TORSION SUBGROUPS OF ELLIPTIC CURVES OVER QUADRATIC FIELDS AND A CONJECTURE OF GRANVILLE

BARINDER S. BANWAIT AND MAARTEN DERICKX

Abstract. We study the problem of determining the groups that can arise as the torsion subgroup of an elliptic curve over a fixed quadratic field, building on work of Kamienny-Najman, Krumm, and Trbović. By employing techniques to study rational points on curves developed by Bruin and Stoll, we determine the possible torsion subgroups of elliptic curves over quadratic fields $\mathbb{Q}(\sqrt{d})$ for all squarefree d with $|d| < 800$, improving on the previously known range of $-5 < d < 26$. We use our computations to study the validity of a conjecture of Granville concerning how many twists of a given hyperelliptic curve admit a nontrivial rational point.

1. Introduction

Let E be an elliptic curve over a number field K. The Mordell-Weil theorem establishes that the group $E(K)$ of K-rational points of E is finitely generated as an abelian group, so one has an isomorphism of groups

$$E(K) \cong E(K)_{tors} \oplus \mathbb{Z}^r,$$

where $E(K)_{tors}$ is a finite abelian group called the **torsion subgroup** of E/K, and r is called the **rank** of E/K.

The question of classifying which possible torsion subgroups may arise as one varies over elliptic curves over a fixed number field K - what in this paper we refer to as **uniformity of torsion over** K - goes back to Levi's 1908 ICM address in Rome [Lev09], in which he conjectured that for $K = \mathbb{Q}$, there are only 15 possible groups that can arise. As is well-known, this conjecture was finally established in Mazur's seminal work [Maz77]; see [SS96] for an interesting history of this landmark result in the arithmetic of elliptic curves.

Theorem 1.1 (Mazur (1977)). *Let E be an elliptic curve over $\mathbb{Q}$. Then $E(\mathbb{Q})_{tors}$ is isomorphic to one of the following* 15 *groups:*

$$\begin{array}{ll} \mathbb{Z}/N\mathbb{Z} & 1 \leq N \leq 10 \text{ or } N = 12; \\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z} & 1 \leq N \leq 4. \end{array}$$

Since Mazur's work in the 70s, much progress has been made towards a closely related question that in the literature is referred to as **strong uniformity of torsion**. Here, instead of fixing a number field K, one fixes an integer d, and asks for a classification $\Phi(d)$ of possible torsion subgroups of *any* elliptic curve over *any* number field of degree d over $\mathbb{Q}$. Mazur's result above establishes this for $d = 1$. Subsequently, in a long series of papers in the 80s by Kenku, Momose, and Kamienny [Kam82, Kam86a, Kam86b, Kam86c, Kam90, Kam92, Ken75, Ken79, Ken81, Ken83, KM88, Mom84a, Mom84b], the $d = 2$ case was studied; the culmination of the work of Kenku and Momose was [KM88], in which they proposed a list of

2010 *Mathematics Subject Classification.* 11G05 (primary), 11Y60, 11G15. (secondary).

26 possible torsion subgroups for elliptic curves over quadratic fields. The authors showed that these 26 groups arise infinitely often as one varies both the elliptic curve and the quadratic field, and moreover showed that this list would be complete if one can show that no elliptic curve over a quadratic field admits a torsion point of prime order $p > 13$. This fact about bounding the so-called **torsion primes** $S(d)$ in degree $d = 2$ by 13 was subsequently established by Kamienny [Kam92]; one therefore has the following result that we refer to as the **Kamienny-Kenku-Momose** (hereafter KKM) classification.

Theorem 1.2 (Kamienny-Kenku-Momose (1992)). *Let E be an elliptic curve over a quadratic field K. Then $E(K)_{tors}$ is isomorphic to one of the following* 26 *groups:*

$$\begin{aligned} &\mathbb{Z}/N\mathbb{Z} && 1 \leq N \leq 16 \text{ or } N = 18;\\ &\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z} && 1 \leq N \leq 6;\\ &\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3N\mathbb{Z} && 1 \leq N \leq 2;\\ &\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}. \end{aligned}$$

Kamienny and Mazur subsequently showed [KM95] that finiteness of $S(d)$ is equivalent to finiteness of $\Phi(d)$, albeit in a non-effective way (that is, knowing exactly what $S(d)$ is does not immediately allow one to determine $\Phi(d)$), and Merel established finiteness of $S(d)$ for all d [Mer96], proving the erstwhile Uniform Boundedness conjecture for torsion primes of elliptic curves over number fields. The only other value of d for which $\Phi(d)$ is known fully is $d = 3$, a recent result due to the second author with Etropolski, van Hoeij, Morrow, and Zureick-Brown [DEvH$^+$21]. There are partial results known for $d = 4, 5, 6$ and 7; see e.g. [DS17] or [Sut12] and the references contained in the introduction there for the state-of-the-art known about strong uniformity in higher degree number fields.

In this paper, however, we will return to the original uniformity question, and attempt to classify the torsion subgroups of elliptic curves over fixed quadratic fields K.

Najman was the first to consider this question, determining which of the 26 groups in the KKM classification actually arise over each of the cyclotomic quadratic fields $\mathbb{Q}(\zeta_3)$ and $\mathbb{Q}(\zeta_4)$ [Naj11]. Very soon thereafter, Kamienny and Najman [KN12] determined the smallest quadratic field (ordered by absolute value of discriminant) realising each of the 26 torsion subgroups in the KKM classification, and obtained results about the rank of elliptic curves having prescribed torsion. This latter phenomenon of the interplay between rank and torsion was further investigated by Bosman, Bruin, Dujella and Najman [BBDN14], and yielded very striking results such as any elliptic curve over any quadratic field with torsion subgroup $\mathbb{Z}/13\mathbb{Z}$ must have even rank.

The idea of determining the torsion subgroups of elliptic curves over all quadratic fields $\mathbb{Q}(\sqrt{d})$ in some range first appears in a paper of Trbović [Trb20], who attempted such a classification for the $0 < d < 100$ that are squarefree; there were however 16 values of d in this range for which she was unable to fully decide on which torsion subgroups arise; more precisely, for these 16 values, it remained undecided whether $\mathbb{Z}/16\mathbb{Z}$ arises as a possible torsion subgroup. Because of these 16 unknowns, a result classifying torsion in a range of d was only established for $0 < d < 26$. Coupling with this Najman's work [Naj11], the range of known quadratic torsion is currently $-5 < d < 26$.

The main result of this paper resolves the situation for these 16 values, considers negative values of d, and significantly extends the range of square free integers considered. To succinctly state our results, we make the following observations:

- the 15 groups in Mazur's classification (which form a subset of the 26 groups in the KKM classification) arise over every quadratic field; see [Trb20, Section 2].
- the groups $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ (respectively, the group $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$) correspond to having full 3 (respectively, 4) torsion, and so by a standard corollary of Galois equivariance of the Weil pairing, can arise only over $\mathbb{Q}(\zeta_3) = \mathbb{Q}(\sqrt{-3})$ (respectively, $\mathbb{Q}(\zeta_4) = \mathbb{Q}(\sqrt{-1})$).

This reduces the problem to determining, for each quadratic field in our range, which of the remaining 8 torsion subgroups arise over that quadratic field. For a group $\mathbb{Z}/M\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z}$ (with $M|N$) and a positive integer B, we therefore make the following definition:

$$T_B(M,N) := \left\{ |d| < B \text{ squarefree } : \mathbb{Z}/M\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z} \text{ is a torsion group over } \mathbb{Q}(\sqrt{d}) \right\}.$$

Based on the convention that is used for modular curves, we write $T_B(N) := T_B(1,N)$. Our task is then to determine, for some chosen value of B, the 8 sets

$$\begin{aligned} \text{genus 1} &: T_B(11), T_B(14), T_B(15), T_B(2,10), T_B(2,12) \\ \text{genus 2} &: T_B(13), T_B(16), T_B(18). \end{aligned} \tag{1.1}$$

These sets have been labelled with a genus that corresponds to the genus of the modular curve $X_1(M,N)$ that plays the role of a moduli space of elliptic curves having $\mathbb{Z}/M\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z}$ as a subgroup of their torsion subgroup, and the genus plays a significant role in the arithmetic geometry of these modular curves. The genus 2 cases pose a more significant challenge, and most of the paper will be focussed on these three cases. Indeed, Kamienny and Najman [KN12] already showed that determination of the genus 1 sets above correspond to computing whether the rank of the d-twist of each of the associated (elliptic) modular curves is positive; we carry this out for $B = 10{,}000$ in Section 2.

We may now state our main result.

