p-ADIC HEIGHTS OF HEEGNER POINTS AND ANTICYCLOTOMIC 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, which enable us to 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, we recast earlier work of Mazur, Stein, and Tate, which then allows us to produce effective algorithms to compute p-adic heights of points of E defined over number fields. These methods make it possible for us to give the first explicit examples of Heegner L-functions and anticyclotomic Λ-adic regulators.

1. 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 [11] 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 $\Lambda = \mathbb{Z}_p[\mathrm{Gal}(K_\infty/K)]$. 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 $K_\infty^{\mathrm{cycl}}/K$. Under the assumptions that the elliptic curve $E/\mathbb{Q}$ has ordinary non-anomalous reduction at p and that p does not divide the product of the Tamagawa numbers, we have that the p-adic height pairing takes values in $\Gamma_{\mathrm{cycl}} \otimes_{\mathbb{Z}_p} \Lambda$. By work of Cornut [4] and Vatsal [17] 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 Heegner points

Date: August 29, 2012.

2000 *Mathematics Subject Classification.* 11Y40, 11G50, 11G05.

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

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

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

give rise to the full module of universal norms, 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 3).

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 giving a rigorous construction of these Heegner points (see Section 2), generalizing various results of Watkins [18] and Cohen [3, §8.6]. This allows us 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 4. Then, since these Heegner points are defined over number fields, we discuss how to adapt the techniques of Mazur, Stein, and Tate [12] to this situation. In particular, [12] 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 p-adic heights, following [12], 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, obtaining a fast generalization of the denominator algorithm is more subtle, especially when the class number of F is not one; see Sections 5 and 6. 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 7 we present an alternative approach which merely involves knowing the minimal polynomial of the x-coordinate of P. Then in Section 8, we build on these improvements and discuss the computation of p-adic height pairings of Galois conjugates of Heegner points. With these algorithms in hand, in Section 9 we provide the first explicit examples of Heegner L-functions and hence Λ-adic regulators.

Remark 1.1. 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 very likely 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.

2. Heegner points and binary quadratic forms

In this section, we generalize various aspects of Watkins [18], and Cohen [3, §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.

2.1. **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 2.1. *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 $N\tau = \frac{-NB+N\sqrt{D}}{2A}$.
($\Longrightarrow$) 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 $\gcd(A/N, B, CN) = 1$.

($\Longleftarrow$) 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 2.2. *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 2.1, 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 2.1 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. □

Lemma 2.3. *Let $\gamma \in M_2(\mathbb{Z})$ be a matrix of nonzero determinant and $f_\tau = (A, B, C)$ for some $\tau \in \mathcal{H}$. 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

$$\begin{pmatrix} A' & B'/2 \\ B'/2 & C' \end{pmatrix} = \gamma^t \begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix} \gamma \tag{2.1}$$

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.

Suppose a prime ℓ divides $n = gcd(A', B', C')$. If ℓ is odd, then viewing (2.1) modulo ℓ we find

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

where $\overline{\gamma}$ (resp. $\overline{m}$) equals γ (resp. m) modulo ℓ. Then, since $\gcd(A, B, C) = 1$ implies that $\overline{m} \neq 0$, 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 (2.1) lie in $M_2(\mathbb{Z})$. By the argument used for odd primes, we see that 2^2 cannot divide B'. Hence viewing (2.1) modulo 2 we have

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

which implies that

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

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

□

Lemma 2.4. *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 2.3 (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 analyze further in Section 2.3.

2.2. **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 of primitive positive definite binary quadratic forms of discriminant D via the following inverse bijections (see [2, Theorem 5.2.8]):

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

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

and

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

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 $\mathrm{Gal}(K/\mathbb{Q})$.

2.3. **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* $W_q(\tau) = \frac{uq\tau + v}{N\tau + q}$ of $\Gamma_0(N)\backslash\mathcal{H}$. The involutions W_q commute and act via a group W isomorphic to $\mathbb{F}_2^\nu$, where ν is the number of prime divisors of N.

Lemma 2.5. *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 2.3 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 2.4, 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 2.6. Observe that in the above proof we have shown that the matrix of $f_{w_q^{-1}(\tau)}$ equals $q^{-1}w_q^t \begin{pmatrix} A & B/2 \\ B/2 & C \end{pmatrix} w_q$.

By the above lemma we have that W acts on $\Gamma_0(N)\backslash\mathcal{H}_N^D$. We will now define the action 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) 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 $\Gamma_0(N)\backslash\mathcal{H}_N^D$.

We will now verify that the above choices define a group action of $\mathrm{Cl}(\mathcal{O}_c)$ on $\Gamma_0(N)\backslash\mathcal{H}_N^D$. Let $\mathfrak{a},\mathfrak{b}\in\mathrm{Cl}(\mathcal{O}_c)$. Observe that since Ψ_{FI} and Ψ_{IF} are inverses of one another we have the following

$$\begin{aligned} f_{\mathfrak{a}\cdot(\mathfrak{b}\cdot\tau)} \in \Psi_{IF}(\Psi_{FI}(f_{\mathfrak{b}\cdot\tau})\mathfrak{a}^{-1}) &= \Psi_{IF}\Big(\Psi_{FI}\big(\Psi_{IF}(\Psi_{FI}(f_\tau)\mathfrak{b}^{-1})\big)\mathfrak{a}^{-1}\Big) = \\ &= \Psi_{IF}\Big(\big(\Psi_{FI}(f_\tau)\mathfrak{b}^{-1}\big)\mathfrak{a}^{-1}\Big) = \Psi_{IF}\big(\Psi_{FI}(f_\tau)\mathfrak{b}^{-1}\mathfrak{a}^{-1}\big) = \\ &= \Psi_{IF}\big(\Psi_{FI}(f_\tau)(\mathfrak{a}\mathfrak{b}))^{-1}\big). \end{aligned}$$

Then by (2) above it follows that $\mathfrak{a}\cdot(\mathfrak{b}\cdot\tau)=(\mathfrak{a}\mathfrak{b})\cdot\tau\in\Gamma_0(N)\backslash\mathcal{H}_N^D$.

Lemma 2.7. *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 2.5 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 2.6, 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

$$\begin{aligned} \Psi_{FI}(f_{w_q^{-1}(\tau)})I_{B,q} &= \left(A/q\mathbb{Z}+\frac{-B+\sqrt{D}}{2}\mathbb{Z}\right)\left(q\mathbb{Z}+\frac{-B+\sqrt{D}}{2}\mathbb{Z}\right) \\ &= A\mathbb{Z}+q\frac{-B+\sqrt{D}}{2}\mathbb{Z}+A/q\frac{-B+\sqrt{D}}{2}\mathbb{Z}+\left(AC+B\frac{-B+\sqrt{D}}{2}\right)\mathbb{Z} \\ &= A\mathbb{Z}+q\frac{-B+\sqrt{D}}{2}\mathbb{Z}+A/q\frac{-B+\sqrt{D}}{2}\mathbb{Z}+B\frac{-B+\sqrt{D}}{2}\mathbb{Z} \\ &= A\mathbb{Z}+\frac{-B+\sqrt{D}}{2}\mathbb{Z} \\ &= \Psi_{FI}(f_\tau). \end{aligned} \tag{2.2}$$

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 (2.2) 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 2.8. *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*

$$b_q \equiv b \pmod{2N/q} \qquad \textit{and} \qquad b_q \equiv -b \pmod{2q}.$$

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

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

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 2.7. 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 2.8 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 2.9. *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 G acts simply on $\mathcal{S}(D,N)\times\mathrm{Cl}(\mathcal{O}_c)$.

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 Φ is well-defined since

i) f_τ is a primitive positive definite quadratic form of discriminant D; and
ii) $B^2 - 4AC = D$ and $N|A$ implies that $B \in \mathcal{S}(D,N)$.

Theorem 2.10. *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 [2], 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

$$2Aab + B(ad + bc) + 2Ccd = 2Aab + B + 2Bbc + 2Ccd.$$

The assumption that $\Phi(\tau) = \Phi(\tau')$ also 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 2.1, 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 $W_q \in W$. Let us start by verifying that Φ is a W-map. By Lemma 2.5 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 (2.2) imply 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 $f_{\mathfrak{a}\cdot\tau} = (A', B', C') \in \Psi_{IF}(\Psi_{FI}(f_\tau)\mathfrak{a}^{-1})$ and $B' \equiv B \pmod{2N}$. It follows that

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

It then follows that Φ is a G-map.

Finally since by Lemma 2.9 we know that G acts transitively on the codomain of Φ, it follows that Φ is surjective, and this concludes the proof. □

Corollary 2.11. *The G-action on $\Gamma_0(N)\backslash\mathcal{H}_N^D$ is simply transitive.*

Proof. This follows immediately by Theorem 2.10 and Lemma 2.9. □

3. 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 of K, $D_K \leq -5$,
ii) every prime dividing the conductor N of $E/\mathbb{Q}$ splits in $K/\mathbb{Q}$,
iii) p satisfies the relevant condition of (3.5) and does not divide $ND_K h_K \prod_{\ell|N} c_\ell$, where h_K denotes the class number of K and c_ℓ the Tamagawa number of E at the prime ℓ.

We will now consider a Heegner point x_{p^n} of level N and discriminant $p^{2n}D_K$. By Gross [7, §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:

$$\mathfrak{a} \cdot x_{p^n} = x_{p^n}^{\mathrm{Artin}(\mathfrak{a})} \quad \text{for all } \mathfrak{a} \in \mathrm{Cl}(\mathcal{O}_{p^n}). \tag{3.1}$$

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.

The anticyclotomic $\mathbb{Z}_p$-extension K_∞ of K lies inside $K[p^\infty] := \cup_n K[p^n]$. Denote by K_n the 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 $\left(p - \left(\frac{D_K}{p}\right)\right) h_K$, where $\left(\frac{D_K}{p}\right)$ denotes the Legendre symbol.

