

The Heegner Point Method

Computing Nontorsion Points on Elliptic Curves of Rank One

**David Brown, Iftikhar Burhanuddin,
Wei Ho, Joseph Rabinoff, Patrick Rault**

Arizona Winter School 2006

Many thanks to Henri Cohen, Mark Watkins, William Stein,
Jeremy Teitelbaum, Fernando Rodriguez Villegas, Lisa, Jen,
Dave, Kevin, Jason...

ELLIPTIC CURVES

- Definition:

$E : y^2 = f(x)$ is an **elliptic curve over \mathbb{Q}** if $f(x) \in \mathbb{Q}[x]$ is a cubic polynomial and f has distinct roots.

- Definition:

The **K -rational points of E** , denoted $E(K)$, are the points on E with coordinates in K . We'll consider $K = \mathbb{Q}$ and $K = \mathbb{F}_p$.

- There is a **group law** on the elliptic curve, and for any field K , $E(K)$ is closed under the operation.

RATIONAL POINTS ON E

- Mordell-Weil Theorem: $E(\mathbb{Q})$ is a finitely generated abelian group.
That is, $E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus T$ where r and $|T|$ are finite.
- r is called the algebraic **rank** of E .
- Mazur's Theorem: $|T| \leq 16$.

RATIONAL POINTS ON CURVES: A CLASSIFICATION

Let C be a curve of genus g . Then:

- If $g = 0$, then $C(\mathbb{Q})$ is **Parameterizable** (conic case).
- If $g = 1$, then $C(\mathbb{Q})$ is **Finitely Generated** (elliptic curve case).
- If $g \geq 2$, then $C(\mathbb{Q})$ is **Finite**.

AN ELLIPTIC CURVE AS A TORUS

To an elliptic curve E , we can associate a lattice $\Lambda = \langle \omega_1, \omega_2 \rangle \subset \mathbb{C}$, such that:

- If we define the **Weierstrass \wp -function of Λ** by

$$\wp_{\Lambda}(z) := \frac{1}{z^2} + \sum_{0 \neq \omega \in \Lambda} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right), \text{ then:}$$

- This induces an analytic isomorphism $\mathbb{C}/\Lambda \cong E(\mathbb{C})$ by $z \mapsto (\wp_{\Lambda}(z), \wp'_{\Lambda}(z))$.

L-FUNCTIONS

- Define $a_p := p + 1 - |E(\mathbb{F}_p)|$ and
 $L(E, s) := \prod (1 - a_p p^{-s} + p^{1-2s})^{-1}$ (up to the bad primes)
- The **Conjecture of Birch and Swinnerton-Dyer**, which has been proven up to the constant for rank 0 and 1, says:

$$\lim_{s \rightarrow 1} \frac{L(E, s)}{(s-1)^r} = \frac{\omega_1 \cdot R \cdot (\prod_{p \leq \infty} c_p) \cdot |\text{III}|}{|E(\mathbb{Q})_{tors}|^2}$$

- For analytic rank one curves, i.e., $L(E, 1) = 0$ and $L'(E, 1) \neq 0$, then algebraic rank is also one.

HEEGNER POINT ALGORITHM

- We implement a method to find certain **Heegner points** in $E(\mathbb{Q})$. When the rank of E is 1, these points are **nontorsion**. Unfortunately when the rank is not 1 they are torsion points.
- Our program in **PARI-gp** does the following:
Input: An elliptic curve E defined over \mathbb{Q} .
Output: A rational point in $E(\mathbb{Q})$ which is $\sqrt{|\text{III}|}$ times a generator of the rank one part.

PROGRAM OUTLINE

1. Wei will use the **Modular Parametrization** to shift our study from Elliptic Curves to **Quotients of the Upper Half Plane**,
 $\Gamma_0(N)\backslash\mathcal{H} \rightarrow E(\mathbb{C})$.
2. Joe will use the **magic of Complex Multiplication** to find points in \mathcal{H} which map to points in $E(\mathbb{Q})$.
3. David will use the **magic of Gross-Zagier** to find what to divide by to get the generator.
4. Ifti will describe some further results from implementing our algorithm.

