Computational aspects of modular parametrizations of elliptic curves

Hao Chen

University of Washington Ph.D. defense

Advisor: William Stein

April 26, 2016

Overview

1. Computing the critical subgroups of elliptic curves
2. q-expansion of newforms at non-unitary cusps
3. Chow-Heegner points

Plan

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 $4A^3 + 27B^2 \neq 0$.

For any field extension $K/\mathbb{Q}$, the points on E with coordinates in K, denoted by $E(K)$, form an abelian group.

Theorem (Mordell-Weil)

$E(\mathbb{Q})$ is finitely generated, i.e., $E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus E(\mathbb{Q})_{tors}$, where $r \in \mathbb{Z}_{\geq 0}$ is the **rank** *of $E(\mathbb{Q})$, and $E(\mathbb{Q})_{tors}$ is a finite group, called the* **torsion subgroup** *of $E(\mathbb{Q})$.*

The BSD conjecture

For every elliptic curve $E/\mathbb{Q}$, there is an analytic function $L(E, s)$ in the complex variable s, called the L-function of E. The rank part of the **Birch and Swinnerton-Dyer (BSD) conjecture** is:

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

LHS is the **algebraic rank**, RHS is the **analytic rank**, denoted by $r_{an}(E)$.

The BSD conjecture is still open when $r_{an}(E) > 1$.

The proof of BSD for $r_{an}(E) = 1$ uses **Heegner points** on **modular curves**.

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 $\mathcal{H} = \{z \in \mathbb{C} : im(z) > 0\}$ be the complex upper half plane.

The group $\Gamma_0(N)$ acts on the extended upper half plane $\mathcal{H}^* = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$ by $\left(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right), z \right) \mapsto \frac{az+b}{cz+d}$.

Definition

The **Modular Curve** $X_0(N)$ is the quotient space of $\mathcal{H}^*$ under the $\Gamma_0(N)$-action.

- $X_0(N)$ is a compact Riemann surface.
- If $z \in \mathcal{H}^*$, we use the symbol $[z]$ to denote the corresponding point on $X_0(N)$.

Modular functions

- $X_0(N)$ is a nonsingular projective curve defined over $\mathbb{Q}$.
- Rational functions on $X_0(N)$ are called **modular functions**. Each modular function has a **q-expansion** at $[\infty]$:

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

  which follows from $u(z+1) = u(z)$.
- The **j-invariant** is a modular function on $X_0(N)$ for every N, with q-expansion

$$j(q) = q^{-1} + 744 + 196884q + \cdots .$$

  From now on, the letter j means the j-invariant.
- If $\omega_1, \omega_2 \neq 0$ are differential forms on $X_0(N)$, then $\frac{\omega_1}{\omega_2}$ is a modular function.

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.

Heegner points

For an imaginary quadratic order $\mathcal{O} = \mathcal{O}_D$ of discriminant $D < 0$, let $H_D(x)$ denote its **Hilbert class polynomial**.

Definition

A point $[z] \in X_0(N)$ is a **"generalized Heegner point"** if there exists D s.t. $H_D(j(z)) = H_D(j(Nz)) = 0$. If in addition, $(D, 2N) = 1$, then $[z]$ is a **Heegner point**.

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

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

Points in $\operatorname{supp} R_\varphi$ are called **critical points** in this talk.

Definition (Mazur, Swinnerton-Dyer)

The **critical subgroup** of E is

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

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

- $E_{crit}(\mathbb{Q})$ is a subgroup of $E(\mathbb{Q})$.
- $R_\varphi = \operatorname{div}(\omega)$. In particular, $\deg R_\varphi = 2g(X_0(N)) - 2$.
- From now on, we use the notation $\operatorname{div}(\omega)$ instead of R_φ.

Motivation

Why consider the critical subgroup?

Theorem

(1) If $r_{an}(E) = 1$, then there exists a Heegner point $[z]$ on $X_0(N)$ such that $tr(\varphi([z])) \in E(\mathbb{Q})$ has infinite order.
(2) If $r_{an}(E) \geq 2$, then $tr(\varphi([z])) \in E(\mathbb{Q})_{tors}$ for every "generalized Heegner point" $[z]$ on $X_0(N)$.

