Computational aspects of modular parametrizations of elliptic curves

Hao Chen

University of Washington Ph.D. defense

Advisor: William Stein

April 26, 2016

Plan

1. Critical subgroups of elliptic curves
   - Ellipitc curves and modular curves
   - The critical subgroup and critical polynomials
   - Application of results to $E_{crit}(\mathbb{Q})$
2. q-expansion of newforms at non-unitary cusps
   - Problem description
   - Fourier expansions
   - Computing twists and pseudo-eigenvalues
   - Examples
3. Chow-Heegner points
   - Computing Chow-Heegner points

Elliptic curves over $\mathbb{Q}$

Definition

An **elliptic curve** over $\mathbb{Q}$ is a nonsingular projective curve $E \subseteq \mathbb{P}^2$ with defining equation

$$y^2z = x^3 + Axz^2 + Bz^3,$$

where $A, B \in \mathbb{Q}$ and $4A^3 + 27B^2 \neq 0$.

Theorem (Mordell-Weil)

$E(\mathbb{Q})$ is a finitely generated abelian group, i.e.,

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus T,$$

for some $r \geq 0$ and T finite.

r is called the rank. T is the torsion subgroup.

The BSD conjecture

There is an entire function $L(E, s)$ called the L-function of E.

The rank part of the Birch and Swinnerton-Dyer (BSD) conjecture is:

$$rank(E(\mathbb{Q})) = \operatorname{ord}_{s=1} L(E, s).$$

RHS is the analytic rank, denoted by $r_{an}(E)$.
The BSD conjecture is open when $r_{an}(E) > 1$.

The proof of BSD for $r_{an}(E) = 1$ uses a construction called Heegner points.

Modular curves

Let $N \geq 1$ be an integer, consider the group

$$\Gamma_0(N) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) : N \mid c \right\}.$$

Let $\mathcal{H}^* = \{z \in \mathbb{C} : im(z) > 0\} \cup \mathbb{P}^1\mathbb{Q}$.
$\Gamma_0(N)$ acts on $\mathcal{H}^* = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$.

Definition

$X_0(N) = \Gamma_0(N)\backslash\mathcal{H}^*$.

- $X_0(N)$ has the structure of a nonsingular projective curve.
- Rational functions on $X_0(N)$ are called **modular functions**. They have **q-expansions** at infinity:

$$u(q) = \sum_{n \geq -m} b_n q^n, \; q = e^{2\pi i z}$$

The modularity theorem

Theorem (Modularity)

For every elliptic curve $E/\mathbb{Q}$, there exists an integer $N > 1$ and a surjective morphism $\varphi : X_0(N) \to E$ defined over $\mathbb{Q}$.

- Let $\omega = \omega_{E,\varphi} = \varphi^*(\frac{dx}{y})$. Then ω is a holomorphic differential on $X_0(N)$.
- ω has a q-expansion $\omega = \left(\sum_{n\geq 0} a_n q^n\right) dq$, where the coefficients a_n depend on E. Moreover, there exists an algorithm to compute this q-expansion.
- The smallest N is called the **conductor** of E.
- φ is called a **modular parametrisation**.
  We assume E is optimal, then φ is unique up to sign.
- From now on, we fix the curve E, the conductor N, the differential ω, and the morphism φ.

The critical subgroup $E_{crit}(\mathbb{Q})$

Let $R_\varphi = \sum(e_\varphi(z) - 1)[z]$ be the ramification divisor of φ.

Definition (Mazur, Swinnerton-Dyer)

The **critical subgroup** of E is

$$E_{crit}(\mathbb{Q}) = \langle tr(\varphi([z])) : [z] \in \operatorname{supp} R_\varphi \rangle \subseteq E(\mathbb{Q}),$$

where $tr(P) = \sum_{\sigma:\mathbb{Q}(P)\to\bar{\mathbb{Q}}} P^\sigma$.

- $R_\varphi = \operatorname{div}(\omega)$. In particular, $\deg R_\varphi = 2g(X_0(N)) - 2$.

Question

Is there an elliptic curve $E/\mathbb{Q}$ with $r_{an}(E) \geq 2$ and $\operatorname{rank}(E_{crit}(\mathbb{Q})) > 0$?

Critical j-polynomial

Plan: investigate $E_{crit}(\mathbb{Q})$ by studying the 'critical j-polynomial' attached to $\mathrm{div}(\omega)$.

