BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 62, Number 2, April 2025, Pages 235–268
https://doi.org/10.1090/bull/1851
Article electronically published on February 12, 2025

OGG'S TORSION CONJECTURE: FIFTY YEARS LATER

JENNIFER S. BALAKRISHNAN AND BARRY MAZUR,
WITH AN APPENDIX BY NETAN DOGRA

Abstract. Andrew Ogg's mathematical viewpoint has inspired an increasingly broad array of results and conjectures. His results and conjectures have earmarked fruitful turning points in our subject, and his influence has been such a gift to all of us. Ogg's celebrated torsion conjecture—as it relates to modular curves—can be paraphrased as saying that rational points (on the modular curves that parametrize torsion points on elliptic curves) exist if and only if there is a good geometric reason for them to exist. We give a survey of Ogg's torsion conjecture and the subsequent developments in our understanding of rational points on modular curves over the last fifty years.

Figure 1. Andrew Ogg; photo by George M. Bergman (Archives of the Mathematisches Forschungsinstitut Oberwolfach)

Received by the editors July 24, 2023, and, in revised form, April 21, 2024, and June 1, 2024.
2020 *Mathematics Subject Classification.* Primary 11G18.

This paper expands the 45-minute talk that the second author gave at the conference at the IAS celebrating the Frank C. and Florence S. Ogg Professorship in Mathematics.

And here's just one (tiny) instance of Ogg's jovial and joyful way of thinking: As Tate and I recorded in one of our papers [72]: "Ogg passed through our town and mentioned that he had discovered a point of order 19" on the Jacobian of $X_1(13)$, allowing us to feel that that Jacobian was "not entitled to have" more than 19 points.

1. An overview

Torsion in algebraic groups—even if not in that vocabulary—has played a fundamental role since Gauss's *Disquisitiones Arithmeticae* (1801), the structure of roots of unity (torsion in the multiplicative group) being a central concern in the development of modern number theory.[1] Let K be a number field, and denote by G_K its absolute Galois group, i.e.,

$$G_K := \mathrm{Gal}(\overline{K}/K).$$

A basic question in the arithmetic of abelian varieties over number fields is to classify (up to the natural notion of isomorphism) pairs

$$(A; C \overset{\alpha}{\hookrightarrow} A(\overline{K}))$$

where

- A is a (polarized) abelian variety defined over K,
- C is a finite abelian group with a G_K-action, and
- α is a G_K-equivariant injection.

These are the three basic parameters in this general question, and you have your choice of how you want to choose the range of each of them. For example, you can:

- allow the groups C to run through all cyclic finite groups with arbitrary G_K-action; and A to range through all abelian varieties with a specified type of polarization. Equivalently, you are asking about ***K*-rational cyclic isogenies of abelian varieties**, or
- restrict to finite groups C with trivial G_K-action, in which case you are asking about ***K*-rational torsion points on abelian varieties**,
- vary over a class of number fields K—e.g., number fields that are of a fixed degree d over a given number field k, or
- fix the dimension of the abelian varieties you are considering.

If you organize your parameters appropriately you can "geometrize" your classification problem by recasting it as the problem of finding K-rational points on a specific algebraic variety.

In more technical vocabulary: you have framed a *representable moduli problem*—and the algebraic variety in question is called the *moduli space representing that moduli problem.*

Some classical examples: Modular curves. Fixing N a positive integer and sticking to elliptic curves, the moduli spaces for rational torsion points or cyclic isogenies are smooth curves defined over $\mathbb{Q}$:

$$\begin{array}{lccc} \text{torsion points of order } N: & Y_1(N) & \hookrightarrow & X_1(N) \\ & \downarrow & & \downarrow \\ \text{cyclic isogenies of degree } N: & Y_0(N) & \hookrightarrow & X_0(N). \end{array}$$

The elliptic curves defined over K *possessing a K-rational point of order N* are classified by the K-rational points of the affine curve $Y_1(N)$—and $X_1(N)$ is the smooth projective completion of $Y_1(N)$ obtained by the adjunction of a finite set of cusps.

[1]See Umberto Zannier's expository article [105], *Torsion in algebraic groups and problems which arise.*

And, similarly, the classification of elliptic curves defined over K *possessing a K-rational cyclic isogeny of degree N* is related to the K-rational points of the affine curve $Y_0(N)$, which is a coarse moduli space. The curve $X_0(N)$ is the smooth projective completion of the curve $Y_0(N)$.

The geometric formulation comes with a number of side-benefits. Here are two:

(1) If, say, the curve $X_0(N)$ is of genus 0—noting that one of the cusps (∞) is defined over $\mathbb{Q}$, it follows that there is a rational parametrization of that curve over $\mathbb{Q}$ which gives us a systematic account (and parametrization); that is, a K-rational parametrization of cyclic N-isogenies of elliptic curves—for any K.

(2) If it is of genus greater than 0, one has a $\mathbb{Q}$-rational embedding (sending the cusp ∞ to the origin)

$$X_0(N) \hookrightarrow J_0(N)$$

of the curve in its Jacobian, which allows us to relate questions about K-rational cyclic N-isogenies to questions about the Mordell–Weil group (of K-rational points) of the abelian variety $J_0(N)$.

Besides being able to apply all these resources of Diophantine techniques, there are the simple constructions that are easy to take advantage of.

For example, if you have a moduli space $\mathcal{M}$ whose K-rational points for every number field K provides a classification of your problem over K, then, say, for any prime p the set of K-rational points of the algebraic variety that is the p-th symmetric power of $\mathcal{M}$—denoted $\mathrm{Symm}^p(\mathcal{M})$—*essentially* classifies the same problem ranging over *all* extensions of K of degree p. Given a variety V over a field K, by a **degree n point (of V over K)** we mean a rational point of V over some field extension of K of degree n. The degree 2 points are known as the quadratic points.

As an illustration of this, consider cyclic isogenies of degree N and noting that the natural $\mathbb{Q}$-rational mapping

$$\mathrm{Symm}^p(X_0(N)) \quad \longrightarrow \quad J_0(N) \tag{1.1}$$

defined by

$$(x_1, x_2, \ldots, x_p) \quad \mapsto \quad \text{Divisor class of } [\sum_i x_i - p \cdot \infty]$$

has linear spaces as fibers, we get that the classification problem of all cyclic N-isogenies of elliptic curves over all number fields of degree p is geometrically related, again, to the Mordell–Weil group of $J_0(N)$ over $\mathbb{Q}$.

A particularly nice example of this strategy carried out in the case of the symmetric square Symm^2 of *Bring's curve* is in the appendix by Netan Dogra. Bring's curve is the smooth projective genus 4 curve in $\mathbb{P}^4$ defined as the locus of common zeros of the following system of equations:

$$\begin{cases} x_1 + x_2 + x_3 + x_4 + x_5 &= 0, \\ x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 &= 0, \\ x_1^3 + x_2^3 + x_3^3 + x_4^3 + x_5^3 &= 0. \end{cases} \tag{1.2}$$

It has no real points and thus no rational points. However, there are a number of points defined over $\mathbb{Q}(i)$, such as $(1 : i : -1 : -i : 0)$. The natural question is to find *all quadratic points* on Bring's curve. Dogra proves that all quadratic points are defined over $\mathbb{Q}(i)$ and produces the complete list of $\mathbb{Q}(i)$-rational points.

Section 2 concentrates on Ogg's torsion conjectures and the results that have emerged that are relevant to them. In Section 3 we review the broad uniformity conjectures (and results) that have evolved from that work. Section 4 is a discussion of the more recent method of Chabauty, Coleman, and Kim designed to compute rational points on curves by p-adic considerations; we focus specifically on the results achieved by this method for computation of rational points on specific families of modular curves.

2. Torsion and isogenies

2.1. **Ogg's torsion conjectures (1973).** Ogg's torsion conjectures taken in broad terms can be formulated in terms of "the geometrizations," as just described—i.e., in terms of $\mathbb{Q}$-rational points of modular curves—and the Mordell–Weil groups of abelian varieties (i.e., of their Jacobians).

2.1.1. $\mathbb{Q}$-*Rational torsion.*

Conjecture 1 (Ogg). *An isomorphism class $\{C\}$ of finite groups occurs as the torsion subgroup of the Mordell–Weil group of some elliptic curve (defined over $\mathbb{Q}$) if and only if the modular curve that classifies this problem is of genus zero.*[2]

Put in another way, an isomorphism class occurs if and only if it is expected to occur; i.e., if it necessarily occurs, as a consequence of the ambient geometry—this view being a continuing guiding inspiration for number theory.

By "geometry" one means the (algebraic) geometry of the curve $X_0(N)$. For example, Ogg's article [81] discusses the curious case of $X_0(37)$ which has two noncuspidal $\mathbb{Q}$-rational points, these being the images of the hyperelliptic involution (a nonmodular involution) applied to the two cusps, both cusps being $\mathbb{Q}$-rational.[3] Ogg comments:

> "As Mazur and I are inclining to the opinion that $Y_0(N)$ has no $\mathbb{Q}$-rational points except for a finite number of values of N, we are certainly interested in knowing when this sort of thing is going on, and in putting a stop to it if at all possible."

2.1.2. $\mathbb{Q}$-*rational cyclic isogenies.* There are two different proofs of Conjecture 1. A major step in one of these proofs of Conjecture 1 is the full classification of $\mathbb{Q}$-rational cyclic isogenies of prime degree; this is proved in [69].

Theorem 2.1. *Let N be a prime number such that some elliptic curve over $\mathbb{Q}$ admits a $\mathbb{Q}$-rational N-isogeny. Then*

$$N = 2, 3, 5, 7, 13 \text{ (the genus zero cases)}$$

[2]A form of this conjecture was made by Beppo Levi in his 1908 ICM address in Rome. See [93], which gives a wonderful account of the story of Levi's engagement with (and his important results about) the arithmetic of elliptic curves—all this being even before Mordell proved that the group of rational points of an elliptic curve over $\mathbb{Q}$ is finitely generated. Levi considers the tactic of producing multiples of a rational point on an elliptic curve $\{n \cdot P\}$ $n = 1, 2, 3, \ldots$ a "failure" if it loops finitely—i.e., if P is a torsion point; his aim is to classify such "failures."

[3]See Section 4.4.

or

$$N = 11, 17, 19, 37, 43, 67, \textit{ or } 163.$$

This result was followed by a sequence of papers of M. A. Kenku [55–58] that extends the classification to cyclic isogenies of any degree.

Theorem 2.2. *The $\mathbb{Q}$-rational cyclic isogenies of degree N of elliptic curves defined over $\mathbb{Q}$ only occur—and do occur—if $1 \leq N \leq 19$ or if $N = 21, 25, 27, 37, 43, 67,$ or 163.*

Following in the spirit of Ogg's original view of torsion points, *all* of these N-isogenies have "geometric reasons" for existing; e.g., the 37-isogenies come by applying the hyperelliptic involution (it is nonmodular!) to the cusps of $X_0(37)$.

2.1.3. *Rational torsion points on the Jacobians of modular curves.* Noting that the cusps of $X_0(N)$ map to torsion points of its Jacobian, $J_0(N)$, denote by $C_0(N) \subset J_0(N)_{\text{tors}} \subset J_0(N)$ the subgroup generated by those cusps.

$$\begin{array}{ccc} \text{Cusps in } X_0(N) & & \\ \downarrow & \searrow & \\ C_0(N) & & X_0(N) \\ \downarrow & & \downarrow \\ J_0(N)_{\text{tors}} & \hookrightarrow & J_0(N) \end{array}$$

We have another, seemingly quite different type of conjecture.

Conjecture 2. *Let N be a prime number. We have:*

$$C_0(N) = J_0(N)_{\text{tors}}(\mathbb{Q}) \subset J_0(N)(\mathbb{Q}).$$

Put in another way, there are no "unexpected" $\mathbb{Q}$-rational torsion points in $J_0(N)$: they all come from cusps.

Conjectures 1 and 2 are known. For Conjecture 1, see [68, Theorem 8] and [69, Theorem 2]. For Conjecture 2, see [69, Theorem 1]. (Also see the broad survey of rational torsion results in Andrew Sutherland's work [98].) That these conjectures are interlinked is a long story, as we discuss in Section 2.2.

2.1.4. *Conjecture* 1. Letting C_n denote the cyclic group of order n, the complete list of possible (isomorphism classes of) finite groups that occur as torsion subgroups of the Mordell–Weil group of $\mathbb{Q}$-rational points of elliptic curves are

- C_n with $1 \leq n \leq 10$, and also C_{12}, and
- the direct sum of C_2 with C_{2m}, for $1 \leq m \leq 4$.

All these torsion groups occur infinitely often over $\mathbb{Q}$, since the corresponding modular curves are all genus zero curves possessing a rational point.[4]

Remark 2.3. Thanks to the work of Loïc Merel [75], Joseph Oesterlé and Pierre Parent [89], and others, we have neat explicit upper bounds for the order of torsion points on elliptic curves over number fields of degree d. For surveys of this work, see [32] and [98].

[4]See [100] where it is proved that each of these groups appears as a possible torsion group over any quadratic field.

2.2. **The connection between algebraic torsion on elliptic curves and rational torsion on abelian varieties related to elliptic curves.** The easiest way to explain this is to follow the ideas of [69, Proof of Conjecture 1], rather than the ideas in the earlier and quite different proof in [67].

To set things up, let N be a prime number such that $X_0(N)$ is of genus greater than 0 and let $J_{/\mathbb{Z}}$ be the Néron model of the Jacobian of $X_0(N)$ over $\mathbb{Q}$. Let

$$X_0(N)^{smooth}_{/\mathbb{Z}} \overset{\iota}{\hookrightarrow} J_{/\mathbb{Z}}$$

be the smooth locus of the Zariski closure of $X_0(N)_{\mathbb{Q}}$ in $J_{/\mathbb{Z}}$, the embedding being defined by sending the cusp ∞—viewed as the $\mathbb{Z}$-valued section $\mathbf{e} \in X_0(N)_{/\mathbb{Z}}$—to the "origin section" of $J_{/\mathbb{Z}}$.

An elliptic curve E with a cyclic isogeny of degree N over $\mathbb{Q}$ is represented by a *noncuspidal* Spec $\mathbb{Z}$-valued section, $\mathbf{x}$, of $X_0(N)^{smooth}_{/\mathbb{Z}}$ and hence (via ι) also of the Néron model $J_{/\mathbb{Z}}$ of the Jacobian of $X_0(N)$ over $\mathbb{Q}$.

