ACTA ARITHMETICA
146.2 (2011)

Cubic points on cubic curves and the Brauer–Manin obstruction on K3 surfaces

by

Ronald van Luijk (Leiden)

1. Introduction. If we want to prove that a variety X defined over the field of rational numbers $\mathbb{Q}$ does not have any rational points, it suffices to show that X has no real points or no p-adic points for some prime number p. For some varieties the converse holds as well. Conics, for instance, have a rational point if and only if they have a real point and a p-adic point for every prime p, i.e., if and only if they have a point locally everywhere. This is phrased by saying that conics satisfy the *Hasse principle*. Selmer's famous example of the plane curve given by

$$3x^3 + 4y^3 + 5z^3 = 0 \tag{1}$$

shows that cubic curves in general do not satisfy the Hasse principle, as this smooth curve has points everywhere locally, but it has no points over $\mathbb{Q}$ (see [15]).

Some varieties with points locally everywhere have no global points because of the so-called Brauer–Manin obstruction to the Hasse principle. This obstruction is based on the Brauer group of the variety. We refer to [20, Section 5.2] for a good description of this obstruction. The main idea is the following. For a smooth, projective, geometrically integral variety X over a number field k, the set $X(\mathbb{A}_k)$ of adelic points on X equals the product $\prod_v X(k_v)$, where v runs over all places of k, and k_v denotes the completion of k at v. This product is nonempty if and only if X has points locally everywhere. Based on class field theory, one associates to each element g in the Brauer group $\mathrm{Br}\, X$ of X a certain subset $X(\mathbb{A}_k)^g$ of $X(\mathbb{A}_k)$ that contains the set $X(k)$ of k-points on X, embedded diagonally in $X(\mathbb{A}_k)$. We say *there is a Brauer–Manin obstruction to the Hasse principle* if $X(\mathbb{A}_k) \neq \emptyset$, but for some subset $B \subset \mathrm{Br}(X)$ we have $\bigcap_{g \in B} X(\mathbb{A}_k)^g = \emptyset$, and thus $X(k) = \emptyset$. Often

2010 *Mathematics Subject Classification*: 11G05, 14J28, 14C22.
Key words and phrases: K3 surfaces, abelian points, cubic curves, Brauer–Manin obstruction.

DOI: 10.4064/aa146-2-3

one focuses on the set $B = \mathrm{Br}_1 X$ of so-called *algebraic elements*, defined as the kernel of the map $\mathrm{Br}\, X \to \mathrm{Br}\, X_{\overline{k}}$, where $\overline{k}$ denotes an algebraic closure of k. These algebraic elements are relatively easy to get our hands on.

For certain classes of varieties the Brauer–Manin obstruction is the only obstruction to the Hasse principle. For a cubic curve C with finite Tate–Shafarevich group, for instance, it is indeed true that if C has points locally everywhere and there is no Brauer–Manin obstruction, then C contains a rational point (see [10], or [20, Thm. 6.2.3]). It is conjectured that the Brauer–Manin obstruction is the only obstruction to the Hasse principle on all curves of genus at least 2 and all smooth, proper, geometrically integral, rationally connected varieties over number fields (see [14] and [5]).

For K3 surfaces, however, it is not at all clear whether the Brauer–Manin obstruction is the only one. Even if in general this is not the case, it could still be true for special K3 surfaces, such as singular K3 surfaces, which are those with maximal Picard number 20. A priori, it could be true that the algebraic part already gives an obstruction, if there is any.

In this paper, a *k-cubic point* is a point defined over some Galois $(\mathbb{Z}/3\mathbb{Z})$-extension of k. Our main theorem states the following.

THEOREM 1.1. *Let k be a number field. Suppose we have a smooth curve $C \subset \mathbb{P}^2_k$ given by $ax^3 + by^3 + cz^3 = 0$ such that*

(i) *the product abc is not a cube in k,*
(ii) *the curve C has points locally everywhere,*
(iii) *the curve C has no k-cubic points.*

Then there exists a quotient of $C \times C$, defined over k, such that its minimal desingularization Y is a singular K3 surface satisfying $Y(\mathbb{A}_k)^{\mathrm{Br}_1 Y} \neq \emptyset$ and $Y(k) = \emptyset$.

In other words, if a certain cubic curve exists, then the Brauer–Manin obstruction coming from the algebraic part of the Brauer group is not the only obstruction to the Hasse principle for singular K3 surfaces, let alone for K3 surfaces in general. The existence of any plane cubic curve satisfying the third condition in Theorem 1.1 is unknown and an interesting object of study by itself. The curve given by equation (1) satisfies the first two conditions of Theorem 1.1. Several people have wondered whether it satisfies the third condition as well. It turns out that this is not the case, as the intersection points of that curve with the lines

$$\begin{aligned} 711x + 172y + 785z &= 0, \\ 657x + 124y + 815z &= 0, \\ 4329x + 3988y + 2495z &= 0 \end{aligned}$$

are all $\mathbb{Q}$-cubic points.

In the following section we will construct the quotient X of the surface $C \times C$ associated to a general plane cubic C that will be used in the proof of Theorem 1.1. We give explicit equations in the case of diagonal cubics and cubics in Weierstrass form and discuss some of the arithmetic properties of X and its desingularization Y. In Section 3 we will go deeper into the geometry in the case that k has characteristic 0 and investigate the Néron–Severi group of Y. In Section 4 we will prove the main theorem. The fact that there is no Brauer–Manin obstruction will follow from the fact that $\mathrm{Br}_1 Y$ is isomorphic to $\mathrm{Br}\, k$, which never yields an obstruction. Some related open problems are stated in the last section.

2. A K3 surface associated to a plane cubic curve. Let k be any field of characteristic not equal to 2 or 3, and C any smooth projective cubic curve in $\mathbb{P}^2_k$. We extend the regular notion of collinearity by saying that any three points P, Q, and R on C are collinear if the divisor $(P)+(Q)+(R)$ is linearly equivalent with a line section of C. By Bézout's theorem we know that for any two points P and Q on C there is a unique third point R on C such that P, Q, and R are collinear. If P equals Q, then R is the "third" intersection point of C with the tangent to C at P. This yields a natural isomorphism

$$C \times C \cong \{(P,Q,R) \in C^3 : P,\ Q, \text{ and } R \text{ are collinear}\} \tag{2}$$

of varieties. Let ρ be the automorphism of $C \times C$ that sends (P,Q) to (Q,R), where P, Q, and R are collinear. Under the identification of (2) this corresponds to sending (P,Q,R) to (Q,R,P). Clearly ρ has order 3. We let X_C denote the quotient $(C \times C)/\rho$, and write $X = X_C$ if C is understood. Let $\pi\colon C \times C \to X$ denote the quotient map. The surface X_C is the quotient mentioned in Theorem 1.1. It is also used in [6], where the number of rational points on X_C is related to random matrix theory.

The fixed points of ρ are exactly the nine points (P,P) where P is a flex of C. Let P be such a flex and let r and s be two copies of a uniformizer at P. Then modulo the square of the maximal ideal at (P,P) in $C \times C$, the automorphism ρ is given by $(r,s) \mapsto (s,t)$ with $t = -r - s$ (cf. [19, p. 115]). The subring of $k[r,s]$ of invariants under the automorphism $(r,s) \mapsto (s,t)$ is generated as k-algebra by $a = -rs - rt - st = r^2 + rs + s^2$, $b = 3rst = -3rs(r+s)$, and $c = r^2s + s^2t + t^2r = r^3 + 3r^2s - s^3$. They satisfy the equation $a^3 = b^2 + bc + c^2$, which locally describes the corresponding singularity on X_C up to higher degree terms, which do not change the type of singularity. We conclude that X_C has nine singular points, all double points. Each is resolved after one blow-up, with two smooth (-2)-curves above it, intersecting each other in one point. Let Y_C denote the blow-up of X_C in its singular points.

Again, we write $Y = Y_C$ if C is understood. As the singular locus of X is defined over k, so is Y.

Definition 2.1. A *K3 surface* over k is a smooth, projective, geometrically integral surface Z over k with trivial canonical sheaf, for which $H^1(Z, \mathcal{O}_Z) = 0$.

Proposition 2.2. *The surface Y is a smooth K3 surface.*

Proof. We have seen that ρ only has isolated fixed points. The corresponding singularities are A_2-singularities, which are rational double points. From the symmetry of the right-hand side of (2), it follows that ρ fixes the unique (up to scaling) nonvanishing regular differential of $C \times C$. By [9, Thm. 2.4], these conditions imply that a relatively minimal model of X is a K3 surface. By [9, Lemma 2.7], this model is isomorphic to the minimal resolution Y of X. ∎

We now discuss some of the arithmetic properties of X and Y.