Definition

Write $\mathrm{div}(\omega) = \sum n_z[z]$. The **critical j-polynomial** of E is

$$F_{E,j}(x) = \prod_{z \in \mathrm{supp}\,\mathrm{div}(\omega), j(z) \neq \infty} (x - j(z))^{n_z}.$$

$F_{E,j}(x) \in \mathbb{Q}[x], \deg F_{E,j} \leq 2g - 2$. Equality holds if N is square free. For $h \in \mathbb{Q}(X_0(N))$, can define $F_{E,h}(x)$.

Polynomial Relation (**PR**): a proposition

Let $r, u \in \mathbb{Q}(C)$, a **minimal polynomial relation** of r and u is an irreducible polynomial $P(x, y) \in \mathbb{Q}[x, y]$, such that $P(r, u) = 0$.
Say $P(x, y) = f_n(y)x^n + \cdots + f_1(y)x + f_0(y)$.

Proposition (C.)

If $\mathbb{Q}(C) = \mathbb{Q}(r, u)$ *and* $\gcd(f_0(y), f_n(y)) = 1$*, then*

$$f_0(y) = c \prod_{z \in \mathrm{div}_0(r) \setminus \mathrm{div}_\infty(u)} (y - u(z))^{mult_z(\mathrm{div}_0(r))}.$$

Polynomial Relation: theorem

Let $C = X_0(N)$ and let $dj = j'(z)dz$. Set

$$r = j(j-1728)\frac{\omega}{dj}, \ u = \frac{1}{j}.$$

Then $r, u \in \mathbb{Q}(X_0(N))$, and $\mathrm{div}_0(r) = \mathrm{div}(\omega) + D_0$, where points in supp D_0 have j-value 0 or 1728.

Proposition (C.)

If $T \in \mathbb{Z}_{>0}$ is sufficiently large and $P(x, y) = f_n(y)x^n + \cdots + f_1(y)x + f_0(y)$ is a minimal polynomial relation between rj^T and u, then

$$F_{E,j}(x) = f_0(1/x) \cdot x^A (x - 1728)^B$$

where A, B are integers depending on N, P and T.

Polynomial Relation: algorithm

Algorithm: **PR**

Input: the q-expansion of the modular form f_E attached to E; Output: $F_{E,j}$.

1. $r = \frac{j(j-1728)f_E dz}{dj}$, $u = \frac{1}{j}$.
2. Fix a large M, compute the q-expansions of r and u to q^M.
3. Write $\sum_{\substack{0\le a\le \deg u \\ 0\le b\le \deg r}} c_{a,b} r(q)^a u(q)^b = 0 \pmod{q^M}$ as a linear system on the coefficients $c_{a,b}$.
4. When M is sufficiently large, the linear system has nullity 1. Let $(c_{a,b})$ be a nonzero solution.
5. Set $P(x,y) = \sum c_{a,b} x^a y^b$ and apply the theorem.

Example

$F_{\mathbf{44a},j}(x) = H_{-44}(x)^2$. $F_{\mathbf{37a},j}(x) = H_{-148}(x)$. $F_{\mathbf{37b},j}(x) = H_{-16}(x)^2$.

Remark: When N is large(~ 1000), the algorithm **PR** is slow. We have another faster algorithm that computes a critical h-polynomial, where h is

The critical subgroup $E_{crit}(\mathbb{Q})$

Let $\mathscr{E}_i(N)$ denote the set of elliptic points on $X_0(N)$ of period i, (i = 2,3).

Lemma (C.)

$6P_{all} = -3\sum_{c\in\mathscr{E}_2(N)}\varphi(c) - 4\sum_{d\in\mathscr{E}_3(N)}\varphi(d).$

Theorem (C.)

Suppose $r_{an}(E) \geq 2$, and assume at least one of the following holds:
(1) $F_{E,j} = \prod_{m=1}^{k} H_{D_m}^{s_i} \cdot F_0$, where $\mathbb{Q}(\sqrt{D_m}) \neq \mathbb{Q}(\sqrt{D_n})$ for all $m \neq n$, and F_0 is irreducible.
(2) $F_{E,h}$ is irreducible for some non-constant function $h \in \mathbb{Q}(X_0(N))$.
Then $rank(E_{crit}(\mathbb{Q})) = 0$.

