Explicit p-adic methods for elliptic and hyperelliptic curves

Jennifer S. Balakrishnan
Mathematical Institute, University of Oxford, Woodstock Road, Oxford OX2 6GG, UK
e-mail: balakrishnan@maths.ox.ac.uk

Abstract. We give an overview of some p-adic algorithms for computing with elliptic and hyperelliptic curves, starting with Kedlaya's algorithm. While the original purpose of Kedlaya's algorithm was to compute the zeta function of a hyperelliptic curve over a finite field, it has since been used in a number of applications. In particular, we describe how to use Kedlaya's algorithm to compute Coleman integrals and p-adic heights on elliptic and hyperelliptic curves. Throughout, we give several numerical examples, and we conclude by showing how to use Coleman integrals to explicitly find integral points on hyperelliptic curves whose Jacobians have Mordell-Weil rank equal to their dimension.

Keywords. Kedlaya's algorithm, hyperelliptic curves, Coleman integration, p-adic heights, integral points

1. Introduction

In 2001, Kedlaya [26] gave an algorithm to calculate the zeta function of a hyperelliptic curve over a finite field of odd characteristic via a p-adic approximation to the characteristic polynomial of Frobenius. This is achieved by explicit computation of the action of Frobenius on Monsky-Washnitzer cohomology.

The action of Frobenius also plays a key role in constructing the analytic continuation of the p-adic line integral known as the *Coleman integral*. This theory of p-adic integration was developed by Coleman [17], who used these integrals to study torsion points on curves. Among other applications, Coleman further used these integrals to reinterpret the method of Chabauty [14] to find rational points on curves whose Jacobians have Mordell-Weil rank less than their dimension [16].

The method of Chabauty-Coleman is, in practice, a terrific tool for finding rational points on curves and has inspired the program of Kim [28,29,30,9,8] to develop a nonabelian analogue of this method to further study rational and integral points on curves, replacing the Jacobian by a nonabelian geometric object known as the *Selmer scheme* and the single Coleman integrals by appropriate *iterated Coleman integrals*.

Furthermore, there is a close relationship between Coleman integrals and p-adic heights [20,4] which can be made quite explicit in the case of elliptic and hyperelliptic curves. Using this, one can give a special case of Kim's program, using double integrals to find integral points on elliptic and hyperelliptic curves, essentially a "quadratic" analogue [6] of the classical method of Chabauty-Coleman.

In these lecture notes, we will touch on a variety of topics, starting with Kedlaya's algorithm in §2. In particular, we give a fully worked out example of carrying out the algorithm in the case of elliptic curves. In §3, we will then show how to use the objects computed in Kedlaya's algorithm to compute single and iterated Coleman integrals on hyperelliptic curves. In §4, we discuss the relationship between Coleman integrals and p-adic heights and give an example of finding integral points on a hyperelliptic curve using the quadratic Chabauty method.

2. Kedlaya's algorithm

2.1. Introduction and motivation

We begin by describing Kedlaya's algorithm for elliptic and hyperelliptic curves, and we draw on [26,27,22] throughout our exposition.

Let C be a smooth projective curve of genus g over $\mathbb{F}_q$, where $q = p^m$. The *zeta function* $\zeta(C,T)$ of C is defined to be

$$\zeta(C,T) = \exp\left(\sum_{k=1}^{\infty} \#C(\mathbb{F}_{q^k})\frac{T^k}{k}\right).$$

Weil showed that the zeta function is a rational function of T: that is,

$$\zeta(C,T) = \frac{P(T)}{(1-qT)(1-T)},$$

where $P(T)$ is a polynomial over $\mathbb{Z}$ of degree $2g$. Since $\zeta(C,0) = 1$, we have $P(0) = 1$. Writing $P(T) = \prod_{i=1}^{2g}(1-\alpha_i T)$, then $|\alpha_i| = \sqrt{q}$ and $\alpha_i\alpha_{g+i} = q$ for $i = 1,\dots,g$.

Note that

$$\#C(\mathbb{F}_{q^k}) = q^k + 1 - \sum_{i=1}^{2g}\alpha_i^k.$$

Furthermore, $P(1) = \#J_C(\mathbb{F}_q)$ is the order of the Jacobian of C.

Recall that the Lefschetz fixed point formula applied to an appropriate cohomology theory of C allows one to compute $\#C(\mathbb{F}_{q^k})$ in terms of the action of Frobenius on cohomology. Kedlaya [26] uses the observation that Monsky-Washnitzer cohomology satisfies a Lefschetz fixed point formula. Then by computing the action of Frobenius on an explicit basis of Monsky-Washnitzer cohomology in the case of a hyperelliptic curve, he computes a p-adic approximation to the characteristic polynomial of Frobenius and recovers the zeta function of the hyperelliptic curve. To say more about this, we review some key facets of Monsky-Washnitzer cohomology.

2.2. A brief introduction to Monsky-Washnitzer cohomology

Let $p > 2$ and let C be an elliptic curve or a genus g hyperelliptic curve over an unramified extension K of $\mathbb{Q}_p$ with good reduction. Let $k = \mathbb{F}_q$ denote the residue field, where $q =$

p^m. We will assume that C is given by a model of the form $y^2 = f(x)$, where f is a monic separable polynomial with $\deg f = 2g+1$. Let C' be the affine curve obtained by deleting the Weierstrass points from C, and let $A = K[x,y,z]/(y^2 - f(x), yz-1)$ be the coordinate ring of C'.

Let $\overline{C}$ denote the smooth projective curve over $\mathbb{F}_q$ cut out by the affine model $y^2 = \overline{f}(x)$. Kedlaya's algorithm computes the zeta function of $\overline{C}$ by working with cohomology attached to C'

Recall that the hyperelliptic involution

$$\iota : (a,b) \mapsto (a,-b)$$

gives us an automorphism of the curves C and C'. This, in turn, induces automorphisms ι^* of algebraic de Rham cohomology $H^1(C')$ and $H^1(C)$, decomposing them into eigenspaces on which ι^* acts as the identity and -1, respectively. In particular,

$$H^1(C') = H^1(C')^+ \oplus H^1(C')^-.$$

The K-vector space $H^1(C')^-$ is spanned by the classes of differentials[1]

$$\left\{ \left[\omega_i := x^i z dx \right] \right\}_{i=0}^{2g-1}. \tag{1}$$

However, the underlying coordinate ring A does not admit the proper lift of Frobenius. To remedy this, we replace A by the dagger ring $A^\dagger$, the Monsky-Washnitzer weak completion of A. It is the ring consisting of infinite sums of the form

$$\sum_{i=-\infty}^{\infty} S_i(x) z^i, \quad S_i(x) = \sum_{j=0}^{2g} a_j x^j \in K[x],$$

subject to the conditions that $\liminf_{i\to\infty} \frac{v_p(S_i)}{i} > 0$ and $\liminf_{i\to\infty} \frac{v_p(S_{-i})}{i} > 0$, where $v_p(S_i(x)) = \min_i\{v_p(a_i)\}$; when necessary, one uses the relation $y^2 = f(x)$ to convert terms with large powers of x into terms with y^2 (recalling that $z = y^{-1}$).

The de Rham complex of $A^\dagger$ is given by

$$\begin{aligned} d : A^\dagger &\longrightarrow A^\dagger \frac{z dx}{2}, \\ \sum_{i,j} a_{i,j} x^i z^j &\mapsto \sum_{i,j} a_{i,j} d(x^i z^j) \\ &= \sum_{i,j} a_{i,j} (2i x^{i-1} z^{j-1} - j x^i f' z^{j+1}) \frac{z dx}{2}. \end{aligned}$$

[1] Note that in this section, we primarily use powers of z (where $z = \frac{1}{y}$) for superficial reasons, so that we avoid having to deal with very large (in absolute value) negative powers of y and instead work with large positive powers of z. In §3, the largest power of z that will be appear is z^1, so we will revert to using $\frac{1}{y}$ in place of z. Furthermore, so that we work with the standard invariant differential in the case of an elliptic curve, in §3, we rescale our basis so that we work with $\omega_i = \frac{x^i dx}{2y}$.

We denote the cohomology groups of this complex by $H^i_{\mathrm{MW}}(C')$, and as before, they are K-vector spaces split into eigenspaces by the hyperelliptic involution. Perhaps more important is that passing from A to $A^\dagger$ does not change the presentation of cohomology, and thus we work with $H^1_{\mathrm{MW}}(C')^-$ and the basis (1). In particular, to compute the p-power Frobenius action ϕ^* on $H^1_{\mathrm{MW}}(C')^-$, we compute its action on the basis elements.

Since K is an unramified extension of $\mathbb{Q}_p$, it has a unique automorphism ϕ_K lifting the Frobenius automorphism $x \to x^p$ on its residue field. Extend ϕ_K to a Frobenius lift on $A^\dagger$ by setting

$$\begin{aligned}
\phi(x) &= x^p \\
\phi(y) &= y^p \left(1 + \frac{\phi_K(f)(x^p) - f(x)^p}{f(x)^p}\right)^{1/2} \\
&= y^p \sum_{i=0}^{\infty} \binom{1/2}{i} \frac{(\phi_K(f)(x^p) - f(x)^p)^i}{y^{2pi}}.
\end{aligned}$$

Note that this gives

$$\begin{aligned}
\phi(z) &= \phi\left(\frac{1}{y}\right) \\
&= y^{-p} \sum_{i=0}^{\infty} \binom{-1/2}{i} \frac{(\phi_K(f)(x^p) - f(x)^p)^i}{y^{2pi}} \\
&= z^p \sum_{i=0}^{\infty} \binom{-1/2}{i} (\phi_K(f)(x^p) - f(x)^p)^i z^{2pi}.
\end{aligned}$$

Example 2.1. Consider $x^i z dx \in H^1_{\mathrm{MW}}(C')^-$. We compute the action of Frobenius on this differential form:

$$\begin{aligned}
\phi^*\left(x^i z dx\right) &= x^{pi} \phi(z) d(x^p) \\
&= p x^{pi+p-1} z^p \left(\sum_{k=0}^{\infty} \binom{-1/2}{k} (\phi_K(f)(x^p) - f(x)^p)^k z^{2pk}\right) dx.
\end{aligned}$$

Remark 2.2. Note that one needs $z = y^{-1}$ as an element of $A^\dagger$, which explains why we compute with C' instead of C.

Remark 2.3. For ease of exposition, we describe all of our algorithms as if it were possible to compute exactly in $A^\dagger$. This is not possible for two reasons: the elements of $A^\dagger$ correspond to infinite series, and the coefficients of these series are polynomials with p-adic coefficients. In practice, each computation will be made with suitable p-adic approximations of the truly desired quantities, so one must keep track of how much p-adic precision is needed in these estimates in order for the answers to bear a certain level of p-adic accuracy.

