REFINED CHABAUTY–KIM COMPUTATIONS FOR THE THRICE-PUNCTURED LINE OVER $\mathbb{Z}[1/6]$

MARTIN LÜDTKE

Abstract. The Chabauty–Kim method and its refined variant by Betts and Dogra aim to cut out the S-integral points $X(\mathbb{Z}_S)$ on a curve inside the p-adic points $X(\mathbb{Z}_p)$ by producing enough Coleman functions vanishing on them. We derive new functions in the case of the thrice-punctured line when S contains two primes. We describe an algorithm for computing refined Chabauty–Kim loci and verify Kim's Conjecture over $\mathbb{Z}[1/6]$ for all choices of auxiliary prime $p < 10{,}000$.

Contents

1. Introduction

Let S be a finite set of primes and let $X = \mathbb{P}^1 \smallsetminus \{0, 1, \infty\}$ be the thrice-punctured line over the ring of S-integers $\mathbb{Z}_S$. By the Siegel–Mahler theorem, the set of S-integral points $X(\mathbb{Z}_S)$ is finite.[1] Kim [Kim05] gave a new p-adic proof of this fact by constructing, for any prime $p \notin S$, a descending chain of subsets of $X(\mathbb{Z}_p)$ containing $X(\mathbb{Z}_S)$:

$$X(\mathbb{Z}_p) \supseteq X(\mathbb{Z}_p)_{S,1} \supseteq X(\mathbb{Z}_p)_{S,2} \supseteq \dots \quad \supseteq X(\mathbb{Z}_S).$$

The set $X(\mathbb{Z}_p)_{S,n}$ is called the Chabauty–Kim locus of depth n. Kim showed that the sets $X(\mathbb{Z}_p)_{S,n}$ eventually become finite, so that $X(\mathbb{Z}_S)$ must be finite as well. This suggests the following strategy for computing $X(\mathbb{Z}_S)$: find as many points in $X(\mathbb{Z}_S)$ as possible; then compute $X(\mathbb{Z}_p)_{S,n}$ for some $p \notin S$ and $n \geq 1$. This gives a lower and an upper bound. If they match, we have found $X(\mathbb{Z}_S)$. In order for this strategy to have a chance of succeeding we need that the set $X(\mathbb{Z}_p)_{S,n}$ contains no p-adic points which are not S-integral points, at least for sufficiently

[1] The finiteness of $X(\mathbb{Z}_S)$ is often referred to as Siegel's theorem but it was first proved by Mahler [Mah33, Folgerung 2] in 1933. He uses a generalisation of Siegel's proof from 1921 of the finiteness of the set of *integral* points $X(\mathcal{O}_K)$ over a general number field K. Siegel's result is not stated explicitly but it can be deduced from [Sie21, Satz 7, Zusatz 1] which implies that the polynomial $f(x) = x(1-x)$ represents a unit of K only finitely many times as x runs through the ring of integers of K. See [EG15, Summary] for a historical overview.

Submitted to Algor. Num. Th. Symp.

large n. In other words, the inclusion $X(\mathbb{Z}_S) \subseteq X(\mathbb{Z}_p)_{S,n}$ should eventually be an equality. This is the content of Kim's Conjecture [BDKW18, Conj. 3.1 & §8.1]. The heuristic behind this is that as n grows larger, we find more and more independent Coleman functions vanishing on $X(\mathbb{Z}_p)_{S,n}$, and any p-adic point in the intersection of their zero loci should be there for a good reason, namely being an S-integral point.

Computing the sets $X(\mathbb{Z}_p)_{S,n}$ is difficult in practice and so far has only been achieved in cases where S contains at most one prime [BDKW18; BKL23; DW16; CD20a]. In this paper we focus on the *refined* Chabauty–Kim sets $X(\mathbb{Z}_p)^{\min}_{S,n}$ introduced by Betts and Dogra [BD20]. These are potentially smaller than the sets $X(\mathbb{Z}_p)_{S,n}$ but still contain $X(\mathbb{Z}_S)$. It is natural to formulate Kim's Conjecture also for the refined sets:

Conjecture 1.1 (Refined Kim's Conjecture)**.** *$X(\mathbb{Z}_p)^{\min}_{S,n} = X(\mathbb{Z}_S)$ for $n \gg 0$.*

If Kim's Conjecture holds for the original unrefined sets then Conjecture 1.1 also holds. Recently, verifying Conjecture 1.1 (for a hyperbolic curve of any genus) has been proposed as a strategy for proving Grothendieck's Section Conjecture for locally geometric sections [BKL23, Theorem A]. In this paper we verify Conjecture 1.1 for the thrice-punctured line over $\mathbb{Z}[1/6]$ for many choices of the auxiliary prime p.

Theorem 1.2 (= Corollary 6.3)**.** *Conjecture 1.1 for $S = \{2, 3\}$ holds in depth $n = 4$ for all primes p with $5 \leq p < 10{,}000$.*

Previously, Kim's Conjecture for $S = \{2, 3\}$ (refined or unrefined) was not known to hold for any prime p. For $S = \{2\}$, Conjecture 1.1 can be proved for all odd primes p by purely algebraic reasoning [BKL23, Theorem B]. In contrast, our proof of Theorem 1.2 uses a combination of theoretical results and computer calculations.

For the most part we work with $S = \{2, q\}$ for an arbitrary odd prime q. The refined Chabauty–Kim method for such sets was first applied in depth $n = 2$ in [BBK+24]. There, an equation is derived which (essentially) defines the depth 2 locus $X(\mathbb{Z}_p)^{\min}_{\{2,q\},2}$ inside $X(\mathbb{Z}_p)$. It takes the form

$$\log(2)\log(q)\operatorname{Li}_2(z) - a_{\tau_q\tau_2}\log(z)\operatorname{Li}_1(z) = 0 \tag{1.1}$$

for some computable p-adic constant $a_{\tau_q\tau_2} \in \mathbb{Q}_p$. Here, log, Li_1 and Li_2 are p-adic (poly)logarithm functions. One part of this paper is devoted to systematically computing the depth 2 loci $X(\mathbb{Z}_p)^{\min}_{\{2,q\},2}$ for any p and q. In §4 we describe an algorithm to achieve this. A SageMath [Sage] implementation is available at `https://github.com/martinluedtke/RefinedCK`. Using this code, we computed the depth 2 loci for many combinations of p and q. We present our findings in §5 and explain the observed behaviour by analysing the Newton polygons of power series. In particular, we are able to explain why the Chabauty–Kim loci are exceptionally large for the auxiliary primes $p = 1093$ and $p = 3511$. This is related to the fact that these are Wieferich primes, i.e., primes for which $2^{p-1} \equiv 1 \bmod p^2$.

In a few cases, notably whenever $q \geq 5$ is a Mersenne prime or a Fermat prime and we take $p = 3$, Conjecture 1.1 for $S = \{2, q\}$ holds already in depth 2 [BBK+24, Cor. 3.15]. Most of the time, however, Eq. (1.1) has p-adic solutions which are not S-integral points. In this case, one has to go to higher depth in order to verify Kim's Conjecture. We take $n = 4$, show that in order to verify Conjecture 1.1 it suffices to look at a certain subset $X(\mathbb{Z}_p)^{(1,0)}_{\{2,q\},4}$ of the refined Chabauty–Kim locus (defined in §2.2) and derive an equation which holds on this set:

Theorem 1.3. *Let $S = \{2, q\}$ for some odd prime q and let $p \notin S$ be an auxiliary prime. Then every point in the refined Chabauty–Kim locus $X(\mathbb{Z}_p)^{(1,0)}_{\{2,q\},4}$ satisfies, in addition to Eq. (1.1), a* *nontrivial equation of the form*

$$a \operatorname{Li}_4(z) + b \log(z) \operatorname{Li}_3(z) + c \log(z)^3 \operatorname{Li}_1(z) = 0 \tag{1.2}$$

for certain p-adic constants $a, b, c \in \mathbb{Q}_p$.

Theorem 1.3 is a simplified version of Theorem 3.4 where more precise expressions for the coefficients appearing in Eq. (1.2) are given; see also §3.4 about the non-triviality of the equation. For general q, an insufficient supply of $\{2, q\}$-integral points on the thrice-punctured line makes it difficult to determine those coefficients. Taking $q = 3$, however, where $X(\mathbb{Z}[1/6])$ contains for example the points -3, 3, 9, we get a completely explicit equation:

Theorem 1.4. *(= Theorem 3.8) Let* $S = \{2, 3\}$ *and* $p \notin S$. *Any point z in the refined Chabauty–Kim locus* $X(\mathbb{Z}_p)^{(1,0)}_{\{2,3\},4}$ *satisfies the equation*

$$\det \begin{pmatrix} \operatorname{Li}_4(z) & \log(z) \operatorname{Li}_3(z) & \log(z)^3 \operatorname{Li}_1(z) \\ \operatorname{Li}_4(3) & \log(3) \operatorname{Li}_3(3) & \log(3)^3 \operatorname{Li}_1(3) \\ \operatorname{Li}_4(9) & \log(9) \operatorname{Li}_3(9) & \log(9)^3 \operatorname{Li}_1(9) \end{pmatrix} = 0. \tag{1.3}$$

Using computations in Sage, we can verify for $S = \{2, 3\}$ and many choices of p that all p-adic points satisfying both equations (1.1) and (1.3) are in fact $\{2, 3\}$-integral points, thus proving Theorem 1.2. This provides evidence for Kim's Conjecture and supports the principle that, while a single Coleman function is usually insufficient to cut out precisely the set of S-integral points, two independent Coleman functions will often suffice.

Structure of the paper. We start by recalling in §2 the necessary background on refined Chabauty–Kim theory for the thrice-punctured line. We then derive in §3 the Coleman functions which vanish on the depth 4 Chabauty–Kim loci in the case $S = \{2, q\}$, proving the precise version of Theorem 1.3 for general q, as well as Theorem 1.4 for $q = 3$. We then turn to the computational aspects of this paper. In §4 we describe how to systematically compute the depth 2 loci $X(\mathbb{Z}_p)^{(1,0)}_{\{2,q\},2}$ for arbitrary p and q and analyse the obtained data in §5. Finally, in §6 we present the computations which we use to verify instances of Kim's Conjecture in Theorem 1.2.

Acknowledgements. I would like to thank Steffen Müller for his encouragement to write this paper and for helpful discussions. I also thank Elie Studnia and David Lilienfeldt for feedback on an earlier draft, and the referees for helpful comments. This work was supported by an NWO Vidi grant.

2. Background on refined Chabauty–Kim

We start by recalling what is known about the refined Chabauty–Kim method for the thrice-punctured line, referring to the existing literature for details. The original (unrefined) method is studied in [Kim05; DW15; DW16; Bro17; BDKW18, §8; CD20a; CD20b], the refined variant in [BBK+24; BKL23].

Let S be a finite set of primes and let $X = \mathbb{P}^1 \smallsetminus \{0, 1, \infty\}$ be the thrice-punctured line over the ring of S-integers $\mathbb{Z}_S$. Let $p \notin S$ be an auxiliary prime and let $U = \pi_1^{\text{ét},\mathbb{Q}_p}(X_{\overline{\mathbb{Q}}}, b)$ be the $\mathbb{Q}_p$-prounipotent étale fundamental group of X at the tangential base point $b = \vec{1}_0$, equipped with its natural action by the absolute Galois group $G_{\mathbb{Q}}$. For any finite-dimensional

$G_{\mathbb{Q}}$-equivariant quotient $U \twoheadrightarrow U'$, we have the following *Chabauty–Kim diagram* [Kim05, §3] [Kim09, Introduction]

$$\begin{array}{ccc} X(\mathbb{Z}_S) & \hookrightarrow & X(\mathbb{Z}_p) \\ \downarrow j_S & & \downarrow j_p \\ \mathrm{H}^1_{f,S}(G_{\mathbb{Q}}, U') & \xrightarrow{\mathrm{loc}_p} & \mathrm{H}^1_f(G_p, U'). \end{array} \tag{2.1}$$

Here, $\mathrm{H}^1_{f,S}(G_{\mathbb{Q}}, U')$ denotes the Bloch–Kato Selmer scheme which parametrises $G_{\mathbb{Q}}$-equivariant U'-torsors which are unramified outside $S \cup \{p\}$ and crystalline at p; the local Selmer scheme $\mathrm{H}^1_f(G_p, U')$ parametrises crystalline G_p-equivariant U'-torsors.[2] Both the global and the local Selmer scheme are affine $\mathbb{Q}_p$-schemes and the localisation map between them is algebraic. Strictly speaking, the vertical maps in the Chabauty–Kim diagram, both of which send a point x of X to the torsor of paths from b to x, map into the $\mathbb{Q}_p$-points of the schemes but this is customarily omitted from the notation. The *Chabauty–Kim locus* for the fundamental group quotient U' is defined as

$$X(\mathbb{Z}_p)_{S,U'} \coloneqq j_p^{-1}(\mathrm{loc}_p(\mathrm{H}^1_{f,S}(G_{\mathbb{Q}}, U'))),$$

in other words as the inverse image under j_p of the scheme-theoretic image of the Selmer scheme under the localisation map. If $U' = U_n$ is the maximal n-step nilpotent quotient of U, we denote the locus by $X(\mathbb{Z}_p)_{S,n}$ and call it the Chabauty–Kim locus of *depth* n. The sets $X(\mathbb{Z}_p)_{S,U'}$ all contain the set of S-integral points $X(\mathbb{Z}_S)$ by construction and are cut out inside $X(\mathbb{Z}_p)$ by Coleman functions, i.e., locally analytic functions given by iterated Coleman integrals. Whenever f is an algebraic function on $\mathrm{H}^1_f(G_p, U')$ such that $\mathrm{loc}_p^\sharp f = 0$, then $f \circ j_p$ is a Coleman function on $X(\mathbb{Z}_p)$ which vanishes on $X(\mathbb{Z}_p)_{S,U'}$. Determining the Chabauty–Kim loci in practice boils down to finding such functions.

