Zeta functions of varieties: tools and applications

Kiran S. Kedlaya

Department of Mathematics, University of California, San Diego
kedlaya@ucsd.edu
http://kskedlaya.org/slides/

Birational Geometry and Arithmetic
Institute for Computational and Experimental Research in Mathematics
Providence, May 16, 2018

Supported by NSF (grant DMS-1501214), UCSD (Warschawski chair).

Contents

Contents

Zeta functions

For X a smooth proper variety over a finite field $\mathbb{F}_q$, its *zeta function* is

$$\zeta_X(s) = \prod_{x \in X^\circ} (1 - |\kappa(x)|^{-s})^{-1} \qquad X^\circ = \{\text{closed points of } X\}$$
$$= \exp\left(\sum_{n=1}^{\infty} \#X(\mathbb{F}_{q^n}) \frac{q^{-ns}}{n}\right),$$

viewed as an absolutely convergent Dirichlet series for $\mathrm{Re}(s) > d = \dim(X)$ which represents a rational function of $T = q^{-s}$. It factors as

$$\frac{P_{X,1}(T) \cdots P_{X,2d-1}(T)}{P_{X,0}(T) \cdots P_{X,2d}(T)},$$

where $P_{X,i}(T) \in 1 + T\mathbb{Z}[T]$ has all $\mathbb{C}$-roots on the circle $|T| = q^{-i/2}$. If X lifts to characteristic 0, $\deg(P_{X,i})$ is the i-th Betti number of any lift.

L-functions

For X a smooth proper variety over a number field K, its (incomplete) i-th *L-function* is

$$L_{X,i}(s) = \prod_{\mathfrak{p}} P_{X_{\mathfrak{p}},i}(s)^{-1}$$

where $\mathfrak{p}$ runs over prime ideals of the ring of integers of K at which X has good reduction, and $X_{\mathfrak{p}}$ is the special fiber of the smooth model of X at $\mathfrak{p}$.

For best results, this product should be completed with additional factors corresponding to the remaining (finite and infinite) places of K; the result conjecturally admits a meromorphic extension and functional equation (known in a few cases), and an analogue of the Riemann hypothesis (known in no cases).

In some cases, $L_{X,i}(s)$ factors as a finite product of functions with good properties, corresponding to a decomposition of X into *motives*.

L-functions

For X a smooth proper variety over a number field K, its (incomplete) i-th *L-function* is

$$L_{X,i}(s) = \prod_{\mathfrak{p}} P_{X_{\mathfrak{p}},i}(s)^{-1}$$

where $\mathfrak{p}$ runs over prime ideals of the ring of integers of K at which X has good reduction, and $X_{\mathfrak{p}}$ is the special fiber of the smooth model of X at $\mathfrak{p}$.

For best results, this product should be completed with additional factors corresponding to the remaining (finite and infinite) places of K; the result conjecturally admits a meromorphic extension and functional equation (known in a few cases), and an analogue of the Riemann hypothesis (known in no cases).

In some cases, $L_{X,i}(s)$ factors as a finite product of functions with good properties, corresponding to a decomposition of X into *motives*.

L-functions

For X a smooth proper variety over a number field K, its (incomplete) i-th *L-function* is

$$L_{X,i}(s) = \prod_{\mathfrak{p}} P_{X_{\mathfrak{p}},i}(s)^{-1}$$

where $\mathfrak{p}$ runs over prime ideals of the ring of integers of K at which X has good reduction, and $X_{\mathfrak{p}}$ is the special fiber of the smooth model of X at $\mathfrak{p}$.

For best results, this product should be completed with additional factors corresponding to the remaining (finite and infinite) places of K; the result conjecturally admits a meromorphic extension and functional equation (known in a few cases), and an analogue of the Riemann hypothesis (known in no cases).

In some cases, $L_{X,i}(s)$ factors as a finite product of functions with good properties, corresponding to a decomposition of X into *motives*.

Computations of zeta and L-functions

The goal of this talk is to survey some aspects of algebraic/arithmetic geometry where zeta functions and L-functions, and numerical computations of them, play an important role. (We generally assume that varieties are being specified by explicit equations.)

In principle, given (a bound on) $\deg(P_{X,i})$, one can compute $\zeta_X(s)$ by brute force by enumerating $X(\mathbb{F}_{q^n})$ for $n = 1, 2, \dots$. This is impractical in all but a few cases.

A more robust approach is to interpret $P_{X,i}(T) = \det(1 - TF, V_i)$ where V_i is a certain finite-dimensional vector space over a field of characteristic 0 and $F : V_i \to V_i$ is a certain automorphism. E.g., one may take $V_i = H^i_{\mathrm{et}}(X_{\overline{\mathbb{F}}_q}, \mathbb{Q}_\ell)$ for $\ell \neq \operatorname{char}(\mathbb{F}_q)$ prime and F to be geometric Frobenius. However, étale cohomology is not defined in a particularly computable manner, so this only helps in a few cases.

Computations of zeta and L-functions

The goal of this talk is to survey some aspects of algebraic/arithmetic geometry where zeta functions and L-functions, and numerical computations of them, play an important role. (We generally assume that varieties are being specified by explicit equations.)

In principle, given (a bound on) $\deg(P_{X,i})$, one can compute $\zeta_X(s)$ by brute force by enumerating $X(\mathbb{F}_{q^n})$ for $n = 1, 2, \dots$. This is impractical in all but a few cases.

A more robust approach is to interpret $P_{X,i}(T) = \det(1 - TF, V_i)$ where V_i is a certain finite-dimensional vector space over a field of characteristic 0 and $F : V_i \to V_i$ is a certain automorphism. E.g., one may take $V_i = H^i_{\mathrm{et}}(X_{\overline{\mathbb{F}}_q}, \mathbb{Q}_\ell)$ for $\ell \neq \mathrm{char}(\mathbb{F}_q)$ prime and F to be geometric Frobenius. However, étale cohomology is not defined in a particularly computable manner, so this only helps in a few cases.

