

Variation of Néron-Severi ranks of reductions of K3 surfaces

Edgar Costa and Yuri Tschinkel

ABSTRACT

We study the behavior of geometric Picard ranks of K3 surfaces over \mathbb{Q} under reduction modulo primes. We compute these ranks for reductions of smooth quartic surfaces modulo all primes $p < 2^{16}$ in several representative examples and investigate the resulting statistics.

1. Introduction

Let k be a number field and X a K3 surface over k , i.e., a smooth projective simply-connected surface with trivial canonical class, for example, a smooth quartic hypersurface in \mathbb{P}^3 . Let \mathfrak{p} be a finite place of k where X has good reduction $X_{\mathfrak{p}}$. Let \overline{X} (resp. $\overline{X}_{\mathfrak{p}}$) be the base change of X (respectively, $X_{\mathfrak{p}}$) to the algebraic closure of k (respectively, of the residue field of \mathfrak{p}), and let $\rho(\overline{X})$ and $\rho(\overline{X}_{\mathfrak{p}})$ be the ranks of the corresponding Néron-Severi groups $\text{NS}(\overline{X})$ and $\text{NS}(\overline{X}_{\mathfrak{p}})$, i.e., the geometric Picard ranks. There is a natural specialization homomorphism

$$s_{\mathfrak{p}} : \text{NS}(\overline{X}) \rightarrow \text{NS}(\overline{X}_{\mathfrak{p}}), \quad (1.1)$$

which is injective (see, e.g., [vL07a, Proposition 6.2]), thus

$$\rho(\overline{X}) \leq \rho(\overline{X}_{\mathfrak{p}}).$$

In fact, for all \mathfrak{p} of good reduction we have

$$\rho(\overline{X}) + \eta(\overline{X}) \leq \rho(\overline{X}_{\mathfrak{p}}), \quad (1.2)$$

for some $\eta(\overline{X}) \geq 0$, defined by (2.2). It is known that there exist infinitely many \mathfrak{p} such that equality occurs; furthermore, over some finite extension of k , the set of such primes has density one [Cha11, Theorem 1]. However, very little is known about the set of primes

$$\Pi_{\text{jump}}(X) := \{\mathfrak{p} : \rho(\overline{X}) + \eta(\overline{X}) < \rho(\overline{X}_{\mathfrak{p}})\},$$

where the inequality (1.2) is strict.

Information about $\Pi_{\text{jump}}(X)$ can be converted into geometric statements: *if this set is infinite*, for all K3 surfaces over number fields with $\rho(X) = 2, 4$, then *all* K3 surfaces over algebraically closed fields of characteristic zero have infinitely many rational curves, by [BHT11] and [LL12].

There are cases, when $\Pi_{\text{jump}}(X)$ is known to be infinite. For example, assume that X is a Kummer surface, i.e., the resolution of singularities of the quotient A/ι , where A is an abelian surface, and $\iota : A \rightarrow A$ the standard involution $\iota(a) = -a$. Then

$$\rho(\overline{X}) = \rho(\overline{A}) + 16.$$

Now assume that $A \sim C_1 \times C_2$, i.e., is isogenous to a product of two elliptic curves. Then

- $\rho(\overline{X}) \geq 18$,
- $\rho(\overline{X}) \geq 19$, if $C_1 \sim C_2$, and
- $\rho(\overline{X}) = 20$, if in addition, C_1 has complex multiplication by $E := \mathbb{Q}(\sqrt{-d})$.

In these extreme cases, the primes in $\Pi_{\text{jump}}(X)$ can be understood as follows:

- if $\rho(\overline{X}) \geq 19$, then $\mathfrak{p} \in \Pi_{\text{jump}}(X)$ provided \mathfrak{p} is a supersingular prime for C_1 (and thus C_2).