OVERVIEW

- Goal: find a nontorsion rational point on an EC E/\mathbb{Q} .
- Often easier to study families than objects—a **modular curve** is one way to parametrize elliptic curves with extra structure.
- We construct special points on modular curves by **complex multiplication**.
- We then apply the **modular parametrization map** $\Phi : X_0(N) \rightarrow E$ to obtain rational points on E .

MODULAR CURVES: ANALYTIC DESCRIPTION

- $\Gamma_0(N) \subset \mathrm{SL}_2(\mathbb{Z})$: upper-triangular matrices mod N
- $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ acts on the upper half plane \mathcal{H} by

$$\gamma(\tau) = \frac{a\tau + b}{c\tau + d} \quad \text{for } \tau \in \mathcal{H}$$

- We define the level N **modular curve**

$$X_0(N) := \Gamma_0(N) \backslash \mathcal{H} \cup \{\text{cusps}\}$$

i.e., we identify $\tau \in \mathcal{H}$ with $\gamma(\tau)$ for all $\gamma \in \Gamma_0(N)$, and take the compactification.

MODULAR CURVES: ALGEBRAIC STRUCTURE

Because $X_0(N)$ is a compact Riemann surface, it has the algebraic structure of a **complex algebraic curve** over \mathbb{C} .

There's also a **moduli** interpretation:

$$X_0(N) \leftrightarrow \{(E/\mathbb{C}, C) : C \cong \mathbb{Z}/N\mathbb{Z}\} \cup \{\text{cusps}\},$$

i.e., points on $X_0(N)$ parametrize isomorphism classes of elliptic curves over \mathbb{C} with cyclic subgroups of order N .

MODULAR PARAMETRIZATION

- Given E/\mathbb{Q} , modularity gives a modular form f .
- The **Eichler-Shimura construction** produces a curve E_f associated to f such that there is an isogeny $E_f \rightarrow E$.
- In fact, for N the conductor of E , this construction gives

$$\Phi : X_0(N) \rightarrow J_0(N) \rightarrow J_0(N)/I_f J_0(N) \cong E_f \rightarrow E$$

where $J_0(N)$ is the Jacobian of $X_0(N)$ and I_f is a certain ideal in the Hecke algebra associated to f .

- This map is **defined over \mathbb{Q}** , which will be important later.

ANALYTIC DESCRIPTION

We define, for f associated to E ,

$$\varphi : \mathcal{H} \rightarrow \mathbb{C}$$

$$\tau \mapsto 2\pi i \int_{i\infty}^{\tau} f(\zeta) d\zeta.$$

For $\gamma \in \Gamma_0(N)$, the difference $\varphi(\gamma\tau) - \varphi(\tau)$ is in the lattice Λ_f , so φ induces

$$\Phi' : \Gamma_0(N) \backslash \mathcal{H} \rightarrow \mathbb{C}/\Lambda_f \cong E.$$

Practically, $\Lambda_f = \Lambda_E$ for the last isomorphism.

LUCKILY...

The two descriptions of the modular parametrization map

$$\begin{aligned}\Phi &: X_0(N) &\longrightarrow & E \\ \Phi' &: \Gamma_0(N) \backslash \mathcal{H} &\longrightarrow & \mathbb{C}/\Lambda\end{aligned}$$

match up!

- Algebraic description: we'll find a rational point in the end
- Analytic description: this map is computable

COMPUTING Φ

- If f_E has the Fourier expansion

$$f_E(\tau) = \sum_{n \geq 1} a_n e^{2\pi i n \tau},$$

then the a_n can be obtained directly from E .

