

CONSTRUCTING RATIONAL POINTS ON ELLIPTIC CURVES USING HEEGNER POINTS

KIMBERLY HOPKINS
OCTOBER 26, 2006

ABSTRACT. These are the notes I wrote for my candidacy talk. The aims for this talk were to understand Heegner points, examine the different ways they can be characterized, and get an idea of how to construct rational points on an elliptic curve using Heegner points. I cite some good references at the end if you are also trying to begin learning about this beautiful topic.

The goal of this talk is to explain how Heegner points provide us with a (non-torsion) rational point on a given (rank 1) rational elliptic curve.

We will do this using a rather abstract approach, and if time permits, we will explain a more concrete construction which is good for numerical computations.

Let $Y_0(N)$ be the open modular curve over \mathbb{Q} which is defined by,

$$Y_0(N)(\mathbb{C}) = \left\{ (E, E', \phi) : \phi : E \rightarrow E' \text{ isogeny with } \ker \phi \text{ cyclic of order } N \right\} / \sim,$$

(i.e. its points correspond to N -isogenous pairs of elliptic curves defined over \mathbb{C}), (where $(E, E', \phi) \sim (\tilde{E}, \tilde{E}', \tilde{\phi})$ if there exist isomorphisms ψ, ψ'

$$(0.1) \quad \begin{array}{ccc} E & \xrightarrow{\phi} & E' \\ \psi \downarrow & & \downarrow \psi' \\ \tilde{E} & \xrightarrow{\tilde{\phi}} & \tilde{E}' \end{array}$$

such that the above diagram commutes.)

Let $X_0(N)$ be the natural compactification of $Y_0(N)$, that is, the modular curve over \mathbb{Q} which classifies N -isogenous generalized elliptic curves.

1. HEEGNER POINTS IN $X_0(N) = \{(E, E', \phi)\}$

Given $(E, E', \phi) \in Y_0(N)(\mathbb{C})$, we get a corresponding pair of N -isogenous tori and a holomorphic (identity preserving) map

$$\phi : \mathbb{C}/M \rightarrow \mathbb{C}/M'$$

where $E \cong \mathbb{C}/M, E' \cong \mathbb{C}/M'$, and $\ker \phi \cong M'/M \cong \mathbb{Z}/N\mathbb{Z}$ is cyclic of order N (by homothety we may assume $M \subset M'$).

And we can choose bases so that

$$M = \mathbb{Z} + \mathbb{Z}\tau \quad \text{and} \quad M' = \frac{1}{N}\mathbb{Z} + \mathbb{Z}\tau$$

for some $\tau \in \mathbb{H}$.

Special thanks to my advisor, Fernando Rodriguez-Villegas, for all his help.

Recall that E is said to have complex multiplication (CM) if

$$\mathcal{O} := \text{End}(E) \supset (\text{properly contains}) \mathbb{Z}.$$

In this case $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Q} =: K$ is an imaginary quadratic field with $\mathcal{O} \subseteq \mathcal{O}_K$ an order of K , and $K = \mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\tau)$ where D is the discriminant of K .

Definition 1.1. A Heegner point of level N and discriminant D is a point $(E, E', \phi) \in Y_0(N)(\mathbb{C}) \subset X_0(N)(\mathbb{C})$ such that E and E' have the same ring \mathcal{O} of CM, i.e.

$$\text{End}(E) = \text{End}(E') = \mathcal{O} \subset K.$$

Let \mathcal{H}_N^D denote the set of Heegner points of level N and discriminant D .

(We will see later that \mathcal{H}_N^D is in fact a finite set.)

Let's assume for this talk that $\mathcal{O} = \mathcal{O}_K$, the maximal order, i.e. the ring of integers of K .

1.1. Possible Orders for Heegner Points. The first question we want to address is *which* (maximal) orders satisfy the above conditions.