By a theorem of Elkies, there are infinitely many such primes [Elk87], at least for elliptic curves over \mathbb{Q} . This motivates us to consider the asymptotic behavior of the proportion of primes in $\Pi_{\text{jump}}(X)$:

$$\gamma(X, B) := \frac{\#\{p \leq B : p \in \Pi_{\text{jump}}(X)\}}{\#\{p \leq B\}}. \quad (1.3)$$

Returning to Kummer surfaces of the form $X \sim C \times C/\iota$, when the elliptic curve C does not have complex multiplication, so that $\rho(\overline{X}) = 19$, the Lang-Trotter conjecture [LT76], implies

$$\gamma(X, B) \sim \frac{c}{\sqrt{B}}, \quad B \rightarrow \infty,$$

for some constant $c > 0$. The Lang-Trotter conjecture has attracted the attention of many experts; for a sample of results we refer to [Elk91, FM96, DP99, Bai07] and to [Kat09], in the function field case. If C does have complex multiplication, then

$$\gamma(X, B) \sim \frac{1}{2}, \quad B \rightarrow \infty. \quad (1.4)$$

Elsenhans and Jahnel conducted an extensive numerical investigation of Kummer surfaces over \mathbb{Q} , in particular of those with $\rho(\overline{X}) = 17$ [EJ12]. They computed $\rho(\overline{X}_p)$, for $p < 1000$, for a large sample of surfaces X with $\rho(\overline{X}) = 17$, and observed that the proportion of such X with $\rho(\overline{X}_p) > 18$ is roughly $2/\sqrt{p}$. In another direction, for some of the examples with $\rho(\overline{X}) = 18$, they were able to show that the density of $\Pi_{\text{jump}}(X)$ is at least $1/2$. The precise shape of asymptotic formulas for $\gamma(X, B)$ for general Kummer surfaces $X \sim A/\iota$ is likely to depend on the Sato-Tate group ST_A of the abelian surface A , investigated in [FKRS12].

More generally, the Kuga-Satake construction (see [Del72]) relates a K3 surface X to an abelian variety $A = A_X$ of dimension 2^{19} . Knowing this abelian variety explicitly, in particular, its Picard group and its endomorphisms, would allow us to compute the Picard group of X , see [HKT13, Proposition 19]. The jumping behavior of Picard ranks of K3 surfaces is therefore related to the jumping behavior on these abelian varieties, similar to the Kummer case above, thus should be controlled by a version of the Lang-Trotter conjecture. However, the Kuga-Satake construction is transcendental, and we do not yet have sufficiently effective control over A , even over its field of definition, except in degree two [HKT13, Remark 9].

In this note we report on a numerical study of the variation of Picard ranks of quartic K3 surfaces over \mathbb{Q} , with *small* $\rho(\overline{X})$. For several representative examples, we compute $\rho(\overline{X})$ and $\rho(\overline{X}_p)$, for all $2 < p < 2^{16}$, where X has good reduction, and we calculate $\gamma(X, B)$, for $B < 2^{16}$.

We observe two different trends. In examples where $\rho(\overline{X}) = 1$ and $\eta(\overline{X}) = 1$ we find that

$$\gamma(X, B) \sim \frac{c_X}{\sqrt{B}}, \quad B \rightarrow \infty,$$

for some constant $c_X > 0$. In other words, a prime p is in $\Pi_{\text{jump}}(X)$ with probability proportional to $1/\sqrt{p}$. On our other examples, when $\rho(\overline{X}) = 2$ (and $\eta(\overline{X}) = 0$), we are lead to believe that

$$\liminf_{B \rightarrow \infty} \gamma(X, B) \geq \frac{1}{2},$$

i.e., the primes at which the geometric Picard number jumps has density $\geq 1/2$. Our data strongly suggests that we are *not* in the same situation as in (1.4), the plots in Figure 2 and Figure 3 are not consistent with statistics for the splitting behavior of primes in quadratic extensions of \mathbb{Q} .

Acknowledgements. We are grateful to David Harvey, Brendan Hassett, Kiran Kedlaya, and Barry Mazur for useful discussions and collaboration on related questions. The first author

was partially supported by FCT doctoral grant SFRH/BD/69914/2010. The second author was supported by National Science Foundation grants 0968318 and 1160859.

2. *Computing the Picard number of a K3 surface*

In this section, we explain our approach to the computation of Picard numbers of quartic K3 surfaces. Over a *finite field*, one only needs to compute the Hasse-Weil zeta function; which may be computationally expensive, but is achievable in bounded time. Over a *number field*, computing the Picard number of an algebraic surface is a hard problem. For K3 surfaces, an effective version of the Kuga-Satake construction as in [HKT13] yields a theoretical algorithm, with *a priori* bounded running time, at least for degree-two K3 surfaces. In [PTvL12, Section 8.6.] the authors provide an alternative algorithm; another algorithm, conditional on the Hodge conjecture for $X \times X$, is presented in [Cha11]; these algorithms do not have *a priori* bounded running times.