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

$$z_0 = \mathrm{tr}_{K[1]/K}(y_{p^0}) \quad \text{and} \quad z_n = \mathrm{tr}_{K[p^{n+1}]/K_n}(y_{p^{n+1}}) \text{ for all } n \geq 1.$$

We will now list some properties of Heegner points:

- By the work of Gross-Zagier [6], 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 [8, Proposition 5.3], we know that $z_n^\tau + \epsilon\sigma(z_n) \in E(\mathbb{Q})_{\mathrm{tors}}$ for some $\sigma \in \mathrm{Gal}(K_n/K)$ where ϵ is the sign of the functional equation of $E/\mathbb{Q}$.
- By [6, §3.1, §3.3] (see also [10, Lemma 4.2]), the Heegner point z_n lies, up to translation by a rational torsion point of E, in the connected component of $E(K_{w_n})$ 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 [13, §3.3, Lemma 2], Perrin-Riou proves that

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

where $a_p = p + 1 - \#E(\mathbb{F}_p)$ and

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

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

$$\mathrm{tr}_{K_{n+2}/K_{n+1}}(z_{n+2}) = a_p z_{n+1} - z_n \text{ for } n \geq 1; \tag{3.2}$$

$$\mathrm{tr}_{K_2/K_1}(z_2) = \begin{cases} a_p z_1 - a_p z_0 & \text{if } p \text{ is inert,} \\ a_p z_1 - (a_p - 2) z_0 & \text{if } p \text{ splits;} \end{cases} \tag{3.3}$$

$$\mathrm{tr}_{K_1/K}(z_1) = \begin{cases} \big((a_p - 1)(a_p + 1) - p\big) z_0 & \text{if } p \text{ is inert,} \\ \big((a_p - 1)^2 - p\big) z_0 & \text{if } p \text{ splits.} \end{cases} \tag{3.4}$$

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 in $u_n \in \mathbb{Z}_p[\mathrm{Gal}(K_\infty/K)]$ under the following conditions:

$$\begin{cases} p \text{ does not divide } (a_p - 1)a_p(a_p + 1) & \text{if } p \text{ is inert,} \\ p \text{ does not divide } (a_p - 1)a_p & \text{if } p \text{ splits.} \end{cases} \tag{3.5}$$

More precisely, if the above conditions hold, then 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 that the conditions (3.5) hold and hence E has good ordinary non-anomalous reduction at p. Following Mazur and Rubin [11] 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. 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 $\Gamma_{\mathrm{cycl}} \otimes_{\mathbb{Z}_p} \Lambda$. We know that $\mathcal{U}$ is free of rank one over $\Lambda = \mathbb{Z}_p[\mathrm{Gal}(K_\infty/K)]$. This implies that the image of the cyclotomic p-adic height pairing is generated by the Λ*-adic regulator*[1] $\mathcal{R} \in \Gamma_{\mathrm{cycl}} \otimes_{\mathbb{Z}_p} \Lambda$. We would like to compute $\mathcal{R}$, and to do so we use Heegner points.

Our assumption of the conditions (3.5) implies that Heegner points give rise to the Heegner submodule $\mathcal{H} \subseteq \mathcal{U}$. In particular, 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 $c \in \mathcal{U}$. Mazur and Rubin define the *Heegner L-function*

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

One can easily see that $\mathcal{L} = \mathcal{R}\,\mathrm{char}(\mathcal{U}/\mathcal{H})^2$.

[1] Note that this definition of the Λ-adic regulator differs slightly from that of Howard [9].

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,
- p divides the p-adic height of z_0.

The first two conditions imply that $\mathrm{char}(\mathcal{U}/\mathcal{H})$ is trivial and the third ensures that $\mathcal{L}$ is not a unit.

We now identify Λ with $\mathbb{Z}_p[[T]]$ by sending 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 $\langle\, ,\, \rangle_{K_n}$ denotes the cyclotomic p-adic height pairing over the field 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

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

We will now proceed to describe algorithms to compute Heegner points and p-adic heights which will then in turn allow us to compute the above p-adic height pairings and hence the coefficients of Heegner L-functions.

4. 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.

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

$$\begin{tikzcd}
K[p^\infty] \arrow[d, dash] \arrow[dr, dash, "(p\pm1)h_k"] & \\
\vdots & K_\infty \\
\vdots & \vdots \\
K[p^3] \arrow[d, dash, "p"'] \arrow[dr, dash, "(p\pm1)h_k"] & K_3 \arrow[d, dash, "p"] \\
K[p^2] \arrow[d, dash, "p"'] \arrow[dr, dash, "(p\pm1)h_k"] & K_2 \arrow[d, dash, "p"] \\
K[p] \arrow[d, dash, "(p\pm1)h_k"'] & K_1 \arrow[dl, dash, "p"] \\
K = K_0 \arrow[d, dash, "2"'] & \\
\mathbb{Q} &
\end{tikzcd}$$

Observe that if we fix $b_0 \in \mathcal{S}(p^{2(n+1)}D_K, N)$ then Theorem 2.10 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 (3.1) 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 2.10 we know that

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

Hence we have that

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

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 [2, 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 4.1 (Computing Heegner points $z_n \in E(K_n)$)**.**

(1) Fix $b_0 \in \mathcal{S}(p^{2(n+1)}D_K, N)$.
(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, 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. Let $\tau_f \in X_0(N)$ be the Heegner point that corresponds to the form $f = Ax^2 + Bxy + Cy^2$.
(3) 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 [14, §2.5] and implemented as the `algebraic_dependency` command in [15] (which relies on the `algdep` command in [16]), algebraically reconstruct the x-coordinate of $z_n \in E(\mathbb{C})$ and one of two possible y-coordinates. Make sure that z_n is defined over a Galois dihedral extension of degree $2p^n$ that is ramified exactly at p and the primes dividing the discriminant of K.

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

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

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 4.1. 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 4.2 (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 4.1.
(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 $E(\mathbb{C})$.

5. Computation of p-adic heights: the class number 1 case

In this section, we begin by using [12] to produce an algorithm to compute p-adic heights in the most basic set up: the case when the relevant number field has class number 1. We then use this algorithm as well as (4.1) to compute p-adic heights of Heegner points $z_1 \in E(K_1)$ in examples when the fields K_1 have class number 1.

5.1. **An algorithm for computing p-adic heights.** Let F be a number field and consider a non-torsion point $P \in E(F)$. When the point P is defined over the fraction field of a principal ideal domain $\mathcal{O}$, then P can be written in the form $(\frac{a}{d^2}, \frac{b}{d^3})$, where $a, b, d \in \mathcal{O}$ and $\gcd(a, d) = \gcd(b, d) = 1$. In particular, for any place v of F 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 F_v denotes the completion of F at a place v, $\mathrm{res}_v : E(F) \to E(F_v)$ is the natural localization map, $a_v(P), b_v(P), d_v(P) \in \mathcal{O}_{F_v}$ and $\gcd(a_v(P), d_v(P)) = \gcd(b_v(P), d_v(P)) = 1$.

If the point $P \in E(F)$ reduces

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

then we have the following formula (see Mazur-Stein-Tate [12]) for computing the cyclotomic p-adic height of P:

$$h_{p,F}(P) = \frac{1}{p} \cdot \left(\sum_{\wp \mid p} \log_p(N_{F_\wp/\mathbb{Q}_p}(\sigma_\wp(P))) - \sum_{v \nmid p} \mathrm{ord}_v(d_v(P)) \cdot \log_p(\# k_v) \right), \tag{5.1}$$

where $\sigma_\wp$ is the p-adic sigma function at the prime $\wp$ and k_v is the residue field of F at v. Note that this assumes that we are working with a minimal model of E/F.

Suppose now that F has class number 1. Then since $\mathcal{O}_F$ is a principal ideal domain, there is a global choice of denominator $d(P)$ and the above formula (5.1) simplifies to the following:

$$h_{p,F}(P) = \frac{1}{p} \cdot \log_p \left(\prod_{\wp \mid p} N_{F_\wp/\mathbb{Q}_p} \left(\frac{\sigma_\wp(P)}{d(P)} \right) \right). \tag{5.2}$$

Note that our point P does not necessarily satisfy the two conditions listed above; in order to use the above formulas we compute the height of mP, where $m \in \mathbb{Z}$ is such that mP does reduce appropriately. Then we use that the height pairing is a quadratic form to recover the height of P.

We now need to compute the denominator $d(mP)$ of mP. We start by computing the denominator $d(P)$ of P. If α is an algebraic number an *integer denominator* of α is some positive integer d such that $d\alpha$ is an algebraic integer. Naturally d is not unique, since any positive multiple of d is also an integer denominator of α. The notion of integer denominator is computationally useful and easy to compute, since we represent algebraic numbers in terms of a power basis.

Algorithm 5.1 (Denominator $d(P)$ of $P \in E(F)$ with F of class number 1)**.**

1. Input $P = (x, y)$, where $P \in E(F)$.
2. Read off an integer denominator $d := d(x)$ of x, and consider the ideal $(x) = \frac{(d \cdot x)}{(d)}$, where $(d \cdot x)$ and (d) denote $\mathcal{O}_F$-ideals.
3. Simplify $(x) = \frac{(d \cdot x)}{(d)}$ by canceling common prime ideals in the numerator and denominator ideals.
4. What is left in the factored denominator ideal is a perfect square of prime ideals in $\mathcal{O}_F$, and the square root of this ideal is generated by the desired denominator $d(P)$.

