Quadratic Chabauty for Modular curves: Algorithms and examples

Jennifer S. Balakrishnan, Netan Dogra, J. Steffen Müller, Jan Tuitman and Jan Vonk

Dedicated to the memory of Bas Edixhoven (1962 – 2022)

Abstract

We describe how the quadratic Chabauty method may be applied to determine the set of rational points on modular curves of genus $g > 1$ whose Jacobians have Mordell–Weil rank g. This extends our previous work on the split Cartan curve of level 13 and allows us to consider modular curves that may have few known rational points or nontrivial local height contributions at primes of bad reduction. We illustrate our algorithms with a number of examples where we determine the set of rational points on several modular curves of genus 2 and 3: this includes Atkin–Lehner quotients $X_0^+(N)$ of prime level N, the curve $X_{S_4}(13)$, as well as a few other curves relevant to Mazur's Program B. We also compute the set of rational points on the genus 6 non-split Cartan modular curve $X_{\mathrm{ns}}^+(17)$.

1. Introduction

In this paper, we describe the current state of quadratic Chabauty–based algorithms for the resolution of Diophantine equations arising from modular curves. Here we consider the usual modular curves associated to congruence subgroups of $SL_2(\mathbf{Z})$, as well as Atkin–Lehner quotients thereof.

Recall the motivating question of the subject: let E be an elliptic curve over a number field K. What are the possible ways for the Galois group $\mathrm{Gal}(\overline{K}/K)$ to act on the group of torsion points of E? Equivalently, what are the conjugacy classes of subgroups of $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$ arising as images of the mod N Galois representation $\rho_{E,N}$?

By a theorem of Serre [Ser72], if E is an elliptic curve without complex multiplication, then for all primes $N \gg 0$, the representation $\rho_{E,N}$ is surjective. Serre's uniformity question [Ser72] asks whether this can be made *uniform* over $\mathbf{Q}$: is there an N_0 such that, for all primes $N > N_0$, if $E/\mathbf{Q}$ is an elliptic curve without complex multiplication, then $\rho_{E,N}$ is surjective? By a classification of maximal subgroups of $\mathrm{GL}_2(\mathbf{Z}/N\mathbf{Z})$, this amounts to determining elliptic curves whose mod N Galois representation is contained in a Borel subgroup, the normaliser of a split Cartan subgroup, the normaliser of a non-split Cartan subgroup, or an 'exceptional' subgroup (such that the projective image is S_4, A_4, or A_5).

Mazur's Program B [Maz77] asks for all of the possible Galois actions on torsion subgroups of elliptic curves without complex multiplication. This question includes Serre's uniformity question but is more general. From a Diophantine perspective, it roughly amounts to determining the rational points on all modular curves.

Rouse and Zureick-Brown [RZB15] settled this in the context of 2-primary torsion and very recently, with Sutherland [RSZB21], studied this in the context of ℓ-primary torsion for other primes ℓ. For each prime, this produces a

2020 Mathematics Subject Classification 11G18, 11G50, 11Y50, 14G05

Keywords: p-adic heights, Diophantine equations, modular curves, non-abelian Chabauty, rational points

JB was supported by NSF grant DMS-1945452, the Clare Boothe Luce Professorship (Henry Luce Foundation), Simons Foundation grant #550023, and a Sloan Research Fellowship. ND was supported by a Royal Society University Research Fellowship. SM was supported by DFG grant MU 4110/1-1 and by NWO Grant VI.Vidi.192.106. JV was supported by ERC-COG Grant 724638 'GALOP' and Francis Brown, the Carolyn and Franco Gianturco Fellowship at Linacre College (Oxford), and NSF Grant No. DMS-1638352, and NWO Grant VI.Vidi.213.084 during various stages of this project.

finite number of curves, the determination of whose rational points would resolve the ℓ-primary part of Mazur's question. In §5.1 and §5.3 we compute the rational points on four modular curves $X_{S_4}(13), X_{\mathrm{ns}}^+(17), X_{11}$, and X_{15} arising in Mazur's Program B. In particular, we show the following:

Theorem 1.1. *We have $\#X_{S_4}(13)(\mathbf{Q}) = 4$. One of these points is a CM point, corresponding to discriminant $D = -3$. The other three are exceptional, with corresponding j-invariants listed in §5.1.*

Here we call a non-cuspidal rational point *exceptional* if it does not correspond to an elliptic curve with complex multiplication. The curve $X_{S_4}(13)$ has genus 3. This completes the classification of elliptic curves $E/\mathbf{Q}$ and prime level $N > 0$ such that $\rho_{E,N}$ is contained in an exceptional subgroup.

We also determine the rational points on $X_{\mathrm{ns}}^+(17)$, the non-split Cartan modular curve of level 17, which is a genus 6 curve:

Theorem 1.2. *We have $\#X_{\mathrm{ns}}^+(17)(\mathbf{Q}) = 7$ and all of these points are CM, corresponding to discriminants $-3, -7, -11, -12, -27, -28, -163$.*

Theorems 1.1 and 1.2 complete the classification of the possible 13-adic and 17-adic images of Galois.

Moving beyond torsion points of elliptic curves over $\mathbf{Q}$, another interesting problem in the Diophantine geometry of modular curves is the determination of the set of rational points on the Atkin–Lehner quotient

$$X_0^+(N) := X_0(N)/\langle w_N \rangle$$

of the modular curve $X_0(N)$. In [Gal02], Galbraith asks whether, for all primes $N \gg 0$, the only rational points on $X_0^+(N)$ are cusps or CM points. From a moduli perspective, this amounts to finding quadratic $\mathbf{Q}$-curves that are N-isogenous to their conjugates. Dogra and Le Fourn [DF21] proved that the quadratic Chabauty set $X_0^+(N)(\mathbf{Q}_p)_2$ is finite whenever the genus of $X_0^+(N)$ is larger than one. Hence it is natural to ask whether the methods of this paper can be used to give an algorithm for computing $X_0^+(N)(\mathbf{Q}_p)_2$ for any N. In fact, in the range of N we consider, finiteness of $X_0^+(N)(\mathbf{Q}_p)_2$ follows from a criterion appearing in earlier work of Siksek [Sik17]. Our computations described in §5.2 prove the following result.

Theorem 1.3. *The only prime values N such that the curve $X_0^+(N)$ is of genus 2 or 3 and has an exceptional rational point are $N = 73, 103, 191$. In particular for prime N, there are no exceptional rational points on curves $X_0^+(N)$ of genus 3.*

All rational points in Theorem 1.3 had already been found by Galbraith [Gal99].

Remark 1.4. These computations were recently extended significantly by Adžaga, Arul, Beneish, Chen, Chidambaram, Keller, and Wen [AAB$^+$21]. They use the quadratic Chabauty method described in this paper to determine the set of rational points on all curves $X_0^+(N)$ of genus 4,5 and 6 and prime level N. Arul and Müller [AM] also compute the rational points on $X_0^+(125)$ using the same method. Adžaga, Chidambaram, Keller, and Padurariu [ACKP] use several techniques, including quadratic Chabauty, to determine the set of rational points on the hyperelliptic Atkin–Lehner star quotient curves $X_0^*(N)$.

Going further, one may wonder what the potential applications of these algorithms are to *non-modular* curves. The main stumbling block in attempting such a generalisation is our running assumption on the Mordell–Weil rank and Picard number of the Jacobian (see §2.1). Since a generic curve has Picard number one, it is not clear how often one should expect a genus g curve with Mordell–Weil rank g to satisfy the quadratic Chabauty hypothesis. Nevertheless, there are other interesting curves where one *would* expect to get some mileage out of such algorithms. The most obvious examples are (Atkin–Lehner quotients of) Shimura curves. In particular, determining the set of rational points on the (infinitely many) curves $X^D/\langle w_D \rangle$, in the notation of Parent–Yafaev [PY07], would resolve a conjecture of Clark [Cla03] (Parent and Yafaev determine the rational points for an infinite family of Shimura curves whose Jacobian contains a rank zero isogeny factor).

Acknowledgements

We are deeply indebted to Bas Edixhoven for his numerous generous insights on this subject. It is a pleasure to thank Noam Elkies, Barry Mazur, Jeremy Rouse, Andrew Sutherland, and David Zureick-Brown for suggesting several modular curves of interest, as well as many helpful discussions, which provided the impetus for this work. We are grateful for the contributions of Nikola Adžaga, Vishal Arul, Lea Beneish, Alex Best, Francesca Bianchi, Mingjie Chen, Shiva Chidambaram, Timo Keller, Nicholas Triantafillou, and Boya Wen in finding a number of bugs in earlier versions of our code. We would also like to thank Michael Stoll for kindly providing an implementation of the Mordell–Weil sieve, on which ours is based and Nils Bruin for sharing another approach to determining $C_{188}(\mathbf{Q})$. We are grateful to Francesca Bianchi, David Holmes, Timo Keller and Michael Stoll for helpful comments on an earlier version of this article. We thank the referee for a helpful and entertaining report.

2. Quadratic Chabauty: Theory

We give a brief overview of the quadratic Chabauty method. A more complete exposition can be found in [BBB$^+$21], and we refer the reader to [BD18, BDM$^+$19] for more precise details and proofs. Our description is in terms of Galois representations and filtered ϕ-modules, but we note that recently, Edixhoven and Lido [EL21] gave a geometric version of quadratic Chabauty, which they used to determine the set of rational points on the bielliptic modular curve $X_0(129)/\langle w_3, w_{43}\rangle$ of genus 2. Duque-Rosero, Hashimoto, and Spelier [DRHS] have related this approach to the one presented here and used this to give algorithms for geometric quadratic Chabauty for hyperelliptic curves. Besser, Müller, and Srinivasan [BMS] have also given an alternative approach to the quadratic Chabauty method based on a new construction of p-adic heights on abelian varieties via p-adic Arakelov theory.

An early version of the method appeared in work of Kim [Kim10, BKK11], where Massey products were used to construct a locally analytic function, vanishing on the set of integral points of an elliptic curve of rank 1. These functions were interpreted as height functions, extending the method, in Balakrishnan–Besser [BB15] and Balakrishnan–Besser–Müller [BBM16]. It was extended to its current form in Balakrishnan–Dogra [BD18], where a systematic use of Nekovář's theory of p-adic heights suggested a streamlined approach towards a very general class of curves allowing an abundance of geometric correspondences. It was carried out to determine the set of rational points on $X_{\mathrm{s}}^+(13)$, the split Cartan curve of level 13, in [BDM$^+$19].

Remark. This method fits into the vastly more general framework developed by Kim [Kim05, Kim09], elaborating on the idea of studying rational points on curves through path torsors of the étale fundamental group, suggested by Grothendieck's section conjecture. The approach discussed here represents an effective way to make this theory computable and applicable to a variety of examples. It is, however, important to note that different quotients of the fundamental group have been successfully used for this purpose, see for instance [BD21]. Finally, although we restrict our attention to the base field $\mathbf{Q}$, suitable versions exist over number fields, see [BD18, BD21, BBBM21].

2.1 Rational points and global heights.

Consider a smooth projective curve $X_{\mathbf{Q}}$ of genus $g \geqslant 2$ whose Jacobian J has rank $r = g$. We also assume that the abelian logarithm induces an isomorphism

$$\log\colon J(\mathbf{Q}) \otimes \mathbf{Q}_p \to \mathrm{H}^0(X_{\mathbf{Q}_p}, \Omega^1)^\vee \tag{2.1}$$

and that $X(\mathbf{Q})$ is non-empty, so we may choose a base point b in $X(\mathbf{Q})$. Suppose that the Néron–Severi rank $\mathrm{rk}_{\mathbf{Z}}\mathrm{NS}(J)$ is at least 2, so that there exists a nontrivial class

$$Z \in \mathrm{Ker}\left(\mathrm{NS}(J) \longrightarrow \mathrm{NS}(X) \simeq \mathbf{Z}\right).$$

As explained in Balakrishnan–Dogra [BD18, Lemma 3.2], we can attach to any such choice of Z a suitable quotient U_Z of the $\mathbf{Q}_p$-pro-unipotent fundamental group of $X_{\bar{\mathbf{Q}}}$, which via a twisting construction by path torsors, gives rise

to a certain family of Galois representations

$$\begin{array}{ccc} X(K) & \longrightarrow & \{G_K \to \mathrm{GL}_{2g+2}(\mathbf{Q}_p)\} \,/\sim \\ x & \longmapsto & \mathrm{A}(x) := \mathrm{A}_Z(b,x) \end{array}$$

where $K \in \{\mathbf{Q}, \mathbf{Q}_p\}$ and G_K is the absolute Galois group of K. We refer the reader to [BD18, §5.1] for the details of this construction (in particular for the equivalence relation), and merely recall here that with respect to a suitable choice of basis, the representation $\mathrm{A}(x)$ is lower triangular, of the form

$$g \in G_K \longmapsto \begin{pmatrix} 1 & & \\ \alpha(g) & \rho_V(g) & \\ \gamma(g) & \beta(g) & \chi_p(g) \end{pmatrix} \tag{2.2}$$

where

$$\rho_V \colon G_K \longrightarrow \mathrm{GL}_{2g}(\mathbf{Q}_p)$$

is a frame for the Galois action on the p-adic étale homology $V = \mathrm{H}^1_{\text{ét}}(X_{\overline{K}}, \mathbf{Q}_p)^\vee$, and $\chi_p \colon G_K \to \mathbf{Q}_p^\times$ is the p-adic cyclotomic character. Representations of this form, which admit a G_K-stable filtration with graded pieces $\mathbf{Q}_p(1), V, \mathbf{Q}_p$, are referred to as *mixed extensions*, see [BDM$^+$19, §3.1].

The theory of p-adic heights due to Nekovář [Nek93, §2] attaches to any mixed extension M a p-adic height $h(M)$. When applied to the family of mixed extensions $\mathrm{A}(x)$, this results in a map

$$h \colon X(\mathbf{Q}) \longrightarrow \mathbf{Q}_p.$$

The algebraic properties of this map lie at the heart of the quadratic Chabauty method. Most notably, the method relies on the following two facts:

- The p-adic height is a bilinear function of the pair of cohomology classes $([\alpha], [\beta])$ associated to the vectors appearing in (2.2).
- It decomposes as a sum of local height functions h_v defined locally at every finite place v.

2.2 Local decomposition.

We now discuss in more detail the decomposition of the global p-adic height h described above, as a sum of local height functions

$$h_v \colon X(\mathbf{Q}_v) \longrightarrow \mathbf{Q}_p.$$

The nature of these local height functions is as follows:

(i) **The case $v \neq p$:** It follows from Kim–Tamagawa [KT08, Corollary 0.2] that the function h_v has finite image, in the sense that there exists a finite set Υ_v such that

$$h_v \colon X(\mathbf{Q}_v) \longrightarrow \Upsilon_v \subset \mathbf{Q}_p.$$

(ii) **The case $v = p$:** The map h_p is locally analytic and has a simple description in terms of linear algebra data of the filtered ϕ-module

$$M(x) := \left(\mathrm{A}(x) \otimes_{\mathbf{Q}_p} \mathrm{B}_{\mathrm{cris}}\right)^{G_{\mathbf{Q}_p}},$$

where $\mathrm{B}_{\mathrm{cris}}$ is Fontaine's crystalline period ring. A crucial point in the method of quadratic Chabauty is that the definition of the family of Galois representations $\mathrm{A}(x)$ comes from a motivic quotient of the fundamental group of X, and non-abelian p-adic Hodge theory yields an analogous de Rham realisation in the form of a filtered connection $(\mathscr{M}, \nabla)$ on X with a Frobenius structure, together with an isomorphism of filtered ϕ-modules

$$x^*\mathscr{M} \simeq M(x)$$

(see [BDM$^+$19, §5]). We have a pair of elements $\pi_1(M(x))$ and $\pi_2(M(x))^\vee(1)$ of $\mathrm{H}^0(X_{\mathbf{Q}_p}, \Omega)^\vee$ associated to the filtered ϕ-module $M(x)$, via the isomorphism

$$\mathrm{Ext}^1_{\mathrm{Fil},\phi}(\mathbf{Q}_p, \mathrm{H}^1_{\mathrm{dR}}(X_{\mathbf{Q}_p})^\vee) \simeq \mathrm{H}^0(X_{\mathbf{Q}_p}, \Omega)^\vee.$$

2.3 Finiteness.

The decomposition $h = \sum_v h_v$ can be used to leverage the bilinear nature of h against the properties of the functions h_v. By (1) in §2.2, we know that there exists a finite set $\Upsilon = \Upsilon_Z \subset \mathbf{Q}_p$ such that

$$h(x) - h_p(x) \ \in \ \Upsilon \tag{2.3}$$

for any x in $X(\mathbf{Q})$. In Section 3, we describe how the terms in this equation may be computed explicitly.

- The set Υ is given by $\{\sum_v \epsilon_v : \epsilon_v \in \Upsilon_v\}$, where the sum is over primes of bad reduction, and Υ_v is the set of values of $h_v(x)$ for $x \in X(\mathbf{Q}_v)$. For $v \neq p$, the map h_v is made more explicit in §3.1 using the results of Betts–Dogra [BD19] to compute Υ_v when a regular semi-stable model $\mathcal{X}$ is known. The map h_v factors through the reduction map to the irreducible components of the special fibre of $\mathcal{X}$.
- The map h_p may be computed using [BDM$^+$19, §§4,5], where it is explained how the universal properties of the bundle $\mathscr{M}$ rigidify the (known) structures on the graded pieces, enough to allow us to compute them explicitly, see §3.2.
- Using the isomorphism (2.1), we may view the global height as a pairing

  $$h\colon \mathrm{H}^0(X_{\mathbf{Q}_p}, \Omega^1)^\vee \otimes \mathrm{H}^0(X_{\mathbf{Q}_p}, \Omega^1)^\vee \ \longrightarrow \ \mathbf{Q}_p.$$

  Using global information, such as an abundance of global points $x \in X(\mathbf{Q})$ if available, we can solve for the height pairing. This is discussed in §3.3, where we also explain what to do when too few rational points are available.

Via the above, the map h may be extended to a bilinear map

$$h\colon X(\mathbf{Q}_p) \to \mathbf{Q}_p\,; \qquad x \mapsto h(\pi_1(\mathrm{A}(x)), \pi_2(\mathrm{A}(x))^\vee(1))\,. \tag{2.4}$$

The resulting map

$$\rho = h - h_p\colon X(\mathbf{Q}_p) \ \longrightarrow \ \mathbf{Q}_p \tag{2.5}$$

is known to be Zariski dense on every residue disk. We call ρ a *quadratic Chabauty function*, and we write ρ_Z if we want to emphasise the dependence on Z. Hence (2.3) implies that $X(\mathbf{Q})$ is finite. Moreover, the computable nature of the quantities involved in (2.3), discussed at length in the next section, allows us to explicitly determine a p-adic approximation of the finite set

$$\{x \in X(\mathbf{Q}_p)\colon h(x) - h_p(x) \in \Upsilon\} \supset X(\mathbf{Q})\,.$$

As explained in [BD18, Proposition 5.5], this finite set contains the Chabauty–Kim set $X(\mathbf{Q}_p)_2$. In particular, a proof that this set equals $X(\mathbf{Q})$ gives a verification of Kim's conjecture [BDCKW18, Conjecture 3.1] for the curve X (we refer the reader to [BDCKW18, Definition 2.7] for the definitions of the set $X(\mathbf{Q}_p)_2$).

3. Quadratic Chabauty: Algorithms

In this section, we discuss the computation of the three ingredients outlined above:

(i) The local height function h_v for v away from p, which is described in §3.1 using the techniques in Betts–Dogra [BD19], given a regular semi-stable model at v.

(ii) The height function h_p, whose computation using the techniques of [BDM$^+$19] is described in §3.2

(iii) The determination of the global height pairing h, described in §3.3 using rational divisors as input in the absence of a supply of rational points on the curve.

Our contribution in this paper lies mainly in (1) and (3), which reflect general features of the method of quadratic Chabauty that were not needed for the curve $X_{\mathrm{s}}^+(13)$ treated in [BDM$^+$19]. In addition, we discuss some computational techniques to further automate the method of quadratic Chabauty to work for a wide class of modular curves.

This includes the Mordell–Weil sieve, which is used to attempt to further refine the finite set of local points in the output to the true set of rational points $X(\mathbf{Q})$.

Remark 3.1. The global height depends on the choice (which we fix henceforth) of

- a nontrivial continuous idèle class character $\chi\colon \mathbf{A}_{\mathbf{Q}}^{\times}/\mathbf{Q}^{\times} \longrightarrow \mathbf{Q}_p$ ramified at p;
- a splitting $s\colon V_{\mathrm{dR}}/\mathrm{Fil}^0 V_{\mathrm{dR}} \longrightarrow V_{\mathrm{dR}}$ of the Hodge filtration, where

$$V_{\mathrm{dR}} = \mathrm{D}_{\mathrm{cris}}(V) = \mathrm{H}^1_{\mathrm{dR}}(X_{\mathbf{Q}_p})^{\vee}.$$

We also fix differentials $\omega_0, \ldots, \omega_{2g-1}$ of the second kind whose classes form a symplectic basis of $\mathrm{H}^1_{\mathrm{dR}}(X_{\mathbf{Q}_p})$ with respect to the cup product, such that $\omega_0, \ldots, \omega_{g-1}$ generate $\mathrm{H}^0(X_{\mathbf{Q}_p}, \Omega^1)$.

