Zeta functions and p-adic integrals; computations and applications

Alex J. Best

16/4/2019

AMS Graduate Student Conference, Brown University

Where are we going?

... Hilbert often interrupted me... he kept interrupting frequently– finally I could not speak any more at all – and he said that from the start he did not even listen since he had the impression that everything was trivial —E. Artin

Please ask questions!

Plan:

- Zeta functions:
  - What are they?
  - Why calculate them?
  - How do you find them?
- Coleman integrals:
  - What are they?
  - Why calculate them?
  - How do you find them?

Curves and their points

Let C be a (smooth, projective) curve over $\mathbf{F}_q$, a finite field with q elements.

As $\mathbf{F}_q$ is finite $C(\mathbf{F}_q)$ is finite, moreover $C(\mathbf{F}_{q^n})$ is finite for all n, what are the values for different n?

Example
If $C = \mathbf{P}^1/\mathbf{F}_p$ then we have $C(\mathbf{F}_q) = \mathbf{F}_q \cup \{\infty\}$ so

$$\#C(\mathbf{F}_{p^n}) = p^n + 1.$$

An elliptic curve

Example
If $E\colon y^2 = x^3 - 1/\mathbf{F}_5$ then

n	1	2	3	4	5	6	7	8
$\#E(\mathbf{F}_{5^n})$	6	36	126	576	3126	15876	78126	389376
5^n	5	25	125	625	3125	15625	78125	390625
$\#E(\mathbf{F}_{5^n}) - 5^n - 1$	0	10	0	-50	0	250	0	-1250

We need a formula that is 0 for odd n and $-2 \cdot (-5)^{n/2}$ for even n:

$$\#E(\mathbf{F}_{5^n}) = 5^n + 1 - \left(\sqrt{-5}^n + (-\sqrt{-5})^n\right)$$

It initially seemed like we had an infinite amount of data here: $\#E(\mathbf{F}_{5^n})$ for all $n \in \mathbf{N}$. But we don't!

The Weil polynomial

Rephrased: we have a polynomial

$$L_E = t^2 + 5$$

so that

$$\#E(\mathbf{F}_{5^n}) = 5^n + 1 - \sum_{\text{roots } \alpha_i \text{ of } L_E} \alpha_i^n$$

how general a phenomenon is this?

Theorem (Schmidt?, Weil?)
Let $C/\mathbf{F}_q$ be a curve, there exists a monic $L_C(t) \in \mathbf{Z}[t]$ of degree $2 \cdot \mathrm{genus}(C)$. Whose roots α_i come in complex conjugate pairs with $|\alpha_i| = q^{1/2}$ and

$$\#C(\mathbf{F}_{q^n}) = q^n + 1 - \sum_{\textit{roots } \alpha_i \textit{ of } L_C} \alpha_i^n$$

The zeta function

The condition on the roots means $\alpha_i \overline{\alpha}_i = q$ so we may write $L_C(t) = q^g \prod_i (1 - \frac{\alpha_i}{q} t)$ then

$$\log(L_C(t)/q^g) = -\sum_i \sum_{n=1}^{\infty} \frac{\alpha_i^n t^n}{q^n n} = \sum_{n=1}^{\infty} -\left(\sum_i \alpha_i^n\right) \frac{t^n}{q^n n}$$

so $\log(L_C(qt)/q^g)$ almost knows the point counts, if we define:

Definition
The (Hasse-Weil) zeta function of $C/\mathbf{F}_q$ is

$$Z(C,t) := \exp\left(\sum_{i=1}^{\infty} \#C(\mathbf{F}_{q^i}) \frac{t^i}{i}\right)$$

And we have that

$$Z(C,t) = \frac{q^{-g} L_C(qt)}{(1-t)(1-qt)}.$$

Why bother?

Reverse engineering: Find point counts!

If we have a way to find the zeta function we can get the point counts in a more sophisticated way.

In fact if $J = \mathrm{Jac}(C)$ the Jacobian (i.e. the class group of C)

$$L_C(1) = \#J(\mathbf{F}_q)$$

We can tell a lot about the Jacobian from this number!

