Effective computations of Hasse–Weil zeta functions

by

Edgar Costa

A dissertation submitted in partial fulfillment

of the requirements for the degree of

Doctor of Philosophy

Department of Mathematics

Courant Institute of Mathematical Sciences

New York University

May 2015

Yuri Tschinkel

Abstract

This work covers two problems centered around arithmetic algebraic geometry and computational number theory. In Chapter 1, we present a new algorithm for computing the Hasse–Weil zeta functions of smooth hypersurfaces over finite fields, based on Kedlaya's approach, by computing an approximation of Frobenius action on p-adic cohomology with sufficient precision. In Chapter 2, 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.

Contents

List of Figures

List of Tables

Chapter 1

Computing zeta functions via p-adic cohomology

1.1 Introduction

An important research topic in number theory is the computation of the Hasse–Weil zeta function of an algebraic variety. In spite of decades of research, going back to elliptic curve experiments by Birch and Swinnerton-Dyer, such computations are in general not feasible over fields of large characteristic. In this chapter we present a new p-adic method to compute the Hasse–Weil zeta function of smooth hypersurfaces in projective spaces. This method enables us to handle generic surfaces and threefolds over fields of large characteristic, e.g., $p \sim 10^6$.

Let $\mathcal{Z}$ be a smooth algebraic variety over $\mathbb{F}_q$, where $q = p^a$, for p a prime. The Weil conjectures tell us that the Hasse–Weil zeta function has the form

$$\zeta_{\mathcal{Z}}(t) := \exp\left(\sum_{m=1}^{\infty} \frac{\#\mathcal{Z}(\mathbb{F}_{q^m})}{m} t^m\right) = \prod_i P_i(\mathcal{Z}, t)^{(-1)^{i+1}}, \tag{1.1}$$

where

$$P_i(\mathcal{Z}, t) := \det\left(1 - t\ \mathrm{Frob}\,|H^i_{\mathrm{et}}(\mathcal{Z}_{\overline{\mathbb{F}_q}}, \mathbb{Q}_\ell)\right) \in \mathbb{Z}[t],$$

and Frob is the Frobenius automorphisms.

We would like to efficiently determine $\zeta_{\mathcal{Z}}(t)$ from the defining equations of $\mathcal{Z}$. Efficient algorithms for this problem are necessary for the implementation of large scale numerical experiments, e.g., for testing the Sato–Tate conjecture [FKRS12], understanding the variation of Néron–Severi ranks [CT14] (see also Chapter 2), and other statistics on algebraic varieties.

For curves, we have at our disposal a variety of practical algorithms which can easily handle large characteristic. For example, for a curve of small genus or for an abelian variety of small dimension we can use Schoof's method [Sch85, Pil90, AH96] to compute $\zeta_{\mathcal{Z}}(t)$ in time and space polynomial in $\log q$, and exponentially in the genus/dimension. For an hyperelliptic curve of high genus one can use Kedlaya's algorithm [Ked01], where one computes the Frobenius action on p-adic cohomology (Monsky–Washnitzer cohomology); in this case the time/space dependence on g is polynomial, and quasi-linear in p. The dependence on p can be futher improved to $p^{1/2+\epsilon}$ [Har07].

However, prior to this method, this was not the case for varieties of higher dimension. Even though a great number of techniques has been developed in recent years, in general, only small primes p could be treated by these methods.

Our new approach relies on techniques introduced in [AKR10] and [Har07]. The time (respectively, space) dependence on p of Abbott–Kedlaya–Roe approach for projective hypersurfaces is at least $p^{\dim(\mathcal{Z})+1}$ (respectively, $p^{\dim(\mathcal{Z})}$). With the goal of improving the time and space dependence on p 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. Altogether, this reduces time dependence on p from polynomial in [AKR10] to quasi-linear. We also reduce the space complexity on p to $\log p$, allowing us to handle examples with much larger p than ever found in the literature.

Theorem 1.1. *Let $\mathcal{Z}$ be smooth hypersurface of degree d in $\mathbb{P}^n(\mathbb{F}_{p^a})$ with $p > \max\{2, n\}$ and $p \nmid d$. Assume that $\mathcal{Z}$ is S-smooth (see Definition 1.12) with $d \geq |S|$. For example, if $\mathcal{Z}$ is a nondegenerate hypersurface or $d > n$. We may compute $\zeta_{\mathcal{Z}}(t)$ in time*

$$p^{1+o(1)} d^{n^2+O(n)} a^{n+O(1)},$$

and space

$$\log p \; d^{n^2+O(n)} a^{n+O(1)}.$$

Using a modified version of [BGS07] one can reduce the time complexity to

$$p^{1/2+o(1)} d^{n^2+O(n)} a^{n+O(1)}.$$

Moreover, if one starts with a hypersurface over $\mathbb{Q}$, one may amortize the cost of computing the zeta functions of its reductions modulo various primes by using a remainder tree method see [CGH14, Har14, HS14a, HS14b]). With this approach the average time complexity for each prime $p < N$ is

$$(\log N)^{4+o(1)} d^{n^2+O(n)} a^{n+O(1)}.$$

Remark 1.2. *The hypotheses that $p > \max\{2, n\}$ and $p \nmid d$ are made solely to simplify the exposition; they could me removed with some extra work.*

Furthermore, jointly with David Harvey and Kiran Kedlaya we are generalizing this method to nondegenerate ample hypersurfaces in a projectively normal toric variety [CHK15].

We have not yet carefully analyzed the time and space complexity of the algorithm for this generalization but we expect that in the simplest case we have:

Theorem 1.3 ([CHK15])**.** *Let $\mathcal{Z}$ be a nondegenerate hypersurface in a projectively normal toric variety of dimension n over a finite field $\mathbb{F}_{p^a}$ with $p > \max\{2, n\}$. We may compute $\zeta_{\mathcal{Z}}(t)$ in time*

$$p^{1+o(1)}(a \operatorname{vol}(\Delta))^{O(n)},$$

and space

$$\log p(a \operatorname{vol}(\Delta))^{O(n)},$$

where Δ is the lattice polytope associated to the toric variety.

Using a modified version of [BGS07] one can reduce the time complexity to

$$p^{1/2+o(1)}(a \operatorname{vol}(\Delta))^{O(n)}.$$

Moreover, if one starts with a hypersurface over $\mathbb{Q}$, one may amortize the cost of computing the zeta functions of its reductions modulo various primes by using a remainder tree method see [CGH14, Har14, HS14a, HS14b]). With this approach the average time complexity for each prime $p < N$ is

$$(\log N)^{4+o(1)}(a \operatorname{vol}(\Delta))^{O(n)}.$$

To demonstrate the feasibility of the algorithm, the author implemented the quasi-linear version in the case that $\mathcal{Z}$ is a smooth hypersurface of degree d in $\mathbb{P}^n(\mathbb{F}_p)$ for $d > n$ and $p \nmid d$.

Jointly with Yuri Tschinkel in [CT14] (see also Chapter 2), we use this implementation to compute the zeta function of various smooth quartic surfaces modulo all primes $p < 2^{16}$. This implementation has also been used in the search for Calabi–Yau threefolds in the Dwork pencil that have height one but are not Bloch–Kato ordinary [BK86], the details will

be presented in [War15].

1.2 p-adic cohomology

In this section we introduce the notation for the rest of the chapter while we set up the theory of p-adic cohomology for use later on.

We denote by $\mathbb{F}_q$ the finite field with q elements and charactheristic $p > 0$. Let $\mathcal{Z}$ be a smooth hypersurface of degree d in $\mathcal{X} := \mathbb{P}^n_{\mathbb{F}_q}$, defined by the homogeneous polynomial $f_{\mathcal{Z}} \in \mathbb{F}_q[x_0, \ldots, x_n]$. Put $\mathcal{U} := \mathcal{X} \backslash \mathcal{Z} \cong \mathrm{Spec}(\mathcal{A})$, where $\mathcal{A}$ is the coordinate ring of $\mathcal{U}$, explicitly,

$$\mathcal{A} \cong \left\{ \sum_{k=0}^{m} \frac{g_k}{f_{\mathcal{Z}}^k} : g_k \in \mathbb{F}_q[x_0, \ldots, x_n] \text{ homogeneous of degree } dk \right\}. \tag{1.2}$$

We use multi-index notation, i.e., let $\beta = (\beta_i) \in \mathbb{N}_0^{n+1}$, then x^β denotes the monomial $x_0^{\beta_0} \ldots x_n^{\beta_n}$ of degree $|\beta| := \sum_{i=0}^n \beta_i$. Put $\mathbf{1} := (1, 1, \ldots, 1) \in \mathbb{N}_0^{n+1}$.

To simplify the exposition we assume $p > \max\{2, n\}$ and $p \nmid d$.

1.2.1 Rigid cohomology

Let H^i_{rig} denote the i-th rigid cohomology group in the sense of Berthelot [Ber97]. The Lefschetz hyperplane theorem combined with Poincaré duality, show that the map

$$H^i_{\mathrm{rig}}(\mathcal{X}) \to H^i_{\mathrm{rig}}(\mathcal{Z}),$$

induced by the inclusion $\mathcal{Z} \hookrightarrow \mathcal{X}$, is bijective for $i \neq n-1$. Moreover, we have the following Frobenius-equivariant exact sequence

$$0 \to H^n_{\mathrm{rig}}(\mathcal{U}) \to H^{n-1}_{\mathrm{rig}}(\mathcal{Z})(-1) \to H^{n+1}_{\mathrm{rig}}(\mathcal{X}) \to 0,$$

where $M(n)$ denotes M with its absolute Frobenius action multiplied by p^{-n}. Therefore, $H^n_{\mathrm{rig}}(\mathcal{U})(1)$ coincides with $H^{n-1}_{\mathrm{rig}}(\mathcal{Z})$, except if n is odd, then its generalized eigenspace for Frobenius of eigenvalue $q^{(n-1)/2}$ has dimension one less. In summary, we can rewrite (1.1) as

$$\zeta_{\mathcal{Z}}(t) = \frac{Q(t)^{(-1)^n}}{\prod_{i=0}^{n-1}(1-q^i t)}, \tag{1.3}$$

where

$$Q(t) = \det(1 - tq^{-1}\operatorname{Frob}_q | H^n_{\mathrm{rig}}(\mathcal{U})). \tag{1.4}$$

1.2.2 De Rham cohomology

For $m \geq 0$, let P_m denote the free $\mathbb{Z}_q$-module of homogenous polynomials in $\mathbb{Z}_q[x_0, \ldots, x_n]$ of degree m, further put $P_{m,\mathbb{Q}_q} := P_m \otimes_{\mathbb{Z}_q} \mathbb{Q}_q$. Choose an arbitrary lift $f \in P_d$ of $f_{\mathcal{Z}}$. Let Z be the zero locus of f in $X := \mathbb{P}^n_{\mathbb{Z}_q}$, $U := X \backslash Z$, and A be the coordinate ring of U, it has the same shape as $\mathcal{A}$, *mutatis mutandis*, in (1.2). Due to Kato [Kat89, Theorem 6.4]

$$H^i_{\mathrm{dR}}(U) \otimes_{\mathbb{Z}_q} \mathbb{Q}_q \cong H^i_{\mathrm{rig}}(\mathcal{U}),$$

where $H^i_{\mathrm{dR}}(U)$ is the i-th algebraic de Rham cohomology group of U over $\mathbb{Z}_q$. Furthermore, in [Gri69, Section 4] Griffiths gives an explicit description of $H^n_{\mathrm{dR}}(U_{\mathbb{Q}_q})$. Let

$$\Omega := \sum_{i=0}^{n} (-1)^i x_i \, \mathrm{d}x_0 \wedge \cdots \wedge (\text{omit } \mathrm{d}x_i) \wedge \cdots \wedge \mathrm{d}x_n \in \Omega^n(U),$$

then $H^n_{\mathrm{dR}}(U_{\mathbb{Q}_q})$ is isomorphic to the quotient of

$$\langle g\Omega/f^m : m \geq 1, g \in P_{dm-n-1,\mathbb{Q}_q}\rangle$$

by

$$\left\langle \left(f\frac{\partial g}{\partial x_i} - mg\frac{\partial f}{\partial x_i}\right)\frac{\Omega}{f^{m+1}} : m \geq 1, g \in P_{dm-n,\mathbb{Q}_q}\right\rangle.$$

In other words, given differential form $g\Omega/f^m$, we can reduce the order of the pole to $m-1$ if, and only if, $g \in \langle \partial f/\partial x_0, \ldots, \partial f/\partial x_n\rangle$.

Theorem 1.4 (Theorem of Macaulay [Mac94, pp 64-66])**.** *Let k be a field. Let $f_1, \ldots, f_r$ be a regular sequence of homogeneous polynomials in $k[x_0, \ldots, x_n]$, i.e., f_i is not a zero-divisor in*

$$k[x_0, \ldots, x_n]/\langle f_1, \ldots, f_{i-1}\rangle.$$

Let $d_i := \deg f_i$. For any ideal $I \subset k[x_0, \ldots, x_n]$, let $I^{(t)}$ denote the k-vector space of polynomails of degree t in I. Let

$$N(r,t) := \dim_k \left(k[x_0, \ldots, x_n]^{(t)}/(f_1, \ldots, f_r)^{(t)}\right).$$

Then

$$H_{k[x_0,\ldots,x_n]/(f_1,\ldots,f_r)}(T) := \sum_{t\geq 0} N(r,t)x^t = (1-x^{d_1})\cdots(1-x^{d_r})(1-x)^{-n-1}.$$

Corollary 1.5. *We have*

$$P_{\alpha,\mathbb{Q}_q} \subset \langle \partial f/\partial x_0, \ldots, \partial f/\partial x_n\rangle$$

for $\alpha > (n+1)(d-2)$.

Altogether, this gives rise to a natural algorithm to compute a basis for $H^n_{\mathrm{dR}}(U_{\mathbb{Q}_q})$ and to

rewrite any class of the form $g\Omega/f^m$ into this basis. First, we write down a monomial basis B for $H^n_{\mathrm{dR}}(U_{\mathbb{Q}_q})$. For $m = 1, \ldots, n$, find monomials of degree $dm - n - 1$ in $\mathbb{F}_q[x_0, \ldots, x_n]$ which project onto a basis of of the coKernel of the map

$$(\mu_0, \ldots, \mu_n) \longmapsto \sum_{i=0}^{n} \mu_i \frac{\partial f_{\mathcal{Z}}}{\partial x_i},$$

where μ_i are monomials of degree $dm - n - 1 - (d-1)$. Then, lift these monomials to $\mathbb{Z}_q[x_0, \ldots, x_n]$. For each such lift $\mu \in \mathbb{Z}_q[x_0, \ldots, x_n]$, include $\mu\Omega/f^m$ in B.

Using Corollary 1.5, we can iteratively reduce the pole order of any class to n, as $P_{dm-n-1,\mathbb{Q}_q} \subset \langle \partial f/\partial x_0, \ldots, \partial f \partial x_n \rangle$ for $m > n$. Lastly, given $g\Omega/f^m$ with $m \leq n$ we can use the previous maps to decompose g as a linear combination of $\partial f/\partial x_i$ plus basis elements. This process is known as the *Griffiths–Dwork reduction method*.

Moreover,

$$\chi(Z_{\mathbb{Q}_q}) = \langle c_n(T_{Z_{\mathbb{Q}_q}}), [Z_{\mathbb{Q}_q}] \rangle = \frac{1}{d}\left((1-d)^{n+1} - 1\right) + n + 1,$$

thus,

$$\dim H^n(U_{\mathbb{Q}_q}) = (-1)^{n+1}\left(\frac{1}{d}\left((1-d)^{n+1} - 1\right) + 1\right). \tag{1.5}$$

1.2.3 Monsky-Washnitzer cohomology

Let $A^\dagger$ be the weak (p-adic) completion of A; explicitly, $A^\dagger$ is the ring of power series

$$\sum_{k \geq 0} \frac{g_k}{f^k},$$

where $g_k \in P_{dk}$ and for some $a, b > 0$, $p^{\max\{0,\lfloor ak-b \rfloor\}} \,|\, g_k$ for all $k \geq 0$. We define the associated logarithm de Rham complex $\Omega^{\dagger,\bullet}$ by

$$\Omega^{\dagger,i} := \Omega^i \otimes_A A^\dagger;$$

denote the cohomology group of this complex by $H^{\dagger,\bullet}$. Moreover, $H^{\dagger,\bullet} \otimes_{\mathbb{Z}_q} \mathbb{Q}_q$ is the definition of the Monsky-Washnitizer cohomology [vdP86].

