Point Counting on K3 surfaces

Andreas-Stephan Elsenhans

University of Würzburg

August 2022

Joint work with J. Jahnel.

Introduction

Theorem (Hasse) For an elliptic curve E over a finite field $\mathbb{F}_p$, we have

$$|p + 1 - \#E(\mathbb{F}_p)| \leq 2\sqrt{p}\,.$$

Example:
Two elliptic curves

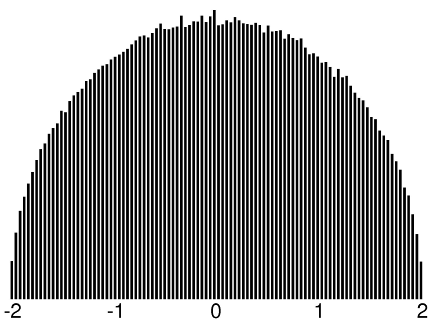
$$E_1 : y^2 = x^3 + x + 3\,,$$
$$E_2 : y^2 = x^3 - 17\,.$$

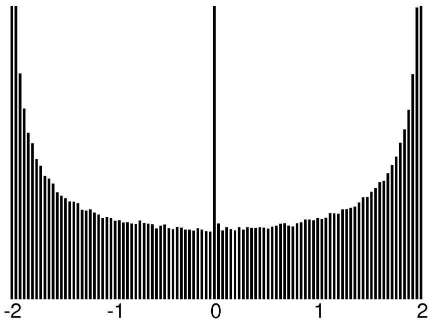
Experiment:
Distribution of

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

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

Introduction II





$$E_1 : y^2 = x^3 + x + 3$$
$$j(E_1) = \frac{55296}{275}$$

$$E_2 : y^2 = x^3 - 17$$
$$j(E_2) = 0$$

(Data from 664579 primes, 100 buckets)

Connection with cohomology

Theorem (Lefschetz trace formula)
Let V be a n-dimensional proper variety over $\mathbb{Q}$ with good reduction at p. Then

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

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

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

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

Theorem (Weil conjectures, proved by Deligne)
The Frobenius eigenvalues of Frob_p on $\mathrm{H}^i_{\mathrm{et}}(V_{\overline{\mathbb{Q}}}, \mathbb{Q}_\ell)$ are algebraic integers of absolute value $p^{i/2}$.

K3 surfaces

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

Hodge diamond

$$\begin{matrix} & & 1 & & \\ & 0 & & 0 & \\ 1 & & 20 & & 1 \\ & 0 & & 0 & \\ & & 1 & & \end{matrix}$$

Lefschetz trace formula (for K3 surfaces)

$$\begin{aligned}\#S(\mathbb{F}_p) &= p^2 + 1 + \mathrm{Tr}(\mathrm{Frob}_p | H^2_{\mathrm{et}}(S_{\overline{\mathbb{Q}}}, \mathbb{Q}_\ell)) \\ &= p^2 + 1 + p \cdot \mathrm{Tr}(\mathrm{Frob}_p | H^2_{\mathrm{et}}(S_{\overline{\mathbb{Q}}}, \mathbb{Z}_\ell(1)))\end{aligned}$$

As $H^1(S, \mathbb{Z}_\ell) = H^3(S, \mathbb{Z}_\ell) = 0$.

Remark
K3 surfaces are one of the possible generalisations 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
Degree 2 model: Double cover of $\mathbf{P}^2$ ramified at a sextic curve.
Degree 4 model: Quartic in $\mathbf{P}^3$.
Degree 6 model: Complete intersection of quadric and cubic in $\mathbf{P}^4$.
Degree 8 model: Complete intersection of three quadrics in $\mathbf{P}^5$.

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

Surfaces of interest

Equations
Double covers of $\mathbf{P}^2$, ramified at the union of 6 lines in general position.
The minimal resolution of singularities is a K3 surface, in each case.

$$\begin{aligned}
S'_1 &\colon W^2 = XYZ(X+Y+Z)(3X+5Y+7Z)(-5X+11Y-2Z), \\
S'_2 &\colon W^2 = XYZ(2X+4Y-3Z)(X-5Y-3Z)(X+3Y+3Z), \\
S'_3 &\colon W^2 = XYZ(4X+9Y+Z)(-X-Y-4Z)(16X+25Y+Z), \\
S'_4 &\colon W^2 = XYZ(X+Y+Z)(X+2Y+3Z)(5X+8Y+20Z), \\
S'_5 &\colon W^2 = XY(X^4 - 7X^3Y - X^3Z + 19X^2Y^2 + 4X^2YZ \\
&\qquad + X^2Z^2 - 23XY^3 - 7XY^2Z - 6XYZ^2 - XZ^3 \\
&\qquad + 11Y^4 + 7Y^3Z + 9Y^2Z^2 + 3YZ^3 + Z^4).
\end{aligned}$$

p-adic point counting

Proposition
For the double cover

$$S' \colon w^2 = f_6(x,y,z)$$

and an odd prime p, we have

$$\#S'(\mathbb{F}_p) \equiv 1 + p + p^2 + C_p \pmod{p},$$

where C_p is the coefficient of $(XYZ)^{p-1}$ of $f_6^{\frac{p-1}{2}}$.