3.1 Local heights away from p

Let $\ell \neq p$ and let F be an endomorphism of J whose class Z lies in $\mathrm{Ker}\,(\mathrm{NS}(J) \to \mathrm{NS}(X))$. In [BD19], a description of the map

$$h_\ell\colon X(\mathbf{Q}_\ell) \longrightarrow \mathrm{H}^1(G_\ell, U_Z) \longrightarrow \mathrm{H}^1(G_\ell, \mathbf{Q}_p(1)) \longrightarrow \mathbf{Q}_p$$

associated to F and χ is given, in terms of harmonic analysis on the reduction graph in the sense of Zhang [Zha93].

To explain the result, we introduce some notation. Over some finite extension $K/\mathbf{Q}_\ell$, the curve X admits a regular semistable model $\mathcal{X}_{\mathrm{reg}}/\mathcal{O}_K$, and a stable model $\mathcal{X}_{\mathrm{st}}/\mathcal{O}_K$. Let Γ_{reg} and Γ_{st} denote the dual graphs of the special fibres of these models. Recall that the *dual graph* of the special fibre is by definition the graph [1] whose vertices are the irreducible components of the special fibre, and whose edges are the singular points of the special fibre. The endpoints of an edge e are defined to be the irreducible components containing the point (by semistability, a singular point e lies on at most two irreducible components). By regularity, we have a reduction map

$$\mathrm{red}\colon X(\mathbf{Q}_\ell) \longrightarrow V(\Gamma_{\mathrm{reg}})$$

from $X(\mathbf{Q}_\ell)$ to the vertices of the dual graph Γ_{reg}.

The definition is the natural one: given $x \in X(\mathbf{Q}_\ell)$, there is a unique extension to an $\mathcal{O}_K$-section $x \in \mathcal{X}_{\mathrm{reg}}(\mathcal{O}_K)$. Let k be the residue field of $\mathcal{O}_K$. By regularity, the specialisation of x to k lies on a unique irreducible component of $\mathcal{X}_{\mathrm{reg},k}$.

We may give Γ_{reg} and Γ_{st} the structure of *rationally metrised* graphs (i.e. graphs whose edges e have associated lengths $\ell(e) \in \mathbf{Q}_{>0}$) by defining the length of an edge e to be $i(e)/r$, where i is the intersection multiplicity of the corresponding singular point and r is the ramification degree of $K/\mathbf{Q}_\ell$.

Choose an orientation of the edges of $\Gamma := \Gamma_{\mathrm{st}}$, so that each $e \in E(\Gamma)$ has a source $s(e)$ and target $t(e)$ in $V(\Gamma)$. We define the (rational) homology of Γ, $H_1(\Gamma) \subset \mathbf{Q}E(\Gamma)$, to be the kernel of the map

$$s - t\colon \mathbf{Q}E(\Gamma) \to \mathbf{Q}V(\Gamma),$$

where $\mathbf{Q}E(\Gamma)$ and $\mathbf{Q}V(\Gamma)$ are the free $\mathbf{Q}$-vector spaces generated by $E(\Gamma)$ and $V(\Gamma)$ respectively.

Define $\Gamma_{\mathbf{Q}}$ to be the set of points on Γ whose distance from a vertex is rational: formally,

$$\Gamma_{\mathbf{Q}} = \sqcup_{e \in E(\Gamma_{\mathrm{st}})} \{e\} \times ([0, \ell(e)] \cap \mathbf{Q})/\sim,$$

where the equivalence relation is that $(e_1, 1) \sim (e_2, 0)$ whenever $t(e_1) = s(e_2)$. Since $\mathcal{X}_{\mathrm{reg}}$ is obtained from $\mathcal{X}_{\mathrm{st}}$ by taking each singular point (corresponding to an edge e) and blowing up $i(e)$ times, we have an inclusion $V(\Gamma_{\mathrm{reg}}) \subset \Gamma_{\mathbf{Q}}$ (in the terminology of [BD19, 3.7.1], we may view Γ_{reg} as a rational subdivision of Γ_{st}). In this way we can think of the reduction map red as a map from $X(K)$ to $\Gamma_{\mathbf{Q}}$, see [BD19, Definition 1.3.1]. The rationally metrised graph we obtain is independent of the choice of extension over which X acquires stable reduction [CR91, Proposition 2.6], and

[1] Here we follow the convention that graphs are allowed multiple edges between two vertices, and loops (i.e. an edge whose endpoints are equal).

in fact there is an equivalent definition of $\Gamma_{\mathbf{Q}}$ as the limit of the dual graphs of special fibres of regular semistable models of X_L over all finite extensions L of K (see [CR93, §2]).

In [BD19, Lemma 12.1.1], a map

$$j_\Gamma \colon \Gamma_{\mathbf{Q}} \to \mathbf{Q}_p$$

is defined such that $h_\ell = c \cdot j_\Gamma \circ \mathrm{red}$, where c is a constant. The map j_Γ is defined in terms of the Laplacian operator associated to Γ_{st}, which we now define. We say a function

$$\Gamma_{\mathbf{Q}} \to \mathbf{Q}_p$$

is *piecewise polynomial* if on each edge it is the restriction of a polynomial function $\mathbf{Q} \to \mathbf{Q}_p$. As in [BD19, Definition 7.2.2], we define the *Laplacian* $\nabla^2(g)$ of a piecewise polynomial function $g \colon \Gamma_{\mathbf{Q}} \to \mathbf{Q}_p$ to be the formal sum

$$-\sum_{e \in E(\Gamma)} g''(x_e) \cdot e + \sum_{v \in V(\Gamma)} \Big(\sum_{s(e)=v} g'(0) - \sum_{t(e)=v} g'(1) \Big) \cdot v.$$

Here we write the function g restricted to the edge e as a polynomial in $\mathbf{Q}_p[x_e]$ for notational simplicity, where x_e is the inclusion from the edge e, thought of as a line segment $[0, \ell(e)] \cap \mathbf{Q}$, into $\mathbf{Q}$. Hence we have

$$\nabla^2(g) \in \bigoplus_{e \in E(\Gamma)} \mathbf{Q}_p[x_e] \cdot e \oplus \bigoplus_{v \in V(\Gamma)} \mathbf{Q}_p \cdot v\,.$$

The Laplacian is linear on piecewise polynomial functions, and its kernel consists of constant functions. Thus g is uniquely determined by $\nabla^2(g)$ and its value at one point.

In [BD19], an explicit construction is given of a piecewise polynomial function that corresponds, via red, to the local height function we wish to compute. Recall that F is an element of $\mathrm{End}(J) \otimes \mathbf{Q}_p$ whose image in $\mathrm{NS}(J)$ lies in the kernel of $\mathrm{NS}(J) \to \mathrm{NS}(X)$, and $b \in X(\mathbf{Q})$ is a rational point.

Theorem 3.2 [BD19, Theorem 1.1.2, Lemma 12.1.1, and Corollary 12.1.3]. *Let Γ be the dual graph of X corresponding to a regular semi-stable model of X over $\mathcal{O}_K$, where $K/\mathbf{Q}_\ell$ is a finite extension. Let $\mathrm{red} \colon X(\mathbf{Q}_\ell) \to V(\Gamma)$ be the reduction map. For an irreducible component X_w of the special fibre of the regular semistable model, let $V_p(X_w)$ denote the $\mathbf{Q}_p$-Tate module of its Jacobian. The morphism j_Γ is the unique piecewise polynomial function*

$$j_\Gamma \colon \Gamma_{\mathbf{Q}} \to \mathbf{Q}_p$$

satisfying $j_\Gamma(\mathrm{red}(b)) = 0$ and $\nabla^2(j_\Gamma) = \mu_F$, where

$$\mu_F := \sum_{e \in E(\Gamma)} \frac{1}{\ell(e)} e^* F(\pi(e)) \cdot e + \frac{1}{2} \sum_{w \in V(\Gamma)} \mathrm{Tr}(F | V_p(X_w)) \cdot w.$$

Here, the morphism π is by definition the orthogonal projection

$$\mathbf{Q}E(\Gamma) \to \mathrm{H}_1(\Gamma, \mathbf{Q})$$

with respect to the pairing $e \cdot e' = \delta_{ee'}$ on $\mathbf{Q}E(\Gamma)$, and e^* is the functional $\mathbf{Q}E(\Gamma) \to \mathbf{Q}$ projecting onto the e component. Recall (e.g. [SGA7, 12.3.7]) that $V_p(X)$ admits a G_K-stable filtration

$$V_p(X) = W_0 V_p(X) \supset W_1 V_p(X) \supset W_2 V_p(X) \supset W_3 V_p(X) = 0,$$

and we have isomorphisms of G_K-representations

$$\begin{aligned} \mathrm{gr}_0^W V_p(X) &\simeq H_1(\Gamma) \otimes \mathbf{Q}_p, \\ \mathrm{gr}_1^W V_p(X) &\simeq \oplus_{w \in V(\Gamma)} V_p(X_w), \\ \mathrm{gr}_2^W V_p(X) &\simeq H_1(\Gamma)^* \otimes \mathbf{Q}_p(1). \end{aligned}$$

The action of F on $V_p(X)$ preserves this filtration since it is a morphism of Galois representations, and hence induces an action of F on the weight -1 part of $V_p(X)$, which is isomorphic to $\oplus_w V_p(X_w)$. Although the action of F need

not respect the direct sum decomposition, the decomposition

$$\mathrm{End}(\oplus_w V_p(X_w)) \simeq \oplus_{w_1,w_2}\mathrm{Hom}(V_p(X_{w_1}), V_p(X_{w_2}))$$

implies that we can define $\mathrm{Tr}(F|V_p(X_w))$ as the trace of the $\mathrm{End}(V_p(X_w))$-component of F.

To determine the possible local heights, it suffices to compute the action of F on $\mathrm{H}_1(\Gamma)$ and on $V_p(X_v)$. In this paper, we do not discuss methods for the algorithmic computation of the action of F on $\mathrm{H}_1(\Gamma)$, but algorithms for these computations in the case when the curve X is hyperelliptic will be discussed in forthcoming joint work of the first, second and fifth authors with David Corwin, Sachi Hashimoto, Benjamin Matschke, Oana Padurariu, Ciaran Schembri, and Tian Wang.

As we explain in Section 5.4, one can sometimes use partial information deduced from Theorem 3.2 to determine the possible local heights without computing the action of F on $\mathrm{H}_1(\Gamma)$ (for example, if one has enough rational points on X that are suitably independent in $J(\mathbf{Q})$ and $\Gamma_{\mathbf{Q}}$).

Example 3.3. One example for which this strategy succeeds is the curve $C_{188}/\mathbf{Q}$ defined by the equation $y^2 = x^5 - x^4 + x^3 + x^2 - 2x + 1$, as described in Example 5.18. This curve does not have semistable reduction over $\mathbf{Q}_2$. Over $K = \mathbf{Q}_2[\sqrt[3]{2}]$, we find a regular semistable model $\mathcal{X}_{\mathrm{reg}}$ whose special fibre consists of two genus 1 curves that do not intersect and a genus 0 curve intersecting both of them transversely in a unique point each. We did not manage to obtain this information using any of the existing software packages for computing regular or semistable models, such as `Magma`'s `RegularModel` or the `SageMath` package `MCLF` [2]) Therefore we computed this model by hand, using a standard (but tedious) sequence of blow-ups.

Hence the metric graph Γ_{reg} is a line segment and the image of $C_{188}(\mathbf{Q}_2)$ in $\Gamma_{\mathbf{Q}}$ consists of three points on this line. The two edges of Γ_{reg} both have length $1/3$. In this case, since Γ has trivial homology, the function j_Γ is affine linear, so it is uniquely determined by evaluating it at two distinct points. We use this to compute the rational points on C_{188} in Example 5.18.

3.2 Local heights at p

We discuss the local height component

$$h_p\colon X(\mathbf{Q}_p) \longrightarrow \mathbf{Q}_p\,,$$

which appeared in [BDM$^+$19, §5]. Recall that h_p is a locally analytic function, described in terms of the filtered ϕ-module $M(x)$ discussed in §2.2. Concretely, we may find two unipotent isomorphisms

$$\lambda^\star(x)\colon\ \mathbf{Q}_p \oplus V_{\mathrm{dR}} \oplus \mathbf{Q}_p(1) \xrightarrow{\sim} M(x), \qquad \text{for } \star \in \{\phi, \mathrm{Fil}\}$$

where λ^ϕ respects the Frobenius action and λ^{Fil} respects the Hodge filtration, which with respect to a suitable basis for $M(x)$ may be represented in $(1+2g+1)$-block matrix form as

$$\lambda^\phi(x) = \begin{pmatrix} 1 & 0 & 0 \\ \boldsymbol{\alpha}_\phi & 1 & 0 \\ \gamma_\phi & \boldsymbol{\beta}_\phi^{\mathsf{T}} & 1 \end{pmatrix}, \qquad \lambda^{\mathrm{Fil}}(x) = \begin{pmatrix} 1 & 0 & 0 \\ \boldsymbol{\alpha}_{\mathrm{Fil}} & 1 & 0 \\ \gamma_{\mathrm{Fil}} & \boldsymbol{\beta}_{\mathrm{Fil}}^{\mathsf{T}} & 1 \end{pmatrix} \tag{3.1}$$

(see [BDM$^+$19, §5.3] and [BDM$^+$19, §4.5] respectively). The isomorphism λ^ϕ is uniquely determined, whereas λ^{Fil} is only well-defined up to the stabiliser of the Hodge filtration Fil^0. A suitable choice gives $\boldsymbol{\alpha}_{\mathrm{Fil}} = 0$.

The splitting s of the Hodge filtration (see Remark 3.1) defines idempotents s_1, s_2 on V_{dR} with images $s(V_{\mathrm{dR}}/\mathrm{Fil}^0 V_{\mathrm{dR}})$ and $\mathrm{Fil}^0 V_{\mathrm{dR}}$ respectively, with respect to which the local height at p is

$$h_p(x) = \gamma_\phi - \gamma_{\mathrm{Fil}} - \boldsymbol{\beta}_\phi^{\mathsf{T}} \cdot s_1(\boldsymbol{\alpha}_\phi) - \boldsymbol{\beta}_{\mathrm{Fil}}^{\mathsf{T}} \cdot s_2(\boldsymbol{\alpha}_\phi) \tag{3.2}$$

by [BDM$^+$19, Equation (17)].

[2] MCLF can be used to show that there is a semistable model with three components, two of genus 1 and one of genus 0. It also lists equations for their function fields, but this information does not suffice for our purposes.

In [BDM+19] we outline a method to compute these quantities explicitly as functions of the local point x in $X(\mathbf{Q}_p)$, which exploits the existence of the connection $(\mathscr{M}, \nabla)$ discussed in §2.2. The Hodge filtration and Frobenius structures of this bundle are characterised by suitable universal properties, discussed at length in [BDM+19, §§4–5]. We have made the algorithms for the computation of h_p more general and streamlined and have added a precision analysis in Section 4 but did not make further contributions to this part of the method beyond what is already contained in *loc. cit.*

3.3 The global height pairing

One key step in the construction of a quadratic Chabauty function is to write the global height pairing h in terms of a basis of the space of bilinear pairings on $\mathrm{H}^0(X_{\mathbf{Q}_p}, \Omega^1)^\vee$. In [BDM+19], we had as a working hypothesis that our curve X had sufficiently many rational points, in the following sense: For $x \in X(\mathbf{Q}_p)$, the Galois representation $\mathrm{A}(x)$ can be projected onto $\mathrm{H}^1_f(G_T, V)$ (respectively $\mathrm{H}^1_f(G_T, V^*(1))$), where G_T is the maximal quotient of $G_{\mathbf{Q}}$ unramified outside $T = \{p\} \cup \{\text{bad primes for } X\}$. With respect to the dual basis $\omega_0^*, \dots, \omega_{g-1}^*$, the image is the vector α (respectively β) in (2.2). Both of these cohomology groups are isomorphic, under our running assumptions, to $\mathrm{H}^0(X_{\mathbf{Q}_p}, \Omega^1)^\vee$, so we obtain

$$\pi(\mathrm{A}(x)) = (\pi_1(\mathrm{A}(x)), \pi_2(\mathrm{A}(x))) \in \mathrm{H}^0(X_{\mathbf{Q}_p}, \Omega^1)^\vee \times \mathrm{H}^0(X_{\mathbf{Q}_p}, \Omega^1)^\vee .$$

Suppose that we can find a basis of $\mathrm{H}^0(X_{\mathbf{Q}_p}, \Omega^1)^\vee \otimes \mathrm{H}^0(X_{\mathbf{Q}_p}, \Omega^1)^\vee$ consisting of elements of the form $\pi(\mathrm{A}_Z(b, x))$, where the Z are cycles on J pulling back to degree 0 cycles on X, and the x are rational points on X. Then we can compute the coefficients of h in terms of the dual basis by evaluating $h_p(\mathrm{A}_Z(b, x))$ (and, if necessary, $h_\ell(\mathrm{A}_Z(b, x))$ for primes $\ell \neq p$). With this choice of basis, the extension of h to a locally analytic function $h\colon X(\mathbf{Q}_p) \to \mathbf{Q}_p$ is immediate.

The number of required rational points can be reduced by working with symmetric heights that are $\mathrm{End}(J)$-equivariant. By the latter we mean that $h(f(x), y) = h(x, f(y))$ for all $f \in \mathrm{End}(J)$, using (2.1). This holds if the splitting s of the Hodge filtration on V_{dR} commutes with $\mathrm{End}(J)$ and has the property that $\ker(s)$ is isotropic with respect to the cup product (see [Nek93, §4.11] and [BD21, §4.1]). For instance, if p is a prime of ordinary reduction for the Jacobian, then the height associated to the unit root splitting (see Remark 3.15) is symmetric and $\mathrm{End}(J)$-equivariant. Henceforth we shall assume that s satisfies these assumptions, and we say that X has *sufficiently many rational points* if the approach outlined above succeeds.

3.3.1 *Heights on the Jacobian* If our curve does not have sufficiently many rational points in the above sense, then, in light of (2.1), it is natural to solve for the height pairing using rational points on the Jacobian. In this case, we do not have an algorithm at our disposal to compute h using Nekovář's construction, but we can use the equivalence between this construction and that of Coleman and Gross [CG89], proved by Besser [Bes04]. In the case when the curve is hyperelliptic and given by an odd degree model over $\mathbf{Q}_p$ (but see Remark 3.7), we can further use the algorithm of Balakrishnan–Besser [BB12, BB21]. In the discussion that follows, we will assume that we are in this situation. We will also assume that we know g independent points on the Jacobian.

Recall from Remark 3.1 that we have fixed a a continuous idèle class character $\chi\colon \mathbf{A}_{\mathbf{Q}}^\times/\mathbf{Q}^\times \longrightarrow \mathbf{Q}_p$ ramified at p and a splitting $s\colon V_{\mathrm{dR}}/\mathrm{Fil}^0 V_{\mathrm{dR}} \longrightarrow V_{\mathrm{dR}}$ of the Hodge filtration on $V_{\mathrm{dR}} = \mathrm{H}^1_{\mathrm{dR}}(X_{\mathbf{Q}_p})^\vee$. The latter corresponds to a subspace $W \subset H^1_{\mathrm{dR}}(X_{\mathbf{Q}_p})$, complementary to the image of $\mathrm{H}^0(X_{\mathbf{Q}_p}, \Omega^1)$. With respect to these choices, Coleman and Gross define the *local p-adic height pairing* $h_v(D_1, D_2) \in \mathbf{Q}_p$ at a finite prime v for divisors $D_1, D_2 \in \mathrm{Div}^0(X_{\mathbf{Q}_v})$ with disjoint support. The local pairing is bi-additive, and we have $h_v(D_1, D_2) = \chi_v(f(D_2))$ if $D_2 = \mathrm{div}(f)$ is principal. For $v \neq p$, the pairing h_v is also symmetric; h_p is symmetric if and only if W is isotropic with respect to the cup product pairing, which we will assume from now on. Moreover, for $D_1, D_2 \in \mathrm{Div}^0(X)$ with disjoint support, only finitely many $h_v(D_1, D_2) := h_v(D_1 \otimes \mathbf{Q}_v, D_2 \otimes \mathbf{Q}_v)$ are nonzero. Therefore $h := \sum_v h_v$ defines a symmetric bilinear pairing $h\colon J(\mathbf{Q}) \times J(\mathbf{Q}) \to \mathbf{Q}_p$ (see [CG89, §6]).

If we have algorithms to compute the local height pairings, we can solve for the global height pairing in terms of the

basis of symmetric bilinear pairings on $J(\mathbf{Q}) \otimes \mathbf{Q}_p$ defined by

$$g_{ij}(D,E) := \frac{1}{2}(\log(D)(\omega_i)\log(E)(\omega_j) + \log(D)(\omega_j)\log(E)(\omega_i))\,,\ \ 0 \leqslant i \leqslant j \leqslant g-1\,. \tag{3.3}$$

Since we can express $\pi_1(\mathrm{A}(x))$ and $\pi_2(\mathrm{A}(x))$ in terms of the dual basis $\{\omega_i^*\}$, we can compute $g_{ij}(\pi(\mathrm{A}(x)))$ for $x \in X(\mathbf{Q}_p)$ (with the obvious abuse of notation) and extend h to a locally analytic function $h\colon X(\mathbf{Q}_p) \to \mathbf{Q}_p$.

