Experimental Mathematics 32.1 (2020): 70-81

DOI: https://doi.org/10.1080/10586458.2020.1771638

AN ALGORITHM FOR DETERMINING TORSION GROWTH OF ELLIPTIC CURVES

ENRIQUE GONZÁLEZ–JIMÉNEZ AND FILIP NAJMAN

Abstract. We present a fast algorithm that takes as input an elliptic curve defined over $\mathbb{Q}$ and an integer d and returns all the number fields K of degree d' dividing d such that $E(K)_{\text{tors}}$ contains $E(F)_{\text{tors}}$ as a proper subgroup, for all $F \quad K$. We ran this algorithm on all elliptic curves of conductor less than 400.000 (a total of 2.483.649 curves) and all $d \leq 23$ and collected various interesting data. In particular, we find a degree 6 sporadic point on $X_1(4,12)$, which is so far the lowest known degree a sporadic point on $X_1(m,n)$, for $m \geq 2$.

1. Introduction

Let E be an elliptic curve defined over $\mathbb{Q}$ and let K a number field. We say that there is *torsion growth over* K if $E(\mathbb{Q})_{\text{tors}} \subsetneq E(K)_{\text{tors}}$. One can easily work out that there is torsion growth (of the 2-primary torsion) in at least one number field of degree 2, 3, or 4. On the other hand, there is no torsion growth in number fields of degree only divisible by primes > 7 (cf. [12, Theorem 7.2(i)]).

The purpose of this paper is to develop a fast algorithm, usable in practice, which for a given elliptic curve E defined over $\mathbb{Q}$ and a positive integer d finds all the pairs (K, H) where K is a number field of degree dividing d and $E(K)_{\text{tors}} \simeq H \supsetneq E(\mathbb{Q})_{\text{tors}}$. Of course, the set of such number fields can be infinite if there exists a number field F of degree d', where d' divides d and $d' < d$ such that $E(F)_{\text{tors}} \supsetneq E(\mathbb{Q})_{\text{tors}}$; then every number field $K \supseteq F$ of degree d will have the desired property. To circumvent this problem, we will say that E has *primitive torsion growth* over a number field K if $E(F)_{\text{tors}} \subsetneq E(K)_{\text{tors}}$, for all subfields $F \subsetneq K$. For a prime ℓ we say that E has *primitive ℓ-power torsion growth* if $E(F)[\ell^\infty] \subsetneq E(K)[\ell^\infty]$, for all subfields $F \subsetneq K$.

It is an easy corollary of Merel's theorem on the boundedness of the torsion of elliptic curves that for a given integer d the list of number fields where the torsion growth will be finite.

The existence of such an algorithm is obvious: for every integer d, by Merel's theorem, there exists an effective bound B_d such that $\#E(K)_{\text{tors}} \leq B_d$. So to determine the number fields F where torsion growth occurs one does the following:

- For all prime powers $\ell^n \leq B_d$ do:
  - factor the ℓ^n-th division polynomial ψ_{ℓ^n} and check whether there are any irreducible factors of degree d' dividing d.
  - If no, move on to the next prime power. If yes, for all irreducible factors f of degree $d' \mid d$ do:
    - Construct the number field F whose minimal polynomial is f - this will be the field of definition of the x-coordinate of a ℓ^n-torsion point P of E.
    - Check whether P is defined over F, if yes add F to the set that will be the output. If P is not defined over F, then check whether $2d'$ divides d, if yes, then add $\mathbb{Q}(P)$ (which will be obtained from F by adjoining the y-coordinate of P to F) to the output set.

However, if implemented as stated above, this algorithm would not be very useful in practice. The main obstacle would be factoring division polynomials, as ψ_n is a polynomial of degree $\frac{n^2-1}{2}$ for n odd, and the values n that need to be checked will grow exponentially in d.

Our algorithm will use information that can be obtained from the images of mod n Galois representations attached to E to avoid factoring division polynomials wherever possible. To make the algorithm usable in practice we will add a number of if-then conditions that will rule out most of the integers n that need to be checked using results from [12] and results that we develop for this purpose in Section 2.2.

Date: May 3, 2019.

2010 *Mathematics Subject Classification.* 11G05.

Key words and phrases. Elliptic curves, torsion over number fields.

The first author was partially supported by the grant MTM2015–68524–P. The second author gratefully acknowledges support from the QuantiXLie Center of Excellence, a project co-financed by the Croatian Government and European Union through the European Regional Development Fund - the Competitiveness and Cohesion Operational Programme (Grant KK.01.1.1.01.0004) and by the Croatian Science Foundation under the project no. IP-2018-01-1313.

One of the main motivations of this paper is to run the algorithm on all elliptic curves of conductor less than 400.000 (see [4, 22]) and for each curve within determine all the number fields of degree ≤ 23 over which there is primitive torsion growth. In Section 4 we present the most interesting data coming out of these computations. In particular we find two elliptic curves defined over $\mathbb{Q}$ with torsion $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ over a degree 6 number field and prove that these are the only two such curves. By [5], there are only finitely many elliptic curves over sextic fields (without supposing that they are defined over $\mathbb{Q}$) with this torsion group, so these curves give us examples of sporadic points of degree 6 on $X_1(4, 12)$. This is the lowest known degree of a sporadic point on a modular curve $X_1(m, n)$, for $m|n$ and $m \geq 2$.

Notation. Specific elliptic curves mentioned in this paper will be referred to by their LMFDB label and a link to the corresponding LMFDB page [22] will be included for the ease of the reader. Conjugacy classes of subgroups of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ will be referred to by the labels introduced by Sutherland in [29, §6.4]. We write $G = H$ (or $G \leq H$) for the fact that G is isomorphic to H (or to a subgroup of H resp.) without further detail on the precise isomorphism.

2. Auxiliary results

In this section, we prove a series of results that will make it possible to replace costly factorizations of division polynomials by simple if-then checks. This will be useful in the computations described in Section 4.

Let E be an elliptic curve defined over a number field K, n a positive integer and $\overline{K}$ a fixed algebraic closure of K. The absolute Galois group $G_K := \mathrm{Gal}(\overline{K}/K)$ acts on $E[n]$, inducing a *mod n Galois representation attached to E*

$$\overline{\rho}_{E,n} : G_K \longrightarrow \mathrm{Aut}(E[n]).$$

Fixing a basis $\{P, Q\}$ of $E[n]$, we identify $\mathrm{Aut}(E[n])$ with $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$. Therefore we can view $\overline{\rho}_{E,n}(G_K)$ as a subgroup of $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, determined uniquely up to conjugacy in $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, and denoted by $G_E(n)$ from now on.

For elliptic curves over $\mathbb{Q}$, we conjecturally (see [29, Conjecture 1.1] and [32, Conjecture 1.12.]) know all the mod ℓ Galois representations attached to non-CM elliptic curves over $\mathbb{Q}$.

Conjecture 2.1. *Let $E/\mathbb{Q}$ be a non-CM elliptic curve, $\ell \geq 17$ a prime and (ℓ, j_E) not in the set*

$$\left\{(17, -17 \cdot 373^3/2^{17}), (17, -17^2 \cdot 101^3/2), (37, -7 \cdot 11^3), (37, -7 \cdot 137^3 \cdot 2083^3 \right. \quad ,$$

then $G_E(\ell) = \mathrm{GL}_2(\mathbb{F}_\ell)$.

For a prime ℓ, $\rho_{E,\ell} : G_K \to \mathrm{GL}_2(\mathbb{Z}_\ell)$ will denote the ℓ-adic representation attached to E (again we assume that we have fixed a basis for the Tate module $T_\ell(E)$). We say that the ℓ-adic representation of E is defined modulo ℓ^n if for all $m \geq n$ we have $G_E(\ell^{m+1}) \geq I + \ell^n M_2(\mathbb{Z}/\ell^{m+1}\mathbb{Z})$.

