EXAMPLES OF $K3$ SURFACES WITH REAL MULTIPLICATION

ANDREAS-STEPHAN ELSENHANS AND JÖRG JAHNEL

Abstract. We construct explicit examples of $K3$ 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 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. I.e., $\mathrm{End}(X)\otimes_{\mathbb{Z}}\mathbb{Q}$ is an imaginary quadratic number field.

There is a rich theory about CM elliptic curves, cf. [38, 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 [41, 17. bis 23. Abschnitt]. The situation becomes slightly more complicated, however, when explicit equations are asked for.

Concerning their arithmetic, CM elliptic curves are, may be, even more special. There are only nine imaginary quadratic number fields that may occur as the endomorphism field of a CM elliptic curve, defined over $\mathbb{Q}$, those being of class number one. Further, on all general elliptic curves, the traces of the Frobenii $\mathrm{Frob}_p \in \mathrm{End}(H^1_{\text{ét}}((X_p)_{\overline{\mathbb{F}}_p}, \mathbb{Q}_l))$ have the same statistics [33], while, in the CM case, a different statistics occurs.

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 $\mathbb{Z}$.

But there is more than one way, in which an abelian surface may be exceptional. A new feature is, for example, that real multiplication occurs [18]. Concerning the possible statistics of the Frobenii on an abelian surface over $\mathbb{Q}$, interesting investigations have been undertaken by K. S. Kedlaya and A.V. Sutherland [23].

From the point of view of the classification of algebraic surfaces, there are natural generalizations of elliptic curves to dimension two, other than abelian surfaces. One kind of these is provided by the so-called $K3$ surfaces. Indeed, elliptic curves may be characterized as being the curves with trivial canonical class.

By definition, a $K3$ surface is a simply connected, projective algebraic surface with trivial canonical class. The property of being $K3$ determines the Hodge diamond. The Picard group of a complex $K3$ surface is isomorphic to $\mathbb{Z}^n$, where n may range from 1 to 20.

Key words and phrases. $K3$ surface, real multiplication, Hodge structure, van Luijk's method
2010 Mathematics Subject Classification. Primary 14J28; Secondary 14C30, 11G15, 14C22

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 rational, the minimal resolutions of singular quartics and double covers of $\mathbf{P}^2$, branched over a singular sextic, are $K3$ surfaces, too.

Since $K3$ surfaces do not carry a natural group structure, the endomorphism algebra may no longer be defined naively. One has to take a look at the cohomology. For $\mathfrak{X}$ a $K3$ surface, 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, consisting of the image P of the Picard group under the Chern class map and its orthogonal complement $T := P^\perp$, which is called the transcendental part of H.

The endomorphism algebra $\mathrm{End}(T)$ may only be $\mathbb{Q}$, a totally real number field, or a CM field. If $E \supsetneqq \mathbb{Q}$ is totally real then T (or the underlying $K3$ surface $\mathfrak{X}$) is said to have *real multiplication.* If E is CM then one speaks of *complex multiplication.* Observe the difference to the situation of an elliptic curve or abelian surface, where $\mathrm{End}(H^1(\mathfrak{X}, \mathbb{Q}))$ is considered.

The Kummer surface $\mathrm{Kum}(E_1 \times E_2)$ attached to the product of two elliptic curves E_1 and E_2 has complex multiplication if one of the elliptic curves has. 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 $T_\mathbb{C} \subset H_\mathbb{C}$.

Nonetheless, B. van Geemen showed that there exist $K3$ surfaces of Picard rank 16 that have real multiplication by $\mathbb{Q}(\sqrt{d})$, as soon as d is an odd number being the sum of two squares [17, 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 [17, paragraph 3.1]. We shall give van Geemen's argument in a slightly more general form in an appendix.

1.1. The results. In this note, we will present algorithms to efficiently test a $K3$ surface X over $\mathbb{Q}$ for real multiplication. These do not provide a proof, but only strong evidence. Experiments using the algorithms 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 in this note (4.13 and Theorem 5.2) 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 are highly suspicious to have real multiplication by $\mathbb{Q}(\sqrt{5})$, while the isolated example is highly suspicious to have real multiplication by $\mathbb{Q}(\sqrt{13})$.

Unfortunately, no practical algorithm is known that proves real (or complex) multiplication for a given $K3$ surface. It seems that, in principle, there is such an algorithm under the assumption of the Hodge conjecture, cf. the indications given in the proof of [4, Theorem 6]. But the idea is to inspect the Hilbert scheme of $X \times X$, which is far from realistic to do in practice.

That is why our proof for real multiplication is an indirect one. It is based on showing that $\#X_p(\mathbb{F}_p) \equiv 1 \pmod p$ for all primes $p \equiv 3, 5 \pmod 8$. In order to do this, we analyze in detail one of the elliptic fibrations the surfaces $X^{(2,t)}$ have. We do not have a geometric explanation for the occurrence of real multiplication.