The map

$$\Omega^\bullet \otimes_{\mathbb{Z}_q} \mathbb{Q}_q \to \Omega^{\dagger,\bullet} \otimes_{\mathbb{Z}_q} \mathbb{Q}_q$$

is a quasi-isomorphism [Kat68, Mon70, vdP86], i.e., the induced maps

$$H^i_{\mathrm{dR}} \otimes_{\mathbb{Z}_q} \mathbb{Q}_q \to H^{\dagger,i} \otimes_{\mathbb{Z}_q} \mathbb{Q}_q$$

are isomorphisms. Thus, we can identify the algebraic de Rham cohomology of $U_{\mathbb{Q}_q}$ with the Monsky-Washnitzer cohomology of $\mathcal{U}$. Furthermore, we also have

$$H^{\dagger,\bullet} \otimes_{\mathbb{Z}_q} \mathbb{Q}_q \cong H^\bullet_{\mathrm{rig}},$$

where the latter isomorphism is functorial with respect to the geometry in charactheristic p [Ber97, Proposition 1.10]. Thus, $H^{\dagger,i}$ receives an action of the Frobenius automorphism.

We lift the p-th power Frobenius on $\mathbb{F}_q$ to $A^\dagger$ as follows. On $\mathbb{Z}_q$, we take the canonical Witt vector Frobenius, and set $\mu^\sigma = \mu^p$ for any monomial $\mu \in \mathbb{Z}_q[x_0, \ldots, x_n]$. Finally, we extend it to $A^\dagger$ by the formula

$$\sigma\left(\frac{g}{f^m}\right) := \sigma(g)\sigma(f)^{-m} = \sigma(g) \sum_{i \geq 0} \binom{-m}{i} \frac{(\sigma(f) - f^p)^i}{f^{p(m+i)}}, \tag{1.6}$$

where $k \geq 0$ and $g \in P_{dk}$. The above series converges (because p divides $\sigma(f) - f^p$) and the definitions ensures that σ is an endomorphism of $A^\dagger$. We further extend σ to $\Omega^{\dagger,\bullet}$ by $\sigma(g\,\mathrm{d}h) := \sigma(g)\,\mathrm{d}(\sigma(h))$.

1.3 The Frobenius action on differentials

Our method follows very closely that introduced by Abbott–Kedlaya–Roe [AKR10]. Following Kedlaya's idea for hyperelliptic curves [Ked01], Abbott–Kedlaya–Roe compute a p-adic approximate of the Frobenius action on $H^n_{\mathrm{rig}}(\mathcal{U})$, by applying a truncation of σ (in $\Omega^{\dagger,n}$) to a basis of $H^n_{\mathrm{dR}}(U_{\mathbb{Q}_q})$. Next, they reduce the image of the truncation back to the basis by applying the Griffiths–Dwork reduction method.

Their approach makes surfaces of low degree feasible for primes < 20. However, examples over large characteristic are out of reach with their method, its running time (respectively, space) dependence on p is at least p^n (respectively, p^{n-1}), as they work with dense polynomials of at least degree p in n variables, e.g., $\sigma(f) - f^p$ in (1.6).

In this section we estimate p-adic precision needed to keep the error introduced by truncation within a fixed range and we find a sparse expression for the truncation of the Frobenius action in a sparser fashion relative to p, i.e., where the number of terms does not depend on p, as in [Har07].

We start by analyzing the loss of p-adic precision incurred when one reduces a given differential into standard form. We say that an element in $H^n_{\mathrm{dR}}(U_{\mathbb{Q}_q})$ is integral if is in the $\mathbb{Z}_q$ span of the basis B constructed in the Section 1.2.2. This definition differs slightly for $p \leq n$, see [AKR10, Section 3.4].

Definition 1.6. *For m a positive integer, we define $\varphi(m)$ be the smallest poisive integer t with the following property: for each form $\omega = g\Omega/f^m$ with $g \in P_{dm-n-1}$, $p^t\omega$ represents an integral element in $H^n_{dR}(U_{\mathbb{Q}_q})$.*

Lemma 1.7. *For $m > 0$,*

$$\varphi(m) \leq \nu_p((m-1)!) \leq \left\lfloor \frac{m-1}{p-1} \right\rfloor.$$

Proof. Applying Griffiths–Dwork reduction to $g\Omega/f^m$ with $g \in P_{dm-n-1}$ involves division at most by $(m-1)!$, and the latter has p-adic valuation at most $\lfloor (m-1)/(p-1) \rfloor$. □

Using a calculation in algebraic de Rham cohomology over $\mathbb{Z}_q$ we can derive a much more permissive inequality.

Proposition 1.8. *[AKR10, Proposition 3.4.6] For $m > 0$,*

$$\varphi(m) \leq \sum_{i=1}^{n} \lfloor \log_p \max\{1, m-i\} \rfloor \leq n \log_p(m-1).$$

With a bit more work, see [AKR10, Proposition 3.4.7], one can can give an upper for $\varphi(m)$ of the form $(n-1)\log_p(m)$ plus a constant.

Remark 1.9. *Let $\omega_m = g_m\Omega/f^m$ and $\omega_l = g_l\Omega/f^l$ a pole reduction of ω_m. One would hope that $\nu_p(g_l) \geq \nu_p(g_m) - \varphi(m)$, but it isn't true in general. There are examples where $\nu_p(g_l) = \nu_p(g_m) - \nu_p((m-1)!/(l-1)!)$.*

Let $x^\beta\Omega/f^m$ be an element of B, i.e., an integral basis element of $H^n_{\mathrm{dR}}(U_{\mathbb{Q}_q})$. Mazur's inequality [Maz73] implies that

$$p^{m-n-1}\sigma\left(\frac{x^\beta\Omega}{f^m}\right)$$

is an integral element. We can state our problem as follows: given $r > 0$ compute the reduction, i.e., the coordinates with respect to B, of

$$p^{m-n-1}\sigma\left(\frac{x^\beta\Omega}{f^m}\right)$$

modulo p^r.

Recall that by (1.6)

$$p^{m-n-1}\sigma\left(\frac{x^\beta\Omega}{f^m}\right) = p^{m-1}\frac{x^{p(\beta+\mathbf{1})}\Omega}{x^{\mathbf{1}}f^{pm}}\sum_{i\geq 0}\binom{-m}{i}\left(\frac{\sigma(f)-f^p}{f^p}\right)^i \tag{1.7}$$

and p divides $\sigma(f) - f^p$. Our first goal is to find N such that the reduction of

$$p^{m-1}\frac{x^{p(\beta+\mathbf{1})}\Omega}{x^{\mathbf{1}}f^{pm}}\sum_{i=0}^{N-1}\binom{-m}{i}\left(\frac{\sigma(f)-f^p}{f^p}\right)^i$$

agrees modulo p^r with reduction of $p^{m-n-1}\sigma(x^\beta\Omega/f^m)$. In other words, we want to determine N such that

$$m - 1 + i - \varphi(p(m+i)) \geq r \quad \text{for } i \geq N. \tag{1.8}$$

For example, using Proposition 1.8, one can take

$$m + N \geq (n+r)\left(1 + \frac{n\log(n+r)}{(n+r)\log p - n}\right) \in O(n+r). \tag{1.9}$$

This inequality is useful for bounding the running time of the algorithm. However, in practice, one can usually pick a much lower N by using a similar approach to the one described in [AKR10, Section 3.5], see Example 1.11.

Now we formally rewrite the action of σ in a sparser fashion, where the number of terms does not depend on p, as in [Har07, Proposition 4.1].

Lemma 1.10. *Let $x^\beta\Omega/f^m$ be an integral basis element of $H^n_{dR}(U_{\mathbb{Q}_q})$. Let N, m and r be positive integers such that equation (1.8) holds. Further, put $s = N + m - 1$ and let $C_{i,\alpha}$ be*

the coefficient of x^α in f^i. For $0 \le i < N$ we define

$$D_{j,m} := \sum_{i=j}^{N-1} (-1)^{i+j} \binom{-m}{i} \binom{i}{j}$$

The reduction of

$$\sum_{j=0}^{N-1} \sum_{|\alpha|=dj} p^{m-1} \left(D_{j,m} \sigma(C_{j,\alpha}) \bmod p^s \right) \frac{x^{p(\beta+\alpha+\mathbf{1})}}{f^{p(m+j)}} \frac{\Omega}{x^{\mathbf{1}}} \tag{1.10}$$

agrees modulo p^r with the reduction of $p^{m-n-1}\sigma\left(\frac{x^\beta \Omega}{f^m}\right)$.

Further, the number of monomials in the expression above is at most $\binom{d(N-1)+n+1}{n+1}$.

Proof. This follows by truncating the series in (1.7), taking into account the observations above, and then rewriting it formally:

$$\begin{aligned}
p^{m-1} \frac{x^{p(\beta+\mathbf{1})}\Omega}{x^{\mathbf{1}} f^{pm}} \sum_{i=0}^{N-1} \binom{-m}{i} \left(\frac{\sigma(f) - f^p}{f^p} \right)^i &= p^{m-1} \frac{x^{p(\beta+\mathbf{1})}\Omega}{x^{\mathbf{1}} f^{pm}} \sum_{i=0}^{N-1} \binom{-m}{i} \sum_{j=0}^{i} \binom{i}{j} (-1)^{i+j} \frac{\sigma(f^j)}{f^{pj}} \\
&= p^{m-1} \frac{x^{p(\beta+\mathbf{1})}\Omega}{x^{\mathbf{1}} f^{pm}} \sum_{j=0}^{N-1} \sum_{i=j}^{N-1} (-1)^{i+j} \binom{-m}{i} \binom{i}{j} \frac{\sigma(f^j)}{f^{pj}} \\
&= p^{m-1} \frac{x^{p(\beta+\mathbf{1})}\Omega}{x^{\mathbf{1}} f^{pm}} \sum_{j=0}^{N-1} D_{j,m} \frac{\sigma(f^j)}{f^{pj}} \\
&= \sum_{j=0}^{N-1} \sum_{|\alpha|=dj} p^{m-1} D_{j,m} \sigma(C_{j,\alpha}) \frac{x^{p(\beta+\alpha+\mathbf{1})}}{f^{p(m+j)}} \frac{\Omega}{x^{\mathbf{1}}}
\end{aligned}$$

Finally, we can evaluate the truncated series modulo p^s, as for $l < N$ we have

$$s - \varphi(p(m+l)) \ge s - \varphi(p(m+N)) \ge r.$$

□

Example 1.11. *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 the characteristic polynomial of the Frobenius action on $H^3_{rig}(\mathcal{U})$ to deduce the Hasse–Weil zeta function. This can be achieved using the Newton identities combined with Mazur's inequality [Maz73]. Using an algorithm similar to the one described in [AKR10, Section 3.5] we can achieve much lower values s and N. We present those in Table 1.1.*

m	1	2	3
r	1	2	2
N	3	3	2
s	3	4	4

Table 1.1: The different values of r, N and s for each m to compute the Hasse–Weil zeta function of a quartic K3 surface over $\mathbb{F}_p$, where $p > 41$.

1.4 Controlled reduction

In this section we introduce our second refinement, a variation of Griffiths–Dwork reduction, called *controlled reduction*, which is optimized to preserve sparsity of forms. This method was first introduced by Harvey in a series of lectures, see [Har10a, Har10b, Har10c]. This technique is crucial for our application, as careless application of Griffiths–Dwork reduction method to a sparse form will easily lead to a dense form.

Definition 1.12. *For $S \subset \{0, \ldots, n\}$ let*

$$J_S := \langle \partial f/\partial x_i \rangle_{i \in S} \oplus \langle x_i \partial f/\partial x_i \rangle_{i \notin S}$$

We say that the hypersurface defined by the homogenous polynomial f is S-smooth if J_S

defines the empty scheme, i.e., $\operatorname{rad} J_S = \langle x_0, \ldots, x_n \rangle$. *We say that* f *is nondegenerate if we can take* $S = \emptyset$.

This condition can be geometrically interpreted as follows. For all subsets T of the complement of S in $\{0, \ldots, n\}$, the intersection of the hypersurface with the coordinate hyperplanes defined by $\{x_i\}_{i \in T}$ is smooth. Taking $S = \{0, \ldots, n\}$ is equivalent to the hypersurface being smooth.

Remark 1.13. *Although smoothness is an intrinsic property of the hypersurface,* S*-smoothness, for* $S \neq \{0, \ldots, n\}$*, is coordinate dependent.*

Remark 1.14. *Let* Δ *be the Newton polytope of* f*, i.e., the convex hull of its support. In a similar fashion, we define* Δ*-nodegeneracy as intersection of the hypersurface with* τ *to be smooth for all the faces* $\tau \subseteq \Delta$*. The set of* Δ*-nondenerate polynomials forms an open subset in the affine space parameterizing their coefficients* $\Delta \cap \mathbb{Z}^{n+1}$*. Under mild hypothesis, such as when* Δ *contains an unimodular simplex, this subset is Zariski dense [GKZ94]. Thus in most cases, for* p *large enough, it is easy to find a change of coordinates* η *for which* $f \circ \eta$ *becomes nondegenerate.*

Proposition 1.15 (Controlled reduction)**.** *Assume that* f *is* S*-smooth with* $d \geq |S|$*. Let* $u = (u_i)$ *and* $v = (v_i) \in \mathbb{N}_0^{n+1}$*, with* $|v| = d$ *and for* $i \in S$ $u_i = 0$ *if* $v_i = 0$*. Put* $x^S := \prod_{i \in S} x_i$.

There is a $\mathbb{Z}_q$*-linear map*

$$R_{u,v} : P_{dn-n} \longrightarrow P_{dn-n}$$

such that

$$m \frac{x^{u+v} g}{x^S} \frac{\omega}{f^{m+1}} \equiv x^u \frac{R_{u,v}(g)}{x^S} \frac{\Omega}{f^m}$$

in $H^n_{dR}(U_{\mathbb{Q}_q})$.

Further, $R_{(x_0,\ldots,x_n),v}$ *can be represented as a* $\binom{dn}{n} \times \binom{dn}{n}$ *matrix with entries in* $\mathbb{Z}_q[x_0, \ldots, x_n]$ *with degree at most 1.*

Proof. From our assumptions one can easily see that $x^S | x^v g$ and $\deg x^v g / x^S = dn - n + d - |S|$, thus, by Macaulay's Theorem 1.4 we have $x^v G / x^S \in J_S$. Combining this with Griffiths–Dwork reduction method we obtain

$$\begin{aligned} m\frac{x^{u+v}g}{x^S}\frac{\Omega}{f^{m+1}} &= mx^u\left(\sum_{i\in S} g_i\frac{\partial f}{\partial x_i} + \sum_{i\notin S} x_i g_i \frac{\partial f}{\partial x_i}\right)\frac{\Omega}{f^{m+1}} \\ &\equiv \left(\sum_{i\in S}\frac{\partial}{\partial x_i}\left(x^u g_i\right) + \sum_{i\notin S}\frac{\partial}{\partial x_i}\left(x_i x^u g_i\right)\right)\frac{\Omega}{f^m}. \end{aligned}$$

Finally, by expanding the previous formula and factoring out x^u we get

$$\begin{aligned} m\frac{x^{u+v}g}{x^S}\frac{\Omega}{f^{m+1}} &\equiv \left(\sum_{i\in S}\frac{u_i x^u g_i + x_i x^u \partial g_i/\partial x_i}{x_i} + \sum_{i\notin S}(u_i+1)x^u g_i + x_i x^u \partial g_i/\partial x_i\right)\frac{\Omega}{f^m} \\ &= x^u \frac{h + \sum_{i=0}^n u_i h_i}{x^S}\frac{\Omega}{f^m}, \end{aligned}$$

where $\deg h_i = \deg h = dn - n$. □

Remark 1.16. *The Proposition 1.15 still holds for $d < |S|$, however we must have $u_i = 0$ for some $i \in S$.*

Remark 1.17. *If $d > n$ then it is enough to assume just smoothness, i.e., we can take $S = \{0, \ldots, n\}$.*

Straightforward application of this technique to each term in equation (1.10) reduces time dependence on p of Abbott–Kedlaya–Roe's approach from p^n to $p^{1+\epsilon}$. However, the time depence on n is still exponential, since using Proposition 1.15 amounts to performing matrix-vector multiplications with matrices of size $\binom{dn}{n} = \Omega((de)^n/\sqrt{2\pi n})$. For example, for a quartic K3 surface, i.e, $d = 4$ and $n = 3$, we must handle matrices of size 220, and for a quintic Calabi-Yau threefold, i.e., $d = 5$ and $n = 4$, the matrix size increases to 4845.