Example (A completely random example, I promise)

$$C\colon y^2 = x^5 + 6x^2 + x + 3/\mathbf{F}_{43}$$

$$L_C(t) = t^4 + 9t^3 + 64t^2 + 387t + 1849$$

$$\implies \#J(\mathbf{F}_{43}) = L_C(1) = 2310 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$$

so $J(\mathbf{F}_{43}) = C_{2\cdot 3\cdot 5\cdot 7\cdot 11}$. So never use this curve for cryptography!!

Distributional questions - Sato-Tate

Let $C/\mathbf{Q}$ be a genus g curve. We can reduce mod p for all primes p of good reduction, get a polynomial $L_{C_{\mathbf{F}_p}}(t)$ for all these p. If we *normalise* to have all roots of complex norm 1 we get

$$\widetilde{L}_{C_{\mathbf{F}_p}}(t) = L_{C_{\mathbf{F}_p}}(\sqrt{p}t),$$

a unitary symplectic polynomial, i.e. the characteristic polynomial of a unitary symplectic matrix.

So we get a map

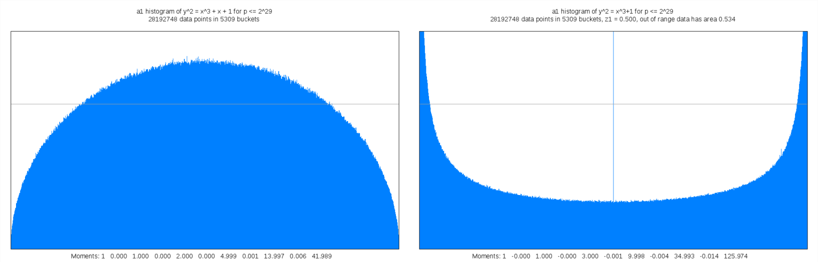
$$\text{good primes} \to \mathrm{Conj}(\mathrm{USp}(2g))$$

the RHS has a Haar measure coming from $\mathrm{USp}(2g)$

How is the image distributed as $p \to \infty$?

Genus 1

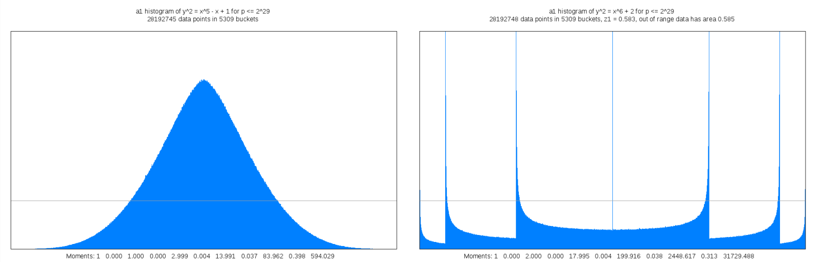
$$y^2 = x^3 + x + 1 \qquad y^2 = x^3 + 1$$



Pictures due to Drew Sutherland. Left is a generic elliptic curve, the right has CM (over $\mathbf{Q}$). By computing enough zeta functions we can *see* the endomorphism algebra of our curve.

Genus 2

$$y^2 = x^5 - x + 1 \qquad y^2 = x^6 + 2$$



Pictures due to Drew Sutherland. Left is a generic genus 2 curve, the right has $\mathrm{End}(\mathrm{Jac}(C)_{\overline{\mathbf{Q}}}) \otimes \mathbf{R} = \mathrm{Mat}_2(\mathbf{C})$. After the work of Fité-Kedlaya-Rotger-Sutherland we can recognise these distributions and guess the structure of the Jacobian, the right one should be square of a CM elliptic curve.

Relations

Let

$$C_1 \colon y^2 + y = x^3 + x/\mathbf{F}_2,\ C_2 \colon y^2 + y = x^5 + x/\mathbf{F}_2$$

then

$$L_{C_1}(t) = t^2 + 2t + 2,\ L_{C_2} = (t^2 + 2t + 2)(t^2 + 2)$$

what does this tell us?

