An Introduction to Heegner Points and the Gross-Zagier Formula

Zachary Gardner

October 23, 2020

Overview

Let $E/\mathbb{Q}$ be an elliptic curve. Our goal is to construct and study certain rational points in $E(K)$, where K is an imaginary quadratic field. We do this as follows.

1. It turns out to be advantageous to assume that E is modular and so there is a "modular covering" $\phi_E : X_0(N) \to E$ for some N (all of this will be made precise). This assumption is harmless by the modularity theorem.
2. Produce a family of points in $X_0(N)(L)$ for L/K a suitable Galois extension that behave nicely under the action of $\mathrm{Gal}(L/K)$. These are the so-called Heegner points.
3. Precompose with ϕ_E and sum over our family to produce a point

$$P_K \in E(L)^{\mathrm{Gal}(L/K)} = E(K).$$

4. Formulate the Gross-Zagier formula, which relates height data of the point P_K to central derivatives of certain L-functions.

Elliptic Curves

As you have probably heard, elliptic curves are one of the central objects of study in number theory.

Definition

An **elliptic curve** E over a field k is a smooth projective algebraic k-curve with genus one and a distinguished k-rational point (i.e., a point with "coefficients in k").

Intuitively, E is a one-dimensional object cut out by some algebraic equations that has a single "hole." One of the key features is that the set $E(k)$ of k-rational points is an abelian group under an appropriately geometric operation. Over $\mathbb{Q}$, E is defined by a Weierstraß model

$$y^2 = x^3 + ax + b$$

with $a, b \in \mathbb{Z}$ and nonzero discriminant measuring smoothness:

$$0 \neq \Delta_{E/\mathbb{Q}} = 16(4a^3 + 27b^2).$$

Isogeny

In math it is often useful to study objects up to a certain notion of equivalence. For elliptic curves, that notion is isogeny.

Definition

An **isogeny** $\phi : E \to E'$ of elliptic curves over k is a nonzero map that preserves the underlying curve and group structures.

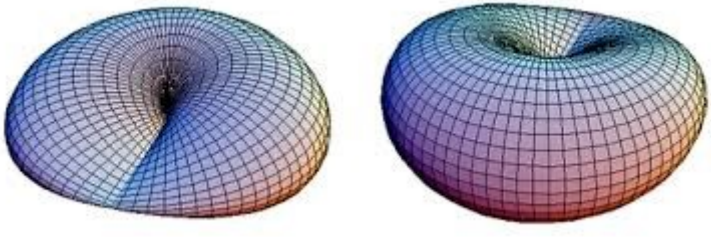
The map ϕ has a well-defined kernel $\ker \phi$ whose structure is mostly determined by what happens to $\overline{k}$-points:

$$(\ker \phi)(\overline{k}) = \ker(\phi(\overline{k}) : E(\overline{k}) \to E'(\overline{k})).$$

The structure of $\ker \phi$ encodes important geometric information – e.g., if $(\ker \phi)(\overline{k}) \cong \mathbb{Z}/N$ for N prime to the characteristic of k then ϕ should be viewed as a degree N covering map. In this case we say that ϕ is a **cyclic N-isogeny**. Note that a 1-isogeny is just an isomorphism (over $\overline{k}$).

Moduli Spaces

We want to build a ("coarse moduli") space $X_0(N)$ that parameterizes elliptic curves up to N-isogeny. We will do this by constructing a homogeneous space $Y_0(N)$ whose points correspond to N-isogeny classes of elliptic curves. The reason this is not the end of the story is that we want to think about elliptic curves in families and not just as isolated objects. Some families in $Y_0(N)$ will degenerate into "cusps." We want to ensure that these cusps are contained in $X_0(N)$, which can be done by appropriately compactifying $Y_0(N)$. To see this in action let's investigate the case $N = 1$.



The Case $N = 1$

Over $\mathbb{C}$, classifying elliptic curves is easy. We have $E = \mathbb{C}/\Lambda$ for some lattice

$$\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}, \qquad \omega_1, \omega_2 \in \mathbb{C} \text{ such that } \omega_1/\omega_2 \notin \mathbb{R}.$$

By rescaling we may assume $\Lambda = \mathbb{Z} + \tau\mathbb{Z}$ for some $\tau \in \mathbb{H}$, where

$$\mathbb{H} := \{x + iy \in \mathbb{C} : y > 0\}$$

is the upper half-plane. Two points $\tau, \tau' \in \mathbb{H}$ yield equivalent ("homothetic") lattices if and only if they lie in the same orbit of $\mathrm{SL}_2(\mathbb{Z})$, which acts on $\mathbb{H}$ by fractional linear transformations à la

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \tau = \frac{a\tau + b}{c\tau + d}.$$

With this in mind, we define $Y_0(1) := \mathbb{H}/\mathrm{SL}_2(\mathbb{Z})$.

