$K3$ surfaces with real multiplication

Jörg Jahnel

University of Siegen

Providence RI
October 21, 2015

joint work with
Andreas-Stephan Elsenhans (Sydney/Paderborn)

$K3$ surfaces

Definition (abstract definition–classification of algebraic surfaces)

A $K3$ *surface* is a simply connected, projective algebraic surface having a global (algebraic, holomorphic) 2-form without zeroes or poles.

$K3$ surfaces

Definition (abstract definition–classification of algebraic surfaces)

A $K3$ *surface* is a simply connected, projective algebraic surface having a global (algebraic, holomorphic) 2-form without zeroes or poles.

Examples

1. A smooth quartic in $\mathbf{P}^3$.
2. A double cover of $\mathbf{P}^2$, ramified at a smooth sextic curve.

   Sextics with ordinary double points may be taken, too. Then the resolution of singularities is a $K3$ surface.

In this talk, we consider $K3$ surfaces that are double covers of $\mathbf{P}^2$, ramified over six lines in $\mathbf{P}^2$.

Point counting–An experiment

Consider a "random" example and a very particular one

$$S_1\colon\ w^2 = x^6 + 2y^6 + 3z^6 + 5x^2y^4 + 7xy^2z^3 + 3y^5z + x^3z^3$$
$$S_2\colon\ w^2 = (-y^2 + 8yz - 8z^2)(7x^2 + 40xz + 56z^2)(2x^2 + 3xy + y^2)\,.$$

p	$(\#S_1(\mathbb{F}_p) \bmod p)$	$(\#S_2(\mathbb{F}_p) \bmod p)$
2	0	1
3	1	1
5	1	1
7	1	1
11	1	1
13	8	1
17	1	7
19	0	1
23	19	18
29	7	1
31	7	7
37	0	1
41	7	1
43	5	1
47	11	19
53	47	1
59	28	1

p	$(\#S_1(\mathbb{F}_p) \bmod p)$	$(\#S_2(\mathbb{F}_p) \bmod p)$
61	44	1
67	54	1
71	23	34
73	11	0
79	41	27
83	57	1
89	46	3
97	28	52
101	42	1
103	55	28
107	20	1
109	60	1
113	7	51
127	89	121
131	78	1
137	20	105
139	22	1

Point counting–An experiment II

Observations

1. In the “random” example S_1, there is no regularity to be seen.
2. In example S_2, however, we observe that

$$\#S_2(\mathbb{F}_p) \equiv 1 \pmod{p}$$

for all primes $p \equiv 3, 5 \pmod{8}$.

Remarks

- One also has $\#S_2(\mathbb{F}_{41}) \equiv 1 \pmod{41}$, which is purely accidental.
- The bound at 140 is just for presentation, one may easily extend it, at least up to 10000 (D. Harvey).
- The primes $p \equiv 3, 5 \pmod{8}$ are exactly those that are inert in $\mathbb{Q}(\sqrt{2})$.

Recall from the theory of elliptic curves

Fact (An arithmetic consequence of CM)

Let X be an elliptic curve with complex multiplication (CM) by $E = \mathbb{Q}(\sqrt{d})$. Then $\#X(\mathbb{F}_p) \equiv 1 \pmod{p}$ for every prime p that is inert in E.

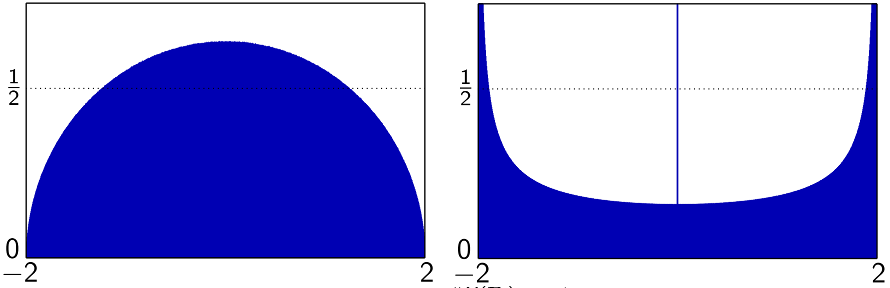

Figure: Distribution of $\frac{\#X(\mathbb{F}_p)-p-1}{\sqrt{p}}$ for $p \to \infty$ for an ordinary elliptic curve (left) and a CM elliptic curve (right)

The spike has area $\frac{1}{2}$ (!!).