Computations of zeta and L-functions

The goal of this talk is to survey some aspects of algebraic/arithmetic geometry where zeta functions and L-functions, and numerical computations of them, play an important role. (We generally assume that varieties are being specified by explicit equations.)

In principle, given (a bound on) $\deg(P_{X,i})$, one can compute $\zeta_X(s)$ by brute force by enumerating $X(\mathbb{F}_{q^n})$ for $n = 1, 2, \dots$. This is impractical in all but a few cases.

A more robust approach is to interpret $P_{X,i}(T) = \det(1 - TF, V_i)$ where V_i is a certain finite-dimensional vector space over a field of characteristic 0 and $F : V_i \to V_i$ is a certain automorphism. E.g., one may take $V_i = H^i_{\mathrm{et}}(X_{\overline{\mathbb{F}}_q}, \mathbb{Q}_\ell)$ for $\ell \neq \mathrm{char}(\mathbb{F}_q)$ prime and F to be geometric Frobenius. However, étale cohomology is not defined in a particularly computable manner, so this only helps in a few cases.

Computations using p-adic cohomology

For $\ell = p = \mathrm{char}(\mathbb{F}_q)$, étale cohomology with $\mathbb{Q}_p$-coefficients does not satisfy the Lefschetz trace formula for Frobenius. Instead, we use *crystalline cohomology* with $\mathbb{Q}_q$-coefficients; this is not defined in a computable manner either, but it is equivalent to other constructions which are.

Notably, if X is smooth proper over a number field K and $X_{\mathfrak{p}}$ is a reduction, then crystalline cohomology with $K_{\mathfrak{p}}$-coefficients can be identified, as a bare vector space, with algebraic de Rham cohomology; in particular, this space is "independent of $\mathfrak{p}$." A construction of Monsky–Washnitzer describes the Frobenius action in terms of some convergent p-adic power series.

This can be made effective in a broad range of cases. The subsequent talk by Edgar Costa will treat in detail the case of (generic) smooth hypersurfaces in toric varieties.

Computations using p-adic cohomology

For $\ell = p = \mathrm{char}(\mathbb{F}_q)$, étale cohomology with $\mathbb{Q}_p$-coefficients does not satisfy the Lefschetz trace formula for Frobenius. Instead, we use *crystalline cohomology* with $\mathbb{Q}_q$-coefficients; this is not defined in a computable manner either, but it is equivalent to other constructions which are.

Notably, if X is smooth proper over a number field K and $X_{\mathfrak{p}}$ is a reduction, then crystalline cohomology with $K_{\mathfrak{p}}$-coefficients can be identified, as a bare vector space, with algebraic de Rham cohomology; in particular, this space is "independent of $\mathfrak{p}$." A construction of Monsky–Washnitzer describes the Frobenius action in terms of some convergent p-adic power series.

This can be made effective in a broad range of cases. The subsequent talk by Edgar Costa will treat in detail the case of (generic) smooth hypersurfaces in toric varieties.

Computations using p-adic cohomology

For $\ell = p = \mathrm{char}(\mathbb{F}_q)$, étale cohomology with $\mathbb{Q}_p$-coefficients does not satisfy the Lefschetz trace formula for Frobenius. Instead, we use *crystalline cohomology* with $\mathbb{Q}_q$-coefficients; this is not defined in a computable manner either, but it is equivalent to other constructions which are.

Notably, if X is smooth proper over a number field K and $X_{\mathfrak{p}}$ is a reduction, then crystalline cohomology with $K_{\mathfrak{p}}$-coefficients can be identified, as a bare vector space, with algebraic de Rham cohomology; in particular, this space is "independent of $\mathfrak{p}$." A construction of Monsky–Washnitzer describes the Frobenius action in terms of some convergent p-adic power series.

This can be made effective in a broad range of cases. The subsequent talk by Edgar Costa will treat in detail the case of (generic) smooth hypersurfaces in toric varieties.

Contents

Zeta functions of elliptic curves

For X an elliptic curve over $\mathbb{F}_q$, its zeta function has the form

$$\frac{1 - aT + qT^2}{(1-T)(1-qT)}, \qquad a = q + 1 - \#X(\mathbb{F}_q), \qquad |a| \leq 2\sqrt{q}.$$

Using the group structure, one can compute a in time $O(q^{1/4})$. This is optimal in practice for "reasonably big" q.

In cryptography, one cares about $\#X(\mathbb{F}_q)$ where q is "unreasonably big" (e.g., $q \sim 2^{256}$). In this case, the Schoof–Elkies–Atkin method, which computes $a \pmod{\ell}$ for various small ℓ by manipulating $X[\ell]$, is polynomial in $\log q$ and optimal in practice.

SEA amounts to working with mod-ℓ étale cohomology. This generalizes *in theory* to all curves (Pila), but has only been executed in genus 2 (Gaudry–Schost). It seems hard to extend to higher-dimensional varieties; an isolated case is Edixhoven's work on computing modular forms.

Zeta functions of elliptic curves

For X an elliptic curve over $\mathbb{F}_q$, its zeta function has the form

$$\frac{1 - aT + qT^2}{(1-T)(1-qT)}, \qquad a = q + 1 - \#X(\mathbb{F}_q), \qquad |a| \leq 2\sqrt{q}.$$

Using the group structure, one can compute a in time $O(q^{1/4})$. This is optimal in practice for "reasonably big" q.

