THE NUMBER OF TWISTS WITH LARGE TORSION OF AN ELLITPIC CURVE

FILIP NAJMAN

ABSTRACT. For an elliptic curve $E/\mathbb{Q}$, we determine the maximum number of twists $E^d/\mathbb{Q}$ it can have such that $E^d(\mathbb{Q})_{tors} \supsetneq E(\mathbb{Q})[2]$. We use these results to determine the number of distinct quadratic fields K such that $E(K)_{tors} \supsetneq E(\mathbb{Q})_{tors}$. The answer depends on $E(\mathbb{Q})_{tors}$ and we give the best possible bound for all the possible cases.

1. INTRODUCTION

Let E/K be an elliptic curve. It is well known, by the Mordell-Weil theorem, that $E(K)$ is a finitely generated abelian group and can hence be written as the direct product of its torsion subgroup and r copies of $\mathbb{Z}$, where r is the rank of E/K. We will be interested mostly in the case $K = \mathbb{Q}$, but we will write statements in greater generality whenever possible.

By Mazur's torsion theorem [16], $E(\mathbb{Q})_{tors}$ is isomorphic to one of the following 15 groups:

(1)
$$C_m, 1 \leq m \leq 12, \ m \neq 11,$$
$$C_2 \oplus C_{2m}, \ 1 \leq m \leq 4,$$

where C_m is a cyclic group of order m. Denote by E^d, where $d \in K^*/(K^*)^2$, a quadratic twist of E/K. We will assume throughout the paper that d is nonsquare, i.e. that E^d is not isomorphic to E over K.

It is natural to ask how the Mordell-Weil group $E(K)$ changes upon (quadratic) twisting. How the rank changes in families of quadratic twists is a subject that has been written extensively about (see [5, 12, 18] and the references therein).

It is a trivial fact the 2-torsion $E(K)[2]$ of $E(K)$ does not change upon quadratic twisting. We will say that a quadratic twist E^d/K has *large* torsion if $E^d(K)_{tors} \neq E(K)[2]$.

Another fact is that in a family of quadratic twists, $E^d(K)_{tors}$ will consist only of the even order torsion points for all but finitely many $d \in K^*/(K^*)^2$ (see [18, Lemma 5.5], [5, Proposition 1]). This statement follows easily from the Uniform Boundedness Conjecture, which has been proven by Merel [19].

The main purpose of this paper is to make this statement effective for $K = \mathbb{Q}$, by determining the maximum number of quadratic twists with large torsion an elliptic curve can have over $\mathbb{Q}$. We will show that this bound is 3 for a general $E/\mathbb{Q}$, and it can be even smaller, depending on $E(\mathbb{Q})_{tors}$.

Theorem 1. *The possible number of quadratic twists $E^d(\mathbb{Q})$ with large torsion of $E/\mathbb{Q}$, depending on $E(\mathbb{Q})_{tors}$ is as in the table below.*

C_1	$0, 1, 2$	C_4	$1, 2$	C_7	0	C_{10}	0	$C_2 \oplus C_4$	$0, 1$
C_2	$0, 1, 2, 3$	C_5	$0, 1$	C_8	1	C_{12}	1	$C_2 \oplus C_6$	0
C_3	$0, 1$	C_6	$0, 1, 2$	C_9	0	$C_2 \oplus C_2$	$0, 1$	$C_2 \oplus C_8$	0

We prove this result in Sections 3 and 4. Explicit examples for all the cases, apart from those in which $E(\mathbb{Q})_{tors}$ uniquely determines the number of twists with large torsion, can be found in Table 1 at the end of the paper.

In Section 5 we look at a related problem: given an elliptic curve $E/\mathbb{Q}$, how many quadratic extensions $K/\mathbb{Q}$ do there exist such that $E(K)_{tors} \supsetneq E(\mathbb{Q})_{tors}$? González-Jiménez and Tornero [4] gave upper bounds for the possible number of such quadratic extensions, depending on $E(\mathbb{Q})_{tors}$, but their bounds are far from optimal. We give the best possible bounds in the following theorem.