Our original motivation–Picard ranks

Fact

Let X be a $K3$ surface over $\mathbb{Q}$ and p a prime of good reduction. Then

$$\operatorname{rk} \operatorname{Pic} X_{\overline{\mathbb{Q}}} \leq \operatorname{rk} \operatorname{Pic} X_{\overline{\mathbb{F}}_p}.$$

Theorem (F. Charles 2012)

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

1. *If X has real multiplication and $(22 - \operatorname{rk} \operatorname{Pic} X_{\overline{\mathbb{Q}}})/[E : \mathbb{Q}]$ is odd then, for every prime p of good reduction,*

$$\operatorname{rk} \operatorname{Pic} X_{\overline{\mathbb{Q}}} + [E : \mathbb{Q}] \leq \operatorname{rk} \operatorname{Pic} X_{\overline{\mathbb{F}}_p}.$$

2. *Otherwise, there exists a prime p of good reduction such that*

$$\operatorname{rk} \operatorname{Pic} X_{\overline{\mathbb{F}}_p} = \operatorname{rk} \operatorname{Pic} X_{\overline{\mathbb{Q}}} \quad \text{or} \quad \operatorname{rk} \operatorname{Pic} X_{\overline{\mathbb{F}}_p} = \operatorname{rk} \operatorname{Pic} X_{\overline{\mathbb{Q}}} + 1\,.$$

[Statistics: Remember E. Costa's talk!]

Hodge structures

Definition (P. Deligne 1971)

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

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

such that $\overline{H^{m,n}} = H^{n,m}$ for every $m, n \in \mathbb{N}_0$, $m + n = i$.

Hodge structures

Definition (P. Deligne 1971)

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

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

such that $\overline{H^{m,n}} = H^{n,m}$ for every $m, n \in \mathbb{N}_0$, $m + n = i$.

Examples

1. 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.
2. 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 $H_P^{0,2} = H_P^{2,0} = 0$.
3. 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.

Real and complex multiplication

Definition

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

Theorem (Yu. Zarhin 1983)

Let T be a polarized weight-2 Hodge structure of $K3$ type.

1. *Then $E := \mathrm{End}(T)$ is either a totally real field or a CM field.*
2. *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 $\overline{}$ the identity map in the case that E is totally real and the complex conjugation in the case that it is a CM field.

3. *If E is totally real then $\dim_E T \geq 2$.*

Real and complex multiplication

Definition

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

Theorem (Yu. Zarhin 1983)

Let T be a polarized weight-2 Hodge structure of $K3$ type.

1. *Then $E := \mathrm{End}(T)$ is either a totally real field or a CM field.*
2. *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 $\overline{}$ the identity map in the case that E is totally real and the complex conjugation in the case that it is a CM field.
3. *If E is totally real then $\dim_E T \geq 2$.*

Definition

If $E \supsetneq \mathbb{Q}$ then one speaks of *real multiplication* when E is totally real and of *complex multiplication* when E is CM.

Real and complex multiplication II

Let X be a $K3$ surface over $\mathbb{C}$. Associated with X, there are

- the polarized weight-2 Hodge structure $H := H^2(X(\mathbb{C}), \mathbb{Q})$,
- its sub-Hodge structure P, given as the image of

$$c_1\colon \operatorname{Pic}(X) \otimes_{\mathbb{Z}} \mathbb{Q} \to H^2(X(\mathbb{C}), \mathbb{Q}),$$

- the orthogonal complement $T := P^{\perp}$ in H. T is a polarized weight-2 Hodge structure of $K3$ type.

Definition

One says that a $K3$ surface X has *real* or *complex multiplication* (*RM* or *CM*), when the Hodge structure T has.

RM/CM on $K3$ surfaces

The difference (Recall)

- For X an elliptic curve, one considers $\mathrm{End}(H)$, for $H := H^1(X(\mathbb{C}), \mathbb{Q})$.
- For X a $K3$ surface, $\mathrm{End}(T)$ is considered, for $T := P^\perp$ the transcendental part of $H^2(X(\mathbb{C}), \mathbb{Q})$.

RM/CM on $K3$ surfaces

The difference (Recall)

- For X an elliptic curve, one considers $\mathrm{End}(H)$, for $H := H^1(X(\mathbb{C}), \mathbb{Q})$.
- For X a $K3$ surface, $\mathrm{End}(T)$ is considered, for $T := P^\perp$ the transcendental part of $H^2(X(\mathbb{C}), \mathbb{Q})$.