1.2. An application. Van Luijk's method. This 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 $\operatorname{rk}\operatorname{Pic} X_{\overline{\mathbb{Q}}} \leq \operatorname{rk}\operatorname{Pic} X_{\overline{\mathbb{F}}_p}$. Further, the method relies on the hope to find good primes such that

$$\operatorname{rk}\operatorname{Pic} X_{\overline{\mathbb{F}}_p} \leq \operatorname{rk}\operatorname{Pic} X_{\overline{\mathbb{Q}}} + 1\,. \tag{1}$$

To see the method at work, the reader is advised to consult the original papers of R. van Luijk [26, 27] or some of the authors' previous articles [10, 12, 13]. Further, there is the remarkable work of N. Elkies and A. Kumar [9], where 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, F. 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 and $(22 - \operatorname{rk}\operatorname{Pic} X_{\overline{\mathbb{Q}}})/[E\colon\mathbb{Q}]$ is odd. In particular, for the explicit examples of $K3$ surfaces with real multiplication, provided by our experiments, the method is bound to fail in its original form.

For $K3$ surfaces having real multiplication, there is a modification of van Luijk's method, cf. [4, Proposition 18]. We will make use of this in the proof of Theorem 5.2. But, still, things will fail whenever a surface is met that has real multiplication, but for which this fact is not known or cannot be assured.

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

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

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

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

iii) If X is a surface then $H := H^2(X(\mathbb{C}), \mathbb{Q})$ is actually 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. The sub-Hodge structure P and its orthogonal complement T are polarized Hodge structures, too.

Yu. G. Zarhin [42, Theorem 1.6.a) and Theorem 1.5.1] proved that, for T a polarized weight-2 Hodge structure of $K3$ type, $E := \mathrm{End}(T)$ is either a totally real field or a CM field. Thereby, every $\varphi \in E$ operates as a self-adjoint mapping. I.e.,

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

for $\bar{\ }$ the identity map in the case that E is totally real and the complex conjugation in the case that it is a CM field. Observe that, in either case, T carries the structure of an E-vector space. Further, in the case of real multiplication, $\dim_E T = 1$ is impossible [42, Remark 1.5.3.c)].

Remark 2.4. Motivated by the analysis of F. Charles, we are interested in $K3$ surfaces having real multiplication and an odd E-dimensional T. The simplest case one can think of is that $E = \mathbb{Q}(\sqrt{d})$ is real quadratic and $\dim_E T = 3$, i.e. $\dim_{\mathbb{Q}} T = 6$.

3. Some arithmetic consequences of real multiplication

Let X be a $K3$ surface over $\mathbb{Q}$. 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.

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 [34, Exposé XI, Théorème 4.4.iii)]

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

An important feature of the l-adic cohomology theory is that it is acted upon by the absolute Galois group of the base field. I.e., 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, in a way compatible with Betti cohomology, the image P_l of $\mathrm{Pic}(X_{\overline{\mathbb{Q}}}) \otimes_{\mathbb{Z}} \mathbb{Q}_l$ under the Chern map and its orthogonal complement T_l. The image of ϱ_l, and hence the whole of G_l, maps P_l to P_l. Thereby, orthogonality is preserved with respect to the pairing $\langle .\,, . \rangle$. Thus, the algebraic monodromy group G_l must map T_l into itself, as well.

Theorem 3.1 ((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 S. G. Tankeev [39, 40], together with Yu. G. Zarhin's explicit description of the Mumford-Tate group in the case of a $K3$ surface [42, Theorem 2.2.1]. We refer the reader to the original articles and to the discussion in [4, Section 2.2]. $\square$

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 [34, Exp. 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 3.2. *There is a positive integer f such that the following statement is true. For every prime number p and every prime number l, 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 M. Larsen and R. Pink [24, Proposition 6.14]. □

Notation 3.3. For every prime p, choose $l \neq p$ and denote by $\chi_{p^n}^T$ the characteristic polynomial of $(\mathrm{Frob}_p)^n$ on 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 [31, Theorem 3.1]. $\chi_{p^n}^T$ is nothing but the characteristic polynomial of $(\mathrm{Frob}_p)^n$ on the transcendental part of $H^2_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_l)$. It might have zeroes of the form p^n times a root of unity.

We write $\chi_{p^n}^{\mathrm{tr}} \in \mathbb{Q}[Z]$ for the corresponding cofactor. If p is a good prime then, according to the Tate conjecture, $\chi_{p^n}^{\mathrm{tr}}$ is the characteristic polynomial of Frob^n on the transcendental part of $H^2_{\text{ét}}(X_{\overline{\mathbb{F}}_p}, \mathbb{Q}_l)$.

For the remainder of this section, we assume that $E = \mathbb{Q}(\sqrt{d})$, for $d \neq 1$ a square-free integer. I.e., that X has real or complex multiplication by a quadratic number field.

