Counting curves and their rational points

Spelier, P.

Chapter 5

A geometric linear Chabauty comparison theorem

This chapter has already been published in Acta Arithmetica [HS22a]. This is joint work with Sachi Hashimoto.

Abstract. The Chabauty–Coleman method is a p-adic method for finding all rational points on curves of genus g whose Jacobians have Mordell–Weil rank $r < g$. Recently, Edixhoven and Lido developed a geometric quadratic Chabauty method that was adapted by Spelier to cover the case of geometric linear Chabauty. We compare the geometric linear Chabauty method and the Chabauty–Coleman method and show that geometric linear Chabauty can outperform Chabauty–Coleman in certain cases. However, as Chabauty–Coleman remains more practical for general computations, we discuss how to strengthen Chabauty–Coleman to make it theoretically equivalent to the geometric linear Chabauty method. We apply these methods to genus 2 and genus 3 curves.

5.1 Introduction

Let $C_{\mathbb{Q}}/\mathbb{Q}$ be a smooth, proper, geometrically integral curve of genus $g \geq 2$. Faltings's theorem [Fal83b] states that the set of rational points $C_{\mathbb{Q}}(\mathbb{Q})$ is finite. However, it does not provide an explicit method for computing this finite set. Let $J_{\mathbb{Q}}/\mathbb{Q}$ be the Jacobian of $C_{\mathbb{Q}}$, with Mordell–Weil rank r. Fix a prime $p > 2$ of good reduction for $C_{\mathbb{Q}}$. The Chabauty–Coleman method is an explicit p-adic method for computing the set of rational points on $C_{\mathbb{Q}}$ when $r < g$. Letting C be a model of $C_{\mathbb{Q}}$ over $\mathbb{Z}_{(p)}$, the method computes a finite set of p-adic points $C(\mathbb{Z}_p)_{\mathrm{CC}}$ containing the rational points $C(\mathbb{Z}_{(p)}) = C_{\mathbb{Q}}(\mathbb{Q})$.

In recent years, the Chabauty–Coleman method has been extended to lift the restriction $r < g$; Balakrishnan, Besser, Müller, Dogra, Tuitman, and Vonk [BBM16, BD18, BD21, BDM$^+$19] developed the quadratic Chabauty method. Edixhoven and Lido proposed a parallel geometric quadratic Chabauty method [EL21] that uses algebro-geometric methods and works in torsors over the Jacobian instead of a certain Selmer variety.

Spelier [Spe20] adapted the geometric method in Edixhoven–Lido to the linear case of Chabauty–Coleman. They outlined a theory of geometric linear Chabauty that parallels the Chabauty–Coleman method. Their method works in the Jacobian itself instead of its image under the logarithm in $\mathbb{Q}_p^g$.

This idea of working in the Jacobian itself is not new. Previously, Flynn [Fly97] also leveraged the Jacobian group law to perform Chabauty-type calculations in a similar way to our geometric method. Flynn's method relied on explicit equations and explicit group laws for $J_{\mathbb{Q}}$ in high-dimensional projective space; the method was used to compute the rational points in several new cases of genus 2 and Mordell–Weil rank 1 curves. However, some of the ideas in [Fly97] do not generalize that easily to higher genus and higher rank examples. Flynn uses specific equations for the embedding of genus 2 curves in $\mathbb{P}^{15}$ and theorems on the number of zeros of p-adic univariate polynomials that both do not extend easily to generic higher genus Jacobians and higher Mordell–Weil ranks.

While geometric linear Chabauty's method sacrifices the explicit nature of Flynn's method, it can nevertheless be applied to curves of any genus. The geometric linear Chabauty method computes a finite set of p-adic points $C(\mathbb{Z}_p)_{\mathrm{GLC}}$ containing the set of rational points $C_{\mathbb{Q}}(\mathbb{Q})$. The method can be performed modulo p^n for any precision $n \in \mathbb{Z}_{>0}$, although it does not always result in an upper bound on the number of rational points. Done modulo p, the computations are simply linear algebra.

In this paper, we survey both the geometric linear Chabauty and Chabauty–Coleman methods, and we provide many examples of the new geometric linear Chabauty method of Spelier. Our main result is a comparison theorem between the two methods. In Theorem 5.5.1, we show that the geometric linear Chabauty method outperforms the Chabauty–Coleman method in certain cases. We have the inclusions:

$$C_{\mathbb{Q}}(\mathbb{Q}) \subseteq C(\mathbb{Z}_p)_o f\mathrm{GLC} \subseteq C(\mathbb{Z}_p)_{\mathrm{CC}}.$$

Furthermore we give an explicit characterization of the set $C(\mathbb{Z}_p)_{\mathrm{CC}} \backslash C(\mathbb{Z}_p)_{\mathrm{GLC}}$, i.e. any excess points the Chabauty–Coleman method finds.

However, because the geometric linear Chabauty method can be prohibitively difficult to implement, in Algorithm 5.5.4 we instead provide an upgrade for the Chabauty–Coleman method that makes it equivalent to geometric linear Chabauty. Finally, this paper makes a practical improvement to the geometric linear Chabauty method, replacing complicated Jacobian arithmetic over $\mathbb{Z}/p^2\mathbb{Z}$ with very low precision Coleman integration on the curve and arithmetic in $\mathbb{F}_p^g$.

We start by defining our notational conventions in Section 5.3.1. In Section 5.3.2 we introduce the geometric linear Chabauty method of Spelier. Section 5.3.5 reviews the Chabauty–Coleman method. We showcase the explicit linear algebra method for finding rational points on $C_{\mathbb{Q}}$ in Section 5.4. The main theorem and discussion on comparison is found in Section 5.5.

5.2 Acknowledgments

We are very grateful to Jennifer Balakrishnan for helpful comments during the preparation of this paper. We are also thankful to Bas Edixhoven for his generous advice and Steffen Müller for assistance with Magma computations. We thank the anonymous referee for many helpful suggestions for improving the paper.

5.3 Background

5.3.1 Set-up

Let $C_{\mathbb{Q}}/\mathbb{Q}$ be a smooth, proper, geometrically integral curve of genus $g \geq 2$. Fix $p > 2$ a prime of good reduction for $C_{\mathbb{Q}}$ and let $C/\mathbb{Z}_{(p)}$ be a smooth model for the curve over the local ring. Then

$$C(\mathbb{Z}_{(p)}) = C_{\mathbb{Q}}(\mathbb{Q}) \tag{5.3.1.1}$$

so the problem of determining $\mathbb{Q}$-points on $C_{\mathbb{Q}}$ can be replaced by the problem of determining $\mathbb{Z}_{(p)}$-points on C.

Let $J/\mathbb{Z}_{(p)}$ be the Jacobian of C and suppose that the Mordell–Weil rank r of $J_{\mathbb{Q}}(\mathbb{Q})$ or, equivalently, $J(\mathbb{Z}_{(p)})$ is less than g. We use M to denote the p-adic closure of the Mordell–Weil group $\overline{J(\mathbb{Z}_{(p)})}$ in $J(\mathbb{Z}_p)$. Denote the torsion subgroup of M by M^{tors}. Let $r' \leq r$ be the rank of M/M^{tors} as a $\mathbb{Z}_p$-module; we assume we have computed r' elements of $J(\mathbb{Z}_{(p)})$ that topologically generate M. We also assume $C(\mathbb{Z}_{(p)})$ is non-empty and fix forever a basepoint $b \in C(\mathbb{Z}_{(p)})$. Let $\overline{b} \in C(\mathbb{F}_p)$ denote the reduction of b modulo p.

Remark 5.3.1. In the case that r is at most g, one usually has $r' = r$. If $r' < r$, there is generally a geometric reason for this, for example the Jacobian splitting as a product of smaller abelian varieties up to isogeny, in which case r' itself and r' topological generators can often be computed if the Mordell–Weil group is known.

For X a scheme, R a local ring with residue field $\mathbb{F}_p$, and $Q \in X(\mathbb{F}_p)$, let $X(R)_Q$ denote the residue disk $\{x \in X(R) : \bar{x} = Q\}$ over Q; we use the same notation for the residue disks of M.

We will need a description of $X(R)_Q$, the residue disk of a smooth scheme over $\mathbb{Z}_p$. For this, we use the following lemma from [Spe20] that can be applied to an affine chart of X containing Q.

Lemma 5.3.2 ([Spe20, Lemma 2.2]). *Let X be a smooth affine scheme over $\mathbb{Z}_p$ of relative dimension d, let Q be an $\mathbb{F}_p$-point of X, and let $t_1, \ldots, t_d$ be parameters of X at Q, i.e. elements of the local ring $\mathcal{O}_{X,Q}$ such that the maximal ideal is given by $(p, t_1, \ldots, t_d)$. Define $\widetilde{t_i} := t_i/p$. Then evaluation of $\widetilde{t}$, the vector $(\widetilde{t_1}, \ldots, \widetilde{t_d})$, gives a bijection $\widetilde{t}\colon X(\mathbb{Z}_p)_Q \to (\mathbb{Z}_p)^d$.*

In fact, this is shown in a geometric fashion by giving a bijection between $X(\mathbb{Z}_p)_Q$ and $\widetilde{X}^p_Q(\mathbb{Z}_p)$, an open affine subscheme of the blowup of X at Q. Then the coordinate ring of $\widetilde{X}^p_Q(\mathbb{Z}_p)$ has p-adic completion equal to the ring of convergent power series

$$\mathbb{Z}_p\langle\widetilde{t_1}, \ldots, \widetilde{t_d}\rangle = \{f \in \mathbb{Z}_p[[\widetilde{t_1}, \ldots, \widetilde{t_d}]] : \text{ for all } n \geq 0, f \in \mathbb{Z}_p[\widetilde{t_1}, \ldots, \widetilde{t_d}] + (p^n)\}.$$

Evaluating the $\widetilde{t_i}$ yields a bijection $\widetilde{X}^p_Q(\mathbb{Z}_p) \to \mathbb{Z}_p^d$ by the formula

$$\widetilde{X}^p_Q(\mathbb{Z}_p) = \mathrm{Hom}(\mathcal{O}_{\widetilde{X}^p_Q}, \mathbb{Z}_p) = \mathrm{Hom}(\mathbb{Z}_p\langle\widetilde{t_1}, \ldots, \widetilde{t_d}\rangle, \mathbb{Z}_p) = \mathbb{A}^d_{\mathbb{Z}_p}.$$

Remark 5.3.3. Lemma 5.3.2 works equally well modulo p^n, giving a bijection

$$X(\mathbb{Z}/p^n\mathbb{Z})_Q \simeq (\mathbb{Z}/p^{n-1}\mathbb{Z})^d.$$

5.3.2 The geometric linear Chabauty method

We recall an idea of Chabauty proving the finiteness of rational points on certain curves of genus $g \geq 2$.

