Computing L-functions of modular curves

Andrew V. Sutherland

Massachusetts Institute of Technology

Michigan – Arithmetic Geometry Initiative – Columbia

May 28, 2020

Mazur's Bonn lectures and Program B

In the course of preparing my lectures for this conference, I found a proof of the following theorem, conjectured by Ogg (conjecture 1 [17b]):

THEOREM 1. Let Φ be the torsion subgroup of the Mordell-Weil group of an elliptic curve E, over $\mathbb{Q}$. Then Φ is isomorphic to one of the following 15 groups:

$$\mathbb{Z}/m\cdot\mathbb{Z} \qquad \text{for} \quad m \le 10 \quad \text{or} \quad m = 12$$

$$\mathbb{Z}/2\cdot\mathbb{Z} \times \mathbb{Z}/2\nu\cdot\mathbb{Z} \qquad \text{for} \quad \nu \le 4 \ .$$

⋮

Theorem 1 also fits into a general program:

B. Given a number field K and a subgroup H of $GL_2\hat{\mathbb{Z}} = \prod_p GL_2\,\mathbb{Z}_p$ classify all elliptic curves $E_{/K}$ whose associated Galois representation on torsion points maps $\mathrm{Gal}(\overline{K}/K)$ into $H \subset GL_2\hat{\mathbb{Z}}$.

Galois representations attached to elliptic curves

Let E be an elliptic curve over a number field k. For each integer $N \geq 1$ the action of $G_k := \mathrm{Gal}(\bar{k}/k)$ on $E[N]$ yields a mod-N Galois representation

$$\rho_{E,N}\colon G_k \to \mathrm{Aut}(E[N]) \simeq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}).$$

Choosing a compatible system of bases and taking the inverse limit yields

$$\rho_E\colon G_k \to \mathrm{GL}_2(\widehat{\mathbb{Z}}) \simeq \prod_\ell \mathrm{GL}_2(\mathbb{Z}_\ell).$$

Theorem (Serre 1972)

For non-CM elliptic curves the image of ρ_E is an open subgroup $H_E \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$.

There is thus a minimal positive integer M_E such that ρ_E factors through $\bar{\rho}_{E,M_E}$ and H_E is completely determined by its reduction modulo M_E.

There are infinitely many possibilities for M and H_E as E/k varies, but it is believed that only finitely many non-surjective projections to $\mathrm{GL}_2(\mathbb{Z}_\ell)$ arise, and only finitely many values of $[\mathrm{GL}_2(\widehat{\mathbb{Z}}) : H_E]$ (even if only $[k : \mathbb{Q}]$ is fixed).

Modular curves

Let H be an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}}) = \varprojlim \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) =: \varprojlim \mathrm{GL}_2(N)$.

Then H contains the kernel of $\pi_N\colon\ \mathrm{GL}_2(\widehat{\mathbb{Z}}) \to \mathrm{GL}_2(N)$ for some $N \geq 1$;
the least such N is the level of H, and H is completely determined by $\pi_N(H)$.

Definition (Deligne-Rapoport 1973)

The modular curves X_H and Y_H are coarse spaces for the stacks $\mathcal{M}_H$ and $\mathcal{M}_H^0$ that parameterize elliptic curves with H-level structure.

- X_H is a smooth proper $\mathbb{Z}[\frac{1}{N}]$-scheme with open subscheme Y_H.
  The complement X_H^∞ of Y_H in X_H (the cusps) is finite étale over $\mathbb{Z}[\frac{1}{N}]$.
- When $\det(H) = \widehat{\mathbb{Z}}^\times$ the generic fiber of X_H is a nice curve $X_H/\mathbb{Q}$,
  and $X_H(\mathbb{C})$ is a Riemann surface isomorphic to $X_{\Gamma_H} := \Gamma_H \backslash \mathcal{H}$,
  where $\Gamma_H \subseteq \mathrm{SL}_2(\mathbb{Z})$ is the inverse image of $\pi_N(H) \cap \mathrm{SL}_2(N)$.
- In particular, $g(X_H) = g(X_{\Gamma_H})$, and X_H and X_{Γ_H} have the same cusps.
  Note: $X_{\Gamma_H} = X_{\Gamma_{H'}} \not\Rightarrow X_H = X_{H'}$, and the levels of X_{Γ_H} and X_H may differ.
- If $\det(H) \neq \widehat{\mathbb{Z}}^\times$ then X_H is not geometrically connected (but that's OK!).