Proposition 2.2. *Let E be an elliptic curve defined over a number field K such that its ℓ-adic representation is defined modulo ℓ^n. Then for any point $P \in E(\overline{K})$ of order ℓ^{n+1}, we have $[K(P) : K(\ell P)] = \ell^2$.*

Proof. We need to prove that $I + \ell M_2(\mathbb{Z}/\ell^{n+1}\mathbb{Z})$ acts transitively on the solutions of $\ell X = P$ (where the action of $I + \ell^n M_2(\mathbb{Z}/\ell^{n+1}\mathbb{Z})$ on the $\mathbb{Z}/\ell^n\mathbb{Z}$-module of the solutions of $\ell X = P$ is defined in the obvious way). The G_K-module $E[\ell^{n+1}]$ is isomorphic to $(\mathbb{Z}/\ell^{n+1}\mathbb{Z})^2$, and we choose an isomorphism sending P to $(\ell, 0)$ and study the action of $I + \ell M_2(\mathbb{Z}/\ell^{n+1}\mathbb{Z})$ on the ℓ^2 solutions of the equation $\ell X = (\ell, 0)$. One easily sees that already the subgroup of $I + \ell^n M_2(\mathbb{Z}/\ell^{n+1}\mathbb{Z})$ generated by $\left(\begin{smallmatrix} 1 & \ell^n \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} \ell^{n+1} & 0 \\ 0 & 1 \end{smallmatrix}\right)$ acts transitively on the solutions of the equation $\ell X = (\ell, 0)$. □

For easier reference we state and prove the following obvious lemma.

Lemma 2.3. *Let E be an elliptic curve defined over a number field K and $\ell \geq 5$ a prime such that the index of its ℓ-Sylow subgroup of the image of its ℓ-adic Galois representation in the ℓ-Sylow subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ is equal to ℓ^n. Then the ℓ-adic Galois representation of E/K is defined modulo ℓ^m for some $m \leq n + 1$.*

Proof. The lemma follows from the fact [28, Lemma 3, IV-24] that for $\ell \geq 5$ if $G_E(\ell^{m+1}) \geq I + \ell M_2(\mathbb{Z}/\ell^{m+1}\mathbb{Z})$ for any $m \geq 1$, then it follows that $G_E(\ell^{k+1}) \geq I + \ell^k M_2(\mathbb{Z}/\ell^{k+1}\mathbb{Z})$ for *all* $k \geq m$. Hence if the ℓ-adic representation is not defined modulo ℓ^n, then $G_E(\ell^{k+1}) \cap (I + \ell^k M_2(\mathbb{Z}/\ell^{k+1}\mathbb{Z}))$ has index at least ℓ in $I + \ell^k M_2(\mathbb{Z}/\ell^{k+1}\mathbb{Z})$ for every $1 \leq k \leq m$ and so the index of the ℓ-Sylow subgroup of the image of the ℓ-adic Galois representaiton of E in the ℓ-Sylow subgroup of $\mathrm{GL}_2(\mathbb{Z}_\ell)$ would be at least equal to ℓ^n. □

Lemma 2.4. *Let $\ell \geq 3$ be a prime and $E/\mathbb{Q}$ an elliptic curve. Then if $G_E(\ell) = \mathrm{GL}_2(\mathbb{F}_\ell)$ and $P \in E(\overline{\mathbb{Q}})$ is a point of order ℓ^2, then $[\mathbb{Q}(P) : \mathbb{Q}] = \ell^2(\ell^2 - 1)$.*

Proof. If $\ell \geq 5$, then it follows from [28, Lemma 3, IV-24] that if $G_E(\ell) = \mathrm{GL}_2(\mathbb{F}_\ell)$, then $\rho_{E,\ell}$ is surjective. It follows that the ℓ-adic representation is defined modulo ℓ, so the lemma follows from Proposition 2.2. For $\ell = 3$, if $G_E(9) = \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$, then the conclusion is the same as before, while if $G_E(9) \neq \mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$ then it follows from [6] that $G_E(9) = G$, where G is a (unique up to conjugacy) subgroup G of $\mathrm{GL}_2(\mathbb{Z}/9\mathbb{Z})$ generated by $\left(\begin{smallmatrix} 4 & 5 \\ 4 & 4 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 4 & 5 \\ 8 & 6 \end{smallmatrix}\right)$. One easily checks that this group acts transitively on the 72 points of order 9 in $E(\overline{\mathbb{Q}})$, so the $[\mathbb{Q}(P) : \mathbb{Q}] = 72$ for all points of order 9 (using the same argumentation as in [12, Section 5]). □

Lemma 2.5. *Let E be an elliptic curve defined over a number field K such that $P \in E(\overline{K})$ of order ℓ^k, $k \geq 2$ and for some prime satisfying $\ell^{k-1} > 2$, $\ell^{k-1}P \in E(K)$. Then $K(x(P)) = K(P)$.*

Proof. Obviously $[K(P) : K(x(P))] = 1$ or 2. Suppose $[K(P) : K(x(P))] = 2$ and let $1 \neq \sigma \in \mathrm{Gal}(K(P)/K(x(P)))$. Then we have $\sigma(x(P)) = x(P)$, so $\sigma(y(P)) = y(-P)$ and hence $\sigma(P) = -P$, as $\sigma \neq 1$. But we have

$$-\ell^{k-1}P = \ell^{k-1}(\sigma(P)) = \sigma(\ell^{k-1}P) = \ell^{k-1}P,$$

where the last equation follows from the fact that $\ell^{k-1}P \in E(K)$. This is obviously a contradiction. □

The most time-consuming part of our algorithm is determining the existence of points of order ℓ^k for $k \geq 2$, and the fields over which such points live if they exist.

We now prove results that will prove the non-existence of points of certain orders ℓ^k over number fields of relatively small degree d.

2.1. Points of order 3^n.

Lemma 2.6. *There are no points of order 81 on an elliptic curve $E/\mathbb{Q}$ over any number field of degree ≤ 53.*

Proof. The result follows by the results of Rouse and Zureick-Brown (shared in personal communication) in which they classify the possible 3-adic images of non-CM elliptic curves. Their classification was not yet complete at the moment of writing of the paper, but from the results that they have it follows that the smallest degree of a number field over which a non-CM elliptic curve $E/\mathbb{Q}$ has a point of order 81 is 81.

For CM elliptic curves defined over $\mathbb{Q}$ an explicit calculation using division polynomials shows that there are no points of degree 81 over any number field of degree ≤ 53. □

2.2. Points of order 125.

Proposition 2.7. *Let $E/\mathbb{Q}$ be an elliptic curve and K a number field of degree < 50. Then $E(K)$ does not have a point of order 125.*

Proof. Let P be a point of order 125. First consider the case when E has a 5-isogeny over $\mathbb{Q}$. Let d be the power of 5 in $[\mathrm{Aut}_{\mathbb{Z}_5} T_5(E) : \mathrm{im}\, \rho_{E,5}]$ (note that this index is finite as elliptic curves with CM do not have 5-isogenies over $\mathbb{Q}$). By [16, Theorem 2], d is at most 5, and we conclude by Lemma 2.3 that the ℓ-adic representation of E is defined modulo 25. From here it follows by Proposition 2.2 that $[\mathbb{Q}(P) : \mathbb{Q}(5P)] = 25$. Since there exist no points of order 25 on elliptic curves over quadratic fields, we have $[\mathbb{Q}(P) : \mathbb{Q}] > 50$.

Suppose now that there is no isogeny of degree 5 over $\mathbb{Q}$. Applying [23, Theorem 2.1] (with $L = \mathbb{Q}$, $p = 5$, $a = 1$ and $n = 3$), we obtain that $[\mathbb{Q}(P) : \mathbb{Q}] \geq 50$. □

2.3. Points of order 49.

Lemma 2.8. *There are no points of order 49 on an elliptic curve $E/\mathbb{Q}$ over any number field of degree $d < 42$.*

Proof. Let us split the proof in two cases depending if E has a 7-isogeny or not. Suppose that E has a 7-isogeny, then by the results of [17] the 7-adic representation is either as large as possible or the curve has $j_E = -15^3$ or 255^3. If the representation is as large as possible, then by Proposition 2.2 we have $[\mathbb{Q}(P) : \mathbb{Q}(7P)] = 49$, eliminating this case. If $j_E = -15^3$ or 255^3, we explicitly check that $[\mathbb{Q}(P) : \mathbb{Q}] \geq 147$.