2.1. **The localisation map.** One fundamental group quotient which is particularly convenient to work with is the so-called *polylogarithmic quotient* of depth n, which we denote by $U_{\mathrm{PL},n}$. We denote the associated Chabauty–Kim loci by $X(\mathbb{Z}_p)_{S,\mathrm{PL},n}$. The Coleman functions defining them involve only single polylogarithms Li_k $(1 \le k \le n)$, as opposed to multiple polylogarithms $\mathrm{Li}_{k_1,\dots,k_r}$ with $r \ge 2$. Thanks to prior work by Corwin and Dan-Cohen [CD20a] we can write down the localisation map in the Chabauty–Kim diagram for $U_{\mathrm{PL},n}$ quite explicitly. The global and local Selmer scheme are both affine spaces over $\mathbb{Q}_p$. Taking $n = 4$, the global Selmer scheme is given by

$$\mathrm{H}^1_{f,S}(G_{\mathbb{Q}}, U_{\mathrm{PL},4}) = \mathrm{Spec}\ \mathbb{Q}_p[(x_\ell)_{\ell \in S}, (y_\ell)_{\ell \in S}, z_3] = \mathbb{A}^S \times \mathbb{A}^S \times \mathbb{A}^1.$$

The functions x_ℓ and y_ℓ are canonical, whereas z_3 depends on certain choices. In [CD20a], these functions are denoted by $x_\ell = \Phi^{\tau_\ell}_{e_0}$, $y_\ell = \Phi^{\tau_\ell}_{e_1}$, $z = \Phi^{\sigma_3}_{e_1 e_0 e_0}$.

The local Selmer scheme has a canonical set of coordinates

$$\mathrm{H}^1_f(G_p, U_{\mathrm{PL},4}) = \mathrm{Spec}\ \mathbb{Q}_p[\log, \mathrm{Li}_1, \mathrm{Li}_2, \mathrm{Li}_3, \mathrm{Li}_4]$$

coming from the non-abelian Bloch–Kato logarithm $\mathrm{H}^1_f(G_p, U_{\mathrm{PL},4}) \cong U^{\mathrm{dR}}_{\mathrm{PL},4}$. They are such that $\log(j_p(z)) = \log^p(z)$ is the p-adic logarithm for $z \in X(\mathbb{Z}_p)$, and $\mathrm{Li}_n(j_p(z)) = \mathrm{Li}^p_n(z)$ is the n-th

[2] Kim [Kim05; Kim09] considers the case that $U' = U_n$ is the maximal n-step nilpotent quotient but the construction of the Chabauty–Kim diagram works for arbitrary $G_{\mathbb{Q}}$-equivariant quotients. Moreover, Kim writes $\mathrm{H}^1_f(G_T, -)$ instead of $\mathrm{H}^1_{f,S}(G_{\mathbb{Q}}, -)$ where $T = S \cup \{p\}$ and G_T is the Galois group of the maximal extension of $\mathbb{Q}$ unramified outside T. This is an equivalent way of imposing the local conditions of being unramified outside T, cf. [BDKW18, §2.8].

Submitted to Algor. Num. Th. Symp.

p-adic polylogarithm. (We often omit the superscript $(-)^p$ from the notation.) These coordinates can be used to write down the localisation map

$$\mathrm{loc}_p\colon \mathrm{H}^1_{f,S}(G_{\mathbb{Q}}, U_{\mathrm{PL},4}) \to \mathrm{H}^1_f(G_p, U_{\mathrm{PL},4}). \tag{2.2}$$

Proposition 2.1. *With respect to the coordinates above, the localisation map (2.2) for the polylogarithmic quotient in depth 4 is given as follows:*

$$\mathrm{loc}_p^\sharp \log = \sum_{\ell\in S} a_{\tau_\ell} x_\ell, \tag{2.3}$$

$$\mathrm{loc}_p^\sharp \mathrm{Li}_1 = \sum_{\ell\in S} a_{\tau_\ell} y_\ell, \tag{2.4}$$

$$\mathrm{loc}_p^\sharp \mathrm{Li}_2 = \sum_{\ell,q\in S} a_{\tau_\ell\tau_q} x_\ell y_q, \tag{2.5}$$

$$\mathrm{loc}_p^\sharp \mathrm{Li}_3 = \sum_{\ell_1,\ell_2,q\in S} a_{\tau_{\ell_1}\tau_{\ell_2}\tau_q} x_{\ell_1}x_{\ell_2} y_q + a_{\sigma_3} z_3, \tag{2.6}$$

$$\mathrm{loc}_p^\sharp \mathrm{Li}_4 = \sum_{\ell_1,\ell_2,\ell_3,q\in S} a_{\tau_{\ell_1}\tau_{\ell_2}\tau_{\ell_3}\tau_q} x_{\ell_1}x_{\ell_2}x_{\ell_3} y_q + \sum_{\ell\in S} a_{\tau_\ell\sigma_3} x_\ell z_3. \tag{2.7}$$

Here, the a_u, subscripted by words in the symbols τ_ℓ ($\ell \in S$) and σ_3, are certain p-adic constants.

Proof. This is [BKL23, Theorem 5.6] for $n = 4$. The formulas are originally derived in [CD20a, Corollary 3.11] for a motivic variant of the Chabauty–Kim diagram, and transferred to the étale setting via a comparison theorem [BKL23, Theorem 3.2]. □

Remark 2.2. The p-adic constants a_u appearing in the localisation map are hard to determine in practice. In §3.5 we discuss this issue and determine the values of the constants in the case $S = \{2, 3\}$.

2.2. **Refined Selmer schemes.** The refined Chabauty–Kim method by Betts and Dogra [BD20] replaces the Selmer scheme $\mathrm{H}^1_{f,S}(G_{\mathbb{Q}}, U')$ by a certain closed subscheme $\mathrm{Sel}^{\min}_{S,U'}(X)$ called the *refined Selmer scheme*. It is defined in such a way that it still fits into the commutative diagram (2.1). The refined Selmer scheme for the thrice-punctured line was first studied in [BBK+24] in depth 2 and later in [BKL23, §4] for general fundamental group quotients. If $2 \notin S$, then both $X(\mathbb{Z}_S)$ and the refined Selmer scheme are automatically empty as a consequence of $X(\mathbb{Z}_2)$ being empty. Conjecture 1.1 is trivially satisfied in this case. So assume $2 \in S$ from now on. Then the refined Selmer scheme can be written as a union of $3^{\#S}$ closed subschemes as follows.

For each $\ell \in S$ we have the mod-ℓ reduction map

$$\mathrm{red}_\ell\colon X(\mathbb{Z}_S) \subseteq X(\mathbb{Q}_\ell) \subseteq \mathbb{P}^1(\mathbb{Q}_\ell) = \mathbb{P}^1(\mathbb{Z}_\ell) \to \mathbb{P}^1(\mathbb{F}_\ell).$$

Let $\Sigma = (\Sigma_\ell)_{\ell\in S} \in \{0, 1, \infty\}^S$ be a tuple consisting of a choice of a boundary point $\Sigma_\ell \in \{0, 1, \infty\}$ for each $\ell \in S$. We call such a tuple a *refinement condition*. (It corresponds roughly to the notion of *reduction type* of [Bet23, §6.1].) Denote by $X(\mathbb{Z}_S)_\Sigma$ the set of S-integral points z such that $\mathrm{red}_\ell(z) \in (X \cup \{\Sigma_\ell\})(\mathbb{F}_\ell)$ for all $\ell \in S$. Note that each S-integral point is contained in $X(\mathbb{Z}_S)_\Sigma$ for some Σ. (If the point is already S'-integral for a proper subset $S' \subsetneq S$, there are multiple possible choices of Σ.) Associated to Σ we have a partial refined Selmer scheme $\mathrm{Sel}^\Sigma_{S,U'}(X)$ fitting into a Σ-refined version of (2.1):

$$\begin{array}{ccc} X(\mathbb{Z}_S)_\Sigma & \hookrightarrow & X(\mathbb{Z}_p) \\ \downarrow{\scriptstyle j_S} & & \downarrow{\scriptstyle j_p} \\ \mathrm{Sel}^{\Sigma}_{S,U'}(X) & \xrightarrow{\mathrm{loc}_p} & \mathrm{H}^1_f(G_p, U'). \end{array} \tag{2.8}$$

This diagram is used to define the Σ-refined Chabauty–Kim locus

$$X(\mathbb{Z}_p)^{\Sigma}_{S,U'} := j_p^{-1}(\mathrm{loc}_p(\mathrm{Sel}^{\Sigma}_{S,U'}(X))).$$

The total refined Selmer scheme $\mathrm{Sel}^{\min}_{S,U'}(X)$ is the union of closed subschemes

$$\mathrm{Sel}^{\min}_{S,U'}(X) = \bigcup_{\Sigma} \mathrm{Sel}^{\Sigma}_{S,U'}(X),$$

with $\Sigma \in \{0, 1, \infty\}^S$ running over all refinement conditions. Accordingly, the total refined Chabauty–Kim locus $X(\mathbb{Z}_p)^{\min}_{S,U'}$ equals the union of the Σ-refined loci:

$$X(\mathbb{Z}_p)^{\min}_{S,U'} = \bigcup_{\Sigma} X(\mathbb{Z}_p)^{\Sigma}_{S,U'}.$$

Diagram (2.8) implies that $X(\mathbb{Z}_p)^{\Sigma}_{S,U'}$ contains the set $X(\mathbb{Z}_S)_\Sigma$. It is natural to formulate Conjecture 1.1 for each refinement condition Σ separately:

Conjecture 2.3 (Σ-refined Kim's Conjecture)**.** *$X(\mathbb{Z}_p)^{\Sigma}_{S,n} = X(\mathbb{Z}_S)_\Sigma$ for $n \gg 0$.*

Here, $X(\mathbb{Z}_p)^{\Sigma}_{S,n}$ denotes the Σ-refined Chabauty–Kim locus for the depth n quotient U_n. Clearly, if Conjecture 2.3 holds for each refinement condition Σ, then Conjecture 1.1 for the total refined locus $X(\mathbb{Z}_p)^{\min}_{S,n}$ also holds.

Remark 2.4. The converse is not true: for example, when $q > 3$ is a Fermat or Mersenne prime then Conjecture 1.1 holds for $X(\mathbb{Z}_3)^{\min}_{\{2,q\},2}$ [BBK+24, Cor. 3.15] whereas the $(1, 0)$-refined variant fails, due to $2 \in X(\mathbb{Z}_3)^{(1,0)}_{\{2,q\},2} \smallsetminus X(\mathbb{Z}[\frac{1}{2q}])_{(1,0)}$ [BBK+24, Rmk. 3.11].

Recall from §2.1 that the Selmer scheme $\mathrm{H}^1_{f,S}(G_\mathbb{Q}, U_{\mathrm{PL},4}) \cong \mathbb{A}^S \times \mathbb{A}^S \times \mathbb{A}^1$ for the polylogarithmic quotient of depth 4 carries canonical functions x_ℓ and y_ℓ for $\ell \in S$. The Σ-refined Selmer scheme can be described as a linear subspace in terms of these coordinates. The following is a special case of [BKL23, Prop. 5.11].

Proposition 2.5. *Let $\Sigma = (\Sigma_\ell)_{\ell \in S} \in \{0, 1, \infty\}^S$ be a refinement condition. The Σ-refined Selmer scheme $\mathrm{Sel}^{\Sigma}_{S,\mathrm{PL},4}(X)$ is the closed subscheme of $\mathrm{H}^1_{f,S}(G_\mathbb{Q}, U_{\mathrm{PL},4})$ defined by the following equations for all $\ell \in S$:*

$$\begin{cases} y_\ell = 0, & \text{if } \Sigma_\ell = 0, \\ x_\ell = 0, & \text{if } \Sigma_\ell = 1, \\ x_\ell + y_\ell = 0, & \text{if } \Sigma_\ell = \infty. \end{cases}$$

3. Refined Kim functions in depth 4

We now consider the case where $S = \{2, q\}$ for some odd prime q. In this section we first reduce Conjecture 1.1 in depth 4 to Conjecture 2.3 for the polylogarithmic depth 4 quotient and for only two particular choices of the refinement condition Σ. We then determine Coleman functions vanishing on the respective Chabauty–Kim sets, proving Theorems 1.3 and 1.4 from the introduction.