It remains to discuss the computation of the local heights. For $D_1, D_2 \in \mathrm{Div}^0(X_{\mathbf{Q}_p})$ with disjoint support, the local height is the Coleman integral certain differential with residue divisor $\mathrm{Res}(\omega_{D_1}) = D_1$ and c_p is a constant so that $c_p^{-1}\chi_p$ extends to a branch $\mathbf{Q}_p^\times \to \mathbf{Q}_p$ of the p-adic logarithm; the Coleman integral is taken with respect to this branch. The differential ω_{D_1} is normalised with respect to the splitting s using

a homomorphism

$$\Psi\colon T(\mathbf{Q}_p)/T_l(\mathbf{Q}_p) \to \mathrm{H}^1_{\mathrm{dR}}(X),$$

from $T(\mathbf{Q}_p)$ the group of differentials of the third kind with integer residues on X quotiented by $T_l(\mathbf{Q}_p)$ the group of logarithmic differentials $\frac{df}{f}$ with $f \in \mathbf{Q}_p(X)^*$, as in the algorithm below. We restrict to degree zero divisors of the form $P - Q$ where P, Q are non-Weierstrass points in $X(\mathbf{Q}_p)$ that do not reduce to a Weierstrass point in $X(\mathbf{F}_p)$ since we will need to compute Coleman integrals between P, Q, and our implementation assumes that these points are in non-Weierstrass disks and defined over $\mathbf{Q}_p$.

Algorithm 3.4 The local height $h_p(D_1, D_2)$ at p of the global p-adic height [BB12].
Input:

- Hyperelliptic curve $X/\mathbf{Q}_p$, given by an affine model $y^2 = f(x)$, where $f \in \mathbf{Z}_p[x]$ is squarefree of degree $2g+1 > 2$
- Prime $p > 2g-1$ of good reduction
- Choice of isotropic subspace W of $H^1_{\mathrm{dR}}(X_{\mathbf{Q}_p})$, complementary to the subspace of regular 1-forms $\mathrm{H}^0(X_{\mathbf{Q}_p}, \Omega^1)$
- Divisors $D_1 = P - Q, D_2 = R - S$, where P, Q, R, S are non-Weierstrass points in $X(\mathbf{Q}_p)$ that do not reduce to a Weierstrass point in $X(\mathbf{F}_p)$, and R, S do not lie in the residue disks of P, Q.

Output: The local height $h_p(D_1, D_2)$ at p of the Coleman–Gross global p-adic height.

(i) Choose ω a differential in $T(\mathbf{Q}_p)$ with $\mathrm{Res}(\omega) = D_1$.

(ii) Solve for the coefficients b_i of $\Psi(\omega) = \sum_{i=0}^{2g-1} b_i\omega_i \in \mathrm{H}^1_{\mathrm{dR}}(X)$ by computing residues, as in [BB12, §5.2]. Then $\Psi(\omega) - \sum_{i=0}^{g-1} b_i\omega_i \in W$. Let

$$\omega_{D_1} := \omega - \sum_{i=0}^{g-1} b_i\omega_i.$$

(iii) Set $\alpha := \phi^*(\omega) - p(\omega)$. Use Frobenius equivariance of the map Ψ (and the matrix of Frobenius computed with respect to the basis $\{\omega_i\}$ of $\mathrm{H}^1_{\mathrm{dR}}(X)$) to compute

$$\Psi(\alpha) = \phi^*\Psi(\omega) - p\Psi(\omega)\,.$$

(iv) Let β be a 1-form with $\mathrm{Res}(\beta) = (R) - (S)$. Compute $\Psi(\beta)$.

(v) Compute

$$h_p(D_1, D_2) := \int_{D_2} \omega_{D_1} = \int_S^R \left(\omega - \sum_{i=0}^{g-1} b_i\omega_i\right),$$

where

$$\int_S^R \omega = \frac{1}{1-p}\left(\Psi(\alpha) \cup \Psi(\beta) + \sum_{A \in X(\mathbf{C}_p)} \mathrm{Res}_A\left(\alpha \int \beta\right) - \int_{\phi(S)}^S \omega - \int_R^{\phi(R)} \omega\right),$$

see [BB12, Remark 4.9].

Remark 3.5. Note that in the last step above, $\int_{\phi(S)}^{S} \omega$ and $\int_{R}^{\phi(R)} \omega$ are tiny integrals, that is, Coleman integrals between points in the same residue disk. Such integrals may be computed merely using a uniformising parameter at any point in the residue disk. The computation $\sum_{A \in X(\mathbf{C}_p)} \mathrm{Res}_A\left(\alpha \int \beta\right)$ will, in most cases, require working over various extension of $\mathbf{Q}_p$ to pick up all contributions at all poles (see [BB12, Remark 4.10]).

Remark 3.6. If our hyperelliptic curve X does not admit an odd degree model over $\mathbf{Q}$, we may choose our prime p such that X has an odd degree model over $\mathbf{Q}_p$ and compute local heights at p on this model. This follows from the fact that $\Psi(\varphi^*\omega) = \varphi^*(\Psi(\omega))$ for φ an isomorphism of curves and ω a differential of the third kind.

Remark 3.7. In his thesis [Gaj22], Gajović has improved Algorithm 3.4 and extended it to even degree models of hyperelliptic curves.

The local height at a prime $\ell \neq p$ is defined in terms of intersection theory. We can extend D_1 and D_2 to divisors $\mathcal{D}_1$ and $\mathcal{D}_2$ on a regular model of $X_{\mathbf{Q}_\ell}$ so that both $\mathcal{D}_i$ have trivial intersection multiplicity with all vertical divisors; then by [CG89, Proposition 1.2], we have

$$h_\ell(D_1, D_2) = -(\mathcal{D}_1 \cdot \mathcal{D}_2)\chi_p(\ell)\,.$$

3.4 Mordell–Weil sieving

The idea of the Mordell–Weil sieve, originally due to Scharaschkin [Sch99], is to deduce information on rational points on X via the intersection of the images of $X(\mathbf{F}_v)$ and $J(\mathbf{Q})$ in $J(\mathbf{F}_v)$ (or suitable quotients) for several primes v of good reduction. It is often applied to verify that $X(\mathbf{Q}) = \varnothing$, but it can also be combined with p-adic techniques to compute $X(\mathbf{Q})$ when there are rational points.

We review the basic idea, which is straightforward. Making the sieve perform well in practice is a different matter; see [BS10] for an elaborate discussion of the issues one encounters and detailed strategies. For ease of exposition, we assume that $J(\mathbf{Q})$ is torsion-free and that we have generators $P_1, \dots, P_r$ of $J(\mathbf{Q})$. Let $M > 1$ be an integer and let S be a finite set of primes of good reduction for X. Then the diagram

$$\begin{array}{ccc} X(\mathbf{Q}) & \longrightarrow & J(\mathbf{Q})/MJ(\mathbf{Q}) \\ \downarrow & & \downarrow{\scriptstyle \alpha_{S,M}} \\ \prod_{v\in S} X(\mathbf{F}_v) & \xrightarrow[\beta_{S,M}]{} & \prod_{v\in S} J(\mathbf{F}_v)/MJ(\mathbf{F}_v) \end{array}$$

is commutative. In the situation of interest to us, the horizontal maps are induced by our choice of base point $b \in X(\mathbf{Q})$.

In our work, we use the Mordell–Weil sieve in two ways. On the one hand, we apply it to show that for a fixed prime p, a given residue disk in $X(\mathbf{Q}_p)$ does not contain a rational point. To this end, we set $M = M' \cdot p$ for some suitable auxiliary integer M', and we choose S to consist of primes ℓ so that $\gcd(\#J(\mathbf{F}_\ell), \#J(\mathbf{F}_q))$ is large for some prime divisors $q \mid pM'$. We can then hope that the image of the reduction of the disk under $\prod \beta_{S,M}$ does not meet the image of the map $\prod \alpha_{S,M}$.

On the other hand, we use the sieve to show for fixed $M > 1$ that a given coset of $MJ(\mathbf{Q})$ does not contain the image of a point in $X(\mathbf{Q})$ under the Abel–Jacobi map $P \mapsto [P - b]$. Suppose a point $P \in X(\mathbf{Q}_p)$ is given to finite precision p^N. If P is rational, then there are integers $a_1, \dots, a_g$ such that

$$[P - b] = a_1 P_1 + \cdots + a_g P_g.$$

Via the abelian logarithm, we compute a tuple $(\tilde{a}_1, \dots, \tilde{a}_g) \in \mathbf{Z}/p^N\mathbf{Z}$ satisfying $a_i \equiv \tilde{a}_i \pmod{p^N}$ for all $i \in \{1, \dots, g\}$. To show that P is not rational, it suffices to show that the corresponding coset of $p^N J(\mathbf{Q})$ does not contain the image of such a point.

In our implementation, we have not tried to optimise the interplay between quadratic Chabauty and the Mordell–Weil sieve. Such an optimisation is discussed in [BBM17, §7]. Let us only note here that we may combine quadratic

Chabauty information coming from several primes, and that we can enhance that information using an auxiliary integer M' similar to the above. Another account of combining quadratic Chabauty with the Mordell–Weil sieve can be found in [BBB+21, §6.7].

Remark 3.8. All examples in this paper

satisfy $r = g = \mathrm{rk}_{\mathbf{Z}}\mathrm{NS}(J)$, resulting in at least two independent locally analytic functions vanishing in $X(\mathbf{Q})$ for the $g > 2$ examples. Since we expect that their common zero set is precisely $X(\mathbf{Q})$ (or that there is a geometric reason for the appearance of any additional p-adic solutions), we do not expect to require the sieve. Indeed, we only had to apply the sieve for curves of genus 2. For these examples, we always required only one prime for the quadratic Chabauty computation; we chose this prime in such a way as to simplify the sieving.

3.5 Implementation and scope

We have implemented the algorithms described in this section in the computer algebra system `Magma` [BCP97]. Our code is freely available at [BDM+]. It extends the code used for $X_{\mathrm{s}}^+(13)$ in [BDM+19] and can be used to recover that example. It is applied to new examples, as discussed in §5.

We begin by summarising our discussion so far and describe the general procedure to determine the finite set $X(\mathbf{Q}_p)_2$ as it would apply to the modular curve X attached to a general congruence subgroup, and Atkin–Lehner quotients thereof. In this generality, several steps cannot be easily automated, so we discuss the extent to which our implementation has automated the procedure, and point out which steps require additional action from the user. See Example 5.3 for a fairly detailed worked example.

Our techniques are built on prior work of Tuitman on computing the action of Frobenius on rigid cohomology [Tui17]. We recall some of the underlying structures present in Tuitman's work and a set of assumptions on these auxiliary structures.

Suppose our modular curve $X/\mathbf{Q}$ is given by a (possibly singular) plane model $Q = 0$ with $Q(x, y) \in \mathbf{Z}[x, y]$ a polynomial that is irreducible and monic in y. Let d_x and d_y denote the degrees of the morphisms x and y, respectively, from X to the projective line. Let $\Delta(x) \in \mathbf{Z}[x]$ denote the discriminant of Q with respect to the variable y. Moreover, define $r(x) \in \mathbf{Z}[x]$ to be the squarefree polynomial with the same zeroes as $\Delta(x)$, in other words, $r = \Delta/(\gcd(\Delta, \frac{d\Delta}{dx}))$.

Definition 3.9. *Let $W^0 \in \mathrm{GL}_{d_x}(\mathbf{Q}[x, 1/r])$ and $W^\infty \in \mathrm{GL}_{d_x}(\mathbf{Q}[x, 1/x, 1/r])$ denote matrices such that, if we denote*

$$b_j^0 = \sum_{i=0}^{d_x-1} W^0_{i+1,j+1} y^i \quad \text{and} \quad b_j^\infty = \sum_{i=0}^{d_x-1} W^\infty_{i+1,j+1} y^i$$

for all $0 \leqslant j \leqslant d_x - 1$, then

(i) $[b_0^0, \ldots, b_{d_x-1}^0]$ is an integral basis for $\mathbf{Q}(X)$ over $\mathbf{Q}[x]$,

(ii) $[b_0^\infty, \ldots, b_{d_x-1}^\infty]$ is an integral basis for $\mathbf{Q}(X)$ over $\mathbf{Q}[1/x]$,

where $\mathbf{Q}(X)$ denotes the function field of X. Moreover, let $W \in \mathrm{GL}_{d_x}(\mathbf{Q}[x, 1/x])$ denote the change of basis matrix $W = (W^0)^{-1}W^\infty$.

Assumption 3.10 [Tui17, Assumption 1].

(i) The discriminant of $r(x)$ is contained in $\mathbf{Z}_p^\times$.

(ii) If we denote $b_j^0 = \sum_{i=0}^{d_x-1} W^0_{i+1,j+1} y^i$ and $b_j^\infty = \sum_{i=0}^{d_x-1} W^\infty_{i+1,j+1} y^i$ for all $0 \leqslant j \leqslant d_x - 1$, and if we let $\mathbf{F}_p(x, y)$ be the field of fractions of $\mathbf{F}_p[x, y]/(Q)$, then:
   (a) The reduction modulo p of $[b_0^0, \ldots, b_{d_x-1}^0]$ is an integral basis for $\mathbf{F}_p(x, y)$ over $\mathbf{F}_p[x]$.
   (b) The reduction modulo p of $[b_0^\infty, \ldots, b_{d_x-1}^\infty]$ is an integral basis for $\mathbf{F}_p(x, y)$ over $\mathbf{F}_p[1/x]$.

(iii) $W^0 \in \mathrm{GL}_{d_x}(\mathbf{Z}_p[x, 1/r])$ and $W^\infty \in \mathrm{GL}_{d_x}(\mathbf{Z}_p[x, 1/x, 1/r])$.

(iv) Denote:

$$\mathcal{R}^0 = \mathbf{Z}_p[x]b_0^0 \quad + \ldots + \mathbf{Z}_p[x]b_{d_x-1}^0,$$
$$\mathcal{R}^\infty = \mathbf{Z}_p[1/x]b_0^\infty + \ldots + \mathbf{Z}_p[1/x]b_{d_x-1}^\infty.$$

For a ring R, let R_{red} denote the reduced ring obtained by quotienting out by the nilradical. Then the discriminants of the finite $\mathbf{Z}_p$-algebras $(\mathcal{R}^0/(r(x)))_{\mathrm{red}}$ and $(\mathcal{R}^\infty/(1/x))_{\mathrm{red}}$ are contained in $\mathbf{Z}_p^\times$.

Remark 3.11. These conditions imply that the curve X has good reduction at p.

Algorithm 3.12 Quadratic Chabauty for modular curves.
Input:

- A modular curve $X/\mathbf{Q}$ with Mordell–Weil rank $r = g$ and $\mathrm{rk}_{\mathbf{Z}}\mathrm{NS}(J) > 1$, and for which the image of $J(\mathbf{Q})$ in $\mathrm{H}^0(X_{\mathbf{Q}_p}, \Omega^1)^\vee$ has rank g.
- A covering of X by affine opens that are birational to a planar curve cut out by an equation that is monic in one variable, has p-integral coefficients and satisfies Assumption 3.10. (See §3.5.1.)
- A prime p of good reduction such that the Hecke operator T_p generates $\mathrm{End}^0(J)$.
- For all primes ℓ that are not of potentially good reduction, the local height functions $X(\mathbf{Q}_\ell) \to \mathrm{Ker}(\mathrm{NS}(J) \to \mathrm{NS}(X))^*_{\mathbf{Q}_p}$, computed using Theorem 3.2. (See §3.5.3.)
- A starting precision n.
- A height bound B.

Output: An approximation to a finite set containing the set of points $X(\mathbf{Q}_p)_2$, computed to precision $n' \leqslant n$ or FAIL.

(i) Compute the set $X(\mathbf{Q})_{\mathrm{known}}$ of points in $X(\mathbf{Q})$ with height bounded by B.

(ii) Compute an integral symplectic basis for $\mathrm{H}^1_{\mathrm{dR}}(X_{\mathbf{Q}})$ or return FAIL.

(iii) Compute the action of Frobenius on $\mathrm{H}^1_{\mathrm{dR}}(X_{\mathbf{Q}_p})$ using Tuitman's algorithm [Tui16, Tui17]. Use the Eichler–Shimura relation to compute the matrix of the action of the Hecke operator T_p on $\mathrm{H}^1_{\mathrm{dR}}(X_{\mathbf{Q}_p})$.

(iv) Compute a splitting of the Hodge filtration that is equivariant for the action of $\mathrm{End}(J)$ in the sense of §3.3.

(v) Compute the matrices of a basis $Z_1, \ldots, Z_{\mathrm{rkNS}(J)-1}$ of $\mathrm{Ker}\,(\mathrm{NS}(J) \to \mathrm{NS}(X))$ acting on $\mathrm{H}^1_{\mathrm{dR}}(X_{\mathbf{Q}_p})$, see §3.5.2.

(vi) Let $A := \varnothing$. For each Z_i, compute the associated heights:

  (a) For each affine patch, do the following:
    (i) Compute the functions λ^{Fil} from (3.1) using [BDM+19, §4].
    (ii) Compute the functions λ^{ϕ} from (3.1) using [BDM+19, §5].
  (b) Solve for the height pairing, either using a large enough supply of known rational points $P_1, \ldots, P_n$ on X, if possible, or by computing the Coleman–Gross height pairing on r independent points in $J(\mathbf{Q})$. (See §3.5.4.) If this is unsuccessful, return FAIL.
  (c) Compute solutions of the function(s) coming from Z_i or return FAIL if there has been too much precision loss to determine these solutions.
  (d) Check that the solutions are simple. If there is a non-simple solution corresponding to a point in $X(\mathbf{Q})_{\mathrm{known}}$, return FAIL. Else, add to the set A the solutions that (simultaneously) satisfy the(se) function(s).

(vii) Return A.

Remark 3.13. We assume that we know a priori that the Mordell-Weil rank of the Jacobian is equal to the genus of the curve. For modular curves, by Gross–Zagier–Kolyvagin–Logachev this amounts to checking that the associated eigenforms have analytic rank one (see e.g. [DF21, §7]). For hyperelliptic curves, it is sometimes simpler to carry out a two-descent.

Remark 3.14. Note that if the algorithm fails due to a loss of precision, it may be possible to remedy this by increasing the starting precision. One place where increasing precision may not work is if the p-adic logarithm does not induce an isomorphism $J(\mathbf{Q}) \otimes \mathbf{Q}_p \simeq \mathrm{H}^0(X_{\mathbf{Q}_p}, \Omega^1)^\vee$, even though the rank of $J(\mathbf{Q})$ is g. For the Atkin-Lehner quotients $X_0^+(N)$, the weak Birch–Swinnerton-Dyer conjecture implies $J(\mathbf{Q})$ always generates $\mathrm{H}^0(X_{\mathbf{Q}_p}, \Omega^1)^\vee$ (see [DF21, Lemma 7]). In general, if $r = g$ and the Zariski closure of $J(\mathbf{Q})$ is J, then a conjecture of Waldschmidt [Wal11, Conjecture 1] (an analogue of the Leopoldt conjecture for abelian varieties) implies that the p-adic logarithm is always an isomorphism. In theory, if one *knew* that J gave a counterexample to Waldschmidt's conjecture, and $r = g$, then one could simply apply the Chabauty–Coleman method. However, a priori it could happen that J gave a counterexample but there was no way of verifying this by a computation to finite p-adic precision. Another place where increasing precision will not help is if there are multiple roots in Step (vi(c)). However, we only expect this to happen for geometric reasons.

One can have $r > g$ for the curves $X_0^+(N)$ with N prime, even though $X_0^+(N)(\mathbf{Q}_p)_2$ is always finite when the genus is greater than one [DF21]. However the smallest genus for which this happens is $g = 206$ (with $N = 5077$), so the $r = g$ hypothesis is not the main restriction to the scope of our algorithms for this family of curves.

Remark 3.15. In the case when p is a prime of ordinary reduction for the Jacobian, one may take the splitting of the Hodge filtration given by the *unit root subspace*, that is, the unit root eigenspace of Frobenius ϕ acting on $\mathrm{H}^1(X_{\mathbf{Q}_p})$. Given a basis $\{\eta_1, \dots, \eta_{2g}\}$ of $\mathrm{H}^1(X_{\mathbf{Q}_p})$, where $\eta_1, \dots, \eta_g$ are holomorphic, a basis for the unit root eigenspace mod p^n is given by $\{(\phi^*)^n \eta_{g+1}, \dots, (\phi^*)^n \eta_{2g}\}$.