Lemma 2.3. *The surface X has a k-rational point if and only if Y does.*

Proof. Any k-rational point of Y maps to a k-rational point of X. Conversely, suppose X has a k-rational point P. If P is not a singular point, then the unique point of Y above P is also k-rational. If P is a singular point, then the unique intersection of the two irreducible components in the exceptional divisor above P is a k-rational point on Y. ∎

Corollary 2.4. *If k is a number field and C has points locally everywhere, then so does Y.*

Proof. Let v be any place of k, and k_v the corresponding completion. By assumption, C contains a k_v-rational point P. Then $\pi((P, P))$ is a k_v-rational point on X. Applying Lemma 2.3 to k_v, we find that Y has a k_v-rational point as well, so Y has points locally everywhere. ∎

Lemma 2.5. *The k-rational points of X correspond to triples (P, Q, R), up to cyclic permutation, of collinear points on C that are defined over some Galois $(\mathbb{Z}/3\mathbb{Z})$-extension l of k and permuted by* $\mathrm{Gal}(l/k)$.

Proof. Suppose l is a Galois $(\mathbb{Z}/3\mathbb{Z})$-extension of k and (P, Q, R) a triple of l-rational collinear points, permuted by $\mathrm{Gal}(l/k)$. Then all permutations of (P, Q, R) induced by $\mathrm{Gal}(l/k)$ are even, so the orbit $\{(P, Q), (Q, R), (R, P)\}$ of ρ is Galois invariant and yields a k-rational point of X. Conversely, any k-rational point of X corresponds to a Galois invariant orbit of ρ, say $\{(P, Q), (Q, R), (R, P)\}$. This implies that Galois permutes $\{P, Q, R\}$, but only by even permutations, so P, Q, and R are defined over k or over some Galois $(\mathbb{Z}/3\mathbb{Z})$-extension of k. They are collinear because (P, Q) and (Q, R) are in the same orbit of ρ. ∎

REMARK 2.6. Note that the words "permuted by $\mathrm{Gal}(l/k)$" mean that the points P, Q, and R are either all defined over k, or they are all conjugates.

LEMMA 2.7. *The surface Y has a k-rational point if and only if there exists a Galois $(\mathbb{Z}/3\mathbb{Z})$-extension l of k such that C contains three collinear points defined over l and permuted by* $\mathrm{Gal}(l/k)$.

Proof. This follows immediately from Lemmas 2.3 and 2.5. ∎

COROLLARY 2.8. *If C has no k-cubic points, then Y has no k-rational points.*

Proof. This follows immediately from Lemma 2.7. ∎

Let $J = \mathrm{Jac}\, C$ denote the Jacobian of C. The following proposition is not needed for the proof of the main theorem, but it is an interesting fact, conveyed and proved to the author by Bjorn Poonen.

PROPOSITION 2.9. *Suppose that $J(k)$ is finite and that* 3 *does not divide the order of $J(k)$. Then the converse of Corollary* 2.8 *holds as well.*

Proof. Suppose that C contains a k-cubic point P. If P is k-rational, then $(P, P) \in C \times C$ maps to a k-rational point on X, so Y has a k-rational point by Lemma 2.3. If P is not k-rational then it is defined over a $(\mathbb{Z}/3\mathbb{Z})$-extension l of k and has two conjugates Q and R. Let L denote a line section of C. Then we have $(P)+(Q)+(R)-L \in J(k)$, while by assumption $J(k) = 3J(k)$, so there is an element $D \in J(k)$ such that $(P) + (Q) + (R) - L \sim 3D$. By Riemann–Roch there exist unique points $P', Q', R' \in C(l)$ that are linearly equivalent to $P - D$, $Q - D$, $R - D$ respectively. Then $(P') + (Q') + (R') \sim L$, so P', Q', and R' are collinear. Since $\mathrm{Gal}(l/k)$ fixes D, it permutes P', Q', and R'. By Lemma 2.7 the surface Y has a k-rational point. ∎

REMARK 2.10. The Jacobian of the Selmer curve C given by (1) has trivial Mordell–Weil group over $\mathbb{Q}$. Since C does not have any $\mathbb{Q}$-rational points, by the proofs of Lemmas 2.3, 2.5, and Proposition 2.9 this implies that the Galois conjugates of any $\mathbb{Q}$-cubic point on C are collinear, so it is no surprise that the $\mathbb{Q}$-cubic points mentioned in the introduction come from intersecting C with a line.

We now show how to find explicit equations for X_C. Let $\breve{\mathbb{P}}^2$ denote the dual of $\mathbb{P}^2$ and let $\tau\colon C \times C \to \breve{\mathbb{P}}^2$ be the map that sends (P, Q) to the line through P and Q, and (P, P) to the tangent to C at P. By Bézout's theorem, for a general line L in $\mathbb{P}^2$ we have $\#(L \cap C) = 3$, so there are six ordered pairs $(P, Q) \in C \times C$ that map under τ to L. We conclude that τ is generically 6-to-1. The map τ factors through π, inducing a 2-to-1 map

$\varphi\colon X \to \breve{\mathbb{P}}^2$ that is ramified over the dual $\breve{C}$ of C:

$$C \times C \xrightarrow{\pi} X \xrightarrow{\varphi} \breve{\mathbb{P}}^2, \qquad \tau$$

The dual $\breve{C}$ has nine cusps, corresponding to the nine flexes of C. As a double cover of $\mathbb{P}^2$ ramified over a curve with a cusp yields the same singularity as the A_2-singularities of X_C, we conclude that X_C is not only birational, but in fact isomorphic to a double cover of $\mathbb{P}^2$, ramified over a sextic with nine cusps.

REMARK 2.11. Suppose that an affine piece of C is given by $f(x,y)=0$. Then the function field $k(C\times C)$ of $C\times C$ is the quotient field of the ring

$$k[x_1,y_1,x_2,y_2]/(f(x_1,y_1),f(x_2,y_2)).$$

The line L through the generic points (x_1,y_1) and (x_2,y_2) on C is given by

$$L : y = \frac{y_2-y_1}{x_2-x_1}x + \frac{x_2y_1-x_1y_2}{x_2-x_1}. \tag{3}$$

Let the coordinates of $\breve{\mathbb{P}}^2$ be given by r,s,t, where the point $[r:s:t]$ corresponds to the line in $\mathbb{P}^2$ given by $rx+sy+tz=0$, or in affine coordinates $y=-\left(\frac{r}{s}\right)x-t/s$. Comparing this to equation (3), we find that the inclusion of function fields

$$\tau^* : k(\breve{\mathbb{P}}^2) = k\left(\frac{r}{s},\frac{t}{s}\right) \to k(C\times C)$$

is given by

$$\frac{r}{s} = -\frac{y_2-y_1}{x_2-x_1} \quad \text{and} \quad \frac{t}{s} = -\frac{x_2y_1-x_1y_2}{x_2-x_1}.$$

Let $x_3 \in k(C\times C)$ be the x-coordinate of the third intersection point of the line L and C. Then the element $d=(x_1-x_2)(x_2-x_3)(x_3-x_1)$ is invariant under ρ, so it is contained in the function field $k(X)$ of X, embedded in $k(C\times C)$ by π^*. The element d is not contained in $k(\breve{\mathbb{P}}^2)$, as it is only invariant under even permutations of the x_i. Hence d generates the quadratic extension $k(X)/k(\breve{\mathbb{P}}^2)$. We may therefore identify $k(X)$ with the field $k(r/s,t/s,d)\subset k(C\times C)$.

EXAMPLE 2.12. After applying a linear transformation defined over some finite extension of k, we may assume that one of the nine inflection points of C is equal to $[0:1:0]$ and that the tangent at that point is the line at infinity given by $z=0$. Assume this can be done over k itself. Then the affine part given by $z=1$ is given by a Weierstrass equation and as the characteristic of k is not equal to 2 or 3, we can arrange for C to be given by

$$y^2 = x^3 + Ax + B$$

with $A, B \in k$. With the point $\mathcal{O} = [0 : 1 : 0]$ as origin, C obtains the structure of an elliptic curve. Note that the inflection points of C are exactly the 3-torsion points on the elliptic curve.