- Therefore, we have an explicit way to compute Φ :

$$\Phi(\tau) = 2\pi i \int_{i\infty}^{\tau} f(\zeta) d\zeta = \sum_{n=1}^{\infty} \frac{a_n}{n} e^{2\pi i n \tau}.$$

OVERVIEW (AGAIN)

- Goal: find a nontorsion rational point on E/\mathbb{Q} .
- Often easier to study families than objects—a **modular curve** is one way to parametrize elliptic curves with extra structure.
- We construct special points on modular curves by **complex multiplication**.
- We then apply the **modular parametrization map** $\Phi : X_0(N) \rightarrow E$ to obtain rational points on E .

COMPLEX MULTIPLICATION (I)

- The modular parameterization is a map over \mathbb{Q} :

$$\Phi : X_0(N) \longrightarrow E$$

We'll find points on $X_0(N)(H)$, over a fixed number field H , and map them to E . This gives points of $E(H)$. (We'll specify H later.)

- How to find H -rational points of $X_0(N)$?

$$X_0(N) = \{\text{elliptic curves with level-}N \text{ subgroup}\}$$

Even better:

$$X_0(N)(H) = \{\text{elliptic curves over } H \text{ with level-}N \text{ subgroup over } H\}$$

So want to find E' over H with level- N subgroup over H .

COMPLEX MULTIPLICATION (II)

CM to the rescue!

Let $\tau \in \mathcal{H}$. Assume it's quadratic over \mathbb{Q} . So satisfies unique equation of the form

$$A\tau^2 + B\tau + C = 0 \quad A, B, C \in \mathbb{Z} \quad A > 0 \quad (A, B, C) = 1$$

Define the **discriminant**:

$$\Delta(\tau) = B^2 - 4AC$$

Theorem 1. *Let K be quadratic over \mathbb{Q} , and let $H = \text{HCF}(K)$. Let $D = \text{disc}(K/\mathbb{Q})$ and let $\tau \in K \cap \mathcal{H}$. If $\Delta(\tau) = D$ then $j(\tau) \in H$.*

So if $E_\tau = \mathbb{C}/\langle 1, \tau \rangle$ then E_τ is defined over H .

COMPLEX MULTIPLICATION (III)

We still need an order- N subgroup defined over H . Have a map

$$E_{N\tau} \longrightarrow E_{\tau}$$

with cyclic kernel of order N . When is $E_{N\tau}$ defined over H ?

Proposition 1. *If $\Delta(\tau) = D = \text{disc}(K/\mathbb{Q})$ is prime to N ,*

$$N \mid A \quad \text{and} \quad D \equiv B^2 \pmod{4N}$$

then $\Delta(\tau) = \Delta(N\tau)$. In particular,

$$\tau \in X_0(N)(H).$$

Such a τ is called a **Heeger point**. Given D , we can algorithmically search for such τ .

COMPLEX MULTIPLICATION (IV)

Miracle! For such τ , $\Phi(\tau) \in E(H)$

Recall that we can compute Φ by:

$$\Phi(\tau) = \sum_{n=1}^{\infty} \frac{a_n}{n} e^{2\pi i n \tau}.$$

If $\tau_1, \dots, \tau_h \in X_0(N)(H)$ are the conjugates under $\text{Gal}(H/K)$ then

$$\sum_{i=1}^h \Phi(\tau_i) \in E(K)$$

But we want a **rational** point of E ! Turns out that because of the functional equation, $\text{Gal}(K/\mathbb{Q})$ acts trivially on the above sum. So in fact

$$\sum_{i=1}^h \Phi(\tau_i) \in E(\mathbb{Q})$$

COMPLEX MULTIPLICATION (V)

Last step: calculate **all** of the τ_i 's.

Theorem 2 (Gauss). *There is a one-to-one correspondence*

$$\text{Gal}(H/K) \longleftrightarrow \{\tau \in K \cap \mathcal{H} \mid \Delta(\tau) = D\} / \text{SL}_2(\mathbb{Z})$$

In other words:

We only have to find a Heeger point τ in each class modulo $\text{SL}_2(\mathbb{Z})$.