Up to \sim in $X_0(N)$, a Heegner point is of the form

$$\mathbb{C}/\mathfrak{a} \rightarrow \mathbb{C}/\mathfrak{a}(\mathfrak{n}^{-1}), \quad (\mathfrak{a} \mapsto \mathfrak{a}(\mathfrak{n}^{-1}))$$

for some $[\mathfrak{a}] \in Cl(\mathcal{O}_K)$ and for some ideal \mathfrak{n} (of norm N) such that $\mathcal{O}_K/\mathfrak{n}\mathcal{O}_K \cong \mathbb{Z}/N\mathbb{Z}$ is cyclic of order N .

I.e. $E := \mathbb{C}/\mathfrak{a}$, $E' := \mathbb{C}/\mathfrak{a}(\mathfrak{n}^{-1})$, and $\phi : E \rightarrow E'$ is the natural isogeny.

Note that replacing \mathfrak{a} in the above with any other representative of its class in $Cl(\mathcal{O}_K)$ gives the same Heegner point (by the \sim relation on $Y_0(N)$).

Hence a Heegner point can be determined by the data,

$$(\mathcal{O}_K, \mathfrak{n}, [\mathfrak{a}])$$

Note that there are $h(D)$ Heegner points for each \mathfrak{n} , and that we get all the Heegner points as we vary \mathfrak{n} , (that is, \mathfrak{n} such that $\mathcal{O}_K/\mathfrak{n} \cong \mathbb{Z}/N\mathbb{Z}$).

2. SHIMURA CONSTRUCTION

Let

$$\Phi_{AJ} : X_0(N) \rightarrow \mathfrak{J}_0(N) := \Omega^1(X_0(N))^\vee / H_1(X_0(N), \mathbb{Z})$$

be Abel-Jacobi map, which is defined by,

$$P \mapsto \left(\omega \mapsto \int_{P_0}^P \omega \right)$$

where $\Omega^1(X_0(N))$ is the (vector) space of holomorphic differentials on $X_0(N)$, $H_1(X_0(N), \mathbb{Z})$ is the first homology group, and P_0 (in our case) the (rational) point at infinity in $X_0(N)$.

Let $S_2(\Gamma_0(N))$ be the space of weight 2 cusp forms on $\Gamma_0(N)$. Since

$$S_2(\Gamma_0(N)) \cong \Omega^1(X),$$

(by the map $f(\tau) \mapsto \omega_f := 2\pi i f(\tau) d\tau$) we can write the Jacobian of $X_0(N)$ as

$$\mathfrak{J}_0(N) \cong S_2(\Gamma_0(N))^\vee / H_1(X_0(N), \mathbb{Z}).$$

Let \mathbb{T} be the Hecke algebra generated over \mathbb{Z} by the Hecke operators $\{T_n\}$ (a commutative subalgebra of $\text{End}_{\mathbb{C}}(S_2(\Gamma_0(N)))$). The Hecke operators then give rise to endomorphisms of $\mathfrak{J}_0(N)$ defined over \mathbb{Q} .

Let W_N be the Atkin-Lehner involution on \mathbb{H} defined by

$$W_N(\tau) := -\frac{1}{N\tau}.$$

W_N (normalizes $\Gamma_0(N)$ and hence) passes to the quotient, $X_0(N)$, so is an involution of $X_0(N)$, and in fact (non trivially) also an involution of $\mathfrak{J}_0(N)$.

Fix a normalized newform $f \in S_2(\Gamma_0(N), \mathbb{Z})$, where $S_2(\Gamma_0(N), \mathbb{Z})$ is the space of modular forms in $S_2(\Gamma_0(N))$ whose Fourier expansion at infinity has integer coefficients. Since f is a normalized newform, there exists a \mathbb{Z} -algebra homomorphism,

$$\lambda : \mathbb{T} \rightarrow \mathbb{Z}$$

attached to f that satisfies

$$T_n f = \lambda(T_n) f \quad \forall T_n.$$

Furthermore f is also an eigenform for W_N , (because W_N stabilizes the one dimensional subspace in $S_2^{\text{new}}(\Gamma_0(N))$ that contains f), so

$$W_N f = \epsilon f$$

where $\epsilon = \pm 1$ is the eigenvalue of W_N acting on this subspace. Also $W_n \in \mathbb{T}$ (not trivial).