If f is nondegenerate, we can reduce the matrix size to d^n, i.e., cutting the size down

by a factor of $e^n/\sqrt{2\pi n}$, at the expense of making the expression for the reduction matrix slightly more complicated. This is achieved by recursively applying the ideas of Proposition 1.15. This trick for f nondegenerate was also discovered independently by Kedlaya. This is a significant improvement even for small n. For example, for a quartic plane curve it reduces the matrix size from 28 to 16, thus we save a factor of $(28/16)^2 \sim 3.06$ over the generic case, for a K3 surface the saving factor is $(220/64)^2 \sim 11.82$ and it increases to $(4845/625)^2 \sim 60.09$ for a Calabi-Yau 3-fold.

Proposition 1.18. *Assume that f is non-degenerate. Let $u = (u_i)$ and $v = (v_i) \in \mathbb{N}_0^{n+1}$, with $|v| = d$. Let Ψ_l denote the free $\mathbb{Z}_q$-module of homogeneous polynomials of degree dl in $\mathbb{Z}_q[x_0, \ldots, x_n]/J_\emptyset$.*

There is a $\mathbb{Z}_q$-linear map

$$S_{u,v} : \Psi_0 \oplus \cdots \oplus \Psi_n \longrightarrow \Psi_0 \oplus \cdots \oplus \Psi_n$$
$$(a_0, \ldots, a_n) \longmapsto (s_0, \ldots, s_n)$$

such that

$$x^{u+v} \sum_{i=0}^{n} (m+i)! a_i \frac{\Omega}{f^{m+i+1}} \equiv x^u \sum_{i=0}^{n} (m+i-1)! s_i \frac{\Omega}{f^{m+i}}$$

in $H^n_{dR}(U_{\mathbb{Z}_q})$.

Further, $S_{(x_0,\ldots,x_n),v}$ can be represented as a $d^n \times d^n$ matrix with entries in $\mathbb{Z}_q[x_0, \ldots, x_n]$ with degree at most $n+1$.

Proof. We start by giving an explicit description of the map. Put $\psi_l := \dim \Psi_l$ and let $\{\mu_{l,j}\}_{j=1,\ldots,\psi_l}$ be a monomial basis of Ψ_l. Observe that $\psi_l = 0$ for $l > n$ and $\psi_0 = 1$, by Macaulay's Theorem 1.4.

Given $h_l \in P_{dl}$, we can rewrite it as

$$h_l = \sum_{i=0}^{n} g_i x_i \frac{\partial f}{\partial x_i} + \sum_{j=1}^{\psi_l} c_j \mu_{l,j}.$$

Thus, by the Griffiths–Dwork reduction method, as in Proposition 1.15, we get

$$\begin{aligned}(m+l)!x^u h_l \frac{\Omega}{f^{m+l+1}} \equiv (m+l-1)!x^u \left(\sum_{i=0}^{n} (u_i+1)g_i + x_i \frac{\partial g_i}{\partial x_i} \right) \frac{\Omega}{f^{m+l}} \\ + (m+l)!x^u \left(\sum_{j=1}^{\psi_l} c_j \mu_{l,j} \right) \frac{\Omega}{f^{m+l+1}}\end{aligned}$$

in $H^n_{\mathrm{dR}}(U_{\mathbb{Q}_q})$. Let $\rho_{l,u}$ and π_l be the $\mathbb{Z}_q$-linear maps

$$\begin{aligned}\rho_{l,u} &: P_{dl} \longrightarrow P_{d(l-1)} \\ \pi_l &: P_{dl} \longrightarrow \Psi_l\end{aligned}$$

defined by

$$\begin{aligned}\rho_{l,u}(h_l) &:= \sum_{i=0}^{n} (u_i+1)g_i + x_i \frac{\partial g_i}{\partial x_i} \\ \pi_l(h_l) &:= \sum_{j=1}^{\psi_l} c_j \mu_{l,j}.\end{aligned}$$

Now we apply the ideas of Proposition 1.15 recursively. Explicitly, put

$$\begin{aligned}b_l &:= \pi_l(h_l) \in \Psi_l \\ h_{l-1} &:= \rho_{l,u}(h_l) \in P_{d(l-1)}.\end{aligned}$$

Therefore,

$$\begin{aligned}(m+l)!x^u h_l \frac{\Omega}{f^{m+l+1}} &\equiv x^u \left((m+l-1)! \frac{h_{l-1}}{f^{l-1}} + (m+l)! \frac{b_l}{f^l} \right) \frac{\Omega}{f^m} \\ &\equiv x^u \left((m+l-2)! \frac{h_{l-2}}{f^{l-2}} + (m+l-1)! \frac{b_{l-1}}{f^{l-1}} + (m+l)! \frac{b_l}{f^l} \right) \frac{\Omega}{f^m} \\ &\dots \\ &\equiv x^u \left(\sum_{i=0}^{l} (m+i)! \frac{b_i}{f^i} \right) \frac{\Omega}{f^m},\end{aligned}$$

and this defines a $\mathbb{Z}_q$-linear map

$$\begin{aligned}\tilde{\rho}_{l,u} : P_{dl} &\longrightarrow \Psi_0 \oplus \cdots \oplus \Psi_l \\ h_l &\longmapsto (b_0, \dots, b_l).\end{aligned}$$

Further, $\tilde{\rho}_{l,(x_0,\dots,x_n)}$ can be represented as a matrix with entries in $\mathbb{Z}_q[x_0, \dots, x_n]$ with degree at most l, since $\rho_{l,(x_0,\dots,x_n)}$ can be represented as a matrix with entries in $\mathbb{Z}_q[x_0, \dots, x_n]$ with degree at most 1.

Finally, given $v = (v_i) \in \mathbb{N}_0^{n+1}$, with $|v| = d$, and $(a_0, \dots, a_n) \in \Psi_0 \oplus \cdots \oplus \Psi_n$ we apply $\tilde{\rho}_{i+1,u}$ to $x^v a_i$ and obtain the desired map, i.e.,

$$S_{u,v}(a_0, \dots, a_n) := \sum_{i=0}^{n} \tilde{\rho}_{i+1,u}(x^v a_i).$$

Therefore, the map $S_{(x_0,\dots,x_n),v}$ can be represented as a matrix with entries in $\mathbb{Z}_q[x_0, \dots, x_n]$ with degree at most $n+1$.

We finish by proving

$$\dim(\Psi_0 \oplus \cdots \oplus \Psi_n) = \sum_{i=0}^{n} \psi_i = d^n.$$

Write

$$\sum_{i=0}^{(d-1)(n+1)} c_{n,i}t^i := \left(\frac{1-t^d}{1-t}\right)^{n+1} = \left(1+\cdots+t^{d-1}\right)^{n+1},$$

by Macaulay's Theorem 1.4, we want to show that $\sum_{i=0}^{n} c_{n,di} = d^n$ for $n \geq 0$. We prove something stronger

$$\sum_{i \bmod d \equiv k} c_{n,i} = d^n.$$

We proceed by induction on n. The base case, $n = 0$, it is straightforward. For $n > 0$, we have the following recursive relation

$$\sum_{i=0}^{(d-1)(n+1)} c_{n,i}t^i = \left(1+\cdots+t^{d-1}\right) \sum_{i=0}^{(d-1)n} c_{n-1,i}t^i.a$$

Therefore,

$$\begin{aligned}
\sum_{i \bmod d \equiv k} c_{n,i} &= \sum_{i \bmod d \equiv k} \sum_{j=0}^{d-1} c_{n-1,i-j} \\
&= \sum_{j=0}^{d-1} \sum_{i \bmod d \equiv k-j} c_{n-1,i} \\
&= dd^{n-1} && \text{(by induction on hypothesis)} \\
&= d^n.
\end{aligned}$$

□

Remark 1.19. *A more careful analysis of the map $S_{(x_0,\ldots,x_n),v}$, shows that the entries of the matrix blocks corresponding to the map $\Psi_i \longrightarrow \Psi_j$ have degree at most $i - j + 1$, except if*

$i - j < 0$, then the entries are all zero.

$$S_{(x_0,\ldots,x_n),v} = \begin{array}{c} \\ \Psi_0 \\ \Psi_1 \\ \Psi_2 \\ \vdots \\ \Psi_n \end{array} \begin{array}{c} \begin{array}{ccccc} \Psi_0 & \Psi_1 & \Psi_2 & \cdots & \Psi_n \end{array} \\ \begin{pmatrix} \deg \leq 1 & \deg \leq 2 & \deg \leq 3 & \cdots & \deg \leq n+1 \\ \deg \leq 0 & \deg \leq 1 & \deg \leq 2 & \cdots & \deg \leq n \\ 0 & \deg \leq 0 & \deg \leq 1 & \cdots & \deg \leq n-1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \deg \leq 1 \end{pmatrix} \end{array}$$

Remark 1.20. *Proposition 1.18 still holds if we redefine Ψ_l as the free $\mathbb{Z}_q$-module of homogeneous polynomials of degree $dl + j$ in $\mathbb{Z}_q[x_0, \ldots, x_n]/J_\emptyset$, for some fixed $j < d$.*

Further, if we take $j > d - (n+1)$, then $\psi_n = 0$, and $S_{(x_0,\ldots,x_n),v}$ can be represented as a $d^n \times d^n$ matrix with entries in $\mathbb{Z}_q[x_0, \ldots, x_n]$ with degree at most n.

1.5 The algorithm

In this section we describe the main algorithm for computing a p-adic approximate of the p-th power Frobenius matrix on $H^n_{\text{rig}}(\mathcal{Z})$ and analyze the time and space requirements. The basic idea is to start with the approximation of $p^{-1}\sigma\left(x^\beta \Omega / f^m\right)$ given by Lemma 1.10, where $x^\beta \Omega / f^m$ is an integral basis element of $H^n_{\text{dR}}(U_{\mathbb{Q}_q})$. Then use the reductions maps from Proposition 1.15 and/or Proposition 1.18 to reduce the order of the pole of each term and compute the coordinates of the approximation of $p^{-1}\sigma\left(x^\beta \Omega / f^m\right)$.

1.5.1 Step I : Precision estimates

Let r_m be the desired relative p-adic precision for $\sigma\left(x^\beta \Omega / f^m\right)$. Pick N_m such that

$$m - 1 + i - \varphi(p(m+i)) \geq r_m \quad \text{for } i \geq N_m,$$

and set $s_m := N_m + m - 1$. The algorithm works in

$$R := \mathbb{Z}_q / p^M \mathbb{Z}_q,$$

where

$$M := \max\{r_m + \nu_p((ps_m - 1)!) - m + 1\}.$$

Let $r := \max\{r_m\}$ and $N := \max\{N_m\}$, then by equation (1.9), we can take N and M to be in $O(n + r)$.

We use the $\tilde{O}(-)$ notation that ignores logarithmic factors, i.e., $\tilde{O}(f)$ denotes the class of functions that lie in $O\left(f \log^k f\right)$ for some $k \geq 0$. Each ring element of R requires $O(Ma \log p)$ storage space. Basic ring operations in R (addition, multiplication and division) have bit-complexity $\tilde{O}(Ma \log p)$. Further, applying σ to any element of the ring can be accomplished in time $\tilde{O}(Ma^2 \log p)$, i.e., it requires the equivalent time as performing $O(a)$ basic ring operations.

1.5.2 Step II: Linear algebra

For certain values of l we want to compute how to write every element of P_l as a linear combination of $\partial f / \partial x_i$ plus possibly some monomials of degree l which are not in the ideal. This is an explicit linear algebra problem associated to the following map

$$\begin{aligned} M_l : (P_{l-(d-1)})^{n+1} &\longrightarrow P_l \\ (\mu_0, \ldots, \mu_n) &\longmapsto \textstyle\sum_{i=0}^{n} \mu_i \frac{\partial f}{\partial x_i}. \end{aligned} \tag{1.11}$$

In general, we may solve this problem over $\mathbb{F}_q$ in $O(mn^2 + m^3)$ field operations for a matrix of size $m \times n$. Applying Newton's method we can lift the solution from $\mathbb{F}_q$ to R in $O(\log(M) m^3)$ operations in R.

Compute a monomial basis B for $H^n_{\mathrm{dR}}(U_{\mathbb{Q}_q})$, as described in Section 1.2.2, by solving these problems for $l = dm - n - 1$, where $m = 1, \ldots, n$.

Solve the same problem associated to the ideal J_S, i.e., to the map

$$\begin{aligned} M_{S,l} : (P_{l-(d-1)})^{|S|} \oplus (P_{l-d})^{n+1-|S|} &\longrightarrow P_l \\ (\mu_0, \ldots, \mu_n) &\longmapsto \textstyle\sum_{i \in S} \mu_i \frac{\partial f}{\partial x_i} + \sum_{i \notin S} \mu_i x_i \frac{\partial f}{\partial x_i}, \end{aligned}$$

where $l = dn - n + d - |S|$. We will use this solution to compute the reduction maps from Proposition 1.15 in the next step.

Further, if f is nondegenerate, solve the problem associated to $M_{\emptyset,l}$ for $l = 0, d, \ldots, dn$, this is necessary to compute the reduction maps from Proposition 1.18.

Altogether, we can solve all these linear algebra problems in $O\left((de)^{3n}\right)$ operations over $\mathbb{F}_q$ and $O\left(\log(M)(de)^{3n}\right)$ operations in R. Further, we can solve and store the solutions of these problems using $O\left((de)^{2n}\right)$ ring elements.

1.5.3 Step III: Reduction matrices

Using the previous step, compute $R_{(x_0,\ldots,x_n)+yv,v}$ for each $|v| = d$. If f is nondegenerate, compute $S_{(x_0,\ldots,x_n)+yv,v}$ instead. In the same fashion, compute the $\mathbb{Z}_q$-linear map

$$T : P_{dl-n-1} \longrightarrow \mathbb{Z}_q^{|B|}, \tag{1.12}$$

where $T(g)$ are the coordinates with respect to B of $(n-1)!g\Omega/f^n$.

To compute $R_{(x_0,\ldots,x_n)+yv,v}$ we iterate over $\{0, \ldots, n\}$, monomials of degree $dn - n$ and monomials of degree $dn - n + d - |S| - (d-1) \leq d(n+1) - n$. Hence, we may compute $R_{(x_0,\ldots,x_n)+yv,v}$ in $O\left((n+1)\binom{dn}{n}\binom{d(n+1)}{n}\right) \subset O\left((de)^{2n}\right)$ ring operations. Thus, computing $R_{(x_0,\ldots,x_n)+yv,v}$ for all $|v| = d$ requires $O\left(\binom{d+n}{n}(de)^{2n}\right)$ ring operations. Analogously, comput-

ing T requires $O\left((de)^{2n}\right)$ operations.

For $S_{(x_0,\ldots,x_n)+yv,v}$ the process is very similar, we iterate over $\{0,\ldots,n\}$, the monomial bases of Ψ_i, and monomials of degree at most $dn-n$. Therefore each reduction matrix requires $O\left(d^{2n}e^n\right)$ ring operations. Thus, all the $S_{(x_0,\ldots,x_n)+yv,v}$ require at most $O\left(\binom{d+n}{n}d^{2n}e^n\right)$ ring operations. Hence, if f is nondegenerate we save a factor of e^n in the time and space requirements.

Overall, computing all these matrices requires $O\left(\binom{d+n}{n}(de)^{2n}\right) \subset d^{O(n)}$ ring operations. The space requirement to compute and store all these matrices is $O\left(\binom{d+n}{n}(de)^{2n}\right) \subset d^{O(n)}$ ring elements.

