Arithmetic L-functions and their Sato-Tate distributions

Andrew V. Sutherland

Massachusetts Institute of Technology

VaNTAGe Seminar
April 28, 2020

Joint work with Andrew Booker, Edgar Costa, Francesc Fité, David Harvey, Kiran Kedlaya, Maike Massierer, David Platt, Victor Rotger, Jeroen Sijsling, John Voight, and Dan Yasaki.

A simple thing we don't know

Let $X/\mathbb{Q}$ be a nice (smooth, projective, geometrically integral) curve of genus g. For each good prime p the trace of Frobenius

$$a_p := p + 1 - \#X(\mathbb{F}_p)$$

satisfies $|a_p| \le 2g\sqrt{p}$, by the Weil bounds, and $x_p := a_p/\sqrt{p} \in [-2g, 2g]$. In particular $g \ge |x_p|/2$ for all primes p.

[Katz12]: Is the lower bound on g ever sharp?

For $g = 1$ this follows from the Sato–Tate conjecture (now a theorem). The question remains open for all $g > 1$.

For $g = 2$ we know $|x_p| \ge 2/3$ for a positive density of p [Taylor18]. For $g > 2$ we know essentially nothing...

The L-function of a curve

Let $X/\mathbb{Q}$ be a nice curve of genus g. The L-function of X is given by

$$L(X,s) = L(\mathrm{Jac}(X),s) := \sum_{n\geq 1} a_n n^{-s} := \prod_p L_p(p^{-s})^{-1}.$$

For primes p of good reduction for X we have the zeta function

$$Z(X_p;s) := \exp\left(\sum_{r\geq 1} \#X(\mathbb{F}_{p^r})\frac{T^r}{r}\right) = \frac{L_p(T)}{(1-T)(1-pT)},$$

and the L-polynomial $L_p \in \mathbb{Z}[T]$ in the numerator satisfies

$$L_p(T) = T^{2g}\chi_p(1/T) = 1 - a_pT + \cdots + p^gT^{2g},$$

where $\chi_p(T)$ is the charpoly of the Frobenius endomorphism of $\mathrm{Jac}(X_p)$.

The Selberg class with polynomial Euler factors

The Selberg class S^{poly} consists of Dirichlet series $L(s) = \sum_{n \geq 1} a_n n^{-s}$:

1. $L(s)$ has an analytic continuation that is holomorphic at $s \neq 1$;
2. For some $\gamma(s) = Q^s \prod_{i=1}^r \Gamma(\lambda_i s + \mu_i)$ and ε, the completed L-function $\Lambda(s) := \gamma(s) L(s)$ satisfies the functional equation

$$\Lambda(s) = \varepsilon \overline{\Lambda(1 - \bar{s})},$$

   where $Q > 0$, $\lambda_i > 0$, $\mathrm{Re}(\mu_i) \geq 0$, $|\varepsilon| = 1$. Define $\deg L := 2 \sum_i^r \lambda_i$.
3. $a_1 = 1$ and $a_n = O(n^{\epsilon})$ for all $\epsilon > 0$; the Ramanujan bound.
4. $L(s) = \prod_p L_p(p^{-s})^{-1}$ for some $L_p \in \mathbb{Z}[T]$ with $\deg L_p \leq \deg L$; in other words $L(s)$ has an Euler product.

The Dirichlet series $L_{\mathrm{an}}(s, X) := L(X, s + \frac{1}{2})$ satisfies (3) and (4), and conjecturally lies in S^{poly}; for $g = 1$ this is known via modularity.

Strong multiplicity one

Theorem (Kaczorowski-Perelli 2001)

If $A(s) = \sum_{n\geq 1} a_n n^{-s}$ *and* $B(s) = \sum_{n\geq 1} b_n n^{-s}$ *lie in* S^{poly} *and* $a_p = b_p$ *for all but finitely many primes* p*, then* $A(s) = B(s)$*.*

Corollary

If $L_{\mathrm{an}}(s, X)$ *lies in* S^{poly} *then it is determined by (any choice of) all but finitely many coefficients* a_p*.*

Henceforth we assume that $L_{\mathrm{an}}(s, X) \in S^{\mathrm{poly}}$.

Let $\Gamma_{\mathbb{C}}(s) = 2(2\pi)^s\Gamma(s)$ and define $\Lambda(X, s) := \Gamma_{\mathbb{C}}(s)^g L(X, s)$. Then

$$\Lambda(X, s) = \varepsilon N^{1-s}\Lambda(X, 2 - s).$$

where the root number $\varepsilon = \pm 1$ and the analytic conductor $N \in \mathbb{Z}_{\geq 1}$ are determined by the a_p (one can take these as definitions).