Questions

- Can one construct $K3$ surfaces having real/complex multiplication?
- How many $K3$ surfaces have real/complex multiplication? I.e., what is the dimension of the corresponding locus in moduli space?
- Are there $K3$ surfaces defined over $\mathbb{Q}$ that have real/complex multiplication?

One answer (CM is simpler)

If E_1, E_2 are elliptic curves and E_1 has CM then $\mathrm{Kum}(E_1 \times E_2)$ has CM.

An analytic construction

The family we work with

Consider the 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.

Observations

- *four-dimensional:* $\dim((\mathbf{P}^2)^\vee)^6 = 12$, $\dim \mathrm{Aut}(\mathbf{P}^2) = \dim \mathrm{PGL}_3 = 8$
- $\mathrm{rk}\,\mathrm{Pic}(X) \geq 16$*: 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* $\mathrm{diag}(2, -2, \ldots, -2)$. *A direct calculation shows* $P' \cong (\mathbb{Q}^{16}, \mathrm{diag}(1, -1, \ldots, -1))$.
- *Hence,* $T' := (P')^\perp \cong (\mathbb{Q}^6, \mathrm{diag}(1, 1, -1, -1, -1, -1))$.

An analytic construction II

Theorem (van Geemen 2008, E.+J. 2014)

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 $\mathbb{Q}(\sqrt{d})$.

An analytic construction II

Theorem (van Geemen 2008, E.+J. 2014)

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 $\mathbb{Q}(\sqrt{d})$.

The condition that d be a sum of two squares is necessary for surfaces in the four-dimensional family.

Theorem (E.+J. 2014)

Let $T \cong \mathbb{Q}^6$, 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.

An analytic construction III

Remark (CM is simpler)

Let $d < 0$. Then $\langle\sqrt{d}v, v\rangle = \langle v, \overline{\sqrt{d}}v\rangle = -\langle\sqrt{d}v, v\rangle$ implies $\sqrt{d}v \perp v$. Hence disc $T = d\cdot\mathbb{Q}^{*2}$, when dim $T \equiv 2 \pmod 4$.

Thus, only $\mathbb{Q}(\sqrt{-1})$ may occur for the family above. The corresponding surfaces form a 2-dimensional family.

Arithmetic consequences of RM/CM

Choose a prime number l and turn to l-adic cohomology. There is the comparison isomorphism

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

The l-adic cohomology is acted upon by the absolute Galois group of the base field. I.e., there is a continuous representation

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

There is a Chern class homomorphism $c_1\colon \operatorname{Pic}(X_{\overline{\mathbb{Q}}})\otimes_{\mathbb{Z}}\mathbb{Q}_l \hookrightarrow H^2_{\text{ét}}(X_{\overline{\mathbb{Q}}},\mathbb{Q}_l)$. Its image P_l maps exactly onto $P\otimes_{\mathbb{Q}}\mathbb{Q}_l$ under the comparison isomorphism. $T_l := (P_l)^{\perp}$ maps exactly onto $T\otimes_{\mathbb{Q}}\mathbb{Q}_l$.

The operation of $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ maps P_l to itself.

Consequently, $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ maps T_l to itself. Indeed, orthogonality is respected by the operation of $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

Arithmetic consequences of RM/CM II

Notation

1. For every prime p, choose $l \neq p$ and denote by $\chi^T_{p^n}$ 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 (Deligne 1974) or not (Ochiai 1999). One has $\deg \chi^T_{p^n} = 22 - \operatorname{rk}\operatorname{Pic} X_{\overline{\mathbb{Q}}}$.
2. We factorize $\chi^T_{p^n} \in \mathbb{Q}[Z]$ in the form
$$\chi^T_{p^n}(Z) = \chi^{\mathrm{tr}}_{p^n}(Z) \cdot \prod_{k,i} (Z - \zeta_k^i)^{e_{k,i}},$$
for $\zeta_k := \exp(2\pi i/k)$, $e_{k,i} \geq 0$, 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.

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 $\operatorname{rk}\operatorname{Pic} X_{\overline{\mathbb{F}}_p} = \operatorname{rk}\operatorname{Pic} X_{\overline{\mathbb{Q}}}$.

Arithmetic consequences of RM/CM III

Theorem (E.+J. 2014)

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 $E = \mathbb{Q}(\sqrt{d})$. Then at least one of the following two statements is true.

