Computational aspects of modular parametrizations of elliptic curves

Hao Chen

University of Washington Ph.D. defense

Advisor: William Stein

April 26, 2016

1. Critical subgroups of elliptic curves
   - Elliptic curves and modular curves
   - The critical subgroup and critical polynomials
   - Computing the critical subgroup
2. q-expansion of newforms at non-unitary cusps
   - Problem description
3. Chow-Heegner points
   - Even index
   - 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

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

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 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

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

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

Theorem (Modularity (Breuil, Conrad, Taylor fixme))

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 $\mathbb{Q}$.

The smallest 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 φ is unique up to sign.

Idea: use φ to find points on E from special points on $X_0(N)$.
– rational points on $X_0(N)$ – cusps. – Heegner points. – Ramification points. – Others??
Note: up to now, no known construction in ≥ 2.

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

Let $R_\varphi \in Div(X_0(N))$ 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 $tr(P) = \sum_{\sigma:\mathbb{Q}(P)\to\bar{\mathbb{Q}}} P^\sigma$.

Question (Mazur and Swinnerton-Dyer, 1974)

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

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

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

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

$F_{E,j}(x) \in \mathbb{Q}[x]$ and $\deg F_{E,j} \leq 2g - 2$ (equality holds if N is square free).

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

Let H_d be the Hilbert class polynomial of disc d.

Example

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

Polynomial Relation (I)

Let

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

Take $T \gg 0$ and let $P(x,y) = f_n(y)x^n + \cdots + f_1(y)x + f_0(y)$ be irreducible and such that $P(u, rj^T) = 0$.

Proposition (C.)

Then

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

where A, B are explicitly computable.

So it suffices to compute the polynomial P. We can compute P using linear algebra, given the q-expansions of r and u.

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

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	$g(X_0(N))$	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 $E =$ **5077a**.
  Current method will take roughly 5500/(number of cpus) hours.
- Prove or disprove that $\text{rank}(E_{crit}(\mathbb{Q})) = 0$ whenever $r_{an}(E)$ is even.
  (For infinitely many?)

q-expansion of newforms at non-unitary cusps

Motivation:

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) $f(z) = f|[\alpha]_k(z), \ \forall \alpha \in \Gamma_0(N)$ $(\Gamma_1(N))$.
(2) f has holomorphic extension to all cusps of $X_0(N)$ $(X_1(N))$.

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

Operators on modular forms

- Hecke operators: a family $\{T_n, n \geq 1\} \cup \{\langle d \rangle : (d, N) = 1\}$ of commuting linear operators on $S_k(N)$.
- B_d and U_d operators: $B_d(\sum a_n q^n) = \sum a_n q^{nd}$, $U_d(\sum a_n q^n) = \sum a_{nd} q^n$.
- The Atkin-Lehner involution W_N. If f is a newform on $\Gamma_1(N)$, then

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

$w(f) \in \mathbb{C}_1$ is called the pseudo-eigenvalue of f.

Newforms

- $S_k(N) = S_k(N)^{old} \oplus S_k(N)^{new}$.
- $S_k(N)^{new}$ has a basis of simultaneous eigenforms for all Hecke operators. These eigenforms are called newforms.

Fourier expansion

Let $f \in S_k(\Gamma_0(N))$ be a newform and let

$$\mathfrak{c} = [\frac{a}{c}] \in X_0(N)$$

be a cusp. Goal: compute the expansion of f at $\mathfrak{c}$. First, the expansion is only well-defined for $denom(\mathfrak{c})^2 \mid N$.
Let's denote the expansion by $f_{\mathfrak{c}}(q)$. Let $c' = \frac{N}{c}$.

Theorem (C.)

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

Here $R(f,\chi)(q)$ can be computed knowing $f \otimes \chi$ and $w(f \otimes \chi)$.

Algorithm for identifying $f \otimes \chi$

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 $g_1 = g_2$.

Algorithm to compute $f \otimes \chi$

Algorithm 1 Identifying $f \otimes \chi$

Input: $f \in S_k(\Gamma_0(N))$ a normalized newform; χ – Dirichlet character of prime power conductor $Q = q^\beta$ $(Q^2 \mid N)$.
Output: The newform $f \otimes \chi$.

  for each $M \mid N$ **do**
    Compute a basis $\{g_1, \ldots, g_s\}$ of $S_k(M, \chi^2)^{new}$.
    $B :=$ the Sturm bound for $\Gamma_1(MQ^2)$.
    for $1 \leq j \leq s$ **do**
      if $a_n(g_i) = a_n(f)\chi(n)$ for all $1 \leq n \leq B, \gcd(n, q) = 1$ **then**
        return g_i.
      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 (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

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

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

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

Chow-Heegner points

1. Critical subgroups of elliptic curves
   - Elliptic curves and modular curves
   - The critical subgroup and critical polynomials
   - Computing the critical subgroup
2. q-expansion of newforms at non-unitary cusps
   - Problem description
3. Chow-Heegner points
   - Even index
   - Computing Chow-Heegner points

Definition: Chow-Heegner points

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

E, F: two non-isogeneous elliptic curves of same conductor N.
φ, ψ: 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 $r_{an}(E) \geq 2$.
When E has rank 1, numerical evidence suggests that the index $i_{E,F} := [E(\mathbb{Q})/tors : \mathbb{Z}P_{E,F}]$ is even, when it is finite.

Theorem (C.)

Let $\sigma_0(N)$ denote the number of distinct prime factors of N. If

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

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

$E = \mathbf{89a}$ and $F = \mathbf{89b}$. 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

$$P_{E,F} = \sum_{i=1}^{4} P_i, \quad \text{where } P_i = (a_i, b_i).$$

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

Future work

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

Thank you!