Abstract. We describe a new quadratic Chabauty algorithm to compute integral points on rank 1 elliptic curves $E$. This algorithm replaces the requirement for an infinite order point of $E$ with computations of special values of $p$-adic $L$-functions. In particular, we describe a method for computing the anticyclotomic $p$-adic $L$-function introduced by Bertolini, Darmon, and Prasanna at its special value. This requires evaluating the $p$-adic $L$-function outside the range of interpolation. To achieve this, we follow a method of Rubin previously used to evaluate the Katz 2-variable $p$-adic $L$-function outside the range of interpolation.

1. Introduction

Let $X$ be a smooth projective geometrically integral curve of genus $g > 1$ over a number field $K$. Faltings’s theorem [Fal83] states that the set $X(K)$ of $K$-rational points of $X$ is finite. However, there is no general method for determining this set explicitly.

When the Mordell–Weil rank of the Jacobian $J$ of $X$ is less than $g$, the Chabauty–Coleman method [MP12, Col85] describes a finite set of $p$-adic points containing $X(K)$. In particular, when $K = \mathbb{Q}$, this has yielded a practical computational approach to computing $X(\mathbb{Q})$ [BBK10, BT20, BBCF+, dFFH19, HM20].

The recent successes of the quadratic Chabauty method [BD18a, BD18b, BDM+19, BDM+21] in determining rational points on modular curves showcase the potential of this algorithm. For example, this technique can be used when the Mordell–Weil rank of $J$ is equal to $g$ and the Néron–Severi rank of $J$ is greater than 1 allowing for a much wider range of applications such as quotients of modular curves. Quadratic Chabauty realizes M. Kim’s program [Kim09] for an explicit Faltings’s theorem via quotients of the unipotent fundamental group at depth 2.

Crucially, to determine $X(\mathbb{Q})$, quadratic Chabauty requires as input a supply of rational points on $X$. Since higher genus curves often do not have many rational points, many interesting cases are not accessible. Several techniques have been developed to reduce the number of rational points needed [BM, Section 5.3.2] [BDM+21, Section 3.3].

Our overall goal is to describe a quadratic Chabauty algorithm for certain modular curves where we replace the requirement for sufficiently many rational points on $X$ with computations of $p$-adic $L$-function values.

In this article we study the case of determining integral points on a rank 1 genus 1 (elliptic) curve $E$. The higher genus case will be discussed in the author’s forthcoming PhD thesis. A consequence of Faltings’s theorem is that the affine curve obtained by removing a point $\mathcal{X} := E - \mathcal{O}$ has finitely many integral points $\mathcal{X}(\mathbb{Z})$. 

While preparing this work the author was supported by National Science Foundation grant DGE-1840990.
Quadratic Chabauty for integral points on rank 1 elliptic curves requires an infinite order point in $E(\mathbb{Q})$. We replace this requirement with the computation of special values of two $p$-adic $L$-functions constructed by Perrin-Riou [PR87b] and Bertolini, Darmon, and Prasanna [BDP13] that determine the height and logarithm of a Heegner point for $E$, respectively. This allows us to determine $\mathcal{X}(\mathbb{Z})$ without knowing a rational point of infinite order.

The main difficulty lies in the computation of the special value of the anticyclotomic $p$-adic $L$-function introduced in [BDP13], which lies outside the range of interpolation. To access this value, we rely on the continuity of the $L$-function on certain central characters and apply a method of Rubin [Rub81, Rub94] originally used to compute the Katz $p$-adic $L$-function at a value outside the range of interpolation.

We begin in Section 2 by giving an overview of quadratic Chabauty for integral points and the necessary modifications for an algorithm using $p$-adic $L$-function values as input. In Section 3 we describe the computation of the anticyclotomic $p$-adic $L$-function inside and outside the range of interpolation. In Section 4 we describe a computation using Perrin-Riou’s $p$-adic Gross–Zagier formula to obtain the height of the Heegner point. Finally in Section 5 we give some example computations of integral points on elliptic curves.

2. INTEGRAL POINTS ON ELLIPTIC CURVES

Let $E$ be a rank one elliptic curve over $\mathbb{Q}$ with conductor $N$. Fix a prime $p > 2$ of good ordinary reduction. Let $\mathcal{E}/\mathbb{Z}$ denote the minimal regular model of $E$ and $\mathcal{X} = \mathcal{E} - \mathcal{O}$ the complement of the zero section in $\mathcal{E}$. Fix also differentials $\omega_0 = \frac{dz}{2y+a_1z+a_3}$ and $\omega_1 = x\omega_0$ where the $a_i$ are the usual Weierstrass coefficients for $E$.

Let $b$ be a tangential basepoint at the point at infinity or an integral 2-torsion point. Consider the two functions, the double Coleman integral

$$D_2(z) := \int_b^z \omega_0\omega_1$$

as well as the logarithm, which can be expressed as the Coleman integral

$$\log(z) := \int_b^z \omega_0.$$

**Theorem 2.1 ([Kim10, BKK11]).** Suppose $\mathcal{E}$ has analytic rank 1 and Tamagawa product 1. Then $D_2(z)/(\log(z))^2$ is constant on non-torsion integral points of $\mathcal{X}$.

We sketch a proof of this fact. Since $E$ is rank 1, the $\mathbb{Z}_p$-module $\mathbb{Z}_p \otimes E(\mathbb{Q})$ is 1-dimensional, and has only a 1-dimensional space of quadratic forms. Both $\log^2$ and $h$ (the global $p$-adic height) are quadratic forms on this space, therefore $\gamma \log(z)^2 = h(z)$ for all $z \in E(\mathbb{Q})$. The global height decomposes into a sum of local heights $h = \sum_v h_v$. In particular, because $E$ has Tamagawa product one, the local height contributions $h_v(z)$ for $v \neq p$ are 0 on integral points of $\mathcal{X}$. The local height at $p$ on $z \in \mathcal{X}(\mathbb{Z})$ is given by $h_p(z) = 2D_2(z) + c\log(z)^2$, for a specific constant $c$ (see (3)). Dividing by $\log(z)^2$, we see $D_2(z)/\log(z)^2$ is constant on $\mathcal{X}(\mathbb{Z})$.

Since $D_2$ and $\log$ are computable [BBK10, Bal13], this gives a viable (if inefficient) method of computing integral points on $\mathcal{X}$.

