p-ADIC HEIGHTS OF HEEGNER POINTS AND Λ-ADIC REGULATORS

JENNIFER S. BALAKRISHNAN, MIRELA ÇIPERIANI, AND WILLIAM STEIN

Abstract. Let E be an elliptic curve defined over $\mathbb{Q}$. The aim of this paper is to make it possible to compute Heegner L-functions and anticyclotomic Λ-adic regulators of E, which were studied by Mazur-Rubin and Howard.

We generalize results of Cohen and Watkins and thereby compute Heegner points of non-fundamental discriminant. We then prove a relationship between the denominator of a point of E defined over a number field and the leading coefficient of the minimal polynomial of its x-coordinate. Using this relationship, we recast earlier work of Mazur, Stein, and Tate to produce effective algorithms to compute p-adic heights of points of E defined over number fields. These methods enable us to give the first explicit examples of Heegner L-functions and anticyclotomic Λ-adic regulators.

Introduction

Let $E/\mathbb{Q}$ be an elliptic curve defined over the rationals, p an odd rational prime of good ordinary reduction, and $K/\mathbb{Q}$ an imaginary quadratic extension satisfying the Heegner hypothesis. We consider the anticyclotomic $\mathbb{Z}_p$-extension K_∞/K. Denote by $K_n \subseteq K_\infty$ the intermediate extension of degree p^n over K. Following Mazur and Rubin [14] we define the *anticyclotomic universal norm module*

$$\mathcal{U} = \varprojlim_n E(K_n) \otimes \mathbb{Z}_p,$$

where the transition maps are the trace maps. Note that $\mathcal{U}$ is a module over $\Lambda = \varprojlim_n \mathbb{Z}_p[\mathrm{Gal}(K_n/K)]$. The complex conjugation $\tau \in \mathrm{Gal}(K_\infty/\mathbb{Q})$ acts on $\mathcal{U}$ and on $\mathrm{Gal}(K_\infty/K)$: $\tau\sigma\tau^{-1} = \sigma^{-1}$ for every $\sigma \in \mathrm{Gal}(K_\infty/K)$. We now consider the Λ-module $\mathcal{U}^{(\tau)}$ where $\mathcal{U}^{(\tau)}$ is equal to $\mathcal{U}$ as an abelian group but $\sigma \cdot u := \tau\sigma\tau^{-1}(u)$ for all $\sigma \in \mathrm{Gal}(K_\infty/K)$. Then we have the cyclotomic p-adic height pairing

$$h : \mathcal{U} \otimes_\Lambda \mathcal{U}^{(\tau)} \to \Gamma_{\mathrm{cycl}} \otimes_{\mathbb{Z}_p} \Lambda \otimes_{\mathbb{Z}_p} \mathbb{Q}_p,$$

where Γ_{cycl} denotes the Galois group of the cyclotomic $\mathbb{Z}_p$-extension $K_\infty^{\mathrm{cycl}}/K$. We will throughout restrict our attention to the case of the elliptic curves $E/\mathbb{Q}$ of ordinary non-anomalous reduction at p and primes p that do not divide the product of the Tamagawa numbers. It then follows that the p-adic height pairing takes values in $\Gamma_{\mathrm{cycl}} \otimes_{\mathbb{Z}_p} \Lambda$. By work of Cornut [5] and Vatsal [21] we know that $\mathcal{U}$ is free of rank one over Λ. This implies that the image of the cyclotomic p-adic height pairing is generated by an element $\mathcal{R} \in \Gamma_{\mathrm{cycl}} \otimes_{\mathbb{Z}_p} \Lambda$, the Λ-*adic regulator* of E. Our main motivation for this paper was to compute examples of the Λ-adic regulator of E. In order to do this we use Heegner points under conditions which ensure that these points give rise to the full module of universal norms,

Date: August 2, 2013.

2010 *Mathematics Subject Classification.* 11Y40, 11G50, 11G05.

Key words and phrases. Elliptic curve, p-adic heights, Heegner points.

The first author was supported by NSF grant DMS-1103831. The second author was supported by NSA grant H98230-12-1-0208. The third author was supported by NSF Grants DMS-1161226 and DMS-1147802.

then compute modulo powers of p the coefficients of the Heegner L-function, which in this case is equal to the Λ-adic regulator of E (see Section 2).

To explicitly compute coefficients of Heegner L-functions, one needs to compute p-adic heights of Heegner points of *non-fundamental* discriminant defined over ring class fields. We begin by proving a correspondence between such Heegner points and certain quadratic forms (see Section 1), generalizing various results of Watkins [22] and Cohen [4, §8.6]. While this correspondence has previously been invoked in the literature, we have been unable to find an account of its theoretical basis. We use these results to give algorithms that construct Heegner points in $E(K_n)$, as well as the full set of conjugates under the action of the Galois group $\mathrm{Gal}(K_n/K)$; see Section 3. Next, since these Heegner points are defined over number fields, we discuss how to adapt the techniques of Mazur, Stein, and Tate [15] to this situation. In particular, [15] gives an algorithm to compute the cyclotomic p-adic height of a rational point $P \in E(\mathbb{Q})$ on an elliptic curve E defined over $\mathbb{Q}$, in terms of two functions: (1) the p-adic sigma function associated to E and (2) the denominator of P. They also give similar formulas to handle the case when E and the point P are defined over a number field.

We discuss effective methods to compute cyclotomic p-adic heights, following [15], when E is defined over $\mathbb{Q}$ but the point P is defined over a number field F. In particular, since our elliptic curve is defined over $\mathbb{Q}$, no generalization of their p-adic sigma function algorithm is needed. However, the naive generalization of the denominator algorithm involves the factorization of several ideals in the ring of integers $\mathcal{O}_F$ which becomes infeasible as the degree of the number field grows. In Section 4 we prove that the denominator of P is determined by the leading coefficient of the minimal polynomial of the x-coordinate of P. This result allows us to give an algorithm to compute cyclotomic p-adic heights which avoids factoring and any additional use of the coordinates of P as elements of a number field. We then simplify it further for the computation of cyclotomic p-adic heights of Heegner points.

Building on this work, in Section 5 we discuss the computation of p-adic height pairings of Galois conjugates of Heegner points. With these algorithms in hand, in Section 6 we provide the first explicit examples of Heegner L-functions and hence Λ-adic regulators. Conjecture 6 of [14] (which the authors of [14] have retracted; see [11], page 815) posited, in effect, that the Λ-adic regulator is a constant times a unit. The examples we obtain provide the first "highly likely" counterexamples to that conjecture. One common feature of all the Λ-adic regulators that we have computed is that they have no cyclotomic roots, i.e. they are non-zero at the roots of $(T+1)^{p^n} - 1 = 0$ for every $n \in \mathbb{N}$.

Remark 0.1. We do not give explicit bounds on the necessary precision of our numerical computations, so we do not obtain "provably correct" computational results. Instead, we apply consistency checks on the results, which suggest that they are *highly likely* to be correct. "Highly likely" results are sufficient for our main goal, which is to numerically investigate a question of Mazur and Rubin about Λ-adic regulators to clarify what should be conjectured and proved via theoretical methods.

Acknowledgments. The authors would like to thank Barry Mazur and Karl Rubin for bringing the question of computing Heegner L-functions to their attention.

1. Heegner points and binary quadratic forms

In this section, we generalize various aspects of Watkins [22], and Cohen [4, §8.6] to nonfundamental discriminant. Because these basic facts are crucial to the rest of this paper, we give precise statements with well-defined notation and proofs, instead of leaving the details to the reader.

Let τ be a quadratic irrational in the complex upper half plane $\mathcal{H}$. Let

$$f_\tau = (A, B, C) \longleftrightarrow Ax^2 + Bxy + Cy^2$$

be the associated integral primitive positive definitive binary quadratic form, so that $A\tau^2+B\tau+C=0$ with $A>0$ and $\gcd(A,B,C)=1$. The discriminant $\Delta(\tau)$ is $\Delta(f_\tau)=B^2-4AC$, which is negative. We do *not* assume that $\Delta(\tau)$ is a fundamental discriminant.

1.1. **Heegner points.** A *Heegner point* of level N and discriminant D is a quadratic irrational in the upper half plane such that $\Delta(\tau)=D=\Delta(N\tau)$. Let $\mathcal{H}_N^D$ be the set of Heegner points of level N and discriminant D. We will assume the *Heegner Hypothesis*: the primes dividing N split in $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$.

Proposition 1.1. *Let $\tau\in\mathcal{H}$ be a quadratic irrational with $f_\tau=(A,B,C)$ of discriminant D. Then $\tau\in\mathcal{H}_N^D$ if and only if $N\mid A$ and $\gcd(A/N,B,CN)=1$.*

Proof. First note that $\tau=\frac{-B+\sqrt{D}}{2A}$, so $N\tau=\frac{-NB+N\sqrt{D}}{2A}$.
($\implies$) Suppose $\tau\in\mathcal{H}_N^D$, so $\Delta(\tau)=\Delta(N\tau)$. Writing $f_{N\tau}=(A',B',C')$, we have $N\tau=\frac{-B'+\sqrt{D}}{2A'}=\frac{-NB+N\sqrt{D}}{2A}$; equating real and imaginary parts yields $A=NA'$ and $B=B'$, so $C=\frac{B^2-D}{4A}=\frac{(B')^2-D}{4NA'}=C'/N$. Then $\gcd(A',B',C')=1$, which holds by definition, is equivalent to $\gcd(A/N,B,CN)=1$.

($\impliedby$) Let $A'=A/N$, $B'=B$ and $C'=NC$. Under our hypothesis, $A',B',C'\in\mathbb{Z}$, A' is positive, $\gcd(A',B',C')=1$, and we have $(A/N)(N\tau)^2+B(N\tau)+(CN)=0$, hence $f_{N\tau}=(A',B',C')$. Thus $\Delta(N\tau)=(B')^2-4A'C'=B^2-4(A/N)(NC)=\Delta(\tau)$, so $\tau\in\mathcal{H}_N^D$. □

Proposition 1.2. *The set $\mathcal{H}_N^D$ is non-empty if and only if D is a square modulo $4N$.*

Proof. Assuming that $\mathcal{H}_N^D$ is non-empty we let $f_\tau=(A,B,C)$ correspond to some $\tau\in\mathcal{H}_N^D$. By Proposition 1.1, we have $N\mid A$, so $D=B^2-4N(A/N)C$ is a square modulo $4N$.

If D is a square modulo $4N$, we have that $D=B^2-4NC$ for some $B,C\in\mathbb{Z}$. Consider the binary quadratic form (N,B,C). Observe that since $\gcd(D,N)=1$ we have that $\gcd(N,B,C)=\gcd(1,B,CN)=1$. Then by Proposition 1.1 we know that the quadratic irrational of the upper half plane τ that corresponds to (N,B,C) is an element of $\mathcal{H}_N^D$. Hence $\mathcal{H}_N^D$ is non-empty. □

Let $\tau\in\mathcal{H}$ and $\delta\in M_2(\mathbb{Q})$ be a matrix of positive determinant. We know that $\delta(\tau):=\delta\begin{pmatrix}\tau\\1\end{pmatrix}\in\mathcal{H}$ and we now analyze the affect of this action on the corresponding quadratic forms if τ is a quadratic irrational.

Lemma 1.3. *Let $\gamma\in M_2(\mathbb{Z})$ be a matrix of positive determinant and $f_\tau=(A,B,C)$ for some quadratic irrational $\tau\in\mathcal{H}$. If $m=\left(\begin{smallmatrix}A & B/2\\ B/2 & C\end{smallmatrix}\right)$ is the matrix that corresponds to the quadratic form f_τ, then $\gamma^t m\gamma$ is a positive integer multiple n of the matrix that corresponds to $f_{\gamma^{-1}(\tau)}$, where γ^t denotes the transpose of γ. Moreover, n can only be divisible by primes that divide* $\det(\gamma)$.

Proof. Let $v=\begin{pmatrix}\gamma^{-1}(\tau)\\1\end{pmatrix}$. Then $\gamma v=\begin{pmatrix}x\\y\end{pmatrix}$ with $x/y=\gamma(\gamma^{-1}(\tau))=\tau\in\mathcal{H}$ (so $\tau\neq\infty$). Then

$$v^t(\gamma^t m\gamma)v=(\gamma v)^t m(\gamma v)=(x,y)m\begin{pmatrix}x\\y\end{pmatrix}=y^2(\tau,1)m\begin{pmatrix}\tau\\1\end{pmatrix}=0.$$

Consequently, we have that $f_{\gamma^{-1}(\tau)}=(A'/n,B'/n,C'/n)$ where

$$\begin{pmatrix}A' & B'/2\\ B'/2 & C'\end{pmatrix}=\gamma^t\begin{pmatrix}A & B/2\\ B/2 & C\end{pmatrix}\gamma \tag{1.1}$$

and $n=\gcd(A',B',C')$ since both f_τ and $f_{\gamma^{-1}(\tau)}$ are positive definite binary quadratic forms. In particular, n is a positive integer.

Let ℓ be a prime divisor of $n = \gcd(A', B', C')$. If ℓ is odd, then viewing (1.1) modulo ℓ we find

$$\gamma^t m \gamma \equiv 0 \pmod{\ell}.$$

Then, since $\gcd(A, B, C) = 1$ implies that $m \not\equiv 0 \pmod{\ell}$, we deduce that $\ell \mid \det(\gamma)$.

If $\ell = 2 \nmid \det(\gamma)$, then since 2 divides B' we have that

$$\det \begin{pmatrix} A' & B'/2 \\ B'/2 & C' \end{pmatrix} = \det(\gamma)^2 (AC - B^2/4) \in \mathbb{Z}$$

and hence $(AC - B^2/4) \in \mathbb{Z}_2$, which then implies that 2 divides B. Consequently, the matrices in (1.1) lie in $M_2(\mathbb{Z})$. By the argument used for odd primes, we see that 2^2 cannot divide B'. Hence viewing (1.1) modulo 2 we have that

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \equiv \gamma^t \begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix} \gamma \pmod{2}. \tag{1.2}$$

Since $2 \nmid \det(\gamma)$, we know that there exists $\delta \in M_2(\mathbb{Z})$ such that $\gamma\delta \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{2}$. Then (1.2) implies that

$$\begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix} \equiv \delta^t \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \delta \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \pmod{2},$$

which is false, since $\gcd(A, B, C) = 1$. This completes the proof of the lemma. □

Lemma 1.4. *The set $\mathcal{H}_N^D$ is closed under the action of $\Gamma_0(N)$.*

Proof. Suppose $\gamma^{-1} \in \Gamma_0(N)$ and $\tau \in \mathcal{H}_N^D$ with $f_\tau = (A, B, C)$. Let $\tau' = \gamma^{-1}(\tau)$. Writing $f_{\tau'} = (A', B', C')$, Lemma 1.3 (using that $\det(\gamma) = 1$) implies that

$$\begin{pmatrix} A' & B'/2 \\ B'/2 & C' \end{pmatrix} = \gamma^t \begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix} \gamma,$$

so $\Delta(\tau') = \Delta(\tau) = D$ (since $\Delta < 0$), again because $\det(\gamma) = 1$. Observe that since $\gamma^{-1} \in \Gamma_0(N)$ we have that

$$N\tau' = N\gamma^{-1}(\tau) = \gamma_0^{-1}(N\tau)$$

for some $\gamma_0 \in \mathrm{SL}_2(\mathbb{Z})$. Hence the same argument applied to $N\tau$ implies that $\Delta(N\tau') = \Delta(N\tau) = D$, so $\tau' \in \mathcal{H}_N^D$. □

The above lemma allows us to consider the set $\Gamma_0(N)\backslash\mathcal{H}_N^D$ which we will analyze further in §1.3.

1.2. **Classes of ideals and binary quadratic forms.** Let K be an imaginary quadratic field and c a positive integer. Let $\mathcal{O}_c = \mathbb{Z} + c\mathcal{O}_K$ be the order of conductor c in $\mathcal{O}_K$, the ring of integers of K. The discriminant of $\mathcal{O}_c$ is $D = c^2 D_K$ where D_K is the discriminant of $\mathcal{O}_K$. We identify fractional ideal classes in $\mathcal{O}_c$ with equivalence classes with respect to the action of $\mathrm{SL}_2(\mathbb{Z})$ of primitive positive definite binary quadratic forms of discriminant D via the following inverse bijections (see [3, Theorem 5.2.8]):

$$\{\text{classes of primitive pos. def. binary quadratic forms of disc. } D\} \longleftrightarrow \{\text{fractional ideal classes in } \mathcal{O}_c\}$$

$$\Psi_{FI}(A, B, C) = A\mathbb{Z} + \frac{-B + \sqrt{D}}{2}\mathbb{Z},$$

and

$$\Psi_{IF}(\mathfrak{a})(x, y) = \frac{\mathcal{N}(x\omega_1 - y\omega_2)}{\mathcal{N}(\mathfrak{a})},$$

where $\mathcal{N}$ denotes the norm map of $K/\mathbb{Q}$, $\mathfrak{a} = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, and $\{\omega_1, \omega_2\}$ are ordered so that

$$\frac{\omega_2\sigma(\omega_1) - \omega_1\sigma(\omega_2)}{\sqrt{D}} > 0,$$

with σ denoting the generator of $\mathrm{Gal}(K/\mathbb{Q})$.

