LMS J. Comput. Math. 17 (Special issue A) (2014) 14–35 © 2014 Authors
doi:10.1112/S1461157014000199

Examples of $K3$ surfaces with real multiplication

Andreas-Stephan Elsenhans and Jörg Jahnel

Abstract

We construct explicit $K3$ surfaces over $\mathbb{Q}$ having real multiplication. Our examples are of geometric Picard rank 16. The standard method for the computation of the Picard rank provably fails for the surfaces constructed.

1. *Introduction*

It is well known that the endomorphism algebra of a general elliptic curve $\mathfrak{X}$ over $\mathbb{C}$ is equal to $\mathbb{Z}$, while for certain exceptional curves the endomorphism algebra is larger. There are only countably many exceptions and these have complex multiplication (CM). That is, $\mathrm{End}(\mathfrak{X}) \otimes_{\mathbb{Z}} \mathbb{Q}$ is an imaginary quadratic number field.

There is a rich theory about CM elliptic curves, cf. [43, Chapter II] or [6, Chapter 3]. We will not go into details, but mention only a few facts that are relevant for what follows. First of all, the construction of CM elliptic curves in an analytic setting is very classical [46, 17. bis 23. Abschnitt]. The situation becomes slightly more complicated, however, when explicit equations are asked for.

For X an elliptic curve over $\mathbb{Q}$, one says that it has complex multiplication if its base extension $\mathfrak{X} := X_{\mathbb{C}}$ has. In this situation, the occurrence of complex multiplication has striking consequences for the arithmetic of X. For example, on all general elliptic curves, the traces of the Frobenii $\mathrm{Frob}_p \in \mathrm{End}(H^1_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_l))$ have the same statistic for $p \to \infty$, while, in the CM case, a different statistic occurs.

To be more precise, for a non-CM elliptic curve, the distribution of the normalized Frobenius traces $\mathrm{Tr}\,\mathrm{Frob}_p/2\sqrt{p}$ for $p < N$ is supposed to converge, in the weak sense, to $(2/\pi)\sqrt{1-t^2}\,dt$ when $N \to \infty$. Under the additional assumption that X has at least one prime of multiplicative reduction, this behaviour has actually been established in 2010 [21, Theorem 4.3]. On the other hand, if X has CM by $\mathbb{Q}(\sqrt{-d})$ then $\mathrm{Tr}\,\mathrm{Frob}_p = 0$ for all primes that are inert in $\mathbb{Q}(\sqrt{-d})$.

Further, there are only nine imaginary quadratic number fields that may occur as the endomorphism field of a CM elliptic curve, defined over $\mathbb{Q}$, namely those of class number one.

The whole theory generalizes to higher dimensions. The most obvious situation is certainly that of an abelian surface. Here, once again, the general case is that the endomorphism algebra is equal to $\mathbb{Z}$.

However, in contrast to the case of elliptic curves, there is more than one way for the endomorphism algebra to be exceptional. For instance, an abelian surface may have real multiplication (RM) [22]. That is, the endomorphism algebra may be an order in a totally real number field $\supsetneq \mathbb{Q}$. Concerning the possible statistics of the Frobenii on an abelian surface over $\mathbb{Q}$, interesting investigations have been undertaken by Fité, Kedlaya, Rotger and Sutherland [17, 27].

Received 27 February 2014; revised 23 May 2014.

2010 Mathematics Subject Classification 14J28 (primary), 14C30, 11G15, 14C22 (secondary).

Contributed to the Algorithmic Number Theory Symposium XI, GyeongJu, Korea, 6–11 August 2014.

https://doi.org/10.1112/S1461157014000199 Published online by Cambridge University Press

The four authors present evidence for the existence of in fact 52 distinct types of abelian surfaces. A theoretical explanation for this is as follows. Associated to every abelian surface X over $\mathbb{Q}$, there is an algebraic group $G \subset \mathrm{End}(H^1_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_l)) \cong \mathrm{GSp}_4(\mathbb{Q}_l)$ such that the image of the natural operation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $H^1_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_l)$ is Zariski dense in G. The reader might compare the theorem of Tankeev and Zarhin (Theorem 4.1), which gives an analogous statement for $K3$ surfaces. Corresponding to G, there is a compact subgroup of USp_4.

On the other hand, up to conjugation, USp_4 has exactly 55 compact subgroups that fulfill a number of necessary conditions [**17**, Definition 3.1]. For 52 of them, an actual abelian surface exists. Among these, however, only 34 may be realized by an abelian surface over $\mathbb{Q}$. The others need larger base fields [**17**, Theorem 4.3]. Furthermore, the idea that the Frobenius elements Frob_p are in fact equidistributed with respect to the Haar measure leads to hypothetical distributions for the normalized Frobenius traces, which seem to agree with experimental observations.

From the point of view of the classification of algebraic surfaces [**2**], abelian surfaces are not the only kind that naturally generalize elliptic curves to dimension two. Another is provided by the so-called $K3$ surfaces. Indeed, elliptic curves may be characterized by the properties that they are of dimension one and have a trivial canonical sheaf. On the other hand, a surface with trivial canonical sheaf is either abelian or $K3$.

In the case of an elliptic curve or abelian surface, the endomorphism field $\mathrm{End}(\mathfrak{X}) \otimes_{\mathbb{Z}} \mathbb{Q}$ is canonically isomorphic to the endomorphism field $\mathrm{End}(H)$ of the associated Hodge structure $H := H^1(\mathfrak{X}, \mathbb{Q})$. This may be just an equivalent reformulation, yet it allows us to carry over the concepts of real and complex multiplication to more general varieties. In the particular situation of a $K3$ surface, the usual convention is to consider the field $\mathrm{End}(T)$ of endomorphisms, in the category of Hodge structures [cf. § 2], of the transcendental part $T \subset H^2(\mathfrak{X}, \mathbb{Q})$ of the second cohomology vector space (Example 2.5(ii)).

Van Geemen's analytic approach. Van Geemen showed that there exists a one-parameter family of $K3$ surfaces of Picard rank 16 that have real multiplication by $\mathbb{Q}(\sqrt{d})$, as soon as d is an odd integer that is a sum of two squares [**19**, Example 3.4].

Van Geemen's approach is analytic and does not lead to explicit equations. He poses the problem to construct explicit examples in [**19**, Paragraph 3.1]. We shall give van Geemen's argument in a slightly more general form in an Appendix. In fact, we will show that his method works for every integer d, being even or odd, that is a sum of two squares. We will also show that the four-dimensional part of the moduli stack of $K3$ surfaces he considered does not contain any surface having real multiplication by $\mathbb{Q}(\sqrt{d})$, when d is not a sum of two squares.

1.1. *The results*

In this note, we will present algorithms to efficiently test a $K3$ surface X over $\mathbb{Q}$ for real multiplication. Our algorithms do not provide a proof, but only strong evidence. Experiments using them delivered two families of $K3$ surfaces of geometric Picard rank 16 and an isolated example.

For infinitely many members $X^{(2,t)}$ of the first family, we will prove (Theorems 5.12 and 6.6) that they have real multiplication by $\mathbb{Q}(\sqrt{2})$. To our knowledge, these are the first explicit examples of $K3$ surfaces for which real multiplication is proven.

The members of the second family $X^{(5,t)}$ are highly likely to have real multiplication by $\mathbb{Q}(\sqrt{5})$, while the isolated example $X^{(13)}$ is strongly suspected to have real multiplication by $\mathbb{Q}(\sqrt{13})$.

Our approach. There is a theoretical algorithm to prove real (or complex) multiplication for a given $K3$ surface under the assumption of the Hodge conjecture; cf. the indications given

https://doi.org/10.1112/S1461157014000199 Published online by Cambridge University Press

in the proof of [4, Theorem 6]. Its main idea is to inspect the Hilbert scheme of $X \times X$; it is far from realistic to do this in practice.

That is why we decided to choose a different, more indirect, approach. We searched for surfaces having real multiplication through their arithmetic consequences. The main idea behind our approach is that real multiplication by $\mathbb{Q}(\sqrt{d})$ implies $\#X_p(\mathbb{F}_p) \equiv 1 \pmod p$, for all primes p that are inert under the field extension $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ (Corollary 4.13(i)). This result is in close analogy with the classical case of a CM elliptic curve and leads to an algorithm that is extremely selective, cf. § 5.

From the surfaces found, we could guess the two families. For the members of the first family, we will give a formal proof that $\#X_p^{(2,t)}(\mathbb{F}_p) \equiv 1 \pmod p$ is true for all primes $p \equiv 3, 5 \pmod 8$, not just for those within the computational range. In order to do this, we analyze in detail one of the elliptic fibrations of the surfaces $X^{(2,t)}$ (Theorem 6.3). The infinitely many congruences $\#X_p^{(2,t)}(\mathbb{F}_p) \equiv 1 \pmod p$ are enough to imply that the endomorphism field $\operatorname{End}(T)$ is strictly larger than $\mathbb{Q}$ (Lemma 6.1). For infinitely many of the surfaces, actually $\operatorname{End}(T) \cong \mathbb{Q}(\sqrt{2})$ (Theorem 6.6).

In the case of the family $X^{(5,t)}$ and for the surface $X^{(13)}$, we do not have a proof for the congruences on the point count. The experimental evidence is, however, overwhelming, cf. Remark 5.14.

1.2. *An application: the analysis of van Luijk's method*

Van Luijk's method is the standard method to determine the geometric Picard rank of a $K3$ surface over $\mathbb{Q}$. Its fundamental idea is that, for every prime p of good reduction, one has $\operatorname{rk}\operatorname{Pic} X_{\overline{\mathbb{Q}}} \leqslant \operatorname{rk}\operatorname{Pic} X_{\overline{\mathbb{F}}_p}$. Further, the method relies on the hope of finding good primes such that

$$\operatorname{rk}\operatorname{Pic} X_{\overline{\mathbb{F}}_p} \leqslant \operatorname{rk}\operatorname{Pic} X_{\overline{\mathbb{Q}}} + 1. \qquad (1)$$

To see the method at work, the reader is advised to consult the original papers of van Luijk [31, 32] or some of the authors' previous articles [11, 13, 14]. Further, there is the remarkable work of Elkies and Kumar [10], in which they compute, among other data, the Néron–Severi ranks of all Hilbert–Blumenthal surfaces corresponding to the real quadratic fields of discriminants up to 100. Several of them are $K3$.

Quite recently, Charles [4] provided a theoretical analysis on the existence of primes fulfilling condition (1). The result is that such primes always exist, unless X has real multiplication by a number field E such that $(22 - \operatorname{rk}\operatorname{Pic} X_{\overline{\mathbb{Q}}})/[E : \mathbb{Q}]$ is odd. Thus, our results provide explicit examples of $K3$ surfaces for which the method is bound to fail in its original form.

Actually, there is a more general version of van Luijk's method that applies to $K3$ surfaces having real multiplication, cf. [4, Proposition 18]. We will make use of this in the proof of Theorem 6.6. It works when the entire endomorphism field $\operatorname{End}(T)$ is known, in particular, when $\operatorname{End}(T) \cong \mathbb{Q}$. Up to now, no practical method has been found that would determine the geometric Picard rank of a $K3$ surface that has real multiplication, but for which this fact is not known.

2. *Hodge structures*

Recall the following definition, cf. [7, Définition 2.1.10 and Proposition 2.1.9].

Definition 2.1. (i) A (pure $\mathbb{Q}$-) *Hodge structure* of weight i is a finite-dimensional $\mathbb{Q}$-vector space V together with a decomposition

$$V_{\mathbb{C}} := V \otimes_{\mathbb{Q}} \mathbb{C} = H^{0,i} \oplus H^{1,i-1} \oplus \ldots \oplus H^{i,0},$$

https://doi.org/10.1112/S1461157014000199 Published online by Cambridge University Press

having the property that $\overline{H^{m,n}} = H^{n,m}$ for every $m, n \in \mathbb{N}_0$ such that $m+n = i$. A *morphism* $f\colon V \to V'$ *of (pure* $\mathbb{Q}$*-) Hodge structures* is a $\mathbb{Q}$-linear map such that $f_\mathbb{C}\colon V_\mathbb{C} \to V'_\mathbb{C}$ respects the decompositions.

(ii) A Hodge structure of weight 2 is said to be *of $K3$ type* if $\dim_\mathbb{C} H^{2,0} = 1$.

Remark 2.2. Hodge structures of weight i form an abelian category [7, 2.1.11]. Further, this category is semisimple. That is, every Hodge structure is a direct sum of primitive ones [7, Définition 2.1.4 and Proposition 2.1.9].

Examples 2.3. (i) Let $\mathfrak{X}$ be a smooth, projective variety over $\mathbb{C}$. Then $H^i(\mathfrak{X}(\mathbb{C}), \mathbb{Q})$ is in a natural way a pure $\mathbb{Q}$-Hodge structure of weight i.

(ii) In $H^2(\mathfrak{X}(\mathbb{C}), \mathbb{Q})$, the image of $c_1\colon \operatorname{Pic}(\mathfrak{X}) \otimes_\mathbb{Z} \mathbb{Q} \to H^2(\mathfrak{X}(\mathbb{C}), \mathbb{Q})$ defines a sub-Hodge structure P such that $H^{0,2}_P = H^{2,0}_P = 0$, which is called the *algebraic part* of $H^2(\mathfrak{X}(\mathbb{C}), \mathbb{Q})$.