In practice, one starts by establishing lower and upper bounds for $\rho(\overline{X})$. Lower bounds can be produced by exhibiting independent divisors on \overline{X} , and upper bounds can be obtained via specialization to finite fields as in (1.1). This approach does not guarantee an answer in every case, but sometimes the bounds agree. In some cases, one can improve the upper bound by a careful analysis of the specialization map. For example, if the lattice structure disagrees over two different specializations, or if some divisor class on $\overline{X}_{\mathfrak{p}}$ is not liftable, then the specializations cannot be surjective. This approach has its limitations, as one cannot in general expect that there exist places \mathfrak{p} such that $\rho(\overline{X}_{\mathfrak{p}}) \leq \rho(\overline{X}) + 1$. An overview of these techniques can be found in [Sch12, Chapter 7].

In [Cha11], Charles proved a general theorem about the jumping behavior of Picard ranks under specialization: Let E_X be the endomorphism algebra of the Hodge structure underlying the transcendental lattice T_X of X ; it is known that E_X is a field, which is either totally real or a CM-field (see, e.g., [Zar83]). In the latter case, one says that X has complex multiplication. By [Cha11, Theorem 1], there are two possibilities,

$$\rho(\overline{X}_{\mathfrak{p}}) \geq \begin{cases} \rho(\overline{X}) & \text{if } E_X \text{ is a CM-field or } \dim_{E_X}(T_X) \text{ is even,} \\ \rho(\overline{X}) + [E_X : \mathbb{Q}] & \text{if } E_X \text{ is totally real field and } \dim_{E_X}(T_X) \text{ is odd.} \end{cases} \tag{2.1}$$

We define

$$\eta(\overline{X}) := 0 \quad \text{or} \quad [E_X : \mathbb{Q}], \tag{2.2}$$

depending on which case we are in.

We turn to finite fields. Let X be a smooth projective surface over \mathbb{F}_q . The Weil conjectures tell us that the Hasse-Weil zeta function has the form

$$Z(X, T) := \exp \left(\sum_{m=1}^{\infty} \frac{\#X(\mathbb{F}_{q^m})}{m} t^m \right) = \frac{P_1(X, t)P_3(X, t)}{(1-t)P_2(X, t)(1-q^2t)}, \tag{2.3}$$

where

$$P_i(X, t) := \det(1 - t \text{Fr}_i | H_{\text{et}}^i(\overline{X}, \mathbb{Q}_{\ell})) \in \mathbb{Z}[t]$$

have reciprocal roots of absolute value $q^{i/2}$, and Fr_i are the Frobenius automorphisms. The Artin-Tate conjecture relates the Néron-Severi group of X with $P_2(X, t)$:

CONJECTURE 1.

- (Tate Conjecture) $\rho(X)$ equals the multiplicity of q as a reciprocal root of $P_2(X, t)$.
- (Artin-Tate Conjecture) Let $\text{Br}(X)$ be the Brauer group of X and

$$\alpha(X) := \chi(X, \mathcal{O}_X) - 1 + \dim(\text{Pic}^0(X)).$$

Then

$$\lim_{s \rightarrow 1} \frac{P_2(X, q^{-s})}{(1 - q^{1-s})^{\rho(X)}} = \frac{(-1)^{\rho(X)-1} \# \text{Br}(X) \cdot \text{disc}(\text{NS}(X))}{q^{\alpha(X)} (\# \text{NS}(X)_{\text{tors}})^2}.$$

In odd characteristic, the Tate conjecture implies the Artin-Tate conjecture [Mil75, Theorem 6.1]. If X is a K3 surface both hold [Cha13, Per13, Mau12]; furthermore, $\# \text{Br}(X)$ is a perfect square (see, e.g., [LLR05]) and

$$\rho(X) \equiv \dim(H_{\text{et}}^i(\bar{X}, \mathbb{Q}_\ell)) \equiv 0 \pmod{2}.$$

Thus,

$$\text{disc}(\text{NS}(X_{\mathbb{F}_q})) = - \lim_{s \rightarrow 1} \frac{P_2(X, q^{-s})}{q(1 - q^{1-s})^{\rho(X)}} \pmod{\mathbb{Q}^{\times 2}}. \quad (2.4)$$

