Point counting and real multiplication on K3 surfaces

Andreas-Stephan Elsenhans

Universität Paderborn

September 2016

Joint work with J. Jahnel.

Introduction

Theorem (Hasse) For an elliptic curve, we have

$$|q + 1 - \#E(\mathbb{F}_q)| \leq 2\sqrt{q}$$

Example:
Two elliptic curves

$$E_1 : y^2 = x^3 + x + 3$$
$$E_2 : y^2 = x^3 - 17$$

Introduction

Theorem (Hasse) For an elliptic curve, we have

$$|q + 1 - \#E(\mathbb{F}_q)| \leq 2\sqrt{q}$$

Example:
Two elliptic curves

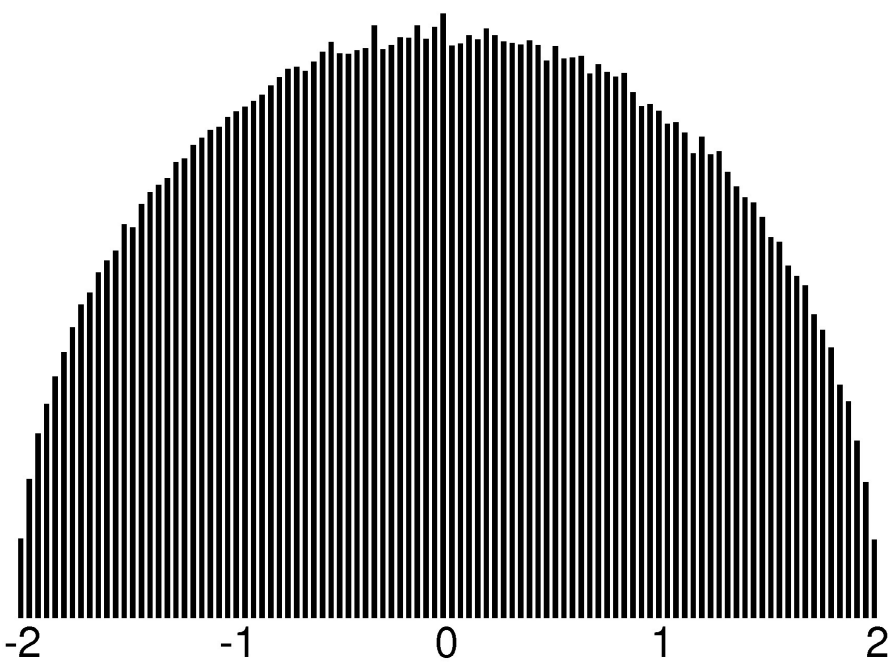
$$E_1 : y^2 = x^3 + x + 3$$
$$E_2 : y^2 = x^3 - 17$$

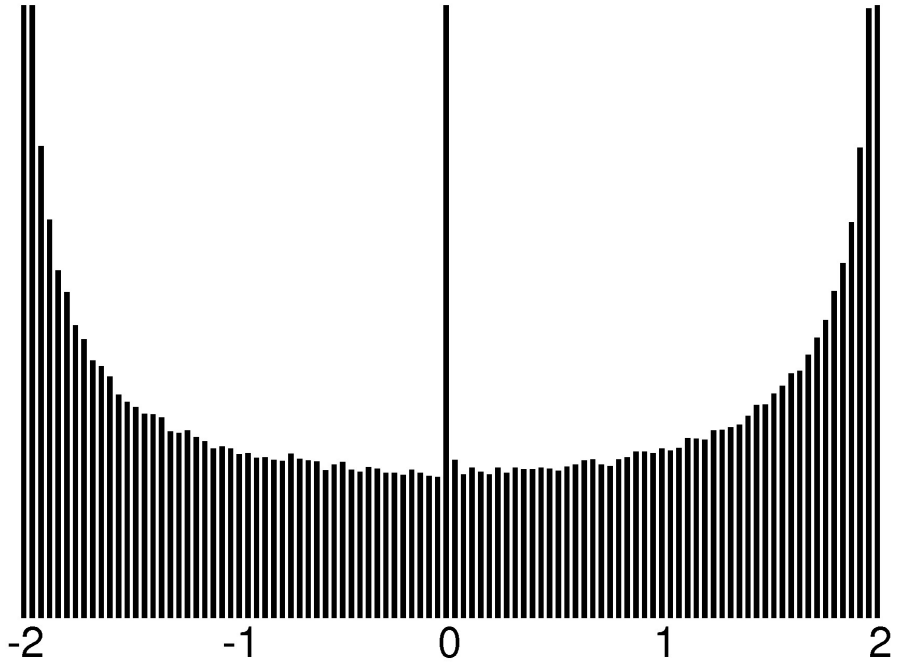
Experiment:
Distribution of

$$\frac{p + 1 - \#E_i(\mathbb{F}_q)}{\sqrt{p}}$$

for all primes $p < 10^7$, $i = 1, 2$. (Normalized Frobenius traces.)