Modular Curves

For general N it turns out the right approach is to define

$$\Gamma_0(N) := \left\{ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \bmod N \right\}$$

and $Y_0(N) := \mathbb{H}/\Gamma_0(N)$. As promised, we obtain $X_0(N)$ by compactifying $Y_0(N)$. There are several (non-stacky) approaches to doing this.

1. Consider the extended upper half-plane $\mathbb{H}^* := \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$ endowed with an extension of the Euclidean topology on $\mathbb{H}$ so that $\mathbb{H}^*$ naturally embeds into the compact Riemann sphere $\mathbb{P}^1(\mathbb{C})$. The group $\Gamma_0(N)$ then acts on $\mathbb{Q} \cup \{\infty\}$ with finitely many orbits that formally give rise to cusps when passing to the quotient.
2. The space $Y_0(N)$ inherits a Riemann surface structure from $\mathbb{H}$ as a quotient of $\mathbb{H}$ by a discrete subgroup of the group $\mathrm{Aut}(\mathbb{H})$ of holomorphic automorphisms of $\mathbb{H}$. This in fact endows $Y_0(N)$ with an affine curve structure, which yields $X_0(N)$ as a (highly singular) compact projective curve (over $\mathbb{Q}$!) by first projectivizing and then looking at monodromy (c.f. §4.2.3 of Donaldson's excellent book *Riemann Surfaces*.) We call $X_0(N)$ the **modular curve** of level N.

The j-function

Elaborating on the second approach, we have the j-function $j : \mathbb{H} \to \mathbb{C}$ given by

$$j(\tau) := 1728 \frac{g_2(\tau)^3}{\Delta(\tau)}$$

for $\Delta(\tau) := g_2(\tau)^3 - 27g_3(\tau)^2$ and

$$g_2(\tau) := 60 \sum_{(m,n)\neq(0,0)} (m + n\tau)^{-4}, \qquad g_3(\tau) := 140 \sum_{(m,n)\neq(0,0)} (m + n\tau)^{-6}.$$

Miraculously, j is well-defined since $\Delta(\tau) \neq 0$. We obtain an associated elliptic curve

$$E_\tau : y^2 = 4x^3 - g_2(\tau)x - g_3(\tau).$$

There is then a bijection between $Y_0(1)$ and 1-isogeny classes of elliptic curves via $[\tau] \longleftrightarrow [E_\tau]$. With some work we may parameterize N-isogeny classes of elliptic curves by pairs $(j(\tau), j(N\tau))$ and produce an affine curve structure from the associated relations. Because of the importance of the j-function, the curve $X_0(1)$ is often called the j-**line**.

Complex Multiplication

Let $X \in X_0(N)$ be a noncuspidal point and $\mathrm{End}(X)$ its ring of endomorphisms relative to a field k of characteristic 0. Generically, we have $\mathrm{End}(X) \cong \mathbb{Z}$ but sometimes extra symmetries arise. We then have $\mathrm{End}(X) \cong \mathcal{O}$ for $\mathcal{O} \subseteq \mathcal{O}_K$ an order in an imaginary quadratic field K, which by definition means that $\mathcal{O}$ is a subring of K which is a free abelian group generated by a $\mathbb{Q}$-basis of K. In this case, X is said to have **complex multiplication** (**CM** for short).

Example

Consider the elliptic curve $E/\mathbb{Q}$ defined by $y^2 = 4x^3 - x$. Then, $\mathrm{End}(E) \cong \mathbb{Z}[i]$ as exhibited by the order 4 automorphisms

$$x \mapsto -x, \qquad y \mapsto \pm iy.$$

It follows that $[E]$ (equivalently, E) has CM.