Finally, suppose that E does not have a 7-isogeny and let P be a point of order 49 of E. By [23, Theorem 2.1], we get that $[\mathbb{Q}(P) : \mathbb{Q}(7P)]$ is divisible by 7, so the only cases which we need to consider for which $[\mathbb{Q}(P) : \mathbb{Q}] = [\mathbb{Q}(P) : \mathbb{Q}(7P)][\mathbb{Q}(7P) : \mathbb{Q}] \leq 42$. This is only possible when $G_E(7)$ is a Borel subgroup, which is a contradiction, since then E would have a 7-isogeny over $\mathbb{Q}$. □

2.4. **Points of order ℓ^2 for $\ell > 7$.**

Lemma 2.9. *There are no points of order ℓ^2 for $\ell \geq 11$ on an elliptic curve $E/\mathbb{Q}$ over any number field of degree $d < 55$.*

Proof. Let P be a point of order ℓ^2. For $\ell = 11$, we note that it follows from [12, Table 1] that if E does not have CM and has no 11-isogenies over $\mathbb{Q}$, that $[\mathbb{Q}(11P) : \mathbb{Q}]$ is divisibly by 55.

On the other hand, if E has a 11-isogeny over $\mathbb{Q}$, and it does not have CM, it follows from the results of [16] and Lemma 2.3 that the 11-adic image is defined modulo 11, from which it follows by Proposition 2.2 that $[\mathbb{Q}(P) : \mathbb{Q}(11P)]$ is divisible by 121.

If $E/\mathbb{Q}$ has CM and an 11-isogeny or an 19-isogeny then $j(E) = -2^{15}$ or $j = -2^{15}3^3$, respectively. An explicit computation shows that such a curve does not have any points of order 121 over any number field of degree ≤ 55.

For $\ell \geq 13$, if E has a ℓ-isogeny over $\mathbb{Q}$ and does not have CM, by the results of [16], it follows that the ℓ-adic image is defined mod ℓ, from which it follows that, that $[\mathbb{Q}(P) : \mathbb{Q}(\ell P)]$ is divisible by ℓ^2.

If E has an ℓ-isogeny over $\mathbb{Q}$ for $\ell > 19$, then the result follows directly from [23, Theorem 1.8.].

On the other hand, if there are no ℓ-isogenies over $\mathbb{Q}$, then $[\mathbb{Q}(\ell P) : \mathbb{Q}] \geq 72$ for $\ell = 13$ and $\geq (\ell^2 - 1)/3$ for $\ell > 13$. □

2.5. **Points of order 37.** The following lemma allows us to deal with points of order 37 over number fields of degree 12, which is the smallest degree over which an elliptic curve defined over $\mathbb{Q}$ can have a point of order 37.

Lemma 2.10. *Let $E/\mathbb{Q}$ be an elliptic curve. Then E has a point of order 37 over a degree 12 number field K if and only if $j_E = -7 \cdot 11^3$. Moreover, K has to be $K = \mathbb{Q}(\alpha, \sqrt{d \cdot f(\alpha)})$ where $f(x) = x^3 - 1155x + 16450$, $d \in \mathbb{Q}^{\square}$ is such that E is $\mathbb{Q}$-isomorphic to the elliptic curve $dy^2 = f(x)$ and α is a root of the irreducible polynomial*

$$g(x) = x^6 - 210x^5 - 8085x^4 + 125300x^3 + 4251975x^2 - 16133250x - 408849875.$$

In particular, $E(K)_{\text{tors}} = \mathbb{Z}/37\mathbb{Z}$.

Proof. From [12] it follows that E has a point of order 37 over a degree 12 field if and only if $G_E(37) = \texttt{37.B.8.1}$, which happens if and only if $j_E = -7 \cdot 11^3$. We note that the elliptic curve $E' : y^2 = f(x)$ has $j_{E'} = -7 \cdot 11^3$ and therefore there exists a number field L of degree 12 such that E' has a point of order 37 over L (see [25, Section 6]). We have that $g(x)$ is an irreducible factor of the 37-division polynomial of E'. In particular $\alpha = x(P)$ where P is a point of order 37 in E' and $L = \mathbb{Q}(P) = \mathbb{Q}(\alpha, \sqrt{f(\alpha)})$. Now if $E/\mathbb{Q}$ is an elliptic curve with $j_E = -7 \cdot 11^3$, it will be a quadratic twist of E'; thus E will have a model $E : dy^2 = f(x)$ for some $d \in \mathbb{Q}$. In particular, $R = (\alpha, \sqrt{d \cdot f(\alpha)})$ is a point of order 37 on E. Then we obtain $K = \mathbb{Q}(R)$ and get the desired result.

Let us prove $E(K)_{\text{tors}} = \mathbb{Z}/37\mathbb{Z}$. The set of non-surjective primes only depends on the j-invariant of E. Therefore it is enough to compute this set for a single elliptic curve with that $j_E = -7 \cdot 11^3$. We have that the elliptic curve E' of minimal conductor with $j_{E'} = -7 \cdot 11^3$ has LMFDB label `1225.b2`; we see in the LMFDB (or alternatively explicitly compute) that 37 is the only non-surjective prime for this elliptic curve. So if $E(K)$ had a point P of order $\ell \neq 37$, $\mathbb{Q}(P)$ would have to be a subfield of K and $\ell^2 - 1$ would have to divide 12. We see that the only possibility is that $\ell = 2$. But the field $\mathbb{Q}(P)$ generated by a point of order 2 will not be Galois over $\mathbb{Q}$ (since the mod 2 representation is surjective) and hence cannot be a subfield of the cyclic field K. □

2.6. **Points of order 17.** We obtain similar results as in Lemma 2.10, but for order 17 and for number fields of degree 8, which is the smallest degree over which an elliptic curve defined over $\mathbb{Q}$ can have a point of order 17.

Lemma 2.11. *Let $E/\mathbb{Q}$ be an elliptic curve. Then E has a point of order 17 over a degree 8 number field K if and only if $j_E = -17 \cdot 373^3/2^{17}$. Moreover, K has to be $K = \mathbb{Q}(\alpha, \sqrt{d \cdot f(\alpha)})$ where $f(x) = x^3 - 95115x - 12657350$, $d \in \mathbb{Q}^{\square}$ is such that E is $\mathbb{Q}$-isomorphic to the elliptic curve $dy^2 = f(x)$ and α is a root the irreducible polynomial*

$$g(x) = x^4 + 340x^3 + 510x^2 - 5560700x - 237673175.$$

In particular $E(K)_{\text{tors}} = \mathbb{Z}/17\mathbb{Z}$.

Proof. By the same arguments as in Lemma 2.10, we get that an elliptic curve $E/\mathbb{Q}$ such that E gains a point of order 17 over a number field K of degree 8 has $j_E = -1 \cdot 2^{-17} \cdot 17 \cdot 373^3$ and 17 is the only surjective prime for all such curves. There cannot be any points of order 3 over K, as K is cyclic and $\mathbb{Q}(P)$ will not be Galois over $\mathbb{Q}$ for any $P \in E[3]$. Note that in this case the quadratic twist with minimal conductor of E' has LMFDB label `14450.o2` □

2.7. **Some special degrees.** From the results proved in this section, we immediately obtain the following result.

Lemma 2.12. *Let $d = 22$ or 26 and $E/\mathbb{Q}$ an elliptic curve. Then there is no primitive torsion growth over any number field of degree d.*

Proof. This follows immediately from Lemma 2.9 and [12, Table 1 and 2]. □

3. The algorithm

In this section we describe our algorithm. We always strive to make the algorithm useful in practice, and not to obtain an algorithm with small worst-case complexity. The reason for this is that in most cases, standard conjectures tell us that certain things will not happen, so we do not worry too much about the run-times of events that are conjecturally impossible. To give an explicit example, it is widely believed (see Conjecture 2.1) that $G_E(\ell) = \mathrm{GL}_2(\mathbb{F}_\ell)$ for all $\ell > 37$ and all non-CM elliptic curves over $\mathbb{Q}$. Hence, we focus on trying to quickly prove that indeed $G_E(\ell) = \mathrm{GL}_2(\mathbb{F}_\ell)$, and not worry too much on the run-time of what happens if $G_E(\ell) \neq \mathrm{GL}_2(\mathbb{F}_\ell)$ for $\ell > 37$, which, as already noted, conjecturally never happens.

We will use the following notation/definition in the algorithm.