Theorem 5.3.4 ([Cha41])**.** *Let $\mathsf{AJ}_b\colon C(\mathbb{Z}_p) \to J(\mathbb{Z}_p)$ denote the Abel–Jacobi map induced by the basepoint b. Then $\mathsf{AJ}_b(C(\mathbb{Z}_p)) \cap M$ is finite and therefore $C(\mathbb{Z}_{(p)})$ is.*

The geometric linear Chabauty method makes Theorem 5.3.4 explicit by computing the set $\mathsf{AJ}_b(C(\mathbb{Z}_p)) \cap M$ exactly. To start, we break up the set into a union of residue disks. Fix $Q \in C(\mathbb{F}_p)$ and consider the set $\mathsf{AJ}_b(C(\mathbb{Z}_p)_Q) \cap M_{Q-\bar{b}}$ in $J(\mathbb{Z}_p)$. We study the closure of the Mordell–Weil group and the image of the curve under Abel–Jacobi separately.

To describe $M_{Q-\bar{b}}$, we simply need to know whether it is empty; if not, fix a choice of $T \in J(\mathbb{Z}_{(p)})_{Q-\bar{b}}$; if it is, then $\mathsf{AJ}_b(C(\mathbb{Z}_p)_Q) \cap M_{Q-\bar{b}}$ is empty, so we can sieve out this residue disk. Indeed, this is a reformulation of the Mordell–Weil sieve at the prime p, as discussed in Section 5.3.4.

Now we identify $J(\mathbb{Z}_p)_{Q-\bar{b}}$ with $\mathbb{Z}_p^g$ by Lemma 5.3.2. Note that this identification does not preserve the additive structure. Then $\mathsf{AJ}_b(C(\mathbb{Z}_p)_Q)$ is cut out by convergent power series $f_1, \ldots, f_{g-1}$ in the ring of convergent p-adic power series $\mathbb{Z}_p\langle z_1, \ldots, z_g\rangle$ [Spe20, Remark 2.6] (for the right choice of parameters, we may assume the f_i are linear), and the inclusion $M_{Q-\bar{b}} \to J(\mathbb{Z}_p)_{Q-\bar{b}}$, identifying the former with $\mathbb{Z}_p^{r'}$, is given by g power series $\kappa_1, \ldots, \kappa_g \in \mathbb{Z}_p\langle x_1, \ldots, x_{r'}\rangle$ [Spe20, Theorem 3.1]. All in all, we get the diagram

$$\begin{tikzcd}
& & 0 \\
& & \mathbb{Z}_p^{g-1} \arrow[u] \\
0 \arrow[r] & M_{Q-\bar{b}} \arrow[r, "\kappa"] \arrow[ru, "\lambda^Q_{\mathrm{GLC}}"] & J(\mathbb{Z}_p)_{Q-\bar{b}} \arrow[u, "f"'] \\
& & C(\mathbb{Z}_p)_Q \arrow[u, "\mathsf{AJ}_b"'] \\
& & 0 \arrow[u]
\end{tikzcd} . \tag{5.3.2.1}$$

The coordinates λ_i for $i = 1, \dots, g-1$ of λ^Q_{GLC} consist of the pullbacks of $f_1, \dots, f_{g-1}$ along κ. They are given by composing convergent power series that are affine linear mod p and thus themselves are given by convergent power series that are affine linear mod p. In this diagram, the vertical sequence is exact in the sense that $f^{-1}(0) = \mathsf{AJ}_b(C(\mathbb{Z}_p)_Q)$. That is the key behind the following proposition.

Proposition 5.3.5 ([Spe20, Theorem 4.1])**.** *Let Q be an $\mathbb{F}_p$-point of C such that there exists an element $T \in J(\mathbb{Z}_{(p)})_{Q-\bar{b}}$. The zero set $Z(\lambda^Q_{\mathrm{GLC}})$ is equal to $M_{Q-\bar{b}} \cap \mathsf{AJ}_b(C(\mathbb{Z}_p)_Q) = (M_0 + T) \cap \mathsf{AJ}_b(C(\mathbb{Z}_p)_Q)$.*

Thus λ^Q_{GLC} consists of the equations we will use to compute Chabauty's finite set explicitly.

Definition 5.3.6. Let

$$C(\mathbb{Z}_p)_{\mathrm{GLC}} \coloneqq \bigcup_{\substack{Q \text{ s.t.} \\ J(\mathbb{Z}_{(p)})_{Q-\bar{b}} \neq \emptyset}} Z(\lambda^Q_{\mathrm{GLC}}) \tag{5.3.2.2}$$

be the geometric linear Chabauty set.

In practice, the λ_i can only be calculated in finite p-adic precision, where, because they are given by convergent power series, they become polynomials. Although one can say quite a lot about the degrees of these polynomials [Spe20, Lemma 3.7], this method is especially fruitful modulo p, where the λ_i become affine linear polynomials. To give an upper bound on $Z(\lambda^Q_{\mathrm{GLC}})$, one can use the following theorem.

Proposition 5.3.7 ([EL21, Theorem 4.12])**.** *Denote*

$$A = \mathbb{Z}_p\langle x_1, \dots, x_{r'}\rangle / (\lambda_1, \dots, \lambda_{g-1})$$

and

$$\bar{A} \coloneqq \mathbb{F}_p[x_1, \dots, x_{r'}]/(\lambda_1, \dots, \lambda_{g-1})$$

its reduction modulo p. Assume $\bar{A}$ is finite. Then $\bar{A}$ is Artinian and so $\bar{A} \simeq \prod_{m \in \mathrm{MaxSpec}(\bar{A})} \bar{A}_m$.

We have the following upper bound on $|\operatorname{Hom}_{\mathbb{Z}_p}(A, \mathbb{Z}_p)|$ and hence on the number of points in $C(\mathbb{Z}_{(p)})_Q$:

$$\sum_m \dim_{\mathbb{F}_p} \bar{A}_m \geq |\operatorname{Hom}_{\mathbb{Z}_p}(A, \mathbb{Z}_p)| \geq C(\mathbb{Z}_{(p)})_Q$$

where the sum is taken over m such that $\bar{A}/m\bar{A} = \mathbb{F}_p$.

By Proposition 5.3.7, as long as $\bar{A}$ is finite-dimensional, it suffices to compute λ_i modulo p to obtain upper bounds for $C(\mathbb{Z}_{(p)})$. The λ_i are affine linear modulo p, so $\bar{A}$ can only be finite-dimensional if it is $\mathbb{F}_p$ or the zero ring, which happens if the linear system of equations $\{\lambda_i \equiv 0 \bmod p \text{ for all } i\}$ has respectively one or zero solution(s). This observation enables the following reformulation of Proposition 5.3.7.

Corollary 5.3.8. *Assume $M_0/pM_0 \to J(\mathbb{Z}/p^2\mathbb{Z})_0$ is injective with image $\overline{\mathcal{M}}_0$. If in every residue disk of $J(\mathbb{Z}/p^2\mathbb{Z})$ there is at most one intersection between the image $\overline{\mathcal{M}}$ of $J(\mathbb{Z}_{(p)})$ and $\mathsf{AJ}_b(C(\mathbb{Z}/p^2\mathbb{Z}))$, then*

$$|C(\mathbb{Z}_{(p)})| \leq |\overline{\mathcal{M}} \cap \mathsf{AJ}_b(C(\mathbb{Z}/p^2\mathbb{Z}))| \leq |C(\mathbb{F}_p)|$$

.

In particular, if the (not necessarily homogeneous) linear system of equations $\{\lambda_i \equiv 0 \bmod p \text{ for all } i\}$ in Proposition 5.3.7 has zero or one solution, there is respectively zero or at most one point in $C(\mathbb{Z}_{(p)})_Q$.

Definition 5.3.9. We say that the Mordell–Weil group is *of good reduction* (modulo p) if the map $M_0/pM_0 \to J(\mathbb{Z}/p^2\mathbb{Z})_0$ is injective. Otherwise, we say that it is *of bad reduction.*

Remark 5.3.10. This method is independent of the choice of $b \in C(\mathbb{Z}_{(p)})$. Choosing a different basepoint b' shifts the image of the curve by $b - b'$. Equivalently, it shifts $\overline{\mathcal{M}}$ by $b' - b$. But $b' - b$ is an element of the Mordell–Weil group, so the translation is equal to $\overline{\mathcal{M}}$.