Suppose that such a rational point $\mathbf{x}$ exists and denote by $\bar{\mathbf{x}}$ its image under the Atkin–Lehner involution $w_n : X_0(N) \to X_0(N)$, the involution that exchanges the two cusp sections $\mathbf{0}$ and ∞ of $X_0(N)$. Neither $\mathbf{x}$ nor $\bar{\mathbf{x}}$ are cuspidal sections of $X_0(N)^{smooth}_{/\mathbb{Z}}$. Articles [68] and [69] construct and discuss a specific smooth group scheme $A_{/\mathbb{Z}}$ that is an optimal quotient[5] of $J_{/\mathbb{Z}}$ for which these two properties are proven:

(1) The generic fiber $A_{\mathbb{Q}}$ of $A_{\mathbb{Z}}$ is an abelian variety with *finite* Mordell–Weil group—i.e., $A(\mathbb{Q})$ consists of rational torsion—and hence the image under f of any $\mathbb{Z}$-valued section of $X_0(N)^{smooth}_{/\mathbb{Z}}$ is either trivial, or else generates a cyclic finite flat subgroup of $A_{/\mathbb{Z}}$; and

(2) The following diagram

$$\begin{array}{ccccc} \mathbf{x} & \longrightarrow & X_0(N)^{smooth}_{/\mathbb{Z}} & \hookrightarrow & J_{/\mathbb{Z}} \\ & \searrow & & \searrow^{f} & \downarrow \\ \mathbf{e} & \longrightarrow & X_0(N)^{smooth}_{/\mathbb{Z}} & \xrightarrow{f} & A_{/\mathbb{Z}} \end{array}$$

has the property that

(i) the mapping $f : X_0(N)^{smooth}_{/\mathbb{Z}} \longrightarrow A_{/\mathbb{Z}}$ is a formal immersion along the cuspidal section $\mathbf{e}$, and

(ii) the diagram

$$\begin{array}{ccc} X_0(N) & \xrightarrow{f} & A \\ \downarrow{\scriptstyle w_N} & & \downarrow{\scriptstyle -1} \\ X_0(N) & \xrightarrow{f} & A \end{array}$$

commutes, where "-1" denotes the involution $z \mapsto z^{-1}$.

So, by (i), f is a formal immersion along both cusp sections. It follows that the image $\alpha := f(\mathbf{x}) \in A(\mathbb{Z})$ is either

- the section defining the origin in the group scheme $A_{/\mathbb{Z}}$, or else

[5]The group scheme A is the relevant *Eisenstein quotient*—cf. [69]. The term "optimal quotient" means that the kernel of $J_{/\mathbb{Z}} \to A_{/\mathbb{Z}}$ is a connected group scheme.

- is the generating section of a (nontrivial) cyclic finite flat subgroup scheme over $\mathbb{Z}$, call it $\mathcal{G}_{/\mathbb{Z}} \subset A_{/\mathbb{Z}}$.

  By the classification of such group schemes we have that either $\mathcal{G}_{/\mathbb{Z}}$ is a constant (nontrivial) group scheme, or else $\mathcal{G}_{/\mathbb{Z}} \simeq \mu_2$ ($\mu_2 \subset \mathbb{G}_m$ being the kernel of multiplication by 2 in the multiplicative group scheme $\mathbb{G}_m$).

These possibilities also hold, of course, for the "conjugate section" $\bar{\alpha} := f(\bar{\mathbf{x}}) \in A(\mathbb{Z})$: it is either the trivial section or it generates a finite flat group scheme $\bar{\mathcal{G}}_{/\mathbb{Z}} \subset A_{/\mathbb{Z}}$ that is either a constant group scheme or μ_2.

Lemma 2.4. *Neither α nor $\bar{\alpha}$ are the trivial section of $A_{/\mathbb{Z}}$.*

Proof. Since f is a formal immersion along the cuspidal sections if α or $\bar{\alpha}$ were the trivial section we would be led to a contradiction, as illustrated by the following diagram (taken from [69, p. 145]): in that the image of the two depicted sections would converge onto the origin section of A contradicting formal smoothness along $\mathbf{e}$. □

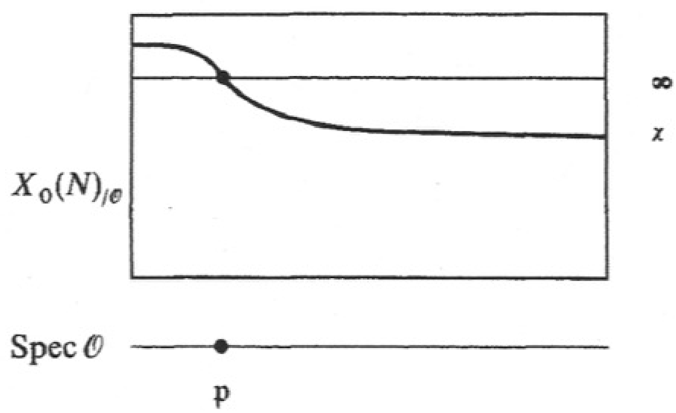

FIGURE 2. Contradiction: *Intersection with the trivial section.*

So α and $\bar{\alpha}$ are generators of nontrivial group schemes $\mathcal{G}$ and $\bar{\mathcal{G}}$, respectively, these being either constant or μ_2.

- If $\mathcal{G}$ and $\bar{\mathcal{G}}$ are constant group schemes, then α and $\bar{\alpha}$ are sections of A over $\mathbb{Z}$ disjoint (as schemes) from the trivial section of A and therefore $\mathbf{x}$ and $\bar{\mathbf{x}}$ are disjoint (as schemes) from the cuspidal sections of $X_0(N)_{/\mathbb{Z}}$. It follows that the elliptic curves E and $\bar{E}$ that are classified by $\mathbf{x}$ and $\bar{\mathbf{x}}$ have *potentially good reduction everywhere.*
- And if α or $\bar{\alpha}$ generates a subgroup isomorphic to μ_2, since μ_2 is étale outside the prime 2 it follows that E or $\bar{E}$ would have *potentially good reduction except for the prime* 2.

Even though this is just the start of a sketch of [69, Proof of Conjecture 1], from what we have just described, we can prove the following theorem.

Theorem 2.5. *The only prime numbers N for which there exist elliptic curves over $\mathbb{Q}$ with rational torsion points of order N are:*

$$N = 2, 3, 5, 7.$$

Proof. First, note that $X_1(N)$ is of genus 0 for $N = 2, 3, 5, 7$, so there are infinitely many elliptic curves with rational torsion points of order N for these primes. That list of primes *and* 13 are precisely the primes for which $X_0(N)$ is of genus 0. Since the curious prime $N = 13$ is taken care of by [72], where it is proven that there are no rational points of order 13 on elliptic curves over $\mathbb{Q}$, to prove the theorem we may suppose N to be different from $N = 2, 3, 5, 7, 13$; equivalently, that $X_0(N)$ is of genus greater than 0, so the discussion above applies.

In particular, we assume that E is an elliptic curve over $\mathbb{Q}$, of potential good reduction away from $p = 2$, and possessing a rational point of order $N = 11$ or $N \geq 17$, where N is a prime. Since it has such a rational point, the Néron model of E over $\mathbb{Z}$ contains a constant subgroup scheme $\mathcal{Z}$ isomorphic to $\mathbb{Z}/(N \cdot \mathbb{Z})$.

For p, a prime, let E_p denote the fiber at the prime p of the Néron model of E, so E_p is a group (scheme) of finite order over the prime field $\mathbb{F}_p$. Since the specialization of $\mathcal{Z}$ to E_p defines N distinct $\mathbb{F}_p$-rational points of E_p it follows that

$$N \text{ divides } |E_p(\mathbb{F}_p)|. \tag{2.1}$$

If $p > 2$, since E is of potentially good reduction, in the terminology of the theorem of Kodaira and Néron (cf. [97, Appendix C, Section 15, Table 15.1 and Theorem 15.2]) we have that E_p is not of multiplicative type—i.e., of type I_ν or I_ν^* for any $\nu > 0$. So, either

- p is a prime of good reduction for E, or
- it is of additive reduction.

If E has additive reduction at p (i.e., the Néron fiber at p is of one of the types II, III, IV, or I_0^*, II^*, III^*, or IV^*; see [97, Table 15.1]) then E_p is an extension of the additive group $\mathbb{G}_a$ over $\mathbb{F}_p$ by a finite group of order ≤ 4. In particular $|E_p(\mathbb{F}_p)|$ is divisible by p and is $\leq 4p$. It follows that Equation (2.1), applied to the prime $p = 3$, already shows that E cannot have additive reduction at $p = 3$ for the primes N we are considering, so it must have good reduction—i.e., be an elliptic curve—at $p = 3$. But since any elliptic curve over $\mathbb{F}_3$ has at most seven $\mathbb{F}_3$-rational points, we see by (2.1) that N is either 2, 3, 5, or 7. □

A significantly more detailed outline of the proof of Conjecture 1 is given as [69, Steps 1–4, pp. 132–33]—the *full proof* itself being in the body of that paper.

3. Boundedness of torsion and isogenies in more general contexts

Conjecture 1, having been completely resolved in the case of elliptic curves, has inspired more general uniform boundedness expectations for rational points. E.g., for abelian varieties A over number fields K; conjectures that the order of the torsion group of an abelian variety over a number field can be bounded in terms of the dimension of the variety and the number field; and still stronger versions: that the torsion is bounded in terms of the dimension of the variety and the degree of the number field.

Moreover, it is striking how few additional isomorphism classes of K-rational torsion subgroups of elliptic curves can occur in elliptic curves over quadratic and cubic number fields K.

3.1. Torsion on elliptic curves over quadratic and cubic number fields.

Theorem 3.1 (Momose, Kenku, and Kamienny [44–49, 53, 54, 58–60, 77, 78])**.** *Let K range through all quadratic number fields, and E all elliptic curves over these fields. Then the torsion subgroup $E(K)_{\text{tors}}$ of $E(K)$ is isomorphic to one of the following 26 groups:*

- *C_n for $1 \leq n \leq 18$, $n \neq 17$,*
- *the direct sum of C_2 with C_{2m} for $1 \leq m \leq 6$,*
- *the direct sum of C_3 with C_{3m} for $m = 1, 2$,*
- *$C_4 \oplus C_4$.*

Theorem 3.2 (Derickx, Etropolski, Van Hoeij, Morrow, and Zureick-Brown [33])**.** *Let K range through all cubic number fields and E all elliptic curves over these fields. Then the torsion subgroup $E(K)_{\text{tors}}$ of $E(K)$ is isomorphic to one of the following 26 groups:*

- *C_n for $1 \leq n \leq 18$, $n \neq 17$,*
- *the direct sum of C_2 with C_{2m} for $1 \leq m \leq 7$,*
- *C_{20}, C_{21}.*

There exist infinitely many $\mathbb{Q}$-isomorphism classes for each such torsion subgroup except for C_{21}. In this case, the base change of the elliptic curve with LMFDB label 162.c3 to $\mathbb{Q}(\zeta_9)^+$ is the unique elliptic curve over a cubic field K with K-rational torsion group isomorphic to C_{21}.

3.1.1. *Conjecture* 2 *expanded and related to cuspidal subgroups.*

- The order of the $C_0(N)$ had been computed for square-free N thanks to Kubert and Lang [64] and Takagi [99]. In this case (i.e., N square-free) the set of cusps are $\mathbb{Q}$-rational.
- Ohta [86, 87] has proved a generalization of this conjecture in the context of square-free N. That is, he proved that the p-primary parts of $J_0(N)_{\text{tors}}(\mathbb{Q})$ and of $C_0(N)$ are equal for $p \geq 5$ and $p = 3$ if 3 does not divide N.

  Related to this, see [66], [30], [104], [90], and [91]. And very recently the PNAS article [92] *Another look at rational torsion of modular Jacobians* by Ken Ribet and Preston Wake appeared, giving another approach to this issue.
- In the more general context of N not square-free, the cuspidal subgroup of $J_0(N)$ may not consist entirely of rational points; nevertheless, we get the following.

Conjecture 2^***.**

$$J_0(N)_{\text{tors}}(\mathbb{Q}) = C_0(N)(\mathbb{Q}) \subset C_0(N).$$

3.1.2. *Conjecture* 2 *further expanded.* Let X be a modular curve (over $\mathbb{Q}$) and $\mathcal{J}$ the Jacobian of X. Let

$$\mathcal{C} \subset \mathcal{J}$$

be the finite étale subgroup scheme of $\mathcal{J}$ generated by the cusps. Let $K/\mathbb{Q}$ be the field cut out by the action of Galois on $\mathcal{C}$. Thus there is an exact sequence

$$0 \to \mathrm{Gal}(\overline{\mathbb{Q}}/K) \to \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(\mathcal{C}(\overline{\mathbb{Q}})).$$

Define the *cuspidal defect* of X to be the cokernel of

$$\mathcal{C}(\overline{\mathbb{Q}}) = \mathcal{C}(K) \hookrightarrow \mathcal{J}(K)_{\text{tors}}. \tag{3.1}$$

Conjecture 2^{**}**.** *Let X be either $X_0(N)$ or $X_1(N)$ for some $N \geq 1$. The "cuspidal defect" of X is trivial.*

3.2. **Remarkable "Diophantine stability".**

Definition 3.3. Let L/K be an extension of (number) fields, and V an algebraic variety defined over K. Denote by $V(K)$ the set of K-rational points of V. Say that V is **Diophantine stable** for L/K or L/K is **Diophantine stable** for V if the inclusion $V(K) \hookrightarrow V(L)$ is an isomorphism, i.e., *if V acquires no new rational points after passing from K to L.*

Note that Theorem 3.1 tells us the following corollary.

Corollary 3.4. *For all but finitely many positive numbers N, the curve $Y_1(N)$ (over $\mathbb{Q}$) is Diophantine stable for* ***all*** *quadratic extensions $L/\mathbb{Q}$.*

This is striking and suggests that Diophantine stability is a common feature.[6] Consider the following theorem.

Theorem 3.5 ([70, Theorem 1.2])**.** *Suppose A is a simple abelian variety over K and all $\overline{K}$-endomorphisms of A are defined over K. Then there is a set $\mathcal{S}$ of rational primes with positive density such that for every $\ell \in \mathcal{S}$ and every $n \geq 1$, there are infinitely many cyclic extensions L/K of degree ℓ^n such that $A(L) = A(K)$.*

If A is an elliptic curve without complex multiplication, then $\mathcal{S}$ can be taken to contain all but finitely many rational primes.

And this is surely not the last word regarding the extent of Diophantine stability, specifically if the base field K is $\mathbb{Q}$ and if $A = E$, an elliptic curve over $\mathbb{Q}$. We conjecture that any such E is Diophantine stable for all but finitely many Galois extensions of prime degree greater than 5.