Submitted to Algor. Num. Th. Symp.

3.1. Reducing Kim's conjecture.

Lemma 3.1. *Assume that $X(\mathbb{Z}_p)^{\Sigma}_{S,\mathrm{PL},4} = X(\mathbb{Z}_S)_\Sigma$ holds for the two refinement conditions $\Sigma = (1,1)$ and $\Sigma = (1,0)$. Then Conjecture 2.3 holds in depth 4 for* all *$\Sigma \in \{0,1,\infty\}^2$. In particular, Kim's Conjecture for the total refined locus (Conjecture 1.1) holds in depth 4.*

Proof. By [BKL23, Lemma 4.11], the quotient map $U_4 \twoheadrightarrow U_{\mathrm{PL},4}$ from the full depth 4 quotient to the polylogarithmic depth 4 quotient of the fundamental group induces an inclusion

$$X(\mathbb{Z}_p)^{\Sigma}_{S,4} \subseteq X(\mathbb{Z}_p)^{\Sigma}_{S,\mathrm{PL},4}.$$

Thus, whenever $X(\mathbb{Z}_p)^{\Sigma}_{S,\mathrm{PL},4} = X(\mathbb{Z}_S)_\Sigma$ holds, then also $X(\mathbb{Z}_p)^{\Sigma}_{S,4} = X(\mathbb{Z}_S)_\Sigma$. By [BKL23, Lemma 4.12], the loci $X(\mathbb{Z}_p)^{\Sigma}_{S,4}$ are functorial with respect to the S_3-action on $\mathbb{P}^1 \setminus \{0,1,\infty\}$. Specifically, for any automorphism $\sigma \in S_{\{0,1,\infty\}} \cong S_3$, given by one of the six Möbius transformations

$$z, \quad 1-z, \quad \frac{1}{z}, \quad \frac{z-1}{z}, \quad \frac{z}{z-1}, \quad \frac{1}{1-z},$$

and for any refinement condition $\Sigma \in \{0,1,\infty\}^2$, we have

$$\sigma(X(\mathbb{Z}_p)^{\Sigma}_{S,4}) = X(\mathbb{Z}_p)^{\sigma(\Sigma)}_{S,4}.$$

In particular, if $X(\mathbb{Z}_p)^{\Sigma}_{S,4} = X(\mathbb{Z}_S)_\Sigma$ holds for some Σ, then it also holds for $\sigma(\Sigma)$. Any refinement condition is either of the form $\sigma((1,1))$ or $\sigma((1,0))$ for some $\sigma \in S_3$, so if Kim's Conjecture holds for $X(\mathbb{Z}_p)^{(1,1)}_{S,4}$ and $X(\mathbb{Z}_p)^{(1,0)}_{S,4}$, then it holds in fact for all refinement conditions, and thus for the total refined locus $X(\mathbb{Z}_p)^{\min}_{S,4}$. □

3.2. The $(1,1)$-locus.

Theorem 3.2. *The following equations hold on $X(\mathbb{Z}_p)^{(1,1)}_{\{2,q\},\mathrm{PL},4}$:*

$$\log(z) = 0, \quad \mathrm{Li}_2(z) = 0, \quad \mathrm{Li}_4(z) = 0.$$

Proof. By Proposition 2.5, the refined Selmer scheme $\mathrm{Sel}^{(1,1)}_{S,\mathrm{PL},4}(X)$ is the closed subscheme of $\mathrm{H}^1_{f,S}(G_\mathbb{Q}, U_{\mathrm{PL},4})$ defined by $x_2 = x_q = 0$. The restriction of the localisation map loc_p to this refined subscheme is given by setting x_2 and x_q equal to zero in Proposition 2.1. The functions log, Li_2, Li_4 pull back to 0 on $\mathrm{Sel}^{(1,1)}_{S,\mathrm{PL},4}(X)$, so their pullbacks along j_p vanish on $X(\mathbb{Z}_p)^{(1,1)}_{\{2,q\},\mathrm{PL},4}$. □

Remark 3.3. The set $X(\mathbb{Z}_p)^{(1,1)}_{\{2,q\},\mathrm{PL},4}$ for $S = \{2,q\}$ agrees with the set $X(\mathbb{Z}_p)^{(1)}_{\{2\},\mathrm{PL},4}$ for $S = \{2\}$; in particular, it is independent of the prime q. This reflects the fact that $X(\mathbb{Z}[\frac{1}{2q}])_{(1,1)} = \{-1\}$ for all q. The two equations $\log(z) = 0$ and $\mathrm{Li}_2(z) = 0$ were already derived for the depth 2 locus in [BBK+24, Proposition 3.8]. We believe that these two functions suffice to cut out exactly the set $\{-1\}$ and we verified this computationally using the method described in Remark 3.6 of loc. cit. for all odd primes $p < 10^5$. Thus, Conjecture 2.3 for $\Sigma = (1,1)$ holds in depth 2 for those primes.

Using the localisation map in infinite depth [BKL23, Theorem 5.6] one sees easily that $X(\mathbb{Z}_p)^{(1,1)}_{\{2,q\},\mathrm{PL},n} = X(\mathbb{Z}_p)^{(1)}_{\{2\},\mathrm{PL},n}$ holds in fact for any depth n. By Corollary 5.16 of loc. cit., the latter locus is exactly $\{-1\}$ when $n = \max(1, p-3)$. Thus, Conjecture 2.3 for $S = \{2,q\}$ and refinement condition $\Sigma = (1,1)$ holds for any choice of p in sufficiently high depth.

3.3. The $(1,0)$-locus.

Theorem 3.4. *The following two equations hold on the* $(1,0)$*-component of the refined Chabauty–Kim locus* $X(\mathbb{Z}_p)^{(1,0)}_{\{2,q\},\mathrm{PL},4}$:

$$a_{\tau_2}a_{\tau_q}\,\mathrm{Li}_2(z) - a_{\tau_q\tau_2}\log(z)\,\mathrm{Li}_1(z) = 0, \tag{3.1}$$

$$\begin{aligned} &a_{\sigma_3}a_{\tau_q}^3 a_{\tau_2}\,\mathrm{Li}_4(z) - a_{\tau_q}^2 a_{\tau_2} a_{\tau_q\sigma_3}\log(z)\,\mathrm{Li}_3(z) \\ &\quad - \big(a_{\sigma_3}a_{\tau_q\tau_q\tau_q\tau_2} - a_{\tau_q\sigma_3}a_{\tau_q\tau_q\tau_2}\big)\log(z)^3\,\mathrm{Li}_1(z) = 0. \end{aligned} \tag{3.2}$$

Proof. By Proposition 2.5, the refined Selmer scheme $\mathrm{Sel}^{(1,0)}_{S,\mathrm{PL},4}(X)$ is the closed subscheme of $\mathrm{H}^1_{f,S}(G_\mathbb{Q}, U_{\mathrm{PL},4})$ defined by $x_2 = 0$ and $y_q = 0$. Denote the inclusion by i_Σ. The restriction of the localisation map loc_p to this refined subscheme is given by setting x_2 and y_q equal to zero in Proposition 2.1:

$$\begin{aligned} (\mathrm{loc}_p \circ i_\Sigma)^\sharp \log &= a_{\tau_q}x_q, \\ (\mathrm{loc}_p \circ i_\Sigma)^\sharp \mathrm{Li}_1 &= a_{\tau_2}y_2, \\ (\mathrm{loc}_p \circ i_\Sigma)^\sharp \mathrm{Li}_2 &= a_{\tau_q\tau_2}x_q y_2, \\ (\mathrm{loc}_p \circ i_\Sigma)^\sharp \mathrm{Li}_3 &= a_{\tau_q\tau_q\tau_2}x_q^2 y_2 + a_{\sigma_3}z_3, \\ (\mathrm{loc}_p \circ i_\Sigma)^\sharp \mathrm{Li}_4 &= a_{\tau_q\tau_q\tau_q\tau_2}x_q^3 y_2 + a_{\tau_q\sigma_3}x_q z_3. \end{aligned}$$

The linear combination $a_{\tau_2}a_{\tau_q}\,\mathrm{Li}_2 - a_{\tau_q\tau_2}\log\cdot\mathrm{Li}_1$ clearly pulls back to zero along $\mathrm{loc}_p \circ i_\Sigma$, which yields Equation (3.1). A slightly longer calculation yields the second equation: form a linear combination of Li_4 and $\log\cdot\mathrm{Li}_3$ to eliminate the variable z_3, resulting in a scalar multiple of $x_q^3 y_2$. Then form a linear combination with $\log^3\cdot\mathrm{Li}_1$ to get a function pulling back to zero along $\mathrm{loc}_p \circ i_\Sigma$. ☐

Remark 3.5. Equation (3.1) alone defines the $(1,0)$-refined Chabauty–Kim locus in depth *two*. It was first derived in [BBK+24] and can be rewritten in a more symmetric form as $a_{\tau_2\tau_q}\,\mathrm{Li}_2(z) = a_{\tau_q\tau_2}\,\mathrm{Li}_2(1-z)$.

3.4. Nontrivial Kim functions.

It is not known unconditionally whether Equation (3.2) is nontrivial for every choice of auxiliary prime p. We can however show that there is *some* nontrivial equation of the same shape.

Theorem 3.6. *There exists a nontrivial equation of the form*

$$a\,\mathrm{Li}_4(z) + b\log(z)\,\mathrm{Li}_3(z) + c\log(z)^3\,\mathrm{Li}_1(z) = 0 \tag{3.3}$$

with $a,b,c \in \mathbb{Q}_p$ *which holds on the Chabauty–Kim locus* $X(\mathbb{Z}_p)^{(1,0)}_{\{2,q\},\mathrm{PL},4}$.

Non-triviality means that the coefficients a,b,c are not all zero. In this case, the left hand side of Eq. (3.3) is a nonzero Coleman function on $X(\mathbb{Z}_p)$ by the Zariski-density of the p-adic unipotent Albanese map j_p [Kim09, Theorem 1].

Proof of Theorem 3.6. In the proof of Theorem 3.4, the three monomials Li_4, $\log\cdot\mathrm{Li}_3$, $\log^3\cdot\mathrm{Li}_1$ all pull back under $\mathrm{loc}_p \circ i_\Sigma$ to linear combinations of the two monomials $x_q^3 y_2$, $x_q z_3$. This gives a $\mathbb{Q}_p$-linear map from a 3-dimensional space to a 2-dimensional space, whose kernel must be nontrivial. ☐

Submitted to Algor. Num. Th. Symp.

We can make Theorem 3.6 more concrete: we know that $a_{\tau_2} \neq 0$ and $a_{\tau_q} \neq 0$, so if we knew that $a_{\sigma_3} \neq 0$ as well, then the coefficient of Li_4 in Equation (3.2) would be nonzero and thus the equation would already be nontrivial. If $a_{\sigma_3} = 0$ on the other hand, then

$$a_{\tau_q}^2 a_{\tau_2} \mathrm{Li}_3(z) - a_{\tau_q\tau_q\tau_2} \log(z)^2 \mathrm{Li}_1(z) = 0$$

would be a nontrivial equation which holds on $X(\mathbb{Z}_p)^{(1,0)}_{\{2,q\},\mathrm{PL},4}$. An equation of the form (3.3) can then be obtained by multiplying by $\log(z)$.

It is conjectured that $a_{\sigma_3} \neq 0$ for every choice of auxiliary prime p. Indeed, the constant a_{σ_3} equals the p-adic zeta value $\zeta(3)$ whose non-vanishing is implied by a p-adic period conjecture [CD20a, Conj. 2.25] [Yam10, Conj. 4]. The non-vanshing of $\zeta(3)$ is known when p is a regular prime [Fur03, Rem. 2.20 (i)].

3.5. **Explicit equations for $S = \{2, 3\}$.** Determining the p-adic constants a_u which appear in the equations (3.1) and (3.2) is difficult in general. It is complicated by the fact that their values depend on a choice of free generators $\{\tau_\ell : \ell \in S\} \cup \{\sigma_3, \sigma_5, \dots\}$ for the Lie algebra of the unipotent mixed Tate Galois group $U^{\mathrm{MT}}_{\mathbb{Q},S}$ (see [CD20a, §4.1] for details). Those constants a_u with a single letter as subscript are however canonical: $a_{\tau_\ell} = \log(\ell)$ for $\ell \in S$ are p-adic logarithms, and $a_{\sigma_3} = \zeta(3)$ is a p-adic zeta value. The values $a_{\tau_q\tau_2}$ which appear in Eq. (3.1) are examples of "Dan-Cohen–Wewers coefficients". They are also canonical and we recall in §4.2 how to compute them. The constants in Eq. (3.2) are not known for a general prime q. They have however been computed in the case $S = \{2, 3\}$, exploiting the fact that -3, 3 and 9 are known $\mathbb{Z}[1/6]$-integral points of the thrice-punctured line.