In cryptography, one cares about $\#X(\mathbb{F}_q)$ where q is "unreasonably big" (e.g., $q \sim 2^{256}$). In this case, the Schoof–Elkies–Atkin method, which computes $a \pmod{\ell}$ for various small ℓ by manipulating $X[\ell]$, is polynomial in $\log q$ and optimal in practice.

SEA amounts to working with mod-ℓ étale cohomology. This generalizes *in theory* to all curves (Pila), but has only been executed in genus 2 (Gaudry–Schost). It seems hard to extend to higher-dimensional varieties; an isolated case is Edixhoven's work on computing modular forms.

Zeta functions of elliptic curves

For X an elliptic curve over $\mathbb{F}_q$, its zeta function has the form

$$\frac{1 - aT + qT^2}{(1-T)(1-qT)}, \qquad a = q + 1 - \#X(\mathbb{F}_q), \qquad |a| \leq 2\sqrt{q}.$$

Using the group structure, one can compute a in time $O(q^{1/4})$. This is optimal in practice for "reasonably big" q.

In cryptography, one cares about $\#X(\mathbb{F}_q)$ where q is "unreasonably big" (e.g., $q \sim 2^{256}$). In this case, the Schoof–Elkies–Atkin method, which computes $a \pmod{\ell}$ for various small ℓ by manipulating $X[\ell]$, is polynomial in $\log q$ and optimal in practice.

SEA amounts to working with mod-ℓ étale cohomology. This generalizes *in theory* to all curves (Pila), but has only been executed in genus 2 (Gaudry–Schost). It seems hard to extend to higher-dimensional varieties; an isolated case is Edixhoven's work on computing modular forms.

Zeta functions of elliptic curves

For X an elliptic curve over $\mathbb{F}_q$, its zeta function has the form

$$\frac{1 - aT + qT^2}{(1-T)(1-qT)}, \qquad a = q + 1 - \#X(\mathbb{F}_q), \qquad |a| \leq 2\sqrt{q}.$$

Using the group structure, one can compute a in time $O(q^{1/4})$. This is optimal in practice for "reasonably big" q.

In cryptography, one cares about $\#X(\mathbb{F}_q)$ where q is "unreasonably big" (e.g., $q \sim 2^{256}$). In this case, the Schoof–Elkies–Atkin method, which computes $a \pmod{\ell}$ for various small ℓ by manipulating $X[\ell]$, is polynomial in $\log q$ and optimal in practice.

SEA amounts to working with mod-ℓ étale cohomology. This generalizes *in theory* to all curves (Pila), but has only been executed in genus 2 (Gaudry–Schost). It seems hard to extend to higher-dimensional varieties; an isolated case is Edixhoven's work on computing modular forms.

L-functions of elliptic curves

For X an elliptic curve over a number field K, the conjecture of Birch–Swinnerton-Dyer predicts that $\operatorname{ord}_{s=1} L_{X,1}(s)$ equals $r = \operatorname{rank}_{\mathbb{Z}} X(K)$ and that

$$\lim_{s \to 1} \frac{L_{X,1}^{(r)}(s)}{r!} = \frac{V \operatorname{Reg}(X(K)) \, |\text{Ш}(X)|}{|X(K)_{\mathrm{tors}}|^2}$$

where V is a certain "easily" computable adelic volume, Reg is the regulator for the canonical height pairing, and $\text{Ш}(X)$ is the (conjecturally finite) Shafarevich–Tate group.

Analytic continuation of $L_{X,1}(s)$ is known when K is totally real or imaginary quadratic (Taylor et al). The first part of BSD is known when $K = \mathbb{Q}$ and $\operatorname{ord}_{s=1} L_{X,1}(s) \leq 1$ (Gross–Zagier, Kolyvagin); under some technical hypothesis, the second part is also known (many authors).

L-functions of elliptic curves

For X an elliptic curve over a number field K, the conjecture of Birch–Swinnerton-Dyer predicts that $\operatorname{ord}_{s=1} L_{X,1}(s)$ equals $r = \operatorname{rank}_{\mathbb{Z}} X(K)$ and that

$$\lim_{s \to 1} \frac{L^{(r)}_{X,1}(s)}{r!} = \frac{V \operatorname{Reg}(X(K)) \, |\text{Ш}(X)|}{|X(K)_{\mathrm{tors}}|^2}$$

where V is a certain "easily" computable adelic volume, Reg is the regulator for the canonical height pairing, and $\text{Ш}(X)$ is the (conjecturally finite) Shafarevich–Tate group.

Analytic continuation of $L_{X,1}(s)$ is known when K is totally real or imaginary quadratic (Taylor et al). The first part of BSD is known when $K = \mathbb{Q}$ and $\operatorname{ord}_{s=1} L_{X,1}(s) \leq 1$ (Gross–Zagier, Kolyvagin); under some technical hypothesis, the second part is also known (many authors).

Zeta functions of general curves

For X a curve of genus g over $\mathbb{F}_q$, its zeta function has the form

$$\frac{P_{X,1}(T)}{(1-T)(1-qT)}, \qquad P_{X,1}(T) = 1 + \cdots + q^g T^{2g}.$$

For "reasonable" q, g this is efficiently computable (K, Harvey, Tuitman, et al).

For J the Jacobian of X, note that $\#J(\mathbb{F}_q) = P_{X,1}(1)$. For small g, this is also relevant for cryptography (but again in the case of "unreasonable" q).

Via the Chabauty–Kim method, such computations have applications to finding rational points on curves over number field. For instance, the $\mathbb{Q}$-points of the split/nonsplit Cartan modular curve $X_{\mathrm{s}}(13) \cong X_{\mathrm{ns}}(13)$ were recently determined by Balakrishnan–Dogra–Müller–Tuitman–Vonk.

