Independence of Heegner Points

Joseph H. Silverman
(Joint work with Michael Rosen)
Brown University

Cambridge University Number Theory Seminar

Thursday, February 22, 2007

Modular Curves and Heegner Points

The Modular Curve $X_0(N)$

The **Modular Curve** $X_0(N)$ parametrizes isomorphism classes of pairs

$$x \in X_0(N) \qquad x \longleftrightarrow (E, C)$$

where

E is an elliptic curve,

$C \subset E[N]$ is a cyclic subgroup of order N.

Two pairs (E, C) and (E', C') are equivalent if there is an isomorphism

$$f : E \xrightarrow{\sim} E' \qquad \text{with} \qquad f(C) = C'.$$

It turns out that the set of pairs (E, C) has a natural structure as an (affine) algebraic curve, and adding a few points (cusps) gives the projective curve $X_0(N)$.

Heegner Points on $X_0(N)$

A **Heegner point** is a special type of point on $X_0(N)$ that is manufactured using:

k	a quadratic imaginary field
$\mathcal{O} \subset k$	the ring of integers of k
$\mathfrak{n} \subset \mathcal{O}$	an ideal with $\mathcal{O}/\mathfrak{n} \cong \mathbb{Z}/N\mathbb{Z}$

Notice that $\mathcal{O}$ is a lattice in $\mathbb{C}$, so it defines an elliptic curve via the classical complex analytic construction

$$E(\mathbb{C}) \cong \mathbb{C}/\mathcal{O}.$$

Futher, this elliptic curve has a subgroup

$$\mathbb{Z}/N\mathbb{Z} \cong \mathfrak{n}^{-1}/\mathcal{O} \subset \mathbb{C}/\mathcal{O}.$$

The pair $(\mathbb{C}/\mathcal{O}, \mathfrak{n}^{-1}/\mathcal{O})$ is an elliptic curve with a cyclic subgroup of order N. The associated point $\xi \in X_0(N)$ is called the **Heegner point** attached to k.

Properties of Heegner Points

Quite a lot is known about the arithmetic properties of Heegner points. Let $\xi \in X_0(N)$ be a Heegner point attached to the quadratic imaginary field k. The theory of complex multiplication implies that

$$k(\xi) = H_k = \text{the Hilbert class field of } k.$$

Thus

$$\big[k(\xi) : k\big] = h_k \approx \sqrt{\mathrm{Disc}_k}\,.$$

Computationally, it is worth mentioning that there is a subexponential algorithm to compute the degree of the field $k(\xi)$.

Class field theory and the theory of complex multiplication provide an explicit description of the action of $\mathrm{Gal}\big(k(\xi)/k\big)$ on $k(\xi)$, analogous to the theory of cyclotomic fields.

Deuring Lifts and Heegner Points

Let $\tilde{E}/\mathbb{F}_p$ be an (ordinary) elliptic curve defined over a finite field and let $\tilde{C} \subset \tilde{E}(\mathbb{F}_p)$ be a cyclic subgroup of order N. The pair $(\tilde{E}, \tilde{C})$ defines a point

$$\tilde{\xi} = (\tilde{E}, \tilde{C}) \in X_0(N)(\mathbb{F}_p).$$

Let

$$\mathcal{O} = \mathrm{End}(E) \qquad \text{and} \qquad k = \mathcal{O} \otimes \mathbb{Q},$$

so k is a quadratic imaginary field and $\mathcal{O}$ is an order in k. For simplicity, we assume that $\mathcal{O}$ is the ring of integers of k.

Theorem. (Deuring) *There is a Heegner point $\xi \in X_0(N)(H_k)$ associated to k and a prime ideal $\mathfrak{p}$ of H_k so that*

$$\xi \bmod \mathfrak{p} = \tilde{\xi}.$$

Elliptic Curves
and
Modular Parametrizations

Modular Parametrizations

Let $E/\mathbb{Q}$ be an elliptic curve. A

Modular Parametrization of E

is a finite morphism

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

Theorem. (Wiles et. al.) *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N. Then E has a modular parametrization $\Phi : X_0(N) \to E$ defined over $\mathbb{Q}$.*

In practice, if N is small, one can explicitly write down and work with a modular parametrization, either algebraically or complex analytically.