Testing the functional equation

Let $G(x)$ be the inverse Mellin transform of $\Gamma_{\mathbb{C}}(s)^g = \int_0^\infty G(x)x^{s-1}dx$, and define

$$S(x) := \frac{1}{x}\sum a_n G(n/x),$$

so that $\Lambda(X,s) = \int_0^\infty S(x)x^{-s}dx$, and for all $x > 0$ we have

$$S(x) = \varepsilon S(N/x).$$

The function $G(x)$ decays rapidly, and for sufficiently large c_0 we have

$$S(x) \approx S_0(x) := \frac{1}{x}\sum_{n \le c_0 x} a_n G(n/x),$$

with an explicit bound on the error $|S(x) - S_0(x)|$.

Effective strong multiplicity one

Fix a finite set of small primes $\mathcal{S}$ (e.g. $\mathcal{S} = \{2\}$) and an integer M that we know is a multiple of the conductor N (e.g. $M = \Delta(X)$).

There is a finite set of possibilities for $\varepsilon = \pm 1$, $N|M$, and the Euler factors $L_p \in \mathbb{Z}[T]$ for $p \in \mathcal{S}$ (the coefficients of $L_p(T)$ are bounded).

Suppose we can compute a_n for $n \le c_1\sqrt{M}$ whenever $p \nmid n$ for $p \in \mathcal{S}$.

We now compute $\delta(x) := |S_0(x) - \varepsilon S_0(N/x)|$ with $x = c_1\sqrt{N})$ for every possible choice of ε, N, and $L_p(T)$ for $p \in \mathcal{S}$. If all but one choice makes $\delta(x)$ larger than our explicit error bound, we know the correct choice.

For a suitable choice of c_1 this is guaranteed to happen.[1] One can explicitly determine a set of $O(N^\epsilon)$ candidate values of c_1, one of which is guaranteed to work; in practice the first one usually works.

[1] Subject to our assumptions; if it does not happen then we have found an explicit counterexample to the Hasse-Weil conjecture.

Conductor bounds

The formula of Brumer and Kramer gives explicit bounds on the p-adic valuation of the algebraic conductor N of $\mathrm{Jac}(X)$:

$$v_p(N) \leq 2g + pd + (p-1)\lambda_p(d),$$

where $d = \lfloor \frac{2g}{p-1} \rfloor$ and $\lambda_p(d) = \sum i d_i p^i$, with $d = \sum d_i p^i$ with $0 \leq d_i < p$.

g	$p = 2$	$p = 3$	$p = 5$	$p = 7$	$p > 7$
1	8	5	2	2	2
2	20	10	9	4	4
3	28	21	11	13	6

For $g \leq 2$ these bounds are tight (see `www.lmfdb.org` for examples).

For hyperelliptic curves N divides $\Delta(X)$; for a suitable definition of $\Delta(X)$ one expects this to hold in general.

Arithmetic L-functions

A more precise description of the properties S^{poly} is intended to capture is given by the axioms for analytic L-functions; see [FPRS 2019].

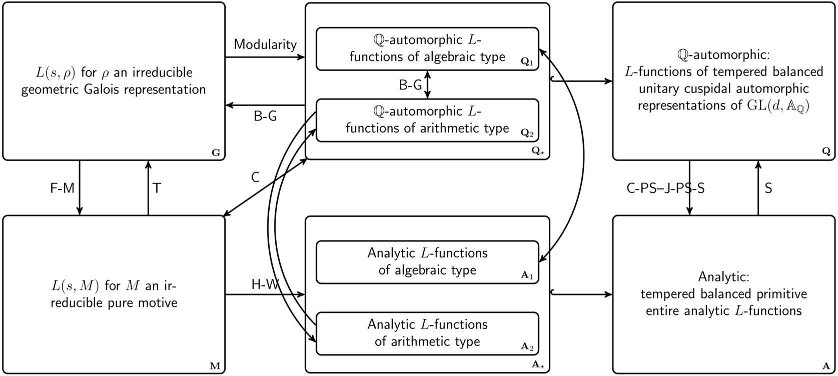
Among these one can distinguish those of arithmetic type.
These are analytic L-functions $L(s) = \sum a_n n^{-s}$ for which there exists $w_{ar} \in \mathbb{Z}$ and a number field K such that $a_n n^{w_{ar}/2} \in \mathcal{O}_K$ for all n.