In quadratic Chabauty for integral points on elliptic curves, Balakrishnan, Besser, and Müller [BB15, BBM17] remove the Tamagawa number 1 hypothesis in Theorem 2.1 and give algorithms to compute a finite set of $p$-adic points $\mathcal{X}(\mathbb{Z})_2$ containing the integral points. We recall a related theorem.
Suppose that \( p > 3 \) and let \( E_2 \) be the Katz \( p \)-adic weight 2 Eisenstein series [Kat76, MST06]. Define the constant
\[
c := \frac{a_1^2 + 4a_2 - E_2(E, \omega_0)}{12}
\]
where the \( a_i \) are the usual Weierstrass coefficients for \( E \). Furthermore, let \( h : E(\mathbb{Q}) \to \mathbb{Q}_p \) be \((-2p)\) times the (global) \( p \)-adic height of [MST06]. For any non-torsion point \( P \in E(\mathbb{Q}) \) define \( \gamma \) by
\[
\gamma := \frac{h(P)}{\log(P)^2}.
\]

**Theorem 2.2.** [Bia20, Theorem 1.7] Let \( E \) be a rank 1 elliptic curve with good ordinary reduction at \( p \) and bad reduction at the primes in a finite set \( S \). There is a computable finite set \( W \subset \mathbb{Q}_p \) such that \( W_q \) is the possible local height contributions for an integral point at bad places, and \( W_q \) is determined by the Kodaira type of the reduction of \( E \) at \( q \). For \( w \in W \) define \( \|w\| \) to be the sum of its elements.

If \( E \) has good reduction at \( q = 2 \) or \( q = 3 \), and \( E(\mathbb{F}_q) = \{O\} \), or if \( E \) has split multiplicative reduction of Kodaira type \( I_1 \) at 2, then
\[
\mathcal{X}(\mathbb{Z}_p)_2 = \mathcal{X}(\mathbb{Z}) = \emptyset.
\]
Otherwise,
\[
\mathcal{X}(\mathbb{Z}) \subseteq \mathcal{X}(\mathbb{Z}_p)_2 := \bigcup_{w \in W} \psi(w),
\]
where
\[
\psi(w) := \{z \in \mathcal{X}(\mathbb{Z}_p) : 2D_2(z) + c \log(z)^2 + \|w\| = \gamma \log(z)^2\}.
\]

We describe \( \gamma \) in terms of two different special values of \( p \)-adic \( L \)-functions associated to \( f \in S_2(\Gamma_0(N)) \) the cusp form related to \( E \) by modularity. We start by collecting some running assumptions that will be used for the remainder of the paper.

1. \( E/\mathbb{Q} \) is of analytic rank 1. (H1)
2. \( K = \mathbb{Q}(\sqrt{D}) \) is an imaginary quadratic field of class number 1 with odd discriminant \( D < -3 \). (H2)
3. Assume also every prime \( q \) dividing the conductor \( N \) of \( E \) splits in \( K \). (H3)
4. \( p = \mathfrak{p}\overline{\mathfrak{p}} \) splits in \( K \) and is of good ordinary reduction for \( E \). (H4)

Let \( \alpha_p \) be the unit root of the Frobenius polynomial of \( E/\mathbb{F}_p \). Perrin-Riou [PR87b] constructs a \( p \)-adic \( L \)-function whose derivative in the cyclotomic direction at the trivial
character is proportional to the global height of the Heegner point:

\[(8) \quad \mathcal{L}_p'(f, 1) = \left(1 - \frac{1}{\alpha_p}\right)^4 h(P_{K,f}).\]

On the other hand, Bertolini, Darmon, and Prasanna [BDP13] construct an anticyclotomic \(p\)-adic \(L\)-function whose special value at the trivial character is proportional to the logarithm of the Heegner point:

\[(9) \quad L_p(f, 1) = \left(\frac{1 - a_p(f) + p}{p}\right)^2 \log(P_{K,f})^2.\]

Then we can express

\[(10) \quad \gamma = \frac{h(P_{K,f})}{\log(P_{K,f})^2} = \frac{\left(1 - \frac{1}{\alpha_p}\right)^4 \mathcal{L}_p'(f, 1)}{\left(\frac{1 - a_p(f) + p}{p}\right)^2 L_p(f, 1)}\]

and use \(\gamma\) as input for a quadratic Chabauty algorithm on \(E\). This allows us to determine \(X(\mathbb{Z})\) without knowing an infinite order point of \(E(\mathbb{Q})\).

**Remark 2.3.** When we compute \(\gamma\) using (10), we do not directly compute the Heegner point \(P_{K,f}\) on \(E(\mathbb{Q})\) using existing methods. Rather, we compute \(p\)-adic \(L\)-values using the CM point \(\tau_n \in X_0(N)(\mathbb{C})\) that maps to \(P_{K,f}\) under the modular parametrization (see (13)). This yields a new algorithm to compute \(P_{K,f}\) by evaluating the \(p\)-adic modular form \((d^{-1}f)\) at the CM point, where \(d\) denotes the Atkin–Serre derivative, since

\[(11) \quad (d^{-1}f)(\tau_n) = \left(\frac{1 - a_p(f) + p}{p}\right)^2 \log(P_{K,f})^2.\]

### 3. The Logarithm

Throughout we denote the modular form associated to \(E\) as \(f \in S_2(\Gamma_0(N))\). We recall the construction of the anticyclotomic \(p\)-adic \(L\)-function in [BDP13] associated to \(f\).

Let \(K^{\text{ac}}/K\) be the anticyclotomic \(\mathbb{Z}_p\)-extension of \(K\), and let \(\Gamma^- := \text{Gal}(K^{\text{ac}}/K)\) denote the Galois group. Write \(\hat{\mathcal{O}}\) for the completion of the ring of integers of the maximal unramified extension of \(\mathbb{Q}_p\) and define \(\Lambda^{\text{ac}} := \mathbb{Z}_p[[\Gamma^-]] \hat{\otimes} \mathbb{Z}_p\hat{\mathcal{O}}\).

Let \(S \subset \text{Hom}_{\text{cts}}(\Gamma^- , \hat{\mathbb{Q}}_p)\) be the subset of Galois characters associated to unramified algebraic Hecke characters \(\chi\) of \(K\) of infinity type \((2 + j, -j)\) for some \(j \in \mathbb{N}\). Bertolini, Darmon, and Prasanna prove that there exists \(L_p(f) \in \Lambda^{\text{ac}}\) interpolating an algebraic \(L\)-value \(L_{\text{alg}}(f, \chi^{-1}, 0)\) for \(\chi \in S\). Each \(\chi \in S\) determines a map \(\Lambda^{\text{ac}} \to \hat{\mathbb{Q}}_p\) by \(\hat{\mathcal{O}}\)-linear extension. The interpolation property [BDP13, (5.2.3)] for \(L_p(f)\) says that for all \(\chi \in S\) and \(\Omega_p\) a \(p\)-adic period associated to the Heegner point defined in [BDP13, (5.2.2)], we have

\[(12) \quad \chi(L_p(f))/\Omega_p^{2(2+2j)} = (1 - \chi^{-1}(\overline{p})a_p + \chi^{-2}(\overline{p})p^{k-1})^2 L_{\text{alg}}(f, \chi^{-1}, 0).\]