Definition 2.4. (i) A *polarization* on a pure $\mathbb{Q}$-Hodge structure V of even weight is a non-degenerate symmetric bilinear form $\langle .\,,.\rangle\colon V \times V \to \mathbb{Q}$ such that its $\mathbb{C}$-bilinear extension $\langle .\,,.\rangle\colon V_\mathbb{C} \times V_\mathbb{C} \to \mathbb{C}$ satisfies the following two conditions.

- One has $\langle x, y\rangle = 0$ for all $x \in H^{m,n}$ and $y \in H^{m',n'}$ such that $m \neq n'$.
- The inequality $i^{m-n}\langle x, \overline{x}\rangle > 0$ is true for every $0 \neq x \in H^{m,n}$.

(ii) A Hodge structure together with a polarization is called a *polarized Hodge structure.*

Examples 2.5. (i) If $\mathfrak{X}$ is a smooth, projective surface then $H := H^2(\mathfrak{X}(\mathbb{C}), \mathbb{Q})$ is a polarized pure Hodge structure, the polarization $\langle .\,,.\rangle\colon H \times H \to \mathbb{Q}$ being given by the cup product, together with Poincaré duality.

(ii) The algebraic part $P \subseteq H$ and its orthogonal complement $T = P^\perp$, which is called the *transcendental part* of H, are polarized Hodge structures, too. If X is a $K3$ surface (§ 3) then H and T are of $K3$ type.

2.6. Zarhin [47, Theorem 1.6(a) and Theorem 1.5.1] proved that, for T a polarized weight-2 Hodge structure of $K3$ type, $E := \operatorname{End}(T)$ is either $\mathbb{Q}$, or a totally real field $\supsetneqq \mathbb{Q}$, or a CM field.

Further, every $\varphi \in E$ operates as a self-adjoint mapping. That is,

$$\langle \varphi(x), y\rangle = \langle x, \overline{\varphi}(y)\rangle,$$

where $^-$ indicates the identity map in the case that E is totally real and the complex conjugation in the case that E is a CM field.

Observe that, in either case, T carries a structure of an E-vector space. If E is totally real then one automatically has $\dim_E T > 1$ [47, Remark 1.5.3(c)].

Definition 2.7. Let T be a polarized weight-2 Hodge structure of $K3$ type. If $\operatorname{End}(T) \supsetneqq \mathbb{Q}$ is a totally real field then T is said to have *real multiplication*. If $\operatorname{End}(T)$ is CM then one speaks of *complex multiplication*.

3. *Some background on $K3$ surfaces*

3.1. By definition, a $K3$ surface is a simply connected, projective algebraic surface with trivial canonical class.

Examples 3.2. Examples include the classical Kummer surfaces, smooth space quartics and double covers of $\mathbf{P}^2$, branched over a smooth sextic curve. As long as the singularities are isolated and rational, the minimal resolutions of singular quartics and double covers of $\mathbf{P}^2$,

https://doi.org/10.1112/S1461157014000199 Published online by Cambridge University Press

branched over a singular sextic, are $K3$ surfaces, too. In this paper, we shall entirely work with the case of a double cover of $\mathbf{P}^2$, branched over a singular sextic.

3.3. The property of being $K3$ determines the Hodge diamond. One has $H^1(\mathfrak{X}, \mathbb{Q}) = 0$, but $H := H^2(\mathfrak{X}, \mathbb{Q})$ is non-trivial. It is a pure weight-2 Hodge structure of dimension 22. Further, $\dim_{\mathbb{C}} H^{2,0}(\mathfrak{X}) = \dim_{\mathbb{C}} H^{0,2}(\mathfrak{X}) = 1$ and $\dim_{\mathbb{C}} H^{1,1}(\mathfrak{X}) = 20$. The Picard group of a complex $K3$ surface is isomorphic to $\mathbb{Z}^n$, where n may range from 1 to 20.

DEFINITION 3.4 (cf. [47, Paragraph 1.1]). (i) Let $\mathfrak{X}$ be a complex $K3$ surface and T be the transcendental part of $H^2(\mathfrak{X}, \mathbb{Q})$. Then $\mathfrak{X}$ is said to have *real* or *complex multiplication* if T has.

(ii) A $K3$ surface X over $\mathbb{Q}$ is said to have *real* or *complex multiplication* if its base extension $X_{\mathbb{C}}$ has.

REMARKS 3.5. (i) The Kummer surface $\mathrm{Kum}(\mathfrak{E}_1 \times \mathfrak{E}_2)$ attached to the product of two elliptic curves $\mathfrak{E}_1$ and $\mathfrak{E}_2$ has complex multiplication if one of the elliptic curves has.

(ii) On the other hand, a Kummer surface does *not* inherit the property of having real multiplication from the underlying abelian surface $\mathfrak{A}$. Indeed, in this case, $\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ operates on $H^{1,0}(\mathfrak{A}, \mathbb{C})$ with eigenvalues $\pm\sqrt{d}$. Consequently, $\mathbb{Q}(\sqrt{d})$ operates on

$$\Lambda^2 H^{1,0}(\mathfrak{A}, \mathbb{C}) = H^{2,0}(\mathfrak{A}, \mathbb{C}) \hookrightarrow H_{\mathbb{C}} := H^2(\mathrm{Kum}\,\mathfrak{A}, \mathbb{C})$$

via multiplication by the norm, and the same is true for the whole $T_{\mathbb{C}} \subset H_{\mathbb{C}}$.

REMARK 3.6. Motivated by the analysis of Charles [4], we are interested in $K3$ surfaces having real multiplication and an odd E-dimensional T. The simplest possible case is that $E = \mathbb{Q}(\sqrt{d})$ is real quadratic and $\dim_E T = 3$, that is $\dim_{\mathbb{Q}} T = 6$.

3.7. *Frobenius eigenvalues.* For varieties over finite fields, there is the l-adic cohomology theory [40]. If Y is a $K3$ surface over $\mathbb{F}_p$ then $\dim H^2_{\text{ét}}(Y_{\overline{\mathbb{F}}_p}, \mathbb{Q}_l) = 22$. This vector space is acted upon by $\langle \mathrm{Frob} \rangle = \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$. The 22 eigenvalues are algebraic integers, independent of the choice of $l \neq p$. They are of absolute value p and l-adic units for every $l \neq p$ [8, Théorème 1.6].

Concerning the p-adic nature of the Frobenius eigenvalues, there is the general result that the Newton polygon always runs above the Hodge polygon [33], cf. [3, Theorem 8.39]. A variety over $\mathbb{F}_p$ is called *ordinary* if the two polygons coincide [25, Définition IV.4.12], cf. [23, 48–49].

In the particular case of a $K3$ surface, ordinarity is equivalent to the situation that the Frobenius eigenvalues are of p-adic valuations $0, 1, \ldots, 1, 2$. On the other hand, non-ordinarity implies that no Frobenius eigenvalue is a p-adic unit, cf. [30, Paragraph 3.6]. Therefore, according to the Lefschetz trace formula [40, Exposé XII, 6.3 and Exemple 7.3], a $K3$ surface Y over $\mathbb{F}_p$ is ordinary if and only if $\#Y(\mathbb{F}_p) \not\equiv 1 \pmod{p}$.

4. *Some arithmetic consequences of real multiplication*

Let X be a $K3$ surface over $\mathbb{Q}$. As above, we put

$$P := \mathrm{im}(c_1\colon\ \mathrm{Pic}(X_{\mathbb{C}}) \otimes_{\mathbb{Z}} \mathbb{Q} \hookrightarrow H^2(X(\mathbb{C}), \mathbb{Q})),$$

$T := P^{\perp}$, and write E for the endomorphism algebra of the Hodge structure T.

https://doi.org/10.1112/S1461157014000199 Published online by Cambridge University Press

Further, let us choose a prime number l and turn to l-adic cohomology. This essentially means to tensor with $\mathbb{Q}_l$, as there is the canonical comparison isomorphism [39, Exposé XI, Théorème 4.4(iii)]

$$H^2(X(\mathbb{C}),\mathbb{Q})\otimes_{\mathbb{Q}}\mathbb{Q}_l \xleftarrow{\cong} H^2_{\text{ét}}(X_{\overline{\mathbb{Q}}},\mathbb{Q}_l).$$

An important feature of the l-adic cohomology theory is that it is acted upon by the absolute Galois group of the base field. That is, there is a continuous representation

$$\varrho_l\colon\ \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}(H^2_{\text{ét}}(X_{\overline{\mathbb{Q}}},\mathbb{Q}_l)).$$

The image of ϱ_l is an l-adic Lie group. Its Zariski closure is an algebraic group G_l, called the algebraic monodromy group associated to ϱ_l.

On the other hand, there are the image $P_l \subseteq H^2_{\text{ét}}(X_{\overline{\mathbb{Q}}},\mathbb{Q}_l)$ of $\mathrm{Pic}(X_{\overline{\mathbb{Q}}})\otimes_{\mathbb{Z}}\mathbb{Q}_l$ under the Chern map to l-adic cohomology and its orthogonal complement T_l. These are compatible with the analogous constructions in Betti cohomology in the sense that P_l and T_l are mapped onto $P\otimes_{\mathbb{Q}}\mathbb{Q}_l$ and $T\otimes_{\mathbb{Q}}\mathbb{Q}_l$, respectively, under the canonical comparison isomorphism.

The image of ϱ_l, and hence the whole of G_l, consists of endomorphisms of $H^2_{\text{ét}}(X_{\overline{\mathbb{Q}}},\mathbb{Q}_l)$ mapping P_l to P_l. Further, these preserve orthogonality with respect to the pairing $\langle\,.\,,.\,\rangle$. Thus, the algebraic monodromy group G_l must map T_l into itself, as well.

THEOREM 4.1 (Tankeev, Zarhin). *The neutral component G_l° of the algebraic monodromy group with respect to the Zariski topology is equal to the centralizer of E in* $\mathrm{GO}(T_l,\langle\,.\,,.\,\rangle)$. *In particular, the operation of E on $T_l \subset H^2_{\text{ét}}(X_{\overline{\mathbb{Q}}},\mathbb{Q}_l)$ commutes with that of G_l°.*

Proof. This follows from the Mumford–Tate conjecture, proven by Tankeev [44, 45], together with Zarhin's explicit description of the Mumford–Tate group in the case of a $K3$ surface [47, Theorem 2.2.1]. We refer the reader to the original articles and to the discussion in [4, § 2.2]. □

For every prime p, choose an absolute Frobenius element $\mathrm{Frob}_p \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. If $p \neq l$ is a prime at which X has good reduction then, by virtue of the smooth base change theorem [39, Experiment XVI, Corollaire 2.5], there is a canonical isomorphism

$$H^2_{\text{ét}}(X_{\overline{\mathbb{Q}}},\mathbb{Q}_l) \cong H^2_{\text{ét}}((X_p)_{\overline{\mathbb{F}}_p},\mathbb{Q}_l).$$

Here, the vector space on the right-hand side is naturally acted upon by $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ and the operation of $\mathrm{Frob}_p \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the left-hand side is compatible with that of $\mathrm{Frob} \in \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ on the right.

COROLLARY 4.2. *There is a positive integer f such that, for every pair (p,l) of prime numbers, the operation of* $(\mathrm{Frob}_p)^f$ *on T_l commutes with that of E.*

Proof. By definition, $\varrho_l(\mathrm{Frob}_p) \in G_l$. Hence, for $f := \#(G_l/G_l^\circ)$, we have $\varrho_l((\mathrm{Frob}_p)^f) \in G_l^\circ$. Further, the groups G_l/G_l° are canonically isomorphic to each other, for the various values of l, as was proven by Larsen and Pink [28, Proposition 6.14]. □

NOTATION 4.3. (i) For every prime p, choose $l \neq p$ and denote by $\chi^T_{p^n}$ the characteristic polynomial of $(\mathrm{Frob}_p)^n$ on the transcendental part T_l. This has coefficients in $\mathbb{Q}$ and is independent of l, whether X has good reduction at p [8, Théorème 1.6] or not [36, Theorem 3.1]. One has $\deg \chi^T_{p^n} = 22 - \mathrm{rk}\,\mathrm{Pic}\,X_{\overline{\mathbb{Q}}}$.

https://doi.org/10.1112/S1461157014000199 Published online by Cambridge University Press

(ii) We factorize $\chi^T_{p^n} \in \mathbb{Q}[Z]$ in the form

$$\chi^T_{p^n}(Z) = \chi^{\mathrm{tr}}_{p^n}(Z) \cdot \prod_{k,i} (Z - \zeta^i_k)^{e_{k,i}},$$

for $\zeta_k := \exp(2\pi i/k)$, $e_{k,i} \geqslant 0$, and such that $\chi^{\mathrm{tr}}_{p^n} \in \mathbb{Q}[Z]$ does not have any roots of the form p^n times a root of unity.