The smallest F and w_{ar} are the field of coefficients and arithmetic weight of $L(s)$. For curves over number fields we always have $F = \mathbb{Q}$ (whether X is defined over $\mathbb{Q}$ or not), so $L(X)$ is a rational L-function, and the arithmetic weight $w_{ar} = 1$ agrees with the motivic weight.

More generally, one expects that the L-function of any pure motive of weight w should have $w_{ar} = w$, and moreover, that every arithmetic L-function should come from a motive.

Example: $L(s) = 1 + 16 \cdot 19^{-s} - 10 \cdot 25^{-s} + 16 \cdot 43^{-s} + 2 \cdot 49^{-s} - \cdots$

Conjectured relationships between sets of L-functions



F–M	Fontaine–Mazur	T	Taylor
B–G	Buzzard–Gee	C	Clozel
C–PS	Codgell–Piatetski-Shapiro	H–W	Hasse–Weil
J-PS-S	Jacquet–Piatetski-Shapiro–Shalika	S	Selberg

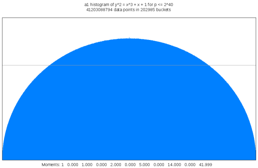
*Figure taken from page 21 of *Analytic L-functions: Definitions theorems and connections*, by D.W. Farmer, A. Pitale, N.C. Ryan, and R. Schmidt, arXiV:1711.10375.

Sato–tate distributions of rational L-functions

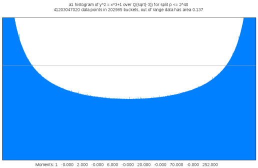
Given an arithmetic L-function $L(s)$ we can study the distribution of its (analytically normalized) coefficients, or equivalently, the distribution of its normalized Euler factors.

If we assume $L(s)$ is motivic (we do), we can associate a Sato-Tate group to $L(s)$; take the Sato-Tate group of a corresponding motive.

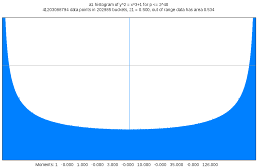
For rational L-functions of degree 2 and weight 1 there are three possible Sato-Tate distributions:



$\mathrm{SU}(2)$



$\mathrm{U}(1)$

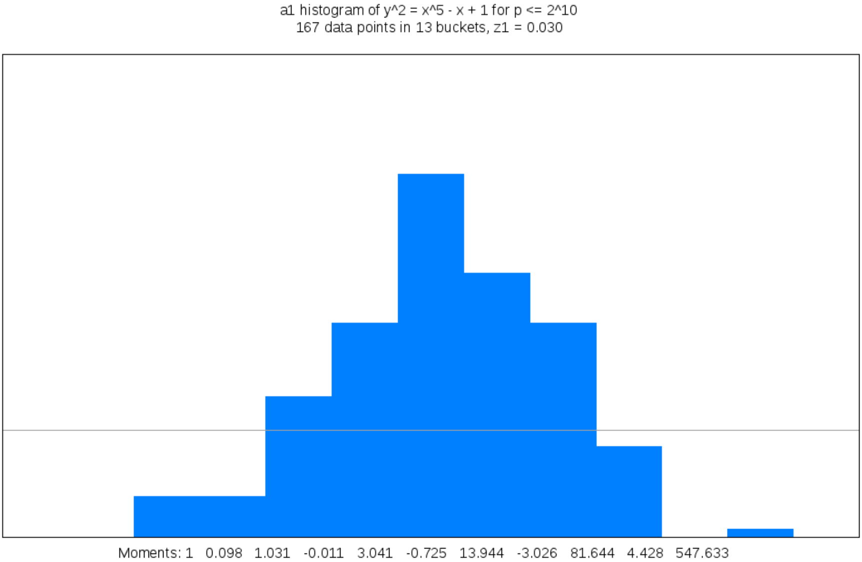


$N(\mathrm{U}(1))$

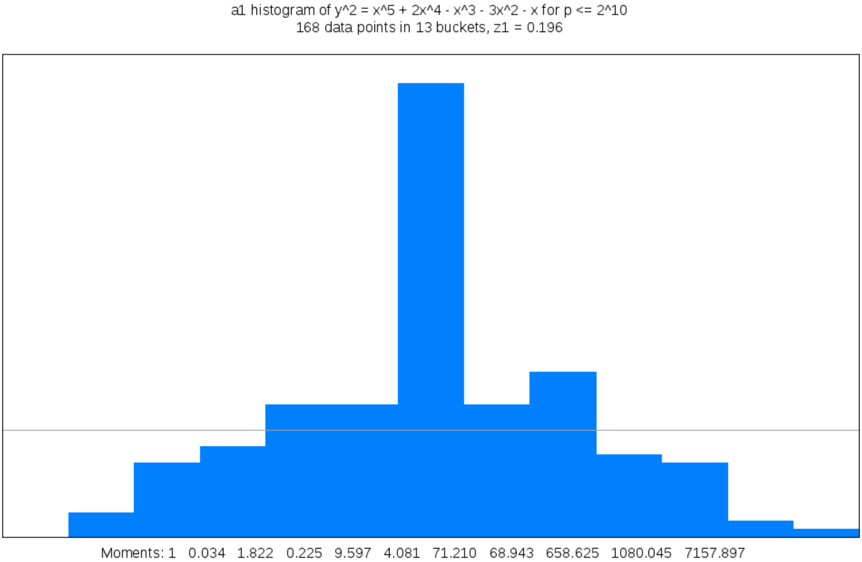
Some rational L-functions of weight w and degree d

w	d	L-function
0	1	$L(\chi,s)$ for a Dirichlet character with $\chi^2=1$, including $\zeta(s)$
	2	$L(f,s)$ for weight 1 CMFs with $\mathbb{Q}(f)=\mathbb{Q}$
	n	$\zeta_K(s)$ with $[K:\mathbb{Q}]=n$
		$L(\rho,s)$ for Artin representation with $\dim\rho=n$ and $\mathrm{tr}(\rho)$ rational
1	2	$L(f,s)$ for weight 2 CMFs with $\mathbb{Q}(f)=\mathbb{Q}$
		$L(E,s)$ for elliptic curves $E/\mathbb{Q}$
	4	$L(f,s)$ for parallel weight 2 HMFs with $\mathbb{Q}(f)=\mathbb{Q}$
		$L(E,s)$ for elliptic curves E/K with $[K:\mathbb{Q}]=2$
		$L(X,s)$ for genus 2 curves $X/\mathbb{Q}$
2	2	$L(f,s)$ for weight 3 CMFs with $\mathbb{Q}(f)=\mathbb{Q}$
	3	$L(\mathrm{Sym}^2(E),s)$ for elliptic curves $E/\mathbb{Q}$
		$L(H,s)$ for hypergeometric motives H with Hodge vector $[1,1,1]$
3	2	$L(f,s)$ for weight 4 CMFs with $\mathbb{Q}(f)=\mathbb{Q}$
	4	$L(\mathrm{Sym}^3(E),s)$ for elliptic curves $E/\mathbb{Q}$
		$L(H,s)$ for hypergeometric motives H with Hodge vector $[1,1,1,1]$

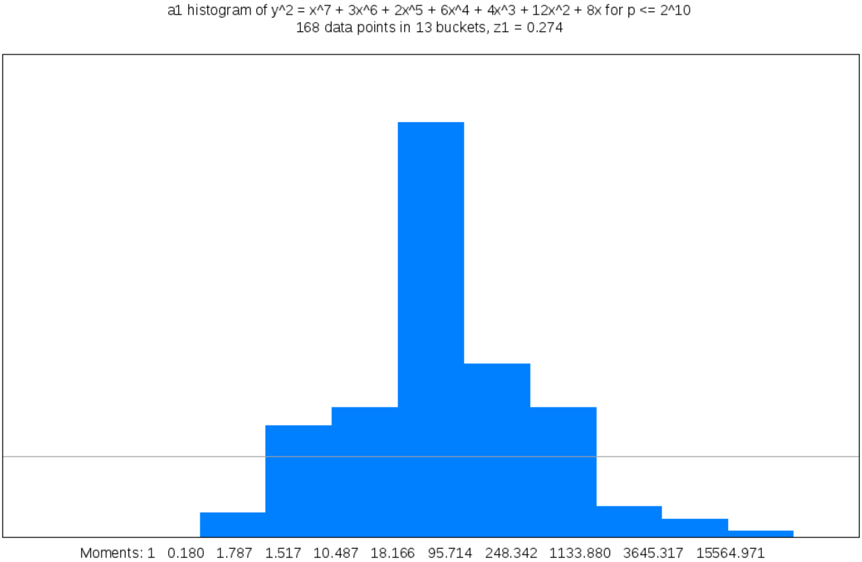
Sato-Tate group $G\subseteq O(d)$ if w is even, $G\subseteq \mathrm{USp}(d)$ if w is odd; $wd\equiv 0 \bmod 2$.