Proposition 3.7. *For a suitable choice of σ_3 we have:*

$$\begin{aligned} a_{\tau_3\tau_2} &= -\mathrm{Li}_2(3), \\ a_{\tau_3\tau_3\tau_2} &= -\mathrm{Li}_3(3), \\ a_{\tau_3\tau_3\tau_3\tau_2} &= -\mathrm{Li}_4(3), \\ a_{\tau_3\sigma_3} &= \frac{18}{13}\mathrm{Li}_4(3) - \frac{3}{52}\mathrm{Li}_4(9). \end{aligned}$$

Proof. The value of $a_{\tau_3\tau_2}$ is derived in [BBK+24, §3.5]. The coefficients $a_{\tau_3\tau_3\tau_3\tau_2}$ and $a_{\tau_3\sigma_3}$ are determined in [CD20a, §4.3.3], and a proof for $a_{\tau_3\tau_3\tau_2}$ (using the same choice of σ_3) can be found in [DJ23, §5.11]. Note that the authors use different notation and conventions. For example $a_{\tau_3\tau_3\tau_3\tau_2}$ is written $f_{\tau_2\tau\tau\tau}$ in [CD20a]. A different expression for $a_{\tau_3\tau_3\tau_3\tau_2}$ is given in [DJ23, §5.23] (denoted $f_{\tau vvv}$ there) but it appears to be incorrect based on numerical evaluation. □

With this the equations for $X(\mathbb{Z}_p)^{(1,0)}_{\{2,3\},\mathrm{PL},4}$ from Theorem 3.4 are completely determined. It is in principle possible to compute the constants a_u for more general sets S; see [Dan20] for an algorithm which achieves this under various conjectures. But if we have enough S-integral points available, which only is the case for $S = \{2, 3\}$, there is a different way to obtain an equation of the form (3.3) which circumvents the problem of determining the a_u, and does not require any non-canonical choices. It uses an argument similar to [Bro17, Cor. 9.1].

Theorem 3.8. *Any z in the Chabauty–Kim locus $X(\mathbb{Z}_p)^{(1,0)}_{\{2,3\},\mathrm{PL},4}$ satisfies*

$$\det\begin{pmatrix} \mathrm{Li}_4(z) & \log(z)\mathrm{Li}_3(z) & \log(z)^3\mathrm{Li}_1(z) \\ \mathrm{Li}_4(3) & \log(3)\mathrm{Li}_3(3) & \log(3)^3\mathrm{Li}_1(3) \\ \mathrm{Li}_4(9) & \log(9)\mathrm{Li}_3(9) & \log(9)^3\mathrm{Li}_1(9) \end{pmatrix} = 0. \tag{3.4}$$

Proof. By Theorem 3.6, some nontrivial equation of the form (3.3) holds on the Chabauty–Kim locus. This means that the vectors

$$(\mathrm{Li}_4(x), \log(x)\,\mathrm{Li}_3(x), \log(x)^3\,\mathrm{Li}_1(x))$$

for $x \in X(\mathbb{Z}_p)^{(1,0)}_{\{2,3\},\mathrm{PL},4}$ lie in some 2-dimensional linear subspace of $\mathbb{Q}_p^3$. In particular, any three vectors of this form are linearly dependent. Taking $x = 3$ and $x = 9$ gives two such vectors since these points belong to $X(\mathbb{Z}[1/6])_{(1,0)}$. □

Remark 3.9. In [Bro17, Cor. 9.1], determinant equations like Eq. (3.4) are derived for *unrefined* Chabauty–Kim loci $X(\mathbb{Z}_p)_{S,\mathrm{PL},n}$ given a sufficient supply of S-integral points. When S has size two, depth $n = 4$ is not sufficient for the unrefined Chabauty–Kim locus to be finite. One needs at least $n = 6$ but then one would need more than $w = 252$ S-integral points to get a determinant equation. Going to even higher depth reduces this to $w = 64$ but this is still too large since $X(\mathbb{Z}[1/2q])$ contains only 21 points for $q = 3$ and even fewer for $q > 3$.

4. Computing Chabauty–Kim loci in depth 2

Let $S = \{2, q\}$ for any odd prime q and let $p \notin S$ be a choice of auxiliary prime. In this section we investigate the depth 2 Chabauty–Kim loci

$$X(\mathbb{Z}_p)^{(1,0)}_{\{2,q\},2}$$

for various combinations of p and q. By [BBK+24, Proposition 3.9], the locus is cut out in $X(\mathbb{Z}_p)$ by the single equation

$$a_{\tau_2}a_{\tau_q}\,\mathrm{Li}_2(z) - a_{\tau_q\tau_2}\log(z)\,\mathrm{Li}_1(z) = 0. \tag{4.1}$$

This is the first of the two functions found in Theorem 3.4 above. We have an inclusion $X(\mathbb{Z}_p)^{(1,1)}_{\{2,q\},2} \subseteq X(\mathbb{Z}_p)^{(1,0)}_{\{2,q\},2}$ as the equations for the $(1,1)$-locus, $\log(z) = \mathrm{Li}_2(z) = 0$, imply Equation (4.1). As a consequence, once we know the locus $X(\mathbb{Z}_p)^{(1,0)}_{\{2,q\},2}$, we actually know the total refined Chabauty–Kim locus $X(\mathbb{Z}_p)^{\min}_{\{2,q\},2}$ by taking S_3-orbits (cf. [BBK+24, Theorem B]).

The problem of finding the solutions in $X(\mathbb{Z}_p)$ to Equation (4.1) is resolved by the code accompanying this paper [Lüd24]. The task can be broken down into the following steps:

1. Determine the constant $a_{\tau_q\tau_2}$ appearing in Eq. (4.1).
2. For each residue disc in $X(\mathbb{Z}_p)$, compute a power series representing the Coleman function on the left hand side of Eq. (4.1) on that disc.
3. For each residue disc, find the p-adic roots of the power series.

Concerning step 1, note that only $a_{\tau_q\tau_2}$ needs to be determined; the constants $a_{\tau_2} = \log(2)$ and $a_{\tau_q} = \log(q)$ are simply given by p-adic logarithms.

4.1. An example.

Before describing the steps of the algorithm in more detail, we demonstrate the function

```
CK_depth_2_locus(p, q, N, a_q2)
```

of the accompanying Sage code. Assume we want to compute the locus $X(\mathbb{Z}_5)^{(1,0)}_{\{2,3\},2}$, i.e., we are looking at the thrice-punctured line over $\mathbb{Z}[1/6]$ (so $q = 3$) and choose the auxiliary prime $p = 5$. The argument N specifices the p-adic precision for the coefficients of power series, and the argument `a_q2` is the constant $a_{\tau_q\tau_2}$, which in the case $q = 3$ is given by $a_{\tau_3\tau_2} = -\mathrm{Li}_2(3)$ by Proposition 3.7. The code

```
p = 5; q = 3
a = -Qp(p)(3).polylog(2)
CK_depth_2_locus(p,q,10,a)
```

outputs the following list of six 5-adic numbers:

```
[2 + O(5^9),
 2 + 4*5 + 4*5^2 + 4*5^3 + 4*5^4 + 4*5^5 + 4*5^6 + 4*5^7 + 4*5^8 + O(5^9),
 3 + O(5^6),
 3 + 5^2 + 2*5^3 + 5^4 + 3*5^5 + O(5^6),
 4 + 4*5 + 4*5^2 + 4*5^3 + 4*5^4 + 4*5^5 + 4*5^6 + 4*5^7 + 4*5^8 + O(5^9),
 4 + 5 + O(5^9)]
```

These form the refined Chabauty–Kim locus $X(\mathbb{Z}_5)^{(1,0)}_{\{2,3\},2}$. This locus must contain the $\{2,3\}$-integral points $\{-3,-1,3,9\}$, as these are the points in $X(\mathbb{Z}[1/6])$ whose mod-2 reduction lies in $X \cup \{1\}$ and whose mod-3 reduction lies in $X \cup \{0\}$. Indeed, we recognise those among the numbers in the list. We moreover observe that $z = 2$ satisfies Eq. (4.1) as a consequence of $\mathrm{Li}_2(2) = 0$ and $\mathrm{Li}_1(2) = -\log(1-2) = 0$, so it belongs to $X(\mathbb{Z}_5)^{(1,0)}_{\{2,3\},2}$ as well. It is a $\{2,3\}$-integral (even $\{2\}$-integral) point of X but we would not a priori expect it to be part of the $(1,0)$-refined locus because it reduces to 0, not 1, modulo 2. Indeed we will see later that it does not survive in depth 4. Finally, there is the exceptional point

$$z_0 = 3 + 5^2 + 2 * 5^3 + 5^4 + 3 * 5^5 + O(5^6) \tag{4.2}$$

which is not a $\{2,3\}$-integral point of X and in fact seems to be transcendental over the rationals. As we noted at the end of [BBK+24], this point is responsible for Kim's Conjecture not holding in depth 2. Again, we will see later that this exceptional solution can be ruled out by going to depth 4.

We now describe the steps for computing $X(\mathbb{Z}_p)^{(1,0)}_{\{2,q\},2}$ in general.

4.2. **Computing DCW coefficients.** The first step consists in computing the p-adic constant $a_{\tau_q\tau_2}$, an example of what is called a "Dan-Cohen–Wewers coefficient" (and denoted by $a_{q,2}$) in [BBK+24]. In some cases, by §3.5 and Lemma 2.2 of loc. cit., we have a simple expression for $a_{\tau_q\tau_2}$:

(1) For $q = 3$ we have $a_{\tau_3\tau_2} = -\mathrm{Li}_2(3) = -\frac{1}{2}\mathrm{Li}_2(-3) = -\frac{1}{6}\mathrm{Li}_2(9)$.
(2) If $q = 2^n + 1$ is a Fermat prime, we have $a_{\tau_q\tau_2} = -\frac{1}{n}\mathrm{Li}_2(q)$.
(3) If $q = 2^n - 1$ is a Mersenne prime, we have $a_{\tau_q\tau_2} = -\frac{1}{n}\mathrm{Li}_2(-q)$.

For general primes q we only have an algorithm for expressing $a_{\tau_q\tau_2}$ as a $\mathbb{Q}$-linear combination of dilogarithms of rational numbers. In general, the DCW coefficients $a_{\tau_\ell\tau_q}$ for $\ell, q \in S$ appear in the localisation map of the Chabauty–Kim diagram (2.1). By Proposition 2.1, they are the coefficients in the bilinear polynomial $\mathrm{loc}_p^\sharp \mathrm{Li}_2 = \sum_{\ell,q\in S} a_{\tau_\ell\tau_q} x_\ell y_q$. An algorithm for computing $a_{\tau_\ell\tau_q}$ for any pair of primes $\ell, q \neq p$ is described in [BBK+24, §2.3], slightly generalising the original algorithm from [DW15, §11]. In short (and simplifying a bit), one considers the $\mathbb{Q}$-vector space

$$E \coloneqq \mathbb{Q} \otimes \mathbb{Q}^\times.$$

Write $[x] \coloneqq 1 \otimes x \in E$ for $x \in \mathbb{Q}^\times$. By Tate's vanishing of the rational Milnor K-group $K_2(\mathbb{Q}) \otimes \mathbb{Q}$ [Mil71, Theorem 11.6], every element of $E \otimes E$ can be written as a $\mathbb{Q}$-linear combination of Steinberg elements $[t] \otimes [1-t]$ where $t \in \mathbb{Q} \smallsetminus \{0,1\}$. Given such a "Steinberg decomposition" in $E \otimes E$

$$[\ell] \otimes [q] = \sum_i c_i \, [t_i] \otimes [1 - t_i] \tag{4.3}$$

for a pair of primes (ℓ, q), a formula for the DCW coefficient $a_{\tau_\ell \tau_q}$ is given by

$$a_{\tau_\ell \tau_q} = -\sum_i c_i \operatorname{Li}_2(t_i). \tag{4.4}$$

The algorithm described in [BBK+24] is slightly more involved in that it computes Steinberg decompositions in the wedge square $E \wedge E$ rather than the tensor square (for efficiency) and takes care to avoid Steinberg elements $[t] \wedge [1-t]$ where t or $1-t$ contains factors of p (to avoid choosing a branch of the p-adic logarithm). In loc. cit., the right hand side of Eq. (4.3) also contains additional terms of the form $[x] \otimes [y] + [y] \otimes [x]$, but those are expressable in terms of Steinberg elements as well, so they can be subsumed under the sum in Eq. (4.3). The algorithm described there is implemented in Sage [KLS22]. It can be used to compute a Steinberg decomposition of $[2] \wedge [q]$ in $E \wedge E$, which can then be passed to the function `depth2_constant` from [Lüd24] to compute the p-adic constant $a_{\tau_q \tau_2}$ with precision N. For example, taking $q = 19$ and $p = 7$, the code

```
p = 7; q = 19
_,dec = steinberg_decompositions(bound=20, p=p)
depth2_constant(p, q, 10, dec[2,q])
```

computes $a_{\tau_{19}\tau_2} \in \mathbb{Q}_7$ as

$$a_{\tau_{19}\tau_2} = 7^2 + 2*7^3 + 6*7^4 + 3*7^5 + 2*7^6 + 6*7^7 + 5*7^8 + O(7^{10}).$$

4.3. **Computing power series.** The second step in the computation of the Chabauty–Kim locus $X(\mathbb{Z}_p)^{(1,0)}_{\{2,q\},2}$ consists in computing on each residue disc a p-adic approximation of the power series representing the defining Coleman function (4.1). We already discussed the computation of the coefficients, so the problem is reduced to finding power series for the polylogarithmic functions $\log(z)$, $\operatorname{Li}_1(z)$, and $\operatorname{Li}_2(z)$. Later we will also need the power series for $\operatorname{Li}_3(z)$ and $\operatorname{Li}_4(z)$, so we discuss here the general problem of computing power series for $\operatorname{Li}_n(z)$ for arbitrary n. In order to achieve this, we adapt the work by Besser and de Jeu [BJ08] which contains an algorithm for computing $\operatorname{Li}_n(z)$ for any $z \in \mathbb{C}_p \smallsetminus \{1\}$. We can exploit the fact that we work in $\mathbb{Z}_p$ rather than $\mathbb{C}_p$ to improve the convergence of the power series.