One could repeat the above process for $mP \in E(F)$, but this may be infeasible due to the numerical explosion in the coordinates of mP. Instead, we make use of m-division polynomials to write $d(mP)$ in terms of $d(P)$. Using Proposition 1 of [19], we easily deduce the following:

Proposition 5.2. *Let F be a number field of class number one, f_m the m-th division polynomial of an elliptic curve E/F, and $P \in E(F)$ a non-torsion point that reduces to a non-singular point in $E(k_v)$ for every bad reduction prime v. Then the denominators $d(P), d(mP) \in \mathcal{O}_F$ are related as follows:*

$$d(mP) = f_m(P) d(P)^{m^2}.$$

Proof. By Proposition 1 of [19] we know that

$$d(mP) = u f_m(P) d(P)^{m^2},$$

where $u \in F$ is a unit in the completion of F at every finite prime. Since F has class number 1 it follows that u is a unit in $\mathcal{O}_F$. Then as $d(mP)$ is only defined up to units the result follows. □

Algorithm 5.3 (Height $h_{p,F}(P)$ of a non-torsion point $P \in E(F)$ with F of class number 1)**.**

1. Find the smallest positive integer m_o such that $m_oP \in E(F)$ reduces to a non-singular point in $E(k_v)$ for every bad reduction prime v.
2. Find a positive integer m such that mm_oP reduces to the identity $\mathrm{O} \in E(k_\wp)$ for all $\wp \mid p$.
3. Compute m_oP and mm_oP.
4. Compute $d(m_oP)$ as in Algorithm 5.1.
5. Compute $\sigma_\wp(t)$, the $\wp$-adic sigma function, for each $\wp \mid p$ as in [12].
6. Let $t_{mm_o} = -\frac{x(mm_oP)}{y(mm_oP)}$. Evaluate $\sigma_\wp(t_{mm_o}) \in F_\wp$ for each $\wp \mid p$. Then combining (5.2) and Proposition 5.2 we compute

$$h_{p,F}(P) = \frac{1}{m^2 m_o^2 p} \log_p \left(\prod_{\wp \mid p} N_{F_\wp/\mathbb{Q}_p} \left(\frac{\sigma_\wp(t_{mm_o})}{f_m(m_oP) d(m_oP)^{m^2}} \right) \right). \tag{5.3}$$

Remark 5.4. Observe that m_o divides the product of the Tamagawa numbers and m can be taken to be the least common multiple of $\#E(k_\wp)$ for $\wp \mid p$. However in practice, one wants m to be as small as possible, in order to reduce numerical explosion in the coordinates. In the case when $P = z_n$, by §3.1 and §3.3 of [6] (see also Lemma 4.2 of [10]), 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 in the case of Heegner points, if $E(\mathbb{Q})_{\mathrm{tors}}$ is trivial then we know that $m_0 = 1$ and m can be taken to be the product over $\wp \mid p$ of the orders of P in $E(k_\wp)$.

5.2. **Examples.** We illustrate these algorithms by computing explicit examples[2]. Throughout this paper we refer to elliptic curves by a version of their Cremona labels [5]; see Table 9.1 for the equations of the specific curves we use.

Example 5.5. Let $E/\mathbb{Q}$ be the rank 1 elliptic curve "57a1", $p = 5$, and $K = \mathbb{Q}(\sqrt{-2})$. Note that E/K has rank 1 and the three conditions listed at the beginning of Section 3 hold. In addition, p is inert in K and it does not divide $(a_p - 1)a_p(a_p + 1) = -24$.

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 this is an example where we are interested in computing the coefficients of the Heegner L-function (see §9).

We will now use Algorithm 4.1 to construct the Heegner point z_1. We fix $b_0 = 4 \in \mathcal{S}(5^4 \cdot (-8), 57)$. Since $h_K = 1$ and 5 is inert, we create a list of 6 equivalence classes of binary quadratic forms of order prime to 5 which satisfy conditions $(i) - (iv)$ of Section 4:

$$\begin{aligned}
f_1 &= 57x^2 + 4xy + 22y^2 &\qquad& \mathrm{ord}(f_1) = 6 \\
f_2 &= 114x^2 + 4xy + 11y^2 && \mathrm{ord}(f_2) = 3 \\
f_3 &= 627x^2 + 4xy + 2y^2 && \mathrm{ord}(f_3) = 2 \\
f_4 &= 627x^2 + 1030xy + 425y^2 && \mathrm{ord}(f_4) = 6 \\
f_5 &= 1254x^2 + 4xy + y^2 && \mathrm{ord}(f_5) = 1 \\
f_6 &= 1254x^2 + 2284xy + 1041y^2 && \mathrm{ord}(f_6) = 3.
\end{aligned}$$

[2] 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 1.1.

Then we compute

$$z_1 = \sum_{i=1}^{6} \pi(\tau_{f_i}) \in E(\mathbb{C}).$$

Numerically[3], we have that

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

Using LLL, we find[4] that the best degree 5 relation satisfied by the x-coordinate of the numerical approximation to z_1 above is

$$18034072681x^5 - 126430131580x^4 + 352783410220x^3 - 489834319200x^2 + 338504989540x - 93144838864.$$

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 last step of the Algorithm 4.1. The point z_1 is defined over

$$K_1 := \mathbb{Q}(b),$$

where b is a root of

$$x^{10} - 10x^8 - 20x^7 + 165x^6 - 12x^5 - 760x^3 + 2220x^2 + 5280x + 7744.$$

Observe that K_1 has class number 1 and hence we can use Algorithm 5.3 to compute the 5-adic height of z_1. Explicitly, we will compute with z_1 with coordinates

$$\begin{aligned}
x(z_1) = {} & \frac{96698852571685}{2145672615243325696}b^9 + \frac{2472249905907}{195061146840302336}b^8 + \frac{916693155514421}{2145672615243325696}b^7 + \frac{1348520950997779}{2145672615243325696}b^6 - \frac{82344497086595}{12191321677518896}b^5 \\
& + \frac{2627122040194919}{536418153810831424}b^4 - \frac{452199105143745}{48765286710075584}b^3 + \frac{4317002771457621}{536418153810831424}b^2 + \frac{2050725777454935}{670522692263539 28}b + \frac{3711967683469209}{3047830419379724}, \\
y(z_1) = {} & \frac{10673542578700487}{6548739117582760250944}b^9 + \frac{21559110337008787}{595339919780250931904}b^8 + \frac{5997724383564410 33}{6548739117582760250944}b^7 - \frac{3521252836571400333}{6548739117582760250944}b^6 \\
& - \frac{145353099505283479}{744174899725313664 88}b^5 + \frac{6974718395834626805}{1637184779395690062736}b^4 + \frac{3525327915265535447}{1488349799450627329 76}b^3 - \frac{3802882910904310907 9}{1637184779395690062736}b^2 \\
& - \frac{23719086146860375069}{20464809742446125784 2}b - \frac{9830025310349811566}{930218624656642081 1}.
\end{aligned}$$

Since E has trivial rational torsion we have that $m_o = 1$. Then observing that $5 = \wp^5$ in K_1, the Heegner point z_1 reduces to $(4, 1) \in E(\mathbb{F}_5)$, and $3z_1 = \mathrm{O} \in E(\mathbb{F}_5)$, we set $m = 3$.

Using Algorithm 5.1 we find that

$$\begin{aligned}
d(z_1) = {} & \frac{170066107}{18679674112}b^9 - \frac{46616573}{1698152192}b^8_3 - \frac{3760482603}{18679674112}b^7 + \frac{11188479427}{18679674112}b^6 + \frac{263947335}{106134512}b^5 \\
& - \frac{40187214425}{4669918528}b^4 - \frac{1074830385}{424538048}b^3 + \frac{67626028101}{4669918528}b^2 + \frac{15616668599}{583739816}b - \frac{738093651}{26533628}.
\end{aligned}$$

Recall that $\wp$ denotes the unique prime of K_1 above $p = 5$. Observe that since E is defined over $\mathbb{Q}$ we have that $\sigma_\wp(t) = \sigma_5(t) \in \mathbb{Z}_5[[t]]$. We now compute the 5-adic sigma function

$$\begin{aligned}
\sigma_5(t) = {} & t + O(5^9)t^2 + \left(1 + 2\cdot 5 + 2\cdot 5^3 + 4\cdot 5^5 + 4\cdot 5^6 + O(5^8)\right)t^3 \\
& + \left(3 + 2\cdot 5 + 2\cdot 5^2 + 2\cdot 5^3 + 2\cdot 5^4 + 2\cdot 5^5 + 2\cdot 5^6 + O(5^7)\right)t^4 \\
& + \left(1 + 4\cdot 5 + 3\cdot 5^3 + 4\cdot 5^4 + O(5^6)\right)t^5 + \left(1 + 3\cdot 5 + 3\cdot 5^3 + O(5^5)\right)t^6 \\
& + \left(5^2 + 5^3 + O(5^4)\right)t^7 + \left(3 + 4\cdot 5 + 3\cdot 5^2 + O(5^3)\right)t^8 \\
& + \left(2 + 2\cdot 5 + O(5^2)\right)t^9 + (1 + O(5))t^{10} + O(t^{11}).
\end{aligned}$$

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

[4] 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.

Finally substituting the appropriate parameters into (5.3), we find that

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

Example 5.6. Let $E/\mathbb{Q}$ be the rank 1 elliptic curve "331a1", $p = 7$ and $K = \mathbb{Q}(\sqrt{-2})$. Note that E/K has analytic rank 1 and the three conditions listed at the beginning of Section 3 hold. In addition, p is inert in K and since $a_p = 2$, it does not divide $(a_p - 1)a_p(a_p + 1)$.

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 this is an example where we are interested in computing the coefficients of the Heegner L-function (see §9).

We will now use Algorithm 4.1 to construct the Heegner point z_1. We fix $b_0 = 68 \in \mathcal{S}(7^4\cdot(-8), 331)$. Since $h_K = 1$ and 7 is inert, we create a list of 8 equivalence classes of binary quadratic forms of order prime to 7 which satisfy conditions $(i) - (iv)$ of Section 4:

$$\begin{aligned}
f_1 &= 2979x^2 + 68xy + 2y^2 && \operatorname{ord}(f_1) = 2\\
f_2 &= 5958x^2 + 68xy + y^2 && \operatorname{ord}(f_2) = 1\\
f_3 &= 6289x^2 + 10660xy + 4518y^2 && \operatorname{ord}(f_3) = 8\\
f_4 &= 10923x^2 + 4040xy + 374y^2 && \operatorname{ord}(f_4) = 8\\
f_5 &= 12578x^2 + 10660xy + 2259y^2 && \operatorname{ord}(f_5) = 8\\
f_6 &= 16881x^2 + 29858xy + 13203y^2 && \operatorname{ord}(f_6) = 4\\
f_7 &= 21846x^2 + 4040xy + 187y^2 && \operatorname{ord}(f_7) = 8\\
f_8 &= 33762x^2 + 63620xy + 29971y^2 && \operatorname{ord}(f_8) = 4.
\end{aligned}$$

Then we compute

$$z_1 = \sum_{i=1}^{8} \pi(\tau_{f_i}) \in E(\mathbb{C}).$$

Numerically, we have that

$$z_1 \approx (0.953040743753736 + 0.149314525423730i, -1.03916093218186 + 0.166961454708477i).$$

Using LLL, we find that the best degree 7 relation satisfied by the x-coordinate of the numerical approximation to z_1 above is

$$\begin{aligned}
&137055595508378273856728767063301336043556x^7 + 596400144777929555460022572186960841860053x^6\\
&\quad + 181041765205432082772264681463297368999472x^5 - 859384933267625997711231611069953797275733 8x^4\\
&\quad + 280931546183003262594245381813315518200302 48x^3 - 773192961869776591438864657956859072964314 11x^2\\
&\quad + 901603400258671589506535272544761774836365 56x - 353141264137808224097694143114714576906094 76
\end{aligned}$$