Distribution of normalized Frobenius traces





$$E_1 : y^2 = x^3 + x + 3$$

$$j(E_1) = \frac{55296}{275}$$

$$E_2 : y^2 = x^3 - 17$$

$$j(E_2) = 0$$

(data from 664579 primes, 100 buckets)

Connections with cohomology

Theorem (Lefschetz trace formula)
V a n-dimensional proper variety with good reduction at p.

$$\#V(\mathbb{F}_p) = \sum_{i=0}^{2n} (-1)^i \mathrm{Tr}(\mathrm{Frob}_p \mid \mathrm{H}^i_{et}(V, \mathbb{Q}_\ell))$$

Example
For an elliptic curve E we know that H^1 is of dimension 2.

$$\#E(\mathbb{F}_p) = 1 + p - \mathrm{Tr}(\mathrm{Frob}_p \mid \mathrm{H}^1_{et}(E, \mathbb{Q}_\ell)) = 1 + p - \lambda - \overline{\lambda}$$

with λ of absolute value $\sqrt{p}$. (Frobenius eigenvalue)

Properties of Frobenius eigenvalues

Theorem (Deligne-Weil)
The Frobenius eigenvalues of Frob_p on H^i_{et} are algebraic integers of absolute value $p^{i/2}$.

Properties of Frobenius eigenvalues

Theorem (Deligne-Weil)
The Frobenius eigenvalues of Frob_p on H^i_{et} are algebraic integers of absolute value $p^{i/2}$.

Special case: CM elliptic curve
$E/\mathbb{Q}$ elliptic curve with complex multiplication by $\mathbb{Q}(\sqrt{-d})$.
p a prime of good reduction.

$$p \text{ inert in } \mathbb{Q}(\sqrt{-d}) \Longrightarrow \text{Frobenius eigenvalues } \pm\sqrt{-p}$$
$$p \text{ split in } \mathbb{Q}(\sqrt{-d}) \Longrightarrow \text{Frobenius eigenvalues } \in \mathbb{Q}(\sqrt{-d})$$

Properties of Frobenius eigenvalues

Theorem (Deligne-Weil)
The Frobenius eigenvalues of Frob_p on H^i_{et} are algebraic integers of absolute value $p^{i/2}$.

Special case: CM elliptic curve
$E/\mathbb{Q}$ elliptic curve with complex multiplication by $\mathbb{Q}(\sqrt{-d})$.
p a prime of good reduction.

$$p \text{ inert in } \mathbb{Q}(\sqrt{-d}) \Longrightarrow \text{Frobenius eigenvalues } \pm\sqrt{-p}$$
$$p \text{ split in } \mathbb{Q}(\sqrt{-d}) \Longrightarrow \text{Frobenius eigenvalues } \in \mathbb{Q}(\sqrt{-d})$$

Consequence
$\#E(\mathbb{F}_p) \equiv 1 \bmod p$ for all inert primes. (I.e, the inert primes are non-ordinary.)

Question
Can we generalize this to other classes of varieties?

K3 surfaces

Definition

A K3 surface is a simply connected algebraic surface having trivial canonical bundle.

Hodge diamond

$$\begin{array}{ccccc} & & 1 & & \\ & 0 & & 0 & \\ 1 & & 20 & & 1 \\ & 0 & & 0 & \\ & & 1 & & \end{array}$$

K3 surfaces

Definition

A K3 surface is a simply connected algebraic surface having trivial canonical bundle.

Hodge diamond

$$\begin{array}{ccccc} & & 1 & & \\ & 0 & & 0 & \\ 1 & & 20 & & 1 \\ & 0 & & 0 & \\ & & 1 & & \end{array}$$

Definition

We have a 22-dimensional vector space of 2-dimensional cycles. We call the ones represented by algebraic curves *algebraic cycles*. The others are *transcendental cycles*.