2.3. The algorithm

Now we describe how to carry out Kedlaya's algorithm. Begin by letting

$$G(x) = \frac{\phi_K(f)(x^p) - (f(x))^p}{p}.$$

Then the action of Frobenius on each of the basis elements in (1) is easily calculated from

$$F_i := \phi^* \left(x^i z dx\right) = \sum_{0 \le k < N'} \left(\binom{-1/2}{k} p^{k+1} G^k x^{p(i+1)-1} z^{(2k+1)p-1} \right) z dx, \tag{2}$$

as an element of $K[x,y,z]/(y^2 - f(x), yz-1)$, with a precision of N p-adic digits, where N' is the smallest integer such that

$$N' - \lfloor \log_p(2N'+1) \rfloor \ge N.$$

The $2g$ differentials in (1) span $H^1_{\mathrm{MW}}(C')^-$, so we are able to write an arbitrary element in $(A^-)^\dagger \frac{zdx}{2}$ (where $A^- = \bigoplus_{0 \le i < 2g+1, j \equiv 1(2)} K x^i z^j$) as a linear combination of $d(x^i z^j)$ and (1); that is, we first compute the action of Frobenius on each basis differential, resulting in (2), and then re-express (2) in terms of a linear combination of (1) and an exact differential (given by a linear combination of appropriate $d(x^i z^j)$). This reduction process, which allows us to write $\omega \in (A^-)^\dagger \frac{zdx}{2}$ as

$$\omega = dh + c_0 \omega_0 + \cdots + c_{2g-1} \omega_{2g-1}, \tag{3}$$

is known as Kedlaya's algorithm.

For the purposes of the reduction algorithm, the following definition is helpful:

Definition 2.4. Given a multivariate polynomial $g(x,y,z)$ in $K[x,y,z]/(y^2 - f(x), yz-1)$, the *highest* monomial of g is the one with smallest power of z and largest power of x.

Example 2.5. Let $y^2 = f(x) = x^3 - x + \frac{1}{4}$. The highest monomial of

$$d(x^i z^j) = (2ix^{i-1}z^{j-1} - 3jx^{i+2}z^{j+1} + jx^i z^{j+1}) \frac{zdx}{2}$$

is $x^{i-1}z^{j-1}$ if $1 \le i < 3$ and $x^2 z^{j+1}$ if $i = 0$.

We now give the reduction algorithm.

Algorithm 1 Kedlaya's algorithm

Input: The basis of differentials $\{\omega_i = x^i z dx\}_{i=0}^{2g-1}$.

Output: The $2g \times 2g$ matrix M of a p-power lift of Frobenius ϕ, as well as functions $f_i \in A^\dagger$ such that $\phi^*(\omega_i) = df_i + \sum_{j=0}^{2g-1} M_{ij}^t \omega_j$.

1. Begin by computing a list of differentials $d(x^i z^j)$, where $0 \leq i < 2g+1$ and $j \equiv 1 \pmod 2$.
2. For each i, compute $F_i = \phi^*(\omega_i)$ (see (2)) and group the resulting terms as $(\sum p^{k+1} c_{i,k,j} z^j) z dx$, where $c_{i,k,j} \in K[x]$ have degree less than or equal to $2g+1$.
3. If F_i has a term $(x^i z^j) z dx$ with $j > 0$, consider the term $(c_{i,k,j} z^j) z dx$ where j is maximal. Take the unique linear combination of the $d(x^k z^{j-1})$ such that when this linear combination is subtracted off of F_i, the resulting "F_i" no longer has terms of the form $(x^m z^j) z dx$. Repeat this process until F_i (or, in more precise terms, the resulting "F_i" at each step minus linear combinations of differentials) has no terms $(x^m z^j) z dx$ with $j > 0$.
4. If F_i has terms with $j \leq 0$, let $(x^m z^j) z dx$ be the term with the highest monomial of F_i. Let $(x^k z^l) z dx$ be the term such that $d(x^k z^l)$ has highest term $(x^m z^j) z dx$ and subtract off the appropriate multiple of $d(x^k z^l)$ such that the resulting F_i no longer has terms of the form $(x^m z^j) z dx$ with $j \neq 0$. Repeat this process until the resulting F_i is of the form $\left(M_{0i} + M_{1i} x + \cdots + M_{2g-1\,i} x^{2g-1}\right) z dx$.
5. For each i, return the expression

$$\phi^*(\omega_i) = df_i + \sum_{j=0}^{2g-1} M_{ij}^t \omega_j.$$

2.4. Example: Computing the matrix of Frobenius for "37.$a1''$ *at* $p = 5$

Let $p = 5$ and consider the elliptic curve with LMFDB label "37.$a1''$ [31, Elliptic Curve 37.a1] with minimal model $y^2 + y = x^3 - x$.

Step 1. Put the elliptic curve into Weierstrass form $y^2 = x^3 + a_4 x + a_6$, via the transformation

$$a_4 = -\frac{c_4}{2^4 \cdot 3}, \qquad a_6 = -\frac{c_6}{2^5 \cdot 3^3}.$$

In our case, we obtain the curve $y^2 = x^3 - x + \frac{1}{4}$. Let

$$f(x) = x^3 - x + \frac{1}{4}.$$

Step 2. Fix the precision N and compute N'. In our case, $N = 2$ and $N' = 3$.

Step 3. Compute the action of Frobenius on the two differentials $z dx$ and $xz dx$ as an element of $\mathbb{Z}_p[x,y,z]/(y^2 - f(x), yz - 1)$, with a precision of N digits. Furthermore, group the terms of $\phi^*(x^i z dx)$ as $\sum (p^{k+1} c_{i,k,j} z^j) z dx$, where the $c_{i,k,j}$ are in $\mathbb{Z}_p[x]$ of degree less than 3. In our case, we compute

$$F_0 = \phi^*(zdx) \equiv (5xz^2 + (5x+5x^2)z^4)zdx \pmod{25}$$
$$F_1 = \phi^*(xzdx) \equiv (10+10x+5x^3+(20+5x+15x^2)z^2+(10+20x+15x^2)z^4)zdx \pmod{25}.$$

Step 4. Now we must reduce the differentials. We want to write each of the

$$F_i = \phi^*(\omega_i)$$

as

$$(M_{0i}\omega_0 + M_{1i}\omega_1) + \sum d(x^l z^j) = (M_{0i} + M_{1i}x)\, zdx$$

in $H^1_{\mathrm{MW}}(C')^-$. We begin with

$$F_0 \equiv (5xz^2 + (5x+5x^2)z^4)zdx \pmod{25}$$

and compute the appropriate list of differentials:

i	j	$d(x^l z^j) \pmod{25}$
0	1	$(13z^2+11z^2x^2)zdx$
1	1	$(12+16z^2+24z^2x)zdx$
2	1	$(13x+16z^2x+24z^2x^2)zdx$
0	3	$(14z^4+8z^4x^2)zdx$
1	3	$(9z^2+23z^4+22z^4x)zdx$
2	3	$(10z^2x+23z^4x+22z^4x^2)zdx$

Thus we wish to write $(5x+5x^2)z^4$ as a linear combination of $14z^4+8z^4x^2$, $23z^4+22z^4x$, and $23z^4x+22z^4x^2$, all modulo 25 (we may ignore the lower powers of z present in the differentials, as we will take care of them in the steps to come). We find that taking

$$F_0 - 5d(z^3) - 10d(xz^3) - 20d(x^2z^3) \pmod{25}$$

leaves us with

$$(10+5x)z^2\, zdx.$$

Now we wish to write $(10+5x)z^2$ as a linear combination of $13z^2+11z^2x^2$, $16z^2+24z^2x$, and $16z^2x+24z^2x^2$, modulo 25. We find that taking

$$(10+5x)z^2\, zdx - 10d(z) - 5d(xz) - 10d(x^2z)$$

leaves us with

$$(15+20x)zdx.$$

Next, we reduce

$$F_1 \equiv (10+10x+5x^3+(20+5x+15x^2)z^2+(10+20x+15x^2)z^4)zdx \pmod{25}.$$

Note that this has an $x^3\,z\,dx$ term, so we take care of this first:

$$F_1 - \frac{1}{3}d(x^4 z) = (13 + 2x + (13 + 10x + 7x^2)z^2 + (10 + 20x + 15x^2)z^4)\; z\,dx.$$

Now we proceed as in the case of F_0, and we wish to write $(10 + 20x + 15x^2)z^4$ as a linear combination of $14z^4 + 8z^4x^2$, $23z^4 + 22z^4x$, and $23z^4x + 22z^4x^2$, all modulo 25. We find that taking

$$(13+2x+13z^2+10z^2x+7z^2x^2+10z^4+20z^4x+15z^4x^2)z\,dx - 10d(z^3) - 15d(xz^3) - 5d(x^2z^3)$$

leaves us with

$$(13 + 2x + (3 + 10x + 7x^2)z^2)\; z\,dx.$$

Finally, we wish to write $(3 + 10x + 7x^2)z^2$ as a linear combination of $13z^2 + 11z^2x^2$, $16z^2 + 24z^2x$, and $16z^2x + 24z^2x^2$, all modulo 25. We find that taking

$$(13 + 2x + (3 + 10x + 7x^2)z^2\; z\,dx - 20d(z) - 23d(xz) - 13d(x^2z)$$

leaves us with

$$(12 + 8x)z\,dx.$$

Step 5. Now we form the matrix M of the reduced differentials, where each reduced differential gives us a column in the matrix of Frobenius. In our case, we have

$$M = \begin{pmatrix} 15 & 12 \\ 20 & 8 \end{pmatrix} \pmod{25}. \tag{4}$$

Moreover, we have that

$$\phi^*(\omega_0) = d(5z^3 + 10xz^3 + 20x^2z^3 + 10z + 5xz + 10x^2z) + M_{00}\omega_0 + M_{10}\omega_1$$
$$\phi^*(\omega_1) = d\left(\frac{1}{3}x^4z + 10z^3 + 15xz^3 + 5x^2z^3 + 20z + 23xz + 13x^2z\right) + M_{10}\omega_0 + M_{11}\omega_1.$$

Recall that the characteristic polynomial of p-power Frobenius on an elliptic curve E is $x^2 - a_p x + p$, where $a_p = p + 1 - \#E(\mathbb{F}_p)$. As a consistency check, we can compute the trace and determinant of M: we see that M has trace 23, which, modulo 25, is congruent to $a_5 = -2$ and determinant -120, which is $p = 5$ modulo 25.

Remark 2.6. Note that running this example in `Sage` [40] yields slightly different results:

```
sage: EllipticCurve('37.a1').matrix_of_frobenius(5,2)
[3*5 + 5^2 + O(5^3)   3 + 4*5 + O(5^2)]
[  5 + 5^2 + O(5^3)     3 + 5 + O(5^2)]
```

That is, Sage computes the matrix of Frobenius to be $\begin{pmatrix} 15 & 23 \\ 5 & 8 \end{pmatrix} \pmod{25}$.