1.5.4 Step IV: Frobenius approximation

For each integral basis element $x^\beta\Omega/f^m \in H^n_{\mathrm{dR}}(U_{\mathbb{Q}_q})$ approximate $p^{-n}\sigma\left(x^\beta\Omega/f^m\right)$, as in Lemma 1.10, by

$$\sum_{j=0}^{N_m-1}\sum_{|\alpha|=dj} D_{j,m}\sigma(C_{j,\alpha})\frac{x^{p(\beta+\alpha+\mathbf{1})}}{f^{p(m+j)}}\frac{\Omega}{x^{\mathbf{1}}}. \tag{1.13}$$

Computing the coefficients $C_{j,\alpha}$ requires $O\left(\binom{d+n}{n}\binom{d(N-1)+n+1}{n+1}\right)$ ring operations. Thus, computing $\sigma(C_{j,\alpha})$ requires the equivalent of $O\left(a\binom{d+n}{n}\binom{d(N-1)+n+1}{n+1}\right) \subset aN^{n+1}d^{O(n)}$ ring operations.

For the $D_{j,m}$, computing all the necessary binomial coefficients requires $O\left(N^2+nN\right)$ ring operations, and then computing all the $D_{j,m}$ requires $O\left(nN^2\right)$ ring operations. Thus, computing the $D_{j,m}$ requires $O\left(nN^2\right)$ ring operations altogether.

Hence, we may compute (1.13) for all the basis elements in the equivalent of $aN^{n+1}d^{O(n)}$ ring operations. The space requirement to store and compute the expansions is $N^{n+1}d^{O(n)}$ ring elements.

1.5.5 Step V: Reduce back to the basis

Compute the coordinates of $p^{-1}\sigma\left(x^{\beta}\Omega/f^{m}\right)$ with respect to B as follows. Let

$$\omega_e := \frac{(p(m+N_m-1)-1)!}{(pe-1)!}\sum_{|\alpha|=dj} D_{j,m}\sigma(C_{j,\alpha})\frac{x^{p(\beta+\alpha+\mathbf{1})}}{f^{p(m+j)}}\frac{\Omega}{x^{\mathbf{1}}}$$

where $j = e - m$.

For $e = m + N_m - 1, m + N_m - 2, \ldots, 1$ do

$$\omega = \omega + \omega_e;$$

use the reduction maps (repeatedly) from Proposition 1.15 and/or Proposition 1.18 to reduce the order of the pole of $\frac{(pe-1)!}{(l-1)!}\omega$ to l, where $l = \max\{p(e-1), n\}$; for last set ω to be this reduction.

By the end of the for loop

$$\omega \equiv (p(m+N_m-1)-1)!p^{-n}\sigma\left(x^{\beta}\Omega/f^{m}\right)$$

in $H^n_{\mathrm{dR}}(U_{\mathbb{Q}_q})$ and the order of the pole of ω is n. Now use the map $\frac{p^{n-1}}{(p(m+N_m-1)-1)!}T$, see Step III, to compute the coordinates of $p^{-1}\sigma\left(x^{\beta}\Omega/f^{m}\right)$ with respect to B.

For each $x^{\beta}\Omega/f^{m}$ this amounts to $O\left(pN\binom{d(N-1)+n+1}{n+1}\right) \subset pN^{n+2}d^{O(n)}$ matrix vector multiplications of size $d^{O(n)}$. Thus, it requires $pN^{n+2}d^{O(n)}$ ring operations.

Theorem 1.21. *Let $r \geq 1$. Assume that f is S-smooth with $d \geq |S|$. The entries of the matrix of the p-th power Frobenius matrix acting on a certain basis of the Monsky–Washnitzer cohomology of $\mathcal{Z}$ may be computed with r p-adic digits in time*

$$p^{1+o(1)}a^2\left(n+r\right)^{n+O(1)}d^{O(n)}$$

and space

$$\log(p)a\,(n+r)^{n+O(1)}\,d^{O(n)}$$

Using a modified version of [BGS07] one can reduce the time complexity to

$$p^{1/2+o(1)}a^2\,(n+r)^{n+O(1)}\,d^{O(n)}.$$

Moreover, if one starts with a hypersurface over $\mathbb{Q}$, one may amortize the cost of computing the p-th power Frobenius matrix of its reductions modulo various primes by using a remainder tree method see [CGH14, Har14, HS14a, HS14b]). With this approach the average time complexity for each prime $p < N$ is

$$(\log N)^{4+o(1)}a^2\,(n+r)^{n+O(1)}\,d^{O(n)}.$$

Proof. The quasi-linear version follows from previous observations.

In Step V, we can express the reduction of the order of the pole by k of an ω term as

$$M(0)\dots M(k)w,$$

where w denotes the vector of the coefficients and $M(y)$ is a matrix with entries in $\mathbb{Z}_q[y]$ with degree at most 1 or $n+1$, see Propositions 1.15 and 1.18 respectively. In the former case we can apply [BGS07, Theorem 8] directly and compute the matrix product $M(0)\dots M(k)$ in $k^{1/2+o(1)}d^{O(n)}$ ring operations. In the latter, we can also compute the matrix product in $k^{1/2+o(1)}d^{O(n)}$ ring operations, however this requires a modified version of [BGS07, Theorem 8], see for example [CH14, Section 2].

For the average polynomial time it follows by applying a remainder tree method to evaluate $M(0)\dots M(k)$, see [CGH14, Har14, HS14a, HS14b]). □

Proof of Theorem 1.1. Recall that

$$\begin{aligned} Q(t) &= \det(1 - tq^{-1} \operatorname{Frob}_q | H^n_{\mathrm{rig}}(\mathcal{U})) \\ &= \det(1 - tq^{-1} F F^{\sigma} \dots F^{\sigma^{a-1}}), \end{aligned}$$

where F is the p-th power Frobenius matrix acting on a certain basis of the Monsky–Washnitzer cohomology of $\mathcal{U}$. Put $k := \deg Q \in O(d^n)$. By the Weil conjectures we know that the polynomial is determined by the coefficients of T^i with $i = 0, \dots, \lceil k/2 \rceil$, and that these coefficients have absolute value at most

$$\binom{k}{\lceil k/2 \rceil} q^{n/2} \lceil k/2 \rceil \in p^{O(ank)}.$$

Thus, we only need to compute F modulo p^r with $r \in O(ank) \subset O(ad^n)$. We may compute $F' = F F^{\sigma} \dots F^{\sigma^{a-1}}$ modulo p^r by repeated squaring, which requires $O(\log a)$ multiplications of $k \times k$ matrices and $O(k^2 \log a)$ applications of powers of σ. Thus, we may compute F' in $O(d^{3n} a \log a)$ ring operations. For last, we may deduce $Q(t) \bmod p^r$ by computing characteristic polynomial of F', this requires $O(d^{3n})$ ring operations. These contributions are all negligible when compared with the computation of $F \bmod p^r$. □

1.6 Sample Computations

To demonstrate the feasibility of the algorithm, the author implemented the quasi-linear version for a smooth, and possibly nondegenerate, hypersurface of degree d in $\mathbb{P}^n(\mathbb{F}_p)$, where $d > n$ and $p \nmid d$. Our implementation is written in C++, using the libraries FLINT [HJP12] and NTL [Sho13].

For each example we deduce the sufficient relative precision, i.e., the vector $(r_1, \dots, r_n)$,

to compute the Hasse–Weil zeta function by combining Newton identities with Mazur's inequality [Maz73]. However, in practice, one can usually recover the zeta function with much less precision, see [Ked07]. To compute the vector $(N_1, \ldots, N_n)$ we use an algorithm similar to the one described in [AKR10, Section 3.5].

All the computations in this section were performed on a node of the Butinah cluster at New York University equipped with a 3.07 GHz Intel Xeon X5675 processor and 48GB of RAM. All the running times and memory footprints below are for the nondegenerate case, as we had no difficulties in finding a change of coordinates for which the hypersurfaces became nondegenerate.

1.6.1 Quartic curve

Table 1.2 displays r_i, N_i and M which are sufficient to compute the Hasse–Weil zeta function of a smooth quartic plane curve over $\mathbb{F}_p$ for $p > 2$, i.e., $d = 4$ and $n = 2$. Figure 1.1 shows the CPU time used to compute the Hasse–Weil zeta function over a range of p, in these examples the peak memory usage was roughly 5.8 MB. The jump observed at 2^{22} is expected, as for $p > 2^{22}$ each element of $\mathbb{Z}/p^3\mathbb{Z}$ requires two machine words to be represented and our implementation is optimized to work over a word-sized moduli. As we will see below, this jump is much more significant for surfaces and threefolds.

p	(r_1, r_2)	$N = N_1 = N_2$	M
3	(2,3)	4	7
5,7,11,13	(2,3)	3	5
≥ 17	(1,2)	2	3

Table 1.2: Values of r_i, N_i and M to deduce the Hasse–Weil zeta function of a smooth quartic curve over $\mathbb{F}_p$.

Alternatively, one can just compute $Q(t) \bmod p$, i.e.,

$$\det(1 - tp^{-1} \operatorname{Frob}_p | H^2_{\mathrm{rig}}(\mathcal{U})) \bmod p,$$

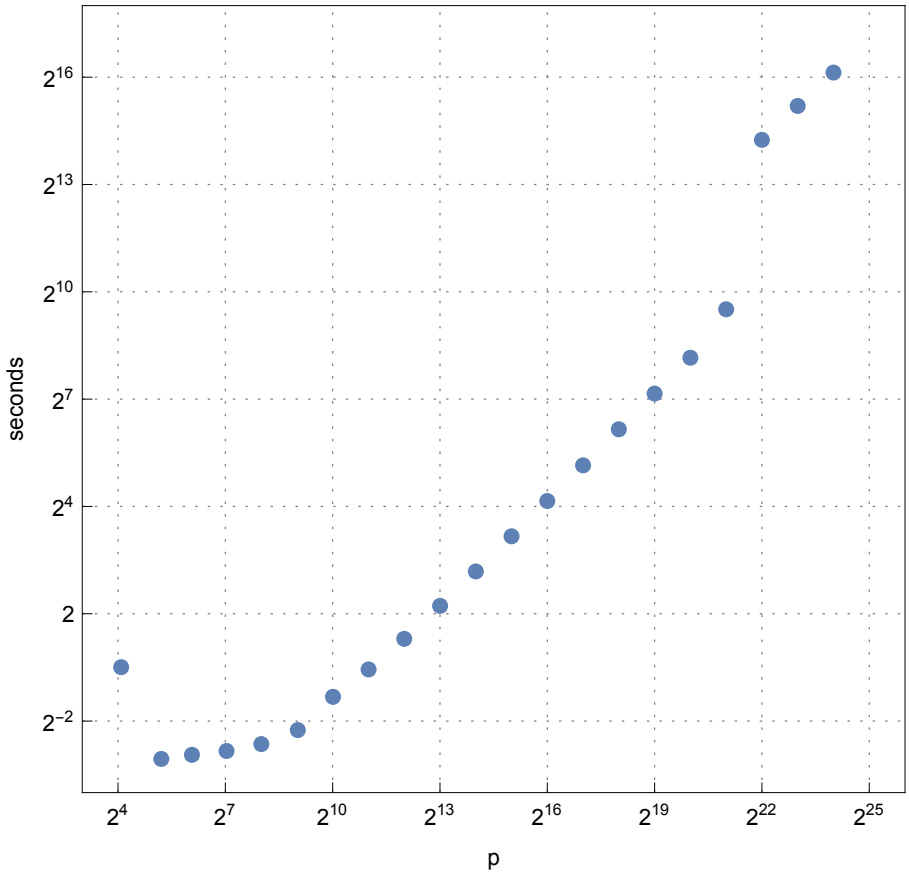


Figure 1.1: CPU time to compute the Hasse–Weil zeta function for a smooth quartic curve over $\mathbb{F}_p$.

and then lift it to $\mathbb{Z}[t]$ by applying a "baby-step giant-step" algorithm to the Jacobian of the curve and this has complexity $\tilde{O}(p^{1/4})$ (see for example [KS08]). We can compute $Q(t)$ mod p by working over $\mathbb{F}_p$ and taking $N_0 = 0$ and $N_1 = 1$. Figure 1.2 shows the CPU time used to compute $Q(t)$ mod p over a range of p, in these examples the peak memory usage was roughly 3.72 MB.

Example 1.22. *Let $\mathbb{X}$ be the quartic curve defined by*

$$15x^4 - 3x^3y - x^2y^2 + 5x^2z^2 + xy^3 - xy^2z - 2xyz^2 + y^4 + 75y^3z - 2y^2z^2 + 6yz^3 + z^4 = 0$$

over $\mathbb{Q}$. The characteristic polynomial of the Frobenius matrix of its reduction modulo p for

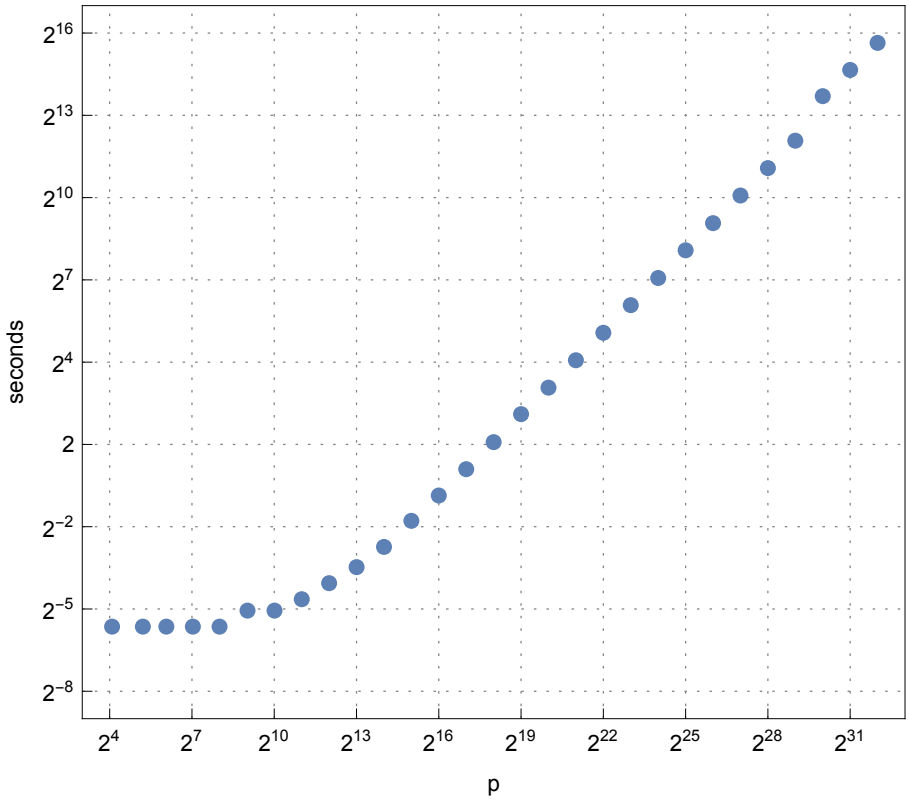


Figure 1.2: CPU time to compute $Q(t)$ mod p for a smooth quartic curve over $\mathbb{F}_p$.

$p = 2^{20} + 7$ is

$$p^3t^6 - 661p^2t^5 - 220754pt^4 + 1486404442t^3 - 220754t^2 - 661t + 1;$$

and for $p = 2^{25} + 35$ is

$$p^3t^6 - 3129p^2t^+31924899pt^4 - 276429965044t^3 + 31924899t^2 - 3129t + 1.$$

Each computation required, respectively, 283 seconds and 36.98 hours of CPU time. The peak memory usage was, respectively, 5.8 MB and 7.37 MB.

1.6.2 Quartic surface

We now turn to quartic smooth surfaces over $\mathbb{F}_p$, i.e., $d = 4$ and $n = 3$, these are K3 surfaces. The middle cohomology of a K3 surface has dimension 22 and Hodge numbers 1, 20, 1. However, $H^3_{\mathrm{rig}}(\mathcal{U})$ has dimension 21 and the central Hodge number is decreased by 1. Table 1.3 shows the arguments r_i, N_i and M that are sufficient to deduce the Hasse–Weil zeta function for different $p > 2$. Figure 1.3 shows the CPU time used to compute the Hasse–Weil zeta function over a range of p. The peak memory usage was roughly 280 MB for $41 < p < 2^{16}$, and 347 MB for $p > 2^{16}$.

p	(r_1, r_2, r_3)	(N_1, N_2, N_3)	M
3	(3,4,5)	(7,7,8)	16
5	(2,3,4)	(4,5,5)	9
7, 11, 13, 17, 19	(2,3,3)	(4,4,3)	6
23, 29, 31, 37, 41	(1,2,3)	(3,3,3)	5
≥ 43	(1,2,2)	(3,3,2)	4

Table 1.3: Values of r_i, N_i and M to deduce the Hasse–Weil zeta function of a smooth quartic surface over $\mathbb{F}_p$.