Critical polynomials for elliptic curves of rank 2 and conductor < 1000 (I)

E[1]	$g(X_0(N))$	h	Factorization of $F_{E,h}(x)$
389a	32	j	$H_{-19}(x)^2(x^{60}+\cdots)$
433a	35	j	$x^{68}+\cdots$
446d	55	j	$x^{108}+\cdots$
563a	47	j	$H_{-43}(x)^2(x^{90}-\cdots)$
571b	47	j	$H_{-67}(x)^2(x^{90}-\cdots)$
643a	53	j	$H_{-19}(x)^2(x^{102}-\cdots)$
664a	81	$\frac{\eta_4\eta_8^2\eta_{332}^5}{\eta_{166}\eta_{664}^6\eta_2}$	$x^{160}-\cdots$
655a	65	j	$x^{128}-\cdots$
681c	75	j	$x^{148}-\cdots$
707a	67	j	$x^{132}-\cdots$

[1] We use Cremona's labels for elliptic curves, where the number represents the conductor, and the letter represents the isogeny class.

Critical polynomials for elliptic curves of rank 2 and conductor < 1000 (II)

E	$g(X_0(N))$	h	Factorization of $F_{E,h}(x)$
709a	58	j	$x^{114} - \cdots$
718b	89	j	$H_{-52}(x)^2(x^{172} - \cdots)$
794a	98	j	$H_{-4}(x)^2(x^{192} - \cdots)$
817a	71	j	$x^{140} - \cdots$
916c	113	j	$H_{-12}(x)^8(x^{216} + \cdots)$
944e	115	$\frac{\eta_{16}^4\eta_4^2}{\eta_8^6}$	$x^{224} - \cdots$.[2]
997b	82	j	$H_{-27}(x)^2(x^{160} - \cdots)$
997c	82	j	$x^{162} - \cdots$

[1] Here 4 of the critical points are cusps, so deg $F = 2g - 6$.

Discussion

From the data and the theorems, we conclude:

Corollary

For all elliptic curves E of rank 2 and conductor $N < 1000$, the rank of $E_{crit}(\mathbb{Q}))$ is 0.

Therefore, it seems hard to find an elliptic curve with $r_{an}(E) \geq 2$ and $rank(E_{crit}(\mathbb{Q})) > 0$.

Future work

- Does $F_{E,j}$ always factor into a product of Hilbert class polynomials and one irreducible polynomial?
- What happens if we do the same for $\mathrm{div}(\omega_g)$ for other modular forms g of level N?
- Use **PR** to compute Fourier expansions of newforms at every cusp(work in progress).
- Use **PR** to compute Chow-Heegner points(work in progress).
- Use **PR** to compute Weierstrass points on $X_0(N)$.

Modular forms

Let f be a function $f : \mathcal{H} \to \mathbb{C}$, $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$, and let $k \in \mathbb{Z}$. The weight-k action of α on f is defined by

$$f|[\alpha]_k(z) := (cz + d)^{-k} f(\alpha z).$$

Definition

A **modular form** of weight k and level N is a holomorphic function $f : \mathcal{H} \to \mathbb{C}$ s.t.
(1) $f(z) = f|[\alpha]_k(z), \ \forall \alpha \in \Gamma_0(N)$.
(2) f has holomorphic extension to all cusps of $X_0(N)$.

Cusp forms = modular forms that are zero at all cusps.
Modular forms have **q-expansions**: $f(q) = \sum_{n \geq 0} a_n q^n$, $q = exp(2\pi iz)$.

Hecke

Newforms

Fourier expansion

Idea of computing

Idea (ctnd)

Algorithm for twists

f: a newform of level N. χ: a Dirichlet character modulo N.

$f_\chi(q) = \sum a_n(f)\chi(n)q^n$ is a modular form of level N'.

$f \otimes \chi :=$ the unique newform such that $a_p(f \otimes \chi) = a_p(f_\chi)$ for almost all p. (We call $f \otimes \chi$ the twist of f by χ).

Lemma

Let ϵ be the character of f. Then the level of $f \otimes \chi$ divides $lcm(N, \mathrm{cond}(\epsilon)\,\mathrm{cond}(\chi), \mathrm{cond}(\chi)^2)$.