For each $(p-1)$-st root of unity ζ in $\mathbb{Z}_p$ write U_ζ for its residue disc, consisting of all elements of $\mathbb{Z}_p$ reducing to ζ modulo p. Those residue discs U_ζ with $\zeta \neq 1$ cover $X(\mathbb{Z}_p)$. Any element $z \in U_\zeta$ can be written as $z = \zeta + pt$ with $t \in \mathbb{Z}_p$ and we wish to compute p-adic approximations of the power series in the parameter t for $\log(\zeta + pt)$ and for $\operatorname{Li}_m(\zeta + pt)$ for various m. We denote the coefficients of the latter series by $(a_{m,k})_{k \geq 0}$, so that we have

$$\operatorname{Li}_m(\zeta + pt) = \sum_{k=0}^{\infty} a_{m,k} t^k. \tag{4.5}$$

Submitted to Algor. Num. Th. Symp.

Definition 4.1. Let $f(t) = \sum_{k=0}^{\infty} a_k t^k \in \mathbb{Q}_p[\![t]\!]$ be a convergent power series on the unit disc (i.e., $|a_k|_p \to 0$). A *p-adic approximation of order N* of $f(t)$ consists of a nonnegative integer k_0 along with a polynomial $\tilde{f}(t) = \sum_{k=0}^{k_0-1} \tilde{a}_k t^k \in \mathbb{Q}_p[t]$ of degree $< k_0$ such that $v_p(a_k - \tilde{a}_k) \geq N$ for $k < k_0$ and $v_p(a_k) \geq N$ for all $k \geq k_0$.

For the p-adic logarithm, computing the power series is straightforward:

Lemma 4.2. *Given a prime p and a $(p-1)$-st root of unity $\zeta \neq 1$ in $\mathbb{Z}_p$, the series expansion of $\log(\zeta + pt)$ on U_ζ is given by*

$$\log(\zeta + pt) = -\sum_{k=1}^{\infty} \frac{(-p)^k}{k\zeta^k} t^k. \tag{4.6}$$

If $N \in \mathbb{Z}_{\geq 0}$ is the desired precision, let k_0 be the smallest integer ≥ 1 satisfying $k_0 - \log_p(k_0) \geq N$. Then for all $k \geq k_0$, the coefficient of t^k in (4.6) has valuation $\geq N$. If $\tilde{\zeta} \in \mathbb{Z}_p$ is an approximation of ζ of order N (i.e., $v_p(\zeta - \tilde{\zeta}) \geq N$), then $-\sum_{k=1}^{k_0-1} \frac{(-p)^k}{k\tilde{\zeta}^k} t^k$ is an approximation of (4.6) of order N.

Proof. Since $\log(\zeta) = 0$ for roots of unity, we have

$$\log(\zeta + pt) = \log(1 + pt/\zeta) = -\sum_{k=1}^{\infty} \frac{(-1)^k}{k} (pt/\zeta)^k = -\sum_{k=1}^{\infty} \frac{(-p)^k}{k\zeta^k} t^k$$

as claimed. Let $c_k = -\frac{(-p)^k}{k\zeta^k}$ be the coefficient of t^k, then since $v_p(k) \leq \lfloor \log_p(k) \rfloor$, the valuation of c_k satisfies $v_p(c_k) = k - v_p(k) \geq k - \log_p(k)$. The real-valued function $x \mapsto x - \log_p(x)$ is increasing to the right of its minimum at $x = 1/\log(p)$, in particular it is increasing in the range $x \geq 1$. (The assumptions on ζ imply $p \geq 3$.) Therefore, if the inequality $k_0 - \log_p(k_0) \geq N$ holds for some $k_0 \geq 1$, it also holds for every $k \geq k_0$. This implies that truncating the power series at the k_0-th term gives an approximation of order N. Finally, if $\tilde{\zeta}$ approximates ζ to order N, then $1/\tilde{\zeta}$ approximates $1/\zeta$ to order N as well. Since $v_p((-p)^k/k) \geq 1$ for all $k \geq 1$, one can replace ζ with $\tilde{\zeta}$ in (4.6). ☐

For the polylogarithms Li_m, consider the following computation problem:

Problem 4.3. Given a prime p, a $(p-1)$-st root of unity $\zeta \neq 1$ in $\mathbb{Z}_p$, a nonnegative integer $n \in \mathbb{Z}_{\geq 0}$, and a precision $N \in \mathbb{Z}_{\geq 0}$, compute p-adic approximations of order N of the power series (4.5) of $\mathrm{Li}_m(\zeta + pt)$ for $m = 0, \ldots, n$.

This problem can be split into two subproblems. In order to compute the power series for $\mathrm{Li}_m(\zeta + pt)$ for $m = 0, \ldots, n$ one first needs to compute the values $\mathrm{Li}_m(\zeta)$ at the root of unity ζ, in other words, the constant coefficients of the power series. The algorithm described in [BJ08] proceeds as follows. One considers the modified polylogarithm $\mathrm{Li}_m^{(p)}(z) := \mathrm{Li}_m(z) - \frac{1}{p^m} \mathrm{Li}_m(z^p)$. It admits a power series expansion around ∞ of the form $\mathrm{Li}_m^{(p)}(z) = g_m(1/(1-z))$ with $g_m(v) \in \mathbb{Q}[\![v]\!]$, converging for $|v|_p < p^{1/(p-1)}$. (Note that $g_m(v)$ depends on p, even though this is not apparent from the notation.) For a $(p-1)$-st root of unity $\zeta \neq 1$ one has

$$\mathrm{Li}_m(\zeta) = \frac{p^m}{p^m - 1} \mathrm{Li}_m^{(p)}(\zeta) = \frac{p^m}{p^m - 1} g_m(1/(1-\zeta)).$$

So we turn attention to the following problem:

Problem 4.4. Given a prime p, an integer $n \in \mathbb{Z}_{\geq 0}$, and a precision $M \in \mathbb{Z}_{\geq 0}$, compute p-adic approximations of order M of $g_m(v) \in \mathbb{Q}[\![v]\!]$ for $m = 0, \ldots, n$.

The series $g_m(v)$ can be computed recursively. For $m = 0$, we have

$$g_0(v) = -(1-v) + (1-v)^p \sum_{i=0}^{\infty} (pf(v))^i, \tag{4.7}$$

where $f(v) \in v\mathbb{Z}[v]$ is the polynomial of degree $p-1$ defined by $(1-v)^p - (-v)^p = 1 - pf(v)$.[3] For $m \geq 1$, the power series $g_m(v)$ can be computed from $g_{m-1}(v)$ via

$$g'_m(v) = -\frac{g_{m-1}(v)}{v}(1 + v + v^2 + \ldots) \tag{4.8}$$

and $g_m(0) = 0$. We know estimates for the valuations of the coefficients of $g_m(v)$:

Lemma 4.5. *[BJ08, Prop. 6.1] For $m \geq 1$, let $g_m(v) = b_{m,1}v + b_{m,2}v^2 + \ldots$ be the power series expansion of $g_m(v) \in \mathbb{Q}[\![v]\!]$. The valuations of the coefficients satisfy*

$$v_p(b_{m,k}) \geq \max\left(0, \frac{k}{p-1} - \log_p(k) - c(m,k)\right)$$

for some explicit constant $c(m,p) > 0$.

Here is how we solve Problem 4.4. Given p, n, and M, we first determine $k_0 \in \mathbb{Z}_{\geq 2}$ such that $\frac{k}{p-1} - \log_p(k) - c(m,p) \geq M$ for all $k \geq k_0$ and $m = 0, \ldots, n$. This is straightforward, exploiting the monotonicity properties of the real-valued function $x \mapsto \frac{x}{p-1} - \log_p(x) - c(m,p)$. Then, by Lemma 4.5, in order to approximate $g_m(v)$ to p-adic order M it suffices to compute the first k_0 terms. We start by computing those terms for $g_0(v)$ using Eq. (4.7). Then for $m \geq 1$, we use the recursive formula (4.8), which in terms of the coefficients $b_{m,k}$ reads

$$b_{m,k} = -\frac{1}{k}(b_{m-1,1} + \ldots + b_{m-1,k}) \quad \text{for } k \geq 1, \tag{4.9}$$

as well as $b_{m,0} = 0$. Even though all coefficients are rational numbers, it is more efficient to only store p-adic approximations. We can estimate how many p-adic digits we need: going from $m-1$ to m, the recursive formula (4.9) for $b_{m,k}$ involves a division by k which decreases the precision by $v_p(k)$. But we are only computing coefficients with $k < k_0$, so the loss of precision can be bounded by $\delta := \lfloor \log_p(k_0 - 1) \rfloor$. Knowing $g_0(v)$ to p-adic precision $M + n\delta$ is therefore enough to subsequently compute all of $g_1(v), \ldots, g_n(v)$ to precision at least M.

We now return to Problem 4.3 asking for p-adic approximations of $\mathrm{Li}_m(\zeta + pt)$. They are computed by iterated integration, using the values $\mathrm{Li}_n(\zeta)$ as integration constants:

Lemma 4.6. *The coefficients of $\mathrm{Li}_m(\zeta + pt) = \sum_{k=0}^{\infty} a_{m,k} t^k$ are recursively given as follows. For $m = 0$ we have*

$$\mathrm{Li}_0(\zeta + pt) = \frac{\zeta}{1-\zeta} + \sum_{k=1}^{\infty} \frac{p^k}{(1-\zeta)^{k+1}} t^k. \tag{4.10}$$

For $m \geq 1$ we have $a_{m,0} = \mathrm{Li}_m(\zeta) = \frac{p^m}{p^m - 1} g_m(1/(1-\zeta))$ and

$$a_{m,k} = -\frac{1}{k} \sum_{j=0}^{k-1} \left(-\frac{p}{\zeta}\right)^{k-j} a_{m-1,j} \quad \text{for } k \geq 1. \tag{4.11}$$

[3] Note that the formulas for $g_0(v)$ and $f(v)$ given in the proof of [BJ08, Prop. 6.1] contain sign errors.