Zeta functions of general curves

For X a curve of genus g over $\mathbb{F}_q$, its zeta function has the form

$$\frac{P_{X,1}(T)}{(1-T)(1-qT)}, \qquad P_{X,1}(T) = 1 + \cdots + q^g T^{2g}.$$

For "reasonable" q, g this is efficiently computable (K, Harvey, Tuitman, et al).

For J the Jacobian of X, note that $\#J(\mathbb{F}_q) = P_{X,1}(1)$. For small g, this is also relevant for cryptography (but again in the case of "unreasonable" q).

Via the Chabauty–Kim method, such computations have applications to finding rational points on curves over number field. For instance, the $\mathbb{Q}$-points of the split/nonsplit Cartan modular curve $X_{\mathrm{s}}(13) \cong X_{\mathrm{ns}}(13)$ were recently determined by Balakrishnan–Dogra–Müller–Tuitman–Vonk.

Zeta functions of general curves

For X a curve of genus g over $\mathbb{F}_q$, its zeta function has the form

$$\frac{P_{X,1}(T)}{(1-T)(1-qT)}, \qquad P_{X,1}(T) = 1 + \cdots + q^g T^{2g}.$$

For "reasonable" q, g this is efficiently computable (K, Harvey, Tuitman, et al).

For J the Jacobian of X, note that $\#J(\mathbb{F}_q) = P_{X,1}(1)$. For small g, this is also relevant for cryptography (but again in the case of "unreasonable" q).

Via the Chabauty–Kim method, such computations have applications to finding rational points on curves over number field. For instance, the $\mathbb{Q}$-points of the split/nonsplit Cartan modular curve $X_{\mathrm{s}}(13) \cong X_{\mathrm{ns}}(13)$ were recently determined by Balakrishnan–Dogra–Müller–Tuitman–Vonk.

L-functions of general curves

For X a curve over a number field K, there is an analogue of BSD about which little is known. However, for hyperelliptic curves of genus ≤ 3 there is a *very* efficient method of Harvey–Sutherland for computing $L_{X,1}(s)$, which can be used to gather evidence.

Assuming analytic continuation of $L_{X,1}(s)$ (and some other L-functions), the (normalized) Euler factors of $L_{X,1}(s)$ converge in measure to a certain group-theoretic distribution. For $g = 1$ this takes one of three values depending on whether X has no CM, CM over K, or CM over a larger field (Sato–Tate conjecture, now known).

For $g = 2$ there are 52 possible distributions (Fité–K–Rotger–Sutherland). The problem for $g = 3$ is still mostly open, but twists of the Fermat and Klein quartics have been analyzed (Fité–Lorenzo Garcia–Sutherland).

L-functions of general curves

For X a curve over a number field K, there is an analogue of BSD about which little is known. However, for hyperelliptic curves of genus ≤ 3 there is a *very* efficient method of Harvey–Sutherland for computing $L_{X,1}(s)$, which can be used to gather evidence.

Assuming analytic continuation of $L_{X,1}(s)$ (and some other L-functions), the (normalized) Euler factors of $L_{X,1}(s)$ converge in measure to a certain group-theoretic distribution. For $g = 1$ this takes one of three values depending on whether X has no CM, CM over K, or CM over a larger field (Sato–Tate conjecture, now known).

For $g = 2$ there are 52 possible distributions (Fité–K–Rotger–Sutherland). The problem for $g = 3$ is still mostly open, but twists of the Fermat and Klein quartics have been analyzed (Fité–Lorenzo Garcia–Sutherland).

L-functions of general curves

For X a curve over a number field K, there is an analogue of BSD about which little is known. However, for hyperelliptic curves of genus ≤ 3 there is a *very* efficient method of Harvey–Sutherland for computing $L_{X,1}(s)$, which can be used to gather evidence.

Assuming analytic continuation of $L_{X,1}(s)$ (and some other L-functions), the (normalized) Euler factors of $L_{X,1}(s)$ converge in measure to a certain group-theoretic distribution. For $g = 1$ this takes one of three values depending on whether X has no CM, CM over K, or CM over a larger field (Sato–Tate conjecture, now known).

For $g = 2$ there are 52 possible distributions (Fité–K–Rotger–Sutherland). The problem for $g = 3$ is still mostly open, but twists of the Fermat and Klein quartics have been analyzed (Fité–Lorenzo Garcia–Sutherland).

Contents

Zeta functions of K3 surfaces

For X a K3 surface over $\mathbb{F}_q$, its zeta function has the form

$$\frac{1}{(1-T)(1-qT)(1-q^2T)q^{-1}Q_{X,2}(qT)}, \quad Q_{X,2}(T) = q + \cdots \pm qT^{21}.$$

The Picard number ρ_X (resp. the geometric Picard number $\tilde{\rho}_X$) counts roots of $(1-T)Q_{X,2}(T)$ equal to 1 (resp. to any root of unity). Note that $Q_{X,2}(T)$ is divisible by $1-T$ or $1+T$, so $\tilde{\rho}_X > 1$.

Computing ζ_X by brute force is only viable for small q; for instance, with no prior lower bound on ρ_X or $\tilde{\rho}_X$, already $q = 7$ is difficult. In many cases (e.g., for smooth quartics in $\mathbf{P}^3$) methods of p-adic cohomology can handle much larger q.

Zeta functions of K3 surfaces

For X a K3 surface over $\mathbb{F}_q$, its zeta function has the form

$$\frac{1}{(1-T)(1-qT)(1-q^2T)q^{-1}Q_{X,2}(qT)}, \quad Q_{X,2}(T) = q + \cdots \pm qT^{21}.$$

The Picard number ρ_X (resp. the geometric Picard number $\tilde{\rho}_X$) counts roots of $(1-T)Q_{X,2}(T)$ equal to 1 (resp. to any root of unity). Note that $Q_{X,2}(T)$ is divisible by $1-T$ or $1+T$, so $\tilde{\rho}_X > 1$.