- Part (1) is essential to the proof of BSD for $r_{an}(E) = 1$.
- When $r_{an}(E) \geq 2$, one can not obtain a non-torsion point using Heegner points.

What if we use critical points? A natural question is

Question

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

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.
- If $h \in \mathbb{Q}(X_0(N))$ is a non-constant function, then $F_{E,h}(x)$ is defined similarly.

What next? We will give an algorithm to compute $F_{E,j}$.

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

Fact: Let $C/\mathbb{Q}$ be a nonsingular projective curve, $r \in \mathbb{Q}(C)$ be a non-constant function, then $[\mathbb{Q}(C) : \mathbb{Q}(r)] = \deg r$.

Let r, u be non-constant functions on C, a **minimal polynomial relation** of r and u is an irreducible polynomial $P(x, y) \in \mathbb{Q}[x, y]$, with $\deg_x(P) \leq \deg u, \deg_y(P) \leq \deg r$, such that $P(r, u) = 0$.

Remark: The minimal polynomial relation always exists and is unique up to multiplication by a constant.
Write $\mathrm{div}(r) = \sum n_z[z]$ and $P(x, y) = f_n(y)x^n + \cdots + f_1(y)x + f_0(y)$.

Proposition (C.)

If $\mathbb{Q}(C) = \mathbb{Q}(r, u)$ *and* $\gcd(f_0(y), f_n(y)) = 1$, *then there is a constant* $c \neq 0$ *s.t.*

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

Polynomial Relation: a proposition (II)

Recall the proposition just stated.

Proposition (C.)

If $\mathbb{Q}(C) = \mathbb{Q}(r, u)$ *and* $\gcd(f_0(y), f_n(y)) = 1$, *then there is a constant* $c \neq 0$ *s.t.*

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

- The right hand side 'looks like a critical polynomial'.
- We will apply the proposition to compute $F_{E,j}$.

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 $\mathrm{supp}\, D_0$ have j-value 0 or 1728.

Theorem (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 $E_{crit}(\mathbb{Q})$: preliminaries

Recall the definition $E_{crit}(\mathbb{Q}) = \langle tr(\varphi([z])) : [z] \in \operatorname{supp} \operatorname{div}(\omega) \rangle$.

Let n_ω denote the number of Galois orbits of $\operatorname{div}(\omega)$.

Fact

$rank(E_{crit}(\mathbb{Q})) \leq n_\omega$.

Reason: to generate $E_{crit}(\mathbb{Q})$, it suffices to take one representative from each Galois orbit of $\operatorname{supp} \operatorname{div}(\omega)$.

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

Definition

Let $[z] \in X_0(N)$, the **period** of $[z]$ is $m_z := \frac{1}{2}|\{\alpha \in \Gamma_0(N) : \alpha(z) = z\}|$. If $m_z > 1$, then $[z]$ is an **elliptic point**.

- elliptic points have period 2 or 3.
- the set of elliptic points is finite and Galois invariant.
- elliptic points are Heegner points.

Let $P_{all} = \sum_{z \in \text{supp div}(\omega)} n_z \varphi([z])$. The point P_{all} is a linear combination of the defining generators of $E_{crit}(\mathbb{Q})$.

Let $E_i(N)$ denote the set of elliptic points on $X_0(N)$ of period i, (i = 2,3).

Lemma (C.)

$6P_{all} = -3\sum_{c \in E_2(N)} \varphi(c) - 4\sum_{d \in E_3(N)} \varphi(d)$.

[1] The set of elliptic points can be empty: for example, it happens when $36 \mid N$. It is not always empty, though, since if $k^2 + 1 \equiv 0 \pmod{N}$ then $i/(ki+1)$ is an elliptic

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

Proposition (C.)

Assume either $r_{an}(E) \geq 2$ or $X_0(N)$ has no elliptic point. Then $P_{all} \in E(\mathbb{Q})_{tors}$, hence $rank(E_{crit}(\mathbb{Q})) \leq n_\omega - 1$.