Heegner Points on E

For the remainder of this talk, we fix an elliptic curve $E/\mathbb{Q}$ and a modular parametrization defined over $\mathbb{Q}$,

$$\Phi_E : X_0(N) \longrightarrow E.$$

Let $\xi \in X_0(N)$ be a Heegner point on $X_0(N)$ attached to k. Then we say that

$P = \Phi_E(\xi) \in E$ is a
Heegner point
of E attached to k.

Since $k(\xi) = H_k$, it follows that Heegner points on E also generate fields of large degree,

$$[k(P) : k] \geq \frac{h_k}{\deg \Phi_E} \approx \frac{\sqrt{\mathrm{Disc}_k}}{\deg \Phi_E}.$$

Independence of Heegner Points

Collections of Heegner Points on E

We can get points in $E(\mathbb{Q})$ by using the trace map:

$$\mathrm{Trace}_{H_k/\mathbb{Q}}(P) = \sum_{\sigma \in \mathrm{Gal}(H_k/\mathbb{Q})} \sigma(P) \in E(\mathbb{Q}).$$

Theorem. (Gross, Zagier, Kohnen) *All traces of all Heegner points on E generate a subgroup of $E(\mathbb{Q})$ of rank at most 1.*

In another direction, Rubin, Kolyvagin, and others have studied families of Heegner points $P_1, P_2, P_3, \ldots$ satisfying norm compatability (Euler system) conditions. These points are defined over towers of ring class fields $k_1 \subset k_2 \subset k_3 \subset \cdots$ of a single quadratic imaginary field k.

We ask a question of a somewhat different flavor.

When Are Heegner Points Independent?

Question. Are Heegner points associated to distinct fields independent?

Under a mild class number condition, we show that the answer is **YES**.

Definition. We write m^{odd} for the largest odd divisor of an integer m.

Independence of Heegner Points on E

Theorem. (Rosen, Silverman) *Let*

$E/\mathbb{Q}$	*an elliptic curve without CM.*
Φ_E	*a modular parametrization of* E.
$k_1, \ldots, k_t$	*distinct quadratic imaginary fields.*
$h_1, \ldots, h_t$	*the class numbers of* $k_1, \ldots, k_t$.
$P_1, \ldots, P_t$	*Heegner points on* E *for* $k_1, \ldots, k_t$.

There is a constant $C = C(E, \Phi_E)$ *such that*

$$h_1^{\text{odd}}, \ldots, h_t^{\text{odd}} > C$$

$$\Longrightarrow$$

$P_1, \ldots, P_t$ *are independent.*

Independence of Heegner Points Sketch of the Proof

Plan of Attack

The overall plan to prove the theorem may be summarized as follows:

$P_1, \ldots, P_t$ are independent if their fields of definition are

sufficiently large,

sufficiently disjoint,

and sufficiently abelian.

Strong Disjointedness of Class Fields of Quadratic Fields

The "sufficiently disjoint" part follows from a general result on class fields of quadratic fields.

Proposition. Set the following quantities:

$$\begin{aligned} k/\mathbb{Q} &\quad \text{a Galois extension with group } (\mathbb{Z}/2\mathbb{Z})^r \\ K &\quad \text{Hilbert class field of } k \\ N &\quad = 2^r - 1 \\ k_1, \ldots, k_N &\quad \text{the distinct quadratic subfields of } k \\ K_1, \ldots, K_N &\quad \text{the Hilbert class fields of } k_1, \ldots, k_N \end{aligned}$$

Then for all $2 \leq i \leq r$, the degree

$$\left[K_i \cap k_i \prod_{j \neq i} K_j \ : \ k_i \right] \quad \text{is a power of 2.}$$