Again, we can do this algorithmically.

AND NOW??

- Joe has handed me a complex number

$$z = \phi(\tau) \in \mathbb{C}$$

and we are interested in the corresponding point on our elliptic curve:

$$P = (\wp(z), \wp'(z)) \in E(\mathbb{C}).$$

- Joe's **Complex Multiplication Magical Mystery Tour** tells us that, in fact,

$$P = (\wp(z), \wp'(z)) \in E(\mathbb{Q}).$$

AND NOW??

Remember, our original goal was to find a **non-torsion point**, and for that we need ...

THE THEOREM OF GROSS-ZAGIER

$$\hat{h}(P) = \frac{\sqrt{|D|}}{4\text{Vol}(E)} L'(E, 1) L(E_D, 1)$$

CANONICAL HEIGHT

$$\hat{h}(P) = \frac{\sqrt{|D|}}{4\text{Vol}(E)} L'(E, 1) L(E_D, 1)$$

- $\hat{h}(P)$ is the **Canonical Height** of the point P .
- The precise definition is a bit tricky; in essence it is a measure of the number of digits necessary to write down the x -coordinate of P .

KEY PROPERTIES

$$\hat{h}(P) = \frac{\sqrt{|D|}}{4\text{Vol}(E)} L'(D, 1) L(E_D, 1)$$

- (1) $\hat{h}(lP) = l^2 \hat{h}(P)$
- (2) Given some bound B , there are only finitely many points P with height less than B
- (3) $\hat{h}(P)$ is zero if and only if P is a torsion point.

$\hat{h}(P)$ IS ZERO IF AND ONLY IF P IS A TORSION POINT

$$\hat{h}(P) = \frac{\sqrt{|D|}}{4\text{Vol}(E)} L'(D, 1) L(E_D, 1)$$

- $|D|$ is non-zero
- $\text{Vol}(E)$ is the volume of the period lattice; this is also non-zero.

$\hat{h}(P)$ IS ZERO IF AND ONLY IF P IS A TORSION POINT

$$\hat{h}(P) = \frac{\sqrt{|D|}}{4\text{Vol}(E)} L'(D, 1) L(E_D, 1)$$

To even get started we needed to know that $L'(D, 1)$ was non-zero.

$\hat{h}(P)$ IS ZERO IF AND ONLY IF P IS A TORSION POINT

$$\hat{h}(P) = \frac{\sqrt{|D|}}{4\text{Vol}(E)} L'(D, 1) L(E_D, 1)$$

- E_D is the **quadratic twist** of E by D .
- $L(E_D, s) = \sum_{n \geq 1} \left(\frac{D}{n}\right) \frac{a_n}{n^s}$
- We chose everything such that $L(E_D, 1)$ will be non-zero.

SO... IS P A TORSION POINT?

$$\hat{h}(P) = \frac{\sqrt{|D|}}{4\text{Vol}(E)} L'(D, 1) L(E_D, 1) \neq 0$$

P is a torsion point if and only if $\hat{h}(P)$ is zero

We conclude that P is **not a torsion point!**

TIME TO PACK UP AND GO HOME?

Of course not.

BSD REVISITED

$$\frac{L_E^{(r)}(1)}{r!} = \frac{\#\text{III}(E) \cdot R(E) \cdot \omega_1 \cdot \prod_{p \leq \infty} c_p}{(\#E(\mathbb{Q})_{tors})^2}$$

BSD REVISITED - REGULATOR

$$\frac{L_E^{(r)}(1)}{r!} = \frac{\#\text{III}(E) \cdot R(E) \cdot \omega_1 \cdot \prod_{p \leq \infty} c_p}{(\#E(\mathbb{Q})_{tors})^2}$$

- For $P, Q \in E(\mathbb{Q})$, define

$$2\hat{h}(P, Q) = \hat{h}(P + Q) - \hat{h}(P) - \hat{h}(Q).$$

- Then $\hat{h}(\cdot, \cdot)$ defines a paring on $E(\mathbb{Q})/E(\mathbb{Q})_{tors}$

BSD REVISITED - REGULATOR

$$\frac{L_E^{(r)}(1)}{r!} = \frac{\#\text{III}(E) \cdot R(E) \cdot \omega_1 \cdot \prod_{p \leq \infty} c_p}{(\#E(\mathbb{Q})_{tors})^2}$$

- Let P_1, \dots, P_r generate the free part of $E(\mathbb{Q})$.