Let I_f be the ideal generated by $\ker(\lambda)$, so

$$I_f = \ker(\lambda) \langle T_n - \lambda(T_n) \rangle \subseteq \mathbb{T}.$$

Since the Hecke operators give endomorphisms of $\mathfrak{J}_0(N)/\mathbb{Q}$, we may consider the image $I_f(\mathfrak{J}_0(N)) \subset \mathfrak{J}_0(N)$ and form the quotient

$$\mathfrak{J}_0(N)/I_f(\mathfrak{J}_0(N)).$$

This is in fact an elliptic curve, E_f , (because it is an abelian variety of dimension 1 over \mathbb{Q}), and we have the maps

$$X_0(N) \rightarrow \mathfrak{J}_0(N) \rightarrow \mathfrak{J}_0(N)/I_f(\mathfrak{J}_0(N)) = E_f$$

whose composition is a non-constant (hence surjective) morphism,

$$\phi : X_0(N) \rightarrow E_f$$

defined over \mathbb{Q} .

(In fact, the existences of the last two maps are equivalent. That is, given $X_0(N) \rightarrow E$ for some elliptic curve E , there exists an f so that the quotient $J_0(N)/I_f(J_0(N))$ is isogenous to E .)

3. RATIONAL POINTS ON ELLIPTIC CURVES

From Wiles (and others) we know that all elliptic curves over \mathbb{Q} are isogenous (over \mathbb{Q}) to some E_f .

Let E/\mathbb{Q} be any elliptic curve of conductor N . Then there exists a normalized new form $f \in S_2(\Gamma_0(N))$ such that

$$\mathfrak{J}_0(N)/I_f(\mathfrak{J}_0(N)) = E_f,$$

and we have the map

$$X_0(N) \rightarrow \mathfrak{J}_0(N) \rightarrow \mathfrak{J}_0(N)/I_f(\mathfrak{J}_0(N)) \rightarrow E$$

(the last map is the isogeny over \mathbb{Q}) which gives the so called "modular parametrization" map, the surjective morphism,

$$\phi : X_0(N) \rightarrow E$$

defined over \mathbb{Q} .

Let P_E be the sum of all the $h(D)$ Heegner points of discriminant D for a fixed \mathfrak{n} ,

$$P_E = \sum_{\mathfrak{a} \in Cl(\mathcal{O}_K)} (\mathcal{O}_K, \mathfrak{n}, [\mathfrak{a}]) \in \text{Div}(X_0(N)).$$

We want to show that P_E gives a rational point on our elliptic curve, that is

$$\phi(P_E) := \sum_{\mathfrak{a} \in Cl(\mathcal{O}_K)} \phi((\mathcal{O}_K, \mathfrak{n}, [\mathfrak{a}])) \in E(\mathbb{Q}),$$

This will mainly follow from the claim below,

Claim. $P_E \in \text{Div}(X_0(N))(K)$

which we now prove.

Let H be the Hilbert Class Field of K , i.e. the maximal unramified abelian extension of K . From class field theory, we know $H = K(j(\mathcal{O}_K))$ (where j is the j -invariant) so our Heegner point $(\mathcal{O}_K, \mathfrak{n}, [\mathfrak{a}])$ is in H , hence

$$P_E \in \text{Div}(X_0(N))(H).$$

Now we will show that P_E is in fact in K .