3.3. ***"Expected"*** **and** ***"unexpected"*** **L-rational cyclic isogenies for L ranging through quadratic fields.**

What about uniformity results regarding cyclic N-isogenies of elliptic curves ranging over *all* quadratic fields? This question has been addressed in [15] and generalized to arbitrary number fields in [13].

One source of uniformity theorems consists of consequences of a general theorem of Faltings.

Theorem 3.6. *Let A be an abelian variety defined over a number field L. Any closed subvariety of A defined over L which is the Zariski-closure of its set of L-rational points is a finite union of translates of abelian subvarieties of A.*

This was first proved by Faltings [37] following [36]; see also [74]. Techniques of [36] have, as their starting point, Vojta's proof [102] of the classical Mordell conjecture; see also [103]. For further discussion of this in the context of generalization(s) of the classical Mordell conjecture—with references listing the people who also worked on this—see [73].

A corollary of a theorem of Faltings combined with [42] is the following.

Corollary 3.7 (Faltings, Harris and Silverman)**.** *Let K be a number field and X a curve defined over K. Then X is Diophantine stable for all but finitely many quadratic extensions L/K unless X is*

[6]Filip Najman suggested that one might add a comment that the Diophantine Stability phenomenon of Corollary 3.4 holds more generally over number fields of any degree, given the results referred to in Remark 2.3.

- *of genus* 0 *or* 1*, or*
- *hyperelliptic or bielliptic (over* K*).*[7]

Proof. Assume that X is not of genus 0 or 1, or hyperelliptic or bielliptic. So the genus of X is ≥ 3. Let $\mathrm{Div}^0(X)$ denote the group of divisors of degree zero in X; let $A := \mathrm{Pic}^0(X)$ and consider the natural diagram

$$\begin{array}{ccc} \mathrm{Symm}^2(X) & \xrightarrow{\ \iota\ } & \mathrm{Div}^0(X) \\ & \searrow^{j} & \downarrow \pi \\ & & A \end{array}$$

where

- for $\{x_1, x_2\} \in \mathrm{Symm}^2(X)$ define
$$\iota : \{x_1, x_2\} \mapsto [x_1] + [x_2] - 2 \cdot [0] \text{ in } \mathrm{Div}^0(X),$$
and
- for $D \in \mathrm{Div}^0(X)$ define
$$\pi : D \mapsto \text{ its linear equivalence class in } \mathrm{Pic}^0(X) = A.$$

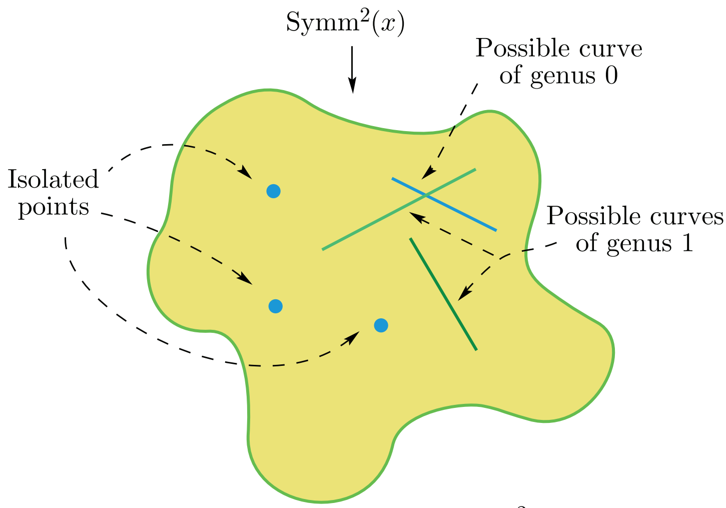

FIGURE 3. Types of rational points on $\mathrm{Symm}^2(X_0(N))$—ignoring the possible existence of abelian surfaces.

Noting that the connected components of the fibers of π and of j are (essentially, by definition) rational varieties—and that since X is assumed to be nonhyperelliptic, $\mathrm{Symm}^2(X)$ contains no rational curve—it follows that we have an injection $j : \mathrm{Symm}^2(X) \hookrightarrow A$. Let $W \subset A$ denote the image of $\mathrm{Symm}^2(X)$ in A (under the injection j). Since X is of genus ≥ 3, W is a proper subsurface in A. If it contained an elliptic curve, then X would be bielliptic [42], but since that is not the case, W contains no (positive-dimensional!) abelian subvarieties—so by Faltings's theorem

[7] See also the discussion and [43, Theorem 1.3], which handles the case when X is a double cover of an elliptic curve of positive rank.

it has only finitely many K-rational points, establishing the corollary. (Compare with [43, Theorem 1.3].) □

3.3.1. *Isolated quadratic points.* Call the set of quadratic points of X that are not among (infinite) systems of parametrized quadratic points **isolated points**. (See [20, Definition 4.1] and [101, Definition 3.1] for the precise definitions and for important relevant discussion. See also [42, 43].)

Infinite systems of parametrized quadratic points deserve to be called "expected quadratic points (over K) in X" given the geometry of the situation.

But when $X = X_0(N)$ for some N and $K = \mathbb{Q}$ there may also be a few other points of $X_0(N)$ over quadratic imaginary fields $\mathbb{Q}(\sqrt{d})$ of class number 1; i.e.,

$$d = -1, -2, -3, -7, -11, -19, -43, -67, -163$$

that deserve the title "expected". Namely, if E is an elliptic curve over $\mathbb{Q}$ that is CM with CM field $K := \mathbb{Q}(\sqrt{d})$ (with d in the above list), then for any positive integer N with the property that all of its prime divisors are (unramified and) split in K, E has a K-rational cyclic isogeny of degree N; hence it is classified by a K-rational point of $X_0(N)$. Such a point is therefore also "expected".

3.3.2. *Sporadic quadratic points.*

Definition 3.8. Call a quadratic point of $X_0(N)$ **sporadic (quadratic)**[8] if

- it is not a cusp; and
- *is* isolated; in particular,
  - if it is *not* the inverse image of a $\mathbb{Q}$-rational point in $\mathbb{P}^1$ via a hyperelliptic covering (i.e., a degree 2 mapping $X_0(N) \to \mathbb{P}^1$), in the case where $X_0(N)$ is hyperelliptic, and
- is not a point of $X_0(N)$ classifying a CM elliptic curve and cyclic isogeny of degree N as described above.

See Figure 3 for an illustration of these points.

Conjecture 3.9. *Ranging over all curves $X_0(N)$ for $N \in \mathbb{Z}_{\geq 1}$ there are only finitely many sporadic quadratic points.*

Surely all of us agree with the spirit of the quotation of Ogg's view regarding rational torsion in Section 2.1. That is, we are interested "in knowing when this [sporadic quadratic points] sort of thing is going on, and in putting a stop to it if at all possible."

Thanks to the recent work of a number of people, the sporadic quadratic points of all of the curves $X_0(N)$ that are hyperelliptic or bielliptic have been computed, as we will discuss in the next section.

Sheldon Kamienny made the following comment:

> "*The existence of sporadic points always left me scratching my head. Do they fit into a framework, or is it just nature being unkind?*"

3.4. **Sporadic quadratic points on hyperelliptic $X_0(N)$.** A classical theorem of Ogg [81] gives the nineteen values of N for which $X_0(N)$ is hyperelliptic (we take

[8] Note that this differs from the concept *sporadic* given in [20, Definition 4.1(4)].

hyperelliptic to require that the genus is > 1).

N:	**22**	23	**26**	**28**	29	**30**	31	**33**	**35**	**37**
genus:	2	2	2	2	2	3	2	3	3	2

N:	**39**	**40**	41	46	47	**48**	**50**	59	71
genus:	3	3	3	5	4	3	2	5	6

The levels N that appear in boldface above are those values of N such that $X_0(N)$ is bielliptic as well as hyperelliptic. All sporadic quadratic points for any of those modular curves $X_0(N)$ (except for $X_0(37)$) have been computed by Peter Bruin and Filip Najman in their article [23] (which has other interesting results as well). The case of $X_0(37)$ is taken care of in Josha Box's paper [21, Section 4], in which all sporadic quadratic points have also been computed for the curves $X_0(N)$ with $N = 43, 53, 61, 65$, these being bielliptic curves covering elliptic curves of positive Mordell–Weil rank.

Proposition 3.10 (Bars [15])**.** *These are the values of N for which $X_0(N)$ is of genus > 1 and bielliptic (over $\mathbb{Q}$).*

Table 1. Values of N for which $X_0(N)$ is of genus > 1 and bielliptic (over $\mathbb{Q}$)

22	26	28	30	33	34	35	37	38	39	40	42	43	44	45	48	50
51	53	54	55	56	60	61	62	63	64	65	69	72	75	79	81	83
89	92	94	95	101	119	131										

Until *very recently*, there remained a dozen entries in Table **??** for which we did not know the set of their isolated quadratic points. Thanks to Filip Najman and Borna Vukorepa [79], we now have computation of the isolated quadratic points for all bielliptic curves $X_0(N)$ (as we also do for all hyperelliptic $X_0(N)$).

3.5. **Exceptional quadratic points.** Let N be prime, and $w_N\colon X_0(N) \to X_0(N)$ the Atkin–Lehner involution. This involution is given by sending a pair (representing a point in $X_0(N)$)

$$(E, C_N \overset{\alpha}{\hookrightarrow} E)$$

—consisting of an elliptic curve E and C_N a cyclic subgroup of order N—to the pair

$$(E', C'_N \overset{\alpha'}{\hookrightarrow} E').$$

Here, $E' := E/C_N$ and $C'_N := E[N]/C_N$ (where $E[N]$ is the kernel of multiplication by N in E).

Forming the quotient

$$X_0^+(N) := X_0(N)/\text{action of } w_N,$$

we get the double cover

$$X_0(N) \xrightarrow{\pi} X_0^+(N).$$

Definition 3.11. For N an integer where $X_0^+(N)$ is of genus > 1,

(1) call a $\mathbb{Q}$-rational point of $X_0^+(N)$ **exceptional** if it is neither a cusp nor a point classifying a CM elliptic curve;
(2) call a quadratic point P of $X_0(N)$ **exceptional** if it is not defined over $\mathbb{Q}$ (i.e., it is an honest quadratic point) and the image of P in $X_0^+(N)$ is an exceptional $\mathbb{Q}$-rational point.

Exceptional points deserve the adjective, since they have the intriguing structure of a duo of cyclic N-isogenies:

$$E \xleftrightarrow{N} E' \qquad \text{and} \qquad E' \xleftrightarrow{N} E.$$

This structure can also be combined into a single abelian surface defined over $\mathbb{Q}$:

$$A := E \times E'$$

endowed with an endomorphism

$$\text{“}\sqrt{N}\text{”} : (x, y) \mapsto (\alpha'(y), \alpha(x)).$$

What tools do we have to compute the exceptional $\mathbb{Q}$-rational points on $X_0^+(N)$?

4. The method of Chabauty, Coleman, and Kim

The classical method of Chabauty and Coleman (see Section 4.2) computes a usable bound for the number of rational points on a curve X (of genus > 1) provided that the rank r of the Mordell–Weil group of the Jacobian of X is strictly less than its genus g.

But the Birch and Swinnerton-Dyer conjecture predicts that (for N prime) the rank $r_0^+(N)$ of $J_0^+(N)(\mathbb{Q})$, the Mordell–Weil group of the Jacobian of $X_0^+(N)$, is greater than or equal to $g_0^+(N)$, the genus of $X_0^+(N)$. So this classical method cannot be brought to bear here.

Computationally, we have many examples where there is actual equality:

$$r_0^+(N) = g_0^+(N).$$

(Indeed, this is true for all $N < 5077$ for which $g_0^+(N) > 1$.) Happily, for exactly such cases—i.e., for curves X of genus > 1 with $r = g$—we have the more recent quadratic Chabauty–Coleman–Kim method that offers a new approach to compute the set of all $\mathbb{Q}$-rational points.[9] For example, see [6–9] (and Section 4.3). Indeed, there are also two new viewpoints on quadratic Chabauty: the geometric perspective of Edixhoven and Lido [34] and the (p-adic) Arakelov theoretic one of Besser, Müller, and Srinivasan [16]. We will say more about these in the following section.

The list of curves $X_0^+(N)$ of genus 2 or 3 with N prime is a result of Ogg. We have the following theorem.

Theorem (Ogg). For N prime, $X_0^+(N)$ is of genus 2 if and only if

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

and it has genus 3 if and only if

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

[9] We think it is reasonable to conjecture that the average value of the ratios

$$\frac{r_0^+(N)}{g_0^+(N)}$$

is 1; e.g., as N ranges through prime values; are these ratios bounded?

Elkies and Galbraith [38] found exceptional rational points on $X_0^+(N)$ for $N = 73, 91, 103, 191$ and $N = 137, 311$ (which are of genus 4). In [8], it was shown that the only prime values of N with $X_0^+(N)$ of genus 2 or 3 that have an exceptional rational point are $N = 73, 103, 191$ (all genus 2). In particular, for prime N, if $X_0^+(N)$ is of genus 3, it has no exceptional rational points. Adžaga, Arul, Beneish, Chen, Chidambaram, Keller, and Wen [2] showed that the only prime values of N with $X_0^+(N)$ of genus 4, 5, or 6 that have an exceptional rational point are $N = 137$ and 311. Thus, for all of the above values of N, we have a complete understanding of the exceptional quadratic points on $X_0(N)$.

We will briefly discuss the work of [2] on the genus 4 curve $X_0^+(311)$. Using the canonical embedding, a model for $X_0^+(311)$ is given by the following equations in $\mathbb{P}^3$:

$$X^2 + WY - 2XY + 2Y^2 + 7XZ - 8YZ + 13Z^2 = 0,$$

$$\begin{aligned} WX^2 - 2WXY + X^2Y - WY^2 - XY^2 - 2Y^3 + W^2Z + 6WXZ \\ - X^2Z - WYZ + 5XYZ + 4Y^2Z + 7WZ^2 - 4XZ^2 - 2Z^3 = 0. \end{aligned}$$

Using quadratic Chabauty (see Section 4.3) at $p = 5$ on a plane model, they show that there are precisely five rational points on the curve.

Table 2. There are five rational points on the curve using quadratic Chabauty at $p = 5$ on a plane model.

rational point on $X_0^+(311)$	type of point
$(1\colon 0\colon 0\colon 0)$	cusp
$(1\colon -1\colon -1\colon 0)$	CM, $D = -11$
$(1\colon 2\colon -1\colon -1)$	CM, $D = -19$
$(2\colon 0\colon -1\colon 0)$	CM, $D = -43$
$(6\colon 8\colon -1\colon -2)$	exceptional

Galbraith [38] had earlier computed that the j-invariant of the $\mathbb{Q}$-curve corresponding to the exceptional point is

$$\begin{aligned} j = {} & 31244183594433270730990985793058589729152601677824000000 \\ & \pm 15658105389980517153973396894921950350775512678400000\sqrt{39816211853}. \end{aligned}$$

See also the survey article [40] (and [38, 39]) in which exceptional points found by Elkies and Galbraith are defined and studied in the context of $\mathbb{Q}$-curves; and for the list of the seven known exceptional N-isogenies, these being rational over a quadratic field of discriminant Δ in Table 3.