Usually, one computes P_2 by counting points in sufficiently many extensions of the base field. For K3 surfaces, this requires computations in fields of size at least p^{10} . Such computations have been performed in [vL07b, EJ08a, EJ08b, EJ11a, EJ11b] for primes < 10 . This direct approach is computationally not feasible for larger primes. Our approach follows an idea of Kedlaya: we extract P_2 by computing the Frobenius action on p -adic cohomology (Monsky-Washnitzer cohomology) with sufficient precision. For example, for a quartic K3 surface over \mathbb{F}_p , where $p > 41$, it suffices to know two significant p -adic digits of the coefficients of P_2 . This can be achieved using the Newton identities combined with Mazur inequalities [Maz73].

The algorithmic implementation of this idea relies on techniques introduced in [AKR10] and [Har07]. The approach by Abbott–Kedlaya–Roe [AKR10] makes primes < 20 computationally feasible, but its dependence on p is at least $p^{\dim(X)+1}$. We make use of refinements of Kedlaya’s algorithm, which were introduced by Harvey [Har07]:

- rewriting the Frobenius action on Monsky-Washnitzer cohomology in terms of sparse polynomials;
- preserving the sparseness throughout the reduction process of differentials in cohomology;
- rewriting each reduction step process as a linear map.

The time complexity is dominated by the reduction of differentials in cohomology, which involves $O(p)$ recurrent matrix vector multiplications in $\mathbb{Z}/\mathbb{Z}p^s$. For a quartic K3 surface the size of the matrices is 220×220 ; for $p > 41$ one can take $s = 4$. Moreover, if the K3 is nondegenerate (as in [SV13]), one can reduce their size to 64×64 . In practice, we had no difficulties to find a change of coordinates for which the surface became nondegenerate.

Altogether, this reduces the polynomial dependence on p in [AKR10] to quasi-linear (or to $p^{1/2+\varepsilon}$ using [BGS07]). The details of the algorithm will be presented in [CHK14]. Our implementation is written in C++, using the libraries FLINT [HJP12] and NTL [Sho13]. The raw data of all experiments is available at www.cims.nyu.edu/~costa.

3. Computations and Numerical Data

In this section, we present numerical data for five representative quartic K3 surfaces over \mathbb{Q} with small $\rho(\bar{X})$. For each surface we compute $\rho(\bar{X})$ and $\rho(\bar{X}_p)$, for all $2 < p < 2^{16}$ where X has good reduction, using the methods introduced in Section 2. This computation consumed around 45000 hours of CPU time of the Bowery and Butinah clusters at New York University. With this data we calculate $\gamma(X, B)$ for $B < 2^{16}$, which we present as a plot. We find two trends for $\gamma(X, B)$:

- When $\rho(\bar{X}) = 1$ and $E_X = \mathbb{Q}$ we have

$$\gamma(X, B) \sim c_X / \sqrt{B}, \quad B \rightarrow \infty,$$

for some constant $c_X > 0$, i.e., $\rho(\overline{X}_p)$ jumps with probability proportional to $1/\sqrt{p}$.
 – When $\rho(\overline{X}) = 2$ the data leads us to believe that

$$\liminf_{B \rightarrow \infty} \gamma(X, B) \geq 1/2,$$

i.e., the primes at which the geometric Picard number jumps has density $\geq 1/2$.

These trends reflect which case of equation (2.1) we are in.

In our examples, we used random homogeneous polynomials:

$$\begin{aligned} f_1 &:= 2x^2y + 2xy^2 + y^3 - x^2z + xyz - y^2z + xz^2 - 8yz^2 + x^2w - 9xyw + 3y^2w \\ &\quad - 10yzw - xw^2 - 9yw^2 + zw^2 - w^3; \\ f_2 &:= -14x^3 + x^2y - y^3 + 2x^2z - 17xyz + 22y^2z + xz^2 - 3yz^2 + 2z^3 - 2x^2w \\ &\quad - 4y^2w - 27xzw + yzw - 5z^2w - xw^2 - yw^2 + 7zw^2; \\ g_1 &:= -14x^2 - y^2 + xz + 2yz + 2z^2 + xw - yw - 2zw; \\ g_2 &:= -3x^2 + 7xy + 22y^2 - 5xz - z^2 - 17xw - 27yw + zw - 4w^2; \\ g_3 &:= 2xy + y^2 + 2xz - yz + xw - yw + zw - w^2; \\ g_4 &:= -8x^2 + xy - y^2 - 9yz - 9z^2 + xw - 10zw + 3w^2; \\ h &:= 2x^4 - 8x^3y - x^2y^2 + xy^3 + y^4 + 3x^3z - x^2yz + 2xy^2z - 10y^3z + x^2z^2 - 2xyz^2 \\ &\quad - 14y^2z^2 - 9xz^3 - z^4 + x^3w + 22x^2yw - 3xy^2w + 2y^3w + 7x^2zw + xyzw - 4xz^2w \\ &\quad - 17yz^2w + z^3w - 9x^2w^2 - xyw^2 - 5xzw^2 - 27yzw^2 + z^2w^2 - yw^3 - w^4. \end{aligned}$$