Remark

K3 surfaces are one of the possible generalizations of elliptic curves.

Models of K3 surfaces

Recall

Every elliptic curve has a Weierstraß equation.
(Double-cover of $\mathbf{P}^1$ with 4 ramification points.)

Models of K3 surfaces

Recall

Every elliptic curve has a Weierstraß equation.
(Double-cover of $\mathbf{P}^1$ with 4 ramification points.)

Models of K3 surfaces

Degree 2 model: Double cover of $\mathbf{P}^2$ ramified at a sextic curve.

Degree 4 model: Quartic in $\mathbb{P}^3$.

Degree 6 model: Complete intersection of quadric and cubic in $\mathbb{P}^4$.

Degree 8 model: Complete intersection of three quadrics in $\mathbb{P}^5$.

Singularities

As long as these models have at most ADE-singularities they still represent K3 surfaces.

Construction by cheating I

Split abelian variety

Let E be a CM elliptic curve.
Construct the Kummer surface corresponding to $E \times E$.

- Geometric Picard rank 20.
- Transcendental Frobenius eigenvalues are the squares of the ones of E.
- More generally, take isogenous surface.

Non-split abelian variety

- Start with genus 2 curve with real or complex multiplication. (E.g., use van Wamelen's list.)
- Construct corresponding Kummer surface.
- Frobenius eigenvalues will be products of eigenvalues of the curve.

Construction by cheating I

Split abelian variety

Let E be a CM elliptic curve.
Construct the Kummer surface corresponding to $E \times E$.

- Geometric Picard rank 20.
- Transcendental Frobenius eigenvalues are the squares of the ones of E.
- More generally, take isogenous surface.

Non-split abelian variety

- Start with genus 2 curve with real or complex multiplication.
  (E.g., use van Wamelen's list.)
- Construct corresponding Kummer surface.
- Frobenius eigenvalues will be products of eigenvalues of the curve.

Conclusion

Try to find examples that are not Kummer.
E.g., geometric Picard rank ≤ 16.

Construction by cheating II

Surfaces as covers

$$V_1 \colon w^4 = f_4(x, y, z)$$
$$V_2 \colon f_2(x, y, z, w) = 0, u^3 = f_3(x, y, z, w)$$

- V_1 is fourfold cover of $\mathbf{P}^2$.
  V_1 has automorphism $w \mapsto iw$.
- V_2 is a threefold cover of $Q \colon f_2(x, y, z, w) = 0$.
  V_2 has automorphism $u \mapsto \zeta_3 u$.
- $p \equiv 3 \bmod 4 \Rightarrow \#V_1(\mathbb{F}_p) = \#\{w^2 = f_4(x, y, z)\} \equiv 1 \bmod p$
- $p \equiv 2 \bmod 3 \Rightarrow \#V_2(\mathbb{F}_p) = \#Q(\mathbb{F}_p) \equiv 1 \bmod p$

Construction by cheating II

Surfaces as covers

$$V_1 \colon w^4 = f_4(x, y, z)$$
$$V_2 \colon f_2(x, y, z, w) = 0, u^3 = f_3(x, y, z, w)$$

- V_1 is fourfold cover of $\mathbf{P}^2$.
  V_1 has automorphism $w \mapsto iw$.
- V_2 is a threefold cover of $Q \colon f_2(x, y, z, w) = 0$.
  V_2 has automorphism $u \mapsto \zeta_3 u$.
- $p \equiv 3 \bmod 4 \Rightarrow \#V_1(\mathbb{F}_p) = \#\{w^2 = f_4(x, y, z)\} \equiv 1 \bmod p$
- $p \equiv 2 \bmod 3 \Rightarrow \#V_2(\mathbb{F}_p) = \#Q(\mathbb{F}_p) \equiv 1 \bmod p$

Question

Can we do better? (more fields, not imaginary quadratic)

New tool: p-adic point counting

Recent progress

Several people worked on efficient point counting methods for varieties over finite fields.

New tool: p-adic point counting

Recent progress
Several people worked on efficient point counting methods for varieties over finite fields.

Magma implementation
We implemented David Harvey's general p-adic method for K3 surfaces of degree 2 in `magma`. Is is accessable for everyone via:

`WeilPolynomialOfDegree2K3Surface`

Details are given in the proceedings.