Computing ζ_X by brute force is only viable for small q; for instance, with no prior lower bound on ρ_X or $\tilde{\rho}_X$, already $q = 7$ is difficult. In many cases (e.g., for smooth quartics in $\mathbf{P}^3$) methods of p-adic cohomology can handle much larger q.

The inverse problem for zeta functions

Given all known constraints on $Q_{X,2}(T)$, which such polynomials actually occur for some X? Constraints include restrictions on roots, the Artin–Tate formula (see next slide), and (for small q) the positivity conditions

$$\#X(\mathbb{F}_q) \geq 0, \qquad \#X(\mathbb{F}_{q^{mn}}) \geq \#X(\mathbb{F}_{q^n}) \quad (m, n \geq 1),$$

A result of Taelman–Ito (conditional for $p \leq 5$) gives partial information: if we consider only the transcendental part of $Q_{X,2}(T)$ (omitting cyclotomic factors), it can always be achieved *after* replacing $\mathbb{F}_q$ with an uncontrolled finite extension (which replaces each root of the polynomial with a corresponding power).

Is the uncontrolled finite extension really necessary? To shed light on this question, K–Sutherland computed all candidates for $Q_{X,2}(T)$ for $\mathbb{F}_2$, and (by brute force) $\zeta_X(T)$ for all smooth quartics in $\mathbf{P}^3$ over $\mathbb{F}_2$.

The inverse problem for zeta functions

Given all known constraints on $Q_{X,2}(T)$, which such polynomials actually occur for some X? Constraints include restrictions on roots, the Artin–Tate formula (see next slide), and (for small q) the positivity conditions

$$\#X(\mathbb{F}_q) \geq 0, \qquad \#X(\mathbb{F}_{q^{mn}}) \geq \#X(\mathbb{F}_{q^n}) \quad (m, n \geq 1),$$

A result of Taelman–Ito (conditional for $p \leq 5$) gives partial information: if we consider only the transcendental part of $Q_{X,2}(T)$ (omitting cyclotomic factors), it can always be achieved *after* replacing $\mathbb{F}_q$ with an uncontrolled finite extension (which replaces each root of the polynomial with a corresponding power).

Is the uncontrolled finite extension really necessary? To shed light on this question, K–Sutherland computed all candidates for $Q_{X,2}(T)$ for $\mathbb{F}_2$, and (by brute force) $\zeta_X(T)$ for all smooth quartics in $\mathbf{P}^3$ over $\mathbb{F}_2$.

The inverse problem for zeta functions

Given all known constraints on $Q_{X,2}(T)$, which such polynomials actually occur for some X? Constraints include restrictions on roots, the Artin–Tate formula (see next slide), and (for small q) the positivity conditions

$$\#X(\mathbb{F}_q) \geq 0, \qquad \#X(\mathbb{F}_{q^{mn}}) \geq \#X(\mathbb{F}_{q^n}) \quad (m, n \geq 1),$$

A result of Taelman–Ito (conditional for $p \leq 5$) gives partial information: if we consider only the transcendental part of $Q_{X,2}(T)$ (omitting cyclotomic factors), it can always be achieved *after* replacing $\mathbb{F}_q$ with an uncontrolled finite extension (which replaces each root of the polynomial with a corresponding power).

Is the uncontrolled finite extension really necessary? To shed light on this question, K–Sutherland computed all candidates for $Q_{X,2}(T)$ for $\mathbb{F}_2$, and (by brute force) $\zeta_X(T)$ for all smooth quartics in $\mathbf{P}^3$ over $\mathbb{F}_2$.

Artin–Tate formula

The Tate conjecture is known for K3 surfaces over finite fields (many authors). This makes the Artin–Tate formula unconditional:

$$\lim_{T \to 1} \frac{Q_{X,2}^{(r-1)}(T)}{(r-1)!} = |\Delta_X|\,|\mathrm{Br}(X)|$$

where Δ_X is the determinant of the Néron–Severi lattice and $\mathrm{Br}(X)$ is the Brauer group. The latter is finite and its order is a square; the possibilities for $Q_{X,2}(T)$ are restricted both by this condition, and by the corresponding condition over extensions of $\mathbb{F}_q$ (Elsenhans–Jahnel).

Over $\mathbb{F}_2$, there is a candidate for $Q_{X,2}(T)$ which would imply $\rho_X = 1$, $|\Delta_X| = 2 \times 463$. I have no idea how to construct such an X!

On the other hand, every candidate for $Q_{X,2}(T)$ over $\mathbb{F}_2$ which can *only* occur for smooth quartics in $\mathbf{P}^3$ over $\mathbb{F}_2$ does occur!

Artin–Tate formula

The Tate conjecture is known for K3 surfaces over finite fields (many authors). This makes the Artin–Tate formula unconditional:

$$\lim_{T \to 1} \frac{Q_{X,2}^{(r-1)}(T)}{(r-1)!} = |\Delta_X|\,|\mathrm{Br}(X)|$$

where Δ_X is the determinant of the Néron–Severi lattice and $\mathrm{Br}(X)$ is the Brauer group. The latter is finite and its order is a square; the possibilities for $Q_{X,2}(T)$ are restricted both by this condition, and by the corresponding condition over extensions of $\mathbb{F}_q$ (Elsenhans–Jahnel).

Over $\mathbb{F}_2$, there is a candidate for $Q_{X,2}(T)$ which would imply $\rho_X = 1$, $|\Delta_X| = 2 \times 463$. I have no idea how to construct such an X!