TABLE 3. Seven known exceptional N-isogenies, which are rational over a quadratic field of discriminant Δ.

N	g	Δ
73	2	-127
91	2	$-3 \cdot 29$
103	2	$5 \cdot 557$
125	2	509
137	4	-31159
191	2	$61 \cdot 229 \cdot 145757$
311	4	$11 \cdot 17 \cdot 9011 \cdot 23629$

By the work of [2, 4, 5, 7, 8] this gives a complete list of exceptional isogenies arising from rational points on the curves $X_0^+(N)$ of level N and genus at most 6. Are these the only exceptional isogenies?

4.1. **The method of Chabauty.** The aim of this classical method is to prove finiteness of the set of $\mathbb{Q}$-rational points of a curve X of genus $g > 1$ under the assumption that the rank r of the Mordell–Weil group of the Jacobian J of X is small; specifically, if it is strictly less than g.

One can assume that X has at least one $\mathbb{Q}$-rational point, for otherwise the job is done. Choosing a rational point $b \in X(\mathbb{Q})$, form the Abel–Jacobi embedding

$$\begin{aligned} i_b : X &\to J \\ P &\mapsto [(P) - (b)]. \end{aligned}$$

For any prime p viewing $J(\mathbb{Q}_p)$ as a p-adic analytic group (of dimension g) containing the Mordell–Weil group $J(\mathbb{Q})$ as subgroup, denote by $\Gamma_p \subset J(\mathbb{Q}_p)$ the topological closure of $J(\mathbb{Q})$ in $J(\mathbb{Q}_p)$ noting that, given our hypothesis, its dimension is at most r, which is less than g. We have

$$\begin{array}{ccc} X(\mathbb{Q}) & \xrightarrow{i_b} & \Gamma_p \\ \downarrow & & \downarrow \\ X(\mathbb{Q}_p) & \xrightarrow{i_b} & J(\mathbb{Q}_p). \end{array}$$

$X(\mathbb{Q}_p)$ is a (proper) p-adic analytic subvariety of $J(\mathbb{Q}_p)$ that generates $J(\mathbb{Q}_p)$ as a p-adic analytic group. It follows that $X(\mathbb{Q}_p)$ is not contained in the proper subgroup Γ_p. Since $X(\mathbb{Q}_p) \cap \Gamma_p$ is a closed proper subvariety of the 1-dimensional compact variety $X(\mathbb{Q}_p)$, it must be compact and have dimension zero and therefore be finite. Hence $X(\mathbb{Q})$ is finite.

How can one make this method effective? We describe how this can be done in the next section.

4.2. **The method of Chabauty as augmented by Coleman.** The Chabauty–Coleman method [27] is one of our most practical tools for actually computing the finite set of rational points on a curve X of genus greater than 1 defined over the rationals, subject to the same Chabauty condition; namely that the Mordell–Weil rank r of the Jacobian of the curve is strictly less than its genus.

Robert Coleman constructed, in the above conditions, a p-adic analytic function ϕ on the p-adic analytic variety $X^{an}_{/\mathbb{Q}_p}$ such that the zeroes of ϕ on $X(\mathbb{Q}_p)$ are

- reasonably computable (to any approximation),
- finite in number, and
- include $X(\mathbb{Q})$.

The construction of such a ϕ uses Coleman's p-adic abelian integrals on the Jacobian of the curve.

Let X be a curve (of genus $g > 1$) defined over the rationals and let J be its Jacobian. Now fix a prime p *of good reduction for* X and a rational point $b \in X(\mathbb{Q})$. Consider, as before, the Abel–Jacobi embedding $i_b : X \to J$ given by $P \mapsto [(P) - (b)]$. Coleman [26, 28] proved that there is a p-adic line integral on holomorphic differentials on the curve satisfying several nice properties (linearity in the integrand, additivity in endpoints, pullbacks under rigid analytic maps, Galois compatibility). The map

$$\begin{aligned} J(\mathbb{Q}_p) \times H^0(X_{\mathbb{Q}_p}, \Omega^1) &\to \mathbb{Q}_p \\ (Q, \omega) &\mapsto \langle Q, \omega\rangle \end{aligned}$$

is additive in Q, is $\mathbb{Q}_p$-linear in ω and is given by

$$\langle Q, \omega\rangle = \langle [D], \omega\rangle =: \int_D \omega$$

for $D \in \mathrm{Div}^0(X)$ with $Q = [D]$. Then

$$\langle i_b(P), \omega\rangle = \int_b^P \omega.$$

The embedding i_b induces an isomorphism of g-dimensional vector spaces

$$H^0(J_{\mathbb{Q}_p}, \Omega^1) \simeq H^0(X_{\mathbb{Q}_p}, \Omega^1),$$

giving us the pairing

$$\begin{aligned} J(\mathbb{Q}_p) \times H^0(J_{\mathbb{Q}_p}, \Omega^1) &\to \mathbb{Q}_p \\ (Q, \omega_J) &\mapsto \int_0^Q \omega_J. \end{aligned}$$

This gives a homomorphism

$$\log : J(\mathbb{Q}_p) \to H^0(J_{\mathbb{Q}_p}, \Omega^1)^*,$$

where log is the logarithm on the p-adic Lie group $J(\mathbb{Q}_p)$, and we have the following diagram:

$$(4.1)\qquad \begin{array}{ccccc} X(\mathbb{Q}) & \longrightarrow & X(\mathbb{Q}_p) & \searrow & \\ \downarrow & & \downarrow & & \\ J(\mathbb{Q}) & \longrightarrow & J(\mathbb{Q}_p) & \xrightarrow{\log} & H^0\left(J_{\mathbb{Q}_p}, \Omega^1\right)^* \simeq H^0(X_{\mathbb{Q}_p}, \Omega^1)^*. \end{array}$$

Recall that under the hypothesis $r < g$, the intersection

$$X(\mathbb{Q}_p)_1 := X(\mathbb{Q}_p) \cap \Gamma_p,$$

and, consequently, $X(\mathbb{Q})$ is finite. Coleman gave a technique to compute $X(\mathbb{Q}_p)_1$ by his construction of p-adic integrals that vanish on Γ_p; in particular, considering an integral of an *annihilating differential* ω, a holomorphic differential such that

$\langle P, \omega \rangle = 0$ for all $P \in J(\mathbb{Q})$, then computing the zero locus of this integral on $X(\mathbb{Q}_p)$. Bounding the number of zeros of this integral via fairly elementary p-adic analysis (for good $p > 2g$) yields the bound

$$\#X(\mathbb{Q}) \leq \#X(\mathbb{Q}_p)_1 \leq \#X(\mathbb{F}_p) + 2g - 2.$$

In Section 4.4, we give a worked example of the Chabauty–Coleman method.

4.3. **The method of Chabauty, Coleman, and Kim.** The construction above crucially uses an assumption that the rank of the Jacobian is small relative to the genus. Nevertheless, there are many interesting curves where this hypothesis is not satisfied, including a number of modular curves we have already seen.

In a series of papers [61–63], Minhyong Kim laid out a program to extend the Chabauty–Coleman method by relaxing the condition on Mordell–Weil rank, going beyond the abelian confines of the Jacobian, replacing it with a sequence of *Selmer varieties*, which are carved out of unipotent quotients of $\pi_1^{\text{ét}}(X_{\overline{\mathbb{Q}}})_{\mathbb{Q}_p}$, the $\mathbb{Q}_p$-étale fundamental group of $X_{\overline{\mathbb{Q}}}$ with base point b.

Remark 4.1. We will consider *unipotent groups* U over $\mathbb{Q}_p$. These are algebraic groups over $\mathbb{Q}_p$ possessing a filtration such that the successive graded pieces are isomorphic to the additive group $\mathbb{G}_a$. By a $\mathbb{Q}_p$*-unipotent group* we will mean a topological group isomorphic to $U(\mathbb{Q}_p)$; such a group is a locally compact topological group that admits a filtration where the successive subquotients of the filtration are topological groups isomorphic to finite-dimensional $\mathbb{Q}_p$-vector spaces. By a $\mathbb{Q}_p$*-pro-unipotent group* we mean a projective limit of $\mathbb{Q}_p$-unipotent groups.

A $\mathbb{Q}_p$*-Malcev completion* $(G \longrightarrow \mathbf{G})$ of a topological group G is the universal solution to the problem of mapping G to $\mathbb{Q}_p$-pro-unipotent groups.

The $\mathbb{Q}_p$*-étale fundamental group* is the $\mathbb{Q}_p$-Malcev completion (see [41, Appendix A]) of the usual étale fundamental group.

We first recast the Chabauty–Coleman method (see also [31], [11]) using p-adic Hodge theory, which adds an extra row of compatibilities to diagram (4.1). Let $V = \mathrm{H}^1_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_p)^*$ and $V_{\mathrm{dR}} := \mathrm{H}^1_{\mathrm{dR}}(X_{\mathbb{Q}_p})^*$, viewed as a filtered vector space with filtration dual to the Hodge filtration. We have an isomorphism $V_{\mathrm{dR}}/F^0 \simeq \mathrm{H}^0(X_{\mathbb{Q}_p}, \Omega^1)^*$. Let T be the set of primes of bad reduction of X, together with the prime p. Let $G_{\mathbb{Q},T}$ be the Galois group of the maximal unramified-outside-T extension of $\mathbb{Q}$. Let G_p denote the absolute Galois group of $\mathbb{Q}_p$. Then the étale formulation of Chabauty–Coleman is given by the following diagram, where the last row is of Bloch–Kato Selmer groups [19]

$$(4.2)\qquad \begin{array}{ccccc}
X(\mathbb{Q}) & \longrightarrow & X(\mathbb{Q}_p) & \overset{i_b}{\searrow} & \\
\downarrow & & \downarrow & & \\
J(\mathbb{Q}) & \longrightarrow & J(\mathbb{Q}_p) & \xrightarrow{\log} & \mathrm{H}^0(X_{\mathbb{Q}_p}, \Omega^1)^* \\
\downarrow & & \downarrow & & \downarrow \simeq \\
\mathrm{H}^1_f(G_{\mathbb{Q},T}, V) & \longrightarrow & \mathrm{H}^1_f(G_p, V) & \xrightarrow{\simeq} & \mathrm{H}_1^{\mathrm{dR}}(X_{\mathbb{Q}_p})/F^0.
\end{array}$$

Let U_n denote the maximal n-unipotent quotient of $\pi_1^{\text{ét}}(X_{\overline{\mathbb{Q}},b})_{\mathbb{Q}_p}$. We have that $U_1 = V$ and U_2 is a central extension

$$1 \to \operatorname{coker}(\mathbb{Q}_p(1) \xrightarrow{\cup^*} \wedge^2 V) \to U_2 \to V \to 1.$$

Suppose that U is a Galois-stable quotient of U_n. Kim defined global and local unipotent Kummer maps j_U and $j_{U,v}$ such that the following diagram commutes:

$$\begin{array}{ccc} X(\mathbb{Q}) & \longrightarrow & \prod_{v\in T} X(\mathbb{Q}_v) \\ {\scriptstyle j_U}\downarrow & & \downarrow{\scriptstyle \prod j_{U,v}} \\ \mathrm{H}^1(G_{\mathbb{Q},T},U) & \xrightarrow{\prod \mathrm{loc}_v} & \prod_{v\in T}\mathrm{H}^1(G_v,U). \end{array}$$

Kim proved that the nonabelian pointed cohomology sets $\mathrm{H}^1(G_{\mathbb{Q},T},U)$ and $\mathrm{H}^1(G_v,U)$ are affine algebraic varieties over $\mathbb{Q}_p$. Motivated by the classical study of Selmer groups, he then refined $\mathrm{H}^1(G_{\mathbb{Q},T},U)$ by local conditions to produce a closed subscheme. Such a closed subscheme is a *Selmer scheme*. We may now give an adapted version [9] of the definition of a *Selmer variety*.

Definition 4.2. The *Selmer variety* $\mathrm{Sel}(U)$ is the reduced scheme associated to the subscheme of $\mathrm{H}^1(G_{\mathbb{Q},T},U)$ containing those classes c such that

- $\mathrm{loc}_p(c)$ is crystalline,
- $\mathrm{loc}_\ell(c)\in j_{U,\ell}(X(\mathbb{Q}_\ell))$ for all $\ell\neq p$,
- the projection of c to $\mathrm{H}^1(G_{\mathbb{Q},T},V)$ comes from an element of $J(\mathbb{Q})\otimes\mathbb{Q}_p$.

Now the Selmer variety gives rise to the following interesting set of points

$$X(\mathbb{Q}_p)_U \coloneqq j_{U,p}^{-1}\left(\mathrm{loc}_p(\mathrm{Sel}(U))\right)\subset X(\mathbb{Q}_p),$$

and note that

$$X(\mathbb{Q})\subset X(\mathbb{Q}_p)_n \coloneqq X(\mathbb{Q}_p)_{U_n}\subset X(\mathbb{Q}_p)_U. \tag{4.3}$$

The set $X(\mathbb{Q}_p)_n$ can be computed in terms of n-fold iterated Coleman integrals, and one has a series of refinements

$$X(\mathbb{Q})\subset\cdots\subset X(\mathbb{Q}_p)_n\subset X(\mathbb{Q}_p)_{n-1}\subset\cdots\subset X(\mathbb{Q}_p)_2\subset X(\mathbb{Q}_p)_1.$$

Note that the set $X(\mathbb{Q}_p)_1$ is the Chabauty–Coleman set from before. We refer to the points in $X(\mathbb{Q}_p)_n$ as the set of **Selmer points of level** n. We call the points in $X(\mathbb{Q}_p)_n\setminus X(\mathbb{Q})$ the set of **mock-rational Selmer points of level** n. Kim has conjectured that for $n\gg 0$, the set $X(\mathbb{Q}_p)_n$ is finite. This conjecture is implied by the conjecture of Bloch and Kato [19].