To find an explicit model for X_C, we find a relation among $r/s, t/s$, and d. The x-coordinates x_1, x_2, x_3 of the intersection points of C with the generic line L given by $rx + sy + t = 0$ are the solutions to the equation

$$-\left(-\frac{r}{s}x - \frac{t}{s}\right)^2 + x^3 + Ax + B = 0.$$

The square of $d = (x_1 - x_2)(x_2 - x_3)(x_3 - x_1)$ is exactly the discriminant of this polynomial, which is easy to compute. We find that X_C can be given in weighted projective space $\mathbb{P}(1, 1, 1, 3)$ with coordinates r, s, t, u by

$$\begin{aligned} u^2 = {} & 4Br^6 - 4Ar^5t + A^2r^4s^2 + 36Br^3s^2t - 4r^3t^3 - 18ABr^2s^4 \\ & - 30Ar^2s^2t^2 + 24A^2rs^4t - (4A^3 + 27B^2)s^6 + 54Bs^4t^2 - 27s^2t^4, \end{aligned}$$

with $u = s^3d$. This is exactly the same as in [6], with $b = -r/s$ and $a = -t/s$ for their variables a and b. The map $\varphi\colon X \to \breve{\mathbb{P}}^2$ ramifies where the right-hand side of the equation vanishes, which describes the dual $\breve{C}$ of C. We can describe the cusps of $\breve{C}$ very explicitly. The cusp corresponding to $\mathcal{O}$ is $[0 : 0 : 1]$. The slopes dy/dx at the inflection points of C that are not equal to $\mathcal{O}$ are the roots of the polynomial

$$F = u^8 + 18Au^4 + 108Bu^2 - 27A^2.$$

If α is a root of F, then the corresponding inflection point is $(x, y) = \left(\frac{1}{3}\alpha^2, \frac{\alpha^4+3A}{6\alpha}\right)$. The corresponding cusp on $\breve{C}$ is $[r : s : t] = [6\alpha^2 : -6\alpha : 3A - \alpha^4]$. Note that the splitting field of F is exactly $k(C[3])$, the field of definition of all 3-torsion.

Example 2.13. Suppose C is given by

$$ax^3 + by^3 + c = 0.$$

Then as in Example 2.12 we find that in this case $X_C \subset \mathbb{P}(1, 1, 1, 3)$ can be given by

$$3u^2 = 2abc(cr^3s^3 + br^3t^3 + as^3t^3) - b^2c^2r^6 - a^2c^2s^6 - a^2b^2t^6,$$

with $u = \frac{1}{9}a^2s^3d = \frac{1}{9}a^2s^3(x_1 - x_2)(x_2 - x_3)(x_3 - x_1)$. Each of the coordinate axes $x = 0$ and $y = 0$ and the line $z = 0$ at infinity intersect the curve C at three flexes. Each of the corresponding nine cusps on $\breve{C}$ lies on one of the coordinate axes given by $rst = 0$ in $\breve{\mathbb{P}}^2$.

In the next section we will investigate the geometry of Y and find its Picard group $\operatorname{Pic} Y$, at least in the general case that C does not admit complex multiplication. The group $\operatorname{Pic} Y$ is generated by irreducible curves on Y, of which we will now describe some explicitly.

Let Π denote the set of the nine cusps of $\check{C}$. We will freely identify the elements of Π with the flexes on C that they correspond to. A priori one would not expect there to be any conics going through six points of Π, but it turns out there are 12. They are described by Proposition 2.14 below. Fix a point $\mathcal{O} \in \Pi$ to give C the structure of an elliptic curve. Then Π is the group $C[3]$ of 3-torsion and thus Π obtains the structure of an $\mathbb{F}_3$-vector space in which a line is any translate of any 1-dimensional linear subspace. Two different translates of the same subspace are called parallel. The three points on such lines are actually collinear as points on C. The set of these 12 lines in Π is thus in bijection with the set of triples of collinear points in Π, and therefore independent of the choice of $\mathcal{O}$.

PROPOSITION 2.14. *The six points on any two parallel lines in Π lie on a conic whose pull back to X consists of two components.*

Proof. It suffices to prove this in the setting of Example 2.12. Let l and m be two parallel lines in Π. After translation by an element of $\Pi = C[3]$ we may assume that $\mathcal{O}$ is not contained in $l \cup m$. Let P be a point other than $\mathcal{O}$ on the linear subspace that l and m are translates of. By Example 2.12, the point P corresponds to a root α of F, which factors as $F = (u^2 - \alpha^2) f_\alpha$. The point $-P$ corresponds to $-\alpha$ and the points in $l \cup m$ correspond to the roots of f_α. These points all lie on the conic given by

$$27t^2 - 6\alpha^2 rt + (\alpha^4 + 18A)r^2 + (\alpha^6 + 21A\alpha^2 + 81B)s^2 = 0. \tag{4}$$

From Example 2.12 we find that the pull back of this conic to X is given by (4) and

$$\alpha^2 u^2 = (Ar^3 + 9Brs^2 + 3rt^2 - 6As^2 t)^2,$$

which indeed contains two components. ∎

REMARK 2.15. Consider the situation of the proof of Proposition 2.14. Over the field $k(\alpha, \sqrt{-3})$, the polynomial f_α splits as the product of two cubics such that the points of l correspond to the roots of one of the two cubics and the points of m correspond to the roots of the other.

REMARK 2.16. The fact that the conics of Proposition 2.14 have a reducible pull back to X also follows without explicit equations. Set $H = \tau^* L$ for any line $L \subset \check{\mathbb{P}}^2$ that does not go through any of the $P \in \Pi$. For each $P \in \Pi$, let $\Theta_P \in \operatorname{Div} Y$ be the sum of the two (-2)-curves above the singular point on X corresponding to P. As these curves intersect each other once, we find $\Theta_P^2 = -2$, while we also have $H \cdot \Theta_P = 0$ and $H^2 = 2$. Any curve $\Gamma \subset \check{\mathbb{P}}^2$ of degree m that goes through $P \in \Pi$ with multiplicity a_P pulls back to a curve on X whose strict transformation to Y is linearly equivalent to

$$D = mH - \sum_{P \in \Pi} a_P \Theta_P.$$

We have $D^2 = 2m^2 - 2\sum a_P^2$. For a conic Γ through six of the points of Π we get $D^2 = -4$. Let $p_a(D)$ be the arithmetic genus of D. As the canonical divisor K_Y of Y is trivial, we find from the adjunction formula $2p_a(D)-2 = D\cdot(D+K_Y)$ (see [7, Prop. V.1.5]) that $p_a(D) = -1$ is negative, which implies that D is reducible.

We can use the same idea to find (-2)-curves on Y. For instance, the strict transformation on Y of any pull back to X of a line through two points of Π, or of a conic through five points of Π will be such a curve.

3. The geometry of the surface. In this section we investigate some geometric properties of X and Y. As our main theorem only concerns characteristic 0, we will for convenience assume that the ground field k equals $\mathbb{C}$ throughout this section. Several of the results, however, also hold in positive characteristic, which we will point out at times. We start with a quick review of lattices.

A *lattice* is a free $\mathbb{Z}$-module L of finite rank, endowed with a symmetric, bilinear, nondegenerate map $L \times L \to \mathbb{Q}$, $(x, y) \mapsto x \cdot y$, called the *pairing* of the lattice. An *integral lattice* is a lattice with a $\mathbb{Z}$-valued pairing. A lattice L is called *even* if $x \cdot x \in 2\mathbb{Z}$ for every $x \in L$. Every even lattice is integral. If L is a lattice and m a rational number, then $L(m)$ is the lattice obtained from L by scaling its pairing by a factor m. A *sublattice* of a lattice Λ is a submodule L of Λ such that the induced bilinear pairing on L is nondegenerate. The orthogonal complement in Λ of a sublattice L of Λ is

$$L^\perp = \{\lambda \in \Lambda : \lambda \cdot x = 0 \text{ for all } x \in L\}.$$

A sublattice L of Λ is *primitive* if Λ/L is torsion-free. The minimal primitive sublattice of Λ containing a given sublattice L is $(L^\perp)^\perp = (L \otimes \mathbb{Q}) \cap \Lambda$. The *Gram matrix* of a lattice L with respect to a given basis $x = (x_1, \dots, x_n)$ is $I_x = (\langle x_i, x_j\rangle)_{i,j}$. The *discriminant* of L is defined by $\operatorname{disc} L = \det I_x$ for any basis x of L. A *unimodular* lattice is an integral lattice with discriminant ± 1. For any sublattice L of finite index in Λ we have $\operatorname{disc} L = [\Lambda : L]^2 \cdot \operatorname{disc} \Lambda$. The dual lattice of a lattice L is

$$\check{L} = \{x \in L \otimes \mathbb{Q} : x \cdot \lambda \in \mathbb{Z} \text{ for all } \lambda \in L\}.$$

If L is integral, then L is contained in $\check{L}$ with finite index $[\check{L} : L] = |\operatorname{disc} L|$ and the quotient $A_L = \check{L}/L$ is called the *dual-quotient* of L. If L is a primitive sublattice of a unimodular lattice Λ, then the dual-quotients A_L and $A_{L^\perp}$ are isomorphic as groups, and we have $|\operatorname{disc} L| = |\operatorname{disc} L^\perp|$. For more details on these dual-quotients and the discriminant form defined on them, see [12].