click histogram to animate (requires adobe reader)

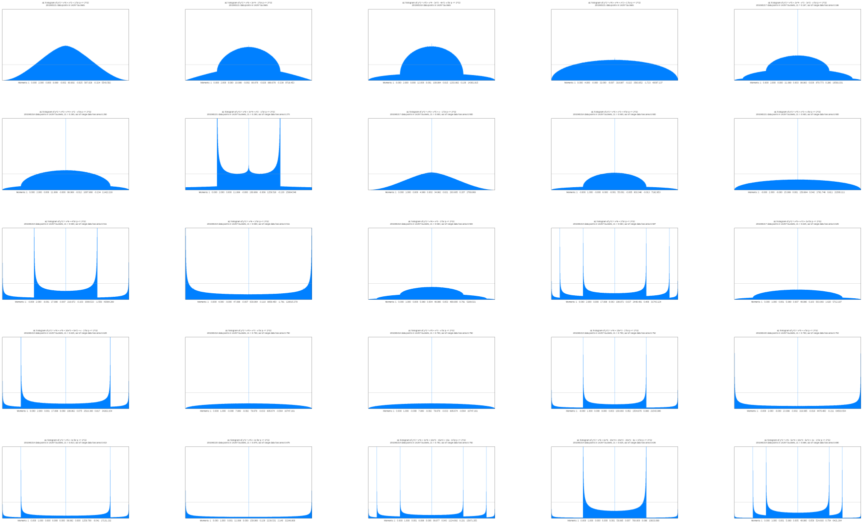


click histogram to animate (requires adobe reader)

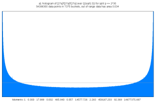


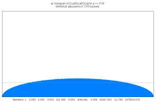
click histogram to animate (requires adobe reader)

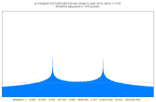
Exceptional distributions for abelian surfaces over $\mathbb{Q}$

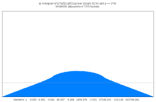


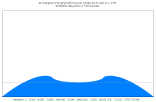
Connected Sato-Tate groups of abelian threefolds:

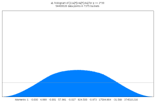

$\mathrm{U}(1)_3$

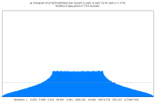

$\mathrm{SU}(2)_3$

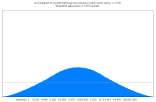

$\mathrm{U}(1) \times \mathrm{U}(1)_2$

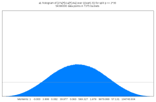

$\mathrm{U}(1) \times \mathrm{SU}(2)_2$

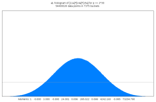

$\mathrm{SU}(2) \times \mathrm{U}(1)_2$

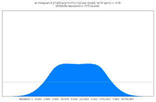

$\mathrm{SU}(2) \times \mathrm{SU}(2)_2$

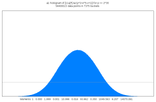

$\mathrm{U}(1) \times \mathrm{U}(1) \times \mathrm{U}(1)$

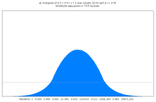

$\mathrm{U}(1) \times \mathrm{U}(1) \times \mathrm{SU}(2)$

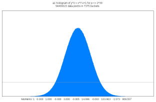

$\mathrm{U}(1) \times \mathrm{SU}(2) \times \mathrm{U}(1)$


$\mathrm{SU}(2) \times \mathrm{SU}(2) \times \mathrm{SU}(2)$


$\mathrm{U}(1) \times \mathrm{USp}(4)$


$\mathrm{SU}(2) \times \mathrm{USp}(4)$


$\mathrm{U}(3)$


$\mathrm{USp}(6)$

Algorithms to compute L-functions

Given $X/\mathbb{Q}$ of genus g, we want to compute $L_p(T)$ for all good $p \le B$.

	complexity per prime (ignoring factors of $O(\log\log p)$)		
algorithm	$g=1$	$g=2$	$g=3$
point enumeration	$p\log p$	$p^2\log p$	$p^3(\log p)^2$
group computation	$p^{1/4}\log p$	$p^{3/4}\log p$	$p(\log p)^2$
p-adic cohomology	$p^{1/2}(\log p)^2$	$p^{1/2}(\log p)^2$	$p^{1/2}(\log p)^2$
CRT (Schoof-Pila)	$(\log p)^5$	$(\log p)^8$	$(\log p)^{14*}$
average poly-time	$(\log p)^4$	$(\log p)^4$	$(\log p)^4$

For $L(X,s) = \sum a_n n^{-s}$, we only need a_{p^2} for $p^2 \le B$, and a_{p^3} for $p^3 \le B$. We can compute all of these in $O(B)$ time using any $O(p)$ method.

