Thoughts about Andrew Ogg's (Torsion) Conjecture

Barry Mazur

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[1]

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.

My talk will discuss this and recent related work[2] .

[1]Here's just one (tiny) instance of the many times I was indebted to Ogg's guidance and appreciated his jovial and joyful way of thinking: As Tate and I recorded in one of our papers [29]:

"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.

[2]I want to thank the organizers of the conference (*Talks Celebrating the Ogg Professorship in Mathematics - October 13, 2022*): these notes constitute background material for my lecture at that conference. I also want to thank Barinder Banwait, Maarten Derickx, Filip Najman, Ken Ribet and Preston Wake for their illuminating comments (and general conversation) that helped me prepare for my talk.

1. An overview

Let K be a number field, and denote by G_K its absolute Galois group, i.e.

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

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

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

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 C's 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 C's with trivial G_K-action in which case you are asking about **K-rational torsion points on abelian varieties**.
- You might also 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,
- and, of course, fix the dimension of the abelian varieties you are considering.

2. 'Geometrization' of the Problem

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've framed a *representable moduli problem*—and the algebraic variety in question is called the *moduli space representing that moduli problem.*

3. 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 $\mathbb{Q}$:

$$\begin{array}{ll} \text{torsion points of order } N: & \begin{tikzcd} Y_1(N) \arrow[r, "\subset"] \arrow[d] & X_1(N) \arrow[d] \\ Y_0(N) \arrow[r, "\subset"] & X_0(N) \end{tikzcd} \\ \text{cyclic isogenies of degree } N: & \end{array}$$

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 projective smooth completion of $Y_1(N)$ given by the adjunction of a finite set of 'cusps'.

And similarly: the classification of elliptic curves defined over K *possessing a K-rational cyclic isogeny of degree N* is given by the K-rational points of the affine curve $Y_0(N)$—with $X_0(N)$ being the corresponding smooth projective completion.

4. The geometric formulation comes with a number of side-benefits.

Here are two:

(i) 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.

(ii) If it is of genus > 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 cyclic N-isogenies to questions about the Mordell-Weil group (of K-rational points of) the abelian variety $J_0(N)$.

(iii) 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 $Symm^p(\mathcal{M})$—

essentially classifies the same problem ranging over *all* extensions of K of degree p.

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

$$Symm^p(X_0(N)) \quad \hookrightarrow \quad J_0(N)$$

given by:

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

is an embedding if $N >> p$, 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 $\mathbb{Q}$ (when $N >> p$).

5. Andrew Ogg's Torsion Conjecture(s) (1973)

Andrew's Torsion Conjectures taken in broad terms can be formulated in terms of "the geometrization(s)," 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):

(i) **Conjecture 1:** 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[3] .

Put in another way: an isomorphism class occurs if and only 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, Andrew's article [33] discusses the curious case of $X_0(37)$ which has two noncuspical $\mathbb{Q}$-rational points, these being the images of the hyperelliptic involution (a non-modular involution) applied to the two cusps, both cusps being $\mathbb{Q}$-rational. Andrew 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.

(ii) Let $J_0(N)$ denote the jacobian of $X_0(N)$. Noting that the cusps of $X_0(N)$ map to torsion points of $J_0(N)$, denote by $C_0(N) \subset J_0(N)_{\text{tors}} \subset J_0(N)$ the subgroup generated by those cusps.

---

[3] A form of this conjecture was made by Beppo Levi in his 1908 ICM address in Rome. See [43] which gives a wonderful account of the story of Beppo 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 curves $\{n \cdot P\}$ $n = 1, 2, 3, \ldots$ a "failure" if it loops finitely—i.e., if P is a torsion point; his aim is to classify such "failures."

$$\begin{tikzcd}
\text{Cusps in } X_0(N) \arrow[d] \arrow[dr] & \\
C_0(N) \arrow[d] & X_0(N) \arrow[d] \\
J_0(N)_{\mathrm{tors}} \arrow[r, "\subset"] & J_0(N)
\end{tikzcd}$$

we have another, seemingly quite different type of conjecture:

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

$$C_0(N) = J_0(N)_{\mathrm{tors}}(\mathbb{Q}) \quad \subset \quad J_0(N)(\mathbb{Q})$$

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

That these two conjectures are interlinked is a long story (cf. [27], [28]).

A. Conjecture 1 is known. Specifically, 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 $1 \le n \le 10$, and also C_{12}, and
- the direct sum of C_2 with C_{2m}, for $1 \le m \le 4$.