We start with examples with geometric Picard number one, produced by forcing different lattice structures on the Néron-Severi groups on different reductions, as in [vL07b].

EXAMPLE 1. Let X be the smooth quartic surface over \mathbb{Q} defined by

$$wf_1 + p_1zf_2 + p_2g_1g_2 + p_1p_2h = 0,$$

where $p_1 = 4409$ and $p_2 = 24659$. Thus X_{p_1} contains the conic C defined by $w = g_1 = 0$, and X_{p_2} contains the line L defined by $w = z = 0$. Using the methods from Section 2, we find

$$\begin{aligned} \rho(\overline{X}_{p_1}) &= 2 \text{ and } \text{disc}(\text{NS}(\overline{X}_{p_1})) = -3 \text{ mod } \mathbb{Q}^{\times 2}; \\ \rho(\overline{X}_{p_2}) &= 2 \text{ and } \text{disc}(\text{NS}(\overline{X}_{p_2})) = -1 \text{ mod } \mathbb{Q}^{\times 2}. \end{aligned}$$

Therefore, $\rho(\overline{X}) = 1$. Furthermore, $\text{NS}(\overline{X}_{p_1})$ is generated by the hyperplane section and the conic C , and $\text{NS}(\overline{X}_{p_2})$ is generated by the hyperplane section and the line L . In this example we observe $\rho(\overline{X}_p) > 4$ only for $p = 29$, where $\rho(\overline{X}_{29}) = 6$ and $\text{disc}(\text{NS}(\overline{X}_{29})) = -537$.

EXAMPLE 2. Let X be the K3 surface over \mathbb{Q} defined by

$$p_1(wf_1 + zf_2) + p_2(g_1g_2 + g_3g_4) + p_1p_2h = 0,$$

with $p_1 = 18869$ and $p_2 = 30047$. As in the previous example, X_{p_2} contains a line L . Now X_{p_1} contains the elliptic curve C defined by $g_1 = g_3 = 0$. Nonetheless, we still have

$$\begin{aligned} \rho(\overline{X}_{p_1}) &= 2 \text{ and } \text{disc}(\text{NS}(\overline{X}_{p_1})) = -3 \text{ mod } \mathbb{Q}^{\times 2}; \\ \rho(\overline{X}_{p_2}) &= 2 \text{ and } \text{disc}(\text{NS}(\overline{X}_{p_2})) = -1 \text{ mod } \mathbb{Q}^{\times 2}. \end{aligned}$$

Consequently, $\rho(\overline{X}) = 1$, $\text{NS}(\overline{X}_{p_1})$ is generated by the hyperplane section and the elliptic curve C , and $\text{NS}(\overline{X}_{p_2})$ is generated by the hyperplane section and the line L . As in the previous example, $\rho(\overline{X}_p) > 4$ for only one prime $p = 7$, where $\rho(\overline{X}_7) = 6$ and $\text{disc}(\text{NS}(\overline{X}_7)) = -345$.

In both examples, $\eta(\overline{X}) = 1$, $E_X = \mathbb{Q}$, and X does not have complex multiplication. We present the log-log plots of $\gamma(X, B)$ for the previous examples and their respective least square fit to a power law in Figure 1. We observe that

$$\gamma(X, B) \sim \frac{c_X}{\sqrt{B}}, \quad B \rightarrow \infty,$$

for some constant $c_X > 0$.