Theorem 1.3. *(1) Letting S_{13} denote the set*

$$\begin{aligned} S_{13} := \{&17, 113, 193, 313, 481, 1153, 1417, \\ &2257, 3769, 3961, 5449, 6217, 6641, 9881\}, \end{aligned}$$

we have

$$S_{13} \subseteq T_{10{,}000}(13) \subseteq S_{13} \cup \{9689\}.$$

(2) Letting S_{18} denote the set

$$S_{18} = \{33, 337, 457, 1009, 1993, 2833, 7369, 8241, 9049\},$$

we have

$$S_{18} \subseteq T_{10{,}000}(18) \subseteq S_{18} \cup \{2841, 4729, 9969\}.$$

(3) We have

$$\begin{aligned} T_{800}(16) = \{&-671, -455, -290, -119, -15, 10, 15, 41, 51, \\ &70, 93, 105, 205, 217, 391, 546, 609, 679\}. \end{aligned}$$

Together with the aforementioned computation of ranks of twists of the five elliptic modular curves alluded to above, this result gives a resolution of the uniformity of torsion question for every quadratic field $\mathbb{Q}(\sqrt{d})$ for $|d| < 800$, offering a significant improvement over the previously known range $-5 < d < 24$. Moreover, for 13 and 18-torsion, only the sets $T_{256}(13)$ and $T_{680}(18)$ were previously known [Kru13, Theorems 2.7.7 and 2.7.8]; this illustrates that parts (1) and (2) above also greatly improve upon previous results.

We briefly describe our methods, based on the aforementioned work of Najman and Trbović, and give an overview of the paper. The problem may be expressed as determining, for each quadratic field $\mathbb{Q}(\sqrt{d})$ in our range, which of the 8 modular curves referred to in (1.1) admit a noncuspidal $\mathbb{Q}(\sqrt{d})$-point. As mentioned above, for the five genus 1 modular curves, Section 2 explains how this essentially boils down to computing the rank of the d-twist of each (elliptic) modular curve, something that we carry out in Magma [BCP97]. The torsion groups $\mathbb{Z}/13\mathbb{Z}$ and $\mathbb{Z}/18\mathbb{Z}$ are dealt with in Section 3, where we use work of Krumm [Kru13] that reduces the problem to determining the existence of a $\mathbb{Q}$-rational point on the d-twist of the modular curves $X_1(13)$ and $X_1(18)$. Krumm already used *two-cover descent* to resolve this problem for many values of d; here we augment this method with two improvements: a necessary condition on the rank of the Jacobian varieties $J_1^d(13)$ and $J_1^d(18)$ of the twisted modular curves, and an application of the *Mordell-Weil sieve*. This yields parts (1) and (2) of Theorem 1.3. The reason for the ambiguity concerning the values 9689, 2841, 4729 and 9969 is that the Mordell-Weil sieve method failed here, as we were unable to find explicit generators of the Mordell-Weil group of the above Jacobians.

Dealing with $\mathbb{Z}/16\mathbb{Z}$ as a possible torsion subgroup is the most difficult, since every twist admits a $\mathbb{Q}$-rational point, so we are essentially forced to compute all $\mathbb{Q}$-rational points, and this is the reason for the significantly smaller value of $B = 800$ in part (3). In this range, the *elliptic curve Chabauty* method is successful in doing this, establishing Part (3) of Theorem 1.3 in Section 4.

Resolving the genus 2 cases comes down to determining whether quadratic twists of these curves in a range admit a nontrivial rational point. This is something that Granville has previously studied [Gra07]; in particular, a conjecture about how many such twists should admit nontrivial points was given there. We compare our results with this conjecture; there is an apparent discrepancy between our data and his conjecture, which we explore in Section 5. Finally in Section 6 we indicate some avenues for future research.

1.1. **Code and computations.** We have used Magma (version V2.28-3) [BCP97] and SageMath [S$^+$12] (version 10.2 using Python 3.9.19) in our computations. The code accompanying our paper has been released under version v1.0.0 at

`https://github.com/isogeny-primes/quadratic-torsion/tree/v1.0.0`

All filenames given in the paper will refer to files in this repository. The computations have been run on a server at the University of Zagreb with an Intel Xeon W-2133 CPU @ 3.60GHz with 12 cores and 64GB of RAM running Ubuntu 18.04.6 LTS. The most memory consuming part of the computation was verifying the algebraic ranks of the twists of the five genus 1 modular curves in Section 2, requiring about 2.5GB of RAM. All other computations used less then 350 MB or RAM. The most time consuming part of the computations is looking for generators of the Mordell-Weil groups of $J_1^d(13)$ and $J_1^d(18)$ for the 20 values of d in eqs. (3.1) and (3.2). The time spend on finding these generators is roughly 2 weeks in total. All other computations combined took less then a week to complete.

More information about runtime of specific computations is described below in the main body of the paper, and can also be found in the `README.md` of the above repository.

Acknowledgements. We are grateful to Jennifer Balakrishnan, Peter Bruin, Aashraya Jha, Steffen Müller, Filip Najman and Alexander Smith for helpful comments and correspondence. We are grateful to Michael Stoll for answering queries about getting his Magma implementation of the Mordell-Weil sieve to work in our setting.

The first named author is supported by Simons Collaboration grant ID #550023 for the Collaboration on Arithmetic Geometry, Number Theory, and Computation. The second named author is supported by the Croatian Science Foundation under the project no. IP-2022-10-5008.

2. The five genus 1 cases

In this section we deal with the genus 1 cases of (1.1); that is, for every quadratic field $\mathbb{Q}(\sqrt{d})$ with $|d| < 10{,}000$, we determine if each of the five modular curves of genus one, viz. $X_1(11)$, $X_1(14)$, $X_1(15)$, $X_1(2,10)$ and $X_1(2,12)$, admits a noncuspidal $\mathbb{Q}(\sqrt{d})$-rational point. The following result of Kamienny and Najman shows that this essentially comes down to determining whether or not the rank of the elliptic modular curve over $\mathbb{Q}(\sqrt{d})$ is positive.

Theorem 2.1 (Kamienny-Najman, Theorems 15 and 16 in [KN12])**.**

(1) If $X_1(11)$, $X_1(2,10)$ or $X_1(2,12)$ possess a noncuspidal quadratic point, then that point has infinite order.

(2) $X_1(14)$ possesses a noncuspidal $\mathbb{Q}(\sqrt{d})$-torsion point of finite order if and only if $d = -7$.

(3) $X_1(15)$ possesses a noncuspidal $\mathbb{Q}(\sqrt{d})$-torsion point of finite order if and only if $d = -15$.

Since, for E an elliptic curve over $\mathbb{Q}$, one has

$$\operatorname{rk}(E(\mathbb{Q}(\sqrt{d})) = \operatorname{rk}(E(\mathbb{Q})) + \operatorname{rk}(E^d(\mathbb{Q})),$$

where E^d denotes the d^{th} quadratic twist of E, dealing with these five cases amounts to checking whether the $\mathbb{Q}$-rank of the corresponding quadratic twists of these elliptic modular curves is zero or not (noting that the $\mathbb{Q}$-rank of the five original curves is zero). Of course, for $d = -7$ and -15, one only has the three curves in (1) to deal with.

Hereafter, E will denote one of the above five elliptic modular curves. We first check via a modular symbols calculation in Sage involving the *twisted winding element* (see [Bos08, Section 2.2.2] or [ECdJ+11, Section 6.3.3] for more details) whether or not the *analytic rank* of E^d is zero. Here we observe that $X_1(2,10)$ is isogenous to $X_0(20)$, and $X_1(2,12)$ is isogenous to $X_0(24)$ (as may be verified in the LMFDB [LMF21]). The file `python_scripts/positive_rank_twists.py` produces a list of values of d for which the analytic rank is positive; these values are automatically output to the `positive_rank_lists` folder as JSON files.

If the analytic rank is zero, then by Kolyvagin [Kol89], we know that the rank is zero. If it is nonzero, we then verify in `magma_scripts/positive_rank_twists.m` that the algebraic rank is nonzero by the standard descent method implemented in Magma, which incorporates 2,4,8 and 3 descent.

3. $X_1(13)$ and $X_1(18)$

In this section we prove parts (2) and (3) of Theorem 1.3. We use the models for these two modular curves from [Kru13, Section 2.6]:

$$X_1(13) : y^2 = x^6 - 2x^5 + x^4 - 2x^3 + 6x^2 - 4x + 1;$$
$$X_1(18) : y^2 = x^6 + 2x^5 + 5x^4 + 10x^3 + 10x^2 + 4x + 1.$$

Our task is to decide, for every squarefree d with $|d| < 10{,}000$, whether each of these modular curves admits a noncuspidal $\mathbb{Q}(\sqrt{d})$-rational point. For this we start by employing the methods outlined by Krumm in Section 2 of his thesis [Kru13]. However we add two important improvements.

The first of these is Proposition 3.6, which implies for $N = 13$ or 18 that if $J_1^d(N)$ has rank zero, then there are no such $\mathbb{Q}(\sqrt{d})$-rational points. In particular, the use of the Magma function `Chabauty0` to compute all points on $X_1^d(N)(\mathbb{Q})$ as mentioned in [Kru13, Section 2.5.1] is no longer necessary since we prove that this set is always empty if $d \neq -3$ and $J_1^d(N)$ has rank zero. The elimination of this computational step, and using modular symbol computations to determine the analytic rank of $J_1^d(N)$ explains why we could extend our computation to a much large range of d.