Putting everything together, Kim's program studies finiteness of $X(\mathbb{Q}_p)_U$ using p-adic Hodge theory and the following diagram is the nonabelian generalization of diagram (4.1):

$$\begin{array}{ccccc} X(\mathbb{Q}) & \longrightarrow & X(\mathbb{Q}_p) & & \\ {\scriptstyle j_U}\downarrow & & {\scriptstyle j_{U,p}}\downarrow & \searrow^{\,j_U^{\mathrm{dR}}} & \\ \mathrm{Sel}(U) & \xrightarrow{\mathrm{loc}_{U,p}} & \mathrm{H}^1_f(G_p,U) & \xrightarrow{\simeq} & U^{\mathrm{dR}}/\mathrm{Fil}^0. \end{array}$$

Computing the depth-2 Selmer set (or a slightly larger finite set containing it), known as *quadratic Chabauty*, has seen progress in recent years [6–9], via aspects of the theory of p-adic height functions [29, 80]. The quadratic Chabauty set $X(\mathbb{Q}_p)_2$ is finite for those curves that satisfy the rank bound [9]

$$r<g+\rho-1,$$

where $\rho := \text{rank}(\text{NS}(J))$ is the Néron–Severi rank of the Jacobian over $\mathbb{Q}$. To carry out the quadratic Chabauty method, one uses a nontrivial element of $\ker(\text{NS}(J) \to \text{NS}(X))$ to construct a nonabelian quotient U of U_2, which is used to compute $X(\mathbb{Q}_p)_U$.

Samir Siksek [96] showed that modular curves of genus 3 or more have ρ at least 2, and consequently, for these curves, quadratic Chabauty allows one to consider Jacobians of higher rank than allowed by Chabauty and Coleman. Balakrishnan, Dogra, Müller, Tuitman, and Vonk [6, 7] made various aspects of quadratic Chabauty computationally practical using explicit p-adic cohomology to compute a certain (global) p-adic height of Nekovář [80], depending on a choice of a nontrivial element of $\ker(\text{NS}(J) \to \text{NS}(X))$.

Roughly speaking, the method starts from the following observation: the global p-adic height admits a decomposition as a sum of local heights; a local height at p that can be computed using p-adic Hodge theory and a finite sum of local heights away from p that, in certain favorable conditions, can be shown to be trivial—or, if not trivial, at least a quantity that can be computed from the geometry of a regular model of the curve. We will discuss this in more detail in the case of bielliptic genus 2 curves in Section 4.5.

Moreover, the global p-adic height is a quadratic form on $H^0(X, \Omega^1)^*$. Choosing an explicit basis for the space of quadratic forms in terms of Coleman integrals and knowing sufficiently many rational points (either on X or on J) and their p-adic heights, one can compute a locally analytic function whose zero locus contains $X(\mathbb{Q}_p)_2$.

Recently, various new perspectives on the Chabauty–Coleman method and quadratic Chabauty have emerged; "symmetric Chabauty" introduced by Siksek [95], a geometric quadratic Chabauty method introduced by Edixhoven and Lido [34], and the p-adic Arakelov theoretic method of Besser, Müller, and Srinivasan [16]:

- Siksek gave a symmetric Chabauty method [95], a variant of the Chabauty–Coleman method (see Section 4.2) for symmetric powers of curves. Symmetric Chabauty has been used and extended in various ways to determine quadratic points on numerous modular curves $X_0(N)$ [3, 21, 79, 88]. Box, Gajović, and Goodman [22] further developed a "partially relative" symmetric Chabauty method to study cubic and quartic points on several modular curves $X_0(N)$.
- In *geometric quadratic Chabauty*, Edixhoven and Lido [34] used line bundles over the Jacobian, the Poincaré torsor (a biextension of the Jacobian by $\mathbb{G}_m$), and models over the integers to study rational points under the same rank bound hypothesis.
- Besser, Müller, and Srinivasan [16] gave a new construction of p-adic heights on varieties over number fields using p-adic adelic metrics on line bundles in the spirit of Zhang's work on real-valued heights using adelic metrics [106]. This led them to formulate *p-adic Arakelov quadratic Chabauty*.

We will not discuss these works in detail in this survey.

4.4. **Rational points on $X_0(37)$: Three perspectives.** As a concrete application of the techniques discussed so far, we present here three perspectives on rational points on the modular curve $X_0(37)$. For further discussion, see [71, Section 5]; and for more, see [21, Section 5].

The modular curve $X := X_0(37)$ is of genus 2 and therefore is hyperelliptic. Denote by

$$X_0(37) \xrightarrow{\sigma} X_0(37)$$

its hyperelliptic involution, and by

$$X_0(37) \xrightarrow{w} X_0(37)$$

its Atkin–Lehner involution. The involutions σ and w commute, generating a Klein group $\mathcal{G}$ of automorphisms. The automorphisms $1, w, \sigma, w\sigma$ are defined over $\mathbb{Q}$ and are the only automorphisms of $X_0(37)$ over $\mathbb{C}$ (see [85]).

Form the quotients

(4.4)
$$\begin{array}{ccccc} & & X_0(37) & & \\ & \swarrow^{i_0} & \downarrow^{x} & \searrow^{i_1} & \\ E_0 := X_0(37)/\langle \sigma \cdot w \rangle & & \mathbb{P}^1_{/\mathbb{Q}} \simeq X_0(37)/\langle \sigma \rangle & & E_1 := X_0(37)/\langle w \rangle. \end{array}$$

Each E_j is a genus one curve, and we consider each as an elliptic curve with identity element $i_j(\infty)$. By the Riemann–Hurwitz formula, the ramification locus of each of the double covers:

$$X_0(37) \xrightarrow{i_0} E_0 \tag{4.5}$$

and

$$X_0(37) \xrightarrow{i_1} E_1 \tag{4.6}$$

are $\mathbb{Q}$-rational (effective) divisors of degree two.

- $D_0 := \{\eta_0, \bar{\eta}_0\} \subset X_0(37)$—for (4.5).
- $D_1 := \{\eta_1, \bar{\eta}_1\} \subset X_0(37)$—for (4.6).

In particular, D_1 is the fixed point set of w and D_0 is the fixed point set of $w\sigma$.

Note that (since σ commutes with w) each of these involutions $(\sigma, w, w\sigma)$ preserves D_1 and D_0. The involution $w\sigma$ interchanges the points $\eta_1, \bar{\eta}_1$. So their image $e_0 \in E_0$—which is therefore the image of a $\mathbb{Q}$-rational divisor in $X_0(37)$—is $\mathbb{Q}$-rational. Consequently, $\{\eta_1, \bar{\eta}_1\}$ either consists of a pair of $\mathbb{Q}$-rational points[10] or a conjugate pair of quadratic points in $X_0(37)$.

For the same reason, the involution w preserves the ramification divisor of $w\sigma$ and interchanges the points $\eta_0, \bar{\eta}_0$, and, therefore, their image $e_1 \in E_1$ is $\mathbb{Q}$-rational.

A visit to the L-Functions and Modular Forms Database[11] (LMFDB) [65] will tell you that we have:

- E_0 is the elliptic curve
$$37.b2 : y^2 + y = x^3 + x^2 - 23x - 50.$$
Its Mordell–Weil group is of order 3.
- E_1 is the elliptic curve
$$37.a1 : y^2 + y = x^3 - x. \tag{4.7}$$
It has Mordell–Weil rank 1, and its group of $\mathbb{Q}$-rational points is isomorphic to $\mathbb{Z}$.

[10]That is not the case; see Lemma 4.4.

[11]See the sidebar of Related Objects on LMFDB.

4.4.1. *The Chabauty–Coleman method gives finiteness.* Let $J_0(37)$ denote the Jacobian of $X_0(37)$. We have:

$$\begin{array}{ccc} X_0(37) & \hookrightarrow & J_0(37) \\ & \overset{i_0 \times i_1}{\searrow} & \downarrow \phi \\ & & E_0 \times E_1 \end{array}$$

where i_0, i_1 are (as above) the modular parametrization of E_0, E_1, and

$$\phi : J_0(37) \twoheadrightarrow E_0 \times E_1$$

is an isogeny. Since $\{E_0 \times E_1\}(\mathbb{Q})$ is—by the data above—a group isomorphic to $\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ (contained in a cyclic group of order three times the elliptic curve E_1) we see that the Zariski closure of the group of $\mathbb{Q}$-rational points $J_0(37)(\mathbb{Q})$ is an algebraic subgroup in $J_0(37)$ of codimension 1, so can intersect only finitely with $X_0(37)$—giving that $X_0(37)(\mathbb{Q})$ is finite.

4.4.2. *The projection to E_0 gets us the precise set of $\mathbb{Q}$-rational points.* The cusp $\infty \in X_0(37)$ is a $\mathbb{Q}$-rational point, as are the four points

$$\mathcal{S} = \mathcal{G} \cdot \infty = \{\infty,\ w(\infty) = \text{ the cusp } \mathbf{0}, \sigma(\infty), \sigma(\mathbf{0})\}. \tag{4.8}$$

Theorem 4.3. *These are the only four $\mathbb{Q}$-rational points on $X_0(37)$.*

Proof. Returning to the mapping of degree two

$$X_0(37)(\mathbb{Q}) \xrightarrow{i_0} E_0(\mathbb{Q}),$$

since $E_0(\mathbb{Q})$ is cyclic of order three, we see that

- the pair $\{\infty, \sigma w(\infty) = \sigma(\mathbf{0})\}$ maps to the origin in $E_0(\mathbb{Q})$ and
- the pair $\{\mathbf{0}, \sigma w(\mathbf{0}) = \sigma(\infty)\}$ maps to a (nonzero) point $e \in E_0(\mathbb{Q})$.
- Recalling that the pair $\{\eta_1, \bar{\eta}_1\}$ discussed above maps to $e_0 \in E_0(\mathbb{Q})$ and noting that e_0 cannot be any of the above two $\mathbb{Q}$-rational points of E_0, it must be the third $\mathbb{Q}$-rational point, giving us

$$e_0 = 2e = -e \in E_0(\mathbb{Q}).$$

These three bullet points show that

$$i_0^{-1}(E_0(\mathbb{Q})) = \mathcal{S} \cup \{\eta_1, \bar{\eta}_1\}.$$

[12]Note that the LMFDB gives a different "simplified" model of $X_0(37)$ which can be seen to be isomorphic to ours, using the following `Magma` commands:

```
> R<x> :=PolynomialRing(RationalField());
> X37v1 :=HyperellipticCurve(x^6 + 8*x^5 - 20*x^4 + 28*x^3 - 24*x^2 +12*x - 4);
> X37v2 :=HyperellipticCurve(-x^6 - 9*x^4 - 11*x^2 + 37);
> IsIsomorphic(X37v1,X37v2);
true Mapping from:  CrvHyp:  X37v1 to CrvHyp:  X37v2
with equations :
1/2*$.1 - $.3
1/2*$.2
1/2*$.1
and inverse
$.3
1/4*$.2
-1/2*$.1 + 1/2*$.3
```

Since

$$X_0(37)(\mathbb{Q}) \subset i_0^{-1}(E_0(\mathbb{Q})),$$

it is enough to show that $\eta_1, \bar{\eta}_1 \notin X_0(37)(\mathbb{Q})$. This is established in Lemma 4.4, completing the proofs. □

Lemma 4.4. *The pair of points* $\{\eta_1, \bar{\eta}_1\} \in X_0(37)(\bar{\mathbb{Q}})$ *are* $\mathbb{Q}(\sqrt{37})$*-conjugate points defined over* $\mathbb{Q}(\sqrt{37})$ *and not over* $\mathbb{Q}$.

Proof. The involutions σ and w of $X_0(37)$ are easily described in terms of the model[12] of $X_0(37)$ given by

$$y^2 = g(x) := -x^6 - 9x^4 - 11x^2 + 37, \tag{4.9}$$

as found by Mazur and Swinnerton-Dyer in [71, §5.1]. We have:

(a) $(x,y) \overset{\sigma}{\mapsto} (x,-y)$,
(b) $(x,y) \overset{w}{\mapsto} (-x,y)$, and
(c) $(x,y) \overset{w\sigma}{\mapsto} (-x,-y)$.

The proof of (c) follows from (a) and (b) by composition.

The proof of (a) is simply that the quotient of the involution $(x,y)\mapsto(x,-y)$ is of genus zero as is clear from the equation; so that involution is the hyperelliptic involution σ.

The proof of (b) follows from considering the following model[13] (over $\mathbb{Q}$) for the expression of $X_0(37)$ as the double cover $X_0(37) \xrightarrow{i_1} E_1 = X_0(37)^+$ over $\mathbb{Q}$:

$$\begin{array}{lcl} X_0(37): & & y^2 = -x^6 - 9x^4 - 11x^2 + 37 \\ \Big\downarrow i_1 & & \Big\uparrow u=x^2;\, v=y \\ E_1: & & v^2 = -u^3 - 9u^2 - 11u + 37. \end{array} \tag{4.10}$$

Since $\{\eta_1, \bar{\eta}_1\}$ consists of the fixed points of the involution w, we have

$$\{\eta_1, \bar{\eta}_1\} = \{(0, \pm\sqrt{37})\},$$

from which it follows that

$$w\sigma : (0, \pm\sqrt{37}) \mapsto (0, \mp\sqrt{37})$$

and, therefore,

$$i_0(\eta_1) = i_0(\bar{\eta}_1) = i_0(0, +\sqrt{37}) = i_0(0, -\sqrt{37}) \in E_0(\mathbb{Q});$$

i.e., it is a $\mathbb{Q}$-rational point of E_0, which can be neither $i_0(\infty)$ nor $i_0(\mathbf{0})$ so must be the third $\mathbb{Q}$-rational point.

[13]This alternative model of E_1 can be checked to be isomorphic to (4.7), using the following `Magma` commands:

```
> P<u,v,z> :=ProjectiveSpace(Rationals(),2);
> C :=Curve(P, v^2*z - (-u^3-9*u^2*z-11*u*z^2+37*z^3));
> pt :=C![1,4,1];
> E :=EllipticCurve(C,pt);
> E1 :=EllipticCurve([0,0,1,-1,0]);
> IsIsomorphic(E1,E);
true
```

4.4.3. *The Chabauty–Coleman method would also give us the set of $\mathbb{Q}$-rational points.* Since $J_0(37) \sim E_0 \times E_1$, we have

$$\mathrm{rank} J_0(37)(\mathbb{Q}) = \mathrm{rank} E_0(\mathbb{Q}) + \mathrm{rank} E_1(\mathbb{Q}) = 1,$$

where the ranks of the elliptic curves E_0, E_1 were earlier found in LMFDB. Since the rank of $J_0(37)(\mathbb{Q})$ is less than the genus of the curve $X := X_0(37)$, we may carry out the Chabauty–Coleman method on (4.9) to compute the set $X(\mathbb{Q})$. We use the prime $p = 3$ and take $\{\frac{dx}{y}, \frac{x\,dx}{y}\}$ as our basis of $H^0(X, \Omega^1)$.