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 $rank(E_{crit}(\mathbb{Q})) = 0$.

- We make the assumptions of this theorem based on the outputs of the **PR** algorithm.
- The proof uses the theorem we introduced on trace of Heegner points.

Motivation (II)

As of now, the only result in the literature on $E_{crit}(\mathbb{Q})$ where $r_{an}(E) \geq 2$ is the work of C.Delaunay in 2002, in his Ph.D. thesis. He computed the divisor $\mathrm{div}(\omega)$ numerically for $E = \mathbf{389a}$, the first elliptic curve of rank 2 over $\mathbb{Q}$.

We quote from Delaunay's paper:
"More astonishing, 2 critical points(for **389a**) are Heegner points. $\cdots$ It also appears that $E(\mathbb{Q})^{crit}$ is a torsion subgroup."

One of my goals is to *prove* this statement for **389a** and investigate the critical subgroup of other elliptic curves.

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 $rank(E_{crit}(\mathbb{Q})) > 0$.

However, all is not lost. Some 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 $X_0(N)$.

Thank you!

Constants A and B in the theorem

$A = \deg f_n - d_N \cdot T - \frac{1}{3}(d_N + 2\epsilon_3(N))$, $B = -\frac{1}{2}(d_N + \epsilon_2(N))$.
$d_N = [SL_2(\mathbb{Z}) : \Gamma_0(N)]$, $\epsilon_i(N) =$ number of of elliptic points of period i on $X_0(N)$(i = 2,3).

Click me to go back

The algorithm **Y**ang **P**air

Click me to go back

Issue: **IPR** is inefficient when N large. So we introduce the algorithm Yang pair.

- It does *not* compute $F_{E,j}$. Instead, computes $F_{E,h}$.
- $h \in \mathbb{Q}(X_0(N))$ is chosen within the algorithm.
- It is fast and space-efficient.

Definition (Y.Yang)

Two functions $s, t \in \mathbb{Q}(X_0(N))$ form a **Yang pair** if $\mathrm{div}_\infty(s) = m[\infty]$, $\mathrm{div}_\infty(t) = n[\infty]$ and $gcd(m, n) = 1$.

- Finding polynomial relation of a Yang pair is fast: use a variant of 'recursive pole cancellation'.
- Moreover, any Yang pair (h, h') satisfies the assumptions of our proposition.

Hence if we can find $h_1, h_2 \in \mathbb{Q}(X_0(N))$ s.t. (1) (rh_1, h_2) form a Yang pair; (2) $\mathrm{div}(h_1)$ is known, then we can compute $F_{E,r}$.

Use η-products to construct Yang pairs

η products $=$ modular function on $X_0(N)$ of the form $\prod_{d|N} \eta(dz)^{r_d}$.

Fact (Ligozat + SAGE)

For every divisor $D \geq 0$ supported on cusps, there exists an explicitly computable η product h s.t. $\mathrm{div}(h) = D + D' - m[\infty], D' \geq 0$.

Using this fact , one can find two η products h_1,h_2 s.t.
(1) $r_1 = rh_1$ has only pole at $[\infty]$.
(2) $\mathrm{div}_0(h_2) \geq \mathrm{div}_\infty(j) - [\infty]$.
Now either (rh_1, h_2) or (rh_1, jh_2) is a Yang pair.

Example

$E =$ **664a** with rank $= 2$, use $h_2 = \frac{\eta_4 \eta_8^2 \eta_{332}^5}{\eta_{166} \eta_{664}^6 \eta_2}$.
$F_{E,h_2}(x) = x^{160} - 14434914...196444x^{158} - \cdots$ is irreducible.

Click me to go back

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**: $f(q) = \sum_{n \geq 0} a_n q^n$, $q = exp(2\pi i z)$.

Hecke

Newforms

Fourier expansion

Idea of computing

Idea (ctnd)

Algorithm for twists

Algorithm for pseudo-eigenvalue

Examples (I)

Examples (II)

Darmon et al. , Stein

asdf

My algorithm

An example

Future work