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 last step of the Algorithm 4.1. The point z_1 is defined over $K_1 := \mathbb{Q}(b)$, where b is a root of

$$x^{14} - 56x^{12} + 966x^{10} - 1792x^8 - 95991x^6 + 1237992x^4 - 6135808x^2 + 10913792.$$

Observe that K_1 has class number 1 and hence we can use Algorithm 5.3 to compute the 7-adic height of z_1. Explicitly, we will compute with z_1 with coordinates

$$\begin{aligned}
x(z_1) = &-\frac{585169739109656630423116726878937703033376348863}{87920483845715129869232222013359063892185847283481600}b^{13} + \frac{235944118649039767015886638499977176691454333891}{43960241922857564934616111006679531946092923641740800}b^{12}\\
&+\frac{400686531670094881623316357193054286071124341829}{10990060480714391233654027751669882986523230910435200}b^{11} - \frac{91204401538345262050725214018446895621736620703}{5495030240357195616827013875834941493261615455217600}b^{10}\\
&-\frac{24772371213377713816512426467657514751630267769957}{43960241922857564934616111006679531946092923641740800}b^{9} - \frac{3005611673686799446861940560611227284439359085951}{21980120961428782467308055503339765973046461820870400}b^{8}\\
&-\frac{6407396515475987120351584608121532635987273587887}{5495030240357195616827013875834941493261615455217600}b^{7} + \frac{4610824733492073145986026393190681654410877230121}{686878780044649452103376734479367686657701931902200}b^{6}\\
&+\frac{7055542259485711973296737972449284714417477891852569}{87920483845715129869232222013359063892185847283481600}b^{5} - \frac{134513241817604087303676280501157818044550476069333}{43960241922857564934616111006679531946092923641740800}b^{4}\\
&-\frac{6290375521847452476451572056404509401638942807073481}{10990060480714391233654027751669882986523230910435200}b^{3} - \frac{1253354489099549885261242667031145632503897919685483}{5495030240357195616827013875834941493261615455217600}b^{2}\\
&+\frac{12898688284496392643622955437049580463984459736827}{9409298356776019891827078554511886118598656601400}b + \frac{8584327322466104945098370055799830401314498062761}{4704649178388009945913539277255943059299328300700}
\end{aligned}$$

$$\begin{aligned}
y(z_1) = &\frac{7149240844372912483938159051891878651775483023015679836677135461999}{13019624121345682534455491748165756363619865269444686720780432020831498240}b^{13}\\
&-\frac{2637021771882752446090507220840916008541593100088257534363589107865}{650981206067284126722774587408287818180993263472234336039021601041574912}b^{12}\\
&-\frac{58589282362281570798187060093143715016683352884349163227457047711239}{1627453015168210316806936468520719545452483158680585840097554002603937280}b^{11}\\
&+\frac{73154294220457714531111990593570240459277124175077046301857498715599}{406863253792052579201734117130179886363120789670146460024388500650984320}b^{10}\\
&+\frac{4869573468555592909958040089761857791336194183672390732953082620976957}{6509812060672841267227745874082878181809932634722343360390216010415749120}b^{9}\\
&-\frac{2395388512240055512437015744236102125312469308463822191846600386638727}{1627453015168210316806936468520719545452483158680585840097554002603937280}b^{8}\\
&-\frac{440738748559383365594514004954449400051488941835062892621659869740107}{203431626896026289600867058565089943181560394835073230012194250325492160}b^{7}\\
&-\frac{5413171345929286878786006625519233101948398795064381379479016614400907}{203431626896026289600867058565089943181560394835073230012194250325492160}b^{6}\\
&-\frac{1196750459273142727789550898022320061263702333906685370935138543012085689}{13019624121345682534455491748165756363619865269444686720780432020831498240}b^{5}\\
&+\frac{912927598070131077113220186681974976164849223524929023726848851184164059}{3254906030336420633613872937041439090904966317361171680195108005207874560}b^{4}\\
&+\frac{1437803753416794010893664925160466136102772137128473726021695979340870361}{1627453015168210316806936468520719545452483158680585840097554002603937280}b^{3}\\
&-\frac{353849008197962603519548324871335153229078310277076633751840267504188331}{406863253792052579201734117130179886363120789670146460024388500650984320}b^{2}\\
&-\frac{3556549292151123075940905696038241322258449445028025199169255755658683}{1393367307507029380827856565514314679325756129007350890494481166612960}b\\
&+\frac{77435799891243719155843270351204420477372727673885031488292679378249}{348341826876757345206964141378578669831439032251837722623620291653240}.
\end{aligned}$$

Note that the computation up to this step takes about 140 seconds on a 2.6Ghz Intel Xeon processor.

Since E has trivial rational torsion we have $m_o = 1$. Then observing that $7 = \wp^7$ in K_1, the Heegner point z_1 reduces to $(0, 2) \in E(\mathbb{F}_7)$, and $3z_1 = \mathrm{O} \in E(\mathbb{F}_7)$, we set $m = 3$.

Using Algorithm 5.1 we find that

$$\begin{aligned}
d(z_1) = &\frac{9320095137052778705014609}{10263920537600}b^{13} - \frac{8115282909632063749363823}{2565980134400}b^{12} - \frac{54100029800785550836577397}{1282990067200}b^{11}\\
&+\frac{54493855110163287593544319}{320747516800}b^{10} + \frac{1264824388774232318857578451}{5131960268800}b^{9} - \frac{1341364742431056265444970077}{1282990067200}b^{8}\\
&+\frac{826738116288954612024672783}{320747516800}b^{7} - \frac{396706442190566940868021183}{40093439600}b^{6} - \frac{548677508767077141885985952167}{10263920537600}b^{5}\\
&+\frac{555332843510658557093059967609}{2565980134400}b^{4} + \frac{403285222795351699117822466383}{1282990067200}b^{3} - \frac{414485789897487899507789710641}{320747516800}b^{2}\\
&-\frac{49354594932569887428687049753}{80186879200}b + \frac{700586184718030225484617527}{274612600}.
\end{aligned}$$

Recall that $\wp$ denotes the unique prime of K_1 above $p = 7$. Since E is defined over $\mathbb{Q}$ we have that $\sigma_\wp(t) = \sigma_7(t) \in \mathbb{Z}_7[[t]]$. We now compute the 7-adic sigma function

$$\begin{aligned}\sigma_7(t) = t &+ \left(4 + 3\cdot 7 + 3\cdot 7^2 + 3\cdot 7^3 + 3\cdot 7^4 + 3\cdot 7^5 + 3\cdot 7^6 + 3\cdot 7^7 + 3\cdot 7^8 + O(7^9)\right) t^2 \\ &+ \left(3 + 6\cdot 7 + 2\cdot 7^2 + 5\cdot 7^4 + 3\cdot 7^5 + 4\cdot 7^6 + 3\cdot 7^7 + O(7^8)\right) t^3 \\ &+ \left(6 + 6\cdot 7^2 + 5\cdot 7^3 + 5\cdot 7^4 + 3\cdot 7^5 + 7^6 + O(7^7)\right) t^4 + \left(2 + 2\cdot 7 + 7^2 + 7^3 + 5\cdot 7^4 + 6\cdot 7^5 + O(7^6)\right) t^5 \\ &+ \left(5 + 3\cdot 7 + 6\cdot 7^2 + 7^3 + O(7^5)\right) t^6 + \left(3 + 6\cdot 7 + 3\cdot 7^2 + O(7^4)\right) t^7 + \left(4 + 2\cdot 7^2 + O(7^3)\right) t^8 \\ &+ \left(6 + 7 + O(7^2)\right) t^9 + (2 + O(7))\, t^{10} + O(t^{11}).\end{aligned}$$

Finally, substituting the appropriate parameters into (5.3) we find that

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

6. Computation of p-adic heights: general case

6.1. **Algorithms.** We will now describe an algorithm to compute the p-adic height of a non-torsion point $P \in E(F)$, where F is a number field. We will assume, only for notational clarity, that $F/\mathbb{Q}$ is a Galois extension but we impose no restrictions on the class number of F .

If P reduces to a non-singular point at all primes of bad reduction and m is an integer such that mP reduces to the identity in $E(k_\wp)$ for all primes $\wp \mid p$, then we can use the formula (5.1) to compute the p-adic height of mP as follows:

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

By Proposition 1 of [19], since P reduces to a non-singular point at all primes of bad reduction, we know that

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

Hence we have

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

where $\mathcal{D}(P) := \prod_{v\nmid p}(\#k_v)^{\mathrm{ord}_v(d_v(P))}$ can be computed by the following algorithm.

Algorithm 6.1 ($\mathcal{D}(P)$ for $P \in E(F)$)**.**

(1) Let $D \in \mathbb{Z}$ be an integer denominator of $x(P)$. Then factor D into rational primes: $D = p^{r_0}\ell_1^{r_1}\cdots{\ell_k}^{r_k}$ where the primes ℓ_i are all distinct from p.

(2) For each ℓ_i above, factor $\ell_i\mathcal{O}_F = \prod_{j=1}^{f_i}\lambda_{i,j}^{s_i}$. Observe that since $F/\mathbb{Q}$ is Galois the exponent s_i depends only on i.