Classical modular curves

For $B_0(N) := \{\left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right)\} \subseteq \mathrm{GL}_2(N)$ we have $X_0(N) = X_{B_0(N)}$ (as curves over $\mathbb{Q}$).
For $B_1(N) := \{\left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)\} \subseteq \mathrm{GL}_2(N)$ we have $X_1(N) = X_{B_1(N)}$.

We similarly define $X_{\mathrm{s}}(p)$, $X_{\mathrm{ns}}(p)$, using Cartan subgroups $H \subseteq \mathrm{GL}_2(p)$.

Example: Let us compute $\#X_1(13)(\mathbb{F}_{37})$.

Over $\mathbb{F}_{37}$ there are 4 elliptic curves with a rational point of order 13:

$$\begin{aligned} y^2 &= x^3 + 4, & y^2 &= x^3 + 33x + 33, \\ y^2 &= x^3 + 8x, & y^2 &= x^3 + 24x + 22. \end{aligned}$$

What is $\#X_1(13)(\mathbb{F}_{37})$?

The genus 2 curve `169.1.169.1` is a smooth model for $X_1(13)$:

$$y^2 + (x^3 + x + 1)y = x^5 + x^4.$$

It has 23 rational points over $\mathbb{F}_{37}$.

What do these 23 points represent?

Moduli spaces of elliptic curves with H-level structure

Let H be an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ of level N with image H in $\mathrm{GL}_2(N)$.
Let k be a perfect field whose characteristic does not divide N.

Definition

An H-level structure on an elliptic curve $E/\bar{k}$ is the equivalence class $[\iota]_H$ of an isomorphism $\iota\colon E[N] \to (\mathbb{Z}/N\mathbb{Z})^2$, where $\iota \sim \iota'$ if $\iota = h \circ \iota'$ for some $h \in H$.

If we fix a basis so $E[N] := (\mathbb{Z}/N\mathbb{Z})^2$, then $[\iota]_H$ is a right H-coset in $\mathrm{GL}_2(N)$.

Definition

The set $Y_H(\bar{k})$ consists of equivalence classes of pairs $(E, [\iota]_H)$, where $(E, [\iota]_H) \sim (E', [\iota']_H)$ if there is an isomorphism $\phi\colon E \to E'$ for which the induced isomorphism $\phi_N\colon E[N] \to E'[N]$ satisfies $\iota \sim \iota' \circ \phi_N$.

Equivalently, $Y_H(\bar{k})$ consists of pairs $(j(E), \alpha)$, where $\alpha = HgA_E$ is a double coset in $H\backslash \mathrm{GL}_2(N)/A_E$, with $A_E := \{\varphi_N : \varphi \in \mathrm{Aut}(E)\}$.

The set of k-rational points $Y_H(k)$

The Galois group $G_k := \mathrm{Gal}(\bar{k}/k)$ acts on $Y_H(\bar{k})$ by acting on coefficients of E and points in $E[N]$, which induces an action on $[\iota]_H$ and pairs $(E, [\iota]_H)$.

More precisely, $\sigma \in G_K$ send E to E^σ and induces an isomorphism $\sigma^{-1} \colon E^\sigma[N] \to E[N]$ defined by $(x : y : z) \mapsto (\sigma^{-1}(x) : \sigma^{-1}(y) : \sigma^{-1}(z))$.

For $P := (E, [\iota]_H) \in Y_H(\bar{k})$ we have $\sigma(P) := (E^\sigma, [\iota \circ \sigma^{-1}]_H)$.

The subset of G_k-stable points in $Y_H(\bar{k})$ forms the set of k-rational points $Y_H(k)$.