Proof. We have $\mathrm{Li}_0(z) = \frac{z}{1-z}$ and $\mathrm{dLi}_m(z) = \mathrm{Li}_{m-1}\frac{\mathrm{d}z}{z}$ for $m \geq 1$ by definition of the polylogarithms as iterated Coleman integrals. An easy calculation shows that this translates into the given formulas for the power series coefficients. □

Lemma 4.7. *The valuations of the coefficients $a_{m,k}$ satisfy $v_p(a_{m,0}) \geq m$ and $v_p(a_{m,k}) \geq k - m\lfloor \log_p(k) \rfloor$ for $k \geq 1$.*

Proof. For $k = 0$, it follows from $a_{m,0} = \mathrm{Li}_m(\zeta) = \frac{p^m}{p^m-1} g_m(1/(1-\zeta))$ and the fact that the coefficients of $g_m(v)$ have valuation ≥ 0 that $a_{m,0}$ has valuation $\geq m$. For $m = 0$, we see from Eq. (4.10) that the coefficient of t^k has valuation exactly k. Let $m \geq 1$ and assume the hypothesis for $m-1$. In the recursive formula (4.11) for computing the $a_{m,k}$ from the $a_{m-1,j}$ with $j < k$, the summands with $j \geq 1$ satisfy

$$\begin{aligned} v_p\left(-\frac{1}{k}\left(-\frac{p}{\zeta}\right)^{k-j} a_{m-1,j}\right) &= k - j - v_p(k) + v_p(a_{m-1,j}) \\ &\geq k - j - v_p(k) + j - (m-1)\lfloor \log_p(j) \rfloor \\ &\geq k - m\lfloor \log_p(k) \rfloor. \end{aligned}$$

The summand for $j = 0$ also satisfies this since $v_p(a_{m-1,0}) \geq m-1$. Hence, from Eq. (4.11) we find $v_p(a_{m,k}) \geq k - m\lfloor \log_p(k) \rfloor$ as claimed. □

In order to compute p-adic approximations of order N to the power series of $\mathrm{Li}_m(\zeta + pt)$ for $m = 0, \ldots, n$, we first determine $k_0 \geq 1$ such that $k - n\lfloor \log_p(k) \rfloor \geq N$ for all $k \geq k_0$. Then, by Lemma 4.7, it suffices to find order N approximations of the coefficients $a_{m,k}$ with $k < k_0$. In the recursive formula (4.11) for $a_{m,k}$, the division by k causes a loss of precision by $v_p(k) \leq \lfloor \log_p(k_0 - 1) \rfloor$. On the other hand, each $a_{m-1,j}$ is multiplied by at least one factor of p. Thus, in order to compute $a_{m,k}$ to precision N it suffices to compute the $a_{m-1,j}$ to precision $N + \delta - 1$, where

$$\delta \coloneqq \lfloor \log_p(k_0 - 1) \rfloor.$$

This tells us two things: firstly, setting

$$M \coloneqq \max(N, N + n(\delta - 1)),$$

it suffices to compute the power series $g_m(v)$ for $m = 0, \ldots, n$ to precision M. This is achieved by the algorithm for Problem 4.4 above. Secondly, we get an estimate on how many p-digits we need to store for each coefficient.

Lemma 4.8. *In order to compute $a_{m,k}$ for $k < k_0$ and $m = 0, \ldots, n$ with precision N, no more than M p-adic digits are needed for each coefficient.*

Proof. If $\delta \leq 1$, no precision is lost and no negative valuations occur when going from $m-1$ to m, so knowing the first N $(= M)$ p-adic digits of the coefficients $a_{0,k} \in \mathbb{Z}_p$ is enough to compute the first N digits of $a_{m,k} \in \mathbb{Z}_p$ for all $m = 1, \ldots, n$. If $\delta \geq 2$ on the other hand, we compute the $a_{0,k} \in \mathbb{Z}_p$ to precision $M = N + n(\delta - 1)$. Subsequently, each step from $m-1$ to m decreases both the precision and the valuations by up to $\delta - 1$, so that we end at $m = n$ with precision N and valuation $\geq -n(\delta - 1)$, still requiring only M digits. □

The algorithms outlined above for solving Problems 4.3 and 4.4 are implemented in the functions `compute_g` and `compute_polylog_series` of the accompanying Sage code [Lüd24].

4.4. **Finding roots of power series.** Consider the following problem.

Problem 4.9. Given a p-adic approximation of order N of a power series $f(t) \in \mathbb{Q}_p[\![t]\!]$ which converges on $\mathbb{Z}_p$, determine the set of roots of f in $\mathbb{Z}_p$.

After rescaling by a power of p, one can assume that the power series has coefficients in $\mathbb{Z}_p$ and has nonzero reduction mod p. Then, in principle, finding the roots of $f(t)$ is achieved by Hensel lifting. There are however some subtleties to take into account if we are only given a p-adic approximation of $f(t)$.

(1) Knowing $f(t)$ to precision N might not be enough to decide whether a root modulo p^N lifts to a root in $\mathbb{Z}_p$. For example, the polynomials $f_1(t) = t^2 - 1$ and $f_2(t) = t^2 - 5$ over $\mathbb{Z}_2$ agree modulo 4 but the roots ± 1 in $\mathbb{Z}/4\mathbb{Z}$ only lift to roots in $\mathbb{Z}_2$ of f_1, not of f_2.
(2) Even if the roots of $f(t)$ modulo p^N lift to roots in $\mathbb{Z}_p$, those roots might be determined only up to a lower precision. This happens if the root is not a simple root modulo p. For example, $f_1(t) = t^2 - 1$ and $f_2(t) = t^2 - 9$ agree modulo 8 but their zero sets $\{1, -1\}$ and $\{-3, 3\}$ agree only modulo 4.

The function `polrootspadic` of PARI/GP (which can also be called from Sage) unfortunately does not take the aforementioned issues with inexact coefficients into account. Therefore, we implemented a function `Zproots` ourselves, also available at https://github.com/martinluedtke/RefinedCK, which solves Problem 4.9 while taking care of precision questions. For example, the Sage code

```
K = Qp(2,prec=2)
R.<t> = K['t']
Zproots(t^2-1)  # => PrecisionError
```

results in a `PrecisionError` since the precision 2 is not enough to decide whether the roots ± 1 in $\mathbb{Z}/4\mathbb{Z}$ lift to $\mathbb{Z}_2$. On the other hand, increasing the precision to 3,

```
K = Qp(2,prec=3)
R.<t> = K['t']
Zproots(t^2-1)  # => [1 + O(2^2), 1 + 2 + O(2^2)]
```

correctly finds $\{1 + O(2^2), 3 + O(2^2)\}$ as the set of roots in $\mathbb{Z}_2$, those roots being determined modulo 4.

The precise version of Hensel's Lemma being used is the following:

Lemma 4.10 ([Con, Theorem 8.2])**.** *Let $f(t) \in \mathbb{Z}_p[\![t]\!]$ be a power series which converges on $\mathbb{Z}_p$. Let $a \in \mathbb{Z}_p$ and set $d := v_p(f'(a))$. If $d < v_p(f(a))/2$, then there is a unique $\alpha \in a + p^{d+1}\mathbb{Z}_p$ such that $f(\alpha) = 0$. Moreover, $v_p(\alpha - a) = v_p(f(a)) - d$.*

From this we obtain the following proposition which says exactly to which precision the roots of an inexact power series can be known.

Proposition 4.11. *Let $f(t)$ and $\tilde{f}(t)$ be two power series in $\mathbb{Z}_p[\![t]\!]$ which converge on $\mathbb{Z}_p$ and satisfy $f \equiv \tilde{f} \bmod p^N\mathbb{Z}_p[\![t]\!]$. Let $a \in \mathbb{Z}_p$ and set $\tilde{d} := v_p(\tilde{f}'(a))$. If $\tilde{d} < N/2$ and $\tilde{d} < v_p(\tilde{f}(a))/2$, then f and $\tilde{f}$ each have a unique root α resp. $\tilde{\alpha}$ in $a + p^{\tilde{d}+1}\mathbb{Z}_p$, and the roots satisfy $v_p(\alpha - \tilde{\alpha}) \geq N - \tilde{d}$.*

Proof. Since $f \equiv \tilde{f} \bmod p^N\mathbb{Z}_p[\![t]\!]$, also $f' \equiv \tilde{f}' \bmod p^N\mathbb{Z}_p[\![t]\!]$ and thus $f'(a) \equiv \tilde{f}'(a) \bmod p^N$. The valuation $\tilde{d}$ of $\tilde{f}'(a)$ is smaller than $N/2 < N$ by assumption, so we get $d \coloneqq v_p(f'(a)) = v_p(\tilde{f}'(a)) = \tilde{d}$. Moreover, we have

$$v_p(f(a)) \geq \min(v_p(f(a) - \tilde{f}(a)), v_p(\tilde{f}(a))) \geq \min(N, v_p(\tilde{f}(a))) > 2\tilde{d} = 2d,$$

where both assumptions on $\tilde{d}$ are used in the strict inequality. Thus, by Lemma 4.10, f and $\tilde{f}$ both have a unique root α resp. $\tilde{\alpha}$ in $a + p^{\tilde{d}+1}\mathbb{Z}_p$, proving the first part of the proposition. We now verify the hypotheses of Lemma 4.10 for f again but with $\tilde{\alpha}$ in place of a. Since $\tilde{\alpha} \equiv a \bmod p^{\tilde{d}+1}$, also $f'(\tilde{\alpha}) \equiv f'(a) \bmod p^{\tilde{d}+1}$, thus $v_p(f'(\tilde{\alpha})) = v_p(f'(a)) = \tilde{d}$. Also, we have $f(\tilde{\alpha}) \equiv \tilde{f}(\tilde{\alpha}) = 0 \bmod p^N$, hence $v_p(f(\tilde{\alpha})) \geq N > 2\tilde{d}$. Now, by Lemma 4.10, f has a unique root in $\tilde{\alpha} + p^{d+1}\mathbb{Z}_p$. But this root must necessarily be α. Now the “moreover” statement of Lemma 4.10 yields $v_p(\alpha - \tilde{\alpha}) = v_p(f(\tilde{\alpha})) - \tilde{d} \geq N - \tilde{d}$. □

Based on Proposition 4.11, we obtain an algorithm to resolve Problem 4.9. Assume that a power series $f(t) \in \mathbb{Z}_p[\![t]\!]$ is given to p-adic precision N. Suppose we want to find the roots of f in a p-adic disc $a + p^m\mathbb{Z}_p$ for some $a \in \mathbb{Z}_p$ and $m \geq 0$, and suppose we know that

$$v_p(f'(a)) \geq m - 1, \quad v_p(f(a)) \geq 2(m-1). \tag{4.12}$$

(At the beginning of the algorithm we take $a = 0$ and $m = 0$ to search in all of $\mathbb{Z}_p$.) We assume also that $N \geq 2m - 1$. For any $a + p^m b$ in $a + p^m\mathbb{Z}_p$, using $v_p(f'(a)) \geq m - 1$ we have

$$f(a + p^m b) \equiv f(a) + p^m b f'(a) \equiv f(a) \bmod p^{2m-1},$$

therefore $f(a) \equiv 0 \bmod p^{2m-1}$ is a necessary condition for the existence of roots in $a + p^m\mathbb{Z}_p$. Since f is known to precision N and we have $N \geq 2m-1$, we can check whether this condition is satisfied. Assume that this is the case. Then we check whether $d \coloneqq v_p(f'(a))$ is equal to $m - 1$. If yes, then by Hensel's Lemma, there is a unique root in $a + p^m\mathbb{Z}_p$, and by Proposition 4.11, knowing f to precision N determines this root to precision $N - d$. It is computed by Newton iteration, starting with the value a. If $d \geq m$ on the other hand, the congruence $f(a+p^m b) \equiv f(a)$ holds even modulo p^{2m}, so if $f(a) \not\equiv 0 \bmod p^{2m}$ (which requires $N \geq 2m$ to check), then we can conclude that there are no roots in $a+p^m\mathbb{Z}_p$. Otherwise, we continue to search in the smaller discs $a + ip^m + p^{m+1}\mathbb{Z}_p$ for $i = 0, \ldots, p-1$, which form a partition of $a + p^m\mathbb{Z}_p$. The conditions (4.12) are satisfied for each of these smaller discs where a is replaced by $a + ip^m$ and m is replaced by $m + 1$. Assuming that $N \geq 2m + 1$, we can proceed as before for each of them. Overall, this leads to the search space $\mathbb{Z}_p$ being explored in a tree-like manner, recursively subdividing into smaller and smaller discs until we can either decide that they don't contain a root, that they contain exactly one root, or they have become too small relative to the precision N to detect the roots, in which case the algorithm will fail with a `PrecisionError`.

Remark 4.12. In finite precision, a power series with a repeated root in $\mathbb{Z}_p$ cannot be distinguished from a power series which has two roots lying very close to each other. The algorithm will always raise a `PrecisionError` in this case. If on the other hand f has only simple roots in $\mathbb{Z}_p$, the outlined algorithm will be able to determine those roots when f is specified with sufficiently large precision.

5. Analysis of depth 2 loci

Using the methods described in §4, we have computed the Chabauty–Kim loci $X(\mathbb{Z}_p)^{(1,0)}_{\{2,q\},2}$ for many p and q. Complete data can be found on GitHub [Lüd24].

p	5	7	11	13	17	19	23	29	31	...	1091	1093	1097	...
$\#X(\mathbb{Z}_p)^{(1,0)}_{\{2,3\},2}$	6	8	18	16	22	20	20	26	36	...	1076	2154	1078	...