Bottom line: It all comes down to computing a_p's.

*For hyperelliptic curves [Abelard18].

Arithmetic schemes

Let X be a scheme of finite type over $\operatorname{Spec}\mathbb{Z}$, an arithmetic scheme.
The Hasse–Weil zeta function (or arithmetic zeta function) of X is

$$\zeta_X(s) := \prod_{x\in X}(1-N(x)^{-s})^{-1} = \prod \zeta_{X_p}(s) = \prod Z_{X_p}(p^{-s}),$$

where the product is over closed points x, the norm $N(x) := \#\kappa(x)$ is the cardinality of the residue field $\kappa(x)$, and $X_p := X \times_{\operatorname{Spec}\mathbb{Z}} \operatorname{Spec}(\mathbb{Z}/p\mathbb{Z})$ is the reduction of X modulo p. The local zeta function $Z_{X_p}(T)$ is

$$Z_{X_p}(T) := \exp\left(\sum_{r\geq 1}^{\infty} \#X_p(\mathbb{F}_{p^r})\frac{T^r}{r}\right) \in 1 + T\mathbb{Z}[[T]],$$

which is known to lie in $\mathbb{Q}(T)$ (by work of Dwork and Grothendieck).

For $X_p(\mathbb{F}_{p^r}) := \operatorname{Hom}_{\mathbb{F}_p}(\operatorname{Spec}(\mathbb{F}_{p^r}), X)$ we then have

$$\#X_p(\mathbb{F}_{p^r}) = \sum_{e|r} e\#\{x \in X : \kappa(x) \simeq \mathbb{F}_{p^e}\}.$$

Arithmetic zeta functions and L-functions

Let $X/\mathbb{Q}$ be a nice curve with integral model $\mathcal{X}$, which we can view as an arithmetic scheme. What is the relationship between $L_X(s)$ and $\zeta_{\mathcal{X}}(s)$?

We have $Z_{X_p}(T) = Z_{\mathcal{X}_p}(T)$ at all good primes p of $\mathcal{X}$, in which case the L-polynomials $L_{X_p}(T)$ and $L_{\mathcal{X}_p}(T)$ in their numerators will agree.

From our multiplicity one perspective, this is all we need; the local zeta functions $Z_{\mathcal{X}_p}(T)$ at good primes determine $L_X(s)$ (for any choice of $\mathcal{X}$).

In general L-polynomials $L_{X_p}(T)$ in $L_X(s) = \prod_p L_{X_p}(p^{-s})$ may differ from the numerator of the local zeta functions $Z_{\mathcal{X}_p}(T)$ at bad primes.

For example, if X is 49a1 and $\mathcal{X}$ is the arithmetic scheme given by its minimal Weierstrass equation $y^2z + xyz = x^3 - x^2z - 2xz^2 - z^3$, then

$$L_{\mathcal{X}_7}(T) = -7T^2 + 1 \neq 1 = L_{X_7}(T).$$

On the other hand, when X is 11a1 we actually have $L_X(s) = \zeta_{\mathcal{X}}(s)$.

Harvey's results for arithmetic schemes

Theorem (Harvey 2015)

Let X be an arithmetic scheme.

1. *There is a deterministic algorithm that, given a prime p, outputs $Z_{X_p}(T)$ in $p(\log p)^{1+o(1)}$ time using $O(\log p)$ space.*
2. *There is a deterministic algorithm that, given a prime p, outputs $Z_{X_p}(T)$ in $\sqrt{p}\,(\log p)^{2+o(1)}$ time using $O(\sqrt{p}\log p)$ space.*
3. *There is a deterministic algorithm that, given an integer N, outputs $Z_{X_p}(T)$ for $p \le N$ in $N(\log N)^{3+o(1)}$ time using $O(N\log^2 N)$ space.*

In these complexity bounds, X is fixed, only p or N are part of the input (the arithmetic scheme X is effectively "hardwired" into the algorithm).

If one constrains X and fixes its representation, the dependence on X can be made explicit; for plane curves one obtains $g^{14}N(\log N)^{3+o(1)}$.

These are not just existence statements; Harvey gives explicit algorithms.