Proposition 3.4. *Let p be a prime number and l be a prime that is ramified or inert in $\mathbb{Q}(\sqrt{d})$. Then the polynomial $\chi_{p^f}^T \in \mathbb{Q}[Z]$ splits as*

$$\chi_{p^f}^{\mathrm{tr}} = g_l g_l^\sigma ,$$

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 3.2, $\varrho_l((\mathrm{Frob}_p)^f)$ 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 $\chi_{p^f}^T = c_l c_l^\sigma$.

c_l may be divisible by polynomials of the form $\Phi(Z/p)$, for Φ a cyclotomic polynomial. The assertion follows, for g_l the cofactor corresponding to the product of all these factors, normalized to a monic polynomial. □

Theorem 3.5. *Let p be a prime of good reduction of the $K3$ surface X over $\mathbb{Q}$, having real or complex multiplication by the quadratic number field $\mathbb{Q}(\sqrt{d})$. Then at least one of the following two statements is true.*

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

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

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 [43], $\chi_p^{\mathrm{tr}} = h^k$, for an irreducible polynomial $h \in \mathbb{Q}[Z]$ and $k \in \mathbb{N}$. The polynomial $h^{(f)}$ having the zeroes x_i^f, for x_i the zeroes of h, might once again be a perfect power. Write $h^{(f)} = \underline{h}^{k'}$, for $\underline{h}$ an irreducible polynomial. Then $\chi^{\rm tr}_{p^f} = \underline{h}^{kk'}$.

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 3.4, $\underline{h}^{kk'} = \chi^{\rm tr}_{p^f}$ splits into two factors conjugate over $\mathbb{Q}_l(\sqrt{d})$, for every l that is not inert 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 $\mathbb{Q}(\sqrt{d})$. [30, Chapter VII, Proposition 13.9] implies that $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{Q}[Z]/(\underline{h})$.

Let now $x_0 \in \overline{\mathbb{Q}}$ be an element having h as its minimal polynomial. Then, clearly, $\mathbb{Q}(x_0^f) \cong \mathbb{Q}[Z]/(\underline{h})$. Altogether, $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{Q}(x_0^f) \subseteq \mathbb{Q}(x_0)$. But, according to Lemma 3.12 below, this is equivalent to h being reducible over $\mathbb{Q}(\sqrt{d})$. It must split into two conjugate factors. $\square$

Remark 3.6. In general, for an irreducible polynomial $h \in \mathbb{Q}[Z]$, the polynomial $h^{(f)}$ may not factor otherwise as into 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 $x_1^f, \ldots, x_r^f$.

Remarks 3.7. i) Let h be an irreducible polynomial such that $\chi^{\rm tr}_p = h^k$ and consider $\mathrm{Gal}(h)$ as a permutation group on the roots of h. As such, it has an obvious block structure $\mathfrak{B} := \big\{\{z, \overline{z}\} \mid h(z) = 0\big\}$ into blocks of size two. Indeed, h is a real polynomial without real roots and every root is of absolute value p. Thus, $\overline{z} = \frac{p^2}{z}$, such that the pairs are respected by the operation of the Galois group.

ii) Assume that k is odd and $d > 0$, i.e., that there is real multiplication. We claim that this causes a second block structure.

Suppose first that variant i) of Theorem 3.5 is true. Then there is the block structure $\mathfrak{B}' := \big\{\{z \mid g(z) = 0\}, \{z \mid g^\sigma(z) = 0\}\big\}$ into two blocks of size $\frac{\deg h}{2}$. 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 3.5 happens to be true then there is the block structure $\mathfrak{B}''$, the blocks in which are formed by the roots of h having their f-th power in common. The mutual refinement of $\mathfrak{B}''$ and $\mathfrak{B}$ is trivial. As k is assumed odd, the blocks 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 3.8. *Suppose that $d > 0$. Then, for every good prime p, $\deg \chi^{\rm tr}_p$ is divisible by 4.*

Proof. Write $\chi^{\rm tr}_p = h^k$. As seen in Remark 3.7.i), $\deg h$ is even, which implies the claim as long as k is even. When k is odd, the observations made in Remark 3.7.ii) show in both cases that $\deg h$ must be divisible by 4. $\square$

Corollary 3.9. *Suppose that $d > 0$. Then, for every good prime $p \geq 5$, we have*

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

Proof. The characteristic polynomial of Frob on $H^2_{\rm \acute{e}t}((X_p)_{\overline{\mathbb{F}}_p}, \mathbb{Q}_l)$ has exactly $22 - \deg \chi^{\rm tr}_p$ zeroes of the form p times a root of unity. Further, the Tate conjecture is known to be true for $K3$ surfaces in characteristic ≥ 5, cf. [5, Corollary 2] and [25]. $\square$

Corollary 3.10. *Suppose that $d > 0$ and let $p \geq 5$ be a good prime number that is inert in $E = \mathbb{Q}(\sqrt{d})$.*

i) *Then X_p is not ordinary.*

ii) *Suppose that $\dim_E T \leq 3$. Then, either $\operatorname{rk}\operatorname{Pic}((X_p)_{\overline{\mathbb{F}}_p}) = 22$ or $\chi_{p^f}^{\mathrm{tr}}$ is the square of an irreducible quadratic polynomial.*

Proof. i) X_p being ordinary would mean that $\chi_{p^f}^{\mathrm{tr}}$ has exactly one zero that is a p-adic unit. Indeed, we have $\dim_{\mathbb{C}} H^{0,2} = 1$ and ordinarity means that the Newton polygon coincides with the Hodge polygon [21, Définition IV.4.12], cf. [19, pages 48f].