Why this discrepancy? This is because the Sage implementation of `matrix_of_frobenius` is internally computing the matrix of Frobenius on "37.a1" using a different model of the elliptic curve: $y^2 = x^3 - 16x + 16$ rather than the model $y^2 = x^3 - x + \frac{1}{4}$.

Note that the matrix produced by Sage also has trace 23 mod 25 and determinant 5 mod 25. By adjusting the internals of `matrix_of_frobenius` to take in a different model or by telling Sage that the curve is a hyperelliptic curve, it is not difficult to check Sage's computation of the matrix of Frobenius of $y^2 = x^3 - x + \frac{1}{4}$:

```
sage: R.<x> = QQ['x']
sage: H = HyperellipticCurve(x^3 - x + 1/4)
sage: H.matrix_of_frobenius(5,2)
[    3*5 + O(5^2) 2 + 2*5 + O(5^2)]
[    4*5 + O(5^2)   3 + 5 + O(5^2)]
```

which indeed agrees with our computation (4) above.

2.5. Generalizations and improvements

Kedlaya's algorithm has since been generalized to arbitrary hyperelliptic curves (over fields of even characteristic [21], even degree models [24]), superelliptic curves [23], as well as more generally to *nondegenerate curves* [13]. The original algorithm has linear runtime dependence on the prime p; Harvey [25] gave a variant of this algorithm for hyperelliptic curves which reduced this to $p^{1/2}$. Recently, Minzlaff [36], building on the work of [25,23], produced the analogous algorithm for superelliptic curves.

3. Coleman integration

In the 1980s, Coleman formulated a p-adic theory of path integration [15,17,19]. This integration theory, now known as *Coleman integration*, has numerous applications in arithmetic geometry. At the end of the next section, we describe a variation on the method of Chabauty-Coleman [16] to find rational points on curves. For more about the method of Chabauty-Coleman, see Siksek's lectures in this volume. For a modern overview of the integration theory, see [12].

A key part of Coleman's construction is *analytic continuation along Frobenius*: using Frobenius to fix the global constant of integration throughout the domain of integration. In [7], this construction was made explicit by using Kedlaya's algorithm and was used to give algorithms to compute single Coleman integrals on odd degree models of hyperelliptic curves. We describe the results of [7] in this section. For similar results in the case of even degree models of hyperelliptic curves, see [2].

3.1. Tiny Coleman integrals and local coordinates

Here we describe how to compute single Coleman integrals on a hyperelliptic curve. We retain our notation from §2. Suppose we are given points $P, Q \in C(K)$, and a positive

integer m such that the residue fields of P,Q are contained in $\mathbb{F}_{p^m}$. We fix the basis of $H^1_{MW}(C')^-$ to be

$$\omega_i = x^i \frac{dx}{2y} \quad (i = 0, \ldots, 2g-1). \tag{5}$$

We restrict to considering odd 1-forms, those negated by the hyperelliptic involution, since even 1-forms can be integrated directly in terms of x, as in Proposition 1 of [7]. Since every odd 1-form ω can be written in the form

$$\omega = dh + \sum_{i=0}^{2g-1} c_i \omega_i \tag{6}$$

by Kedlaya's algorithm (Algorithm 1), we focus our attention on computing the integrals of basis differentials.

A few definitions are in order. Let $C_{\mathbb{Q}}$ denote the generic fiber of C as a rigid analytic space, and let $\overline{C}$ denote the special fiber of C. There is a natural reduction map from $\mathbb{C}_{\mathbb{Q}}$ to $\overline{C}$. The inverse image of any point of $\overline{C}$ is a subspace of $\mathbb{C}_{\mathbb{Q}}$ isomorphic to an open unit disk. We call such a disk a *residue disk* of C.

Algorithms for computing definite Coleman integrals differ based on the residue disks of the endpoints of integration: the first consideration is whether the endpoints lie in the same residue disk. If the endpoints do not lie in the same residue disk, we will further distinguish cases based on whether the residue disks correspond to non-Weierstrass or Weierstrass points. Since we will often distinguish between such residue disks, we will refer to *non-Weierstrass residue disks* and *Weierstrass residue disks* of C, corresponding to non-Weierstrass and Weierstrass points of $\overline{C}$.

When P,Q are in the same residue disk, computing the Coleman integral is accomplished by a "tiny integral": computing a parametrization of the path between P,Q and using change of variables to integrate along that path. For this, we introduce algorithms to compute local coordinates. Let $K(C)$ denote the field of rational functions of C. Recall that a *local parameter* or a *local coordinate* at a $\overline{K}$-rational point P is a function $t \in K(C)$ such that $\mathrm{ord}_P(t) = 1$.

Here we record our local coordinate algorithms:

Algorithm 2 Local coordinate at a point in a non-Weierstrass residue disk
Input: A point $P = (a,b)$ in $C(K)$ in a non-Weierstrass residue disk and precision n.
Output: A parametrization $(x(t), y(t))$ at P in terms of a local coordinate.

---

1. Let $x(t) = t + a$, where t is a local coordinate.
2. Solve for $y(t) = \sqrt{f(x(t))}$ by Newton's method: take $y_0(t) = b$, then set

$$y_i(t) = \frac{1}{2}\left(y_{i-1}(t) + \frac{f(x(t))}{y_{i-1}(t)}\right), \quad i \geq 1$$

with $y_i(t) \to y(t)$. The number of iterates i to be taken depends on the necessary power series precision; for precision $O(t^n)$, one can take i to be $\lceil \log_2 n \rceil$.

Algorithm 3 Local coordinate at a point in a finite Weierstrass residue disk
Input: A point $P=(a,b)$ in $C(K)$ in a finite Weierstrass residue disk and precision n.
Output: A parametrization $(x(t),y(t))$ at P in terms of a local coordinate.

1. Let $y(t)=t+b$, where t is a local coordinate.
2. Iteratively solve for $x(t)$ as follows: take $x_0(t)=a$; then Newton's method yields

$$x_i(t)=x_{i-1}(t)-\frac{f(x_{i-1}(t))-y(t)^2}{f'(x_{i-1}(t))},\quad i\geq 1$$

with $x_i(t)\to x(t)$. The number of iterates i to be taken depends on the necessary power series precision; for precision $O(t^n)$, one can take i to be $\lceil \log_2 n\rceil$.

Finally for the case of infinity, since $y^2=f(x)$, where $\deg f(x)=2g+1$, we have that x has a pole of order 2 at ∞, while y has a pole of order $2g+1$ at ∞. Let $t=\frac{x^g}{y}$ be the local parameter at ∞. To find the parametrization, we do as follows:

Algorithm 4 Local coordinate at infinity
Input: The point P_∞ above $x=\infty$ on C and precision n.
Output: A local coordinate $(x(t),y(t))$ at P_∞ such that t has a zero at ∞.

1. Take $x_0=t^{-2}$, let $h(x,t)=\left(\frac{x^g}{t}\right)^2-f(x)$ and compute $h'(x,t)=\frac{\partial h(x,t)}{\partial x}$. Newton's method yields

$$x_i(t)=x_{i-1}(t)-\frac{h(x_{i-1}(t),t)}{h'(x_{i-1}(t),t)},\quad i\geq 1$$

with $x_i(t)\to x(t)$. The number of iterates i to be taken depends on the necessary power series precision; for n digits of precision in t, i can be taken to be $\lceil \log_2 n\rceil$.
2. Take $y(t)=\frac{(x(t))^g}{t}$.

Example 3.1. Let C be the hyperelliptic curve

$$y^2=x(x-2)(x+2)(x+3)(x+7),$$

as in Müller's lectures in this volume, and consider the points $P_1=(-1,6)$ and $P_2=(-4,12)$ on C. Using `Sage`, we can compute a parametrization $(x(t),y(t))$ at P_1 in terms of a local coordinate t:

$$\begin{aligned}x(t)&=-1+t,\\ y(t)&=6+t-\frac{7}{2}t^2-\frac{1}{2}t^3-\frac{25}{48}t^4-\frac{35}{288}t^5-\frac{263}{864}t^6+O(t^7).\end{aligned}$$

Similarly, at P_2, we have

$$x(t) = -4+t,$$
$$y(t) = 12 - \frac{19}{2}t - \frac{19}{32}t^2 + \frac{61}{256}t^3 - \frac{5965}{24576}t^4 - \frac{81805}{589824}t^5 - \frac{3515573}{28311552}t^6 + O(t^7).$$

At the Weierstrass point (2,0), we have

$$x(t) = 2 + \frac{1}{360}t^2 - \frac{191}{23328000}t^4 + \frac{7579}{188956800000}t^6 + O(t^7),$$
$$y(t) = t.$$

At ∞, we have

$$x(t) = t^{-2} - 10 - 17t^2 - 130t^4 - 1105t^6 + O(t^7)$$
$$y(t) = t^{-5} + -20t^{-3} + 66t^{-1} + 80t + 679t^3 + O(t^4).$$

We now use these local coordinate algorithms to compute "tiny" Coleman integrals. We refer to any Coleman integral of the form $\int_P^Q \omega$ in which P, Q lie in the same residue disk (Weierstrass or not) as a *tiny integral*. As an easy first case, we give an algorithm to compute tiny integrals of basis differentials.

Algorithm 5 Tiny Coleman integrals
Input: Points $P, Q \in C(K)$ in the same residue disk and a basis differential ω_i without poles in the disk.
Output: The integral $\int_P^Q \omega_i$.

---

1. Using the relevant algorithm (Algorithm 2, 3 or 4), compute a parametrization $(x(t), y(t))$ at P in terms of a local coordinate t.
2. Formally integrate the power series in t:

$$\int_P^Q \omega_i = \int_P^Q x^i \frac{dx}{2y} = \int_0^{t(Q)} \frac{x(t)^i}{2y(t)} \frac{dx(t)}{dt} dt.$$

One useful computation of tiny integrals involves the *Teichmüller point* in a non-Weierstrass residue disk.

Example 3.2. Let C be the hyperelliptic curve

$$y^2 = x(x-2)(x+2)(x+3)(x+7)$$

as in Example 3.1 and let $K = \mathbb{Q}_{13}$. We consider $P_2 = (-4, 12) \in C(K)$.