Let $\sigma \in \text{Gal}(H/K)$ be any automorphism of $\text{Gal}(H/K)$. Then (by the Artin-Reciprocity theorem) $\sigma = \left(\frac{H/K}{\mathfrak{b}}\right)$ (the Artin map) for some $[\mathfrak{b}] \in Cl(\mathcal{O}_K)$ and we have

$$\begin{aligned} P_E^\sigma &= \sum_{\mathfrak{a} \in Cl(\mathcal{O}_K)} (\mathcal{O}_K, \mathfrak{n}, [\mathfrak{a}])^\sigma \\ &= \sum_{\mathfrak{a} \in Cl(\mathcal{O}_K)} (\mathcal{O}_K, \mathfrak{n}, [\mathfrak{a}])^{\left(\frac{H/K}{\mathfrak{b}}\right)} \\ &= \sum_{\mathfrak{a} \in Cl(\mathcal{O}_K)} (\mathcal{O}_K, \mathfrak{n}, [\mathfrak{a}\mathfrak{b}^{-1}]) \quad (\text{Shimura Reciprocity Law}) \\ &= \sum_{\mathfrak{a} \in Cl(\mathcal{O}_K)} (\mathcal{O}_K, \mathfrak{n}, [\mathfrak{a}]) \quad (\text{since } [\mathfrak{a}\mathfrak{b}^{-1}] \text{ runs through all the class of } Cl(\mathcal{O}_K) \text{ as } \mathfrak{a} \text{ does}) \\ &= P_E. \end{aligned}$$

Therefore

$$P_E^\sigma = P_E \quad \forall \sigma \in \text{Gal}(H/K)$$

so $P_E \in \text{Div}(X_0(N))(K)$.

So far we have that

$$\phi(P_E) = \sum_{\mathfrak{a} \in Cl(\mathcal{O}_K)} \phi((\mathcal{O}_K, \mathfrak{n}, [\mathfrak{a}])) \in E(K)$$

(because ϕ is defined over \mathbb{Q} , (and hence over K)) and now we will show that it is a *rational* point.

Observe that

$$\begin{aligned}
 W_N(P_E) &= \sum_{\mathfrak{a} \in \mathcal{CI}(\mathcal{O}_K)} (\mathcal{O}_K, \mathfrak{n}, [\mathfrak{a}])^{W_N} \\
 &= \sum_{\mathfrak{a} \in \mathcal{CI}(\mathcal{O}_K)} (\mathcal{O}_K, \bar{\mathfrak{n}}, [\mathfrak{a}\mathfrak{n}^{-1}]) \quad (\text{a result from the theory of CM}) \\
 &= \sum_{\mathfrak{a} \in \mathcal{CI}(\mathcal{O}_K)} (\mathcal{O}_K, \bar{\mathfrak{n}}, [\bar{\mathfrak{a}}]) \\
 &= \sum_{\mathfrak{a} \in \mathcal{CI}(\mathcal{O}_K)} \overline{(\mathcal{O}_K, \mathfrak{n}, [\mathfrak{a}])}.
 \end{aligned}$$

Hence

$$W_N(P_E) = \overline{P_E}.$$

As we said above, f is an eigenform for W_N and

$$W_N f = \epsilon f$$

where $\epsilon = \pm 1$.

Assume $\epsilon = +1$. (This is equivalent to the assumption that E has odd functional equation: from the correspondence between E and f we have, $\Lambda(E, s) = -\epsilon \Lambda(E, 2-s)$.)

So

$$W_n f = f$$

By construction, the quotient $\mathfrak{J}_0(N)/I_f(\mathfrak{J}_0(N))$ corresponds to the one-dimensional subspace of $S_2^{\text{new}}(\Gamma_0(N))$ containing f that is an eigenspace for all T_n and for W_N , which implies

$$\phi \circ W_N = \phi.$$

Putting the above two pieces together we get

$$\begin{aligned}
 \phi(P_E) &= \phi(W_N(P_E)) \quad \text{since } \phi = \phi \circ W_N, \\
 &= \phi(\overline{P_E}) \quad \text{since } W_N(P_E) = \overline{P_E}, \\
 &= \overline{\phi(P_E)} \quad \text{since } \phi \text{ is defined over } \mathbb{Q},
 \end{aligned}$$

which implies

$$\phi(P_E) \in E(\mathbb{Q})$$

as wanted.