Lemma (DR73, Z15)

Each $P \in Y_H(k)$ is represented by a pair $(E, [\iota]_H) \in Y_H(k)$ with E defined over k, and any such a pair lies in $Y_H(k)$ if and only if for all $\sigma \in G_k$ there exists a $\varphi \in \mathrm{Aut}(E_{\bar{k}})$ and an $h \in H$ such that

$$\iota \circ \sigma^{-1} = h \circ \iota \circ \varphi_N.$$

In other words, a pair $(j(E), \alpha)$ with $j(E) \in k$ and $\alpha = HgA_E$ lies in $Y_H(k)$ if and only if $Hg\sigma^{-1}A_E = HgA_E$ for all $\sigma \in G_k$, where $A_E := \{\varphi_N : \varphi \in \mathrm{Aut}(E_{\bar{k}})\}$.

Interpreting rational points on Y_H

Recall that if E is an elliptic curve over a number field K, the action of G_K on torsion points of $E(\overline{K})$ yields a Galois representation

$$\rho_E\colon G_K \to \mathrm{Aut}(E(\overline{K})_{\mathrm{tor}}) \simeq \mathrm{GL}_2(\widehat{\mathbb{Z}}) \simeq \varprojlim \mathrm{GL}_2(N).$$

For each positive integer N, let $\rho_{E,N}$ denote the projection to $\mathrm{GL}_2(N)$.

Lemma (DR73, RZB15)

Let H be an open subgroup of $\mathrm{GL}_2(\widehat{\mathbb{Z}})$ of level N and let E be an elliptic curve over a number field K. There exists an isomorphism $\iota\colon E[N] \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^2$ such that $(E, [\iota]_H) \in Y_H(K)$ if and only if the image of $\rho_{E,N}$ is contained in a subgroup of $\mathrm{GL}_2(N)$ conjugate to $\pi_N(H)$.

This is how we should understand the moduli interpretation of Y_H and X_H.

The set of k-rational cusps $X_H^\infty(k)$

Let $U(N) := \langle \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right), -1 \rangle \subseteq \mathrm{GL}_2(N)$.
We define a right G_k-action on $H \backslash \mathrm{GL}_2(N)/U$ via $hgu \mapsto hg\chi_N(\sigma)u$,
where $\chi_N(\sigma) := \left(\begin{smallmatrix} e & 0 \\ 0 & 1 \end{smallmatrix}\right)$ is defined by $\sigma(\zeta_N) = \zeta_N^e$.

Lemma (DR73)

The cardinality of $X_H^\infty(k)$ is equal to the cardinality of the subset of $H \backslash \mathrm{GL}_2(N)/U(N)$ fixed by $\chi_N(G_k)$.

When k is finite, we can compute both $\#X_H^\infty(k)$ and $\#Y_H(k)$ by counting the fixed points of a right G_k-action on a double coset spaces of $\mathrm{GL}_2(N)$.

We have

$$\#X_H(k) = \#(H \backslash \mathrm{GL}_2(N)/U(N))^{\chi_N(G_k)} + \sum_{j(E) \in k} \#(H \backslash \mathrm{GL}_2(N)/A_E)^{G_k}.$$

This does not depend on the choice of E or the choice of basis for $E[N]$.

Where the 23 points of $X_1(13)(\mathbb{F}_{37})$ come from

For $k = \mathbb{F}_{37}$ and the action of G_k is generated by the 37-power Frobenius σ, which induces the action of $\chi_{13}(G_k)$ on $\mu_{13}(\bar{k})$ and the Frobenius endomorphism π_E which acts on $E[13]$. We have

$$\#\,\mathrm{GL}_2(13) = 12^2 \cdot 13 \cdot 14, \qquad \#B_1(13) = 12 \cdot 13, \qquad \#U = 26,$$

and the right coset space $B_1(13)\backslash\,\mathrm{GL}_2(13)$ has cardinality $12 \cdot 14 = 168$.

- The space $B_1(13)\backslash\,\mathrm{GL}_2(13)/U(13)$ partitions $B_1(13)\backslash\,\mathrm{GL}_2(13)$ as $2^6 26^6$. These 12 double cosets correspond to the 12 cusps of $X_1(13)$.