The second improvement is that we apply the Mordell-Weil sieve to try and show $X_1^d(N)(\mathbb{Q}) = \emptyset$ in cases where the methods of Krumm fail. This extra step explains why we can show for example that 18-torsion does not occur over $\mathbb{Q}(\sqrt{681})$, while this is one of the cases that Krumm couldn't handle.

Throughout this section, we shall use N to denote either 13 or 18. We may also ignore the values $d = -1$ and -3 since, as mentioned in the introduction, Najman has already dealt with these.

Krumm shows that any noncuspidal $\mathbb{Q}(\sqrt{d})$-rational point on $X_1(N)$ must have $\mathbb{Q}$-rational x-coordinate, and therefore yields a $\mathbb{Q}$-rational point on the d-twisted modular curve $X_1^d(N)$. Conversely, if $X_1^d(N)$ admits a $\mathbb{Q}$-rational point, then this in turn would correspond to a noncuspidal $\mathbb{Q}(\sqrt{d})$-rational point on $X_1(N)$; these facts are proved in [Kru13, Lemma 2.7.3]. This reduces the task to checking whether any of these twists of these two modular curves possess a $\mathbb{Q}$-rational point.

If such a twist of $X_1(N)$ possesses a rational point, then several necessary conditions must be satisfied. We collect these into the following subsections.

3.1. Everywhere Local solubility.

If a curve X over a number field K admits a K-rational point, then it certainly admits a point rational over every completion of K; i.e., the curve must be everywhere locally soluble. This is a finite computation to check for any explicitly given curve, for which Magma has an implementation.

3.2. Congruence conditions on d.

Krumm provides a necessary condition on d for there to exist a $\mathbb{Q}$-point on $X_1^d(N)$.

Proposition 3.1 (Krumm, Theorems 2.6.5 and 2.6.9 in [Kru13])**.**

(1) If $X_1^d(13)(\mathbb{Q}) \neq \emptyset$, then:

(a) $d > 0$;
(b) $d \equiv 1 \pmod 8$.

(2) If $X_1^d(18)(\mathbb{Q}) \neq \emptyset$, *then:*
(a) $d > 0$;
(b) $d \equiv 1$ *or* $9 \pmod{24}$.

Remark 3.2. That d must be positive here was independently proved by Bosman, Bruin, Dujella, and Najman; see [BBDN14, Theorem 9].

3.3. **Two-cover descent.** This is a technique due to Bruin and Stoll [BS09b]. Briefly, they provide a refinement of a classical theorem of Chevalley and Weil [CW32] to say that, for any fixed $n \geq 2$, if a hyperelliptic curve C over a number field k admits a k-rational point, then this rational point must have a rational preimage on one of finitely many covering curves of a particular form depending on n, called n-covers. By considering the set of (isomorphism classes of) everywhere locally soluble n-coverings, called the n-Selmer set of C, one has the result that if this Selmer set is empty, then C has no k-rational points. Bruin and Stoll make this explicit and algorithmic in the case $n = 2$, by working with a closely related Selmer object (the *fake* 2*-Selmer group*), and most importantly, provide a Magma implementation of this for genus 2 curves over $\mathbb{Q}$, accessible via the intrinsic `TwoCoverDescent`. The upshot is that another necessary condition for $X_1^d(N)(\mathbb{Q})$ to be nonempty is that its fake 2-Selmer set must be nonempty.

3.4. **Positive rank of $J_1^d(N)$.** One necessary condition that we introduce is Corollary 3.7 below, which is that the rank of $J_1^d(N)(\mathbb{Q})$ must be positive. We first establish the following preparatory lemmas concerning torsion growth in $J_1(N)$ over quadratic fields.

Lemma 3.3. *For every quadratic field K, we have*

$$J_1(13)(K)_{tors} = J_1(13)(\mathbb{Q})_{tors} \cong \mathbb{Z}/19\mathbb{Z}.$$

Proof. For $p \geq 5$, $p \neq 13$, the torsion subgroup $J_1(13)(K)_{tors}$ injects into the reduction $\widetilde{J_1(13)}(\mathbb{F}_{p^2})$ (see [Kat80, Appendix]). By computing this latter group for $p = 5$ and 17, one sees that it must be a subgroup of $\mathbb{Z}/19\mathbb{Z}$. On the other hand, the torsion over $\mathbb{Q}$ is $\mathbb{Z}/19\mathbb{Z}$, as may be directly verified in Magma. These computations may be found in `magma_scripts/torsionVerifications.m` (this also includes the verifications for Lemmas 3.5 and 4.1 below). □

Remark 3.4. That $J_1(13)(\mathbb{Q})_{tors} \cong \mathbb{Z}/19\mathbb{Z}$ was first proved by Ogg in [Ogg72], and this discovery is of great historical importance in the arithmetic of elliptic curves. Shortly after finding a point of order 19 on $J_1(13)$, Ogg passed through Cambridge, MA, and communicated this discovery to Mazur and Tate; this inspired them to prove that in fact $J_1(13)(\mathbb{Q})$ consists only of the 19 torsion points; i.e., that it has zero rank over $\mathbb{Q}$; this has the corollary that no elliptic curve over $\mathbb{Q}$ possesses a rational point of order 13 [MT73]. This argument was shortly thereafter generalised by Mazur to deal with all primes $p \geq 13$; combined with existing work of Kubert [Kub76], this provided the classification of torsion subgroups of rational elliptic curves (Theorem 1.1) mentioned at the beginning of this paper.

Lemma 3.5. *For K any quadratic field that is not $\mathbb{Q}(\sqrt{-3})$, we have*

$$J_1(18)(K)_{tors} = J_1(18)(\mathbb{Q})_{tors} \cong \mathbb{Z}/21\mathbb{Z}.$$

Furthermore,

$$J_1(18)(\mathbb{Q}(\sqrt{-3}))_{tors} \cong \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/21\mathbb{Z}.$$

Proof. The last part was already proved by Najman [Naj10, Lemma 7]. For the first part, by computing the group structure of $J_1(18)(\mathbb{F}_{p^2})$ for prime p in the range $5 \leq p \leq 30$, we obtain that, for all quadratic fields K, we have $J_1(18)(K(\zeta_3))_{tors} = J_1(18)(\mathbb{Q}(\zeta_3))_{tors}$ (noting that the residue fields of $K(\zeta_3)$ are always contained in $\mathbb{F}_{p^2}$ for p as above), and that $J_1(18)(K)_{tors}$ is at most $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/21\mathbb{Z}$. That the torsion over $\mathbb{Q}$ is isomorphic to $\mathbb{Z}/21\mathbb{Z}$ is a straightforward Magma computation. That the 3-torsion rank of $J_1(18)$ is the same over $K(\zeta_3)$ as over $\mathbb{Q}(\zeta_3)$ implies that there can be no extra torsion attained over K. □

Proposition 3.6. *Let $d \neq -3$ be a squarefree integer, $N \in \{13, 18\}$, and $K = \mathbb{Q}(\sqrt{d})$. If $X_1(N)(K) \neq X_1(N)(\mathbb{Q})$, then $J_1(N)(K)$ and hence $J_1^d(N)(\mathbb{Q})$ has positive rank.*

Proof. If P is a K-point of $X_1(N)$ that is not a $\mathbb{Q}$-point, then it embeds under the Abel-Jacobi map to a K-point of $J_1(N)$ that is not a $\mathbb{Q}$-point. Therefore by Lemmas 3.3 and 3.5 it must be of infinite order. The final assertion comes from the equality $\mathrm{rk}(J_1(N)(K)) = \mathrm{rk}(J_1(N)(\mathbb{Q})) + \mathrm{rk}(J_1^d(N)(\mathbb{Q}))$. □

Corollary 3.7. *For $N \in \{13, 18\}$ and $d \neq -3$, if $X_1^d(N)(\mathbb{Q}) \neq \emptyset$, then $J_1^d(N)(\mathbb{Q})$ has positive rank.*

Proof. As explained at the beginning of this section (and shown by Krumm), rational points on $X_1^d(N)(\mathbb{Q})$ correspond to noncuspidal $\mathbb{Q}(\sqrt{d})$-points on $X_1(N)$ that are not $\mathbb{Q}$-points; the result then follows from the previous proposition. □

As in Section 2, we use the twisted winding element method to check whether or not the analytic rank of $J_1^d(N)(\mathbb{Q})$ is positive; if it is zero, then by Kato's generalisation of the work of Kolyvagin-Logachëv [Kat04], we know that the Mordell-Weil rank is zero.