Remark 3.16. In this paper, we do not discuss algorithms for computing the input of the local height functions as maps from $\mathbf{Q}_\ell$-points to $\mathbf{Q}_p$-linear functionals on $\mathrm{Ker}(\mathrm{NS}(J) \to \mathrm{NS}(X))$. In Section 5 we give examples where this function can be nontrivial, and where $X(\mathbf{Q})$ can still be determined using quadratic Chabauty. There are two procedures we illustrate for doing this. In Section 5.4, we calculate regular semistable models at bad primes and have a sufficient supply of rational points (and sufficiently simple dual graphs) to reconstruct the functions j_ℓ from Theorem 3.2 using evaluation of p-adic local heights at known rational points. In Section 5.5, although we know a regular semistable model "abstractly," we do not know the relation between the stable model (at the bad prime 17) and the model we use for p-adic calculations. This, together with the relative paucity of known rational points, makes it infeasible to apply the first procedure. Instead, we use extra information about the action of inertia on the stable model, together with Theorem 3.2 to identify a subspace of line bundles in $\mathrm{Ker}(\mathrm{NS}(J) \to \mathrm{NS}(X))$ for which the associated local heights vanish.

To further determine the subset of rational points $X(\mathbf{Q})$ from the finite set of points produced by our algorithm, we carry out the Mordell–Weil sieve. In practice it may happen (see below) that $X(\mathbf{Q})$ is returned by the algorithm, but this is typically not the case when X has genus two.

3.5.1 *Affine patches* Most of the examples discussed in Section 5 are either hyperelliptic curves or smooth plane quartics. As demonstrated in Section 5.5, our code is sometimes able to treat more general examples. Our implementation was designed to take as input a plane affine patch $Y\colon Q(x, y) = 0$ of a modular curve $X/\mathbf{Q}$ satisfying the requirements in §2.1 and a prime p of good reduction. It returns all rational points on X in affine residue disks where the lift of Frobenius constructed in [Tui16, Tui17] is defined. Note that we do not require Y to be smooth, but we need Q to be monic with p-integral coefficients.

We can sometimes find an affine patch Y having the convenient property that all rational points on X must be among the points returned by running our algorithm on Y. If no such Y is found, then we need to find two suitable affine patches such that every rational point on X is contained in at least one patch. For smooth plane quartics, our implementation includes an algorithm that automates this process for convenience of the user. For other curves, this step is left to the user.

3.5.2 *The Néron–Severi classes Z_i* Under the assumption that T_p generates the endomorphism ring of the Jacobian, which we made for convenience above, one may proceed precisely as in [BDM$^+$19, §6.4] to determine a nontrivial

class

$$Z \in \mathrm{Ker}\left(\mathrm{NS}(J) \longrightarrow \mathrm{NS}(X)\right).$$

Indeed, the matrix A_p of the Hecke operator T_p acting on $\mathrm{H}^1_{\mathrm{dR}}(X_{\mathbf{Q}_p})$ is easily determined from the matrix of Frobenius F_p (which is already a byproduct of the algorithms for the local height at p), by the Eichler–Shimura relation:

$$T_p = F_p + pF_p^{-1}.$$

Under our assumption, the matrices of the classes Z_i acting on $\mathrm{H}^1_{\mathrm{dR}}(X_{\mathbf{Q}_p})$ may then be computed as linear combinations of powers of A_p.

Remark 3.17. This is the only part of our algorithm specific to modular curves, since it relies on the Eichler–Shimura relation. It should however be noted that this is mainly a matter of convenience adopted for the purpose of automation. More generally, for a smooth projective curve $X/\mathbf{Q}$ satisfying the assumptions of §2.1, one could find p-adic approximations of the action of the nontrivial classes Z_i on $\mathrm{H}^1_{\mathrm{dR}}(X_{\mathbf{Q}_p})$ using just p-adic linear algebra. Indeed, the space of correspondences which are symmetric under the Rosati involution and induce endomorphisms of trace zero on the Tate module maps under the cycle class into the intersection of the Fil^1 and $\phi = p$ subspaces of

$$\ker\left(\wedge^2\mathrm{H}^1_{\mathrm{dR}}(X_{\mathbf{Q}_p}) \xrightarrow{\cup} \mathrm{H}^2_{\mathrm{dR}}(X_{\mathbf{Q}_p})\right). \tag{3.4}$$

In fact, by the Tate conjecture, the rank of the space of (crystalline) cohomology classes of such correspondences over $\mathbf{F}_p$ is equal to the dimension of the $\phi = p$ subspace of (3.4), and by the p-adic Lefschetz-(1,1) theorem of Berthelot and Ogus [BO83, §3.8] such a correspondence over $\mathbf{F}_p$ lifts to $\mathbf{Q}_p$ if and only if its cycle class lies in Fil^1. Note that the dimension of the space of correspondences symmetric under the Rosati involution need not equal the dimension of $\wedge^2\mathrm{H}^1_{\mathrm{dR}}(X_{\mathbf{Q}_p})^{\phi=p} \cap \mathrm{Fil}^1$, as was erroneously claimed in [BDM+19, Lemma 4.5], since the rank of the intersection of a $\mathbf{Z}$-lattice with a $\mathbf{Q}_p$-subspace may be less than the dimension of the intersection with the $\mathbf{Q}_p$-subspace it spans. However, if one knows a set of generators of a finite index subgroup of $\mathrm{End}(J)$ in advance (e.g. using algorithms for rigorous computation of the endomorphism algebra of the Jacobian [CMSV19])) then one can use this to compute the classes of generators in cohomology.

Therefore the assumption that T_p generates the endomorphism algebra could be circumvented in this step with a little work, although it is used in the computation of the local heights away from p, see below. When the assumption is not satisfied, our implementation throws an error, urging the user to try a different choice of prime p.

3.5.3 *The local heights away from p* This step requires an explicit knowledge of a semi-stable model of the modular curve X, as well as a description of the action of Z_i on the concomitant cohomological structures in order to be able to apply Theorem 3.2. It is clear that a full automation of this step, starting from a set of defining equations for X, falls outside the scope of our implementation.

Semi-stable models for modular curves are known in many cases, see for instance the recent work of Edixhoven–Parent [EP21]. In practice, one can also often use the `SageMath` toolbox `MCLF` [3] due to Rüth and Wewers to compute such models. The main advantage of having computed the Z_i in §3.5.2 as combinations of powers of T_p is that this makes it easier to compute the quantities appearing in Theorem 3.2. Even though we see no way to fully automate this step, we hope to convince the reader of its practicality by working it out for the genus 2 curves C_{188} and C_{161} in Examples 5.18 and 5.19.

3.5.4 *The global height pairing* If there are not sufficiently many rational points on the curve to solve for the height pairing, we instead compute the local heights h_v in the sense of Coleman and Gross, see §3.3.1. For hyperelliptic curves $X/\mathbf{Q}_p$ of odd degree, $h_p(D_1, D_2)$ can be computed using an algorithm due to Balakrishnan–Besser [BB12, BB21]. Based on earlier `SageMath` code due to Balakrishnan, we have implemented this in `Magma` for divisors D_1 and D_2 that split over $\mathbf{Q}_p$, have support contained in disjoint residue disks and for which no points in the support

[3] `https://github.com/MCLF/mclf`

reduce to Weierstrass points mod p. To compute the local heights h_ℓ for $\ell \neq p$, we rely on Magma's implementation of an algorithm for local canonical heights on hyperelliptic curves described by Holmes and Müller [Hol12, Mül14]. An algorithm for general curves was given by van Bommel, Holmes and Müller [vBHM20].

To solve for the height pairing, we need to find representatives for r independent points in $J(\mathbf{Q})$ that satisfy the assumptions mentioned above. Our implementation is currently restricted to genus 2 curves, since this step was only necessary for such curves, but a generalisation to higher genus hyperelliptic curves would be straightforward.

Remark 3.18. The code is currently restricted to the base field $K = \mathbf{Q}$. To extend it to more general number fields, one would need to combine these algorithms with those used in [BD18] for imaginary quadratic fields in certain cases, or for general number fields, with those in [BBBM21].

4. Precision analysis

In this section, we bound the loss of absolute p-adic precision that may occur in our computations by bounding the valuations of the error terms. We also estimate the valuations of the power series expansion of the quadratic Chabauty function ρ and use this to bound the precision of its roots.

We keep the notation used in the previous sections. Recall from (2.5) that $\rho = h - h_p$, where

- h is the global p-adic height defined in (2.4);
- h_p is the local component of h, discussed in §2.2.

By (3.2), the local height h_p satisfies

$$h_p(x) = \gamma_\phi - \gamma_{\mathrm{Fil}} - \boldsymbol{\beta}_\phi^{\mathsf{T}} \cdot s_1(\boldsymbol{\alpha}_\phi) - \boldsymbol{\beta}_{\mathrm{Fil}}^{\mathsf{T}} \cdot s_2(\boldsymbol{\alpha}_\phi)\,,$$

where the Hodge filtration of the filtered ϕ-module $M(x) := \left(\mathrm{A}_Z(b,x) \otimes_{\mathbf{Q}_p} \mathrm{B}_{\mathrm{cris}}\right)^{G_{\mathbf{Q}_p}}$ discussed in §2.2 is encoded by $\boldsymbol{\beta}_{\mathrm{Fil}}$ and γ_{Fil} and $\boldsymbol{\alpha}_\phi, \boldsymbol{\beta}_\phi$ and γ_ϕ encode the Frobenius structure of $M(x)$.

We will bound the loss of precision in the computation of the Hodge filtration in §4.1, and we do the same for the Frobenius structure in §4.2. In §4.3, we bound the precision loss for the global height computation. In the final part of this section, §4.4 we bound the valuation of the coefficients of the expansion of ρ in a residue disk, and we discuss how this may be used to provably determine the roots of ρ to a certain precision. This section relies heavily on [BDM$^+$19, Sections 4,5].

4.1 Hodge filtration

We first bound the loss of precision in Steps (ii)–(v) of Algorithm 3.12. For simplicity, we restrict to one class Z; the extension to $\mathrm{rkNS}(J)-1$ such classes is immediate. Let $Y/\mathbf{Q}$ be an affine open subset of X, birational to a curve given by an equation that satisfies Assumption 3.10. We may compute an integral, symplectic basis $\boldsymbol{\omega} = (\omega_0, \ldots, \omega_{2g-1})$ of de Rham cohomology over $\mathbf{Q}$ exactly, and extend this to an integral basis of $H^1_{\mathrm{dR}}(Y)$ via differentials $(\omega_{2g}, \ldots, \omega_{2g+d-2})$ of the third kind. Using such a basis, we may compute the action of the Frobenius operator F on $\mathrm{H}^1_{\mathrm{dR}}(X/\mathbf{Q}_p)$ to any desired p-adic precision using Tuitman's algorithm [Tui16, Tui17], from which we obtain the action of the Hecke operator $T_p = F + pF^{-1}$ on $\mathrm{H}^1_{\mathrm{dR}}(X/\mathbf{Q}_p)$ by Eichler–Shimura. The inversion of F results in a finite and computable loss of precision, which the code takes into account. This results in an algorithm that returns the action of the correspondence Z correctly modulo p^n for some $n \geqslant 1$ that is returned by the algorithm.

Using this, we may compute a matrix Λ with entries in $H^0(Y, \Omega_{Y_{\mathbf{Q}}})$, of the form

$$\Lambda := -\begin{pmatrix} 0 & 0 & 0 \\ \boldsymbol{\omega} & 0 & 0 \\ \eta & \boldsymbol{\omega}^{\mathsf{T}} Z & 0 \end{pmatrix}$$

such that $d+\Lambda$ extends to a flat connection on X. From this, we may compute γ_{Fil} and $\boldsymbol{\beta}_{\mathrm{Fil}}$ from (3.1). We recall from [BDM$^+$19, §4] that the defining properties of η, the $\boldsymbol{\beta}_{\mathrm{Fil}}$ and γ_{Fil} are as enumerated below. For $x \in (X-Y)(\overline{\mathbf{Q}})$, we let t_x denote a parameter, and $\boldsymbol{\Omega}_x$ denote the vector of formal integrals of the basis differentials ω_i:

$$d\boldsymbol{\Omega}_{x,i} = \omega_i \in \overline{\mathbf{Q}}[\![t_x]\!].$$

(i) The first g entries of $\boldsymbol{\beta}_{\mathrm{Fil}}$ are zero, and the last g are given by a vector $\mathbf{b}_{\mathrm{Fil}}$ of constants specified below.

(ii) η is a linear combination of $\omega_{2g}, \ldots, \omega_{2g+d-2}$, unique by [BDM$^+$19, Lemma 4.10] such that

$$d\boldsymbol{\Omega}_x^{\intercal} Z \boldsymbol{\Omega}_x - \eta \tag{4.1}$$

has vanishing residues at all $x \in (X-Y)(\overline{\mathbf{Q}})$.

(iii) $\mathbf{b}_{\mathrm{Fil}}$ and $\gamma_{\mathrm{Fil}} \in \mathcal{O}(Y)$ are the unique solutions to the equation $\gamma_{\mathrm{Fil}}(b) = 0$ and

$$g_x + \gamma_{\mathrm{Fil}} - \mathbf{b}_{\mathrm{Fil}}^{\intercal} N^{\intercal} \boldsymbol{\Omega}_x - \boldsymbol{\Omega}_x^{\intercal} Z N N^{\intercal} \boldsymbol{\Omega}_x \in L[\![t_x]\!] \tag{4.2}$$

for all $x \in (X-Y)(\overline{\mathbf{Q}})$, where $g_x \in \overline{\mathbf{Q}}[\![t_x]\!]$ is defined to be the formal integral of $d\boldsymbol{\Omega}_x^{\intercal} Z d\boldsymbol{\Omega}_x - \eta$ and N is the block $2g \times g$ matrix with top block zero and lower block a $g \times g$ identity matrix.

Given our basis $\boldsymbol{\omega}$, we may calculate $\boldsymbol{\Omega}_x$ to any given t_x-adic precision. Note that to solve (4.1), we only need to know $\boldsymbol{\Omega}_x$ modulo $t_x^{m_x}$, where m_x is the maximum of the order of the poles of the entries of $\boldsymbol{\Omega}_x$. Similarly, to solve for γ_{Fil} and $\mathbf{b}_{\mathrm{Fil}}$ in (4.2), we need only compute the principal parts of $\boldsymbol{\Omega}_x$ and $\boldsymbol{\Omega}_x^{\intercal} Z N N^{\intercal} \boldsymbol{\Omega}_x$. Hence given the above we may calculate η, γ_{Fil} and $\mathbf{b}_{\mathrm{Fil}}$ to precision $p^{n-2\nu}$, where ν is minus the minimum of the valuations of the t_x^i coefficients of the entries of $\boldsymbol{\Omega}_x$, for $i \leqslant m_x$.

4.2 Frobenius-equivariant splitting

We now bound the loss of precision in the computation of the Frobenius-equivariant splitting

$$\lambda^{\phi}(x) = \begin{pmatrix} 1 & 0 & 0 \\ \boldsymbol{\alpha}_{\phi}(b,x) & 1 & 0 \\ \gamma_{\phi}(b,x) & \boldsymbol{\beta}_{\phi}^{\intercal}(b,x) & 1 \end{pmatrix}$$

from (3.1) for $x \in X(\mathbf{Q}_p) \cap]\mathcal{U}[$ where $\mathcal{U}$ is an open of $Y_{\mathbf{F}_p}$ on which we have an overconvergent lift of Frobenius. This computation is the content of [BDM$^+$19, §5].

The first step is to find the Frobenius structure on the filtered ϕ-module $M(b)$. By [BDM$^+$19, §5.3.2], the inverse of the Frobenius structure is given by a matrix

$$G \in (\mathrm{H}^0(]Y[, j^{\dagger}\mathcal{O}_Y))^{(2g+2)\times(2g+2)}$$

such that

$$\Lambda_{\phi} G + dG = G\Lambda, \tag{4.3}$$

where $j^{\dagger}\mathcal{O}_Y$ is the overconvergent structure sheaf on the tube $]Y[$.

Compared to [BDM$^+$19, §5.3.2], we give a slightly more detailed account of the algorithm to find G. We first apply the algorithms in [Tui16, Tui17] (see [BT20, Algorithm 2.18]) to compute the action of Frobenius on $\mathrm{H}^1_{\mathrm{rig}}(X \otimes \mathbf{Q}_p)$ as

$$\phi^* \boldsymbol{\omega} = F\boldsymbol{\omega} + d\mathbf{f} \tag{4.4}$$

for a matrix $F \in M_{2g}(\mathbf{Q}_p)$ and a column vector $\mathbf{f}$ with entries in $\mathrm{H}^0(]Y[, j^{\dagger}\mathcal{O}_Y)$, uniquely determined by the condition that $\mathbf{f}(b_0) = \mathbf{0}$, where b_0 is the Teichmüller point in the disk of b.

Next, we define a vector of functions $\mathbf{g}_0 := -F^T Z \mathbf{f}$. Then, the differential

$$\xi := (\phi^* \boldsymbol{\omega}^T) Z \mathbf{f} + (\phi^* \eta - p\eta) - \mathbf{g}_0^T \boldsymbol{\omega} \tag{4.5}$$

is of the second kind, and therefore the reduction algorithms in $\mathrm{H}^1_{\mathrm{rig}}(Y)$ from [Tui16, Tui17] can be applied to compute a vector of constants $\mathbf{c} \in \mathbf{Q}_p^{2g}$ and a function $H^4 \in \mathrm{H}^0(]Y[, j^\dagger \mathcal{O}_Y)$ such that

$$\mathbf{c}^T \boldsymbol{\omega} + dH = \xi. \tag{4.6}$$

Hence the function $\mathbf{g} := \mathbf{g}_0 + \mathbf{c}$ satisfies

$$d\mathbf{g}^\intercal = d\mathbf{f}^\intercal Z F \quad \text{and} \quad dH = \boldsymbol{\omega}^\intercal F^\intercal Z \mathbf{f} + d\mathbf{f}^\intercal Z \mathbf{f} - \mathbf{g}^\intercal \boldsymbol{\omega} + \phi^* \eta - p\eta\,,$$

and we normalise H by requiring that $H(b_0) = 0$. The matrix

$$G = \begin{pmatrix} 1 & 0 & 0 \\ \mathbf{f} & F & 0 \\ H & \mathbf{g}^\intercal & p \end{pmatrix} \tag{4.7}$$

then satisfies (4.3).

4.2.1 *Frobenius-equivariant splitting for Teichmüller points* Suppose that $x_0 \in X(\mathbf{Q}_p) \cap]\mathcal{U}[$ is a Teichmüller point. As described in [BDM$^+$19, §5.3.2], the Frobenius-equivariant splitting of $M(x_0)$ is given by

$$\lambda^\phi(x_0) = \begin{pmatrix} 1 & 0 & 0 \\ (I-F)^{-1}\mathbf{f} & 1 & 0 \\ \frac{1}{1-p}\left(\mathbf{g}^\intercal (I-F)^{-1}\mathbf{f} + H\right) & \mathbf{g}^\intercal (F-p)^{-1} & 1 \end{pmatrix} (x_0)\,. \tag{4.8}$$

The loss of precision in the computation of $\mathbf{f}$ and F is estimated in [Tui17]. Hence it is easy to bound the precision loss in the computation of $\lambda^\phi(x_0)$ using the following result.

Proposition 4.1. *Suppose that the entries of the matrix G and a point $P \in X(\mathbf{Q}_p) \cap]\mathcal{U}[$ are accurate to n digits of precision. Then $G(P)$ is also accurate to n digits of precision.*

Our proof of Proposition 4.1 is somewhat similar, but more involved than the proofs in [BT20, §4], where the loss of precision in the evaluation of $\mathbf{f}$ and of single Coleman integrals is estimated. We may expand

$$\xi = \sum_{j \in \mathbf{Z}} \left(\sum_{k=0}^{d_x - 1} \frac{w_{j,k}(x)}{r(x)^j} b_k^0 \right) \frac{dx}{r}\,. \tag{4.9}$$

The hardest part of the proof of Proposition 4.1 is to find lower bounds on the valuation of the coefficients $w_{j,k}$, which we now describe. Let e_0 (resp., e_∞) be the maximum of the ramification indices of the map $x\colon X \to \mathbf{P}^1$ with respect to our chosen model at points lying in affine (resp., infinite) disks.