Example 1.23. *Let $\mathbb{X}$ be the K3 surface defined by*

$$g_1 g_2 + g_3 g_4 = 0$$

over $\mathbb{Q}$ where

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

Recall that $Q(t)$ is the characteristic polynomial of the Frobenius matrix of its reduction

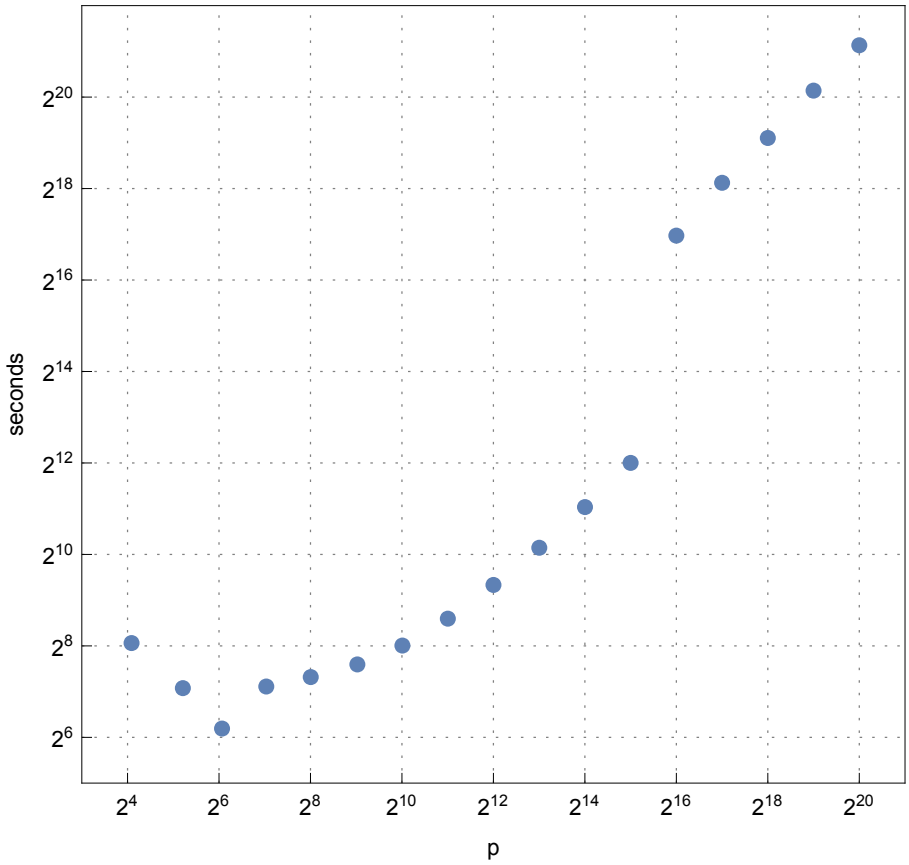


Figure 1.3: CPU time to compute the Hasse–Weil zeta function of a smooth quartic surface over $\mathbb{F}_p$.

modulo p. *For* $p = 3$ *we have*

$$Q(t/p) = \frac{1}{p}(1-t)^4(1+t)^2(pt^{16} - 3t^{15} + 6t^{14} - 4t^{13} + 7t^{12} - 5t^{11} + 8t^{10} - 5t^9 + 7t^8 - 5t^7 + 8t^6 - 5t^5 + 7t^4 - 4t^3 + 6t^2 - 3t + p);$$

for $p = 2^{16} - 15$ *we have*

$$\begin{aligned} Q(t/p) = \frac{1}{p}(1-t)^2(pt^{20} + 7440t^{19} - 73587t^{18} + 42202t^{17} + 38425t^{16} - 82474t^{15} \\ + 44098t^{14} + 121316t^{13} - 76406t^{12} - 34984t^{11} + 112194t^{10} \\ - 34984t^9 - 76406t^8 + 121316t^7 + 44098t^6 - 82474t^5 \\ + 38425t^4 + 42202t^3 - 73587t^2 + 7440t + p); \end{aligned}$$

and for $p = 2^{20} + 7$ *we have*

$$\begin{aligned} Q(t/p) = \frac{1}{p}(1-t)^3(t+1)(pt^{18} + 1208991t^{17} + 1893721t^{16} + 2148202t^{15} + 2192485t^{14} \\ + 2476907t^{13} + 1945459t^{12} + 1881975t^{11} + 1833476t^{10} \\ + 1266215t^9 + 1833476t^8 + 1881975t^7 + 1945459t^6 + 2476907t^5 \\ + 2192485t^4 + 2148202t^3 + 1893721t^2 + 1208991t + p). \end{aligned}$$

Each computation required, respectively, 27.47 minutes, 2.89 hours and 26.66 days of CPU time. The peak memory usage was, respectively, 1355 MB, 280 MB and 347 MB. In Section 2.5 we revisit this example, see Example 2.11.

1.6.3 Quintic surface

We now consider quintic smooth surfaces over $\mathbb{F}_p$, i.e., $d = 5$ and $n = 3$. The middle cohomology is 53-dimensional with Hodge numbers 4, 45, 4, however the space we compute in is only 52-dimensional with the middle Hodge number 44. Table 1.4 shows the r_i, N_i and M that are sufficient to deduce the Hasse–Weil zeta function for different $p > 2$. Figure 1.4 shows the CPU time used to compute Hasse–Weil zeta function over a range of p, in these examples the peak memory usage was roughly 8 GB.

p	(r_1, r_2, r_3)	(N_1, N_2, N_3)	M
3	(6,7,7)	(11,11,10)	21
5	(5,6,7)	(8,8,9)	17
7	(5,6,6)	(8,8,7)	14
11, 13, 17, 19	(5,6,6)	(7,7,6)	12
23	(4,5,6)	(6,6,6)	11
≥ 29	(4,5,5)	(6,6,5)	10

Table 1.4: Values of r_i, N_i and M to deduce the Hasse–Weil zeta function of a smooth quintic surface over $\mathbb{F}_p$.

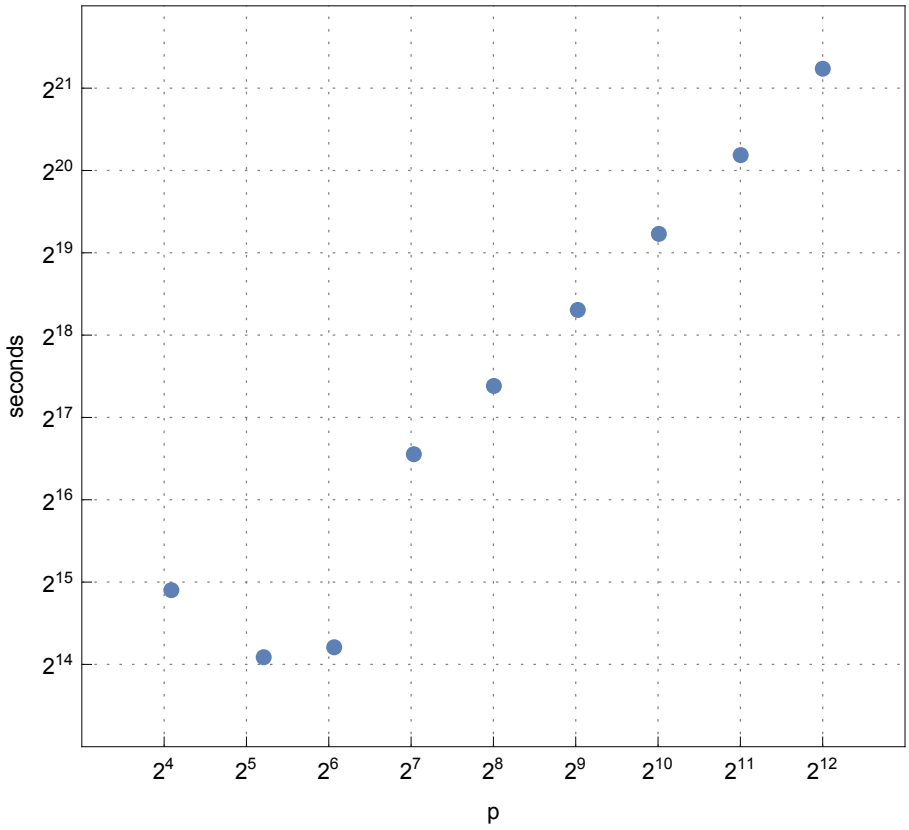


Figure 1.4: CPU time to compute the Hasse–Weil zeta function of a smooth quintic surface over $\mathbb{F}_p$.

Example 1.24. *Let $\mathcal{Z}$ be the quintic surface in $\mathbb{P}_{\mathbb{F}_p}$ with $p = 4099$ defined by zero locus of*

the following polynomial

$$45x^5 - 8x^4y - x^4z + x^4w - x^3y^2 - x^3yz + 14x^3z^2 + 3x^3zw + x^3w^2 - 13x^2y^3 + x^2y^2z$$
$$+ x^2y^2w - x^2yz^2 - x^2yzw - 37x^2yw^2 - x^2z^3 + x^2z^2w - x^2zw^2 - 3x^2w^3 + xy^4 - xy^3z$$
$$- xy^3w - xy^2z^2 - 19xy^2zw + xy^2w^2 - xyz^3 - xyz^2w - 35xyzw^2 - xyw^3 + xz^4$$
$$- 2xz^3w - xz^2w^2 + 5xzw^3 - 23xw^4 + y^5 + y^4z + y^4w + 12y^3z^2 + 2y^3zw + 5y^3w^2$$
$$- y^2z^3 - y^2z^2w - y^2zw^2 - y^2w^3 + 4yz^4 - 2yz^3w + yz^2w^2 - 3yzw^3 + yw^4 - 2z^4w$$
$$- 4z^3w^2 + 2z^2w^3.$$

The computation of $Q(t)$ required 28.59 days of CPU time and 7.93 GB of RAM.

$$\begin{aligned} Q(t/p) = \frac{1}{p^4}(1-t)(&p^4t^{52} - 3979p^3t^{51} - 1047019p^2t^{50} + 12125862568pt^{49} \\ &+ 220808266528838t^{48} + 82636219229347t^{47} - 68866921646391t^{46} \\ &- 425146312315 93t^{45} - 108942774993413t^{44} - 73683908581325t^{43} \\ &+ 245952210630380t^{42} - 88508798120450t^{41} - 12662041284647t^{40} \\ &- 153951100834834t^{39} - 70923325722618t^{38} + 200078578341633t^{37} \\ &+ 73607413405334t^{36} + 33218626758725t^{35} - 129777778091755t^{34} \\ &- 47837638385982t^{33} + 177727208881848t^{32} - 22306132859011t^{31} \\ &+ 44720579337792t^{30} + 20670838447126t^{29} - 2719506962136 13t^{28} \\ &+ 560862244868 14t^{27} + 195369760686304t^{26} + 560862244868 14t^{25} \\ &- 2719506962136 13t^{24} + \dots) \end{aligned}$$

1.6.4 Quintic Threefold in the Dwork pencil

We now turn to quintic smooth threefolds over $\mathbb{F}_p$, i.e., $d = 5$ and $n = 4$, these are Calabi-Yau threefolds. The middle cohomology of a Calabi-Yau threefold has dimension 204 and Hodge numbers 1, 101, 101, 1. Admittedly, with the current implementation, one could compute the Hasse–Weil zeta function of a quintic threefold, however it would require very significant amount of computational resources to carry out such computation.

Instead, we focus on computing a factor of the characteristic polynomial of the Frobenius action on $H^4_{\mathrm{rig}}(\mathcal{U})$ for a specific family of threefolds, the Dwork pencil, the one parameter family of quintic threefolds $\mathcal{Z}_\lambda$ described by the zero locus of the polynomial

$$f_\lambda := \sum_{i=0}^{4} x_i^5 + \lambda x_0 x_1 x_2 x_3 x_4$$

over $\mathbb{F}_p$. For general values λ the numerator of the Hasse–Weil zeta function takes a very special form, it can be factored as $R(t)S(t)$, where

$$R(t) = 1 + at + bpt^2 + ap^3t^3 + p^6t^4, \quad a, b \in \mathbb{Z},$$

and $S(t) \in \mathbb{Z}[t]$ can be described in terms of the Frobenius action on two genus 4 curves, see [CdlORV03] for more details. Moreover, let x^β be the unique monomial of degree 15 not in $\langle \partial f_\lambda / \partial x_i \rangle_{i=0,\ldots,4}$ and put

$$V := \langle \Omega/f, x^\beta \Omega/f_\lambda^4, \mathrm{Frob}(\Omega/f), \mathrm{Frob}(x^\beta \Omega/f_\lambda^4) \rangle.$$

Then V has dimension 4, all Hodge numbers are 1 and

$$R(t) = \det(1 - tp^{-1} \,\mathrm{Frob}\,|V).$$

Furthermore, it is enough to compute four columns of the Frobenius matrix, with sufficient p-adic precision, to deduce $R(t)$. Table 1.5 shows the arguments r_i, N_i and M that are sufficient to compute $R(t)$ for different $p > 2$. Figure 1.5 shows the CPU time used to compute $R(t)$ over a range of p, in these examples the peak memory usage was roughly 39 GB, with exception of $p = 2053$ where we observed 45 GB.

p	(r_1, r_2, r_3, r_4)	(N_1, N_2, N_3, N_4)	M
3	(2,3,4,4)	(8,9,9,8)	16
5	(1,2,3,3)	(4,5,5,4)	8
≥ 7	(1,2,3,3)	(4,5,5,4)	6

Table 1.5: Values of r_i, N and M to compute $R(t)$.

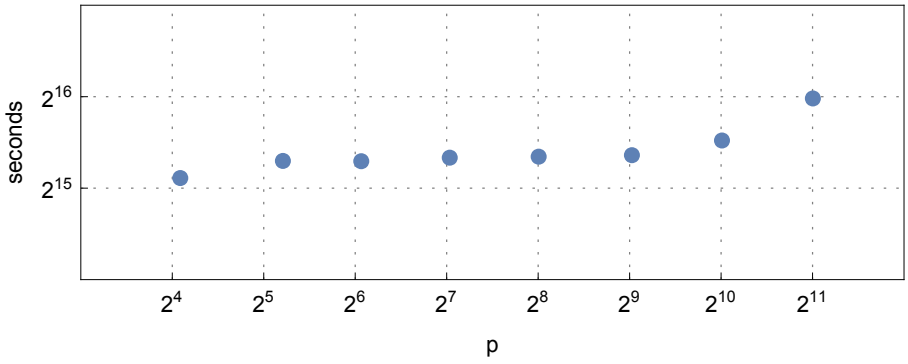


Figure 1.5: CPU time to compute $R(t)$.

Other use for this implementation is the search for a Calabi-Yau threefold in the Dwork pencil such that the Newton polygon has two slopes of the form 3/2, i.e., a height 1 Calabi-Yau threefold that is not Bloch-Kato ordinary [BK86], see [War15] for more details. For a Calabi-Yau threefold in the Dwork pencil this can be read from $R(t)$, expressly, the Newton polygon has two slopes of the form 3/2 if, and only if, $b \equiv 0 \bmod p$ and $a \not\equiv 0 \bmod p$, hence we just need to compute $R(t) \bmod p^2$. To perform this test is sufficient to work over $\mathbb{Z}/p^2\mathbb{Z}$ and compute two of columns of the Frobenius matrix with one significant p-adic digit, i.e., $r_3 = r_4 = 1$, $N_3 = 2$ and $N_4 = 1$. We looked for such threefolds in the Dwork pencil for all $17 \leq p \leq 109$, this consumed a total of 4300 hours of CPU time. We found 26 such

threefolds, we present those in Table 1.6. Figure 1.6 shows the CPU time used to test if a threefold in the Dwork pencil is Bloch-Kato ordinary over a range of p, in these examples the peak memory usage was roughly 33 GB.

p	λ	p	λ
19	10	67	24, 48
29	20	79	19, 42, 58
31	3, 6, 12, 17, 24	89	13
37	14	97	45
43	6, 20, 37	103	18, 41, 52, 83
47	15	107	7
59	15, 31		

Table 1.6: λ and $17 \leq p \leq 109$ for which $\mathcal{Z}_\lambda$ is not Bloch-Kato ordinary over $\mathbb{F}_p$.