Putting these four necessary conditions together - which is done in `magma_scripts/x1_13.m` and `magma_scripts/x1_18.m` (see the corresponding log files in the `logs` folder for the output) - we obtain

$$\begin{aligned} T_{10,000}(13) \subseteq \{&17, 113, 193, 313, 481, 673, 1153, 1417, 1609, 1921, 2089, 2161, \\ &2257, 3769, 3961, 5449, 6217, 6641, 8473, 8641, 9689, 9881\}; \\ T_{10,000}(18) \subseteq \{&33, 337, 457, 681, 1009, 1329, 1761, 1993, 2833, 2841, 2913, 3769, \\ &4729, 5281, 6217, 7057, 7321, 7369, 8241, 9049, 9969\}. \end{aligned}$$

Out of these possible values of d, we run a search for rational points on $X_1^d(N)$; the values for which this search yields no rational points (and hence we expect that there are none) are as follows:

$$\mathbb{Z}/13\mathbb{Z} : 673, 1609, 1921, 2089, 2161, 8473, 8641, 9689 \tag{3.1}$$

$$\mathbb{Z}/18\mathbb{Z} : 681, 1329, 1761, 2841, 2913, 3769, 4729, 5281, 6217, 7057, 7321, 9969. \tag{3.2}$$

To prove that these twists of $X_1(N)$ have no rational points, we employ the Mordell-Weil sieve, a technique also due to Bruin and Stoll [BS10] who have also provided a Magma implementation [BS09a] for genus 2 curves over $\mathbb{Q}$.

One input that this Magma implementation needs in order to use the Mordell-Weil sieve on a curve C of genus 2 is a divisor D of degree 3 on C, see [BS10][Section 7]. This divisor is used by them to provide a map $C \to J(C)$ given by $P \mapsto P + W - D$, where W is a canonical divisor. Such a degree 3 divisor is not always guaranteed to exist. However in the cases where we will apply it, we know *a priori* that it has to exist by the following lemma.

Lemma 3.8. *Let C be hyperelliptic curve over a number field K with an automorphism γ of order* 3 *such that $C/\langle\gamma\rangle$ has genus 0. Then every hyperelliptic quadratic twist C' of C that is everywhere locally solvable has a divisor of degree 3.*

Proof. Since the hyperelliptic involution is unique, the automorphism of order 3 commutes with it. In particular γ is also a K-rational isomorphism on every hyperelliptic quadratic twist. Now $C'/\langle\gamma\rangle$ is of genus 0 since over $\overline{K}$ it is isomorphic to $C/\langle\gamma\rangle$. The curve C' is everywhere locally solvable, so $C'/\langle\gamma\rangle$ is everywhere locally solvable as well. By the Hasse principle for genus 0 curves there is a K-rational point P on $C'/\langle\gamma\rangle$. The pullback of P along the quotient map $C' \to C'/\langle\gamma\rangle$ will then be a divisor of degree 3 on C'. □

The above proof also gives a practical algorithm to find this degree 3 point. Namely just search for rational points on the genus 0 curve $C'/\langle\gamma\rangle$ and pull them back to C'. Under the hypothesis of the lemma this curve is isomorphic to $\mathbb{P}^1_K$ so rational points will be easy to find.

Remark 3.9. We found that Mordell-Weil sieving in order to show that $X_1^d(N)$ is empty was much faster then we initially expected. The Mordell-Weil sieve works by choosing a suitable set S of primes and an auxilary integer N'. The integer N' here is actually called N in [BS10]. The Mordell-Weil sieve applied to $X_1^d(N)$ works by trying to prove $X_1^d(N) = \emptyset$ using the commutativity of the the diagram

$$\begin{tikzcd}
X_1^d(N)(\mathbb{Q}) \arrow[r] \arrow[d] & J_1^d(N)(\mathbb{Q})/N'J_1^d(N)(\mathbb{Q}) \arrow[d] \\
\prod_{p\in S} X_1^d(N)(\mathbb{F}_p) \arrow[r] & \prod_{p\in S} J_1^d(N)(\mathbb{F}_p)/N'J_1^d(N)(\mathbb{F}_p)
\end{tikzcd}$$

and trying to show that $J_1^d(N)(\mathbb{Q})/N'J_1^d(N)(\mathbb{Q})$ and $\prod_{p\in S} X_1^d(N)(\mathbb{F}_p)$ have empty intersection in $\prod_{p\in S} J_1^d(N)(\mathbb{F}_p)/N'J_1^d(N)(\mathbb{F}_p)$. In order for this strategy to be successful we need the different $|J_1^d(N)(\mathbb{F}_p)|$ to share many common factors [BS10, §3.1] for the primes $p \in S$. It turns out that many of these common factors will also be factors of N'; the reason for this is that there is no new information learned from reducing mod p if $J_1^d(N)(\mathbb{F}_p)/N'J_1^d(N)(\mathbb{F}_p) = \{0\}$. In running the Mordell-Weil sieve for $N = 13$ we found that the value of N' chosen by the Mordell-Weil sieve implementation of Bruin and Stoll [BS09a] was often either 19 or divisible by 19. Here we give a heuristic explanation of why this is to be expected.

Let N' be some fixed integer. If the integers $|J_1^d(N)(F_p)|$ are roughly uniformly distributed modulo N', then the chance of $|J_1^d(N)(F_p)|$ being divisible by N' is roughly $1/N'$, which seems a reasonable assumption at first. However for $N = 13$ and a fixed d we have that $|J_1^d(13)(\mathbb{F}_p)|$ is far from randomly distributed modulo 19. Indeed let p be a prime that splits in $\mathbb{Q}(\sqrt{d})$; then $|J_1(13)(\mathbb{F}_p)| = |J_1^d(13)(\mathbb{F}_p)|$; however the left hand side is $0 \mod 19$ since $J_1(13)(\mathbb{Q})$ contains a point of order

19, meaning that $19 \mid |J_1^d(13)(\mathbb{F}_p)|$ for a density of at least 1/2 of the primes. So the fact that a multiple of 19 is often chosen in the Mordell-Weil sieve can be explained by this unusually high density of primes for which $19 \mid |J_1^d(13)(\mathbb{F}_p)|$. A similar story holds for $N = 18$ where N' was often divisible by 21.

Carrying out this strategy in `magma_scripts/MWSieve-x1_13.m` (and the analogous file for $X_1(18)$) dealt with all of the above values, *except* 9689 for 13-torsion, and the three values $2841, 4729, 9969$ for 18-torsion. In these cases, the reason for the failure was the call to `MordellWeilGroupGenus2`; this did not finish given the search bounds declared there, so we were unable to find explicit generators for the Mordell-Weil group of the Jacobian of the twist. It is possible that increasing these bounds and waiting longer might yield these generators in these cases. However, already for the value 8641, it took over two days of Magma computation to furnish the generators.

This concludes the proof of parts (2) and (3) of Theorem 1.3.

4. $X_1(16)$

In this section we prove part (4) of Theorem 1.3. We work with the following model, as before to be found in [Kru13, Section 2.6]:

$$X_1(16) : y^2 = x(x^2 + 1)(x^2 + 2x - 1).$$

The curve $X_1(16)$ has 14 cusps. On this model, the point at infinity and the 5 points with $y = 0$ are cusps. The other 8 cusps are the points whose x-coordinate satisfies the equation:

$$(x - 1)(x + 1)(x^2 - 2x - 1) = 0.$$

As for $X_1(13)$ and $X_1(18)$, Krumm showed that any noncuspidal quadratic point must have rational x-coordinate on this model, and so corresponds to a $\mathbb{Q}$-rational point on the d-twist $X_1^d(16)$. However, unlike before, it is not the case that every $\mathbb{Q}$-rational point on $X_1^d(16)$ corresponds to a noncuspidal quadratic point on $X_1(16)$, because the point $(0, 0)$ on $X_1(16)$ (which is a cusp) gives the rational point $(0, 0)$ on every twist $X_1^d(16)$. In this way we see that our problem reduces to determining the existence or otherwise of a rational point on $X_1^d(16)$ with nonzero y-coordinate.

In particular, since $X_1^d(16)$ admits a rational point for every d, this is a different problem than that of the previous section. Indeed the existence of a global rational point prevents all local techniques from yielding any results. And hence we are essentially forced to compute all $\mathbb{Q}$-rational points on $X_1^d(16)$, rather than merely determining the existence of them, and it is this that makes this case the most difficult. Many of the necessary conditions in the previous section no longer apply. One that does survive, however, is the condition of positive rank of the Jacobian $J_1^d(16)$ of $X_1^d(16)$.

4.1. Positive rank of $J_1^d(16)$.

We again start with a preparatory lemma concerning torsion growth of $J_1(16)$ in quadratic fields.

Lemma 4.1.

(1) $J_1(16)(\mathbb{Q})_{tors} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$.
(2) $J_1(16)(\mathbb{Q}(i))_{tors} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$.
(3) $J_1(16)(\mathbb{Q}(\sqrt{2}))_{tors} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$.