Lemma 4.2. *There is a constant κ such that for all j, k we have*

$$\mathrm{ord}_p(w_{jk}) \geqslant \begin{cases} \left\lfloor \frac{j}{p} \right\rfloor + 1 - \log_p(je_0) + \kappa, & j \neq 0 \\ \kappa, & j = 0. \end{cases} \tag{4.10}$$

Proof. Looking at the constituent parts of (4.5), we start with $(\phi^* \boldsymbol{\omega}^T) Z \mathbf{f}$. We write

$$(\phi^* \boldsymbol{\omega}^T)_i = \sum_{j_1 \in \mathbf{Z}} \left(\sum_{k_1=0}^{d_x - 1} \frac{d^{(i)}_{j_1,k_1}(x)}{r^{j_1}} b^0_{k_1} \right) \frac{dx}{r}.$$

Then $\mathrm{ord}_p(d^{(i)}_{j_1,k_1}) \geqslant \lfloor \frac{j_1}{p} \rfloor + 1$ by [Tui17, Proof of Proposition 4.9]. We have

$$f_i = f_{i,0} + f_{i,\infty} + f_{i,end}\,,$$

[4]The function H is denoted h in [BDM$^+$19], but we chose a different notation to avoid confusion with the global height, which is also denoted by h.

where $f_{i,0}$, $f_{i,\infty}$ and $f_{i,end}$ correspond to the three reduction steps (2), (3) and (4) in the reduction algorithm from [Tui17], summarised in [BT20, Algorithm 2.18]. By equations (1), (3) and (4) of [BT20], there are $\mu_1, \lambda_1 \geqslant 0$ such that

$$f_{i,0} = \sum_{j_2=1}^{\infty} \left(\sum_{k_2=0}^{d_x-1} \frac{c^{(i)}_{j_2,k_2}(x)}{r^{j_2}} b^0_{k_2} \right),$$

$$f_{i,\infty} = \sum_{k_3=0}^{d_x-1} \sum_{l=0}^{\mu_1} e^{(i)}_{k_3,l} x^l b^0_{k_3}, \qquad f_{i,end} = \sum_{k_4=0}^{d_x-1} \sum_{m=0}^{\lambda_1} u^{(i)}_{k_4,m} x^m b^0_{k_4}.$$

Equation (2) of [BT20] implies the lower bound $\mathrm{ord}_p(c^{(i)}_{j_2,k_2}) \geqslant \left\lfloor \frac{j_2}{p} \right\rfloor + 1 - \log_p \lfloor j_2 e_0 \rfloor$. Let

$$\kappa^{(i)} := \min(\{0, \mathrm{ord}_p(e^{(i)}_{k_3,l})\} \cup \{\mathrm{ord}_p(u^{(i)}_{k_4,m})\}) \quad \text{and} \quad \kappa_1 := \min_i \{\kappa^{(i)}\}. \tag{4.11}$$

Without loss of generality, the matrix Z has p-integral entries. Hence every $(Z\mathbf{f})_i$ is of the form

$$(Z\mathbf{f})_i = \sum_{j_2=0}^{\infty} \sum_{k_2=0}^{d_x-1} \frac{g^{(i)}_{j_2,k_2}(x)}{r^{j_2}} b^0_{k_2} \tag{4.12}$$

where for all k_2, we have

$$\mathrm{ord}_p(g^{(i)}_{j_2,k_2}) \geqslant \begin{cases} \left\lfloor \frac{j_2}{p} \right\rfloor + 1 - \log_p \lfloor j_2 e_0 \rfloor \text{ , if } j_2 > 0 \\ \kappa_1 \text{ , if } j_2 = 0 . \end{cases} \tag{4.13}$$

Let us now consider, for each i,

$$\begin{aligned} \left(\phi^* \boldsymbol{\omega}^T\right)_i (Z\mathbf{f})_i &= \sum_{j_1 \in \mathbf{Z}} \left(\sum_{k_1=0}^{d_x-1} \frac{d^{(i)}_{j_1,k_1}}{r^{j_1}} b^0_{k_1} \right) \left(\sum_{j_2=0}^{\infty} \sum_{k_2=0}^{d_x-1} \frac{g^{(i)}_{j_2,k_2}}{r^{j_2}} b^0_{k_2} \right) \frac{dx}{r} \\ &= \sum_{j=j_1+j_2 \in \mathbf{Z},\, j_1 \in \mathbf{Z},\, j_2 \geqslant 0} \frac{1}{r^j} \left(\sum_{k=k_1+k_2,\, k_i \in \{0,\ldots,d_x-1\}} \left(d^{(i)}_{j_1,k_1} g^{(i)}_{j_2,k_2} \right) b^0_k \right) \frac{dx}{r} \\ &=: \sum_{j \in \mathbf{Z}} \left(\frac{1}{r^j} \sum_{k=1}^{d_x-1} \tau_{jk} b^0_k \right) \frac{dx}{r}. \end{aligned}$$

We distinguish two cases: If $j_2 > 0$ then

$$\mathrm{ord}_p(d^{(i)}_{j_1,k_1} g^{(i)}_{j_2,k_2}) \geqslant \left\lfloor \frac{j_1}{p} \right\rfloor + 1 + \left\lfloor \frac{j_2}{p} \right\rfloor + 1 - \log_p(j_2 e_0) \geqslant \left\lfloor \frac{j}{p} \right\rfloor + 1 - \log_p((j-1)e_0). \tag{4.14}$$

If $j_2 = 0$, then $\mathrm{ord}_p(d^{(i)}_{j_1,k_1} g^{(i)}_{j_2,k_2}) \geqslant \left\lfloor \frac{j_1}{p} \right\rfloor + 1 + \kappa_1$. Together, we obtain

$$\mathrm{ord}_p(\tau_{jk}) \geqslant \left\lfloor \frac{j}{p} \right\rfloor + 1 - \log_p((j-1)e_0) + \kappa_1. \tag{4.15}$$

The next term to consider in (4.5) is $\phi^*\eta - p\eta$, where η is constructed in [BDM$^+$19, §4]. Let κ_2 denote the p-adic valuation of the vector of coefficients of η in terms of the basis differentials $\omega_{2g}, \ldots, \omega_{2g+2-d}$ (see [BDM$^+$19, §4.1]). Write

$$\phi^*\eta - p\eta = \sum_{j \in \mathbf{Z}} \left(\sum_{k=0}^{d_x-1} \frac{s_{jk}(x)}{r^j} b^0_k \right) \frac{dx}{r}.$$

Then the s_{jk} satisfy $\mathrm{ord}_p(s_{jk}) \geqslant \kappa_2 + \left\lfloor \frac{j}{p} \right\rfloor + 1$ if $j \neq 0$ and $\mathrm{ord}_p(s_{0k}) \geqslant \kappa_2 + 1$, so

$$\mathrm{ord}_p(s_{jk}) \geqslant \kappa_2 + \left\lfloor \frac{j}{p} \right\rfloor + 1 \text{ for all } j\,. \tag{4.16}$$

For the final summand $\mathbf{g}_0^T\boldsymbol{\omega}$ in (4.5) note that since F has p-integral entries, every $(F^T Z\mathbf{f})_i$ has an expansion as in (4.12). Because ω_i is integral for all i, the lower bounds in (4.13) remain valid for $\mathbf{g}_0^T\boldsymbol{\omega}$. The proof of Lemma 4.2 follows from this and from (4.14) and (4.15) upon setting $\kappa = \min\{\kappa_1, \kappa_2\}$. □

We now estimate the precision loss that can occur during the application of the reduction algorithm from [Tui17] to the differential ξ. Our proof is similar to the proof of [Tui17, Prop 4.9], which estimates the precision loss in the reduction of $F^*(\omega_i)$. Suppose that ξ is correct to n digits of p-adic precision. First consider terms in (4.9) with $j > 0$. It follows from (4.10) that $j - p\log_p(je_0) \leqslant pm - p\kappa$ (note that $\kappa \leqslant 0$). By [Tui17, Prop 3.7], the precision loss at pole order j during the reduction at finite points is at most $\lfloor \log_p(j_{\max}e_0) \rfloor$, where $j_{\max}$ is the largest integer j such that $j - p\log_p(je_0) \leqslant pn - p\kappa$. As in the proof of [Tui17, Prop 4.9], this might introduce small poles above ∞, but by the same reasoning as in op. cit., the reduction of these poles leads to a loss of precision bounded by $\lfloor \log_p(-(\mathrm{ord}_\infty W^{-1}) + 1)e_\infty \rfloor$. We set

$$g_1(n) := \lfloor \log_p(j_{\max}e_0) \rfloor + \lfloor \log_p(-(\mathrm{ord}_\infty W^{-1}) + 1)e_\infty \rfloor\,.$$

If we write

$$\xi = \left(\sum_{i=0}^{d_x - 1} \alpha_i(x, x^{-1}) b_i^\infty \right) \frac{dx}{r} \quad \text{and} \quad m_\infty = -\min_i \{\mathrm{ord}_\infty \alpha_i - \deg(r) + 1\}\,,$$

then the loss of precision during the reductions above infinity (where $j \leqslant 0$) is bounded by $g_2 := \lfloor \log_p(m_\infty e_\infty) \rfloor$.

Hence we have shown the following:

Lemma 4.3. *Suppose that ξ is correct to n digits of precision. Then $\mathbf{c}$ and H are correct to $n - \max\{g_1(n), g_2\}$ digits of precision.*

Proof of Proposition 4.1. Similar to the f_i, we may decompose H as $H = H_0 + H_\infty + H_{end}$, corresponding to steps (2), (3) and (4), respectively, in [BT20, Algorithm 2.18]. By the above, the reduction above finite points introduces a denominator of valuation at most $\log_p(je_0)$ for pole order j, therefore we have

$$H_0 = \sum_{j \geqslant 1} \sum_{k=0}^{d_x - 1} \frac{c_{jk}(x)}{r^j} b_k^0\,, \quad \text{where } \mathrm{ord}_p(c_{jk}) \geqslant \left\lfloor \frac{j}{p} \right\rfloor - 2\log_p(je_0) + \kappa\,. \tag{4.17}$$

Recall that the matrix G is defined in (4.7). There is no loss of precision when evaluating $\mathbf{f}(P)$ by [BT20, Prop. 4.5]. By our assumption that F and Z are p-integral, there is no precision loss when evaluating $\mathbf{g_0}(P)$. Using the bounds (4.17), the proof of [BT20, Prop. 4.5] shows that $H(P)$ is accurate to n digits of precision as well. Since $\mathbf{g} = \mathbf{g_0} + \mathbf{c}$, the proposition follows. □

4.2.2 *Frobenius-equivariant splitting for general points* For $x \in X(\mathbf{Q}_p) \cap]\mathcal{U}[$, not necessarily Teichmüller, the Frobenius-equivariant splitting $\lambda^\phi(x)$ of $M(x)$ is given by

$$\begin{pmatrix} 1 & 0 & 0 \\ \int_x^{x_0} \boldsymbol{\omega} & 1 & 0 \\ \int_x^{x_0} \eta + \int_{x_0}^{x} \boldsymbol{\omega}^\intercal Z \boldsymbol{\omega} & \int_x^{x_0} \boldsymbol{\omega}^\intercal Z & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ \int_{b_0}^{b} \boldsymbol{\omega} & 1 & 0 \\ \int_{b_0}^{b} \eta + \int_{b_0}^{b} \boldsymbol{\omega}^\intercal Z \boldsymbol{\omega} & -\int_{b_0}^{b} \boldsymbol{\omega}^\intercal Z & 1 \end{pmatrix} \cdot \lambda^\phi(x_0), \tag{4.18}$$

where x_0 is the Teichmüller point in the disk of x. The first two matrices in (4.18) correspond to parallel transport of Λ from x to x_0 and from b_0 to b, respectively.

For the local height $h_p(A(x))$, we need the Frobenius-equivariant splitting $\lambda^\phi(x)$ both for fixed x and for x varying inside a residue disk. We start by bounding the valuations of the coefficients of power series expansions of the differentials in the parallel transport matrices of Λ in terms of a local coordinate t at a fixed affine point $y_0 \in X(\mathbf{Q}_p)\cap]\mathcal{U}[$. By assumption, the entries of the expansions of $\boldsymbol{\omega}$ and $\boldsymbol{\omega}^\intercal Z$ all have integral coefficients, so their integrals have entries whose i-th coefficient has valuation $\geqslant -\mathrm{ord}_p(i)$. Therefore, we have

$$\boldsymbol{\omega}(t)^\intercal Z \int \boldsymbol{\omega}(t) = \sum_{i\geqslant 1} a_i t^i\,, \quad \text{where } \mathrm{ord}_p(a_i) \geqslant -\lfloor \log_p(i)\rfloor\,. \tag{4.19}$$

It follows that

$$\int (\boldsymbol{\omega}(t)^\intercal Z \int \boldsymbol{\omega}(t)) = \sum_{i\geqslant 1} b_i t^i\,, \quad \text{where } \mathrm{ord}_p(b_i) \geqslant -2\lfloor \log_p(i)\rfloor\,. \tag{4.20}$$

By construction, the coefficients of η in terms of $\omega_{2g},\dots,\omega_{2g+d-2}$ are polynomials in x. Define $d_i(\eta)$ to be the valuation of the ith coefficient if i is smaller than the maximum of the degrees of these coefficients and 0 otherwise. Then the ith coefficient of the integral of η has valuation $\geqslant -\mathrm{ord}_p(i) - d_i(\eta)$. Hence, the ith coefficient of every expansion of the parallel transport matrix in t has valuation at least

$$\varphi(i) := -\lfloor \log_p(i)\rfloor + \min\{d_i(\eta), -\lfloor \log_p(i)\rfloor\}\,. \tag{4.21}$$

For definite parallel transport from y_0 to another $\mathbf{Q}_p$-point y_1 in the same residue disk, we need to evaluate the integrals above. Suppose that y_0, y_1, and the coefficients of the expansions of $\boldsymbol{\omega}$ and η are correct to n digits of p-adic precision, and suppose that the expansions are truncated modulo t^l. Let

$$\nu_1 := 1 + \min_{i\geqslant l}\{i - \lfloor \log_p(i+1)\rfloor\} \quad \text{and } \nu_2 := n + \min_{0\leqslant i\leqslant l-1}\{i - \lfloor \log_p(i+1)\rfloor\}\,.$$

Then $\int_{y_0}^{y_1}\omega_j$ and $\int_{y_0}^{y_1}(Z\boldsymbol{\omega})_j$ are correct to $\min\{\nu_1,\nu_2\}$ digits by [BT20, Prop. 4.1]. The proof of [BT20, Prop. 4.1] requires that the differential we integrate has integral coefficients. A modification of this proof yields that the integral $\int_{y_0}^{y_1}\eta$ is correct to $\min\{\nu_1',\nu_2\}$ digits, where $\nu_1' = 1 + \min_{i\geqslant l}\{i - \lfloor \log_p(i+1)\rfloor - d_i(\eta)\}$. A similar modification shows that the double integral $\int_{y_0}^{y_1}\boldsymbol{\omega}^\intercal Z\boldsymbol{\omega}$ is correct to $\min\{\nu_1'',\nu_2'\}$ digits, where $\nu_1'' = 1+\min_{i\geqslant l}\{i-2\lfloor \log_p(i+1)\rfloor\}$ and

$$\nu_2' = n - \lfloor \log_p(n)\rfloor + \min_{0\leqslant i\leqslant l-1}\{1 - \lfloor \log_p(i+1)\rfloor\}\,.$$

Hence we obtain the following:

LEMMA 4.4. *The parallel transport matrix from y_0 to y_1 is correct to $\min\{\nu_1',\nu_2'',\nu_2'\}$ digits of precision.*

Using (4.18), we can finally bound the loss of precision in the computation of $\lambda^\phi(x)$ for fixed points $x \in X(\mathbf{Q}_p)\cap]\mathcal{U}[$ by combining Lemma 4.4 and Proposition 4.1.

4.3 Global heights

We now discuss the possible precision loss in the computation of the global height h. In Step (vi(b)) of Algorithm 3.12 we solve for $d_1,\dots,d_g$ such that

$$h = \sum_i d_i \Psi_i \tag{4.22}$$

in terms of a basis $\{\Psi_i\}$ of bilinear pairings on $\mathrm{H}^0(X_{\mathbf{Q}_p},\Omega^1)^\vee$ by evaluating h and the Ψ_i. Recall that our method for determining the coefficients depends on whether there are sufficiently many rational points on X in the sense of §3.3. If this is the case, meaning that we can use a basis of consisting of $\pi(\mathrm{A}_Z(b,x))$ for rational points $x \in X(\mathbf{Q})\cap]\mathcal{U}[$, then we need to compute $h_p(\mathrm{A}_Z(b,z)$ and $\pi(\mathrm{A}_Z(b,x))$, and then apply simple linear algebra. The precision loss in the computation $h_p(\mathrm{A}_Z(b,x))$ has already been bounded and $\pi(\mathrm{A}_Z(b,x))$ can be obtained directly from the same data (see [BBB+21, Equation (41)]). The loss of precision in the linear algebra computations is easy to detect in practice, so we do not bound it explicitly here.

In the other case, the basis Ψ_i is given in terms of products of abelian integrals. As mentioned above, the loss of precision in their computation is estimated in [BT20]. It remains to discuss precision loss in the computation of Coleman–Gross local heights $h_p(D_1, D_2)$, where D_1, D_2 are divisors in $\mathrm{Div}^0(X)(\mathbf{Q}_p)$ for X a hyperelliptic curve subject to the hypotheses of Algorithm 3.4; see [BB12, §6.2] for further details. Choosing ω in Step (1) can be done up to the precision of the points in the support of the divisor D_1. To compute $\Psi(\omega)$ and ω_{D_1} to $O(p^n)$ in Step (2), see Section 5.2 and Section 6.2.3 of [BB12]: one needs to compute the local coordinates $(x(t), y(t))$ at infinity, with $x(t)$ to precision $t^{2(2g-1)}$ and $y(t)$ to precision t^{2g-1}, where these t-adic estimates are made based on the maximal pole order in the basis of $H^1_{\mathrm{dR}}(X)$. Step (4) proceeds similarly to this step as well.

In Step (5), the tiny integrals are computed as in [BB12, §6]. In previous steps, we wrote $\Psi(\alpha)$ and $\Psi(\beta)$ as $\mathbf{Q}_p$-linear combinations of the basis elements of $H^1_{\mathrm{dR}}(X)$, up to precision $O(p^n)$. Note that the hypothesis that $p > 2g-1$ is to ensure that the cup product matrix has entries that are p-integral, so no precision loss comes from the cup product matrix.

Finally, for $\sum_{A \in X(\mathbf{C}_p)} \mathrm{Res}_A\left(\alpha \int \beta\right)$, we consider the cases of A a non-Weierstrass point (where we describe the computation in the annulus of A) versus A Weierstrass (where we have just one contribution, at the Weierstrass point). If $A \neq (0,0)$ is a Weierstrass point, we compute the local coordinate $(x(t), y(t))$ at A to precision $t^{2pn-p-1}$ (see the corrected Proposition 6.5 in [BB21]) so that $\mathrm{Res}_A(\alpha \int \beta)$ is computed to n digits of p-adic precision.

Now we consider the non-Weierstrass poles of α. For the annulus of a non-Weierstrass pole A, the generic situation is handled by [BB12, Corollary 6.4]. By [BB12, Remark 4.10], we consider all $A \in \{P_i, Q_j\}_{i,j}$ where $x(P_i)$ corresponds to a root of an irreducible factor of $x^p - x(P)$ (and similarly where $x(Q_j)$ corresponds to a root of an irreducible factor of $x^p - x(Q)$). For these i, j, we compute $\int_P^{P_i} \beta$ and $\int_Q^{Q_j} \beta$ and trace down to $\mathbf{Q}_p$. We suppose $P \in X(\mathbf{Q}_p)$ has precision $O(p^n)$. Fix m and suppose β is computed to $t^{d_i m}$ at P_i, where $d_i = [\mathbf{Q}_p(P_i) : \mathbf{Q}_p]$. Let π_i be a uniformiser of $\mathbf{Q}_p(P_i)$. Note that P is known to $d_i n$ π_i-adic digits, and suppose that P_i is known to n_i π_i-adic digits. Then the π_i-adic precision of $\int_P^{P_i} \beta$ is at least $\min\{n_i, d_i n, \lfloor d_i m + 1 \rfloor - \log_p(d_i m + 1)\}$. We similarly repeat this for Q and the corresponding Q_j. Hence $\sum_A \mathrm{Res}_A(\alpha \int \beta)$, where the sum is over all non-Weierstrass poles A of α, is correct to p-adic precision

$$\min_{i,j}\{n_i, d_i n, \lfloor d_i m + 1 \rfloor - \log_p(d_i m + 1), n_j, d_j n, \lfloor d_j m + 1 \rfloor - \log_p(d_j m + 1)\},$$

where we consider the corresponding i, j for all P_i and all Q_j.

4.4 Coefficients of the quadratic Chabauty function and root finding

The previous results of this section bound the loss of precision in the computation of the quadratic Chabauty function $\rho = h - h_p$. Let $D \subset X(\mathbf{Q}_p) \cap]\mathcal{U}[$ be a residue disk and let x_0 be the Teichmüller point in D. We now bound the valuations of the coefficients of the expansion of ρ in D and show how to provably compute its roots to desired precision.