The *Teichmüller point* T in the residue disk of P_2 is the point fixed by Frobenius ϕ: that is, $\phi(T) = T$, and $x(T) \equiv x(P_2) \pmod{13}, y(T) \equiv y(P_2) \pmod{13}$. We can find the Teichmüller point by taking the Teichmüller lift of $x(P_2)$ and then using the equation of the curve to solve for the y-coordinate, choosing the correct "sign" of the square root by considering $y(P_2) \pmod{13}$. We find that the Teichmüller point in the disk of P_2 is

$$T = (9 + 13 + 6\cdot 13^2 + 3\cdot 13^3 + 5\cdot 13^4 + 10\cdot 13^5 + 8\cdot 13^6 + 8\cdot 13^7 + O(13^8),$$
$$12 + 7\cdot 13 + 2\cdot 13^2 + 13^3 + 6\cdot 13^4 + 5\cdot 13^5 + 2\cdot 13^6 + 6\cdot 13^7 + O(13^8)).$$

Example 3.3. Let C be the hyperelliptic curve

$$y^2 = x(x-2)(x+2)(x+3)(x+7)$$

as in Example 3.1, and let $K = \mathbb{Q}_{13}$. We consider $P_2 = (-4, 12) \in C(K)$ and the Teichmüller point in its residue disk, computed in Example 3.2. Using the local coordinate at P_2 computed in Example 3.1, we compute the integral of ω_0 between P_2 and T:

$$\int_{P_2}^{T} \omega_0 = 12\cdot 13 + 11\cdot 13^2 + 3\cdot 13^3 + 4\cdot 13^4 + 13^5 + 11\cdot 13^6 + 3\cdot 13^7 + O(13^8).$$

3.2. Single Coleman integrals

To consider more general integrals, we recall a theorem of Coleman. Let ω be a 1-form, with $(\omega)_\infty$ denoting its polar support. For $P, Q \in C(K)$, Coleman showed in [17] the existence of the definite integral $\int_P^Q \omega \in K$ with the following properties.

Theorem 3.4. *Let ω, η be 1-forms on C and $P, Q, R \in C(K)$. The definite Coleman integral has the following properties:*

1. *Linearity: $\int_P^Q (a\omega + b\eta) = a\int_P^Q \omega + b\int_P^Q \eta$, for $P, Q \notin (\omega)_\infty \cup (\eta)_\infty$.*
2. *Additivity: $\int_P^R \omega = \int_P^Q \omega + \int_Q^R \omega$, for $P, Q, R \notin (\omega)_\infty$.*
3. *Change of variables: The Coleman integral can also be defined on certain subdomains on the curve, called* wide open spaces. *If $U \subset C$ is a wide open space, $U' \subset C'$ is another such space, and $\phi : U \to U'$ a* rigid analytic map *between these wide opens, then $\int_P^Q \phi^* \omega = \int_{\phi(P)}^{\phi(Q)} \omega$.*
4. *Fundamental theorem of calculus: $\int_P^Q df = f(Q) - f(P)$ for a meromorphic function f on a wide open subset.*

Proof. See [17, Thm 2.3, Prop 2.4, Thm 2.7] for details. □

Remark 3.5. Note that the lift of p-power Frobenius as in §2 is a rigid analytic map.

Now we may compute integrals of the form $\int_P^Q \omega_i$ in which $P, Q \in C(K)$ lie in distinct non-Weierstrass residue disks. To do this, we use Dwork's principle of analytic continuation along Frobenius, in the form of Kedlaya's algorithm (Algorithm 1).

Algorithm 6 Coleman integration in non-Weierstrass disks

Input: The basis differentials $(\omega_i)_{i=0}^{2g-1}$, points $P,Q \in C(K)$ in non-Weierstrass residue disks, and a positive integer m such that the residue fields of P,Q are contained in $\mathbb{F}_{p^m}$.

Output: The integrals $\left(\int_P^Q \omega_i\right)_{i=0}^{2g-1}$.

1. Using Kedlaya's algorithm (Algorithm 1), calculate the action of the m-th power of Frobenius on each basis element:

$$(\phi^m)^* \omega_i = dh_i + \sum_{j=0}^{2g-1} M_{ij}^t \omega_j.$$

2. By changing variables and breaking up the path from P to Q, we obtain

$$(M^t - I) \begin{pmatrix} \vdots \\ \int_P^Q \omega_j \\ \vdots \end{pmatrix} = \begin{pmatrix} \vdots \\ h_i(P) - h_i(Q) - \int_P^{\phi^m(P)} \omega_i - \int_{\phi^m(Q)}^Q \omega_i \\ \vdots \end{pmatrix}. \tag{7}$$

Since the eigenvalues of the matrix M are algebraic integers of $\mathbb{C}$-norm $p^{m/2} \neq 1$ (see [26, §2]), the matrix $M^t - I$ is invertible, and we may solve (7) to obtain the integrals $\int_P^Q \omega_i$.

Remark 3.6. To compute the action of ϕ^m, first perform Algorithm 1 to write

$$\phi^* \omega_i = dg_i + \sum_{j=0}^{2g-1} B_{ij}^t \omega_j,$$

where B^t denotes the transpose of B, the matrix of p-power Frobenius. We compute the action of ϕ^m by iteratively computing the action of ϕ, using the vector of functions $\mathbf{g} = (g_i)$ and the matrix B above to write

$$(\phi^m)^* \omega_i = dh_i + \sum_{j=0}^{2g-1} M_{ij}^t \omega_j,$$

where

$$\mathbf{h} = \phi^{m-1}(\mathbf{g}) + \sum_{i=1}^{m-1} \phi_K^{m-1}(B^t) \cdots \phi_K^i(B^t) \phi^{i-1}(\mathbf{g})$$

$$M^t = \phi_K^{m-1}(B^t) \cdots \phi_K(B^t) B^t. \tag{8}$$

Remark 3.7. We obtain (7) as follows. By change of variables,

$$\begin{aligned}\int_{\phi^m(P)}^{\phi^m(Q)} \omega_i &= \int_P^Q (\phi^m)^* \omega_i \\ &= \int_P^Q (dh_i + \sum_{j=0}^{2g-1} M_{ij}^t \omega_j) \\ &= h_i(Q) - h_i(P) + \sum_{j=0}^{2g-1} M_{ij}^t \int_P^Q \omega_j.\end{aligned}$$

Adding $\int_P^{\phi^m(P)} \omega_i + \int_{\phi^m(Q)}^Q \omega_i$ to both sides of this equation yields

$$\int_P^Q \omega_i = \int_P^{\phi^m(P)} \omega_i + \int_{\phi^m(Q)}^Q \omega_i + h_i(Q) - h_i(P) + \sum_{j=0}^{2g-1} M_{ij}^t \int_P^Q \omega_j,$$

which is equivalent to (7).

Finally, given an arbitrary odd differential ω, we use the previous algorithms, linearity, and the fundamental theorem of calculus to recover the integral of ω between non-Weierstrass points P and Q:

Algorithm 7 Coleman integral of an odd ω
Input: Non-Weierstrass points $P, Q \in C(K)$ and an odd differential ω holomorphic outside Weierstrass disks.
Output: The integral $\int_P^Q \omega$.

---

1. Use Kedlaya's algorithm (Algorithm 1) to write ω in the form

$$\omega = dh + c_0\omega_0 + \cdots + c_{2g-1}\omega_{2g-1}$$

2. For each ω_i, compute $\int_P^Q \omega_i$.
3. Use the fundamental theorem of calculus and linearity to obtain the integral

$$\int_P^Q \omega = h(Q) - h(P) + c_0 \int_P^Q \omega_0 + \cdots + c_{2g-1} \int_P^Q \omega_{2g-1}.$$

We now consider the case where P, Q lie in different residue disks, at least one of which is Weierstrass. Note that because a differential ω of the form (6) is not meromorphic on Weierstrass residue disks, we cannot always define $\int_P^Q \omega$. To ease exposition, we will assume that ω is everywhere meromorphic, with no poles in the residue disks of P and Q. For the case where ω is allowed a simple pole in one of the relevant residue disks, see [6].

First, we show how having a Weierstrass endpoint can simplify the computation of single Coleman integrals.

Lemma 3.8. *Let $P, Q \in C(K)$, with P a Weierstrass point. Let ω be an odd, everywhere meromorphic differential on C with no poles in the residue disks of P and Q. Then for*

ι the hyperelliptic involution, $\int_P^Q \omega = \frac{1}{2}\int_{\iota(Q)}^Q \omega$. In particular, if Q is also a Weierstrass point, then $\int_P^Q \omega = 0$.

Proof. Let $I := \int_P^Q \omega = \int_P^{\iota(Q)}(-\omega) = \int_{\iota(Q)}^P \omega$. Then by additivity in the endpoints, we have $\int_{\iota(Q)}^Q \omega = 2I$, from which the result follows. □

More generally, if P belongs to a finite Weierstrass residue disk while Q does not, we can find the characteristic zero Weierstrass point P' in the disk of P, then apply Lemma 3.8 to yield $\int_P^Q \omega = \int_P^{P'} \omega + \frac{1}{2}\int_{\iota(Q)}^Q \omega$.

It is worth noting that the strategy of Lemma 3.8 does not necessarily generalize to higher n-fold iterated Coleman integrals: in particular, a double integral of basis differentials between two Weierstrass points can be nonzero! For an example of this, see [3, Example 7.14].

With that in mind, we continue by describing a different approach for computing Coleman integrals with an endpoint in a Weierstrass disk; this approach does generalize to iterated Coleman integrals. We may reduce to the case where P lies in a Weierstrass residue disk but Q does not, since we can always write $\int_P^Q \omega = \int_P^R \omega + \int_R^Q \omega$ for an auxiliary point R in a non-Weierstrass residue disk.

To carry out Algorithm 6, one must be able to evaluate the function f_i (an element of $A^\dagger$) on each of the endpoints of integration. In particular, while f_i does not necessarily converge at P, it does converge at any point S near the boundary of the disk. To use this observation, we break up the path between P and Q using S, writing $\int_P^Q \omega_i = \int_P^S \omega_i + \int_S^Q \omega_i$ for suitable S in the disk of P. Then the integral between P and S can be computed using a tiny integral, and the integral from S to Q can be computed using Algorithm 6, which by construction, now has the aforementioned function f_i converging on both endpoints. However, note that this approach is computationally quite expensive, since by requiring S to be near the boundary of its residue disk, S must be defined over a highly ramified extension of $\mathbb{Q}_p$. We have the following algorithms:

Algorithm 8 Finding a near-boundary point in a finite Weierstrass disk
Input: A finite Weierstrass point $P \in C(\mathbb{Q}_p)$, and a positive integer d.
Output: A point $S = (x(p^{1/d}), p^{1/d})$ in the disk of P defined over the totally ramified extension $\mathbb{Q}_p(p^{1/d})$.

1. Compute a parametrization $(x(t),t)$ at P in terms of the local coordinate t.
2. Evaluate the parametrization at $t = p^{1/d}$. This is S.

Algorithm 9 Coleman integration in a finite Weierstrass disk
Input: A finite Weierstrass point P, a positive integer d, a non-Weierstrass point Q, and a basis differential ω_i.
Output: The integral $\int_P^Q \omega_i$.

1. Use Algorithm 8 to find S. Keep the local coordinate $(x(t),t)$ at P.
2. Compute $\int_P^S \omega_i$ as a tiny integral: $\int_P^S \omega_i = \int_0^{p^{1/d}} \frac{x(t)^i dx(t)}{2t} dt$.
3. Use Algorithm 6 to compute $\int_S^Q \omega_i$.
4. Use additivity in endpoints to recover $\int_P^Q \omega_i = \int_P^S \omega_i + \int_S^Q \omega_i$.