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].

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:

B. Torsion on elliptic curves over quadratic number fields.

Theorem 1. *(Momose, Kenku, Kamienny) Let K range through all quadratic number fields, and E all elliptic curves over these fields. Then the torsion subgroup $E(K)_{\mathrm{tors}}$ of $E(K)$ is isomorphic to one of the following 26 groups:*

- *C_n for $1 \le n \le 18,\ n \ne 17$,*
- *the direct sum of C_2 with C_{2m} for $1 \le m \le 6$,*

[4] See [45] where it is proved that each of these groups appears as a possible torsion group over any quadratic field.

- *the direct sum of C_3 with C_{3m} for $m = 1, 2$,*
- *$C_4 \oplus C_4$.*

C. Torsion on elliptic curves over cubic number fields.

Theorem 2. *(Derickx, Ttropolski, Van Hoeij, Morrow, Zureick-Brown) Let K range through all cubic number fields, and E all elliptic curves over these fields. Then the torsion subgroup $E(K)_{\mathrm{tors}}$ 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 162b1 to $\mathbb{Q}(\zeta_9)^+$ is the unique elliptic curve over a cubic field K with K-rational torsion group isomorphic to C_{21}.

6. Conjecture 2 expanded

- The order of the $C_0(N)$ had been computed for square-free N thanks to Kubert, Lang, and Takagi (see ref. 4 for an example). In this case (i.e., N square-free) the set of cusps are $\mathbb{Q}$-rational.
- Ohta ([38], [39])) has proved a generalization of Ogg's conjecture in the context of square-free N. That is, he proved that the p-primary parts of $J_0(N)_{\mathrm{tors}}(\mathbb{Q})$ and of $C_0(N)$ are equal for $p \geq 5$ and $p = 3$ if 3 doesn't divide N.

  Related to this, see [26], [12], [38], [39], [46], and [40], [41]. And just last week the PNAS article [42] (*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 squarefree, the cuspidal subgroup of $J_0(N)$ may not consist entirely of rational points; nevertheless:

  Conjecture 2':

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

7. Conjecture 2 further expanded

Now let $\mathcal{X}$ (over $\mathbb{Q}$) denote either $X_0(N)$ or $X_1(N)$ for some $N \geq 1$. Let $\mathcal{J}$ be the Jacobian of $\mathcal{X}$, and

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

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's an exact sequence

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

Define the **cuspidal defect** of $\mathcal{X}$ to be the cokernel of

$$\mathcal{C}(\bar{\mathbb{Q}}) = \mathcal{C}(K) \hookrightarrow \mathcal{J}(K)_{\mathrm{tors}}. \tag{3}$$

Conjecture 2": The 'cuspidal defect' of any $\mathcal{X}$ listed above is trivial.

8. Remarkable 'Diophantine Stability'

Definition 4. 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 1 tells us that:

Corollary 5. *For all but finitely many positive numbers N, the curve $X_1(N)$ (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.

Karl Rubin and I have a theorem:

Theorem 6 (Theorem 1.2 of [30])**.** *Suppose A is a simple abelian variety over K and all $\bar{K}$-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.

which Karl and I think is hardly 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 > 5.

9. $\mathbb{Q}$-rational cyclic isogenies

It has long been known, thanks to a tradition of work (cf. [28] and a sequence of papers of M.A. Kenku ([21], [22], [23], [24]) that 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 can be given 'geometric reasons' for existing; e.g., the 37-isogenies 'come by' applying the hyperelliptic involution (it is non-modular!) to the cusps of $X_0(37)$.

So, what about uniformity results regarding cyclic N-isogenies of elliptic curves ranging over *all* quadratic fields?