Definition 1. For an elliptic curve $E/\mathbb{Q}$ and a positive integer d, we define $R(d, E)$ to be the set of primes such that there exists a number field K of degree $d'|d$ such that there is primitive ℓ-power torsion growth over K.

Recall that in [12] the set $R_{\mathbb{Q}}(d)$ is defined to be the set of all primes ℓ such that there exists a point of order ℓ on some elliptic curve $E/\mathbb{Q}$ over some number field of degree d. Note that $R_{\mathbb{Q}}(d)$ is unconditionally known for all $d < 3.343.296$ (and in the larger cases we know a set containing $R_{\mathbb{Q}}(d)$), so for all values of d in which one hopes to be able to run the algorithm.

The algorithm consists of 3 sub-algorithms.

Algorithm 1: $R(E, d)$
Input: An elliptic curve $E/\mathbb{Q}$ and integer d.
Output: The set $R(E, d)$

1. Set $R(E, d) := \emptyset$.
2. If the largest prime divisor of d is larger than 7, exit this algorithm and return $R(E, d) = \emptyset$.
3. Compute $R_{\mathbb{Q}}(d)$ using [12, Corollary 6.1].
4. For $\ell \in R_{\mathbb{Q}}(d)$ compute $G_E(\ell)$.
5. For $\ell \in R_{\mathbb{Q}}(d)$ compute the degrees n of number fields over which there is ℓ-torsion, depending on $G_E(\ell)$ using [12, Table 1 & 2] for non-CM curves and [12, Theorem 3.6 and 5.6]. If any such n divides d, add ℓ to $R(E, d)$.
6. Return $R(E, d)$.

Remark 3.1. Algorithm 1 is used to determine the (finite) set of primes ℓ such that there will be primitive ℓ-power torsion growth over number fields of degree d' dividing d.

Remark 3.2. Step (2) follows from [12, Theorem 7.1. (i)]. In step (4), we compute $G_E(\ell)$ using the algorithm sketched in [32, 1.8.].

Algorithm 2: ℓ-primary torsion growth

In this algorithm we will store a point or points generating the torsion group of $E(K)$. These are necessary for computing the ℓ-power torsion, but will not be returned in the output of the algorithm (although they could be), as they will not be necessary. We will also store an auxiliary sequence F of pairs $(F_i, (P_i, Q_i))$, where $K = \mathbb{Q}(E[\ell^i])$ and P_i and Q_i generate the ℓ^i-torsion of E and such that $[F_i : \mathbb{Q}]$ divides d. In Algorithm 2, F_i will always denote $\mathbb{Q}(E[\ell^i])$.

Input: An elliptic curve $E/\mathbb{Q}$, $d \in \mathbb{Z}_+$, a prime ℓ
Output: A set A of all pairs (K, T) such that E has primitive ℓ-power torsion growth over K, and $T := E(K)[\ell^\infty]$ and such that $[K : \mathbb{Q}]$ divides d.

1. $A := \emptyset$ and $F := \emptyset$.
2. If $E(\mathbb{Q})[\ell] \neq \{0\}$: $A := A \cup (\mathbb{Q}, E(\mathbb{Q})[\ell], S)$, where S is a set of generators of $E(\mathbb{Q})[\ell]$, and if $\#G_E(\ell)$ divides d, then factor ψ_l and let $F_1 = \mathbb{Q}(E[\ell])$ be the field defined by an irreducible factor of degree > 1 and then $A := A \cup (F_1, (\mathbb{Z}/\ell\mathbb{Z})^2, S)$ and $F := (F_1, S)$, where S is a set of generators of $E[\ell]$.

(3) If $E(\mathbb{Q})[\ell] = \{0\}$: Explicitly determine the triples $(K_i := \mathbb{Q}(P_i), \mathbb{Z}/\ell\mathbb{Z}, \{P_i\})$ for all $P_i \in E[\ell]$ by factoring the ℓ-division polynomial ψ_ℓ, keeping only one number field up to isomorphism. For all K_i constructed, check whether $\#G_E(\ell) = [K_i : \mathbb{Q}]$ for any i; if yes, change $(K_i, \mathbb{Z}/\ell\mathbb{Z}, \{P_i\})$ to $(K_i, (\mathbb{Z}/\ell\mathbb{Z})^2, S)$ and $F := F \cup (F_1, S)$, where S generates $E[\ell]$.

(4) Set $k := 2$. Repeat: if ($\ell < 11$ or $d \geq 55$) and ($\ell \neq 3$ or $k \leq 3$ or $d \geq 53$) and ($\ell \neq 5$ or $k = 2$ or $d \geq 50$) and ($\ell \neq 7$ or $d \geq 42$)

(i) Factor the primitive ℓ^k-division polynomial $\psi_{\ell^k}/\psi_{\ell^{k-1}}$, and check whether there are any irreducible factors of degree dividing d modulo small primes of good reduction. If not, then there exit the loop.

(ii) Now for each element (K_i, T, S) that we have in our set, for each cyclic subgroup of T of order ℓ^{k-1} (if it exists): select a generator Q. Factor over K_i the polynomial

$$\phi_\ell(x) - x(Q)\psi_\ell(x)^2 = g_1(x) \cdot \ldots \cdot g_u(x), \tag{1}$$

where ϕ_ℓ and ψ_ℓ are as defined in [31, Chapter 3.2. p.81].
Let P_i be a point of order ℓ^k such that $x(P_i)$ is a root of g_i; if $[\mathbb{Q}(P_i) : \mathbb{Q}]$ divides d, add the field, the appropriate subgroup and its generators into A.

(iii) For each element $(K_i, \mathbb{Z}/\ell^m\mathbb{Z} \times \mathbb{Z}/\ell^n\mathbb{Z}, S)$, where $m \geq n$, in A check whether K_iF_j is of degree dividing d for $j = m, \ldots, k$; if yes add $(K_iF_j, \mathbb{Z}/\ell^m\mathbb{Z} \times \mathbb{Z}/\ell^j\mathbb{Z}, S')$ to the list.

(iv) Check whether F_k is of degree dividing d by checking whether in A there exists an entry $(K_i, \mathbb{Z}/\ell^k\mathbb{Z} \times \mathbb{Z}/\ell^{k-1}\mathbb{Z}, S)$; if yes, check whether the element $P \in S$ of order ℓ^{k-1} is divisible by ℓ over K_i. If yes, change the previous entry into $(K_i, \mathbb{Z}/\ell^k\mathbb{Z} \times \mathbb{Z}/\ell^k\mathbb{Z}, S')$, where $S' = \{Q, R\}$ is obtained from $S = \{P, Q\}$, where Q is of order ℓ^k and $\ell R = P$ and add $(F_k := K_i, S')$ to F.

(v) k:=k+1;

until the first occurrence that there are no points of order ℓ^k in A.

(5) Return A.

Remark 3.3. Note that in (2), we have $\mathbb{Q}(E[\ell]) = F_1$ by [29, Lemma 5.17].

The conditions at the beginning of (4) come from Lemmas 2.6, 2.7, 2.8 and 2.9, and make the algorithm much faster for "small" (< 50) degrees, i.e. in all the ones where it is feasible to use the algorithm in practice.

In (4) (ii), we use [29, Corollary 5.18] where possible. By [31, Theorem 3.6] we have that

$$x(Q) = \frac{\phi_\ell(x)}{\psi_\ell(x)^2},$$

for any $P = (x, y)$ such that $Q = \ell P$. Using this step is crucial (instead of factoring ℓ^k-division polynomials) as one uses the polynomial (1) of degree ℓ^2 (over number fields) instead of factoring (over $\mathbb{Q}$) the primitive ℓ^k-division polynomial, which is of degree $\ell^{2k-2}(\ell^2 - 1)/2$.

In (4) (iii), if K_iF_j is not of degree dividing d, then neither is K_iF_{j+1}, so we can stop for the smallest j such K_iF_j is not of degree dividing d.

In (5), the generators of the torsion groups can be deleted from A, as they will not be used again later.

Algorithm 3: Combining different ℓ-primary torsion growths

Input: A positive integer d and a set A of all pairs (K, T) such that E has primitive ℓ-power torsion growth over K for some prime ℓ, and $T := E(K)[\ell^\infty]$ and such that $[K : \mathbb{Q}]$ divides d.

Output: A set B of all pairs (K, T) such that E has primitive torsion growth over K, and $T := E(K)_{\text{tors}}$ and such that $[K : \mathbb{Q}]$ divides d.