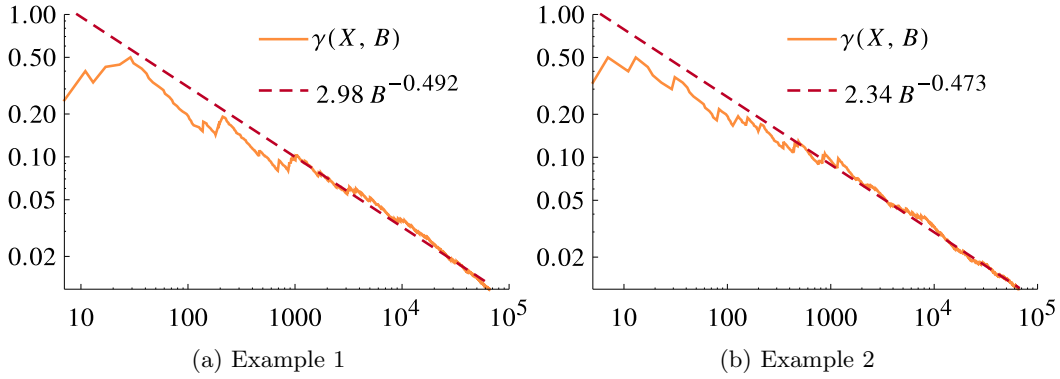


Figure 1: Log-log plots of γ and their least-square-fit to a power law in Examples 1 and 2.

Next, we present examples of K3 surfaces over \mathbb{Q} with geometric Picard number two. We achieve this by forcing an additional curve on X and by finding a prime p such that $\rho(\overline{X}_p) = 2$.

EXAMPLE 3. Let X be the K3 surface given by

$$wf_1 + zf_2 = 0;$$

it contains the line L defined by $w = z = 0$. For $p = 23$ we have $\rho(\overline{X}_p) = 2$.

EXAMPLE 4. Let X be the smooth quartic surface given by

$$wf_1 + g_1g_2 = 0,$$

containing the conic C defined by $w = g_1 = 0$. For $p = 17$ we have $\rho(\overline{X}_p) = 2$.

EXAMPLE 5. Let X be defined by

$$g_1g_2 + g_3g_4 = 0, \tag{3.1}$$

and containing the curve C given by $g_1 = g_3 = 0$. For $p = 31$ we have $\rho(\overline{X}_p) = 2$.

In Figure 2 we present plots of $\gamma(X, B)$ for the previous examples. These suggest that

$$\liminf_{B \rightarrow \infty} \gamma(X, B) \geq 1/2.$$

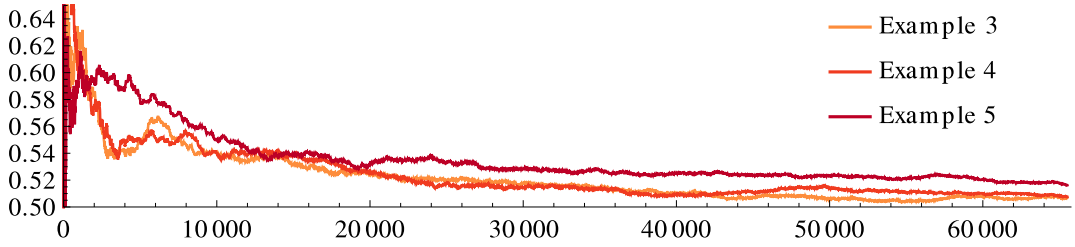


Figure 2: Plots of $\gamma(X, B)$ for the Examples 3, 4 and 5.

For these examples we also inspected the local density of $\Pi_{\text{jump}}(X)$. For this we resort to a moving average,

$$\delta(X, i, j) := \frac{\#\{i - j/2 < l \leq i + j/2 : p_l \in \Pi_{\text{jump}}(X)\}}{j}$$

where $\{p_1, p_2, p_3, \dots\}$ denotes the primes, on their natural order, at which X has good reduction. We present $\delta(X, i, 250)$ in Figure 3. We observe that the moving average oscillates slightly above $1/2$.