By Theorem 3.5, in any case, we can say that there is a factorization $\chi_{p^f}^{\mathrm{tr}} = \underline{g}\underline{g}^\sigma$, 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 being inert, 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 second variant comes from option ii) of Theorem 3.5. The quadratic polynomial appearing is irreducible, as its zeroes are non-reals.

Otherwise, there is a factorization $\chi_p^{\mathrm{tr}} = gg^\sigma$, for some $g \in E[Z]$. We have to show that $\deg g = 0$. Assume the contrary. Then $\deg g = 2$, since $\dim_E T \leq 3$ implies that $\deg g \leq 3$. Further, from Corollary 3.8, we know that $\deg g$ is even.

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 $\min(\nu_p(x_1), \nu_p(x_2)) \leq \nu_p(x_1 + x_2) = \nu_p(-a)$, with equality obviously being true when $\nu_p(x_1) \neq \nu_p(x_2)$. However, $a \in \mathbb{Q}(\sqrt{d})$ implies that $\nu_p(-a)$ is an integer and $\nu_p(x_i) \geq 0$ is well-known. 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. Further, since $x_1/p, x_2/p, x_1^\sigma/p$, and x_2^σ/p are known to be l-adic units for every $l \neq p$, they must be roots of unity. This is a contradiction to the definition of χ_p^{tr}.

If, without restriction, $\nu_p(x_1) = 0$ and $\nu_p(x_2) = 2$ then $\nu_p(x_1^\sigma) = 0$, too. We obtain a contradiction to the classical result that the Newton polygon always runs above the Hodge polygon [28], cf. [3, Theorem 8.39]. □

Corollary 3.11. *Suppose that $\dim_E T \leq 3$. If $\chi_{p^f}^{\mathrm{tr}}$ is the square of a quadratic polynomial, but χ_p^{tr} is not, then $\operatorname{Gal}(\chi_p^{\mathrm{tr}}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

Proof. The assumption implies that $\chi_p^{\mathrm{tr}} = h$ is irreducible of degree four. Further, $\operatorname{Gal}(h)$ 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. □

Lemma 3.12. *Let K be any field, $K(\sqrt{d})/K$ a quadratic field extension, and $h \in K[Z]$ an irreducible polynomial. Then h splits in $K(\sqrt{d})$ if and only if $K(\sqrt{d}) \subseteq K[Z]/(h)$.*

Proof. "$\Longleftarrow$" Let $z_0 \in K[Z]/(h)$ be a zero of h. As $[\mathbb{Q}(z_0) : \mathbb{Q}(\sqrt{d})] = \frac{\deg h}{2}$, the minimal polynomial over $\mathbb{Q}(\sqrt{d})$ is of degree $\frac{\deg h}{2}$ and a factor of h.

"$\Longrightarrow$" 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. $\square$

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

Generalities. According to the Lefschetz trace formula [35, Exposé XII, 6.3 and Exemple 7.3], a $K3$ surface Y over $\mathbb{F}_p$ is non-ordinary if and only if $\#Y(\mathbb{F}_p) \equiv 1 \pmod p$. In particular, non-ordinarity may be tested by counting points only over $\mathbb{F}_p$.

Further, we expect naively that a $K3$ surface X over $\mathbb{Q}$ has non-ordinary reduction at p with a probability of $\frac{1}{p}$. Thus, the number of non-ordinary primes $\leq N$ should be of the order of $\log\log N$. However, for $K3$ surfaces with real multiplication by $\mathbb{Q}(\sqrt{d})$, we expect approximately half the primes to be non-ordinary.

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

Algorithm 4.1 (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 [11, Examples 27 and 28]. It involves to count, in addition, the points on X_{p_0} defined over $\mathbb{F}_{p_0^2}$ and, possibly, those defined over $\mathbb{F}_{p_0^3}$. Factorize the polynomial obtained to determine the factor $\chi^{\text{tr}}_{p_0}$. If $\deg \chi^{\text{tr}}_{p_0} \neq 4$ then terminate. If $\text{Gal}(\chi^{\text{tr}}_{p_0}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $\chi^{\text{tr}}_{p_0}$ is the square of a quadratic polynomial then raise p_0 to the next good and ordinary prime and iterate this step.

iv) Now, one has $\deg \chi^{\text{tr}}_{p_0} = 4$. Further, $\chi^{\text{tr}}_{p_0^f}$ is certainly irreducible, although the value of f is not known to us. Determine the Galois group of $\chi^{\text{tr}}_{p_0}$ and the quadratic subfields of its splitting field. Only one real quadratic field may occur. Put d to be the corresponding radicand.

v) Let p run over all good primes below 300, starting from the lowest. If $\#X_p(\mathbb{F}_p) \not\equiv 1 \pmod p$ for a prime inert in $\mathbb{Q}(\sqrt{d})$ then terminate.