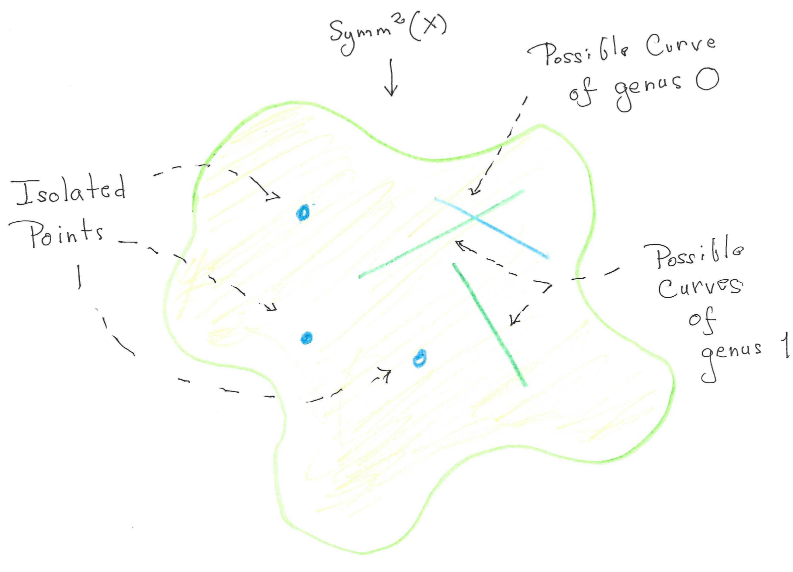
10. *'Expected' and 'Unexpected'* L-RATIONAL CYCLIC ISOGENIES FOR L RANGING THROUGH QUADRATIC FIELDS

A corollary of a theorem of Faltings[5] is that:

Corollary 7. *(Faltings) 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—of genus 0 or 1, or—hyperelliptic or bielliptic (over K).*

And, for a hyperelliptic and/or bielliptic curve X defined over K, Faltings proves that there are only finitely many quadratic points (relative to K) that are *not parametrized by an infinite system of quadratic points* arising by X being the double cover of a rational curve Y with a K-rational point; or an elliptic curve of Mordell-Weil rank > 0 over K):

$$\begin{tikzcd}
\pi^{-1}(Y(K)) \arrow[r, "\subset"] \arrow[d, "\pi"] & X(\bar{K}) \arrow[d, "\pi"] \\
Y(K) \arrow[r, "\subset"] & Y(\bar{K}).
\end{tikzcd}$$



[5] For a 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 my talk *Thoughts about Mordell and uniformity of finiteness bounds:* `https://people.math.harvard.edu/~mazur/papers/M.pdf`

A. Isolated quadratic points. Call the set of quadratic points of X that are not among such (infinite) systems of parametrized quadratic points **isolated points**. The infinite systems 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 is classified by a K-rational point of $X_0(N)$. Such a point is therefore also 'expected." So:

B. Sporadic quadratic points.

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

- it is not a cusp,

and

- *is* isolated; i.e.,
  - 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* the inverse image of a $\mathbb{Q}$-rational point in an elliptic curve E via a bielliptic covering (i.e., a degree 2 mapping $X_0(N) \to E$), in the case where $X_0(N)$ is bielliptic,

and

- is not a point of $X_0(N)$ classifying a CM elliptic curve and cyclic isogeny of degree N as described above.

Conjecture 9. *Ranging over all $X_0(N)$'s for $N \in \mathbb{Z}_{\geq 1}$ there are only finitely many sporadic quadratic points.*

> Following the quotation I gave of Andrew's view regarding rational torsion, I'm guessing that both of us are certainly 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 points of all of the curves $X_0(N)$ that are hyperelliptic or bielliptic have been computed.

Sheldon Kamienny, on reading these notes, 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?*

11. Hyperelliptic $X_0(N)$

A classical theorem of Ogg [33] gives the nineteen values of N for which $X_0(N)$ is hyperelliptic (we take 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 [9] (which has other interesting results as well). The case of $X_0(37)$ is taken care of in Josha Box's paper [8], 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 10. *(Francesc Bar [7]) These are the 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 the above table for which we did not know the set of their isolated quadratic points. Thanks to Filip Najman and Borna Vukorepa ([32]) we now have computation of the isolated quadratic points for all bielliptic curves $X_0(N)$ (as we also do for all hyperelliptic $X_0(N)$).

12. Exotic quadratic points

Let N be prime, and $w_N : X_0(N) \to X_0(N)$ 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 multiplicative 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 11. For N prime such that $X_0(N)^+$ of genus > 1, call a quadratic point P of $X_0(N)$ **exotic (quadratic)** if

- it is not a cusp,
- is not a point of $X_0(N)$ classifying a CM elliptic curve (and cyclic isogeny of degree N)

and

- $\pi(P)$ is a $\mathbb{Q}$-rational point of $X_0(N)^+$.

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

$$E \overset{N}{\leftrightarrow} E'$$

and

$$E' \overset{N}{\leftrightarrow} E.$$

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

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

endowed with an endomorphism:

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

So, the exotic quadratic points of $X_0(N)$ correspond to some of the $\mathbb{Q}$-rational points of $X_0^+(N)$. What tools do we have compute those $\mathbb{Q}$-rational points?

The classical method of Chabauty-Coleman computes usable bounds for the numbers 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 to its genus g.