Remark 4.4. If p is a good prime then, according to the Tate conjecture, $\chi^{\mathrm{tr}}_{p^n}$ is the characteristic polynomial of Frob^n on the transcendental part of $H^2_{\text{ét}}(X_{\overline{\mathbb{F}}_p}, \mathbb{Q}_l)$. In particular, $\deg \chi^{\mathrm{tr}}_{p^n} = 22 - \operatorname{rk} \operatorname{Pic} X_{\overline{\mathbb{F}}_p}$. Further, $\chi^{\mathrm{tr}}_{p^n} = \chi^T_{p^n}$ if and only if $\operatorname{rk} \operatorname{Pic} X_{\overline{\mathbb{F}}_p} = \operatorname{rk} \operatorname{Pic} X_{\overline{\mathbb{Q}}}$.

For the remainder of this section, we assume that $E \supseteq \mathbb{Q}(\sqrt{d})$, for $d \neq 1$ a square-free integer. That is, that X has real or complex multiplication by a number field E that contains $\mathbb{Q}(\sqrt{d})$. Further, we shall use the symbol f for an arbitrary positive integer such that the operation of $(\mathrm{Frob}_p)^f$ on T_l commutes with that of $\mathbb{Q}(\sqrt{d})$ (Corollary 4.2).

Proposition 4.5. *Let p be a prime number and l be a prime that is ramified or inert in $\mathbb{Q}(\sqrt{d})$. Then the polynomial $\chi^{\mathrm{tr}}_{p^f} \in \mathbb{Q}[Z]$ splits as*

$$\chi^{\mathrm{tr}}_{p^f} = g_l g^\sigma_l,$$

for $g_l \in \mathbb{Q}_l(\sqrt{d})[Z]$ and $\sigma\colon \mathbb{Q}_l(\sqrt{d}) \to \mathbb{Q}_l(\sqrt{d})$ the conjugation.

Proof. The assumption ensures that $\mathbb{Q}_l(\sqrt{d})$ is a quadratic extension field. Further, T_l is a $\mathbb{Q}_l(\sqrt{d})$-vector space and, by Corollary 4.2, $\varrho_l((\mathrm{Frob}_p)^f)$ commutes with the operation of $\sqrt{d} \in E$. In other words, $\varrho_l((\mathrm{Frob}_p)^f)$ is a $\mathbb{Q}_l(\sqrt{d})$-linear map.

For the corresponding characteristic polynomial $c_l \in \mathbb{Q}_l(\sqrt{d})[Z]$, we have $\chi^T_{p^f} = c_l c^\sigma_l$. The assertion immediately follows from this. □

Lemma 4.6. *Let K be any field, $K(\sqrt{d})/K$ a quadratic field extension, and $h \in K[Z]$ an irreducible polynomial. Then h splits over $K(\sqrt{d})$ if and only if $K(\sqrt{d}) \subseteq K[Z]/(h)$.*

Proof. Suppose first that $K(\sqrt{d}) \subseteq K[Z]/(h)$ and let $z_0 \in K[Z]/(h)$ be a root of h. Then $K[Z]/(h) \cong K(z_0)$ and $[K(z_0) : K(\sqrt{d})] = (\deg h)/2$. Therefore, the minimal polynomial of z_0 over $K(\sqrt{d})$ is of degree $(\deg h)/2$ and a factor of h.

On the other hand, assume that h splits over $K(\sqrt{d})$ and write $h = gg^\sigma$. Then the extension fields $K[Z]/(h)$ and $K(\sqrt{d})[Z]/(g)$ both contain a zero of g and have the same degree over K. Hence, they must be isomorphic to each other. □

Notation 4.7. For $e \in \mathbb{N}$ and a normalized polynomial $h \in \mathbb{Q}[Z]$, we will write $h^{(e)}$ to denote the normalized polynomial of the same degree as h that has the zeroes $x^e_1, \ldots, x^e_r$, for $x_1, \ldots, x_r$ the zeroes of h, taken with multiplicities.

Remarks 4.8. (i) For an irreducible polynomial $h \in \mathbb{Q}[Z]$, the polynomial $h^{(e)}$ must not factor, except as the power of an irreducible polynomial. In fact, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ permutes the roots $x_1, \ldots, x_r$ of h transitively. Therefore, it does the same to $x^e_1, \ldots, x^e_r$.

(ii) If $h \in \mathbb{Q}[Z]$ is irreducible of degree r and $h(\zeta Z) \neq \zeta^r h(Z)$ for every eth root of unity ζ then $h^{(e)}$ is irreducible.

Theorem 4.9. *Let p be a prime of good reduction of the $K3$ surface X over $\mathbb{Q}$, having real or complex multiplication by a field E containing the quadratic number field $\mathbb{Q}(\sqrt{d})$. Then at least one of the following two statements is true.*

https://doi.org/10.1112/S1461157014000199 Published online by Cambridge University Press

(i) *The polynomial* $\chi_p^{\mathrm{tr}} \in \mathbb{Q}[Z]$ *splits in the form*

$$\chi_p^{\mathrm{tr}} = gg^\sigma,$$

for $g \in \mathbb{Q}(\sqrt{d})[Z]$ *and* $\sigma\colon \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}(\sqrt{d})$ *the conjugation.*

(ii) *The polynomial* $\chi_{p^f}^{\mathrm{tr}}$ *is a square in* $\mathbb{Q}[Z]$.

Proof. According to [48, Theorem 1.4.1], $\chi_p^{\mathrm{tr}} = h^k$, for an irreducible polynomial $h \in \mathbb{Q}[Z]$ and $k \in \mathbb{N}$. Write $h^{(f)} = \underline{h}^{k'}$, for $\underline{h}$ an irreducible polynomial. Then $\chi_{p^f}^{\mathrm{tr}} = \underline{h}^{kk'}$.

If one of the integers k and k' is even then assertion (ii) is true. Thus, assume from now on that k and k' are both odd. By Proposition 4.5, $\underline{h}^{kk'} = \chi_{p^f}^{\mathrm{tr}}$ splits into two factors conjugate over $\mathbb{Q}_l(\sqrt{d})$, for every l that is not split in $\mathbb{Q}(\sqrt{d})$. As kk' is odd, the same is true for $\underline{h}$.

In particular, for every prime $\mathfrak{L}$ lying above (l) in the field $\mathbb{Q}[Z]/(\underline{h})$, one has that $f(\mathfrak{L}|(l))$ is even for l inert in $\mathbb{Q}(\sqrt{d})$ and that $e(\mathfrak{L}|(l))$ is even for l ramified in $\mathbb{Q}(\sqrt{d})$. Then [35, Chapter VII, Proposition 13.9] implies that $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{Q}[Z]/(\underline{h})$.

Now let $x_0 \in \overline{\mathbb{Q}}$ be an element having minimal polynomial h. Then $\mathbb{Q}(x_0^f) \cong \mathbb{Q}[Z]/(\underline{h})$. Altogether, $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{Q}(x_0^f) \subseteq \mathbb{Q}(x_0)$. But, according to Lemma 4.6, this is equivalent to h being reducible over $\mathbb{Q}(\sqrt{d})$. It must split into two conjugate factors. □

Remarks 4.10. (i) Let h be an irreducible polynomial such that $\chi_p^{\mathrm{tr}} = h^k$ and consider $\mathrm{Gal}(h)$ as a permutation group on the roots of h. As such, it has an obvious block structure $\mathfrak{B} := \{\{z, \overline{z}\} \mid h(z) = 0\}$ into blocks of size two [9, § 1.5]. Indeed, h is a real polynomial without real roots and every root is of absolute value p. Thus, $\overline{z} = p^2/z$ and so the pairs are respected by the operation of the Galois group.

(ii) Assume that k is odd and that $d > 0$. We claim that this causes a second block structure. To show this, let us suppose first that variant (i) of Theorem 4.9 is true. Then there is the block structure $\mathfrak{B}' := \{\{z \mid g(z) = 0\}, \{z \mid g^\sigma(z) = 0\}\}$ into two blocks of size $(\deg h)/2$. As g and g^σ are real polynomials, the blocks in $\mathfrak{B}'$ are non-minimal. Each is a union of some of the blocks in $\mathfrak{B}$.

If option (ii) of Theorem 4.9 happens to be true then there is a block structure $\mathfrak{B}''$, the blocks of which are formed by the roots of h having their fth power in common. The mutual refinement of $\mathfrak{B}''$ and $\mathfrak{B}$ is the trivial block structure into blocks of size one. As k is assumed odd, the blocks in $\mathfrak{B}''$ are of even size. Thus, the block structure generated by $\mathfrak{B}''$ and $\mathfrak{B}$ consists of blocks of a size that is a multiple of 4.

Corollary 4.11. *Suppose that* $d > 0$. *Then, for every good prime* p, $\deg \chi_p^{\mathrm{tr}}$ *is divisible by* 4.

Proof. Write $\chi_p^{\mathrm{tr}} = h^k$. As seen in Remark 4.10(i), $\deg h$ is even, which implies the claim as long as k is even. When k is odd, the observations made in Remark 4.10(ii) show in both cases that $\deg h$ must be divisible by 4. □

Corollary 4.12. *Suppose that* $d > 0$. *Then, for every good prime* $p \geqslant 3$, *we have*

$$\mathrm{rk}\,\mathrm{Pic}((X_p)_{\overline{\mathbb{F}}_p}) \equiv 2 \pmod 4.$$

Proof. The Tate conjecture is known to be true for $K3$ surfaces in characteristic $\geqslant 3$, cf. [37, Theorem 1], [5, Corollary 2], and [29]. Further, the characteristic polynomial of Frob on $H^2_{\text{ét}}((X_p)_{\overline{\mathbb{F}}_p}, \mathbb{Q}_l)$ has exactly $22 - \deg \chi_p^{\mathrm{tr}}$ zeroes of the form p times a root of unity. □

https://doi.org/10.1112/S1461157014000199 Published online by Cambridge University Press

COROLLARY 4.13. *Suppose that $d > 0$ and let $p \geqslant 3$ be a good prime number that is inert in $E = \mathbb{Q}(\sqrt{d})$:*

(i) *then X_p is non-ordinary;*

(ii) *suppose that $\dim_E T \leqslant 3$. Then, either $\operatorname{rk} \operatorname{Pic}((X_p)_{\overline{\mathbb{F}}_p}) = 22$ or χ_{pf}^{tr} is the square of an irreducible quadratic polynomial.*

Proof. (i) X_p being ordinary would mean that χ_{pf}^{tr} has exactly one zero that is a p-adic unit. By Theorem 4.9, in any case, we can say that there is a factorization $\chi_{pf}^{\mathrm{tr}} = \underline{g}\underline{g}^{\sigma}$, for some $\underline{g} \in \mathscr{O}_E[Z]$. Assume without restriction that the zero being a p-adic unit is a root of $\underline{g}^{\sigma}$. Then, for the coefficients of the polynomial

$$\underline{g}(Z) = Z^n + a_{n-1}Z^{n-1} + \ldots + a_0,$$

one has that $\nu_p(a_j) > 0$, for every j. But, p is inert, hence the same is true for $\underline{g}^{\sigma}$. In particular, $\nu_p(a_{n-1}^{\sigma}) > 0$. This shows that it is impossible for $\underline{g}^{\sigma}$ to have exactly one root that is a p-adic unit.

(ii) The assumption $\dim_E T \leqslant 3$ means $\operatorname{rk} \operatorname{Pic} X_{\overline{\mathbb{Q}}} \geqslant 16$. Then, further, $\operatorname{rk} \operatorname{Pic}((X_p)_{\overline{\mathbb{F}}_p}) \geqslant 16$. From Corollary 4.12, we know that either $\operatorname{rk} \operatorname{Pic}((X_p)_{\overline{\mathbb{F}}_p}) = 18$ or $\operatorname{rk} \operatorname{Pic}((X_p)_{\overline{\mathbb{F}}_p}) = 22$. The proof is complete in the latter case, so let us suppose that the rank is 18.

Then $\deg \chi_p^{\mathrm{tr}} = \deg \chi_{pf}^{\mathrm{tr}} = 4$. Theorem 4.9 gives us two options. Option (ii) is that $\chi_{pf}^{\mathrm{tr}} = g^2$ is the square of a quadratic polynomial $g \in \mathbb{Q}[Z]$. Since its roots are non-reals, this polynomial must be irreducible.

Otherwise, according to option (i), there is a factorization $\chi_p^{\mathrm{tr}} = gg^{\sigma}$, for some $g \in E[Z]$. Write $g(Z) = Z^2 + aZ \pm p^2 = (Z - x_1)(Z - x_2)$. Then

$$\nu_p(x_1) + \nu_p(x_2) = \nu_p(x_1x_2) = \nu_p(\pm p^2) = 2$$

and $\min(\nu_p(x_1), \nu_p(x_2)) \leqslant \nu_p(x_1 + x_2) = \nu_p(-a)$. If $\nu_p(x_1) \neq \nu_p(x_2)$ then equality is true.

Further, $a \in \mathbb{Q}(\sqrt{d})$ implies that $\nu_p(-a)$ is an integer and it is well known that $\nu_p(x_i) \geqslant 0$. Thus, there are only two cases. We will show that they are both contradictory.

If $\nu_p(x_1) = \nu_p(x_2) = 1$ then, as p is inert, the same is true for x_1^{σ} and x_2^{σ}. Hence, the four quotients x_1/p, x_2/p, x_1^{σ}/p, and x_2^{σ}/p are p-adic units. On the other hand, the eigenvalues of Frob_p on l'-adic cohomology are known to be l'-adic units for every $l' \neq p$. Hence, x_1/p, x_2/p, x_1^{σ}/p, and x_2^{σ}/p are actually l-adic units for all primes l. Consequently, they must be roots of unity. This, however, is a contradiction to the definition of χ_p^{tr}, given in Notation 4.3(ii).

