# Computational aspects of modular parametrizations of elliptic curves

Hao Chen

University of Washington Ph.D. defense

Advisor: William Stein

April 26, 2016

# Part I: Critical subgroups of elliptic curves

## Definition

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

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

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

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

- $\operatorname{ord}_{s=1} L(E, s)$ is called the analytic rank, denoted by $r_{an}(E)$.
- The BSD conjecture is open when $r_{an}(E) > 1$.
- The proof of rank BSD for $r_{an}(E) \leq 1$ uses Heegner points.

# Modular curves

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

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

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

**Definition**

$X_0(N) = \Gamma_0(N) \backslash \mathcal{H}^*$ is the modular curve of level $N$.

- $X_0(N)$ is a nonsingular projective curve.

## The modularity theorem

The Modularity Theorem (Breuil, Conrad, Diamond, Taylor) states the existence of an integer $N > 1$ and a surjective morphism $\varphi : X_0(N) \to E$ defined over $\mathbb{Q}$.

The smallest such $N$ is called the conductor of $E$.

Let $\omega = \varphi^*(\frac{dx}{y})$. Then

$$\omega = cf(z)\mathrm{d}z$$

where $f$ is the modular form attached to $E$.

We assume $E$ is optimal. Then $\varphi$ is unique up to sign.

# Motivation: find rational points on $E$

Idea: use $\varphi$ to find rational points on $E$ from special points on $X_0(N)$.

- Rational points on $X_0(N)$ – usually cusps, so only get torsion points.
- Heegner points. – Great for $r_{an}(E) = 1$. Always torsion when $r_{an}(E) \geq 2$.
- Ramification points – probably always torsion when $r_{an}(E)$ is even.
- Others??

Up to now, there is no known construction of points of infinite order on elliptic curves with analytic rank at least 2!

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

Observation: if $K$ is a number field and $P \in E(K)$, then we can "trace down to $\mathbb{Q}$". That is, The point $tr(P) := \sum_{\sigma:\mathbb{Q}(P)\to\bar{\mathbb{Q}}} P^\sigma$ is in $E(\mathbb{Q})$.

**Definition (Mazur, Swinnerton-Dyer)**

The critical subgroup of $E$, denoted by $E_{crit}(\mathbb{Q})$, is the group generated by traces of images of ramification points of $\varphi$.

**Question (Mazur and Swinnerton-Dyer, 1974)**

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

**Theorem (C.)**

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

To prove this, we compute $E_{crit}(\mathbb{Q})$ for each curve.

# Critical $j$-polynomial

To help compute $E_{crit}(\mathbb{Q})$, we make the following definition.

**Definition**

The critical j-polynomial of $E$ is

$$F_{E,j}(x) = \prod_{z \in Y_0(N)} (x - j(z))^{mult_{Ram(\varphi)}(z)}.$$

We have $F_{E,j}(x) \in \mathbb{Q}[x]$ and $\deg F_{E,j} \leq 2g - 2$.

For $h \in \mathbb{Q}(X_0(N))$, can define $F_{E,h}(x)$.

**Example**

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

Here $H_d$ is the Hilbert class polynomial of disc $d$.

# Computing $F_{E,j}$

Idea: use the fact that $Ram(\varphi) = Div(\omega)$. Take two rational functions $r := (j - 1728)\frac{\omega}{dj}$, $u := \frac{1}{j}$ on $X_0(N)$.

**Proposition (C.)**

*For $T \gg 0$, let $P(x, y) = f_n(y)x^n + \cdots + f_1(y)x + f_0(y)$ be an irreducible polynomial over $\mathbb{Q}$, such that $P(u, rj^T) = 0$. Then*

$$F_{E,j}(x) = P\left(\frac{1}{x}, 0\right) \cdot x^A(x - 1728)^B$$

*where $A, B$ are explicitly computable.*

Hence, it suffices to compute the polynomial $P$, which can be done using linear algebra, given the $q$-expansions of $r$ and $u$.

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

**Theorem (C.)**

*Suppose the analytic rank of $E$ is at least 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 $\mathrm{rank}(E_{crit}(\mathbb{Q})) = 0$. In other words, the critical subgroup does not contain points of infinite order.*

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

| $E$ | $g(X_0(N))$ | $h$ | 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 | $j$ | $x^{132}-\cdots$ |

# 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 | $\frac{\eta_{16}^4\eta_4^2}{\eta_8^6}$ | $x^{224} - \cdots$.[1] |
| 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

Future work:

- Compute $E_{crit}(\mathbb{Q})$ for $E = \mathbf{5077a}$.
  Current method will take roughly 230 days (parallel computation using 64 cpus).
- Prove there are infinitely many elliptic curves with rank 2 such that the critical subgroup is torsion.

# Part II: $q$-expansion of newforms at all cusps

Why study $q$-expansion of newforms at all cusps? (The theory of expansion at the cusp $\infty$ is well known).

- It gives a direct way to compute the critical subgroup.
- It gives information about the ramification of $\varphi$ at cusps.
- It is useful in computing the Galois representation attached to modular forms.

# 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 $\alpha$ 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: $f(q) = \sum_{n \geq 0} a_n q^n$, $q = exp(2\pi iz)$.

# Newforms and Twists

Let $S_k(N)$ denote the space of cusp forms.

- $S_k(N)$ decomposes in to a direct sum of the old subspace and the new subspace.
- The new subspace has a basis of simultaneous eigenforms for certain operators (Hecke operators). These eigenforms are called newforms.

Also, modular forms attached to elliptic curves over $\mathbb{Q}$ are newforms.
We will focus on newforms from now.