1.3. **Action of Atkin-Lehner involutions and the class group.** For each positive integer $q \mid N$ with $\gcd(q, N/q) = 1$, define an Atkin-Lehner matrix as follows: fix any choice $u, v \in \mathbb{Z}$ such that $w_q = \left(\begin{smallmatrix} uq & v \\ N & q \end{smallmatrix}\right)$ has determinant q. Then w_q induces a well-defined *involution* $W_q(\tau) := w_q(\tau)$ on $\Gamma_0(N)\backslash\mathcal{H}$. The involutions W_q commute and generate a group W isomorphic to $\mathbb{F}_2^\nu$, where ν is the number of prime divisors of N. We will now show that the group W acts of $\Gamma_0(N)\backslash\mathcal{H}_N^D$.

Lemma 1.5. *The set $\Gamma_0(N)\backslash\mathcal{H}_N^D$ is closed under the action of W_q.*

Proof. Let $\tau \in \mathcal{H}_N^D$ and $f_\tau = (A, B, C)$. As in Lemma 1.3 we have

$$w_q^t \begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix} w_q = \begin{pmatrix} Aq^2u^2 + BNqu + CN^2 & (2Aquv + Bq^2u + BNv + 2CNq)/2 \\ * & Av^2 + Bqv + Cq^2 \end{pmatrix},$$

where this matrix is a multiple of the matrix that corresponds to $f_{w_q^{-1}(\tau)}$. Since $q \mid N \mid A$, we see that q divides each entry of the right hand matrix above (or 2 times the upper right entry). Since w_q^t and w_q both have determinant q, it follows that $\Delta(w_q^{-1}(\tau)) \mid \Delta(\tau)$. Applying Lemma 1.4, we have $\Delta(w_q^{-1}(\tau)) = \Delta(w_q(\tau))$, since W_q is an involution of $\Gamma_0(N)\backslash\mathcal{H}$ and $\Gamma_0(N)$ preserves Δ. Applying the above argument with τ replaced by $w_q(\tau)$ implies that $\Delta(\tau) \mid \Delta(w_q(\tau))$. Thus $\Delta(w_q(\tau)) = \Delta(\tau)$. It remains to show that $\Delta(Nw_q(\tau)) = \Delta(w_q(\tau))$.

Observe that $Nw_q^{-1}(\tau) = \sigma_q^{-1}(N\tau)$ where $\sigma_q = \left(\begin{smallmatrix} uq & Nv \\ 1 & q \end{smallmatrix}\right)$. As above, we have that

$$\sigma_q^t \begin{pmatrix} A/N & B/2 \\ B/2 & CN \end{pmatrix} \sigma_q = \begin{pmatrix} (A/N)q^2u^2 + Bqu + CN & (2Aquv + Bq^2u + BNv + 2CNq)/2 \\ * & ANv^2 + BqNv + CNq^2 \end{pmatrix}$$

is a multiple of the matrix that corresponds to $f_{Nw_q^{-1}(\tau)}$. Since $\det(\sigma_q) = q$ and q divides all the entries of the above matrix (or 2 times the upper right entry), it follows that $\Delta(Nw_q^{-1}(\tau)) \mid \Delta(N\tau)$ which just as above implies that $\Delta(N\tau) \mid \Delta(Nw_q(\tau))$. Observing that $Nw_q(\tau) = (q^{-1}\sigma_q)(N\tau)$, we deduce that

$$(q\sigma_q^{-1})^t \begin{pmatrix} A/N & B/2 \\ B/2 & CN \end{pmatrix} (q\sigma_q^{-1}) = \begin{pmatrix} (A/N)q^2 - Bq + CN & (-2Aqv + Bq^2u + BNv - 2CNuq)/2 \\ * & ANv^2 - BuqNv + CNu^2q^2 \end{pmatrix}$$

is a multiple of the matrix that corresponds to $f_{Nw_q(\tau)}$. Since $\det(q\sigma_q^{-1}) = q$ and q divides each entry of the above matrix we have that $\Delta(Nw_q(\tau)) \mid \Delta(N\tau)$. It then follows that

$$\Delta(Nw_q(\tau)) = \Delta(N\tau) = \Delta(\tau) = \Delta(w_q(\tau)).$$

This proves that $w_q(\tau) \in \mathcal{H}_N^D$. □

Remark 1.6. Observe that in the above proof we have shown that the matrix of $f_{w_q^{-1}(\tau)}$ equals $q^{-1}w_q^t \begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix} w_q$.

We will now define the action[1] of the ideal class group $\mathrm{Cl}(\mathcal{O}_c)$ on $\Gamma_0(N)\backslash\mathcal{H}_N^D$. Let $\tau \in \mathcal{H}_N^D$, $f_\tau = (A, B, C)$, and $\mathfrak{a} \in \mathrm{Cl}(\mathcal{O}_c)$. Then we define $\mathfrak{a} \cdot \tau \in \Gamma_0(N)\backslash\mathcal{H}_N^D$ as follows:

[1]This choice of the action of $\mathrm{Cl}(\mathcal{O}_c)$ on $\Gamma_0(N)\backslash\mathcal{H}_N^D$ is the one that is compatible with the action of the Galois group on Heegner points when they are viewed as points of an elliptic curve, see (2.1) and Gross [8, §1.4].

(1) First, consider the following class of primitive positive definite binary quadratic forms of discriminant D:
$$\Psi_{IF}(\Psi_{FI}(f_\tau)\mathfrak{a}^{-1}).$$
(2) Since we are assuming the Heegner Hypothesis, we have that $\gcd(N, D) = 1$ and consequently the class $\Psi_{IF}(\Psi_{FI}(f_\tau)\mathfrak{a}^{-1})$ contains an element (A', B', C') such that $\gcd(C', N) = 1$ and $B' \equiv B \pmod{2N}$. It follows that $A'C' \equiv AC \pmod{N}$ which implies that $N|A'$. Moreover, if $(A'', B'', C'') \in \Psi_{IF}(\Psi_{FI}(f_\tau)\mathfrak{a}^{-1})$ satisfies the conditions $\gcd(C'', N) = 1$ and $B'' \equiv B \pmod{2N}$ then
$$\begin{pmatrix} A'' & B''/2 \\ B''/2 & C'' \end{pmatrix} = \gamma^t \begin{pmatrix} A' & B'/2 \\ B'/2 & C' \end{pmatrix} \gamma \text{ for some } \gamma \in \Gamma_0(N).$$
(3) Set $f_{\mathfrak{a}\cdot\tau} = (A', B', C') \in \Psi_{IF}(\Psi_{FI}(f_\tau)\mathfrak{a}^{-1})$. By the above we know that $\mathfrak{a} \cdot \tau$ is a uniquely determined element of $\Gamma_0(N)\backslash\mathcal{H}_N^D$.

In order to see that we have defined a group action of $\mathrm{Cl}(\mathcal{O}_c)$ on $\Gamma_0(N)\backslash\mathcal{H}_N^D$, we observe that since
- the map $\mathfrak{a} \mapsto (\mathfrak{b} \mapsto \mathfrak{b}\mathfrak{a}^{-1})$ defines an action of $\mathrm{Cl}(\mathcal{O}_c)$ on $\mathrm{Cl}(\mathcal{O}_c)$, and
- Ψ_{FI} and Ψ_{IF} are inverses of one another,

it follows that
$$f_{\mathfrak{a}\cdot(\mathfrak{b}\cdot\tau)} \in \Psi_{IF}\big(\Psi_{FI}(f_\tau))(\mathfrak{a}\mathfrak{b})^{-1}\big) \qquad \text{for any } \mathfrak{a}, \mathfrak{b} \in \mathrm{Cl}(\mathcal{O}_c).$$
Then by (2) above we have that $\mathcal{O}_c \cdot \tau \in \Gamma_0(N)\tau$ and $\mathfrak{a} \cdot (\mathfrak{b} \cdot \tau) = (\mathfrak{a}\mathfrak{b}) \cdot \tau \in \Gamma_0(N)\backslash\mathcal{H}_N^D$.

Lemma 1.7. *The actions of W and $\mathrm{Cl}(\mathcal{O}_c)$ on $\Gamma_0(N)\backslash\mathcal{H}_N^D$ commute.*

Proof. Let $\tau \in \mathcal{H}_N^D$, $f_\tau = (A, B, C)$, and q a positive integer such that $q|N$ and $\gcd(q, N/q) = 1$. As in Lemma 1.5 we fix $u, v \in \mathbb{Z}$ such that $uq - vN/q = 1$ and set $w_q = \left(\begin{smallmatrix} uq & v \\ N & q \end{smallmatrix}\right)$. In addition, we now consider the matrix $m_q := \left(\begin{smallmatrix} 1 & -v \\ -N/q & uq \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Observe that
$$m_q^t w_q^t \begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix} w_q m_q = q \begin{pmatrix} A/q & B/2 \\ B/2 & Cq \end{pmatrix}.$$
Using Remark 1.6, we deduce that $f_{w_q^{-1}(\tau)}$ is equivalent to $(A/q, B, Cq)$.

Let us now set $I_{B,q} := q\mathbb{Z} + \frac{-B+\sqrt{D}}{2}\mathbb{Z}$. Notice that $I_{B,q}$ is an ideal of $\mathcal{O}_c$. Moreover, since $D = B^2 - 4AC$ and $\gcd(B, q) = 1$ we have
$$\begin{aligned} \Psi_{FI}(f_{w_q^{-1}(\tau)})I_{B,q} &= \left(A/q\mathbb{Z} + \frac{-B+\sqrt{D}}{2}\mathbb{Z}\right)\left(q\mathbb{Z} + \frac{-B+\sqrt{D}}{2}\mathbb{Z}\right) \\ &= A\mathbb{Z} + q\frac{-B+\sqrt{D}}{2}\mathbb{Z} + A/q\frac{-B+\sqrt{D}}{2}\mathbb{Z} + \left(AC + B\frac{-B+\sqrt{D}}{2}\right)\mathbb{Z} \\ &= A\mathbb{Z} + q\frac{-B+\sqrt{D}}{2}\mathbb{Z} + A/q\frac{-B+\sqrt{D}}{2}\mathbb{Z} + B\frac{-B+\sqrt{D}}{2}\mathbb{Z} \\ &= A\mathbb{Z} + \frac{-B+\sqrt{D}}{2}\mathbb{Z} \\ &= \Psi_{FI}(f_\tau). \end{aligned} \tag{1.3}$$

Now let $\mathfrak{a} \in \mathrm{Cl}(\mathcal{O}_c)$. We want to show that $\mathfrak{a} \cdot W_q(\tau) = W_q(\mathfrak{a} \cdot \tau)$ which, by our definition of the action of $\mathrm{Cl}(\mathcal{O}_c)$ on $\Gamma_0(N)\backslash\mathcal{H}_N^D$, is equivalent to showing that
$$\Psi_{FI}(f_{W_q(\mathfrak{a}\cdot\tau)}) = \Psi_{FI}(f_{W_q(\tau)})\mathfrak{a}^{-1},$$
where $f_{W_q(\tau)}$ denotes the equivalence class of $f_{w_q(\tau)}$ and hence contains $f_{w_q^{-1}(\tau)}$.

Using (1.3) and the commutativity of $\mathrm{Cl}(\mathcal{O}_c)$ we get

$$\Psi_{FI}(f_{W_q(\tau)})\mathfrak{a}^{-1} = \Psi_{FI}(f_\tau)I_{B,q}^{-1}\mathfrak{a}^{-1} = (\Psi_{FI}(f_\tau)\mathfrak{a}^{-1})I_{B,q}^{-1} = \Psi_{FI}(f_{\mathfrak{a}\cdot\tau})I_{B,q}^{-1} = \Psi_{FI}(f_{W_q(\mathfrak{a}\cdot\tau)}).$$

This completes the proof of the lemma. □

Consider the group $G = W \times \mathrm{Cl}(\mathcal{O}_c)$. The above lemma implies that we have a well-defined action of G on $\Gamma_0(N)\backslash\mathcal{H}_N^D$. We will now define the action of G on another set.

Let $\mathcal{S}(D,N)$ be the set of square roots modulo $2N$ of D mod $4N$, i.e.,

$$\mathcal{S}(D,N) = \{b \in \mathbb{Z}/2N\mathbb{Z} \ : \ b^2 \equiv D \pmod{4N}\}.$$

Lemma 1.8. *Let $b \in \mathcal{S}(D,N)$. For every positive integer $q|N$ such that $\gcd(q, N/q) = 1$ there exists $b_q \in \mathcal{S}(D,N)$ such that*

$$b_q \equiv b \pmod{2N/q} \quad \text{and} \quad b_q \equiv -b \pmod{2q}.$$

Proof. Since $\gcd(2q, 2N/q) = 2$ and $b \equiv -b \pmod 2$ we know that there exists $b_q \in \mathbb{Z}/2N\mathbb{Z}$ satisfying the above two conditions and it follows that

$$b_q^2 \equiv b^2 \pmod{4N/q} \quad \text{and} \quad b_q^2 \equiv b^2 \pmod{4q}.$$

Hence $b_q \in \mathcal{S}(D,N)$. □

Then for every integer $q > 1$ such that $q|N$ and $\gcd(q, N/q) = 1$ the involution W_q acts on $\mathcal{S}(D,N)$ as follows:

$$W_q \cdot b = b_q.$$

This defines the action of the group W on $\mathcal{S}(D,N)$.

We now define the action of W on the set $\mathcal{S}(D,N) \times \mathrm{Cl}(\mathcal{O}_c)$. Let q be a positive integer dividing N such that $\gcd(q,N) = 1$ and $(b,J) \in \mathcal{S}(D,N) \times \mathrm{Cl}(\mathcal{O}_c)$. Then we set

$$W_q \cdot (b,J) = (b_q, JI_{b,q}^{-1}),$$

where $I_{b,q} = q\mathbb{Z} + \frac{-b+\sqrt{D}}{2}\mathbb{Z} \in \mathrm{Cl}(\mathcal{O}_c)$, as in Lemma 1.7. In order to verify that this is a group action we show that $W_q \cdot (W_q \cdot (b,J)) = (b,J)$. Since

$$W_q \cdot (W_q \cdot (b,J)) = W_q(b_q, JI_{b,q}^{-1}) = (b, JI_{b,q}^{-1}I_{b_q,q}^{-1}),$$

it suffices to show that $(q\mathbb{Z} + \frac{-b+\sqrt{D}}{2}\mathbb{Z})(q\mathbb{Z} + \frac{-b_q+\sqrt{D}}{2}\mathbb{Z})$ is a principal ideal of $\mathcal{O}_c$.

By Lemma 1.8 we have that $b_q \equiv -b \pmod{2q}$ and hence $q\mathbb{Z} + \frac{-b_q+\sqrt{D}}{2}\mathbb{Z} = q\mathbb{Z} + \frac{b+\sqrt{D}}{2}\mathbb{Z}$. Observe that

$$\left(q\mathbb{Z} + \frac{-b+\sqrt{D}}{2}\mathbb{Z}\right)\left(q\mathbb{Z} + \frac{b+\sqrt{D}}{2}\mathbb{Z}\right) = \gcd\left(q^2, qb, \frac{b^2-D}{4}\right)\mathbb{Z} + q\frac{-b+\sqrt{D}}{2}\mathbb{Z}.$$

Since $(D,N) = 1$, $q|N$ and $b^2 \equiv D \pmod{4N}$, it follows that $4q \mid (b^2 - D)$ and $(b,q) = 1$. Consequently, $\gcd(q^2, qb, (b^2-D)/4) = q$. Finally, since b and D have the same parity, it follows that

$$\left(q\mathbb{Z} + \frac{-b+\sqrt{D}}{2}\mathbb{Z}\right)\left(q\mathbb{Z} + \frac{b+\sqrt{D}}{2}\mathbb{Z}\right) = q\left(\mathbb{Z} + \frac{D+\sqrt{D}}{2}\mathbb{Z}\right) = q\mathcal{O}_c.$$

We finally define the action of $\mathrm{Cl}(\mathcal{O}_c)$ on the set $\mathcal{S}(D,N) \times \mathrm{Cl}(\mathcal{O}_c)$ as follows. Let $I \in \mathrm{Cl}(\mathcal{O}_c)$ and $(b,J) \in \mathcal{S}(D,N) \times \mathrm{Cl}(\mathcal{O}_c)$. We set

$$I \cdot (b,J) = (b, JI^{-1}).$$

Since $\mathrm{Cl}(\mathcal{O}_c)$ is commutative, the actions of W and $\mathrm{Cl}(\mathcal{O}_c)$ on $\mathcal{S}(D,N) \times \mathrm{Cl}(\mathcal{O}_c)$ commute. Hence the group $G = W \times \mathrm{Cl}(\mathcal{O}_c)$ acts on $\mathcal{S}(D,N) \times \mathrm{Cl}(\mathcal{O}_c)$.

Lemma 1.9. *The action of G on $\mathcal{S}(D,N)\times \mathrm{Cl}(\mathcal{O}_c)$ is simply transitive.*

Proof. Since $(D,N)=1$, the only element of W that acts trivially on an element b of $\mathcal{S}(D,N)$ is the identity. It is then clear that the action of G on $\mathcal{S}(D,N)\times \mathrm{Cl}(\mathcal{O}_c)$ is free.