(1) To each pair (K, T) previously obtained we adjoin the set containing the pair (ℓ, K^ℓ) containing a prime ℓ such that T is a ℓ-group and $K^\ell := K$. So we get triples $(K, T, \{(\ell, K)\})$. For a triple (K, T, S), we will denote by $S' := \bigcup_{a \in S} a[1]$ the set of all first coordinates of S.

(2) Set k:=2; Repeat: new:=false; For each pair of triples (K_i, T_i, S_i) and (K_j, T_j, S_j) satisfying $|S_i' \cup S'| = k$ do:

(i) Check whether for all $(k-1)$-subsets B_m of $S_i \cup S_j$ there exists a triple $(K_r, T_r, S_r), r \neq i, j$ such that $B_m = S_r$, if no, discard this pair of triples and move onto the next one.

(ii) If the previous test has been passed, check whether the degree of K_iK_j divides d. If yes put new:=true, construct the triple $(K_iK_j, T, S_i \cup S_j)$ where

$$T = \prod_{\ell \in (S_i \cup S_j)'} T[\ell^\infty].$$

(3) Return the obtained results, forgetting the third element of the triples, i.e returning just the values (K, T).

Remark 3.4. In step (1) the elements in S_i and S_j are the same only if both coordinates are the same.

Finally the whole algorithm:

Algorithm TorsionGrowth

Input: An elliptic curve $E/\mathbb{Q}$ and a positive integer d.

Output: A sequence of all pairs (K, T) of a number field K of degree d' such that $d'|d$ and that E has primitive torsion growth over K, together with the group $T := E(K)_{\text{tors}}$.

(1) $R(E, d) :=$ `Algorithm1(E,d)`
(2) $A := \emptyset$
For $\ell \in R(E, d)$:
$A := A \cup$ `Algorithm2(E,`ℓ`,d)`
(3) $B :=$ `Algorithm3(A,d)`
(4) Return B

4. Computational results

Let d a positive integer and $\Phi(d)$ be the set of groups, up to isomorphism, that occur as torsion groups of some elliptic curve defined over a number field of degree d. Note that the set $\Phi(d)$ is finite thanks to Merel's uniform boundedness theorem. These sets have so far been determined for only* $d \leq 2$ [24, 20, 21]. For degree $d = 1, 2$, each group in $\Phi(d)$ occurs for infinitely many $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves, but for $d = 3$ this is not the case (see [25, Theorem 1] and [18, Theorem 3.4]). Therefore we define $\Phi^{\infty}(d) \subseteq \Phi(d)$ to be the set of groups that arise for infinitely many $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves. While $\Phi(d)$ is not completely known even for $d = 3$, $\Phi^{\infty}(d)$ is known for $d \leq 6$ [18, 19, 5].

Let d be a positive integer and $\Phi_{\mathbb{Q}}(d) \subseteq \Phi(d)$ be the set of groups, up to isomorphism, that occur as the torsion group $E(K)_{\text{tors}}$ of an elliptic curve E defined over $\mathbb{Q}$ base changed to a number field K of degree d. Notice that $\Phi_{\mathbb{Q}}(d)$ does not have to be contained in $\Phi^{\infty}(d)$, as the group $\mathbb{Z}/21\mathbb{Z}$ shows† for $d = 3$, and $\Phi^{\infty}(d)$ does not have to be contained in $\Phi_{\mathbb{Q}}(d)$ as the group $\mathbb{Z}/15\mathbb{Z}$ shows for $d = 2$ (see [25, Theorem 1] and [21]).

Similarly, for a fixed $G \in \Phi(1)$, let $\Phi_{\mathbb{Q}}(d, G)$ be the subset of $\Phi_{\mathbb{Q}}(d)$ consisting of all possible torsion groups $E(K)_{\text{tors}}$ of an elliptic curve E defined over $\mathbb{Q}$ such that $E(\mathbb{Q})_{\text{tors}} = G$ base changed to K, a number field of degree d. The sets $\Phi_{\mathbb{Q}}(d)$ and $\Phi_{\mathbb{Q}}(d, G)$, for any $G \in \Phi(1)$, have been completely determined for $d = 2, 3, 4, 5, 7$ in a series of papers [25, 14, 15, 11, 2, 12, 7]. Moreover, in [12] it has been established $\Phi_{\mathbb{Q}}(d) = \Phi(1)$ for any positive integer d whose prime divisors are greater than 7.

Our algorithm takes as input an elliptic curve E defined over $\mathbb{Q}$ and a positive integer d and outputs all the pairs (K, H) (up to isomorphism) where K is a number field of degree dividing d, E has primitive torsion growth over K, and $E(K)_{\text{tors}} \simeq H$. We denote by $\mathcal{H}_{\mathbb{Q}}(d, E)$ the multiset formed by $E(\mathbb{Q})_{\text{tors}}$ together with the groups H in the above computation. Note that we are allowing the possibility of two (or more) of the torsion subgroups H being isomorphic if the corresponding number fields K are not isomorphic. We call the set $\mathcal{H}_{\mathbb{Q}}(d, E)$ the set of torsion configurations of degree d of the elliptic curve $E/\mathbb{Q}$. We let $\mathcal{H}_{\mathbb{Q}}(d)$ denote the set of $\mathcal{H}_{\mathbb{Q}}(d, E)$ as E runs over all elliptic curves defined over $\mathbb{Q}$ such that $\mathcal{H}_{\mathbb{Q}}(d, E) \neq \{E(\mathbb{Q})_{\text{tors}}\}$, that is E has torsion growth over a number field of degree d. For $S \in \mathcal{H}_{\mathbb{Q}}(d)$ define $N_{\mathbb{Q}}(S)$ to be the minimum conductor $N_{\mathbb{Q}}(E)$ such that $\mathcal{H}_{\mathbb{Q}}(d, E) = S$ and we denote by $N_{\mathbb{Q}}(d)$ the maximum‡ of $N_{\mathbb{Q}}(S)$ for all $S \in \mathcal{H}_{\mathbb{Q}}(d)$. Note that if we denote the maximum of the cardinality of the sets S when $S \in \mathcal{H}_{\mathbb{Q}}(d)$ by $h_{\mathbb{Q}}(d)$, then $h_{\mathbb{Q}}(d)$ gives the maximum number of field extension of degrees dividing d where there is primitive torsion growth. The sets $\mathcal{H}_{\mathbb{Q}}(d)$ have been completely determined for $d = 2, 3, 5, 7$ and for any d not divisible by a prime smaller than 11 (see [15, 11, 7, 12]). From these results, one can read out the value of $h_{\mathbb{Q}}(d)$ for $d = 2, 3, 5, 7$ (see [26] for a different approach to obtain $h_{\mathbb{Q}}(2)$). For $d = 4, 6$, exhaustive computations to obtain bounds on the above sets and values have been carried out (see [10, 8]).

As d grows, all these problems become much more difficult, so it makes sense to obtain lower bounds on some of these sets, where possible. We will obtain such a lower bound for $d \leq 23$, by finding all the possible torsion

*M. Derickx. A. Etropolski, M. van Hoeij, J. Morrow and D. Zureick-Brown have announced results for $d = 3$.

†The second author showed in [25] that the elliptic curve with LMFDB label `162.c3` has torsion subgroup $\mathbb{Z}/21\mathbb{Z}$ defined over the cubic field $\mathbb{Q}(\zeta_9)^+ = \mathbb{Q}(\zeta_9 + \zeta_9^{-1})$ where ζ_9 is a primitive 9-th root of unity.

‡Note that the smallest integer B such that for every torsion group T possible over $\mathbb{Q}$ there exists an elliptic curve E with $E(\mathbb{Q})_{\text{tors}} = T$ and $N_{\mathbb{Q}}(E) \leq B$ is $B = 210$.

groups of the 2.483.649 elliptic curves of conductor less than 400.000 over number fields of degree up to 23. We chose to stop at 23 (although it could probably be feasible to do computations for a few more degrees), as this is the largest degree of number fields that have been included in the LMFDB at the moment of writing of this paper. The algorithm has been implemented in `Magma` [1] and can be found in the online supplement [13].