Remark 5.3.11. In genus $g > 2$, finding the generators of the Mordell–Weil group can be intractable using the current methods. Often, one can hazard a guess by giving a subgroup $G \subset M$ (for example, taking the subgroup generated by the differences of rational points on C of bounded height). But verifying that the given subgroup is indeed the entire Mordell–Weil group is a very difficult task. For genus 3 hyperelliptic curves, this can be done (see [Sto17]), but it may take weeks of CPU time. However, to execute the geometric linear Chabauty algorithm in a fixed residue disk over $Q \in C(\mathbb{F}_p)$, given $T \in J(\mathbb{Z}_{(p)})_{Q-\bar{b}}$, we do not need generators of the Mordell–Weil group; we only need p-adic generators of the closure of the kernel of reduction of the Mordell–Weil group $\overline{M_0}$. This is immediately satisfied if the index $[M : G]$ is not divisible by p, equivalently, if G is saturated at p. The condition that G is saturated at p can be checked by reducing G modulo ℓ for small primes ℓ. Regarding the required $T \in J(\mathbb{Z}_{(p)})_{Q-\bar{b}}$, we can just produce such a T; if instead we want to prove that it does not exist, we need that the image of G

in $J(\mathbb{F}_p)$ is equal to the image of M; it is enough to check G is saturated at (some of) the primes dividing $|J(\mathbb{F}_p)|$.

For applications and more details, see Example 5.5.7 and Example 5.5.8.

5.3.3 The modulo p method

We now describe how to translate geometric linear Chabauty modulo p into $\mathbb{F}_p$-linear algebra. For each $Q \in C(\mathbb{F}_p)$, we can find $T \in J(\mathbb{Z}_{(p)})_{Q-\bar{b}}$, or there is no rational point in the residue disk $C(\mathbb{Z}_p)_Q$ (these two options are not mutually exclusive); this is explained in greater detail in Section 5.3.4. Fix a choice of T. We want to calculate $\mathsf{AJ}_b(C(\mathbb{Z}_p)_Q) \cap M_{Q-\bar{b}}$ by finding the affine linear polynomials $\lambda_i \mod p$ of Proposition 5.3.5. To calculate these linear polynomials modulo p it suffices to work in residue disks of $J(\mathbb{Z}/p^2\mathbb{Z})$. In this section, we assume the Mordell–Weil group is of good reduction.

Choosing a parameter t_Q for C at Q gives a bijection $\widetilde{t}_Q \colon C(\mathbb{Z}/p^2\mathbb{Z})_Q \xrightarrow{\sim} \mathbb{F}_p$; we write Q_μ for the point mapping to μ. In the same way, by choosing parameters, we have an isomorphism $J(\mathbb{Z}/p^2\mathbb{Z})_0 \simeq \mathbb{F}_p^g$ as groups. After translation by $-T$, we see $C(\mathbb{Z}/p^2\mathbb{Z})_Q$ embeds as a 1-dimensional affine subspace of $J(\mathbb{Z}/p^2\mathbb{Z})_0$ by the map $C(\mathbb{Z}/p^2\mathbb{Z})_Q \to J(\mathbb{Z}/p^2\mathbb{Z})_0$, sending $x \mapsto x - b - T$.

Write $M_{Q-\bar{b}} = T + M_0$. Let $\overline{\mathcal{M}}$ denote the image of M in $J(\mathbb{Z}/p^2\mathbb{Z})$; then $\overline{\mathcal{M}}_0 \cong \mathbb{F}_p^{r'}$ and we see that $(\mathsf{AJ}_b(C(\mathbb{Z}/p^2\mathbb{Z})_Q) \cap \overline{\mathcal{M}}_{Q-\bar{b}}) - T$ is exactly equal to $(\mathsf{AJ}_b(C(\mathbb{Z}/p^2\mathbb{Z})_Q) - T) \cap \overline{\mathcal{M}}_0$.

Now, let $D_Q \subset J(\mathbb{Z}/p^2\mathbb{Z})_0$ be the one-dimensional subspace

$$D_Q \coloneqq \{Q_\mu - Q_0 : \mu \in \mathbb{F}_p\}, \tag{5.3.3.1}$$

and let $v \coloneqq Q_0 - b - T$. We can rephrase Corollary 5.3.8 purely in terms of linear algebra: let φ denote the linear map $\varphi : D_Q \oplus \overline{\mathcal{M}}_0 \to J(\mathbb{Z}/p^2\mathbb{Z})_0$ arising from taking the sum of the embeddings $D_Q, \overline{\mathcal{M}}_0 \subset J(\mathbb{Z}/p^2\mathbb{Z})_0$, then by the equations $\mathsf{AJ}_b(C(\mathbb{Z}/p^2\mathbb{Z})_Q) = D_Q + Q_0 - b$ and $\overline{\mathcal{M}}_{Q-\bar{b}} = \overline{\mathcal{M}}_0 + T$ we get

$$|(\mathsf{AJ}_b(C(\mathbb{Z}/p^2\mathbb{Z})_Q) \cap \overline{\mathcal{M}}_{Q-\bar{b}})| = |\varphi^{-1}(v)|. \tag{5.3.3.2}$$

Remark 5.3.12. If we know there is a rational point P in the residue disk $C(\mathbb{Z}_p)_Q$, then we can take t_Q to be a parameter at P, and choose $T = P - b$ to get $v = 0$ and hence $|\varphi^{-1}(0)|$ on the right side of this equation. (In general, $|\varphi^{-1}(0)|$ is always an upper bound on $|\varphi^{-1}(v)|$.)

5.3.4 The Mordell–Weil sieve

For each residue disk $C(\mathbb{Z}_p)_Q$, if it contains a rational point then there exists $T \in J(\mathbb{Z}_{(p)})_{Q-\bar{b}}$. Assuming we have generators of a subgroup of the Mordell–Weil group that has the same image in $J(\mathbb{F}_p)$, as described in Remark 5.3.11, the existence of T can be checked by a simple calculation in $J(\mathbb{F}_p)$. This calculation can be thought of as a Mordell–Weil sieve [BS10, Sik15] at the single prime p. The Mordell–Weil sieve is a more general technique that produces information about congruence conditions of rational points for subvarieties of abelian varieties.

To determine whether T exists, we consider the diagram

$$\begin{tikzcd} C(\mathbb{Z}_{(p)}) \arrow[r, hook, "\mathsf{AJ}_b"] \arrow[d] & J(\mathbb{Z}_{(p)}) \arrow[d, "\alpha"] \\ C(\mathbb{F}_p) \arrow[r, hook, "\beta"] & J(\mathbb{F}_p) \end{tikzcd} . \tag{5.3.4.1}$$

For $Q \in C(\mathbb{F}_p)$, if $\beta(Q)$ is not in the image of α, then we say Q *fails the Mordell–Weil sieve* (at p). In this case, the residue disk $C(\mathbb{Z}_p)_Q$ cannot contain a rational point. Otherwise, Q *passes the Mordell–Weil sieve* (at p).

5.3.5 The Chabauty–Coleman method

We briefly outline the Chabauty–Coleman method for producing a finite set of p-adic points $C(\mathbb{Z}_p)_{\mathrm{CC}} \subset C(\mathbb{Z}_p)$ that contains the rational points $C(\mathbb{Z}_{(p)})$. For more details and other perspectives on the method, we refer the reader to [Col85c, Wet97, MP12].

Fix a basepoint $b \in C(\mathbb{Z}_{(p)})$ and consider the inclusion of the curve into the Jacobian $\mathsf{AJ}_b \colon C(\mathbb{Z}_p) \to J(\mathbb{Z}_p)$ via the Abel–Jacobi map. Coleman [Col85c, Theorem 2.11] defined a p-adic integral on the curve C. The Coleman integral on regular one-forms agrees with the logarithm on $J(\mathbb{Z}_p)_0$ interpreted as a p-adic Lie group via the equality $J(\mathbb{Q}_p)_0 = J(\mathbb{Z}_p)_0$. We recall some properties of the logarithm here.

Remark 5.3.13. Much of the literature on formal groups and the logarithm works with $\mathbb{Q}_p$-vector spaces. We will need results about $\mathbb{Z}_p$-modules. Most results carry over; for details on the $\mathbb{Z}_p$-module case we reference [Spe20, Section 3]; for the $\mathbb{Q}_p$-vector space case see [Hon70] or [Bou89, III §7].

Recall $H^0(J_{\mathbb{Z}_p}, \Omega^1_{J_{\mathbb{Z}_p}})$ is a free $\mathbb{Z}_p$-module of rank g. For any element $j \in J(\mathbb{Z}_p)$, we have an element

$$\mathsf{log}(j) := \frac{1}{p}\int_0^j \in \mathrm{Hom}_{\mathbb{Z}_p}(H^0(J_{\mathbb{Z}_p}, \Omega^1_{J_{\mathbb{Z}_p}}), \mathbb{Q}_p), \tag{5.3.5.1}$$

sending a differential ω to the logarithm $1/p\int_0^j \omega$. The resulting map $\mathsf{log}\colon j \mapsto 1/p\int_0^j$ is a homomorphism of abelian groups.

Remark 5.3.14. The value of the logarithm in (5.3.5.1) is defined to be $1/p$ the value of the usual Coleman integral. We divide by p to renormalize: the value $\int_0^j \omega$ is always divisible by p if $j \in J(\mathbb{Z}_p)_0$.