The trivial character \(1\) (associated to the Hecke character of \(K\) with infinity type \((1, 1)\)) is not in \(S\), so we cannot use (12) to evaluate \(1(L_p(f))\). However, for \(\chi \in S\), we can evaluate \(\chi(L_p(f))\), which we will now explain.
3.1. Evaluating in the range of interpolation. The algebraic $L$-function $L_{\text{alg}}(f, \chi^{-1}, 0)$ is defined to be an explicit constant multiple of $L(f, \chi^{-1}, 0)$. However, the value of the algebraic $L$-function can be rewritten in terms of the Shimura–Maass derivative of $f$ evaluated at the CM point associated to the Heegner point and a complex period $\Omega_K$. Since $N$ satisfies (H3), we can write $N = n\bar{n}$ in $\mathcal{O}_K$ where $n = ZN + Z^{\frac{b + \sqrt{D}}{2}}$ for some $b \in \mathbb{Z}$. Then $C/n^{-1}$ is an elliptic curve with CM by $\mathcal{O}_K$ over $\mathbb{C}$ isomorphic to $C/(\mathbb{Z} \oplus \mathbb{Z} \tau_n)$ where

$$
\tau_n := \frac{b + \sqrt{D}}{2N}
$$

is a representative on $X_0(N)$ for the Heegner point $C/n^{-1} \to C/O_K$. Let $\chi \in S$ be the Galois character associated to the Hecke character of infinity type $(2 + j, -j)$ with $j \geq 0$. Then

$$
L_{\text{alg}}(f, \chi^{-1}, 0) = \frac{(\delta^j f(\tau_n))^2}{(\bar{n}\Omega_K)^{2j+2}}.
$$

More precisely, if we consider $\delta^j f$ as a modular form in the sense of Katz (e.g. see [BDP13, Section 1.1]), and consider $(A, A[n], \omega_A)$ as a point on $X_0(N)$, then [BCD+14, (31)] [BDP17, Appendix B] we have $\Omega_K = \Omega_A/\sqrt{D}$.

Shimura [Shi75] showed that the values of the Shimura–Maass derivative $\delta$ of $f$ evaluated at this CM point are algebraic. Let $\chi \in S$ be the Galois character associated to the Hecke character of infinity type $(2 + j, -j)$ with $j \geq 0$. Then

$$
L_{\text{alg}}(f, \chi^{-1}, 0) = \frac{(\delta^j f(\tau_n))^2}{(\bar{n}\Omega_K)^{2j+2}}.
$$

We describe how to compute these values.

Let $g$ be a modular form of weight $k$. Let $d$ be the Atkin–Serre derivative that acts on $q$-expansions by $qd/dq$. By [VW14, Lemma 2.4], we have

$$
\delta^r g = \sum_{j=0}^{r} \binom{r}{j} \frac{(k+j)_{r-j}}{(-4\pi y)^{r-j}} d^j g
$$

where $y = \text{Im } z$ is the imaginary part of the standard complex coordinate and $(a)_m$ is the Pochhammer symbol $a(a+1)\cdots(a+m-1)$. In particular, we can apply the formula to $f$ at $\tau_n$. As $r$ gets large in the usual absolute value, this also gets large, and a naive strategy like evaluating a truncated $q$-expansion of $\delta^r f(\tau_n)$ does not approximate the true algebraic value well.

However, [Zag08, Section 6.3] and [VZ93] explain that the values of the Shimura–Maass derivative of a modular form evaluated at any CM point satisfy a recurrence relation due to a large amount of algebraic structure on the ring of modular forms $M_k(\Gamma_0(N))$. We recall briefly some of the essential ideas involved in the proof.

In addition to the Shimura–Maass and Atkin–Serre differential operators, we introduce the $\vartheta$ differential operator that acts by

$$
\vartheta g = dg - \frac{k}{12} E_2 g
$$

where $E_2$ is the Eisenstein series of weight 2.
where $E_2$ is the weight 2 Eisenstein series. Table 1 shows some properties of these differential operators; by “preserves modularity”, we mean that modular forms of weight $k$ map to modular forms of weight $k + 2$.

<table>
<thead>
<tr>
<th></th>
<th>$d$</th>
<th>$\delta$</th>
<th>$\vartheta$</th>
</tr>
</thead>
<tbody>
<tr>
<td>modularity</td>
<td>not preserved</td>
<td>preserved</td>
<td>preserved</td>
</tr>
<tr>
<td>holomorphicity</td>
<td>preserved</td>
<td>not preserved</td>
<td>preserved</td>
</tr>
<tr>
<td>Fourier expansions</td>
<td>simple action</td>
<td>simple action</td>
<td>complicated</td>
</tr>
</tbody>
</table>

Table 1. Properties of the differential operators

Let $g$ be a modular form of weight $k$. Since $dg$ is not modular, if $h$ is a modular form of weight $\ell$, then $(dg)h$ is not modular. However, $k(dh)g - \ell(dg)h$ is a weight $k + \ell + 2$ modular form. We call this bracket $[g, h]$; it turns $M_k(\Gamma_0(N))$ into a graded Lie algebra. Generalizing, there is a Rankin–Cohen bracket, with $[g, h]_0 = gh$ and $[g, h]_1 = [g, h]$, so that

$$[g, h]_n = \sum_{r+s=n} \frac{(-1)^r}{r!s!} \left( \begin{array}{c} k + n - 1 \\ s \end{array} \right) \left( \begin{array}{c} \ell + n - 1 \\ r \end{array} \right) (d^r g)(d^s h)$$

and $[g, h]_n$ is a weight $k + \ell + 2n$ modular form for $\Gamma_0(N)$.

Instead to write this with $\vartheta$, we have the identities $[g, h]_0 = gh$ and $[g, h]_1 = k(\vartheta h)g - \ell(\vartheta g)h$. To make higher brackets we define

$$[g, h]_n = \sum_{r+s=n} \frac{(-1)^r}{r!s!} \left( \begin{array}{c} k + n - 1 \\ s \end{array} \right) \left( \begin{array}{c} \ell + n - 1 \\ r \end{array} \right) (\vartheta^{[r]} g)(\vartheta^{[s]} h)$$

where $\vartheta^{[0]} g = g$ and $\vartheta^{[r+1]} g = \vartheta(\vartheta^{[r]} g) - r(k + r - 1)(E_4/144)\vartheta^{[r-1]} g$ for $r \geq 1$.