Table 1 gives a short overview of our computations. For the sake of simplicity we denote in Table 1 by (n) and (n,m) the groups $\mathbb{Z}/n\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}\times\mathbb{Z}/m\mathbb{Z}$, respectively. The values in the table are:

- 1^{st} column: degree d.
- 2^{nd} column: all the possible torsion subgroups H such that there exists an elliptic curve $E/\mathbb{Q}_{\supsetneq}$ and a number field K of degree d such that there is primitive torsion growth over K and such that $E(K)_{\text{tors}}=H$. Or in the other words, the subgroups in $\Phi_{\mathbb{Q}}(d)$ that do not appear in $\Phi_{\mathbb{Q}}(d')$ for any proper divisor $d'|d$.
- 3^{rd} column: a lower bound of $h_{\mathbb{Q}}(d)$ (or the exact value, where it is known), the maximum number of field extension of degrees dividing d where there is primitive torsion growth.
- 4^{th} column: a lower bound of $N_{\mathbb{Q}}(d)$, the minimum value such that there exist elliptic curves over $\mathbb{Q}_{\supsetneq}$ of conductor less than $N_{\mathbb{Q}}(d)$ with every possible torsion configuration over number fields of degree d.
- 5^{th} column: a lower bound of $\#\mathcal{H}_{\mathbb{Q}}(d)$, the number of torsion configurations over number fields of degree d.

d	$\Phi_{\mathbb{Q}}(d)\setminus\cup_{d'\|d,d'<d}\Phi_{\mathbb{Q}}(d')\supseteq$	$h_{\mathbb{Q}}(d)$	$N_{\mathbb{Q}}(d)$	$\#\mathcal{H}_{\mathbb{Q}}(d)$
1	$\{(1),(2),(3),(4),(5),(6),(7),(8),(9),(10),(12),(2,2),(2,4),(2,6),(2,8)\}$	–	–	–
2	$\{(15),(16),(2,10),(2,12),(3,3),(3,6),(4,4)\}$	4	3150	52
3	$\{(13),(14),(18),(21),(2,14)\}$	3	3969	26
4	$\{(13),(20),(24),(2,16),(4,8),(5,5),(6,6)\}$	≥ 9	≥ 14400	≥ 130
5	$\{(11),(25)\}$	1	121	4
6	$\{(30),(2,18),(3,9),(3,12),(4,12),(6,6)\}$	≥ 9	≥ 10816	≥ 137
7	–	1	26	1
8	$\{(17),(21),(30),(32),(2,20),(2,24),(3,12),(4,12)\}$	≥ 17	≥ 277440	≥ 275
9	$\{(19),(26),(27),(28),(36),(42),(2,18)\}$	≥ 6	≥ 3969	≥ 34
10	–	≥ 4	≥ 3150	≥ 58
12	$\left\{\begin{array}{c}(26),(28),(36),(37),(42),\\(2,28),(2,30),(2,42),(3,15),(3,21),(5,10),(6,12)\end{array}\right\}$	≥ 19	≥ 18176	≥ 268
14	–	≥ 4	≥ 3150	≥ 52
15	$\{(22),(50)\}$	≥ 3	≥ 3969	≥ 30
16	$\{(40),(48),(2,30),(2,32),(3,15),(4,16),(4,20),(5,15),(6,12),(8,8)\}$	≥ 25	≥ 277440	≥ 480
18	$\{(45),(2,26),(2,36),(2,42),(3,18),(3,21),(4,28),(6,18),(7,7),(9,9)\}$	≥ 17	≥ 254016	≥ 192
20	$\{(22),(33),(2,22),(5,10),(5,15)\}$	≥ 9	≥ 14400	≥ 149
21	$\{(43)\}$	≥ 3	≥ 3969	≥ 29

TABLE 1. Bounds on $\Phi_{\mathbb{Q}}(d)$ for $d\leq 23$.

In the online supplement [13] we give more data about our computations. For each degree $d\leq 23$ we include the following:

- For any $G\in\Phi_{\mathbb{Q}}(1)$ we include a table with a lower bound for the set $\Phi_{\mathbb{Q}}(d,G)$.
- For each torsion configuration $S\in\mathcal{H}_{\mathbb{Q}}(d)$ obtained, we provide the Cremona label [4] of the elliptic curve $E/\mathbb{Q}$ with minimal conductor such that $S=\mathcal{H}_{\mathbb{Q}}(E,d)$.

Remark 4.1. At the moment of writing this paper, each elliptic curve defined over $\mathbb{Q}_{\supsetneq}$ with conductor less than 400.000 and for any degree $d\leq 7$, the data obtained with our algorithm appears in LMFDB. We have in plan to include all the data for $d\leq 23$.

4.1. **Primitive torsion growth.** An interesting question is to restrict our attention to the case of primitive torsion growth of exactly a fixed degree instead of the whole growth over number fields of degree dividing a fixed

degree. For a positive integer d, we denote by $\Psi_{\mathbb{Q}}(d) \subseteq \Phi_{\mathbb{Q}}(d)$ the set of groups, up to isomorphism, that appear as primitive torsion growth of an elliptic curve defined over $\mathbb{Q}$ over a number field of degree d. In the same vein, we define $\Psi_{\mathbb{Q}}(d,G)$, $\mathcal{G}_{\mathbb{Q}}(d,E)$, $\mathcal{G}_{\mathbb{Q}}(d)$, $g_{\mathbb{Q}}(d)$, $M_{\mathbb{Q}}(d)$ analogously as we did $\Phi_{\mathbb{Q}}(d,G)$, $\mathcal{H}_{\mathbb{Q}}(d,E)$, $\mathcal{H}_{\mathbb{Q}}(d)$, $h_{\mathbb{Q}}(d)$, $N_{\mathbb{Q}}(d)$, respectively.

In Table 2 we include a lower bound for the set $\Psi_{\mathbb{Q}}(d)$ for $d \leq 23$. In particular, in each line the first column is the degree d, the second column includes the cyclic groups $\mathbb{Z}/n\mathbb{Z}$, denoted by (n), that we have obtained, and the rest of the columns $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mn\mathbb{Z}$, denoted by (m, mn), for $2 \leq m \leq 9$.

In Table 3 we show lower bounds for the values $g_{\mathbb{Q}}(d)$, $M_{\mathbb{Q}}(d)$ and $\#\mathcal{G}_{\mathbb{Q}}(d)$ for $d \leq 23$ non-prime.

Again, in the online supplement [13] we give more data which gives lower bounds on the sets $\Psi_{\mathbb{Q}}(d,G)$ and the Cremona labels of the elliptic curves $E/\mathbb{Q}$ with minimal conductor for each torsion configuration in $\mathcal{G}_{\mathbb{Q}}(d)$ that we have obtained.

d	(n)	$(2,2n)$	$(3,3n)$	$(4,4n)$	$(5,5n)$	$(6,6n)$	$(7,7n)$	$(8,8n)$	$(9,9n)$
2	3-10,12,15,16	1-6	1,2	1	-	-	-	-	-
3	2-4,6,7,9,10, 12-14,18,21	1,3,7	-	-	-	-	-	-	-
4	3-6,8,10,12, 13,15,16,20,24	2-6,8	1,2	1,2	1	1	-	-	-
5	5,10,11,25	-	-	-	-	-	-	-	-
6	3,4,6,7,9,10, 12-15,18,21,30	1,3,5-7,9	1-4	1,3	-	1	-	-	-
7	7	-	-	-	-	-	-	-	-
8	3,5,6,8,10,12,15,16, 17,20,21,24,30,32	2-6,8,10,12	1,2,4	1-3	1	1	-	-	-
9	6,7,9,12,14,18, 19,21,26-28,36,42	3,7,9	-	-	-	-	-	-	-
10	5,10,11,15,25	5	-	-	-	-	-	-	-
12	4,6,7-10,12-15,18,20, 21,24,26,28,30,36,37,42	2,3,5,6,7, 9,14,15,21	1-5,7	1,3	2	1,2	-	-	-
14	7	-	-	-	-	-	-	-	-
15	10,22,50	-	-	-	-	-	-	-	-
16	5,8,10,12,15,16,17 20,21,24,30,32,40,48	3-6,8,10, 12,15,16	1,2,4,5	1-5	1,3	1,2	-	1	-
18	6,7,9,12,14,18,19,21, 26-28,30,36,42,45	3,7,9,13,18,21	2-4,6,7	3,7	-	1,3	1	-	1
20	5,10,11,15,20,22,25,33	5,11	-	-	1-3	-	-	-	-
21	7,14,21,43	7	-	-	-	-	-	-	-