Proposition 5.3.15 ([Spe20, Lemma 3.7]). *Recall that we assume $p > 2$; then the logarithm induces an isomorphism of abelian groups on the kernel of reduction $J(\mathbb{Z}_p)_0 \xrightarrow{\sim} H^0(J_{\mathbb{Z}_p}, \Omega^1_{J_{\mathbb{Z}_p}})^\vee$, where the dual is taken in the category of $\mathbb{Z}_p$-modules.*

Write $m := \mathrm{Ann}(J)(\mathbb{F}_p)$ to denote the smallest positive integer such that $m\cdot j = 0$ for all $j \in J(\mathbb{F}_p)$. In particular, the integral $1/p\int_0^j := 1/p\cdot(1/m\cdot\int_0^{mj})$ lands in the submodule $\mathrm{Hom}_{\mathbb{Z}_p}(H^0(J_{\mathbb{Z}_p}, \Omega^1_{J_{\mathbb{Z}_p}}), (1/\mathrm{Ann}(J)(\mathbb{F}_p))\cdot\mathbb{Z}_p)$.

As $\Omega^1_{J_{\mathbb{Z}_p}}$ is locally free,

$$\begin{gathered}\mathsf{log} : J_{\mathbb{Z}/p^n\mathbb{Z}}(\mathbb{Z}/p^n\mathbb{Z})_0 \to H^0(J_{\mathbb{Z}/p^n\mathbb{Z}}, \Omega^1_{J_{\mathbb{Z}/p^n\mathbb{Z}}})^\vee \otimes \mathbb{Z}/p^{n-1}\mathbb{Z},\\ j \mapsto 1/p\int_0^j\end{gathered}$$

is an isomorphism given by lifting j to $\mathbb{Z}_p$, taking log, then reducing modulo p^{n-1}. If $|J(\mathbb{F}_p)|$ is invertible in $\mathbb{Z}_p$, this even extends to a morphism

$$J_{\mathbb{Z}/p^n\mathbb{Z}}(\mathbb{Z}/p^n\mathbb{Z}) \to H^0(J_{\mathbb{Z}/p^n\mathbb{Z}}, \Omega^1_{J_{\mathbb{Z}/p^n\mathbb{Z}}})^\vee \otimes \mathbb{Z}/p^{n-1}\mathbb{Z}. \tag{5.3.5.2}$$

Choosing a basis $(\omega_i)_{i=1}^g$ of $H^0(J_{\mathbb{Z}_p}, \Omega^1_{J_{\mathbb{Z}_p}})$ and dualizing, we get $\mathsf{log} : J(\mathbb{Z}_p)_0 \to \mathbb{Z}_p^g$, reducing to $\mathsf{log} : J(\mathbb{Z}/p^n\mathbb{Z})_0 \to (\mathbb{Z}/p^{n-1}\mathbb{Z})^g$.

Fix a point $R \in J(\mathbb{F}_p)$. For $j \in J(\mathbb{Z}_p)_R$, the logarithm $\mathsf{log}(j)$ has a convergent power series expansion [Spe20, Lemma 3.7]. Let $t_1, \ldots, t_g$ be local parameters of J at R and expand $\omega_i(t_1, \ldots, t_g) = \sum_{i=1}^g f_i(t_1, \ldots, t_g)dt_i$, with $f_i \in \mathbb{Z}_p[[t_1, \ldots, t_g]]$.

By formally integrating, ω_i has a unique local antiderivative g_i on $J(\mathbb{Z}_p)_R$ such that $dg_i = \omega_i$ and $g_i \in \mathbb{Q}_p[[t_1, \ldots, t_g]]$ with constant term 0. Let $\widetilde{R} \in J(\mathbb{Z}_p)_R$

be the point where all t_i vanish. We may then evaluate the power series at j using the local parameters at R by

$$\mathsf{log}(j) \coloneqq (g_1(t_1(j),\dots,t_g(j))/p,\dots,g_j(t_1(j),\dots,t_g(j))/p) + \mathsf{log}(\widetilde{R}). \quad (5.3.5.3)$$

Remark 5.3.16. For computational purposes, it is easier to exploit the isomorphism $\mathsf{AJ}_b^* : H^0(C,\Omega^1_C) \simeq H^0(J,\Omega^1_J)$. Then we may evaluate $\mathsf{log}(j)$ using linearity of the logarithm and expanding in a local parameter on $C_{\mathbb{Z}_p}$ at each point. As C is one-dimensional over $\mathbb{Z}_{(p)}$, we only need one parameter, see [Bal15] for example.

Consider the inclusion of M into $J(\mathbb{Z}_p)$. Let

$$V \coloneqq \{v \in H^0(J_{\mathbb{Z}_p},\Omega^1_{J_{\mathbb{Z}_p}}) : 1/p\int_0^m v = 0 \text{ for all } m \in M\}. \quad (5.3.5.4)$$

Since $\operatorname{rank}_{\mathbb{Z}_p} H^0(J_{\mathbb{Z}_p},\Omega^1_{J_{\mathbb{Z}_p}}) = g$ but $\operatorname{rank}_{\mathbb{Z}_p} M = r'$, we see V is a rank $(g-r')$ $\mathbb{Z}_p$-module. Let B be a basis for V and let

$$v\colon \operatorname{Hom}_{\mathbb{Z}_p}(H^0(J_{\mathbb{Z}_p},\Omega^1_{J_{\mathbb{Z}_p}}),(1/\operatorname{Ann}(J)(\mathbb{F}_p))\cdot\mathbb{Z}_p) \to \frac{1}{\operatorname{Ann}(J)(\mathbb{F}_p)}\mathbb{Z}_p^{g-r'}$$

denote the map $\psi \mapsto (\psi(\nu))_{\nu\in B}$. By construction, the map v vanishes on $\mathsf{log}(j)$ for $j \in M$.

Next consider the Abel–Jacobi embedding $\mathsf{AJ}_b\colon C(\mathbb{Z}_p) \to J(\mathbb{Z}_p)$ and the composition $\Lambda_{\mathrm{CC}} \coloneqq v \circ \mathsf{log} \circ \mathsf{AJ}_b$. We get the following diagram:

$$\begin{tikzcd}
M \arrow[r] & J(\mathbb{Z}_p) \arrow[r, "\mathsf{log}"] & \operatorname{Hom}_{\mathbb{Z}_p}(H^0(J_{\mathbb{Z}_p},\Omega^1_{J_{\mathbb{Z}_p}}),\frac{1}{\operatorname{Ann}(J)(\mathbb{F}_p)}\cdot\mathbb{Z}_p) \arrow[r, "v"] & (\frac{1}{\operatorname{Ann}(J)(\mathbb{F}_p)})\cdot\mathbb{Z}_p^{g-r'} \\
& C(\mathbb{Z}_p) \arrow[u, "\mathsf{AJ}_b"] \arrow[urr, "\Lambda_{\mathrm{CC}}"] & & \\
& 0 \arrow[u] & &
\end{tikzcd}$$

(5.3.5.5)

Definition 5.3.17. We define the Chabauty–Coleman set to be the following:

$$C(\mathbb{Z}_p)_{\mathrm{CC}} \coloneqq Z(\Lambda_{\mathrm{CC}}) = \{P \in C(\mathbb{Z}_p) : 1/p\int_0^{P-b} \nu = 0 \text{ for all } \nu \in B\}. \quad (5.3.5.6)$$

Then $\mathsf{AJ}_b(C(\mathbb{Z}_p)) \cap M$ is contained in $C(\mathbb{Z}_p)_{\mathrm{CC}}$.

Lemma 5.3.18. *Fix $R = \mathsf{AJ}_b(Q) \in J(\mathbb{F}_p)$ with $Q \in C(\mathbb{F}_p)$. Let $\widetilde{z} : C(\mathbb{Z}_p)_Q \xrightarrow{\sim} \mathbb{Z}_p$ be given by a parameter z at Q, and denote by Q_μ the element with image μ. Then $\mathsf{log}(Q_\mu - b)$ can be expressed as $f + c$ where $f \in \mathbb{Z}_p\langle\mu\rangle^g$ and $c \in 1/\operatorname{Ann}(J)(\mathbb{F}_p) \cdot \mathbb{Z}_p^g$.*

Proof. Write $\mathsf{log}(Q_\mu - b) = \mathsf{log}(Q_\mu - Q_0) + \mathsf{log}(Q_0 - b)$, and $t_1, \ldots, t_g$ for parameters of J at 0. Then by [Spe20, Remark 2.3] the function $\mu \mapsto \widetilde{t_i}(Q_\mu - Q_0)$ is given by a convergent power series in μ. Also, $\mathsf{log}\colon J(\mathbb{Z}_p)_0 \to \mathbb{Z}_p^g$ consists of g convergent power series in $\widetilde{t_1}, \ldots, \widetilde{t_g}$. The composition of convergent power series exists and is itself a convergent power series, so $\mathsf{log}(Q_\mu - Q_0) \in \mathbb{Z}_p\langle\mu\rangle^g$.

By Proposition 5.3.15, the constant term $\mathsf{log}(Q_0 - b)$ lives in $1/\operatorname{Ann}(J)(\mathbb{F}_p) \cdot \mathbb{Z}_p^d$. □

In practice, to compute $C(\mathbb{Z}_p)_{\mathrm{CC}}$, we must truncate the power series by working modulo p^n for some $n \in \mathbb{Z}_{>0}$. The choice of n depends on the Newton polygon of the power series: n must be large enough so that the truncated power series has the same number of zeros as the original power series, allowing us to Hensel lift the solutions of the truncated power series to $\mathbb{Z}_p$.