In our algorithm, we fix a point $x_1 \in D$, and we compute the Frobenius-equivariant splitting $\lambda^\phi(x)$ on D as a power series in a local coordinate t in x_1 by first computing $\lambda^\phi(x_1)$ from $\lambda^\phi(x_0)$ and then multiplying this by the parallel transport matrix from x_1 to x. To bound the valuations of the coefficients of the entries of $\lambda^\phi(x)$,

we first compute

$$c_1 := \mathrm{ord}_p(\lambda^\phi(x_1))$$

using Lemma 4.4. By the above, we find that the ith coefficient of every entry of the expansion of $\lambda^\phi(x)$ has valuation at least $\varphi(i) + c_1$. We use this to bound the valuations of the coefficients of the local height h_p. Recall from §3.3 that we use a height with respect to an $\mathrm{End}(J)$-equivariant splitting of the Hodge filtration; let v_{spl} be the smallest valuation of the coefficients of this splitting in terms of our basis $\boldsymbol{\omega}$. We denote by $\mathrm{ord}_p(\gamma_{\mathrm{Fil}})$ the smallest valuation in the coefficients of the rational function γ_{Fil}, and we set

$$c_2 := \min\{0, v_{\mathrm{spl}}, \mathrm{ord}_p(\beta_{\mathrm{Fil}}), v_{\mathrm{spl}} + \mathrm{ord}_p(\beta_{\mathrm{Fil}})\}.$$

LEMMA 4.5. *Let*

$$h_p(x(t)) = \sum_{i \geqslant 0} h_i t^i$$

be the expansion of h_p on the residue disk D in the local parameter t. Then we have

$$\mathrm{ord}_p(h_i) \geqslant \min\{\mathrm{ord}_p(\gamma_{\mathrm{Fil}}), \varphi(i) + c_2\}. \tag{4.23}$$

Proof. This follows from the discussion above and from (3.2), which expresses $h_p(x)$ in terms of $\lambda^{\mathrm{Fil}}(x)$ and $\lambda^{\phi}(x)$. □

We set $c_3 := \min_i\{\mathrm{ord}_p(d_i)\}$, where the d_i are the coefficients in (4.22). Let $i_0 \geqslant 0$ be such that

$$-\lfloor \log_p(i) \rfloor \leqslant \min\left\{ d_i(\eta), \left\lfloor \frac{\mathrm{ord}_p(\beta_{\mathrm{Fil}})}{2} \right\rfloor, \left\lfloor \frac{\mathrm{ord}_p(\gamma_{\mathrm{Fil}}) - c_2}{2} \right\rfloor \right\}$$

for all $i \geqslant i_0$. Then we have $\varphi(i) = -2\lfloor \log_p(i) \rfloor + c_1$ for all $i \geqslant i_0$. This proves the following:

PROPOSITION 4.6. *Let*

$$\rho(t) = \sum_{i \geqslant 0} \rho_i t^i$$

be the expansion of the quadratic Chabauty function $\rho = h - h_p$ on D. If $i \geqslant i_0$, then we have

$$\mathrm{ord}_p(\rho_i) \geqslant -2\lfloor \log_p(i) \rfloor + c_1 + \min\{c_2, c_3\}.$$

Together with Proposition 4.6, the following result allows us to provably determine the roots of ρ to any desired precision.

LEMMA 4.7. *Suppose $F(x) = \sum_{i \geqslant 0} F_i x^i \in \mathbf{Q}_p[\![x]\!]$ is such that there are integers k, m, n satisfying*

$$\min\{\mathrm{ord}_p(F_i) + i : i \geqslant 0\} = k$$

and

$$\max\{i \geqslant 0 : \mathrm{ord}_p(F_i) + i = n\} < m,$$

and furthermore that F has at most d roots in the closed disk $\{\mathrm{ord}_p(x) \geqslant 1\}$. Then the roots of F in the ball $\{\mathrm{ord}_p(x) \geqslant 1\}$ can be determined, with multiplicity, to precision $(n-k)/d$, by computing $F_0, \ldots, F_{m-1}$ modulo p^n.

Proof. By our assumptions, $F(px)$ lies in $p^k\mathbf{Z}_p[\![x]\!] - p^{k+1}\mathbf{Z}_p[\![x]\!]$. Hence the power series $G(x) := p^{-k}F(px)$ lies in $\mathbf{Z}_p[\![x]\!] - p\mathbf{Z}_p[\![x]\!]$. Furthermore, by our assumptions, for any $\alpha \in \mathbf{Z}_p$, the positive slopes of the Newton polygon of $G(x+\alpha)$ are uniquely determined by the first m coefficients. If $G(x)$ is congruent modulo p^{n-k} to a polynomial H in $\mathbf{Z}_p[x]$ with a root $\alpha \in \overline{\mathbf{Z}}_p$ of multiplicity e, then the valuation of the first e coefficients of $G(x+\alpha)$ must be at least $n-k$. Since $G(x+\alpha)$ has degree $\leqslant m$ mod p^{n-k} and has at least one coefficient of valuation zero, we deduce that the Newton polygon of $G(x+\alpha)$ must contain a segment of slope $\geqslant (n-k)/d$ of length at least e. □

Remark 4.8. In practice, we usually apply this with $d = 1$, by recentering and rescaling our power series so that there is only one root in the ball $\{\mathrm{ord}_p(x) \geqslant 1\}$ (and because in practice the power series do not typically have repeated roots). Hence most loss of precision occurs from k being large, rather than d.

5. Examples

In this section, we apply our techniques to compute the rational points on

- the exceptional modular curve $X_{S_4}(13)$ (see §5.1);
- all curves $X_0^+(N)$ of genus 2 and 3 for which N is prime and the rational points were not previously known (see §5.2);

- two genus 2 curves of interest in Mazur's Program B (see §5.3);
- two genus 2 curves with Jacobian of GL_2-type that have nontrivial local height contributions away from p (see §5.4);
- the non-split Cartan curve $X_{\mathrm{ns}}^+(17)$ (see §5.5).

For the computations, we used our `Magma` implementation. The code used for the examples, along with log files, can be found in the folder `Examples` at [BDM$^+$].

5.1 The exceptional curve $X_{S_4}(13)$

Recall that for a prime $\ell \geqslant 5$, any proper subgroup of $\mathrm{GL}_2(\mathbf{F}_\ell)$ is conjugate to a subgroup of a Borel subgroup, the normaliser of a Cartan subgroup, or an "exceptional" subgroup with projective image isomorphic to S_4, A_4, or A_5. The field of definition of the modular curves attached to the exceptional subgroups is the unique quadratic subfield $\mathbf{Q}(\sqrt{\pm\ell})$ of the cyclotomic field $\mathbf{Q}(\zeta_\ell)$, with the exception of the curves $X_{S_4}(\ell)$ for $\ell \equiv \pm 3 \pmod 8$, which are defined over $\mathbf{Q}$. For such values of ℓ, we would therefore like to determine $X_{S_4}(\ell)(\mathbf{Q})$.

Serre [Ser72] shows by a monodromy argument that such tetrahedral modular curves have no points defined over $\mathbf{Q}_\ell$ when ℓ is large enough, and in particular he obtains

$$X_{S_4}(\ell)(\mathbf{Q}) = \emptyset, \qquad \text{if } \ell > 13.$$

The curves $X_{S_4}(3)$ and $X_{S_4}(5)$ are both of genus zero, and contain a unique rational cusp. Ligozat [Lig77] showed that $X_{S_4}(11)$ is an elliptic curve of conductor 11^2 whose Mordell–Weil group is trivial, where the unique rational point is CM, corresponding to discriminant $D = -3$. This leaves only the curve $X_{S_4}(13)$, which has genus 3. In fact, this curve is the last remaining modular curve of level 13^n whose rational points have not been determined.

Using modular symbols algorithms, Banwait–Cremona [BC14] show that the curve $X_{S_4}(13)$ is a smooth plane quartic whose canonical model is given by

$$\begin{aligned} &4x^3y - 3x^2y^2 + 3xy^3 - x^3z + 16x^2yz - 11xy^2z + \\ &5y^3z + 3x^2z^2 + 9xyz^2 + y^2z^2 + xz^3 + 2yz^3 = 0. \end{aligned}$$

Furthermore, they exhibit the following four rational points

$$\{(1:3:-2), (0:0:1), (0:1:0), (1:0:0)\} \subseteq X_{S_4}(13)(\mathbf{Q}),$$

where the rational point $(0:0:1)$ corresponds to an elliptic curve with CM by the order of discriminant $D = -3$, and the three other rational points correspond to non-CM elliptic curves over $\mathbf{Q}$ with projective mod 13 image equal to S_4, whose j-invariants are given by

$$\begin{aligned} j &= \frac{2^4 \cdot 5 \cdot 13^4 \cdot 17^3}{3^{13}} \qquad j = -\frac{2^{12} \cdot 5^3 \cdot 11 \cdot 13^4}{3^{13}} \\ j &= \frac{2^{18} \cdot 3^3 \cdot 13^4 \cdot 127^3 \cdot 139^3 \cdot 157^3 \cdot 283^3 \cdot 929}{5^{13} \cdot 61^{13}}. \end{aligned}$$

The Jacobian of $X_{S_4}(13)$ is isogenous to that of $X_{\mathrm{s}}^+(13)$, so it is absolutely simple and has Mordell–Weil rank 3 over $\mathbf{Q}$ by the results of [BDM$^+$19, §6]. The curve has potential good reduction at $p = 13$, as can be seen, for instance, using the `Sage` toolbox `MCLF`.

We determine the set of rational points on the curve $X_{S_4}(13)$ using quadratic Chabauty with $p = 11$ for the affine patches

$$\begin{aligned} &y^4 + (18x+9)y^3 + (160x^2 + 176x + 52)y^2 + (560x^3 + 832x^2 + 384x + 48)y \\ &\quad + 192x^4 + 512x^3 + 384x^2 + 64x = 0 \end{aligned}$$

and

$$y^4 + (9x+9)y^3 + (52x^2+72x+36)y^2 + (48x^3+240x^2+208x+64)y \\ + 64x^3 + 192x^2 - 64x = 0.$$

The computation is analogous to the computation of $X_s^+(13)(\mathbf{Q})$ in [BDM+19]. The Hecke operator T_{11} generates the Hecke algebra, as can be verified, for instance, by checking the analogous statement for $X_s^+(13)$. Hence we may construct suitable cycles Z_1, Z_2 from T_{11} and its square, respectively. The set of common zeroes of the resulting quadratic Chabauty functions consists precisely of the known rational points, so we obtain Theorem 1.1.

In order to solve for the height pairing, we use the 4 known rational points and the cycle Z_1, so the resulting function automatically vanishes there. However, since the cycles Z_1 and Z_2 are independent, and Z_2 is not used to solve for the height, the vanishing of the resulting function in the rational points provides a check for the correctness of our code.

Remark 5.1. Since the Jacobian of $X_{S_4}(13)$ is isogenous to that of $X_s^+(13)$, even if there were not enough rational points on $X_{S_4}(13)$ to solve for the height pairing, one could instead solve for it using $X_s^+(13)$.

5.2 The Atkin–Lehner quotients $X_0^+(N)$

For a positive integer N, consider the Atkin–Lehner involution w_N acting on the modular curve $X_0(N)$. Then the quotient

$$X_0^+(N) := X_0(N)/\langle w_N \rangle$$

is a smooth projective curve defined over $\mathbf{Q}$ whose non-cuspidal points classify unordered pairs $\{E_1, E_2\}$ of elliptic curves admitting an N-isogeny between them. The study of rational points on these curves is also important in an ongoing research program aiming to compute quadratic points on the modular curves $X_0(N)$; see, for instance, recent work of Box [Box21]. Among the rational points, we distinguish between cusps, CM-points and *exceptional points*, those which are neither cusps nor CM points. The exceptional points correspond to quadratic $\mathbf{Q}$-curves without CM.

In this section, we restrict to prime values N such that $X_0^+(N)$ has genus 2 or 3. Galbraith [Gal96] has computed models for all these curves (and many more) by finding relations in the vector space spanned by the newforms of level N and weight 2 that are invariant under w_N. Up to conjugation, there is a unique such newform.

By work of Ogg, for prime level N, the curve $X_0^+(N)$ has genus 2 if and only if

$$N \in \{67, 73, 103, 107, 167, 191\}. \tag{5.1}$$

It has genus 3 if and only if

$$N \in \{97, 109, 113, 127, 139, 149, 151, 179, 239\}. \tag{5.2}$$

Models for all these curves were communicated to us by Elkies; one can also find such models in Galbraith's thesis [Gal96] or by using the Magma command `X0NQuotient`.

Via a search for small rational points, Galbraith [Gal99] found exceptional rational points on $X_0^+(N)$ for $N = 73, 91, 103, 191$ (genus 2) and $N = 137, 311$ (genus 4). The latter examples disproved an earlier conjecture of Elkies that there are no exceptional rational points on non-hyperelliptic $X_0^+(N)$ for prime level N. In [Gal02], Galbraith also finds an exceptional point on $X_0^+(125)$ and conjectures that there are no further exceptional points on modular curves $X_0^+(N)$ of genus $2 \leqslant g \leqslant 5$.

Together with [BBB+21] and [Gal96], our computations described below prove Theorem 1.3. We first check that for level N as in (5.1) and (5.2) the curves $X_0^+(N)$ satisfy the requirements to apply our algorithm. The Jacobian $J_0^+(N)$ of $X_0^+(N)$ has real multiplication over $\mathbf{Q}$, so the Picard number is at least g. Using `Magma` we computed the L-function of the corresponding newforms to show that the analytic rank is g, so the work of Gross–Zagier and Kolyvagin–Logachev proves that the rank of $J(\mathbf{Q})$ is exactly g. For the genus 2 examples, we also applied two-descent on $J_0^+(N)$, as implemented in `Magma`, to have an independent check.

The curves $X_0^+(N)$ have good reduction away from N, but in contrast to $X_{\mathrm{ns}}^+(13)$ and $X_{S_4}(13)$, they do not have potentially good reduction at N. Nevertheless, the following result implies that when applying quadratic Chabauty, there are no nontrivial contributions to the height away from p.

Lemma 5.2. *There is a regular semi-stable model $\mathcal{X}_0^+(N)$ of $X_0^+(N)$ over $\mathbf{Z}_N$ whose special fibre has a unique irreducible component. In particular, the local height h_N is trivial on $X_0^+(\mathbf{Q}_N)$.*

Proof. If $N = 2, 3$ the result is readily checked. When $N > 3$ the Atkin-Lehner quotient of the model $\mathcal{X}_0(N)$ for $X_0(N)$ over $\mathrm{Spec}\mathbf{Z}$ constructed by Deligne–Rapoport [DR73] is shown by Xue [Xue09] to be regular and semi-stable. Its special fibre at N is a projective line, with an ordinary double point for every conjugate pair of supersingular j-invariants in $\mathbf{F}_{N^2}\backslash\mathbf{F}_N$. It follows from Theorem 3.2 that h_N is trivial. □

Finally, we checked for all N in (5.1) and in (5.2) that the Jacobian is absolutely simple by finding a prime q of good reduction such that $J_{\mathbf{F}_q}$ is absolutely simple, using the criterion of Howe and Zhu [HZ02, Proposition 3].

5.2.1 *Genus 2* In [BBB+21], the rational points on $X_0^+(N)$ for $N = 67, 73, 103$ were computed. Using a combination of quadratic Chabauty and the Mordell–Weil sieve, it is shown there that $X_0^+(67)(\mathbf{Q})$ contains no exceptional points and that the sets $X_0^+(73)(\mathbf{Q})$ and $X_0^+(103)(\mathbf{Q})$ both contain one pair of exceptional points each, with respective j-invariants (see [Gal99, Table 1])

$$\begin{aligned} j &= (81450017206599109708140525 \pm 14758692270140155157349165 \cdot \sqrt{-127})/2^{74}, \\ j &= (35982263935929364331785036841779200 \\ &\quad \pm 669908635472124980731701532753920 \cdot \sqrt{5 \cdot 577}. \end{aligned}$$

The remaining prime level genus 2 curves $X_0^+(107)$, $X_0^+(167)$, and $X_0^+(191)$ are more challenging, because they do not have sufficiently many rational points in the sense of §3.3 to solve for the height pairing, so we need to compute heights between divisors. In all cases, the quadratic Chabauty function $\rho = h - h_p$ has p-adic zeroes that do not come from a rational point; to verify this, we apply the Mordell–Weil sieve.

Example 5.3. We discuss our computations for the example $X := X_0^+(107)$ in some detail.

We look for a prime p of good reduction such that

- there is a unique $\mathbf{Q}_p$-rational Weierstrass disk, and it does not contain known rational points,
- the Hecke operator T_p generates the Hecke algebra, and
- p is suitable for the Mordell–Weil sieve.

For $p = 61$, the first two conditions are satisfied; moreover, we have

$$J(\mathbf{F}_{229}) \simeq \mathbf{Z}/(4 \cdot 61)\mathbf{Z} \times \mathbf{Z}/(4 \cdot 61)\mathbf{Z},$$

and since $J(\mathbf{F}_{61}) \simeq \mathbf{Z}/(31 \cdot 151)\mathbf{Z}$ has quite smooth order, 61 is a suitable prime. We now go through the steps in Algorithm 3.12, applied to X.

Step (i) The model

$$y^2 = -3x^6 - 4x^5 - 2x^4 + 2x^3 + 5x^2 + 2x + 1 =: f(x),$$

of X has 6 small rational points of exponential height at most 1000, given by $\{(0, \pm 1), (\pm 1, \pm 1)\}$. It also has no $\mathbf{Q}_{61}$-adic points at infinity, so that we only need to run our algorithm for one affine patch. We fix the base point $b = (0, -1)$.

Steps (ii, iii) are exactly as in [BDM+19].

Step (iv): We may use the unit root splitting, since $p = 61$ is ordinary. (See Remark 3.15.)

Step (v): Using Step (iii), we find for

$$Z = Z_1 = (\mathrm{Tr}(T_{61}) \cdot I_4 - 4T_{61})C^{-1} = \begin{pmatrix} 0 & 2/3 & -2 & 4 \\ -2/3 & 0 & 4 & 2 \\ 2 & -4 & 0 & 0 \\ -4 & -2 & 0 & 0 \end{pmatrix}, \tag{5.3}$$

that

$$Z = \sum_{i,j} Z_{ij}\omega_i \otimes \omega_j \in \mathrm{H}^1_{\mathrm{dR}}(X/\mathbf{Q}_{61}) \otimes \mathrm{H}^1_{\mathrm{dR}}(X/\mathbf{Q}_{61})$$

corresponds to a nontrivial cycle $Z \in \ker(\mathrm{NS}(J) \longrightarrow \mathrm{NS}(X))$ where C is the standard symplectic matrix of dimension $2g$ and $\boldsymbol{\omega}$ is the basis found in Step (ii).

Step (vi(a)): The Hodge filtration for Z is given by $\gamma_{\mathrm{Fil}} = -4x - 4$ and $\beta_{\mathrm{Fil}} = 0$. After computing the Frobenius structure, we obtain a power series expansion of the function $x \mapsto h_{61}(\mathrm{A}(x))$ on all residue disks of $X(\mathbf{Q}_{61})$, except for the disks at infinity and the unique Weierstrass disk containing points that reduce to $(31, 0)$.

Step (vi(b)): The points $P, Q \in J(\mathbf{Q})$ with respective Mumford representations $(x^2 + x, 1)$ and $(x^2 + 1, 2x - 1)$ generate a subgroup of $J(\mathbf{Q})$ of index 2. To solve for the height pairing via §3.3.1, we need divisor representatives with support in distinct non-Weierstrass residue disks. Let E be the degree 2 divisor on X cut out by the functions $x^2 + 1$ and $2x - 1$ and let E' be its image under the hyperelliptic involution. We set

$$\begin{aligned} D_1 &= (0, 1) + (-1, 1) - \mathrm{div}_0(x - 1), \quad D_1' = (0, -1) + (-1, -1) - \mathrm{div}_0(x - 7) \\ D_2 &= E - \mathrm{div}_0(x - 7), \quad D_2' = E' - \mathrm{div}_0(x - 1)\,. \end{aligned}$$

Then we have $h(P, Q) = \sum_v h_v(D_1, D_2)$ and

$$h(P, P) = -\sum_v h_v(D_1, D_1')\,, \quad h(Q, Q) = -\sum_v h_v(D_2, D_2')\,.$$

The divisors above all split over $\mathbf{Q}_{61}$, so we can compute the height pairings $h_{61}(D_1, D_2)$, $h_{61}(D_1, D_1')$ and $h_{61}(D_2, D_2')$, working on a monic odd degree model over $\mathbf{Q}_{61}$. Using `Magma`'s implementation of the algorithm described in [Mül14], we also find

$$\begin{aligned} \sum_{\ell \neq 61} h_\ell(D_1, D_1') &= -2\log_{61} 2 + 2\log_{61} 3 - \log_{61} 7\,, \\ \sum_{\ell \neq 61} h_\ell(D_1, D_2) &= 2\log_{61} 2 - 2\log_{61} 3 + \log_{61} 7, \\ \sum_{\ell \neq 61} h_\ell(D_2, D_2') &= 3\log_{61} 2 - \log_{61} 5\,, \end{aligned}$$

and we conclude that

$$h = \alpha_{00} g_{00} + \alpha_{01} g_{01} + \alpha_{11} g_{11}\,,$$

where

$$\begin{aligned} \alpha_{00} &= 58 \cdot 61^{-1} + 19 + 2 \cdot 61 + 43 \cdot 61^2 + O(61^3) \\ \alpha_{01} &= 43 \cdot 61^{-1} + 48 + 44 \cdot 61 + 41 \cdot 61^2 + O(61^3) \\ \alpha_{11} &= 49 \cdot 61^{-1} + 13 + 55 \cdot 61 + 2 \cdot 61^2 + O(61^3)\,, \end{aligned}$$

and the g_{ij} are defined in (3.3).

Steps (vi(c)) – (vii): Combining the functions resulting from Steps (vi(a)) and (vi(b)), we find a power series expansion of the quadratic Chabauty function

$$\rho = h - h_{61} \colon X(\mathbf{Q}_{61}) \to \mathbf{Q}_{61}$$

in all affine non-Weierstrass disks. By Lemma 5.2, the local heights $h_\ell(\mathrm{A}(x))$ are trivial for $\ell \neq 61$, so $\Upsilon = \{0\}$ and all rational points are zeroes of ρ. We find that ρ indeed vanishes on the known rational points, and that these are simple zeroes of ρ.