TABLE 2. Bounds on $\Psi_{\mathbb{Q}}(d)$ for $d \leq 23$.

d	4	6	8	9	10	12	14	15	16	18	20	21
$g_{\mathbb{Q}}(d) \geq$	5	5	9	3	1	6	1	1	10	6	3	1
$M_{\mathbb{Q}}(d) \geq$	18176	5184	223494	3969	150	18176	208	121	277440	254016	18176	1922
$\#\mathcal{G}_{\mathbb{Q}}(d) \geq$	104	88	200	20	7	134	1	3	336	101	26	6

TABLE 3. Data for $\Psi_{\mathbb{Q}}(d)$

4.2. **Timing.** We ran our algorithm for all elliptic curves defined over $\mathbb{Q}$ of conductor less than 400.000 and for degree $d \leq 23$ on the Number Theory Warwick Grid, in particular at two computers (`atkin` and `lehner`) with 64 CPUs at 2.50 GHz and 128GB of memory RAM each. In Table 4 we show for each degree d the total time of the whole computation, the maximum time taken for a single elliptic curve, and other statistics. Note that this project used roughly 2.7 cpu-years of computing time.

d	2	3	4	5	6	7	8	9	10	12	14	15	16	18	20	21
Mode (s)	0.06	0.06	0.06	0.06	0.09	0.06	0.08	0.06	0.06	0.23	0.06	0.06	0.08	0.09	0.06	0.06
Median (s)	0.07	0.06	0.07	0.06	0.13	0.06	0.10	0.06	0.07	4.7	0.07	0.06	0.10	0.13	0.07	0.06
Mean (s)	0.08	0.06	0.15	0.06	0.17	0.06	1.1	0.13	0.1	6.5	0.08	0.07	24	1.4	0.35	0.06
Maximum (s)	1.3	3.7	9.0	3.5	9.1	16	98	16	27	110	16	16	1200	440	470	17
Total (h)	54.4	43.5	106.4	42.2	119.6	41.6	774.7	87	66.8	4492.8	55.45	44.85	16339	988.1	241.3	43.8

TABLE 4. Timings for the computations

5. On sporadic torsion

Another motivation for our computations are sporadic points on the modular curves $X_1(m,n)$.

Definition 2. Let m, n positive integers such that $m|n$. We say that a degree d non-cuspidal point on the modular curve $X_1(m,n)$ is sporadic if there exists only finitely many degree d points on $X_1(m,n)$.

Obviously there exists a non-cuspidal sporadic point on $X_1(m,n)$ if and only if $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \in \Phi(d) \backslash \Phi^{\infty}(d)$.

There exist no sporadic points on modular curves $X_1(m,n)$ of degree $d \leq 2$, and hence the aforementioned elliptic curve with $\mathbb{Z}/21\mathbb{Z} \subsetneq$ torsion over a cubic field provides the lowest possible degree of a sporadic point on $X_1(n)$. There are many examples of sporadic points on $X_1(n)$ of degree ≥ 5, see [30] for a long list.

It is somewhat surprising that there is no (to our knowledge) known example of a sporadic point on $X_1(m,n)$ for $m \geq 2$. Hence it is interesting to ask what is the lowest possible degree of a sporadic point on $X_1(m,n)$ for $m \geq 2$. During our computation, we find a degree 6 sporadic non-cuspidal point on $X_1(4,12)$ about which we will say more in Section 5.1.

5.1. **A degree 6 sporadic point on $X_1(4,12)$.** As mentioned in the previous section, during our computations of torsion growth for elliptic curves of conductor less than 400.000, we found two elliptic curve with $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} \subsetneq$ torsion over a sextic field. By [5, Theorem 1.1], there are only finitely many such curves over sextic fields, so these curves induce sporadic points on $X_1(4,12)$.

We prove a stronger result below.

Theorem 5.1. *Let E be an elliptic curve defined over $\mathbb{Q} \subsetneq$ and $K/\mathbb{Q} \subsetneq$ such that $[K:\mathbb{Q}] = 6$. If $E(K)_{\text{tors}} = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} \subsetneq$ then the LMFDB label of E is `162.d2` or `1296.l2`. In particular, $j(E) = 109503/64$.*

Proof. Suppose $E/\mathbb{Q}$ is an elliptic curve satisfying the assumptions of the theorem. First notice that E does not have CM by [3, 4.6].

Denote by $G := E(\mathbb{Q})_{\text{tors}}$ and $H := E(K)_{\text{tors}}$. Let G_2 (resp. H_2) denote the 2-primary part of G (resp. H). We have the classification of the possible growth of the 2-primary part of the torsion over sextic fields (cf. [8, Proposition 6 (b), Table 2]):

G_2	H_2
$\{0\}$	$\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \subsetneq$
$\mathbb{Z}/2\mathbb{Z} \subsetneq$	$\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/16\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \subsetneq$
$\mathbb{Z}/4\mathbb{Z} \subsetneq$	$\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \subsetneq$
$\mathbb{Z}/8\mathbb{Z} \subsetneq$	$\mathbb{Z}/16\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \subsetneq$
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \subsetneq$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \subsetneq$
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \subsetneq$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \subsetneq$
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \subsetneq$	$--$

It now follows that:

- $G \neq \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/6\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ since then H_2 cannot be $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

- $G \neq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$since if $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \subsetneq G$ then $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} \not\subset H$; see the Remark below [10, Theorem 7].
- $G \neq \mathbb{Z}/12\mathbb{Z}$ since otherwise $G_2 = \mathbb{Z}/4\mathbb{Z}$ and $H_2 = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. The first author together with Lozano-Robledo, based on the classification of all the possible 2-adic images of Galois representations attached to elliptic curves without CM defined over $\mathbb{Q}$ given by Rouse and Zureick-Brown [27], have computed the degree of the field of definition of the $\mathbb{Z}/2^i\mathbb{Z} \times \mathbb{Z}/2^{i+j}\mathbb{Z}$ torsion for $i + j \leq 6$ (cf. [9, `2primary_Ss.txt`]). Using the above data it would follow that the number field K would have to have a quadratic subfield and that E would have full 4-torsion over it. Then E would have $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ torsion over this quadratic field, which is impossible [21, 20].
- $G \neq \mathbb{Z}/4\mathbb{Z}$. Using the same argument as above, we see that E has full 4-torsion over a quadratic field. Since $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} \notin \Phi_{\mathbb{Q}}(d)$ for $d = 2, 3, 4$, we have that the image of the mod 3 representation is such that there does not exist a point $P \in E(\overline{\mathbb{Q}})[3]$ such that $[\mathbb{Q}(P) : \mathbb{Q}] = 1$ or 2. On the other hand, by assumption, there exists a point $R \in E(\overline{\mathbb{Q}})[3]$ such that $[\mathbb{Q}(R) : \mathbb{Q}]$ divides 6. Checking for example [12, Table 1], we see that there is no mod 3 Galois representation satisfying both these conditions.