To compare the geometric linear Chabauty and Chabauty–Coleman methods, we describe how the Chabauty–Coleman method works in a single residue disk. We fix an $\mathbb{F}_p$-point $Q \in C(\mathbb{F}_p)$, and assume Q passes the Mordell–Weil sieve, i.e. $J(\mathbb{Z}_{(p)})_{Q-\overline{b}}$ contains an element T. Since $T \in M$, we know $1/p \int_b^T v$ vanishes, so $\ker(v \circ \mathsf{log}) = \ker(v \circ \mathsf{log} \circ \mathrm{tr}_{-T})$. Then diagram (5.3.5.5), restricted to this residue disk, becomes

$$\begin{tikzcd}
M_{Q-\overline{b}} \arrow[r] & J(\mathbb{Z}_p)_{Q-\overline{b}} \arrow[r, "\mathsf{log}\circ\mathrm{tr}_{-T}"] & H^0(J_{\mathbb{Z}_p}, \Omega^1_{J_{\mathbb{Z}_p}})^\vee \arrow[r, "v"] & \mathbb{Z}_p^{g-r'} \\
 & C(\mathbb{Z}_p)_Q \arrow[u, "\mathsf{AJ}_b"] \arrow[urr, "\lambda_{\mathrm{CC}}^Q"] & & \\
 & 0 \arrow[u] & &
\end{tikzcd} \tag{5.3.5.7}$$

where λ_{CC}^Q is now the composition $v \circ \mathsf{log} \circ \mathrm{tr}_{-T} \circ \mathsf{AJ}_b$. Note that $\mathsf{log} \circ \mathrm{tr}_{-T}$ is a bijection $J(\mathbb{Z}_p)_{Q-\overline{b}} \to H^0(J_{\mathbb{Z}_p}, \Omega^1_{J_{\mathbb{Z}_p}})^\vee$.

Unfortunately, the sequence

$$0 \to M_{Q-\bar{b}} \xrightarrow{\mathsf{log} \circ \mathrm{tr}_{-T} \circ \kappa} H^0(J_{\mathbb{Z}_p}, \Omega^1_{J_{\mathbb{Z}_p}})^\vee \xrightarrow{v} \mathbb{Z}_p^{g-r'} \to 0$$

is not necessarily exact at the middle term. In fact, $\ker(v \circ \mathsf{log})$ is the p-saturation N_0 of M_0 inside $J(\mathbb{Z}_p)_0$, by the following lemma.

Lemma 5.3.19. *Let A be a free $\mathbb{Z}_p$-module of rank n, let B be a $\mathbb{Z}_p$-submodule of rank m, and let $v \colon A \to \mathbb{Z}_p^{n-m}$ be a full rank linear map vanishing on B. Then $\ker v$ is the p-saturation of B.*

Proof. By linearity of v, $\ker v$ contains the p-saturation of B. Comparing dimensions, we see that $(\ker v) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ must equal $B \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. Then $\ker v$ is contained in $(B \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) \cap A$, which is exactly the p-saturation of B. □

Applying Lemma 5.3.19 to $A = J(\mathbb{Z}_p)_0$ and $B = M_0$, we see $\ker(v \circ \mathsf{log} \circ \mathrm{tr}_{-T}) = T + N_0$. That gives us the following corollary.

Corollary 5.3.20. *Let Q be an $\mathbb{F}_p$-point of C that passes the Mordell–Weil sieve, with $T \in J(\mathbb{Z}_{(p)})_{Q-\bar{b}}$. Then $Z(\lambda^Q_{\mathrm{CC}})$ is exactly the intersection $(N_0 + T) \cap \mathsf{AJ}_b(C(\mathbb{Z}_p)_{Q-\bar{b}})$ pulled back along AJ_b.*

5.4 Explicit Geometric linear Chabauty mod p

We outline a practical method for doing explicit geometric linear Chabauty modulo p using Coleman integration. Previously, in [Spe20], this was done by using the birationality of the map $\mathrm{Sym}^g C \to J$ given by subtracting a generic degree g divisor, and using the Khuri-Makdisi representation of elements of the Jacobian ([KM04]), where elements of the Jacobian are represented as certain submodules of Riemann–Roch spaces. This approach of using the birationality of the map $\mathrm{Sym}^g C \to J$ is taken in [EL21] for geometric quadratic Chabauty as well.

The advantage of using Coleman integration is that the map $J(\mathbb{Z}/p^2\mathbb{Z})_0 \to \mathbb{F}_p^g$ can be made much more explicit, making the computations simple linear algebra. In what follows, we describe this map and give examples of the method.

The logarithm is linear modulo p for $p > 2$ [Spe20, Lemma 3.7] (when $p = 2$ the logarithm is not necessarily linear modulo p, hence we exclude this case). We choose parameters for $J(\mathbb{Z}/p^2\mathbb{Z})_0$ and a $\mathbb{Z}_p$-basis of $H^0(J_{\mathbb{Z}_p}, \Omega^1_{J_{\mathbb{Z}_p}})$. Then again by [Spe20, Lemma 3.7] the reduction modulo p of the logarithm, i.e. the map $\mathsf{log}\colon \mathbb{F}_p^g \to \mathbb{F}_p^g$, is an isomorphism of vector spaces over $\mathbb{F}_p$, allowing us to carry out the methods in Section 5.3.2. For example, the vector in $\mathbb{F}_p^g$ corresponding to $j \in J(\mathbb{Z}/p^2\mathbb{Z})_0$ is $(1/p\int_0^j \omega_i)_{i=1}^g$. This translates linear algebra in a vector space $J(\mathbb{Z}/p^2\mathbb{Z})_0$ of dimension g where addition is difficult, to linear algebra in $\mathbb{F}_p^g$. This is the final step needed to perform geometric linear Chabauty modulo p.

5.4.1 Examples

Example 5.4.1. Let $C/\mathbb{Z}_{(5)}$ be (the smooth projective model of) the genus 2 curve (LMFDB label `10989.a.10989.1`) given by

$$y^2 = x^5 + x^3 + x^2 + 1/4$$

with Mordell–Weil rank 1. Then C has the known rational points

$$C(\mathbb{Z}_{(5)})_{\text{known}} = \{\infty = (1:0:0), P_1 = (0:-1/2:1), P_2 = (0:1/2:1)\}.$$

The Mordell–Weil group of J is isomorphic to $\mathbb{Z}$ and generated by $P_1 - \infty$.

Let $p = 5$. Over $\mathbb{F}_5$ we have the points

$$C(\mathbb{F}_5) = \{(1:0:0), (0:2:1), (0:3:1)\}.$$

At the finite non-Weierstrass residue disks corresponding to the points $\overline{P}_1 = (0:2:1)$ and $\overline{P}_2 = (0:3:1)$, we have the local parameter x giving isomorphisms $C(\mathbb{Z}/5^2\mathbb{Z})_{\overline{P}_i} \xrightarrow{\sim} 5\mathbb{Z}/5^2\mathbb{Z}$. At the infinite point, the local parameter is $t = x^2/y$. We identify $J(\mathbb{Z}/5^2\mathbb{Z})_0$ with $\mathbb{F}_5^2$ by choosing the basis of differentials $\omega_0 = dx/y, \omega_1 = xdx/y$, then applying $\mathsf{log}\colon j \mapsto (1/5\int_0^j \omega_0, 1/5\int_0^j \omega_1)$.

Consider the residue disk $C(\mathbb{Z}_5)_{\overline{P}_1}$: our goal is to show there is only one point in this disk (and each other disk). We start by computing $\overline{\mathcal{M}}_0$. Since $P_1 - \infty$ generates the Mordell–Weil group, computing $\overline{\mathcal{M}}_0$ is equivalent to finding the smallest n such that $n(P_1 - \infty) = 0$ in $J(\mathbb{F}_5)$. We find $n = 15$, that is, $m = 15(P_1 - \infty)$ generates M_0. A simple calculation with tiny Coleman integrals shows that $\mathsf{log} m = (3,1) \in \mathbb{F}_5^2$. That automatically means that the map $M_0 \to J(\mathbb{Z}_5)_0$ is of good reduction, and $\overline{\mathcal{M}}_0$ is the $\mathbb{F}_5$-vector space generated by $(3,1)$.

By specializing $\lambda = 0$ and $\lambda = 1$ we see that $D_{\overline{P}_1} \subset J(\mathbb{Z}/5^2\mathbb{Z})_0$ is generated by $d = (5:-1/2:1) - (0:-1/2:1)$ and $\mathsf{log} d = (4,0)$.

Now the matrix A representing the map $\varphi\colon D_{\overline{P}_1} \oplus \overline{\mathcal{M}}_0 \to J(\mathbb{Z}/5^2\mathbb{Z})_0$ is

$$\begin{pmatrix} 4 & 3 \\ 0 & 1 \end{pmatrix}.$$

As A is invertible, $|\varphi^{-1}(v)| = 1$. Hence, by (5.3.3.2) the only rational point in the residue disk of P_1 is P_1 itself. Using the hyperelliptic involution, we see the same holds for P_2.

For the point ∞, we carry out a similar calculation. We change our basepoint to ∞, allowing us to again work in $J(\mathbb{Z}/5^2\mathbb{Z})_0 = \mathbb{F}_5^2$. Then $D_{\overline{\infty}}$ is generated by $d' = (1 : 5 : 0) - (1 : 0 : 0)$ and $\mathsf{log} d' = (0, 4)$. So we again conclude that the only rational point in the residue disk containing ∞ is ∞.