Practical average polynomial-time algorithms

To date all practical implementations compute $L_p(T) \bmod p$ by computing Hasse–Witt (Cartier–Manin) matrices $A_p \in \mathbb{F}_p^{g\times g}$ for $p \le B$.

We have $a_p \equiv \operatorname{tr}(A_p) \bmod p$, which determines $a_p \in \mathbb{Z}$ for $p > 16g^2$. (for $p \le 16g^2$ one can simply count point naïvely).

Fast implementations are currently available in the following cases:

- Hyperelliptic curves over $\mathbb{Q}$ [HS14, HS16].
- Geometrically hyperelliptic genus 3 curves over $\mathbb{Q}$ [HMS16].
- Smooth plane quartics over $\mathbb{Q}$ [CHS20].
- Superelliptic curves over $\mathbb{Q}$ [S20].

A toy implementation of Harvey's algorithm for smooth plane curves of arbitrary genus is available, but much still remains to be done...

Average polynomial-time in genus 1

Let $X: y^2 = f(x)$ with $\deg f = 3, 4$ and $f(0) \neq 0$, and let f_k^n be the coefficient of x^k in f^n. Then $a_p \equiv f_{p-1}^{(p-1)/2} \bmod p$ for all good p.

The relations $f^{n+1} = f \cdot f^n$ and $(f^{n+1})' = (n+1)f' \cdot f^n$ yield the identity

$$k f_0 f_k^n = \sum_{1 \leq i \leq d} (i(n+1) - k) f_i f_{k-i}^n,$$

for all $k, n \geq 0$. Suppose for simplicity $\deg f = 3$, and define

$$v_k^n := [f_{k-2}^n, f_{k-1}^n, f_k^n], \qquad M_k^n := \begin{bmatrix} 0 & 0 & (3n+3-k)f_3 \\ kf_0 & 0 & (2n+2-k)f_2 \\ 0 & kf_0 & (n+1-k)f_1 \end{bmatrix},$$

so that we have the recurrence $v_k^n = \frac{1}{kf_0} v_{k-1}^n M_k^n$.

Average polynomial-time in genus 1

We then have
$$v_k^n = \frac{1}{(f_0)^k k!} v_0^n M_1^n \cdots M_k^n.$$
We want to compute $a_p \equiv f_{2n}^n \bmod p$ with $n := (p-1)/2$.
This is just the last entry of the vector v_{2n}^n reduced modulo $p = 2n+1$.

Observe that $2(n+1) \equiv 1 \bmod p$, so $2M_k^n \equiv M_k \bmod p$, where
$$M_k := \begin{bmatrix} 0 & 0 & (3-2k)f_3 \\ kf_0 & 0 & (2-2k)f_2 \\ 0 & kf_0 & (1-2k)f_1 \end{bmatrix}$$
is an integer matrix whose entries do not depend on $p = 2n+1$, and
$$v_{2n}^n \equiv -\left(\frac{f_0}{p}\right) V_0 M_1 \cdots M_{p-1} \bmod p \qquad \text{(where } V_0 = [0,0,1]\text{)}.$$

Accumulating remainder tree

Given matrices $M_0, \ldots, M_{n-1}$ and moduli $m_1, \ldots, m_n$, to compute

$$\begin{aligned} M_0 \bmod m_1 \\ M_0 M_1 \bmod m_2 \\ M_0 M_1 M_2 \bmod m_3 \\ M_0 M_1 M_2 M_3 \bmod m_4 \\ \cdots \\ M_0 M_1 \cdots M_{n-2} M_{n-1} \bmod m_n \end{aligned}$$

multiply adjacent pairs and recursively compute

$$\begin{aligned} (M_0 M_1) \bmod m_2 m_3 \\ (M_0 M_1)(M_2 M_3) \bmod m_4 m_5 \\ \cdots \\ (M_0 M_1) \cdots (M_{n-2} M_{n-1}) \bmod m_n \end{aligned}$$

and adjust the results as required (for better results, use a forest).

Complexity analysis

Assume $\log|f_i| = O(\log B)$. The recursion has depth $O(\log B)$ and in each recursive step we multiply and reduce 3×3 matrices with integer entries whose total bitsize is $O(B \log B)$.

We can do all the multiplications/reductions at any given level of the recursion in time $O(\mathsf{M}(B \log B)) = B(\log B)^{2+o(1)}$.

Total complexity is $B(\log B)^{3+o(1)}$, or $(\log p)^{4+o(1)}$ per prime $p \leq B$.