- Then $R(E) = \begin{vmatrix} \hat{h}(P_1, P_1) & \cdots & \hat{h}(P_1, P_n) \\ \vdots & & \vdots \\ \hat{h}(P_n, P_1) & \cdots & \hat{h}(P_n, P_n) \end{vmatrix}$

BSD REVISITED - REGULATOR + 'RANK = 1'

$$L'(E, 1) = \frac{\#\text{III}(E) \cdot R(E) \cdot \omega_1 \cdot \prod_{p \leq \infty} c_p}{(\#E(\mathbb{Q})_{tors})^2}$$

Let G generate the free part of $E(\mathbb{Q})$.

$$R(E) = \hat{h}(G, G) = \frac{1}{2} \left(\hat{h}(2G) - \hat{h}(G) - \hat{h}(G) \right) = \hat{h}(G)$$

BSD REVISITED - ONE MORE THING...

$$L'(E, 1) = \frac{\#\text{III}(E) \cdot R(E) \cdot \omega_1 \cdot \prod_{p \leq \infty} c_p}{(\#E(\mathbb{Q})_{tors})^2}$$

- Let $P = lG + T$, where T is torsion.
- Then $\hat{h}(P) = l^2 \hat{h}(Q)$

BSD REVISITED - THE POINT

$$L'(E, 1) = \frac{\#\text{III}(E) \cdot R(E) \cdot \omega_1 \cdot \prod_{p \leq \infty} c_p}{(\#E(\mathbb{Q})_{tors})^2}$$

$$\hat{h}(P) = l^2 \hat{h}(G) = l^2 R(E)$$

$$\hat{h}(P) = \frac{\sqrt{|D|}}{4\text{Vol}(E)} L'(E, 1) L(E_D, 1)$$

BSD REVISITED - THE POINT

$$L'(E, 1) = \frac{\#\text{III}(E) \cdot R(E) \cdot \omega_1 \cdot \prod_{p \leq \infty} c_p}{(\#E(\mathbb{Q})_{tors})^2}$$

$$\hat{h}(P) = l^2 \hat{h}(G) = l^2 R(E)$$

$$\hat{h}(P) = \frac{\sqrt{|D|}}{4\text{Vol}(E)} L'(E, 1) L(E_D, 1)$$

BSD REVISITED - THE POINT

$$m^2 := \frac{l^2}{\#\text{III}(E)} = \omega_1 \frac{\sqrt{|D|} \cdot \prod_{p \leq \infty} c_p}{4 \text{Vol}(E) |E_t(\mathbb{Q})|^2} L(E_D, 1)$$

$$P = lG + T$$

BSD REVISITED - $P = lG + T$

Now we know that for some torsion point T :

$$\sqrt{\#\text{III}(E)} \cdot G = \frac{1}{m} (P - T), m = l \cdot \sqrt{\#\text{III}(E)}$$

for some choice of m^{th} root.

BSD REVISITED - $\sqrt{\#\text{III}(E)} \cdot G = \frac{1}{m} (P - T)$

- We have computed $\sqrt{\#\text{III}(E)} \cdot G$ as a real number.
- Gross-Zagier's height formula gives us a bound on the numerator and denominator of $\sqrt{\#\text{III}(E)} \cdot G$.
- Finally, using this bound and LLL, we can compute $\sqrt{\#\text{III}(E)} \cdot G$ as a rational point on our curve E .