(4) $J_1(16)(K)_{tors} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$ *for* $K \neq \mathbb{Q}(i), \mathbb{Q}(\sqrt{2})$ *any quadratic field.*

Proof. Part (1) may be directly verified in Magma. Parts (2) and (3) follow from a Magma computation that shows that the torsion subgroup is at most $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/10\mathbb{Z}$ (`TorsionBound`), together with finding the points $(\sqrt{-1}, 0)$, $(-\sqrt{-1}, 0)$, $(-1+\sqrt{2}, 0)$ and $(-1-\sqrt{2}, 0)$ that are 2-torsion (since they are Weierstrass points; note that these correspond to cusps on $X_1(16)$). Part (4) follows in a similar way to the proof of Lemma 3.5, by computing the abelian group structure of $\widetilde{J_1(16)}(\mathbb{F}_{p^2})$ for several small p to show that over any quadratic field K, one has

- $J_1(16)(K)_{tors}$ is at most $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$;

one then concludes by considering 2-torsion rank which can easily be read off from the factorisation of the hyperelliptic equation. □

Corollary 4.2. *For* $d \neq -1, 2$, *if* $X_1^d(16)(\mathbb{Q})$ *admits a point with nonzero* y*-coordinate, then* $J_1^d(16)(\mathbb{Q})$ *has positive rank.*

Proof. A point on $X_1^d(16)(\mathbb{Q})$ with nonzero y-coordinate corresponds to a K-point of $X_1(16)$ that is not a $\mathbb{Q}$-point, so the same proof as Proposition 3.6 applies. □

Using the twisted winding element computation from before, we compute the squarefree values of d with $|d| < 10{,}000$ for which the analytic rank of $J_1^d(16)$ is positive; this yields 674 values. We search for rational points with nonzero y-coordinate, and find such points on 55 of the twists, leaving 619 values to be dealt with. While we are not able to deal with all of these values, we can deal with the majority of them - 581 to be specific - via a method due to Bruin known as *elliptic curve Chabauty*, which we use in conjunction with a two-cover descent.

4.2. **Elliptic curve Chabauty.** The use of elliptic curve quotients in explicitly carrying out Chabauty's method for the computation of rational points goes back to Bruin's paper [Bru03]; the method we use is described in [BS09b, Section 8], which we now briefly summarise. For simplicity here C will denote a hyperelliptic curve of genus 2 over $\mathbb{Q}$, although the method works for higher genus hyperelliptic curves over arbitrary number fields. It is based on the idea that, even if $C(\mathbb{Q})$ is nonempty and so the fake 2-Selmer group $\mathrm{Sel}^{(2)}_{\mathrm{fake}}(C/\mathbb{Q})$ is nonempty, it still contains useful information that can be exploited to fully determine $C(\mathbb{Q})$.

The main theoretical result of [BS09b] is a refined version of the Chevalley-Weil theorem, that every rational point on C lifts to a rational point on one of finitely many 2-covers $D \xrightarrow{\pi} C$; the algorithmic result is that one can explicitly construct these covers D. So if, for each D, we can determine $\pi(D(\mathbb{Q}))$, then we are done. The problem is that D has large genus, so computing $D(\mathbb{Q})$ is difficult. The idea is to work with other quotients of D besides C. Indeed, if C is given by a model $y^2 = f(x)$ with f of odd degree, then by taking a degree 3 factor of f over some number field L, and by taking an appropriate twist γ_D, one may construct the elliptic curve defined over L:

$$E_D : \gamma_D y^2 = g(x)$$

together with an L-rational map $D \to E_D$. The Chabauty condition is that, if $\mathrm{rk}(E_D(L)) < [L : \mathbb{Q}]$, then $x(E_D(L)) \cap \mathbb{P}^1(\mathbb{Q})$ is finite and explicitly computable by [Bru03]. And since $x(\pi(D(\mathbb{Q}))$ is contained in this finite set, then so is $D(\mathbb{Q})$. If this method successfully manages to compute $x(E_D(L)) \cap \mathbb{P}^1(\mathbb{Q})$ and prove that it is finite for every 2-covering D in the fake 2-Selmer set of C, then one can successfully determine $C(\mathbb{Q})$. The algorithm is implemented in Magma as the intrinsic `Chabauty` (note that this is overloaded: the same intrinsic works for the classical Chabauty-Coleman method; the type of the parameters passed to it determine which is used).

In our case, the polynomial $f(x)$ that determines the model of $X_1(16)$ we are working with is highly composite, meaning that the number fields L arising in the above construction will always be quite small (of degrees $1, 2$ or 4), which aids the computation. Our implementation, as well as the execution of it, may be found in `magma_scripts/x1_16_chabauty.m`. (The point search occurs in `magma_scripts/x1_16_point_search.m`; the output of the Magma sessions may be found in the `logs` folder.)

The values for which this method did not succeed are as follows:

$$\begin{gathered}-8259, -7973, -7615, -7161, -7006, -6711, -6503, -6095, -6031,\\ -6005, -4911, -4847, -4773, -4674, -4371, -4191, -4074, -3503,\\ -3199, -1810, -1749, -815, 969, 1186, 3215, 3374, 3946, 4633, 5257,\\ 5385, 7006, 7210, 7733, 8459, 8479, 8569, 9709, 9961.\end{gathered} \tag{4.1}$$

In particular, we see that we are able to deal with all values in the range $|d| < 800$, completing the proof of part (4) of Theorem 1.3.

Remark 4.3. It would be interesting to attempt to deal with the above values for which elliptic curve Chabauty failed using two-cover descent together with quadratic Chabauty on curves D' intermediate to D and C. We did attempt to run quadratic Chabauty directly on these twists of $X_1(16)$, but in each case the Picard rank was 1 (as may be verified with the code associated to [CMSV19]), which is a nonstarter for that method. However, a combination method may be successful, and would be of interest to consider further.

In particular, if one can use this to determine the rational points on the two twists $C = X_1^{-815}(16)$ and $C = X_1^{969}(16)$ of $X_1(16)$, one would have established explicit uniformity of torsion over quadratic fields $\mathbb{Q}(\sqrt{d})$ for all $|d| < 1000$.

5. Comparison of our results with a conjecture of Granville

In this section we report on the results of the computation for the genus 2 curves $X_1(13)$, $X_1(16)$, and $X_1(18)$. We focus only on the genus 2 cases because the question of when twists of elliptic curves have positive rank has already been well-studied in the literature; see for example [WDE$^+$14] for computational work in this direction, [LJC$^+$18] for an overview of what was known as of 2018, and Smith's recent work [Smi22] showing that Goldfeld's conjecture (that asymptotically 50% of twists in a quadratic twist family have rank 0 and 50% have rank 1) follows from BSD under some additional assumptions on the level-2 structure of the elliptic curve. (In forthcoming work of Smith [Smi] these additional assumptions have been removed.)

Our data can be compared to work of Granville [Gra07] that studies how many twists of a given hyperelliptic curve admit nontrivial rational points. By trivial, Granville means those with y-coordinate 0, as well as the points at ∞ when the defining polynomial of the curve has odd degree, so this is exactly the situation we have studied in Sections 3 and 4. In particular, Granville makes the following conjecture about the number of twists that admit such a nontrivial rational point.

Conjecture 5.1 (Granville, part of Conjecture 1.3 in [Gra07]). *Let C be a hyperelliptic curve over $\mathbb{Q}$ of genus $g \geq 2$, defined by a model $y^2 = f(x)$ for $f \in \mathbb{Z}[x]$ that does not have repeated roots. Then there exists a positive constant κ'_f such that there are $\sim \kappa'_f B^{1/(g+1)}$ squarefree integers d with $|d| < B$ for which the quadratic twist C_d has a nontrivial rational point.*

Remark 5.2. Granville makes a similar conjecture about integral points that also applies to elliptic curves; this part of the conjecture is not relevant for our purposes so we omit it here.

The basis upon which this may be elevated to the stature of a conjecture is one of the main theorems of that paper; namely that this conjecture follows from the *abc*-conjecture provided various assumptions on f are satisfied (see Theorem 1.4 in *loc. cit.*). These conditions do not cover our case of $g = 2$, so in this case, the conjecture is still open even if one assumes the *abc*-conjecture. In this section, we wish to see if our computations agree with the above conjecture of Granville; that is, we will study the growth of $|T_B(N)|$ as B grows, for $N = 13$, 16 and 18, and compare it to $\kappa'_f B^{1/3}$.