Remark
David Harvey (and others) have worked on methods to compute

$$(C_p \bmod p)_{p \in \mathbb{P}}$$

and similar sequences as fast as possible.

Using the Delinge-Weil bound

Definition
Every K3 surface has a 22-dimensional vector space of 2-dimensional cycles. We call the ones represented by algebraic curves *algebraic cycles*. The others are *transcendental cycles*.

Example
The resolution of each A_1-singularity results in an algebraic cycle.

Application of the Weil conjectures, proven by Deligne
One has
$$|\#S'_i(\mathbb{F}_p) - (p^2 + p + 1)| \leq 6p,$$
for the singular models $S'_1, \ldots, S'_5$.

Conclusion
It suffices to determine $\#S'_i(\mathbb{F}_p)$ modulo some integer $> 12p$. In combination with the p-adic approach, it suffices to determine $(\#S'_i(\mathbb{F}_p) \bmod 16)$.

Relation with the Brauer group

Idea
As we know the Picard group as a Galois module, it suffices to work on its orthogonal complement.

Transcendental lattice
$$T(S_{\overline{k}}, \mathbb{Z}_2) := c_1(\mathrm{Pic}(S_{\overline{k}}))^{\perp} \subset H^2_{\mathrm{et}}(S_{\overline{k}}, \mathbb{Z}_2(1))$$

$\mathrm{Gal}(\overline{k}/k)$ acts on $T(S_{\overline{k}}, \mathbb{Z}_2)$ via orthogonal maps (with respect to the pairing induced by the cup product and Poincaré duality).

Theorem (van Geemen, Jahnel & E.)
One has
$$\mathrm{Br}(S_{\overline{k}})_2 \cong \mathrm{Hom}(T(S_{\overline{k}}, \mathbb{Z}_2), \mathbb{Z}/2\mathbb{Z}),$$
as $\mathrm{Gal}(\overline{k}/k)$-modules.

$\mathrm{Br}(S_{\overline{k}})_2$ as a Galois module

Theorem (Skorobogatov)
Let k be a field of characteristic not 2 and let S be a K3 surface over k as above. Let $\sigma\colon S_{\overline{k}} \to S_{\overline{k}}$ be the involution and $\pi\colon S_{\overline{k}} \to S_{\overline{k}}/\sigma$ the projection. Then there is a *Gal*$(\overline{k}/k)$-equivariant isomorphism
$$\mathrm{Br}(S_{\overline{k}})_2 \to \mathrm{Pic}(S_{\overline{k}}/\sigma)^{\mathrm{even}}/\pi_* \,\mathrm{Pic}(S_{\overline{k}}),$$
for $\mathrm{Pic}(S_k)^{\mathrm{even}} \subset \mathrm{Pic}(S_k)$ the subgroup formed by the classes having an even intersection number with each connected component of the branch locus.

Situation of Application
$S_{\overline{k}}/\sigma$ is $\mathbf{P}^2$ blown up in the 15 singularities of the ramification locus.
Thus, the Galois action on $\mathrm{Br}(S_{\overline{k}})_2$ is determined by the action on the singularities of the ramification locus.

Abelian extensions

Action via finite quotients
For each e, there is a smallest number field K_e such that $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-action on $H^2_{\mathrm{et}}(S_{\overline{k}}, \mathbb{Z}_2(1)) \otimes_{\mathbb{Z}_2} \mathbb{Z}/2^e\mathbb{Z}$ factors via $\mathrm{Gal}(K_e/\mathbb{Q})$. It is called the *splitting field* of the cohomology.

Example
By Skorobogatov's result, K_1 is $\mathbb{Q}$ or $\mathbb{Q}(\zeta_5)$ in the examples above.

Remark
The quotients
$$\{A \in \mathrm{GL}_n(\mathbb{Z}_2) \mid A \equiv E_n \pmod{2^e}\}/\{A \in \mathrm{GL}_n(\mathbb{Z}_2) \mid A \equiv E_n \pmod{2^{e+1}}\}$$
are abelian of exponent 2. Therefore, K_{e+1}/K_e is an abelian field extension of exponent 2.