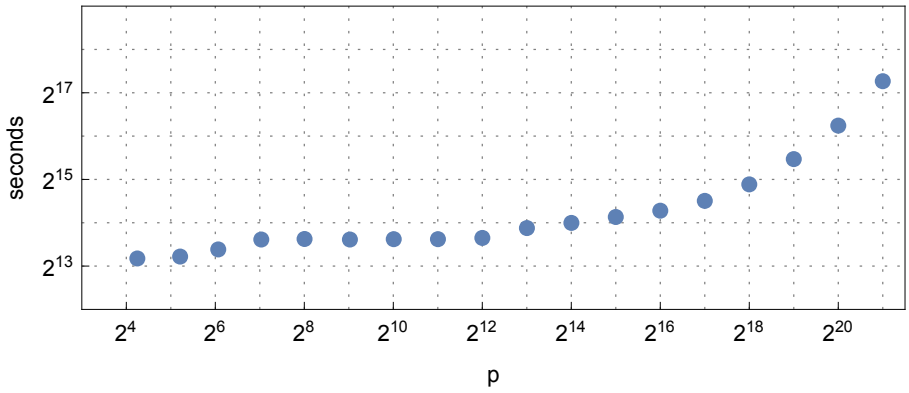


Figure 1.6: CPU time to test if a threefold in the Dwork pencil is Bloch-Kato ordinary over $\mathbb{F}_p$.

Chapter 2

Variation of Néron–Severi ranks

2.1 Introduction

A central theme in Arithmetic Geometry is the study of deep interactions between geometric and topological properties of an algebraic variety defined over a number field and the geometry of its reductions modulo primes. For instance, one would like to understand how the global geometry of a surface influences the properties of its reductions modulo primes, such as the behaviour of the Picard group. The case of curves has been the object of intense investigation for several decades. In this chapter we will focus on surfaces.

Let k be a number field and X a K3 surface defined 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 $\mathrm{NS}(\overline{X})$ and $\mathrm{NS}(\overline{X}_\mathfrak{p})$, i.e., the geometric Picard ranks. Understanding the variation of $\rho(\overline{X}_\mathfrak{p})$ is of central importance in many applications.

There is a natural specialization homomorphism

$$s_{\mathfrak{p}} : \mathrm{NS}(\overline{X}) \to \mathrm{NS}(\overline{X}_{\mathfrak{p}}), \tag{2.1}$$

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

$$\rho(\overline{X}) + \eta(\overline{X}) \leq \rho(\overline{X}_{\mathfrak{p}}), \tag{2.2}$$

for some $\eta(\overline{X}) \geq 0$, defined by (2.7). It is known that there exist infinitely many $\mathfrak{p}$ such that equality occurs in (2.2); 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

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

where the inequality (2.2) is strict.

Information about $\Pi_{\mathrm{jump}}(X)$ can be converted into geometric statements: *if* this set contains infinitely many primes of non-supersingular reduction, 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 where $\Pi_{\mathrm{jump}}(X)$ 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 $\iota : A \to A$ 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

(i) $\rho(\overline{X}) \geq 18$,

(ii) $\rho(\overline{X}) \geq 19$, if $C_1 \sim C_2$, and

(iii) $\rho(\overline{X}) = 20$, if in addition, C_1 has complex multiplication by $E := \mathbb{Q}(\sqrt{-d})$, for some $d > 0$.

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 $\mathbb{Q}$.

In case (i), $\mathfrak{p} \in \Pi_{\text{jump}}(X)$ provided the reductions of C_1 and C_2 modulo $\mathfrak{p}$ are isogenous. There are infinitely many such $\mathfrak{p}$, by a recent theorem of Charles [Cha14].

This motivates us to consider the asymptotic behavior of the proportion of primes in $\Pi_{\text{jump}}(X)$:

$$\gamma(X, B) := \frac{\#\left\{\|\mathfrak{p}\| \leq B : \mathfrak{p} \in \Pi_{\text{jump}}(X)\right\}}{\#\left\{\|\mathfrak{p}\| \leq B\right\}}. \tag{2.3}$$

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

$$\gamma(X, B) \sim \frac{c}{\sqrt{B}}, \quad B \to \infty, \tag{2.4}$$

for some constant $c > 0$. However, the conjecture has not been proven for a single elliptic curve. Nonetheless, it is known to be true on "average" in various senses. For a sample of results we refer to [Ser81, Elk91, FM96, DP99, Bai07] and to [Kat09], in the function field case. If C does have complex multiplication, by $\mathbb{Q}(\sqrt{-d})$, then

$$\Pi_{\mathrm{jump}}(X) = \left\{p : \, p \text{ is ramified or inert in } \mathbb{Q}(\sqrt{-d})\right\} \quad \text{(see [Deu41])},$$

and by Chebotarev's density theorem with k the field $\mathbb{Q}$ of rational numbers we have

$$\gamma(X, B) \sim \frac{1}{2}, \quad B \to \infty. \tag{2.5}$$

The situation is similar when A is not a product of elliptic curves (see Section 2.3). Using analogous tools we can either describe $\Pi_{\mathrm{jump}}(X)$ as a frobenian set (see [Ser12]) or heuristicaly deduce, based on the Sato–Tate group ST_A of the abelian surface A [FKRS12], that $\gamma(X, B)$ should behave as in (2.4), i.e., as in the Lang–Trotter conjecture for elliptic curves. Furthermore, in the latter case, for some families, we know that $\Pi_{\mathrm{jump}}(X)$ is infinite [BG08, Jao03, Sad04].

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 closely 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. Moreover, this construction should also help us to classify groups which are realizable as Sato–Tate groups for a K3 surface, as in [FKRS12]. 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].

Here, we also 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 evidence that

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

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

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

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

These numerical experiments lead us to the following result which bring us closer to understanding $\Pi_{\text{jump}}(X)$ for the case that $\rho(\overline{X})$ is even.

Theorem 2.1. *Let X be a K3 surface over $\mathbb{Q}$ and assume that the discriminant of X is not square modulo p. If $\rho(X_p) \geq 2r$, then $\rho(X_p) \geq 2r + 1$.*

Corollary 2.2. *Let X be a K3 surface over $\mathbb{Q}$. If $\rho(X) = 2r$ then $\rho(\overline{X}_p) \geq 2r + 2$ at all primes p such that the discriminant of X is not square modulo p.*

Corollary 2.3. *Let X be a K3 surface over $\mathbb{Q}$ and K a number field such that $\rho(X_K) = \rho(\overline{X}) = 2r$ and $\eta(\overline{X}) = 0$. If the discriminant of X is not square in K, then*

$$\liminf_{B\to\infty} \gamma(X, B) > 0.$$

Corollary 2.4. *Let X be a K3 surface over $\mathbb{Q}$ and K a number field such that $\rho(X_K) = \rho(\overline{X}) = 2r$. If the discriminant of X is not square in K or $\eta(\overline{X}) > 0$, then $\overline{X}$ has infinitely many rational curves.*

Our examples with geometric Picard number 2 are indeed K3 surfaces over $\mathbb{Q}$ with arithmetic Picard number 2, i.e., $\rho(X) = \rho(\overline{X}) = 2$. As expected, for these examples we observe

$$\left\{p < 2^{16} : p \text{ is inert in } \mathbb{Q}(\sqrt{D_X})\right\} \subset \Pi_{\text{jump}}(X),$$

where D_X is the discriminant of X. Furthermore, we also find evidence that

$$\gamma\left(X_{\mathbb{Q}(\sqrt{D_X})}, B\right) \sim \frac{c_X}{\sqrt{B}}, \quad B \to \infty,$$

for some constant $c_X > 0$. In other words, we expect the following: if p is inert $\mathbb{Q}(\sqrt{D_X})$ then p is in $\Pi_{\text{jump}}(X)$, and if p splits in $\mathbb{Q}(\sqrt{D_X})$, then p is in $\Pi_{\text{jump}}(X)$ with probability proportional to $1/\sqrt{p}$.

2.2 Computing the Picard number of a K3 surface

In this section, we explain our approach to the computation of Picard numbers of 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 (2.1). 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,

$$\rho(\overline{X}_{\mathfrak{p}}) \geq \begin{cases} \rho(\overline{X}) & \text{if } E_X \text{ is a CM-field or } \dim_{E_X}(T_X) \text{ is even,} \\ \rho(\overline{X}) + [E_X : \mathbb{Q}] & \text{if } E_X \text{ is totally real field and } \dim_{E_X}(T_X) \text{ is odd.} \end{cases} \tag{2.6}$$

We define

$$\eta(\overline{X}) := 0 \quad \text{or} \quad [E_X : \mathbb{Q}], \tag{2.7}$$

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

$$\zeta_X(t) := \exp\left(\sum_{m=1}^{\infty} \frac{\#X(\mathbb{F}_{q^m})}{m} t^m\right) = \frac{P_1(X,t)P_3(X,t)}{(1-t)P_2(X,t)(1-q^2t)}, \tag{2.8}$$

where

$$P_i(X,t) := \det\left(1 - t\ \mathrm{Frob}_i\,|H^i_{\mathrm{et}}(\overline{X}, \mathbb{Q}_\ell)\right) \in \mathbb{Z}[t] \tag{2.9}$$

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

Conjecture 2.5.

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

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

Then

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

The Tate conjecture implies the Artin-Tate conjecture, see [Mil75a, Theorem 6.1] and [Mil75b]. If X is a K3 surface both hold in odd characteristic [Cha13, Per13, Mau12]; furthermore, $\#\,\mathrm{Br}(X)$ is a perfect square (see, e.g., [LLR05]). Thus,

$$\mathrm{disc}(\mathrm{NS}(X_{\mathbb{F}_q})) = \lim_{s\to 1} \frac{(-1)^{\rho(X)-1} P_2(X,q^{-s})}{q(1-q^{1-s})^{\rho(X)}} \bmod \mathbb{Q}^{\times 2}. \tag{2.10}$$

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's inequality [Maz73].

The algorithmic implementation of this idea relies on techniques introduced in [AKR10] and [Har07]. The details of the algorithm are presented in Chapter 1 and here we present a short overview. The approach by Abbott–Kedlaya–Roe [AKR10] makes primes < 20 computationally feasible and it was used in [vL06], 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 $\mathbb{Z}/p^M\mathbb{Z}$. For a quartic K3 surface the size of the matrices is 220×220; for $p > 41$ one can take $M = 4$. Moreover, if the K3 is nondegenerate (as in [SV13]), one can reduce their size to 64×64. In practice, we had no difficulties finding 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]). Our implementation is written in C++, using the libraries FLINT [HJP12] and NTL [Sho13]. The raw data of all experiments is available at

2.3 Kummer surfaces

In this section, we study $\Pi_{\text{jump}}(X)$, where X is a Kummer surface, i.e., the resolution of singularities of the quotient A/ι, where A is an abelian surface, and $\iota : A \to A$ the standard involution $\iota(a) = -a$.

Using the theory of abelian varieties, in this case, we can either describe $\Pi_{\text{jump}}(X)$ as a frobenian set (see [Ser12]) or heuristicaly deduce, based on the Sato–Tate group ST_A of the abelian surface A [FKRS12], that $\gamma(X, B)$ should behave as in (2.4), i.e., as in the Lang–Trotter conjecture for elliptic curves. Furthermore, for some families, we know that $\Pi_{\text{jump}}(X)$ is infinite [BG08, Jao03, Sad04].

The geometric Picard number of a Kummer surface can be computed by

$$\rho(\overline{X}) = \rho(\overline{A}) + 16, \quad \text{(see [EJ12, 4.1])}$$

and $\rho(A)$ may be computed directly using the theory of abelian varieties. More precisely,

$$\mathrm{NS}(A) \otimes \mathbb{Q} \cong (\mathrm{End}(A) \otimes \mathbb{Q})^{\dagger}, \tag{2.11}$$

where $\dagger$ denotes the Rosati involution [Mum70, Section 21]. Furthermore,

$$H^2_{\text{et}}(\overline{A}, \mathbb{Q}_\ell) \cong \Lambda^2 H^1_{\text{et}}(\overline{A}, \mathbb{Q}_\ell). \tag{2.12}$$

Hence, we can derive $P_2(A_{\mathfrak{p}}, t)$ from $P_1(A_{\mathfrak{p}}, t)$. Explicitly, if

$$P_1(A_{\mathfrak{p}}, t/q^{1/2}) = 1 + a_1 t + a_2 t^2 + a_1 t^3 + t^4,$$

then

$$\begin{aligned} P_2(A_{\mathfrak{p}}, t/q) &= 1 - a_2 t + (a_1^2 - 1)t^2 + (2a_2 - 2a_1^2)t^3 + (a_1^2 - 1)t^4 - a_2 t^5 + t^6 \\ &= \left(1 + (2 - a_2)t + (2 + a_1^2 - 2a_2)t^2 + (2 - a_2)t^3 + t^4\right)(t-1)^2. \end{aligned} \tag{2.13}$$

If A is isogeneous to the Jacobian of a genus-2 curve C, then $P_1(A_{\mathfrak{p}}, t) = P_1(C_{\mathfrak{p}}, t)$ and we can reduce the computation of $\rho(\overline{A}_{\mathfrak{p}})$ to one dimension, which is faster (see [KS08]). For example, with [Sut15] one can easily test numerically the assymptotic behavior of $\gamma(X, B)$.

Elsenhans and Jahnel used these techniques, where they conducted an extensive numerical investigation of Kummer surfaces over $\mathbb{Q}$ [EJ12], in particular of those with $\rho(\overline{X}) = 17$. 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 $2/\sqrt{p}$.

For simplicity of our analysis we assume for the rest of the section that k is the field $\mathbb{Q}$ of rational numbers.

2.3.1 Product of elliptic curves

Assume that $\overline{A} \sim C_1 \times C_2$, i.e., is isogenous to a product of two elliptic curves. According to (2.11), one has

$$\rho(A) = 2 + \mathrm{rk}(\mathrm{Hom}(C_1, C_2)) = 2 + \begin{cases} 0 & C_1 \not\sim C_2; \\ \mathrm{rk}(\mathrm{End}(C_1)) & C_1 \sim C_2. \end{cases}$$

If C_1 and C_2 are isogenous, then $p \in \Pi_{\mathrm{jump}}(X)$ provided p is a supersingular prime for C_1 (and thus C_2). When the elliptic curve C_1 does not have complex multiplication the

Lang-Trotter conjecture [LT76], implies

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

for some constant $c_X > 0$. If C_1 does have complex multiplication, by $\mathbb{Q}(\sqrt{-d})$, then

$$\Pi_{\text{jump}}(X) = \left\{p : p \text{ is ramified or inert in } \mathbb{Q}(\sqrt{-d})\right\} \quad \text{(see [Deu41])},$$
$$\gamma(X,B) \sim \frac{1}{2}, \quad B \to \infty$$

by Chebotarev's density theorem.

If C_1 and C_2 are not isogenous, then $p \in \Pi_{\text{jump}}(X)$ provided the reductions of C_1 and C_2 modulo p are isogenous, equivalently, if the traces of the Frobenius at p are equal [Tat66]. There are infinitely many such p, by a recent theorem of Charles [Cha14]. We now address the four possible cases when C_1 and C_2 are not isogenous.

(i) C_1 and C_2 are not isogenous and both have complex multiplication, by $\mathbb{Q}(\sqrt{-d_1})$ and $\mathbb{Q}(\sqrt{-d_2})$, respectively:

In this instance C_1 and C_2 modulo p can only be isogenous if both p is a supersingular prime for both elliptic curves, i.e., $\rho(\overline{A}_p) = 2$ or 6 and

$$\Pi_{\text{jump}}(X) = \left\{p : p \text{ is ramified or inert in } \mathbb{Q}(\sqrt{-d_1}) \text{ and } \mathbb{Q}(\sqrt{-d_2})\right\} \quad \text{(see [Deu41])},$$
$$\gamma(X,B) \sim \frac{1}{4}, \quad B \to \infty$$

by Chebotarev's density theorem.

(ii) C_1 and C_2 are Galois conjugates:

Then they cannot have complex multiplication, and their j-invariants are the roots of

a quadratic polynomial. Let K_j be the splitting field of the polynomial associated to the j-invariants, then

$$\Pi_{\text{jump}}(X) = \{p : p \text{ is ramified or inert in } K_j\},$$
$$\gamma(X, B) \sim \frac{1}{2}, \quad B \to \infty,$$

by Chebotarev's density theorem.