Searching in a box for rational points of small height, one finds the points $(\pm 1, \pm 4) \in X(\mathbb{Q})$. The point $P := [(1,-4) - (-1,4)] \in J_0(37)(\mathbb{Q})$ is nontorsion, since the 3-adic Coleman integral of a holomorphic differential along this point is nonzero:

$$\int_{(-1,4)}^{(1,-4)} \frac{x\,dx}{y} = 3^2 + 2 \cdot 3^3 + 3^4 + 2 \cdot 3^5 + 3^7 + O(3^9).$$

Moreover, $\int_{(-1,4)}^{(1,-4)} \frac{dx}{y} = O(3^9)$. In fact, $\int_{(-1,4)}^{(1,-4)} \frac{dx}{y}$ is identically 0, as can be seen by applying the involution $w\sigma$ to the integrand and the endpoints of involution. Thus we may take $\frac{dx}{y}$ as our annihilating differential. The curve X over $\mathbb{F}_3$ has the following rational points

$$(\overline{0}, \overline{1}), (\overline{0}, \overline{2}), (\overline{1}, \overline{1}), (\overline{1}, \overline{2}), (\overline{2}, \overline{1}), (\overline{2}, \overline{2}) \in X_{\mathbb{F}_3}(\mathbb{F}_3),$$

which correspond to the residue disks over which we carry out our computation.

Fixing as our basepoint $(-1, 4) \in X(\mathbb{Q})$, we start in the residue disk corresponding to $(\overline{0}, \overline{1})$. We take the point $S_0 = (0, y_0)$ in the residue disk, where $y_0 \in \mathbb{Z}_3$ is the unique square root of 37 that satisfies $y_0 \equiv 1 \pmod 3$. We compute our local coordinate at S_0: since $x = 0$, we take $x(t) = t$. Then $y(t)$ correspondingly is found by applying Hensel's lemma to produce the 3-adic power series expansion of the square root

$$\begin{aligned} y(t) &= \sqrt{g(x(t))}, \\ &= \sqrt{-t^6 - 9t^4 - 11t^2 + 37}, \end{aligned}$$

which yields the following:

$$\begin{aligned} S_t = (t, &-3788 + (2159 + O(3^{10}))t^2 - (15737 + O(3^{10}))t^4 + \\ &- (23833 + O(3^{10}))t^6 + (746 \cdot 3^3 + O(3^{10}))t^8 + O(t^{10})) \\ =:\ &(x(t), y(t)). \end{aligned}$$

We now wish to compute the zeros of the power series $I(3T)$, where

$$I(T) = \int_{(-1,4)}^{S_0} \frac{dx}{y} + \int_{S_0}^{S_T} \frac{dx(t)\,dt}{y(t)}.$$

Using the 3-adic power series expansions calculated for $x(t), y(t)$ above, as well as the value of the Coleman integral between $(-1,4)$ and S_0, this yields

$$\begin{aligned} I(3T) = &\left(3+3^3+2\cdot 3^4+2\cdot 3^5+3^6+3^7+2\cdot 3^8+3^9+3^{10}+O(3^{11})\right)T \\ &+\left(3^2+2\cdot 3^4+2\cdot 3^5+3^7+2\cdot 3^8+2\cdot 3^9+3^{10}+O(3^{12})\right)T^3 \\ &+\left(3^6+3^7+2\cdot 3^8+3^9+3^{10}+3^{11}+2\cdot 3^{13}+2\cdot 3^{14}+O(3^{15})\right)T^5 \\ &+\left(3^8+2\cdot 3^9+3^{10}+2\cdot 3^{11}+2\cdot 3^{12}+2\cdot 3^{13}+2\cdot 3^{15}+O(3^{17})\right)T^7 \\ &+\left(3^7+2\cdot 3^8+2\cdot 3^{10}+2\cdot 3^{11}+3^{12}+3^{14}+2\cdot 3^{16}+O(3^{17})\right)T^9 \\ &+O(T^{10}), \end{aligned}$$

which has precisely one zero at $T=0$, corresponding to S_0, which we can identify as $(0,\sqrt{37})$.

Continuing in this way, parametrizing each residue disk by a local coordinate and computing the zeros of the corresponding $I(3T)$ in each residue disk, we find that

$$X(\mathbb{Q}_3)_1 = \{(0,\pm\sqrt{37}), (\pm 1, \pm 4)\},$$

from which we immediately produce

$$X(\mathbb{Q}) = (\pm 1, \pm 4).$$

Remark 4.5. It was fairly lucky that $X(\mathbb{Q}_3)_1 = \{(0,\pm\sqrt{37}), (\pm 1,\pm 4)\}$ and was not much larger. Finding a small good prime p such that there are no mock-rational Selmer points—or where the mock-rational points are easily recognized algebraic points—may be an issue. By the Weil bound, we know that $\#X(\mathbb{F}_p)$ grows linearly as p grows. So if we had used a larger prime p in the Chabauty–Coleman method, we would expect more p-adic points in $X(\mathbb{Q}_p)_1$ and we may not be able to immediately recognize these extra points.

4.5. **Quadratic points on bielliptic curves of genus 2 using quadratic Chabauty.** In the previous section, we considered the problem of determining the finitely many rational points on $X_0(37)$. We could also study the finite sets $X_0(37)(K)$ for various other number fields K, one number field at a time. Or, we could further study $\mathrm{Symm}^d(X_0(37))(\mathbb{Q})$, as described in Part 1, which would tell us about all degree d points on $X_0(37)$.

We start by considering $X_0(37)(K)$ for a fixed quadratic field K. If the rank of $J_0(37)(K)$ is now 2, and if this is because the rank of $E_0(K)$ increases to 1—recall from Section 4.4 that the rank of $E_0(\mathbb{Q})$ is 0—then the Chabauty–Coleman method no longer applies. However, since $X_0(37)$ is bielliptic and genus 2, we can use the method of [9], which gives a particularly explicit description of quadratic Chabauty functions (an elaboration of the case $n=2$ in Section 4.3) using p-adic height functions and double Coleman integrals on elliptic curves, for bielliptic genus 2 curves. We describe this below in some generality, and then use it to study rational points on $X_0(37)$ over $K=\mathbb{Q}(i)$.

Let $K=\mathbb{Q}$ or a quadratic imaginary extension, and let X/K be a genus 2 bielliptic curve

$$y^2 = x^6 + a_4x^4 + a_2x^2 + a_0,$$

with $a_i \in K$. Let C_1 and C_2 be the elliptic curves over K defined by the equations

$$C_1 : y^2 = x^3 + a_4x^2 + a_2x + a_0, \qquad C_2 : y^2 = x^3 + a_2x^2 + a_4a_0x + a_0^2,$$

and let $f_1 : X \to C_1$ be the map that sends (x, y) to (x^2, y) and $f_2 : X \to C_2$ be the map that sends $(x, y) \to (a_0 x^{-2}, a_0 y x^{-3})$.

We will be considering the case where the Mordell–Weil ranks of C_1 and C_2 over K are equal to 1. Letting J denote the Jacobian of X we have that the rank of J over K is 2. The natural mapping defined over K

$$\mathrm{Symm}^2(X) \to J \tag{4.11}$$

(i.e., setting $p = 2$ in Equation (1.1)) is

- an isomorphism if X is not hyperelliptic, or is
- an isomorphism in the complement of an exceptional fiber $\mathcal{E} \subset \mathrm{Symm}^2(X)$ isomorphic to $\mathbb{P}^1$ over K if X is hyperelliptic.

In other words, all quadratic points of X over K are parameterized, in an appropriate sense, either by $J(K)$, if X is not hyperelliptic, or by $J(K)$ together with the isomorphism $\mathcal{E} \simeq \mathbb{P}^1(K)$, if X is hyperelliptic.

These parametrizations are neat, and explicit, but they still leave untouched the question: For a given quadratic field K what—exactly—is the finite set $X(K)$? We want to use quadratic Chabauty to answer such questions.

Fix some auxiliary choices, including an idèle class character $\chi : G_K^{\mathrm{ab}} \to \mathbb{Q}_p$. Define $Z_1, Z_2 \subset X \times X$ to be the graphs of the automorphisms $g_1 : (x, y) \mapsto (-x, y)$ and $g_2 : (x, y) \mapsto (-x, -y)$, respectively. We take as our correspondence $Z := Z_1 - Z_2$. When $K = \mathbb{Q}$ fix a prime $\mathfrak{p} = (p)$ to be a prime of good ordinary reduction. When K is imaginary quadratic, take p to be a rational prime that splits as $\mathfrak{p}\overline{\mathfrak{p}}$ where both $\mathfrak{p}$ and $\overline{\mathfrak{p}}$ are primes of good ordinary reduction.

Let h_{C_1} and h_{C_2} denote the global $\mathfrak{p}$-adic height functions associated to the choices made above and $h_{C_i,\mathfrak{p}}$ the respective local height at $\mathfrak{p}$, with the global height written as the sum of local heights

$$h_{C_i} = \sum_v h_{C_i,v}.$$

Suppose $C_1(K)$ and $C_2(K)$ each have Mordell–Weil rank 1, and let $P_i \in C_i(K)$ be points of infinite order. Let

$$\alpha_i = \frac{h_{C_i}(P_i)}{[K : \mathbb{Q}] \log_{C_i}(P_i)^2}.$$

Let Ω denote the finite set of values taken by

$$-\sum_{v \nmid p} (h_{C_1,v}(f_1(z_v)) - h_{C_2,v}(f_2(z_v)) - 2\chi_v(x(z_v)))$$

for $(z_v) \in \prod_{v \nmid p} X(K_v)$. Then $X(K)$ is contained in the finite set of $z \in X(K_\mathfrak{p})$ cut out by the quadratic Chabauty function

$$h_{C_1,\mathfrak{p}}(f_1(z)) - h_{C_2,\mathfrak{p}}(f_2(z)) - 2\chi_\mathfrak{p}(x(z)) - \alpha_1 \log_{C_1}(f_1(z))^2 + \alpha_2 \log_{C_2}(f_2(z))^2 \in \Omega,$$

where

$$\log_{C_i}(Q) = \int_\infty^Q \frac{dx}{2y},$$

the single Coleman integral we saw in the Chabauty–Coleman method (with ∞ denoting the point at infinity on the corresponding elliptic curve) and

$$h_{C_i,\mathfrak{p}}(z)$$

is a double Coleman integral.

Remark 4.6. Over $K = \mathbb{Q}(i)$, the elliptic curves 37.a1 and 37.b2 each have rank 1. The computation in [9] applies quadratic Chabauty as described above at the primes $p = 41, 73, 101$ to produce, for each prime p, a finite superset of p-adic points containing $X(K)$. This is then combined with another method, the *Mordell–Weil sieve*, to give

$$X_0(37)(K) = \{(\pm 2i, \pm 1), (\pm 1, \pm 4), \infty, \mathbf{0}\}. \tag{4.12}$$

4.5.1. *Explicitly determining quadratic points.* Quadratic Chabauty for bielliptic curves over $\mathbb{Q}$ was subsequently refined by Bianchi [17] using p-adic sigma functions in place of double Coleman integrals. This was recently extended by Bianchi and Padurariu [18], where an implementation was given to study rational points on *all* rank 2 genus 2 bielliptic curves in the LMFDB, including the Atkin–Lehner quotient curve $X_0(166)^* := X_0(166)/\langle w_2, w_{83}\rangle$ (with LMFDB label 13778.a.27556.1), as well as the Shimura curve $X_0(10, 19)/\langle w_{190}\rangle$.

Using a slight extension of their work to $K = \mathbb{Q}(i)$, as done in [10], one can use a smaller prime to carry out the computation of a finite set containing the depth 2 Selmer set for $X_0(37)$. (Recall Definition 4.2.) We carried out this computation for $p = 13$ and recovered the points $(\pm 2i, \pm 1), (\pm 1, \pm 4)$, and $\infty, \mathbf{0}$. But lurking within the set of depth 2 Selmer points we also found the *algebraic* points $(\pm\sqrt{-3}, \pm 4)$, these being initially observed 73-adically in [9]. We also found several other mock-rational Selmer points, such as

$$\begin{aligned}(5 + 8\cdot 13 + 12\cdot 13^2 + 4\cdot 13^3 + 2\cdot 13^4 + 3\cdot 13^5 + O(13^6),\\ 1 + 3\cdot 13 + 3\cdot 13^2 + 9\cdot 13^3 + 12\cdot 13^4 + 5\cdot 13^5 + O(13^6)).\end{aligned}$$

See Banwait, Najman, and Padurariu [14] for an extensive discussion—and for results—regarding quadratic points on $X_0(N)$. In particular, they show that

$$X_0(37)(\mathbb{Q}(\sqrt{d})) = X_0(37)(\mathbb{Q})$$

for

$$\begin{aligned}d = -6846, -2289, 213, 834, 1545, 1885, 1923, 2517, 2847, 4569,\\ 6537, 7131, 7302, 7319, 7635, 7890, 8383, 9563, 9903.\end{aligned}$$

We could continue by varying the quadratic fields K; and in principle, if the rank is not too large, apply the Chabauty–Coleman method, quadratic Chabauty or variations thereof—possibly combining with other Diophantine techniques—to determine the K-rational points on $X_0(37)$. But, eventually, the ranks outpace our current collection of Diophantine tools. For instance, over $K = \mathbb{Q}(\sqrt{-139})$, a `Magma` computation reveals that the elliptic curve E_0 has rank 3, as does E_1, and so $J_0(37)(K)$ here altogether has rank 6, making it a challenge for existing methods.

Now indeed, since $X_0(37)$ is hyperelliptic, it has *infinitely many* quadratic points. Nevertheless, one can describe all quadratic points on $X_0(37)$ using the Symm^2 perspective and the maps to the various quotients of $X_0(37)$ in diagram (4.4), as was done by Box [21]. The hyperelliptic covering map $x : X_0(37) \to \mathbb{P}^1$ is one source of infinitely many rational points, and the rank 1 elliptic curve quotient E_1 is another source of infinitely many rational points. Finally, the elliptic curve quotient E_0 gives three rational points, and Box pieced together these three sources of rational points to describe $\mathrm{Symm}^2(X_0(37))(\mathbb{Q})$, as below.

The x-map gives us all points

$$\{(x_i, \sqrt{g(x_i)}), (x_i, -\sqrt{g(x_i)})\} \in \mathrm{Symm}^2(X_0(37))(\mathbb{Q}),$$

where x_i ranges through all rational numbers. We can find $P_1 \in X_0(37)(\mathbb{Q}(\sqrt{-3}))$, such that $[P_1 + \overline{P_1} - \infty - \mathbf{0}]$ generates the free part of the Mordell–Weil group of $J_0(37)(\mathbb{Q})$, and we have the points $\mathcal{P}_{1,0} := \{P_1, \overline{P_1}\}$ and $\mathcal{P}_{0,1} := \{\infty, w(\mathbf{0})\}$. Finally, for any $(a, b) \in \mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \setminus \{(0, 0)\}$, there is a point $\mathcal{P}_{a,b} \in \mathrm{Symm}^2(X_0(37)(\mathbb{Q}))$ defined by the unique effective degree 2 divisor P such that

$$P - \infty - \mathbf{0} \sim a\mathcal{P}_{1,0} + b\mathcal{P}_{0,1} - (a + b)(\infty + \mathbf{0})$$

for any lift of b to $\mathbb{Z}$.