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

Remarks 4.2. i) The reason for restricting in step i) to primes 1 mod 4 is that, otherwise, too many surfaces are found that are suspicious to have complex multiplication by $\mathbb{Q}(\sqrt{-1})$.

ii) 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. That is why we restricted the calculations to primes $p > 40$.

iii) Algorithm 4.1 is, of course, only statistically correct. There is a certain, very low but positive, probability that a $K3$ surface with real multiplication is thrown away in step i).

iv) On the other hand, the algorithm is extremely efficient. The point is that, for the lion's share of the surfaces, it terminates directly after step i). Only for a negligible percentage of the surfaces, the more time-consuming steps ii)-v) have to be carried out.

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.

When testing surfaces for real multiplication by a particular field $\mathbb{Q}(\sqrt{d})$, the following modification of Algorithm 4.1 may be used.

Algorithm 4.3 (Testing a $K3$ surface for real multiplication–deterministic version)**.**
o) In an initialization step, list the first ten primes that are inert in $\mathbb{Q}(\sqrt{d})$.

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 turns out not to be congruent to 1 modulo p then terminate immediately.

ii) Let p run over all good primes below 300, starting from the lowest. If $\#X_p(\mathbb{F}_p) \not\equiv 1 \pmod{p}$ for a prime inert in $\mathbb{Q}(\sqrt{d})$ then terminate.

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

Remarks 4.4. i) This algorithm finds every surface in the sample having real multiplication by $\mathbb{Q}(\sqrt{d})$. It could, in principle, find a few others, too.

ii) One might be afraid that, for some of the surfaces X having real multiplication by $\mathbb{Q}(\sqrt{d})$, there exists an inert prime p of bad reduction, for which $\#X_p(\mathbb{F}_p) \not\equiv 1 \pmod{p}$. These surfaces would be thrown away in step i). However, this does not happen, at least not in our samples.

Lemma 4.5. *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 σ running 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,

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

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

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

too, cf. [34, 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 $H^2_{\text{ét}}(X_{\overline{\mathbb{Q}}_p}, \mathbb{Q}_p)$ [31, Theorem 3.1]. In addition, a main result of p-adic Hodge theory [14, 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 (2) expresses the property that, among the eigenvalues, there is actually no 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 [36, Exposés I, XIII, and XV] applies, as X_p has only isolated singularities [20, 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 [34, 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.

4.6 (Structure of our samples)**.** $K3$ surfaces that are given as desingularizations of the double covers of the projective plane, branched over the union of six lines. Our reason is that this family offers computational advantages, too.

We do not ask all lines to be defined over $\mathbb{Q}$, however, as this seems to be too restrictive. At least, this is what we learned during our experiments. A 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 to be the standard base of $\mathbf{P}^2$. 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. I.e., up to permutation and scaling of the variables.

Algorithm 4.7 (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 4.8 (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

$$\lambda_{x,y} := \sum_{t\in\mathbb{F}_q} \chi(q_1(y,t)q_2(x,t)) \tag{3}$$

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

Strategy 4.9 (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 (3), 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 4.10. 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 4.11 (Detecting real multiplication)**.** We used the point counting algorithm, in the version described in 4.9, within the deterministic Algorithm 4.3, 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 4.1 over all triples (q_1, q_2, q_3) of coefficient height ≤ 12, using the method described in 4.9 for point counting, found the first five surfaces suspicious 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.

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 reduces 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 suspicious for 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. Further, it clearly suggests to use the deterministic version of the algorithm.

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 4.12. 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 let us suspect the following.

Observation–Theorem 4.13. *Let $t \in \mathbb{Q}$ be arbitrary and $X^{(2,t)}$ be the $K3$ surface given by*

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

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 5.3, under some additional restrictions on t. For the cases left out there, similar arguments work. Cf. Remark 5.4 for a few details. $\square$

Observation–Conjecture 4.14. 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 4.15. 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 primes p below 100. It turns out that indeed they show the very particular behaviour, described in Theorem 3.5 and its corollaries.

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

Lemma 5.1. *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 $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\zeta_D))$, 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 $-22 < -r \leq k \leq r < 22$, 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 3.1, this is enough to imply real or complex multiplication. $\square$

Theorem 5.2. *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 will prove $\#X_p^{(2,t)}(\mathbb{F}_p) \equiv 1 \pmod p$ for all primes $p \equiv 3, 5 \pmod 8$, $p > 3$, in Theorem 5.3, below. By Lemma 5.1, 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

$$\begin{aligned}\chi_{17}^{\mathrm{tr}}(Z) &= Z^4 + 28Z^3 + 646Z^2 + 8092Z + 83521 \qquad \text{and}\\ \chi_{23}^{\mathrm{tr}}(Z) &= Z^4 + 52Z^3 + 1702Z^2 + 27508Z + 279841\,,\end{aligned}$$

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 [29, Theorem 6.1] show

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

From this information, one deduces that $\mathrm{rk}\,\mathrm{Pic}(X_{\overline{\mathbb{Q}}}^{(2,t)}) = 16$ or 17. If the rank was 17 then [4, Theorem 1, together with Remark 2] shows that

$$\mathrm{rk}\,\mathrm{Pic}(X_{\overline{\mathbb{Q}}}^{(2,t)}) \leq \mathrm{rk}\,\mathrm{Pic}(X_{\overline{\mathbb{F}}_{17}}^{(2,t)}) - [E : \mathbb{Q}]\,,$$

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, it must be CM. In both cases, there is a totally real, cubic number field E', contained in $\mathrm{End}(T)$.