Theorem 2. *The possible numbers of quadratic fields $K/\mathbb{Q}$ such that $E(K)_{tors} \supsetneq E(\mathbb{Q})_{tors}$, depending on $E(\mathbb{Q})_{tors}$, is given in the table below.*

C_1	$0, 1, 2$	C_4	$1, 2, 3$	C_7	0	C_{10}	1	$C_2 \oplus C_4$	$0, 1, 2, 3$
C_2	$1, 2, 3, 4$	C_5	$0, 1$	C_8	$1, 3$	C_{12}	1	$C_2 \oplus C_6$	$0, 1$
C_3	$0, 1$	C_6	$1, 2, 3$	C_9	0	$C_2 \oplus C_2$	$0, 1, 2, 3$	$C_2 \oplus C_8$	0

Explicit examples for all the cases, apart from those in which $E(\mathbb{Q})_{tors}$ uniquely determines the number of quadratic fields in which the torsion grows, can be found in Table 2 at the end of the paper.

2. Auxiliary results

In this section we fix notation and list the main tools, most of which are well known, which we will later use to prove Theorems 1 and 2.

Let $E[n] = \{P \in E(\overline{\mathbb{Q}}) | nP = 0\}$ denote the n-th division group of E over $\overline{\mathbb{Q}}$ and let $\mathbb{Q}(E[n])$ be the n-th division field of E. The Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $E[n]$ and gives rise to an embedding

$$\rho_n : \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}) \hookrightarrow \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$$

called the *mod n Galois representation*. For a number field K, $E(K)[n]$ denotes the set of K-rational points in $E[n]$.

If there exists a K-rational cyclic isogeny $\phi : E \to E'$ of degree n, this implies that $\mathrm{Ker}\,\phi$ is a $\mathrm{Gal}(\overline{K}/K)$-invariant cyclic group of order n and we will say that E/K has an n-isogeny.

When we say that an elliptic curve over a field K has n-torsion we mean that it contains a subgroup isomorphic to C_n.

We start with the following important lemma.

Lemma 3 (Lemma 1.1 in [15]). *Let L/K be a quadratic extension of number fields and let $L = K(\sqrt{d})$. There exist homomorphisms*

$$f : E(K) \oplus E^d(K) \to E(L),$$

$$g : E(L) \to E(K) \oplus E^d(K),$$

such that the kernels and cokernels of f and g are annihilated by $[2]$.

For odd order torsion Lemma 3 translates to the following.

Corollary 4. *Let n be an odd integer. Using the same notation as in Lemma 3,*

$$E(K)[n] \oplus E^d(K)[n] \simeq E(L)[n].$$

Odd order torsion over quadratic extensions will induce an isogeny of the same order over the base field.

Lemma 5 (Lemma 5 in [20]). *Let L/K be a quadratic extension, n an odd positive integer, and E/K an elliptic curve such that $E(L)$ contains $\mathbb{Z}/n\mathbb{Z}$. Then E/K has an n-isogeny.*

Note that in the statement of [20, Lemma 5], the base field is $K = \mathbb{Q}$, but that everything generalizes trivially to a general number field K.

It will be important for us to know which are the possible n-isogenies (by which we mean a cyclic isogeny of degree n) over $\mathbb{Q}$ and which are the possible torsion groups over quadratic fields.

Theorem 6 ([8, 9, 10, 17]). *Let $E/\mathbb{Q}$ be an elliptic curve with an n-isogeny. Then $n \leq 19$ or $n \in \{21, 25, 27, 37, 43, 67, 163\}$.*

Theorem 7 ([7, 11]). *Let E/K be an elliptic curve over a quadratic field K. Then $E(K)_{tors}$ is isomorphic to one of the following groups.*

(2)
$$\begin{aligned} C_m, 1 \leq m \leq 18, \ m \neq 17, \\ C_2 \oplus C_{2m}, \ 1 \leq m \leq 6, \\ C_3 \oplus C_{3m}, \ m = 1, 2, \\ C_4 \oplus C_4. \end{aligned}$$

We denote by ψ_n the n-th division polynomial of an elliptic curve E (see [22, Section 3.2] for details), which satisfies that, for a point $P \in E$, $\psi_n(x(P)) = 0$ if and only if $nP = 0$. A method we will often use throughout the paper to determine whether a quadratic twist of a given elliptic curve has large torsion is to factor ψ_n and then compute what the torsion is in the extensions generated by factors of degree 2 and in the fields of definition of the y-coordinate of the point (x, y), where x is the root of a linear factor of ψ_n.

3. Quadratic twists of curves with odd order torsion

The easier case will be when an elliptic curve has torsion of odd order. We will use the names of particular elliptic curves as they appear in [2].