Appendix A. Quadratic points on Bring's curve by Netan Dogra

We consider *Bring's curve*, the smooth projective genus 4 curve X in $\mathbb{P}^4$ given as the locus of common zeros of the following system of equations:

$$\text{(A.1)} \qquad \begin{cases} x_1 + x_2 + x_3 + x_4 + x_5 & = 0, \\ x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 & = 0, \\ x_1^3 + x_2^3 + x_3^3 + x_4^3 + x_5^3 & = 0. \end{cases}$$

From the quadratic defining equation of Bring's curve, we see that $X(\mathbb{R}) = \emptyset$, so we have that $X(\mathbb{Q}) = \emptyset$. However, considering the curve instead over $K = \mathbb{Q}(i)$, we see several K-rational points: for instance, all permutations of the coordinates of the points $(1 : \pm i : -1 : \mp i : 0)$ are in $X(\mathbb{Q}(i))$. Could there possibly be more points?

Proposition A.1. *The only quadratic points on Bring's curve are over* $\mathbb{Q}(i)$*, and up to permutation of coordinates, they are* $(1 : \pm i : -1 : \mp i : 0)$.

The automorphism group of X is the symmetric group S_5, given by permutation of the five coordinates. Using the action of S_5 on X, one can see that the Jacobian J of X is isogenous to E^4 [94, Section 8.3.2], where E is the rank zero elliptic curve with LMFDB label 50.a3. Since Bring's curve is not hyperelliptic, the map

$$\mathrm{Symm}^2(X) \hookrightarrow \mathrm{Pic}^0(X)$$

is injective, and since $\mathrm{Pic}^0(X)(\mathbb{Q})$ is finite it follows that there are only finitely many quadratic points on Bring's curve.

There is also a simple description of a map $\mathrm{Symm}^2(X) \to E^4$ with finite fibers. The quotient of Bring's curve by the involution swapping two coordinates is isomorphic to the curve

$$E' : x^3 + y^3 + 1 + x^2y + y^2x + x^2 + y^2 + xy + x + y = 0$$

by projecting the three non-permuted coordinates to $\mathbb{P}^2$. This is isomorphic to the elliptic curve

$$E : y^2 + 5x^3 + 5x^2 + 4 = 0 \qquad \text{(LMFDB label 50.a3)}$$

via

$$(x, y) \mapsto \left(\frac{2}{1 + 2x + 2y}, \frac{4(y - x)}{1 + 2x + 2y} \right).$$

We have $E(\mathbb{Q}) = \{\infty, (-2, \pm 4)\}$. The S_3-action on E' corresponds to the action of $E(\mathbb{Q})$ and -1 on E.

Now fix a quadratic point $P = (x_0 : x_1 : x_2 : x_3 : 1)$ on Bring's curve. Up to an S_3 permutation, we may assume it maps to ∞ in E after quotienting by the involution switching x_0 and x_1. Suppose σ generates the Galois group of the field of definition of P. Let $x = x_2$ and $y = x_3$. Then

$$\frac{y-x}{1+2x+2y} = -\frac{\sigma y - \sigma x}{1+2\sigma x+2\sigma y}.$$

This reduces to the equation

$$\mathrm{Tr}(y) + 4\mathrm{Nm}(y) = \mathrm{Tr}(x) + 4\mathrm{Nm}(x).$$

Thus quadratic points on Bring's curve are 5-tuples $(x_1 : x_2 : x_3 : x_4 : x_5)$ of quadratic points in $\mathbb{P}^5$ satisfying, for all $i_1, i_2, i_3 \subset \{1,2,3,4,5\}$,

$$\prod_{\sigma \in S_3} (\mathrm{Tr}(x_{i_{\sigma(1)}}/x_{i_{\sigma(3)}}) + 4\mathrm{Nm}(x_{i_{\sigma(1)}}/x_{i_{\sigma(3)}}) \\ - \mathrm{Tr}(x_{i_{\sigma(2)}}/x_{i_{\sigma(3)}}) - 4\mathrm{Nm}(x_{i_{\sigma(2)}}/x_{i_{\sigma(3)}})) = 0.$$

Up to the S_5-action, we may reduce to finding tuples (x_1, x_2, x_3, x_4) defining a quadratic point $(x_1 : x_2 : x_3 : x_4 : 1)$ on Bring's curve and satisfying

$$\mathrm{Tr}(x_1) + 4\mathrm{Nm}(x_1) = \mathrm{Tr}(x_2) + 4\mathrm{Nm}(x_2),$$

and either

$$\mathrm{Tr}(x_1) + 4\mathrm{Nm}(x_1) = \mathrm{Tr}(x_3) + 4\mathrm{Nm}(x_3),$$

$$\mathrm{Tr}\left(\frac{1}{x_1}\right) + 4\mathrm{Nm}\left(\frac{1}{x_1}\right) = \mathrm{Tr}\left(\frac{x_3}{x_1}\right) + 4\mathrm{Nm}\left(\frac{x_3}{x_1}\right),$$

or

$$\mathrm{Tr}\left(\frac{1}{x_3}\right) + 4\mathrm{Nm}\left(\frac{1}{x_3}\right) = \mathrm{Tr}\left(\frac{x_1}{x_3}\right) + 4\mathrm{Nm}\left(\frac{x_1}{x_3}\right).$$

Write each quadratic point $x_i = u_i + w_i$, where u_i and w_i are in plus and minus eigenspaces for the Galois involution. These equations define a finite scheme over $\mathbb{Q}$, and one may check that its rational points correspond exactly to the quadratic points in the statement of the proposition.

Acknowledgments

We are grateful to Barinder Banwait, Alexander Betts, Francesca Bianchi, Maarten Derickx, Netan Dogra, Minhyong Kim, Steffen Müller, Filip Najman, Ken Ribet, Matthias Schütt, Bianca Viray, Isabel Vogt, Preston Wake, and the anonymous referees for their illuminating and extremely helpful comments. Thanks also to Netan Dogra for providing the appendix on Bring's curve. Thanks to the organizers in the IAS for organizing and hosting the Frank C. and Florence S. Ogg Professorship in Mathematics, and thanks to Andrew for inspiring all of us.

The research for this paper was partially supported by NSF grant DMS-1945452, the Clare Boothe Luce Professorship (Henry Luce Foundation), Simons Foundation grant no. 550023 (J.S.B.), and NSF grant DMS-2152149 (B.M.).

References

[1] D. Abramovich and J. Harris, *Abelian varieties and curves in $W_d(C)$*, Compositio Math. **78** (1991), no. 2, 227–238. MR1104789

[2] 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*, Acta Arith. **208** (2023), no. 1, 15–49, DOI 10.4064/aa220110-7-3. MR4616870

[3] N. Adžaga, T. Keller, P. Michaud-Jacobs, F. Najman, E. Ozman, and B. Vukorepa, *Computing quadratic points on modular curves $X_0(N)$*, Math. Comp. **93** (2024), no. 347, 1371–1397, DOI 10.1090/mcom/3902. MR4708039

[4] V. Arul and J. S. Müller, *Rational points on $X_0^+(125)$*, Expo. Math. **41** (2023), no. 3, 709–717, DOI 10.1016/j.exmath.2023.02.009. MR4644846

[5] 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*, Arithmetic L-functions and differential geometric methods, Progr. Math., vol. 338, Birkhäuser/Springer, Cham, [2021] ©2021, pp. 31–74, DOI 10.1007/978-3-030-65203-6_2. MR4311238

[6] 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*, Ann. of Math. (2) **189** (2019), no. 3, 885–944, DOI 10.4007/annals.2019.189.3.6. MR3961086

[7] J. S. Balakrishnan, N. Dogra, J. S. Müller, J. Tuitman, and J. Vonk, *Quadratic Chabauty for modular curves: Algorithms and examples*, Compos. Math. **159** (2023), no. 6, 1111–1152, DOI 10.1112/s0010437x23007170. MR4589060

[8] J. S. Balakrishnan, A. Besser, F. Bianchi, and J. S. Müller, *Explicit quadratic Chabauty over number fields*, Israel J. Math. **243** (2021), no. 1, 185–232, DOI 10.1007/s11856-021-2158-5. MR4299146

[9] J. S. Balakrishnan and N. Dogra, *Quadratic Chabauty and rational points, I: p-adic heights*, Duke Math. J. **167** (2018), no. 11, 1981–2038, DOI 10.1215/00127094-2018-0013. With an appendix by J. Steffen Müller. MR3843370

[10] J. S. Balakrishnan, B. Mazur, SageMath code, `https://github.com/jbalakrishnan/QC_bielliptic`, 2023.

[11] J. S. Balakrishnan, J. S. Müller, *Computational tools for quadratic Chabauty*, Arizona Winter School Lecture notes 2020.

[12] B. S. Banwait, *Explicit isogenies of prime degree over quadratic fields*, Int. Math. Res. Not. IMRN **14** (2023), 11829–11876, DOI 10.1093/imrn/rnac134. MR4615219

[13] B. S. Banwait, *Explicit isogenies of prime degree over quadratic fields*, Int. Math. Res. Not. IMRN **14** (2023), 11829–11876, DOI 10.1093/imrn/rnac134. MR4615219

[14] B. S. Banwait, F. Najman, and O. Padurariu, *Cyclic isogenies of elliptic curves over fixed quadratic fields*, Math. Comp. **93** (2024), no. 346, 841–862, DOI 10.1090/mcom/3894. MR4678586

[15] F. Bars, *Bielliptic modular curves*, J. Number Theory **76** (1999), no. 1, 154–165, DOI 10.1006/jnth.1998.2343. MR1688168

[16] A. Besser, J. S. Müller, and P. Srinivasan, *p-adic adelic metrics and quadratic Chabauty I*, Preprint, `arXiv:2112.03873`, (2021).

[17] F. Bianchi, *Quadratic Chabauty for (bi)elliptic curves and Kim's conjecture*, Algebra Number Theory **14** (2020), no. 9, 2369–2416, DOI 10.2140/ant.2020.14.2369. MR4172711

[18] F. Bianchi and O. Padurariu, *Rational points on rank 2 genus 2 bielliptic curves in the LMFDB*, LuCaNT: LMFDB, computation, and number theory, Contemp. Math., vol. 796, Amer. Math. Soc., [Providence], RI, [2024] ©2024, pp. 215–242, DOI 10.1090/conm/796/16003. MR4732689

[19] S. Bloch and K. Kato, *L-functions and Tamagawa numbers of motives*, The Grothendieck Festschrift, Vol. I, Progr. Math., vol. 86, Birkhäuser Boston, Boston, MA, 1990, pp. 333–400. MR1086888

[20] A. Bourdon, Ö. Ejder, Y. Liu, F. Odumodu, and B. Viray, *On the level of modular curves that give rise to isolated j-invariants*, Adv. Math. **357** (2019), 106824, 33, DOI 10.1016/j.aim.2019.106824. MR4016915

[21] J. Box, *Quadratic points on modular curves with infinite Mordell–Weil group*, Math. Comp. **90** (2021), no. 327, 321–343, DOI 10.1090/mcom/3547. MR4166463

[22] J. Box, S. Gajović, and P. Goodman, *Cubic and quartic points on modular curves using generalised symmetric Chabauty*, Int. Math. Res. Not. IMRN **7** (2023), 5604–5659, DOI 10.1093/imrn/rnab358. MR4565697

[23] P. Bruin and F. Najman, *Hyperelliptic modular curves $X_0(n)$ and isogenies of elliptic curves over quadratic fields*, LMS J. Comput. Math. **18** (2015), no. 1, 578–602, DOI 10.1112/S1461157015000157. MR3389884

[24] L. Caporaso, J. Harris, and B. Mazur, *Uniformity of rational points: An update and corrections*, Tunis. J. Math. **4** (2022), no. 1, 183–201, DOI 10.2140/tunis.2022.4.183. MR4401791

[25] L. Caporaso, J. Harris, and B. Mazur, *Uniformity of rational points*, J. Amer. Math. Soc. **10** (1997), no. 1, 1–35, DOI 10.1090/S0894-0347-97-00195-1. MR1325796

[26] R. F. Coleman, *Dilogarithms, regulators and p-adic L-functions*, Invent. Math. **69** (1982), no. 2, 171–208, DOI 10.1007/BF01399500. MR674400

[27] R. F. Coleman, *Torsion points on curves and p-adic abelian integrals*, Ann. of Math. (2) **121** (1985), no. 1, 111–168, DOI 10.2307/1971194. MR782557

[28] R. F. Coleman, *Effective Chabauty*, Duke Math. J. **52** (1985), no. 3, 765–770, DOI 10.1215/S0012-7094-85-05240-8. MR808103

[29] R. F. Coleman and B. H. Gross, *p-adic heights on curves*, Algebraic number theory, Adv. Stud. Pure Math., vol. 17, Academic Press, Boston, MA, 1989, pp. 73–81, DOI 10.2969/aspm/01710073. MR1097610

[30] B. Conrad, B. Edixhoven, and W. Stein, *$J_1(p)$ has connected fibers*, Doc. Math. **8** (2003), 331–408. MR2029169

[31] David Corwin, *From Chabauty's method to Kim's non-abelian Chabauty's method*, `https://math.berkeley.edu/~dcorwin/files/ChabautytoKim.pdf`, 2019.