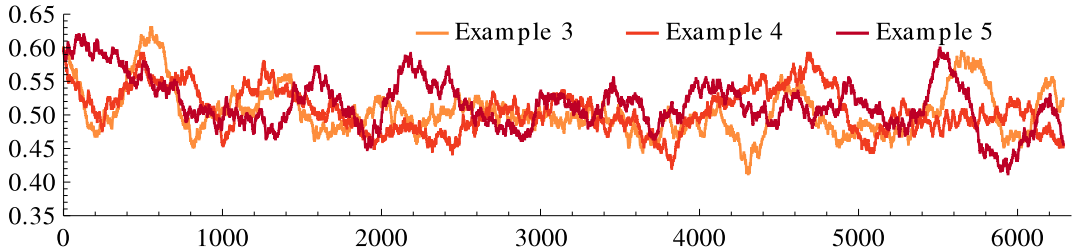


Figure 3: Plots of $\delta(X, i, 250)$ for the Examples 3, 4 and 5.

While in these examples we observed $\rho(\overline{X}_p) > 2$ more frequently, the number of primes such that $\rho(\overline{X}_p) > 4$ is quite small. We present those in Table 1.

Example 3		Example 4		Example 5	
p	$\rho(\overline{X}_p)$	p	$\rho(\overline{X}_p)$	p	$\rho(\overline{X}_p)$
3	6	3	10	3	6
11	6	5	10	17	6
13	6	11	6	347	6
47	6	29	6		
53	6	83	6		
181	6	491	6		
239	6	2777	6		
25087	6	3187	6		

Table 1: Primes $p < 2^{16}$ for which $\rho(\overline{X}_p) > 4$.