Observe that our assumption that all primes dividing N split in $\mathbb{Q}(\sqrt{D})/\mathbb{Q}$ implies that for every odd prime divisor p of N the equation $b^2 \equiv D \pmod{p^{n_p}}$ has two solutions; here $n_p = \mathrm{ord}_p(N)$. Finally, since D is a discriminant, $b^2 \equiv D \pmod{2^{n_2+2}}$ has a solution. Moreover,

i) if N is odd then $b^2 \equiv D \pmod 4$ has a unique solution $b \in \mathbb{Z}/2\mathbb{Z}$; and
ii) if N is even then $b^2 \equiv D \pmod{2^{n_2+2}}$ has exactly two solutions $b \in \mathbb{Z}/2^{n_2+1}\mathbb{Z}$.

This proves that the order of G equals the cardinality of the set $\mathcal{S}(D,N)\times \mathrm{Cl}(\mathcal{O}_c)$. Then since the stabilizer of $b \in \mathcal{S}(D,N)$ is trivial it follows that the action of G on $\mathcal{S}(D,N)\times \mathrm{Cl}(\mathcal{O}_c)$ is simply transitive. □

Define a map $\Phi : \Gamma_0(N)\backslash \mathcal{H}_N^D \to \mathcal{S}(D,N)\times \mathrm{Cl}(\mathcal{O}_c)$ by

$$[\tau] \in \Gamma_0(N)\backslash \mathcal{H}_N^D \longrightarrow (B \pmod{2N}, \Psi_{FI}(f_\tau)).$$

where $f_\tau = (A,B,C)$. Observe that the map Φ is well-defined:

- $\Phi(\tau) \in \mathcal{S}(D,N)\times \mathrm{Cl}(\mathcal{O}_c)$ since
  - f_τ is a primitive positive definite quadratic form of discriminant D,
  - $B^2 - 4AC = D$ and $N|A$ implies that $B \in \mathcal{S}(D,N)$;
- $\Phi(\tau) = \Phi(\tau')$ for $\tau' = \gamma\tau$ with $\gamma \in \Gamma_0(N)$ because
  - by Lemma 1.3 we know that f_τ and $f_{\tau'}$ lie in the same equivalence class under the action of $\mathrm{SL}_2(\mathbb{Z})$ which implies that $\Psi_{FI}(f_{\tau'}) = \Psi_{FI}(f_\tau)$,
  - if $f_{\tau'} = (A',B',C')$ then $B \equiv B' \pmod{2N}$ since

$$\begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix} = \gamma^t \begin{pmatrix} A' & B'/2 \\ B'/2 & C' \end{pmatrix} \gamma$$

    with $\gamma \in \Gamma_0(N)$ and $N \mid A'$.

Theorem 1.10. *The map $\Phi : \Gamma_0(N)\backslash \mathcal{H}_N^D \to \mathcal{S}(D,N)\times \mathrm{Cl}(\mathcal{O}_c)$ is an isomorphism of G-sets.*

Proof. We start by showing that Φ is injective. Let $\tau,\tau' \in \mathcal{H}_N^D$ and assume that $\Phi(\tau) = \Phi(\tau')$. It follows that $\Psi_{FI}(f_\tau) = \Psi_{FI}(f_{\tau'})$ which, by Theorem 5.2.8 of [3], implies that $f_\tau = (A,B,C)$ and $f_{\tau'} = (A',B',C')$ lie in the same equivalence class under the action of $\mathrm{SL}(2,\mathbb{Z})$ and hence

$$B' = 2Aab + B(ad+bc) + 2Ccd, \quad \text{where } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}).$$

Observe that since $ad - bc = 1$ we have that

$$B' = 2Aab + B + 2Bbc + 2Ccd.$$

Then the assumption that $\Phi(\tau) = \Phi(\tau')$ implies that $B \equiv B' \pmod{2N}$ and consequently

$$Aab + Bbc + Ccd \equiv 0 \pmod N.$$

Since $\tau,\tau' \in \mathcal{H}_N^D$, by Proposition 1.1, we know that $N|A$ and $N|A' = (Aa^2 + Bac + Cc^2)$. Hence

$$c(Bb+Cd) \equiv 0 \pmod N \quad \text{and} \quad c(Ba+Cc) \equiv 0 \pmod N.$$

If $N \nmid c$ then there exists p a prime divisor of N dividing both $Bb+Cd$ and $Ba+Cc$. This implies that p divides $C = a(Bb+Cd) - b(Ba+Cc)$, which in turn implies that p divides Ba and Bb. Since $(a,b)=1$, it follows that p divides B which in turns contradicts the assumption that $(N,D)=1$. Consequently

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N),$$

which proves that Φ is injective.

We will now show that Φ is a G-map. Let $\tau \in \Gamma_0(N)\backslash\mathcal{H}_N^D$, $\mathfrak{a} \in \mathrm{Cl}(\mathcal{O}_c)$, and $W_q \in W$. We start by verifying that Φ is a W-map. By Lemma 1.5 and Remark 1.6 we know that $f_{W_q(\tau)} = f_{w_q^{-1}(\tau)} = (A', B', C')$ where

$$B' = 2Auv + Bqu + B(N/q)v + 2CN \equiv \begin{cases} B(N/q)v - Bqu = -B & \pmod{2q} \\ Bqu - B(N/q)v = B & \pmod{2N/q} \end{cases}$$

since $qu - N/qv = 1$. This together with (1.3) implies that

$$\Phi(W_q(\tau)) = (B' \pmod{2N}, \Psi_{FI}(f_{W_q(\tau)})) = (B_q, \Psi_{FI}(f_\tau)I_{B,q}^{-1}) = W_q \cdot \Phi(\tau).$$

In order to see that Φ is a $\mathrm{Cl}(\mathcal{O}_c)$-map recall that we have defined $\mathfrak{a} \cdot \tau$ such that

$$f_{\mathfrak{a}\cdot\tau} = (A', B', C') \in \Psi_{IF}(\Psi_{FI}(f_\tau)\mathfrak{a}^{-1}) \quad \text{and} \quad B' \equiv B \pmod{2N}.$$

It follows that

$$\Phi(\mathfrak{a} \cdot \tau) = (B \pmod{2N}, \Psi_{FI}(f_\tau)\mathfrak{a}^{-1}) = \mathfrak{a} \cdot (B \pmod{2N}, \Psi_{FI}(f_\tau)).$$

Hence we conclude that Φ is a G-map.

Finally, since by Lemma 1.9 we know that G acts transitively on the codomain of Φ, it follows that Φ is surjective, and this completes the proof. □

Corollary 1.11. *The G-action on $\Gamma_0(N)\backslash\mathcal{H}_N^D$ is simply transitive.*

Proof. This follows immediately by Theorem 1.10 and Lemma 1.9. □

2. Heegner points and universal norms

Let us now consider an elliptic curve $E/\mathbb{Q}$, an imaginary quadratic field K, and an odd prime p such that

i) the discriminant D_K of K is at most -5;
ii) every prime dividing the conductor N of $E/\mathbb{Q}$ splits in $K/\mathbb{Q}$;
iii) p does not divide

$$ND_K h_K a_p(a_p - 1)\left(a_p - \left(\frac{D_K}{p}\right)\right)\prod_{\ell|N} c_\ell,$$

where h_K denotes the class number of K, $a_p = p+1-\#E(\mathbb{F}_p)$, $\left(\frac{D_K}{p}\right)$ denotes the Legendre symbol, and c_ℓ is the Tamagawa number of E at the prime ℓ.

We will now consider a Heegner point x_{p^n} of level N and discriminant $p^{2n}D_K$. We view x_{p^n} as an element of $X_0(N) = \Gamma_0(N)\backslash\mathcal{H}$. By Gross [8, §1.4] we know that $x_{p^n} \in X_0(N)(K[p^n])$, where $K[p^n]$ is the ring class field of K of conductor p^n, and the Galois group $\mathrm{Gal}(K[p^n]/K) \simeq \mathrm{Cl}(\mathcal{O}_{p^n})$ acts on x_{p^n} as follows:

$$\mathfrak{a} \cdot x_{p^n} = \mathrm{Artin}(\mathfrak{a})\,(x_{p^n}) \qquad \text{for all } \mathfrak{a} \in \mathrm{Cl}(\mathcal{O}_{p^n}), \tag{2.1}$$

where $\mathrm{Artin}(\mathfrak{a})$ denotes the image of $\mathfrak{a}$ in $\mathrm{Gal}(K[p^n]/K)$ under the Artin map.

Using a fixed choice of minimal modular parametrization $\pi : X_0(N) \to E$, we define

$$y_{p^n} = \pi(x_{p^n}) \in E(K[p^n]).$$

We will refer to y_n as a *Heegner point of conductor p^n*. Note that the action of Atkin-Lehner involutions on Heegner points of conductor p^n is well-understood since by [13, Theorem 9.27] we know that $\pi\left(W_q(x_{p^n})\right) - \epsilon_q y_{p^n} \in E(\mathbb{Q})_{\mathrm{tors}}$ where $\epsilon_q = \pm 1$. Hence, by Corollary 1.11 we know that

Heegner points of conductor p^n form a single orbit under the action of $\mathrm{Gal}(K[p^n]/K)$ up to sign and rational torsion.

The anticyclotomic $\mathbb{Z}_p$-extension K_∞ of K lies inside $K[p^\infty] := \cup_n K[p^n]$. Denote by K_n the unique subfield of K_∞ such that $\mathrm{Gal}(K_n/K) \simeq \mathbb{Z}/p^n\mathbb{Z}$. We know that under our assumption that $p \nmid h_K$ we have that $K_n \subseteq K[p^{n+1}]$. More precisely,

a) $K_0 = K$,
b) for all $n \geq 1$ $K_n \subseteq K[p^{n+1}]$ and $K_n \not\subseteq K[p^n]$,
c) $\mathrm{Gal}(K[p^{n+1}]/K_n) \simeq \mathrm{Gal}(K[p]/K)$ and its order equals $\left(p - \left(\frac{D_K}{p}\right)\right) h_K$.

Then the Heegner points defined over the anticylotomic $\mathbb{Z}_p$-extension are

$$z_0 = \mathrm{tr}_{K[1]/K}(y_1) \quad \text{and} \quad z_n = \mathrm{tr}_{K[p^{n+1}]/K_n}(y_{p^{n+1}}) \text{ for all } n \geq 1.$$

We will now list some properties of Heegner points:

- By the work of Gross-Zagier [7], we know that z_0 is not torsion if and only if the analytic rank of E/K, i.e., the order of vanishing of the L-function $L(E/K, s)$ of E/K, equals 1.
- The complex conjugation $\tau \in \mathrm{Gal}(K_\infty/\mathbb{Q})$ acts on the Heegner points z_n and by [9, Proposition 5.3], we know that $\tau z_n + \epsilon\sigma z_n \in E(\mathbb{Q})_{\mathrm{tors}}$ for some $\sigma \in \mathrm{Gal}(K_n/K)$ where ϵ is the sign of the functional equation of $E/\mathbb{Q}$.
- By [7, §3.1,§3.3] (see also [12, Lemma 4.2]), the Heegner point z_n lies, up to translation by a rational torsion point of E, in the connected component of the Néron model of E over K_{w_n} at all primes w_n of K_n that divide the conductor N (here K_{w_n} denotes the completion of K_n at w_n).
- The points z_n are related to one another as n varies. In [17, §3.3, Lemma 2], Perrin-Riou proves that

$$\mathrm{tr}_{K[p^{n+2}]/K[p^{n+1}]}(x_{p^{n+2}}) = a_p x_{p^{n+1}} - x_{p^n} \text{ for } n \geq 0,$$
$$\mathrm{tr}_{K[p]/K[1]}(x_p) = b_p x_1,$$

where

$$b_p = \begin{cases} a_p & \text{if } p \text{ is inert,} \\ a_p - \sigma - \sigma' \text{ for some } \sigma, \sigma' \in \mathrm{Gal}(K[1]/K) & \text{if } p \text{ splits.} \end{cases}$$

Since $\mathrm{Gal}(K[p^{n+1}]/K_n) \simeq \mathrm{Gal}(K[p]/K)$ for every $n \geq 0$, it follows that

$$\mathrm{tr}_{K_{n+2}/K_{n+1}}(z_{n+2}) = a_p z_{n+1} - z_n \text{ for } n \geq 1; \tag{2.2}$$
$$\mathrm{tr}_{K_2/K_1}(z_2) = \begin{cases} a_p z_1 - a_p z_0 & \text{if } p \text{ is inert,} \\ a_p z_1 - (a_p - 2) z_0 & \text{if } p \text{ splits;} \end{cases}$$
$$\mathrm{tr}_{K_1/K}(z_1) = \begin{cases} \big((a_p - 1)(a_p + 1) - p\big) z_0 & \text{if } p \text{ is inert,} \\ \big((a_p - 1)^2 - p\big) z_0 & \text{if } p \text{ splits.} \end{cases}$$

We can now see that for every $n \geq 0$, we have that $\mathrm{tr}_{K_{n+1}/K_n}(z_{n+1}) = u_n z_n$ for some unit $u_n \in \mathbb{Z}_p[\mathrm{Gal}(K_\infty/K)]$ if

$$p \text{ does not divide } (a_p - 1) a_p \left(a_p - \left(\frac{D_K}{p}\right)\right). \tag{2.3}$$

More precisely, under the above condition we have

$$u_0 = \begin{cases} (a_p-1)(a_p+1)-p & \text{if } p \text{ is inert,} \\ (a_p-1)^2-p & \text{if } p \text{ splits;} \end{cases}$$

$$u_1 = \begin{cases} a_p - a_p u_0^{-1}\,\mathrm{tr}_{K_1/K} & \text{if } p \text{ is inert,} \\ a_p - (a_p-2)u_0^{-1}\,\mathrm{tr}_{K_1/K} & \text{if } p \text{ splits;} \end{cases}$$

$$u_n = a_p - u_{n-1}^{-1}\,\mathrm{tr}_{K_n/K_{n-1}} \quad \text{for } n \geq 2.$$

Throughout the paper we assume condition (2.3) which in particular implies that E has good ordinary non-anomalous reduction at p. Following Mazur and Rubin [14] we consider the anticyclotomic universal norm module

$$\mathcal{U} = \varprojlim_n E(K_n) \otimes \mathbb{Z}_p,$$

where the transition maps are the trace maps. Observe that $\mathcal{U}$ is a module over $\Lambda = \varprojlim_n \mathbb{Z}_p[\mathrm{Gal}(K_n/K)]$. We set $\mathcal{U}^{(\tau)}$ to be equal to $\mathcal{U}$ as an abelian group but $\sigma \cdot u := \tau\sigma\tau^{-1}(u)$ for all $\sigma \in \mathrm{Gal}(K_\infty/K)$. Then the cyclotomic p-adic height pairing

$$h : \mathcal{U} \otimes_\Lambda \mathcal{U}^\tau \to \Gamma_{\mathrm{cycl}} \otimes_{\mathbb{Z}_p} \Lambda \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$$

is τ-Hermitian, i.e.

$$h(u \otimes v) = h(u \otimes v)^\tau = h(\tau u \otimes \tau v),$$

for all universal norms $u, v \in \mathcal{U}$. Observe that since p is a prime of ordinary non-anomalous reduction which does not divide the product of the Tamagawa numbers, the cyclotomic p-adic height pairing takes values in $\Gamma_{\mathrm{cycl}} \otimes_{\mathbb{Z}_p} \Lambda$.

By work of Cornut [5], Vatsal [21], and Bertolini [2] we know that $\mathcal{U}$ is free of rank one over Λ, see [14, Theorem 4]. This implies that the image of the cyclotomic p-adic height pairing is generated by the Λ-*adic regulator*[2] $\mathcal{R} \in \Gamma_{\mathrm{cycl}} \otimes_{\mathbb{Z}_p} \Lambda$. Note that $\mathcal{R}$ is uniquely determined only up to units of Λ. We would like to compute $\mathcal{R}$, and to do so we use Heegner points.

Heegner points give rise to the Heegner submodule $\mathcal{H} \subseteq \mathcal{U}$. Our assumption of the condition (2.3) implies that the points

$$c_0 = z_0 \quad \text{and} \quad c_n = \left(\prod_{i=0}^{n-1} u_i\right)^{-1} z_n \quad \text{for } n \geq 1$$

are trace compatible and correspond to an element $c \in \mathcal{H} \subseteq \mathcal{U}$. Mazur and Rubin define the *Heegner L-function*

$$\mathcal{L} := h(c \otimes \tau c) \in \Gamma_{\mathrm{cycl}} \otimes_{\mathbb{Z}_p} \Lambda.$$

One can easily see that $\mathcal{L} = \mathcal{R}\,\mathrm{char}(\mathcal{U}/\mathcal{H})\mathrm{char}(\mathcal{U}/\mathcal{H})^\tau$ where $\mathrm{char}(\mathcal{U}/\mathcal{H})^\tau = \tau\mathrm{char}(\mathcal{U}/\mathcal{H})\tau^{-1}$.

The cyclotomic character gives rise to $\Gamma_{\mathrm{cycl}} \simeq 1 + p\mathbb{Z}$ which after composition with

$$\frac{1}{p}\log_p : 1 + p\mathbb{Z} \xrightarrow{\sim} \mathbb{Z}_p$$

induces the isomorphism $\Gamma_{\mathrm{cycl}} \simeq \mathbb{Z}_p$. This allows us to identify $\Gamma_{\mathrm{cycl}} \otimes_{\mathbb{Z}_p} \Lambda$ with Λ, view the cyclotomic p-adic height pairing as Λ-valued

$$h : \mathcal{U} \otimes_\Lambda \mathcal{U}^\tau \to \Lambda,$$

and the Λ-adic regulator $\mathcal{R}$ as well as the Heegner L-function $\mathcal{L}$ as elements of Λ.