In Section 1.1 of his paper, Granville gives a formula for the κ'_f constant, which we now briefly review in our case of $g = 2$ and with various simplifications; we refer the interested reader to *loc. cit.* for the more general case. To this end, we let f be a monic polynomial of degree 5 or 6 with integer coefficients and no repeated roots. We define $F(x,z) := z^6 f(x/z)$. For each integer r let $\omega(r)$ be the number of residue classes $t \pmod r$ for which r divides $f(t)$, and for k a positive integer write $\omega'(p^k) := p^{k-1}(p-1)\omega(p^k)$. We define V'_f to be the area of $\{(x,y) \in \mathbb{R}^2 : |F(x,y) \leq 1\}$ and $A_f(\mathbb{Q})$ to be $|\operatorname{Aut}_{\mathbb{Q}}(C)|/2$, which must equal 1, 2, 3, 4, 6, 8 or 12. We then have

$$\kappa'_f := \frac{V'_f}{A_f(\mathbb{Q})} \prod_p \left\{ 1 + \left(1 - \frac{1}{p^{2/3}}\right) \left(\frac{\omega'(p^2)}{p^{10/3}} + \frac{\omega'(p^4)}{p^{20/3}} + \cdots \right) \right\}$$

which converges to a well-defined real number. For $p \nmid \Delta(f)$, the pth term of the Euler product is more simply $1 + \omega(p)(p-1)(p^{2/3}-1)/(p^3 - p^{5/3})$.

Remark 5.3. Granville defines $A_f(\mathbb{Q})$ as the number of distinct $\mathbb{Q}$-linear transformations $(x,z) \mapsto (\alpha x + \beta z, \gamma x + \delta z)$ of F for which $F(\alpha x + \beta z, \gamma x + \delta z) \equiv F(x,z) \pmod{(\mathbb{Q}^*)^2}$, and $\alpha\delta - \beta\gamma \neq 0$; this is equal to $|\operatorname{Aut}_{\mathbb{Q}}(C)|/2$. Indeed if $F(\alpha x + \beta z, \gamma x + \delta z) = k^2 F(x,y)$ for some rational number k then $y^2 - F(x,z) = 0 \Leftrightarrow (ky)^2 - F(ax + bz, cx + dz)$. So both $(x,y,z) \mapsto (\alpha x + \beta z, ky, \gamma x + \delta z)$ and $(x,y,z) \mapsto (\alpha x + \beta z, -ky, \gamma x + \delta z)$ are automorphisms of C seen as a curve in weighted projective space. Since every automorphism of C commutes with the hyperelliptic involution one also gets $(x,z) \mapsto (\alpha x + \beta z, \gamma x + \delta z)$ back since every automorphism of C induces an automorphism of $\mathbb{P}^1 = C/h$ where h is the hyperelliptic involution.

See `granville/kappa_consts.py` for the implementation of these constants for the three defining polynomials of interest for us (written explicitly at the beginning of Sections 3 and 4). The most challenging aspect of this was the computation of V'_f for $X_1(16)$, which is an unbounded region with 8 cuspidal spikes; see `granville/euclidean_contribution.ipynb` to see this and the other such regions. Note that this implementation does not use interval arithmetic, or yield rigorously proven

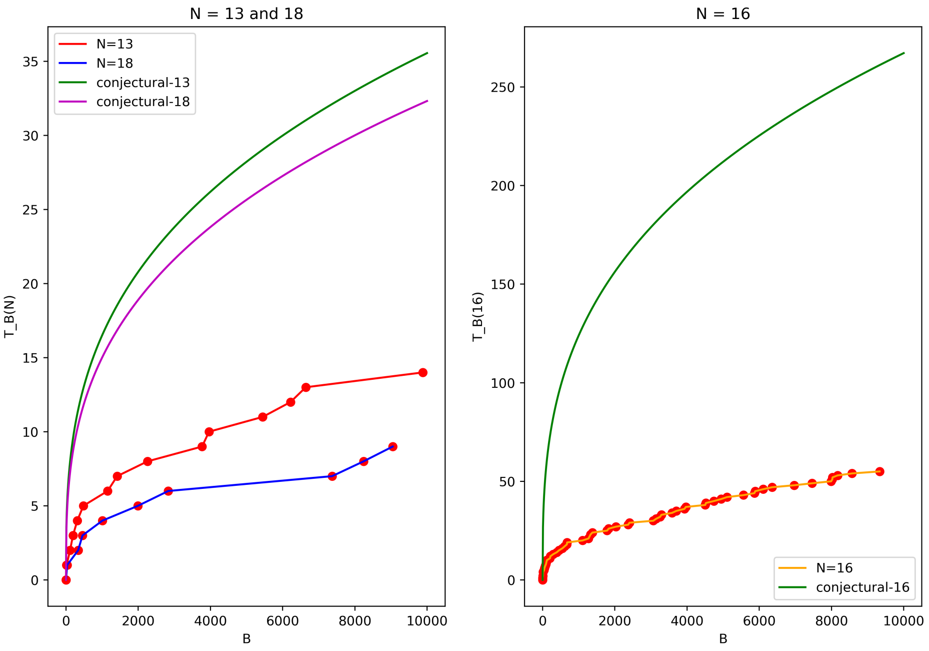

FIGURE 5.1. Graphs showing how $|T_B(N)|$ grows with B for $N = 13$, 16 and 18, together with the conjectural growth of $\kappa'_f B^{1/3}$; the values of κ'_f here are, respectively, 1.65, 12.4 and 1.5.

upper or lower bounds of V'_f; this is sufficient for our purpose of getting a sense of the larger picture.

Plotting $|T_B(N)|$ against B, and comparing it to $\kappa'_f B^{1/3}$ yields Figure 5.1. Here we have assumed that the values we have not been able to decide upon (specifically, 9689 for $X_1(13)$; 2841, 4729 and 9969 for $X_1(18)$; and the 38 values in (4.1) for $X_1(16)$) are not in $T_B(N)$; this seems the most likely outcome for the vast majority of the unhandled cases given that we have searched for points whose x-coordinate has naïve height at most $10,000$ on each of the relevant twists. Indeed, as can be seen in `logs/x1_16_point_search_log.txt`, the vast majority of the rational points found on $X_1^d(16)$ have x-coordinate whose naïve height is < 100. Furthermore, the point

$$\left(\frac{1681}{882}, \frac{479110914870}{882^3}\right)$$

on $X_1^{8570}(16)$ was the only point we found where the height of its x coordinate exceeded 1000. This is also what is expected according to [Gra07, Thm. 1.1], which states that under the *abc*-conjecture rational points on twists should have a small x-coordinate. In any case, these exceptions make up less than 1% of the total number of squarefree integers d with $|d| <$ 10,000 that we can deal with for each of our three curves, so this also does not affect the larger picture.

One clearly sees that the conjectural distribution of $\kappa'_f B^{1/3}$ is significantly larger than what the data is suggesting. From Figure 5.1 even the shape of the asymptotic behaviour is not apparent; so in Figure 5.2 we have artifically reduced the κ'_f

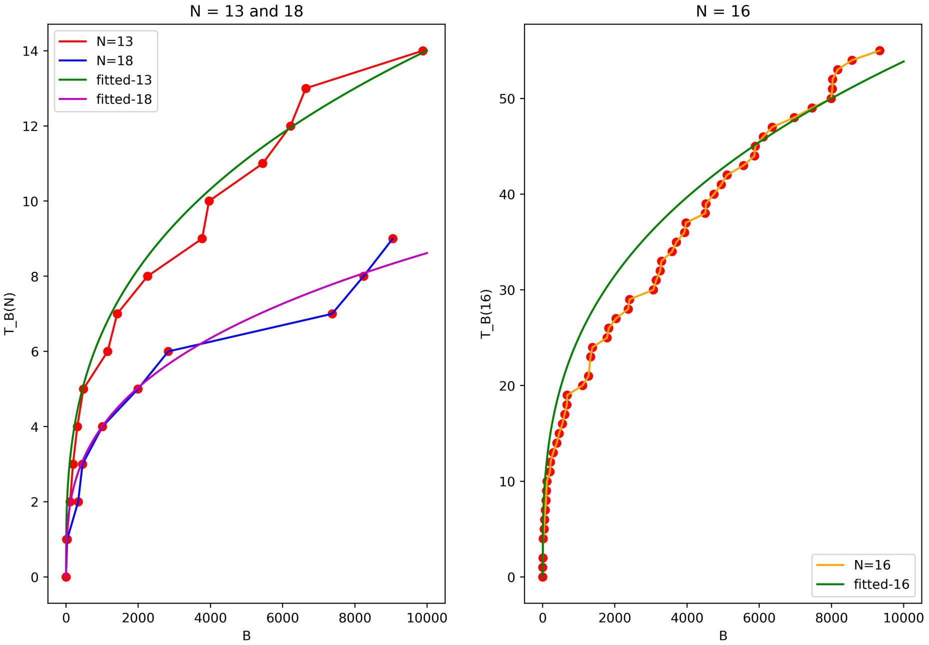

FIGURE 5.2. The same graph as Figure 5.1 but with smaller values of κ'_f, viz. respectively, 0.65, 2.5, 0.4.

constant to show more clearly that the growth of the data is indeed asymptotically proportional to $B^{1/3}$.

Therefore, for $X_1(16)$ (respectively, $X_1(13)$, $X_1(18)$), it seems that the constant κ'_f is about 5 (respectively, 2.5, 3.75) times too big. To investivate this discrepancy, we plot in Figure 5.3 B against $|T_B(N)|/B^{1/3}$, which conjecturally should converge to κ'_f.