On the other hand, every candidate for $Q_{X,2}(T)$ over $\mathbb{F}_2$ which can *only* occur for smooth quartics in $\mathbf{P}^3$ over $\mathbb{F}_2$ does occur!

Artin–Tate formula

The Tate conjecture is known for K3 surfaces over finite fields (many authors). This makes the Artin–Tate formula unconditional:

$$\lim_{T \to 1} \frac{Q_{X,2}^{(r-1)}(T)}{(r-1)!} = |\Delta_X| \, |\mathrm{Br}(X)|$$

where Δ_X is the determinant of the Néron–Severi lattice and $\mathrm{Br}(X)$ is the Brauer group. The latter is finite and its order is a square; the possibilities for $Q_{X,2}(T)$ are restricted both by this condition, and by the corresponding condition over extensions of $\mathbb{F}_q$ (Elsenhans–Jahnel).

Over $\mathbb{F}_2$, there is a candidate for $Q_{X,2}(T)$ which would imply $\rho_X = 1$, $|\Delta_X| = 2 \times 463$. I have no idea how to construct such an X!

On the other hand, every candidate for $Q_{X,2}(T)$ over $\mathbb{F}_2$ which can *only* occur for smooth quartics in $\mathbf{P}^3$ over $\mathbb{F}_2$ does occur!

L-functions of K3 surfaces

For X a K3 surface over a number field K, conjecturally the leading term of $L_{X,2}(s)$ at $s = 2$ reflects the Picard number and some other arithmetic (by conjectures of Beilinson, Bloch, Deligne).

If X is the Kummer surface of an abelian surface A, this is related *not* to the BSD conjecture for A, but to a corresponding conjecture about the symmetric square L-function (Bloch–Kato). This still involves $|\text{Ш}(A)|$.

One can study Sato–Tate distributions; this includes the case of abelian surfaces via the Kummer construction, but otherwise little is known.

By comparing the L-functions of X and its base extensions, one gets information about the kernel of $\mathrm{Br}(X) \to \mathrm{Br}(X_{\overline{K}})$. This kernel can be used to study Brauer–Manin obstructions to rational points; it is also believed to obey a *uniform boundedness conjecture* analogous to torsion of elliptic curves. (See Várilly-Alvarado's AWS 2015 notes for more discussion.)

L-functions of K3 surfaces

For X a K3 surface over a number field K, conjecturally the leading term of $L_{X,2}(s)$ at $s = 2$ reflects the Picard number and some other arithmetic (by conjectures of Beilinson, Bloch, Deligne).

If X is the Kummer surface of an abelian surface A, this is related *not* to the BSD conjecture for A, but to a corresponding conjecture about the symmetric square L-function (Bloch–Kato). This still involves $|\text{Ш}(A)|$.

One can study Sato–Tate distributions; this includes the case of abelian surfaces via the Kummer construction, but otherwise little is known.

By comparing the L-functions of X and its base extensions, one gets information about the kernel of $\mathrm{Br}(X) \to \mathrm{Br}(X_{\overline{K}})$. This kernel can be used to study Brauer–Manin obstructions to rational points; it is also believed to obey a *uniform boundedness conjecture* analogous to torsion of elliptic curves. (See Várilly-Alvarado's AWS 2015 notes for more discussion.)

L-functions of K3 surfaces

For X a K3 surface over a number field K, conjecturally the leading term of $L_{X,2}(s)$ at $s = 2$ reflects the Picard number and some other arithmetic (by conjectures of Beilinson, Bloch, Deligne).

If X is the Kummer surface of an abelian surface A, this is related *not* to the BSD conjecture for A, but to a corresponding conjecture about the symmetric square L-function (Bloch–Kato). This still involves $|\text{Ш}(A)|$.

One can study Sato–Tate distributions; this includes the case of abelian surfaces via the Kummer construction, but otherwise little is known.

By comparing the L-functions of X and its base extensions, one gets information about the kernel of $\mathrm{Br}(X) \to \mathrm{Br}(X_{\overline{K}})$. This kernel can be used to study Brauer–Manin obstructions to rational points; it is also believed to obey a *uniform boundedness conjecture* analogous to torsion of elliptic curves. (See Várilly-Alvarado's AWS 2015 notes for more discussion.)

L-functions of K3 surfaces

For X a K3 surface over a number field K, conjecturally the leading term of $L_{X,2}(s)$ at $s = 2$ reflects the Picard number and some other arithmetic (by conjectures of Beilinson, Bloch, Deligne).

If X is the Kummer surface of an abelian surface A, this is related *not* to the BSD conjecture for A, but to a corresponding conjecture about the symmetric square L-function (Bloch–Kato). This still involves $|\text{Ш}(A)|$.

One can study Sato–Tate distributions; this includes the case of abelian surfaces via the Kummer construction, but otherwise little is known.

By comparing the L-functions of X and its base extensions, one gets information about the kernel of $\mathrm{Br}(X) \to \mathrm{Br}(X_{\overline{K}})$. This kernel can be used to study Brauer–Manin obstructions to rational points; it is also believed to obey a *uniform boundedness conjecture* analogous to torsion of elliptic curves. (See Várilly-Alvarado's AWS 2015 notes for more discussion.)

Jumping of Picard numbers

The Picard number (resp. geometric Picard number) does not decrease under specialization from X to $X_{\mathfrak{p}}$, but may increase. If $\tilde{\rho}_X$ is odd then it *must* increase!

Nonetheless, by combining information from *two* primes of good reduction, one can often use zeta function information to pin down $\tilde{\rho}_X$. E.g., van Luijk gave an explicit example where $\tilde{\rho}_X = 1$ is established using brute force computations modulo 2 and 3.