4. CRITERIA FOR NONTRIVIAL RATIONAL POINTS ON E

So far we have given no reason why $\phi(P_E)$ is not a trivial or torsion point on $E(\mathbb{Q})$.

In 1983, Gross-Zagier proved,

Theorem 4.1. *If $\gcd(D, 2N) = 1$ and $D \neq -3$ then*

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

where \hat{h} is the canonical height function on $E(\mathbb{Q})$, $\text{Vol}(E)$ is the area of the period parallelogram, and E_D is the quadratic twist of E (defined by $E_D : y^2 D = x^3 + ax^2 + bx + c$ for $E : y^2 = x^3 + ax^2 + bx + c$).

If E has analytic rank equal to 1, then we can pick a fundamental discriminant $D < 0$ (with D a square modulo $4N$ and) with $L(E_D, 1) \neq 0$. (The existence of such a D is due to Bump, Friedberg, and Hoffstein). So $\hat{h}(\phi(P_E))$ is nonzero which is iff $\phi(P_E)$ is a non-torsion point.

Furthermore, from this theorem and from the work of (Victor) Kolyvagin, it follows that if the rank (analytic or algebraic) is strictly greater than 1, then this point, $\phi(P_E)$ will always be a torsion point.

(Kolyvagin proved that

$$\begin{aligned} \text{analytic rank equal to 0} &\Rightarrow \text{algebraic rank equal to 0, and} \\ \text{analytic rank equal to 1} &\Rightarrow \text{algebraic rank equal to 1.} \end{aligned}$$

So if the algebraic (or analytic) rank is greater than 1, then the analytic rank is greater than 1, so $L'(E, 1) = 0$ so the $\hat{h}(\phi(P_E)) = 0$ which is iff $\phi(P_E)$ is a torsion point.)

5. HEEGNER POINTS IN $X_0(N) = \mathbb{H}^*/\Gamma_0(N)$

The complex points of $Y_0(N)$ have the structure of an open Riemann surface, and are analytically isomorphic to the quotient space (which we will also denote as " $Y_0(N)$ "),

$$Y_0(N) = \mathbb{H}/\Gamma_0(N), \quad N \geq 3$$

where

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

And $X_0(N)(\mathbb{C})$ may be identified with the quotient

$$X_0(N) := \mathbb{H}^*/\Gamma_0(N)$$

where $\mathbb{H}^* = \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$.

The following can be given as the *definition* of Heegner points or by the definition we gave in our other viewpoint of $X_0(N)$,

Definition/Lemma 5.1. *Let τ be a CM point (i.e. τ is a root of $f_\tau = (A, B, C)$ with $D := \text{disc}(\tau) := \text{disc}(f_\tau) < 0$). τ is a Heegner point of level N and discriminant $D \pmod{\Gamma_0(N)}$ if*

$$D = \text{disc}(\tau) = \text{disc}(N\tau).$$

Note

$$\tau = \frac{-B + \sqrt{D}}{2A}.$$

From this it is not hard to prove,

Lemma 5.2. $\tau \in H_N^D \Leftrightarrow f_\tau = (A, B, C)$ with $A|N$ and $\text{gcd}(A/N, B, CN) = 1$.

