

Computational aspects of modular parametrizations of elliptic curves

Hao Chen

University of Washington Ph.D. defense

Advisor: William Stein

April 26, 2016

Critical subgroups of elliptic curves

- 1 Critical subgroups of elliptic curves
 - Elliptic 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
 - Computing twists and pseudo-eigenvalues
 - Examples
- 3 Chow-Heegner points: a preliminary study
 - 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:

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

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

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

The proof of rank BSD for $r_{an}(E) \leq 1$ uses Heegner points.

Modular curves

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

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

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

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:

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

The modularity theorem

Theorem (Modularity)

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

The smallest N is called the conductor of E .

Let $\omega = \varphi^*\left(\frac{dx}{y}\right)$. Then $\omega = cf(z)dz$, 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 .

– rational points on $X_0(N)$ – cusps. – Heegner points. – Ramification points. – Others??

Note up to now, there is no known construction in ≥ 2 .

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

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

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

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

Question (Mazur and Swinnerton-Dyer, 1974)

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

Critical j -polynomial

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

Definition

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

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

$F_{E,j}(x) \in \mathbb{Q}[x]$ 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 $F_{E,h}(x)$.

Polynomial Relation (I)

Let C be a curve and 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 $P(x, y) = f_n(y)x^n + \cdots + f_1(y)x + f_0(y)$.

Lemma (C.)

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

$$f_0(y) = c \prod_{z \in \text{supp div}_0(r) \setminus \text{supp div}_\infty(u)} (y - u(z))^{\text{mult}_z(\text{div}_0(r))}.$$

Polynomial Relation (II)

Set

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

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

Proposition (C.)

For $T \gg 0$, let $P(x, y) = f_n(y)x^n + \cdots + f_1(y)x + f_0(y)$ be a minimal polynomial relation of ry^T and u . Then

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

where A, B are explicitly computable.

The Algorithm

Input: The newform f_E attached to elliptic curve E/\mathbb{Q} ;

Output: $F_{E,j}$.

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

Compute the q -expansions of r and u to precision q^M .

Solve the linear equations $\sum c_{a,b} r(q)^a u(q)^b = 0 \pmod{q^M}$ for $c_{a,b}$.

Set $P(x, y) = \sum c_{a,b} x^a y^b$ and apply the proposition.

(Fixme: define H_d).

Example

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

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

For $i = 2, 3$, let $\mathcal{E}_i(N)$ be the set of elliptic points on $X_0(N)$ of period i .
(Fixme: informally define elliptic points).

(Fixme: P_{all} is not defined).

Lemma (C.)

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

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

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	$H_{-19}(x)^2(x^{60} + \dots)$
433a	35	j	$x^{68} + \dots$
446d	55	j	$x^{108} + \dots$
563a	47	j	$H_{-43}(x)^2(x^{90} - \dots)$
571b	47	j	$H_{-67}(x)^2(x^{90} - \dots)$
643a	53	j	$H_{-19}(x)^2(x^{102} - \dots)$
664a	81	$\frac{\eta_4 \eta_8^2 \eta_{332}^5}{\eta_{166} \eta_{664}^6 \eta_2}$	$x^{160} - \dots$
655a	65	j	$x^{128} - \dots$
681c	75	j	$x^{148} - \dots$
707a	67	j	$x^{132} - \dots$

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	$x^{114} - \dots$
718b	89	j	$H_{-52}(x)^2(x^{172} - \dots)$
794a	98	j	$H_{-4}(x)^2(x^{192} - \dots)$
817a	71	j	$x^{140} - \dots$
916c	113	j	$H_{-12}(x)^8(x^{216} + \dots)$
944e	115	$\frac{\eta_{16}^4 \eta_4^2}{\eta_8^6}$	$x^{224} - \dots$ ¹
997b	82	j	$H_{-27}(x)^2(x^{160} - \dots)$
997c	82	j	$x^{162} - \dots$

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

Corollary

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

Future work:

- Compute $E_{crit}(\mathbb{Q})$ for $E = \mathbf{5077a}$. (Fixme: have a time estimate).
- 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

- 1 Critical subgroups of elliptic curves
 - Elliptic 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
 - Computing twists and pseudo-eigenvalues
 - Examples
- 3 Chow-Heegner points: a preliminary study
 - Computing Chow-Heegner points

Modular forms

Let f be a function $f : \mathcal{H} \rightarrow \mathbb{C}$, $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, 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 $f : \mathcal{H} \rightarrow \mathbb{C}$ 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 .

- When $M \mid N$, \exists degeneracy maps $S_k(M) \rightarrow S_k(N)$.
- Old subspace = span of images of all degeneracy maps.
- New subspace = (Old subspace) $^\perp$.
- $S_k(N)^{new}$ 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 $\mathfrak{c} \in X_0(N)$ be a cusp other than ∞ .

Goal: compute the expansion of f at \mathfrak{c} .

First, only well-defined for $\text{denom}(\mathfrak{c})^2 \mid N$.

Equivalent to computing the expansion of

$$f \mid \left[\begin{pmatrix} 1 & 0 \\ Id & 1 \end{pmatrix} \right]$$

at ∞ for all $d^2 \mid N, l \in (\mathbb{Z}/N\mathbb{Z})^\times$.