As we have now treated all three residue disks, we have proven

$$C_{\mathbb{Q}}(\mathbb{Q}) = \{(1 : 0 : 0), (0 : -1/2 : 1), (0 : 1/2 : 1)\}.$$

Example 5.4.2. Let $C/\mathbb{Z}_{(3)}$ be (the smooth projective model of) the genus 2 curve (LMFDB label `29395.a.29395.1`) given by the equation

$$y^2 + (x^2 + x + 1)y = x^5 - x^4 + x^3$$

with Mordell–Weil rank 1. Then C has known rational points

$$C(\mathbb{Z}_{(3)})_{\text{known}} = \{\infty = (1 : 0 : 0), (0 : 0 : 1), (0 : -1 : 1)\}.$$

The Mordell–Weil group is $J(\mathbb{Z}_{(p)}) \simeq \mathbb{Z}$ and is generated by $d \coloneqq (0 : -1 : 1) - \infty$.

Let $p = 3$, then $C(\mathbb{F}_3)$ is

$$\{(1 : 0 : 0), (0 : 0 : 1), (0 : 2 : 1), (1 : 1 : 1), (1 : 2 : 1), (2 : 0 : 1), (2 : 2 : 1)\}.$$

In this example we show how to rule out some of the residue disks that do not contain rational points using geometric linear Chabauty.

For each residue disk $C(\mathbb{Z}_3)_Q$ not containing a known rational point, using arithmetic in $J(\mathbb{F}_3)$ we are able to find $T \coloneqq md$ such that $T \in J(\mathbb{Z}_{(3)})_{Q-\overline{\infty}}$. The order of $\overline{d}$ in $J(\mathbb{F}_3)$ is 29 so $m < 29$. Since all $Q \in C(\mathbb{F}_3)$ pass the Mordell–Weil sieve, we proceed to compute the matrix A for each Q.

First we compute $\overline{\mathcal{M}}_0$, which does not depend on Q. To do this, we compute $\mathsf{log}(29d) = (2, 2) \in \mathbb{F}_3^2$.

Then, for each residue disk $C(\mathbb{Z}_3)_Q$ without a known rational point, we will compute the one-dimensional subspace D_Q. To do this, we lift Q in two different ways Q_1 and Q_2 to finite precision, and then take the tiny Coleman integral $\mathsf{log}(Q_1 - Q_2)$.

Q	m	Q_1	Q_2	$\mathsf{log}(Q_1 - Q_2)$
$(1:1:1)$	20	$(1+O(3^3):4+O(3^3):1)$	$(4+O(3^3):1+O(3^3):1)$	$(0,2)$
$(1:2:1)$	9	$(1+O(3^3):20+O(3^3):1)$	$(4+O(3^3):5+O(3^3):1)$	$(0,1)$
$(2:0:1)$	16	$(2+O(3^3):6+O(3^3):1)$	$(5+O(3^3):6+O(3^3):1)$	$(2,2)$
$(2:2:1)$	13	$(2+O(3^3):14+O(3^3):1)$	$(5+O(3^3):17+O(3^3):1)$	$(1,1)$

Table 5.1: Values for D_Q

For the $\mathbb{F}_3$-points, $(2:0:1)$ and $(2:2:1)$, we see modulo 3 that $\overline{\mathcal{M}}_0$ and D_Q give determinant zero matrices:

$$A_{(2:0:1)} = \begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix}, A_{(2:2:1)} = \begin{pmatrix} 2 & 1 \\ 2 & 1 \end{pmatrix}.$$

We check whether for $v = Q_1 - \infty - md$, the vector $\mathsf{log}v$ is in the image of A_Q. For $(2:0:1)$ we have $\mathsf{log}v = (-3+O(3^2), -2+O(3^2))$ and for $(2:2:1)$ we have $\mathsf{log}v = (O(3^2), 2+O(3^2))$. Therefore by (5.3.3.2) neither residue disk can contain a $\mathbb{Z}_{(3)}$-point.

However, for $(1:1:1)$ and $(1:2:1)$, we see that A_Q is invertible:

$$A_{(1:1:1)} = \begin{pmatrix} 2 & 0 \\ 2 & 2 \end{pmatrix}, A_{(2:2:1)} = \begin{pmatrix} 2 & 0 \\ 2 & 1 \end{pmatrix}.$$

Hence geometric linear Chabauty modulo 3 shows that there is at most one rational point in each of the two corresponding residue disks.

It is possible to show that there are no rational points in these residue disks, for example using a Mordell–Weil sieve at strategically chosen primes $\ell \neq 3$.

In the previous pair of examples, the geometric linear Chabauty method and Chabauty–Coleman method find the same set of 3-adic points, i.e. $C(\mathbb{Z}_3)_{\mathrm{CC}} = C(\mathbb{Z}_3)_{\mathrm{GLC}}$. In the following example we show this is not always the case. We will study the differences between the two methods in the final section.

Example 5.4.3. Let $C/\mathbb{Z}_{(3)}$ be (the smooth projective model of) the genus 2 curve (LMFDB label `9470.a.37880.1`) given by the equation

$$y^2 + xy = x^5 + 2x^4 + 4x^3 + 4x^2 + 3x + 1$$

with Mordell–Weil rank 1. Then C has the known rational points

$$C(\mathbb{Z}_{(3)})_{\text{known}} = \{(1:0:0), (0:-1:1), (0:1:1)\}.$$

But

$$C(\mathbb{F}_3) = \{(1:0:0), (0:1:1), (0:2:1), (1:0:1), (1:2:1), (2:2:1)\}.$$

The Mordell–Weil group of J is isomorphic to $\mathbb{Z}$, generated by $d := (0:-1:1) - (1:0:0)$. In $J(\mathbb{F}_3)$, d has order 11. Sieving, we find the only residues $c \in C(\mathbb{F}_3)$ such that there exists $m \in \mathbb{Z}$ such that $c - \infty = md$ are the images of rational points under the reduction map.

In their corresponding residue disks, the geometric linear Chabauty method only finds one solution, so $C(\mathbb{Z}_3)_{\text{GLC}} = C(\mathbb{Z}_{(3)})_{\text{known}} = C(\mathbb{Z}_{(3)})$.

However, the Chabauty–Coleman method finds the rational points along with the p-adic points

$$\begin{gathered}
\{(2+3+3^2+2\cdot 3^3+2\cdot 3^4+3^5+3^6+O(3^7) : 2+2\cdot 3^2+3^3+3^4+2\cdot 3^6+O(3^7) : 1), \\
(1+2\cdot 3^2+2\cdot 3^3+2\cdot 3^4+3^6+O(3^7) : 2\cdot 3+3^3+2\cdot 3^5+O(3^7) : 1), \\
(1+2\cdot 3^2+2\cdot 3^3+2\cdot 3^4+3^6+O(3^7) : 2+2\cdot 3^3+2\cdot 3^4+2\cdot 3^5+O(3^7) : 1)\}.
\end{gathered}$$

One of the 3-adic points lies in a Weierstrass disk. Since it is the only point in its disk and is fixed by the hyperelliptic involution, the point is 2-torsion, while the other two points do not readily have explanations for being in the Chabauty–Coleman set (in particular, they are not torsion in $J(\mathbb{Z}_3)$ and not recognizably algebraic).

5.5 Comparison

Throughout this section, Q still denotes a point in $C(\mathbb{F}_p)$ and T still denotes a point in $J(\mathbb{Z}_{(p)})_{Q-\bar{b}}$ (i.e., we assume Q passes the Mordell–Weil sieve at p, see Section 5.3.4).

To compare the geometric linear Chabauty and Chabauty–Coleman methods, we first recall some notation in the following commutative diagram, which is the union of the diagrams (5.3.2.1) and (5.3.5.7):

$$\begin{tikzcd}
 & & 0 & & \\
 & & \mathbb{Z}_p^{g-1} \arrow[u] & & \\
0 \arrow[r] & M_{Q-\bar{b}} \arrow[r, "\kappa"] \arrow[ur, "\lambda^Q_{\mathrm{GLC}}"] & J(\mathbb{Z}_p)_{Q-\bar{b}} \arrow[r, "\mathsf{log}\circ \mathrm{tr}_{-T}"] \arrow[u, "f"] & H^0(J_{\mathbb{Z}_p}, \Omega^1_{J_{\mathbb{Z}_p}})^\vee \arrow[r, "v"] & \mathbb{Z}_p^{g-r'} \\
 & & C(\mathbb{Z}_p)_Q \arrow[u, "\mathsf{AJ}_b"] \arrow[urr, "\lambda^Q_{\mathrm{CC}}"] & & \\
 & & 0 \arrow[u] & &
\end{tikzcd}$$

(5.5.0.1)

where we recall

- the maps κ and f are defined as in diagram (5.3.2.1);
- $\mathsf{AJ}_b : C(\mathbb{Z}_p)_Q \to J(\mathbb{Z}_p)_{Q-\bar{b}}$ is the Abel–Jacobi embedding at $b \in C(\mathbb{Z}_{(p)})$;
- the map v is given by $g - r'$ linearly independent Coleman integrals that vanish on M;
- and $\mathsf{log} : J(\mathbb{Z}_p)_0 \xrightarrow{\sim} H^0(J_{\mathbb{Z}_p}, \Omega^1_{J_{\mathbb{Z}_p}})^\vee$ is given by the (normalized) Coleman integral $\mathsf{log}\colon x \mapsto (\omega \mapsto 1/p \int_0^x \omega)$.

Now we can give a comparison theorem for the geometric linear Chabauty and Chabauty–Coleman methods.