On the graph for $X_1(16)$, there is a clear upward trend, so while it seems to hover at about 2.5 (the value of the fitted graph), it is not inconceivable that it will continue to drift upwards and reach Granville's value of 12.5. Put in other words, Figure 5.3 suggests that our results are not necessarily incompatible with Granville's κ'_f constant; more data is needed to determine this.

Other potential reasons for this discrepancy are as follows:

(1) When computing κ'_f we clearly had to take only finitely many summands in the sum for bad primes, and only finitely many primes in the Euler product. However, taking more would only *increase* κ'_f, making the discrepancy larger.
(2) The value of V'_f was approximate, and involved numerical integration in the real plane. However, it seems unlikely that this would be off by an order of magnitude.
(3) Our assumption that the values we were not able to determine are not actually in $T_B(N)$. However, as explained above, these account for a tiny percentage of the total values (especially so in the case of $X_1(13)$ and $X_1(18)$), and so also would not explain this larger observed discrepancy. Taking the

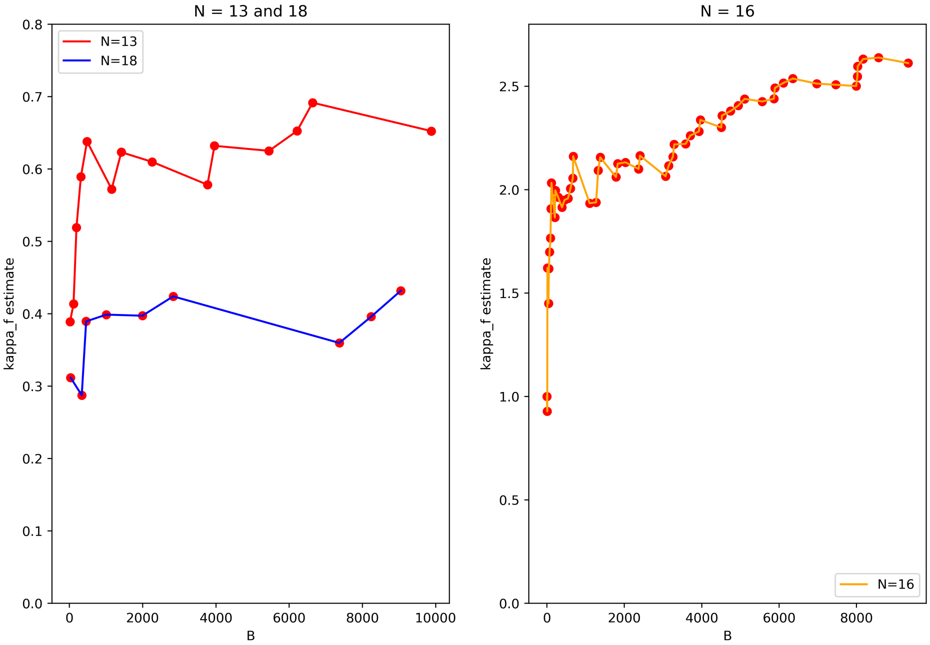

FIGURE 5.3. Plot of B against $|T_B(N)|/B^{1/3}$; this should conjecturally converge to κ'_f.

other extreme - that all of these unknown values actually are in $T_B(N)$ - would increase $|T_{10{,}000}(16)|$ (respectively, $|T_{10{,}000}(13)|$, $|T_{10{,}000}(18)|$) by 69% (respectively, 7%, 33%). This does seem more significant (even if extremely unlikely), but still is not enough to explain the e.g. factor of 5 discrepancy in the $X_1(16)$ case (much less for the other two curves).

The graphs in this section may be generated with the script `granville/results.py` in the top level.

5.1. ***abc* triples from quadratic twists.** Recall that an *abc* **triple** is a triple of positive coprime integers a, b and c such that $a + b = c$ and $c > \mathrm{rad}(abc)$, where $\mathrm{rad}(abc)$ denotes the product of all distinct prime divisors of abc. The **quality** of such a triple is $\log(c)/\log(\mathrm{rad}(abc))$. The *abc* conjecture states that for any $q > 1$ there are only finitely many *abc* triples whose quality is larger than q.

One of Granville's main theorems in *loc. cit.* is as follows.

Theorem 5.4 (Granville, Theorem 1.1(ii) in [Gra07])**.** *Assume that the abc conjecture is true. Suppose that $f(x) \in \mathbb{Z}[x]$ does not have repeated roots, and let $d \in \mathbb{Z}$. Consider the curve $C_d : dy^2 = f(x)$, and assume that its genus g is at least 2. Given any rational point on C_d, write its x-coordinate as r/s with $\gcd(r, s) = 1$. Then r and s satisfy*

$$|r|, |s| \ll |d|^{1/(2g-2)+o(1)}.$$

The proof of this theorem contains a method of constructing *abc* triples from points on C_d. However, this construction relies on a Belyi map on C_d (i.e. a map to $\mathbb{P}^1$ ramified only at 0, 1 and ∞) that factors via the hyperelliptic involution.

Now for the modular curves $X_1(N)$ one has that the j-invariant $j : X_1(N) \to X(1) \cong \mathbb{P}^1$ only ramifies at $0, 1728, \infty$, so in particular $j/1728$ is a Belyi map. Furthermore the hyperelliptic involutions of $X_1(13)$ and $X_1(16)$ are the diamond operators $\langle 5\rangle$ and $\langle 7\rangle$ and hence the j-invariant factors via the hyperelliptic map. A consequence of this is that any point $P \in X_1^d(13)(\mathbb{Q})$ or $P \in X_1^d(16)(\mathbb{Q})$ whose x coordinate has large enough height with respect to d will give an abc triple that can easily be derived from the j-invariant, by setting $c = \text{Numerator}(j(P)/1728)$, $a = \text{Denominator}(j(P)/1728)$, and $b = c - a$; if any of these are negative, one takes absolute values and possibly reorders a, b and c to obtain an actual abc triple.

We computed the j-invariants of all noncuspidal points that we found on $X_1^d(16)$. This led to 57 distinct j-invariants. Of these j-invarants, 46 had an associated abc-triple of quality > 1. The abc-triple of highest quality we found is:

$$\begin{aligned} a &= 2^{18} \cdot 3^{51} \cdot 5^4 \cdot 7 \cdot 11^{16} \cdot 17^2 \cdot 19^4 \cdot 601 \\ b &= 191^4 \cdot 353^2 \cdot 4289^2 \cdot 4993^2 \cdot 6143^2 \cdot 204751^2 \cdot 3945233^2 \\ c &= 4801^3 \cdot 31153^3 \cdot 116833^3 \cdot 9407089^3. \end{aligned}$$

The quality of this triple is ≈ 1.06919289. This triple comes from the point with x-coordinate $\frac{8}{19}$ and j-invariant $1728c/a$ on $X_1^{4522}(16)(\mathbb{Q})$. The other abc-triples we computed via the method above can be found in `logs/x1_16_abc_triples_list.txt`, which was generated from `magma_scripts/x1_16_abc_triples.m`.

The **size** of an abc triple is the number of decimal digits of c (i.e. $\log(c)/\log(10)$), and we say that one abc triple **beats** another if it has both a larger size and a larger quality. Bart de Smit maintains a list [dS19] of record-breaking triples; there we find triples of comparable quality to the found exhibited above, but with a much larger size of roughly 300 digits.

For $X_1(18)$ the hyperelliptic involution is $w_2\langle 7\rangle$, meaning that the j-invariant does not factor via the hyperelliptic map and hence the idea sketched above will not work here. It would therefore be interesting to try and find a suitable Belyi map in this case.

6. Future research

In light of the results and discussion of Section 5 it would therefore be interesting to obtain more data to fully ascertain the situation regarding the growth of $|T_B(N)|$ as B increases, or for this to be investigated further. More rigorous computation of Granville's κ'_f constants would also be of value to undertake.

In a different direction, one could consider the uniformity of torsion question for cubic fields, given that we now have the list of groups in this case. Note that Bruin and Najman [BN16] have found all possible torsion subgroups over the cyclic cubic field $\mathbb{Q}(\zeta_{13} + \zeta_{13}^5 + \zeta_{13}^8 + \zeta_{13}^{12})$ as well as the quartic field $\mathbb{Q}(\zeta_5)$, so this would be a good place to start with this investigation.

References

[BBDN14] Johan Bosman, Peter Bruin, Andrej Dujella, and Filip Najman. Ranks of elliptic curves with prescribed torsion over number fields. *International mathematics research notices*, 2014(11):2885–2923, 2014.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[BN16] Peter Bruin and Filip Najman. A criterion to rule out torsion groups for elliptic curves over number fields. *Research in Number Theory*, 2:1–13, 2016.

[Bos08] Johan G. Bosman. *Explicit computations with modular Galois representations.* Thesis, Universiteit Leiden, December 2008.

[Bru03] Nils Bruin. Chabauty methods using elliptic curves. *Journal für die reine und angewandte Mathematik*, 2003(562):27–49, 2003.