Table 5.1. Sizes of the depth 2 Chabauty–Kim loci $X(\mathbb{Z}_p)^{(1,0)}_{\{2,3\},2}$ for various choices of auxiliary prime p

p	3	5	7	11	13	17	19	23	29	31	37	41	43	47
$\#X(\mathbb{Z}_p)^{(1,0)}_{\{2,5\},2}$	3	–	6	10	8	12	18	24	38	28	36	34	50	44
$\#X(\mathbb{Z}_p)^{(1,0)}_{\{2,7\},2}$	3	6	–	10	12	15	18	22	32	38	36	44	38	44
$\#X(\mathbb{Z}_p)^{(1,0)}_{\{2,11\},2}$	3	6	6	–	8	14	18	18	38	28	40	34	36	48
$\#X(\mathbb{Z}_p)^{(1,0)}_{\{2,19\},2}$	2	4	8	8	18	20	–	20	30	26	36	44	78	44

Table 5.2. Sizes of the depth 2 Chabauty–Kim loci $X(\mathbb{Z}_p)^{(1,0)}_{\{2,q\},2}$ for $q = 5, 7, 11, 19$ and $p < 50$

5.1. **Observations.** Taking $q = 3$, Table 5.1 shows the size of $X(\mathbb{Z}_p)^{(1,0)}_{\{2,3\},2}$ for a few choices of auxiliary prime p. We have computed these loci for all primes $p < 5000$ and made the following observations:

(1) The size of the locus is even in each case.
(2) Each residue disc of $X(\mathbb{Z}_p)$ contains either 0 or 2 points of $X(\mathbb{Z}_p)^{(1,0)}_{\{2,3\},2}$.
(3) For most primes, the locus is roughly of size p, so the $p-2$ residue discs are split more or less evenly between containing two points and containing no points of the locus.
(4) When p is equal to one of the two known Wieferich primes 1093 and 3511, the locus is of size $\approx 2p$. For $p = 1093$ only 14 residue discs contain no points. These are stable under the S_3-action and include the residue discs of $i = \sqrt{-1}$ and the primitive 6-th roots of unity ζ_6. For $p = 3511$, only 2 residue discs contain no points of the locus, namely those of ζ_6 and ζ_6^{-1}.

Similar observations hold for primes q other than 3. We have computed the size of the depth 2 loci $X(\mathbb{Z}_p)^{(1,0)}_{\{2,q\},2}$ for all $q < 100$ and $p < 1000$; an excerpt is shown in Table 5.2. For $p = 3$, the locus always has size 2 or 3. This is a general fact proved in [BBK+24, Prop. 3.14]. For $p \geq 5$, most of the time the size of the locus is even, but it can occasionally be odd; for example the size is 15 for $p = 17$ and $q = 7$. Also, the size is usually close to p, but in a few cases it is close to $2p$. The latter always occurs if p is one of the known Wieferich primes 1093 and 3511, but occasionally it happens for non-Wieferich p as well; for example, Table 5.2 shows that the locus for $q = 19$ and $p = 43$ has size 78.

5.2. **Newton polygon analysis.** We can explain many of these observations by analysing the Newton polygons of the power series defining the Chabauty–Kim locus $X(\mathbb{Z}_p)^{(1,0)}_{\{2,q\},2}$. Setting $a := \frac{a_{\tau_q \tau_2}}{a_{\tau_2} a_{\tau_q}}$, this locus is defined in $X(\mathbb{Z}_p)$ by the function

$$f(z) := \mathrm{Li}_2(z) - a \log(z) \mathrm{Li}_1(z). \tag{5.1}$$

Lemma 5.1. *Let $\zeta \neq 1$ be a $(p-1)$-st root of unity in $\mathbb{Z}_p$. Then the first three coefficients of the power series $f(\zeta + pt) = \sum_{k=0}^{\infty} c_k t^k \in \mathbb{Q}_p[\![t]\!]$ are given by*

$$c_0 = \mathrm{Li}_2(\zeta),$$
$$c_1 = p(1-a)\frac{\mathrm{Li}_1(\zeta)}{\zeta},$$
$$c_2 = p^2(1-2a)\frac{1}{2\zeta(1-\zeta)} - p^2(1-a)\frac{\mathrm{Li}_1(\zeta)}{2\zeta^2}.$$

Proof. The k-th coefficient of $f(\zeta + pt)$ is given by $p^k f^{(k)}(\zeta)/k!$. Computing the first two derivatives of $f(z)$ is straightforward using the differential equations $\mathrm{Li}_2'(z) = \mathrm{Li}_1(z)/z$ and $\mathrm{Li}_1'(z) = 1/(1-z)$. Plugging in ζ and using $\log(\zeta) = 0$ gives the claimed formulas. ☐

Proposition 5.2. *Let q be an odd prime and let $p \geq 5$ be a prime not equal to q. Set $a := \frac{a_{\tau_q \tau_2}}{a_{\tau_2} a_{\tau_q}}$ and assume that $v_p(a) < 0$ or $a \not\equiv \frac{1}{2} \bmod p$. Then the Chabauty–Kim set $X(\mathbb{Z}_p)^{(1,0)}_{\{2,q\},2}$ contains at most 2 points from each residue disc.*

Proof. Let $\nu := v_p(a)$ and assume first that $\nu = v_p(a) < 0$. Let $\zeta \neq 1$ be a $(p-1)$-st root of unity in $\mathbb{Z}_p$. By Lemma 5.1, the valuations of the first three coefficients of $f(\zeta + pt)$ are ≥ 2, $\geq 2 + \nu$, $= 2 + \nu$, respectively. It follows from Lemma 4.7 that the k-th coefficients of both $\mathrm{Li}_2(\zeta + pt)$ and $\log(\zeta + pt)\,\mathrm{Li}_1(\zeta + pt)$ have valuation $\geq k - 2\lfloor \log_p(k) \rfloor$. For $k \geq 3$ this is always ≥ 3, so that all coefficients of $f(\zeta + pt)$ for $k \geq 3$ have valuation $\geq 3 + \nu$. In conclusion, the minimal valuation of all coefficients is equal to $2 + \nu$; it is attained at the t^2-coefficient and this is the last time it is attained. By Strassmann's Theorem it follows that $f(z)$ has at most 2 zeros on U_ζ.

Assume now that $\nu = v_p(a) \geq 0$ and $a \not\equiv \frac{1}{2} \bmod p$. In this case the first three coefficients of $f(\zeta + pt)$ have valuations ≥ 2, ≥ 2, $= 2$, respectively, and all other coefficients have larger valuation. We conclude again by Strassmann's Theorem. ☐

Remark 5.3. From [Bet23, Lemma 7.0.5] one has an a priori bound of

$$\#X(\mathbb{Z}_p)^{(1,0)}_{\{2,q\},2} \leq 8(p-2) + \frac{8(p-1)}{\log(p)}$$

for all $p \neq q$. When Proposition 5.2 applies, we get the improved bound

$$\#X(\mathbb{Z}_p)^{(1,0)}_{\{2,q\},2} \leq 2(p-2)$$

since there are $p-2$ residue discs, each containing at most 2 points of the locus. This bound is sometimes attained, e.g., $\#X(\mathbb{Z}_{29})^{(1,0)}_{\{2,41\},2} = 54 = 2 \cdot (29-2)$.

In Proposition 5.2, the valuation of $a = \frac{a_{\tau_q \tau_2}}{a_{\tau_2} a_{\tau_q}}$ is determined by the valuation of $a_{\tau_q \tau_2}$ and the valuations of the p-adic logarithms $a_{\tau_2} = \log(2)$ and $a_{\tau_q} = \log(q)$. About the first we can show the following:

Lemma 5.4. *For fixed q, we have $v_p(a_{\tau_q \tau_2}) \geq 2$ for all but finitely many p.*

Proof. Recall from §4.2 that there are rational numbers $c_i \in \mathbb{Q}$ and $t_i \in \mathbb{Q} \setminus \{0, 1\}$ (independent of p) such that $a_{\tau_q \tau_2} = -\sum_i c_i \,\mathrm{Li}_2(t_i)$. Analysing the coefficients of the power series of $\mathrm{Li}_2(\zeta + pt)$ as in the proof of Proposition 5.2, one sees that for $p \geq 3$ all coefficients have valuation ≥ 2, so that $v_p(\mathrm{Li}_2(x)) \geq 2$ for all $x \in \mathbb{Z}_p$ with $x \not\equiv 0, 1 \bmod p$. In particular, if p is not any of the finitely many primes occuring in the prime factorisation of c_i, t_i or $1 - t_i$, then $v_p(a_{\tau_q \tau_2}) \geq 2$. ☐

The valuation of a p-adic logarithm is related to the Wieferich property. Recall that p is called a *base-b Wieferich prime* if $b^{p-1} \equiv 1 \bmod p^2$. A base-2 Wieferich prime is simply called a Wieferich prime.

Lemma 5.5. *Let p be an odd prime and let $b > 1$ be an integer not divisible by p. The valuation of the p-adic logarithm $\log(b)$ is given by $v_p(\log(b)) = v_p(b^{p-1} - 1)$. In particular, $v_p(\log(b)) > 1$ if and only if p is a base-b Wieferich prime.*

Proof. We have $\log(b) = \frac{1}{p-1} \log(b^{p-1})$, hence the p-adic valuation of $\log(b)$ agrees with the valuation of $\log(b^{p-1})$. By Fermat's little theorem, $b^{p-1} \equiv 1 \bmod p$. For $x \in 1 + p\mathbb{Z}_p$ one has $v_p(\log(x)) = v_p(x - 1)$. The claim follows. □

It is conjectured that infinitely many Wieferich primes exist, although they occur very scarcely. Heuristically, the number of Wieferich primes below x grows like $\log(\log(x))$. The only currently known Wieferich primes are 1093 and 3511. Interestingly, it is also not known whether there are infinitely many *non*-Wieferich primes, although this would follow from the abc conjecture [Sil88].

5.3. **Large loci.** We can explain the observation that $\#X(\mathbb{Z}_p)^{(1,0)}_{\{2,q\},2} \approx 2p$ when p is a base-2 or base-q Wieferich prime. Usually the inequality $v_p(a_{\tau_q\tau_2}) \geq 2$ from Lemma 5.4 is an equality. In this case, the Wieferich property and Lemma 5.5 imply that the valuation ν of $a = \frac{a_{\tau_q\tau_2}}{a_{\tau_2}a_{\tau_q}}$ is negative. For most ζ we have $v_p(\mathrm{Li}_1(\zeta)) = 1$ (the primitive 6-th roots of unity being an exception). Then the first three coefficients of $f(\zeta + pt)$ from Lemma 5.1 have valuations ≥ 2, $= 2 + \nu$, $= 2 + \nu$, respectively, and all subsequent coefficients have larger valuation. The Newton polygon has then exactly two segments of non-positive slope: negative slope from 0 to 1 and slope zero from 1 to 2. It follows that $f(z)$ has exactly two roots in the residue disc U_ζ. With most of the $p - 2$ residue discs containing 2 points, the Chabauty–Kim locus contains roughly $2p$ points in total.

This explains why the Chabauty–Kim loci are exceptionally large when $p = 1093$ or $p = 3511$ since these are base-2 Wieferich primes. It also explains why the locus for $q = 19$ and $p = 43$ is exceptionally large since 43 is a base-19 Wieferich prime. Another large locus (of size 42) occurs for $q = 47$ and $p = 23$. This one is not explained by a Wieferich property but rather the fact that the valuation $v_{23}(a_{\tau_{47}\tau_2}) = 1$ is smaller than expected. The prime $p = 23$ belongs to the finitely many exceptions in Lemma 5.4, causing $\nu = v_p(a) = -1$ to be negative.

5.4. **Typical loci.** We can also explain heuristically why $\#X(\mathbb{Z}_p)^{(1,0)}_{\{2,q\}} \approx p$ almost always when p is not a base-2 or base-q Wieferich prime. Typically, $a_{\tau_q\tau_2}$ has valuation 2, so that $a = \frac{a_{\tau_q\tau_2}}{a_{\tau_2}a_{\tau_q}}$ has valuation $\nu = 0$. Consider first the case that $a \not\equiv \frac{1}{2} \bmod p$. For most ζ we have $v_p(\mathrm{Li}_2(\zeta)) = 2$. On the residue discs of such ζ, the valuations of the first three coefficients of $f(\zeta + pt)$ given in Lemma 5.1 are then $= 2, \geq 2, = 2$, respectively, and all subsequent coefficients have valuation ≥ 3. After normalising, the power series reduces to a polynomial in $\mathbb{F}_p[t]$ of degree 2 with nonzero constant coefficient. If its discriminant behaves like a random element in $\mathbb{F}_p$, the cases of having two simple roots or no roots in $\mathbb{F}_p$ should occur about half of the time each, with a small leftover probability of $1/p$ of having a double root. By Hensel's lemma, we can therefore expect the $p - 2$ residue discs to be split roughly evenly between containing 0 points and 2 points of the Chabauty–Kim locus, amounting to $\approx p$ points in total.

Assume now that $a \equiv \frac{1}{2} \bmod p$. In this case, using that $v_p(\mathrm{Li}_1(\zeta)) = 1$ for most $(p-1)$-st roots of unity ζ (primitive 6-th roots of unity being an exception), the Newton polygon of $f(\zeta + pt)$ usually has just a single non-positive slope, so that almost all residue discs contain exactly 1

Submitted to Algor. Num. Th. Symp.

point of the locus. The total size is then $\approx p$ as well, despite distributing differently over the residue discs than in the case $a \not\equiv \frac{1}{2} \bmod p$.

