Heegner Points

on Mordell Curves

Arav V. Karighattam
Massachusetts Institute of Technology

2026 AMS Eastern Sectional Meeting
March 28, 2026, Boston College

The Problem

Consider the elliptic curve with equation $y^2 = x^3 + D$, for any rational number D. When does it have rational points?

For example:

- If $D = 1$, there are 6 rational points: $O, (-1, 0), (0, \pm 1), (2, \pm 3)$.
- If $D = 5$, there are infinitely many rational points, generated by $(-1, 2)$.
- If $D = 7$, there are no rational points other than O.

Recall by the Mordell-Weil theorem that the rational points on an elliptic curve E form a finitely generated abelian group $E(\mathbb{Q})$. We wish to understand the (*algebraic*) *rank* of $E(\mathbb{Q})$.

Upper bounds are usually obtained from Selmer groups, and lower bounds from Heegner points. We use the latter!

Some recent work on cases where Heegner points have been used to show that $E(\mathbb{Q})$ has rank 1:

- Gross–Zagier (1986) + others: Rational points on E if it has analytic rank 1 over $\mathbb{Q}$
- Satgé (1987), Elkies (1994), and others: $x^3 + y^3 = k$ ($\cong y^2 = x^3 - 432k^2$) when k is a prime or product of two primes satisfying congruence conditions
- Monsky (1992), Tian (2012), and others: Rational points on $ny^2 = x^3 - x$; n can have many prime factors (Tian), with congruence and class group conditions
- Burungale–Skinner (2022): CM elliptic curves with correct p-Selmer group and good ordinary reduction at p

Main Result

Let a and b be squarefree integers such that 6, a, and b are pairwise relatively prime and $|a||b|^{-1} \equiv 5$ or $7 \pmod 9$. Let $D = a/b$ and $K = \mathbb{Q}(\sqrt[3]{D})$, and suppose the class number h_K of K is odd. Our main result is the following.

THEOREM. *If $a \equiv b \pmod 4$, then $y^2 = x^3 + D$ has algebraic rank 1 over $\mathbb{Q}$. If $a \equiv -b \pmod 4$, then $y^2 = x^3 + D$ has algebraic rank 0 over $\mathbb{Q}$.*

Why the condition on h_K?

Idea. Our proof uses Heegner points, and that method isn't known to work on curves of rank > 1 (Kolyvagin).

But if $D = 113$, $y^2 = x^3 + D$ has three independent (integer!) points $(-4, 7)$, $(2, 11)$, and $(8, 25)$.

Modular Curves

Recall $\mathrm{PSL}_2\,\mathbb{Z}$ acts on $\mathbb{H}^*$ (extended upper half plane) by linear fractional transformations. For a congruence subgroup $\Gamma \leq \mathrm{PSL}_2\,\mathbb{Z}$, the *modular curve* $X(\Gamma)$ is $\Gamma\backslash\mathbb{H}^*$ (over $\mathbb{C}$).

Examples:

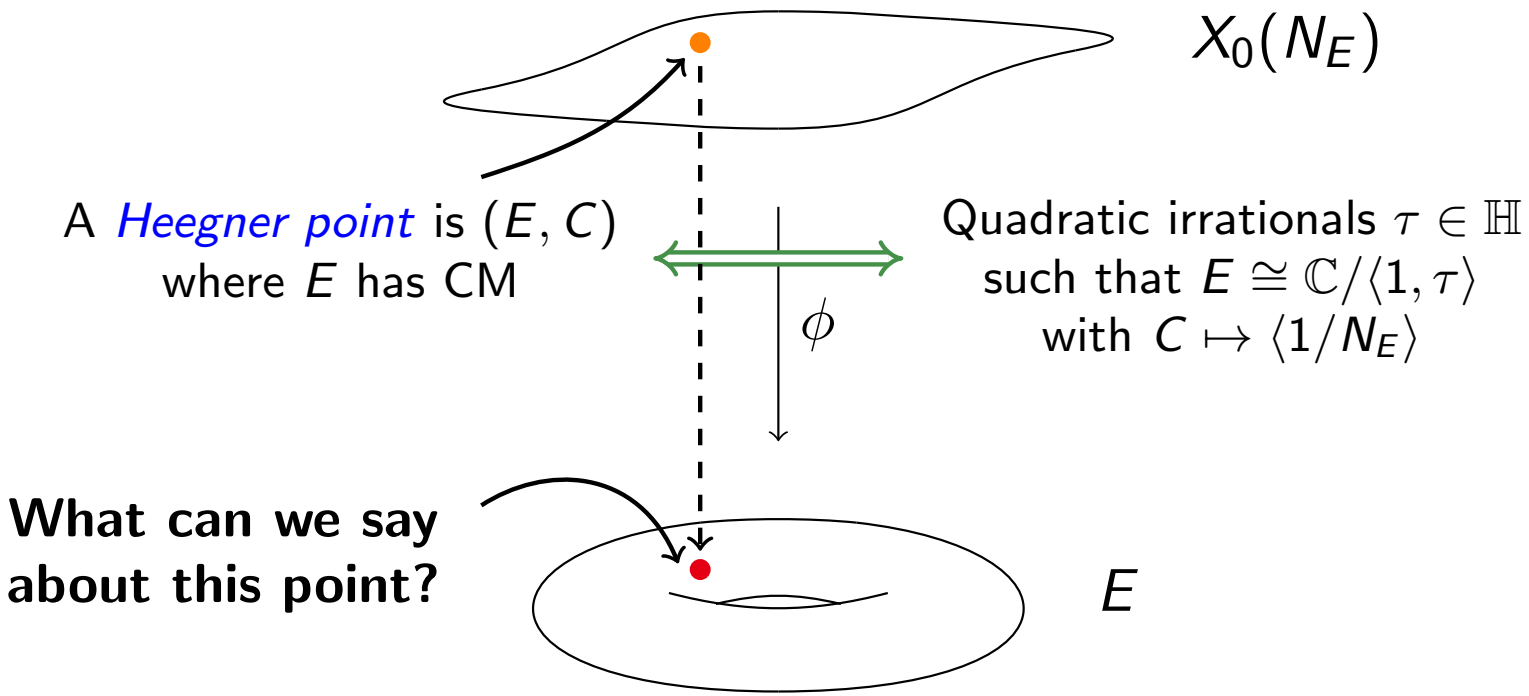
- $X_0(N) \setminus$ cusps ($\Gamma = \Gamma_0(N)$) parametrizes elliptic curves E and an order N cyclic subgroup of $E[N]$
- $X(N) \setminus$ cusps ($\Gamma = \Gamma(N)$) parametrizes elliptic curves E and two generators of $E[N]$ with a fixed Weil pairing
- Meromorphic functions on $X(\Gamma)$ are *modular functions* of level Γ.

Modular curves also define algebraic curves over $\mathbb{Q}$; functions are modular functions with rational Fourier coefficients at ∞.

Heegner Points

Modularity Theorem: $E/\mathbb{Q}$ elliptic curve, N_E its conductor $\Longrightarrow$ $\exists$ surjective morphism $\phi\colon X_0(N_E) \to E$ defined over $\mathbb{Q}$.

We call this a *modular parametrization* of E.



Shimura Reciprocity

For any $\tau \in \mathbb{H}$, the quotient $\mathbb{C}/\langle 1, \tau \rangle$ defines an elliptic curve $4y^2 = x^3 - g_2(\tau)x - g_3(\tau)$, with $z \mapsto (\wp(z;\tau), \wp'(z,\tau))$.

If $k/\mathbb{Q}$ is imaginary quadratic and $\mathcal{O} = \langle 1, \tau \rangle \subseteq k$ is an order, the corresponding elliptic curve has CM by $\mathcal{O}$.

Moreover, if f is any "good" modular function, $f(\tau) \in k^{ab}$!

Example: The *Fricke functions* on $X(N)$ send $\tau \mapsto x(P)$ for a given N-torsion point P on the associated elliptic curve.

As a consequence of the theory of CM, Shimura computed the action of $\mathrm{Gal}(k^{ab}/k)$ of special values of the Fricke functions.

THEOREM. *(Shimura, 1971) If f is a Fricke function, $f(\tau) \in k^{ab}$. For any $s \in \mathbb{A}_k^\times$, the associated automorphism $[s, K] \in \mathrm{Gal}(k^{ab}/k)$ sends $f(\tau) \mapsto g(\gamma\tau)$ for some Fricke function g and $\gamma \in \mathrm{GL}_2(\mathbb{Q})$, both easily computable in terms of f, s.*

Theory for our curves I

Recall that we are interested in the family $E_D\colon y^2 = x^3 + D$. Let $k := \mathbb{Q}(\sqrt{-3})$.