On the other hand, if, without restriction, $\nu_p(x_1) = 0$ and $\nu_p(x_2) = 2$ then $\nu_p(x_1^{\sigma}) = 0$, too. This is a contradiction to the general fact that the Newton polygon always runs above the Hodge polygon. □

COROLLARY 4.14. *Suppose that $\dim_E T \leqslant 3$. If χ_{pf}^{tr} is the square of a quadratic polynomial, but χ_p^{tr} is not, then $\mathrm{Gal}(\chi_p^{\mathrm{tr}}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

Proof. The assumption implies that $\chi_p^{\mathrm{tr}} = h$ is irreducible of degree four. Further, $\mathrm{Gal}(h)$ has two different block structures, both into blocks of size two. The only transitive subgroup of S_4 having this property is the Klein four group. □

5. *Efficient algorithms to test a $K3$ surface for real multiplication*

Generalities. Recall that a $K3$ surface Y over a finite field $\mathbb{F}_p$ is ordinary if and only if $\#Y(\mathbb{F}_p) \not\equiv 1 \pmod{p}$. In particular, non-ordinarity may be tested by counting points only over $\mathbb{F}_p$.

https://doi.org/10.1112/S1461157014000199 Published online by Cambridge University Press

For $K3$ surfaces with real multiplication by $\mathbb{Q}(\sqrt{d})$, we expect non-ordinary reduction at approximately half the primes. On the other hand, consider a general $K3$ surface X over $\mathbb{Q}$ of a certain geometric Picard rank. That is, assume that $\mathrm{End}(T) \cong \mathbb{Q}$. Then Theorem 4.1 implies that the Frobenii $\varrho_l(\sigma\mathrm{Frob}_p\sigma^{-1})$, for p running through the primes and σ through $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, are Zariski dense in $\mathrm{GO}(T_l, \langle\,.\,,.\rangle)$. In particular, the values $(\#X_p(\mathbb{F}_p) - p^2 - 1)/p = (1/p)\,\mathrm{Tr}\,\mathrm{Frob}_p$ are Zariski dense in $\mathbf{A}^1$. In a way similar to [27], one may hope that $((1/p)\,\mathrm{Tr}\,\mathrm{Frob}_p \bmod 1)$ is equidistributed in $[0, 1]$.

Thus, somewhat naively, we expect that a general $K3$ surface X over $\mathbb{Q}$ has non-ordinary reduction at p with a probability of $1/p$. The number of primes $\leqslant N$, at which the reduction is non-ordinary, should be of the order of $\log\log N$.

This suggests generating a huge sample of $K3$ surfaces over $\mathbb{Q}$, each having geometric Picard rank $\geqslant 16$, and executing the following statistical algorithm on all of them.

Algorithm 5.1 (Testing a $K3$ surface for real multiplication, statistical version).

(i) Let p run over all primes $p \equiv 1 \pmod 4$ between 40 and 300. For each p, count the number $\#X_p(\mathbb{F}_p)$ of $\mathbb{F}_p$-rational points on the reduction of X modulo p. If $\#X_p(\mathbb{F}_p) \equiv 1 \pmod p$ for not more than five primes then terminate immediately.

(ii) Put p_0 to be the smallest good and ordinary prime for X.

(iii) Determine the characteristic polynomial of Frob on $H^2_{\text{ét}}((X_{p_0})_{\overline{\mathbb{F}}_{p_0}}, \mathbb{Q}_l)$. For this, use the strategy described in [12, Examples 27 and 28]. Factorize the polynomial obtained to calculate the polynomial $\chi^{\mathrm{tr}}_{p_0}$. If $\deg \chi^{\mathrm{tr}}_{p_0} \neq 4$ then terminate.

Test whether $\chi^{\mathrm{tr}}_{p_0}$ is the square of a quadratic polynomial. In this case, raise p_0 to the next good and ordinary prime and iterate this step.

Otherwise, determine the Galois group $\mathrm{Gal}(\chi^{\mathrm{tr}}_{p_0})$. If $\mathrm{Gal}(\chi^{\mathrm{tr}}_{p_0})$ is isomorphic to the Klein four group then raise p_0 to the next good and ordinary prime and iterate this step.

(iv) Now, $\chi^{\mathrm{tr}}_{p_0}$ is irreducible of degree four. Determine the quadratic subfields of the splitting field of $\chi^{\mathrm{tr}}_{p_0}$. Only one real quadratic field may occur. Put d to be the corresponding radicand.

(v) Let p run over all primes < 300 that are inert in $\mathbb{Q}(\sqrt{d})$, starting from the lowest. If $\#X_p(\mathbb{F}_p) \not\equiv 1 \pmod p$ for one of these then terminate.

(vi) Output a message saying that X is highly likely to have real or complex multiplication by a field containing $\mathbb{Q}(\sqrt{d})$.

Remarks 5.2. (i) Algorithm 5.1 does not give false negatives due to bad reduction cf. Lemma 5.5, below.

Nevertheless, the algorithm is only statistically correct. It is possible, in principle, that a $K3$ surface with real multiplication is thrown away in step (i). However, in the case that $\mathrm{End}(T) = \mathbb{Q}(\sqrt{d})$, this may occur only if not more than five of the primes used in the algorithm are inert in $\mathbb{Q}(\sqrt{d})$. The smallest discriminant for which this happens is $d = 8493$.

(ii) On the other hand, Algorithm 5.1 is extremely efficient. The point is that, for the lion's share of the surfaces, it terminates directly after step (i). In fact, according to the inclusion–exclusion principle [20, formula (2.1.3)], the likelihood that a surface with $\mathrm{End}(T) \cong \mathbb{Q}$ survives step (i) should be

$$\sum_{r=6}^{\#S} \sum_{\substack{R \subset S \\ \#R = r}} (-1)^{r-6} \binom{r}{6} \frac{1}{\prod_{p \in R} p} \approx 2.66 \cdot 10^{-8},$$

for $S := \{p \mid p \text{ prime}, 40 < p < 300,\ p \equiv 1 \pmod 4\}$. Thus, the more time-consuming steps (ii)–(v) have to be carried out for only a negligible percentage of the surfaces.

This shows, in particular, that step (i) is the only time-critical one. An efficient algorithm for point counting over relatively small prime fields is asked for.

https://doi.org/10.1112/S1461157014000199 Published online by Cambridge University Press

(iii) In our samples, step (iii) involves counting, in addition, the points on X_{p_0} that are defined over $\mathbb{F}_{p_0^2}$ and, possibly, over $\mathbb{F}_{p_0^3}$, but not over larger fields. The reason for this is that 16 generators of the cohomology vector space are explicitly known, including the Galois operation on them. Thus, only a degree six factor of the desired polynomial of degree 22 needs to be computed.

(iv) The second part of step (iii) has the potential to create an infinite loop. But this never happened for any of the surfaces we tested. Whenever step (i) suggested real multiplication, after a few trials we found a prime p_0 such that $\deg \chi_{p_0}^{\mathrm{tr}}$ was irreducible of degree four and had the cyclic group of order four or the dihedral group of order eight as its Galois group.

(v) In step (iv), the polynomial $\chi_{p_0^f}^{\mathrm{tr}}$ is certainly irreducible although the value of f is not known to us. This is simply the assertion of Corollary 4.14. As a consequence of this, Theorem 4.9 shows that $\chi_{p_0}^{\mathrm{tr}}$ must split over the RM field.

(vi) The reason for restricting to primes congruent to 1 modulo 4 in step (i) is a practical one. Otherwise, too many surfaces are found showing the pattern that $\#X_p(\mathbb{F}_p) \equiv 1 \pmod{p}$ for every prime $p \equiv 3 \pmod{4}$. These primes are inert under $\mathbb{Q}(\sqrt{-1})/\mathbb{Q}$, but not under any real quadratic field extension. We do not exactly understand why our samples contained many more such surfaces than those we were looking for.

On the other hand, for small primes p, it happens too often that $\#X_p(\mathbb{F}_p) \equiv 1 \pmod{p}$, independently of whether or not X has real multiplication. As this would slow down the algorithm, we incorporated the restriction to primes $p > 40$.

(vii) The likelihood that a random surface would survive step (v) is

$$\prod_{\substack{p \text{ inert in } \mathbb{Q}(\sqrt{d}), \\ p<300}} 1/p, \tag{2}$$

which is less than 10^{-60} for small values of d. Thus, we do not expect any false positives to be given by Algorithm 5.1.

When testing surfaces for real multiplication by a particular field $\mathbb{Q}(\sqrt{d})$, the following modification of Algorithm 5.1 may be used.

Algorithm 5.3 (Testing a $K3$ surface for real multiplication, deterministic version).

(o) This algorithm assumes that, in an initialization step, the primes $p < 300$ that are inert in $\mathbb{Q}(\sqrt{d})$ have been listed.

(i) Let p run over the list. For each p, count the numbers $\#X_p(\mathbb{F}_p)$ of $\mathbb{F}_p$-rational points on the reduction X_p. If one of them is not congruent to 1 modulo p then terminate immediately.

(ii) Let p run over all good primes < 100, starting from the lowest.

For each prime, calculate the polynomial χ_p^{tr}, as in Algorithm 5.1(iii). If $\deg \chi_p^{\mathrm{tr}} \neq 0$ or 4 then terminate. If $\deg \chi_p^{\mathrm{tr}} = 4$ then test whether χ_p^{tr} is the square of a quadratic polynomial. If this is the case then go to the next prime.

Factor χ_p^{tr} over $\mathbb{Q}(\sqrt{d})$ and determine the Galois group $\mathrm{Gal}(\chi_p^{\mathrm{tr}})$. If neither χ_p^{tr} splits over $\mathbb{Q}(\sqrt{d})$ nor $\mathrm{Gal}(\chi_p^{\mathrm{tr}}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ then terminate. Otherwise, go to the next prime.

(iii) Output a message saying that X is highly likely to have real or complex multiplication by a field containing $\mathbb{Q}(\sqrt{d})$.

Remarks 5.4. (i) Algorithm 5.3 does not give false negatives. Bad reduction does not cause any problem, due to Lemma 5.5.

(ii) The likelihood that a general $K3$ surface survives step (i) is again given by formula (2) above. In the cases $d = 2$, 5, 13, and 17, where we actually run the algorithm, the values of the product are approximately $3.26 \cdot 10^{-64}$, $2.69 \cdot 10^{-63}$, $4.07 \cdot 10^{-61}$, and $1.30 \cdot 10^{-63}$. In accordance with this, no statistical outliers showed up in step (ii).

https://doi.org/10.1112/S1461157014000199 Published online by Cambridge University Press

LEMMA 5.5. *Let X be a double cover of $\mathbf{P}^2_{\mathbb{Q}}$, branched over the union of six lines. Suppose there is a quadratic number field $\mathbb{Q}(\sqrt{d})$ such that $\#X_q(\mathbb{F}_q) \equiv 1 \pmod q$ for every good prime q that is inert in $\mathbb{Q}(\sqrt{d})$.*

Then $\#X_p(\mathbb{F}_p) \equiv 1 \pmod p$, too, for every bad prime p that is inert.

Proof. If at least two of the six lines coincide modulo p then X_p is a rational surface and $\#X_p(\mathbb{F}_p) \equiv 1 \pmod p$ is automatic. Thus, let us assume the contrary.

We fix an auxiliary prime number l that is split in $\mathbb{Q}(\sqrt{d})$ and let p be a bad, inert prime. For every prime q inert in $\mathbb{Q}(\sqrt{d})$, choose an absolute Frobenius element $\mathrm{Frob}_q \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. By Cebotarev, the elements $\sigma^{-1}\mathrm{Frob}_q\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, for q running through the inert primes and σ through $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, are dense in the coset $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \setminus \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\sqrt{d}))$, to which Frob_p belongs. The same is still true when restricting to the primes q, at which X has good reduction.