(iii) If C_1 and C_2 are not Galois conjugates and do not have complex multiplication:
The Sato–Tate conjecture for a product of elliptic curves [FKRS12] predicts that as p varies, the traces of the Frobenius at p of each curve will be roughly equidistributed between $-2\sqrt{p}$ and $2\sqrt{p}$ and the distributions of the traces to be independent. Therefore, one expects the traces to be equal with probability of the order of $1/\sqrt{p}$, thus

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

for some constant $c_X > 0$.

(iv) C_1 does not have complex multiplication and C_2 does have complex multiplication:
As in the previous case, *mutatis mutandis*, we can *heuristically* deduce that the traces should match with probability of the order of $1/\sqrt{p}$, thus

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

for some constant $c_X > 0$.

2.3.2 A is absolutely simple

Assume that A is simple, then Albert's classification of division algebras with involution [Mum70, Section 21], together with the work of Shimura [Shi63] restrict $\mathrm{End}(\overline{A})$ to four possibilities:

(i) an order in a division quaternion algebra over $\mathbb{Q}$:

For some special cases, we know that $\Pi_{\mathrm{jump}}(X)$ is infinite [BG08, Jao03, Sad04]. However, in general, very little is known about $\Pi_{\mathrm{jump}}(X)$ and the asymptotic behaviour of $\gamma(X, B)$. Nonetheless, we expect

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

for some constant $c_X > 0$. For any prime of good reduction A splits as the square of an elliptic curve, i.e., $\overline{A}_p \sim C \times C$ [Oor88, 6.4]. Furthermore, the Sato–Tate group of A can also be realizable as the Sato–Tate group of an abelian surface which is geometrically isogenous to the square of an elliptic curve without complex multiplication [FKRS12]. In other words, the Sato–Tate group is an invariant which is too coarse to distinguish between these cases. Hence, for both cases, we should expect the same asymptotic behaviour of $\gamma(X, B)$.

(ii) An order in a quartic CM-field:

Due to our assumption of $k = \mathbb{Q}$, the CM-field is a Galois extension $\mathbb{Q}$ and the Galois group of the extension is $\mathbb{Z}/4\mathbb{Z}$ [FKRS12]. Furthermore, according to [Oor88, 6.5], $\overline{A}_p$ is supersingular if, and only if, p does not split totally in the CM-field, otherwise

$\rho(\overline{A}_p) = 2$, by (2.11). Therefore,

$$\Pi_{\text{jump}}(X) = \left\{p : p \text{ does not split totally in } \operatorname{End}(\overline{A}) \otimes \mathbb{Q}\right\},$$
$$\gamma(X, B) \sim \frac{3}{4}, \quad B \to \infty,$$

by Chebotarev's density theorem.

(iii) an order in a real quadratic field:

As reported in [Oor88, 6.3], if a prime splits in $\operatorname{End}(\overline{A}) \otimes \mathbb{Q}$, the A splits as the square of an elliptic curve, otherwise $\rho(\overline{A}_p) = 2$, by (2.11). Thus,

$$\Pi_{\text{jump}}(X) = \left\{p : p \text{ splits in } \operatorname{End}(\overline{A}) \otimes \mathbb{Q}\right\},$$
$$\gamma(X, B) \sim \frac{1}{4}, \quad B \to \infty,$$

by Chebotarev's density theorem.

(iv) $\mathbb{Z}$:

This is the generic case. From equation (2.13) we have that $p \in \Pi_{\text{jump}}(X)$ provided that

$$\frac{P_2(A_p, t/p)}{(t-1)^2} := 1 + (2 - a_2)t + (2 + a_1^2 - 2a_2)t^2 + (2 - a_2)t^3 + t^4$$

is divisible by a cyclotomic polynomial ϕ_n. We can easily convert this statement in conditions on the pair (a_1, a_2). More precisely, if $\deg \phi_n = 4$, then

$$(a_1, a_2) \in \left\{\{\pm 1, 1\}, \{\pm\sqrt{2}, 2\}, \{\pm\sqrt{5}, 3\}, \{\pm 1, 2\}\right\}.$$

Otherwise, if $\deg \phi_n \leq 2$, then the pair must satisfy one of the following equations:

$$a_1 = 0; \tag{2.14}$$

$$a_1^2 - 4a_2 + 8p = 0; \tag{2.15}$$

$$-a_1^2 + a_2 + p = 0; \tag{2.16}$$

$$2a_2 - a_1^2 = 0; \tag{2.17}$$

$$-a_1^2 + 3a_2 - 3p = 0. \tag{2.18}$$

Therefore,

$$\#\left\{(a_1, a_2) : p \in \Pi_{\text{jump}}(X)\right\} \sim 4\sqrt{p} + p + O(1), \quad \text{(see Figure 2.1)}.$$

Furthermore, for each p the number of possible pairs is of the order $p^{3/2}$, and the Sato–Tate conjecture predicts that as p varies these pairs will be roughly equidistributed in

$$S = \left\{(a_1, a_2) \in \mathbb{R}^2 : a_2 \geq \pm 2a_1 - 2, a_2 \leq \frac{1}{4}a_1^2 + 2\right\},$$

i.e., the support of the Haar measure of $\mathrm{USp}_4 = \mathrm{ST}_A$ (see Figure 2.1). Altogether, this heuristic argument leads us to believe

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

for some constant $c_X > 0$.

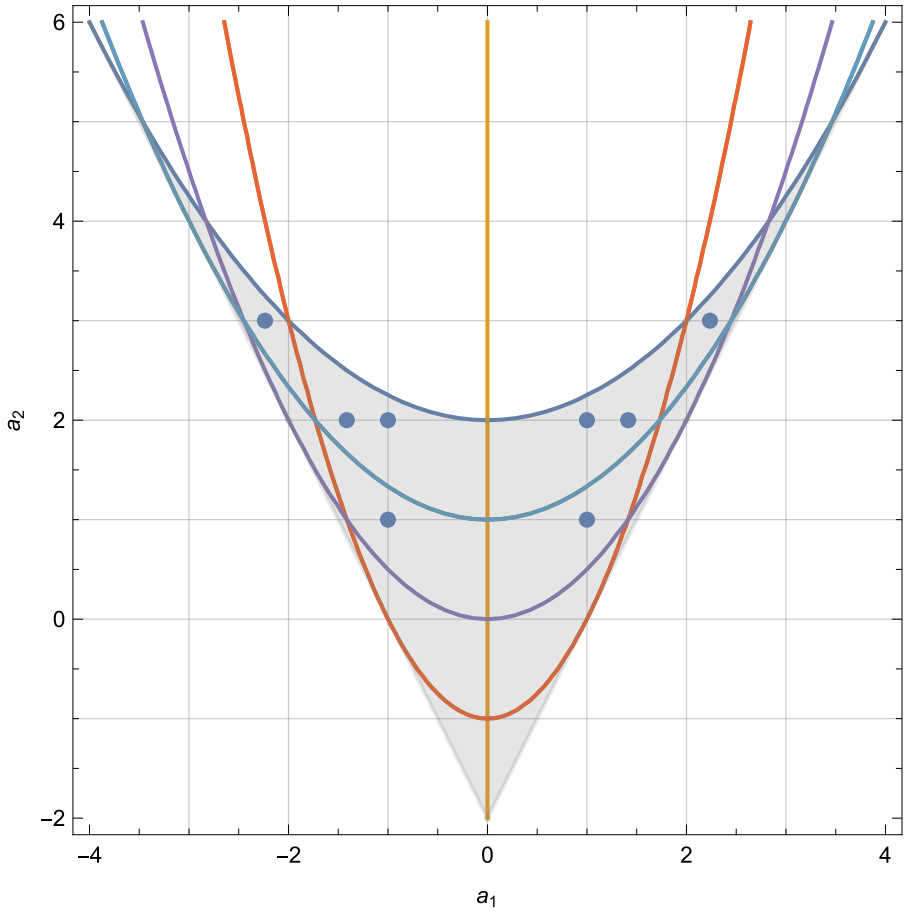


Figure 2.1: Plot of S and the pairs (a_1, a_2) that correspond to $p \in \Pi_{\text{jump}}(X)$.

2.4 Discriminant of a K3 surface

In this section, we explain our approach to compute the discriminant D_X of a K3 surface X over $\mathbb{Q}$ as a square class, and we study how it influences $\Pi_{\text{jump}}(X)$. For existence and uniqueness we refer to [GKZ94], where they study discriminants in a very general setting. However, their approach is from an geometric point of view and scaling factors are not discussed from an arithmetic perspective.

Usually, the computation of D_X is unfeasible. Nonetheless, in our situation it is sufficient to know D_X as a square class, i.e., as an element of $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$. A key ingredient for this compuation is a recent theorem of Elsenhans and Jahnel (personal communication), where

they explicitly link D_X being a quadratic residue modulo p and the sign of the functional equation for the Hasse–Weil zeta function, expressly,

$$\det\left(1-\frac{t}{p}\operatorname{Frob}|H^2_{\mathrm{et}}(\overline{X}_{\mathfrak{p}},\mathbb{Q}_\ell)\right)=\left(\frac{D_X}{p}\right)t^{22}\det\left(1-\frac{1}{tp}\operatorname{Frob}|H^2_{\mathrm{et}}(\overline{X}_{\mathfrak{p}},\mathbb{Q}_\ell)\right). \tag{2.19}$$

We compute $D_X \bmod \mathbb{Q}^{\times 2}$ for X defined over $\mathbb{Q}$ by $f=0$ as follows. Using Gröbner basis, compute N such that

$$N\mathbb{Z}=\mathbb{Z}\cap\langle\partial f/\partial x_0,\ldots,\partial f/\partial x_3\rangle.$$

Now compute the prime factorization of $N=\prod_{i=1}^n p_i^{\alpha_i}$. The set $S=\{p_1,\ldots,p_n\}$ is a supset of the primes of bad reduction, thus

$$D_X \bmod \mathbb{Q}^{\times 2}=\pm 1\prod_{i\in R}p_i$$

for some $R\subset S$. Finally, sieve out R using equation (2.19) over multiple p. In practice, the dominant step is factoring N, as N has quite large prime factors, see Examples 2.9, 2.10 and 2.11.

Proof of Theorem 2.1. Let

$$Q(t):=\det\left(1-\frac{t}{p}\operatorname{Frob}|H^2_{\mathrm{et}}(\overline{X},\mathbb{Q}_\ell)\right)\in\mathbb{Q}[t].$$

Since $\rho(X_p)\geq 2r$ we have $Q(t)=(1-t)^{2r}P(t)$ with $P(t)\in\mathbb{Q}[t]$. Morever, from equation (2.19) it follows $P(t)=-t^{22-2r}P(1/t)$, i.e., $P(t)$ is an antipalindromic polynomial (the term antireciprocal is also used) of even degree. Hence, $P(t)$ must be divisible by $(1-t)(1+t)$ and $\rho(X_p)\geq 2r+1$. □

Corollary 2.6. *If the discriminant of X is not square modulo p and $\rho(X_p) \geq 2r$, then $\rho(X_{\mathbb{F}_{p^2}}) \geq 2r + 2$.*

2.5 Computations and numerical data

In this section, we present numerical data for five representative quartic K3 surfaces over $\mathbb{Q}$ with small $\rho(\overline{X})$. For each surface we compute $\rho(\overline{X})$ and $\rho(\overline{X}_p)$, for all $2 < p < 2^{16}$ where X has good reduction, using the methods introduced in Section 2.2. 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 $\rho(\overline{X}) = 1$ and $E_X = \mathbb{Q}$ we find evidence that

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

  for some constant $c_X > 0$, i.e., $\rho(\overline{X_p})$ jumps with probability proportional to $1/\sqrt{p}$.

- When $\rho(\overline{X}) = 2$ we obeserve

$$\left\{p : p \text{ is inert in } \mathbb{Q}(\sqrt{D_X})\right\} \subset \Pi_{\text{jump}}(X), \tag{2.20}$$

  where D_X is the discriminant of X. Furthermore, for these examples we find evidence that

$$\gamma\left(X_{\mathbb{Q}(\sqrt{D_X})}, B\right) \sim \frac{c_X}{\sqrt{B}}, \quad B \to \infty,$$

  for some constant $c_X > 0$. In other words, if p is inert $\mathbb{Q}(\sqrt{D_X})$ then p is in $\Pi_{\text{jump}}(X)$, and if p splits in $\mathbb{Q}(\sqrt{D_X})$, then p is in $\Pi_{\text{jump}}(X)$ with probability proportional to $1/\sqrt{p}$.

These trends seem to reflect which case of equation (2.6) we are in. However, equation (2.20) does not hold in general for $\rho(\overline{X}) = 2r$ with $r > 1$.

In our examples, we used the following, sufficiently generic, homogeneous polynomials:

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

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 2.7. *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 2.2, we find

$$\rho(\overline{X}_{p_1}) = 2 \text{ and } \operatorname{disc}(\mathrm{NS}(\overline{X}_{p_1})) = -3 \bmod \mathbb{Q}^{\times 2};$$
$$\rho(\overline{X}_{p_2}) = 2 \text{ and } \operatorname{disc}(\mathrm{NS}(\overline{X}_{p_2})) = -1 \bmod \mathbb{Q}^{\times 2}.$$

Therefore, $\rho(\overline{X}) = 1$. Furthermore, $\mathrm{NS}(\overline{X}_{p_1})$ is generated by the hyperplane section and the conic C and $\mathrm{NS}(\overline{X}_{p_2})$ is generated by the hyperplane section and the line L, see [vL07b, Remark 4]. In this example we observe $\rho(\overline{X}_p) > 4$ only for $p = 29$, where

$$\rho(\overline{X}_{29}) = 6 \text{ and } \operatorname{disc}(\mathrm{NS}(\overline{X}_{29})) = -537 \bmod \mathbb{Q}^{\times 2}.$$

Example 2.8. *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 $g_1 = g_3 = 0$. Now we have

$$\rho(\overline{X}_{p_1}) = 2 \text{ and } \operatorname{disc}(\mathrm{NS}(\overline{X}_{p_1})) = -1 \bmod \mathbb{Q}^{\times 2};$$
$$\rho(\overline{X}_{p_2}) = 2 \text{ and } \operatorname{disc}(\mathrm{NS}(\overline{X}_{p_2})) = -1 \bmod \mathbb{Q}^{\times 2}.$$

As in the previous example, $\mathrm{NS}(\overline{X}_{p_2})$ is generated by the hyperplane section and the line L, thus $\operatorname{disc}(\mathrm{NS}(\overline{X}_{p_2})) = -9$. On the other hand, the hyperplane section and the elliptic curve C generate a subllatice of $\mathrm{NS}(\overline{X}_{p_1})$ with discriminant -16. Consequently, $\operatorname{disc}\mathrm{NS}(\overline{X}_{p_1}) = -1, -4$ or -16, thus $\rho(\overline{X}) = 1$. Alternatively, one could have inspected $\overline{X}_{19}$ where

$$\rho(\overline{X}_{19}) = 2 \text{ and } \operatorname{disc}(\mathrm{NS}(\overline{X}_{19})) = -26 \bmod \mathbb{Q}^{\times 2}.$$

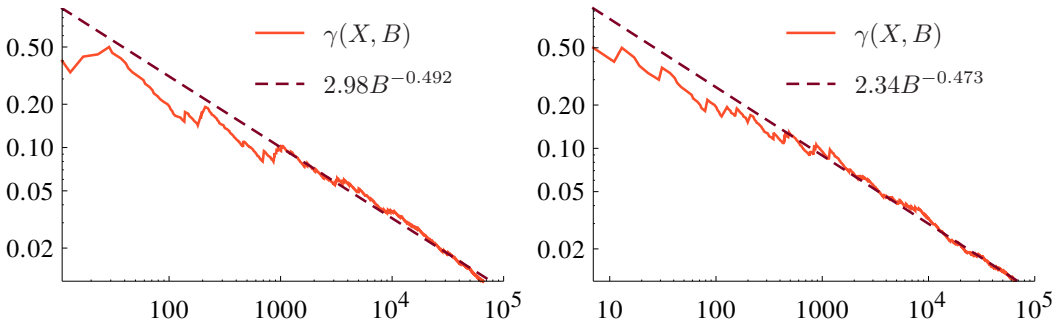
As in the previous example, $\rho(\overline{X}_p) > 4$ *for only one prime* $p = 7$*, where*

$$\rho(\overline{X}_7) = 6 \text{ and } \operatorname{disc}(\mathrm{NS}(\overline{X}_7)) = -345 \bmod \mathbb{Q}^{\times 2}.$$

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 2.2. We observe that

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

for some constant $c_X > 0$.