Example 3.9. We compute Coleman integrals on our running genus 2 curve (see Examples 3.1-3.3) given by

$$C : y^2 = x(x-2)(x+2)(x+3)(x+7)$$

over $K = \mathbb{Q}_{13}$. Consider $P_1 = (-1,6), P_2 = (-4,12), P_3 = (3,30)$, and $\iota(P_3) = (3,-30)$ in $C(K)$. Using Algorithm 6, we compute the following Coleman integrals on basis differentials:

$$\begin{pmatrix} \int_{P_3}^{P_1} \omega_0 \\ \int_{P_3}^{P_1} \omega_1 \\ \int_{P_3}^{P_1} \omega_2 \\ \int_{P_3}^{P_1} \omega_3 \end{pmatrix} = \begin{pmatrix} 2\cdot 13 + 6\cdot 13^3 + 13^4 + 5\cdot 13^5 + 11\cdot 13^6 + 3\cdot 13^7 + O(13^8) \\ 10\cdot 13 + 6\cdot 13^2 + 8\cdot 13^4 + 10\cdot 13^5 + 4\cdot 13^6 + 10\cdot 13^7 + O(13^8) \\ 5 + 7\cdot 13 + 8\cdot 13^2 + 13^3 + 3\cdot 13^4 + 5\cdot 13^5 + 9\cdot 13^6 + 7\cdot 13^7 + O(13^8) \\ 6 + 6\cdot 13 + 4\cdot 13^2 + 2\cdot 13^3 + 4\cdot 13^4 + 12\cdot 13^5 + 9\cdot 13^6 + 2\cdot 13^7 + O(13^8) \end{pmatrix},$$

$$\begin{pmatrix} \int_{\iota(P_3)}^{P_2} \omega_0 \\ \int_{\iota(P_3)}^{P_2} \omega_1 \\ \int_{\iota(P_3)}^{P_2} \omega_2 \\ \int_{\iota(P_3)}^{P_2} \omega_3 \end{pmatrix} = \begin{pmatrix} 3\cdot 13 + 4\cdot 13^2 + 12\cdot 13^3 + 2\cdot 13^4 + 12\cdot 13^5 + 10\cdot 13^6 + 12\cdot 13^7 + O(13^8) \\ 6\cdot 13^2 + 9\cdot 13^3 + 2\cdot 13^4 + 10\cdot 13^5 + 12\cdot 13^6 + 8\cdot 13^7 + O(13^8) \\ 3 + 7\cdot 13 + 12\cdot 13^2 + 10\cdot 13^3 + 6\cdot 13^4 + 2\cdot 13^5 + 2\cdot 13^6 + 3\cdot 13^7 + O(13^8) \\ 8 + 9\cdot 13 + 8\cdot 13^2 + 4\cdot 13^3 + 3\cdot 13^4 + 6\cdot 13^5 + 2\cdot 13^6 + 9\cdot 13^7 + O(13^8) \end{pmatrix}.$$

3.3. Iterated Coleman integrals

Coleman's theory of integration is not limited to single integrals; it gives rise to an entire class of locally analytic functions, the *Coleman functions*, on which antidifferentiation is well-defined. In other words, one can define n-fold iterated p-adic integrals [11,15]

$$\int_P^Q \xi_n \cdots \xi_1$$

which behave formally like iterated path integrals

$$\int_0^1 \int_0^{t_1} \cdots \int_0^{t_{n-1}} f_n(t_n) \cdots f_1(t_1)\, dt_n \cdots dt_1.$$

Kedlaya's algorithm can also be applied to compute these iterated Coleman integrals. We give an overview of these methods, following [3].

We set the following notation

$$\int_P^Q \xi_1 \xi_2 \cdots \xi_{n-1} \xi_n := \int_P^Q \xi_1(R_1) \int_P^{R_1} \xi_2(R_2) \cdots \int_P^{R_{n-2}} \xi_{n-1}(R_{n-1}) \int_P^{R_{n-1}} \xi_n,$$

for a collection of dummy parameters $R_1, \ldots, R_{n-1}$ and 1-forms $\xi_1, \ldots, \xi_n$.

We begin with an algorithm to compute tiny iterated integrals.

Algorithm 10 Tiny iterated integrals
Input: Points $P, Q \in C(K)$ in the same residue disk (neither equal to the point at infinity) and differentials $\xi_1, \ldots, \xi_n$ without poles in the disk of P.
Output: The integral $\int_P^Q \xi_1 \xi_2 \cdots \xi_n$.

1. Compute a parametrization $(x(t), y(t))$ at P in terms of a local coordinate t, using Algorithm 2 or 3.
2. For each k, write $\xi_k(x,y)$ in terms of t: $\xi_k(t) := \xi_k(x(t), y(t))$.
3. Let $I_{n+1}(t) := 1$.
4. Compute, for $k = n, \ldots, 2$, in descending order,

$$\begin{aligned} I_k(t) &= \int_P^{R_{k-1}} \xi_k I_{k+1} \\ &= \int_0^{t(R_{k-1})} \xi_k(u) I_{k+1}(u), \end{aligned}$$

   with R_{k-1} in the disk of P.
5. Upon computing $I_2(t)$, we arrive at the desired integral:

$$\int_P^Q \xi_1 \xi_2 \cdots \xi_n = I_1(t) = \int_0^{t(Q)} \xi_1(u) I_2(u).$$

For ease of exposition, we focus on the case of $n = 2$ and assume $P, Q \in C(\mathbb{Q}_p)$ when discussing the iterated analogue of the fundamental linear system (Algorithm 11). First, we need an analogue of "additivity in endpoints" (Theorem 3.4(2)) for double integrals. Let P' and Q' be in the disks of P and Q, respectively.

Lemma 3.10 (Link lemma for double integrals)**.** *Suppose we have two differential* 1*-forms* ξ_0, ξ_1*. Then we have*

$$\int_P^Q \xi_0 \xi_1 = \int_P^{P'} \xi_0 \xi_1 + \int_{P'}^{Q'} \xi_0 \xi_1 + \int_{Q'}^{Q} \xi_0 \xi_1 + \int_P^{P'} \xi_1 \int_{P'}^{Q} \xi_0 + \int_{P'}^{Q'} \xi_1 \int_{Q'}^{Q} \xi_0.$$

Using Lemma 3.10, we may link double integrals between different residue disks:

$$\int_P^Q \omega_i \omega_k = \int_P^{P'} \omega_i \omega_k + \int_{P'}^{Q'} \omega_i \omega_k + \int_{Q'}^{Q} \omega_i \omega_k + \int_P^{P'} \omega_k \int_{P'}^{Q} \omega_i + \int_{P'}^{Q'} \omega_k \int_{Q'}^{Q} \omega_i. \quad (9)$$

We can directly compute double integrals using a linear system. Indeed, using Lemma 3.10, we take $\phi(P)$ and $\phi(Q)$ to be the points in the disks of P and Q, respectively, which gives

$$\int_P^Q \omega_i \omega_k = \int_P^{\phi(P)} \omega_i \omega_k + \int_{\phi(P)}^{\phi(Q)} \omega_i \omega_k + \int_{\phi(Q)}^{Q} \omega_i \omega_k + \int_P^{\phi(P)} \omega_k \int_{\phi(P)}^{Q} \omega_i + \int_{\phi(P)}^{\phi(Q)} \omega_k \int_{\phi(Q)}^{Q} \omega_i. \quad (10)$$

Then we expand the following

$$\int_{\phi(P)}^{\phi(Q)} \omega_i\omega_k = \int_P^Q \phi^*(\omega_i\omega_k) = \int_P^Q \phi^*(\omega_i)\phi^*(\omega_k) \tag{11}$$

$$= \int_P^Q (df_i + \sum_{j=0}^{2g-1} M_{ij}^t \omega_j)(df_k + \sum_{j=0}^{2g-1} M_{kj}^t \omega_j) \tag{12}$$

$$= c_{ik} + \int_P^Q \left(\sum_{j=0}^{2g-1} M_{ij}^t \omega_j\right)\left(\sum_{j=0}^{2g-1} M_{kj}^t \omega_j\right), \tag{13}$$

where

$$c_{ik} = \int_P^Q df_i(R)(f_k(R)) - f_k(P)(f_i(Q) - f_i(P)) + \int_P^Q \sum_{j=0}^{2g-1} M_{ij}^t \omega_j(R)(f_k(R) - f_k(P))$$
$$+ f_i(Q)\int_P^Q \sum_{j=0}^{2g-1} M_{kj}^t \omega_j - \int_P^Q f_i(R)(\sum_{j=0}^{2g-1} M_{kj}^t \omega_j(R)).$$

Putting together (10) and (11), we get

$$\begin{pmatrix} \vdots \\ \int_P^Q \omega_i\omega_k \\ \vdots \end{pmatrix} = (I_{4g^2\times 4g^2} - (M^t)^{\otimes 2})^{-1} \begin{pmatrix} \vdots \\ c_{ik} - \int_{\phi(P)}^P \omega_i\omega_k - \left(\int_P^Q \omega_i\right)\left(\int_{\phi(P)}^P \omega_k\right) \\ - \left(\int_Q^{\phi(Q)} \omega_i\right)\left(\int_{\phi(P)}^{\phi(Q)} \omega_k\right) + \int_{\phi(Q)}^Q \omega_i\omega_k \\ \vdots \end{pmatrix}. \tag{14}$$

This gives us the following algorithm:

Algorithm 11 Double Coleman integration between non-Weierstrass endpoints

Input: The basis differentials $(\omega_i)_{i=0}^{2g-1}$, points $P,Q \in C(\mathbb{Q}_p)$ in non-Weierstrass residue disks or in Weierstrass disks in the region of convergence.

Output: The double integrals $\left(\int_P^Q \omega_i\omega_j\right)_{i,j=0}^{2g-1}$.

---

1. Use Algorithm 6 to compute the single integrals $\int_P^Q \omega_i, \int_{\phi(P)}^{\phi(Q)} \omega_i$ for all i.
2. Use Algorithm 10 to compute $\int_{\phi(P)}^P \omega_i\omega_k, \int_{\phi(Q)}^Q \omega_i\omega_k$ for all i,k
3. Compute the constants c_{ik} for all i,k using single integrals.
4. Recover the double integrals using the linear system

$$\begin{pmatrix} \vdots \\ \int_P^Q \omega_i\omega_k \\ \vdots \end{pmatrix} = (I_{4g^2\times 4g^2} - (M^t)^{\otimes 2})^{-1} \begin{pmatrix} \vdots \\ c_{ik} - \int_{\phi(P)}^P \omega_i\omega_k - \left(\int_P^Q \omega_i\right)\left(\int_{\phi(P)}^P \omega_k\right) \\ - \left(\int_Q^{\phi(Q)} \omega_i\right)\left(\int_{\phi(P)}^{\phi(Q)} \omega_k\right) + \int_{\phi(Q)}^Q \omega_i\omega_k \\ \vdots \end{pmatrix}.$$

---

4. p-adic height pairings

Much like the canonical (Néron-Tate) height pairing plays a crucial role in the arithmetic of abelian varieties number fields, so do *p-adic height pairings* [33,39,38]. Throughout this section, we assume that $p \geq 5$ is a prime of good and *ordinary* reduction.