For a single prime p we can give an $O(p^{1/2}(\log p)^{1+o(1)})$ algorithm using the same matrices.

This is a silly way to compute a_p in genus 1, but it is in practice the fastest than method known for $g > 2$ and $p \leq B$ (for any reasonable value of B).

Open problem: Given a polynomial-time algorithm that takes as input a defining equation for a nice curve $X/\mathbb{F}_p$ and outputs $\#X(\mathbb{F}_p)$.

Efficiently handling a single prime

Simply computing $V_0 M_1 \cdots M_{p-1}$ modulo p is surprisingly quick (faster than semi-naïve point-counting); it takes $p(\log p)^{1+o(1)}$ time.

But we can do better.

Viewing $M_k \bmod p$ as $M \in \mathbb{F}_p[k]^{3\times 3}$, we compute

$$A(k) := M(k)M(k+1)\cdots M(k+r-1) \in \mathbb{F}_p[k]^{3\times 3}$$

with $r \approx \sqrt{p}$ and then instantiate $A(k)$ at roughly r points to get

$$M_1 M_2 \cdots M_{p-1} \equiv_p A(1)A(r+1)A(2r+1)\cdots A(p-r).$$

Using standard product tree and multipoint evaluation techniques this takes $O(\mathsf{M}(p^{1/2})\log p) = p^{1/2}(\log p)^{2+o(1)}$ time.

Bostan-Gaudry-Schost: $p^{1/2}(\log p)^{1+o(1)}$ time [BGS07].

References

[BGS07] A. Bostan, P. Gaudry, and É. Schost, *Linear recurrences with polynomial coefficients and computation of the Cartier–Manin operator on hyperelliptic curves*, Siam J. Comput. **36** (2007), 1777–1806.

[BK94] A. Brumer and K. Kramer, *The conductor of an abelian variety*, Compos. Math. **92** (1994), 227–248.

[BSSVY16] A.R. Booker, J. Sijsling, A.V. Sutherland, J. Voight, and D. Yasaki, *A database of genus 2 curves*, LMS J. Comput. Math. **19A** (2016), 220–234.

[CHS20] E. Costa, D. Harvey, and A.V. Sutherland *Counting points on smooth plane quartics*, in preparation.

[FPRS19] D.W. Farmer, A. Pitale, N.C. Ryan, and R. Schmidt, *Analytic L-functions: Definitions theorems, and connections*, Bull. Amer. Math. Soc. **56** (2019), 261–280.

[FKRS12] F. Fité, K.S. Kedlaya, V. Rotger, and A.V. Sutherland, *Sato-Tate distributions and Galois endomorphism modules in genus 2*, Compos. Math. **148** (2012), 1390–1442.

[FKS15] F. Fité, K.S. Kedlaya, and A.V. Sutherland, *Sato-Tate groups of some weight 3 motives*, in "Frobenius Distributions", Contemp. Math. **663** (2016), AMS, 103–126.

[FKS19] F. Fité, K.S. Kedlaya, and A.V. Sutherland, *Sato-Tate groups of abelian threefolds: a preview of the classification*, Contemp. Math., AMS, to appear.

References

[Harvey15] D. Harvey, *Computing zeta functions of arithmetic schemes*, Proc. Lond. Math. Soc. **111** (2015), 1379–1401.

[HMS16] D. Harvey, M. Massierer, *Computing L-series of geometrically hyperelliptic curves of genus three*, ANTS XII, LMS J. Comput. Math. **19A** (2016), 220-234.

[HS14] . Harvey and A.V. Sutherland *Computing Hasse-Witt matrices of hyperelliptic curves in average polynomial time*, ANTS XI LMS J. Comput. Math. **17** (2014), 257-273.

[HS16] D. Harvey and A.V. Sutherland, *Computing Hasse-Witt matrices of hyperelliptic curves in average polynomial time II*, Contemp. Math. **663**, AMS, 127–148.

[Katz12] N.M. Katz, *Simple things we don't know*, in Colloquium De Giorgi 2010–2012 Pub. Scuola Norm. Sup. **4** (2013), 9–16.

[KP01] J. Kaczorowski and A. Perelli, *Strong multiplicity one for the Selberg class*, C.R. Acad. Sci. Paris. Ser. 1 Math. **332** (2001), 963–968.

[S] A.V. Sutherland, *Counting points on superelliptic curves in average polynomial time*, ANTS XIV, to appear.

[Taylor18] N. Taylor, *Sato-Tate distributions on abelian surfaces*, arXiv:1808.00243.