The Cohen–Kuznetsov series are formal generating series that allow us to prove facts about the Rankin–Cohen algebra structure. We can define them for each operator by

$$\tilde{g}_\delta(z, X) = \sum_{n=0}^{\infty} \frac{\delta^n g(z)}{n!(k)_n} X^n, \quad \tilde{g}_\vartheta(z, X) = \sum_{n=0}^{\infty} \frac{\vartheta^{[n]} g(z)}{n!(k)_n} X^n, \quad \tilde{g}_d(z, X) = \sum_{n=0}^{\infty} \frac{d^n g(z)}{n!(k)_n} X^n.$$

These are related by the following:

$$\tilde{g}_\vartheta(z, X) = e^{-XE_2(z)/12} \tilde{g}_d(z, X) = e^{-XE_2(z)/12} \tilde{g}_\delta(z, X)$$

where $E_2^2(z) := E_2(z) - 3/(\pi y)$.

The key idea is that if $E_2^2(z_0) = 0$, then (21) implies that $\vartheta^{[i]} g(z_0) = \delta^i g(z_0)$ for all $i \geq 0$. Then, because $\vartheta^{[i]} g(z_0)$ is defined recursively, this allows us to compute $\delta^i g(z_0)$ recursively. This method requires two pieces of input.

1. We need to modify the operator $\vartheta^{[i]}$ for the CM point $\tau_n$ so that the resulting relationship (21) becomes $\tilde{g}_{\vartheta^{[i]}}(z, X) = e^{-XE_2(z)\phi^*(\tau_n)/12} \tilde{g}_d(z, X)$ with $\phi^*(\tau_n) = 0$.

2. We need generators $g_1, \ldots, g_n$ for $M_*(\Gamma_0(N))$ so that we can compute $\vartheta^{[i]}$ of each generator as well as the values $g_i(\tau_n)$ and $(\vartheta^{[i]} g_i)(\tau_n)$ for each generator to determine the recurrence relation.

In particular, [VZ93] show that $\phi(z)$ should satisfy:

1. $\phi(z)$ is holomorphic;
Remark 3.1. The recursive methods explained here combined with the rigorous methods in the appendix to [BDP17] resolve the issue described in [BDP17, Remark 5.1.4] of how to compute rigorous tables of values of Shimura–Maass derivatives at CM points for a fixed modular form.

We give some intuition following the discussion in [BDP17, Appendix B]. Consider the $O_K$-module $M_k(\Gamma_0(N), O_K)$ consisting of weight $k$ modular forms $g$ for $\Gamma_0(N)$ whose $q$-expansions have coefficients in $O_K$. The problem is that for $g \in M_k(\Gamma_0(N), O_K)$, the evaluation of $g(A, A[n], \omega_A)$ is not necessarily $O_K$-integral, but belongs to $1/N \cdot O_K$. One can construct a finite index $O_K$-module $M_k, O_K \subseteq M_k(\Gamma_0(N), O_K)$ such that for every $g \in M_k, O_K$, $g(A, A[n], \omega_A)$ is $O_K$-integral. This is tensor compatible with the corresponding $\mathbb{Z}$-modules:

$$O_K \otimes \mathbb{Z} M_k, \mathbb{Z} = M_k, O_K, O_k \otimes \mathbb{Z} M_k(\Gamma_0(N), \mathbb{Z}) = M_k(\Gamma_0(N), O_K)$$

so the exponent on the finite abelian group $M_k(\Gamma, \mathbb{Z})/M_k, \mathbb{Z}$ multiplies $M_k(\Gamma_0(N), O_K)$ into $M_k, O_K$ and is an explicit bound on the denominator. (In fact, it gives a much stronger result: this gives a bound on all denominators for all number fields $K$.)

Example 3.2. Let $E$ be the elliptic curve with LMFDB label $37.a.1$. We have a basis of weight 2 forms on $\Gamma_0(37)$ given by

$$f_1 = 1 - 2q^3 + 10q^4 + 2q^5 + 14q^6 + 6q^7 + 10q^8 + 18q^9 + O(q^{10})$$

$$f_2 = q + q^3 - 2q^4 - q^5 + 2q^6 + q^7 - 2q^8 + O(q^{10})$$

$$f_3 = q^2 + 2q^3 - 2q^4 + q^5 - 3q^6 + 4q^7 - 4q^8 + O(q^{10})$$

Let $\tau_n = \frac{-27 + \sqrt{-11}}{2 \sqrt{37}}$. By the discussion above, we can bound the denominators of $f_i(\tau_n)$ and $E_2^*(\tau_n)$ by $37^{|2p/(p-1)|} = 37^3$. We can compute $E_2^*(\tau_n)/\Omega_K^2 = 4400 - 3696\sqrt{-11}$. We also compute $f_i(\tau_n)$:

$$f_1(\tau_n)/\Omega_K^2 = 2420 + 572\sqrt{-11}$$

$$f_2(\tau_n)/\Omega_K^2 = -726 + 154\sqrt{-11}$$

$$f_3(\tau_n)/\Omega_K^2 = -1210 - 286\sqrt{-11}.$$
Given an expression $M_\star(\Gamma) = \mathbb{Q}[g_1, ..., g_n]/I$, we can use the iterative relation
\begin{equation}
\psi_\phi^{[r+1]} f = \partial_\phi(\psi_\phi^{[r]} f) + r(k + r - 1)\Phi(\psi_\phi^{[r-1]} f) \quad \text{for } r \geq 1
\end{equation}
and apply the Leibniz rule to the monomials in $\psi_\phi^{[r]} f$ to apply $\partial_\phi$ iteratively. For example, to compute $\psi_\phi^{[2]} f$ given $\psi_\phi^{[1]} f$ as a sum of monomials in the generators, we need to apply $\partial_\phi$ to each monomial of weight 4. Either the monomial is one variable and we look up the precomputed $\partial_\phi(g_i)$ or it is of the form $\partial_\phi(g_ig_j) = \partial_\phi(g_i)g_j + g_i\partial_\phi(g_j)$ where we look up the $\partial_\phi(g_i)$ in a table. We simply need to precompute $\psi_\phi^{[r]}(g_i)/\Omega_{K}^{\text{wt}(g_i)+2}$ and $g_i(\tau_n)/\Omega_{K}^{\text{wt}(g_i)}$.

Remark 3.3. The slowest part of the computation is expressing $\psi_\phi^{[r+1]} f$ in the basis of monomials for the graded weight $2(r + 1) + 2$ piece. We use $\mathbb{Q}$-linear algebra: we evaluate $\psi_\phi^{[r+1]} f$ and the monomial generators as $q$-expansions, using precision equal to the Sturm bound, then solve for $\psi_\phi^{[r+1]} f$ in terms of the generators.

To obtain the generators and relations
\begin{equation}
M_\star(\Gamma_0(N)) = \mathbb{Q}[g_1, ..., g_n]/I
\end{equation}
we use the Magma code for computing canonical rings found in the repository [ABC+]. By [VZB19] we need generators up to degree 6 and relations up to degree 12.