For those, we have the congruence $\mathrm{Tr}\,\mathrm{Frob}_{H^2_{\text{ét}}((X_q)_{\overline{\mathbb{F}}_q},\mathbb{Q}_l)} \equiv 0 \pmod q$. In other words,

$$\mathrm{Tr}\,\frac{1}{q}\mathrm{Frob}_{H^2_{\text{ét}}((X_q)_{\overline{\mathbb{F}}_q},\mathbb{Q}_l)} = \mathrm{Tr}\,\frac{1}{q}\mathrm{Frob}_{q,H^2_{\text{ét}}(X_{\overline{\mathbb{Q}}},\mathbb{Q}_l)} = \mathrm{Tr}\,\mathrm{Frob}_{q,H^2_{\text{ét}}(X_{\overline{\mathbb{Q}}},\mathbb{Q}_l(1))}$$

is an integer, necessarily within the range $[-22, 22]$. As the condition $\mathrm{Tr}\,(1/q)\varphi \in \mathbb{Z} \cap [-22, 22]$ defines a Zariski closed subset of $\mathrm{GL}(H^2_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_l(1)))$, one has

$$\mathrm{Tr}\,\mathrm{Frob}_{H^2_{\text{ét}}(X_{\overline{\mathbb{Q}}_p},\mathbb{Q}_l)} = \mathrm{Tr}\,\mathrm{Frob}_{p,H^2_{\text{ét}}(X_{\overline{\mathbb{Q}}},\mathbb{Q}_l)} \equiv 0 \pmod p, \tag{3}$$

too, cf. [39, Exposé XVI, Corollaire 1.6]

Further, the eigenvalues of Frob on $H^2_{\text{ét}}(X_{\overline{\mathbb{Q}}_p}, \mathbb{Q}_l)$ are the same as those on $H^2_{\text{ét}}(X_{\overline{\mathbb{Q}}_p}, \mathbb{Q}_p)$ [36, Theorem 3.1]. In addition, a main result of p-adic Hodge theory [15, Theorem III.4.1] implies, as X is $K3$, that not more than one of the eigenvalues of Frob on $H^2_{\text{ét}}(X_{\overline{\mathbb{Q}}_p}, \mathbb{Q}_p)$ may be a p-adic unit, the others being of strictly positive p-adic valuation. Under these circumstances, the congruence (3) implies that none of the eigenvalues is a p-adic unit.

For comparison with the cohomology $H^2_{\text{ét}}((X_p)_{\overline{\mathbb{F}}_p}, \mathbb{Q}_l)$ of the singular fiber, the theory of vanishing cycles [41, Exposés I, XIII, and XV] applies, as X_p has only isolated singularities [24, Corollaire 2.9]. In our case, it states that $H^2_{\text{ét}}((X_p)_{\overline{\mathbb{F}}_p}, \mathbb{Q}_l)$ naturally injects into $H^2_{\text{ét}}(X_{\overline{\mathbb{Q}}_p}, \mathbb{Q}_l)$. In particular, the eigenvalues of Frob on $H^2_{\text{ét}}((X_p)_{\overline{\mathbb{F}}_p}, \mathbb{Q}_l)$ form a subset of the 22 eigenvalues of Frob on $H^2_{\text{ét}}(X_{\overline{\mathbb{Q}}_p}, \mathbb{Q}_l)$.

This shows that all eigenvalues on $H^2_{\text{ét}}((X_p)_{\overline{\mathbb{F}}_p}, \mathbb{Q}_l)$ are of strictly positive p-adic valuation. Further, using the Leray spectral sequence together with the proper base change theorem [39, Exposé XII, Corollaire 5.2(iii)], one sees that blow-ups do not affect the transcendental part $T_l \subset H^2_{\text{ét}}((X_p)_{\overline{\mathbb{F}}_p}, \mathbb{Q}_l)$. Hence, $\#\widetilde{X}_p(\mathbb{F}_p) \equiv 1 \pmod p$, for $\widetilde{X}_p$ the minimal resolution of singularities. The same is true for X_p. □

Counting points on degree-2 K3-surfaces: structure of our samples

We consider $K3$ surfaces that are given as desingularizations of the double covers of the projective plane, branched over the union of six lines. One reason for choosing this particular family is that it is the one studied before by van Geemen [19, Example 3.4]. On the other hand, this family offers computational advantages, too.

Our trial computations with all six lines defined over $\mathbb{Q}$ did not lead to any success. On the other hand, six lines defined over an S_6-extension of $\mathbb{Q}$ and forming a Galois orbit would not be easy to handle. Our compromise is as follows.

The lines are allowed to form three Galois orbits, each of size two. Assuming the three $\mathbb{Q}$-rational points of intersection not to be collinear, we may suppose them without restriction

https://doi.org/10.1112/S1461157014000199 Published online by Cambridge University Press

to be $(1:0:0)$, $(0:1:0)$, and $(0:0:1)$. The equation of the surface then takes the form

$$w^2 = q_1(y,z)q_2(x,z)q_3(x,y).$$

This representation is unique up to action of the monomial group. That is, up to permutation and scaling of the variables.

Algorithm 5.6 (Counting points on one surface). In order to determine the number of $\mathbb{F}_q$-rational points on one surface, we count the points over the q affine lines of the form $(1:u:\star)$ and the affine line $(0:1:\star)$ and sum up these numbers. Finally, we add 1, as, on each of our surfaces, there is exactly one point lying above e_3.

Remark 5.7 (Counting points above one line). It is easy to count the number of points above the affine line $L_{x,y}\colon \mathbf{A}^1 \to \mathbf{P}^2$, given by $t \mapsto (x:y:t)$. Observe that q_3 is constant on this line. Thus, we get a quadratic twist of an elliptic curve. The number of points on it is $q + \chi(q_3(x,y))\lambda_{x,y}$, for

$$\lambda_{x,y} := \sum_{t\in\mathbb{F}_q} \chi(q_1(y,t)q_2(x,t)) \tag{4}$$

and χ the quadratic character of $\mathbb{F}_q$.

Strategy 5.8 (Treating a sample of surfaces). Our samples are given by three lists of quadratic forms. One list for q_1, another for q_2, and third one for q_3. In the case that we want to count the points on all surfaces given by the Cartesian product of the three lists, we perform as follows.

(i) For each quadratic form q_3, compute the values of $\chi(q_3(1,\star))$ and $\chi(q_3(0,1))$ and store them in a table.

(ii) Run in an iterated loop over all pairs (q_1,q_2). For each pair, do the following.

- Using formula (4), compute $\lambda_{1,\star}$ and $\lambda_{0,1}$.
- Run in a loop over all forms q_3. Each time, calculate $S_{q_1,q_2,q_3} := \sum_\star \chi(q_3(1,\star))\lambda_{1,\star}$, using the precomputed values. The number of points on the surface, corresponding to (q_1,q_2,q_3), is then $q^2+q+1+\chi(q_3(0,1))\lambda_{0,1}+S_{q_1,q_2,q_3}$.

Remarks 5.9. (i) (Complexity and performance). In the case that the number of quadratic forms is bigger than q, the costs of building up the tables are small compared to the final step. Thus, the complexity per surface is essentially reduced to $(q{+}1)$ table look-ups for the quadratic character and $(q+1)$ look-ups in the small table, containing the values $\lambda_{1,\star}$ and $\lambda_{0,1}$.

(ii) We are limited by the memory transfer generated by the former table access. We store the quadratic character in an 8-bit signed integer variable. This doubles the speed compared to a 16-bit variable.

Remark 5.10 (Detecting real multiplication). We used the point counting algorithm, in the version described in Strategy 5.8, within the deterministic Algorithm 5.3, in order to detect $K3$ surfaces having real multiplication by a prescribed quadratic number field. This allowed us to test more than $2.2\cdot 10^7$ surfaces per second on one core of a 3.40 GHz Intel$^{(\mathrm{R})}$Core$^{(\mathrm{TM})}$i7-3770 processor. The code was written in plain `C`.

The results. (i) A run of Algorithm 5.1 over all triples (q_1,q_2,q_3) of coefficient height $\leqslant 12$, using the method described in Strategy 5.8 for point counting, discovered the first five surfaces that were likely to have real multiplication by $\mathbb{Q}(\sqrt{5})$. Observe that a sample of more than 10^{11} surfaces was necessary to bring these examples to light.

https://doi.org/10.1112/S1461157014000199 Published online by Cambridge University Press

Analyzing the examples, we observed that the product of the discriminants of the three binary quadratic forms was always a perfect square.

(ii) We added this restriction to our search strategy, which massively reduced the number of surfaces to be inspected. Doing so, we could raise the search bound up to 80. This resulted in more surfaces with probable real multiplication by $\mathbb{Q}(\sqrt{5})$ and one example that was likely to have real multiplication by $\mathbb{Q}(\sqrt{2})$.

From the results, we observed that the square class of one of the three discriminants always coincided with the discriminant of the field of real multiplication.

(iii) This restriction led to a further reduction of the search space. At a final stage, we could raise the search bound to 200 for real multiplication by $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt{13})$, and $\mathbb{Q}(\sqrt{17})$. We found many more examples for $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{5})$, one example for $\mathbb{Q}(\sqrt{13})$, but none for $\mathbb{Q}(\sqrt{17})$.

REMARK 5.11. The final sample for $\mathbb{Q}(\sqrt{17})$ consisted of about $4.18 \cdot 10^{13}$ surfaces and required about 24 days of CPU time. The computations were executed in parallel on two machines, making use of two cores on each machine. The other samples were comparable in size.

In the cases of $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{5})$, the examples found were sufficient to guess 1-parameter families. To summarize, our experiments led us to expect the following two results. For the first, we could later devise a proof, the second remains a conjecture.

THEOREM 5.12. *Let $t \in \mathbb{Q}$ be arbitrary and $X^{(2,t)}$ be the $K3$ surface given by*

$$\begin{aligned} w^2 = {} & [(\tfrac{1}{8}t^2 - \tfrac{1}{2}t + \tfrac{1}{4})y^2 + (t^2 - 2t + 2)yz + (t^2 - 4t + 2)z^2] \\ & \cdot [(\tfrac{1}{8}t^2 + \tfrac{1}{2}t + \tfrac{1}{4})x^2 + (t^2 + 2t + 2)xz + (t^2 + 4t + 2)z^2][2x^2 + (t^2 + 2)xy + t^2y^2]. \end{aligned}$$

Then $\#X_p^{(2,t)}(\mathbb{F}_p) \equiv 1 \pmod{p}$ for every prime $p \equiv 3, 5 \pmod{8}$.

Proof. The case $p = 3$ is elementary. For $p \neq 3$, we shall prove this result below in Theorem 6.3, under some additional restrictions on t. For the cases left out there, similar arguments work; cf. Remark 6.4 for a few details. □

CONJECTURE 5.13. (i) *Let $t \in \mathbb{Q}$ be arbitrary and $X^{(5,t)}$ be the $K3$ surface given by*

$$w^2 = [y^2 + tyz + (\tfrac{5}{16}t^2 + \tfrac{5}{4}t + \tfrac{5}{4})z^2][x^2 + xz + (\tfrac{1}{320}t^2 + \tfrac{1}{16}t + \tfrac{5}{16})z^2][x^2 + xy + \tfrac{1}{20}y^2].$$

Then $\#X_p^{(5,t)}(\mathbb{F}_p) \equiv 1 \pmod{p}$ for every prime $p \equiv 2, 3 \pmod{5}$.

(ii) *Let $X^{(13)}$ be the $K3$ surface given by*

$$w^2 = (25y^2 + 26yz + 13z^2)(x^2 + 2xz + 13z^2)(9x^2 + 26xy + 13y^2).$$

Then $\#X_p^{(13)}(\mathbb{F}_p) \equiv 1 \pmod{p}$ for every prime $p \equiv 2, 5, 6, 7, 8, 11 \pmod{13}$.

REMARK 5.14. We verified the congruences above for all primes $p < 1000$. This concerns $X^{(13)}$ as well as the $X^{(5,t)}$, for any residue class of t modulo p.

There is further evidence, as we computed the characteristic polynomials of Frob_p for $X^{(13)}$ as well as for $X^{(5,t)}$ and several exemplary values of $t \in \mathbb{Q}$, for the good primes p below 100. It turns out that they do indeed all show the very particular behaviour described in Theorem 4.9. To put it concretely, in each case, either χ_p^{tr} is of degree zero, or $\chi_{p^f}^{\mathrm{tr}}$ is the square of a quadratic polynomial for a suitable positive integer f, or χ_p^{tr} is irreducible of degree four, but splits into two factors conjugate over $\mathbb{Q}(\sqrt{5})$, respectively $\mathbb{Q}(\sqrt{13})$.

https://doi.org/10.1112/S1461157014000199 Published online by Cambridge University Press

6. *The proof for real multiplication in the case of the* $\mathbb{Q}(\sqrt{2})$*-family*

Lemma 6.1. *Let $a, D \in \mathbb{Z}$ be such that $\gcd(a, D) = 1$ and X a $K3$ surface over $\mathbb{Q}$. Suppose that $\#X_p(\mathbb{F}_p) \equiv 1 \pmod p$ for every good prime $p \equiv a \pmod D$. Then X has real or complex multiplication.*

Proof. For each prime p, choose an absolute Frobenius element $\mathrm{Frob}_p \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. By Cebotarev's density theorem, the elements $\sigma^{-1}\mathrm{Frob}_p\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, for the good primes $p \equiv a \pmod D$ and $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, are topologically dense in the coset of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ modulo $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_D))$ that they belong to. Thus, there are finitely many elements $\sigma_1, \ldots, \sigma_k \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ such that

$$\{\sigma_i\sigma^{-1}\mathrm{Frob}_p\,\sigma \mid i = 1, \ldots, k, p \equiv a \pmod D, p \text{ good for } X,\ \sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})\}$$

is dense in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Now choose any prime $l \not\equiv a \pmod D$, put $T_l \subset H^2_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_l)$ to be the transcendental part of l-adic cohomology, and write $r := \dim T_l$. Then, for every good prime $p \equiv a \pmod D$, one has $\mathrm{Tr}\,\mathrm{Frob}_{p,T_l} = kp$, for $-22 < -r \leqslant k \leqslant r < 22$, and $\det \mathrm{Frob}_{p,T_l} = \pm p^r$. Hence,

$$(\mathrm{Tr}\,\mathrm{Frob}_{p,T_l})^r = \pm k^r \det \mathrm{Frob}_{p,T_l},$$

which defines a Zariski closed subset $I \subsetneqq \mathrm{GO}(T_l, \langle .\,, .\rangle)$, invariant under conjugation. As $\mathrm{GO}(T_l, \langle .\,, .\rangle)$ is irreducible, the union $\sigma_1 I \cup \ldots \cup \sigma_k I$ cannot be the whole group. Consequently, the image of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GO}(T_l, \langle .\,, .\rangle)$ is not Zariski dense. In view of Theorem 4.1, this is enough to imply real or complex multiplication. □

Lemma 6.2. *Let $C\colon w^2 = F_4(x, y, l)$ be a family of smooth genus-one curves, parametrized by $l \in B$, for B an integral scheme in characteristic $\neq 2$ or 3, $c_4(l)$ and $c_6(l)$ its classical invariants, and $\Delta := (c_4^3(l) - c_6^2(l))/1728$. Then, over the open subscheme $D(\Delta) \subseteq B$,*

$$I\colon w^2 = x^3 - 27c_4(l)x - 54c_6(l)$$

defines a family of elliptic curves, fiber-wise isomorphic to the relative Jacobian of C.