Theorem 5.5.1. *Let $C(\mathbb{Z}_p)_{\mathrm{GLC}}$ and $C(\mathbb{Z}_p)_{\mathrm{CC}}$ be the finite subsets of $C(\mathbb{Z}_p)$ defined in Definition 5.3.6 and Definition 5.3.17. We have the inclusions*

$$C(\mathbb{Z}_{(p)}) \subseteq C(\mathbb{Z}_p)_{\mathrm{GLC}} \subseteq C(\mathbb{Z}_p)_{\mathrm{CC}}.$$

Furthermore, for any point $R \in C(\mathbb{Z}_p)_{\mathrm{CC}} \setminus C(\mathbb{Z}_p)_{\mathrm{GLC}}$, one of the following two conditions holds:

1. *the point $\overline{R}$ fails the Mordell–Weil sieve at p, i.e. the image of $R - b$ in $J(\mathbb{F}_p)$ is not contained in the image of M in $J(\mathbb{F}_p)$;*
2. *or for $T \in J(\mathbb{Z}_{(p)})_{\overline{R}-\bar{b}}$, the element $\mathsf{log}(R - b - T)$ is not in the $\mathbb{Z}_p$-submodule $\mathsf{log}M_0$ of $H^0(J_{\mathbb{Z}_p}, \Omega^1_{J_{\mathbb{Z}_p}})^\vee$, only in its p-saturation $\mathsf{log}N_0$.*

Proof. We may prove this disk-by-disk. Suppose $Q \in C(\mathbb{F}_p)$ fails the Mordell–Weil sieve. Then $M_{Q-\bar{b}} = Z(\lambda^Q_{\mathrm{GLC}}) = \emptyset$, and so Item 1 holds.

Otherwise, we can find $T \in J(\mathbb{Z}_{(p)})_{Q-\bar{b}}$. Then, by Proposition 5.3.5, we know

$$Z(\lambda^Q_{\mathrm{GLC}}) = (M_0 + T) \cap \mathsf{AJ}_b(C(\mathbb{Z}_p)_{Q-\bar{b}})$$

and by Corollary 5.3.20 we know

$$\mathsf{AJ}_b(Z(\lambda^Q_{\mathrm{CC}})) = (N_0 + T) \cap \mathsf{AJ}_b(C(\mathbb{Z}_p)_{Q-\bar{b}}).$$

So we see that $R - b$ belongs to $\mathsf{AJ}_b(Z(\lambda^Q_{\mathrm{CC}})) - \kappa(Z(\lambda^Q_{\mathrm{GLC}}))$ if and only if $\mathsf{log} \circ \mathrm{tr}_{-T}(R - b) = \mathsf{log}(R - b - T)$ is in $\mathsf{log}N_0 \setminus \mathsf{log}M_0$. (As any two choices of T differ by an element of M_0, this statement is choice-independent.) □

Remark 5.5.2. In the case of good reduction of the Mordell–Weil group, the obstruction Item 2 cannot occur, as then by definition M_0 is its own p-saturation.

Corollary 5.5.3. *If $p \nmid |J(\mathbb{F}_p)|$, then Theorem 5.5.1 Item 2 is equivalent to $\mathsf{log}(R - b)$ not lying in the submodule $\mathsf{log}M$ of $H^0(J_{\mathbb{Z}_p}, \Omega^1_{J_{\mathbb{Z}_p}})^\vee$.*

Proof. Recall from Proposition 5.3.15 that the isomorphism $\mathsf{log}\colon J(\mathbb{Z}_p)_0 \to H^0(J_{\mathbb{Z}_p}, \Omega^1_{J_{\mathbb{Z}_p}})^\vee$ extends to a map $\mathsf{log}\colon J(\mathbb{Z}_p) \to m^{-1}H^0(J_{\mathbb{Z}_p}, \Omega^1_{J_{\mathbb{Z}_p}})^\vee$ where $m = \mathrm{Ann}(J)(\mathbb{F}_p)$, by sending x to $\mathsf{log}(mx)/m$. Under the condition $p \nmid |J(\mathbb{F}_p)|$, we see that m is a p-adic unit, so the logarithm extends to a map $\mathsf{log}\colon J(\mathbb{Z}_p) \to H^0(J_{\mathbb{Z}_p}, \Omega^1_{J_{\mathbb{Z}_p}})^\vee$. Hence $\mathsf{log}M_0 = \mathsf{log}M$ as submodules of $H^0(J_{\mathbb{Z}_p}, \Omega^1_{J_{\mathbb{Z}_p}})^\vee$. As $\mathsf{log}T$ is an element of $\mathsf{log}M$, we conclude that $\mathsf{log}(R-b-T)$ not lying in $\mathsf{log}M_0$ is equivalent to $\mathsf{log}(R - b)$ not lying in $\mathsf{log}M$. □

Hence the geometric method is theoretically strictly better. However, depending on the curve and the level of precision needed, the geometric linear Chabauty method can be tricky to execute; the best known method for expressing λ^Q_{GLC} as polynomials modulo some power of p uses interpolation, then one has to solve multiple power series in r variables. Sometimes one can use the implicit function theorem for power series [Haz12, Proposition A.4.5] to reduce to fewer variables, but in general this can be an arduous task. Hence in practice, we advise the following adjustment of the Chabauty–Coleman method.

Algorithm 5.5.4.

1. *Calculate $S \coloneqq C(\mathbb{Z}_p)_{\mathrm{CC}}$ using the Chabauty–Coleman method.*

2. *Let* $(E_i)_{i=1}^{r'} \in J(\mathbb{Z}_{(p)})$ *be a set of topological generators of* M_0 *and* $(\omega_j)_{j=1}^{g}$ *a basis of* $H^0(J_{\mathbb{Z}_p}, \Omega^1_{J_{\mathbb{Z}_p}})$.
3. *Calculate* $\mathsf{log}E_i = (1/p \int_0^{E_i} \omega_j)_{j=1}^{g} \in \mathbb{Z}_p^g$ *for* $i = 1, \dots, r'$.
4. *For* $R \in S$*, remove* R *from* S *if it does not pass the Mordell–Weil sieve at* p.
5. *For* $R \in S$*, let* $T \in J(\mathbb{Z}_{(p)})_{\overline{R-b}}$*. If* $\mathsf{log}(R - b - T)$ *is not a* $\mathbb{Z}_p$*-linear combination of* $(\mathsf{log}E_i)_{i=1}^{r'}$*, remove* R *from* S.
6. *Return* S.

From the previous discussion, we have the following theorem.

Theorem 5.5.5. *Algorithm 5.5.4 computes* $\mathsf{AJ}_b(C(\mathbb{Z}_p)) \cap M$.

Proof. This is immediate from Theorem 5.5.1 and Proposition 5.3.5. □

Remark 5.5.6. Note that Step 4 in Algorithm 5.5.4 executes a Mordell–Weil sieve at the single prime p on top of the usual Chabauty–Coleman method. The Mordell–Weil sieve is often used in combination with Chabauty–Coleman to sieve out extra p-adic points that are not rational. For example, the implementation of Chabauty–Coleman in Magma for genus 2 curves based on [BS10, Section 4.4] executes the Chabauty–Coleman method to find $C(\mathbb{Z}_p)_{\mathrm{CC}}$ and then runs a Mordell–Weil sieve at a set of primes $\{\ell_1, \dots, \ell_n\}$ to try to determine $C(\mathbb{Z}_{(p)}) = C_{\mathbb{Q}}(\mathbb{Q})$. This is a more extensive Mordell–Weil sieve than the one used in Algorithm 5.5.4. In practice, for the genus 2 curves in Example 5.4.1, Example 5.4.2, and Example 5.4.3, Magma determines $C(\mathbb{Z}_{(p)})$ in a fraction of a second.

The points removed in Step 5 pass a Mordell–Weil sieve at p, but are ruled out by Theorem 5.5.1 Item 2. They may fail a Mordell–Weil sieve at some other prime $\ell \neq p$.

In Theorem 5.5.1 there are two obstructions to the Chabauty–Coleman method calculating $\mathsf{AJ}_b(C(\mathbb{Z}_p)) \cap M$ exactly. We give two examples that show these both occur, and where geometric linear Chabauty outperforms Chabauty–Coleman. In light of Remark 5.5.6, we turn our attention to genus 3 curves.

The following examples were computed in Magma and Sage. The code is available at the repository [HS].

Example 5.5.7. Let $C/\mathbb{Z}_{(5)}$ be the (smooth projective model of) the genus 3 curve given by the equation

$$y^2 = 4x^7 - 12x^6 + 16x^5 - 12x^4 + 4x^3 + 4x^2 - 4x + 1$$

taken from a database of genus 3 hyperelliptic curves over $\mathbb{Q}$ [Sut] computed using the methods in [BSS$^+$16]. According to computations with the fake 2-Selmer group done by the method `RankBounds` in Magma, the Mordell–Weil rank of J is 2.

Computing the Chabauty–Coleman set with $p = 5$ we find

$$\begin{aligned}
&C(\mathbb{Z}_5)_{\mathrm{CC}} = \{\infty = (1:0:0), (0:-1:1), (0:1:1), (1:-1:1), (1:1:1),\\
&W \coloneqq (2 + 5 + 5^2 + 2\cdot 5^3 + 4\cdot 5^4 + 4\cdot 5^5 + 3\cdot 5^6 + O(5^6) : O(5^6) : 1)\\
&R_1 \coloneqq (4 + 3\cdot 5 + 2\cdot 5^2 + 3\cdot 5^4 + 3\cdot 5^5 + O(5^6) : 4 + 2\cdot 5 + 4\cdot 5^3 + 5^4 + 4\cdot 5^5 + O(5^6) : 1)\\
&R_2 \coloneqq (4 + 3\cdot 5 + 2\cdot 5^2 + 3\cdot 5^4 + 3\cdot 5^5 + O(5^6) : -(4 + 2\cdot 5 + 4\cdot 5^3 + 5^4 + 4\cdot 5^5 + O(5^6)) : 1)\\
&R_3 \coloneqq (3 + 5 + 2\cdot 5^2 + 4\cdot 5^3 + 4\cdot 5^4 + 4\cdot 5^5 + O(5^6) : 3 + 5 + 5^3 + 2\cdot 5^5 + O(5^6) + : 1)\\
&R_4 \coloneqq (3 + 5 + 2\cdot 5^2 + 4\cdot 5^3 + 4\cdot 5^4 + 4\cdot 5^5 + O(5^6) : -(3 + 5 + 5^3 + 2\cdot 5^5 + O(5^6)) : 1)\}.
\end{aligned}$$

Then W is a Weierstrass point, and therefore gives rise to a 2-torsion point in J, but the R_i are not readily recognizable. We can verify by computing Coleman integrals that they are not torsion in $J(\mathbb{Z}_5)$. However, the geometric linear Chabauty method rules out the residue disks of the R_i.