Continuing Example 3.2, we can use these methods to compute
\begin{equation}
f(\tau_n)/\Omega_{K}^2 = 1694 + 726\sqrt{-11} \quad \text{and} \quad \delta f(\tau_n)/\Omega_{K} = 532400 - 447216\sqrt{-11}.
\end{equation}

3.2. Evaluating outside of the range of interpolation. We now discuss an application of Rubin’s method to compute the value $L_p(f, 1)$ outside of the range of interpolation.

Let $r \in \mathbb{N}$. Let $\chi_r \in S$ be the Galois character associated to the Hecke character of infinity type $(1 + r, 1 - r)$. Define
\begin{equation}
\ell(r) := L_p(f, \chi_r)\Omega_p^{-4r}.
\end{equation}

We want to compute $\ell(0)$. Since this is not in the range of interpolation, we compute auxiliary values $\ell((p - 1)), \ell(2(p - 1)), \ldots, \ell(B(p - 1))$ in the range of interpolation and recover $\ell(0)$ modulo $p^B$ from a version of [Rub94, Theorem 9, Proposition 7] for the anticyclotomic $p$-adic $L$-function of Bertolini, Darmon, and Prasanna.

Proposition 3.4. Let $\ell$ be defined as above. Then
\begin{equation}
\ell(0)^{(p-1)/2} \equiv \sum_{j=1}^{B} \left( \sum_{i=j}^{B} (-1)^{i-j-1}\binom{i-1}{j-1} \ell(j(p - 1))^{(p-1)/2} \right) \pmod{p^B}.
\end{equation}

Furthermore, $\ell(0) \equiv \ell((p - 1)^2/2) \pmod{p}$.

Assuming $\ell(0) \not\equiv 0 \pmod{p}$, Proposition 3.4 allows us to uniquely recover $\ell(0)$ from the auxiliary values $\ell(j(p - 1))$. We now prove Proposition 3.4.

Following Rubin, we introduce a ring of generalized Iwasawa functions $\mathcal{I}$. A function $g$ on $\mathbb{Z}_p$ is in $\mathcal{I}$ if there exist units $u_1, \ldots, u_m \in 1 + p\hat{O}$ and a power series $H \in \hat{O}[[X_1, \ldots, X_m]]$ such that $g(s) = H(u_1^s - 1, \ldots, u_m^s - 1)$ for all $s \in \mathbb{Z}_p$. 

8
Recall $\chi_{i(p-1)} \in S$ is a Galois character associated to a Hecke infinity type $(1 + i(p-1), 1 - i(p-1))$. By composing with a projection arising from $\mathbb{Z}_p^\times \simeq (\mathbb{Z}/p\mathbb{Z})^\times \times (1 + p\mathbb{Z}_p)$, we have
\begin{equation}
\langle \chi_{i(p-1)} \rangle : \Gamma^- \to \mathbb{Z}_p^\times \to 1 + p\mathbb{Z}_p
\end{equation}

since $\chi_{i(p-1)}$ already takes values in $1 + p\mathbb{Z}_p$ [dS87, §II.4.17]. For $F \in \Lambda^\infty$, we have $\langle \chi_{i(p-1)} \rangle(F) \in \hat{\mathcal{Q}}_p$, and furthermore for $s \in \mathbb{Z}_p$ we can define $\chi_{s(p-1)} := \langle \chi_{(p-1)} \rangle^s$ and evaluate $\chi_{s(p-1)}(F) \in \hat{\mathcal{Q}}_p$ by continuity.

Define
\begin{equation}
H(s) := (\Omega_p^{(p-1)^2})^{-2s} L_p(f, \chi_{s(p-1)})^{(p-1)/2}.
\end{equation}

By [dS87, §II.4.3(10)], we have
\begin{equation}
\Omega_p^{(p-1)^2} \in 1 + p\mathcal{O}
\end{equation}

so $H$ is well-defined. For $i \in \mathbb{Z}$, note that
\begin{equation}
H(i) = \ell((p - 1)i)^{(p-1)/2}.
\end{equation}

Analogously to [Rub94, Proposition 7], we have the following proposition:

**Proposition 3.5.**

(1) $H \in \mathcal{I}$.

(2) $\ell(0) \equiv \ell((p - 1)^2/2) \mod p$.

**Proof.** We define functions $f_1$ and $f_2$ by
\begin{equation}
f_1(s) := L_p(f, \chi_{s(p-1)})
\end{equation}
\begin{equation}
f_2(s) := (\Omega_p^{(p-1)^2})^{-2s}.
\end{equation}

Then $H = f_1^{(p-1)/2} f_2$. We know $f_1 \in \mathcal{I}$ since $\chi_{i(p-1)}$ is a character into $1 + p\mathbb{Z}_p$ for all $i \in \mathbb{N}$ (see (30)) and by (32) we know $f_2 \in \mathcal{I}$, so $H \in \mathcal{I}$.

Finally, since $f_1(s) \equiv f_1(s') \mod p$ for all $s, s' \in \mathbb{Z}_p$ we have
\begin{equation}
\ell(0) = f_1(0) \equiv \Omega_p^{-2(p-1)^2} f_2((p - 1)/2) = \ell((p - 1)^2/2) \mod p.
\end{equation}

\[ \square \]

**Remark 3.6.** Proposition 3.5 (2) is only helpful if $\ell((p - 1)^2/2) \neq 0 \mod p$. More generally, one can see that by (32), for $n \geq 1$ we have
\begin{equation}
\ell(0) = f_1(0) \equiv \Omega_p^{-2(p-1)^2 p^{n-1}} f_2((p - 1)p^{n-1}/2) = \ell((p - 1)^2 p^{n-1}/2) \mod p^n.
\end{equation}

The main difficulty in applying this congruence is computing $\ell((p - 1)^2 p^{n-1}/2)$.

From here it is straightforward to follow Rubin’s proof to obtain a proof of Proposition 3.4: we recapitulate it briefly. He defines a difference operator $\Delta$ on $\mathcal{I}$ by $\Delta(g)(s) := g(s + 1) - g(s)$. If $g \in \mathcal{I}$ then $\Delta(g) \in p\mathcal{I}$ [Rub94, Lemma 8].

By inverting $(1 + \Delta)^{-1} = \sum_{i=0}^\infty (-1)^i \Delta^i$ and applying the congruence, we obtain the desired formula [Rub94, Theorem 9]
\begin{equation}
g(0) = \sum_{j=1}^B \left( \sum_{i=j}^B (-1)^{j-1} \binom{i-1}{j-1} \right) g(j) \mod p^B.
\end{equation}
By applying this to $H \in \mathcal{I}$ we can compute the special values. This works for a variety of elliptic curves as summarized in Table 2. We take $B = 5$ by default, though we have tested higher values of $B$ on many curves.