[2]Howard [11] defines the Λ-adic regulator to be $\mathcal{R}\Lambda \otimes \mathbb{Q}_p$ after identifying Γ_{cycl} with $\mathbb{Z}_p$ and hence views it as a submodule of $\Lambda \otimes \mathbb{Q}_p$.

We now identify Λ with $\mathbb{Z}_p[[T]]$ by sending a choice of a topological generator of $\mathrm{Gal}(K_\infty/K)$ to $T+1$. Then since

$$\mathcal{L} = \varprojlim_n \sum_{\sigma \in \mathrm{Gal}(K_n/K)} \langle c_n, \sigma c_n \rangle_{K_n} \sigma,$$

where $\langle\, , \rangle_{K_n} : E(K_n) \times E(K_n) \to \mathbb{Z}_p$ denotes the cyclotomic p-adic height pairing over K_n, we see that the coefficients of the Heegner L-function, under the above identification, are $\mathsf{b}_0 = \langle c_0, c_0 \rangle_{K_0}$ and

$$\mathsf{b}_k \equiv \sum_{k \le i < p^n} \binom{i}{k} \langle c_n, \sigma^i c_n \rangle_{K_n} \pmod{p^n} \quad \text{for } k \ge 1.$$

Note that the cyclotomic p-adic height pairings $\langle\, , \rangle_{K_n}$ are invariant under the action of $\mathrm{Gal}(K_n/K)$ and are related as follows for $n \ge m$:

$$\langle x, y \rangle_{K_n} = [K_n : K_m] \langle x, y \rangle_{K_m} \quad \text{for all } x, y \in E(K_m).$$

In addition, cyclotomic p-adic heights are related[3] to the above p-adic height pairings as follows:

$$h_{p,K_n}(x) = -\frac{1}{2} \langle x, x \rangle_{K_n}.$$

We would like to compute the Λ-adic regulator $\mathcal{R}$ of E in cases when it is non-trivial. In order to do this, we put ourselves in a situation where $\mathrm{char}(\mathcal{U}/\mathcal{H})$ is trivial and $\mathcal{L}$ is non-trivial by assuming that

- the analytic rank of E/K equals 1,
- the Heegner point z_0 is not divisible by p in $E(K)$,
- p divides the cyclotomic p-adic height of z_0 over K_0.

By [7] the first condition implies that z_0 is non-torsion which together with the second condition implies that $\mathrm{char}(\mathcal{U}/\mathcal{H})$ is trivial; the third ensures that $\mathcal{L}$ is not a unit.

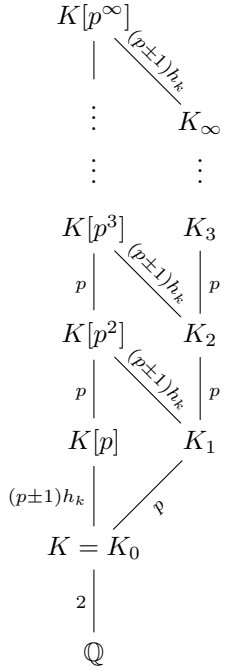
We will now proceed to describe algorithms to compute Heegner points z_n, and cyclotomic p-adic heights $h_{p,K_n}(x)$ for $x \in E(K_n)$. This will then enable us to compute the p-adic height pairings $\langle z_n, \sigma z_n \rangle_{K_n}$ for $\sigma \in \mathrm{Gal}(K_n/K)$ and hence the coefficients of Heegner L-functions.

3. Algorithm for the Heegner point construction

In this section we will give the algorithm that we use to construct the Heegner points $z_n = \mathrm{tr}_{K[p^{n+1}]/K_n}(y_{p^{n+1}})$ whose p-adic heights we wish to compute. Note that the assumption that our prime p does not divide h_K is used in the following algorithm.

[3]This choice of a normalization of the p-adic height follows that of [15].

For convenience, we point out the relevant tower of fields:



Observe that if we fix $b_0 \in \mathcal{S}(p^{2(n+1)}D_K, N)$ then Theorem 1.10 implies that there exists a Heegner point $x_{p^{n+1}}$ of level N and discriminant $p^{2(n+1)}D_K$ such that $\Phi(x_{p^{n+1}}) = (b_0, \mathcal{O}_{p^{n+1}})$. Our aim is to compute

$$z_n = \mathrm{tr}_{K[p^{n+1}]/K_n}(y_{p^{n+1}}) = \sum_{\sigma \in \mathrm{Gal}(K[p^{n+1}]/K_n)} \pi(\sigma x_{p^{n+1}}).$$

Since the order of $\mathrm{Gal}(K[p^{n+1}]/K_n)$ equals $\left(p - \left(\frac{D_K}{p}\right)\right) h_K$ and $\mathrm{Gal}(K[p^{n+1}]/K_n)$ is the maximal subgroup of $\mathrm{Gal}(K[p^{n+1}]/K)$ of order prime to p (this is where we use the assumption that $\gcd(h_K, p) = 1$) and $\mathrm{Gal}(K[p^{n+1}]/K) \simeq \mathrm{Cl}(\mathcal{O}_{p^{n+1}})$, using (2.1) we have that

$$z_n = \sum_{\mathfrak{a} \in \mathrm{Cl}(\mathcal{O}_{p^{n+1}}),\, p \nmid \mathrm{ord}(\mathfrak{a})} \pi(\mathfrak{a} \cdot x_{p^{n+1}})$$

and the sum has $\left(p - \left(\frac{D_K}{p}\right)\right) h_K$ terms. By Theorem 1.10 we know that

$$\Phi(\mathfrak{a} \cdot x_{p^{n+1}}) = \mathfrak{a} \cdot \Phi(x_{p^{n+1}}) = (b_0, \mathfrak{a}).$$

Hence we have that

$$z_n = \sum_{\mathfrak{a} \in \mathrm{Cl}(\mathcal{O}_{p^{n+1}}),\, p \nmid \mathrm{ord}(\mathfrak{a})} \pi(\Phi^{-1}(b_0, \mathfrak{a})).$$

We know that the Heegner point $\tau \in X_0(N)$ of level N and discriminant $p^{2(n+1)}D_K$ corresponds to a class (under the action of $\Gamma_0(N)$) of binary quadratic forms $f_\tau = Ax^2 + Bxy + Cy^2$ such that

(i) $A, B, C \in \mathbb{Z}$, $A > 0$, $N | A$,
(ii) $\gcd(A, B, C) = \gcd(A/N, B, CN) = 1$,
(iii) $B^2 - 4AC = p^{2(n+1)}D_K$.

Since $\tau = \Psi^{-1}(b_0, \mathfrak{a}) \in X_0(N)$ we have the following additional conditions:

(iv) $B \equiv b_0 \pmod{2N}$,
(v) $\Psi_{IF}(\mathfrak{a}) = f_\tau$.

Finally since Ψ_{IF} is a group isomorphism [3, Theorem 5.2.4 and Theorem 5.2.8] the set

$$\{\Psi^{-1}(b_0, \mathfrak{a}) | \mathfrak{a} \in \mathrm{Cl}(\mathcal{O}_{p^{n+1}}),\, p \nmid \mathrm{ord}(\mathfrak{a})\}$$

corresponds to the set of $\tau \in X_0(N)$ such that f_τ satisfies conditions (i)-(iv) listed above and $p \nmid \mathrm{ord}(f_\tau)$.

Algorithm 3.1 (Computing Heegner points $z_n \in E(K_n)$)**.**

(1) Fix $b_0 \in \mathcal{S}(p^{2(n+1)}D_K, N) = \{b \in \mathbb{Z}/2N\mathbb{Z} \ : \ b^2 \equiv p^{2(n+1)}D_K \pmod{4N}\}$.

(2) Create a set Q_{b_0} of $\left(p - \left(\frac{D_K}{p}\right)\right) h_K$ binary quadratic forms (A, B, C) that satisfy conditions (i)-(iv) listed above, where p does not divide the order of the equivalence class (under the action of $\mathrm{SL}_2(\mathbb{Z})$) of binary quadratic forms $[(A, B, C)]$, and any two binary quadratic forms in Q_{b_0} give rise to distinct equivalence classes.

To create[4] the set Q_{b_0} we fix $b \in \mathbb{Z}$ such that $b \equiv b_0 \pmod{2N}$. Then we set $A = Na$ and starting with $a = 1$, we run incrementally through $a \in \mathbb{N}$ prime to p (this condition ensures that the quadratic forms that we find correspond to ideals that are prime to p and hence to elements of $\mathrm{Cl}(\mathcal{O}_{p^{n+1}})$). For the current value of a

- we consider the finite set of primitive integral binary quadratic forms of discriminant $p^{2(n+1)}D_K$ such that $A = Na$ and $B = b + 2Ns$ for $s \in \{0, \ldots, a-1\}$ such that

$$\frac{B^2 - D}{4N} = Ns^2 + bs + \frac{b^2 - p^{2(n+1)}D_K}{4N} \equiv 0 \pmod{a}$$

since $aC = \frac{B^2 - D}{4N}$ and $C \in \mathbb{Z}$ (Note that we restrict $s \in \{0, \ldots, a-1\}$ since other values of s would not give rise to additional equivalence classes of quadratic forms.);
- we then run incrementally through $s \in \{0, \ldots, a-1\}$ satisfying the above conditions, consider the corresponding quadratic form, and we insert it in the set Q_{b_0} if it is not equivalent to any quadratic form that is already in Q_{b_0} (we use reduced quadratic forms in order to check whether two quadratic forms lie in the same equivalence class) and its order is prime to p.

We stop the process of incrementing a when the cardinality of Q_{b_0} reaches $\left(p - \left(\frac{D_K}{p}\right)\right) h_K$.

(3) Let $\tau_f \in X_0(N)$ be the Heegner point that corresponds to the form $f = Ax^2 + Bxy + Cy^2$. Compute $z_n = \sum_f \pi(\tau_f) \in E(\mathbb{C})$ for $f \in Q_{b_0}$, with sufficient numerical precision to satisfy the natural consistency checks of the following step.

(4) Using lattice basis reduction (LLL), as explained in [18, §2.5] and implemented as the `algebraic_dependency` command in [19] (which relies on the `algdep` command in [20]), algebraically reconstruct the x-coordinate of $z_n \in E(\mathbb{C})$ and then one of two possible y-coordinates. Make sure that z_n is defined over a dihedral Galois extension of degree $2p^n$ that is ramified exactly at p and the primes dividing the discriminant of K, and verify that several randomly chosen primes which are inert in $K/\mathbb{Q}$ split completely in K_n/K.

(5) We have now constructed z_n or $-z_n$ as a point of $E(K_n)$. Since by (3) we know z_n as a point of $E(\mathbb{C})$, we now identify $z_n \in E(K_n)$.

We will also need to know the set of conjugates of the Heegner point $z_n \in E(K_n)$:

$$\{\sigma z_n \in E(\mathbb{C}) \mid \sigma \in \mathrm{Gal}(K_n/K)\}.$$

[4]This follows an algorithm implemented in Sage by W. Stein and R. Bradshaw.

Since $\mathrm{Gal}(K[p^{n+1}]/K) \simeq \mathrm{Cl}(\mathcal{O}_{p^{n+1}})$ is of order $\left(p - \left(\frac{D_K}{p}\right)\right) h_K p^n$ and h_K is prime to p, an element $\mathfrak{a}_0 \in \mathrm{Cl}(\mathcal{O}_{p^{n+1}})$ of order p^n corresponds to a generator of $\mathrm{Gal}(K_n/K)$. Hence

$$\{\sigma z_n \in E(\mathbb{C}) \mid \sigma \in \mathrm{Gal}(K_n/K)\} = \left\{ \sum_{f \in Q_{b_0}} \pi(\mathfrak{a}_0^i \cdot \tau_f) \mid 0 \leq i \leq p^n - 1 \right\},$$

where b_0 is a fixed element of $\mathcal{S}(p^{2(n+1)}D_K, N)$ and Q_{b_0} is defined as in Step 2 of Algorithm 3.1. Observe that if $\tau = \Psi^{-1}(b_0, \mathfrak{a})$ for some $\mathfrak{a} \in \mathrm{Cl}(\mathcal{O}_{p^{n+1}})$ then $\mathfrak{a}_0^i \cdot \tau = \Psi^{-1}(b_0, \mathfrak{a}\mathfrak{a}_0^{-1})$ and

$$\Psi_{IF}(\mathfrak{a}\mathfrak{a}_0^{-1}) = \Psi_{IF}(\mathfrak{a})\Psi_{IF}(\mathfrak{a}_0)^{-1} = f_\tau \Psi_{IF}(\mathfrak{a}_0)^{-1}.$$

Hence we have that

$$\{\sigma z_n \in E(\mathbb{C}) \mid \sigma \in \mathrm{Gal}(K_n/K)\} = \left\{ \sum_{f \in f_0^i Q_{b_0}} \pi(\tau_f) \mid 0 \leq i \leq p^n - 1 \right\},$$

where

i) f_0 is a primitive positive definite binary quadratic form of discriminant $p^{2(n+1)}D_K$ such that $\mathrm{ord}[f_0] = p^n$,

ii) $f_0^i Q_{b_0}$ is a set of $\left(p - \left(\frac{D_K}{p}\right)\right) h_K$ binary quadratic forms (A, B, C) which satisfy conditions (i)-(iv) listed above and $[(A, B, C)] = [f_0^i f]$ for $f \in Q_{b_0}$.

Algorithm 3.2 (Computing the conjugates of the Heegner point $z_n \in E(K_n)$ as elements of $E(\mathbb{C})$)**.**

(1) Fix $b_0 \in \mathcal{S}(p^{2(n+1)}D_K, N)$ and create a list of equivalence classes of binary quadratic forms Q_{b_0} as in Step 2 of Algorithm 3.1.
(2) Find f_0 a primitive positive definite binary quadratic form of discriminant $p^{2(n+1)}D_K$ such that $\mathrm{ord}[f_0] = p^n$.
(3) For each $i \in \{0, \ldots, p-1\}$ compute the set $f_0^i Q_{b_0}$.
(4) Compute $\sum_{f \in f_0^i Q_{b_0}} \pi(\tau_f) \in E(\mathbb{C})$ for $i \in \{0, \ldots, p^n - 1\}$ and record this p^n-tuple of points of $E(\mathbb{C})$.

4. Computation of p-adic heights

In this section, we begin by using [15] to give an effective algorithm for computing the cyclotomic p-adic height of a non-torsion point $P \in E(F)$, where F is a finite Galois extension of $\mathbb{Q}$. We then refine this algorithm for the computation of cyclotomic p-adic heights of Heegner points. To conclude we illustrate this algorithm as well as Algorithm 3.1 by computing p-adic heights of Heegner points in two concrete examples.

4.1. An algorithm for computing p-adic heights.

Let E be an elliptic curve defined over $\mathbb{Q}$, F a number field, and P a non-torsion point in $E(F)$. For every prime v of F we consider the localization map

$$\mathrm{res}_v : E(F) \to E(F_v)$$

where F_v denotes the completion of F at v. Then we have that

$$\mathrm{res}_v(P) = \left(\frac{a_v(P)}{d_v(P)^2}, \frac{b_v(P)}{d_v(P)^3} \right) \in E(F_v),$$

where $a_v(P), b_v(P), d_v(P) \in \mathcal{O}_{F_v}$ such that $\gcd(a_v(P), d_v(P)) = \gcd(b_v(P), d_v(P)) = 1$ (here $\mathcal{O}_{F_v}$ denotes the ring of integers of F_v).

By Mazur-Stein-Tate [15] we know that if the point $P \in E(F)$ reduces

(1) to a non-singular point at all primes of bad reduction, and
(2) to the identity in $E(k_\wp)$ for all primes $\wp \mid p$, where $k_\wp$ is the residue field of F at $\wp$,

the cyclotomic p-adic height of P over F is given by the following formula

$$h_{p,F}(P) = \frac{1}{p} \cdot \left(\sum_{\wp \mid p} \log_p \left(N_{F_\wp/\mathbb{Q}_p}(\sigma_p(\mathrm{res}_\wp(P))) \right) - \sum_{v \nmid p} \mathrm{ord}_v(d_v(P)) \cdot \log_p(\#k_v) \right), \tag{4.1}$$

where σ_p is the p-adic sigma function of E, $\sigma_p\left(\mathrm{res}_\wp(P)\right) := \sigma_p\left(-\frac{x(\mathrm{res}_\wp(P))}{y(\mathrm{res}_\wp(P))}\right)$, and k_v is the residue field of F at v. This assumes that we are working with a minimal model of E/F. By the work of Mazur and Tate [16], we have the following characterization of the p-adic sigma function:

Theorem 4.1. *Let E be an elliptic curve defined over a complete field of residue characteristic p with good ordinary reduction at p, and $x(t) = \frac{1}{t^2} = \ldots \in \mathbb{Z}_p((t))$ be the formal power series that expresses x in terms of the local parameter at $t = -x/y$ at infinity. There is exactly one odd function $\sigma_p(t) = t + \cdots \in t\mathbb{Z}_p[[t]]$ and constant $c \in \mathbb{Z}_p$ that together satisfy the differential equation*

$$x(t) + c = -\frac{d}{\omega}\left(\frac{1}{\sigma_p}\frac{d\sigma_p}{\omega}\right), \tag{4.2}$$

where ω is the invariant differential $dx/(2y + a_1x + a_3)$ associated with our chosen Weierstrass equation for E.