  The 6 partitions of size 26 are fixed by $\chi_{13}(\sigma) = \left(\begin{smallmatrix} 11 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ but not the others.

  So we have 6 rational cusps.

- The four elliptic curves $E/\mathbb{F}_{37}$ with a points of order 13 have j-invariants $0, 16, 26, 35$ (note $1728 \equiv 26 \bmod 37$), so A_E is cyclic of order $6, 2, 4, 2$.

  The 168 right cosets of $B_1(13)$ correspond to the 168 points of order 13 in $E[13]$; in all 4 cases exactly 12 of these are fixed by π_E.

  We thus get $2 + 6 + 3 + 6 = 17$ non-cuspidal rational points.

2 + 6 + 3 + 6 + 6 = 23

Counting $\mathbb{F}_q$-points on X_H

Let $j_H\colon X_H \to X(1)$ be the morphism induced by $H \subseteq \mathrm{GL}_2(\widehat{\mathbb{Z}})$.

$$\#X_H(\mathbb{F}_q) = \#X_H^\infty(\mathbb{F}_q) + \textstyle\sum_{j\in\mathbb{F}_q} \#\{P \in Y_H(\mathbb{F}_q) : j_H(P) = j\}$$

Every term is computed by counting double cosets fixed by a right action. Computing $\chi_N(\sigma)$ is easy (reduce q modulo N). To compute π_E we use [DT02].

Theorem (DT02)

Let $E/\mathbb{F}_q$ be an elliptic curve, and let π_E denote its Frobenius endomorphism. Define $a := \operatorname{tr}\pi_E = q+1-\#E(\mathbb{F}_q)$ and $R := \operatorname{End}(E)\cap\mathbb{Q}(\pi_E)$, let $\Delta := \operatorname{disc}(R)$ and $\delta := \Delta \bmod 4$, and let $b := \sqrt{(a^2-4q)/\Delta}$ if $\Delta \neq 1$ and $b := 0$ otherwise. The integer matrix

$$A_\pi := \begin{pmatrix} (a+b\delta)/2 & b \\ b(\Delta-\delta)/4 & (a-b\delta)/2 \end{pmatrix}$$

determines the action of π_E on $E[N]$ for all $N \geq 1$.

Note: A_π is determined only up to conjugacy, but we must compute A_E and A_π with respect to the same basis for $E[N]$.

Computational issues

1. Computing b typically requires determining $[\mathcal{O}_K : \mathrm{End}(E)]$ where $K = \mathbb{Q}(\sqrt{a^2 - 4q})$. This is much harder than computing $\mathrm{tr}\,\pi_E$.
   The brute force approach tests $H_D(j(E)) \stackrel{?}{=} 0$ for discriminants D of all orders in $\mathcal{O}_K$ containing $\mathbb{Z}[\pi_E]$. This is expensive and unnecessary.

   We will enumerate every root of H_D for all such D as we enumerate $j(E)$!
2. Computing an explicit basis for $E[N]$ is painful when N is large; this only matters when $j(E) = 0, 1728$, but these two cases can get very expensive.

Solution to (1): Instead of enumerating j-invariants, enumerate Frobenius traces a and compute A_π for each triple (a, b, Δ) satisfying $4q = a^2 - b^2\Delta$. Then multiply the number of double cosets fixed by A_π by $h(D)$.

This reduces the problem to computing class numbers rather than Hilbert class polynomials, which is much easier (and can be done via table lookup).

Solution to (2): Instead of computing A_E, enumerate twists of elliptic curves with $j(E) = 0, 1728$ and compute A_π for each. No need to fix a basis for $E[N]$.