4.1. p-adic heights on an elliptic curve

In 2006, Mazur-Stein-Tate [32] gave an algorithm for computing the *cyclotomic p-adic height pairing*[2] on an elliptic curve over $\mathbb{Q}$. This p-adic height pairing is used to define the p-adic regulator appearing in Mazur-Tate-Teitelbaum's formulation of the p-adic Birch and Swinnerton-Dyer conjecture [35].

Let $E/\mathbb{Q}$ be an elliptic curve with good, ordinary reduction at p and fix a Weierstrass model for E of the form $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. Let $\mathscr{O}$ denote the point at infinity. Let $P \in E(\mathbb{Q})$ be a non-torsion point which reduces to $\mathscr{O}$ mod p and to the connected component of the Néron model $\mathscr{E}_\ell^0$ at bad primes ℓ. Then the cyclotomic p-adic height pairing of P is given by the following formula:

$$\langle P,P\rangle = -2\log_p\left(\frac{\sigma_p(P)}{D(P)}\right),$$

where $D(P)$ is the *denominator* of P and σ_p is the p-adic sigma function [34]. Note that the (symmetric, bilinear) pairing induces a quadratic form $h_p(P) = -\frac{1}{2}\langle P,P\rangle$, which allows us to extend the height to the entire Mordell-Weil group by $h_p(nP) = n^2h_p(P)$.

The denominator of $P \in E(\mathbb{Q})$, denoted $D(P)$, is quite simple to compute. For a point $P \in E(\mathbb{Q})$ written as $\left(\frac{a}{d^2}, \frac{b}{d^3}\right)$ with $(a,d) = (b,d) = 1$ and $a,b,d \in \mathbb{Z}$, we have $D(P) = d$.

By the work of Mazur-Tate [34], we have the following characterization of the p-adic sigma function of E:

Theorem 4.1. *There is precisely one odd function $\sigma_p(t) = t + \cdots \in t\mathbb{Z}_p[[t]]$ and constant $c \in \mathbb{Z}_p$ that together satisfy the p-adic differential equation*

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

where ω is the invariant differential $\frac{dx}{2y+a_1x+a_3}$ associated to the model of E above.

An important part of the method of Mazur-Stein-Tate is a fast way of computing the p-adic sigma function, which in turn, relies on computing a special value of the p-adic modular form $\mathbf{E}_2$. This special value is found by carrying out Kedlaya's algorithm! We give a short sketch of the circle of ideas involved, following [32].

The constant c appearing in the differential equation for the p-adic sigma function is defined to be $\frac{a_1^2+4a_2}{12} - \frac{1}{12}\mathbf{E}_2(E,\omega_0)$, where $\mathbf{E}_2(E,\omega_0)$ is the special value of the $p-$adic weight 2 Eisenstein series $\mathbf{E}_2$ at (E,ω_0). Mazur-Stein-Tate gives the following algorithm for computing this special value:

[2] Note that our normalization of the p-adic height pairing differs from that in [32] by a factor of p for consistency with the p-adic Birch and Swinnerton-Dyer conjecture, which is also the convention in `Sage`.

Algorithm 12 Computing $\mathbf{E}_2(E,\omega_0)$
Input: An elliptic curve $E/\mathbb{Q}$, a good ordinary prime $p \geq 5$, and desired digits of precision n
Output: $\mathbf{E}_2(E,\omega_0)$ to precision $O(p^n)$

1. Compute a minimal model of E and let c_4 and c_6 denote its c-invariants. Let $a_4 = -\frac{c_4}{48}$ and $a_6 = -\frac{c_6}{864}$.
2. Apply Kedlaya's algorithm (Algorithm 1) to the curve $y^2 = x^3 + a_4x + a_6$ to obtain the matrix of Frobenius M.
3. Compute M^n, and denote the entries of its second column as a_{01}, a_{11}, so that $M^n(\omega_1) = a_{01}\omega_0 + a_{11}\omega_1$.
4. The special value of $\mathbf{E}_2(E,\omega_0)$ is given by $-12\frac{a_{01}}{a_{11}}$. Output this value.

Example 4.2. Let $E =$ "$37.a1''$ be given by the model $y^2 = x^3 - x + \frac{1}{4}$. as in Section 2.4. Using Sage, we compute the matrix of Frobenius to higher precision:

```
sage: H = HyperellipticCurve(x^3 - x + 1/4)
sage: M = H.matrix_of_frobenius(5)
```

To compute the special value of $\mathbf{E}_2$ to precision $O(5^5)$, we compute the 5th power of the matrix and use its entries:

```
sage: M5 = M^5
sage: -12*M5[0,1]/M5[1,1] + O(5^5)
2 + 4*5 + 2*5^3 + 5^4 + O(5^5)
```

We can check that this agrees with the built-in Sage method for computing the special value of $\mathbf{E}_2$:

```
sage: E = EllipticCurve([-1,1/4])
sage: E.padic_E2(5,prec=5)
2 + 4*5 + 2*5^3 + 5^4 + O(5^5)
```

Using the algorithm for the special value of $\mathbf{E}_2$, Mazur-Stein-Tate gives an algorithm for computing the p-adic height on E:

Algorithm 13 Computing the cyclotomic p-adic height pairing on $E/\mathbb{Q}$
Input: An elliptic curve $E/\mathbb{Q}$, a good ordinary prime $p \geq 5$, a non-torsion $P \in E(\mathbb{Q})$
Output: The cyclotomic p-adic height pairing $\langle P,P\rangle$

1. Compute a positive integer m such that mP reduces to $\mathscr{O}$ mod p and to $\mathscr{E}_\ell^0$ at all bad primes ℓ. Let $Q := mP$ and write $Q = (x,y)$
2. Compute the denominator $D(Q)$ of Q
3. Compute $\sigma_p(t)$ using [32, Algorithm 3.1] and Algorithm 12 and set $s = \sigma_p\left(-\frac{x}{y}\right)$.
4. Compute $h_p(Q) = \log_p\left(\frac{s}{D(Q)}\right)$; then $h_p(P) = \frac{1}{m^2}h_p(Q)$. Output $\langle P,P\rangle = -2h_p(P)$.

Example 4.3. We use Sage to compute the p-adic regulators of the rank 1 elliptic curve "37.a1" for a small range of values p. Note that since E has rank 1, each value of the p-adic regulator is merely the pairing of a Mordell-Weil generator with itself:

```
sage: E = EllipticCurve('37.a1')
sage: for p in prime_range(5,20):
....:     if E.is_good(p) and E.is_ordinary(p):
....:         E.padic_regulator(p,5)
....:
5 + 5^2 + 5^3 + O(5^5)
7 + 7^2 + 3*7^3 + 7^4 + O(7^5)
7*11 + 9*11^2 + 7*11^3 + 8*11^4 + O(11^5)
12*13^2 + 5*13^3 + 9*13^4 + O(13^5)
```

4.2. p-adic heights on Jacobians of hyperelliptic curves

The work of Coleman-Gross [20] gave an interpretation of a global p-adic height pairing on the Jacobian of a curve in terms of a sum of local height pairings. In particular, the local height pairing at a prime above p was given in terms of a Coleman integral. This was revisited in [5] using a variant of Coleman reciprocity [18] and explicit Coleman integration to compute the component at p of the Coleman-Gross p-adic height pairing.

Recently, the explicit computation of local height pairings [5,37] on hyperelliptic curves was used as a means of producing examples of Kim's nonabelian Chabauty method, in the case of hyperelliptic curves with genus equal to Mordell-Weil rank [6]. We describe this "quadratic Chabauty" method below.

We set some notation. Let $C : y^2 = f(x)$ be a hyperelliptic curve as before, with the additional hypothesis that $f(x) \in \mathbb{Z}[x]$. Let J denote the Jacobian of C. Let $\bar{\omega}_i$ denote a differential 1-form dual to the holomorphic basis differential ω_i with respect to the cup product pairing. For $i \in \{0,\dots,g-1\}$, let $f_i(P) = \int_\infty^P \omega_i$ and $f_i(D) = \int_D \omega_i$, and let $g_{ij}(D_k, D_l) = \frac{1}{2}(f_i(D_k)f_j(D_l) + f_j(D_k)f_i(D_l))$.

Theorem 4.4 ("Quadratic Chabauty"). *Suppose that the Mordell-Weil rank of $J(\mathbb{Q})$ is g and that the f_i induce linearly independent $\mathbb{Q}_p$-valued functionals on $J(\mathbb{Q}) \otimes \mathbb{Q}$. Then there exist constants $\alpha_{ij} \in \mathbb{Q}_p$, $i, j \in \{0,\dots,g-1\}$ such that*

$$\rho := -2\int_\infty^P \sum_{i=0}^{g-1} \omega_i \bar{\omega}_i - \sum_{i \le j} \alpha_{ij} g_{ij} \tag{15}$$

only takes values on $C(\mathbb{Z}[1/p])$ in an effectively computable finite set T.

In forthcoming work with Besser and Müller, we show how to combine quadratic Chabauty with the Mordell-Weil sieve to prove that the set of integral points found by ρ and T is complete. Here we give an example showing how to use quadratic Chabauty to find integral points on C.

Example 4.5. Consider the hyperelliptic curve

$$C : y^2 = x(x-2)(x+2)(x+3)(x+7)$$

over $\mathbb{Q}_{13}$, with $P_1 = (-1,6), P_2 = (-4,12), P_3 = (3,30)$. In §4.8 of Müller's lecture notes in this volume, the Mordell-Weil rank of the Jacobian of this curve is computed to be 2. We take as generators for the free part of the Mordell-Weil group

$$D_1 = P_1 - P_3,$$
$$D_2 = P_2 - \iota(P_3).$$

We show how to carry out quadratic Chabauty on C using the prime $p = 13$ to find integral points on this model of C.