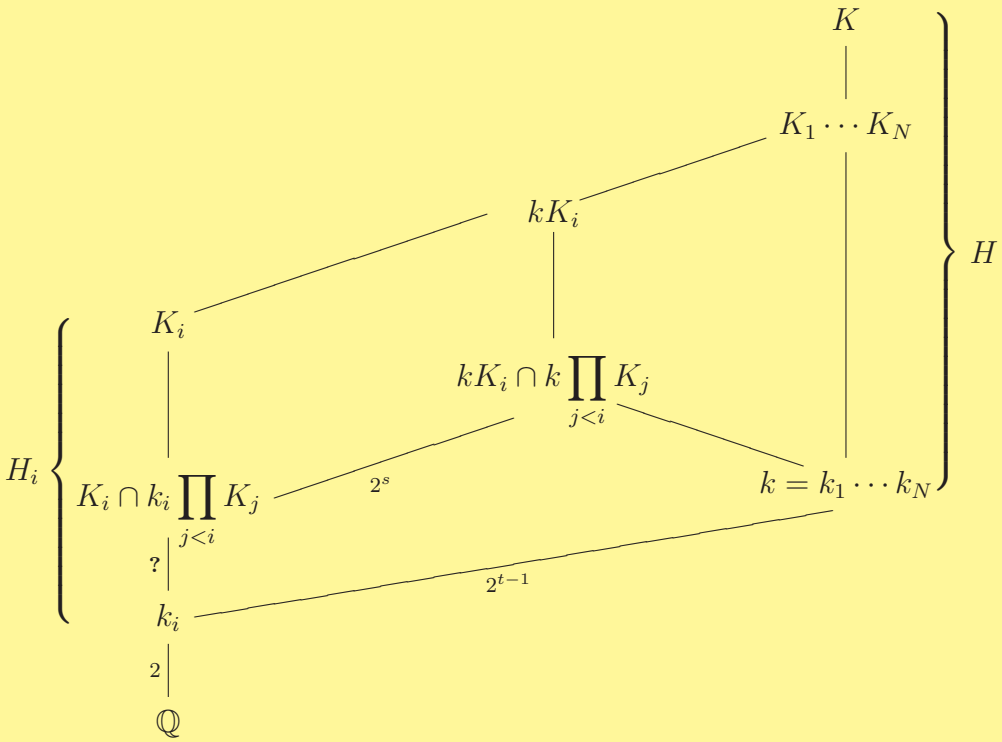
Thus up to 2-power extensions, each K_i is linearly disjoint from the *compositum* of all of the other K_j.

Proof of Strong Disjointedness

The proof uses class field theory and idempotent relations to analyze

$$\mathcal{C}\ell(K)^{\mathrm{odd}} \quad \text{as a} \quad \mathbb{Z}\left[\tfrac{1}{2}\right]\left[\mathrm{Gal}(K/\mathbb{Q})\right]\text{-module.}$$

Thus the **?** is a 2-power extension.



Sketch of the Proof of Independence of Heegner Points

Assume that $P_1, \ldots, P_t$ are a minimal dependent set and write

$$n_t P_t = \sum_{i=1}^{t-1} n_i P_i.$$

To ease notation, let

$$n = n_t, \qquad P = P_t, \qquad k = k_t.$$

Also let

$$\begin{aligned} K &= k_1 k_2 \cdots k_t, \\ \mathcal{C}\ell(K) &= \text{ideal class group of } K, \\ H_i &= \text{Hilbert class field of } k_i. \end{aligned}$$

Step 1: $[k(nP) : k]$ is a power of 2

Proof: The fact that $nP = \sum n_i P_i$ implies that

$$K(nP) \subset KH_t \cap KH_1H_2 \cdots H_{t-1}.$$

The maximal disjointedness theorem then tells us that

$$\big[K(nP) : K\big] \quad \text{is a power of 2.}$$

This completes the proof of Step 1, since $[K : k]$ is also a power of 2.

Step 2: There is a constant C_0 such that

$$\big[k(P) : k(mP)\big] \;\big|\; C_0 \quad \text{for all } m \geq 1.$$

Proof: There are two parts to Step 2.

For the first part, we apply Serre's Theorem stating that the image of

$$\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\hat{\mathbb{Z}})$$

is open. Thus the image of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ in $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ has bounded index, independent of m, so it tends to be highly nonabelian.

Note that this is where we are using our "no CM" assumption.

Step 2 (continued): The second part of Step 2 is the following

Lemma. *Let*

$\Gamma \subset \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ *a subgroup,*

$I(\Gamma)$ *the index of* Γ *in* $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$,

$W \subset (\mathbb{Z}/m\mathbb{Z})^2$ *a* Γ*-invariant submodule.*

Assume that the action of Γ *on* W *is* **abelian**. *Then*

$$|W| \leq I(\Gamma)^3.$$

The proof is elementary, but somewhat intricate.

- The Chinese Remainder Theorem reduces it to the case that m is a prime power.
- What is the best exponent? We can prove $I(\Gamma)^2$ and can show that $I(\Gamma)^{4/3-\epsilon}$ is not possible.
- What is true for GL_n?