But the Birch and Swinnerton-Dyer conjecture predicts that (for N prime) the rank $r_0(N)^+$ of 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 can't be brought to bear here.

Computationally, we have many examples where there's actual equality:

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

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 powerful approach to compute the set of all $\mathbb{Q}$-rational points[6]. And we have an enormous amount of progress. For example see [2], [3], [4], and [5].

Elkies and Galbraith [14] found exceptional rational points on $X_0^+(N)$ for $N = 73, 91, 103, 191$ (genus 2) and $N = 137, 311$ (genus 4). and in [3] Balakrishnan, Dogra, Müller, Tuitman, and Vonk proved that the only prime values of N with $X_0^+(N)$ of genus 2 or 3 that have an exotic rational point are $N = 73, 103, 191$. Moreover, for prime N, if $X_0^+(N)$ is of genus 3, it has no exotic rational points. The list of curves $X_0(N)^+$ of genus 2 or 3 with N prime is a result of Ogg: We have:

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

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

See also the survey article [16] (and [14], [15]) in which exotic points (found by Elkies and Galbraith) are defined and studied in the context of $\mathbb{Q}$-curves; and for the list of the five known exotic N-isogenies (with N being prime), these being rational over a quadratic field of discriminant Δ:

N	Δ
73	-127
103	$5 \cdot 557$
137	-31159
191	$61 \cdot 229 \cdot 145757$
311	$11 \cdot 17 \cdot 9011 \cdot 23629$

[6] I 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?

Are these the only exotic isogenies? There's lots to be done.

Thanks Andrew for inspiring all of us; thanks to the organizers of the

References

[1] D. Abramovich and J. Harris, Abelian varieties and curves in $W_d(C)$, Compositio Math. **78** 227-238 (1991)

[2] J. Balakrishnan, N. Dogra, J. Müller, J. Tuitman, J. Vonk, Quadratic Chabauty for modular curves: Algorithms and examples (2021) `https://arxiv.org/abs/2101.01862`

[3] J. Balakrishnan, A.Besser, F. Bianchi, J. Müller, Explicit quadratic Chabauty over number fields, `arXiv:1910.04653`

[4] J. Balakrishnan, N. Dogra, Quadratic Chabauty and rational points I: p-adic heights, `arXiv.org>math>arXiv:1601.00388`

[5] J. Balakrishnan, N. Dogra, Quadratic imaginary points on Bring's curve, (recent unpublished).

[6] Barinder S. Banwait, Explicit isogenies of prime degree over quadratic fields `https://arxiv.org/abs/2101.02673`

[7] Francesc Bars, Bielliptic Modular Curves Journal of Number Theory **76**, 154-165 (1999)

[8] Josha Box, Quadratic points on modular curves with infinite Mordell-Weil group, `arXiv:1906.05206v3`

[9] P. Bruin, F. Najman, Hyperelliptic modular curves and isogenies of elliptic curves over quadratic fields, LMS Journal of Computation and Mathematics (2015)

[10] L. Caporaso, J. Harris, B. Mazur Corrections to *Uniformity of rational points* and further comments, `https://arxiv.org/abs/2012.14461`

[11]] L. Caporaso, J. Harris, and B. Mazur, Uniformity of rational points. J. Amer. Math. Soc., **10** 1-5 (1997)

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

[13] Derickx, M., Etropolski, A., van Hoeij, M., Morrow, J.S., Zureick-Brown, Sporadic Cubic Torsion, `arXiv:2007.13929`

[14] S. D. Galbraith. Rational points on $X_0^+(p)$ Experiment. Math.,**8** (4) 311-318 (1999)

[15] S. D. Galbraith. Rational points on $X_0^+(p)$ and quadratic $\mathbb{Q}$-curves. J. Théor. Nombres Bordeaux, **14**(1) 205-219 (2002)

[16] Gonzalez, J., Lario, J-C., Quer, J., Arithmetic of $\mathbb{Q}$-curves, Progress in Mathematics, **224,** 125-139 (2004)

[17] S. Kamienny, Torsion points on elliptic curves over all quadratic fields, Duke Mathematical Journal, **53** 157-162 (1986)

[18] S. Kamienny, Torsion points on Elliptic Curves over all quadratic fields II, Bull. Soc. Math. de France. bf 114 (1986) 119-122

[19] S.n Kamienny, Torsion points on elliptic curves. Proceedings of the Conference on Number Theory, (1991) 12-15, GH Essen Preprint Series (G. Frey, ed.) (1991).