Note that the p-adic sigma function converges only in a neighborhood of the local parameter $t = -x/y$ at infinity and this is where condition (2) comes in. Thus to evaluate the p-adic sigma function at a point $P \in E(F)$, one may have to work with a multiple of P.

If condition (1) holds for P and m an integer such that mP reduces to the identity in $E(k_\wp)$ for all primes $\wp \mid p$, we use the formula (4.1) to compute the p-adic height of mP as follows:

$$h_{p,F}(mP) = \frac{1}{p} \cdot \left(\sum_{\wp \mid p} \log_p \left(N_{F_\wp/\mathbb{Q}_p}(\sigma_p(m\,\mathrm{res}_\wp(P))) \right) - \sum_{v \nmid p} \mathrm{ord}_v(d_v(mP)) \cdot \log_p(\#k_v) \right).$$

and then recover the height of P by using the fact that the p-adic height pairing is a quadratic form. The issue with this process is that the coefficients of mP become very large and hence the direct computation of $d_v(mP)$ for primes $v \nmid p$ becomes yet more difficult. However, since P reduces to a non-singular point at all primes of bad reduction, by Proposition 1 of [23] we know that

$$d_v(mP) = \mathrm{res}_v(f_m(P)) d_v(P)^{m^2},$$

where f_m is the m-th division polynomial of the elliptic curve $E/\mathbb{Q}$. Hence we have

$$\begin{aligned} h_{p,F}(mP) &= \frac{1}{p} \cdot \left(\sum_{\wp \mid p} \log_p \left(N_{F_\wp/\mathbb{Q}_p}(\sigma_p(m\,\mathrm{res}_\wp(P))) \right) - \sum_{v \nmid p} \mathrm{ord}_v(f_m(P) d_v(P)^{m^2}) \cdot \log_p(\#k_v) \right) \\ &= \frac{1}{p} \cdot \left(\log_p \prod_{\wp \mid p} \frac{(N_{F_\wp/\mathbb{Q}_p}(\sigma_p(m\,\mathrm{res}_\wp(P)))}{N_{F_\wp/\mathbb{Q}_p}(f_m(P))} - m^2 \sum_{v \nmid p} \mathrm{ord}_v(d_v(P)) \cdot \log_p(\#k_v) \right) \\ &= \frac{1}{p} \cdot \left(\log_p \prod_{\wp \mid p} \frac{(N_{F_\wp/\mathbb{Q}_p}(\sigma_p(m\,\mathrm{res}_\wp(P)))}{N_{F_\wp/\mathbb{Q}_p}(f_m(P))} - m^2 \log_p(\mathcal{D}_F(P)) \right), \end{aligned}$$

where $\mathcal{D}_F(P) := \prod_{v\nmid p}(\#k_v)^{\mathrm{ord}_v(d_v(P))}$. Computing $\mathcal{D}_F(P)$ directly involves factoring ideals in the ring of integers of F but the following result allows us to bypass the factorization process.

Proposition 4.2. *Let F be a Galois extension of $\mathbb{Q}$, $P\in E(F)$, $b(P)$ be the prime to p part of the leading coefficient of the minimal polynomial of the x-coordinate $x(P)$ over $\mathbb{Z}$ and r its degree. Then*

$$\mathcal{D}_F(P)^2 = b(P)^{[F:\mathbb{Q}]/r}.$$

Proof. Since by definition $b(P)$ and $\mathcal{D}_F(P)$ are positive integers prime to p, we will prove the above equality by analyzing the valuation of $b(P)$ and $\mathcal{D}_F(P)$ at every rational prime $\ell\neq p$.

Let $b_rx^r+\cdots+b_0=0$ be the minimal polynomial of $x(P)$ over $\mathbb{Z}$. Since $b_rx(P)\in\mathcal{O}_F$, it follows that $d_v(P)$ is a unit at all primes v where b_r has trivial valuation. Then the assumption that $b_r=p^eb(P)$ implies that $\mathcal{D}_F(P)$ has trivial valuation at all primes which do not divide $b(P)$.

We now consider the set $\{\ell_1,\dots\ell_t\}$ of rational prime divisors of $b(P)$. Denote by $\lambda_{i,j}$ the primes of F which divide ℓ_i, and $F_{\lambda_{i,j}}$ is the localization of F at $\lambda_{i,j}$. Recall that $\mathrm{res}_{\lambda_{i,j}}x(P)=\frac{a_{\lambda_{i,j}}(P)}{d_{\lambda_{i,j}}(P)^2}$ where $a_{\lambda_{i,j}}(P)$ and $d_{\lambda_{i,j}}(P)$ are coprime $\lambda_{i,j}$-adic integers and observe that

$$\mathcal{D}_F(P)=\prod_{i,j}N_{F_{\lambda_{i,j}}/\mathbb{Q}_{\ell_i}}(d_{\lambda_{i,j}}(P)),$$

$$N_{F/\mathbb{Q}}(x(P))=c\prod_{i,j}N_{K_{\lambda_{i,j}}/\mathbb{Q}_{\ell_i}}(\mathrm{res}_{\lambda_{i,j}}x(P)),$$

where c is an integer with trivial valuation at the primes ℓ_i.

We start by considering primes ℓ_i that do not divide $\gcd(b_r,b_0)$. Then, if the valuation at λ_{i,j_0} of $x(P)$ is negative then the valuation at $\lambda_{i,j}$ of $x(P)$ is not positive for any j (since otherwise ℓ_i would divide b_0 when it already must divide b_r). Hence, since

$$(b_0/b_r)^{[F:\mathbb{Q}]/r}=c\prod_{i,j}N_{K_{\lambda_{i,j}}/\mathbb{Q}_{\ell_i}}(\mathrm{res}_{\lambda_{i,j}}x(P)),$$

if ℓ_i does not divide $\gcd(b_r,b_0)$ then $\mathrm{ord}_{\ell_i}(\mathcal{D}_F(P))^2=\mathrm{ord}_{\ell_i}\left(b(P)^{[F:\mathbb{Q}]/r}\right)$.

We now consider the valuations of $\mathcal{D}_F(P)$ and $b(P)$ at primes ℓ_i which divide $\gcd(b_r,b_0)$. Since $F/\mathbb{Q}$ is a Galois extension we have that

$$b_r^{-[F:\mathbb{Q}]/r}(b_rx^r+\cdots+b_0)^{[F:\mathbb{Q}]/r}=\prod_{\sigma\in\mathrm{Gal}(F/\mathbb{Q})}(x-\sigma(x(P))). \tag{4.3}$$

For every $\sigma\in\mathrm{Gal}(F/\mathbb{Q})$ we set e_σ to be the valuation of $x(P)$ at $\sigma(\lambda_{i,1})$. Viewing the right hand side of the equation (4.3) over the completion of F at $\lambda_{i,1}$ we have that

$$\prod_{\sigma\in\mathrm{Gal}(F/\mathbb{Q})}(x-\sigma(x(P)))=\prod_{\sigma\in\mathrm{Gal}(F/\mathbb{Q})}(x-u_\sigma\pi^{e_{\sigma^{-1}}})$$

where π is a uniformizer of $\lambda_{i,1}$ and u_σ are units. In addition, since the greatest common divisor of the coefficients of $b_rx^r+\cdots+b_0$ is trivial, the same holds for $(b_rx^r+\cdots+b_0)^{[F:\mathbb{Q}]/r}$. It then follows that the valuation at ℓ_i of $b(P)^{-[F:\mathbb{Q}]/r}$ equals the sum of the negative e_σ. Since $\mathrm{res}_{\lambda_{i,j}}x(P)=\frac{a_{\lambda_{i,j}}(P)}{d_{\lambda_{i,j}}(P)^2}$, the valuation at ℓ_i of $\mathcal{D}_F(P)^2$ also equals

$$\sum_{\sigma\in\mathrm{Gal}(F/\mathbb{Q}),\ e_\sigma<0}e_\sigma.$$

Hence, the valuations of $b^{[F:\mathbb{Q}]/r}$ and $\mathcal{D}_F(P)^2$ are equal at every prime. This concludes the proof of the proposition. □

We can now describe the algorithm for computing the p-adic height of P.

Algorithm 4.3 (The p-adic height $h_{p,F}(P)$ of $P \in E(F)$)**.**

(1) Find the smallest positive integer m_o such that m_oP reduces to a non-singular point at all primes of bad reduction.
(2) Compute m_oP.
(3) Compute the minimal polynomial of $x(m_oP)$ over $\mathbb{Z}$. Let $b(P)$ be the prime to p part of its leading coefficient and r be the degree of this polynomial. Then set $\mathcal{D}_F(m_oP) = b(P)^{[F:\mathbb{Q}]/2r}$.
(4) Compute the p-adic sigma function $\sigma_p(t) \in \mathbb{Z}_p[[t]]$ using the algorithms of [15, 10].
(5) Compute $\operatorname{res}_\wp(m_oP)$ and $f_m \operatorname{res}_\wp(m_oP)$ for each $\wp \mid p$.
(6) Compute the order of m_oP in $E(k_\wp)$ for each $\wp \mid p$; set m to be the least common multiple of these orders.
(7) Evaluate $\sigma_p(m \operatorname{res}_\wp(m_oP)) = \sigma_p\left(-\frac{x(m \operatorname{res}_\wp(m_oP))}{y(m \operatorname{res}_\wp(m_oP))}\right) \in F_\wp$ for each $\wp \mid p$.
(8) Compute $h_{p,F}(P)$ as follows:

$$h_{p,F}(P) = \frac{1}{p \cdot m_o^2}\left(\frac{1}{m^2}\log_p \prod_{\wp|p} \frac{N_{F_\wp/\mathbb{Q}_p}\left(\sigma_p(m \operatorname{res}_\wp(m_oP))\right)}{N_{F_\wp/\mathbb{Q}_p}\left(f_m(m_oP)\right)} - \log_p\left(\mathcal{D}_F(m_oP)\right)\right).$$

Observe that in the above algorithm m_o divides the product of the Tamagawa numbers, and our choice of $m \in \mathbb{Z}$ ensures that the point mm_oP reduces to the identity $\mathrm{O} \in E(k_\wp)$ for all $\wp \mid p$.

4.2. **p-adic heights of Heegner points.** We will now focus on the computation of p-adic heights of Heegner points. In addition to the conditions (i)-(iii) listed in the beginning of §2 in this section we will also assume that

iv) the elliptic curve $E/\mathbb{Q}$ has trivial rational torsion.

Observe that by §3.1 and §3.3 of [7] (see also Lemma 4.2 of [12]) we know that the Heegner point z_n lies, up to translation by a rational torsion point of E, in the connected component of E at every bad reduction prime v. Hence, under the above assumption $m_o = 1$ in the computation of p-adic heights of Heegner points. This trivializes the first two steps of Algorithm 4.3. Moreover, if E/K has analytic rank 1 and p does not divide z_0, the following corollary of Proposition 4.2 will do the same with the third step.

Corollary 4.4. *Let E be an elliptic curve defined over $\mathbb{Q}$ of analytic rank 1 over K, z_n a Heegner point in $E(K_n)$, and $b(z_n)$ the prime to p part of the leading coefficient of the minimal polynomial of the x-coordinate of z_n over $\mathbb{Z}$. Then $\mathcal{D}_{K_n}(z_n) = b(z_n)^{p^{n-r}}$ where p^r is the degree of the minimal polynomial of $x(z_n)$ over $\mathbb{Z}$. Moreover, if p does not divide z_0 in $E(K)$ then $\mathcal{D}_{K_n}(z_n) = b(z_n)$.*

Proof. Consider the action of complex conjugation $\tau \in \mathrm{Gal}(K_n/\mathbb{Q})$ on the Heegner point $z_n \in E(K_n)$. Since the rational torsion $E(\mathbb{Q})_{\mathrm{tors}}$ is trivial and the order of $\mathrm{Gal}(K_n/K)$ is odd, there exist $\sigma \in \mathrm{Gal}(K_n/K)$ such that $\tau(\sigma(z_n) = -\epsilon(\sigma(z_n))$ where ϵ is the sign of the functional equation of $E/\mathbb{Q}$; see the listed properties of Heegner points in §2. This implies that $x(\sigma z_n) \in K_n^{\langle\tau\rangle}$. Observe that $[K_n^{\langle\tau\rangle} : \mathbb{Q}] = p^n$. This implies that the degree of the minimal polynomial of $x(z_n)$ over $\mathbb{Z}$ equals p^r for some $r \leq n$. Then Proposition 4.2 we have that

$$\mathcal{D}_{K_n}(z_n)^2 = b(z_n)^{(2p^n)/p^r} = \left(b(z_n)^{p^{n-r}}\right)^2.$$

Then, since $\mathcal{D}_{K_n}(z_n)$ and $b(z_n)$ are positive integers it follows that $\mathcal{D}_{K_n}(z_n) = b(z_n)^{p^{n-r}}$.

If p does not divide z_0 in $E(K)$, then since $\mathrm{tr}_{K_n/K}\, z_n$ is a unit multiple of z_0 it follows that $K_n = K(x(\sigma z_n), y(\sigma z_n))$ which together with the fact that $\tau(\sigma(z_n) = -\epsilon(\sigma(z_n))$, implies $K_n^{\langle\tau\rangle} = \mathbb{Q}(x(\sigma z_n))$. Hence, the degree of the minimal polynomial of $x(\sigma z_n) = \sigma(x(z_n)$ over $\mathbb{Z}$ equals p^n, and by the above it follows that $\mathcal{D}_{K_n}(z_n) = b(z_n)$. □

There is one further simplification. In our construction of Heegner points, we first determine a Heegner point z_n as an element of $E(\mathbb{C})$. If our only aim is to compute the p-adic height $h_{p,K_n}(z_n)$ then $\mathcal{D}_{K_n}(z_n)$ is determined by the minimal polynomial of $x(z_n)$ over $\mathbb{Z}$ and we do not need to construct the coordinates of z_n as elements of a number field. Since the coordinates of z_n are only used as input for the p-adic sigma function we will only need the coordinates of $\mathrm{res}_{\wp} z_n$ to some $\wp$-adic approximation for all $\wp \mid p$; this can be done cheaply with a Newton iteration. In fact, we first compute $\mathrm{res}_{\wp} x(z_n)$ and then solve for $\mathrm{res}_{\wp} y(z_n)$. Note that while we need to choose the sign of the y-coordinate, this choice is irrelevant in the end since the sigma function is known to be odd.

In order to compute $\mathrm{res}_{\wp} z_n$ for $\wp \mid p$, we must use lattice basis reduction (LLL) to determine the minimal polynomial of $x(z_n)$ over $\mathbb{Z}$. Consider $L_n = \mathbb{Q}(x(z_n))$ and observe that p is totally ramified in $L_n/\mathbb{Q}$. In addition, we also know that $L_n/\mathbb{Q}$ is unramified away from the prime divisors of $p \cdot D_K$ and that all rational primes which are inert in $K/\mathbb{Q}$ split completely in $L_n/\mathbb{Q}$ (since both of these conditions hold for $K_n/\mathbb{Q}$). We use these three properties of $L_n/\mathbb{Q}$ as consistency checks in our computation of the minimal polynomial of $x(z_n)$ over $\mathbb{Z}$.

We will now analyze the fields of definition of $\mathrm{res}_{\wp} z_n$ for $\wp \mid p$. Let $\mathfrak{p}_n$ be the unique prime of L_n above p and $L_{\mathfrak{p}_n}$ be the completion of L_n at $\mathfrak{p}_n$. In addition, $\wp_n$ denotes primes of K_n above p and $K_{\wp_n}$ is the completion of K_n at $\wp_n$. Observe that

(1) if the analytic rank of $E/\mathbb{Q}$ is 1 then $\tau\sigma z_n = \sigma z_n$ for some $\sigma \in \mathrm{Gal}(K_n/K)$ which in turn implies that $z_n \in E(L_n)$.
(2) if the analytic rank of $E/\mathbb{Q}$ is 0 and p splits in $K/\mathbb{Q}$ then there are exactly two primes $\wp_n$, $\wp_n'$ of K_n above p and $\mathfrak{p}_n\mathcal{O}_{K_n} = \wp_n\wp_n'$. Hence $K_{\wp_n} = K_{\wp_n} = L_{\mathfrak{p}_n}$ and $\mathrm{res}_{\wp_n} z_n, \mathrm{res}_{\wp_n'} z_n \in E(L_{\mathfrak{p}_n})$. Moreover, since $\tau\sigma z_n = -\sigma z_n$ for some $\sigma \in \mathrm{Gal}(K_n/K)$, we have that $\mathrm{res}_{\wp_n'} \sigma z_n = -\mathrm{res}_{\wp_n} \sigma z_n$.

Consequently, in both of the above cases setting m to be the order of $\mathrm{res}_{\mathfrak{p}_n}(z_n)$ in $E(\mathbb{F}_p)$, since the residue field of L_n at $\mathfrak{p}_n$ equals $\mathbb{F}_p$, we find that

$$\log_p \prod_{\wp_n \mid p} \frac{N_{K_{\wp_n}/\mathbb{Q}_p}\left(\sigma_p(m\,\mathrm{res}_{\wp_n}(z_n))\right)}{N_{K_{\wp_n}/\mathbb{Q}_p}\left(f_m\,\mathrm{res}_{\wp_n}(z_n)\right)} = 2\log_p\left(N_{L_{\mathfrak{p}_n}/\mathbb{Q}_p}\left(\frac{\sigma_p(m\,\mathrm{res}_{\mathfrak{p}_n}(z_n))}{f_m(\mathrm{res}_{\mathfrak{p}_n}(z_n))}\right)\right).$$

While in the above cases all our computations are over extensions of degree p^n, this is no longer possible in the following case:

(3) if the analytic rank of $E/\mathbb{Q}$ is 0 and p is inert in $K/\mathbb{Q}$, then there is a unique prime $\wp_n$ of K_n above p and $K_{\wp_n} = L_{\mathfrak{p}_n}[\sqrt{D_K}]$. While $x(\mathrm{res}_{\wp_n}(z_n)) \in L_{\mathfrak{p}_n}$, since $\tau z_n = -\sigma z_n$ for some $\sigma \in \mathrm{Gal}(K_n/K)$, it follows that $y(\mathrm{res}_{\wp_n}(z_n)) \in K_{\wp_n} \setminus L_{\mathfrak{p}_n}$.