For fixed X, one can study frequency of Picard number jumping; some experiments have been done (Costa–Tschinkel). For $\rho_X \gg 0$, this is related to supersingular reductions of abelian varieties, for which some infinitude results are conjectured (Lang–Trotter) and/or known (Elkies, Charles).

A certain infinitude statement for Picard number jumping would imply that every K3 surface over $\mathbb{C}$ contains infinitely many rational curves (Bogomolov et al, Li–Liedtke).

Jumping of Picard numbers

The Picard number (resp. geometric Picard number) does not decrease under specialization from X to $X_{\mathfrak{p}}$, but may increase. If $\tilde{\rho}_X$ is odd then it *must* increase!

Nonetheless, by combining information from *two* primes of good reduction, one can often use zeta function information to pin down $\tilde{\rho}_X$. E.g., van Luijk gave an explicit example where $\tilde{\rho}_X = 1$ is established using brute force computations modulo 2 and 3.

For fixed X, one can study frequency of Picard number jumping; some experiments have been done (Costa–Tschinkel). For $\rho_X \gg 0$, this is related to supersingular reductions of abelian varieties, for which some infinitude results are conjectured (Lang–Trotter) and/or known (Elkies, Charles).

A certain infinitude statement for Picard number jumping would imply that every K3 surface over $\mathbb{C}$ contains infinitely many rational curves (Bogomolov et al, Li–Liedtke).

Jumping of Picard numbers

The Picard number (resp. geometric Picard number) does not decrease under specialization from X to $X_{\mathfrak{p}}$, but may increase. If $\tilde{\rho}_X$ is odd then it *must* increase!

Nonetheless, by combining information from *two* primes of good reduction, one can often use zeta function information to pin down $\tilde{\rho}_X$. E.g., van Luijk gave an explicit example where $\tilde{\rho}_X = 1$ is established using brute force computations modulo 2 and 3.

For fixed X, one can study frequency of Picard number jumping; some experiments have been done (Costa–Tschinkel). For $\rho_X \gg 0$, this is related to supersingular reductions of abelian varieties, for which some infinitude results are conjectured (Lang–Trotter) and/or known (Elkies, Charles).

A certain infinitude statement for Picard number jumping would imply that every K3 surface over $\mathbb{C}$ contains infinitely many rational curves (Bogomolov et al, Li–Liedtke).

Jumping of Picard numbers

The Picard number (resp. geometric Picard number) does not decrease under specialization from X to $X_{\mathfrak{p}}$, but may increase. If $\tilde{\rho}_X$ is odd then it *must* increase!

Nonetheless, by combining information from *two* primes of good reduction, one can often use zeta function information to pin down $\tilde{\rho}_X$. E.g., van Luijk gave an explicit example where $\tilde{\rho}_X = 1$ is established using brute force computations modulo 2 and 3.

For fixed X, one can study frequency of Picard number jumping; some experiments have been done (Costa–Tschinkel). For $\rho_X \gg 0$, this is related to supersingular reductions of abelian varieties, for which some infinitude results are conjectured (Lang–Trotter) and/or known (Elkies, Charles).

A certain infinitude statement for Picard number jumping would imply that every K3 surface over $\mathbb{C}$ contains infinitely many rational curves (Bogomolov et al, Li–Liedtke).

Contents

Zeta functions of CY threefolds

For X a CY threefold over $\mathbb{F}_q$, its zeta function has the form

$$\frac{P_{X,3}(T)}{(1-T)(1-qT)(1-q^2T)(1-q^3T)}, \qquad P_{X,3}(T) \in 1 + T\mathbb{Z}[T].$$

Note that there is no *a priori* bound on $\deg(P_{X,3})$.

In many cases of interest, $P_{X,3}(T)$ will have a *known factor* of the form $Q_{Y,1}(qT)$ where Y is a curve or abelian variety. For example, if X is a smooth quintic in $\mathbf{P}^4$ then $\deg(P_{X,3}) = 104$, but if X belongs to the Dwork pencil

$$x_0^5 + \cdots + x_4^5 + \lambda x_0 \cdots x_4 = 0$$

then $P_{X,3}(T)$ has a known factor of degree 100.

Known factors can usually be explained by geometric considerations, e.g., by comparing toric embeddings.

Zeta functions of CY threefolds

For X a CY threefold over $\mathbb{F}_q$, its zeta function has the form

$$\frac{P_{X,3}(T)}{(1-T)(1-qT)(1-q^2T)(1-q^3T)}, \qquad P_{X,3}(T) \in 1 + T\mathbb{Z}[T].$$

Note that there is no *a priori* bound on $\deg(P_{X,3})$.

In many cases of interest, $P_{X,3}(T)$ will have a *known factor* of the form $Q_{Y,1}(qT)$ where Y is a curve or abelian variety. For example, if X is a smooth quintic in $\mathbf{P}^4$ then $\deg(P_{X,3}) = 104$, but if X belongs to the Dwork pencil

$$x_0^5 + \cdots + x_4^5 + \lambda x_0 \cdots x_4 = 0$$

then $P_{X,3}(T)$ has a known factor of degree 100.

Known factors can usually be explained by geometric considerations, e.g., by comparing toric embeddings.

Zeta functions of CY threefolds

For X a CY threefold over $\mathbb{F}_q$, its zeta function has the form

$$\frac{P_{X,3}(T)}{(1-T)(1-qT)(1-q^2T)(1-q^3T)}, \qquad P_{X,3}(T) \in 1 + T\mathbb{Z}[T].$$

Note that there is no *a priori* bound on $\deg(P_{X,3})$.