In addition, ρ vanishes to multiplicity 1 on 82 points in $X(\mathbf{Q}_{61})$ that do not appear to be rational. As described in §3.4, these yield cosets of $61^2 J(\mathbf{Q})$, and our implementation of the Mordell–Weil sieve shows that the image of these cosets does not intersect the image of $X(\mathbf{F}_{229})$ inside $J(\mathbf{F}_{229})/61^2 J(\mathbf{F}_{229})$. Hence these additional zeroes do not come from a rational point.

Recall that there are no $\mathbf{Q}_{61}$-rational points at infinity, so it only remains to show that there are no rational points in the Weierstrass disk. To this end, we show that for

$$S = \{41, 83, 641, 1697, 4057, 10853\},$$

the image of the reduction of this disk does not intersect

$$\mathrm{im}(\beta_{S,\,2\cdot 61}) \subset \prod_{v \in S} {}^{J(\mathbf{F}_v)}\!/_{MJ(\mathbf{F}_v)}\,,$$

where $M = 2\#J(\mathbf{F}_{61})$ and $\beta_{2,61}\colon \prod_{v\in S} X(\mathbf{F}_v) \to \prod_{v\in S} J(\mathbf{F}_v)/MJ(\mathbf{F}_v)$ is induced by the Abel-Jacobi map with respect to b and the canonical surjections.

This completes the proof that $\#X(\mathbf{Q}) = 6$. According to Galbraith [Gal96], these points are all cusps or CM-points.

Example 5.4. We were able to prove that the curve

$$X_0^+(167)\colon y^2 = x^6 - 4x^5 + 2x^4 - 2x^3 - 3x^2 + 2x - 3$$

only contains the four obvious rational points $\{(-1, \pm 1), \infty_\pm\}$; these are all cusps or CM by Galbraith [Gal96]. In our computation, we use our quadratic Chabauty algorithm for $p = 7$ and the Mordell–Weil sieve, following the same strategy as in Example 5.3. The verification that the additional solutions of the resulting p-adic functions are not rational was the most challenging Mordell–Weil sieve computation we encountered in our work; it required the auxiliary integer $5 \cdot 11 \cdot 19$ and the set of good primes

$$S = \{3, 5, 19, 29, 31, 67, 263, 281, 283, 769, 1151, 2377, 3847, 4957, 67217\}.$$

Example 5.5. A model for $X_0^+(191)$ is given by

$$y^2 = x^6 + 2x^4 + 2x^3 + 5x^2 - 6x + 1\,.$$

We use quadratic Chabauty for $p = 31$ together with the Mordell–Weil sieve exactly as above to show that $X_0^+(191)(\mathbf{Q}) = \{(0, \pm 1), (2, \pm 11), \infty_\pm\}$. Galbraith (see [Gal99, Table 1]) has shown that $(2, -11)$ is exceptional, with corresponding j-invariant

$$\begin{aligned} j =& 2891249511562231668955764266428063102082570956800000 \\ & \pm 64074939271375546714155254091066566840131584000\sqrt{61 \cdot 229 \cdot 145757}\,. \end{aligned}$$

5.2.2 *Genus 3* We apply our algorithm to show that the rational points on the curves $X_0^+(N)$ for N as in (5.2) are precisely the ones already found by Galbraith. All curves in our list are non-hyperelliptic and they have the convenient feature that they have sufficiently many rational points, so no heights on divisors need to be computed. We always find two independent cycles in $\ker(\mathrm{NS}(J) \longrightarrow \mathrm{NS}(X))$, and, as expected, the common zero set of the corresponding functions consists precisely of the rational points found by Galbraith.

Theorem 5.6. *Let N be a prime such that $X_0^+(N)$ has genus 3. Then the rational points on $X_0^+(N)$ are as below. In particular, all rational points are either cusps or CM-points, with discriminant Δ.*

Example 5.7. A model for $X_0^+(97)$ is given by

$$zx^3 + (-y^2 + zy)x^2 + (-y^3 - zy^2 - z^3)x + (zy^3 + z^2y^2) = 0.$$

Using our algorithm for $p = 5$, we find that the rational points are as follows:

Δ	cusp	-3	-4	-8	-11	-12	-16	-27	-43	-163
Point	$(1:0:0)$	$(-2:1:1)$	$(-1:0:1)$	$(0:0:1)$	$(0:1:0)$	$(0:-1:1)$	$(1:0:1)$	$(1:1:1)$	$(-1:1:0)$	$(5:3:2)$

Example 5.8. A model for $X_0^+(109)$ is given by

$$zx^3 + (zy + z^2)x^2 + (-y^3 - zy^2 - z^3)x + (-zy^3 - 3z^2y^2 - 2z^3y) = 0.$$

Using our algorithm for $p = 29$, we find that the rational points are as follows:

Δ	cusp	-3	-4	-7	-12	-16	-27	-28	-43
Point	$(1:0:0)$	$(-2:1:2)$	$(0:-2:1)$	$(0:-1:1)$	$(0:1:0)$	$(0:0:1)$	$(-1:-1:1)$	$(-2:1:1)$	$(1:-1:1)$

Example 5.9. A model for $X_0^+(113)$ is given by

$$zx^3 + (-y^2 - z^2)x^2 + (y^3 + z^3)x + (-2z^2y^2 + z^3y) = 0.$$

Using our algorithm for $p = 17$, we find that the rational points are as follows:

Δ	cusp	-4	-7	-8	-11	-16	-28	-163
Point	$(1:0:0)$	$(2:2:1)$	$(0:1:0)$	$(1:1:1)$	$(1:1:0)$	$(0:0:1)$	$(0:1:2)$	$(5:3:1)$

Example 5.10. A model for $X_0^+(127)$ is given by

$$zx^3 + (-y^2 - 3z^2)x^2 + (y^3 - z^2y + 4z^3)x + (2zy^3 - 3z^2y^2 + 3z^3y - 2z^4) = 0.$$

Using our algorithm for $p = 11$, we find that the rational points are as follows:

Δ	cusp	-3	-7	-12	-27	-28	-43	-67
Point	$(1:0:0)$	$(5:3:2)$	$(2:1:1)$	$(1:1:0)$	$(1:0:1)$	$(0:1:1)$	$(0:1:0)$	$(4:2:1)$

Example 5.11. A model for $X_0^+(139)$ is given by

$$zx^3 + (-y^2 + zy)x^2 + (-y^3 - 2zy^2 - 3z^2y - z^3)x + (y^4 + zy^3 + z^2y^2 + z^3y) = 0.$$

Using our algorithm for $p = 19$, we find that the rational points are as follows:

Δ	cusp	-3	-8	-12	-19	-27	-43
Point	$(1:0:0)$	$(4:-3:1)$	$(0:0:1)$	$(0:-1:1)$	$(1:-1:1)$	$(1:0:1)$	$(-1:0:1)$

Example 5.12. A model for $X_0^+(149)$ is given by

$$zx^3 - y^2x^2 + (y^3 + zy^2 - 2z^2y - z^3)x + (-y^4 + zy^3 + z^2y^2 - z^3y) = 0.$$

Using our algorithm for $p = 11$, we find that the rational points are as follows:

Δ	cusp	-4	-7	-16	-19	-28	-67
Point	$(1:0:0)$	$(-1:0:1)$	$(0:1:1)$	$(1:0:1)$	$(0:0:1)$	$(0:-1:1)$	$(2:2:1)$

Example 5.13. A model for $X_0^+(151)$ is given by

$$zx^3 + (-2zy + z^2)x^2 + (-y^3 + 2zy^2)x + (-zy^3 + 3z^2y^2 - z^3y - 2z^4) = 0.$$

Using our algorithm for $p = 19$, we find that the rational points are as follows:

Δ	cusp	-3	-7	-12	-27	-28	-67	-163
Point	$(1:0:0)$	$(-2:-2:1)$	$(0:1:0)$	$(0:2:1)$	$(1:1:1)$	$(2:3:2)$	$(1:0:1)$	$(3:2:1)$

Example 5.14. A model for $X_0^+(179)$ is given by

$$zx^3 + (-2zy - z^2)x^2 + (-y^3 - zy^2 - 2z^2y - z^3)x + (-zy^3 + z^3y) = 0.$$

Using our algorithm for $p = 17$, we find that the rational points are as follows:

Δ	cusp	-7	-8	-11	-28	-163
Point	$(1:0:0)$	$(0:-1:1)$	$(0:1:0)$	$(0:0:1)$	$(0:1:1)$	$(-2:2:1)$

Example 5.15. A model for $X_0^+(239)$ is given by

$$zx^3 + (-y^2 + zy + z^2)x^2 + (-y^3 - zy^2 - z^2y)x + (y^4 + 3zy^3 + 2z^2y^2 + z^3y) = 0.$$

Using our algorithm for $p = 13$, we find that the rational points are as follows:

Δ	cusp	-7	-19	-28	-43
Point	$(1:0:0)$	$(-1:0:1)$	$(0:0:1)$	$(1:-2:1)$	$(1:-1:1)$

5.3 Genus 2 curves in Mazur's Program B

In this section, we determine the rational points on two genus 2 curves that were communicated to us by David Zureick-Brown. They arise in the work of Rouse, Sutherland, and Zureick-Brown [RSZB21] on Mazur's Program B as modular curves $X_H = X(25)/H$, where $\Gamma(25) \subset H \subset \mathrm{GL}_2(\mathbf{Z}_5)$. Both curves have the following properties:

- They each have two rational points of exponential height at most 1000, good reduction away from 5, and potentially good reduction at 5.
- Their Jacobians have real multiplication, no rational torsion and Mordell–Weil rank 2; they are both absolutely simple.
- The Galois action on the 2-torsion field is A_5, which is too large for an elliptic curve Chabauty computation.

We prove that $\#X_H(\mathbf{Q}) = 2$ for each curve X_H using quadratic Chabauty and the Mordell–Weil sieve, similar to the computation of $X_0^+(107)(\mathbf{Q})$ described in detail in Example 5.3.

Example 5.16. A suitable affine model of the curve X_{11} is given by

$$X_{11}\colon y^2 = -35x^6 + 310x^5 - 675x^4 + 750x^3 - 450x^2 + 140x - 15.$$

As in Example 5.3, we found the rather large prime $p = 61$ to be the most convenient one for our computations. We determine the height pairing on the Jacobian using divisors as in §3.3.1. The quadratic Chabauty function ρ has 62 solutions in addition to the rational ones. Applying the Mordell–Weil sieve with the primes 7, 29, 257 and 3457, we show that these are in fact not rational; to prove non-existence of rational points in the unique Weierstrass disk, we sieve with the primes 31, 61 and 191. This shows that $X_{11}(\mathbf{Q}) = \{(1, \pm 5)\}$.

Example 5.17. We use the model

$$X_{15}\colon y^2 = 5x^6 - 50x^4 - 150x^3 + 25x^2 + 90x + 25$$

with small rational points $(0, \pm 5)$. Again we run quadratic Chabauty for a fairly large prime, namely $p = 71$, resulting in 78 additional zeroes in $X(\mathbf{Q}_{71})$ that we show to be non-rational by sieving with the primes $7, 43, 83, 101$, and 1399. There is an additional final sieving to show there are no rational points in the Weierstrass disk. We conclude that $X_{15}(\mathbf{Q}) = \{(0, \pm 5)\}$.

5.4 Two curves with nontrivial local heights away from p

We compute the rational points on two genus 2 curves C_{188} and C_{161} considered in [FLS$^+$01]. In both cases, the Jacobian of C_N is an optimal quotient of $J_0(N)$, so it has real multiplication and Picard number 2. The Mordell–Weil ranks are both 2 as well, and the rational torsion subgroup is trivial. In [FLS$^+$01] empirical evidence was presented that the full conjecture of Birch and Swinnerton-Dyer holds for both Jacobians. The curves themselves have good reduction away from N.

So far, all curves whose rational points were computed via quadratic Chabauty had trivial contributions away from p, except for the bielliptic examples in [BD18, BD21]. However, for those examples it was possible to find the local contributions away from p by relating them to local heights on the elliptic quotients. In the examples presented here, we compute these contributions using Theorem 3.2. As discussed in §3.1, we do not have a general algorithm for the action induced by an endomorphism on étale cohomology. Nevertheless, we show below that we can sometimes derive sufficient information from Theorem 3.2 to pin down the local contributions precisely, by computing the local heights at $p = 3$ for the known rational points and by exploiting the bilinearity of the global height pairing.

We include these examples to illustrate the practicality of our algorithms. However, we note that the rational points on both curves can be computed by combining covering collections with elliptic curve Chabauty. For C_{188} this was pointed out to us by Nils Bruin, and for C_{161}, this computation is due to Bars, González, and Xarles [BGX21].

Example 5.18. We first consider the genus 2 curve

$$C_{188}\colon y^2 = x^5 - x^4 + x^3 + x^2 - 2x + 1\,. \tag{5.4}$$

Over $\mathbf{Z}_{47}$, it has a regular semistable model whose special fibre is a curve of genus 1 with a node, so h_{47} is trivial by Theorem 3.2. However, as we shall see, there are nontrivial contributions to the local height at 2.

The integral points on C_{188} over $\mathbf{Q}(\sqrt{-3})$ were computed in [BBBM21, Example 6.5]. In the present work, we show that

$$C_{188}(\mathbf{Q}) = \{(0,\pm 1),(1,\pm 1),(-1,\pm 1),(2,\pm 5),(4,\pm 29),\infty\}. \tag{5.5}$$

For our computations, we use the good ordinary prime $p = 3$, the base point $b = (1,1)$, and a cycle Z constructed from the Hecke operator T_3 as in (5.3).

Recall from Example 3.3 that there is a regular semistable model over $K = \mathbf{Q}_2(\sqrt[3]{2})$ and that the corresponding metric graph Γ_{reg} is a line segment. The two genus one vertices w_0 and w_1 have pre-images

$$\mathcal{U}_0 := \{P \in C_{188}(\mathbf{Q}_2) : \mathrm{ord}_2(x(P)) > 0\}\ ,\ \mathcal{U}_1 := \{P \in C_{188}(\mathbf{Q}_2) : \mathrm{ord}_2(x(P)) = 0\},$$

respectively. The set $\mathcal{U}_2 := \{P \in C_{188}(\mathbf{Q}_2) : \mathrm{ord}_2(x(P)) < 0\}$ maps to the midpoint w_2 of the line segment.

Since the function j_Γ from Theorem 3.2 is affine linear and vanishes at w_1, there is a constant κ such that for all $x \in C_{188}(\mathbf{Q}_2)$ we have

$$h_2(\mathrm{A}(P)) = m(P)\cdot\kappa,$$

where

$$m(P) = \begin{cases} 2, & \text{when } x(P) \text{ is divisible by 2,} \\ 0, & \text{when } x(P) \text{ is a 2-adic unit,} \\ 1, & \text{when } x(P) \text{ is non-integral.} \end{cases}$$

One could determine κ by further computing the trace of Z acting on the cohomology of the two genus one curves in the special fibre of the regular model described in Example 3.3. In this example, we can determine κ by computing local heights at p, as there is a unique choice of κ such that

$$h_3(\mathrm{A}(P)) + m(P)\cdot\kappa$$

satisfies the bilinearity properties of a global height. We can reduce the determination of κ to linear algebra by computing $h_3(\mathrm{A}(P))$ and the values of a basis of the space of $\mathrm{End}_0(J)$-equivariant bilinear pairings for $3 = g+1$ rational points $P \in X(\mathbf{Q})$. We find $\kappa = \frac{4}{3}\log_p(2)$.

To finish the computation of the rational points, we first solve for the zeroes of the quadratic Chabauty function ρ on the affine patch (5.4). In order to deal with the Weierstrass disk at infinity, we move the point at infinity to $(0,0)$ and repeat the computation for the resulting affine patch. We then apply the trick described in [BDM$^+$19, §5.5], changing the base point and reducing the computation of the Frobenius structure to the computation of Coleman integrals.

We find that ρ vanishes on the known rational points and that it vanishes on 13 additional $\mathbf{Q}_3$-points to precision 3^5. Upon noticing that $J(\mathbf{F}_{43}) \simeq (\mathbf{Z}/54\mathbf{Z})^2$, we show that the reductions of the corresponding cosets of $27J(\mathbf{Q})$ do not meet the image of $C_{188}(\mathbf{F}_{43})$ in $J(\mathbf{F}_{43})/27J(\mathbf{F}_{43})$. This suffices to prove (5.5).

Example 5.19. The curve C_{161} has an affine equation

$$y^2 = x^6 + 2x^4 + 6x^3 + 17x^2 + 18x + 5 = (x^3 - 2x^2 + 3x + 5)(x^3 + 2x^2 + 3x + 1).$$

As discussed in [BGX21], this is in fact a model for the modular curve $X_0^*(161) = X_0(161)/\langle w_7, w_{23}\rangle$. The curve has ten small rational points

$$\left(\frac{1}{4}, \pm\frac{209}{64}\right), (-1,\pm 1), (1,\pm 7), \left(\frac{1}{2}, \pm\frac{35}{8}\right), \infty_\pm. \tag{5.6}$$

Anticipating the need to use the Mordell–Weil sieve, we choose the prime $p = 29$ and the cycle Z corresponding to the endomorphism $4T_{29} - \mathrm{Tr}(T_{29})I_4$.

The bad primes are 7 and 23. At both of these primes, the stable model has special fibre a genus zero curve with two double points. One can show this, for instance, using the program `genus2reduction` due to Qing Liu,

now contained in `Pari/GP` or `Sage`. This (or `Magma`'s `RegularModel` package) also shows that the model over $\mathbf{Z}_{23}$ defined by the given equation is regular. Indeed, the 23-adic valuation of the discriminant is 2; therefore both singular points $(2,0)$ and $(11,0)$ on the reduction modulo 23 define regular points on this model. Hence the given equation defines a regular semistable model over $\mathbf{Z}_{23}$, and all of the $\mathbf{Q}_{23}$ points lie on a common irreducible component of a minimal regular model over $\mathbf{Z}_{23}$, so the height contribution at this prime is zero by Theorem 3.2.

At 7, the discriminant has valuation 4, so the model defined by the given equation is not regular. The singular points on the special fibre are $(1,0)$ and $(4,0)$. Blowing up once in both of these yields a semistable regular model whose special fiber consists of two genus 0 curves w_1 and w_2 that do not intersect and another genus 0 curve w_0 which reduces to the smooth locus of the stable model and which intersects w_1 and w_2 transversely in two points each, e_1 and e_2 and e_3 and e_4 respectively. This information can also be obtained from `genus2reduction` or `RegularModel`.

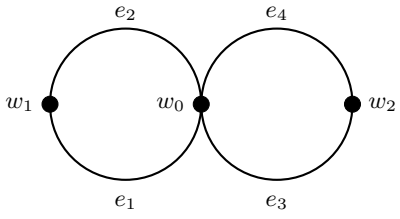

Figure 1: Dual graph of the minimal regular model of C_{161} at $\ell = 7$.

The corresponding dual graph is shown in Figure 1. We choose an orientation by designating w_0 as the source of e_1 and e_3 and as the target of e_2 and e_4. The points $\left(\frac{1}{4}, \pm\frac{209}{64}\right), (-1, \pm 1), \infty_\pm$ listed in (5.6) reduce to the component w_0. The points $(1, \pm 7)$ reduce to w_1 and the points $\left(\frac{1}{2}, \pm\frac{35}{8}\right)$ reduce to w_2. We may again use Theorem 3.2 to determine the possible values of $h_7(P)$, without computing the action of our chosen correspondence on $\mathrm{H}^1(\Gamma)$. Note that in this case, the homology $\mathrm{H}_1(\Gamma)$ is generated by $\gamma_1 = e_2 + e_1$ and $\gamma_2 = e_3 + e_4$ respectively. Since Z is trace zero on $\mathrm{H}_1(\Gamma)$, with respect to this basis, the corresponding endomorphism must be of the form $\begin{pmatrix} a & b \\ c & -a \end{pmatrix}$. Then, by Theorem 3.2, the measure μ_Z is simply given by $\frac{a}{2}(\gamma_1 - \gamma_2)$, since both edges have length 2. The image of $X(\mathbf{Q}_7)$ in Γ consists of the three vertices w_0, w_1, and w_2 and hence if we take the basepoint $(\frac{1}{4}, \frac{209}{64})$ reducing to w_0, the values of j_Γ are simply $a, 0, -a$. We solve for a using a 29-adic computation similar to the previous example, and we find that $a = -4$. Finally, we apply the Mordell–Weil sieve with $M = 4 \cdot 29^3$ and primes $199, 373, 463$ to show that the only 29-adic points in the zero set of ρ modulo 29^3 are the rational points listed in (5.6). This proves that these are indeed the only rational points on C_{161}.

5.5 The nonsplit Cartan modular curve $X_{\mathrm{ns}}^+(17)$

The modular curve

$$X := X_{\mathrm{ns}}^+(17)$$

attached to the normaliser of the non-split Cartan subgroup of level 17 has genus 6. By [DF21, §5.3], the rank of $J_{\mathrm{ns}}^+(17)(\mathbf{Q})$ is also 6. The set of rational points $X(\mathbf{Q})$ can be determined *without* computing local heights at the bad prime 17, even though these contribute nontrivially when determining $X(\mathbf{Q}_p)_2$, by choosing the correspondence Z carefully.