To summarize, in order to compute p-adic heights of Heegner points we use the following modified versions of Algorithm 4.3:

Algorithm 4.5 (The p-adic height $h_{p,K_n}(z_n)$ of a Heegner point $z_n \in E(K_n)$)**.**
Assume one of the following conditions holds:

- the analytic rank of $E/\mathbb{Q}$ equals 1, or
- the analytic rank of $E/\mathbb{Q}$ is 0 and p splits in $K/\mathbb{Q}$.

(1) Compute $x(z_n) \in \mathbb{C}$ using the first three steps of Algorithm 3.1.
(2) Use lattice basis reduction (LLL) to find the minimal polynomial of $x(z_n)$ over $\mathbb{Z}$. As a consistency check, we verify that the corresponding extension of $L_n/\mathbb{Q}$ is unramified away from the prime divisors of $p \cdot D_K$, p is totally ramified in $L_n/\mathbb{Q}$, and that several randomly chosen primes which are inert in $K/\mathbb{Q}$ split completely in $L_n/\mathbb{Q}$.
(3) Compute $\mathcal{D}_{K_n}(z_n)$, see Corollary 4.4.
(4) Compute the p-adic sigma function $\sigma_p(t) \in \mathbb{Z}_p[[t]]$.
(5) p-adically construct $\mathrm{res}_{\mathfrak{p}_n}(z_n) \in E(L_{\mathfrak{p}_n})$.

(6) Compute m, the order of $\mathrm{res}_{\mathfrak{p}_n}(z_n)$ in $E(\mathbb{F}_p)$.
(7) Compute $m\,\mathrm{res}_{\mathfrak{p}_n}(z_n) \in E(L_{\mathfrak{p}_n})$ and $f_m(\mathrm{res}_{\mathfrak{p}_n}(z_n)) \in L_{\mathfrak{p}_n}$.
(8) Recover

$$h_{p,K_n}(z_n) = \frac{1}{p}\left(\frac{2}{m^2}\log_p N_{L_{\mathfrak{p}_n}/\mathbb{Q}_p}\left(\frac{\sigma_p(m\,\mathrm{res}_{\mathfrak{p}_n}(z_n))}{f_m(\mathrm{res}_{\mathfrak{p}_n}(z_n))}\right) - \log_p(\mathcal{D}_{K_n}(z_n))\right).$$

Algorithm 4.6 (The p-adic height $h_{p,K_n}(z_n)$ of a Heegner point $z_n \in E(K_n)$)**.**
Assume that the analytic rank of $E/\mathbb{Q}$ is 0 and p is inert in $K/\mathbb{Q}$.

Complete steps (1)-(4) as in Algorithm 4.5.
(5) p-adically construct $\mathrm{res}_{\wp_n} x(z_n) \in E(L_{\mathfrak{p}_n})$ and then $\mathrm{res}_{\wp_n} y(z_n) \in E(K_{\wp_n})$.
(6) Compute m, the order of $\mathrm{res}_{\wp_n}(z_n) \in E(\mathbb{F}_{p^2})$.
(7) Compute $m\,\mathrm{res}_{\wp_n}(z_n) \in E(K_{\wp_n})$ and $f_m(\mathrm{res}_{\mathfrak{p}_n}(z_n)) \in K_{\wp_n}$.
(8) Recover

$$h_{p,K_n}(z_n) = \frac{1}{p}\left(\frac{1}{m^2}\log_p\left(\frac{N_{K_{\wp_n}/\mathbb{Q}_p}\left(\sigma_p(m\,\mathrm{res}_{\wp_n}(z_n))\right)}{N_{L_{\mathfrak{p}_n}/\mathbb{Q}_p}\left(f_m(\mathrm{res}_{\mathfrak{p}_n}(z_n))\right)^2}\right) - \log_p(\mathcal{D}_{K_n}(z_n))\right).$$

4.3. **Examples.** We now illustrate the algorithms developed in §3 and §4.2 by going through the steps in one explicit example[5] and listing the results of another. Throughout this paper we refer to elliptic curves by a version of their Cremona labels [6]; see the Appendix for the equations of the specific curves we use.

Example 4.7. Let $E/\mathbb{Q}$ be the rank 1 elliptic curve "57a1", $p = 5$, and $K = \mathbb{Q}(\sqrt{-14})$. Note that conditions (i)-(iii) listed at the beginning of §2 as well as condition (iv) of §4.2 hold. In addition, we have that E/K has analytic rank 1, K has class number $h_K = 4$, and the prime $p = 5$ splits in $K/\mathbb{Q}$.

Using Sage we compute the Heegner point $z_0 \in E(K)$ and its 5-adic height:

$$h_{5,K}(z_0) = 5 + 3\cdot 5^2 + 5^3 + 5^4 + 2\cdot 5^5 + 5^7 + O(5^8).$$

Hence, 5 does not divide z_0 in $E(K)$, and this is an example where the Heegner L-function of E is non-trivial and equal to the Λ-adic regulator $\mathcal{R}$ of E, see §2. We are interested in computing the coefficients of the Heegner L-function, and as a first step we will compute a Heegner point z_1 and its 5-adic height $h_{5,K_1}(z_1)$.

We will now use the first three steps of Algorithm 3.1 to approximate the coordinate of the Heegner point $z_1 \in E(\mathbb{C})$. Fix $b_0 = 32 \in \mathcal{S}(5^4\cdot(-4\cdot 14), 57)$. Since $h_K = 4$ and $p = 5$ splits in $K/\mathbb{Q}$, we create a list of $16 = h_K(p-1)$ equivalence classes of binary quadratic forms of order prime to 5 which satisfy conditions $(i) - (iv)$ of Section 3:

[5]We emphasize again that *all* computational results in this paper assume that certain non-exact, non-proven numerical computation of points gave correct answers; see Remark 0.1.

$$\begin{aligned}
f_1(x,y) &= 741x^2 + 146xy + 19y^2 & \operatorname{ord}(f_1) &= 8\\
f_2(x,y) &= 1311x^2 + 2426xy + 1129y^2 & \operatorname{ord}(f_2) &= 2\\
f_3(x,y) &= 1482x^2 + 1628xy + 453y^2 & \operatorname{ord}(f_3) &= 8\\
f_4(x,y) &= 2622x^2 + 5048xy + 2433y^2 & \operatorname{ord}(f_4) &= 2\\
f_5(x,y) &= 4503x^2 + 32xy + 2y^2 & \operatorname{ord}(f_5) &= 2\\
f_6(x,y) &= 4617x^2 + 5390xy + 1575y^2 & \operatorname{ord}(f_6) &= 4\\
f_7(x,y) &= 5187x^2 + 4592xy + 1018y^2 & \operatorname{ord}(f_7) &= 8\\
f_8(x,y) &= 9006x^2 + 32xy + y^2 & \operatorname{ord}(f_8) &= 1\\
f_9(x,y) &= 9234x^2 + 14624xy + 5791y^2 & \operatorname{ord}(f_9) &= 4\\
f_{10}(x,y) &= 10089x^2 + 7100xy + 1250y^2 & \operatorname{ord}(f_{10}) &= 4\\
f_{11}(x,y) &= 10374x^2 + 4592xy + 509y^2 & \operatorname{ord}(f_{11}) &= 8\\
f_{12}(x,y) &= 12141x^2 + 15308xy + 4826y^2 & \operatorname{ord}(f_{12}) &= 8\\
f_{13}(x,y) &= 20178x^2 + 7100xy + 625y^2 & \operatorname{ord}(f_{13}) &= 4\\
f_{14}(x,y) &= 23883x^2 + 7556xy + 598y^2 & \operatorname{ord}(f_{14}) &= 8\\
f_{15}(x,y) &= 83163x^2 + 70028xy + 14742y^2 & \operatorname{ord}(f_{15}) &= 8\\
f_{16}(x,y) &= 166269x^2 + 175022xy + 46059y^2 & \operatorname{ord}(f_{16}) &= 8.
\end{aligned}$$

Then we compute

$$z_1 = \sum_{i=1}^{16} \pi(\tau_{f_i}) \in E(\mathbb{C}).$$

Numerically[6], we have that

$$z_1 \approx (0.649281815494878 + 0.730235331103786i, -1.54792819990164 + 0.894427675896415i).$$

We will now use Algorithm 4.5 to compute the p-adic height of z_1. Using LLL, we find[7] that the best degree 5 relation satisfied by the x-coordinate of the numerical approximation to z_1 above is

$$528126361x^5 - 1204116445x^4 + 172671870x^3 + 1926267530x^2 - 2409168275x + 1066099823.$$

We will now assume that the above polynomial is the minimal polynomial of $x(z_1)$, which is highly likely due to consistency checks described in the second step of Algorithm 4.5. Then by Corollary 4.4 we have that

$$\mathcal{D}_{K_1}(z_1) = 528126361.$$

We compute $\sigma_5(t) \in \mathbb{Z}_5[[t]]$. Then p-adically construct $\operatorname{res}_{\mathfrak{p}_1}(z_1) \in E(L_{\mathfrak{p}_1})$. Since $\operatorname{res}_{\mathfrak{p}_1}(z_1)$ reduces to $(2,3) \in E(\mathbb{F}_5)$ which has order 9, we set $m = 9$. We now compute $9\operatorname{res}_{\mathfrak{p}_1}(z_1) \in E(L_{\mathfrak{p}_1})$, $f_9(\operatorname{res}_{\mathfrak{p}_1} x(z_1)) \in L_{\mathfrak{p}_1}$, and evaluate

$$\sigma_5(9\operatorname{res}_{\mathfrak{p}_1}(z_1)) = \sigma_5\left(-\frac{x(\operatorname{res}_{\mathfrak{p}_1}(z_1))}{y(\operatorname{res}_{\mathfrak{p}_1}(z_1))}\right) \in L_{\mathfrak{p}_1}.$$

[6]In our actual calculation, we used 2000 bits of precision.

[7]This is only "likely" to be the best since LLL is not guaranteed to give the best answer; we will suppress mention of this issue in future computations.

Then we find that

$$N_{L_{\mathfrak{p}_1}/\mathbb{Q}_5}\left(\sigma_5(9\,\mathrm{res}_{\mathfrak{p}_1}(z_1))\right) = 5 + 3\cdot 5^2 + 4\cdot 5^4 + 4\cdot 5^5 + 2\cdot 5^6 + 2\cdot 5^8 + 4\cdot 5^9 + O(5^{10}),$$
$$N_{L_{\mathfrak{p}_1}/\mathbb{Q}_5}\left(f_9(\mathrm{res}_{\mathfrak{p}_1}\, x(z_1))\right) = 2\cdot 5 + 2\cdot 5^2 + 5^3 + 5^4 + 2\cdot 5^5 + 3\cdot 5^6 + 4\cdot 5^7 + 2\cdot 5^8 + 2\cdot 5^9 + O(5^{10}).$$

Finally, putting this all together yields

$$\begin{aligned} h_{p,K_1}(z_1) &= \frac{1}{5}\left(\frac{2}{9^2}\log_p\left(N_{L_{\mathfrak{p}_1}/\mathbb{Q}_5}\left(\sigma_5(9\,\mathrm{res}_{\mathfrak{p}_1}(z_1))\right)\right) - \frac{2}{9^2}\log_p\left(N_{L_{\mathfrak{p}_1}/\mathbb{Q}_5}\left(f_9(\mathrm{res}_{\mathfrak{p}_1}\, x(z_1))\right)\right) - \log_p(\mathcal{D}_{K_1}(z_1))\right) \\ &= 3 + 2\cdot 5 + 5^2 + 4\cdot 5^5 + 2\cdot 5^6 + O(5^7). \end{aligned}$$

Example 4.8. Let $E/\mathbb{Q}$ be the rank 1 elliptic curve "331a1", $p = 7$ and $K = \mathbb{Q}(\sqrt{-2})$. Note that conditions (i)-(iii) listed at the beginning of §2 as well as condition (iv) of §4.2 hold. In addition, we have that E/K has analytic rank 1, K has class number $h_K = 1$, and $p = 7$ is inert in $K/\mathbb{Q}$.

Using Sage we compute the Heegner point $z_0 \in E(K)$ and its 7-adic height:

$$h_{7,K}(z_0) = 6\cdot 7 + 3\cdot 7^2 + 4\cdot 7^3 + 7^4 + 2\cdot 7^5 + 2\cdot 7^6 + 4\cdot 7^7 + O(7^8).$$

Hence, 7 does not divide z_0 in $E(K)$ and this is another example where we wish to compute the coefficients of the Heegner L-function (see §6). As a first step we use Algorithm 4.5 to compute the 7-adic height of z_1 and find that

$$h_{7,K_1}(z_1) = 4 + 3\cdot 7 + 3\cdot 7^2 + 7^3 + 6\cdot 7^4 + 2\cdot 7^5 + 4\cdot 7^6 + 2\cdot 7^7 + O(7^8).$$

Remark 4.9. As a double check on our implementation of the height algorithms, one can compute $h_{p,F}(P) - \frac{h_{p,F}(nP)}{n^2}$ for several $n \in \mathbb{N}$ and verify that the result is p-adically small. We have completed this check for $n = 2$ in all the examples that appear in this article.

5. Computing p-adic height pairings of Heegner points

In this section, we give an algorithm to compute the p-adic height pairing

$$\langle z_n, \sigma z_n\rangle_{K_n} \qquad \text{for } \sigma \in \mathrm{Gal}(K_n/K),$$

and then illustrate it in an example. We continue to assume conditions (i)-(iii) listed at the beginning of §2 as well as condition (iv) of §4.2. Recall that ϵ denotes the sign of the functional equation of $E/\mathbb{Q}$. Then since $h_{p,K_n}(x) = -\frac{1}{2}\langle x, x\rangle_{K_n}$ and $h_{p,K_n}(\sigma z_n) = h_{p,K_n}(z_n)$ for every $\sigma \in \mathrm{Gal}(K_n/K)$, we have that

$$\begin{aligned} \langle z_n, \sigma z_n\rangle_{K_n} &= h_{p,K_n}(z_n) + h_{p,K_n}(-\epsilon\sigma z_n) - h_{p,K_n}(z_n - \epsilon\sigma z_n) \\ &= 2h_{p,K_n}(z_n) - h_{p,K_n}(z_n - \epsilon\sigma z_n). \end{aligned}$$

It remains to discuss the auxiliary computation of $h_{p,K_n}(z_n - \epsilon\sigma z_n)$.

We know that there exist $\sigma_0 \in \mathrm{Gal}(K_n/K)$ such that the Heegner point such that $\tau\sigma_0 z_n = -\epsilon\sigma_0 z_n$. It then follows that

$$\tau\sigma_0(\sigma z_n - \epsilon\sigma^{-1} z_n) = \sigma_0(-\epsilon\sigma^{-1} z_n + \sigma z_n). \tag{5.1}$$

and hence $(\sigma z_n - \epsilon\sigma^{-1} z_n) \in E(L_n)$ for every $\sigma \in \mathrm{Gal}(K_n/K)$, where $[L_n : \mathbb{Q}] = p^n$. This allows us to compute the height of $(\sigma z_n - \epsilon\sigma^{-1} z_n)$ by using Algorithm 4.5 independently of the analytic rank of $E/\mathbb{Q}$, simply replacing z_n by $(\sigma z_n - \epsilon\sigma^{-1} z_n)$.

