Computing the zeta function of varieties over finite fields

Nitin Saxena and Madhavan Venkatesh

CSE, IIT Kanpur

National Mathematics Day

IITK MTH-STAT, February 2025

Outline

The problem

Point counting

Given a system of equations over a ring k, can we efficiently count /classify its number of points defined over k?

- If $k = \mathbb{Z}$, there is no general-purpose algorithm which does this (Matiyasevich 1970). $k = \mathbb{Q}$ is open, even when the system has dimension 1.
- $k = \mathbb{Q}$, for an elliptic curve, algorithm known conjecturally, under BSD: Birch–Swinnerton-Dyer conjecture (1965).
- $k = \mathbb{Q}$ smooth projective higher genus curves: Alpöge-Lawrence (2024) under heavy-duty conjectures.
- $\dim > 1$: Completely open. e.g.: Euler's brick (6 lengths).

The problem

Point counting

- We are concerned with k a finite field of char p.
- We've a smooth, projective geometrically irreducible variety $X \subset \mathbb{P}^N$ of dimension n and degree D over $\mathbb{Q}$, given by homogeneous forms $f_1, \ldots, f_m$, each of degree $\leq d$. Let p be a prime of good reduction.
- (Question) Does there exist an algorithm which computes $\#X(\mathbb{F}_p)$ in time poly$(\log p)$?
- (Serre) What if X is simply a scheme of finite type over $\mathbb{Z}$?

Motivation

Cryptography

- Elliptic and hyperelliptic curve cryptography.
- Coding theory, in particular Goppa codes.

Distribution of point-counts

- Sato-Tate conjecture, 1960: equidistribution of Frobenius angles/ errors in the point-count.
- Katz-Sarnak philosophy, 1999: statistics of zeros of L – functions of varieties over finite fields and links to eigenvalues of random matrices in classical groups.

Zeta function

Let X be as above. Define the *zeta-function*

$$Z(X/\mathbb{F}_q, T) := \exp\left(\sum_{j=1}^{\infty} \#X(\mathbb{F}_{q^j})\frac{T^j}{j}\right).$$

It encodes the point-counts over all finite extensions of $\mathbb{F}_q$, in an *exponential generating function*. (Power-series)

Computational Qn: can one compute $Z(X/\mathbb{F}_q, T)$ in time polynomial in $\log q$?

Weil Conjectures (Deligne 1974)

- *Rational* function:

$$Z(X/\mathbb{F}_q, T) = \prod_{i=0}^{2n} P_i(T)^{(-1)^{i+1}} \in \mathbb{Q}(T).$$

- *Functional* equation:

$$Z(X/\mathbb{F}_q, 1/q^n T) = \pm q^{n(\chi/2)} \cdot T^{\chi} \cdot Z(X/\mathbb{F}_q, T).$$

- Riemann hypothesis: If $P_i(T) =: \prod_{j=1}^{\deg P_i}(1 - \alpha_{i,j} T)$, then $|\alpha_{i,j}| = q^{i/2}$. [i.e. complex roots 'know' q]

Instantiate it to Curves

Artin, Hasse, Weil

Let $C/\mathbb{F}_q$ be a smooth projective curve of *genus* g. Then,

$$Z(C/\mathbb{F}_q, T) = \frac{P(T)}{(1-T)(1-qT)},$$

where $P(T) \in \mathbb{Z}[T]$, of degree $2g$ such that $P(0) = 1$.

- $Z(C/\mathbb{F}_q, 1/qT) = q^{1-g} \cdot T^{2-2g} \cdot Z(C/\mathbb{F}_q, T)$.
- Finally, writing $P(T) = \prod_{i=1}^{2g}(1-\alpha_i T)$, we have $|\alpha_i| = \sqrt{q}$. This is equivalent to the Weil-bound

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

Elliptic Curves

Schoof (1985)

Let $E/\mathbb{F}_q$ be an elliptic curve, i.e., a smooth projective curve of genus 1. There exists an algorithm that computes $\#E(\mathbb{F}_q)$ in time polynomial in $\log q$.

Idea:

- The charpoly (inverted) of the Frobenius endomorphism ϕ_q is $qT^2 - a_q T + 1 = 0$, where $a_q = q + 1 - \#E(\mathbb{F}_q)$.
- Compute $a_q \bmod \ell$ by working with $E[\ell]$, using division polynomials for small primes ℓ.
- Recover a_q by CRT using Hasse bound.