Idea of computing

Let $S'_c = \begin{pmatrix} 1 & \frac{1}{c'} \\ 0 & 1 \end{pmatrix}$ and $A'_c = \begin{pmatrix} 1 & 0 \\ c' & 1 \end{pmatrix}$. Then

$$A_c^{-u} = W_N S'_c{}^u W_N, \forall u \in \mathbb{Z}.$$

For a character χ modulo c' , put

$$f|R_\chi(c') := \sum_{u=0}^{c'-1} \bar{\chi}(u) f|S'_c{}^u.$$

$f|R_\chi(\text{cond } \chi) = g(\bar{\chi})f_\chi$. ($f_\chi(q) = \sum a_n(f)\chi(n)q^n$ is a modular form of level N' .) We have

$$\varphi(c')A_c^{-a} = \sum_{\text{cond}(\chi)|c'} \chi(a)W_N R_\chi(c')W_N. \quad (2.1)$$

Applying to f , we arrive at

$$\boxed{f_{[\frac{a}{c}]}(q) = \frac{w(f)}{\varphi(c')} \sum_{\text{cond}(\chi)|c'} \chi(-a) f|R_\chi(c')W_N.} \quad (2.2)$$

Idea (ctnd)

It suffices to compute the expansions of each $f|R_\chi(c')W_N$ in the sum.
 $f \otimes \chi :=$ 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**).
If $c' = \text{cond}(\chi)$ and $f_\chi = f \otimes \chi$, then $f|R_\chi(c')W_N = w(f \otimes \chi)f_\chi$.

Otherwise, $f_\chi = (f \otimes \chi)|(1 - U_d|B_d)$, and we use

Lemma

$$f|B_d|W_N = \left(\frac{N}{Md^2}\right)^{k/2} w(f)(f|B_{\frac{N}{Md}})^*.$$

Conclusion: suffices to compute $f \otimes \chi$ and $w(f \otimes \chi)$.

Algorithm for twists

Lemma

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

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 $\{g_1, \dots, g_s\}$ of $S_k(M, \chi^2)^{new}$.

$B :=$ the Sturm bound for $\Gamma_1(MQ^2)$.

for $1 \leq j \leq s$ **do**

if $a_n(g_j) = a_n(f)\chi(n)$ for all $1 \leq n \leq B, \gcd(n, q) = 1$ **then**

return g_j .

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

$$\langle f, \{\alpha, \beta\} \rangle := \int_{\alpha}^{\beta} f dz.$$

Lemma (C.)

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*

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

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

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

Example

Let $E = \mathbf{48a}$ and let $\mathfrak{c} = [\frac{1}{12}]$. 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 $\varphi : X_0(48) \rightarrow E$ 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

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

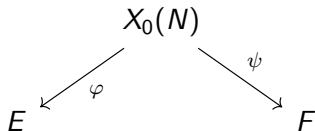
Assume E/\mathbb{Q} , $f = f_E$ is minimal by twist.

- relation to automorphic side:
pseudo-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 $\pm 1 \pmod{p}$. Can we prove this?

Chow-Heegner points: a preliminary study

- 1 Critical subgroups of elliptic curves
 - Elliptic 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
 - Computing twists and pseudo-eigenvalues
 - Examples
- 3 Chow-Heegner points: a preliminary study
 - Computing Chow-Heegner points

Definition: Chow-Heegner points



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

Numerical evidence suggests that the index $i_{E,F}$ is always divisible by 2.

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 $P_{E,F} \in 2E(\mathbb{Q})$.

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.

My algorithm and an example

We present an algorithm that either computes the Chow-Heegner point $P_{E,F}$.

Let x_E, y_E, x_F, y_F be the compositions of φ, ψ with the x and y coordinate functions on E and F , respectively. Note that there exists an algorithm to compute the q -expansions of x_E, x_F, y_E and y_F .

Algorithm: computing Chow-Heegner points

Input: E, F = non-isogeneous elliptic curves of conductor N ; q -expansions of x_E, y_E, x_F, y_F .

Output: $P_{E,F}$.

$u_E := (x_E)^{-1}$ and $u_F := (x_F)^{-1}$.

Compute a polynomial $F(x, y)$ such that $F_{E,F}(u_E, u_F) = 0$.

$f_{ch,x}(x) := F_{E,F}(u_E, 0)$.

Repeat for $v_E = (y_E)^{-1}$ and u_F , get $f_{ch,y}(x)$.

Factor $f_{ch,x} = \prod (x - a_i)$ over $\bar{\mathbb{Q}}$.

for each a_i **do**

if $f_{ch,y}(b_i) = 0$ **then** $P_i = (a_i, b_i)$

else $P_i = -(a_i, b_i)$.

end if

end for

Output $P_{E,F} = \sum_i P_i$.

Example

Example

Consider $E = \mathbf{89a}$ and $F = \mathbf{89b}$. Here $\deg(\varphi) = 2$ and $\deg(\psi) = 5$. Let $D = D_{\varphi,\psi} = \varphi(\psi^*(\infty)) \in \text{div}(E)$. Define $G_1(x) = \prod_{P \in D} (x - x(P))$ and $G_2(y) = \prod_{P \in D} (y - y(P))$. We computed

$$G_1(x) = x^4 + \frac{13}{4}x^3 + \frac{17}{4}x^2 + \frac{21}{4}x + \frac{9}{2}, \quad G_2(y) = y^4 + \frac{1}{8}y^3 + \frac{21}{4}y^2 + \frac{7}{2}y + 3.$$

Write $G_1(x) = \prod (x - a_i)$ with $a_i \in \bar{\mathbb{Q}}$. We found $b_i = -\frac{8}{9}a_i^3 - \frac{20}{9}a_i^2 - \frac{28}{9}a_i - \frac{10}{3}$ is the root of G_2 such that $(a_i, b_i) \in E$. Hence

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

Carrying out the summation, we obtain $P_{E,F} = (\frac{3}{4}, -\frac{15}{8})$.

- Compute Chow-Heegner points for curves of different conductors.
- Prove even index in all cases.
- Verify the data of Chow-Heegner points in Stein's paper and extend the table.

Thank you!