Observe that the assumption that E has trivial rational torsion implies that both σz_n and $\sigma^{-1} z_n$ reduce to non-singular points at all bad primes, hence so does $(\sigma z_n - \epsilon\sigma^{-1} z_n)$ and consequently in its p-adic height computation $m_o = 1$. In addition, by (5.1) we know that the degree of the minimal polynomial of $x(\sigma z_n - \epsilon\sigma^{-1} z_n)$ divides p^n and hence Proposition 4.2 implies that

$$\mathcal{D}_{K_n}\left(\sigma z_n - \epsilon\sigma^{-1} z_n\right) = b\left(\sigma z_n - \epsilon\sigma^{-1} z_n\right)^{p^{n-r}},$$

where p^r is the degree of the minimal polynomial of $x\left(\sigma z_n - \epsilon\sigma^{-1}z_n\right)$ over $\mathbb{Z}$ and $b\left(\sigma z_n - \epsilon\sigma^{-1}z_n\right)$ is the prime to p part of its leading coefficient. Moreover, since $\mathrm{tr}_{K_n/K}\, z_n$ is a unit multiple of z_0, if the analytic rank of $E/\mathbb{Q}$ equals 1 and p does not divide z_0 in $E(K)$ it follows that

$$\mathcal{D}_{K_n}\left(\sigma z_n - \epsilon\sigma^{-1}z_n\right) = b\left(\sigma z_n - \epsilon\sigma^{-1}z_n\right).$$

Algorithm 5.1 (The pairings $\langle z_n, \sigma z_n\rangle$ for all $\sigma \in \mathrm{Gal}(K_n/K)$)**.**

(1) Depending on the analytic rank of $E/\mathbb{Q}$ and the behavior of p in $K/\mathbb{Q}$ we use the appropriate algorithm of §4.2 to compute a Heegner point $z_n \in E(\mathbb{C})$ and its p-adic height $h_{p,K_n}(z_n)$.
(2) Use Algorithm 3.2 to compute of the conjugates of z_n as points in $E(\mathbb{C})$. This fixes an ordering of the conjugates of z_n:
$$(z_n, \sigma_0 z_n, \ldots, \sigma_0^{p^n-1}z_n) \in E(\mathbb{C})^{p^n}$$
where $\sigma_0 \in \mathrm{Gal}(K_n/K)$ is an element of order p^n that is now fixed.
(3) We can then compute $\sigma_0^j z_n - \epsilon\sigma_0^{p^n-j}z_n \in E(\mathbb{C})$ for any $j \in \{1, \ldots, (p^n-1)/2\}$.
(4) Use Algorithm 4.5 to compute $h_{p,K_n}(\sigma_0^j z_n - \epsilon\sigma_0^{-j}z_n)$.
(5) This gives
$$\langle \sigma_0^j z_n, \sigma_0^{-j}z_n\rangle_{K_n} = 2h_{p,K_n}(z_n) - h_{p,K_n}(\sigma_0^j z_n - \epsilon\sigma_0^{-j}z_n).$$
(6) Since $\langle z_n, \sigma_0^{2j}z_n\rangle_{K_n} = \langle \sigma_0^j z_n, \sigma_0^{-j}z_n\rangle_{K_n}$ and p^i is odd, this gives us all pairings $\langle z_n, \sigma_0^j z_n\rangle$.

Example 5.2. Let $E/\mathbb{Q}$ be the rank 1 elliptic curve "57a1", $p = 5$, and $K = \mathbb{Q}(\sqrt{-2})$. We will use Algorithm 5.1 to compute a Heegner point z_1 and the 5-adic pairings:

$$\langle z_1, \sigma z_1\rangle_{K_1} \qquad \text{for all } \sigma \in \mathrm{Gal}(K_1/K).$$

Conditions (i)-(iii) listed at the beginning of §2 as well as condition (iv) of §4.2 hold. Using Sage we compute the Heegner point $z_0 \in E(K)$ and its 5-adic height:

$$h_{5,K}(z_0) = 5 + 3\cdot 5^2 + 5^3 + 5^4 + 2\cdot 5^5 + 5^7 + O(5^8).$$

Hence, p does not divide z_0 in $E(K)$, and we proceed to compute $z_1 \in E(\mathbb{C})$ and its 5-adic height following Algorithm 4.5. Through the first three steps of Algorithm 3.1 we approximate the coordinate of the Heegner point $z_1 \in E(\mathbb{C})$:

$$z_1 \approx (1.09134357351891, -0.919649689611060).$$

Then we use this point to find

$$h_{5,K_1}(z_1) = 2 + 2\cdot 5 + 2\cdot 5^2 + 5^4 + 4\cdot 5^5 + 4\cdot 5^6 + 3\cdot 5^7 + O(5^8).$$

Following Algorithm 3.2 we compute the 5-tuple of the conjugates of z_1 as points in $E(\mathbb{C})$:

$$(z_1, \sigma z_1, \sigma^2 z_1, \sigma^3 z_1, \sigma^4 z_1) \in E(\mathbb{C})^5$$

where $\sigma \in \mathrm{Gal}(K_1/K)$ denotes the element of order 5 that is now fixed.

Since $\epsilon = -1$ we proceed to compute

$$\begin{aligned}
\sigma z_1 + \sigma^4 z_1 &\approx (1.28240225474401 - 0.182500350994469i, -0.761690770112933 + 0.117006496908598i)\\
&\quad + (1.28240225474401 + 0.182500350994469i, -0.761690770112933 - 0.117006496908598i)\\
&\approx (-1.15375650323736, -1.80020432012303),\\
\sigma^2 z_1 + \sigma^3 z_1 &\approx (1.67723875767367 - 0.0866463691344989i, -1.39041234698688 + 0.149731706982934i)\\
&\quad + (1.67723875767367 + 0.0866463691344989i, -1.39041234698688 - 0.149731706982934i)\\
&\approx (0.631776964264686, -1.41622745195929),
\end{aligned}$$

and then use Algorithm 4.5 to compute the 5-adic heights of these points.

We compute the minimal polynomial of the x coordinate $\sigma z_1 + \sigma^4 z_1$:

$$575045004169216x^5 + 1883069884256000x^4 + 2633285660453540x^3 + 2747042174769680x^2 + 2325461580346885x + 909442872123731,$$

which gives

$$\mathcal{D}_{K_1}(\sigma z_1 + \sigma^4 z_1) = 575045004169216.$$

Since the point $(\sigma z_1 + \sigma^4 z_1)$ has order 3 in $E(\mathbb{F}_5)$, we have that $m = 3$ and

$$\begin{aligned} h_{5,K_1}(\sigma z_1 + \sigma^4 z_1) &= \frac{1}{5}\left(\frac{1}{3^2}\log_5\left(N_{L_{\mathfrak{p}_1}/\mathbb{Q}_5}\left(\frac{\sigma_5(3\operatorname{res}_{\mathfrak{p}_1}(\sigma z_1 + \sigma^4 z_1))}{f_3(x(\operatorname{res}_{\mathfrak{p}_1}(\sigma z_1 + \sigma^4 z_1)))}\right)^2\right) - \log_5(\mathcal{D}_{K_1}(\sigma z_1 + \sigma^4 z_1))\right) \\ &= 1 + 5 + 5^2 + 2\cdot 5^3 + 5^4 + 4\cdot 5^7 + 5^8 + 5^9 + O(5^{10}). \end{aligned}$$

Repeating the computation for $\sigma^2 z_1 + \sigma^3 z_1$, we first compute the minimal polynomial of the x-coordinate of $(\sigma^2 z_1 + \sigma^3 z_1)$:

$$258022025068096x^5 + 852975284094800x^4 + 587418614311065x^3 - 166184992922095x^2 + 75604423293285x - 291423856921639,$$

which gives

$$\mathcal{D}_{K_1}(\sigma^2 z_1 + \sigma^3 z_1) = 258022025068096.$$

As the point $\sigma^2 z_1 + \sigma^3 z_1$ has again order 3 in $E(\mathbb{F}_5)$, we have $m = 3$ and

$$\begin{aligned} h_{5,K_1}(\sigma^2 z_1 + \sigma^3 z_1) &= \frac{1}{5}\left(\frac{1}{3^2}\log_5\left(N_{L_{\mathfrak{p}_1}/\mathbb{Q}_5}\left(\frac{\sigma_5(3\operatorname{res}_{\mathfrak{p}_1}(\sigma^2 z_1 + \sigma^3 z_1))}{f_3(x(\operatorname{res}_{\mathfrak{p}_1}(\sigma^2 z_1 + \sigma^3 z_1)))}\right)^2\right) - \log_5(\mathcal{D}_{K_1}(\sigma^2 z_1 + \sigma^3 z_1))\right) \\ &= 4\cdot 5^3 + 3\cdot 5^4 + 2\cdot 5^5 + 3\cdot 5^6 + 2\cdot 5^7 + 2\cdot 5^8 + 3\cdot 5^9 + O(5^{10}). \end{aligned}$$

To finish the computation, we note that

$$\begin{aligned} \langle z_1, z_1\rangle_{K_1} &= -2h_{5,K_1}(z_1) \\ \langle z_1, \sigma z_1\rangle_{K_1} &= \langle \sigma^2 z_1, \sigma^3 z_1\rangle_{K_1} \\ &= 2h_{5,K_1}(z_1) - h_{5,K_1}(\sigma^2 z_1 + \sigma^3 z_1) \\ &= 4 + 4\cdot 5 + 4\cdot 5^2 + 5^3 + 3\cdot 5^4 + 5^6 + 2\cdot 5^8 + O(5^{10}) \\ \langle z_1, \sigma^2 z_1\rangle_{K_1} &= \langle z_1, \sigma^3 z_1\rangle_{K_1} \\ \langle z_1, \sigma^3 z_1\rangle_{K_1} &= \langle \sigma z_1, \sigma^4 z_1\rangle_{K_1} \\ &= 2h_{5,K_1}(z_1) - h_{5,K_1}(\sigma^4 z_1 + \sigma z_1) \\ &= 3 + 3\cdot 5 + 3\cdot 5^2 + 3\cdot 5^3 + 3\cdot 5^5 + 4\cdot 5^6 + 3\cdot 5^7 + 2\cdot 5^8 + 2\cdot 5^9 + O(5^{10}) \\ \langle z_1, \sigma^4 z_1\rangle_{K_1} &= \langle z_1, \sigma z_1\rangle_{K_1}. \end{aligned}$$

Observe that as a numerical check, we can compute the sum of these pairings to obtain the following

$$\langle z_1, z_1\rangle_{K_1} + \langle z_1, \sigma z_1\rangle_{K_1} + \cdots + \langle z_1, \sigma^4 z_1\rangle_{K_1} = 2\cdot 5 + 2\cdot 5^2 + 5^4 + 4\cdot 5^5 + 5^6 + 2\cdot 5^9 + O(5^{10})$$

Using (2.2) we see that $\operatorname{tr}_{K_1/K}(z_1) = 3z_0$, and since $z_0 \in E(\mathbb{Q})$, Sage tells us that

$$\langle z_0, z_0\rangle_{\mathbb{Q}} = 4\cdot 5 + 5^2 + 3\cdot 5^3 + 3\cdot 5^4 + 2\cdot 5^5 + 4\cdot 5^6 + 3\cdot 5^7 + 2\cdot 5^8 + 4\cdot 5^9 + O(5^{10}).$$

This allows us see, numerically, that

$$\begin{aligned} \langle \operatorname{tr}_{K_1/K}(z_1), \operatorname{tr}_{K_1/K}(z_1)\rangle_{K_1} &= 5\langle z_1, \operatorname{tr}_{K_1/K}(z_1)\rangle_{K_1} \\ &= 2\cdot 5^2 + 2\cdot 5^3 + 5^5 + 4\cdot 5^6 + 5^7 + O(5^{10}) \\ &= [K_1 : \mathbb{Q}]\langle 3z_0, 3z_0\rangle_{\mathbb{Q}}, \end{aligned}$$

which also tests consistency with the existing Sage implementation of p-adic heights of rational points on elliptic curves.

6. Λ-adic regulators

In this section we compute coefficients of Λ-adic regulators of several elliptic curves $E/\mathbb{Q}$. In all these examples z_0 is not divisible by p in $E(K)$ and the valuation of $h_{p,K}(z_0)$ is strictly positive. Hence, we know that the Heegner L-function $\mathcal{L}$ equals the Λ-adic regulator $\mathcal{R}$ up to a unit and they are non-trivial. Recall from §2 that the coefficients of the Heegner L-function are

$$\begin{aligned}\mathsf{b}_0 &= \langle c_0, c_0\rangle_{K_0},\\ \mathsf{b}_k &\equiv \sum_{k\le i<p^n}\binom{i}{k}\langle c_n, \sigma^i c_n\rangle_{K_n} \pmod{p^n} \quad \text{for } k\ge 1,\end{aligned}$$

where $c_0 = z_0$, $c_1 = u_0^{-1}z_1$, and $c_2 = (u_0u_1)^{-1}z_2$. Observe that since $\langle c_n, \sigma^i c_n\rangle = \langle c_n\sigma^{p^n-i}c_n\rangle$, it follows that

$$\mathsf{b}_1 \equiv 0 \pmod{p^n} \qquad \text{for all } n,$$

and hence $\mathsf{b}_1 = 0$. Consequently, in order to get any further information about the Heegner L-function we will need to compute $\mathsf{b}_2 \pmod{p^n}$ and perhaps additional coefficients also.

Observe that one common feature of all the Λ-adic regulators computed below, is that they are non-zero at the roots of $(T+1)^{p^n}-1=0$ for every $n\in\mathbb{N}$.

Example 6.1. Let $E/\mathbb{Q}$ be the rank 1 elliptic curve "57a1", $p=5$, and $K=\mathbb{Q}(\sqrt{-2})$. Using the computation of $h_{5,K}(z_0)$ in Example 5.2, we find that

$$\mathsf{b}_0 = \langle c_0, c_0\rangle_{K_0} = -2h_{5,K}(c_0) = -2h_{5,K}(z_0) = 3\cdot 5 + 3\cdot 5^2 + 5^3 + 2\cdot 5^4 + 4\cdot 5^6 + 2\cdot 5^7 + O(5^8).$$

In Example 5.2, we have also computed

$$\begin{aligned}\langle z_1, \sigma z_1\rangle_{K_1} &\equiv 4 \pmod 5\\ \langle z_1, \sigma^2 z_1\rangle_{K_1} &\equiv 3 \pmod 5.\end{aligned}$$

Since $p=5$ is inert in $K/\mathbb{Q}$ and $a_5=-3$, we see that $u_0=3$ and

$$\begin{aligned}\mathsf{b}_2 &\equiv u_0^{-2}(\langle z_1, \sigma z_1\rangle_{K_1} + 4\langle z_1, \sigma^2 z_1\rangle_{K_1}) \pmod 5\\ &\equiv 4 \pmod 5.\end{aligned}$$

Then we have that $\mathcal{R}(T) = \mathcal{L}(T) \equiv 4T^2$ modulo $(T^3, 5)$ and hence $\mathcal{R}$ equals the product of a unit of and a distinguished polynomial of degree 2 in $\mathbb{Z}_5[[T]]$.

Example 6.2. Let $E/\mathbb{Q}$ be the rank 1 elliptic curve "57a1", $p=5$, and $K=\mathbb{Q}(\sqrt{-14})$, as in Example 4.7. We have that $\mathsf{b}_0 = -2h_{5,K}(z_0) \equiv 0 \pmod 5$ and

$$\begin{aligned}\langle z_1, \sigma z_1\rangle_{K_1} &= 3\cdot 5 + 5^2 + 5^4 + 2\cdot 5^5 + O(5^6)\\ \langle z_1, \sigma^2 z_1\rangle_{K_1} &= 3 + 3\cdot 5 + 2\cdot 5^2 + 5^3 + 3\cdot 5^4 + 2\cdot 5^5 + O(5^6).\end{aligned}$$

Then since $p=5$ is splits in $K/\mathbb{Q}$ and $a_5=-3$, we see that $u_0=11$ and

$$\begin{aligned}\mathsf{b}_2 &\equiv u_0^{-2}(\langle z_1, \sigma z_1\rangle_{K_1} + 4\langle z_1, \sigma^2 z_1\rangle_{K_1}) \pmod 5\\ &\equiv 2 \pmod 5.\end{aligned}$$

This implies that $\mathcal{R}(T) = \mathcal{L}(T) \equiv 2T^2$ modulo $(T^3, 5)$ and $\mathcal{R}$ is the product of a unit and a distinguished polynomial of degree 2 in $\mathbb{Z}_5[[T]]$.

Example 6.3. Let $E/\mathbb{Q}$ be the rank 1 elliptic curve "331a1", $p = 7$, and $K = \mathbb{Q}(\sqrt{-2})$. We compute

$$\mathsf{b}_0 = \langle c_0, c_0 \rangle_{K_0} = 2 \cdot 7 + 6 \cdot 7^2 + 4 \cdot 7^3 + 3 \cdot 7^4 + 2 \cdot 7^5 + 2 \cdot 7^6 + 5 \cdot 7^7 + O(7^8).$$

For $\sigma \in \mathrm{Gal}(K_1/K)$ the element of order p fixed in Step 2 of Algorithm 5.1 we then find

$$\begin{aligned}
\langle z_1, \sigma z_1 \rangle_{K_1} &= 2 + 2 \cdot 7 + 2 \cdot 7^2 + 7^3 + 6 \cdot 7^5 + 2 \cdot 7^6 + 2 \cdot 7^7 + O(7^8) \\
\langle z_1, \sigma^2 z_1 \rangle_{K_1} &= 2 \cdot 7 + 6 \cdot 7^2 + 5 \cdot 7^3 + 3 \cdot 7^4 + 2 \cdot 7^6 + 7^7 + O(7^8) \\
\langle z_1, \sigma^3 z_1 \rangle_{K_1} &= 2 + 7 + 3 \cdot 7^2 + 5 \cdot 7^3 + 3 \cdot 7^4 + 2 \cdot 7^5 + 4 \cdot 7^6 + 6 \cdot 7^7 + O(7^8).
\end{aligned}$$

Moreover, since 7 is inert in $K/\mathbb{Q}$ and $a_7 = 2$, we have $u_0 = -4$ and

$$\begin{aligned}
\mathsf{b}_2 &\equiv u_0^{-2}(\langle z_1, \sigma z_1 \rangle_{K_1} + 4\langle z_1, \sigma^2 z_1 \rangle_{K_1} + 2\langle z_1, \sigma^3 z_1 \rangle_{K_1}) \pmod 7 \\
&\equiv 3 \pmod 7.
\end{aligned}$$

Hence, $\mathcal{R}(T) = \mathcal{L}(T) \equiv 3T^2$ modulo $(T^3, 7)$ and the Λ-adic regulator $\mathcal{R}$ is the product of a unit and a distinguished polynomial of degree 2 in $\mathbb{Z}_7[[T]]$.