Limited Ramification
The extensions $K_e/\mathbb{Q}$ are unramified outside 2 and the bad primes.

Using class field theory
In theory, we could construct fields containing K_e, for $e \geq 2$, inductively.

2-adic overdetermination of the trace

Theorem (Jahnel, E.)

a) For $A, B \in O_n(\mathbb{Z}_2)$ with $A \equiv E_n \pmod 2$, we have

$$A \equiv B \pmod 4 \Longrightarrow \mathrm{Tr}(A) \equiv \mathrm{Tr}(B) \pmod{16}.$$

b) For $A, B \in O_n(\mathbb{Z}_2)$ with $A^2 \equiv E_n \pmod 2$, we have

$$A \equiv B \pmod 4 \Longrightarrow \mathrm{Tr}(A) \equiv \mathrm{Tr}(B) \pmod 8.$$

Consequence
In order to compute $(\#S_i(\mathbb{F}_p) \bmod 16)$ for $i = 1, \dots, 4$ we use part a).
This implies that it suffices to determine the field K_2.
Thus, we work only with multi-quadratic extensions of $\mathbb{Q}$.

Proof (first part in the special case of the standard form)

$A = E + 2A'$, $B = A(E + 4\widetilde{B})$. Orthogonality results in

$$(E + 4\widetilde{B})(E + 4\widetilde{B}^\top) = E, \quad (E + 2A')(E + 2A'^\top) = E,$$

and

$$A' + A'^\top \equiv 0 \pmod 2, \quad \widetilde{B} = -\widetilde{B}^\top - 4\widetilde{B}\widetilde{B}^\top. \qquad (1)$$

We get

$$\mathrm{Tr}(B) = \mathrm{Tr}(A) + 4\mathrm{Tr}((E + 2A')\widetilde{B}) = \mathrm{Tr}(A) + 4\mathrm{Tr}(\widetilde{B}) + 8\mathrm{Tr}(A'\widetilde{B})$$

and

$$\mathrm{Tr}(A'\widetilde{B}) = \sum_{i<j} (a_{ij}b_{ji} + a_{ji}b_{ij}) + \sum_i a_{ii}b_{ii}.$$

Using (1), we find that $(a_{ij}b_{ji} + a_{ji}b_{ij})$ and b_{ii} are even. Thus, $\mathrm{Tr}(A'\widetilde{B})$ is even. Similarly, $\mathrm{Tr}(\widetilde{B}\widetilde{B}^\top)$ is even and therefore,

$$2\mathrm{Tr}(\widetilde{B}) = \mathrm{Tr}(\widetilde{B} + \widetilde{B}^\top)$$

is divisible by 8. □

Proof of the general case

Idea:

- We view $\mathbb{Z}_2^n$ as a $\mathbb{Z}_2$-lattice Λ.
- Trivial action on $\Lambda/4\Lambda$ implies trivial action on $\Lambda^\vee/4\Lambda^\vee$ and intermediate lattices.
- This way, we can reduce to the case of a regular $\mathbb{Z}_2[\sqrt{2}]$-lattice.
- For regular $\mathbb{Z}_2[\sqrt{2}]$-lattices, a proof similar to the one above is possible.

Proof of part b)
The same techniques apply.

Counting points modulo 16 on $S_1, \dots, S_4$

Algorithm (Initialisation)

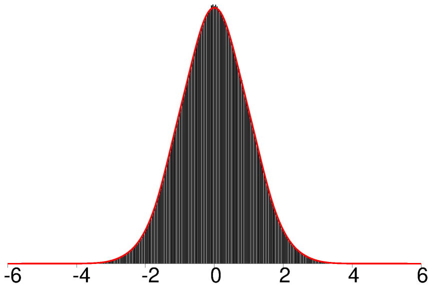
- We have $k = K_1 = \mathbb{Q}$, $K_2 \subset L := \mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{p} \mid p \text{ bad prime})$.
- For each $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$, find a prime p such that $\mathrm{Frob}_p = \sigma$.
- Compute $\#S(\mathbb{F}_p)$, for each such p, using a naive method.
- Store σ and the resulting trace on T modulo 16 in a table.

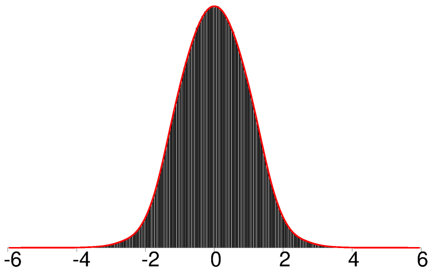
Algorithm (Point count)
For a good prime p, do the following.