If Z is a smooth projective irreducible surface, let $\operatorname{Pic}^0 Z \subset \operatorname{Pic} Z$ denote the group of divisor classes that are algebraically equivalent to 0. The quotient $\operatorname{NS}(Z) = \operatorname{Pic} Z/\operatorname{Pic}^0 Z$ is called the *Néron–Severi group* of Z. The

exponential map $\mathbb{C} \to \mathbb{C}^*$, $z \mapsto \exp(2\pi i z)$, induces a short exact sequence $0 \to \mathbb{Z} \to \mathcal{O}_Z \to \mathcal{O}_Z^* \to 1$ of sheaves on the complex analytic space Z_h associated to Z. The induced long exact sequence includes $H^1(Z_h, \mathcal{O}_Z) \to H^1(Z_h, \mathcal{O}_Z^*) \to H^2(Z_h, \mathbb{Z})$. There is an isomorphism $H^1(Z_h, \mathcal{O}_Z^*) \cong \operatorname{Pic} Z$ and the image of the first map $H^1(Z_h, \mathcal{O}_Z) \to H^1(Z_h, \mathcal{O}_Z^*)$ is exactly $\operatorname{Pic}^0 Z$. We conclude that there is an embedding $\mathrm{NS}(Z) \hookrightarrow H^2(Z_h, \mathbb{Z})$. The intersection pairing induces a pairing on $\mathrm{NS}(Z)$, which coincides with the cup-product on $H^2(Z_h, \mathbb{Z})$. By abuse of notation we will write $H^2(Z, \mathbb{Z}) = H^2(Z_h, \mathbb{Z})$. See [7, App. B.5] for statements, and [17] and [2, §IV.2] for more details.

Proposition 3.1. *If Z is a K3 surface, then* $\operatorname{Pic}^0 Z = 0$ *and we have an isomorphism* $\operatorname{Pic} Z \cong \mathrm{NS}(Z)$.

Proof. By definition we have $H^1(Z, \mathcal{O}_Z) = 0$, so from the above we find $\operatorname{Pic}^0 Z = 0$. The isomorphism follows immediately. ∎

Note that by fixing a point on C, the surface $C \times C$ obtains the structure of an abelian surface.

Proposition 3.2. *Let Z be an abelian surface (resp. K3 surface). Then $H^2(Z, \mathbb{Z})$ is an even lattice with discriminant -1 of rank* 6 *(resp.* 22*) in which* $\mathrm{NS}(Z)$ *embeds as a primitive sublattice.*

Proof. The lattice $H^2(Z, \mathbb{Z})$ is even by [2, Lemma VIII.3.1]. If Z is an abelian surface, then this lattice is unimodular by [2, §V.3], and indefinite by the Hodge index theorem (see [7, Thm. V.1.9]. From the classification of even indefinite unimodular lattices we find that $H^2(Z, \mathbb{Z})$ is isomorphic to U^3, where U is the hyperbolic lattice with discriminant -1 (see [16, Thm. V.5]). A similar argument holds for K3 surfaces (see [2, Prop. VIII.3.3 (VIII.3.2 in first edition)]). This implies that in both cases the map $H^2(Z, \mathbb{Z}) \to H^2(Z, \mathbb{C})$ is injective, so $\mathrm{NS}(Z)$ is the image of $\operatorname{Pic} Z$ in $H^2(Z, \mathbb{C})$. By [2, Thm. IV.2.13 (IV.2.12 in first edition)], this image is the intersection of $H^2(X, \mathbb{Z})$ with the $\mathbb{C}$-vector space $H^{1,1}(X, \Omega_X)$ inside $H^2(X, \mathbb{C})$. This implies the last part of the claim. ∎

Remark 3.3. From Propositions 3.1 and 3.2 it follows that linear, algebraic, and numerical equivalence all coincide on a complex K3 surface. In positive characteristic this is the case as well (see [4, Thm. 5]).

Lemma 3.4. *Let Z be an abelian variety or a K3 surface. Let D be a curve on Z with arithmetic genus $p_a(D)$. Then $D^2 = 2p_a(D) - 2$.*

Proof. The canonical divisor K_Z is trivial for both abelian varieties and K3 surfaces. The adjunction formula therefore implies that $2p_a(D) - 2 = D \cdot (D + K_Z) = D^2$ (see [7, Prop. V.1.5]). ∎

LEMMA 3.5. *Take any point $R \in C$ and define the divisors*

$$D_1 = \{(P,Q) : P, Q, R \text{ collinear}\}, \quad D_2 = C \times \{R\}, \quad D_3 = \{R\} \times C$$

on $C \times C$. The automorphism ρ acts on the D_i as the permutation $(D_1\ D_2\ D_3)$. The images in $\mathrm{NS}(C \times C)$ of the D_i are independent of the choice of R. We have $D_i \cdot D_j = 1$ if $i \neq j$, and $D_i^2 = 0$. The elements D_1, D_2, D_3 are numerically independent.

Proof. The first statement is obvious. All fibers of the projection of $C \times C$ onto the second copy of C are algebraically equivalent to each other, so the image of D_2 in $\mathrm{NS}(C \times C)$ is independent of R. As D_1 and D_3 are in the orbit of D_2 under ρ, their images are independent of R as well. The divisors D_2 and D_3 intersect each other transversally in one point, so $D_2 \cdot D_3 = 1$. As D_2 is isomorphic to C, the genus $p_a(D_2)$ of D_2 equals 1, so Lemma 3.4 gives $D_2^2 = 0$. The other intersection numbers follow by applying ρ. The last statement follows immediately. ∎

For any $R \in C$ the three divisors D_i of Lemma 3.5 all map birationally to the same curve on X_C, namely the pull back $\varphi^*(\breve{R})$ of the dual $\breve{R}$ of R, i.e., the line in $\breve{\mathbb{P}}^2$ consisting of all lines in $\mathbb{P}^2$ going through R.

For each $P \in \Pi$, let $L_P \subset \mathrm{NS}(Y)$ be the lattice generated by the two (-2)-curves above the singularity on X corresponding to P. Then the lattice L generated by all these (-2)-curves is isomorphic to the orthogonal direct sum $\bigoplus_{P \in \Pi} L_P$. For each $P \in \Pi$, the dual-quotient A_{L_P} is a 1-dimensional $\mathbb{F}_3$-vector space. Let $\Lambda = (L^\perp)^\perp$ be the minimal primitive sublattice of $\mathrm{NS}(Y)$ that contains L. Then Λ is contained in the dual $\breve{L}$ of L, so Λ/L is a subspace of the dual-quotient $A_L \cong \bigoplus_{P \in \Pi} A_{L_P}$.

LEMMA 3.6. *We can identify each A_{L_P} with $\mathbb{F}_3$ and give Π the structure of an $\mathbb{F}_3$-vector space in such a way that*

$$\Lambda/L \subset \bigoplus_{P \in \Pi} A_{L_P} \cong \mathbb{F}_3^{\Pi}$$

consists of all affine linear functions $\Pi \to \mathbb{F}_3$.

Proof. See [3, Thm. 2.5]. The subspace Λ/L corresponds to L_3 as defined on page 269 of [3]. ∎

COROLLARY 3.7. *We have $[\Lambda : L] = 27$ and $\operatorname{disc} \Lambda = 27$.*

Proof. The first equality follows from Lemma 3.6 and the fact that there are 27 affine linear functions $\mathbb{F}_3^2 \to \mathbb{F}_3$. The second equality then follows from the equation $[\Lambda : L]^2 \cdot \operatorname{disc} \Lambda = \operatorname{disc} L = 3^9$. ∎

REMARK 3.8. Fix a point $\mathcal{O} \in \Pi$. Then C obtains the structure of an elliptic curve and Π corresponds to the group $C[3]$ of 3-torsion elements, which naturally has the structure of an $\mathbb{F}_3$-vector space. The 24 nonconstant

affine linear functions $\Pi \to \mathbb{F}_3$ correspond to the irreducible components of the 12 pull backs of the conics of Proposition 2.14.