(a) Example 2.7 (b) Example 2.8

Figure 2.2: Log-log plots of γ and their least-square-fit to a power law in Examples 2.7 and 2.8.

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 $\rho(\overline{X}_p) = 2$. Further, we also compute its discriminant D_X modulo $\mathbb{Q}^{\times 2}$ as described in Section 2.4.

Example 2.9. *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 $\rho(\overline{X}_p) = 2$.

$$\begin{aligned} D_X = &- 1 \cdot 5 \cdot 151 \cdot 22490817357414371041 \cdot \\ &387308497430149337233666358807996260780875056740850\ldots \\ &98421327697034327893534206888970614673331378 9 \bmod \mathbb{Q}^{\times 2} \end{aligned}$$

Example 2.10. *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 $\rho(\overline{X}_p) = 2$.

$$\begin{aligned} D_X = &53 \cdot 2624174618795407 \cdot 5128545618469648171394942020727783 41 \cdot \\ &12152183700890287690767181021269217443533628 73 \cdot \\ &68471243971589504569213004351581154456270727349961490419905638575 03 \bmod \mathbb{Q}^{\times 2} \end{aligned}$$

Example 2.11. *Let X be defined by*

$$g_1g_2 + g_3g_4 = 0,$$

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

$$\begin{aligned} D_X = &- 1 \cdot 47 \cdot 3109 \cdot 4969 \cdot 14857095849982608071 \cdot \\ &44541027766092834776258676433187443220258468801614 9 \cdot \\ &65865270852505269999342419873884248 59\ldots \\ &98115218667979560362214198830101650254490711 \bmod \mathbb{Q}^{\times 2} \end{aligned}$$

In Figure 2.3 we present plots of $\gamma(X, B)$ for the previous examples. These suggest that

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

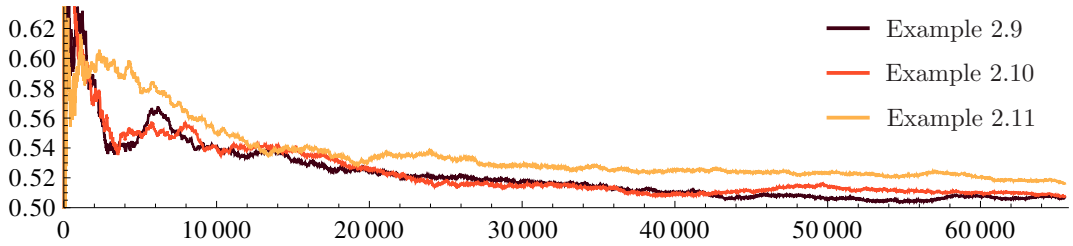


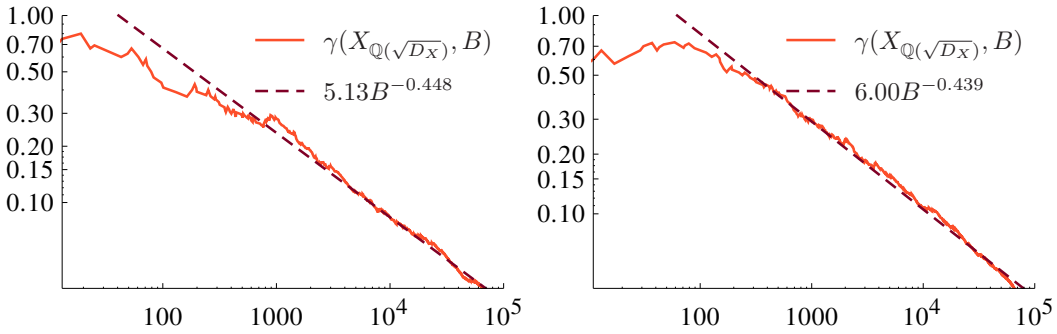
Figure 2.3: Plots of $\gamma(X, B)$ for the Examples 2.9, 2.10 and 2.11.

For these examples we also inspected $\gamma\left(X_{\mathbb{Q}(\sqrt{D_X})}, B\right)$. We present the log-log plots of $\gamma\left(X_{\mathbb{Q}(\sqrt{D_X})}, B\right)$ for the previous examples and their respective least square fit to a power law in Figure 2.4. We observe

$$\gamma\left(X_{\mathbb{Q}(\sqrt{D_X})}, B\right) \sim \frac{c_X}{\sqrt{B}}, \quad B \to \infty,$$

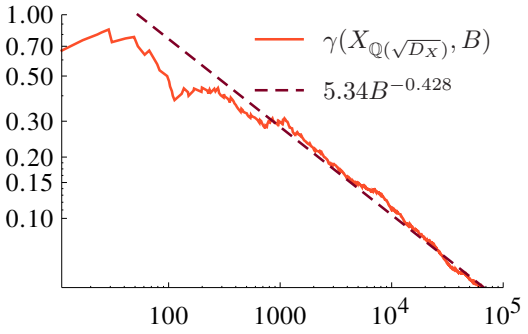
for some constant $c_X > 0$.

While in these examples we observed $\rho(\overline{X}_p) > 2$ more frequently than in Examples 2.7 and 2.8, the number of primes such that $\rho(\overline{X}_p) > 4$ is quite small. We present those in Table 2.1.



(a) Example 2.9

(b) Example 2.10



(c) Example 2.11

Figure 2.4: Log-log plots of $\gamma\left(X_{\mathbb{Q}(\sqrt{D_X})}, B\right)$ and their least-square-fit to a power law in Examples 2.9, 2.10 and 2.11.

Example 2.9

p	$\rho(\overline{X}_p)$
3	6
11	6
13	6
47	6
53	6
181	6
239	6
25087	6

Example 2.10

p	$\rho(\overline{X}_p)$
3	10
5	10
11	6
29	6
83	6
491	6
2777	6
3187	6

Example 2.11

p	$\rho(\overline{X}_p)$
3	6
17	6
347	6

Table 2.1: Primes $p < 2^{16}$ for which $\rho(\overline{X}_p) > 4$.

Bibliography

[AH96] Leonard M. Adleman and Ming-Deh A. Huang. Counting rational points on curves and abelian varieties over finite fields. In *Algorithmic number theory (Talence, 1996)*, volume 1122 of *Lecture Notes in Comput. Sci.*, pages 1–16. Springer, Berlin, 1996.

[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.

[Ber97] Pierre Berthelot. Finitude et pureté cohomologique en cohomologie rigide. *Invent. Math.*, 128(2):329–377, 1997. With an appendix in English by Aise Johan de Jong.

[BG08] Srinath Baba and Håkan Granath. Primes of superspecial reduction for QM abelian surfaces. *Bull. Lond. Math. Soc.*, 40(2):311–318, 2008.

[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.

[BK86] Spencer Bloch and Kazuya Kato. p-adic étale cohomology. *Inst. Hautes Études Sci. Publ. Math.*, (63):107–152, 1986.

[CdlORV03] Philip Candelas, Xenia de la Ossa, and Fernando Rodriguez-Villegas. Calabi-Yau manifolds over finite fields. II. In *Calabi-Yau varieties and mirror symmetry (Toronto, ON, 2001)*, volume 38 of *Fields Inst. Commun.*, pages 121–157. Amer. Math. Soc., Providence, RI, 2003.

[CGH14] Edgar Costa, Robert Gerbicz, and David Harvey. A search for Wilson primes. *Math. Comp.*, 83(290):3071–3091, 2014.

[CH14] Edgar Costa and David Harvey. Faster deterministic integer factorization. *Math. Comp.*, 83(285):339–345, 2014.

[Cha11] François Charles. On the Picard number of K3 surfaces over number fields. *preprint*, 2011. `arXiv:1111.4117`.

[Cha13] François Charles. The Tate conjecture for $K3$ surfaces over finite fields. *Invent. Math.*, 194(1):119–145, 2013.

[Cha14] François Charles. Frobenius distribution for pairs of elliptic curves and exceptional isogenies. *preprint*, 2014. `arXiv:1411.2914`.

[CHK15] Edgar Costa, David Harvey, and Kiran S. Kedlaya. Zeta functions of nondegenerate toric hypersurfaces via controlled reduction in p-adic cohomology. *in preparation*, 2015.

[CT14] Edgar Costa and Yuri Tschinkel. Variation of nronseveri ranks of reductions of k3 surfaces. *Experimental Mathematics*, 23(04):475–481, 2014.

[Del72] Pierre Deligne. La conjecture de Weil pour les surfaces $K3$. *Invent. Math.*, 15:206–226, 1972.

[Deu41] Max Deuring. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hansischen Univ.*, 14:197–272, 1941.

[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.

[GKZ94] I. M. Gel′fand, M. M. Kapranov, and A. V. Zelevinsky. *Discriminants, resultants, and multidimensional determinants*. Mathematics: Theory & Applications. Birkhäuser Boston, Inc., Boston, MA, 1994.

[Gri69] Phillip A. Griffiths. On the periods of certain rational integrals. I, II. *Ann. of Math. (2) 90 (1969), 460-495; ibid. (2)*, 90:496–541, 1969.

[Har07] David Harvey. Kedlaya's algorithm in larger characteristic. *Int. Math. Res. Not. IMRN*, (22):Art. ID rnm095, 29, 2007.

[Har10a] David Harvey. Computing zeta functions of certain varieties in larger characteristic. `http://web.maths.unsw.edu.au/~davidharvey/talks/zetasqrtp-talk.pdf`, 2010. [Online; accessed 14-March-2015].

[Har10b] David Harvey. Computing zeta functions of projective surfaces in large characteristic. `http://web.maths.unsw.edu.au/~davidharvey/talks/zetasqrtp-talk3.pdf`, 2010. [Online; accessed 14-March-2015].

[Har10c] David Harvey. Counting points on projective hypersurfaces. `http://web.maths.unsw.edu.au/~davidharvey/talks/zetasurface.pdf`, 2010. [Online; accessed 14-March-2015].

[Har14] David Harvey. Counting points on hyperelliptic curves in average polynomial time. *Ann. of Math. (2)*, 179(2):783–803, 2014.

[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.

[HS14a] David Harvey and Andrew V. Sutherland. Computing Hasse-Witt matrices of hyperelliptic curves in average polynomial time. *LMS J. Comput. Math.*, 17(suppl. A):257–273, 2014.

[HS14b] David Harvey and Andrew V. Sutherland. Counting points on hyperelliptic curves in average polynomial time, ii. *preprint*, 2014. `arXiv:1410.5222`.

[Jao03] David Yen Jao. *Supersingular primes for rational points on modular curves*. ProQuest LLC, Ann Arbor, MI, 2003. Thesis (Ph.D.)–Harvard University.

[Kat68] Nicholas M. Katz. On the differential equations satisfied by period matrices. *Inst. Hautes Études Sci. Publ. Math.*, (35):223–258, 1968.

[Kat89] Kazuya Kato. Logarithmic structures of Fontaine-Illusie. In *Algebraic analysis, geometry, and number theory (Baltimore, MD, 1988)*, pages 191–224. Johns Hopkins Univ. Press, Baltimore, MD, 1989.

[Kat09] Nicholas M. Katz. Lang-Trotter revisited. *Bull. Amer. Math. Soc. (N.S.)*, 46(3):413–457, 2009.

[Ked01] Kiran S. Kedlaya. Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology. *J. Ramanujan Math. Soc.*, 16(4):323–338, 2001.

[Ked07] Kiran S. Kedlaya. Search techniques for root-unitary polynomials. *preprint*, 2007. `arXiv:0608104`.

[KS08] Kiran S. Kedlaya and Andrew V. Sutherland. Computing L-series of hyperelliptic curves. In *Algorithmic number theory*, volume 5011 of *Lecture Notes in Comput. Sci.*, pages 312–326. Springer, Berlin, 2008.

[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.

[Mac94] F. S. Macaulay. *The algebraic theory of modular systems*. Cambridge Mathematical Library. Cambridge University Press, Cambridge, 1994. Revised reprint of the 1916 original, With an introduction by Paul Roberts.

[Mau12] Davesh Maulik. Supersingular k3 surfaces for large primes. *preprint*, 2012. arXiv:1203.2889.

[Maz73] Barry Mazur. Frobenius and the Hodge filtration (estimates). *Ann. of Math. (2)*, 98:58–95, 1973.

[Mil75a] James S. Milne. On a conjecture of Artin and Tate. *Ann. of Math. (2)*, 102(3):517–533, 1975.

[Mil75b] James S. Milne. On a conjecture of Artin and Tate - addendum, 1975. http://www.jmilne.org/math/articles/add/1975a.pdf.

[Mon70] Paul Monsky. *p-adic analysis and zeta functions*, volume 4 of *Lectures in Mathematics, Department of Mathematics, Kyoto University*. Kinokuniya Book-Store Co., Ltd., Tokyo, 1970.

[Mum70] David Mumford. *Abelian varieties*. Tata Institute of Fundamental Research Studies in Mathematics, No. 5. Published for the Tata Institute of Fundamental Research, Bombay; Oxford University Press, London, 1970.

[Oor88] Frans Oort. Endomorphism algebras of abelian varieties. In *Algebraic geometry and commutative algebra, Vol. II*, pages 469–502. Kinokuniya, Tokyo, 1988.

[Per13] Keerthi Madapusi Pera. The Tate conjecture for K3 surfaces in odd characteristic. *preprint*, 2013. arXiv:1301.6326.

[Pil90] J. Pila. Frobenius maps of abelian varieties and finding roots of unity in finite fields. *Math. Comp.*, 55(192):745–763, 1990.

[PTvL12] Bjorn Poonen, Damiano Testa, and Ronald van Luijk. Computing Néron-Severi groups and cycle class groups. *preprint*, 2012. arXiv:1210.3720.

[Sad04] Marat Sadykov. *Two results in the arithmetic of Shimura curves*. ProQuest LLC, Ann Arbor, MI, 2004. Thesis (Ph.D.)–Columbia University.

[Sch85] René Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Math. Comp.*, 44(170):483–494, 1985.

[Sch12] Matthias Schuett. Two lectures on the arithmetic of K3 surfaces. *preprint*, 2012. `arXiv:1202.1066`.

[Ser81] Jean-Pierre Serre. Quelques applications du théorème de densité de Chebotarev. *Inst. Hautes Études Sci. Publ. Math.*, (54):323–401, 1981.

[Ser12] Jean-Pierre Serre. *Lectures on $N_X(p)$*, volume 11 of *Chapman & Hall/CRC Research Notes in Mathematics*. CRC Press, Boca Raton, FL, 2012.

[Shi63] Goro Shimura. On analytic families of polarized abelian varieties and automorphic functions. *Ann. of Math. (2)*, 78:149–192, 1963.

[Sho13] Victor Shoup. NTL: Number Theory Library, 2013. Version 6.0.0, `http://www.shoup.net/ntl/`.

[Sut15] Andrew V. Sutherland. smalljac software library, 2015. Version 4.0.28, `http://math.mit.edu/~drew/`.

[SV13] Steven Sperber and John Voight. Computing zeta functions of nondegenerate hypersurfaces with few monomials. *LMS J. Comput. Math.*, 16:9–44, 2013.

[Tat66] John Tate. Endomorphisms of abelian varieties over finite fields. *Invent. Math.*, 2:134–144, 1966.

[vdP86] Marius van der Put. The cohomology of Monsky and Washnitzer. *Mém. Soc. Math. France (N.S.)*, (23):4, 33–59, 1986. Introductions aux cohomologies p-adiques (Luminy, 1984).

[vL06] Ronald van Luijk. Quartic $K3$ surfaces without nontrivial automorphisms. *Math. Res. Lett.*, 13(2-3):423–439, 2006.

[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.

[War15] Matthew Ward. Canonical lifts of ordinary calabi-yau threefolds. *in preparation*, 2015.

[Zar83] Yuri G. Zarhin. Hodge groups of $K3$ surfaces. *J. Reine Angew. Math.*, 341:193–220, 1983.