[BS09a] Nils Bruin and Michael Stoll. The Mordell-Weil sieve; Magma implementation, 2009. `https://www.mathe2.uni-bayreuth.de/stoll/magma/MWSieve-new.m`.

[BS09b] Nils Bruin and Michael Stoll. Two-cover descent on hyperelliptic curves. *Mathematics of computation*, 78(268):2347–2370, 2009.

[BS10] Nils Bruin and Michael Stoll. The mordell–weil sieve: proving non-existence of rational points on curves. *LMS Journal of Computation and Mathematics*, 13:272–306, 2010.

[CMSV19] Edgar Costa, Nicolas Mascot, Jeroen Sijsling, and John Voight. Rigorous computation of the endomorphism ring of a jacobian. *Mathematics of Computation*, 88(317):1303–1339, 2019.

[CW32] Claude Chevalley and André Weil. Un théorème d'arithmétique sur les courbes algébriques. *C. R. Acad. Sci. Paris*, 195:570–572, 1932.

[DEvH$^+$21] Maarten Derickx, Anastassia Etropolski, Mark van Hoeij, Jackson S Morrow, and David Zureick-Brown. Sporadic cubic torsion. *Algebra & Number Theory*, 15(7):1837–1864, 2021.

[DS17] Maarten Derickx and Andrew V. Sutherland. Torsion subgroups of elliptic curves over quintic and sextic number fields. *Proceedings of the American Mathematical Society*, 145(10):4233–4245, 2017.

[dS19] Bart de Smit. ABC triples, 2019. `https://www.math.leidenuniv.nl/~desmit/abc/index.php?set=4`.

[ECdJ$^+$11] Bas Edixhoven, Jean-Marc Couveignes, Robin de Jong, Franz Merkl, and Johan Bosman. *Computational Aspects of Modular Forms and Galois Representations.* Annals of Mathematics Studies. Princeton University Press, Princeton, 2011.

[Gra07] Andrew Granville. Rational and integral points on quadratic twists of a given hyperelliptic curve. *International Mathematics Research Notices*, 2007(9):rnm027–rnm027, 2007.

[Kam82] Sheldon Kamienny. Points of order p on elliptic curves over $\mathbb{Q}(\sqrt{p})$. *Mathematische Annalen*, 261:414–424, 1982.

[Kam86a] Sheldon Kamienny. On the torsion subgroups of elliptic curves over totally real fields. *Inventiones Mathematicae*, 83:545–551, 1986.

[Kam86b] Sheldon Kamienny. Torsion points on elliptic curves over all quadratic fields. *Duke Mathematics Journal*, 53:157–162, 1986.

[Kam86c] Sheldon Kamienny. Torsion points on elliptic curves over all quadratic fields II. *Bulletin de la Société Mathématique de France*, 114:119–122, 1986.

[Kam90] Sheldon Kamienny. Torsion points on elliptic curves. *American Mathematical Society Bulletin. New Series*, 23:371–373, 1990.

[Kam92] Sheldon Kamienny. Torsion points on elliptic curves and q-coefficients of modular forms. *Inventiones Mathematicae*, 109:221–229, 1992.

[Kat80] Nicholas M Katz. Galois properties of torsion points on abelian varieties. *Inventiones mathematicae*, 62(3):481–502, 1980.

[Kat04] Kazuya Kato. p-adic Hodge theory and values of zeta functions of modular forms. *Astérisque*, 295:117–290, 2004.

[Ken75] M. A. Kenku. Rational 2^n-torsion points on elliptic curves defined over quadratic fields. *Journal of the London Mathematical Society (2)*, 11:93–98, 1975.

[Ken79] M. A. Kenku. Certain torsion points on elliptic curves defined over quadratic fields. *Journal of the London Mathematical Society (2)*, 19:232–240, 1979.

[Ken81] M. A. Kenku. On the modular curves $X_0(125), X_1(25)$, and $X_1(49)$. *Journal of the London Mathematical Society (2)*, 23:415–427, 1981.

[Ken83] M. A. Kenku. Rational torsion points on elliptic curves defined over quadratic fields. *Journal of the Nigerian Mathematical Society*, 2:1–16, 1983.

[KM88] M. A. Kenku and F. Momose. Torsion points on elliptic curves defined over quadratic fields. *Naguya Mathematical Journal*, 109:125–149, 1988.

[KM95] Sheldon Kamienny and Barry Mazur. Rational torsion of prime order in elliptic curves over number fields. *Astérisque*, 228:81–100, 1995. With an appendix by Andrew Granville.

[KN12] Sheldon Kamienny and Filip Najman. Torsion groups of elliptic curves over quadratic fields. *Acta Arithmetica*, 152:291–305, 2012.

[Kol89] Victor Kolyvagin. Finiteness of $E(\mathbb{Q})$ and $Ш(E, \mathbb{Q})$ for a subclass of Weil curves. *Mathematics of the USSR-Izvestiya*, 32(3):523, 1989.

[Kru13] David Krumm. *Quadratic points on modular curves.* Thesis, University of Georgia, 2013.

[Kub76] Daniel Sion Kubert. Universal bounds on the torsion of elliptic curves. *Proceedings of the London Mathematical Society*, 33:193–237, 1976.

[Lev09] Beppo Levi. Sull'equazione indeterminata del 3. ordine. In *Atti del IV Congresso Internatzionale dei matematici*, volume 2, pages 175–177. Accademia dei Lincei, 1909.

[LJC$^+$18] Chao Li, L Ji, SY Cheng, ST Yau, and XP Zhu. Recent developments on quadratic twists of elliptic curves. *Proceedings of the International Consortium of Chinese Mathematicians 2017*, pages 381–399, 2018.

[LMF21] The LMFDB Collaboration. The L-functions and modular forms database. `http://www.lmfdb.org`, 2021. [Online; accessed 5 February 2021].

[Maz77] Barry Mazur. Modular curves and the Eisenstein ideal. *Publications Mathématiques de l'Institut des Hautes Études Scientifiques*, 47(1):33–186, 1977. With an appendix by Barry Mazur and Michael Rapoport.

[Mer96] Loïc Merel. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Inventiones mathematicae*, 124(1-3):437–449, 1996.

[Mom84a] Fumiyuki Momose. p-torsion points on elliptic curves defined over quadratic fields. *Nagoya Mathematical Journal*, 96:139–165, 1984.

[Mom84b] Fumiyuki Momose. Rational points on the modular curves $X_{split}(p)$. *Compositio Mathematica*, 52(1):115–137, 1984.

[MT73] Barry Mazur and John Tate. Points of order 13 on elliptic curves. *Inventiones mathematicae*, 22:41–49, 1973.

[Naj10] Filip Najman. Complete classification of torsion of elliptic curves over quadratic cyclotomic fields. *Journal of number theory*, 130(9):1964–1968, 2010.

[Naj11] Filip Najman. Torsion of elliptic curves over quadratic cyclotomic fields. *Math J. Okayama Univ.*, 53:75–82, 2011.

[Ogg72] Andrew P. Ogg. Rational points on certain elliptic modular curves. Talk given at AMS Symposium on Analytic Number Theory and Related Parts of Analysis. St. Louis, 1972.

[S$^+$12] William A. Stein et al. *Sage Mathematics Software (Version 10.2)*. The Sage Development Team, 2012. `http://www.sagemath.org`.

[Smi] Alexander D. Smith. The Birch and Swinnerton-Dyer conjecture implies Goldfeld's conjecture. in preparation.

[Smi22] Alexander D. Smith. The distribution of ℓ^∞-Selmer groups in degree ℓ twist families I. Preprint available online at `https://arxiv.org/abs/2207.05674`, 2022.

[SS96] Norbert Schappacher and René Schoof. Beppo Levi and the Arithmetic of Elliptic Curves. *The Mathematical Intelligencer*, 18(1):57–69, 1996.

[Sut12] Andrew V Sutherland. Torsion subgroups of elliptic curves over number fields. *Avalaible at https://math.mit.edu/~drew/MazursTheoremSubsequentResults.pdf*, 1:14, 2012.

[Trb20] Antonela Trbović. Torsion groups of elliptic curves over quadratic fields $\mathbb{Q}(\sqrt{d})$, $0 < d < 100$. *Acta Arithmetica*, 192(1):141–153, 2020.

[WDE$^+$14] Mark Watkins, Stephen Donnelly, Noam D Elkies, Tom Fisher, Andrew Granville, and Nicholas F Rogers. Ranks of quadratic twists of elliptic curves. *Publications matheématiques de Besançon. Algeèbre et theéorie des nombres*, 2:63–98, 2014.

Barinder S. Banwait, Department of Mathematics & Statistics, Boston University, Boston, MA, USA
Email address: `barinder.s.banwait@gmail.com`

Maarten Derickx, University of Zagreb, Bijenička Cesta 30, 10000 Zagreb, Croatia
Email address: `maarten@mderickx.nl`