In the following three examples we will have that $p = 3$, p splits in $K/\mathbb{Q}$, and $a_p = -1$. Consequently, we find that $u_0 = 1$, $u_1^{-1} \equiv 5 + 6\sigma + 6\sigma^2 \pmod 9$, and hence

$$\begin{aligned}
\langle c_2, \sigma^i c_2 \rangle_{K_2} &\equiv \langle 5z_2 + 6\sigma z_2 + 6\sigma^2 z_2, 5\sigma^i z_2 + 6\sigma^{i+1} z_2 + 6\sigma^{i+2} z_2 \rangle_{K_2} \pmod 9 \\
&\equiv 3\langle z_2, \sigma^{i-2} z_2 \rangle_{K_2} + 3\langle z_2, \sigma^{i-1} z_2 \rangle_{K_2} + 7\langle z_2, \sigma^i z_2 \rangle_{K_2} + 3\langle z_2, \sigma^{i+1} z_2 \rangle_{K_2} + 3\langle z_2, \sigma^{i+2} z_2 \rangle_{K_2} \pmod 9.
\end{aligned}$$

Example 6.4. Let $E/\mathbb{Q}$ be the rank 1 elliptic curve "203b1", $p = 3$, and $K = \mathbb{Q}(\sqrt{-5})$. We compute 3-adic heights and the 3-adic sigma function for elliptic curves over $\mathbb{Q}$ using the methods in [1]. We find that the first coefficient of the Heegner L-function is

$$\mathsf{b}_0 = \langle c_0, c_0 \rangle_{K_0} = 3^2 + 3^3 + 3^5 + O(3^8).$$

Then for $\sigma \in \mathrm{Gal}(K_1/K)$ the element of order p fixed in Step 2 of Algorithm 5.1 we compute

$$\begin{aligned}
\langle z_1, z_1 \rangle_{K_1} &= 2 + 2 \cdot 3 + 2 \cdot 3^2 + 3^3 + 3^4 + O(3^8) \\
\langle z_1, \sigma z_1 \rangle_{K_1} &= 2 + 3 + 3^3 + 2 \cdot 3^4 + 3^5 + 3^6 + 3^7 + O(3^8) \\
\langle z_1, \sigma^2 z_1 \rangle_{K_1} &= \langle z_1, \sigma z_1 \rangle_{K_1}.
\end{aligned}$$

Note that this gives $\mathsf{b}_2 \equiv u_0^{-2}\langle z_1, \sigma z_1 \rangle_{K_1} \equiv 2 \pmod 3$.

In this example $\mathcal{R}(T) \equiv 2T^2$ modulo $(T^3, 3)$ and it is again the product of a unit and a distinguished polynomial of degree 2 in $\mathbb{Z}_3[[T]]$. However, while in the previous examples b_0 has valuation 1 which implies that $\mathcal{R}$ is irreducible, in this case b_0 has valuation 2 and the computed data does not imply that $\mathcal{R}$ is irreducible but it does show that $\mathcal{R}$ is squarefree.

Example 6.5. Let $E/\mathbb{Q}$ be the rank 1 elliptic curve "185b1", $p = 3$, and $K = \mathbb{Q}(\sqrt{-11})$. First, we have

$$\mathsf{b}_0 = \langle c_0, c_0 \rangle_{K_0} = 2 \cdot 3 + 3^2 + 3^3 + 3^5 + 2 \cdot 3^6 + 3^7 + O(3^8).$$

For $\sigma \in \mathrm{Gal}(K_1/K)$ the element of order p fixed in Step 2 of Algorithm 5.1 we have:

$$\begin{aligned}
\langle z_1, z_1 \rangle_{K_1} &= 2 \cdot 3 + 2 \cdot 3^2 + 3^4 + 2 \cdot 3^6 + 3^7 + O(3^8) \\
\langle z_1, \sigma z_1 \rangle_{K_1} &= 3^2 + 3^4 + O(3^8) \\
\langle z_1, \sigma^2 z_1 \rangle_{K_1} &= \langle z_1, \sigma z_1 \rangle_{K_1}.
\end{aligned}$$

So we see that we have $\mathsf{b}_2 \equiv 0 \pmod 3$. Thus we now compute $\mathsf{b}_3 \pmod 9$. For $\sigma \in \mathrm{Gal}(K_2/K)$ the element of order p^2 fixed in Step 2 of Algorithm 5.1 we have:

$$\begin{aligned}
\langle z_2, z_2\rangle_{K_2} &= 1+3+3^3+2\cdot 3^4+2\cdot 3^5+O(3^7)\\
\langle z_2, \sigma z_2\rangle_{K_2} &= 1+3+3^2+2\cdot 3^3+3^4+3^5+O(3^7)\\
\langle z_2, \sigma^2 z_2\rangle_{K_2} &= 2+3+2\cdot 3^3+2\cdot 3^4+2\cdot 3^5+O(3^7)\\
\langle z_2, \sigma^3 z_2\rangle_{K_2} &= 1+2\cdot 3^2+2\cdot 3^3+3^4+O(3^7)\\
\langle z_2, \sigma^4 z_2\rangle_{K_2} &= 3^2+3^3+3^4+2\cdot 3^5+O(3^7)\\
\langle z_2, \sigma^5 z_2\rangle_{K_2} &= \langle z_2, \sigma^4 z_2\rangle_{K_2}\\
\langle z_2, \sigma^6 z_2\rangle_{K_2} &= \langle z_2, \sigma^3 z_2\rangle_{K_2}\\
\langle z_2, \sigma^7 z_2\rangle_{K_2} &= \langle z_2, \sigma^2 z_2\rangle_{K_2}\\
\langle z_2, \sigma^8 z_2\rangle_{K_2} &= \langle z_2, \sigma z_2\rangle_{K_2}.
\end{aligned}$$

Consequently, we find that

$$\begin{aligned}
\langle c_2, \sigma c_2\rangle_{K_2} &\equiv 7 \pmod 9\\
\langle c_2, \sigma^2 c_2\rangle_{K_2} &\equiv 8 \pmod 9\\
\langle c_2, \sigma^3 c_2\rangle_{K_2} &\equiv 7 \pmod 9\\
\langle c_2, \sigma^4 c_2\rangle_{K_2} &\equiv 3 \pmod 9,
\end{aligned}$$

which gives $\mathsf{b}_2 \equiv 6 \pmod 9$ and

$$\begin{aligned}
\mathsf{b}_3 &\equiv 2\langle c_2, \sigma c_2\rangle_{K_2} + 8\langle c_2, \sigma^2 c_2\rangle_{K_2} + 3\langle c_2, \sigma^3 c_2\rangle_{K_2} + 5\langle c_2, \sigma^4 c_2\rangle_{K_2} \pmod 9\\
&\equiv 6 \pmod 9.
\end{aligned}$$

So, we must now compute $\mathsf{b}_4 \pmod 9$. We find that

$$\begin{aligned}
\mathsf{b}_4 &\equiv 7\langle c_2, \sigma c_2\rangle_{K_2} + 8\langle c_2, \sigma^2 c_2\rangle_{K_2} + 6\langle c_2, \sigma^3 c_2\rangle_{K_2} + 6\langle c_2, \sigma^4 c_2\rangle_{K_2} \pmod 9\\
&\equiv 2 \pmod 9.
\end{aligned}$$

Hence, $\mathcal{R}(T) = \mathcal{L}(T) \equiv 6 + 6T^2 + 6T^3 + 2T^4$ modulo $(T^5, 9)$ and in this case the regulator $\mathcal{R}$ is the product of a unit and a distinguished polynomial of degree 4 in $\mathbb{Z}_3[[T]]$.

Example 6.6. Let $E/\mathbb{Q}$ be the rank 1 elliptic curve "325b1", $p = 3$, and $K = \mathbb{Q}(\sqrt{-14})$. First, we have

$$\mathsf{b}_0 = \langle c_0, c_0\rangle_{K_0} = 3 + 3^3 + 2\cdot 3^4 + 2\cdot 3^5 + O(3^8).$$

For $\sigma \in \mathrm{Gal}(K_1/K)$ the element of order p fixed in Step 2 of Algorithm 5.1:

$$\begin{aligned}
\langle z_1, z_1\rangle_{K_1} &= 2\cdot 3 + 3^2 + 2\cdot 3^4 + 2\cdot 3^6 + 2\cdot 3^7 + O(3^8)\\
\langle z_1, \sigma z_1\rangle_{K_1} &= 3 + 2\cdot 3^2 + 3^3 + 3^4 + 2\cdot 3^5 + O(3^8)\\
\langle z_1, \sigma^2 z_1\rangle_{K_1} &= \langle z_1, \sigma z_1\rangle.
\end{aligned}$$

So we see that we have $\mathsf{b}_2 \equiv 0 \pmod 3$. Thus we go to the next coefficient; for $\sigma \in \mathrm{Gal}(K_2/K)$ the element of order p^2 fixed in Step 2 of Algorithm 5.1 we have:

$$\begin{aligned}
\langle z_2, z_2\rangle_{K_2} &= 2+3+2\cdot 3^2+3^3+2\cdot 3^4+2\cdot 3^5+3^6+O(3^8)\\
\langle z_2, \sigma z_2\rangle_{K_2} &= 1+2\cdot 3+2\cdot 3^4+2\cdot 3^5+3^6+3^7+O(3^8)\\
\langle z_2, \sigma^2 z_2\rangle_{K_2} &= 1+2\cdot 3^2+3^3+2\cdot 3^6+3^7+O(3^8)\\
\langle z_2, \sigma^3 z_2\rangle_{K_2} &= 2+3+3^2+2\cdot 3^4+2\cdot 3^5+3^7+O(3^8)\\
\langle z_2, \sigma^4 z_2\rangle_{K_2} &= 1+3+2\cdot 3^3+3^5+3^6+O(3^8)\\
\langle z_2, \sigma^5 z_2\rangle_{K_2} &= \langle z_2, \sigma^4 z_2\rangle_{K_2}\\
\langle z_2, \sigma^6 z_2\rangle_{K_2} &= \langle z_2, \sigma^3 z_2\rangle_{K_2}\\
\langle z_2, \sigma^7 z_2\rangle_{K_2} &= \langle z_2, \sigma^2 z_2\rangle_{K_2}\\
\langle z_2, \sigma^8 z_2\rangle_{K_2} &= \langle z_2, \sigma z_2\rangle_{K_2}.
\end{aligned}$$

Consequently, we find that

$$\begin{aligned}
\langle c_2, \sigma c_2\rangle_{K_2} &\equiv 4 \pmod 9\\
\langle c_2, \sigma^2 c_2\rangle_{K_2} &\equiv 7 \pmod 9\\
\langle c_2, \sigma^3 c_2\rangle_{K_2} &\equiv 2 \pmod 9\\
\langle c_2, \sigma^4 c_2\rangle_{K_2} &\equiv 1 \pmod 9,
\end{aligned}$$

which gives $\mathsf{b}_2 \equiv 3 \pmod 9$ and

$$\begin{aligned}
\mathsf{b}_3 &\equiv 2\langle c_2, \sigma c_2\rangle_{K_2} + 8\langle c_2, \sigma^2 c_2\rangle_{K_2} + 3\langle c_2, \sigma^3 c_2\rangle_{K_2} + 5\langle c_2, \sigma^4 c_2\rangle_{K_2} \pmod 9\\
&\equiv 3 \pmod 9.
\end{aligned}$$

We continue to compute successive $\mathsf{b}_i \pmod 9$ until we find one which is not divisible by 3:

$$\begin{aligned}
\mathsf{b}_4 &\equiv 7\langle c_2, \sigma c_2\rangle_{K_2} + 8\langle c_2, \sigma^2 c_2\rangle_{K_2} + 6\langle c_2, \sigma^3 c_2\rangle_{K_2} + 6\langle c_2, \sigma^4 c_2\rangle_{K_2} \pmod 9\\
&\equiv 3 \pmod 9.\\
\mathsf{b}_5 &\equiv 2\langle c_2, \sigma c_2\rangle_{K_2} + 3\langle c_2, \sigma^2 c_2\rangle_{K_2} + 6\langle c_2, \sigma^3 c_2\rangle_{K_2} + \langle c_2, \sigma^4 c_2\rangle_{K_2} \pmod 9\\
&\equiv 6 \pmod 9,\\
\mathsf{b}_6 &\equiv \langle c_2, \sigma c_2\rangle_{K_2} + 7\langle c_2, \sigma^2 c_2\rangle_{K_2} + \langle c_2, \sigma^3 c_2\rangle_{K_2} \pmod 9\\
&\equiv 1 \pmod 9.
\end{aligned}$$

Hence, $\mathcal{R}(T) = \mathcal{L}(T) \equiv 3 + 3T^2 + 3T^3 + 3T^4 + 6T^5 + T^6$ modulo $(T^7, 9)$ and we have now found an example where the Λ-adic regulator $\mathcal{R}$ is the product of a unit and a distinguished polynomial of degree 6 in $\mathbb{Z}_3[[T]]$.

Appendix: elliptic curves and their Cremona labels

Label	**Equation**
57a1	$y^2 + y = x^3 - x^2 - 2x + 2$
185b1	$y^2 + y = x^3 - x^2 - 5x + 6$
203b1	$y^2 + xy + y = x^3 + x^2 - 2$
325b1	$y^2 + y = x^3 - x^2 - 3x + 3$
331a1	$y^2 + xy = x^3 - 5x + 4$

References

[1] J. S. Balakrishnan, *On 3-adic heights on elliptic curves*, Preprint (2012), 1–8, http://www.math.harvard.edu/~jen/three_adic_heights.pdf.

[2] M. Bertolini, *Selmer groups and Heegner points in anticyclotomic $\mathbb{Z}_p$-extensions*, Compositio Math. **99** (1995), no. 2, 153–182.

[3] H. Cohen, *A course in computational algebraic number theory*, Springer-Verlag, Berlin, 1993.

[4] ———, *Number theory. Vol. I. Tools and Diophantine equations*, Graduate Texts in Mathematics, vol. 239, Springer, New York, 2007.

[5] C. Cornut, *Mazur's conjecture on higher Heegner points*, Invent. Math. **148** (2002), no. 3, 495–523.

[6] J. E. Cremona, *Elliptic Curve Data*, http://www.warwick.ac.uk/~masgaj/ftp/data/.

[7] B. Gross and D. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320.

[8] B. H. Gross, *Heegner points on $X_0(N)$*, Modular forms (Durham, 1983), Ellis Horwood Ser. Math. Appl.: Statist. Oper. Res., Horwood, Chichester, 1984, pp. 87–105.

[9] ———, *Kolyvagin's work on modular elliptic curves*, L-functions and arithmetic (Durham, 1989), Cambridge Univ. Press, Cambridge, 1991, pp. 235–256.

[10] D. Harvey, *Efficient computation of p-adic heights*, LMS J. Comput. Math. **11** (2008), 40–59.

[11] B. Howard, *The Iwasawa theoretic Gross-Zagier theorem*, Compos. Math. **141** (2005), no. 4, 811–846.

[12] D. Jetchev, *Global divisibility of Heegner points and Tamagawa numbers*, Compos. Math. **144** (2008), no. 4, 811–826.

[13] A. W. Knapp, *Elliptic curves*, Princeton University Press, Princeton, NJ, 1992.

[14] B. Mazur and K. Rubin, *Elliptic curves and class field theory*, Proceedings of the International Congress of Mathematicians, vol. II, Higher Ed. Press, Beijing, 2002, pp. 185–195.

[15] B. Mazur, W. Stein, and J. Tate, *Computation of p-adic heights and log convergence*, Doc. Math. (2006), no. Extra Vol., 577–614 (electronic).

[16] B. Mazur and J. Tate, *The p-adic sigma function*, Duke Math. J. **62** (1991), no. 3, 663–688. MR 93d:11059

[17] B. Perrin-Riou, *Fonctions L p-adiques, théorie d'Iwasawa et points de Heegner*, Bull. Soc. Math. France **115** (1987), no. 4, 339–456.

[18] W. Stein, *Algebraic number theory, a computational approach*, 2007, http://wstein.org/books/ant/.

[19] W. A. Stein et al., *Sage Mathematics Software (Version 5.10)*, The Sage Development Team, 2013, http://www.sagemath.org.

[20] The PARI Group, Bordeaux, *PARI/GP, version* 2.5.0, 2011, available from http://pari.math.u-bordeaux.fr/.

[21] V. Vatsal, *Special values of anticyclotomic L-functions*, Duke Math. J. **116** (2003), no. 2, 219–261.

[22] M. Watkins, *Some remarks on Heegner point computations*, Preprint (2006), http://arxiv.org/abs/math/0506325.

[23] C. Wuthrich, *On p-adic heights in families of elliptic curves*, J. London Math. Soc. (2) **70** (2004), no. 1, 23–40.

Jennifer S. Balakrishnan, Department of Mathematics, Harvard University, 1 Oxford Street, Cambridge, MA 02138, USA

E-mail address: jen@math.harvard.edu

URL: http://www.math.harvard.edu/~jen/

Mirela Çiperiani, Department of Mathematics, the University of Texas at Austin, 1 University Station, C1200 Austin, Texas 78712, USA

E-mail address: mirela@math.utexas.edu

URL: http://www.ma.utexas.edu/users/mirela/

William Stein, Department of Mathematics, University of Washington, Seattle, Box 354350 WA 98195, USA

E-mail address: wstein@uw.edu

URL: http://wstein.org/