Proof. The existence of the relative Jacobian $\mathscr{J}$ follows from [18, Exposé 232, Théorème 3.1]. This is a family of elliptic curves, and I is a family of elliptic curves, too, as $-16[4(-27c_4(l))^3 + 27(-54c_6(l))^2] = 6^{12}\Delta(l) \neq 0$.

Further, the generic fiber I_η is isomorphic to the Jacobian of C_η [16, Proposition 2.3]. Thus, over $D(\Delta)$, we have two families of elliptic curves that coincide over the generic point $\eta \in D(\Delta)$. The assertion follows from this, since the moduli stack of elliptic curves is separated [26, First main Theorem 5.1.1, together with 2.2.11]. □

Theorem 6.3 (The point count). *Let $\mathbb{F}_q$ be a finite field of characteristic $\neq 2, 3$ such that 2 is a non-square in $\mathbb{F}_q$ and V the singular surface given by $w^2 = q_1(y, z)q_2(x, z)q_3(x, y)$, for $t \in \mathbb{F}_q$ and*

$$\begin{aligned}
q_1(y, z) &:= (\tfrac{1}{8}t^2 - \tfrac{1}{2}t + \tfrac{1}{4})y^2 + (t^2 - 2t + 2)yz + (t^2 - 4t + 2)z^2,\\
q_2(x, z) &:= (\tfrac{1}{8}t^2 + \tfrac{1}{2}t + \tfrac{1}{4})x^2 + (t^2 + 2t + 2)xz + (t^2 + 4t + 2)z^2,\\
q_3(x, y) &:= (x + y)(2x + t^2y).
\end{aligned}$$

Suppose that $t \neq 0$ and $t^2 \neq -2$. Then $\#V(\mathbb{F}_q) = q^2 + q + 1$.

https://doi.org/10.1112/S1461157014000199 Published online by Cambridge University Press

Proof. We will prove this result in several steps.

First step: preparations. We will count fiber-wise using the fibration, given by $y : x = l$, for $l \in \mathbf{P}^1(\mathbb{F}_q)$. This will yield a result by q too large, as the point lying over $(0 : 0 : 1)$ will be counted $(q+1)$ times.

The fiber V_l is the curve, given by $w^2 = (1+l)(2+t^2l)x^2q_1(lx,z)q_2(x,z)$. A partial resolution is provided by $C_l\colon w^2 = (1+l)(2+t^2l)q_1(lx,z)q_2(x,z)$, which defines an elliptic fibration.

We claim that $\sum_l \#C_l(\mathbb{F}_q) = \sum_l \#V_l(\mathbb{F}_q)$. Indeed, the two fibrations differ only over the line '$x = 0$'. Since V ramifies over this line, V_x has exactly $(q+1)$ points. On the other hand, the curve C_x is given by $w^2 = (t^4 - 12t^2 + 4) \cdot (1+l)(2+t^2l)$. Here, the constant

$$t^4 - 12t^2 + 4 = (t^2 - 6)^2 - 32$$

is non-zero, as 2 is not a square. Thus, C_x is a double cover of $\mathbf{P}^1$, ramified at (-1) and $(-2/t^2)$. But $-1 \neq -2/t^2$, since 2 is a non-square. In other words, C_x is a conic, which has exactly $(q+1)$ points.

Second step: singular fibers. There are four singular fibers, at $l = -1$, $-2/t^2$, 0, and ∞. In fact, for the first two, the coefficient is zero, while, for the others, one of the quadratic forms has a double zero. We claim that these are the only singular $\mathbb{F}_q$-rational fibers.

To see this, we first observe that q_1 is of discriminant

$$(t^2-2t+2)^2 - 4(\tfrac{1}{8}t^2 - \tfrac{1}{2}t + \tfrac{1}{4})(t^2-4t+2) = (t^2+2t+2)^2 - \tfrac{1}{2}(t^2+4t+2)^2 = \tfrac{1}{2}(t^2-2)^2$$

and the same for q_2. This term does not vanish, for any value of t. Therefore, q_1 and q_2 always define two lines each, never a double line. Consequently, for $l \neq 0, \infty$, neither of the two quadratic factors $q_1(lx,z)$ and $q_2(x,z)$ may have a double zero.

To exclude a common zero, one has to compute the resultant, which turns out to be

$$\tfrac{1}{64}(t^4-12t^2+4)^2\big(l^2 + \tfrac{-6t^4+8t^2-24}{t^4-12t^2+4}l + 1\big)\big(l^2 + \tfrac{-2t^4-8t^2-8}{t^4-12t^2+4}l + 1\big).$$

Here, $t^4 - 12t^2 + 4 \neq 0$. Further, the quadratic polynomials in l are of the discriminants $32(t^2-2)^2(t^2+2)^2/(t^4-12t^2+4)^2$ and $128t^2(t^2-2)^2/(t^4-12t^2+4)^2$, which are non-squares in $\mathbb{F}_q$, because of $t \neq 0$ and $t^2 \neq \pm 2$. Thus, the resultant does not vanish for any value of l, as long as t is admissible.

Third step: points on the singular fibers. The curves C_{-1} and C_{-2/t^2} are part of the ramification locus and therefore degenerate to lines. They have $(q+1)$ points each.

On the other hand, the fibers C_0 and C_∞ are given by $w^2 = 2(t^2-4t+2)z^2q_2(x,z)$ and $w^2 = t^2(t^2+4t+2)z^2q_1(y,z)$. Both are conics with the points over $z = 0$ unified into a double point. The corresponding points on the non-singular conics C_0^{ns} and C_∞^{ns} satisfy $w^2 = \frac{1}{4}(t^4-12t^2+4)$, and $w^2 = t^2(t^4-12t^2+4)/8$, respectively. The two equations differ by a factor of $t^2/2$, which is a non-square. Hence, one of the curves C_0^{ns} and C_∞^{ns} has two points such that $z = 0$, the other none. Accordingly, one of the singular curves C_0 and C_∞ has q points, the other $(q+2)$.

It therefore remains to show that $\sum_{l, C_l \text{ smooth}} \#C_l(\mathbb{F}_q) = (q-3)(q+1)$.

Fourth step: the classical invariants c_4 and c_6. The invariants c_4 and c_6 of the family of binary quartic forms defining C are polynomials in l and t. They may easily be written down, but the formulas become quite lengthy. The discriminant Δ turns out to be

$$\Delta = \tfrac{1}{1024}t^{12}(t^2-2)^4(t^4-12t^2+4)^4l^2\big(l+\tfrac{2}{t^2}\big)^6(l+1)^6$$
$$\cdot\big(l^2 + \tfrac{-6t^4+8t^2-24}{t^4-12t^2+4}l + 1\big)^2\big(l^2 + \tfrac{-2t^4-8t^2-8}{t^4-12t^2+4}l + 1\big)^2.$$

The arguments given in the second step show that $\Delta \neq 0$, except for $l = -1$, $-2/t^2$, 0, and ∞.

https://doi.org/10.1112/S1461157014000199 Published online by Cambridge University Press

By Lemma 6.2, $I_l\colon w^2 = x^3 - 27c_4(l)x - 54c_6(l)$ is isomorphic to the Jacobian $\operatorname{Jac} C_l$, for $l \neq -1, -2/t^2, 0, \infty$. This implies $\#C_l(\mathbb{F}_q) = \#(\operatorname{Jac} C_l)(\mathbb{F}_q) = \#I_l(\mathbb{F}_q)$, since genus-one curves over finite fields always have points.

We have to prove that $\sum_{l, C_l \text{ smooth}} \#I_l(\mathbb{F}_q) = (q-3)(q+1)$. That is, that the $(q-3)$ smooth fibers of I have, on average, exactly $(q+1)$ points.

Fifth step: l versus $1/l$. For the j-invariant $j = c_4^3/\Delta$, one computes that $j(1/l) = j(l)$. More precisely,

$$c_4\left(\frac{1}{l}\right) = K^2 c_4(l) \quad \text{and} \quad c_6\left(\frac{1}{l}\right) = K^3 c_6(l),$$

for $K := (2l + t^2)/l^4(t^2 l + 2)$.

In other words, the elliptic curves I_l and $I_{1/l}$ are geometrically isomorphic to each other. They are quadratic twists, according to the extension $\mathbb{F}_q(\sqrt{K})/\mathbb{F}_q$. Consequently, if $(2l + t^2)/(t^2 l + 2) \in \mathbb{F}_q$ is a non-square then I_l and $I_{1/l}$ together have exactly $2(q+1)$ points.

Sixth step: reparametrization. We reparametrize according to the Möbius transformation $\mathbf{P}^1 \to \mathbf{P}^1$, $l \mapsto s := (2l + t^2)/(t^2 l + 2)$. This is not a constant map, for any value of t. Indeed, the determinant of the corresponding 2×2-matrix is $4 - t^4 = (2 - t^2)(2 + t^2) \neq 0$. The inverse transformation is given by $s \mapsto l := (-2s + t^2)/(t^2 s - 2)$.

Write I' for the fibration, defined by $I'_s := I_l$. Then the bad fibers are located at $s = -1, \infty, t^2/2, 2/t^2$. The correspondence $l \mapsto 1/l$ goes over into

$$s = \frac{2l + t^2}{t^2 l + 2} \mapsto \frac{2/l + t^2}{t^2/l + 2} = \frac{2 + t^2 l}{t^2 + 2l} = \frac{1}{s}.$$

Thus, for $s \neq -1, t^2/2, 2/t^2 \in \mathbb{F}_q^*$ a non-square, the fibers I'_s and $I'_{1/s}$ together have exactly $2(q+1)$ points.

Seventh step: pairing the squares I. It remains to consider the fibers for $s \in \mathbb{F}_q^*$, $s \neq -1$, a square and for $s = 0$. For these, $I'_s \cong I'_{1/s}$, except for $s = 0$. There are $4n + 2$ such fibers, for $q = 8n + 3$ as well as for $q = 8n + 5$.

It turns out that $j'(s_2) = j'(s_1)$, for $s_1 = a^2$ and $s_2 = (a-1)^2/(a+1)^2$. More precisely,

$$c'_4(s_2) = F^2 c'_4(s_1) \quad \text{and} \quad c'_6(s_2) = F^3 c'_6(s_1),$$

for

$$F := 8\,\frac{(a+1)^2(a^2 - 2/t^2)^4}{(a^2 - ((2t^2 + 4)/(t^2 - 2))a + 1)^4}.$$

We observe here that the denominator never vanishes for $t \neq 0$, In fact, the discriminant of the quadratic polynomial is equal to $32t^2/(t^2 - 2)^2$, which is always a non-square. As 8 is a non-square, we see that F is a non-square as long as $F \neq 0$, which happens to be true for $a \neq -1$.

In other words, for $a \neq -1$, the elliptic curves I'_{s_1} and I'_{s_2} are non-trivial quadratic twists of each other. This shows that $\#I'_{s_1}(\mathbb{F}_q) + \#I'_{s_2}(\mathbb{F}_q) = 2(q+1)$.

Eighth step: pairing the squares II. In particular, we have $\#I'_1(\mathbb{F}_q) + \#I'_0(\mathbb{F}_q) = 2(q+1)$. For the other $4n$ fibers, we argue as follows. The group $V := \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ operates on $\mathbf{P}^1(\mathbb{F}_q)$ via $e_1 \cdot a := -a$ and $e_2 \cdot a := 1/a$. The orbits are of size four, except for $\{0, \infty\}$, $\{1, -1\}$, and, possibly, $\{i, -i\}$. The map $I\colon \mathbf{P}^1(\mathbb{F}_q) \to \mathbf{P}^1(\mathbb{F}_q), a \mapsto (a-1)/(a+1)$, is compatible with the operation of V in the sense that $e_1 \cdot I(a) = I(e_2 \cdot a)$ and $e_2 \cdot I(a) = I(e_1 \cdot a)$.

https://doi.org/10.1112/S1461157014000199 Published online by Cambridge University Press

Therefore, I defines a mapping $\overline{I}\colon \mathbf{P}^1(\mathbb{F}_q)/V \to \mathbf{P}^1(\mathbb{F}_q)/V$ from the orbit set to itself. One easily sees that $I(I(a)) = e_1 e_2 \cdot a$. That is, $\overline{I}$ is actually an involution. Solving the equations $(a-1)/(a+1) = \pm a$ and $(a-1)/(a+1) = \pm 1/a$, utilizing the fact that 2 is a non-square, we find that I has no fixed points, except for the possible orbit $\{i, -i\}$.