Questions
How far can we get with this?
What can we do with it?

Performance of our implementation

Surface

Smooth model $w^2 = f_6(x, y, z)$.

Compute the characteristic polynomial of the Frobenius action on H^2.

Main steps

Work with large *generalized Hasse-Witt matrices* that consist of coefficients of high powers of f_6.

Performance of our implementation

Surface

Smooth model $w^2 = f_6(x, y, z)$.

Compute the characteristic polynomial of the Frobenius action on H^2.

Main steps

Work with large *generalized Hasse-Witt matrices* that consist of coefficients of high powers of f_6.

Time (in seconds)

p	powers of f_6	matrix build	matrix operations
31	12.65	21.05	55.36
61	76.91	21.63	71.00
97	236.92	22.30	73.53
127	489.92	22.36	73.97

Memory: 13 GB, **Matrix size:** 2080×2080

Computing Picard groups

Algebraic part of H^2 (for K3 surfaces)

- H^2 is of dimension 22.
- $H^{1,1}$ is of dimension 20.
- At most 20 dimensional vector space of algebraic cycles.
- Algebraic cycles result in Frobenius eigenvalues of the form $p\zeta$.
- Bound the Picard number by the number of these eigenvalues.
- Refine this by using the discriminant of the Picard lattice. (Computable via the Artin-Tate formula.)

Computing Picard groups

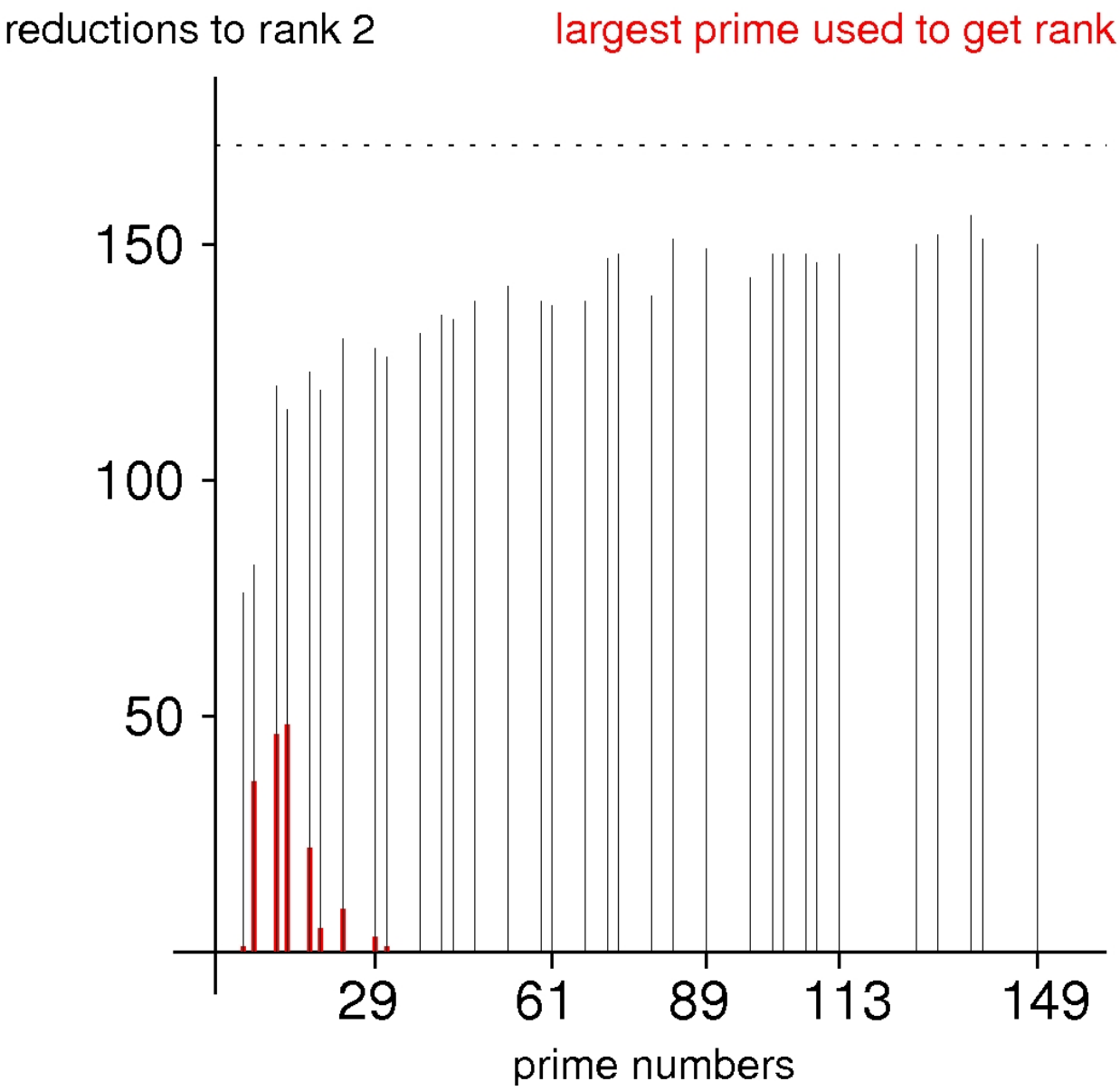
Algebraic part of H^2 (for K3 surfaces)