Given the reduction type of the curve, Müller computed the set T:

$$\{a\log(2)+b\log(3)+c\log(5)+d\log(7) \mid a \in \{0,1,5/4,3/2\}, b \in \{0,1/2,3/4,1\}, c,d \in \{0,1/2\}\}.$$

Using [10, Algorithm 3.8], compute the global 13-adic height pairings:

$$\langle D_1, D_1\rangle = 12\cdot 13 + 2\cdot 13^2 + 7\cdot 13^3 + 13^4 + 13^5 + 10\cdot 13^6 + 11\cdot 13^7 + 13^8 + 10\cdot 13^9 + O(13^{10}),$$
$$\langle D_1, D_2\rangle = 9\cdot 13 + 2\cdot 13^2 + 13^3 + 2\cdot 13^4 + 6\cdot 13^5 + 6\cdot 13^6 + 4\cdot 13^9 + O(13^{10}),$$
$$\langle D_2, D_2\rangle = 2\cdot 13 + 2\cdot 13^2 + 7\cdot 13^3 + 8\cdot 13^4 + 6\cdot 13^5 + 8\cdot 13^6 + 4\cdot 13^7 + 10\cdot 13^8 + 9\cdot 13^9 + O(13^{10}).$$

We find the α_{ij} using the matrix of Coleman integrals evaluated at D_1, D_2 (see Example 3.9) and the global 13-adic heights computed above:

$$\begin{pmatrix}\alpha_{00}\\ \alpha_{01}\\ \alpha_{11}\end{pmatrix} = \begin{pmatrix} \int_{D_1}\omega_0\int_{D_1}\omega_0 & \int_{D_1}\omega_0\int_{D_1}\omega_1 & \int_{D_1}\omega_1\int_{D_1}\omega_1 \\ \int_{D_1}\omega_0\int_{D_2}\omega_0 & \frac{1}{2}\left(\int_{D_1}\omega_0\int_{D_2}\omega_1 + \int_{D_1}\omega_1\int_{D_2}\omega_0\right) & \int_{D_1}\omega_1\int_{D_2}\omega_1 \\ \int_{D_2}\omega_0\int_{D_2}\omega_0 & \int_{D_2}\omega_0\int_{D_2}\omega_1 & \int_{D_2}\omega_1\int_{D_2}\omega_1 \end{pmatrix}^{-1} \begin{pmatrix}\langle D_1,D_1\rangle\\ \langle D_1,D_2\rangle\\ \langle D_2,D_2\rangle\end{pmatrix}$$
$$= \begin{pmatrix} 6\cdot 13^{-1} + 5 + 13^2 + 8\cdot 13^3 + 4\cdot 13^4 + 10\cdot 13^5 + 9\cdot 13^6 + 5\cdot 13^7 + 7\cdot 13^8 + O(13^9) \\ 6\cdot 13^{-1} + 8\cdot 13 + 12\cdot 13^2 + 4\cdot 13^3 + 6\cdot 13^5 + 11\cdot 13^6 + 11\cdot 13^7 + 5\cdot 13^8 + O(13^9) \\ 7\cdot 13^{-1} + 8 + 11\cdot 13 + 3\cdot 13^3 + 7\cdot 13^4 + 5\cdot 13^5 + 13^6 + 9\cdot 13^8 + O(13^9) \end{pmatrix}.$$

Using the α_{ij}, we can construct the p-padic power series expansion of ρ (see (15)) and set it equal to each of the values in the set T. The theorem tells us that the integral points on C will be among the $\mathbb{Z}_{13}$-points satisfying this relationship. More precisely, for each of the following residue disks:

$$\{\overline{(0,0)}, \overline{(2,0)}, \overline{(6,0)}, \overline{(10,0)}, \overline{(11,0)}, \overline{(9,\pm 1)}, \overline{(4,\pm 2)}, \overline{(7,\pm 2)}, \overline{(8,\pm 2)}, \overline{(3,\pm 4)}, \overline{(12,\pm 6)}\},$$

we use a local coordinate at a point in the disk to compute the Coleman integrals defining ρ. Then for each $t \in T$, we compute the zeros of $\rho - t$ and try to determine if any of the zeros correspond to integral points on the curve.

For example, in the residue disk $\overline{(7,2)}$, we find the following points, noting the corresponding value of (a,b,c,d) giving $a\log(2)+b\log(3)+c\log(5)+d\log(7) = t \in T$.

disk	$x(z)$	(a,b,c,d)
$\overline{(7,2)}$	$7+5\cdot 13+11\cdot 13^3+8\cdot 13^4+4\cdot 13^5+3\cdot 13^7+O(13^8)$	$(0,0,\frac{1}{2},0)$
	$7+3\cdot 13+6\cdot 13^2+10\cdot 13^3+3\cdot 13^4+5\cdot 13^5+7\cdot 13^6+4\cdot 13^7+O(13^8)$	
	$7+12\cdot 13+9\cdot 13^2+9\cdot 13^3+3\cdot 13^4+12\cdot 13^5+8\cdot 13^6+3\cdot 13^7+O(13^8)$	$(0,\frac{1}{2},0,\frac{1}{2})$
	$7+9\cdot 13+4\cdot 13^2+5\cdot 13^3+12\cdot 13^4+9\cdot 13^5+3\cdot 13^6+7\cdot 13^7+O(13^8)$	
	$7+6\cdot 13+4\cdot 13^2+6\cdot 13^3+2\cdot 13^4+10\cdot 13^5+5\cdot 13^6+10\cdot 13^7+O(13^8)$	$(0,1,0,0)$
	$7+2\cdot 13+3\cdot 13^2+13^3+9\cdot 13^5+9\cdot 13^6+13^7+O(13^8)$	
	$7+12\cdot 13+8\cdot 13^2+6\cdot 13^3+7\cdot 13^4+2\cdot 13^5+O(13^8)$	$(0,1,\frac{1}{2},0)$
	$7+9\cdot 13+5\cdot 13^2+7\cdot 13^3+10\cdot 13^4+7\cdot 13^5+7\cdot 13^6+6\cdot 13^7+O(13^8)$	
	$7+13+9\cdot 13^2+7\cdot 13^3+8\cdot 13^4+2\cdot 13^5+12\cdot 13^6+8\cdot 13^7+O(13^8)$	$(1,0,0,\frac{1}{2})$
	$7+7\cdot 13+4\cdot 13^2+11\cdot 13^3+8\cdot 13^4+11\cdot 13^5+5\cdot 13^6+8\cdot 13^7+O(13^8)$	
	$7+11\cdot 13+9\cdot 13^2+3\cdot 13^3+8\cdot 13^4+9\cdot 13^5+4\cdot 13^6+2\cdot 13^7+O(13^8)$	$(1,0,\frac{1}{2},0)$
	$7+10\cdot 13+12\cdot 13^2+4\cdot 13^3+5\cdot 13^4+9\cdot 13^5+7\cdot 13^6+6\cdot 13^7+O(13^8)$	
	$7+6\cdot 13+11\cdot 13^2+7\cdot 13^3+13^4+12\cdot 13^5+7\cdot 13^6+6\cdot 13^7+O(13^8)$	$(1,0,\frac{1}{2},\frac{1}{2})$
	$7+2\cdot 13+9\cdot 13^2+4\cdot 13^3+4\cdot 13^4+6\cdot 13^6+8\cdot 13^7+O(13^8)$	
	$7+5\cdot 13+11\cdot 13^2+10\cdot 13^3+4\cdot 13^4+12\cdot 13^5+12\cdot 13^6+5\cdot 13^7+O(13^8)$	$(1,\frac{1}{2},0,0)$
	$7+3\cdot 13+8\cdot 13^2+13^4+13^5+12\cdot 13^6+7\cdot 13^7+O(13^8)$	
	$7+13+3\cdot 13^2+11\cdot 13^3+11\cdot 13^4+6\cdot 13^5+9\cdot 13^6+2\cdot 13^7+O(13^8)$	$(1,\frac{1}{2},\frac{1}{2},0)$
	$7+7\cdot 13+10\cdot 13^2+6\cdot 13^3+7\cdot 13^4+12\cdot 13^5+4\cdot 13^6+13^7+O(13^8)$	
	$7+13^2+13^3+7\cdot 13^4+2\cdot 13^5+4\cdot 13^6+10\cdot 13^7+O(13^8)$	$(1,\frac{1}{2},\frac{1}{2},\frac{1}{2})$
	$7+8\cdot 13+10\cdot 13^2+7\cdot 13^3+11\cdot 13^4+7\cdot 13^5+12\cdot 13^6+5\cdot 13^7+O(13^8)$	
	$7+5\cdot 13+13^2+3\cdot 13^3+8\cdot 13^4+4\cdot 13^5+7\cdot 13^6+3\cdot 13^7+O(13^8)$	$(1,\frac{3}{4},0,\frac{1}{2})$
	$7+3\cdot 13+5\cdot 13^2+10\cdot 13^3+7\cdot 13^4+7\cdot 13^5+13^6+5\cdot 13^7+O(13^8)$	
	$7+13+2\cdot 13^2+9\cdot 13^3+9\cdot 13^4+13^5+4\cdot 13^6+O(13^8)$	$(1,\frac{3}{4},\frac{1}{2},\frac{1}{2})$
	$7+7\cdot 13+11\cdot 13^2+10\cdot 13^3+6\cdot 13^4+7\cdot 13^5+2\cdot 13^7+O(13^8)$	
	$7+5\cdot 13+2\cdot 13^2+4\cdot 13^3+7\cdot 13^4+5\cdot 13^5+7\cdot 13^6+8\cdot 13^7+O(13^8)$	$(\frac{5}{4},0,0,0)$
	$7+3\cdot 13+4\cdot 13^2+13^3+10\cdot 13^4+9\cdot 13^5+5\cdot 13^6+9\cdot 13^7+O(13^8)$	
	$7+13+6\cdot 13^2+11\cdot 13^3+8\cdot 13^4+13^5+2\cdot 13^6+2\cdot 13^7+O(13^8)$	$(\frac{5}{4},0,\frac{1}{2},0)$
	$7+7\cdot 13+7\cdot 13^2+9\cdot 13^4+7\cdot 13^5+10\cdot 13^7+O(13^8)$	
	7	$(\frac{5}{4},0,\frac{1}{2},\frac{1}{2})$
	$7+8\cdot 13+11\cdot 13^2+2\cdot 13^3+4\cdot 13^4+9\cdot 13^5+12\cdot 13^6+3\cdot 13^7+O(13^8)$	
	$7+5\cdot 13+10\cdot 13^2+10\cdot 13^3+5\cdot 13^4+8\cdot 13^5+6\cdot 13^6+9\cdot 13^7+O(13^8)$	$(\frac{5}{4},\frac{3}{4},\frac{1}{2},0)$
	$7+3\cdot 13+9\cdot 13^2+8\cdot 13^3+10\cdot 13^4+12\cdot 13^5+12\cdot 13^6+5\cdot 13^7+O(13^8)$	
	$7+12\cdot 13+5\cdot 13^2+5\cdot 13^3+13^4+7\cdot 13^5+11\cdot 13^6+3\cdot 13^7+O(13^8)$	$(\frac{5}{4},1,0,0)$
	$7+9\cdot 13+8\cdot 13^2+5\cdot 13^3+8\cdot 13^4+3\cdot 13^5+13^6+11\cdot 13^7+O(13^8)$	
	$7+5\cdot 13+6\cdot 13^3+8\cdot 13^4+7\cdot 13^5+3\cdot 13^6+3\cdot 13^7+O(13^8)$	$(\frac{5}{4},1,\frac{1}{2},\frac{1}{2})$
	$7+3\cdot 13+6\cdot 13^2+2\cdot 13^3+5\cdot 13^4+12\cdot 13^5+11\cdot 13^6+5\cdot 13^7+O(13^8)$	
	$7+4\cdot 13+6\cdot 13^2+3\cdot 13^3+8\cdot 13^4+7\cdot 13^6+13^7+O(13^8)$	$(\frac{3}{2},0,0,0)$
	$7+4\cdot 13+4\cdot 13^2+5\cdot 13^3+4\cdot 13^4+7\cdot 13^5+2\cdot 13^6+6\cdot 13^7+O(13^8)$	
	-6	$(\frac{3}{2},\frac{1}{2},0,0)$
	$7+9\cdot 13+13^2+5\cdot 13^3+8\cdot 13^4+2\cdot 13^5+O(13^8)$	
	$7+5\cdot 13+4\cdot 13^2+4\cdot 13^3+13^4+4\cdot 13^6+6\cdot 13^7+O(13^8)$	$(\frac{3}{2},\frac{1}{2},\frac{1}{2},\frac{1}{2})$
	$7+3\cdot 13+2\cdot 13^2+11\cdot 13^3+10\cdot 13^4+8\cdot 13^5+6\cdot 13^6+9\cdot 13^7+O(13^8)$	
	$7+12\cdot 13+13^2+13^3+10\cdot 13^4+2\cdot 13^5+5\cdot 13^6+12\cdot 13^7+O(13^8)$	$(\frac{3}{2},\frac{3}{4},0,\frac{1}{2})$
	$7+9\cdot 13+12\cdot 13^2+5\cdot 13^3+8\cdot 13^4+10\cdot 13^5+10\cdot 13^6+12\cdot 13^7+O(13^8)$	