Theorem (Kleiman, Serre)
If there is a morphism of curves $C \to D$ over $\mathbf{F}_q$ then

$$L_D(t) | L_C(t)$$

In our example we have a map

$$(x, y) \mapsto (x^2 + x, y + x^3 + x^2).$$

Relations again

The converse is false!

$$D_1\colon y^2 + xy = x^5 + x/\mathbf{F}_2,\ D_2\colon y^2 + xy = x^7 + x/\mathbf{F}_2$$

where

$$L_{D_1}(t) = t^4 + t^3 + 2t + 4,\ L_{D_2} = (t^4 + t^3 + 2t + 4)(t^2 + 2)$$

but no map exists!

How to compute?

Reverse reverse engineering: Count points for a few n ($n \leq g$ is sufficient), recover $L_C(t)$. This can take a long time!

p-**adic cohomology:** A method due to Kedlaya relates $L_C(t)$ to p-adic cohomology. $L_C(t)$ is the characteristic polynomial of "Frobenius" acting on "$H^1_{MW}(\tilde{C})$". If we can compute this action (as a matrix) we win!

Average time: Harvey-Sutherland have an approach to compute $L_{C_{\mathbf{F}_p}}(t)$ for a curve over $\mathbf{Q}$ for all $p < N$ at once! This works out faster on average.

Monsky-Washnitzer cohomology in general

Let $C/\mathbf{F}_q$ be an (odd) hyperelliptic curve.

First choose a lift $\tilde{C}/\mathbf{Z}_q$ and an affine open $U = \operatorname{Spec}(A) \subseteq C$. And a lift of the q-power Frobenius on $\overline{A} = A/pA$ to $\phi\colon A^\dagger \to A^\dagger$.

Now the weak completion $A^\dagger$ is the set of p-adic power series on U that p-adically overconverge.

We have differentials $\Omega^1_{A^\dagger}$ and a derivative $\mathrm{id}\colon A^\dagger \to \Omega^1_{A^\dagger}$

$$H^1_{\mathrm{MW}}(\overline{A}) = \Omega^1_{A^\dagger} \otimes \mathbf{Q}_p / \mathrm{d}(A^\dagger \otimes \mathbf{Q}_p)$$

Monsky-Washnitzer cohomology (for hyperelliptic curves)

Let $C\colon y^2 = \overline{Q}(x)/\mathbf{F}_q$ be an (odd) hyperelliptic curve.

First choose a lift $\tilde{C}\colon y^2 = Q(x)/\mathbf{Z}_q$.

The affine coordinate ring of the punctured curve is

$$A = \mathbf{Z}_p[x, y, y^{-1}]/(y^2 - Q(x))$$

$$A^\dagger = \left\{ \sum_{i=-\infty}^{\infty} R_i(x) y^{-i} : R_i \in \mathbf{Z}_p[x]_{\deg \leq 2g} \text{ where } \liminf_{|i| \to \infty} v_p(R_i)/|i| > 0 \right\}$$

The q-power Frobenius on A/pA can be lifted to $\phi\colon A^\dagger \to A^\dagger$

$$x \mapsto x^p$$

$$y \mapsto y^{-p} \sum_{k=0}^{\infty} \binom{-1/2}{k} (\phi(Q(x)) - Q(x)^p)^k / y^{2pk}.$$

Monsky-Washnitzer cohomology (for hyperelliptic curves)

$$\Omega_{A^\dagger} = A^\dagger \,\mathrm{d}x \oplus A^\dagger \,\mathrm{d}y / (2y\,\mathrm{d}y - Q'(x)\,\mathrm{d}x))$$

$$\begin{aligned} \mathrm{d}\colon A^\dagger &\to \Omega^1_{A^\dagger} \\ \sum_{i=-\infty}^{\infty} \frac{R_i(x)}{y^i} &\mapsto \sum_{i=-\infty}^{\infty} R_i'(x) y^{-i}\,\mathrm{d}x - R_i(x) i y^{-i-1}\,\mathrm{d}y. \end{aligned}$$