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 $(\mathrm{Frob}_p)^f$ 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 $(\mathrm{Frob}_p)^f$, 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

$$\chi_{17}^{\mathrm{tr}}(Z) = Z^4 + 28Z^3 + 646Z^2 + 8092Z + 83521$$

is cyclic of order four. In particular, variant i) of Theorem 3.5 applies, showing that χ_{17}^{tr} splits over E into two conjugate factors. But $\mathbb{Q}(\sqrt{\mathrm{disc}\,\chi_{17}^{\mathrm{tr}}})$ is the only quadratic subfield of the splitting field of χ_{17}^{tr}. A direct calculation yields, finally, that $\mathrm{disc}\,\chi_{17}^{\mathrm{tr}} = 2^{29} \cdot 17^6$. $\square$

Theorem 5.3 (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* $\#V(\mathbb{F}_q) = q^2+q+1$.

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 is non-zero, as 32 is not a square. Thus, C_x is a double cover of $\mathbf{P}^1$, ramified at (-1) and $(-\frac{2}{t^2})$. But $-1 \neq -\frac{2}{t^2}$, 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 $l = -1$, $-\frac{2}{t^2}$, 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, $t^4-12t^2+4 \neq 0$, as 32 is a non-square. Further, the quadratic polynomials in l are of the discriminants $\frac{32(t^2-2)^2(t^2+2)^2}{(t^4-12t^2+4)^2}$ and $\frac{128t^2(t^2-2)^2}{(t^4-12t^2+4)^2}$, 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 $C_{-\frac{2}{t^2}}$ 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 $C_0^{\rm ns}$ and $C_\infty^{\rm ns}$ satisfy $w^2 = \frac{1}{4}(t^4-12t^2+4)$, and $w^2 = \frac{t^2}{8}(t^4-12t^2+4)$, respectively. The two equations differ by a factor of $\frac{t^2}{2}$, which is a non-square. Hence, one of the curves $C_0^{\rm ns}$ and $C_\infty^{\rm ns}$ 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

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

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

By Lemma 5.6, $I_l \colon w^2 = x^3 - 27c_4(l)x - 54c_6(l)$ is isomorphic to the Jacobian $\operatorname{Jac} C_l$, for $l \neq -1, -\frac{2}{t^2}, 0, \infty$. 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 $\sum_{l, C_l \text{ smooth}} \#I_l(\mathbb{F}_q) = (q-3)(q+1)$. I.e., that the $(q-3)$ smooth fibers of I have, on average, exactly $(q+1)$ points.

Fifth step. l versus $\frac{1}{l}$.
For the j-invariant $j = \frac{c_4^3}{\Delta}$, one observes that $j(\frac{1}{l}) = j(l)$. More precisely,

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

for $K := \frac{2l+t^2}{l^4(t^2l+2)}$.

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

Sixth step. Reparametrization.
We reparametrize according to the Möbius transformation $\mathbf{P}^1 \to \mathbf{P}^1$, $l \mapsto s := \frac{2l+t^2}{t^2l+2}$. 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 $s \mapsto l := \frac{-2s+t^2}{t^2s-2}$.

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

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

Thus, for $s \neq -1, \frac{t^2}{2}, \frac{2}{t^2} \in \mathbb{F}_q^*$ a non-square, the fibers I'_s and $I'_{\frac{1}{s}}$ 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, $I'_s \cong I'_{\frac{1}{s}}$, 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 $s_2 = \frac{(a-1)^2}{(a+1)^2}$. 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

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

We observe here that the denominator never vanishes for $t \neq 0$, In fact, the discriminant of the quadratic polynomial is equal to $\frac{32t^2}{(t^2-2)^2}$, 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 $e_2{\cdot}a := \frac{1}{a}$. The orbits are of size four, except for $\{0, \infty\}$, $\{1, -1\}$, and, possibly, $\{i, -i\}$. The map $I\colon \mathbf{P}^1(\mathbb{F}_q) \to \mathbf{P}^1(\mathbb{F}_q), a \mapsto \frac{a-1}{a+1}$, is compatible with the operation of V in the sense that $e_1 \cdot I(a) = I(e_2 \cdot a)$ and $e_2 \cdot I(a) = I(e_1 \cdot a)$.

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 $I(I(a)) = e_1 e_2 \cdot a$. I.e., $\overline{I}$ is actually an involution. Solving the equations $\frac{a-1}{a+1} = \pm a$ and $\frac{a-1}{a+1} = \pm\frac{1}{a}$, 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, $J\colon a^2 \mapsto (\frac{a-1}{a+1})^2$ defines an involution of the squares in $\mathbf{P}^1(\mathbb{F}_q)$ modulo the equivalence relation generated by $x \sim \frac{1}{x}$. 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 $\{a^2, \frac{1}{a^2}, (\frac{a-1}{a+1})^2, (\frac{a+1}{a-1})^2\}$ of exactly four elements. The assertion follows immediately from this. $\square$

Remark 5.4. 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 5.5. i) Elliptic $K3$ surfaces generally have 24 singular fibers. In our case, I_{-1} and $I_{-\frac{2}{t^2}}$ each have have multiplicity six, while the other six singular fibers, four of which are defined only over $\mathbb{F}_{q^2}$, each have multiplicity two.

ii) The symmetry under $l \leftrightarrow \frac{1}{l}$ 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 $a_1, a_2, \frac{Kb_1}{l}, \frac{Kb_2}{l}$, for $K := \frac{a_1 a_2}{b_1 b_2}$. For our fibration, independently of the parameter t, we have $K = \frac{q_2(1,0)}{q_2(0,1)} : \frac{q_1(1,0)}{q_1(0,1)} = 1$.