Generalize to curves and abelian varieties

Pila (1988), Huang-Ierardi (1993)

Let $C/\mathbb{F}_q$ be a smooth projective curve of fixed genus g. There exists an algorithm that computes $\#C(\mathbb{F}_q)$ in time polynomial in $\log q$.

Idea:

- Move to the Jacobian variety $J = J(C)$ by choosing a rational point.
- Use ideal theory/ semi-algebraic sets to compute representatives of $J[\ell]$ for small primes ℓ.
- Recover char poly of Frobenius via action on $J[\ell]$ and CRT.

Beyond Curves? – Weil cohomology

A contravariant functor (from prime char(k) to zero char(K))

$$H^\bullet : \mathbf{SmVar}_k \longrightarrow \mathbf{GrAlg}_K$$

$$H^\bullet(X) = \bigoplus_{j\in\mathbb{Z}} H^j(X)$$

satisfying several 'nice' *analytic* properties such as

- Trace map
- Cycle class map
- Künneth formula
- Poincaré duality

Cohomological interpretation

Consequence: Zeta has a nice closed form expression coming from the Lefschetz trace formula.

$$Z(X/\mathbb{F}_q, T) = \frac{P_1(T)\cdots P_{2n-1}(T)}{P_0(T)\cdots P_{2n}(T)} = \prod_{i=0}^{2n} (P_i(T))^{(-1)^{i+1}}$$

where

$$P_i(T) = \det\left(1 - TF_q^\star \mid H^i(X)\right).$$

Étale cohomology development

- Modern School [Grothendieck et.al. 1950s - 60s]:
- Identified that constant (non-torsion) coefficients cannot work, *Zariski topology is too coarse*.
- Changed the notion of 'open set' to étale covers.
- Realized constant torsion coefficients within the structure sheaf by the Kummer sequence by choosing ℓ coprime to base char p.
- Defined ℓ-adic (étale) cohomology as the limit of ℓ^r-cohomology groups.

p-adic cohomologies – better for computation?

- Monsky-Washnitzer cohomology.
- Crystalline cohomology.
- Rigid cohomology.

Algorithms

- Kedlaya 2002, and others, for curves.
- Lauder 2004 Deformation theory and p-adic calculus.
- Lauder-Wan 2006 Dwork type trace-formula.
- Harvey 2015 'Non-cohomological' trace formula.

Problem: They're all exponential-time in $\log p$.

H^1 or Tate/ Picard computation?

- Kummer sequence makes it explicit.
- Isomorphic to Tate module of Picard variety.
- Schoof'85–Pila'88 is actually étale algorithm in disguise.

Higher-dimension issues

- A priori, Picard group has sums of codim=1 subvarieties modulo a relation.
- The equivalence relation is non-explicit.
- How to computationally represent the required divisors?

Computing $P_1(T)$ – char poly of H^1

Theorem (Roy, Saxena, Venkatesh 2024)

Let $X \subset \mathbb{P}^N$ be a smooth projective variety over $\mathbb{F}_q$ of degree D and let $P_1(X/\mathbb{F}_q, T) := \det(1 - TF_q^\star \mid \mathrm{H}^1(X, \mathbb{Q}_\ell))$. There exists:

- *randomised* algorithm to compute $P_1(X/\mathbb{F}_q, T)$ for fixed D in time $O((\log q)^\Delta)$,
- *quantum* algorithm to compute $P_1(X/\mathbb{F}_q, T)$ in time polynomial in $D \log q$.

  Can also certify (in the sense of Arthur-Merlin protocol) with similar time complexity.

Algorithm

- Reduce to surface-case via weak-Lefschetz.
- Let $(X_t)_{t\in\mathbb{P}^1}$ be a Lefschetz pencil of hyperplane sections on X.
- Sample smooth curves X_{u_1}, X_{u_2} for $u_1, u_2 \in \mathbb{F}_Q$, in a *poly*-bounded field extension.
- Compute their zeta functions and take gcd of the numerators. With high probability this is $P_1(X/\mathbb{F}_Q, T)$.
- Recover $P_1(X/\mathbb{F}_q, T)$ using Kedlaya's recipe.

Proof Ideas

- Hard-Lefschetz, big mod-ℓ monodromy of vanishing cycles.
- Equidistribution of Frobenius mod-ℓ.