1. *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.
2. *For a certain positive integer f, the polynomial $\chi_{p^f}^{\mathrm{tr}}$ is a square in $\mathbb{Q}[Z]$.*

Arithmetic consequences of RM/CM III

Theorem (E.+J. 2014)

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 $E = \mathbb{Q}(\sqrt{d})$. Then at least one of the following two statements is true.

1. *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.
2. *For a certain positive integer f, the polynomial $\chi_{p^f}^{\mathrm{tr}}$ is a square in $\mathbb{Q}[Z]$.*

Corollary

Suppose that p is inert in E. Then $\#X_p(\mathbb{F}_p) \equiv 1 \pmod{p}$.

Idea of Proof. This uses the Lefschetz trace formula, information on the p-adic nature of the eigenvalues of Frobenius (Mazur 1973, Berthelot/Ogus 1978), and the splitting $\chi_p^{\mathrm{tr}} = gg^{\sigma}$ over $\mathbb{Q}_p(\sqrt{d})$. $\square$

Arithmetic consequences of real multiplication

Corollary

Suppose that $d > 0$, i.e. that X has real multiplication by $E = \mathbb{Q}(\sqrt{d})$. Let p be a prime of good reduction.

1. *Then $\deg \chi_p^{\mathrm{tr}}$ is divisible by 4.*
2. *If $p \geq 3$ then $\operatorname{rk} \operatorname{Pic} X_{\overline{\mathbb{F}}_p} \equiv 2 \pmod 4$.*

Idea of Proof. 1. $\chi_{p^f}^{\mathrm{tr}} = h^2$ or $\chi_p^{\mathrm{tr}} = gg^\sigma$ are real factorizations.
g (resp. h) real polynomial without real roots. Thus, $\deg g$ (or $\deg h$) even.

2. The Tate conjecture is proven for $K3$ surfaces in characteristic ≥ 3 (Lieblich/Maulik/Snowden 2011, Charles 2012, Pera 2012). □

Algorithms

Summary

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

1. If X has RM/CM then $\#X_p(\mathbb{F}_p) \equiv 1 \pmod{p}$ for half the primes.
2. Otherwise, we (naively) expect $\#X_p(\mathbb{F}_p) \equiv 1 \pmod{p}$ for only $O(\log\log N)$ primes below N.

This lets arise the idea to search for explicit examples of $K3$ surfaces having RM/CM **through the arithmetic consequences.** I.e., to generate a huge sample of $K3$ surfaces of Picard rank ≥ 16 and to run the following statistical algorithm on them.

[But, recall, we expect only one-dimensional families with RM in a six-dimensional space of surfaces. And there are also two-dimensional families with CM.]

Algorithms II

Algorithm (Testing a $K3$ surface for RM–statistical version)

1. 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.
2. Put p_0 to be the smallest good and ordinary prime for X.
   [I.e. $\#X_p(\mathbb{F}_{p_0}) \not\equiv 1 \pmod{p_0}$.]
3. Determine the characteristic polynomial of Frob on $H^2_{\text{ét}}((X_{p_0})_{\overline{\mathbb{F}}_{p_0}}, \mathbb{Q}_l)$.
   Factorize the polynomial obtained to calculate the polynomial $\chi^{\text{tr}}_{p_0}$. If $\deg \chi^{\text{tr}}_{p_0} \neq 4$ then terminate.

   Test whether $\chi^{\text{tr}}_{p_0}$ 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 $\text{Gal}(\chi^{\text{tr}}_{p_0})$. If $\text{Gal}(\chi^{\text{tr}}_{p_0}) \cong (\mathbb{Z}/2\mathbb{Z})^2$ then raise p_0 to the next good and ordinary prime and iterate this step. [We wait for D_4, which should be the generic answer.]

Algorithms III

4. Now, $\chi_{p_0}^{\mathrm{tr}}$ is irreducible of degree four. Determine the quadratic subfields of the splitting field of $\chi_{p_0}^{\mathrm{tr}}$. Only one real quadratic field may occur. Put d to be the corresponding radicand.
5. Let p run over all good primes < 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.
6. Output a message saying that X is highly likely to have real multiplication by a field containing $\mathbb{Q}(\sqrt{d})$.