- H^2 is of dimension 22.
- $H^{1,1}$ is of dimension 20.
- At most 20 dimensional vector space of algebraic cycles.
- Algebraic cycles result in Frobenius eigenvalues of the form $p\zeta$.
- Bound the Picard number by the number of these eigenvalues.
- Refine this by using the discriminant of the Picard lattice. (Computable via the Artin-Tate formula.)

Experiment

- Take random degree 2 K3 surfaces with $0, \pm 1$ coefficients.
- Try to get the Picard rank.

Sample of 171 smooth surfaces



Interpretation of experiment

Observation
The computed upper bound is sharp in all cases inspected.

Theorem (F. Charles)
If the K3 surface V does not have real multiplication, primes resulting in sharp upper bounds have positive Dirichlet density.

Remark
Let V be a K3 surface with real multiplication by E. Then the bound is never sharp if and only if $\frac{22-\mathrm{rk}(\mathrm{Pic}(V))}{\deg(E)}$ is odd.

Recall
Real multiplication means that the transcendental lattice $T \subset H^2(V, \mathbb{Q})$ (as a Hodge-structure) has real multiplication.

ToDo
Find K3 surfaces with real multiplication that are not Kummer.

Arithmetic consequences of additional endomorphisms

Non-ordinary primes

- A prime is called *non-ordinary* if the Newton polygon of the reduction differs from the Hodge polygon.
- For a K3 surface, this means $\#V(\mathbb{F}_p) \equiv 1 \bmod p$.

Arithmetic consequences of additional endomorphisms

Non-ordinary primes

- A prime is called *non-ordinary* if the Newton polygon of the reduction differs from the Hodge polygon.
- For a K3 surface, this means $\#V(\mathbb{F}_p) \equiv 1 \bmod p$.

Theorem (quadratic endomorphism field)
For a K3 surface $V/\mathbb{Q}$, all the primes inert in the endomorphism field are non-ordinary.

Theorem (quadratic endomorphism field)
For all primes splitting in the endomorphism field the transcendental factor of the Weil polynomial factors over the endomorphism field.

Idea
Use these theorems to test examples.

Where to start searching?

Theorem (van Geemen, Jahnel, E.)
The 4-dimensional family

$$w^2 = xyz(x+y+z)l_1(x,y,z)l_2(x,y,z)$$

contains 1-parameter sub-families with Picard rank 16 and real multiplication by $\mathbb{Q}(\sqrt{d})$ for exactly those d that are a sum of two squares.

Where to start searching?

Theorem (van Geemen, Jahnel, E.)
The 4-dimensional family

$$w^2 = xyz(x+y+z)l_1(x,y,z)l_2(x,y,z)$$

contains 1-parameter sub-families with Picard rank 16 and real multiplication by $\mathbb{Q}(\sqrt{d})$ for exactly those d that are a sum of two squares.

Warning
The theorem uses the analytic moduli space.
Thus, the 6 lines of the ramification locus may not be defined over $\mathbb{Q}$.

Searching for real multiplication examples

Sample
Consider surfaces like

$$w^2 = f(x, y, z)g(x, y, z)$$

Search in Cartesian product of lists of forms.

Idea for fast point counting
Precompute as much data as possible for the forms in the lists.

Point counting using bit vectors

Input: Two lists of ternary forms. A small prime p.
Count points on $w^2 = f_i(x, y, z)g_j(x, y, z)$ over $\mathbb{F}_p$.