Reductions in cohomology

$\{\omega_i = x^i \,\mathrm{d}x/y\}_{i=1,\ldots,2g}$ are a basis for $H^1_{MW}(C)$ and for each i we get an expansion

$$\phi^*\omega_i \equiv \sum_{j=0}^{N-1} \sum_{r=0}^{(2g+1)j} B_{j,r} x^{p(i+r+1)-1} y^{-p(2j+1)+1} \frac{\mathrm{d}x}{2y} \pmod{p^N}$$

We need to write this in the form

$$\phi^*\omega_i \equiv \sum_{j=1}^{2g} a_{ij}\omega_j - \mathrm{d}(f_i) \pmod{p^N}$$

to do this we iteratively use relations like

$$\begin{aligned} \mathrm{d}(x^s y^{-2t+1}) = {} & (2s - (2t-1)(2g+1))\, x^{2g+1} x^{s-1} y^{-2t} \frac{\mathrm{d}x}{2y} \\ & + \big(2sP(x) - (2t-1)xP'(x)\big)\, x^{s-1} y^{-2t} \frac{\mathrm{d}x}{2y}. \end{aligned}$$

to reduce the exponents of monomials appearing in the expansion.

Reductions in cohomology

We end up with

$$\phi^*\omega_i \equiv \sum_{j=1}^{2g} a_{ij}\omega_j - \mathrm{d}(f_i) \pmod{p^N}$$

The L-polynomial is then the characteristic polynomial of the matrix $F = (a_{ij})_{i,j}$.

Interlude: Computing things quickly - a silly example

Suppose we want to evaluate $N!$ for N large, how many ring operations does this take? Naively: N operations, but we can break up the product into chunks by dividing into products of length $\sqrt[4]{N}$ (so $\sqrt[4]{N}^3$ subproducts in total)

$$N! = P(0) \cdot P(\sqrt{N}) \cdot P(2\sqrt{N}) \cdots P((\sqrt{N}-1)\sqrt{N})$$

where

$$P(x) = (x+1)(x+2)\cdots(x+\sqrt[4]{N})$$

once we compute $\sqrt[4]{N}$ of these $P(i)$ (for $i = 0, \ldots, \sqrt[4]{N}$) in $\sqrt{N}$ steps we have a degree $\sqrt[4]{N}$ polynomial evaluated at $\sqrt[4]{N}$ points. If you know a (monic) degree n polynomial at n points, you know the polynomial! $\rightsquigarrow$ interpolate to find other values

Interlude: Computing things quickly - Fancy version

In general if we have $M(t) \in \mathrm{Mat}_{n\times n}(R[t])$ a matrix with linear polynomials as coefficients. We can evaluate lots of products

$$\begin{aligned}
&M(0)M(1)\cdots M(k-1),\\
&M(k)M(k+1)\cdots M(2k-1),\\
&\vdots\\
&M((m-1)k)M((m-1)k+1)\cdots M(mk-1)
\end{aligned}$$

quickly in practice! (Bostan-Gaudry-Schost,Harvey)

Using this we can reduce quickly and compute $L_C(t)$ in time roughly $\sqrt{p}$ (Harvey).

With Arul, Costa, Magner, Triantafillou we can do this for general cyclic covers $y^a = f(x)$.

Part II - Coleman integrals

Take $C/\mathbf{Z}_p$ a genus g curve and p an odd prime.

Theorem (Coleman)
There is a $\mathbf{Q}_p$-linear map $\int_b^x \colon \Omega^1_{A^\dagger} \otimes \mathbf{Q}_p \to A_{\mathrm{loc}}(X)$ for which:

$$\mathrm{d} \circ \int_b^x = (\mathrm{id} \colon \Omega^1_{A^\dagger} \otimes \mathbf{Q}_p \to \Omega^1_{loc}) \quad \text{“FTC”}$$

$$\int_b^x \circ \, \mathrm{d} = (\mathrm{id} \colon A^\dagger \hookrightarrow A_{\mathrm{loc}})$$

$$\int_b^x \phi^* \omega = \phi^* \int_b^x \omega \quad \text{“Frobenius equivariance”}$$

Locally we can integrate power series formally.