References

- AKR10** Timothy G. Abbott, Kiran S. Kedlaya, and David Roe. Bounding Picard numbers of surfaces using p -adic cohomology. In *Arithmetics, geometry, and coding theory (AGCT 2005)*, volume 21 of *Sémin. Congr.*, pages 125–159. Soc. Math. France, Paris, 2010.
- Bai07** Stephan Baier. The Lang-Trotter conjecture on average. *J. Ramanujan Math. Soc.*, 22(4):299–314, 2007.
- BGS07** Alin Bostan, Pierrick Gaudry, and Éric Schost. Linear recurrences with polynomial coefficients and application to integer factorization and Cartier-Manin operator. *SIAM J. Comput.*, 36(6):1777–1806, 2007.
- BHT11** Fedor Bogomolov, Brendan Hassett, and Yuri Tschinkel. Constructing rational curves on K3 surfaces. *Duke Math. J.*, 157(3):535–550, 2011.
- Cha11** François Charles. On the Picard number of K3 surfaces over number fields. *preprint*, 2011. [arXiv:1111.4117](https://arxiv.org/abs/1111.4117).
- Cha13** François Charles. The Tate conjecture for K3 surfaces over finite fields. *Invent. Math.*, 194(1):119–145, 2013.
- CHK14** Edgar Costa, David Harvey, and Kiran S. Kedlaya. Zeta functions of nondegenerate toric hypersurfaces via controlled reduction in p -adic cohomology. *in preparation*, 2014.
- Del72** Pierre Deligne. La conjecture de Weil pour les surfaces K3. *Invent. Math.*, 15:206–226, 1972.
- DP99** Chantal David and Francesco Pappalardi. Average Frobenius distributions of elliptic curves. *Internat. Math. Res. Notices*, (4):165–183, 1999.
- EJ08a** Andreas-Stephan Elsenhans and Jörg Jahnel. K3 surfaces of Picard rank one and degree two. In *Algorithmic number theory*, volume 5011 of *Lecture Notes in Comput. Sci.*, pages 212–225. Springer, Berlin, 2008.
- EJ08b** Andreas-Stephan Elsenhans and Jörg Jahnel. K3 surfaces of Picard rank one which are double covers of the projective plane. In *Higher-dimensional geometry over finite fields*, volume 16 of *NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur.*, pages 63–77. IOS, Amsterdam, 2008.
- EJ11a** Andreas-Stephan Elsenhans and Jörg Jahnel. On the computation of the Picard group for K3 surfaces. *Math. Proc. Cambridge Philos. Soc.*, 151(2):263–270, 2011.
- EJ11b** Andreas-Stephan Elsenhans and Jörg Jahnel. The Picard group of a K3 surface and its reduction modulo p . *Algebra Number Theory*, 5(8):1027–1040, 2011.
- EJ12** Andreas-Stephan Elsenhans and Jörg Jahnel. Kummer surfaces and the computation of the Picard group. *LMS J. Comput. Math.*, 15:84–100, 2012.
- Elk87** Noam D. Elkies. The existence of infinitely many supersingular primes for every elliptic curve over \mathbf{Q} . *Invent. Math.*, 89(3):561–567, 1987.
- Elk91** Noam D. Elkies. Distribution of supersingular primes. *Astérisque*, (198-200):127–132 (1992), 1991. Journées Arithmétiques, 1989 (Luminy, 1989).
- FKRS12** Francesc Fité, Kiran S. Kedlaya, Víctor Rotger, and Andrew V. Sutherland. Sato-Tate distributions and Galois endomorphism modules in genus 2. *Compos. Math.*, 148(5):1390–1442, 2012.
- FM96** Etienne Fouvry and M. Ram Murty. On the distribution of supersingular primes. *Canad. J. Math.*, 48(1):81–104, 1996.
- Har07** David Harvey. Kedlaya’s algorithm in larger characteristic. *Int. Math. Res. Not. IMRN*, (22):Art. ID rnm095, 29, 2007.
- HJP12** William Hart, Fredrik Johansson, and Sebastian Pancratz. FLINT: Fast Library for Number Theory, 2012. Version 2.3.0, <http://flintlib.org>.
- HKT13** Brendan Hassett, Andrew Kresch, and Yuri Tschinkel. Effective computation of Picard groups and Brauer-Manin obstructions of degree two K3 surfaces over number fields. *Rend. Circ. Mat. Palermo (2)*, 62(1):137–151, 2013.
- Kat09** Nicholas M. Katz. Lang-Trotter revisited. *Bull. Amer. Math. Soc. (N.S.)*, 46(3):413–457, 2009.
- LL12** Jun Li and Christian Liedtke. Rational curves on K3 surfaces. *Invent. Math.*, 188(3):713–727, 2012.
- LLR05** Qing Liu, Dino Lorenzini, and Michel Raynaud. On the Brauer group of a surface. *Invent. Math.*, 159(3):673–676, 2005.
- LT76** Serge Lang and Hale Trotter. *Frobenius distributions in GL_2 -extensions*. Lecture Notes in Mathematics, Vol. 504. Springer-Verlag, Berlin, 1976. Distribution of Frobenius automorphisms in GL_2 -extensions of the rational numbers.
- Mau12** Daves Maulik. Supersingular k3 surfaces for large primes. *preprint*, 2012. [arXiv:1203.2889](https://arxiv.org/abs/1203.2889).
- Maz73** Barry Mazur. Frobenius and the Hodge filtration (estimates). *Ann. of Math. (2)*, 98:58–95, 1973.
- Mil75** James S. Milne. On a conjecture of Artin and Tate. *Ann. of Math. (2)*, 102(3):517–533, 1975.
- Per13** Keerthi Madapusi Pera. The Tate conjecture for K3 surfaces in odd characteristic. *preprint*, 2013. [arXiv:1301.6326](https://arxiv.org/abs/1301.6326).
- PTvL12** Bjorn Poonen, Damiano Testa, and Ronald van Luijk. Computing Néron-Severi groups and cycle class groups. *preprint*, 2012. [arXiv:1210.3720](https://arxiv.org/abs/1210.3720).
- Sch12** Matthias Schuett. Two lectures on the arithmetic of K3 surfaces. *preprint*, 2012. [arXiv:1202.1066](https://arxiv.org/abs/1202.1066).
- Sho13** Victor Shoup. NTL: Number Theory Library, 2013. Version 6.0.0, <http://www.shoup.net/ntl/>.
- SV13** Steven Sperber and John Voight. Computing zeta functions of nondegenerate hypersurfaces with few monomials. *LMS J. Comput. Math.*, 16:9–44, 2013.
- vL07a** Ronald van Luijk. An elliptic K3 surface associated to Heron triangles. *J. Number Theory*, 123(1):92–119, 2007.

- vL07b** Ronald van Luijk. K3 surfaces with Picard number one and infinitely many rational points. *Algebra Number Theory*, 1(1):1–15, 2007.
- Zar83** Yuri G. Zarhin. Hodge groups of K3 surfaces. *J. Reine Angew. Math.*, 341:193–220, 1983.

Courant Institute of Mathematical Sciences
New York University
251 Mercer Street
New York, N.Y. 10012-1185
U.S.A.

edgarcosta@nyu.edu

Simons Foundation
160 Fifth Av.
New York, NY 10010
U.S.A.

tschinkel@cims.nyu.edu