Algorithms IV

Remarks

1. The algorithm is extremely efficient. Step 1 is the only time-critical one. An efficient algorithm for point counting over relatively small prime fields is asked for.
2. The likelihood that a random surface survives step 5 to give a false positive is
$$\prod_{\substack{p \text{ inert in } \mathbb{Q}(\sqrt{d}),\\ p<300}} 1/p < 10^{-60}$$
for small values of d.
3. If one wants to find surfaces that are likely to have CM by $\mathbb{Q}(\sqrt{-1})$ then one has to verify in step 4 that $\chi_{p_0}^{\mathrm{tr}}$ splits over $\mathbb{Q}(\sqrt{-1})$ and, in step 5, that $\#X_p(\mathbb{F}_p) \equiv 1 \pmod{p}$ for all primes $p \equiv 3 \pmod{4}$.

Our samples

Double covers of the projective plane, branched over the union of six lines

We do not ask all lines to be defined over $\mathbb{Q}$, however, as this seems to be too restrictive. [We did not find any RM examples in such samples.]

Compromise

The lines are allowed to form three Galois orbits, each of size two.

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

Our samples II

Algorithm (Counting 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. Finally, we add 1.

Our samples II

Algorithm (Counting 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. Finally, we add 1.

Remark (Counting points above one line)

The number of points above the affine line $L_{x,y}\colon \mathbf{A}^1 \to \mathbf{P}^2$, $t \mapsto (x:y:t)$, is $q + \chi(q_3(x,y))\lambda_{x,y}$, for

$$\lambda_{x,y} := \sum_{t \in \mathbb{F}_q} \chi(q_1(y,t)q_2(x,t))\,. \tag{1}$$

Our samples III

Strategy (Treating a sample of surfaces)

Given three lists of quadratic forms, one for q_1, another for q_2, and third for q_3. To count the points on all surfaces, given by the Cartesian product of the three lists, we perform as follows.

1. 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.
2. Run in an iterated loop over all pairs (q_1, q_2). For each pair, do the following.
   - Using formula (1), 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 $q^2+q+1+\chi(q_3(0,1))\lambda_{0,1}+S_{q_1,q_2,q_3}$.

Our samples IV

Remark (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 $\lambda_{0,1}$.

Our samples IV

Remark (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 $\lambda_{0,1}$.

Remark (Detecting real multiplication)

We used this point counting algorithm within the deterministic algorithm, 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(R)Core(TM)i7-3770 processor. The code was written in plain `C`.

Results

A run over all triples (q_1, q_2, q_3) of coefficient height ≤ 12, found the first five surfaces suspicious to have real multiplication by $\mathbb{Q}(\sqrt{5})$. A sample of more than 10^{11} surfaces was necessary to bring these examples to light!

Observations: One of the three discriminants was that of the quadratic field. The product of the three discriminants was a square.

Incorporated these restrictions to raise the bound to 200.

Results

A run over all triples (q_1, q_2, q_3) of coefficient height ≤ 12, found the first five surfaces suspicious to have real multiplication by $\mathbb{Q}(\sqrt{5})$. A sample of more than 10^{11} surfaces was necessary to bring these examples to light!

Observations: One of the three discriminants was that of the quadratic field. The product of the three discriminants was a square.

Incorporated these restrictions to raise the bound to 200.

Theorem (E.+J. 2014)

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

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

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

Although the family was found experimentally, we have a proof.

Results II

Idea: Work in the elliptic fibration, given by $y : x = l$.

It has exactly four singular fibers, at $l = -1, -\frac{2}{t^2}, 0, \infty$.

The other $(p-3)$ fibers together have exactly $(p-3)(p+1)$ points, due to some deep symmetry.

- $j(F_l) = j(F_{1/l})$, quadratic twists of each other, twist factor $\frac{2l+t^2}{l^4(t^2l+2)}$.
  Thus $\#F_l(\mathbb{F}_p) + \#F_{1/l}(\mathbb{F}_p) = 2(p+1)$, when $\frac{2l+t^2}{t^2l+2}$ is a non-square.
- To pair the other fibers, reparametrize according to $s := \frac{2l+t^2}{t^2l+2}$.
  - Then $l \mapsto \frac{1}{l}$ goes over into $s \mapsto \frac{1}{s}$.
  - Singular fibers at $s = -1, \infty, \frac{t^2}{2}, \frac{2}{t^2}$.
  - Still need to consider the fibers for s a square.

$$j(F'_{a^2}) = j(F'_{\frac{(a-1)^2}{(a+1)^2}})$$

The fibers are quadratic twists of each other. The twist factor is

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

which is always a non-square.