Carrying over this setup, suppose $X \in X_0(N)$ has CM. The **conductor** $c := |\mathcal{O}_K : \mathcal{O}|$ encodes important Galois theoretic information about K. We will assume for the sake of simplicity that $c = 1$. We have an isomorphism

$$\mathrm{Art}_K : \mathrm{Cl}(K) \to \mathrm{Gal}(H_K/K), \qquad [\mathfrak{p}] \mapsto \mathrm{Frob}_{\mathfrak{p}},$$

where Art_K is the Artin map, $\mathrm{Cl}(K)$ is the class group of K, and H_K is the Hilbert class field of K (i.e., the maximal unramified abelian extension of K). The symbol $\mathrm{Frob}_{\mathfrak{p}}$ denotes the Frobenius automorphism associated to $\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K$, which corresponds to the usual Frobenius automorphism for extensions of finite fields and does not depend on lifts because H_K is an abelian extension. The Artin map generalizes the Legendre symbol and allows us to analyze ramification behavior of prime ideals.

Reminder

Given L/k an extension of number fields, prime ideals of $\mathcal{O}_L$ restrict down to prime ideals of $\mathcal{O}_k$. Moreover, $\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K$ generates an ideal $\mathfrak{p}\mathcal{O}_L$ that factors uniquely as a product of prime ideals of $\mathcal{O}_L$. You should think of the map $\operatorname{Spec} \mathcal{O}_L \to \operatorname{Spec} \mathcal{O}_K$ as a (potentially ramified) map between curves, analogous to a ramified map between Riemann surfaces.

Heegner Points

Assume now the so-called **Heegner hypothesis**:

every prime dividing N is split in K.

For instance, if $K = \mathbb{Q}(i)$ then we may take any N all of whose prime factors are 1 mod 4. Because of the splitting, we may choose an ideal $\mathfrak{n} \subseteq \mathcal{O}_K$ such that $\mathcal{O}_K/\mathfrak{n} \cong \mathbb{Z}/N$. Thinking of fractional ideals of K as lattices in $\mathbb{C}$, we have a map

$$\gamma_{\mathfrak{n}} : \mathrm{Cl}(K) \to X_0(N)(\mathbb{C}), \qquad [\mathfrak{a}] \mapsto [\mathbb{C}/\mathfrak{a} \to \mathbb{C}/\mathfrak{n}^{-1}\mathfrak{a}]$$

which in fact defines points in $X_0(N)(H_K)$ that have the Galois equivariance property

$$\mathrm{Art}_K([\mathfrak{p}]) \cdot \gamma_{\mathfrak{n}}([\mathfrak{a}]) = \gamma_{\mathfrak{n}}([\mathfrak{p}\mathfrak{a}]).$$

Such points are called **Heegner points** and are worthy of study in their own right. We won't get into this, however.

Suppose now that $E/\mathbb{Q}$ is an elliptic curve and let $N \in \mathbb{Z}$ be its conductor, which measures ramification of E at certain torsion rational points and is an isogeny invariant. By the modularity theorem there is a rational map $\phi_E : X_0(N) \to E$ with integer coefficients called the **modular covering**. Given a family of Heegner points as before, we obtain a point

$$P_{K,\mathfrak{n}} := \sum_{[\mathfrak{a}] \in \mathrm{Cl}(K)} \phi_E(\gamma_{\mathfrak{n}}([\mathfrak{a}])) \in E(H_K).$$

The modular covering respects the earlier Galois equivariance and so we deduce

$$P_{K,\mathfrak{n}} \in E(H_K)^{\mathrm{Gal}(H_K/K)} = E(K)$$

since we are just permuting the terms in a sum. It turns out that different choices of $\mathfrak{n}$ either leave $P_{K,\mathfrak{n}}$ fixed or change it by a readily calculable amount and so we drop $\mathfrak{n}$ from the notation.

Exercise

To get a feel for this, look at the case $N = p$ prime so that $p\mathcal{O}_K = \mathfrak{p}\overline{\mathfrak{p}}$. Consider the action of conjugation and of the dual isogeny involution on $X_0(p)$.