The twist factor is $q_3(1, \frac{K}{l})/q_3(1, l)$, which would be fractional-quadratic, in general, 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 5.3.

Lemma 5.6. *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 $\Delta := \frac{c_4^3(l) - c_6^2(l)}{1728}$. 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 [16, Exposé 232, Théorème 3.1]. This is a family of elliptic curves. 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 [15, 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 [22, First main Theorem 5.1.1, together with 2.2.11]. □

Appendix A. Dimension counting

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. Assume the contrary. Then, in particular, 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_-, both must 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

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

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. I.e., $-1 = a^2 - db^2$ for suitable $a, b \in \mathbb{Q}$, such that d is a sum of two squares. □

Remark A.2 (cf. [17, 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 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 a 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 $(\mathbb{Q}^6, \mathrm{diag}(1,1,-1,-1,-1,-1))$ and real multiplication by $\mathbb{Q}(\sqrt{d})$.*

Proof. i) follows immediately from Proposition A.1. Cf. [42, Theorem 1.6.a) and Theorem 1.5.1].

ii) To convert $T := (\mathbb{Q}^6, \mathrm{diag}(1,1,-1,-1,-1,-1))$ 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 $e_i - \frac{u-\sqrt{d}}{v} e_{i+1}$, for $i = 1,3,5$. In this basis, the pairing $\langle\,.\,,.\rangle|_{T_{\mathbb{C},+}}$ is given by the non-degenerate matrix $\mathrm{diag}(1 + (\frac{u-\sqrt{d}}{v})^2, -1 - (\frac{u-\sqrt{d}}{v})^2, -1 - (\frac{u-\sqrt{d}}{v})^2)$, 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. $\square$

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

Anyway, 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 $\mathrm{diag}(2,-2,\ldots,-2)$. Indeed, the exceptional curves have self-intersection number (-2) [2, Proposition VIII.13.i)]. According to [32, Ch. IV, Theorem 9], $P' \cong (\mathbb{Q}^{16}, \mathrm{diag}(1,-1,\ldots,-1))$.

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 $H \cong (\mathbb{Q}^{22}, \mathrm{diag}(1,1,1,-1,\ldots,-1))$. By [1, Corollary 14.2], cf. [37, Ch. IX, Theorem 4], there exists a complex-analytic $K3$ surface $\mathfrak{X}$ for every choice of a one-dimensional subspace $\mathrm{span}(x) \subset H_\mathbb{C}$ 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 $\mathrm{span}(x) \subset T' \subset H_\mathbb{C}$. By the classification of the quadratic forms over $\mathbb{Q}$ [32, Ch. IV, §3], we have $T' \cong (\mathbb{Q}^6, \mathrm{diag}(1,1,-1,-1,-1,-1))$.

Therefore, Theorem A.3 guarantees the existence of a one-dimensional family of subspaces $\mathrm{span}(x) \subset T'$ 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.

We still have to show that, generically, $\mathrm{rk}\,\mathrm{Pic}(\mathfrak{X}) = 16$. For this observe, 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 $v \in \mathrm{span}(x)^\perp$. I.e.,

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

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 $\mathrm{rk}\,\mathrm{Pic}(\mathfrak{X}) > 16$. $\square$

References

[1] Barth, W., Peters, C., and Van de Ven, A.: Compact complex surfaces, *Springer,* Berlin, Heidelberg, New York, Tokyo 2004

[2] Beauville, A.: Surfaces algébriques complexes, Astérisque 54, *Société Mathématique de France,* Paris 1978

[3] Berthelot, P. and Ogus, A.: Notes on crystalline cohomology, *Princeton University Press,* Princeton 1978

[4] Charles, F.: On the Picard number of $K3$ surfaces over number fields, `arXiv:1111.4117`

[5] Charles, F.: The Tate conjecture for $K3$ surfaces over finite fields, `arXiv:1206.4002`

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

[7] Deligne, P.: Théorie de Hodge II, *Publ. Math. IHES* **40** (1971), 5–57

[8] Deligne, P.: La conjecture de Weil I, *Publ. Math. IHES* **43** (1974), 273–307

[9] Elkies, N. and Kumar, A.: $K3$ surfaces and equations for Hilbert modular surfaces, `arXiv:1209.3527`

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

[11] Elsenhans, A.-S. and Jahnel, J.: On Weil polynomials of $K3$ surfaces, in: Algorithmic Number Theory (ANTS 9), Lecture Notes in Computer Science 6197, *Springer,* Berlin 2010, 126–141