Using the composition group law on BQF's gives an effective way to describe the set of all Heegner points of level N and discriminant D in $X_0(N) = \mathbb{H}^*/\text{SL}_2(\mathbb{Z})$,

Claim.

$$\mathcal{H}_N^D \leftrightarrow S := \left\{ \sqrt{D \pmod{4N} \pmod{2N}} \right\} \times \text{Cl}(D).$$

One direction of the above is easy. Given a Heegner point

$$\tau = \frac{-B + \sqrt{D}}{2A}$$

, let $f_\tau = (A, B, C)$ and send,

$$\tau \bmod \Gamma_0(N) \mapsto (B \bmod 2N, [f_\tau]).$$

For the other direction we need the following fact about BQF's,

Lemma 5.3. *Given any integer M , every class in $C(D)$ contains a primitive form $f = (M', b, c)$ such that $\gcd(M, M') = 1$.*

Let $(\beta, [f])$ be an element of the right hand side. Since $\beta^2 \equiv D \pmod{4N}$, there exists an integer c such that

$$D = \beta^2 - 4NC$$

hence $[h := (N, \beta, c)] \in Cl(D)$. Consider the class $[fh^{-1}] \in Cl(D)$. Pick $g \in [fh^{-1}]$ such that $g = (A', B', C')$ where $(A', N) = 1$ (possible by the lemma). Now consider the form gh . By the (Dirichlet) composition law,

$$gh = (NA', B, \frac{B^2 - D}{4NA'})$$

where B satisfies $B \equiv B' \pmod{2A'}$ and $B \equiv \beta \pmod{2N}$.

Let $f' := (A, B, C) = (NA', B, \frac{B^2 - D}{4NA'})$. We have shown there exists a form $f' \in [f]$ such that $N|A$ and $B \equiv \beta \pmod{2N}$, so we can send

$$(\beta, [f]) \mapsto \tau := \frac{-B + \sqrt{D}}{2A}.$$

Fixing an n and varying over all elements of $Cl(\mathcal{O}_K)$ thus corresponds to fixing a β and varying over all elements of $Cl(\sqrt{D})$.

Let $\mathcal{H}_N^D(\beta)$ be the subset of $\tau \in \mathcal{H}_N^D$ such that the associated form $f_\tau = (A, B, C)$ has $B \equiv \beta \pmod{2N}$.

There is an analytic description of ϕ given by the map

$$\begin{aligned} \phi : X_0(N) = \mathbb{H}^* / \text{SL}_2(\mathbb{Z}) &\rightarrow \mathbb{E} \\ \tau &\mapsto \int_{P_0}^\tau f(z) dz. \end{aligned}$$

Then the above work shows that

$$\phi(P_E) = \sum_{\tau \in \mathcal{H}_N^D(\beta)} \phi(\tau) = \sum_{f \in Cl(\mathcal{O}_K)} \phi(\beta \times f) \in \mathbb{E}(\mathbb{Q}).$$

REFERENCES

1. B. Birch, *Heegner Points: The Beginnings*, Heegner Points and Rankin L-Series, MSRI Publications, **49**, 2004.
2. D. Cox, *Primes of the Form $x^2 + ny^2$* , Wiley, New York, 1989.
3. H. Darmon, *Rational points on modular elliptic curves*, CBMS Regional Conference Series in Mathematics, **101**. Published for the Conference Board of the Mathematical Sciences, Washington, DC; by the American Mathematical Society, Providence, RI, 13-39, 2004.
4. B. Gross, *Heegner Points on $X_0(N)$* , in: *Modular Forms* (ed. R.A. Rankin), 87-106, Chichester: Ellis Horwood, 1984.
5. K. Heegner, *Diophantische analysis and modulfunktionen*, *Mathematische Zeitschrift*, **56**, 237-238, 1952.
6. J.S. Milne, *Elliptic Curves*, online notes, 1996.

7. M. Watkins, *Some remarks on Heegner point computations*, 2006, arXiv:math.NT/0506325 v2.
8. D. Zagier, *Modular points, modular curves, modular surfaces and modular forms*, Workshop Bonn 1984, 225-248, Lecture Notes in Mathematics, **1111**, Springer, Berlin, 1985.