Accordingly, $J\colon a^2 \mapsto ((a-1)/(a+1))^2$ defines an involution of the squares in $\mathbf{P}^1(\mathbb{F}_q)$ modulo the equivalence relation generated by $x \sim 1/x$. The only possible fixed point of J is $\{-1\}$. Further, $J(\{0,\infty\}) = \{1\}$.

As a consequence, we see that the squares $x \in \mathbb{F}_q^*$, different from ± 1, decompose into sets $\{a^2, 1/a^2, ((a-1)/(a+1))^2, ((a+1)/(a-1))^2\}$ of exactly four elements. The assertion follows immediately from this. □

Remark 6.4. If $t^2 = -2$ then the same result is true. For $t = 0$, however, one has $\#V(\mathbb{F}_q) = q^2 + 2q + 1$, while, for $t = \infty$, $\#V(\mathbb{F}_q) = q^2 + 1$. Only minor modifications of the argument are necessary. The case $t^2 = -2$ is actually simpler, as then $K = -1$ is constant and easily seen to be a non-square. In each case, there are exactly four singular $\mathbb{F}_q$-rational fibers.

Remarks 6.5. (i) Elliptic $K3$ surfaces generally have 24 singular fibers. In our case, I_{-1} and I_{-2/t^2} are of Kodaira type $\mathbf{I}_0^*$, thus being of multiplicity six. The other six singular fibers, four of which are defined only over $\mathbb{F}_{q^2}$, are of Kodaira type $\mathbf{I}_2$ and multiplicity two.

(ii) The symmetry under $l \leftrightarrow 1/l$ is enforced by the construction. In fact, consider the double cover of $\mathbf{P}^2$, branched over the union of the four lines $z = a_1 x$, $z = a_2 x$, $z = b_1 y$, and $z = b_2 y$. The fiber for $y : x = l$ has branch points at $a_1, a_2, b_1 l, b_2 l$, which is a quadruple projectively equivalent to $a_1, a_2, K b_1/l, K b_2/l$, for $K := a_1 a_2 / b_1 b_2$. For our fibration, independently of the parameter t, we have $K = (q_2(1,0)/q_2(0,1)) : (q_1(1,0)/q_1(0,1)) = 1$.

The twist factor is $q_3(1, K/l)/q_3(1,l)$. This expression would be fractional-quadratic, in general, but is fractional-linear in our case.

(iii) We found the second symmetry, which allowed us to pair the squares, by looking at the factorizations of the rational functions $j(l) - C$. It seems to be very specific for the particular fibrations, occurring in the proof of Theorem 6.3.

Theorem 6.6 (A family of $K3$ surfaces with real multiplication). *Let $t \in \mathbb{Q}$ be such that $\nu_{17}(t-1) > 0$ and $\nu_{23}(t-1) > 0$. Then the $K3$ surface $X^{(2,t)}$ has geometric Picard rank 16 and real multiplication by $\mathbb{Q}(\sqrt{2})$.*

Proof. We proved $\#X_p^{(2,t)}(\mathbb{F}_p) \equiv 1 \pmod p$ for all primes $p \equiv 3, 5 \pmod 8$, $p > 3$, in Theorem 6.3. By Lemma 6.1, this guarantees that $X^{(2,t)}$ has real or complex multiplication by a number field E.

Further, all the surfaces $X^{(2,t)}$ considered coincide modulo 17 and modulo 23, these two primes being good. Counting points, one finds $\#X_{17}^{(2,t)}(\mathbb{F}_{17^i}) = 313$, 83 881, and 24 160 345, as well as $\#X_{23}^{(2,t)}(\mathbb{F}_{23^i}) = 547$, 280 729, and 148 114 771, for $i = 1, 2, 3$. The characteristic polynomials of Frob_{17} and Frob_{23} turn out to be

$$\chi_{17}^{\mathrm{tr}}(Z) = Z^4 + 28Z^3 + 646Z^2 + 8092Z + 83521$$
$$\chi_{23}^{\mathrm{tr}}(Z) = Z^4 + 52Z^3 + 1702Z^2 + 27508Z + 279841,$$

both being irreducible. In particular, $\mathrm{rk}\,\mathrm{Pic}(X_{\overline{\mathbb{F}}_{17}}^{(2,t)}) = \mathrm{rk}\,\mathrm{Pic}(X_{\overline{\mathbb{F}}_{23}}^{(2,t)}) = 18$. Applications of the Artin–Tate formula [34, Theorem 6.1] show

$$\mathrm{disc}\,\mathrm{Pic}(X_{\overline{\mathbb{F}}_{17}}^{(2,t)}) \in (2 \bmod (\mathbb{Q}^*)^2) \quad \text{and} \quad \mathrm{disc}\,\mathrm{Pic}(X_{\overline{\mathbb{F}}_{23}}^{(2,t)}) \in (14 \bmod (\mathbb{Q}^*)^2).$$

https://doi.org/10.1112/S1461157014000199 Published online by Cambridge University Press

From this information, one deduces that $\operatorname{rk}\operatorname{Pic}(X^{(2,t)}_{\overline{\mathbb{Q}}}) = 16$ or 17. If the rank was 17 then [4, Theorem 1, together with Remark 2] shows that $\operatorname{rk}\operatorname{Pic}(X^{(2,t)}_{\overline{\mathbb{Q}}}) \leqslant \operatorname{rk}\operatorname{Pic}(X^{(2,t)}_{\overline{\mathbb{F}}_{17}}) - [E:\mathbb{Q}]$, a contradiction as the right-hand side is at most 16.

Our next assertion is that $[E:\mathbb{Q}] = 2$. As $\dim T = 6$, the potential alternative degrees would be 3 or 6. In the first case, E is certainly totally real. In the second case, in view of [47, Remark 1.5.3(c)], E must be CM. In both cases, there is a totally real, cubic number field E', contained in $\operatorname{End}(T)$.

For l a prime that is inert in E', T_l carries the structure of a vector space over the field $E' \otimes_{\mathbb{Q}} \mathbb{Q}_l$. Further, there is a constant f such that $(\operatorname{Frob}_p)^f$ is an $E' \otimes_{\mathbb{Q}} \mathbb{Q}_l$-linear map, for every prime $p \neq l$. This, however, implies that the number of eigenvalues of $(\operatorname{Frob}_p)^f$, considered as a $\mathbb{Q}_l$-linear map, that are roots of unity multiplied by p, is a multiple of 3. The calculations shown above for $p = 17$ and $p = 23$ clearly disagree with that.

It remains to determine the quadratic number field E exactly. For this, an easy computation reveals that the Galois group of $\chi^{\mathrm{tr}}_{17}(Z) = Z^4 + 28Z^3 + 646Z^2 + 8092Z + 83\,521$ is cyclic of order four. In particular, variant (i) of Theorem 4.9 applies, showing that χ^{tr}_{17} splits over E into two conjugate factors. But $\mathbb{Q}(\sqrt{\operatorname{disc}\chi^{\mathrm{tr}}_{17}})$ is the only quadratic subfield of the splitting field of χ^{tr}_{17}. A direct calculation yields, finally, that $\operatorname{disc}\chi^{\mathrm{tr}}_{17} = 2^{29} \cdot 17^6$. □

Appendix. *The analytic approach*

Proposition A.1. *Let T be a $\mathbb{Q}$-vector space of dimension six, equipped with a non-degenerate symmetric, bilinear pairing $\langle\,.\,,.\rangle\colon T \times T \to \mathbb{Q}$ of discriminant $(1 \bmod (\mathbb{Q}^*)^2)$ and $\varphi\colon T \to T$ be a self-adjoint endomorphism such that $\varphi \circ \varphi = [d]$.*

Then $d \in \mathbb{Q}$ is a sum of two rational squares.

Proof. The proposition is immediate when d is a square. Thus, assume that d is a non-square. The assumptions on φ imply that $\varphi_{\mathbb{Q}(\sqrt{d})}$ is diagonalizable. For the eigenvalues $\pm\sqrt{d}$, the eigenspaces, which we will denote by T_+ and T_-, must both be three-dimensional. As φ is self-adjoint, they are perpendicular to each other.

In particular, the pairings $\langle\,.\,,.\rangle|_{T_+}$ and $\langle\,.\,,.\rangle|_{T_-}$ are non-degenerate, too. We may choose an orthogonal system $\{x_1, x_2, x_3\} \subset T_+$ such that $\langle x_i, x_i\rangle =: a_i \neq 0$, for $i = 1, 2, 3$. Then the real conjugates $x'_1, x'_2, x'_3 \in T_-$ also form an orthogonal system, and one has $\langle x'_i, x'_i\rangle = a'_i \neq 0$.

From this, one finds an orthogonal decomposition $T = T_1 \oplus T_2 \oplus T_3$, defined over $\mathbb{Q}$, when putting

$$T_i := \operatorname{span}(x_i + x'_i, \sqrt{d}\,(x_i - x'_i)).$$

The discriminant of T_i is in the class of

$$\det\begin{pmatrix} a_i + a'_i & \sqrt{d}\,(a_i - a'_i) \\ \sqrt{d}\,(a_i - a'_i) & d(a_i + a'_i) \end{pmatrix} = d[(a_i + a'_i)^2 - (a_i - a'_i)^2] = 4da_ia'_i = 4dN_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(a_i)$$

modulo squares. Consequently, $\operatorname{disc} T = ((4d)^3 N_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(a_1a_2a_3) \bmod (\mathbb{Q}^*)^2)$. By our assumption about $\operatorname{disc} T$, this implies that d is a norm from $\mathbb{Q}(\sqrt{d})$.

As $(-d)$ is clearly a norm, we conclude that (-1) must be a norm from $\mathbb{Q}(\sqrt{d})$, too. That is, $-1 = a^2 - db^2$ for suitable $a, b \in \mathbb{Q}$. Therefore, d is a sum of two squares. □

Remark A.2 (cf. [19, Example 3.4]). Suppose $T \cong \mathbb{Q}^6$ and that $\langle\,.\,,.\rangle$ is the bilinear form defined by the matrix $\operatorname{diag}(1, 1, -1, -1, -1, -1)$. Then, for every $d \in \mathbb{Q}$ being a sum of two squares, there exists a self-adjoint endomorphism $\varphi\colon T \to T$ such that $\varphi \circ \varphi = [d]$.

Indeed, decompose T orthogonally as $\mathbb{Q}^2 \oplus \mathbb{Q}^2 \oplus \mathbb{Q}^2$ such that, on each summand, the bilinear form is given by either $\operatorname{diag}(1, 1)$ or $\operatorname{diag}(-1, -1)$. Then define φ component-wise by

https://doi.org/10.1112/S1461157014000199 Published online by Cambridge University Press

taking the matrix $\left(\begin{smallmatrix} u & v \\ v & -u \end{smallmatrix}\right)$, for $d = u^2 + v^2$, three times. The symmetry of the matrix implies that φ is self-adjoint and $\varphi \circ \varphi = [d]$ is obvious.

THEOREM A.3. *Let $d \in \mathbb{Q}$ be a non-square.*

(i) *If d is not a sum of two squares then there is no weight-2 Hodge structure of dimension six, having a polarization of discriminant $(1 \bmod (\mathbb{Q}^*)^2)$ and an endomorphism algebra containing $\mathbb{Q}(\sqrt{d})$.*

(ii) *Suppose that d is a sum of two squares. Then there exists a one-dimensional family of polarized, six-dimensional weight-2 Hodge structures of $K3$ type, having the underlying quadratic space $(\mathbb{Q}^6, \operatorname{diag}(1, 1, -1, -1, -1, -1))$ and real multiplication by $\mathbb{Q}(\sqrt{d})$.*

Proof. (i) This follows immediately from Proposition A.1; cf. [47, Theorem 1.6(a) and Theorem 1.5.1].

(ii) To convert $T := (\mathbb{Q}^6, \operatorname{diag}(1, 1, -1, -1, -1, -1))$ into a weight-2 Hodge structure of $K3$ type, one has to select a one-dimensional isotropic subspace $H^{2,0} \subset T_{\mathbb{C}}$ such that $\overline{H^{2,0}}$ is not perpendicular to $H^{2,0}$. This will automatically fix $H^{0,2} := \overline{H^{2,0}}$ and $H^{1,1} := (H^{2,0} + \overline{H^{2,0}})^{\perp}$.

In addition, we choose the endomorphism $\varphi\colon T \to T$ constructed in Remark A.2. By construction, $\varphi_{\mathbb{C}}$ commutes with complex conjugation on $T_{\mathbb{C}}$. Furthermore, as $\varphi_{\mathbb{C}}$ is self-adjoint and fulfills $\varphi_{\mathbb{C}} \circ \varphi_{\mathbb{C}} = [d]$, it respects orthogonality. Therefore, $\varphi_{\mathbb{C}}(H^{2,0}) \subseteq H^{2,0}$ alone will be sufficient for φ to cause real multiplication.