6. Verifying Kim's Conjecture

We now verify instances of Conjecture 1.1 for the thrice-punctured line over $\mathbb{Z}[1/6]$ in depth 4, saying that the refined Chabauty–Kim locus $X(\mathbb{Z}_p)^{\min}_{\{2,3\},4}$ consists exactly of the 21 points

$$X(\mathbb{Z}[1/6]) = \left\{2, \frac{1}{2}, -1, 3, \frac{1}{3}, \frac{2}{3}, \frac{3}{2}, -\frac{1}{2}, -2, 4, \frac{1}{4}, \frac{3}{4}, \frac{4}{3}, -\frac{1}{3}, -3, 9, \frac{1}{9}, \frac{8}{9}, \frac{9}{8}, -\frac{1}{8}, -8\right\}.$$

(Finding $X(\mathbb{Z}[1/6])$ boils down to finding all pairs of consecutive integers containing only the prime factors 2 and 3. The fact that $(1,2),(2,3),(3,4),(8,9)$ is a complete list of such pairs was proved in 1342 by Gersonides, also known as Levi ben Gershon. The proof was published in his book *The Harmony of Numbers*.)

Recall from Lemma 3.1 that it suffices to verify Conjecture 2.3 for the polylogarithmic depth 4 quotient of the fundamental group and for the two refinement conditions $\Sigma = (1,1)$ and $\Sigma = (1,0)$. Recall also that the conjecture for $\Sigma = (1,1)$ was already checked for all $p < 10^5$ in [BBK+24, Remark 3.6] (and is proved in higher depth for arbitrary p, see Remark 3.3.) Therefore it is enough to look at the case $\Sigma = (1,0)$ and show that the inclusion

$$\{-3,-1,3,9\} = X(\mathbb{Z}[1/6])_{(1,0)} \subseteq X(\mathbb{Z}_p)^{(1,0)}_{\{2,3\},\mathrm{PL},4}$$

is an equality. As shown in §3, the locus in question is defined by the two equations

$$f_2(z) := \log(2)\log(3)\operatorname{Li}_2(z) + \operatorname{Li}_2(3)\log(z)\operatorname{Li}_1(z) = 0, \tag{6.1}$$

$$f_4(z) := \det\begin{pmatrix} \operatorname{Li}_4(z) & \log(z)\operatorname{Li}_3(z) & \log(z)^3\operatorname{Li}_1(z) \\ \operatorname{Li}_4(3) & \log(3)\operatorname{Li}_3(3) & \log(3)^3\operatorname{Li}_1(3) \\ \operatorname{Li}_4(9) & \log(9)\operatorname{Li}_3(9) & \log(9)^3\operatorname{Li}_1(9)\end{pmatrix} = 0. \tag{6.2}$$

The first equation (6.1) defines the depth 2 Chabauty–Kim locus $X(\mathbb{Z}_p)^{(1,0)}_{\{2,3\},2}$ and we explained in §4 how it can be computed. In order to verify Kim's Conjecture in depth 4 it suffices to check that $f_4(z) \neq 0$ for every point z of the depth 2 locus which is not in $\{-3,-1,3,9\}$.

We demonstrate this for $p = 5$, continuing the example from §4.1. There we found that the depth 2 locus contains two points in addition to $\{-3,-1,3,9\}$: one of them is $z = 2$ and the other is given in (4.2). In Sage, we can define the depth 4 function f_4 from Eq. (6.2) as follows:

```
# p-adic polylogarithms
K = Qp(5)
log = lambda z: K(z).log()
Li = [lambda z,n=n: K(z).polylog(n) for n in range(5)]

# our depth-4 function
def f(z):
    rows = [[Li[4](x), log(x)*Li[3](x), log(x)^3*Li[1](x)] for x in [z,3,9]]
    return matrix(rows).determinant()
```

We can check that the depth 4 function does indeed vanish on $-3, -1, 3, 9$:

```
f(-3)  # => O(5^20)
f(-1)  # => O(5^28)
f(3)  # => O(5^20)
f(9)  # => O(5^20)
```

Now we verify that the function does *not* vanish on the extra points 2 and z_0:

```
f(2)
# => 4*5^13 + 4*5^14 + 3*5^15 + 5^16 + 3*5^18 + 3*5^19 + O(5^20)
f(3 + 5^2 + 2*5^3 + 5^4 + 3*5^5 + 5^6 + 5^7 + 5^9 + 2*5^10 + 3*5^11 + 2*5^12 + O(5^13))
# => 4*5^13 + O(5^14)
```

This shows that Conjecture 1.1 holds for $S = \{2, 3\}$ and $p = 5$.

The accompanying Sage code has a function

`CK_depth_4_locus(p, q, N, coeffs)`

which computes an approximation of the locus $X(\mathbb{Z}_p)^{(1,0)}_{\{2,q\},\mathrm{PL},4}$ for any p and q. It takes the tuple of p-adic coefficients $(a_{\tau_q\tau_2}, a, b, c)$ as an argument, where $a_{\tau_q\tau_2}$ is the DCW coefficient appearing in the depth 2 function (1.1), and (a, b, c) are the coefficients in the depth 4 function (1.2). At the moment we only know all these constants explicitly in the case $q = 3$ where $a_{\tau_3\tau_2} = -\operatorname{Li}_2(3)$ and for (a, b, c) one can either use the formulas from Proposition 3.7 or 2×2-minors of the matrix in (6.2). The code is however flexible enough to compute the Chabauty–Kim loci for other primes q in the future. The function `Z_one_sixth_coeffs(p,N)` can be used to compute the p-adic coefficients for $q = 3$ conveniently. Let us use this to determine the depth 4 locus for $p = 7$:

```
p = 7; q = 3; N = 10
coeffs = Z_one_sixth_coeffs(p,N)
CK_depth_4_locus(p,q,N,coeffs)
```

This outputs the following list of 7-adic numbers:

```
[2 + 7 + O(7^9),
 3 + O(7^9),
 4 + 6*7 + 6*7^2 + 6*7^3 + 6*7^4 + 6*7^5 + 6*7^6 + 6*7^7 + 6*7^8 + O(7^9),
 6 + 6*7 + 6*7^2 + 6*7^3 + 6*7^4 + 6*7^5 + 6*7^6 + 6*7^7 + O(7^8)]
```

These are precisely the $\{2, 3\}$-integral points $9, 3, -3, -1$, which shows that Kim's Conjecture for $S = \{2, 3\}$ also holds with the auxiliary prime $p = 7$.

Remark 6.1. Computing the common zero set of two inexact functions is not a well-posed problem. For the locus defined by $f_2(z) = f_4(z) = 0$ we can only compute approximations of the roots of f_2 and check whether $f_4(z)$ is *indistinguishable* from 0 up to the given precision. If the precision is chosen too low one might not be able to rule out certain points to be roots of f_4 and end up with a too large set. However, in all cases we considered, increasing the precision if necessary, we were always able to eliminate all points other than the four points $\{-3, -1, 3, 9\}$ which we know to be common zeros of f_2 and f_4.

Computing depth 4 loci by the methods layed out in this paper we have verified:

Theorem 6.2. *Kim's Conjecture for $S = \{2, 3\}$ and refinement condition $\Sigma = (1, 0)$ holds for the polylogarithmic depth 4 quotient, i.e., the inclusion*

$$\{-3, -1, 3, 9\} = X(\mathbb{Z}[1/6])_{(1,0)} \subseteq X(\mathbb{Z}_p)^{(1,0)}_{\{2,3\},\mathrm{PL},4}$$

is an equality, for all auxiliary primes p with $5 \leq p < 10{,}000$.

Corollary 6.3. *Conjecture 1.1 for $S = \{2, 3\}$ holds in depth 4 for all auxiliary primes p with $5 \leq p < 10{,}000$.*

References

[BBK+24] A. Best, L. A. Betts, T. Kumpitsch, M. Lüdtke, A. McAndrew, L. Qian, E. Studnia, and Y. Xu. "Refined Selmer equations for the thrice-punctured line in depth two". In: *Math. Comp.* 93 (2024), pp. 1497–1527.

[BD20] L. A. Betts and N. Dogra. *The local theory of unipotent Kummer maps and refined Selmer schemes*. 2020. arXiv: `1909.05734v2 [math.NT]`.

[BDKW18] J. S. Balakrishnan, I. Dan-Cohen, M. Kim, and S. Wewers. "A non-abelian conjecture of Tate–Shafarevich type for hyperbolic curves". In: *Mathematische Annalen* 372.1-2 (2018), pp. 369–428.

[Bet23] L. A. Betts. "Weight filtrations on Selmer schemes and the effective Chabauty–Kim method". In: *Compositio Mathematica* 159.7 (2023), pp. 1531–1605.

[BJ08] A. Besser and R. de Jeu. "$\mathrm{Li}^{(p)}$-service? An algorithm for computing p-adic polylogarithms". In: *Math. Comp.* 77.262 (2008), pp. 1105–1134.

[BKL23] L. A. Betts, T. Kumpitsch, and M. Lüdtke. *Chabauty–Kim and the Section Conjecture for locally geometric sections*. 2023. arXiv: `2305.09462v1 [math.NT]`.

[Bro17] F. Brown. *Integral points on curves, the unit equation, and motivic periods*. 2017. arXiv: `1704.00555v1 [math.NT]`.

[CD20a] D. Corwin and I. Dan-Cohen. "The polylog quotient and the Goncharov quotient in computational Chabauty–Kim theory I". In: *International Journal of Number Theory* 16 (2020), pp. 1859–1905.

[CD20b] D. Corwin and I. Dan-Cohen. "The polylog quotient and the Goncharov quotient in computational Chabauty–Kim theory II". In: *Transactions of the American Mathematical Society* 373 (2020), pp. 6835–6861.

[Con] K. Conrad. *Hensel's lemma*. URL: `https://kconrad.math.uconn.edu/blurbs/gradnumthy/hensel.pdf`.

[Dan20] I. Dan-Cohen. "Mixed Tate motives and the unit equation II". In: *Algebra & Number Theory* 14.5 (July 2020), pp. 1175–1237.

[DJ23] I. Dan-Cohen and D. Jarossay. "$M_{0,5}$: toward the Chabauty-Kim method in higher dimensions". English. In: *Mathematika* 69.4 (2023), pp. 1011–1059.

[DW15] I. Dan-Cohen and S. Wewers. "Explicit Chabauty–Kim theory for the thrice punctured line in depth 2". In: *Proceedings of the London Mathematical Society* 110.1 (2015), pp. 133–171.

[DW16] I. Dan-Cohen and S. Wewers. "Mixed Tate motives and the unit equation". In: *International Mathematics Research Notices. IMRN* 17 (2016), pp. 5291–5354.

[EG15] J.-H. Evertse and K. Győry. *Unit equations in Diophantine number theory*. Vol. 146. Camb. Stud. Adv. Math. Cambridge: Cambridge University Press, 2015.

[Fur03] H. Furusho. “p-adic multiple zeta values I – p-adic multiple polylogarithms and the p-adic KZ equation”. In: *Inventiones Mathematicae* 155 (May 2003).

[Kim05] M. Kim. “The motivic fundamental group of $\mathbf{P}^1 \smallsetminus \{0, 1, \infty\}$ and the theorem of Siegel”. In: *Invent. Math.* 161.3 (2005), pp. 629–656.

[Kim09] M. Kim. “The unipotent Albanese map and Selmer varieties for curves”. In: *Kyoto University. Research Institute for Mathematical Sciences. Publications* 45.1 (2009), pp. 89–133.

[KLS22] T. Kumpitsch, M. Lüdtke, and E. Studnia. *dcw_coefficients: Sage code for computing Dan-Cohen–Wewers coefficients*. Version 2.0. 2022. URL: https://github.com/martinluedtke/dcw_coefficients.

[Lüd24] M. Lüdtke. *RefinedCK: Sage code for computing refined Chabauty–Kim loci for the thrice-punctured line*. 2024. URL: https://github.com/martinluedtke/RefinedCK.

[Mah33] K. Mahler. “Zur Approximation algebraischer Zahlen. I: Über den größten Primteiler binärer Formen”. German. In: *Math. Ann.* 107 (1933), pp. 691–730.

[Mil71] J. Milnor. *Introduction to algebraic K-theory*. Annals of Mathematics Studies, No. 72. Princeton University Press, 1971.

[Sage] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 10.3)*. https://www.sagemath.org. 2024.

[Sie21] C. L. Siegel. “Approximation algebraischer Zahlen.” German. In: *Math. Z.* 10 (1921), pp. 173–213.

[Sil88] J. H. Silverman. “Wieferich’s criterion and the abc-conjecture”. In: *Journal of Number Theory* 30.2 (1988), pp. 226–237.

[Yam10] G. Yamashita. “Bounds for the dimensions of p-adic multiple L-value spaces”. In: *Doc. Math.* Extra Vol. (2010), pp. 687–723.