The curve X has a semistable model $\mathcal{X}$ over $W(\overline{\mathbf{F}}_{17})[\varpi]$ with $\varpi = (1+\zeta_{17})^{1/9}$, where $W(\overline{\mathbf{F}}_{17})$ is the ring of Witt vectors of $\overline{\mathbf{F}}_{17}$, described by Edixhoven–Parent [EP21]. Its special fibre has two irreducible components

$$\begin{aligned} C_1 &: \quad y^2 = x(x^9 + a), \qquad a \in \overline{\mathbf{F}}_{17}^\times, \\ C_2 &: \quad z^2 = w(w^3 + b), \qquad b \in \overline{\mathbf{F}}_{17}^\times, \end{aligned}$$

which have genus 4 and 1, respectively. They are smooth and intersect transversely in two points, so that the Jacobian has toric rank 1. The inertia subgroup $I \subset G_{\mathbf{Q}_{17}}$ acts via automorphisms on the special fibre of this model, and the stabiliser of the set of irreducible components is contained in $\mu_{18}(\overline{\mathbf{F}}_{17^2}) = \langle\zeta\rangle$, where the root of unity $\zeta^{18} = 1$ acts on the components by

$$\begin{array}{rcccl} \zeta & : & (x,y) & \longmapsto & (\zeta^4 x, \zeta^2 y), \\ \zeta & : & (z,w) & \longmapsto & (\zeta^{12} z, \zeta^6 w). \end{array}$$

The resulting operator $[\zeta]$ on the cohomology of these curves has characteristic polynomial

$$\begin{aligned} \det\big(1 - t[\zeta] : \mathrm{H}^1(C_1, \mathbf{Q}_p)\big) &= (t^2+t+1)(t^6+t^3+1), \\ \det\big(1 - t[\zeta] : \mathrm{H}^1(C_2, \mathbf{Q}_p)\big) &= (t^2+t+1). \end{aligned}$$

Since the Hecke action on the cohomology of X is defined over $\mathbf{Q}$, it must commute with the action of inertia, and therefore the irreducible Hecke modules of the Jacobian up to isogeny must be contained in the submodules coming from the toric part (dimension 1) and the parts where the operator $[\zeta]$ is of order 3 (dimension 2) and of order 9 (dimension 3). By the work of Chen and Edixhoven–de Smit [Che00, EdS00] the Jacobian of X admits an isogeny to the new part of the Jacobian of $X_0^+(17^2)$ equivariant for the anemic Hecke algebra. The new part of the Jacobian of $X_0^+(17^2)$ decomposes up to isogeny into irreducible factors $M_1 \times M_2 \times M_3$ of dimensions $1, 2, 3$ respectively, where M_1, M_2, M_3 are killed by the Hecke operators

$$\begin{array}{rcl} M_1 & : & (T_2 + 1) = 0, \\ M_2 & : & (T_2^2 + T_2 - 3) = 0, \\ M_3 & : & (T_2^3 - 3T_2 + 1) = 0. \end{array}$$

If we set $M = (T_2+1)(T_2^2+T_2-3)$, we find that $Z = M$ and $Z = 2M^3 + 3M^2$ are nontrivial trace zero correspondences that induce the zero endomorphisms on $H_1(\Gamma, \mathbf{Q})$ and the cohomology of C_2, so that Theorem 3.2 implies that $\mu_F = 0$, and hence the 17-adic height vanishes:

$$h_{17}(\mathrm{A}_Z(x)) = 0, \qquad \text{for all } x \in X(\mathbf{Q}_{17}).$$

In fact, starting from any generator T of the Hecke algebra (like $T = T_2$ above), one easily computes two linearly independent trace zero correspondences $Z \in \mathbf{Z}[T]$ that act trivially on the dual graph and the cohomology of C_2, which therefore likewise ensures the triviality of the associated 17-adic height.

To put these observations into action, we choose $p = 31$ and use the model of X found by Mercuri and Schoof [MS20, §6] as an intersection of six quadrics in $\mathbf{P}^5$. Our strategy for finding a suitable singular plane curve model largely follows [AAB+21]: To find a model with small coefficients, we use the Magma function `Genus6PlaneCurveModel`, and then apply an automorphism of $\mathbf{P}^2$ to ensure that there are two rational points at infinity (this speeds up the computation of the Hodge filtration (see [BDM+19, Section 4]) where one passes to a number field over which the divisor at infinity splits completely). We obtain a singular plane curve model $Q(x,y) = 0$, where

$$\begin{aligned} 5 \cdot Q(x,y) = 5y^6 &+ (24x+12)\,y^5 + \big(-495x^2 - 543x - 153\big)\,y^4 + \\ &\big(-1472x^3 - 2814x^2 - 1719x - 337\big)\,y^3 + \\ &\big(-1686x^4 - 4875x^3 - 4761x^2 - 1902x - 263\big)\,y^2 + \\ &\big(-540x^5 - 2082x^4 - 2952x^3 - 1875x^2 - 535x - 56\big)\,y + \\ &188x^6 + 534x^5 + 567x^4 + 284x^3 + 70x^2 + 7x. \end{aligned}$$

The fact that T_{31} generates the Hecke algebra can be checked from the LMFDB page for newforms of weight two, level 289, trivial character and Atkin–Lehner eigenvalue one [LMFDB]. We compute two correspondences $Z \in \mathbf{Z}[T_{31}]$ as above, and obtain a pair of power series in each residue disk, whose common zeroes to precision $O(31^{20})$ correspond to the rational points

$$\left\{\left(-\frac{4}{9}, \frac{1}{9}\right), \left(-\frac{2}{3}, -\frac{1}{3}\right), \left(-\frac{1}{2}, \frac{1}{2}\right), (0,0), (-1,0), \infty_1, \infty_2\right\} \subset X(\mathbf{Q})$$

where ∞_1 and ∞_2 are the points $(1:-1:0)$ and $(1:-\frac{1}{5}:0)$. Therefore, this must be the full set of rational points $X(\mathbf{Q})$. These were already found by Mercuri–Schoof [MS20, §6]; they are all CM points and the corresponding discriminants are $-3, -7, -11, -12, -27, -28, -163$. This proves Theorem 1.2.

Remark 5.20. It would be interesting to use the techniques of this paper to compute the rational points on $X_{\mathrm{ns}}^{+}(19)$. Mercuri and Schoof [MS20, §7] found a model for this curve as well. Nevertheless, we were unable to find a plane affine equation for this curve and a prime p, satisfying Assumption 3.10, such that it is feasible to carry out Algorithm 3.12. Difficulties arose in computing a basis of $\mathrm{H}^1_{\mathrm{dR}}(X_{\mathbf{Q}_p})$ due to the large degrees of the field extensions we encountered when applying the algorithms in [Tui17, §3].

References

AAB+21 N. Adžaga, V. Arul, L. Beneish, M. Chen, S. Chidambaram, T. Keller, and B. Wen. Quadratic Chabauty for Atkin-Lehner quotients of modular curves of prime level and genus 4, 5, 6. *ArXiv preprint*, arXiv:2105.04811, 2021. ↑2, 33.

ACKP N. Adžaga, S. Chidambaram, T. Keller, and O. Padurariu. Rational points on hyperelliptic Atkin-Lehner quotients of modular curves and their coverings, *Res. Number Theory*, 8:Art. 87, 2022. ↑2.

AM V. Arul and J. S. Müller Rational points on $X_0^+(125)$ *Expo. Math.*, to appear. ↑2.

BB12 J. S. Balakrishnan and A. Besser. Computing local p-adic height pairings on hyperelliptic curves. *IMRN*, 2012(11):2405–2444, 2012. ↑9, 10, 11, 15, 22.

BB15 J. S. Balakrishnan and A. Besser. Coleman-Gross height pairings and the p-adic sigma function. *J. Reine Angew. Math.*, 698:89–104, 2015. ↑3.

BB21 J. S. Balakrishnan and A. Besser. Errata for "Computing local p-adic height pairings on hyperelliptic curves". `http://math.bu.edu/people/jbala/cg_heights_errata.pdf`, 2021. ↑9, 15, 22.

BBBM21 J. S. Balakrishnan, A. Besser, F. Bianchi, and J. S. Müller. Explicit quadratic Chabauty over number fields. *Israel J. Math*, 243:185–232, 2021. ↑3, 16, 31.

BBM16 J. S. Balakrishnan, A. Besser, and J. S. Müller. Quadratic Chabauty: p-adic heights and integral points on hyperelliptic curves. *J. Reine Angew. Math.*, 720:51–79, 2016. ↑3.

BBM17 J. S. Balakrishnan, A. Besser, and J. S. Müller. Computing integral points on hyperelliptic curves using quadratic Chabauty. *Math. Comp.*, 86(305):1403–1434, 2017. ↑11.

BBB+21 J. S. Balakrishnan, A.J. Best, F. Bianchi, B. Lawrence, J. S. Müller, N. Triantafillou, and J. Vonk. Two recent p-adic approaches towards the (effective) Mordell conjecture. In *Regulators IV: An international conference on arithmetic L-functions and differential geometric methods*, volume 338 of *Progr. Math.*, pages 31–74. Birkhäuser Boston, Boston, MA, 2021. ↑3, 12, 21, 25, 26.

BD18 J. S. Balakrishnan and N. Dogra. Quadratic Chabauty and rational points I: p-adic heights. *Duke Math. J.*, 167(11):1981–2038, 2018. ↑3, 4, 5, 16, 30.

BD21 J. S. Balakrishnan and N. Dogra. Quadratic Chabauty and rational points II: Generalised height functions on Selmer varieties. *Int. Math. Res. Not. IMRN*, (15):11923–12008, 2021. ↑3, 9, 30.

BDM+ J. S. Balakrishnan, N. Dogra, J. S. Müller, J. Tuitman, and J. Vonk. QCMod (Magma code). `https://github.com/steffenmueller/QCMod`. ↑12, 24.

BDM+19 J. S. Balakrishnan, N. Dogra, J. S. Müller, J. Tuitman, and J. Vonk. Explicit Chabauty–Kim for the split Cartan modular curve of level 13. *Annals of Math.*, 189(3), 2019. ↑3, 4, 5, 8, 9, 12, 13, 14, 15, 16, 17, 18, 19, 24, 25, 26, 31, 33.

BDCKW18 J. S. Balakrishnan, I. Dan-Cohen, M. Kim, and S. Wewers. A non-abelian conjecture of Tate-Shafarevich type for hyperbolic curves. *Math. Ann.*, 372(1-2):369–428, 2018. ↑5.

BKK11 J. S. Balakrishnan, K. S. Kedlaya, and M. Kim. Appendix and erratum to "Massey products for elliptic curves f rank 1". *J. Amer. Math. Soc.*, 24(1):281–291, 2011. ↑3.

BT20 J. S. Balakrishnan and J. Tuitman. Explicit Coleman integration for curves. *Math. Comp.*, 89(326):2965–2984, 2020. ↑17, 18, 19, 20, 21, 22.

BC14 B. S. Banwait and J. E. Cremona. Tetrahedral elliptic curves and the local-global principle for isogenies. *Algebra & Number Theory*, 8(5):1201–1229, 2014. ↑24.

BGX21 F. Bars, J. González, and X. Xarles. Hyperelliptic parametrizations of $\mathbb{Q}$ curves. *Ramanujan J.*, 56(1):103–120, 2021. ↑30, 31.

Bes04 A. Besser. The p-adic height pairings of Coleman–Gross and of Nekovář. In *Number Theory*, volume 36 of *CRM Proc. Lect. Notes*, pages 13–25. Amer. Math. Soc., 2004. ↑9.

BMS A. Besser, J. S. Müller and P. Srinivasan. p-adic adelic metrics and Quadratic Chabauty I *Arxiv preprint*, arXiv:2112.03873, 2021. ↑3.

BO83 P. Berthelot and A. Ogus. F-isocrystals and de Rham cohomology I. *Invent. Math.*, 72:159–199, 1983. ↑15.

BD19 A. Betts and N. Dogra. The local theory of unipotent Kummer maps and refined Selmer schemes. *ArXiv preprint*, arXiv:1909.05734v2, 2019. ↑5, 6, 7.

vBHM20 R. van Bommel, D. Holmes, and J. S. Müller. Explicit arithmetic intersection theory and computation of Néron-Tate heights. *Math. Comp.*, 89(321):395–410, 2020. ↑16.

BCP97 W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system I: The user language. *J. Symb. Comp*, 24(3-4):235–265, 1997. ↑12.

Box21 J. Box. Quadratic points on modular curves with infinite Mordell-Weil group. *Math. Comp.*, 90(327):321–343, 2021. ↑25.

BS10 N. Bruin and M. Stoll. The Mordell-Weil sieve: proving non-existence of rational points on curves. *LMS J. Comput. Math.*, 13:272–306, 2010. ↑11.

CG89 R. F. Coleman and B. H. Gross. p-adic heights on curves. In *Algebraic number theory*, volume 17 of *Adv. Stud. Pure Math.*, pages 73–81. Academic Press, Boston, MA, 1989. ↑9, 11.

Che00 I. Chen. On relations between Jacobians of certain modular curves. *J. Algebra*, 231(1):414–448, 2000. ↑33.

CR91 T. Chinburg and R. Rumely. Well-adjusted models for curves over Dedekind rings *Arithmetic algebraic geometry (Texel, 1989)*, Progr. Math., 89, 3–24, 1991. ↑6.

CR93 T. Chinburg and R. Rumely. The capacity pairing *J. Reine Angew. Math.*, 434, 1993, 1–44. ↑7.

Cla03 P. L. Clark. *Rational points on Atkin-Lehner quotients of Shimura curves.* ProQuest LLC, Ann Arbor, MI, 2003. Thesis (Ph.D.)–Harvard University. ↑2.

CMSV19 E. Costa, N. Mascot, J. Sijsling, and J. Voight. Rigorous computation of the endomorphism ring of a Jacobian. *Math. Comp.*, 88(317):1303–1339, 2019. ↑15.

DR73 P. Deligne and M. Rapoport. Les schemas de modules de courbes elliptiques. *Modular Functions of one Variable II*, Proc. internat. Summer School, Univ. Antwerp 1972, Lect. Notes Math. 349, 143–316, 1973. ↑26.

DF21 N. Dogra and S. Le Fourn. Quadratic Chabauty for modular curves and modular forms of rank one. *Math. Ann.*, 380(1-2):393–448, 2021. ↑2, 13, 14, 32.

DRHS J. Duque-Rosero and S. Hashimoto and P. Spelier. Geometric Quadratic Chabauty and p-adic heights. *Arxiv preprint*, arXiv:2207.10389, 2022. ↑3.

EdS00 B. Edixhoven and B. de Smit. Sur un résultat d'Imin Chen. *Math. Res. Lett.*, (2–3):147–153, 2000. ↑33.

EL21 B. Edixhoven and G. Lido. Geometric quadratic Chabauty. *J. Inst. Math. Jussieu*, to appear, `https://doi.org/10.1017/S1474748021000244`, 2021. ↑3.

EP21 B. Edixhoven and P. Parent. Semistable reduction of modular curves associated with maximal subgroups in prime level. *Doc. Math.*, 26:231–269, 2021. ↑15, 32.

FLS+01 E. V. Flynn, G. Leprévost, E. F. Schaefer, W. A. Stein, M. Stoll, and J. L. Wetherell. Empirical evidence for the Birch and Swinnerton-Dyer conjectures for modular Jacobians of genus 2 curves. *Math. Comp.*, 70(236):1675–1697, 2001. ↑30.

Gaj22 S. Gajović. *Variations on the method of Chabauty and Coleman* Thesis (Ph.D.)–University of Groningen, 2022. `https://research.rug.nl/en/publications/variations-on-the-method-of-chabauty-and-coleman` ↑11.

Gal96 S. D. Galbraith. Equations for modular curves. *Oxford DPhil thesis*, 1996. ↑25, 28.

Gal99 S. D. Galbraith. Rational points on $X_0^+(p)$. *Experiment. Math.*, 8(4):311–318, 1999. ↑2, 25, 26, 28.

Gal02 S. D. Galbraith. Rational points on $X_0^+(N)$ and quadratic $\mathbb{Q}$-curves. *J. Théor. Nombres Bordeaux*, 14(1):205–219, 2002. ↑2, 25.

SGA7 A. Grothendieck SGA 7, exposé IX. In *Lecture Notes in Mathematics 288*, pages 313-523. Springer-Verlag, New York, 1972. ↑7.

Hol12 D. Holmes. Computing Néron-Tate heights of points on hyperelliptic Jacobians. *J. Number Theory*, 132(6):1295–1305, 2012. ↑16.

HZ02 E. W. Howe and H. J. Zhu. On the existence of absolutely simple abelian varieties of a given dimension over an arbitrary field. *J. Number Theory*, 92(1):139–163, 2002. ↑26.

Kim05 M. Kim. The motivic fundamental group of $\mathbf{P}^1\backslash\{0,1,\infty\}$ and the theorem of Siegel. *Invent. Math.*, 161:629–656, 2005. ↑3.

Kim09 M. Kim. The unipotent Albanese map and Selmer varieties for curves. *Publ. RIMS*, 45:89–133, 2009. ↑3.

Kim10 M. Kim. Massey products for elliptic curves of rank 1. *J. Amer. Math. Soc.*, 23(3):725–747, 2010. ↑3.

KT08 M. Kim and A. Tamagawa. The l-component of the unipotent Albanese map. *Math. Ann.*, 340(1):223–235, 2008. ↑4.

Lig77 G. Ligozat. Courbes modulaires de niveau 11. In *Modular Functions of One Variable V*, volume 601 of *Lecture Notes in Math.*, pages 149–237. Springer, Berlin, 1977. ↑24.

LMFDB The LMFDB Collaboration. The L-functions and modular forms database, 2021. `http://www.lmfdb.org` ↑33.

Maz77 B. Mazur. Rational points on modular curves. In *Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976)*, pages 107–148. Lecture Notes in Math., Vol. 601, 1977. ↑1.

MS20 P. Mercuri and R. Schoof. Modular forms invariant under non-split Cartan subgroups. *Math. Comp.*, 89(324):1969–1991, 2020. ↑33, 34.

Mül14 J. S Müller. Computing canonical heights using arithmetic intersection theory. *Math. Comp.*, 83(285):311–336, 2014. ↑16, 27.

Nek93 J. Nekovář. On p-adic height pairings. In *Séminaire de Théorie des Nombres, Paris 1990–1991*, pages 127–202. Birkhäuser Boston, 1993. ↑4, 9.

PY07 P. Parent and A. Yafaev. Proving the triviality of rational points on Atkin-Lehner quotients of Shimura curves. *Math. Ann.*, 339(4):915–935, 2007. ↑2.

RSZB21 J. Rouse, A. V. Sutherland, and D. Zureick-Brown. ℓ-adic images of Galois for elliptic curves over $\mathbb{Q}$ (and an appendix with J. Voight). *Forum of Math. Sigma*, 10, E62, 2022. ↑1, 30.

RZB15 J. Rouse and D. Zureick-Brown. Elliptic curves over $\mathbb{Q}$ and 2-adic images of Galois. *Res. Number Theory*, 1:Art. 12, 34, 2015. ↑1.

Sch99 V. Scharaschkin. *Local-global problems and the Brauer-Manin obstruction.* ProQuest LLC, Ann Arbor, MI, 1999. Thesis (Ph.D.)–University of Michigan. ↑11.

Ser72 J.-P. Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972. ↑1, 24.

Sik17 S. Siksek. Quadratic Chabauty for modular curves. *Arxiv preprint*, arXiv:1704.00473, 2017. ↑2.

Tui16 J. Tuitman. Counting points on curves using a map to $\mathbf{P}^1$. *Math. Comp.*, 85(298):961–981, 2016. ↑13, 14, 16, 17, 18.

Tui17 J. Tuitman. Counting points on curves using a map to $\mathbf{P}^1$, II. *Finite Fields Appl.*, 45:301–322, 2017. ↑12, 13, 14, 16, 17, 18, 19, 20, 34.

Wal11 M. Waldschmidt. On the p-adic closure of a subgroup of rational points on an Abelian variety. *Afr. Mat.*, 22(1):79–89, 2011. ↑14.

Xue09 H. Xue. Minimal resolution of Atkin–Lehner quotients of $X_0(N)$. *J. Number Theory*, 129(9):2072–2092, 2009. ↑26.

Zha93 S. Zhang. Admissible pairing on a curve. *Invent. Math.*, 112(1):171–193, 1993. ↑6.

Jennifer S. Balakrishnan
Department of Mathematics & Statistics, Boston University, 665 Commonwealth Avenue, Boston, MA 02215, USA

Netan Dogra
Department of Mathematics, King's College London, Strand, London, WC2R 2LS, UK

J. Steffen Müller
Bernoulli Institute, University of Groningen, Nijenborgh 9, 9747 AG Groningen, The Netherlands

Jan Tuitman

Jan Vonk
Mathematical Institute, Leiden University, Niels Bohrweg 1, 2333 CA Leiden, The Netherlands