Results III

Theorem (E.+J. 2014)

Let $t \in \mathbb{Q}$ be such that $\nu_{17}(t-1) > 0$ and $\nu_{23}(t-1) > 0$. Then $X^{(2,t)}$ has geometric Picard rank 16 and real multiplication by $\mathbb{Q}(\sqrt{2})$.

Results III

Theorem (E.+J. 2014)

Let $t \in \mathbb{Q}$ be such that $\nu_{17}(t-1) > 0$ and $\nu_{23}(t-1) > 0$. Then $X^{(2,t)}$ has geometric Picard rank 16 and real multiplication by $\mathbb{Q}(\sqrt{2})$.

Idea of Proof. The point count implies that $\varrho_l(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ cannot be Zariski dense in $\mathrm{GO}(T_l, \langle.,.\rangle)$. By the Theorem of Tankeev/Zarhin, there must be real or complex multiplication by a number field $E \supsetneq \mathbb{Q}$.
[Infinitely many congruences for the point count imply RM/CM.]

To prove that the Picard rank is exactly 16, we use reduction modulo 17 and 23 and a modification of van Luijk's method.

Finally, as there are reductions to Picard rank 18, $[E : \mathbb{Q}]$ must divide 4 and 6, hence E is a quadratic number field.

To prove $E = \mathbb{Q}(\sqrt{2})$, we observe that χ_{17}^{tr} splits over $\mathbb{Q}(\sqrt{2})$, but not over any other quadratic number field. $\square$

Results IV

Conjecture

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* $p \equiv 2, 3 \pmod{5}$.

Conjecture

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* $p \equiv 2, 5, 6, 7, 8, 11 \pmod{13}$.

Results V

Remarks

1. 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.
2. 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 the theory above.

   To be concrete, 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 $\mathbb{Q}(\sqrt{13})$.

Results VI

Theorem (E.+J. 2015)

Let $a_1, a_2, a_3, b_1, b_2, b_3 \in \mathbb{Q}$ *be such that*

$$a_1 b_3 + a_2 b_1 - 2a_3 b_1 = 0 \qquad \text{and}$$
$$a_1 b_2 + a_2 b_3 - 2a_3 b_2 = 0$$

and let $X^{(-1;a_1,a_2,a_3,b_1,b_2,b_3)}$ *be the* $K3$ *surface given by*

$$w^2 = xyz(x+y+z)(a_1x + a_2y + a_3z)(b_1x + b_2y + b_3z)$$

Then $\#X_p^{(-1;a_1,a_2,a_3,b_1,b_2,b_3)}(\mathbb{F}_p) \equiv 1 \pmod{p}$*, whenever* $p \equiv 3 \pmod{4}$*.*

Also this family was found experimentally [working with a sample with six rational lines]. It is a second one, for which we have a proof. The style of the proof is similar to that for the family $X^{(2,t)}$.

The base of the family is a degree-6 del Pezzo surface. The generic member should have Picard rank exactly 16 and CM exactly by $\mathbb{Q}(\sqrt{-1})$.

Results VII

Conjecture

The K3 surface given by

$$w^2 = xyz(x^3 - 3x^2z - 3xy^2 - 3xyz + y^3 + 9y^2z + 6yz^2 + z^3)$$

has CM by $\mathbb{Q}(\zeta_9 + \zeta_9^{-1}, i)$.

Conjecture

The K3 surface given by

$$w^2 = xyz(7x^3 - 7x^2y + 49x^2z - 21xyz + 98xz^2 + y^3 - 7y^2z + 49z^3)$$

has CM by $\mathbb{Q}(\zeta_7 + \zeta_7^{-1}, i)$.

Results VII

Conjecture

The K3 surface given by

$$w^2 = xyz(x^3 - 3x^2z - 3xy^2 - 3xyz + y^3 + 9y^2z + 6yz^2 + z^3)$$

has CM by $\mathbb{Q}(\zeta_9 + \zeta_9^{-1}, i)$.

Conjecture

The K3 surface given by

$$w^2 = xyz(7x^3 - 7x^2y + 49x^2z - 21xyz + 98xz^2 + y^3 - 7y^2z + 49z^3)$$

has CM by $\mathbb{Q}(\zeta_7 + \zeta_7^{-1}, i)$.

Thank you!!!