Step 3: $\big[k(P) : k\big]^{\mathrm{odd}} \mid C_0^{\mathrm{odd}}$

Proof: Use Steps 1 and 2 on the odd parts of

$$\big[k(P) : k\big] = \big[k(P) : k(nP)\big]\big[k(nP) : k\big].$$

Step 4: $\big[k(\xi) : k(P)\big] \mid (\deg \Phi_E)!$

Proof: Follows from our earlier observation that

$$\big[k(\xi) : k(P)\big] \leq \deg \Phi_E.$$

Step 5: $C = \big(C_0(\deg \Phi_E)!\big)^{\mathrm{odd}}$ works

Proof: Combining Steps 1–4 tells us that

$$h_t^{\mathrm{odd}} = \big[k(\xi) : k\big]^{\mathrm{odd}} = \big[k(\xi) : k(P)\big]^{\mathrm{odd}}\big[k(P) : k\big]^{\mathrm{odd}}$$

divides C, contradicting the assumption $h_t^{\mathrm{odd}} > C$.

Final Remarks and Open Questions

Remarks on the Odd Class Number Condition

Is the condition $h_i^{\text{odd}} \geq C$ necessary? (Do need $h_i \geq C$.)

We don't know, but it is certainly necessary at several stages of our proof!

Further, it is true for "most" quadratic fields.

Theorem. (Soundararajan) *Let $k_1, k_2, \ldots$ be the list of all quadratic imaginary fields arranged in order of increasing absolute discriminant. Then for any constant C,*

$$\#\{k_i : h_{k_i}^{\text{odd}} \leq C \text{ and } |D_{k_i}| \leq X\} \ll X \frac{(\log\log X)^6}{\log X}$$

Additional Questions

- Is the "no CM" condition necessary?
- Prove analogous results for Heegner points associated to nonmaximal orders.

Motivation — Elliptic Curve Discrete Logarithms

A motivation for this research was an idea to solve the

Elliptic Curve Discrete Logarithm Problem (ECDLP)

by using Heegner Points and Deuring's Lifting Theorem.

In order for the method to work, we would need Heegner points from different quadratic imaginary fields to have at least a small tendency to be dependent. So a consequence of our independence theorem is that the method does not work.

The general idea of solving ECDLP by lifting to global fields has been tried in various contexts, although no one has found a practical method.

ECDLP and Lifting

Let $\bar{P}, \bar{Q} \in \bar{E}(\mathbb{F}_p)$.

ECDLP: Find m so that $\bar{Q} = m\bar{P}$.

Very roughly, here is the lifting approach to ECDLP:

1. Choose many multiples $\bar{R}_i = a_i\bar{P} - b_i\bar{Q}$.
2. Let $\Phi : X_0(N) \to E$. Find $\bar{\xi}_i \in X_0(N)(\mathbb{F}_p)$ with $\Phi(\bar{\xi}_i) = \bar{R}_i$.
3. Use Deuring's Theorem to lift $\bar{\xi}_i$ to a Heegner point $\xi_i \in X_0(N)(\bar{\mathbb{Q}})$.
4. Take the image points $R_i = \Phi(\xi_i) \in E(\bar{\mathbb{Q}})$.
5. If $R_1, \ldots, R_t$ are dependent, take a linear relation and reduce mod p to get a relation between $\bar{P}$ and $\bar{Q}$.

The independence theorem says that Step 5 is unlikely to work.

Heegner Points for Real Quadratic Fields

Henri Darmon has described a way to (conjecturally) attach a Heegner point $P_k \in E(\bar{\mathbb{Q}})$ to a *real* quadratic field k. The construction uses Tate's p-adic uniformization

$$\mathbb{C}_p^* \longrightarrow E(\mathbb{C}_p).$$

Conjecurally, "Darmon-Heegner points" share many properties with classical Heegner points, including the fact that P_k is defined over the Hilbert class field of k.

In particular, if k has class number 1, which is quite common, and if $w(E/\mathbb{Q}) = -1$, then P_k is in $E(\mathbb{Q})$. Hence if $P_1, \ldots, P_r$ are Darmon-Heegner points with $r > \operatorname{rank} E(\mathbb{Q})$, then they are dependent.

An open problem is to find an analog of the Deuring Lifting Theorem in the setting of Darmon-Heegner points.