<table>
<thead>
<tr>
<th>Label</th>
<th>$D$</th>
<th>$p$</th>
</tr>
</thead>
<tbody>
<tr>
<td>37.a1</td>
<td>−11</td>
<td>5</td>
</tr>
<tr>
<td>43.a1</td>
<td>−19, −7</td>
<td>5, 11</td>
</tr>
<tr>
<td>58.a1</td>
<td>−7</td>
<td>11</td>
</tr>
<tr>
<td>61.a1</td>
<td>−19</td>
<td>5, 7</td>
</tr>
<tr>
<td>77.a1</td>
<td>−19</td>
<td>5</td>
</tr>
<tr>
<td>83.a1</td>
<td>−19</td>
<td>5</td>
</tr>
<tr>
<td>89.a1</td>
<td>−11</td>
<td>3</td>
</tr>
<tr>
<td>101.a1</td>
<td>−19</td>
<td>5</td>
</tr>
<tr>
<td>131.a1</td>
<td>−19</td>
<td>5, 7</td>
</tr>
</tbody>
</table>

Table 2. Some curves for which we have used Proposition 3.4 to compute $\ell(0) \mod p^B$

Remark 3.7. The biggest impediment to considering large conductors $N$ is the time it takes to compute generators and relations for the ring $M_\ast(\Gamma_0(N))$, which becomes very long when $N \geq 100$. This scales with the Sturm bound [Ste07, Corollary 9.20]

$$\left\lceil \frac{k \cdot [\text{SL}_2(\mathbb{Z}) : \Gamma_0(N)]}{12} \right\rceil = \left\lceil \frac{k \cdot N \prod_{p|N} \left(1 + \frac{1}{p}\right)}{12} \right\rceil$$

which gives the precision needed to do linear algebra in $q$-expansions on $M_k(\Gamma_0(N))$.

For example when $E$ is the elliptic curve with LMFDB label 37.a1, $D = −11$, and $p = 5$, we have the values in Table 3. So Proposition 3.4 implies that

<table>
<thead>
<tr>
<th>$r$</th>
<th>$\ell(r) \mod p^{10}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>−2341944</td>
</tr>
<tr>
<td>8</td>
<td>830906</td>
</tr>
<tr>
<td>12</td>
<td>−3933069</td>
</tr>
<tr>
<td>16</td>
<td>−35494</td>
</tr>
<tr>
<td>20</td>
<td>1760756</td>
</tr>
<tr>
<td>24</td>
<td>1706556</td>
</tr>
<tr>
<td>28</td>
<td>1972781</td>
</tr>
<tr>
<td>32</td>
<td>−3662194</td>
</tr>
<tr>
<td>36</td>
<td>3734381</td>
</tr>
<tr>
<td>40</td>
<td>4015256</td>
</tr>
</tbody>
</table>

Table 3.

(39) $H(0) = L_p(f, 1)^2 \equiv 2502536 \mod p^{10}$
and
\[(40) \quad L_p(f, 1) \equiv \ell(8) \equiv 830906 \mod p\]
so
\[(41) \quad L_p(f, 1) \equiv 4635631 \mod p^{10}.
\]
For 77.a1, \(D = -19\), and \(p = 5\), we can similarly compute \(\ell(0) \mod B = 7\):
\[(42) \quad L_p(f, 1) \equiv 4 + 2 \cdot 5 + 4 \cdot 5^2 + 3 \cdot 5^3 + 5^4 + 3 \cdot 5^6 \mod p^7.
\]
This agrees with the computed value of \(\left(\frac{1-\alpha_p(f)+p}{p}\right)^2 \log(P_{K,f})^2\). In this case the Heegner point has index 2 in \(E(\mathbb{Q})\).

4. The height

Recall that \(f \in S_2(\Gamma_0(N))\) is the weight 2 cusp form associated to \(E/\mathbb{Q}\) and \(K\) is an imaginary quadratic field of class number 1 with discriminant \(D\).

In this section we discuss the computation of \(h(P_{K,f})\) using the \(p\)-adic Gross–Zagier formula of Perrin-Riou [PR87b] and relate the \(p\)-adic \(L\)-function to the one defined by Amice-Vélu and Vishik as discussed in [MTT86, SW13].

Let \(K_\infty/K\) be the (unique) \(\mathbb{Z}_p^2\) extension of \(K\) with Galois group \(\Gamma := \text{Gal}(K_\infty/K)\). Let \(\psi : \Gamma \rightarrow 1 + p\mathbb{Z}_p\) be a finite order character. The theta series
\[(43) \quad \Theta_\psi := \sum_{a \in \mathcal{O}_K} \psi(a)q^{N(a)}
\]
is a weight 1 modular form. We denote the Rankin–Selberg convolution by \(L(f, \psi, s) := L(f, \Theta_\psi, s)\). Perrin-Riou constructs a \(p\)-adic \(L\)-function \(L_p(f) \in \mathbb{Z}_p[[\Gamma]]\) characterized by the interpolation property that for any finite order character \(\psi : \Gamma \rightarrow 1 + p\mathbb{Z}_p\), the value \(\psi(L_p(f))\) is proportional to \(L(f, \psi, 1)\).

Perrin-Riou relates the derivative of this \(p\)-adic \(L\)-function to a \(p\)-adic height pairing defined by Schneider and Mazur–Tate [Sch82, MT83]. This height pairing \(\langle \cdot, \cdot \rangle_{\ell_K}\) depends on a choice of idèle class character:
\[(44) \quad \ell_K : \mathbb{A}_K^\times/K^\times \rightarrow \mathbb{Q}_p
\]
equivalently, a homomorphism \(\Gamma \rightarrow \mathbb{Q}_p^\times\). We can decompose \(\ell_K\) as the composition \(\ell_K = p^{-n} \log \lambda\) for some integer \(n\) and \(\lambda : \Gamma \rightarrow 1 + p\mathbb{Z}_p\) [Sch15, Section 1.1.2]. Then the derivative of \(L_p(f, \chi)\) in the direction of \(\ell_K\) at 1 is defined as
\[(45) \quad L'_{p,\ell_K}(f, \chi) := p^{-n} \left(\frac{d}{ds} \lambda^s(L_p(f, \chi))\right)\bigg|_{s=0}.
\]
Then