We know that both the cases $G = \{0\}$ and $G = \mathbb{Z}/3\mathbb{Z}$ can happen. For those cases we have that $G_2 = \{0\}$ and $H_2 = \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. We check using [9] and [27] that this happens over a sextic number field if and only the 2-adic image correspond to the modular curve `X20b` (using the notation of [27]), implying that there exists a $t \in \mathbb{Q}$ such that E is isomorphic to E_t, where:

$$E_t : y^2 = x^3 - 27\left(t^2 - 3\right)\left(t^2 - 8t - 11\right)^3 x + 54\left(t^2 - 8t - 11\right)^4\left(t^2 - 6t - 9\right)\left(t^2 + 2t + 3\right).$$

In particular,

$$j(E_t) = -\frac{4\left(t^2 - 3\right)^3\left(t^2 - 8t - 11\right)}{(t+1)^4}.$$

Now we need a point of order 3 defined over a subfield of a sextic number field. Checking [12, Table 1] we obtain that this could happen when $G_E(3)$ is `3Cs.1.1`, `3B.1.1`, `3Cs`, `3B.1.2` or `3B`. Then, thanks to the classification of mod 3 Galois representation of [32, Theorem 1.2] we have that $j(E) = J_1(s)$ or $j(E) = J_3(s)$ for some $s \in \mathbb{Q}$, where:

$$J_1(s) = \frac{27(s+1)^3(s+3)^3(s^2+3)^3}{t^3(t^2+3t+3)^3} \qquad \text{and} \qquad J_3(s) = \frac{27(s+1)(s+9)^3}{s^3}.$$

- $j(E_t) = J_1(s)$. Since $J_1(s)$ is a cube we have to solve the following Diophantine equation over $\mathbb{Q}$:

  $$(t+1)z^3 = -4\left(t^2 - 8t - 11\right).$$

  This equation defines a curve C of genus 2, which is birational to $C' : y^2 = x^6 - 10x^3 + 27$. The Jacobian of C' has rank 0 over $\mathbb{Q}$, so it is easy to determine that the points on $C'(\mathbb{Q}) = \{\pm\infty\}$, from which it follows that $C(\mathbb{Q}) = \{\pm\infty\}$. So there do not exist $t, s \in \mathbb{Q}$ satisfying $j(E_t) = J_1(s)$.
- $j(E_t) = J_3(s)$. In this case the equation defines a genus 1 curve, which is birational to the elliptic curve `48.a3` which has Mordell-Weil group over $\mathbb{Q}$isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. An easy computation shows that the possible t are $7, -5, -1/2$ and $-5/4$. The following table shows for each t the corresponding elliptic curve (by plugging in t into the equation of E_t) and the torsion over $\mathbb{Q}$:

t	label	G
7	`1296.l2`	(1)
-5	`1296.l1`	(1)
$-1/2$	`162.d1`	(1)
$-5/4$	`162.d2`	(3)

  Note that for the elliptic curve `162.d2` we have already obtained that the torsion over some sextic the torsion is $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$. For the remaining curves we check that only `1296.l2` has torsion $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$over a sextic field.

□

Acknowledgements. We would like to thank Jeremy Rouse and David Zureick–Brown for sharing with us the data related to 3-adic Galois representations of elliptic curves over $\mathbb{Q}$. We also thank John Cremona for providing access to computer facilities on the Number Theory Warwick Grid at University of Warwick, where the main part of the computations where done.

References

[1] W. Bosma, J. J. Cannon, C. Fieker, and A. Steel (eds.), Handbook of Magma functions, Edition 2.21 (2015). 8

[2] M. Chou, *Torsion of rational elliptic curves over quartic Galois number fields*, J. Number Theory **160** (2016) 603–628. 7

[3] P. L. Clark, P. Corn, A. Rice, and J. Stankewicz, *Computation on elliptic curves with complex multiplication*, LMS J. Comput. Math. **17** (2014), 509–539. 10

[4] J. E. Cremona, *ecdata: 2016-10-17 (Elliptic curve data for conductors up to 400.000)*, available on `http://johncremona.github.io/ecdata/`. 2, 8

[5] M. Derickx and A. V. Sutherland, *Torsion subgroups of elliptic curves over quintic and sextic number fields*, Proc. Amer. Math. Soc. **145** (2017), 4233–4245. 2, 7, 10

[6] N. D. Elkies, *Elliptic curves with 3-adic Galois representation surjective mod 3 but not mod 9*, arXiv/math: 0612734. 3

[7] E. González–Jiménez, *Complete classification of the torsion structures of rational elliptic curves over quintic number fields*, J. Algebra **478** (2017), 484–505. 7

[8] H. B. Daniels and E. González–Jiménez, *On the torsion of rational elliptic curves over sextic fields*, to appear in Math. Comp. arXiv: 1808.02887. 7, 10

[9] E. González-Jiménez and Á. Lozano-Robledo, *On the minimal degree of definition of p-primary torsion subgroups of elliptic curves*, Math. Res. Lett. **24** (2017), 1067–1096. (Data file `2primary_Ss.txt` available at `http://matematicas.uam.es/~enrique.gonzalez.jimenez/`) 11

[10] E. González–Jiménez and Á. Lozano–Robledo, *On torsion of rational elliptic curves over quartic fields*, Math. Comp. **87** (2018), 1457–1478. 7, 11

[11] E. González–Jiménez, F. Najman, and J.M. Tornero, *Torsion of rational elliptic curves over cubic fields*, Rocky Mountain J. Math. **46** (2016), 1899–1917. 7

[12] E. González–Jiménez and F. Najman, *Growth of torsion of elliptic curves upon base change*, arXiv: 1609.02515. 1, 3, 4, 5, 7, 11

[13] E. González–Jiménez and F. Najman. Magma scripts and electronic transcript of computations for the paper *"An algorithm for determining torsion growth of elliptic curves"*, `http://matematicas.uam.es/~enrique.gonzalez.jimenez/` 8, 9

[14] E. González–Jiménez and J.M. Tornero, *Torsion of rational elliptic curves over quadratic fields*, Rev. R. Acad. Cienc. Exactas Fís. Nat. Ser. A Math. RACSAM **118** (2014), 923–934. 7

[15] E. González–Jiménez and J.M. Tornero, *Torsion of rational elliptic curves over quadratic fields II*, Rev. R. Acad. Cienc. Exactas Fís. Nat. Ser. A Math. RACSAM **110** (2016), 121–143. 7

[16] R. Greenberg, *The image of Galois representations attached to elliptic curves with an isogeny*, Amer. J. Math. **134** (2012), 1167–1196. 3, 4

[17] R. Greenberg, K. Rubin, A. Silverberg, and M. Stoll, *On elliptic curves with an isogeny of degree 7*, Amer. J. Math. **136** (2014), 77–109. 3

[18] D. Jeon, C. H. Kim, and A. Schweizer, *On the torsion of elliptic curves over cubic number fields*, Acta Arith. **113** (2004) 291–301. 7

[19] D. Jeon, C. H. Kim, and E. Park, *On the torsion of elliptic curves over quartic number fields*, J. London Math. Soc. **74** (2006), 1–12. 7

[20] S. Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms*, Invent. Math. **109** (1992), 221–229. 7, 11

[21] M. A. Kenku and F. Momose, *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. **109** (1988), 125–149. 7, 11

[22] The LMFDB Collaboration, *The L-functions and Modular Forms Database*, (2019), http://www.lmfdb.org 2

[23] A. Lozano-Robledo, *Uniform bounds in terms of ramification*, Res. Number Theory **2018**, 4:6. 3, 4

[24] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. **47** (1978), 33–186. 7

[25] F. Najman, *Torsion of rational elliptic curves over cubic fields and sporadic points on $X_1(n)$*, Math. Res. Letters, **23** (2016) 245–272. 4, 7

[26] F. Najman, *The number of twists with large torsion of an elliptic curve*, Rev. R. Acad. Cienc. Exactas Fís. Nat. Ser. A Mat. RACSAM **109** (2015), 535–547. 7

[27] J. Rouse and D. Zureick-Brown, *Elliptic curves over $\mathbb{Q}$ and 2-adic images of Galois*, Research in Number Theory 1:12, 2015. (Data files and subgroup descriptions available at http://users.wfu.edu/rouseja/2adic/). 11

[28] J.-P. Serre, *Abelian ℓ-adic representations and elliptic curves*, Research Notes in Mathematics, vol. 7. A. K. Peters Ltd. Wellesy, MA, 1998. 2, 3

[29] A. V. Sutherland, *Computing images of Galois representations attached to elliptic curves*, Forum Math. Sigma **4** (2016), e4, 79 pp. 2, 6

[30] M. Van Hoeij, *Low Degree Places on the Modular Curve $X_1(N)$*, preprint, `http://arxiv.org/abs/1202.4355`. 10

[31] L. Washington, *Elliptic Curves: Number Theory and Cryptography*, Second Edition, Taylor & Francis, 2008. 6

[32] D. Zywina, *On the possible images of the mod ℓ representations associated to elliptic curves over $\mathbb{Q}$*, arXiv:1508.07660. 2, 5, 11

Universidad Autónoma de Madrid, Departamento de Matemáticas, Madrid, Spain
E-mail address: `enrique.gonzalez.jimenez@uam.es`

University of Zagreb, Bijenička cesta 30, 10000 Zagreb, Croatia
E-mail address: `fnajman@math.hr`