Initialization:

- List the points of $\mathbf{P}^2(\mathbb{F}_p)$.
- Evaluate each form for each point.
- Build bit-vector encoding $f = 0$ or $f \neq 0$ for each form f.
- Build bit-vector encoding $f = \square$ or $f \neq \square$ for each form f.

Counting

For each pair f_i, g_j do the following

- Apply logical operations on the precomputed bit-vectors.
- Generate bit vector encoding $f_i g_j = 0$ or $\neq 0$.
- Generate bit vector encoding $f_i g_j = \square$ or $\neq \square$.
- Use `popcount` on the bit vectors to count the points on the surface.

Performance

More than 10^6 surfaces per second.

Surfaces and conjectural endomorphism fields found

Geometry

All surfaces have geometric Picard rank 16.

Real quadratic endomorphism fields

$\mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{5})$: 1-parameter families.
$\mathbb{Q}(\sqrt{13})$: several examples.

Complex sextic endomorphism fields

$\mathbb{Q}(i, \zeta_7 + \zeta_7^{-1}), \mathbb{Q}(i, \zeta_9 + \zeta_9^{-1}), L(i)$: one example each.
(Here $L \subset \mathbb{Q}(\zeta_{19})$ unique cubic subfield.)

Application of p-adic point counting

- Generate strong numerical evidence.
- Search for patterns in the families.

One example in detail

Equation

$$w^2 = xyz(49x^3 - 304x^2y + 570x^2z + 361xy^2 - 2793xyz \\ + 2033xz^2 + 361y^3 + 2888y^2z - 5415yz^2 + 2299z^3)$$

Conjecture

Complex multiplication by $K = L(i)$ with L cubic subfield of $\mathbb{Q}(\zeta_{19})$.

One example in detail

Equation

$$w^2 = xyz(49x^3 - 304x^2y + 570x^2z + 361xy^2 - 2793xyz \\ + 2033xz^2 + 361y^3 + 2888y^2z - 5415yz^2 + 2299z^3)$$

Conjecture

Complex multiplication by $K = L(i)$ with L cubic subfield of $\mathbb{Q}(\zeta_{19})$.

Numerical evidence (all primes < 1000)

- p totally split in $K \Longrightarrow$ transcendental Frobenius eigenvalues in K.
- p splits into 3 primes in $K \Longrightarrow$ transcendental Frobenius eigenvalues are roots of $t^2 - p^2$.
- p splits into 2 primes in $K \Longrightarrow$ third powers of transcendental Frobenius eigenvalues are in $\mathbb{Q}(i)$.
- p totally inert in $K \Longrightarrow$ transcendental factor $t^6 - p^6$.

Statistics – Picard rank of reductions

Effect of real multiplication

The reduction modulo p of a Picard rank 16 K3 surface with real multiplication is 18 or 22.

Experiment

Compute the Picard ranks for all surfaces in the families and all $p < 500$:

E	# relative frequency (in %) of rank 22 per prime					
	inert primes			split primes		
	min	average	max	min	average	max
$\mathbb{Q}(\sqrt{2})$	0.00	7.42	25.00	0.00	6.14	25.00
$\mathbb{Q}(\sqrt{5})$	2.33	9.32	24.24	0.00	5.84	16.00
$\mathbb{Q}(\sqrt{3})$	0.00	0.00	0.000	2.33	7.40	20.59

Tabelle: Frequency of reduction to geometric Picard rank 22

Statistics – Picard rank of reductions

Effect of real multiplication

The reduction modulo p of a Picard rank 16 K3 surface with real multiplication is 18 or 22.