(3) For each $\lambda_{i,j}$, we compute $v_{\lambda_{i,j}}(D \cdot x(P))$. If $r_i s_i > v_{\lambda_{i,j}}(D \cdot x(P))$, then we know that $r_i s_i - v_{\lambda_{i,j}}(D \cdot x(P))$ must be even. We set

$$m_{i,j} = \begin{cases} \frac{r_i s_i - v_{\lambda_{i,j}}(D\cdot x(P))}{2} & \text{if } r_i s_i > v_{\lambda_{i,j}}(D \cdot x(P)), \\ 0 & \text{otherwise.} \end{cases}$$

Since $m_{i,j} = \operatorname{ord}_{\lambda_{i,j}} d_{\lambda_{i,j}}(P)$ and $\# k_{\lambda_{i,j}} = \ell_i^{[F:\mathbb{Q}]/(f_i \cdot s_i)}$, we compute

$$\mathcal{D}(P) = \prod_{i=1}^{k} \prod_{j=1}^{f_i} \ell_i^{m_{i,j} \cdot [F:\mathbb{Q}]/(f_i \cdot s_i)}.$$

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

Algorithm 6.2 (The p-adic height $h_{p,F}(P)$ of $P \in E(F)$)**.**

(1) Find the smallest positive integer m_o such that $m_o P$ reduces to a non-singular point at all primes of bad reduction.
(2) Find a positive integer m such that $m m_o P$ reduces to the identity in $E(k_\wp)$ for all primes $\wp \mid p$.
(3) Compute $m_o P$ and $m m_o P$.
(4) Compute $\mathcal{D}(m_o P)$ as in Algorithm 6.1.
(5) Compute $\sigma_\wp(t)$ for each $\wp \mid p$.
(6) Let $t_{m m_o} = -\frac{x(m m_o P)}{y(m m_o P)}$. Evaluate $\sigma_\wp(t_{m m_o}) \in F_\wp$ for each $\wp \mid p$.
(7) Compute $h_{p,F}(m m_o P)$ as follows:

$$h_{p,F}(P) = \frac{1}{m^2 m_o^2 p} \cdot \left(\log_p \prod_{\wp \mid p} \left(N_{F_\wp/\mathbb{Q}_p}\left(\sigma_\wp(t_{m m_o})\right) / N_{F_\wp/\mathbb{Q}_p}\left(f_m(m_o P)\right) \right) - m^2 \log_p\left(\mathcal{D}(m_o P)\right) \right).$$

6.2. **Examples.** We now give examples to illustrate the algorithms of this section.

Example 6.3. Let E be the elliptic curve "57a1", $p = 5$, and $K = \mathbb{Q}(\sqrt{-14})$. Note that K has class number $h_K = 4$, that E/K has analytic rank 1 and the three conditions listed at the beginning of Section 3 hold. Moreover, the prime $p = 5$ splits in $K/\mathbb{Q}$ and it does not divide $(a_p - 1)a_p$ since $a_p = -3$. We compute the Heegner point $z_0 \in E(K)$ and its 5-adic height:

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

Using Algorithm 4.1, we find that Heegner point z_1 has the following numerical coordinates:

$$(0.649281815494878 + 0.730235331103786i, -1.54792819990164 + 0.894427675896415i)$$

and $x(z_1)$ has minimal polynomial

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

Making this polynomial monic and taking the compositum with $K = \mathbb{Q}(\sqrt{-14})$ yields

$$\begin{aligned} x(z_1) = {} & \frac{16282333}{1992135746048}b^9 - \frac{122237657}{3984271492096}b^8 - \frac{314403157}{498033936512}b^7 + \frac{4752477831}{1992135746048}b^6 + \frac{54694163}{4446731576}b^5 \\ & - \frac{46894130863}{996067873024}b^4 + \frac{22141536649}{124508484128}b^3 - \frac{47631155337}{71147705216}b^2 - \frac{7805940803}{17786926304}b + \frac{256310331}{79405921} \\ y(z_1) = {} & \frac{891443463539}{52321453234204672}b^9 - \frac{162265125943}{6540181654275584}b^8 - \frac{34181434543565}{261607266171023336}b^7 + \frac{6275525342097}{3270090827137792}b^6 + \frac{46754847864491}{1868623329793024}b^5 \\ & - \frac{61952459298857}{1635045413568896}b^4 + \frac{2470785238769109}{6540181654275584}b^3 - \frac{59992556017783}{116788958112064}b^2 - \frac{54005898107995}{58394479056032}b + \frac{212461799073}{260689638643}, \end{aligned}$$

as elements of

$$K_1 = \mathbb{Q}[b]/(b^{10} - 80b^8 + 1720b^6 + 17600b^4 - 139760b^2 + 229376),$$

which has class number 20.

We will now use Algorithm 6.2 to compute the p-adic height of z_1. Since $E(\mathbb{Q})_{\mathrm{tors}}$ is trivial we have that $m_o = 1$. In order to determine m, we start by observing that $5 = \wp_1^5\wp_2^5$ in K_1 and hence $k_{\wp_i} = \mathbb{F}_5$. Then since z_1 reduces to $(2, 3) \in E(\mathbb{F}_5)$ which has order 9, we set $m = 9$. We then compute $9z_1 \in E(K_1)$.

In order to compute $\mathcal{D}(z_1)$ we begin by taking an integral denominator D of $x(z_1)$:

$$D = 79405921 = 7^2 \cdot 19^2 \cdot 67^2$$

The rational prime divisors of D factor in K_1 as follows:

$$\begin{aligned} \ell_1 = 7 = \prod_{j=1}^{5} \lambda_{1,j}^2 & \qquad\qquad f_1 = 5, s_1 = 2, \\ \ell_2 = 19 = \prod_{j=1}^{10} \lambda_{2,j} & \qquad\qquad f_2 = 10, s_2 = 1, \\ \ell_3 = 67 = \prod_{j=1}^{5} \lambda_{3,j} & \qquad\qquad f_3 = 5, s_3 = 1. \end{aligned}$$

We then compute

$$m_{i,j} = \begin{cases} 1 & \text{for } (i,j) = (1,1), (1,2), (3,1) \\ 4 & \text{for } (i,j) = (1,3) \\ 0 & \text{otherwise} \end{cases}$$

which gives

$$\mathcal{D}(z_1) = \prod_{i=1}^{k} \prod_{j=1}^{f_i} \ell_i^{m_{i,j} \cdot [F:\mathbb{Q}]/(f_i \cdot s_i)} = 7 \cdot 7 \cdot 7^4 \cdot 67^2 = 7^6 \cdot 67^2 = 528126361.$$

Recall that $\wp_1$ and $\wp_2$ denote the two primes of K_1 above $p = 5$. Let $K_{\wp_i}$ be the completion of K_1 at $\wp_i$. We now need to compute $\sigma_{\wp_1}(t)$ and $\sigma_{\wp_2}(t)$. Since E is defined over $\mathbb{Q}$ we have that

$$\sigma_{\wp_1}(t) = \sigma_{\wp_2}(t) = \sigma_5(t) \in \mathbb{Z}_5[[t]].$$

We now evaluate $\sigma_5(t_9) \in K_{\wp_1}$, $\sigma_5(t_9) \in K_{\wp_2}$, and find that

$$N_{K_{\wp_1}/\mathbb{Q}_5}(\sigma_5(t_9)) = N_{K_{\wp_2}/\mathbb{Q}_5}(\sigma_5(t_9)) = 1960712391 \cdot 5 + O(5^{15}).$$

We then compute

$$N_{K_{\wp_1}/\mathbb{Q}_5}(f_9(z_1)) = N_{K_{\wp_2}/\mathbb{Q}_5}(f_9(z_1)) = -1872036088 \cdot 5 + O(5^{15}).$$

Finally, putting this all together yields

$$\begin{aligned} h_{p,K_1}(z_1) &= \frac{1}{5 \cdot 9^2}(2\log_p(N_{K_{\wp_1}/\mathbb{Q}_5}(\sigma_5(t_9)) - 2\log_p(N_{K_{\wp_1}/\mathbb{Q}_5} f_9(z_1)) - 9^2 \log_p(\mathcal{D}(z_1))) \\ &= \frac{1}{5 \cdot 9^2}(2\log_p(1960712391 + O(5^{15})) - 2\log_p(-1872036088 \cdot 5 + O(5^{15})) - 9^2 \log_p(528126361)) \\ &= 3 + 2 \cdot 5 + 5^2 + 4 \cdot 5^5 + 2 \cdot 5^6 + O(5^7). \end{aligned}$$

Remark 6.4. Observe that $\mathcal{D}(z_1)$, the most difficult part of the height computation of z_1, is numerically equal to the leading coefficient of the minimal polynomial of $x(z_1)$. We will explore this connection in Section 7.

Example 6.5. We revisit Example 5.6: let E be "331a1", $p = 7$, and $K = \mathbb{Q}(\sqrt{-2})$. As the class number of K_1 equals 1, one can find a global choice of denominator and thus use formula (5.2) as was done earlier. For clarity, we also illustrate how one would compute with the "long" formula (5.1) following Algorithm 6.2.

We know that $m_o = 1$, $m = 3$, and we have already computed $mz_1 \in E(K_1)$. We now use Algorithm 6.1 to compute $\mathcal{D}(z_1)$. We find that $x(z_1)$ has an integer denominator

$$D = 87920483845715129869232222013359063892185847283481600,$$

which factors as

$$D = 2^{10} \cdot 5^2 \cdot 29 \cdot 73 \cdot 113 \cdot 419 \cdot 2647^2 \cdot 207079^2 \cdot 331141^2 \cdot 1019801^2.$$

The rational prime divisors of D factor in $\mathcal{O}_{K_1}$ as follows:

$$\begin{aligned}
\ell_1 &= 2 = \prod_{j=1}^{7} \lambda_{1,j}^2 && f_1 = 7, s_1 = 2,\\
\ell_2 &= 5 = \prod_{j=1}^{7} \lambda_{2,j} && f_2 = 7, s_2 = 1,\\
\ell_3 &= 29 = \prod_{j=1}^{7} \lambda_{3,j} && f_3 = 7, s_3 = 1,\\
\ell_5 &= 73 = \prod_{j=1}^{14} \lambda_{5,j} && f_5 = 14, s_5 = 1,\\
\ell_6 &= 113 = \prod_{j=1}^{14} \lambda_{6,j} && f_6 = 14, s_6 = 1,\\
\ell_7 &= 419 = \prod_{j=1}^{7} \lambda_{7,j} && f_7 = 7, s_7 = 1,\\
\ell_8 &= 2647 = \prod_{j=1}^{7} \lambda_{8,j} && f_8 = 7, s_8 = 1,\\
\ell_9 &= 207079 = \prod_{j=1}^{7} \lambda_{9,j} && f_9 = 7, s_9 = 1,\\
\ell_{10} &= 331141 = \prod_{j=1}^{7} \lambda_{10,j} && f_{10} = 7, s_{10} = 1,\\
\ell_{11} &= 1019801 = \prod_{j=1}^{14} \lambda_{11,j} && f_{11} = 14, s_{11} = 1.
\end{aligned}$$

We then compute

$$m_{i,j} = \begin{cases} 1 & \text{for } (i,j) = (8,1),(9,1),(10,1),(11,1),(11,2) \\ 2 & \text{for } (i,j) = (1,1) \\ 0 & \text{otherwise} \end{cases}$$

which gives

$$\begin{aligned} \mathcal{D}(z_1) &= \prod_{i=1}^{k} \prod_{j=1}^{f_i} \ell_i^{m_{i,j}\cdot[F:\mathbb{Q}]/(f_i\cdot s_i)} \\ &= 2^2 \cdot 2647^2 \cdot 207079^2 \cdot 331141^2 \cdot 1019801^2 = 1370555955083782738567287670633013360435 56, \end{aligned}$$

which is equal to the leading coefficient of the minimal polynomial of $x(z_1)$; see Example 5.6.