**Theorem 4.1** ([PR87b, Corollary to Theorem 1.3]).

\[(46) \quad L'_{p,\ell_K}(f, 1) = \left(1 - \frac{1}{\alpha_p}\right)^4 \langle P_{K,f}, P_{K,f} \rangle_{\ell_K}.
\]
Perrin-Riou provides a comparison of the $p$-adic $L$-function described here, of $E/K$, to the $p$-adic $L$-function $L_{p,MTT}(E)$ of $E/Q$ of Amice-Vélu and Vishik [PR87b, (1.1)]. Let $v$ be the cyclotomic character of $\text{Gal}(\overline{Q}/K)$ and $v_Q$ the cyclotomic character of $\text{Gal}(\overline{Q}/Q)$. Let $\Omega_f$ be the period of the modular form $f$ [PR87a, p.409]. Let $E^D$ be the quadratic twist of $E$ by $D$. Then

$$v(L_p(f, 1)) = v_Q(L_{p,MTT}(E))v_Q(L_{p,MTT}(E^D)) \left( \frac{\sqrt{|D|}}{\Omega_f} \right).$$

(47)

SageMath has an implementation of the $p$-adic $L$-function of Amice-Vélu and Vishik, so in practice, we use (47) and the fact that $L(E, 1) = 0$ to translate Theorem 4.1 from a statement about the derivative of $L_p(f, 1)$ in the direction of $v$ into a statement about this $p$-adic $L$-function to compute the cyclotomic $p$-adic height of $P_{K,f}$:

$$L'_{p,v}(f, 1) = L'_{p,MTT}(E, 1)L_{p,MTT}(E^D, 1) \left( \frac{\sqrt{|D|}}{\Omega_f} \right).$$

(48)

(See [SW13, Section 3] for more details on the definition of $L'_{p,MTT}(E, s)$, the series expansion, and the derivative.) To compute $L_{p,MTT}(E^D, 1)$ we use the interpolation property of the $p$-adic $L$-function [SW13, Section 3.2]. This turns the right hand side of (48) into

$$L'_{p,MTT}(E, 1) \left( 1 - \frac{1}{\alpha_p} \right)^2 \frac{L(E^D, 1)}{\Omega_{E^D}^+} \left( \frac{\sqrt{|D|}}{\Omega_f} \right).$$

(49)

Remark 4.2. The normalization for the $p$-adic $L$-function in [SW13] is different from the normalization originally stated in [MTT86] and taken here. The $L$-function differs by a multiple of the real period $\Omega_E^+$, so that $L_{p,MTT}(E, s)/\Omega_E^+ = L_p(E, s)$ where the left hand side is the one discussed in Mazur–Tate–Teitelbaum and the right hand side is the one computed in Sage and used in [SW13].

Example 4.3. Let $E$ be the elliptic curve with LMFDB label 61.a1 and $p = 5$ a prime of good ordinary reduction. Choose $D = -19$ a Heegner discriminant for $E$. Then the $p$-adic $L$-series expansion for $E/Q$ can be computed using [PS11]

$$L_{p,MTT}(E, T) = O(5^{10}) + (1 + 2 \cdot 5^2 + 5^3 + 5^4 + 3 \cdot 5^5 + 2 \cdot 5^7 + O(5^8)) \cdot T
+ (1 + 4 \cdot 5 + 3 \cdot 5^2 + 2 \cdot 5^3 + 2 \cdot 5^4 + 5^5 + O(5^6)) \cdot T^2 + O(T^3).$$

(50)

The conversion from $L_{p,MTT}(E, s)$ to the series expansion $L_{p,MTT}(E, T)$ requires a choice of topological generator $1 + p$ for the Galois group of the cyclotomic $\mathbb{Z}_p$-extension $\text{Gal}(K_{\text{cyc}}^+/K)$ (see [SW13, (3.1)]), so we also compute:

$$\log_p(1 + p) = 5 + 2 \cdot 5^2 + 4 \cdot 5^3 + 2 \cdot 5^4 + 5^6 + 4 \cdot 5^7 + O(5^8).$$

(51)

Using the interpolation property, we have $v_Q(L_{p,MTT}(E^D)) = \left( 1 - \frac{1}{\alpha_p} \right)^2 L(E^D, 1)/\Omega_{E^D}^+$ and we can evaluate

$$L(E^D, 1)/\Omega_{E^D}^+ = 2$$

(52)
while
\[
(53) \quad \left(1 - \frac{1}{\alpha_p}\right)^2 = 4 + 2 \cdot 5 + 4 \cdot 5^3 + 2 \cdot 5^4 + 5^5 + 5^6 + 2 \cdot 5^7 + 3 \cdot 5^8 + 2 \cdot 5^9 + O(5^{10}).
\]

Finally
\[
(54) \quad \left(\frac{\Omega_+^+ \sqrt{|D|}}{\Omega_f}\right) = 2.
\]

Altogether, we find the following formula for the (global) $p$-adic height of $P_{K,f}$.
\[
\langle P_{K,f}, P_{K,f} \rangle_v = h(P_{K,f})
\]
\[
= \left(\frac{\Omega_+^+ \sqrt{|D|}}{\Omega_f}\right) \left(1 - \frac{1}{\alpha_p}\right)^{-2} L(E^D, 1) / \Omega_+^+ \left. \frac{d}{dT} \left(\frac{L_p,MTT(E,T)}{\Omega_E}\right)\right|_{T=0} \log_p(1 + p)
\]
\[
= 4 \cdot 5 + 4 \cdot 5^2 + 2 \cdot 5^3 + 5^4 + 4 \cdot 5^5 + 5^6 + 2 \cdot 5^7 + 4 \cdot 5^8 + O(5^9).
\]

5. Examples

Example 5.1. Let $E$ be the elliptic curve with LMFDB label 43.a1 and consider $p = 11$ a prime of good ordinary reduction. We choose $D = -7$ a Heegner discriminant for $E$ in which $p$ and $N = 43$ split. Fix a model for $E$
\[
\mathcal{X} : y^2 + y = x^3 + x^2.
\]

Using the methods described in previous sections, we compute the constant $\gamma$:
\[
\gamma = \frac{h(P_{K,f})}{\log(P_{K,f})^2}
\]
\[
= \frac{\mathcal{L}_{p,v}^E(f, 1) \left(1 - \frac{1}{\alpha_p}\right)^{-4}}{L_p(f, 1) \left(1 - \alpha_p(f) + \frac{p}{p}\right)^{-2}}
\]
\[
= \frac{9 \cdot 11 + 5 \cdot 11^2 + 5 \cdot 11^3 + 3 \cdot 11^4 + 7 \cdot 11^6 + 4 \cdot 11^7 + 4 \cdot 11^8 + O(11^9)}{11^2 + 8 \cdot 11^3 + 9 \cdot 11^4 + 6 \cdot 11^5 + 8 \cdot 11^6 + 6 \cdot 11^7 + 4 \cdot 11^8 + 4 \cdot 11^9 + 4 \cdot 11^{10} + O(11^{12})}
\]
\[
= 9 \cdot 11^{-1} + 10 + 2 \cdot 11 + 4 \cdot 11^2 + 5 \cdot 11^4 + 8 \cdot 11^5 + 10 \cdot 11^6 + O(11^7).
\]