The algorithm

Given $H \subseteq \mathrm{GL}_2(N)$ and a prime power q, compute $X_H(\mathbb{F}_q)$ as follows:

1. Compute $f_H \colon \mathrm{GL}_2(N) \to \mathbb{Z}$ defined by $g \mapsto \#(H\backslash \mathrm{GL}_2(N)/\{\pm 1\})^g$.
   Note that f_H does not depend on q and factors through the class map.
   Indeed: $f_H(g) = [\mathrm{GL}_2(N) : H] \cdot \#(\pm H \cap g^{\mathrm{GL}_2(N)}) \cdot (\# g^{\mathrm{GL}_2(N)})^{-1}$.
2. Compute $n_\infty := \# X_H^\infty(\mathbb{F}_q) = \#(H\backslash \mathrm{GL}_2(N)/U(N))^{\chi_N(\sigma)}$.
   (this step is fast in practice, but asymptotically annoying).
3. Compute $n_0 := \# j_H^{-1}(0)$ and $n_{1728} := \# j_H^{-1}(1728)$ by computing A_π for each twist, summing $f_H(A_\pi)$ values, and dividing by $\# \mathrm{Aut}(E_{\bar{k}})$.
4. Set $n_{\mathrm{ord}} := 0$ and for a from 1 to $\lfloor 2\sqrt{q} \rfloor$ coprime to q:
   - Compute $D = a^2 - 4q$, put $D_0 := \operatorname{disc} \mathbb{Q}(\sqrt{D_\pi})$ and for $b^2 | (D/D_0)$:
     - Set $D' := b^2 D_0$ and $\delta := D \bmod 4$ and compute A_π (for $D' < -4$).
       If $f_H(A_\pi) \neq 0$, compute/lookup $h(D)$ and add $f_H(A_\pi)h(D)$ to n_{ord}.
5. Compute n_{ss} by computing A_π for supersingular elliptic curves with $j \neq 0, 1728$ (only $a = 0, \pm 2q$ possible), and multiplying $f_H(A_\pi)$ by the counts of such curves (using $h(\sqrt{-q})$, $h(\sqrt{-4q})$ and [W69]).
6. Output $\# X_H(\mathbb{F}_q) = n_\infty + n_0 + n_{1728} + n_{\mathrm{ord}} + n_{\mathrm{ss}}$.

A trivial (but still very useful) real life example

Consider the following genus 12 subgroup on the Mazur-B 7-adic list:

$$H := \langle \left(\begin{smallmatrix} 41 & 1 \\ 1 & 8 \end{smallmatrix}\right), \left(\begin{smallmatrix} 37 & 3 \\ 11 & 26 \end{smallmatrix}\right) \rangle \subseteq \mathrm{GL}_2(49);$$

Running the algorithm above produces $\#X_H(\mathbb{F}_2) = 0$.

The curve X_H has good reduction at 2, and it follows that $X_H(\mathbb{Q}) = \emptyset$.

There is therefore no elliptic curve $E/\mathbb{Q}$ whose 7-adic image lies in H.

This is all we need to know, but for pedagogical purposes we note by counting points over $\mathbb{F}_{2^r}$ for $r = 1, 2, \ldots 12$ we may compute the L-polynomial

$$\begin{aligned} L_2(T) = &(2^3T^6 - 12T^5 + 4T^4 + T^3 + 2T^2 - 3T + 1) \\ &(2^3T^6 - 8T^5 + 10T^4 - 7T^3 + 5T^2 - 2T + 1)^2 \\ &(2^3T^6 + 16T^5 + 18T^4 + 15T^3 + 9T^2 + 4T + 1). \end{aligned}$$

A curve with many points

Consider the following genus 8 group:

$$H := \langle \left(\begin{smallmatrix} 1 & 15 \\ 12 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 15 & 16 \\ 4 & 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 9 & 4 \\ 8 & 3 \end{smallmatrix}\right) \rangle \subseteq \mathrm{GL}_2(18).$$

Running the algorithm above with $q = 13^2$ yields $\#X_H(\mathbb{F}_{13^2}) = 364$.

This sets a new record for genus 8 curves over $\mathbb{F}_{13^2}$, see the website

`manypoints.org`.

There are only finitely many $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ of genus 8, see the

Cummins and Pauli database

there are infinitely many non-isomorphic modular curves X_H of genus 8.