[20] S. Kamienny, B.Mazur, Rational torsion of prime order in elliptic curves over number fields Astérisque, **228** (1995) 81-98 `http://www.numdam.org/item?id=AST_1995__228__81_0`

[21] M.A. Kenku, The modular curve $X_0(39)$ and rational isogeny, Mathematical Proceedings of the Cambridge Philosophical Society, **85**, Cambridge University Press, (1979) 21-23.

[22] M.A. Kenku, The modular curve $X_0(169)$ and rational isogeny, Journal of the London Mathematical Society 2 (1980), no. 2, 239-244.

[23] M.A. Kenku, The modular curves $X_0(65)$ and $X_0(91)$ and rational isogeny, Mathematical Proceedings of the Cambridge Philosophical Society, **87** Cambridge University Press (1980) 15-20.

[24] M.A. Kenku, On the modular curves $X_0(125)$, $X_0(25)$, and $X_0(49)$, Journal of the London Mathematical Society **2** (1981), no. 3, 415-427

[25] M. A. Kenku, F. Momose, Torsion points on elliptic curves defined over quadratic fields, Nagoya Math. J. **109** (1988) 125-149

[26] Lorenzini, D., Torsion points on the modular Jacobian $J_0(N)$. Compos. Math. **96**, 149-172 (1995).

[27] Mazur, B. Rational Isogenies of Prime Degree, Inventiones math. **44** 129-162 (1978)

[28] Mazur, B. Modular curves and the Eisenstein ideal, Publ. Math. IHES **47** 33-186 (1977)
[29] Mazur, B. ,Tate, J. Points of order 13 on elliptic curves, Invent. Math. **22** 41-49 1973)
[30] Mazur, B., Rubin, K. (With an appendix by Michael Larsen) Diophantine stability Amer. J. Math. **140** 571- 616 (2018) https://doi-org.jproxy.lib.ecu.edu/10.1353/ajm.2018.0014
[31] P. Michaud-Rodgers, Quadratic points on non-split Cartan modular curves, https://arxiv.org/pdf/2011.00590
[32] Najman, F., Vukorepa, B., Quadratic points on bielliptic modular curves, arXiv:2112.03226
[33] Andrew Ogg, Hyperelliptic modular curves Bulletin de la S. M. F., **102** 449-462 (1974)
[34] Ogg, A. P. Diophantine equations and modular forms. Bull. Amer. Math. Soc. **81** 14-27 (1975)
[35] Ekin Ozman, Samir Siksek, Quadratic Points on Modular Curves, arXiv.org>math>arXiv:1806.08192 (2018)
[36] Ogg, A. P. On the cusps of $\Gamma_0(N)$), Proceedings of the Number Theory Conference (Univ. Colorado, Boulder, Colo., 173-177 (1972)
[37] Ogg, A. P. Rational points of finite order on elliptic curves. Invent. Math. **12** 105-111 (1971)
[38] Ohta, M., Eisenstein ideals and the rational torsion subgroups of modular Jacobian varieties J. Math. Soc. Japan **65** 733-772 (2013).
[39] Ohta, M. Eisenstein ideals and the rational torsion subgroups of modular Jacobian varieties II.Tokyo J. Math. **37** 273-318 (2014).
[40] Ren, Y., Rational torsion subgroups of modular Jacobian varieties. J. Number Theory **190**, 169-186
[41] Ren, Y., Quadratic torsion subgroups of modular Jacobian varieties, Israel Journal of mathematics, **245** 675-710 (2021),
[42] Ribet, K., Wake, P., Another look at rational torsion of modular Jacobians, PNAS 2022 **119** No. 41 https://doi.org/10.1073/pnas.2210032119
[43] Norbert Schappacher, René Schoof, Beppo Levi and the Arithmetic of Elliptic Curves, The Mathematical Intelligencer **18**, 57-69 (1996) https://irma.math.unistra.fr/~schappa/NSch/Publications_files/1996_RSchNSch.pdf
[44] Andrew V. Sutherland, Torsion subgroups of elliptic curves over number fields, https://math.mit.edu/~drew/MazursTheoremSubsequentResults.pdf
[45] A. Trbovic, Torsion groups of elliptic curves over Quadratic fields $\mathbb{Q}(\sqrt{d}), 0 < d < 100$ (2018) https://arxiv.org/pdf/1806.05993
[46] Yoo, H., Rational torsion points on Jacobians of modular curves. Acta Arith. **172** 299-304 (2016).