- E_1 has conductor 36, and $X_0(36) \cong X(6)$
- We can *explicitly define* a modular parametrization $(/k)$ $\phi = (X, Y)\colon X(6) \to E_1$ using Fricke functions of level 6
- E_D has CM by k and E_D is isogenous to E_{-27D} over $\mathbb{Q}$
- Idea: we can get points in $E_D(\mathbb{Q})$ from $E_1(k(\sqrt[3]{D}))$
- $k(\sqrt[3]{D})/k$ is abelian, so can use Heegner points on E_1!

If $D = a/b$ as in our main result, choose $n = |a||b|^5$ and let us consider the image of $n\omega \in \mathbb{H}$, where $\omega = e^{2\pi i/3}$.

Shimura reciprocity $\implies$ $\phi(n\omega) \in R_{6n}$, the *ring class field* of the order $\mathbb{Z}[6n\omega] \subseteq k$. For our choice of n, $\sqrt[3]{D} \in R_{6n}$!

Theory for our curves II

Trick to getting a point on E_D (generalization of Satgé, 1987):

Let $\widetilde{E}_a$ be $X^3 + Y^3 = a$ for any $a \in \mathbb{Q}$. Choose a genus one curve C which is isomorphic to $\widetilde{E}_2$ over $L := \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{n})$ and admits a degree 9 isogeny $\lambda\colon C \to \widetilde{E}_{2n^2}$ over $\mathbb{Q}$.

$$\begin{array}{ccccccccc} E_1 & \xrightarrow{\cong/k} & \widetilde{E}_2 & \xrightarrow{\cong/L} & C & \xrightarrow{\lambda} & \widetilde{E}_{2n^2} & \xrightarrow{\cong/k(\sqrt{\rho n})} & E_{\rho n} \\ \cup & & & & & & & & \cup \\ \phi(n\omega) & & & & & & & & P \\ \text{def.}/R_{6n} & \longmapsto & R_{6n} & \longmapsto & R_n & \longmapsto & R_n & \longmapsto & R_n \end{array}$$

Point: Choose C such that the image of $\phi(n\omega)$ in C is defined over R_n, not just R_{6n}. (Let $\rho := (-1)^{(n-1)/2}$.)

Define the Heegner point trace $S := \mathrm{tr}_{R_n/\mathbb{Q}}\, P \in E_{\rho n}(\mathbb{Q})$.
Is this point nontrivial?

Norms of special values

To show that S is nontrivial, we use our new result on the norms of special values of our modular function X of level 6.

Inspired by the following classical theorem (Dirichlet, 1840) ...

- If $D \equiv 1 \pmod 4$ squarefree, $(a/D) = -1$, $K = \mathbb{Q}(\sqrt{D})$,

$$N_{\mathbb{Q}(\zeta_D)/K}\left(\frac{1-\zeta_D^a}{1-\zeta_D}\right) = u^{2h_K}$$

  where $u > 1$ is a fundamental unit of $\mathcal{O}_K$; $\zeta_D = e^{2\pi i/D}$.

... we prove the following theorem.

THEOREM. *Under our hypotheses of n, let u be the fundamental unit of the ring of integers of $K = \mathbb{Q}(\sqrt[3]{n})$. Then*

$$N_{R_{6n}/K}(X(n\omega)+1) = 3^{f(n)}u^{3h_K\sigma(n/n')}$$

where n' is the largest squarefree divisor of n.

Nontorsion points

Let $K := \mathbb{Q}(\sqrt[3]{D})$ and $L \supseteq K$ be a number field. The connecting homomorphism of the Galois cohomology of

$$0 \to E[2] \to E \to E \to 0$$

induces a map

$$r_L \colon E_{\rho n}(L)/2E_{\rho n}(L) \to L^\times/(L^\times)^2, \quad (x, y) \mapsto x + \rho\sqrt[3]{n}.$$

By our result on the norms of special values of modular functions, we show that $r_L(s)$ lands nontrivially in $L^\times/(L^\times)^2$! Moreover, we can conclude the following.

THEOREM. *Under our assumptions on D, the point S is an odd multiple of the generator of $E_D(\mathbb{Q})$.*

Cassels (1950) proved that $\mathrm{rk}(E_D/\mathbb{Q}) + \mathrm{rk}(E_{-D}/\mathbb{Q}) \leq 1$ under our hypotheses on D, concluding the proof of the main result.

Thank you!