In many cases of interest, $P_{X,3}(T)$ will have a *known factor* of the form $Q_{Y,1}(qT)$ where Y is a curve or abelian variety. For example, if X is a smooth quintic in $\mathbf{P}^4$ then $\deg(P_{X,3}) = 104$, but if X belongs to the Dwork pencil

$$x_0^5 + \cdots + x_4^5 + \lambda x_0 \cdots x_4 = 0$$

then $P_{X,3}(T)$ has a known factor of degree 100.

Known factors can usually be explained by geometric considerations, e.g., by comparing toric embeddings.

Comparison of Galois representations (e.g., modularity)

In some cases, the Galois representation associated to two different motives can be identified up to semisimplification, implying an equality of L-functions. This is a *finite*[1] *computation*: once one has enough matching local factors, an argument of Faltings–Serre kicks in.

This can be used to establish comparisons of L-functions between various varieties and modular forms (i.e., *modularity*). For CY threefolds, this has been done by van Geemen–Nygaard, Dieulefait–Manoharmayum, Verrill, Ahlgren–Ono, Saito–Yui, Livné–Yui, Meyer, Lee, Hulek-Verrill, Schütt, Cynk–Hulek, Gouvêa–Yui, Dieulefait–Pacetti–Schütt, etc.

This is also feasible in higher dimensions; see Cynk–Hulek.

[1] This statement does not include a runtime bound. A weak bound can be obtained using analytic number theory, but in practice very few local factors are needed.

Comparison of Galois representations (e.g., modularity)

In some cases, the Galois representation associated to two different motives can be identified up to semisimplification, implying an equality of L-functions. This is a *finite*[1] *computation*: once one has enough matching local factors, an argument of Faltings–Serre kicks in.

This can be used to establish comparisons of L-functions between various varieties and modular forms (i.e., *modularity*). For CY threefolds, this has been done by van Geemen–Nygaard, Dieulefait–Manoharmayum, Verrill, Ahlgren–Ono, Saito–Yui, Livné–Yui, Meyer, Lee, Hulek-Verrill, Schütt, Cynk–Hulek, Gouvêa–Yui, Dieulefait–Pacetti–Schütt, etc.

This is also feasible in higher dimensions; see Cynk–Hulek.

[1] This statement does not include a runtime bound. A weak bound can be obtained using analytic number theory, but in practice very few local factors are needed.

Arithmetic aspects of mirror symmetry

In certain cases, pairs of CY threefolds occurring in mirror families have related factors in their L-functions. This was observed in the Dwork pencil and its mirror by Candelas–de la Ossa–Rodriguez Villegas and more generally by Gährs, Miyatami, and Doran–Kelly–Salerno–Sperber–Voight–Whitcher. (This is not exclusive to dimension 3; some of the examples are K3 surfaces.)

Is there something more general going on here? Would experimental data about L-functions of CY (or other) varieties help identify the right framework?

Arithmetic aspects of mirror symmetry

In certain cases, pairs of CY threefolds occurring in mirror families have related factors in their *L*-functions. This was observed in the Dwork pencil and its mirror by Candelas–de la Ossa–Rodriguez Villegas and more generally by Gährs, Miyatami, and Doran–Kelly–Salerno–Sperber–Voight–Whitcher. (This is not exclusive to dimension 3; some of the examples are K3 surfaces.)

Is there something more general going on here? Would experimental data about *L*-functions of CY (or other) varieties help identify the right framework?

Contents

Hypergeometric motives

A family of motives indexed by a rational parameter t is *hypergeometric* if its associated Picard–Fuchs equation is hypergeometric; in particular, it has singularities only at $t = 0, 1, \infty$. There are *many* Hodge vectors that can occur, which touch many interesting cases.

One can compute zeta and L-functions of hypergeometric motives efficiently using a p-adic version of the finite hypergeometric trace formula (Greene, Katz, Cohen–Rodriguez Villegas–Watkins) or by computing the Frobenius structure on the hypergeometric equation (Dwork, K).

This potentially gives divers(e) cases where L-functions can be computed even when p-adic cohomology cannot be computed directly (e.g., most cases of dimension > 4). I would expect similar considerations to apply to GKZ-hypergeometric families (indexed by multiple parameters), which would provide even more examples.

Hypergeometric motives

A family of motives indexed by a rational parameter t is *hypergeometric* if its associated Picard–Fuchs equation is hypergeometric; in particular, it has singularities only at $t = 0, 1, \infty$. There are *many* Hodge vectors that can occur, which touch many interesting cases.

One can compute zeta and L-functions of hypergeometric motives efficiently using a p-adic version of the finite hypergeometric trace formula (Greene, Katz, Cohen–Rodriguez Villegas–Watkins) or by computing the Frobenius structure on the hypergeometric equation (Dwork, K).

This potentially gives divers(e) cases where L-functions can be computed even when p-adic cohomology cannot be computed directly (e.g., most cases of dimension > 4). I would expect similar considerations to apply to GKZ-hypergeometric families (indexed by multiple parameters), which would provide even more examples.

Hypergeometric motives

A family of motives indexed by a rational parameter t is *hypergeometric* if its associated Picard–Fuchs equation is hypergeometric; in particular, it has singularities only at $t = 0, 1, \infty$. There are *many* Hodge vectors that can occur, which touch many interesting cases.

One can compute zeta and L-functions of hypergeometric motives efficiently using a p-adic version of the finite hypergeometric trace formula (Greene, Katz, Cohen–Rodriguez Villegas–Watkins) or by computing the Frobenius structure on the hypergeometric equation (Dwork, K).

This potentially gives divers(e) cases where L-functions can be computed even when p-adic cohomology cannot be computed directly (e.g., most cases of dimension > 4). I would expect similar considerations to apply to GKZ-hypergeometric families (indexed by multiple parameters), which would provide even more examples.