Let $T_{C\times C}$ and T_Y denote the orthogonal complements of $\mathrm{NS}(C\times C)$ and $\mathrm{NS}(Y)$ in $H^2(C\times C,\mathbb{Z})$ and $H^2(Y,\mathbb{Z})$ respectively. The main result of this section is the following.

PROPOSITION 3.9. *There is a natural isomorphism $T_Y \cong T_{C\times C}(3)$ of lattices.*

Proof. For convenience write $H^\rho_{C\times C} = H^2(C\times C,\mathbb{Z})^{\langle\rho\rangle}$. From Katsura's table in [9, p. 17], we find $\operatorname{rk} H^\rho_{C\times C} = 4$ and the remaining eigenvalues of ρ^* acting on $H^2(C\times C,\mathbb{Z})$ are ζ and ζ^2, where ζ is a primitive cube root of unity. Let $\Gamma' \subset \mathrm{NS}(C\times C)$ denote the sublattice generated by the D_i of Proposition 3.5, and set $D = D_1 + D_2 + D_3$. By Proposition 3.5, D is fixed by ρ. As ρ^* acts unitarily on $H^2(C\times C,\mathbb{C})$, its eigenspaces corresponding to different eigenvalues are orthogonal. We conclude from Proposition 3.5 that the orthogonal complement Γ of $\langle D\rangle$ inside Γ' corresponds to the eigenvalues ζ and ζ^2, which in turn implies $H^\rho_{C\times C} = \Gamma^\perp$ inside the unimodular lattice $H^2(C\times C,\mathbb{Z})$, because $H^\rho_{C\times C}$ corresponds to the eigenvalue 1. The lattice Γ is generated by $D_1 - D_2$ and $D_2 - D_3$ and has discriminant 3, so it is primitive and we also have $|\operatorname{disc} H^\rho_{C\times C}| = |\operatorname{disc}\Gamma| = 3$. Set $N = \Gamma'^\perp$. Taking orthogonal complements in $\Gamma \subset \Gamma' \subset \mathrm{NS}(C\times C)$ we find $T_{C\times C} \subset N \subset H^\rho_{C\times C}$. From the fact that $(\Gamma'/\Gamma)\otimes\mathbb{Q}$ is generated by D, it follows that N is the orthogonal complement of D inside $H^\rho_{C\times C}$.

Let H_X denote the orthogonal complement of L (or Λ) in the unimodular lattice $H^2(Y,\mathbb{Z})$, so that by Corollary 3.7 we have $|\operatorname{disc} H_X| = |\operatorname{disc}\Lambda| = 27$. Recall that π denotes the quotient map $C\times C \to X_C$. There are maps $\pi^*\colon H_X \to H^\rho_{C\times C}$ and $\pi_*\colon H^\rho_{C\times C} \to H_X$ such that π^* and π_* send transcendental cycles to transcendental cycles and

$$\begin{aligned}
&\text{(i)} && \pi^*(x)\cdot\pi^*(y) = 3x\cdot y, && \forall x,y \in H_X,\\
&\text{(ii)} && \pi_*(x)\cdot\pi_*(y) = 3x\cdot y, && \forall x,y \in H^\rho_{C\times C},\\
&\text{(iii)} && \pi_*(\pi^*(x)) = 3x, && \forall x \in H_X,\\
&\text{(iv)} && \pi^*(\pi_*(x)) = 3x, && \forall x \in H^\rho_{C\times C};
\end{aligned}$$

see [8, §1] and [3, p. 273]. From (iv) and the fact that $H^2(C\times C,\mathbb{Z})$ is torsion-free, we find that π_* is injective. Therefore, by (ii) we have an isomorphism $\pi_*(H^\rho_{C\times C}) \cong H^\rho_{C\times C}(3)$ and

$$|\operatorname{disc}\pi_*(H^\rho_{C\times C})| = |\operatorname{disc} H^\rho_{C\times C}(3)| = 3^{\operatorname{rk} H^\rho_{C\times C}}\cdot|\operatorname{disc} H^\rho_{C\times C}| = 3^5.$$

From

$$[H_X : \pi_*(H^\rho_{C\times C})]^2\cdot|\operatorname{disc} H_X| = |\operatorname{disc}\pi_*(H^\rho_{C\times C})|,$$

we then find $[H_X : \pi_*(H^\rho_{C\times C})] = 3$.

Recall that $\pi_*(D_1) = \pi_*(D_2) = \pi_*(D_3) = H$, where H denotes the class of the strict transformation of the pull back of a line in $\breve{\mathbb{P}}^2$ to X. Therefore, $\pi_*(D) = 3H$. From $9 \nmid 6 = D^2$ we conclude $D \notin 3H^\rho_{C\times C}$, and thus $3H = \pi_*(D) \notin 3\pi_*(H^\rho_{C\times C})$, which implies $H \in H_X \setminus \pi_*(H^\rho_{C\times C})$. As the index $[H_X : \pi_*(H^\rho_{C\times C})] = 3$ is prime, it follows that $H_X/\pi_*(H^\rho_{C\times C})$ is generated by H, so the orthogonal complement $\pi_*(N)$ of $3H = \pi_*(D)$ in $\pi_*(H^\rho_{C\times C})$ is primitive in H_X. From the primitive inclusion $\pi_*(T_{C\times C}) \subset \pi_*(N)$ it follows that also $\pi_*(T_{C\times C})$ is primitive in H_X, and thus in $H^2(Y,\mathbb{Z})$.

From $L \subset \mathrm{NS}(Y)$ we find $T_Y \subset H_X$. From (i)–(iv) and the fact that π_* and π^* send transcendental elements to transcendental elements, we find $3T_Y \subset \pi_*(T_{C\times C}) \subset T_Y$. This implies $\operatorname{rk} T_Y = \operatorname{rk} T_{C\times C}$ and together with the fact that $\pi_*(T_{C\times C})$ is primitive in $H^2(Y,\mathbb{Z})$, it follows that $T_Y = \pi_*(T_{C\times C}) \cong T_{C\times C}(3)$, where the last isomorphism follows from $\pi_*(H^\rho_{C\times C}) \cong H^\rho_{C\times C}(3)$. ∎

Remark 3.10. Proposition 3.9 is mentioned without proof in [13], where it is claimed that the proof is exactly the same as in the classical Kummer case, where Y is the desingularization of the quotient X of an abelian surface A by an involution ι. Indeed there are many similarities between the proof of the classical case (see for instance [11, Prop. 4.3]) and the one just presented, but there are some essential differences. A first difference is that in the classical case ι acts trivially on $H^2(A,\mathbb{Z})$. There is, however, a much more significant difference. In the classical case the lattice $\pi_*H^2(A,\mathbb{Z})^{\langle\iota\rangle}$ is easily proved to be primitive in the orthogonal complement H_X of the lattice L generated by the 16 exceptional divisors on Y. This immediately implies that π_*T_A is primitive in $H^2(Y,\mathbb{Z})$. As in our case the index $[H_X : \pi_*H^\rho_{C\times C}] = 3$ is not trivial, certainly the classical proof does not directly apply.

As before, let $\operatorname{Jac} C$ denote the Jacobian of C and $\operatorname{End}\operatorname{Jac}(C)$ its endomorphism ring, which is isomorphic to $\mathbb{Z}$ or an order in either an imaginary quadratic field or a quaternion algebra.

Proposition 3.11. *We have* $\operatorname{rk}\mathrm{NS}(C\times C) = 2 + \operatorname{rk}\operatorname{End}\operatorname{Jac} C$.