A non-trivial real life example

Consider the following genus 14 subgroup on the Mazur-B 5-adic list:

$$H := \langle \left(\begin{smallmatrix} 8 & 6 \\ 4 & 4 \end{smallmatrix}\right), \left(\begin{smallmatrix} 9 & 18 \\ 7 & 16 \end{smallmatrix}\right) \rangle \subseteq \mathrm{GL}_2(25);$$

this is the normalizer of a non-split Cartan subgroup of $\mathrm{GL}_2(25)$. Counting points on X_H over $\mathbb{F}_{2^r}$, $\mathbb{F}_{5^r}$, $\mathbb{F}_{7^r}$ for $1 \leq r \leq 14$ yields the L-polynomials

$$\begin{aligned}
L_2(T) &= (2^2T^4 - 2T^3 + 3T^2 - T + 1)(2^2T^4 + 2T^3 + 3T^2 + T + 1)^2(2^8T^{16} + \cdots + 5T + 1), \\
L_3(T) &= (3T^2 - T + 1)^2(3T^2 + T + 1)^2(3^2T^4 + 9T^3 + 7T^2 + 3T + 1)(3^8T^{16} + \cdots + 5T + 1), \\
L_7(T) &= (7^2T^4 - 7T^3 + 13T^2 - T + 1)(7^2T^4 + 7T^3 + 13T^2 + T + 1)(7^2T^4 + 7T^3 + 3T^2 + T + 1) \\
&\quad (7^8T^{16} + \cdots + 10T + 1),
\end{aligned}$$

suggesting the $\mathbb{Q}$-isogeny decomposition of the Jacobian has shape 2-2-2-8. Hashing traces and searching for 5-power conductor genus 2 curves yields

$$\begin{aligned}
y^2 + (x^3 + x + 1)y &= -3x^4 + 7x^3 + x^2 - 5x + 1, \\
y^2 + (x^3 + x + 1)y &= x^6 - 13x^4 + 37x^3 + 6x^2 - 23x + 6, \\
y^2 + (x^3 + x + 1)y &= 6x^6 - 5x^5 + 12x^4 - 13x^3 + 6x^2 - 13x - 4,
\end{aligned}$$

each of which have RM by $\mathbb{Q}(\sqrt{5})$ and Jacobians of Mordell-Weil rank 2.

Complexity analysis

We can use sub-exponential time Monte-Carlo algorithms to compute class numbers and still get a provably correct result (in practice we just look up class numbers in a precomputed table).

As written, the complexity of this algorithm is

$$N^{4+o(1)} + q^{1/2+o(1)} N^{o(1)}.$$

The constant factors are very small (the inner loop is just table lookups). The dependency on N can easily be improved to $N^{3+o(1)}$, and even to $N^{2+o(1)}$ for suitable H.

If we wish to compute $\#X_H(\mathbb{F}_q)$ for many values of q (for example, all primes $p \nmid N$ up to some bound B), the computation of $f_H\colon\ \mathrm{GL}_2(N) \to \mathbb{Z}$ only needs to be done once, and we can precompute all the class numbers up to $4B$ in $O(B^{3/2+o(1)})$ time (deterministically) by counting binary quadratic forms.

Corollary: We can compute $L(X_H, s)$ in time $\mathrm{cond}(\mathrm{Jac}(X_H))^{3/4+o(1)}$.

Performance comparison

Time to compute $\#X_0(N)(\mathbb{F}_p)$ for all primes $p \leq B$.

	Pari/GP v2.11				new algorithm			
B	$N = 41$	42	209	210	$N = 41$	42	209	210
2^{12}	0.1	0.4	0.2	0.7	0.0	0.0	0.0	0.0
2^{13}	0.3	1.0	0.5	1.8	0.0	0.0	0.1	0.0
2^{14}	0.6	2.5	1.1	4.8	0.1	0.1	0.1	0.1
2^{15}	1.7	7.1	3.1	12.8	0.2	0.2	0.2	0.2
2^{16}	4.8	19.6	8.9	35.4	0.4	0.4	0.6	0.5
2^{17}	14.4	55.1	25.7	97.8	1.1	0.9	1.5	1.2
2^{18}	43.5	156	74.3	274	2.8	2.6	4.0	3.3
2^{19}	128	442	214	769	7.8	7.0	11.0 1	9.1
2^{20}	374	1260	610	2169	22.2	19.8	31.1	26.2
2^{21}	1100	3610	1760	6100	69.0	61.3	91.8	77.9
2^{22}	?	?	?	?	213	187	263	228
2^{23}	?	?	?	?	665	579	762	678
2^{24}	?	?	?	?	2060	1790	2220	1990