How do we define the map ϕ_E? By the modularity theorem, there is a unique elliptic curve $E'/\mathbb{Q}$ isogenous to E such that

$$f_{E'}(z) = \sum_{n \geq 1} a_n(E') e^{2\pi i n z}$$

is a holomorphic cusp form of weight 2 and level N such that

$$|E'(\mathbb{F}_p)| = p + 1 - a_p(E')$$

for every prime p. Concretely, this means that $f_E : \mathbb{H} \to \mathbb{C}$ is a holomorphic function such that

- $f_{E'}(\gamma z) = (cz + d)^2 f_{E'}(z)$ for every $\gamma \in \Gamma_0(N)$ and
- $(cz + d)^{-2} f_{E'}(\gamma z) \to 0$ as $\operatorname{Im} z \to +\infty$ for every $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

Assume for the sake of simplicity that $E = E'$. The map ϕ_E need not be unique, but we can rigidify things by demanding that $\phi_E(\infty) = 0$ and $\phi_E^*(\omega) = 2\pi i c f_E(z) dz$ for some $c > 0$ and ω a translation-invariant holomorphic 1-form on $E(\mathbb{C})$. We then have

$$\phi_E(z) = -2\pi i c \int_z^{i\infty} f_E(\tau)\, d\tau.$$

We now have a point $P_K \in E(K)$. What can we say about it? The field K is imaginary quadratic and so is of the form $K = \mathbb{Q}(\sqrt{D})$ for $D < 0$ a quadratic fundamental discriminant, which concretely means that

$$D = \begin{cases} d, & d \equiv 1 \bmod 4, \\ 4d, & d \equiv 2, 3 \bmod 4, \end{cases}$$

for $d < 0$ squarefree. There is a unique quadratic Dirichlet character χ_D of period $|D|$ arising from a group homomorphism $(\mathbb{Z}/D)^\times \to \{\pm 1\}$ that satisfies

$$\zeta_K(s) = \zeta_{\mathbb{Q}}(s) L(s, \chi_D).$$

Note that, for $D = p$ prime, χ_p is given by the Legendre symbol $\left(\frac{\cdot}{-p}\right)$. The Heegner hypothesis is precisely the statement that $\gcd(N, D) = 1$.

Table of L-Functions

Name	Notation	Series	Product
Riemann zeta function	$\zeta_{\mathbb{Q}}(s)$	$\sum_{n\geq 1} n^{-s}$	$\prod_{p} \frac{1}{1-p^{-s}}$
Dedekind zeta function	$\zeta_K(s)$	$\sum_{I\subseteq \mathcal{O}_K} (N_{K/\mathbb{Q}}I)^{-s}$	$\prod_{\mathfrak{p}} \frac{1}{1-N_{K/\mathbb{Q}}\mathfrak{p}^{-s}}$
Dirichlet L-function	$L(s,\chi_D)$	$\sum_{n\geq 1} \chi_D(n)n^{-s}$	$\prod_{p} \frac{1}{1-\chi_D(p)p^{-s}}$
Hasse-Weil L-function	$L_{E/\mathbb{Q}}(s)$	$\sum_{n\geq 1} a_n(E)n^{-s}$	$\prod_{p} \frac{1}{1-a_p(E)p^{-s}+\beta_N(p)p^{1-2s}}$
Twisted L-function	$L_{E/\mathbb{Q}}(s,\chi_D)$	$\sum_{n\geq 1} a_n(E)\chi_D(n)n^{-s}$	$\prod_{p} \frac{1}{1-a_p(E)\chi_D(p)p^{-s}+\beta_N(p)\chi_D(p)^2p^{1-2s}}$

Here, $N_{K/\mathbb{Q}}\mathfrak{p} = |\mathcal{O}_K/\mathfrak{p}|$, $I \subseteq \mathcal{O}_K$ is a proper ideal, and

$$\beta_N(p) := \begin{cases} 1, & p \nmid N, \\ 0, & p \mid N. \end{cases}$$

These product expansions are often called **Euler products** and their terms **Euler factors**. Euler products typically converge on some right half-plane. Suitably "completing" the associated L-function yields a new function satisfying a functional equation and we may use this symmetry to build an analytic continuation. For instance, the completed Hasse-Weil L-function

$$\Lambda_{E/\mathbb{Q}}(s) := (2\pi)^{-s} N^{s/2} \Gamma(s) L_{E/\mathbb{Q}}(s)$$

satisfies the function equation

$$\Lambda_{E/\mathbb{Q}}(s) = \epsilon(E/\mathbb{Q}) \Lambda_{E/\mathbb{Q}}(2-s),$$

where $\epsilon(E/\mathbb{Q}) \in \{\pm 1\}$ is the **root number**. Similarly, the completed twisted L-function

$$\Lambda_{E/\mathbb{Q}}(s, \chi_D) := (2\pi)^{-s} (ND^2)^{s/2} \Gamma(s) L_{E/\mathbb{Q}}(s, \chi_D)$$

satisfies

$$\Lambda_{E/\mathbb{Q}}(s, \chi_D) = \epsilon(E/\mathbb{Q}) \chi_D(-N) \Lambda_{E/\mathbb{Q}}(2-s, \chi_D).$$