Proof. Note that for a curve D the group $\operatorname{Pic}^0 D$ is the kernel of the degree map $\operatorname{Pic} D \to \mathbb{Z}$, so that we have an isomorphism $\mathrm{NS}(D) \cong \mathbb{Z}$. The statement then follows from [18, App.] or [1, Thm. 3.11]. ∎

Proposition 3.12. *With* $r = \operatorname{rk}\operatorname{End}\operatorname{Jac} C$ *we have*

$$\operatorname{rk}\mathrm{NS}(Y) = 18 + r \quad \textit{and} \quad \operatorname{disc}\mathrm{NS}(Y) = 3^{4-r}\operatorname{disc}\mathrm{NS}(C\times C).$$

Proof. By Propositions 3.2 and 3.11 we get $\operatorname{rk} T_{C\times C} = 6 - \operatorname{rk}\mathrm{NS}(C\times C) = 4 - r$. From Propositions 3.2 and 3.9 we then conclude

$$\operatorname{rk}\mathrm{NS}(Y) = 22 - \operatorname{rk} T_Y = 22 - \operatorname{rk} T_{C\times C} = 18 + r.$$

From Proposition 3.9 we also get

$$\operatorname{disc} T_Y = \operatorname{disc} T_{C\times C}(3) = 3^{\operatorname{rk} T_{C\times C}} \operatorname{disc} T_{C\times C} = 3^{4-r} \operatorname{disc} T_{C\times C}.$$

From Proposition 3.2 we then find

$$\operatorname{disc} \mathrm{NS}(Y) = -\operatorname{disc} T_Y = -3^{4-r} \operatorname{disc} T_{C\times C} = 3^{4-r} \operatorname{disc} \mathrm{NS}(C\times C). \blacksquare$$

REMARK 3.13. The conclusion $\operatorname{rk}\mathrm{NS}(Y) = 18 + \operatorname{rk}\operatorname{End}\operatorname{Jac} C$ of Proposition 3.12 is much weaker than the statement of Proposition 3.9 as it suffices to work with coefficients in $\mathbb{Q}$ or $\mathbb{C}$ instead of $\mathbb{Z}$ in the cohomology. By working with étale cohomology instead, we can deduce the same equation in positive characteristic. For most of the details, see [9], which only gives $\operatorname{rk}\mathrm{NS}(Y) \geq 19$ ([9, p. 17]).

COROLLARY 3.14. *If C does not admit complex multiplication, then the Néron–Severi lattice $\mathrm{NS}(Y_C)$ has rank 19, discriminant 54, and is generated by the pull back H of a line in $\breve{\mathbb{P}}^2$, the irreducible components above the $P \in \Pi$, and the irreducible components of the pull backs of the conics of Proposition 2.14.*

Proof. If C does not admit complex multiplication, then $\operatorname{End}\operatorname{Jac} C$ has rank $r = 1$ by definition, so by Proposition 3.12 we have $\operatorname{rk}\mathrm{NS}(Y_C) = 19$ and $27 \mid \operatorname{disc}\mathrm{NS}(Y)$. The lattice Λ generated by the irreducible components above the $P \in \Pi$ and the conics of Proposition 2.14 has rank 18 and discriminant 27 by Corollary 3.7 and Remark 3.8. The class H is orthogonal to Λ and satisfies $H^2 = 2$, so $\langle H\rangle \oplus \Lambda$ has discriminant $27 \cdot 2 = 54$ and rank 19, and thus finite index in $\mathrm{NS}(Y)$. From

$$\operatorname{disc}\mathrm{NS}(Y) \cdot [\mathrm{NS}(Y) : \langle H\rangle \oplus \Lambda]^2 = \operatorname{disc}\langle H\rangle \oplus \Lambda = 54,$$

and the fact that $27 \mid \operatorname{disc}\mathrm{NS}(Y)$, we find that the index equals 1, so $\mathrm{NS}(Y) = \langle H\rangle \oplus \Lambda$. $\blacksquare$

4. Diagonal cubics and the proof of the main theorem. Let $C \subset \mathbb{P}^2$ be a diagonal cubic, defined over a number field k, given by $ax^3 + by^3 + cz^3 = 0$. Let $\zeta \in \overline{k}$ denote a primitive cube root of unity. Then $J = \operatorname{Jac} C$ is an elliptic curve of j-invariant 0, with endomorphism ring $\operatorname{End} J \cong \mathbb{Z}[\zeta]$. Consider the automorphism $\zeta_x\colon [x : y : z] \mapsto [\zeta x : y : z]$ of C. The line through a point $P = [x_0 : y_0 : z_0]$ and $\zeta_x P$ is given by $z_0 y - y_0 z = 0$ and also goes through $\zeta_x^2 P$, so the map $\tau\colon C \times C \to \breve{\mathbb{P}}^2$ sends both $(P, \zeta_x P)$ and $(P, \zeta_x^2 P)$ to $[0 : z_0 : -y_0]$. It follows that both curves

$$D_4 = \{(P, \zeta_x P) \in C \times C : P \in C\}, \qquad D_5 = \{(P, \zeta_x^2 P) \in C \times C : P \in C\}$$

map under τ to the line L_r in $\breve{\mathbb{P}}^2$ given by $r = 0$. However, the two curves are both fixed by ρ, so they map to different curves in X_C. Hence, the pull back to X_C of L_r consists of two irreducible components. The same could be concluded from an argument similar to that in Remark 2.16. The line L_r

goes through three cusps of $\breve{C}$ (see Example 2.13), so the strict transform D on Y_C of the pull back to X_C of L_r is linearly equivalent to $H-\sum_{P\in\Pi\cap L_r}\Theta_P$, which implies $D^2=-4<-2$, so D is reducible. Obviously, the same holds for the lines given by $s=0$ and $t=0$.

By Proposition 3.11 we have $\operatorname{rk}\mathrm{NS}(C\times C)=4$. The divisors D_1,D_2,D_3 of Proposition 3.5 and D_4 from above mutually intersect each other exactly once. They are all isomorphic to C, so they have genus 1 and we have $D_i^2=0$ by Lemma 3.4. It follows that the D_i $(1\le i\le 4)$ generate a sublattice V of $\mathrm{NS}(C\times C)$ of rank 4 and discriminant -3. As this discriminant is squarefree, we find $\mathrm{NS}(C\times C)=V$, and thus $\operatorname{disc}\mathrm{NS}(C\times C)=-3$. By Proposition 3.12 we conclude $\operatorname{disc}\mathrm{NS}(Y)=-27$ and $\operatorname{rk}\mathrm{NS}(Y)=20$. We will now describe the Néron–Severi group more concretely.

By Example 2.13, the pull back of the line L_r given by $r=0$ to $X_C\subset\mathbb{P}(1,1,1,3)$ is given by $r=0$ and $-3u^2=a^2(bt^3-cs^3)^2$. We will denote the two components by D_r^ω, where $\omega\in\{\zeta,\zeta^2\}$ is such that $1+2\omega=a(bt^3-cs^3)/u$ on the corresponding component. We have $D_r^\zeta+D_r^{\zeta^2}\sim H-\sum_{P\in\Pi\cap L_r}\Theta_P$ with Θ_P as in Remark 2.16. Similarly, D_s^ω and D_t^ω denote the irreducible components above $s=0$ and $t=0$ with ω such that $1+2\omega$ equals the value along the corresponding component of $b(cr^3-at^3)/u$ and $c(as^3-br^3)/u$ respectively.

Choose elements $\alpha,\beta\in\overline{k}$ such that $\alpha^3=-c/b$ and $\beta^3=-a/c$, and set $\gamma=-\alpha^{-1}\beta^{-1}$, so that $\gamma^3=-b/a$. The flexes of C are given by $[0:\alpha:\zeta^i]$, $[\zeta^i:0:\beta]$, and $[\gamma:\zeta^i:0]$, with $0\le i\le 2$. The corresponding cusps of $\breve{C}$ are $[0:-\zeta^i:\alpha]$, $[\beta:0:-\zeta^i]$, and $[-\zeta^i:\gamma:0]$ respectively. Let $\mathcal{O}$, P, and Q denote the cusps $[0:-1:\alpha]$, $[0:-\zeta:\alpha]$, and $[\beta:0:-1]$ respectively. Identifying the cusps of $\breve{C}$ with the flexes of C, the curve C gets the structure of an elliptic curve with origin $\mathcal{O}$. The following addition table shows what the other cusps correspond to.

	$\mathcal{O}$	Q	$-Q$
$\mathcal{O}$	$[0:-1:\alpha]$	$[\beta:0:-1]$	$[-1:\gamma:0]$
P	$[0:-\zeta:\alpha]$	$[\beta:0:-\zeta]$	$[-\zeta:\gamma:0]$
$-P$	$[0:-\zeta^2:\alpha]$	$[\beta:0:-\zeta^2]$	$[-\zeta^2:\gamma:0]$

The curve in $\breve{\mathbb{P}}^2$ given by

$$r^2+\alpha^2\beta^2s^2+\beta^2t^2+\alpha\beta rs-\beta rt-\alpha\beta^2st=0$$

is one of the conics of Proposition 2.14, going through the points $nQ\pm P$ for any integer n. Its pull back to $X_C\subset\mathbb{P}(1,1,1,3)$ is given by the same equation together with $\alpha^2u=\pm\beta^2c^2rst$, therefore containing two irreducible components that we will denote according to the sign in the equation by $D_{\alpha,\beta}^{\pm}$. By choosing α and β differently, we get nine out of the twelve conics

of Proposition 2.14. The remaining three are the three possible pairs out of the three lines given by $rst = 0$.