To ensure this, let us take $H^{2,0} \subset T_{\mathbb{C},+}$. The eigenspace $T_{\mathbb{C},+}$ has a real basis, given by $e_i - ((u - \sqrt{d})/v)e_{i+1}$, for $i = 1, 3, 5$. In this basis, the pairing $\langle\,.\,,.\rangle|_{T_{\mathbb{C},+}}$ is given by the non-degenerate matrix

$$\operatorname{diag}\big(1 + (\tfrac{u-\sqrt{d}}{v})^2, -1 - (\tfrac{u-\sqrt{d}}{v})^2, -1 - (\tfrac{u-\sqrt{d}}{v})^2\big),$$

which is indefinite. Consequently, on $\mathbf{P}(T_{\mathbb{C},+}) \cong \mathbf{P}^2$, the condition $\langle x, x\rangle = 0$ defines a conic C and, on this conic, $\langle x, \overline{x}\rangle \neq 0$ is fulfilled on a dense open subset. □

REMARK A.4. Consider the four-dimensional family of $K3$ surfaces that are given as desingularizations of the double covers of $\mathbf{P}^2$, branched over the union of six lines. Then $\operatorname{rk} \operatorname{Pic}(\mathfrak{X}) \geqslant 16$ and we are particularly interested in the surfaces for which equality occurs.

In any case, the pull-back of a general line and the 15 exceptional curves generate a sub-Hodge structure P' of dimension 16. The symmetric, bilinear form on P' is given by the matrix $\operatorname{diag}(2, -2, \ldots, -2)$. Indeed, the exceptional curves have self-intersection number (-2) [2, Proposition VIII.13(i)]. According to [38, Chapter IV, Theorem 9], there is an isometry $P' \cong (\mathbb{Q}^{16}, \operatorname{diag}(1, -1, \ldots, -1))$.

COROLLARY A.5. *Let $d \in \mathbb{Q}$ be a non-square being the sum of two squares. Then there exists a one-dimensional family of $K3$ surfaces over $\mathbb{C}$, the generic member of which has Picard rank 16 and real multiplication by $\mathbb{Q}(\sqrt{d})$.*

Proof. As a quadratic space, $H = H^2(\mathfrak{X}, \mathbb{Q})$ is the same for all $K3$ surfaces. One has $H \cong (\mathbb{Q}^{22}, \operatorname{diag}(1, 1, 1, -1, \ldots, -1))$. By [1, Corollary 14.2], cf. [42, Chapter IX, Theorem 4], there exists a complex-analytic $K3$ surface $\mathfrak{X}$ for every choice of a one-dimensional subspace $\operatorname{span}(x) \subset H_{\mathbb{C}}$ fulfilling $\langle x, x\rangle = 0$ and $\langle x, \overline{x}\rangle > 0$.

We choose $P' \subset H_{\mathbb{C}}$ as in Remark A.4, put $T' := (P')^{\perp}$, and restrict considerations to subspaces $\operatorname{span}(x) \subset T' \subset H_{\mathbb{C}}$. By the classification of the quadratic forms over $\mathbb{Q}$ [38, Chapter IV, § 3], we have $T' \cong (\mathbb{Q}^6, \operatorname{diag}(1, 1, -1, -1, -1, -1))$.

Therefore, Theorem A.3 guarantees the existence of a one-dimensional family of subspaces $\operatorname{span}(x) \subset T'$ such that $\langle x, x\rangle = 0$ and $\langle x, \overline{x}\rangle \neq 0$. The construction given shows that the first condition actually defines a conic C and that $\langle x, \overline{x}\rangle > 0$ is satisfied on a non-empty open subset of C.

https://doi.org/10.1112/S1461157014000199 Published online by Cambridge University Press

We still have to show that, generically, $\operatorname{rk}\operatorname{Pic}(\mathfrak{X}) = 16$. For this, observe that by the Lefschetz theorem on $(1,1)$-classes Picard rank 16 is equivalent to $\mathbb{Q}^6 \cap H^{1,1} = 0$. To investigate this condition, let $0 \neq v = (v_1, \ldots, v_6) \in \mathbb{Q}^6$ be any vector. The inclusion $v \in H^{1,1}$, for a particular choice of x, implies that $v \in \operatorname{span}(x)^\perp$. That is,

$$v_1x_1 + v_2x_2 - v_3x_3 - \ldots - v_6x_6 = 0.$$

This hyperplane meets the conic C in at most two points. Indeed, the plane $\mathbf{P}(T_{\mathbb{C},+})$ is not contained in any $\mathbb{Q}$-rational hyperplane, as an inspection of the base vectors given above immediately shows. In total, there are only countably many exceptions, for which $\operatorname{rk}\operatorname{Pic}(\mathfrak{X}) > 16$. □

References

1. W. Barth, C. Peters and A. van de Ven, *Compact complex surfaces* (Springer, Berlin, Heidelberg, New York, Tokyo, 2004).

2. A. Beauville, ‘Surfaces algébriques complexes’, Astérisque 54 (Société Mathématique de France, Paris, 1978).

3. P. Berthelot and A. Ogus, *Notes on crystalline cohomology* (Princeton University Press, Princeton, 1978).

4. F. Charles, ‘On the Picard number of $K3$ surfaces over number fields’, *Algebra Number Theory* 8 (2014) 1–17.

5. F. Charles, ‘The Tate conjecture for $K3$ surfaces over finite fields’, *Invent. Math.* 194 (2013) 119–145.

6. D. A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, class field theory and complex multiplication* (John Wiley & Sons, New York, 1989).

7. P. Deligne, ‘Théorie de Hodge II’, *Publ. Math. Inst. Hautes Études Sci.* 40 (1971) 5–57.

8. P. Deligne, ‘La conjecture de Weil I’, *Publ. Math. Inst. Hautes Études Sci.* 43 (1974) 273–307.

9. J. D. Dixon and B. Mortimer, *Permutation groups*, Graduate Texts in Mathematics 163 (Springer, New York, 1996).

10. N. Elkies and A. Kumar, ‘$K3$ surfaces and equations for Hilbert modular surfaces’, Preprint, 2012, arXiv:1209.3527.

11. A.-S. Elsenhans and J. Jahnel, ‘$K3$ surfaces of Picard rank one and degree two’, *Algorithmic number theory (ANTS 8)*, Lecture Notes in Computer Science 5011 (Springer, Berlin, 2008) 212–225.

12. A.-S. Elsenhans and J. Jahnel, ‘On Weil polynomials of $K3$ surfaces’, *Algorithmic number theory (ANTS 9)*, Lecture Notes in Computer Science 6197 (Springer, Berlin, 2010) 126–141.

13. A.-S. Elsenhans and J. Jahnel, ‘Kummer surfaces and the computation of the Picard group’, *LMS J. Comput. Math.* 15 (2012) 84–100.

14. A.-S. Elsenhans and J. Jahnel, ‘On the computation of the Picard group for certain singular quartic surfaces’, *Math. Slovaca* 63 (2013) 215–228.

15. G. Faltings, ‘p-adic Hodge theory’, *J. Amer. Math. Soc.* 1 (1988) 255–299.

16. T. Fisher, ‘The invariants of a genus one curve’, *Proc. Lond. Math. Soc.* 97 (2008) 753–782.

17. F. Fité, K. Kedlaya, V. Rotger and A. V. Sutherland, ‘Sato–Tate distributions and Galois endomorphism modules in genus 2’, *Compos. Math.* 148 (2012) 1390–1442.

18. A. Grothendieck, *Fondements de la Géométrie Algébrique (FGA)*, Séminaire Bourbaki 149, 182, 190, 195, 212, 221, 232, 236 (Paris, 1957–62).

19. B. van Geemen, ‘Real multiplication on $K3$ surfaces and Kuga-Satake varieties’, *Michigan Math. J.* 56 (2008) 375–399.

20. M. Hall Jr., *Combinatorial theory* (Blaisdell Publishing Co., Waltham, Toronto, London, 1967).

21. M. Harris, N. Shepherd-Barron and R. Taylor, ‘A family of Calabi-Yau varieties and potential automorphy’, *Ann. of Math.* 171 (2010) 779–813.

22. G. Humbert, ‘Sur les fonctions abéliennes singulières’, *J. Math. Pures Appl. 5e série* 5 (1899) 233–350.

23. L. Illusie, ‘Crystalline cohomology’, *Motives* (Seattle 1991), Proceedings of Symposia in Pure Mathematics 55-1 (American Mathematical Society, Providence, RI, 1994) 43–70.

24. L. Illusie, ‘Perversité et variation’, *Manuscripta Math.* 112 (2003) 271–295.

25. L. Illusie and M. Raynaud, ‘Les suites spectrales associées au complexe de de Rham–Witt’, *Publ. Math. Inst. Hautes Études Sci.* 57 (1983) 73–212.

26. N. M. Katz and B. Mazur, *Arithmetic moduli of elliptic curves*, Annals of Mathematics Studies 108 (Princeton University Press, Princeton, 1985).

27. K. S. Kedlaya and A. V. Sutherland, ‘Hyperelliptic curves, L-polynomials, and random matrices’, *Arithmetic, geometry, cryptography and coding theory*, Contemporary Mathematics 487 (American Mathematical Society, Providence, 2009) 119–162.

https://doi.org/10.1112/S1461157014000199 Published online by Cambridge University Press

28. M. Larsen and R. Pink, 'On l-independence of algebraic monodromy groups in compatible systems of representations', *Invent. Math.* 107 (1992) 603–636.

29. M. Lieblich, D. Maulik and A. Snowden, 'Finiteness of $K3$ surfaces and the Tate conjecture', Preprint, 2011, arXiv:1107.1221.

30. C. Liedtke, 'Lectures on supersingular $K3$ surfaces and the crystalline Torelli theorem', Preprint, 2014, arXiv:1403.2538.

31. R. van Luijk, 'Rational points on $K3$ surfaces', PhD Thesis, Berkeley, 2005.

32. R. van Luijk, '$K3$ surfaces with Picard number one and infinitely many rational points', *Algebra Number Theory* 1 (2007) 1–15.

33. B. Mazur, 'Frobenius and the Hodge filtration (estimates)', *Ann. of Math.* (2) 98 (1973) 58–95.

34. J. S. Milne, 'On a conjecture of Artin and Tate', *Ann. of Math.* (2) 102 (1975) 517–533.

35. J. Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften 322 (Springer, Berlin, 1999).

36. T. Ochiai, 'l-independence of the trace of monodromy', *Math. Ann.* 315 (1999) 321–340.

37. K. M. Pera, 'The Tate conjecture for $K3$ surfaces in odd characteristic', Preprint, 2013, arXiv:1301.6326.

38. J.-P. Serre, *Cours d'arithmétique* (Presses Universitaires de France, Paris, 1970).

39. M. Artin, A. Grothendieck and J.-L. Verdier, *Théorie des Topos et Cohomologie Étale des Schémas* (*Séminaire de Géométrie Algébrique du Bois Marie 1963–1964* (*SGA 4*)), Lecture Notes in Mathematics 269, 270, 305 (Springer, 1972–1973).

40. A. Grothendieck, *Cohomologie l-adique et Fonctions L* (*Séminaire de Géométrie Algébrique du Bois Marie 1965–1966* (*SGA 5*)), Lecture Notes in Mathematics 589 (Springer, 1977).

41. P. Deligne and N. Katz, *Groupes de Monodromie en Géométrie Algébrique, Séminaire de Géométrie Algébrique du Bois Marie 1967–1969* (*SGA 7*), Lecture Notes in Mathematics 288, 340 (Springer, 1973).

42. I. G. Petrovskiĭ and S. M. Nikol'skiĭ (eds), *Algebraic surfaces*, Proceedings of the Steklov Institute of Mathematics 75 (American Mathematical Society, Providence, RI, 1967).

43. J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics 151 (Springer, New York, 1994).

44. S. G. Tankeev, 'Surfaces of $K3$ type over number fields and the Mumford–Tate conjecture', *Izv. Akad. Nauk SSSR Ser. Mat.* 54 (1990) 846–861 (in Russian).

45. S. G. Tankeev, 'Surfaces of $K3$ type over number fields and the Mumford–Tate conjecture II', *Izv. Ross. Akad. Nauk Ser. Mat.* 59 (1995) 179–206 (in Russian).

46. H. Weber, *Lehrbuch der Algebra 2*, Auflage, 3. Band: Elliptische Funktionen und algebraische Zahlen (Friedr. Vieweg & Sohn, Braunschweig, 1908).

47. Yu. G. Zarhin, 'Hodge groups of $K3$ surfaces', *J. reine angew. Math.* 341 (1983) 193–220.

48. Yu. G. Zarhin, 'Transcendental cycles on ordinary $K3$ surfaces over finite fields', *Duke Math. J.* 72 (1993) 65–83.

Andreas-Stephan Elsenhans
School of Mathematics and Statistics F07
University of Sydney
NSW 2006
Australia

stephan@maths.usyd.edu.au

Jörg Jahnel
Département Mathematik
Universität Siegen
Walter-Flex-Straße 3
D-57068 Siegen
Germany

jahnel@mathematik.uni-siegen.de

https://doi.org/10.1112/S1461157014000199 Published online by Cambridge University Press