Experiment

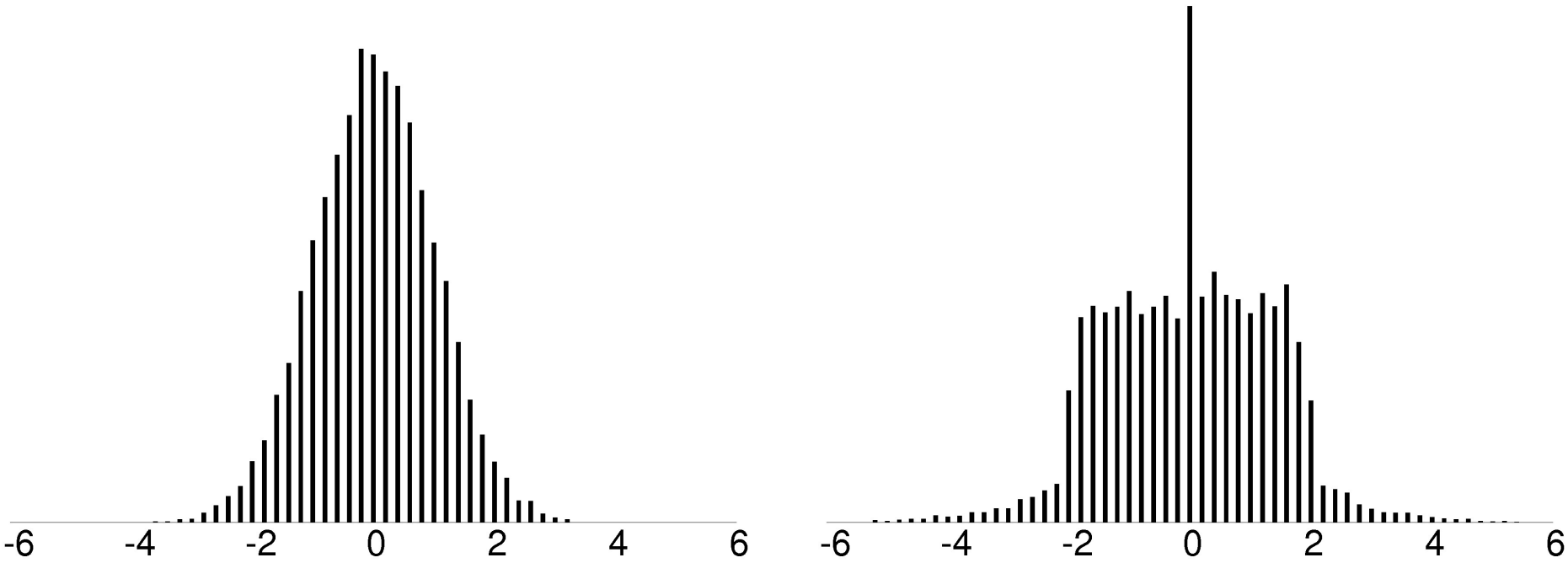
Compute the Picard ranks for all surfaces in the families and all $p < 500$:

E	# relative frequency (in %) of rank 22 per prime					
	inert primes			split primes		
	min	average	max	min	average	max
$\mathbb{Q}(\sqrt{2})$	0.00	7.42	25.00	0.00	6.14	25.00
$\mathbb{Q}(\sqrt{5})$	2.33	9.32	24.24	0.00	5.84	16.00
$\mathbb{Q}(\sqrt{3})$	0.00	0.00	0.000	2.33	7.40	20.59

Tabelle: Frequency of reduction to geometric Picard rank 22

Observation: No inert prime in $\mathbb{Q}(\sqrt{3})$ and no surface in our $\mathbb{Q}(\sqrt{3})$-family results in reduction to rank 22.

Distribution of normalized transcendental Frobenius traces



$V_1 : w^2 = xyz(x+y+z)(3x+5y+7z)(-5x+11y-2z)$

$V_2 : w^2 = xyz(x^3+3x^2y-2x^2z+5xy^2-xz^2+3y^3-2y^2z-3yz^2+2z^3)$

$M_1 = [0.0153, 0.9894, 0.0291, 2.9546, 0.1504]$ $(B = 175000)$

$M_2 = [-0.0039, 0.9705, -0.0865, 5.6756, -1.4465]$ $(B = 250000)$

V_1 generic rank 16, V_2 real multiplication by $\mathbb{Q}(\sqrt{3})$

Summary

Code available

`magma` implementation of p-adic point counting for degree 2 K3 surfaces.

Usability

Can do primes beyond 100.

Applications

- Sharp upper bounds of Picard ranks in almost all cases.
- Study of endomorphism fields.

New examples

Surfaces with various endomorphism fields. (Some conjectural some proven.)
Strong numerical evidence.

Summary

Code available

`magma` implementation of p-adic point counting for degree 2 K3 surfaces.

Usability

Can do primes beyond 100.

Applications

- Sharp upper bounds of Picard ranks in almost all cases.
- Study of endomorphism fields.

New examples

Surfaces with various endomorphism fields. (Some conjectural some proven.)
Strong numerical evidence.

Thank you!