Take any $\alpha' \in \{\alpha, \zeta\alpha, \zeta^2\alpha\}$ and consider the affine coordinates $u' = u/s^3$, $r' = r/s$, and $t' = t/s + \alpha'$. By Example 2.13, X_C is locally given by $u'^2 = -3a^2b^2\alpha'^4t'^2 + (\text{higher order terms})$, where the point $R = [0 : -1 : \alpha']$ corresponds to $(0, 0, 0)$. Therefore, the square of the ratio $3ab\alpha'^2t'/u'$ equals -3 on both irreducible components of the exceptional divisor of the blow-up at R. We denote these components by $\Theta^{\omega}_{r,\alpha'}$ or Θ^{ω}_R, with $\omega \in \{\zeta, \zeta^2\}$ such that $1+2\omega = 3ab\alpha'^2t'/u' = 3ab\alpha'^2s^2(t+\alpha' s)/u$ on the corresponding component. Note that $\Theta^{\zeta}_R + \Theta^{\zeta^2}_R = \Theta_R$ (cf. Remark 2.16). Similarly, for $\beta' \in \{\beta, \zeta\beta, \zeta^2\beta\}$ and $R = [\beta' : 0 : -1]$, we denote the irreducible components above R by $\Theta^{\omega}_{s,\beta'}$ or Θ^{ω}_R, with ω such that $1 + 2\omega = 3bc\beta'^2t^2(r + \beta' t)/u$. For $\gamma' \in \{\gamma, \zeta\gamma, \zeta^2\gamma\}$ and $R = [-1 : \gamma' : 0]$, we denote the irreducible components above R by $\Theta^{\omega}_{t,\gamma'}$ or Θ^{ω}_R in such a way that we have $1 + 2\omega = 3ac\gamma'^2r^2(s + \gamma' r)/u$ on the corresponding component.

We will see that the 43 divisors H, Θ^{ω}_R, D^{ω}_v and $D^{\pm}_{\alpha',\beta'}$ generate the Néron–Severi group. Their intersection numbers are easily computed from the above and given by

$$\begin{array}{lll} H^2 = 2, & H \cdot D^{\omega}_v = 1, & D^{+}_{\alpha',\beta'} \cdot D^{-}_{\alpha'',\beta''} = 0, \\ H \cdot \Theta^{\omega}_R = 0, & H \cdot D^{\pm}_{\alpha',\beta'} = 2, & D^{\omega}_v \cdot D^{\pm}_{\alpha',\beta'} = 0, \end{array}$$

$$\Theta^{\omega_1}_{v,\delta} \cdot \Theta^{\omega_2}_{w,\delta'} = \begin{cases} -2 & \text{if } v = w \text{ and } \delta = \delta' \text{ and } \omega_1 = \omega_2, \\ 1 & \text{if } v = w \text{ and } \delta = \delta' \text{ and } \omega_1 \neq \omega_2, \\ 0 & \text{otherwise,} \end{cases}$$

$$D^{\omega_1}_v \cdot D^{\omega_2}_w = \begin{cases} -2 & \text{if } v = w \text{ and } \omega_1 = \omega_2, \\ 1 & \text{if } v \neq w \text{ and } \omega_1 \neq \omega_2, \\ 0 & \text{otherwise,} \end{cases}$$

$$D^{\epsilon}_{\alpha',\beta'} \cdot D^{\epsilon}_{\alpha'',\beta''} = \begin{cases} -2 & \text{if } \alpha'' = \alpha' \text{ and } \beta'' = \beta', \\ 1 & \text{if } \alpha''\alpha'^{-1} = \beta''\beta'^{-1} \neq 1, \\ 0 & \text{otherwise,} \end{cases}$$

$$D^{\omega_1}_v \cdot \Theta^{\omega_2}_{w,\delta} = \begin{cases} 1 & \text{if } v = w \text{ and } \omega_1 = \omega_2, \\ 0 & \text{otherwise,} \end{cases}$$

$$D^{\epsilon}_{\alpha',\beta'} \cdot \Theta^{\omega}_{v,\delta} = \begin{cases} 1 & \text{if } v = r \text{ and } \alpha'/\delta = \omega^{\epsilon}, \\ 1 & \text{if } v = s \text{ and } \beta'/\delta = \omega^{\epsilon}, \\ 1 & \text{if } v = t \text{ and } \gamma'/\delta = \omega^{\epsilon} \ (\gamma' = -(\alpha'\beta')^{-1}), \\ 0 & \text{otherwise} \end{cases}$$

for any $R \in \Pi, v, w \in \{r, s, t\}, \omega \in \{\zeta, \zeta^2\}, \epsilon \in \{+, -\}, \alpha', \alpha'' \in \{\alpha, \zeta\alpha, \zeta^2\alpha\}$, $\beta', \beta'' \in \{\beta, \zeta\beta, \zeta^2\beta\}$, $\delta \in \{\zeta^i\alpha, \zeta^i\beta, \zeta^i\gamma : 0 \le i \le 2\}$ and $\omega^+ = \omega$ and $\omega^- = \omega^{-1}$. The names of all the divisors are chosen to optimize symmetry. In particular, under the identification of the multiplicative group μ_3 with the additive group $\mathbb{F}_3$, and with the $\mathbb{F}_3$-vector space structure on Π coming from the addition on the elliptic curve, the superscripts of the Θ_R^ω correspond exactly to the choices that need to be made in Lemma 3.6. Many of these intersection numbers follow from that lemma, but we preferred this concrete distinction between the Θ_R^ζ and $\Theta_R^{\zeta^2}$, which more easily reveals the intersection numbers with the D_v^ω and where the Galois action on these divisors is given by the action on the superscripts and subscripts.

PROPOSITION 4.1. *The Néron–Severi group of Y has rank* 20 *and discriminant* -27. *It is generated by the Galois-invariant set*

$$\{D_r^\zeta, D_r^{\zeta^2}\} \cup \{\Theta_R^\omega : R \in \Pi, \omega \in \{\zeta, \zeta^2\}\} \cup \{D_{\alpha',\beta'}^+ : \alpha' \in \{\alpha, \zeta\alpha, \zeta^2\alpha\}, \beta' \in \{\beta, \zeta\beta, \zeta^2\beta\}\}.$$

Proof. The 29 given divisors generate a lattice Λ of rank 20 and discriminant -27. As we have already proved that $\operatorname{rk} \mathrm{NS}(Y) = 20$ and $\operatorname{disc} \mathrm{NS}(Y) = -27$, we conclude $\Lambda = \mathrm{NS}(Y)$. ∎

PROPOSITION 4.2. *If abc is not a cube in k, then $H^1(k, \operatorname{Pic} \overline{Y}) = \{1\}$.*

Proof. From Proposition 4.1 we know a Galois-invariant set of generators for $\operatorname{Pic} \overline{Y}$. Let ρ, σ, τ be the automorphisms of $\operatorname{Pic} \overline{Y}$ induced by acting as follows on the superscript and subscripts:

$$\begin{aligned} \rho&\colon (\alpha, \beta, \zeta) \mapsto (\zeta\alpha, \beta, \zeta), \\ \sigma&\colon (\alpha, \beta, \zeta) \mapsto (\alpha, \zeta\beta, \zeta), \\ \tau&\colon (\alpha, \beta, \zeta) \mapsto (\alpha, \beta, \zeta^2). \end{aligned}$$

The automorphisms ρ and σ commute and the group $G = \langle \rho, \sigma, \tau \rangle$ is isomorphic to the semi-direct product $\langle \rho, \sigma \rangle \rtimes \langle \tau \rangle \cong (\mathbb{Z}/3\mathbb{Z})^2 \rtimes \mathbb{Z}/2\mathbb{Z}$, where τ acts on $\langle \rho, \sigma \rangle$ by inversion. The group $\operatorname{Pic} \overline{Y}$ is defined over $k(\zeta, \alpha, \beta)$, so we have $H^1(k, \operatorname{Pic} \overline{Y}) \cong H^1(k(\zeta, \alpha, \beta)/k, \operatorname{Pic} \overline{Y})$. The Galois group $\mathrm{Gal}(k(\zeta, \alpha, \beta)/k)$ injects into G. In for instance MAGMA we can compute $H^1(H, \operatorname{Pic} \overline{Y})$ for every subgroup H of G (see [21]). It turns out that if $H^1(H, \operatorname{Pic} \overline{Y})$ is nontrivial, then H is contained in $\langle \rho\sigma, \tau \rangle$. This implies that if $H^1(k(\zeta, \alpha, \beta)/k, \operatorname{Pic} \overline{Y})$ is nontrivial, then $\mathrm{Gal}(k(\zeta, \alpha, \beta)/k)$ injects into the group $\langle \rho\sigma, \tau \rangle$, so β/α is fixed by the action of Galois and therefore contained in k, so $abc = (c\beta/\alpha)^3$ is a cube in k. ∎