Intel Skylake 3.1 GHz CPU times (seconds)

(? entries did not complete within one day)

Zeta functions and L-functions

Let $X/\mathbb{Q}$ be a nice (smooth, projective, geometrically integral) curve of genus g. For primes p of good reduction (for X) we have a zeta function

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

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

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

here $\chi_p(T)$ is the charpoly of the Frobenius endomorphism of $\operatorname{Jac}(X_p)$ (this implies $\#\operatorname{Jac}(X_p) = L_p(1)$, for example). The L-function of X is

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

where the Dirichlet coefficients $a_n \in \mathbb{Z}$ are determined by the $L_p(T)$.
In particular, $a_p = p + 1 - \#X_p(\mathbb{F}_p)$ is the trace of Frobenius.

The Selberg class with polynomial Euler factors

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

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 $\epsilon > 0$ (Ramanujan conjecture).
4. $L(s)$ has an Euler product $L(s) = \prod_p L_p(p^{-s})^{-1}$ in which each local factor $L_p \in \mathbb{Z}[T]$ has degree at most $\deg L$.

For any nice curve X the Dirichlet series $L_{\text{an}}(s, X) := L(X, s + \frac{1}{2})$ satisfies both (3) and (4) (by Weil), and conjecturally lies in S^{poly}.

For modular curves we also know (1) and (2), so $L(s, X_H) \in S^{\text{poly}}$.

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. In particular, all of the local factors are completely determined by the Frobenius traces a_p at good primes.

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 analytic root number $\varepsilon = \pm 1$ and analytic conductor $N \in \mathbb{Z}_{\geq 1}$ are also determined by the Frobenius traces a_p at good primes.

Effective strong multiplicity one

Fix a finite set of primes $\mathcal{S}$ (e.g. bad primes) 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 know the a_n for all $n \leq c_1\sqrt{M}$ with $p \nmid n$ for $p \in \mathcal{S}$. For a suitably large c_1, exactly one choice of ε, N, and $L_p(T)$ for $p \in \mathcal{S}$ will make it possible for $L(X, s)$ to satisfy its functional equation.

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.

This gives an effective algorithm to compute ε, N, and $L_p(T)$ for $p \in \mathcal{S}$, provided we can compute $L_p(T)$ at good $p \leq B$, where $B = O(\sqrt{N})$.

References

[BS11] G. Bisson and A.V. Sutherland, *Computing the endomorphism ring of an ordinary elliptic curve over a finite field*, J. Number Theory **131** (2011), 815–831.

[DT02] W. Duke and A. Toth, *The splitting of primes in division fields of elliptic curves*, Experimental Mathematics **11** (2002), 555–565.

[RZB15] J. Rouse and D. Zureick-Brown, *Elliptic curves over $\mathbb{Q}$ and 2-adic images of Galois*, Research in Number Theory **1** (2015).

[DR73] P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*, in Modular functions of one variable, II, P. Deligne and W. Kuijk (eds), 143–316, Springer, 1973.

[Se72] J.-P. Serre, *Propriétés galoisiennes des points dordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259–331.

[Su15] A. V. Sutherland, *Computing images of Galois representations attached to elliptic curves*, Forum of Mathematics, Sigma **4** (2016), 79 pages.

[W69] W. C. Waterhouse, *Abelian varieties over finite fields*, Annales scientifique de L'É.N.S **2** (1969), 521–560.

[Z15] D. Zywina, *Possible indices for the Galois image of elliptic curves over $\mathbb{Q}$*, arXiv:1508.07663.