3.10. *Let K be a field of characteristic zero with an element $j_0 \in K$. Let N be a positive integer. Set $\mu(j_0) = 4$ if $j_0 = 1728$, or $\mu(j_0) = 6$ if $j_0 = 0$, or $\mu(j_0) = 2$ otherwise. Let E be an elliptic curve over K with j-invariant j_0. Then the number of points in $E(K)$ of order N is at most*

$$\mu(j_0) \cdot \#(\gamma_N^{-1}(j_0) \cap X_1(N)(K)). \tag{3.3}$$

Proof. Each point $P \in E(K)$ of order N determines a point on $X_1(N)$ corresponding to the pair (E, P), which maps under γ_N to j_0. Two points $P, P' \in E(K)$ determine the same point on $X_1(N)$ if and only if there is an automorphism of E that sends P to P'. As E has only $\mu(j_0)$ automorphisms over $\overline{K}$, there are at most $\mu(j_0)$ points in $E(K)$ that determine a given point on $X_1(N)$. The lemma follows. ■

Definition 3.11. For any number field K of degree d over $\mathbb{Q}$ we set

$$n_K = 2\sum_{N=16}^{B}\big(\#X_1(N)(K) + \#(\gamma_N^{-1}(1728)\cap X_1(N)(K))\\ + 2\#(\gamma_N^{-1}(0)\cap X_1(N)(K))\big),$$

with B as in (3.2).

Note that n_K is well defined for every number field K, as $X_1(N)(K)$ is finite for all $N \geq 16$ by Faltings' Theorem [5]. Note also that n_K equals the sum of (3.3) over all $j_0 \in K$ and all $N \in \{16,\ldots,B\}$.

For $i = 1,2$, let the j-maps $j_i\colon C_i \to \mathbb{P}^1$ and their "degrees" d_i be as in Section 2. In the next statements, we use the convention $\infty\cdot 0 = 0$ and $\infty \cdot m = \infty$ for any positive integer m.

Lemma 3.12. *Suppose $i \in \{1,2\}$ and let K be any field extension of k. Then there are at most $d_iM_in_K$ points in $W(K)$ that satisfy $\Xi_i(15)$.*

Proof. Let d be the degree of K over $\mathbb{Q}$ and let B be as in (3.2). We know $X_1(N)(K)$ is empty for $N > B$ by Theorem 3.1. If $n_K = 0$, then $X_1(N)(K)$ is empty for all $N > 15$, so no point in $W(K)$ satisfies $\Xi_i(15)$ and we are done. Assume $n_K > 0$. If $d_i = \infty$, then we are done, so we also assume $d_i < \infty$. Then the j-map $j_i\colon C_i \to \mathbb{P}^1$ and the induced j-map $j_i' = j_i \circ \psi_i\colon D_i \to \mathbb{P}^1$ are nonconstant of degree d_i. Let Γ denote the set of all points $P \in W(K)$ that satisfy $\Xi_i(15)$. Every point $P \in \Gamma$ lies on the smooth fiber $F = g_i^{-1}(t)$ above some $t \in D_i(K)$, where the divisor class of $(\beta_i(P)) - (P)$ has finite order N in the Jacobian $J(F)$ of F for some $N \geq 16$; by Theorem 3.1 we have $N \leq B$. Summing over all $N \in \{16,\ldots,B\}$, over all $t \in D_i(K)$, and all points Q of $J(g_i^{-1}(t))$ of order N we find

$$\#\Gamma = \sum_{N=16}^{B}\ \sideset{}{'}\sum_{t\in D_i(K)}\ \sum_{\substack{Q\in J(g_i^{-1}(t))\\ \text{order}\,Q=N}} \#\{P \in g_i^{-1}(t) : [(\beta_i(P)) - (P)] = Q\},$$

where the restricted sum is only over those $t \in D_i(K)$ for which $g_i^{-1}(t)$ is smooth. The summand is bounded by the degree of the map $F \to J(F)$, $P \mapsto (P) - (\beta_i(P))$, with $F = g_i^{-1}(t)$, which equals the degree of the analogous map from the generic fiber of g_i to its Jacobian; this generic map is geometrically equivalent to the map $\chi_i\colon \mathcal{V}_i \to J(\mathcal{V}_i)$, so the degree in question is M_i. By Lemma 3.10 the number of terms of the inner sum is bounded by (3.3) with $j_0 = j(g_i^{-1}(t)) = j_i'(t)$. For any $j_0 \in K$ there are at most d_i points $t \in D_i(K)$ with $j_i'(t) = j_0$, so grouping the points $t \in D_i(K)$ according to the j-invariant, we find

$$\#\Gamma \le d_i M_i \sum_{N=16}^{B} \sum_{j_0 \in K} \mu(j_0) \cdot \#(\gamma_N^{-1}(j_0) \cap X_1(N)(K)) = d_i M_i n_K. \ \blacksquare$$