Recall that there is a unique prime $\wp$ of K_1 above $p = 7$ and $K_\wp$ denotes the completion of K_1 at $\wp$. We compute $\sigma_\wp(t) = \sigma_7(t)$ as before and evaluate $\sigma_7(t_3) \in K_\wp$. Then we have

$$\begin{aligned} N_{K_\wp/\mathbb{Q}_7}(\sigma(t_3)) &= 4\cdot 7^2 + 4\cdot 7^3 + 3\cdot 7^4 + 2\cdot 7^5 + 2\cdot 7^6 + 4\cdot 7^7 + 6\cdot 7^8 + 5\cdot 7^9 + O(7^{10}), \\ N_{K_\wp/\mathbb{Q}_7}(f_3(z_1)) &= 4\cdot 7^2 + 6\cdot 7^3 + 2\cdot 7^4 + 3\cdot 7^6 + 4\cdot 7^7 + 6\cdot 7^8 + 7^9 + O(7^{10}). \end{aligned}$$

Finally, we compute

$$\begin{aligned} h_{7,K_1}(z_1) &= \frac{1}{7\cdot 3^2}\left(\log_7\left(\frac{N_{K_\wp/\mathbb{Q}_7}(\sigma(t_3))}{N_{K_\wp/\mathbb{Q}_7}(f_3(z_1))}\right) - 3^2\log_7(\mathcal{D}(z_1))\right) \\ &= 4 + 3\cdot 7 + 3\cdot 7^2 + 7^3 + 6\cdot 7^4 + 2\cdot 7^5 + 4\cdot 7^6 + 2\cdot 7^7 + O(7^8). \end{aligned}$$

Remark 6.6. 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.

7. Improvements

We have previously observed that the leading coefficient of the minimal polynomial of $x(z_1)$ equals $\mathcal{D}(z_1)$. In this section we analyze the relation between $\mathcal{D}(P)$ and the leading coefficient of the minimal polynomial of $x(P)$ for a point $P \in E(F)$ where $F/\mathbb{Q}$ is a Galois extension. We then prove the observed equality in the case of Heegner points $z_n \in E(K_n)$ under the assumption that $E(\mathbb{Q})_{\text{tors}} = \text{O}$. We conclude the section by giving a few more algorithmic improvements to the computation of p-adic heights of Heegner points under the assumption that $E(\mathbb{Q})$ has trivial torsion.

We begin with a result that vastly simplifies the computation of a denominator of a point, allowing us to bypass factorization of ideals in $\mathcal{O}_F$. In view of the following proposition all that remains in the denominator computation is the evaluation of a division polynomial.

Proposition 7.1. *Let $F/\mathbb{Q}$ be a Galois extension, $P \in E(F)$, $b_n x^n + \cdots + b_0 = 0$ the minimal polynomial of $x(P)$ over $\mathbb{Z}$, and b a positive integer prime to p such that $b_n = p^m b$. Then $\mathcal{D}(P)^2 = b^{[F:\mathbb{Q}]/n}$.*

Proof. Since by definition b and $\mathcal{D}(P)$ are positive integers prime to p we will prove that $\mathcal{D}(P)^2 = b^{[F:\mathbb{Q}]/n}$ by analyzing the valuation of b and $\mathcal{D}(P)$ at every rational prime $\ell \neq p$.

The valuation of $\mathcal{D}(P)$ at primes ℓ which do not divide b is trivial since $\operatorname{res}_\lambda x(z_n)$ is then integral over $\mathbb{Z}_\ell$ for every prime $\lambda \subset F$ above ℓ.

We know that the norm $N_{F/\mathbb{Q}}(x(P)) = (b_n/b_0)^{[F:\mathbb{Q}]/n}$. Observe that $D = b_n$ is an integer denominator of $x(z_n)$. As before we consider the set of rational primes ℓ_i dividing b_n and distinct from the prime p, i.e. the set of rational prime divisors of b. Then as before we denote by $\lambda_{i,j}$ the primes of

F which divide ℓ_i. We know that $\mathrm{res}_{\lambda_{i,j}} x(P) = a_{i,j}/d_{i,j}^2$ where either $a_{i,j}$ or $d_{i,j}$ is a unit. Observe that $\mathcal{D}(P) = \prod_{i,j} N_{F_{\lambda_{i,j}}/\mathbb{Q}_{\ell_i}}(d_{i,j})$ where $F_{\lambda_{i,j}}$ is the localization of F at $\lambda_{i,j}$ and

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

where $r \in \mathbb{Z}$ and c is an integer with trivial valuation at the primes ℓ_i.

We start by assuming that ℓ_i does not divide $\gcd(b_n, b_0)$. Then if the valuation at λ_{i_0,j_0} of $x(P)$ is negative then the valuation at $\lambda_{i_0,j}$ of $x(P)$ is not positive for any j (since otherwise ℓ_{i_0} would divide b_0 when it already must divide b_n). Hence, since

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

if $\gcd(b_n, b_0)$ is prime to ℓ_i then $\mathrm{ord}_{\ell_i}(\mathcal{D}(P))^2 = \mathrm{ord}_{\ell_i}(b)^{[F:\mathbb{Q}]/n}$.

We will now consider the valuations of $\mathcal{D}(P)$ and b at primes which divide $\gcd(b_n, b_0)$ and $\mathcal{D}(P)$. Let ℓ_i be a rational prime factor of $\mathcal{D}(P)$ dividing $\gcd(b_n, b_0)$ and $\lambda_{i,1}$ a prime of F dividing ℓ_i. We know that

$$b_n^{-[F:\mathbb{Q}]/n}(b_n x^{p^n} + \cdots + b_0)^{[F:\mathbb{Q}]/n} = \prod_{\sigma \in \mathrm{Gal}(F/\mathbb{Q})} (x - \sigma(x(P))). \tag{7.1}$$

Set e_σ to be the valuation of $x(P)$ at $\sigma(\lambda_{i,1})$. Viewing the right hand side of the equation (7.1) 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 $b_n x^n + \cdots + b_0$ is trivial, the same holds for $(b_n x^n + \cdots + b_0)^{[F:\mathbb{Q}]/n}$. It then follows that the valuation at ℓ_i of $b^{-[F:\mathbb{Q}]/n}$ equals the sum of the negative e_σ.

Moreover, since $\mathrm{res}_{\lambda_{i,j}} x(P) = a_{i,j}/d_{i,j}^2$, the valuation at ℓ_i of $\mathcal{D}(P)^2$ also equals

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

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

Corollary 7.2. *Let $E/\mathbb{Q}$ be an elliptic curve with trivial rational torsion. Then the prime to p component of the leading coefficient of the minimal polynomial of $x(z_n)$ over the ring of integers $\mathbb{Z}$ equals $\mathcal{D}(z_n)$.*

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 $E(\mathbb{Q})_{\mathrm{tors}} = \mathrm{O}$ and the order of $\mathrm{Gal}(K_n/K)$ is odd, we know that there exist $\sigma \in \mathrm{Gal}(K_n/K)$ such that $(\sigma z_n)^\tau = -\epsilon(\sigma z_n)$; see the listed properties of Heegner points in Section 3. This implies that $x(z_n) \in K_n^{\langle\tau\rangle}$ Observe that $[K_n^{\langle\tau\rangle} : \mathbb{Q}] = p^n$ and $K_n^{\langle\tau\rangle} = \mathbb{Q}(x(\sigma(z_n)))$. Hence the degree of the minimal polynomial $x(z_n)$ over $\mathbb{Z}$ equals p^n. Then by Proposition 7.1 we have that

$$\mathcal{D}(z_n)^2 = b^{(2p^n)/p^n} = b^2$$

where b denotes the prime to p component of the leading coefficient of the minimal polynomial of $x(z_n)$ over the ring of integers $\mathbb{Z}$. Since $\mathcal{D}(z_n)$ and b are positive integers, we have that $\mathcal{D}(z_n) = b$. □

From the point of view of studying p-adic heights of Heegner points, we can further simplify our methods. Note that as an intermediate step, we take a Heegner point with complex coordinates, reconstruct the coordinates as elements of a number field, only to care about p-adic information at the end of the day. Indeed, since we construct the point and then input its restriction into a p-adic power series (the p-adic sigma function), using the two algorithms in tandem shows us that this step is not actually necessary: one can make do with the coordinates of the Heegner point as elements of an extension of $\mathbb{Q}_p$ and bypass the exact arithmetic. So given our setup, we can simplify the computation of p-adic heights by making the following observations.

We know that $x(\sigma z_n)$ is defined over a degree p^n extension of $\mathbb{Q}$ for some $\sigma \in \mathrm{Gal}(K_n/K)$. We assume that this holds for $\sigma = \mathrm{id}$ since otherwise we replace z_n by σz_n and compute its p-adic height which is equal to that of z_n. The computational difficulty in getting the $x(z_n)$ and $y(z_n)$ as elements of a number field lies in getting an "optimized" representation of the degree $2p^n$ extension of $\mathbb{Q}$.

If the Heegner point $z_n \in E(K_n)$ has both coordinates in a degree p^n subfield, then the computation is much simpler. (Note that this holds for some conjugate of z_n if the sign of the functional equation of $E/\mathbb{Q}$ equals -1 and E has trivial rational torsion.) Indeed, to compute the p-adic height of the Heegner point, we do not actually need to know the point (in particular, its y-coordinate) algebraically. We merely need to compute its y-coordinate to some p-adic approximation (which can be done cheaply with a Newton iteration), as the end goal is to input this into a power series with p-adic coefficients.

To summarize, in order to compute p-adic heights of Heegner points we use the following modified versions of Algorithm 6.2:

Algorithm 7.3 (The p-adic height $h_{p,K_n}(P)$ of a Heegner point $z_n \in E(K_n)$)**.** Assume that

a) $E(\mathbb{Q})_{\mathrm{tors}} = \mathrm{O}$, and
b) the analytic rank of $E/\mathbb{Q}$ equals 1.