By solving the equations described by (7) using a modified version of the code associated to [Bia20], we obtain the finite set:
\[
\{(−1, −1), (−1, 0), (0, −1), (0, 0), (1, −2), (1, 1), (2, −4), (2, 3), (21, −99), (21, 98), (10 \cdot 11 + 7 \cdot 11^2 + O(11^3), 10 + 10 \cdot 11 + 9 \cdot 11^2 + 5 \cdot 11^3 + O(11^4)), (10 \cdot 11 + 7 \cdot 11^2 + O(11^3), 11^2 + 5 \cdot 11^3 + O(11^4)), (1 + 6 \cdot 11 + 2 \cdot 11^2 + O(11^3), 9 + 3 \cdot 11^2 + O(11^3)), (1 + 6 \cdot 11 + 2 \cdot 11^2 + O(11^3), 1 + 10 \cdot 11 + 7 \cdot 11^2 + O(11^3)), (2 + 9 \cdot 11 + 7 \cdot 11^2 + O(11^3), 3 + 8 \cdot 11 + 11^2 + O(11^3)), (2 + 9 \cdot 11 + 7 \cdot 11^2 + O(11^3), 7 + 2 \cdot 11 + 9 \cdot 11^2 + O(11^3))\}.
\]
This contains the 10 integral points on $\mathcal{X}$ as well as 3 pairs of $\mathbb{Z}_{11}$-points conjugate under the hyperelliptic involution.

**Example 5.2.** Let $E$ be the elliptic curve with LMFDB label 131.a1 and $p = 7$ a prime of good ordinary reduction. We choose $D = -19$ a Heegner discriminant for $E$ in which $p$ and $N = 131$ split. Fix a model for $E$

$$\mathcal{X} : y^2 + y = x^3 - x^2 + 1.$$ 

Using the methods described in previous sections, we compute the constant $\gamma$: 

$$\gamma = \frac{h(P_{K,f})}{\log(P_{K,f})^2} = \frac{L'_p(f, 1)(1 - \frac{1}{\alpha_p})^{-4}}{L_p(f, 1)\left(\frac{1 - a_p(f) + p}{p}\right)^{-2}}$$

$$= \frac{4 \cdot 7 + 5 \cdot 7^2 + 3 \cdot 7^3 + 3 \cdot 7^6 + 2 \cdot 7^7 + 3 \cdot 7^8 + 7^9 + 2 \cdot 7^{10} + 4 \cdot 7^{11} + 4 \cdot 7^{12} + O(7^{13})}{2 \cdot 7^2 + 2 \cdot 7^3 + 2 \cdot 7^4 + 4 \cdot 7^6 + 6 \cdot 7^7 + 7^8 + 4 \cdot 7^{10} + 5 \cdot 7^{11} + 4 \cdot 7^{12} + 3 \cdot 7^{13} + 3 \cdot 7^{14} + 7^{15} + O(7^{16})}$$

$$= 2 \cdot 7^{-1} + 4 + 7 + 7^2 + 5 \cdot 7^3 + 7^4 + 6 \cdot 7^5 + 2 \cdot 7^6 + 6 \cdot 7^7 + 3 \cdot 7^8 + 4 \cdot 7^9 + 4 \cdot 7^{10} + O(7^{11}).$$

By solving the equations described by (7), we obtain the finite set:

$$\{(0, -1), (0, 0), (2, 2), (5 + 6 \cdot 7 + 4 \cdot 7^2 + 3 \cdot 7^4 + 7^5 + O(7^6), 6 + 7 + 3 \cdot 7^2 + 2 \cdot 7^5 + O(7^6)), (5 + 6 \cdot 7 + 4 \cdot 7^2 + 3 \cdot 7^4 + 7^5 + O(7^6), 5 \cdot 7 + 3 \cdot 7^2 + 6 \cdot 7^3 + 6 \cdot 7^4 + 4 \cdot 7^5 + O(7^6)), (5 + 4 \cdot 7 + 6 \cdot 7^2 + 3 \cdot 7^5 + O(7^6), 6 \cdot 7 + 2 \cdot 7^3 + 6 \cdot 7^4 + 6 \cdot 7^5 + O(7^6)), (5 + 4 \cdot 7 + 6 \cdot 7^2 + 3 \cdot 7^5 + O(7^6), 6 + 6 \cdot 7^2 + 4 \cdot 7^3 + O(7^6)), (4 \cdot 7 + 6 \cdot 7^2 + 2 \cdot 7^3 + 3 \cdot 7^5 + O(7^6), 4 \cdot 7 + 2 \cdot 7^2 + 5 \cdot 7^3 + 4 \cdot 7^4 + 4 \cdot 7^5 + O(7^6)), (4 \cdot 7 + 6 \cdot 7^2 + 2 \cdot 7^3 + 3 \cdot 7^5 + O(7^6), 6 + 2 \cdot 7 + 4 \cdot 7^2 + 2 \cdot 7^3 + 2 \cdot 7^4 + 2 \cdot 7^5 + O(7^6)), (2 + 2 \cdot 7^3 + O(7^4), 2 + 5 \cdot 7^3 + O(7^4)), (2 + 2 \cdot 7^3 + O(7^4), 4 + 6 \cdot 7 + 6 \cdot 7^2 + 7^3 + O(7^4))\}.$$ 

This contains the 4 integral points on $\mathcal{X}$ as well as 4 pairs of $\mathbb{Z}_7$-points conjugate under the hyperelliptic involution.

6. Future work

The author’s PhD thesis will discuss the case of higher genus modular curves whose associated modular forms all have analytic rank at most one. The Jacobian of such modular curves is generated up to finite index by Heegner points, and the algorithms discussed here can be extended to give a quadratic Chabauty algorithm on these modular curves.

7. Acknowledgements

I am very grateful to my advisor Jennifer Balakrishnan for many helpful conversations and encouragement while working on this project. I thank John Voight for his advice on computing Shimura–Masss derivatives of modular forms and Henri Darmon for his suggestion to consider
Rubin’s method. I am also thankful to Alex Best for many interesting conversations about Coleman integration and Francesca Bianchi for helpful suggestions for improving the paper.

References


Don Zagier. Elliptic modular forms and their applications. In The 1-2-3 of modular forms, Universitext, pages 1–103. Springer, Berlin, 2008. \cite{Zag08} and \cite{Zag08}.

Sachi Hashimoto, Department of Mathematics and Statistics, Boston University, 111 Cummington Mall, Boston, MA 02215, USA

Email address: svh@bu.edu

URL: http://math.bu.edu/people/svh/