PROPOSITION 3.13. *Suppose the j-maps j_1, j_2 are nonconstant. Let K be a finite extension of k. If $W(K)$ contains more than $n_K \cdot \min(d_1M_1, d_2M_2)$ points outside $\varphi^{-1}(Z)$ for $Z = Z_0(15) \cup Z_1(15) \cup Z_2(15)$, then $W(K)$ is dense in W.*

Proof. We can assume $d_1M_1 \le d_2M_2 < \infty$. Suppose $W(K)$ contains more than $n_K d_1 M_1$ points outside $\varphi^{-1}(Z) \supset \varphi^{-1}(Z_1(15))$. Then by Lemma 3.12 there is such a point P that does not satisfy $\Xi_1(15)$. Lemma 3.5 says that there is an irreducible component C of the fiber of g_1 through P with $P \in C(K)$ for which $C(K)$ is infinite. From $\varphi(P) \notin Z_0(15)$ we conclude $\varphi(C) \notin \mathcal{C}(15)$, so C is a horizontal curve with respect to g_2 and C is not contained in $\varphi^{-1}(T_2(15))$. By Lemma 3.12 only finitely many points in $W(K)$ satisfy $\Xi_2(15)$, so by Lemma 3.6 the set $W(K)$ is dense in W. ■

Proof of Theorem 2.5. By Proposition 3.13 we may take $Z = Z_0(15) \cup Z_1(15) \cup Z_2(15)$. ■

The following proposition shows that we can take the set Z much smaller, as long as we require the existence of more K-rational points outside $\varphi^{-1}(Z)$.

PROPOSITION 3.14. *Let K be a finite extension of k. If $W(K)$ contains more than $n_K(d_1M_1 + d_2M_2)$ points outside $\varphi^{-1}(Z)$ for $Z = Z_0(15) \cup (Z_1(15) \cap Z_2(15))$, then $W(K)$ is dense in W.*

Proof. Suppose $W(K)$ contains more than $n_K(d_1M_1+d_2M_2)$ points outside $\varphi^{-1}(Z)$. Then we have $d_iM_i < \infty$ for $i = 1, 2$, and $W(K)$ contains either more than $d_1M_1n_K$ points outside $Z_0(15) \cup Z_1(15)$ or more than $d_2M_2n_K$ points outside $Z_0(15) \cup Z_2(15)$. Without loss of generality we assume the former holds. Then by Lemma 3.12 there is a point P outside $Z_0(15) \cup Z_1(15)$ that does not satisfy $\Xi_1(15)$. The proof now continues literally as the proof of Proposition 3.13. ■

References

[1] A. Beauville, *Complex Algebraic Surfaces*, London Math. Soc. Lecture Note Ser. 68, Cambridge Univ. Press, Cambridge, 1983.

[2] F. A. Bogomolov and Yu. Tschinkel, *On the density of rational points on elliptic fibrations*, J. Reine Angew. Math. 511 (1999), 87–93.

[3] F. A. Bogomolov and Yu. Tschinkel, *Density of rational points on elliptic $K3$ surfaces*, Asian J. Math. 4 (2000), 351–368.

[4] N. D. Elkies, *On $A^4 + B^4 + C^4 = D^4$*, Math. Comp. 51 (1988), 825–835.

[5] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. 73 (1983), 349–366.

[6] J. Harris and Yu. Tschinkel, *Rational points on quartics*, Duke Math J. 104 (2000), 477–500.

[7] R. Hartshorne, *Algebraic Geometry*, Grad. Texts in Math. 52, Springer, New York, 1977.

[8] A. Logan, D. McKinnon and R. van Luijk, *Density of rational points on diagonal quartic surfaces*, Algebra Number Theory 4 (2010), 1–20.

[9] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. 47 (1977), 33–186.

[10] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. 124 (1996), 437–449.

[11] A. P. Ogg, *Rational points of finite order on elliptic curves*, Invent. Math. 12 (1971), 105–111.

[12] P. Parent, *Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres*, J. Reine Angew. Math. 506 (1999), 85–116.

[13] H. W. Richmond, *On the Diophantine equation $F \equiv ax^4 + by^4 + cz^4 + dw^4 = 0$, the product abcd being a square number*, J. London Math. Soc. 19 (1944), 193–194.

[14] H. P. F. Swinnerton-Dyer, *Density of rational points on certain $K3$ surfaces*, preprint.

[15] H. P. F. Swinnerton-Dyer, *Arithmetic of diagonal quartic surfaces, II*, Proc. London Math. Soc. (3) 80 (2000), 513–544; Corrigenda, ibid. 85 (2002), 564.

Ronald van Luijk
Mathematisch Instituut
Universiteit Leiden
P.O. Box 9512
2300 RA Leiden, The Netherlands
E-mail: rvl@math.leidenuniv.nl

Received on 16.8.2011
and in revised form on 5.8.2012 (6793)