Consider now the product

$$L_{E/K}(s) := L_{E/\mathbb{Q}}(s)L_{E/\mathbb{Q}}(s, \chi_D),$$

which is in fact the Hasse-Weil L-function for E/K. The associated root number is

$$\epsilon(E/K) = \epsilon(E/\mathbb{Q})^2\chi_D(-N) = \chi_D(-1)\chi_D(N) = -1$$

since $D < 0$ and N is split in K. It follows that all even-order derivatives of $L_{E/K}(s)$ at $s = 1$ (the fixed point of the involution $s \mapsto 2 - s$) vanish and so calculations originally done by Birch suggest looking at the first derivative.

Exercise

Let $p, q > 0$ be distinct odd primes and $p^* := (-1)^{(p-1)/2}p$. Show that

$$\left(\frac{q}{p}\right) = \begin{cases} 1, & q \text{ is split in } \mathbb{Q}(\sqrt{p^*}), \\ -1, & q \text{ is inert in } \mathbb{Q}(\sqrt{p^*}). \end{cases}$$

The Gross-Zagier Formula

Without further ado, here is the main result.

Theorem (Gross-Zagier)

Let $E/\mathbb{Q}$ be an elliptic curve of conductor N and $P_K \in E(K)$ built from the $\mathrm{Gal}(H_K/K)$-orbit of a Heegner point $X \in X_0(N)$ with associated order $\mathcal{O} \subseteq \mathcal{O}_K$ of conductor 1. Then,

$$L'_{E/K}(1) = \frac{d}{ds}\bigg|_{s=1} L_{E/K}(s) = \frac{32\pi^2 \langle f_E, f_E \rangle}{|\mathcal{O}_K^\times|^2 \sqrt{|D|}} \cdot \frac{\hat{h}_E(P_K)}{\deg \phi_E},$$

following the notation of our earlier constructions.

Note that

$$|\mathcal{O}_K^\times| = \begin{cases} 4, & K = \mathbb{Q}(\sqrt{-1}), \\ 6, & K = \mathbb{Q}(\sqrt{-3}), \\ 2, & \text{otherwise}, \end{cases}$$

and the term $|\mathcal{O}_K^\times|^2$ in the denominator can be eliminated if we preemptively divide f_E through by $|\mathcal{O}_K^\times|$. We will spend the rest of our time unpacking what this formula means.

Petersson Inner Product

Let's first tackle the term $32\pi^2 \langle f_E, f_E \rangle$. This is a form of the Petersson inner product

$$\langle f, g \rangle := \int_{Y_0(N)} f(\tau)\overline{g(\tau)}(\mathrm{Im}\tau)^2 \, d\nu(\tau) = \int_{Y_0(N)} f(x+iy)\overline{g(x+iy)} \, dxdy$$

defined for pairs (f, g) of weight 2 holomorphic cusp forms of level N.

- The quantity $32\pi^2$ arises from normalization and from changes to the choice of domain of integration – e.g., using a fundamental domain for $Y_0(N)$ instead of the entirety of $Y_0(N)$. You should think of a fundamental domain as supplying distinct coset representatives for the homogeneous space $Y_0(N)$.
- The quantity $\langle f_E, f_E \rangle$ is closely related to the integral $\int_{E(\mathbb{C})} \omega \wedge \overline{\omega}$ for ω defined as before and so some forms of the Gross-Zagier formula use this integral instead.