For a complete list of the recovered $\mathbb{Z}_{13}$-points, see [1]. Going through the list of these $\mathbb{Z}_{13}$-points, we find the following integral points z and record the value of (a,b,c,d) giving $a\log(2)+b\log(3)+c\log(5)+d\log(7)=t\in T$ which recovered it:

disk	z	t
$\overline{(0,0)}$	$(0,0)$	$(1,\frac{1}{2},0,\frac{1}{2})$
$\overline{(2,0)}$	$(2,0)$	$(\frac{3}{2},1,\frac{1}{2},0)$
$\overline{(6,0)}$	$(-7,0)$	$(1,1,\frac{1}{2},\frac{1}{2})$
$\overline{(10,0)}$	$(-3,0)$	$(1,\frac{1}{2},\frac{1}{2},0)$
$\overline{(11,0)}$	$(-2,0)$	$(\frac{3}{2},0,\frac{1}{2},0)$
$\overline{(9,\pm1)}$	$(-4,\mp12)$	$(1,\frac{3}{4},0,0)$
$\overline{(7,\pm2)}$	$(7,\pm210)$	$(\frac{5}{4},0,\frac{1}{2},\frac{1}{2})$
	$(-6,\mp24)$	$(\frac{3}{2},\frac{1}{2},0,0)$
$\overline{(3,\pm4)}$	$(3,\pm30)$	$(\frac{5}{4},\frac{1}{2},\frac{1}{2},0)$
$\overline{(12,\pm6)}$	$(-1,\pm6)$	$(\frac{5}{4},\frac{3}{4},0,0)$

References

[1] J. S. Balakrishnan, Data for Example 4.5 of "Explicit p-adic methods for elliptic and hyperelliptic curves": `http://people.maths.ox.ac.uk/balakrishnan/nato/quadchabauty_ex4.5`.

[2] ———, *Coleman integration for even models of hyperelliptic curves*, preprint (2012), 1–8, `http://people.maths.ox.ac.uk/balakrishnan/even_coleman.pdf`.

[3] ———, *Iterated Coleman integration for hyperelliptic curves*, ANTS-X: Proceedings of the Tenth Algorithmic Number Theory Symposium (E. W. Howe and K. S. Kedlaya, eds.), Open Book Series, vol. 1, Mathematical Sciences Publishers, 2013, pp. 41–61.

[4] J. S. Balakrishnan and A. Besser, *Coleman-Gross height pairings and the p-adic sigma function*, J. Reine Angew. Math. (2012), to appear.

[5] ———, *Computing local p-adic height pairings on hyperelliptic curves*, IMRN **2012** (2012), no. 11, 2405–2444.

[6] J. S. Balakrishnan, A. Besser, and J. S. Müller, *Quadratic Chabauty: p-adic height pairings and integral points on hyperelliptic curves*, J. Reine Angew. Math., to appear.

[7] J. S. Balakrishnan, R. W. Bradshaw, and K. S. Kedlaya, *Explicit Coleman integration for hyperelliptic curves*, Algorithmic Number Theory (G. Hanrot, F. Morain, and E. Thomé, eds.), Lecture Notes in Computer Science, vol. 6197, Springer, 2010, pp. 16–31.

[8] J. S. Balakrishnan, I. Dan-Cohen, M. Kim, and S. Wewers, *A non-abelian conjecture of Birch and Swinnerton-Dyer type for hyperbolic curves*, preprint (2012), 1–28, `arxiv:1209.0640`.

[9] J. S. Balakrishnan, K. S. Kedlaya, and M. Kim, *Appendix and erratum to "Massey products for elliptic curves of rank 1"*, J. Amer. Math. Soc. **24** (2011), no. 1, 281–291.

[10] J. S. Balakrishnan, J.S. Müller, and W. A. Stein, *A p-adic Birch and Swinnerton-Dyer conjecture for modular abelian varieties*, preprint (2012), 1–33, `arxiv:1210.2739`.

[11] A. Besser, *Coleman integration using the Tannakian formalism*, Math. Ann. **322** (2002), 19–48.

[12] ———, *Heidelberg lectures on Coleman integration*, The Arithmetic of Fundamental Groups (J. Stix, ed.), Contributions in Mathematical and Computational Sciences, vol. 2, Springer Berlin Heidelberg, 2012, pp. 3–52.

[13] W. Castryck, J. Denef, and F. Vercauteren, *Computing zeta functions of nondegenerate curves*, IMRP Int. Math. Res. Pap. (2006), Art. ID 72017, 57.

[14] C. Chabauty, *Sur les points rationnels des courbes algébriques de genre supérieur à l'unité*, C. R. Acad. Sci. Paris **212** (1941), 882–885.

[15] R. F. Coleman, *Dilogarithms, regulators and p-adic L-functions*, Invent. Math. **69** (1982), no. 2, 171–208.

[16] ———, *Effective Chabauty*, Duke Math. J. **52** (1985), no. 3, 765–770.

[17] ———, *Torsion points on curves and p-adic abelian integrals*, Ann. of Math. (2) **121** (1985), no. 1, 111–168.
[18] ———, *Reciprocity laws on curves*, Compositio Math. **72** (1989), no. 2, 205–235.
[19] R. F. Coleman and E. de Shalit, *p-adic regulators on curves and special values of p-adic L-functions*, Invent. Math. **93** (1988), no. 2, 239–266.
[20] R. F. Coleman and B. H. Gross, *p-adic heights on curves*, Algebraic Number Theory – in honor of K. Iwasawa, Advanced Studies in Pure Mathematics, vol. 17, 1989, pp. 73–81.
[21] J. Denef and F. Vercauteren, *An extension of Kedlaya's algorithm to hyperelliptic curves in characteristic 2*, J. Cryptology **19** (2006), no. 1, 1–25.
[22] B. Edixhoven, *Point counting after Kedlaya, EIDMA-Stieltjes graduate course, Leiden, September 22-26,2003,* `http://www.math.leidenuniv.nl/ edix/oww/mathofcrypt/carls_edixhoven/kedlaya.pdf`.
[23] P. Gaudry and N. Gürel, *An extension of Kedlaya's point-counting algorithm to superelliptic curves*, Advances in cryptology—ASIACRYPT 2001 (Gold Coast), Lecture Notes in Comput. Sci., vol. 2248, Springer, Berlin, 2001, pp. 480–494.
[24] M. C. Harrison, *An extension of Kedlaya's algorithm for hyperelliptic curves*, J. Symb. Comp. **47** (2012), no. 1, 89 – 101.
[25] D. Harvey, *Kedlaya's algorithm in larger characteristic*, Int Math Res Notices **2007** (2007), no. rnm095, rnm095–29.
[26] K. S. Kedlaya, *Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology*, J. Ramanujan Math. Soc. **16** (2001), 323–338, erratum *ibid.* **18** (2003), 417–418.
[27] ———, *Computing zeta functions via p-adic cohomology*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 3076, Springer, Berlin, 2004, pp. 1–17.
[28] M. Kim, *The non-abelian (or non-linear) method of Chabauty*, Noncommutative geometry and number theory, Aspects Math., E37, Vieweg, Wiesbaden, 2006, pp. 179–185.
[29] ———, *The unipotent Albanese map and Selmer varieties for curves*, Publ. Res. Inst. Math. Sci. **45** (2009), no. 1, 89–133.
[30] ———, *Massey products for elliptic curves of rank 1*, J. Amer. Math. Soc. **23** (2010), 725–747.
[31] The LMFDB Collaboration, *The L-functions and modular forms database*, `http://www.lmfdb.org`, 2014, [Online; accessed 15 September 2014].
[32] B. Mazur, W. Stein, and J. Tate, *Computation of p-adic heights and log convergence*, Doc. Math. (2006), no. Extra Vol., 577–614 (electronic).
[33] B. Mazur and J. Tate, *Canonical height pairings via biextensions*, Arithmetic and geometry, Vol. I, Progr. Math., vol. 35, Birkhäuser Boston, Boston, MA, 1983, pp. 195–237.
[34] ———, *The p-adic sigma function*, Duke Math. J. **62** (1991), no. 3, 663–688.
[35] B. Mazur, J. Tate, and J. Teitelbaum, *On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer*, Invent. Math. **84** (1986), no. 1, 1–48.
[36] M. Minzlaff, *Computing zeta functions of superelliptic curves in larger characteristic*, Mathematics in Computer Science **3** (2010), no. 2, 209–224.
[37] J. S. Müller, *Computing canonical heights using arithmetic intersection theory*, Math. Comp. **83** (2014), no. 285, 311–336.
[38] J. Nekovář, *On p-adic height pairings*, Séminaire de Théorie des Nombres, Paris, 1990–91, Birkhäuser Boston, Boston, MA, 1993, pp. 127–202.
[39] P. Schneider, *p-adic height pairings I*, Invent. Math. **69** (1982), no. 3, 401–409.
[40] W. A. Stein et al., *Sage Mathematics Software (Version 6.2)*, The Sage Development Team, 2014, `http://www.sagemath.org`.