It follows that $m_o = 1$.

(1) Compute $x(z_n) \in \mathbb{R}$ using Algorithm 4.1. (If the x-coordinate of the first z_n is not real then we use an element of $\mathrm{Gal}(K_n/K)$ to find a conjugate that is. This is the z_n that we want.) Save the leading coefficient $\mathcal{D}(z_n)$ of the minimal polynomial $h(x)$ of $x(z_n)$ over $\mathbb{Z}$.

(2) Set $L_n := K_n^{\langle\tau\rangle}$. We know that $z_n \in E(L_n)$ and L_n is totally ramified at p.

We p-adically construct $\mathrm{res}_{\mathfrak{p}_n} z_n \in E(L_{\mathfrak{p}_n})$ where $\mathfrak{p}_n$ is the unique prime of L_n above p and $L_{\mathfrak{p}_n}$ is the completion of L_n at $\mathfrak{p}_n$(the x-coordinate is trivial, and the y-coordinate is determined via Newton iteration). Observe 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.

(3) Compute m so that mz_n reduces to the identity in $E(k_\wp)$ at all primes $\wp$ of L_n above p (here $k_\wp$ denotes the residue field of L_n at $\wp$). Use it to compute $\mathrm{res}_{\mathfrak{p}_n}(mz_n) \in E(L_{\mathfrak{p}_n})$, $f_m(x(z_n)), t_m = -\frac{x(\mathrm{res}_{\mathfrak{p}_n}(mz_n))}{y(\mathrm{res}_{\mathfrak{p}_n}(mz_n))} \in L_{\mathfrak{p}_n}$.

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

Algorithm 7.4 (The p-adic height $h_{p,K_n}(z_n)$ of a Heegner point $z_n \in E(K_n)$)**.** Assume that

a) $E(\mathbb{Q})_{\mathrm{tors}} = \mathrm{O}$,
b) the analytic rank of $E/\mathbb{Q}$ equals 0, and
c) p splits in $K/\mathbb{Q}$.

It follows that $m_o = 1$.

(1) Compute $x(z_n) \in \mathbb{R}$ using Algorithm 4.1. (If the x-coordinate of the first z_n is not real then we use an element of $\mathrm{Gal}(K_n/K)$ to find a conjugate that is. This is the z_n that we want.) Save the leading coefficient $\mathcal{D}(z_n)$ of the minimal polynomial $h(x)$ of $x(z_n)$ over $\mathbb{Z}$.

(2) We know that $x(z_n) \in L_n$ and $L_n = K_n^{\langle\tau\rangle}$ is totally ramified at p. Let $\mathfrak{p}_n$ be the unique prime of L_n above p and $L_{\mathfrak{p}_n}$ the completion of L_n at $\mathfrak{p}_n$. Since p splits in $K/\mathbb{Q}$ we know that there are two primes $\wp_n$, $\wp_n'$ of K_n that divide $\mathfrak{p}_n$. Hence, $K_{\wp_n} = K_{\wp_n'} = L_{\mathfrak{p}_n}$ and $\operatorname{res}_{\wp_n} z_n, \operatorname{res}_{\wp_n'} z_n \in E(L_{\mathfrak{p}_n})$. Since $z_n^\tau = -z_n$ it follows that $\operatorname{res}_{\wp_n'} z_n = -\operatorname{res}_{\wp_n} z_n$.

We p-adically construct $\operatorname{res}_{\wp_n} z_n \in E(L_{\mathfrak{p}_n})$. Observe that while we need to choose the sign of the y-coordinate, this choice is irrelevant in the end since $\operatorname{res}_{\wp_n'} z_n = -\operatorname{res}_{\wp_n} z_n$ and the sigma function is odd.

(3) Compute m. Use it to compute $\operatorname{res}_{\wp_n}(mz_n) \in E(L_{\mathfrak{p}_n})$, $f_m(x(z_n)), t_m = -\frac{x(\operatorname{res}_{\wp_n}(mz_n))}{y(\operatorname{res}_{\wp_n}(mz_n))} \in L_{\mathfrak{p}_n}$.

(4) Recover

$$\begin{aligned} h_{p,K_n}(z_n) &= \frac{1}{p\cdot m^2}\left(\log_p\left(-N_{L_{\mathfrak{p}_n}/\mathbb{Q}_p}\left(\frac{\sigma_p(t_m)}{f_m(x(z_n))}\right)^2\right) - m^2\log_p(\mathcal{D}(z_n))\right) \\ &= \frac{1}{p\cdot m^2}\left(\log_p\left(N_{L_{\mathfrak{p}_n}/\mathbb{Q}_p}\left(\frac{\sigma_p(t_m)}{f_m(x(z_n))}\right)^2\right) - m^2\log_p(\mathcal{D}(z_n))\right). \end{aligned}$$

Algorithm 7.5 (The p-adic height $h_{p,K_n}(z_n)$ of a Heegner point $z_n \in E(K_n)$)**.** Assume that

a) $E(\mathbb{Q})_{\text{tors}} = \text{O}$,
b) the analytic rank of $E/\mathbb{Q}$ equals 0, and
c) p is inert in $K/\mathbb{Q}$.

It follows that $m_o = 1$.

(1) Compute $x(z_n) \in \mathbb{R}$ using Algorithm 4.1. (If the x-coordinate of the first z_n is not real then we use an element of $\operatorname{Gal}(K_n/K)$ to find a conjugate that is. This is the z_n that we want.) Save the leading coefficient $\mathcal{D}(z_n)$ of the minimal polynomial $h(x)$ of $x(z_n)$ over $\mathbb{Z}$.

(2) We know that $x(z_n) \in L_n$. As before $L_n = K_n^{\langle\tau\rangle}$ is totally ramified at p, $\mathfrak{p}_n$ is the unique prime of L_n above p, and $L_{\mathfrak{p}_n}$ the completion of L_n at $\mathfrak{p}_n$. Since p is inert in $K/\mathbb{Q}$ there is a unique prime $\wp_n$ of K_n above p and $K_{\wp_n} = L_{\mathfrak{p}_n}[\sqrt{D_K}]$.

We p-adically construct $\operatorname{res}_{\wp_n} z_n \in E(L_{\mathfrak{p}_n}[\sqrt{D_K}])$. Observe that while we need to choose the sign of the y-coordinate, this choice is irrelevant since the sigma function is odd.

(3) Compute m. Use it to compute $\operatorname{res}_{\wp_n}(mz_n) \in E(L_{\mathfrak{p}_n}[\sqrt{D_K}])$, $f_m(x(z_n)) \in L_{\mathfrak{p}_n}$, and $t_m = -\frac{x(\operatorname{res}_{\wp_n}(mz_n))}{y(\operatorname{res}_{\wp_n}(mz_n))} \in L_{\mathfrak{p}_n}[\sqrt{D_K}]$.

(4) Recover

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

8. Computing p-adic height pairings of Heegner points

In this section, we give an algorithm to compute the p-adic height pairing $\langle z_n, \sigma z_n\rangle_{K_n}$ for $\sigma \in \operatorname{Gal}(K_n/K)$ and then illustrate it in an example. Recall that ϵ denotes the sign of the functional equation of $E/\mathbb{Q}$. Then since $h_{p,K_n}(\sigma z_n) = h_{p,K_n}(z_n)$ for every $\sigma \in \operatorname{Gal}(K_n/K)$, we have that

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

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

We will assume that E has trivial rational torsion which implies that there exist a Heegner point $z_n \in K_n$ such that $z_n^\tau = -\epsilon z_n$. It then follows that

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

and hence $(\sigma z_n - \epsilon\sigma^{-1}z_n) \in E(L_n)$ for every $\sigma \in \mathrm{Gal}(K_n/K)$, where $L_n = K_n^{\langle\tau\rangle}$. This allows us to use Algorithm 7.3 (simply replacing z_n by $(\sigma z_n - \epsilon\sigma^{-1}z_n)$) in order to compute the height of $(\sigma z_n - \epsilon\sigma^{-1}z_n)$ even if the analytic rank of E is not assumed to be 1. 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 we have $m_o = 1$ in its p-adic height computation.

Algorithm 8.1 (The pairings $\langle z_n, \sigma z_n\rangle$ for all $\sigma \in \mathrm{Gal}(K_n/K)$)**.**

Assume that $E(\mathbb{Q})_{\mathrm{tors}} = \mathrm{O}$ and $z_n^\tau = -\epsilon z_n$.

(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 §7 to compute $h_{p,K_n}(z_n)$.

(2) Use Algorithm 4.2 to compute of the conjugates of z_n as points in $E(\mathbb{C})$. This fixes an ordering of the conjugates of z_n.

(3) Shift the p^n-tuple of the conjugates of z_n so that it starts with z_n by checking that the x-coordinate of the first entry of this p^n-tuple is real. We then have
$$(z_n, \sigma_0 z_n, \ldots, \sigma_0^{p^n-1}z_n) \in E(\mathbb{C})^{p^n}$$
where $\sigma_0 \in \mathrm{Gal}(K_n/K)$ is an element of order p^n that is now fixed.

(4) We can then compute $\sigma_0^j z_n - \epsilon\sigma_0^{p^n-j}z_n \in E(\mathbb{C})$ for any $j \in \{1, \ldots, (p^n-1)/2\}$.

(5) Since we know that $\sigma_0^j z_n - \epsilon\sigma_0^{-j}z_n \in E(L_n)$ we use Algorithm 7.3 to compute $h_{p,K_n}(\sigma_0^j z_n - \epsilon\sigma_0^{-j}z_n)$.

(6) This gives
$$\langle\sigma_0^j z_n, \sigma_0^{-j}z_n\rangle_{K_n} = h_{p,K_n}(\sigma_0^j z_n - \epsilon\sigma_0^{-j}z_n) - 2h_{p,K_n}(z_n).$$

(7) 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 8.2. Let $E/\mathbb{Q}$ be the rank 1 elliptic curve "57a1", $p = 5$, and $K = \mathbb{Q}(\sqrt{-2})$, as in Example 5.5. Let $z_1 \in E(K_1)$ denote the Heegner point that is fixed by complex conjuagtion τ (since in this case $\epsilon = -1$). Hence $z_1 \in E(L_1)$. We will now use the above algorithm to compute $\langle z_1, \sigma z_1\rangle_{K_1}$ for all $\sigma \in \mathrm{Gal}(K_1/K)$.