- Identify Frob_p in $\mathrm{Gal}(L/\mathbb{Q})$.
- Read the trace modulo 16 of the table.
- Combine this with $(\#S(\mathbb{F}_p) \bmod p)$ to determine $\#V(\mathbb{F}_p)$.

Result
The number of points on $S(\mathbb{F}_p)$ for all $p < 10^8$.

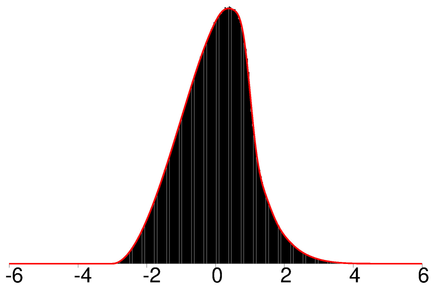
Distributions found for S_1 and S_2

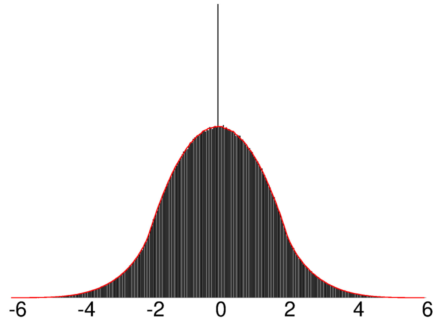




Parameters
Search bound 10^8. Geometric Picard rank 16.
Moments: $1, 0, 1, 0, 3, 0, 15, 0, 105, \ldots$ and $1, 0, 1, 0, 3, 0, 16, 0, 126, \ldots$.

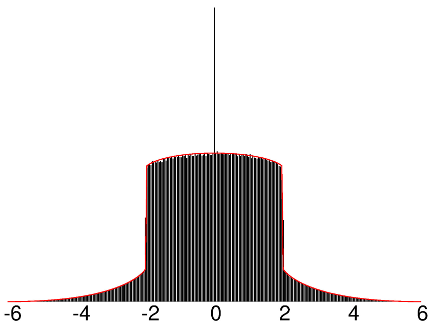
Distributions found for S_3 and S_4





Parameters
Geometric Picard rank 17 and geometric Picard rank 16 with complex multiplication by $\mathbb{Q}(i)$.
Moments: $1, -1, 2, -4, 10, -25, 70, 196, \ldots$ and $1, 0, 1, 0, 6, 0, 60, 0, 805, \ldots$.

Distributions found for S_5



Parameters
Geometric Picard rank 16, real multiplication by $\mathbb{Q}(\sqrt{5})$.
Moments: $1, 0, 1, 0, 6, 0, 70, \ldots$.

Theoretical background

Sato-Tate group

1. $\varrho_\ell \colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{O}(T)$ is a continuous Galois representation. The image is an ℓ-adic Lie group.
2. The Zariski closure of the image is an ℓ-adic algebraic group, called *algebraic monodromy group*.
3. In the case of K3 surfaces, Tankeev and Zarhin showed, that the neutral component of the algebraic monodromy group is the centralizer of the endomorphism field in $\mathrm{SO}(T)$. The component group depends on the example.
4. Base change $\mathbb{Q}_\ell \to \mathbb{C}$ results in a complex algebraic group.
5. Up to conjugation, a complex Lie group has only one maximal compact subgroup. In this context, it is called the *Sato-Tate group*.

The Sato-Tate conjecture

- The red lines show the trace distribution resulting from an equidistribution with respect to the Haar measure in the Sato-Tate group.
- The Sato-Tate conjecture predicts that the two distributions coincide.

Summary

Tools:
2-adic and p-adic point counting on K3 surfaces.

Application:
Study the distribution of the normalized Frobenius traces on étale cohomology for primes up to 10^8.

Results:
Strong numerical evidence for the Sato-Tate conjecture.

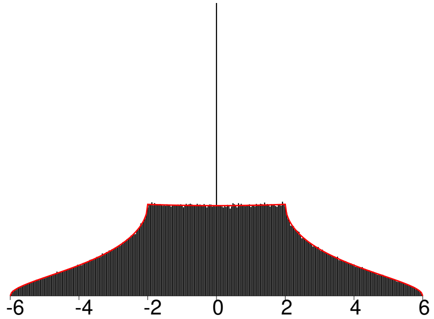
Thank you!

Last example

Equation

$S_6'\colon W^2 = XYZ(X^3 - 3X^2Z - 3XY^2 - 3XYZ + Y^3 + 9Y^2Z + 6YZ^2 + Z^3).$

Geometric Picard rank 16,
Conjectural complex multiplication by $\mathbb{Q}(i, \zeta_9 + \zeta_9^{-1})$.



Moments: $1, 0, 1, 0, 15, 0, 310, \ldots$.