To integrate between far away points we use Frobenius equivariance.

Frobenius equivariance

Switch to an odd hyperelliptic curve now, some manipulation with the set of all $\int_P^\infty \omega_i$ gives:

$$\begin{pmatrix} \vdots \\ \int_P^\infty \omega_i \\ \vdots \end{pmatrix} = (F - I)^{-1} \begin{pmatrix} \vdots \\ f_i(P) \\ \vdots \end{pmatrix}$$

where from earlier

$$\phi^* \omega_i \equiv \sum_{j=1}^{2g} M_{ij} \omega_j - \mathrm{d} f_i$$

Effective Chabauty

One consequence of Coleman's work we saw earlier is

Theorem (Coleman's effective Chabauty)
Let $C/\mathbf{Q}$ be a curve of genus g. If $\operatorname{rank} J(C)(\mathbf{Q}) < g$ and $p > 2$ is a prime of good reduction for C then

$$\#C(\mathbf{Q}) \leq \#C_p(\mathbf{F}_p) + 2g - 2.$$

Explicit Chabauty

Given an individual curve we can often compute $X(\mathbf{Q})$ by explicitly evaluating enough of these integrals.

More generally via non-abelian Chabauty we can approach more curves, this requires computing iterated Coleman integrals.

$$X_s(13)$$

or

$$X_0(67)^+ \text{ and friends?}$$

A fun converse

Thinking about effective Chabauty backwards: if we have a lot of $\mathbf{Q}$-points and few $\mathbf{F}_p$ points, the Jacobian must have large rank!

Example
To force a curve to have many $\mathbf{Q}$ points and few $\mathbf{F}_7$ points, let

$$C\colon y^2 = x(x-7)(x-14)(x+7)(x+14)+1$$

this has a bunch of rational points $(7n, \pm 1)$ for $n = -2, -1, 0, 1, 2$ (and ∞ so ≥ 11 in all), but these give the same $\mathbf{F}_7$ points $(0, \pm 1)$. In fact $\#C(\mathbf{F}_7) = 8$ so we fail the Coleman bound as

$$11 \leq 8 + 2g - 2 = 10$$

so we must have $\operatorname{rank} \operatorname{Jac}(C)(\mathbf{Q}) \geq g = 2$. (Magma tells me $\operatorname{rank} \operatorname{Jac}(C)(\mathbf{Q}) = 5$ in fact!)

More generally

In fact Coleman showed:

Corollary (Coleman)
Let $k \in \mathbf{Z}$, $p \nmid k$ prime and $f(x)/\mathbf{Z}$ monic with $f(x) \equiv x^k \pmod{p}$ and $\lfloor (k+1)/2 \rfloor$ roots over $\mathbf{Z}$ then the rank of the Jacobian of

$$y^2 = f(x) + 1$$

is at least the genus (which is $\lfloor (k-1)/2 \rfloor$)

The proof is a little more serious than our example above, it shows that the points $(\alpha_i, 1)$ where α_i are roots of f are actually linearly independent in the Jacobian.

Fast Coleman

Recall to compute a Coleman integral we need to find

$$F, \{f_i(P)\}_i$$

we can coerce the evaluation of $f_i(P)$ into a linear recurrence and apply Bostan-Gaudry-Schost!

Generalities

Coleman integration can be more general, Coleman de Shallit define:

$$r_C \colon K_2(\overline{k}(C)) \to \mathrm{Hom}(H^0(C, \Omega^1_{C/\overline{k}}), \overline{k}).$$

$$r(f, g)(\omega) = -\int_{(g)} \log(f) \in \overline{k}$$

Where next?

- Coleman integration quickly on general curves
- Coleman integration for many primes at once?
- Distribution?