Height Theory

The term $\hat{h}_E(P_K)$ is a bit harder to describe. The function $\hat{h}_E : E(\overline{K}) \to \mathbb{R}^{\geq 0}$ is called the **Tate canonical height** of E and is built up as follows. Let k be a number field and Ω_k its set of places. For each $v \in \Omega_k$, let $|\cdot|_v$ be the associated normalized absolute value. For example, for $\mathbb{Q}$ we get the real absolute value $|\cdot|$ as well as the standard p-adic absolute values $|\cdot|_p$ that measure divisibility by a prime p. Define the height function

$$h_{k/\mathbb{Q}} : \mathbb{P}^2(k) \to \mathbb{R}^{\geq 0}, \qquad [t_0, t_1, t_2] \mapsto \frac{1}{[k : \mathbb{Q}]} \log \prod_{v \in \Omega_k} \max\{|t_0|_v, |t_1|_v, |t_2|_v\},$$

which is well-defined by the product formula

$$\prod_{v \in \Omega_k} |t|_v = 1, \qquad t \in k^\times.$$

We think of heights as measuring the "arithmetic complexity" of points, with larger heights rarer in a sense that can be made precise (see, e.g., Northcott's theorem).

Height Theory

Given L/k a finite extension, $h_{k/\mathbb{Q}}$ is equal to the composition of $h_{L/\mathbb{Q}}$ with the natural map $\mathbb{P}^2(k) \to \mathbb{P}^2(L)$ and so there is an induced map $h_k : \mathbb{P}^2(\overline{k}) \to \mathbb{R}^{\geq 0}$. Concretely, $h_k(P) = h_{L/\mathbb{Q}}(P)$ for any L/k finite such that L contains the coordinates of P. Let now E/k be any elliptic curve (which need not be the same one as before) and choose a projective embedding $\iota : E \hookrightarrow \mathbb{P}^2_k$. We obtain

$$h_E := h_k \circ \iota : E(\overline{k}) \to \mathbb{R}^{\geq 0},$$

which only depends on ι up to a bounded function. We can eliminate this ambiguity by considering

$$\hat{h}_E : E(\overline{k}) \to \mathbb{R}^{\geq 0}, \qquad P \mapsto \lim_{n\to\infty} \frac{h(nP)}{n^2}.$$

It turns out that this function is not only well-defined but also quadratic in the sense that

$$\hat{h}_E(P+Q+R) - (\hat{h}_E(P+Q) + \hat{h}_E(P+R) + \hat{h}_E(Q+R)) + (\hat{h}_E(P) + \hat{h}_E(Q) + \hat{h}_E(R))$$

vanishes for all $P, Q, R \in E(\overline{k})$. Additionally, $\hat{h}_E(P) = 0 \iff P$ is torsion.

Height Theory

It follows that there is an associated $\mathbb{Z}$-bilinear pairing $\langle \cdot, \cdot \rangle_{\mathrm{NT}}$ called the **Néron-Tate pairing**. This pairing actually provides some insight into how to go about deducing the Gross-Zagier formula. Intuitively, $\langle \cdot, \cdot \rangle_{\mathrm{NT}}$ lets us "decouple" – we can relate $\langle P_K, P_K \rangle_{\mathrm{NT}}$ to $\langle P_{\chi_1}, P_{\chi_2} \rangle_{\mathrm{NT}}$ for P_{χ_1}, P_{χ_2} rational points associated to appropriate characters

$$\chi_1, \chi_2 : \mathrm{Gal}(H_K/K) \to \{\pm 1\}.$$

Returning to the Gross-Zagier formula, it turns out that $\hat{h}_E(P_K)/\deg \phi_E$ is an isogeny invariant of E. Heights make sense for general abelian varieties over number fields. In particular, we can work with heights over the Jacobian $J_0(N)$ of $X_0(N)$. It turns out $X_0(N)$ embeds into $J_0(N)$ in such a way that we may envision ϕ_E as a well-behaved map $J_0(N) \to E$ via a suitable quotient construction. We realize $\hat{h}_E$ by choosing a projective embedding of E, which is equivalent to a choice of an ample line bundle $\mathscr{L}$ on E. Heights behave well under pullback, and the term $\deg \phi_E$ arises from pulling back $\mathscr{L}$ by ϕ_E.

Horizons

Here are a few applications of the Gross-Zagier formula and its generalizations.

1. Solving the Gauss class number 1 problem and proving Goldfeld's theorem.
2. Computing central values of L-functions.
3. Understanding more about the BSD conjecture and associated rank bounds.

We've barely scratched the surface on this topic. Here are some things I haven't said anything about.

- How things work if we try to use a real quadratic field (integration over geodesics)
- Role of Hecke algebra and notion of Rankin L-series

THANKS FOR COMING!!!