We have already computed the 5-adic height of z_1:
$$h_{5,K_1}(z_1) = 2 + 2\cdot 5 + 2\cdot 5^2 + 5^4 + 4\cdot 5^5 + 4\cdot 5^6 + 3\cdot 5^7 + O(5^8).$$

We now compute the 5-tuple of the conjugates of z_1 as points in $E(\mathbb{C})$ and ensure that our 5-tuple starts with z_n. So we have
$$(z_n, \sigma z_n, \sigma^2 z_n, \sigma^3 z_n, \sigma^4 z_n) \in E(\mathbb{C})^5$$
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 7.3 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

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

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

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

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

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

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

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

To finish the computation, we note that

$$\begin{aligned} \langle z_1, z_1\rangle_{K_1} &= 2h_{5,K_1}(z_1) \\ \langle z_1, \sigma z_1\rangle_{K_1} &= \langle \sigma^2 z_1, \sigma^3 z_1\rangle_{K_1} \\ &= h_{5,K_1}(\sigma^2 z_1 + \sigma^3 z_1) - 2h_{5,K_1}(z_1) \\ &= 1 + 3\cdot 5^3 + 5^4 + 4\cdot 5^5 + 3\cdot 5^6 + 4\cdot 5^7 + 2\cdot 5^8 + 4\cdot 5^9 + O(5^{10}) \\ \langle z_1, \sigma^2 z_1\rangle_{K_1} &= \langle z_1, \sigma^3 z_1\rangle_{K_1} \\ \langle z_1, \sigma^3 z_1\rangle_{K_1} &= \langle \sigma z_1, \sigma^4 z_1\rangle_{K_1} \\ &= h_{5,K_1}(\sigma^4 z_1 + \sigma z_1) - 2h_{5,K_1}(z_1) \\ &= 2 + 5 + 5^2 + 5^3 + 4\cdot 5^4 + 5^5 + 5^7 + 2\cdot 5^8 + 2\cdot 5^9 + O(5^{10}) \\ \langle z_1, \sigma^4 z_1\rangle_{K_1} &= \langle z_1, \sigma z_1\rangle_{K_1}. \end{aligned}$$

Note that as a numerical check, we can compute the sum of these pairings to obtain the following $\langle z_1, z_1\rangle_{K_1} + \langle z_1, \sigma z_1\rangle_{K_1} + \cdots + \langle z_1, \sigma^4 z_1\rangle_{K_1} = 4 + 3\cdot 5 + 2\cdot 5^2 + 2\cdot 5^5 + 4\cdot 5^6 + 2\cdot 5^7 + 5^8 + 2\cdot 5^9 + O(5^{10})$. Then using (3.2) gives us that

$$\mathrm{tr}_{K_1/K}(z_1) = 3z_0,$$

and since $z_0 \in E(\mathbb{Q})$, Sage tells us that

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

This lets us see, numerically, that

$$\begin{aligned} \langle \mathrm{tr}_{K_1/K}(z_1), \mathrm{tr}_{K_1/K}(z_1)\rangle_{K_1} &= 5\langle z_1, \mathrm{tr}_{K_1/K}(z_1)\rangle_{K_1} \\ &= 3\cdot 5^2 + 2\cdot 5^3 + 4\cdot 5^4 + 3\cdot 5^5 + 3\cdot 5^7 + 4\cdot 5^8 + 4\cdot 5^9 + O(5^{10}) \\ &= [K_1 : \mathbb{Q}]\langle 3z_0, 3z_0\rangle_{\mathbb{Q}}, \end{aligned}$$

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

9. Λ-adic regulators

In this section we compute coefficients of Λ-adic regulators of several elliptic curves $E/\mathbb{Q}$. In all these examples we have that c_0 is not divisible by p in $E(K)$ and the valuation of $\langle c_0, c_0\rangle_{K_0}$ 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 Section 3 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 $c_2 = (u_0 u_1)^{-1} z_2$. Observe that since $\langle c_n, \sigma^i c_n\rangle = \langle c_n \sigma^{p^n - i} c_n\rangle$, we have

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

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.

Example 9.1. Let $E/\mathbb{Q}$ be the rank 1 elliptic curve "57a1", $p = 5$, and $K = \mathbb{Q}(\sqrt{-2})$, as in Examples 5.5 and 8.2. Using the computation of $h_{5,K}(z_0)$ in Example 5.5, we compute

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

In Example 8.2, we computed

$$\begin{aligned}\langle z_1, \sigma z_1\rangle_{K_1} &\equiv 1 \pmod 5\\ \langle z_1, \sigma^2 z_1\rangle_{K_1} &\equiv 2 \pmod 5.\end{aligned}$$

Since $u_0 = 3$ we see that

$$\begin{aligned}\mathsf{b}_2 &\equiv u_0^{-2}(\langle z_1, \sigma z_1\rangle_{K_1} + 4\langle z_1, \sigma^2 z_1\rangle_{K_1}) \pmod 5\\ &\equiv 1 \pmod 5.\end{aligned}$$

Since b_2 is a unit while b_0 and b_1 are not, it follows that the Heegner L-function $\mathcal{L}$ and hence $\mathcal{R}$ equal the product of a unit and a distinguished polynomial of degree 2 in $\mathbb{Z}_5[[T]]$.

Example 9.2. Let $E/\mathbb{Q}$ be the rank 1 elliptic curve "57a1", $p = 5$, and $K = \mathbb{Q}(\sqrt{-14})$, as in Example 6.3. We have

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

Moreover, $u_0 = 11$ and we see that

$$\begin{aligned}\mathsf{b}_2 &\equiv u_0^{-2}(\langle z_1, \sigma z_1\rangle_{K_1} + 4\langle z_1, \sigma^2 z_1\rangle_{K_1}) \pmod 5\\ &\equiv 3 \pmod 5.\end{aligned}$$

This implies that $\mathcal{R}$ is the product of a unit and a distinguished polynomial of degree 2 in $\mathbb{Z}_5[[T]]$.

Example 9.3. Let $E/\mathbb{Q}$ be the rank 1 elliptic curve "331a1", $p = 7$, and $K = \mathbb{Q}(\sqrt{-2})$. We compute

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

For $\sigma \in \mathrm{Gal}(K_1/K)$ the element of order p fixed in Step 3 of Algorithm 8.1 we then find

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

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

$$\begin{aligned} \mathsf{b}_2 &\equiv u_0^{-2}(\langle z_1, \sigma z_1 \rangle_{K_1} + 4\langle z_1, \sigma^2 z_1 \rangle_{K_1} + 2\langle z_1, \sigma^3 z_1 \rangle_{K_1}) \pmod 7 \\ &\equiv 1 \pmod 7. \end{aligned}$$

Hence, 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 9.4. 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

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

Then for $\sigma \in \mathrm{Gal}(K_1/K)$ the element of order p fixed in Step 3 of Algorithm 8.1 we compute

$$\begin{aligned} \langle z_1, z_1 \rangle_{K_1} &= 1 + 3^3 + 3^4 + 2 \cdot 3^5 + 2 \cdot 3^6 + 2 \cdot 3^7 + O(3^8) \\ \langle z_1, \sigma z_1 \rangle_{K_1} &= 1 + 3 + 2 \cdot 3^2 + 3^3 + 3^5 + 3^6 + 3^7 + O(3^8) \\ \langle z_1, \sigma^2 z_1 \rangle_{K_1} &= \langle z_1, \sigma z_1 \rangle_{K_1}. \end{aligned}$$

Note that this gives $\mathsf{b}_2 \equiv u_0^{-2} \langle z_1, \sigma z_1 \rangle_{K_1} \equiv 1 \pmod 3$.

In this example $\mathcal{R}$ 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 9.5. Let $E/\mathbb{Q}$ be the rank 1 elliptic curve "185b1", $p = 3$, and $K = \mathbb{Q}(\sqrt{-11})$. First, we have

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

For $\sigma \in \mathrm{Gal}(K_1/K)$ the element of order p fixed in Step 3 of Algorithm 8.1 we have:

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

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 3 of Algorithm 8.1 we have:

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

Consequently, we find that

$$\begin{aligned}
\langle c_2, \sigma c_2\rangle_{K_2} &\equiv 2 \pmod 9\\
\langle c_2, \sigma^2 c_2\rangle_{K_2} &\equiv 1 \pmod 9\\
\langle c_2, \sigma^3 c_2\rangle_{K_2} &\equiv 2 \pmod 9\\
\langle c_2, \sigma^4 c_2\rangle_{K_2} &\equiv 6 \pmod 9,
\end{aligned}$$

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

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

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

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

Hence $\mathcal{R}$ is the product of a unit and a distinguished polynomial of degree 4 in $\mathbb{Z}_3[[T]]$.

Example 9.6. Let $E/\mathbb{Q}$ be the rank 1 elliptic curve "325b1", $p = 3$, and $K = \mathbb{Q}(\sqrt{-14})$. First, we have

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

For $\sigma \in \mathrm{Gal}(K_1/K)$ the element of order p fixed in Step 3 of Algorithm 8.1:

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

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 3 of Algorithm 8.1 we have:

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

Consequently, we find that

$$\begin{aligned}
\langle c_2, \sigma c_2\rangle_{K_2} &\equiv 5 \pmod 9\\
\langle c_2, \sigma^2 c_2\rangle_{K_2} &\equiv 2 \pmod 9\\
\langle c_2, \sigma^3 c_2\rangle_{K_2} &\equiv 7 \pmod 9\\
\langle c_2, \sigma^4 c_2\rangle_{K_2} &\equiv 8 \pmod 9,
\end{aligned}$$

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 compute $\mathsf{b}_4 \pmod 9$:

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

Then we find that

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

and finally

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

Hence, 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

Table 9.1. Elliptic Curves

Label	**Equation**
57a1	$y^2 + y = x^3 - x^2 - 2x + 2$
158b1	$y^2 + xy = x^3 + x^2 - 3x + 1$
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] H. Cohen, *A course in computational algebraic number theory*, Springer-Verlag, Berlin, 1993.

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

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

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

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

[7] 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.

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

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

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

[11] 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.

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

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

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

[15] W. A. Stein et al., *Sage Mathematics Software (Version 4.8)*, The Sage Development Team, 2012, `http://www.sagemath.org`.

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

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

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

[19] 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/`