# Fourier expansion

Let $f \in S_k(N)$ be a newform and let $\mathfrak{c} = [\frac{a}{c}] \in X_0(N)$ be a cusp.
Goal: compute the expansion of $f$ at $\mathfrak{c}$. Denote the expansion by $f_{\mathfrak{c}}(q)$.

**Theorem (C.)**

*Let $c' = \frac{N}{c}$. Then*

$$f_{[\frac{a}{c}]}(q) = \frac{w(f)}{\varphi(c')} \sum_{\chi:\mathrm{cond}(\chi)|c'} \chi(-a)R(f,\chi)(q)$$

Here $R(f,\chi)(q)$ is certain power series in $q$, and it can be computed knowing the twist $f \otimes \chi$ and the pseudo-eigenvalue $w(f \otimes \chi)$.

# Examples (I)

**Example**

Let $E = \mathbf{50a}$ and let $f = f_E$. 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

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

where $\bar{n} = n \mod 5 \in \{0, 1, 2, 3, 4\}$.

# Examples (II)

### 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 $\mathfrak{c}$.

### Example

Let $E = \mathbf{98a}$ and $\mathfrak{c} = [\frac{1}{14}]$. We computed numerically that

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

We can use this to deduce that $F_{E,j}$ is not integral at the prime 13.

# Twist of newforms

Let $f$ be a newform on $\Gamma_0(N)$ and $\chi$ be a Dirichlet character of modulus $N$. Then there is a newform $f \otimes \chi$, called the twist of $f$ by $\chi$, on some other group $\Gamma_1(N')$, defined uniquely by

$$a_p(f \otimes \chi) = a_p(f)\chi(p), \text{ for almost all primes } p.$$

# Pseudo-eigenvalue

The Atkin-Lehner involution $W_N$: Let $f$ be a newform on $\Gamma_1(N)$. Then

$$f|W_N = w(f)\bar{f}$$

where $w(f)$ has absolute value 1, and

$$\bar{f} = \sum \overline{a_n(f)} q^n.$$

The number $w(f)$ is called the pseudo-eigenvalue of $f$.

# Algorithm for identifying $f \otimes \chi$

**Lemma (Li)**

*Suppose $f$ is a newform on $\Gamma_0(N)$. Then the level of $f \otimes \chi$ divides $lcm(N, \mathrm{cond}(\chi)^2)$.*

The following lemma is a small modification of the Sturm bound argument.

**Lemma (C.)**

*For every $N \geq 1$, there exists an integer $B$ such that: if $g_1$, $g_2$ are two newforms of levels $N_1, N_2$, both dividing $N$ and*

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

*then $g_1 = g_2$.*

## Computing the pseudo-eigenvalue

Recall that modular symbols are linear combinations of $\{\alpha, \beta\}$, $\alpha, \beta \in \mathbb{Q} \cup \infty$, and we can integrate a modular symbol against a modular form via

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

**Lemma (C.)**

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

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

# Part III: Chow-Heegner points

Motivation: construct rational points on elliptic curves (again).

$$\begin{tikzcd} & X_0(N) \arrow[dl, "\varphi"'] \arrow[dr, "\psi"] & \\ E & & F \end{tikzcd}$$

$E, F$: two non-isogeneous elliptic curves of same conductor $N$.
$\varphi, \psi$: modular parametrisations of $E, F$.
The Chow-Heegner point associated to the pair $(E, F)$ is

$$P_{E,F} = \sum \varphi(\psi^*(Q)), \forall Q \in F(\mathbb{C})$$

Facts: (1) $P_{E,F}$ is independent of the choice of $Q$;
(2) $P_{E,F} \in E(\mathbb{Q})$.

# Even index of Chow-Heegner points

Fact: $P_{E,F}$ is torsion when $r_{an}(E) \geq 2$. What else can be done?
When $E$ has rank 1, numerical evidence suggests that

$$i_{E,F} := [E(\mathbb{Q})/tors : \mathbb{Z}P_{E,F}]$$

is always even, when it is finite.

**Theorem (C.)**

*If*

$$\sigma_0(N) > \log_2(\#E[2](\mathbb{Q}) \cdot F[2](\mathbb{Q})) + 2,$$

*then* $P_{E,F} \in 2E(\mathbb{Q})$.
*In particular, if* $N$ *is divisible by 7 distinct primes , then* $P_{E,F} \in 2E(\mathbb{Q})$.

# Computing Chow-Heegner points: previous work

There exist numerical algorithms to compute Chow-Heegner points.

- Darmon, Daub, Lichtenstein and Rotger – using (complex and $p$-adic) iterated integrals.
- Stein – using complex integration to lift points via modular parametrization.

We have developed an algebraic algorithm to compute the Chow-Heegner points, again using $q$-expansions.

# Example

## Example

$E =$ **89a** and $F =$ **89b**. Let

$$G_1(x) = x^4 + \frac{13}{4}x^3 + \frac{17}{4}x^2 + \frac{21}{4}x + \frac{9}{2} = \prod (x - a_i)$$

and

$$b_i = -\frac{8}{9}a_i^3 - \frac{20}{9}a_i^2 - \frac{28}{9}a_i - \frac{10}{3}.$$

Then $(a_i, b_i) \in E$

$$P_{E,F} = \sum_{i=1}^{4} P_i.$$

We obtain $P_{E,F} = (\frac{3}{4}, -\frac{15}{8})$.

# Future work

- Compute Chow-Heegner points for curves of different conductors.
- Prove that 2 divides $i_{E,F}$ without assumptions on $N$.
- Verify the numerical data of Chow-Heegner points in Stein's table and extend the table.