[12] Elsenhans, A.-S. and Jahnel, J.: Kummer surfaces and the computation of the Picard group, *LMS Journal of Computation and Mathematics* **15** (2012), 84–100

[13] Elsenhans, A.-S. and Jahnel, J.: On the computation of the Picard group for certain singular quartic surfaces, *Mathematica Slovaca* **63** (2013), 215–228

[14] Faltings, G.: p-adic Hodge theory, *J. Amer. Math. Soc.* **1** (1988), 255–299

[15] Fisher, T.: The invariants of a genus one curve, *Proc. Lond. Math. Soc.* **97** (2008), 753–782

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

[17] van Geemen, B.: Real multiplication on $K3$ surfaces and Kuga-Satake varieties, *Michigan Math. J.* **56** (2008), 375–399

[18] Humbert, G.: Sur les fonctions abéliennes singulières, *J. Math. Pures et Appl.* 5$^\mathrm{e}$ série, **5** (1899), 233–350

[19] Illusie, L.: Crystalline cohomology, in: Motives (Seattle 1991), Proc. Sympos. Pure Math. 55-1, *AMS,* Providence 1994, 43–70

[20] Illusie, L.: Perversité et variation, *Manuscripta Math.* **112** (2003), 271–295

[21] Illusie, L. and Raynaud, M.: Les suites spectrales associées au complexe de de Rham-Witt, *Publ. Math. IHES* **57** (1983), 73–212

[22] Katz, N. M. and Mazur, B.: Arithmetic moduli of elliptic curves, Annals of Mathematics Studies 108, *Princeton University Press,* Princeton 1985

[23] Kedlaya, K. S. and Sutherland, A.V.: Hyperelliptic curves, L-polynomials, and random matrices, in: Arithmetic, geometry, cryptography and coding theory, Contemp. Math. 487, *AMS,* Providence 2009, 119–162

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

[25] Lieblich, M., Maulik, D., and Snowden, A.: Finiteness of $K3$ surfaces and the Tate conjecture, `arXiv:1107.1221`

[26] van Luijk, R.: Rational points on $K3$ surfaces, *Ph.D. thesis,* Berkeley 2005

[27] van Luijk, R.: $K3$ surfaces with Picard number one and infinitely many rational points, *Algebra & Number Theory* **1** (2007), 1–15

[28] Mazur, B.: Frobenius and the Hodge filtration (estimates), *Ann. of Math.* **98** (1973), 58–95

[29] Milne, J. S.: On a conjecture of Artin and Tate, *Ann. of Math.* **102** (1975), 517–533

[30] Neukirch, J.: Algebraic number theory, Grundlehren der Mathematischen Wissenschaften 322, *Springer,* Berlin 1999

[31] Ochiai, T.: l-independence of the trace of monodromy, *Math. Ann.* **315** (1999), 321–340

[32] Serre, J.-P.: Cours d'arithmétique, *Presses Universitaires de France,* Paris 1970

[33] Serre, J.-P.: Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972), 259–331

[34] Artin, M., Grothendieck, A. et Verdier, J.-L. (avec la collaboration de Deligne, P. et Saint-Donat, B.): Théorie des Topos et Cohomologie Étale des Schémas, Séminaire de Géométrie Algébrique du Bois Marie 1963–1964 (SGA 4), Lecture Notes in Math. 269, 270, 305, *Springer,* Berlin, Heidelberg, New York 1972–1973

[35] Grothendieck, A. (avec la collaboration de Bucur, I., Houzel, C., Illusie, L. et Serre, J.-P.): Cohomologie l-adique et Fonctions L, Séminaire de Géométrie Algébrique du Bois Marie 1965–1966 (SGA 5), Lecture Notes in Math. 589, *Springer,* Berlin, Heidelberg, New York 1977

[36] Deligne, P. and Katz, N.: Groupes de Monodromie en Géométrie Algébrique, Séminaire de Géométrie Algébrique du Bois Marie 1967–1969 (SGA 7), Lecture Notes in Math. 288, 340, *Springer,* Berlin, Heidelberg, New York 1973

[37] The members of the seminar of I. R. Šafarevič: Algebraic surfaces, *AMS,* Providence 1965

[38] Silverman, J. H.: Advanced topics in the arithmetic of elliptic curves, Graduate Texts in Mathematics 151, *Springer,* New York 1994

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

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

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

[42] Zarhin, Yu. G.: Hodge groups of $K3$ surfaces, *J. Reine Angew. Math.* **341** (1983), 193–220

[43] Zarhin, Yu. G.: Transcendental cycles on ordinary $K3$ surfaces over finite fields, *Duke Math. J.* **72** (1993), 65-83

School of Mathematics and Statistics F07, University of Sydney, NSW 2006, Sydney, Australia, `http://www.staff.uni-bayreuth.de/~bt270951/`

E-mail address: `stephan@maths.usyd.edu.au`

Département Mathematik, Universität Siegen, Walter-Flex-Str. 3, D-57068 Siegen, Germany, `http://www.uni-math.gwdg.de/jahnel`

E-mail address: `~jjahnel@mathematik.uni-siegen.de`