Zeta function of a surface

Question (Couveignes-Edixhoven, 2011)

When X is a surface, i.e., dim=2, is there an algorithm that counts points in poly($\log q$) time?

Difficulties

- While our earlier algorithm computes $P_1(T)$, it doesn't make $\mathrm{H}^1(X, \mu_\ell)$ explicit.
- Higher degree cohomology only recently shown to be computable (Madore-Orgogozo, 2015), with no complexity analysis.
- Levrat 2023: Proposes a strategy to reduce to a curve of genus poly(ℓ), by moving over a function field.

Cohomology reduction & challenges

Let $\overline{\eta} \to \mathbb{P}^1$ be a geometric generic point and write the push-forward sheaf $\mathcal{F} := R^1\pi_\star\mu_\ell$. $\mathcal{F}|_U$ is locally constant. By Léray sequence $\mathrm{H}^i(\mathbb{P}^1, R^j\pi_\star\mu_\ell) \Rightarrow \mathrm{H}^{i+j}(X, \mu_\ell)$, we have

$$\mathrm{H}^i(X, \mu_\ell) \simeq \begin{cases} \mathrm{H}^0(\mathbb{P}^1, \mathcal{F}), i = 1; \\ \mathrm{H}^1(\mathbb{P}^1, \mathcal{F}) \oplus \langle\gamma_E\rangle \oplus \langle\gamma_F\rangle, \ i = 2; \\ \mathrm{H}^2(\mathbb{P}^1, \mathcal{F}), \ i = 3. \end{cases} \tag{1}$$

If we trivialise $\mathcal{F}|_U$ with a cover $V \to U$, then $\mathrm{H}^2(X, \mu_\ell)$ can be found inside $\mathrm{H}^1(V, \mu_\ell)$, where V is the normalisation of $k(\mathbb{P}^1)$ in $k(\mathrm{Pic}^0(X_{\overline{\eta}})[\ell])$. But, V has genus $\mathrm{poly}(\ell)$ and algos to compute H^1 run in time exp in genus.

Vanishing cycles (**Monodromy** around singularities)

- Let Z be the singular locus of X over the line. Consider now a *singular fibre* X_z for $z \in Z$ and its *normalisation* $\tilde{X}_z \to X_z$. It induces the map on torsion $\mathrm{Pic}^0(X_z)[\ell] \to \mathrm{Pic}^0(\tilde{X}_z)[\ell]$. Its kernel is rk one and generated by say δ_z, the vanishing cycle at z.
- Under a cospecialisation map $\mathcal{F}_z \hookrightarrow \mathcal{F}_{\overline{\eta}}$, the vanishing cycle δ_z is uniquely determined (upto sign) by the Picard-Lefschetz formula

$$\sigma_z(\gamma) = \gamma - \langle \gamma, \delta_z \rangle \delta_z \,. \tag{2}$$

To realize σ_z: Fix root of unity ζ_ℓ s.t. $\sigma_z\left(\theta_z^{1/\ell}\right) = \zeta_\ell \cdot \theta_z^{1/\ell}$ for a local parameter θ_z at z (say, $t - z$).

Cohomology of a surface, algebraically

From the Galois cohomology of étale fundamental group of X, one gets the following complex

$$\mathcal{F}_{\overline{\eta}} \xrightarrow{\alpha} \mu_\ell^r \xrightarrow{\beta} \mathcal{F}_{\overline{\eta}} \tag{3}$$

where $r := \#Z$ and with, for any $\gamma \in \mathcal{F}_{\overline{\eta}}$, use Weil pairing,

$$\alpha(\gamma) := (\langle\gamma, \delta_{z_1}\rangle, \ldots, \langle\gamma, \delta_{z_r}\rangle)$$

and for any r – tuple $(a_1, \ldots, a_r) \in \mu_\ell^r$

$$\beta(\mathbf{a}) := a_1 \cdot \delta_{z_1} + a_2 \cdot \sigma_{z_1}(\delta_{z_2}) + \ldots + a_r \cdot \sigma_{z_1} \cdots \sigma_{z_{r-1}}(\delta_{z_r}) \,.$$