We first compute

$$\begin{aligned}
C(\mathbb{F}_5) = \{&(1:0:0), (0:4:1), (0:1:1), (1:4:1), (1:1:1),\\
&(2:0:1), (4:4:1), (4:1:1), (3:3:1), (3:2:1)\}.
\end{aligned}$$

In general, one does not always have computational access to generators of the Mordell–Weil group of a genus 3 curve. However, this is not needed; see Remark 5.3.11. Instead, we can consider the set of differences of pairs of known rational points inside the Mordell–Weil group. Computing the canonical height pairing of each of the set of differences themselves, we look for the elements with the smallest canonical height (using code from [Sto17]); let $G_1 \coloneqq (0:1:1) - \infty$ and $G_2 \coloneqq (1:1:1) - \infty$. We can check that G_1 and G_2 are linearly independent by computing that their logarithms are linearly independent. Let H be the subgroup of the Mordell–Weil group generated by G_1 and G_2. We cannot always expect H is equal to the full Mordell–Weil group $J(\mathbb{Z})$, but by Remark 5.3.11 it is enough for H to be saturated at 5 and the primes dividing $|J(\mathbb{F}_5)| = 340$.

To check whether H is saturated at a given prime ℓ, we compute the kernel of the map

$$G/\ell G \to \prod_q J(\mathbb{F}_q)/\ell J(\mathbb{F}_q)$$

where q runs over some small primes such that $\ell \mid |J(\mathbb{F}_q)|$ and check if this kernel is trivial [Sto17, Section 12] (using code from [MS]). If the kernel is not trivial, then we cannot apply geometric linear Chabauty, but if we suspect G is equal to M, then in practice, this verification step terminates almost instantaneously.

We construct the following subgroup of $J(\mathbb{F}_5)$:

$$\overline{H} := \langle \overline{G}_1, \overline{G}_2 \rangle .$$

This allows us to sieve at 5 by intersecting with the image of $C(\mathbb{F}_5)$

$$H' := \{c : c \in C(\mathbb{F}_p) \text{ and } (c - \infty) \in \overline{H}\} = \{(1:0:0), (0:\pm 1:1), (1:\pm 1:1)\},$$

showing that only the reductions of the $\mathbb{Z}_{(5)}$-points modulo 5 do not fail the Mordell–Weil sieve.

The Chabauty–Coleman method finds points in residue disks corresponding to the $\mathbb{F}_5$-points $\{(2:0:1), (4:4:1), (4:1:1), (3:3:1), (3:2:1)\}$, which are ruled out by this test.

The extra points R_i and W found by the Chabauty–Coleman method but not the geometric linear Chabauty method are torsion in $J(\mathbb{Z}_5)/M$ but do not lie in M.

Example 5.5.8. Finally, we give an example of Theorem 5.5.1 Item 2 where M does not have good reduction, and the Chabauty–Coleman set contains extra points R such that $\mathsf{log}(R - b)$ is not in $\mathsf{log} M$, only in its p-saturation. These extra points pass the Mordell–Weil sieve but are ruled out by the geometric linear Chabauty method.

Let $C/\mathbb{Z}_{(3)}$ be (the smooth projective model of) the genus 3 curve

$$y^2 = x^7 - 3x^6 + 5x^5 - 5x^4 + 3x^3 - x^2 + 1/4$$

taken from a database of genus 3 hyperelliptic curves over $\mathbb{Q}$ [Sut] computed using the methods in [BSS+16].

The points up to height 1000 are

$$C(\mathbb{Z}_{(3)})_{\text{known}} := \{(1:0:0), (0:-1/2:1), (0:1/2:1), (1:-1/2:1), (1:1/2:1)\}.$$

According to computations with the fake 2-Selmer group done by the method `RankBounds` in Magma, the Mordell–Weil rank of J is 2.

The Chabauty–Coleman method produces the set

$$\begin{aligned}&C(\mathbb{Z}_3)_{\mathrm{CC}} =\\ &\{(1:0:0),(0:-1/2:1),(0:1/2:1),(1:-1/2:1),(1:1/2:1),\\ &R_1 := (2+3^3+2\cdot 3^4+2\cdot 3^7+O(3^8) : 1+3+2\cdot 3^4+2\cdot 3^5+2\cdot 3^6+O(3^8) : 1),\\ &R_2 := (2+3^3+2\cdot 3^4+2\cdot 3^7+O(3^8) : -(1+3+2\cdot 3^4+2\cdot 3^5+2\cdot 3^6+O(3^8)) : 1)\}.\end{aligned}$$

However, we will use geometric linear Chabauty modulo $p = 3$ to show that the residue disks over the reductions $\overline{R_i}$ do not contain any rational points. We consider the residue disk over $\overline{R_1} = (2 : 1 : 1)$; the other will follow by the hyperelliptic involution. Using Magma, we can check the residue disk of the Mordell–Weil group over $\overline{R_1 - b}$ is non-empty, and we can even find an explicit $T \in M_{\overline{R_1-b}}$, namely $T := 73((1 : 0 : 0) - (0 : -1 : 1))$.

Similar to the previous example, as per Remark 5.3.11, we compute $G_1 := (0 : 1/2 : 1) - \infty$ and $G_2 := (1 : 1/2 : 1) - \infty$ generating a subgroup H of the Mordell–Weil group, and verify that H is saturated at the single prime $p = 3$. Since $\overline{R_1}$ passes the Mordell–Weil sieve at 3, we do not have to check H is saturated at any other primes.

To compute $\overline{\mathcal{M}}_0$, we find a basis $\langle \widetilde{G_1} := -6G_1 - 4G_2,\ \widetilde{G_2} := -10G_1 + 11G_2\rangle$ for the kernel of reduction modulo 3, and compute

$$\begin{aligned}\mathsf{log}(\widetilde{G_1}) &= (2, 1, 1)\\ \mathsf{log}(\widetilde{G_2}) &= (2, 1, 1)\end{aligned}$$

in $\mathbb{F}_3^3$. The map $M_0/3M_0 \to J(\mathbb{Z}/3^2\mathbb{Z})_0$ has a 1-dimensional kernel generated by $\widetilde{G_1} - \widetilde{G_2}$, so $\overline{\mathcal{M}}_0$ has bad reduction.

By lifting $\overline{R_1}$ in two different ways, Q_1 and Q_2, and taking a tiny integral, we compute that the subspace $D_Q = \langle Q_1 - Q_2\rangle$ is spanned by the vector $\mathsf{log}(Q_1 - Q_2) = (2, 1, 2)$ in $\mathbb{F}_3^3$. Finally, $\mathsf{log}(v) = \mathsf{log}(Q_1 - \infty - T) = (2, 2, 1)$. Altogether, we have computed the determinant zero matrix

$$A_{(2:1:1)} = \begin{pmatrix} 2 & 2 & 2\\ 1 & 1 & 1\\ 1 & 1 & 2\end{pmatrix}$$

representing the linear map $\varphi : D_Q \oplus \overline{\mathcal{M}}_0 \to J(\mathbb{Z}/3\mathbb{Z})_0$. Since $\mathsf{log}(v)$ is not in the image of this matrix, the residue disk over $\overline{R_1}$ does not contain any rational points. Furthermore, applying the hyperelliptic involution to the calculations, we can also rule out the residue disk of R_2 from containing rational points.

Hence $C(\mathbb{Z}_3)_{\mathrm{GLC}} = C(\mathbb{Z}_{(3)}) = C(\mathbb{Z}_{(3)})_{\mathrm{known}}$ does not contain R_1 and R_2. Another way to see this, by Corollary 5.5.3, which is applicable as $|J(\mathbb{F}_3)| = 2 \cdot 53$, is to compute the following integral

$$\begin{aligned}&\mathsf{log}(R_1 - \infty)\\&\qquad = (2 + 2 \cdot 3 + 2 \cdot 3^2 + O(3^3), 2 + 3 + O(3^3), 1 + 2 \cdot 3 + 2 \cdot 3^2 + O(3^3));\end{aligned}$$

we see that reduced modulo 3, this is not in the span of the reductions modulo 3 of $\mathsf{log}(\widetilde{G_1})$ and $\mathsf{log}(\widetilde{G_2})$. We can compute that, truncated to 5 digits of precision, we have

$$\begin{aligned}\mathsf{log}(R_1 - \infty) = (2 \cdot 3^{-1} + 2 + 3^4 + O(3^5))&\mathsf{log}(\widetilde{G_1}) +\\ &(3^{-1} + 1 + 3 + 3^2 + 2 \cdot 3^3 + 2 \cdot 3^4 + O(3^5))\mathsf{log}(\widetilde{G_2}),\end{aligned}$$

further explaining why this point is found by the Chabauty–Coleman method but not by geometric linear Chabauty, since $R_1 - \infty$ lies in the 3-saturation of M inside $J(\mathbb{Z}_3)$, but not in M itself.