[32] M. Derickx, *Torsion points on elliptic curves over number fields of small degree*, Several variations of Kamienny's criterion, `https://wstein.org/wiki/attachments/seminar(2f)nt(2f)20110318/slides.pdf`

[33] M. Derickx, A. Etropolski, M. van Hoeij, J. S. Morrow, and D. Zureick-Brown, *Sporadic cubic torsion*, Algebra Number Theory **15** (2021), no. 7, 1837–1864, DOI 10.2140/ant.2021.15.1837. MR4333666

[34] B. Edixhoven and G. Lido, *Geometric quadratic Chabauty*, J. Inst. Math. Jussieu **22** (2023), no. 1, 279–333, DOI 10.1017/S1474748021000244. MR4556934

[35] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern* (German), Invent. Math. **73** (1983), no. 3, 349–366, DOI 10.1007/BF01388432. MR718935

[36] G. Faltings, *Diophantine approximation on abelian varieties*, Ann. of Math. (2) **133** (1991), no. 3, 549–576, DOI 10.2307/2944319. MR1109353

[37] G. Faltings, *The general case of S. Lang's conjecture*, Barsotti Symposium in Algebraic Geometry (Abano Terme, 1991), Perspect. Math., vol. 15, Academic Press, San Diego, CA, 1994, pp. 175–182. MR1307396

[38] S. D. Galbraith, *Rational points on $X_0^+(p)$*, Experiment. Math. **8** (1999), no. 4, 311–318. MR1737228

[39] S. D. Galbraith, *Rational points on $X_0^+(N)$ and quadratic $\mathbb{Q}$-curves* (English, with English and French summaries), J. Théor. Nombres Bordeaux **14** (2002), no. 1, 205–219. MR1925998

[40] J. González, J.-C. Lario, and J. Quer, *Arithmetic of $\mathbb{Q}$-curves*, Modular curves and abelian varieties, Progr. Math., vol. 224, Birkhäuser, Basel, 2004, pp. 125–139. MR2058647

[41] R. Hain and M. Matsumoto, *Weighted completion of Galois groups and Galois actions on the fundamental group of $\mathbb{P}^1 - \{0, 1, \infty\}$*, Compositio Math. **139** (2003), no. 2, 119–167, DOI 10.1023/B:COMP.0000005077.42732.93. MR2025807

[42] J. Harris and J. Silverman, *Bielliptic curves and symmetric products*, Proc. Amer. Math. Soc. **112** (1991), no. 2, 347–356, DOI 10.2307/2048726. MR1055774

[43] B. Kadets and I. Vogt, *Subspace configurations and low degree points on curves*, Adv. Math. **460** (2025), Paper No. 110021, 36, DOI 10.1016/j.aim.2024.110021. MR4828751

[44] S. Kamienny, *Points of order p on elliptic curves over $\mathbf{Q}(\sqrt{p})$*, Math. Ann. **261** (1982), no. 4, 413–424, DOI 10.1007/BF01457444. MR682654

[45] S. Kamienny, *Torsion points on elliptic curves over all quadratic fields*, Duke Math. J. **53** (1986), no. 1, 157–162, DOI 10.1215/S0012-7094-86-05310-X. MR835802

[46] S. Kamienny, *On the torsion subgroups of elliptic curves over totally real fields*, Invent. Math. **83** (1986), no. 3, 545–551, DOI 10.1007/BF01394421. MR827366

[47] S. Kamienny, *Torsion points on elliptic curves over all quadratic fields. II* (English, with French summary), Bull. Soc. Math. France **114** (1986), no. 1, 119–122. MR860654

[48] S. Kamienny, *Torsion points on elliptic curves*, Bull. Amer. Math. Soc. (N.S.) **23** (1990), no. 2, 371–373, DOI 10.1090/S0273-0979-1990-15935-X. MR1058689

[49] S. Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms*, Invent. Math. **109** (1992), no. 2, 221–229, DOI 10.1007/BF01232025. MR1172689

[50] S. Kamienny, *Torsion points on elliptic curves*, Bull. Amer. Math. Soc. (N.S.) **23** (1990), no. 2, 371–373, DOI 10.1090/S0273-0979-1990-15935-X. MR1058689

[51] S. Kamienny and B. Mazur, *Rational torsion of prime order in elliptic curves over number fields*, Astérisque **228** (1995), 3, 81–100. With an appendix by A. Granville; Columbia University Number Theory Seminar (New York, 1992). MR1330929

[52] E. Katz and D. Zureick-Brown, *The Chabauty–Coleman bound at a prime of bad reduction and Clifford bounds for geometric rank functions*, Compos. Math. **149** (2013), no. 11, 1818–1838, DOI 10.1112/S0010437X13007410. MR3133294

[53] M. A. Kenku, *Rational 2^n-torsion points on elliptic curves defined over quadratic fields*, J. London Math. Soc. (2) **11** (1975), no. 1, 93–98, DOI 10.1112/jlms/s2-11.1.93. MR379508

[54] M. A. Kenku, *Certain torsion points on elliptic curves defined over quadratic fields*, J. London Math. Soc. (2) **19** (1979), no. 2, 233–240, DOI 10.1112/jlms/s2-19.2.233. MR533321

[55] M. A. Kenku, *The modular curve $X_0(39)$ and rational isogeny*, Math. Proc. Cambridge Philos. Soc. **85** (1979), no. 1, 21–23, DOI 10.1017/S0305004100055444. MR510395

[56] M. A. Kenku, *The modular curve $X_0(169)$ and rational isogeny*, J. London Math. Soc. (2) **22** (1980), no. 2, 239–244, DOI 10.1112/jlms/s2-22.2.239. MR588271

[57] M. A. Kenku, *The modular curves $X_0(65)$ and $X_0(91)$ and rational isogeny*, Math. Proc. Cambridge Philos. Soc. **87** (1980), no. 1, 15–20, DOI 10.1017/S0305004100056462. MR549292

[58] M. A. Kenku, *On the modular curves $X_0(125)$, $X_1(25)$ and $X_1(49)$*, J. London Math. Soc. (2) **23** (1981), no. 3, 415–427, DOI 10.1112/jlms/s2-23.3.415. MR616546

[59] M. A. Kenku, *Rational torsion points on elliptic curves defined over quadratic fields*, J. Nigerian Math. Soc. **2** (1983), 1–16. MR780869

[60] M. A. Kenku and F. Momose, *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. **109** (1988), 125–149, DOI 10.1017/S0027763000002816. MR931956

[61] M. Kim, *The unipotent Albanese map and Selmer varieties for curves*, Publ. Res. Inst. Math. Sci. **45** (2009), no. 1, 89–133, DOI 10.2977/prims/1234361156. MR2512779

[62] M. Kim, *The motivic fundamental group of $\mathbf{P}^1\backslash\{0,1,\infty\}$ and the theorem of Siegel*, Invent. Math. **161** (2005), no. 3, 629–656, DOI 10.1007/s00222-004-0433-9. MR2181717

[63] M. Kim, *Massey products for elliptic curves of rank 1*, J. Amer. Math. Soc. **23** (2010), no. 3, 725–747, DOI 10.1090/S0894-0347-10-00665-X. MR2629986

[64] D. S. Kubert and S. Lang, *Modular units*, Grundlehren der Mathematischen Wissenschaften, vol. 244, Springer-Verlag, New York-Berlin, 1981. MR648603

[65] The LMFDB Collaboration, *The L-functions and modular forms database*, `https://www.lmfdb.org`, 2024, [Online; accessed 27 March 2024].

[66] D. J. Lorenzini, *Torsion points on the modular Jacobian $J_0(N)$*, Compositio Math. **96** (1995), no. 2, 149–172. MR1326710

[67] B. Mazur, *Rational points on modular curves*, Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976), Lecture Notes in Math., Vol. 601, Springer, Berlin-New York, 1977, pp. 107–148. MR450283

[68] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. **47** (1977), 33–186 (1978). With an appendix by Mazur and M. Rapoport. MR488287

[69] B. Mazur, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. **44** (1978), no. 2, 129–162, DOI 10.1007/BF01390348. MR482230

[70] B. Mazur and K. Rubin, *Diophantine stability*, Amer. J. Math. **140** (2018), no. 3, 571–616, DOI 10.1353/ajm.2018.0014. With an appendix by Michael Larsen. MR3805014

[71] B. Mazur and P. Swinnerton-Dyer, *Arithmetic of Weil curves*, Invent. Math. **25** (1974), 1–61, DOI 10.1007/BF01389997. MR354674

[72] B. Mazur and J. Tate, *Points of order* 13 *on elliptic curves*, Invent. Math. **22** (1973/74), 41–49, DOI 10.1007/BF01425572. MR347826

[73] B. Mazur, *Thoughts about Mordell and uniformity of finiteness bounds*, `https://sites.harvard.edu/barry-mazur/files/2023/01Thoughts-about-Mordell-and-Uniformity-of-`

finiteness-bounds.pdf (a lecture in) the conference *Mordell 2022*, Cambridge University, August 15–19, 2022.

[74] M. McQuillan, *Quelques compléments à une démonstration de Faltings* (French, with English and French summaries), C. R. Acad. Sci. Paris Sér. I Math. **319** (1994), no. 7, 649–652. MR1300063

[75] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres* (French), Invent. Math. **124** (1996), no. 1-3, 437–449, DOI 10.1007/s002220050059. MR1369424

[76] P. Michaud-Rodgers, *Quadratic points on non-split Cartan modular curves*, Int. J. Number Theory **18** (2022), no. 2, 245–267, DOI 10.1142/S1793042122500178. MR4390660

[77] F. Momose, *p-torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. **96** (1984), 139–165, DOI 10.1017/S0027763000021206. MR771075

[78] F. Momose, *Rational points on the modular curves* $X_{\mathrm{split}}(p)$, Compositio Math. **52** (1984), no. 1, 115–137. MR742701

[79] F. Najman and B. Vukorepa, *Quadratic points on bielliptic modular curves*, Math. Comp. **92** (2023), no. 342, 1791–1816, DOI 10.1090/mcom/3805. MR4570342

[80] J. Nekovář, *On p-adic height pairings*, Séminaire de Théorie des Nombres, Paris, 1990–91, Progr. Math., vol. 108, Birkhäuser Boston, Boston, MA, 1993, pp. 127–202, DOI 10.1007/s10107-005-0696-y. MR1263527

[81] A. P. Ogg, *Hyperelliptic modular curves*, Bull. Soc. Math. France **102** (1974), 449–462. MR364259

[82] A. P. Ogg, *Diophantine equations and modular forms*, Bull. Amer. Math. Soc. **81** (1975), 14–27, DOI 10.1090/S0002-9904-1975-13623-8. MR354675

[83] A. P. Ogg, *On the cusps of* $\Gamma_0(N)$, Proceedings of the 1972 Number Theory Conference (Univ. Colorado, Boulder, Colo.), University of Colorado, Boulder, CO, 1972, pp. 173–177. MR393037

[84] A. P. Ogg, *Rational points of finite order on elliptic curves*, Invent. Math. **12** (1971), 105–111, DOI 10.1007/BF01404654. MR291084

[85] A. P. Ogg, *Über die Automorphismengruppe von* $X_0(N)$ (German), Math. Ann. **228** (1977), no. 3, 279–292, DOI 10.1007/BF01420295. MR562500

[86] M. Ohta, *Eisenstein ideals and the rational torsion subgroups of modular Jacobian varieties*, J. Math. Soc. Japan **65** (2013), no. 3, 733–772. MR3084978

[87] M. Ohta, *Eisenstein ideals and the rational torsion subgroups of modular Jacobian varieties II*, Tokyo J. Math. **37** (2014), no. 2, 273–318, DOI 10.3836/tjm/1422452795. MR3304683

[88] E. Ozman and S. Siksek, *Quadratic points on modular curves*, Math. Comp. **88** (2019), no. 319, 2461–2484, DOI 10.1090/mcom/3407. MR3957901

[89] P. Parent, *Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres* (French, with French summary), J. Reine Angew. Math. **506** (1999), 85–116, DOI 10.1515/crll.1999.009. MR1665681

[90] Y. Ren, *Rational torsion subgroups of modular Jacobian varieties*, J. Number Theory **190** (2018), 169–186, DOI 10.1016/j.jnt.2018.02.009. MR3805452

[91] Y. Ren, *Quadratic torsion subgroups of modular Jacobian varieties*, Israel J. Math. **245** (2021), no. 2, 675–710, DOI 10.1007/s11856-021-2223-0. MR4358260

[92] K. A. Ribet and P. Wake, *Another look at rational torsion of modular Jacobians*, Proc. Natl. Acad. Sci. USA **119** (2022), no. 41, Paper No. e2210032119, 8. MR4512691

[93] N. Schappacher and R. Schoof, *Beppo Levi and the arithmetic of elliptic curves*, Math. Intelligencer **18** (1996), no. 1, 57–69, DOI 10.1007/BF03024818. MR1381581

[94] J.-P. Serre, *Topics in Galois theory*, Research Notes in Mathematics, vol. 1, Jones and Bartlett Publishers, Boston, MA, 1992. Lecture notes prepared by Henri Damon [Henri Darmon]; With a foreword by Darmon and the author. MR1162313

[95] S. Siksek, *Chabauty for symmetric powers of curves*, Algebra Number Theory **3** (2009), no. 2, 209–236, DOI 10.2140/ant.2009.3.209. MR2491943

[96] S. Siksek, *Quadratic Chabauty for modular curves*, Preprint, arXiv:1704.00473, 2017.

[97] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, New York, 1986, DOI 10.1007/978-1-4757-1920-8. MR817210

[98] A. V. Sutherland, *Torsion subgroups of elliptic curves over number fields*, https://math.mit.edu/~drew/MazursTheoremSubsequentResults.pdf

[99] T. Takagi, *The cuspidal class number formula for the modular curves* $X_0(M)$ *with* M *square-free*, J. Algebra **193** (1997), no. 1, 180–213, DOI 10.1006/jabr.1996.6993. MR1456573

[100] A. Trbović, *Torsion groups of elliptic curves over quadratic fields* $\mathbb{Q}(\sqrt{d})$*,* $0 < d < 100$, Acta Arith. **192** (2020), no. 2, 141–153, DOI 10.4064/aa180725-8-1. MR4042408

[101] I. B. Viray and I. Vogt, *Isolated and parameterized points on curves*, Preprint, `arXiv:2406.14353v1`, 2024.

[102] P. Vojta, *Siegel's theorem in the compact case*, Ann. of Math. (2) **133** (1991), no. 3, 509–548, DOI 10.2307/2944318. MR1109352

[103] P. Vojta, *Applications of arithmetic algebraic geometry to Diophantine approximations*, Arithmetic algebraic geometry (Trento, 1991), Lecture Notes in Math., vol. 1553, Springer, Berlin, 1993, pp. 164–208, DOI 10.1007/BFb0084730. MR1338861

[104] H. Yoo, *Rational torsion points on Jacobians of modular curves*, Acta Arith. **172** (2016), no. 4, 299–304, DOI 10.4064/aa8140-12-2015. MR3471044

[105] U. Zannier, *Torsion in algebraic groups and problems which arise*, European Congress of Mathematics, EMS Press, Berlin, [2023] ©2023, pp. 161–180. MR4615742

[106] S. Zhang, *Small points and adelic metrics*, J. Algebraic Geom. **4** (1995), no. 2, 281–300. MR1311351

Department of Mathematics and Statistics, Boston University, Boston, Massachusetts 02215
Email address: `jbala@bu.edu`

Department of Mathematics, Harvard University, Cambridge, Massachusetts 02138
Email address: `mazur@math.harvard.edu`