H^2 of a surface, algebraically

The cohomology groups of the above complex are related to the cohomology of X, i.e.,

$$\mathrm{H}^i(X, \mathbb{Z}/\ell\mathbb{Z}) \simeq \begin{cases} \ker(\alpha), & i = 1; \\ (\ker(\beta)/\mathrm{im}(\alpha)) \oplus \langle\gamma_E\rangle \oplus \langle\gamma_F\rangle, & i = 2; \\ \mathrm{coker}(\beta), & i = 3. \end{cases} \tag{4}$$

H^2 of a surface, algebraically

The cohomology groups of the above complex are related to the cohomology of X, i.e.,

$$\mathrm{H}^i(X, \mathbb{Z}/\ell\mathbb{Z}) \simeq \begin{cases} \ker(\alpha), & i = 1; \\ (\ker(\beta)/\mathrm{im}(\alpha)) \oplus \langle \gamma_E \rangle \oplus \langle \gamma_F \rangle, & i = 2; \\ \mathrm{coker}(\beta), & i = 3. \end{cases} \tag{4}$$

The second cohomology measures the subtlety of monodromy across the singular loci.

Surface algorithm

Theorem 1 (Saxena-Venkatesh, 2025).

Let $X \subset \mathbb{P}^N$ be a nice surface of fixed degree D over a finite field $\mathbb{F}_q$, obtained via good reduction from a nice surface $\mathcal{X}$ defined over a number field K at a prime $\mathfrak{p} \subset \mathcal{O}_K$. Further, assume the coefficients of the equations defining $\mathcal{X}$ have Weil – height bounded by $H \in \mathbb{R}_{>0}$ and write $\Delta = [K : \mathbb{Q}]$. Then, there exists a randomised algorithm that outputs

- *on input a prime number ℓ coprime to q, the étale cohomology groups $\mathrm{H}^i(X, \mathbb{Z}/\ell\mathbb{Z})$ for $0 \leq i \leq 4$ along with the Frobenius action in time $\mathrm{poly}(\ell \cdot H \cdot \Delta)$*
- *the zeta function $Z(X/\mathbb{F}_q, T)$, and the point-count $\#X(\mathbb{F}_q)$ in time $\mathrm{poly}(\log q \cdot H \cdot \Delta)$.*

Puiseux series makes things *explicit*

Goal: Make the complex (3) explicit along with the maps α, β and $\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ – action.

This gives $\mathrm{H}^i(X, \mathbb{Z}/\ell\mathbb{Z})$ with Frobenius action, from which zeta fn and point-count follow via standard arguments.

Main question

- How to view the cospecialisation map $\mathcal{F}_z \hookrightarrow \mathcal{F}_{\overline{\eta}}$? In particular, for $z \in Z$, what is $\delta_z \in \mathcal{F}_{\overline{\eta}}$?
- **Toy example:** Given a plane curve $F(x, y) = 0$, with x-singularities parametrized by set Z. For $z_1, z_2 \in Z$, how to consistently identify Puiseux branches $\delta_{z_1}, \delta_{z_2}$ of y around $x = z_1, z_2$ respectively, with roots of $F(x, y)$ living in $\overline{k[x]}$?
  E.g. $F : y^2 = x(1 - x)$, with $z_1 = 0$, $z_2 = 1$. The root y *requires* Puiseux series in the *local* parameters $\pm\sqrt{x}$, $\pm\sqrt{1 - x}$ respectively. ($x \mapsto 0.4$?)

High-level algorithm

Idea: To complex analysis and back!

- Use Puiseux expansions for cospec. to the generic fibre, after computing an ℓ – division polynomial system.
- As the situation is over $\mathbb{Q}$, for each $z \in Z$, work around a smooth point u_z lying within the radii of convergence.
- Compute the vanishing cycle in the fibre of the cohomology at u_z using the Picard-Lefschetz formulas.
- Reduce to positive characteristic assuming the u_z are all congruent modulo the prime ideal $\mathfrak{p}$ to a common u $\in \mathbb{F}_q$. *This collects all the vanishing cycles in a common fibre $\mathcal{F}_u$, from which the result follows.*

Our papers

Based on: [Click here for the Preprints]

(i) Diptajit Roy, Nitin Saxena, Madhavan Venkatesh *"Complexity of counting points on curves, and the factor $P_1(T)$ of the zeta function of surfaces"*, submitted, 2024.

(ii) Nitin Saxena, Madhavan Venkatesh *"Counting points on surfaces in polynomial time"*, submitted, 2025.

Thank you!