Proof of Theorem 1.1. By Proposition 2.2 the surface Y is a K3 surface. As its Picard number equals 20 by Proposition 4.1, it is in fact a singular K3 surface. By Corollary 2.8 we have $Y(k) = \emptyset$. By Corollary 2.4 the surface Y

has points locally everywhere, so $Y(\mathbb{A}_k) \neq \emptyset$. By the Hochschild–Serre spectral sequence we have an exact sequence $\operatorname{Br} k \to \operatorname{Br}_1 Y \to H^1(k, \operatorname{Pic} \overline{Y})$ (see [20, Cor. 2.3.9]). By Proposition 4.2 we find $\operatorname{Br}_1 Y = \operatorname{im} \operatorname{Br} k$. As $\operatorname{Br} k$ never yields a Brauer–Manin obstruction, we find $Y(\mathbb{A}_k)^{\operatorname{Br}_1 Y} \neq \emptyset$. ∎

Remark 4.3. For some fields k the conditions (ii) and (iii) of Theorem 1.1 imply condition (i). To see this, assume that we have a smooth curve $C \subset \mathbb{P}^2_k$ given by $ax^3 + by^3 + cz^3 = 0$ that satisfies conditions (ii) and (iii) while abc is a cube in the number field k, say $abc = d^3$. For any $\lambda \in k$ we consider $e = \lambda^3 b/a$. Then the linear transformation $[x : y : z] \to [x : \lambda^{-1}y : \lambda^{-2}b^{-1}dz]$ sends C isomorphically to the curve given by $x^3 + ey^3 + e^2z^3$, so without loss of generality we will assume $a = 1$ and $b = e$ and $c = e^2$. By picking λ suitably, we may also assume that e is integral. Let $\mathfrak{p}$ be a place of k. If $3 \nmid v_{\mathfrak{p}}(e)$, then C is not locally solvable at $\mathfrak{p}$ as the three terms of the defining equation have different valuations, so we find $3 \mid v_{\mathfrak{p}}(e)$ for each place $\mathfrak{p}$ of k, which means that the ideal (e) is the cube of some ideal I of the ring $\mathcal{O}_k$ of integers of k. Now assume that the class number of k is not a multiple of 3. Then from the fact that I^3 is principal we find that I itself is principal, so $e = uv^3$ for some $v \in \mathcal{O}_k$ and $u \in \mathcal{O}_k^*$. By rescaling y and z by a factor of v and v^2 respectively, we may assume $v = 1$, so that C is given by $x^3 + uy^3 + u^2z^3 = 0$. This means that C is isomorphic to one in a fixed finite set of curves, depending on k, namely those curves given by $x^3 + wy^3 + w^2z^3 = 0$ where $w \in \mathcal{O}_k^*$ runs over a set of representatives of $\mathcal{O}_k^*/(\mathcal{O}_k^*)^3$. For some fields k, none of these curves satisfy both (ii) and (iii) so that we have a contradiction. For $k = \mathbb{Q}$ for instance, the group $\mathcal{O}_k^*/(\mathcal{O}_k^*)^3$ is trivial and the curve $x^3 + y^3 + z^3 = 0$ does not satisfy (iii) as it contains the point $[0 : -1 : 1]$. For any imaginary quadratic field the same argument holds, except for $k = \mathbb{Q}(\sqrt{-3})$, where $\mathcal{O}_k^*/(\mathcal{O}_k^*)^3$ is generated by a primitive cube root ζ of unity. In that case there is one extra isomorphism class represented by the curve given by $x^3 + \zeta y^3 + \zeta^2 z^3 = 0$, which contains the rational point $[1 : 1 : 1]$. We conclude that if $k = \mathbb{Q}$ or k is an imaginary quadratic field whose class number is not a multiple of 3, then conditions (ii) and (iii) of Theorem 1.1 imply condition (i).

5. Open problems

Question 1. Is there any (not necessarily diagonal) plane cubic curve over a number field k that has points locally everywhere, but no k-cubic points?

Question 2. Is there any diagonal plane cubic curve over a number field k that has points locally everywhere, but no k-cubic points?

QUESTION 3. Is the Brauer–Manin obstruction the only obstruction to the Hasse principle on K3 surfaces?

Acknowledgements. The author would like to thank Hershy Kisilevsky, Michael Stoll, Bjorn Poonen, and Bas Edixhoven for helpful discussions and suggestions. He also thanks Universidad de los Andes, PIMS, University of British Columbia, and Simon Fraser University for their support.

References

[1] P. Argentin, *Sur certaines surfaces de Kummer*, Ph.D. thesis, Université de Genève, 2006.

[2] W. Barth, K. Hulek, C. Peters, and A. Van de Ven, *Compact Complex Surfaces*, 2nd ed., Ergeb. Math. Grenzgeb. 4, Springer, 2004.

[3] J. Bertin, *Réseaux de Kummer et surfaces K3*, Invent. Math. 93 (1988), 267–284.

[4] E. Bombieri and D. Mumford, *Enriques' classification of surfaces in char. p, II*, in: Complex Analysis and Algebraic Geometry—Collection of papers dedicated to K. Kodaira, W. L. Baily and T. Shioda (eds.), Iwanami and Cambridge Univ. Press, 1977, 23–42.

[5] J.-L. Colliot-Thélène, *Points rationnels sur les fibrations*, in: Higher Dimensional Varieties and Rational Points, Budapest, 2001, K. Böröczky et al. (eds.), Bolyai Soc. Colloq. Publ., Springer, 2003, 171–221.

[6] J. Fearnley and H. Kisilevsky, *Vanishing and non-vanishing Dirichlet twists of L-functions of elliptic curves*, Research report, Concordia Univ., 2004.

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

[8] H. Inose, *On certain Kummer surfaces which can be realized as non-singular quartic surfaces in* $\mathbb{P}^3$, J. Fac. Sci. Univ. Tokyo Sect. IA Math. 23 (1976), 545–560.

[9] T. Katsura, *Generalized Kummer surfaces and their unirationality in characteristic p*, ibid. 34 (1987), 1–41.

[10] Yu. I. Manin, *Le groupe de Brauer–Grothendieck en géométrie diophantienne*, in: Actes Congrès Int. Math. Nice, 1970, tome I, Gauthier-Villars, 1971, 401–411.

[11] D. Morrison, *On K3 surfaces with large Picard number*, Invent. Math. 75 (1984), 105–121.

[12] V. Nikulin, *Integral symmetric bilinear forms and some of their applications*, Math. USSR-Izv. 14 (1980), 103–167.

[13] H. Önsiper and S. Sertöz, *Generalized Shioda–Inose structures on K3 surfaces*, Manuscripta Math. 98 (1999), 491–495.

[14] B. Poonen, *Heuristics for the Brauer–Manin obstruction for curves*, Experiment. Math. 15 (2006), 415–420.

[15] E. S. Selmer, *The Diophantine equation* $ax^3 + by^3 + cz^3 = 0$, Acta Math. 85 (1951), 203–362.

[16] J.-P. Serre, *A Course in Arithmetic*, Grad. Texts in Math. 7, Springer, 1973.

[17] —, *Géométrie algébrique et géométrie analytique*, Ann. Inst. Fourier (Grenoble) 6 (1956), 1–42.

[18] T. Shioda, *Algebraic cycles on certain K3 surfaces in characteristic p*, in: Manifolds (Tokyo, 1973), A. Hattori (ed.), Univ. of Tokyo Press, 1975, 357–364.

[19] J. Silverman, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math. 106, Springer, 1986.

[20] A. Skorobogatov, *Torsors and Rational Points*, Cambridge Tracts in Math. 144, Cambridge Univ. Press, 2001.
[21] Electronic file with MAGMA-code to verify some of the computations in this article, available from the author upon request.

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

Received on 8.6.2009
and in revised form on 23.3.2010 (6049)