Lemma

For every $N \geq 1$, there exists an integer $B = B(N)$ such that if g_1, g_2 be two normalised newforms of levels N_1, N_2 dividing N and

$$a_n(g_1) = a_n(g_2), \text{ for all } 1 \leq n \leq B \text{ such that } \gcd(n, N) = 1,$$

then $g_1 = g_2$.

fixme: replace with pseudocode

Algorithm 1 Identifying $f \otimes \chi$

Input: $f \in S_k(\Gamma_1(N), \epsilon)$ a normalized newform; χ – Dirichlet character of prime power conductor $Q = q^{\beta}$; Assume $Q^2 \mid N$.

Output: The newform $f \otimes \chi$.

$Q' := \mathrm{cond}(\chi^2)$; $N_0 := \frac{N}{q^{v_q(N)}}$; $M_0 := Q'N_0$; $t := \frac{N}{M_0} \in \mathbb{Z}$.
for each $d \mid t$ **do**
  Compute a basis $\{g_1^{(d)}, \cdots g_{s_d}^{(d)}\}$ of $S_k(M_0 d, \chi^2)^{new}$.
  $B_d :=$ the Sturm bound for $\Gamma_1(M_0 d q^2)$.
  for $1 \leq j \leq s_d$ **do**
    if $a_n(g_i^{(d)}) = a_n(f)\chi(n)$ for all $1 \leq n \leq B_d, \gcd(n, q) = 1$ **then**
      return $g_i^{(d)}$.
    end if
  end for
end for
return Error.

Computing the pseudo-eigenvalue

Recall that modular symbols are linear combinations of $\{\alpha, \beta\}$, $\alpha, \beta \in \mathbb{Q} \cup \infty$, and we put

$$\langle f, \{\alpha, \beta\} \rangle := \int_{\alpha}^{\beta} f \mathrm{d}z.$$

Lemma

There exists a weight-k modular symbol M be such that $W_N(M) = N^{k/2-1} M^*$. Moreover, if $\langle f, M \rangle \neq 0$, then

$$w(f) = \frac{\langle f, M \rangle}{\overline{\langle f, M \rangle}}.$$

Examples (I)

Example

$E = \mathbf{50a}$. f_E is twist-minimal. Let $\mathfrak{c} = [\frac{1}{10}]$, write $\alpha_0 = 0$ and

$$x^4 + x^3 + x^2 - x + \frac{1}{5} = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)(x - \alpha_4).$$

Then

$$f_{\mathfrak{c}}(q) = \sum_{n \geq 1} \alpha_{n \mod 5} a_n(f) q^n.$$

Example

Let $E = \mathbf{48a}$ and let $\mathfrak{c} = \left[\frac{1}{12}\right]$. We computed that

$$f_{\mathfrak{c}}(q) = -2iq^2 + 2iq^6 + O(q^7).$$

Since the first coefficient vanishes, we conclude that the modular parametrization $\varphi : X_0(48) \to E$ is ramified at the cusp $\mathfrak{c}$.

Examples (II)

Definition

A newform f is *twist-minimal* if it is not a twist of a newform of lower level.

Example

Let $E = \mathbf{98a}$ and $\mathfrak{c} = [\frac{1}{14}]$. Then f_E is not twist-minimal. More precisely, if χ is the quadratic character modulo 7, then

$$f \otimes \chi(q) = q - q^2 - 2q^3 + q^4 + O(q^6)$$

is a newform of level 14. We computed numerically that

$$\begin{aligned} f_{\mathfrak{c}}(q) = {} & (-0.755 - 0.172i)\, q + (0.441 - 0.916i)\, q^2 + (1.392 + 1.110i)\, q^3 \\ & + (0.696 - 0.555i)\, q^4 + (1.510 - 0.344i)\, q^6 - 3.023iq^7 + O(q^8) \end{aligned}$$

Further work

Assume $E/\mathbb{Q}$, $f = f_E$ is minimal by twist.

- relation to automorphic side:
  psuedo-eigenvalues relates to epsilon factors of $\pi_{f\otimes\chi}$. Another way to determine the local components of π_f.
- Let $\mathfrak{c}$ be a cusp of prime denominator $p \geq 5$. Seems that $a_1(f_{\mathfrak{c}})$ is only divisible by primes that are $\pm 1 \mod p$. Can we prove this?

Definition: Chow-Heegner points

Even index of Chow-Heegner points

Darmon et al. , Stein

asdf

My algorithm and an example

Future work

Thank you!