Proposition 8. *If $E(\mathbb{Q})_{tors} \simeq C_n$, where n is odd, then $E^d(\mathbb{Q})_{tors}$ has odd order for all $d \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$. Furthermore,*

a) *If $E(\mathbb{Q})_{tors} \simeq C_n$, where $n > 5$ is odd, then $E^d(\mathbb{Q})_{tors} \simeq C_1$ for all $d \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$.*

b) *If $E(\mathbb{Q})_{tors} \simeq C_5$, then $E^d(\mathbb{Q})_{tors} \simeq C_1$ for all $d \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$, except if E is the curve 50b1 and $d_1 = 5$ or if E is 50b2 and $d_1 = -15$; in both of these cases $E^{d_1}(\mathbb{Q})_{tors} \simeq C_3$ and $E^d(\mathbb{Q})_{tors} \simeq C_1$ for all other $d \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$.*

c) *If $E(\mathbb{Q})_{tors} \simeq C_3$, then there are 3 cases:*

   i) *$E^d(\mathbb{Q})_{tors} \simeq C_1$ for all $d \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$.*

   ii) *$E^{-3}(\mathbb{Q})_{tors} \simeq C_3$ and $E^d(\mathbb{Q})_{tors} \simeq C_1$ for all $-3 \neq d \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$.*

   iii) *E is the curve 50a3 and $d_1 = 5$ or E is 450b4 and $d_1 = -15$; in both of these cases $E^{d_1}(\mathbb{Q})_{tors} \simeq C_5$ and $E^d(\mathbb{Q})_{tors} \simeq C_1$ for all other $d \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$.*

d) *If $E(\mathbb{Q})_{tors} \simeq C_1$, then there are the following cases:*

   i) *$E^d(\mathbb{Q})_{tors} \simeq C_1$ for all $d \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$.*

   ii) *$E^{d_1}(\mathbb{Q})_{tors} \simeq C_n$, where $n = 7$ or 9 for some $d_1 \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$. Then $E^d(\mathbb{Q})_{tors} \simeq C_1$ for all other $d_1 \neq d \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$.*

   ii) *There exist 2 quadratic twists E^{d_1} and E^{d_2} such that $E^{d_1}(\mathbb{Q})_{tors} \simeq E^{d_2}(\mathbb{Q})_{tors} \simeq C_3$. Then for all other $d \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$, it holds that $E^d(\mathbb{Q})_{tors} \simeq C_1$.*

   iii) *There exists 1 quadratic twist such that $E^{d_1}(\mathbb{Q})_{tors} \simeq C_3$ and for all other $d \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$, it holds that $E^d(\mathbb{Q})_{tors} \simeq C_1$.*

   iv) *If E is a twist of 50b1 or 50b3, and is not 50b2 or 450b4, respectively, then E has one twist such that $E^{d_1}(\mathbb{Q})_{tors} \simeq C_3$ and one twist such that $E^{d_2}(\mathbb{Q})_{tors} \simeq C_5$ and for all other $d \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$, it holds that $E^d(\mathbb{Q})_{tors} \simeq C_1$. These are the only instances where an elliptic curve can have 2 quadratic twists of different odd order torsion.*

   v) *If E is not a twist of 50b1 or 50b3 and $E^{d_1}(\mathbb{Q})_{tors} \simeq C_5$, for some $d_1 \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$, then for all other $d \in \mathbb{Q}^*/(\mathbb{Q}^*)^2$, it holds that $E^d(\mathbb{Q})_{tors} \simeq C_1$.*

Proof. **a)** If there existed a quadratic twist E^d such that $E^d(\mathbb{Q})_{tors} \simeq C_m$ for some odd m, then it would hold, by Corollary 4 that

$$E(\mathbb{Q}(\sqrt{d}))_{tors} \simeq E(\mathbb{Q})_{tors} \oplus E^d(\mathbb{Q})_{tors},$$

which is a contradiction with Theorem 7.

b) If E had a quadratic twist with torsion C_n, where $n \geq 5$ is odd, Corollary 4 would give a contradiction with Theorem 7. The only cases when an elliptic curve E^d with torsion C_5 has a quadratic twist with torsion

C_3 is when $E(\mathbb{Q}(\sqrt{d}))_{tors} \simeq C_{15}$, and there are only 2 such cases (see [20, Theorem 2 c)]).

c) As before, E cannot have a quadratic twist with torsion C_n where $n > 5$ because of Corollary 4 and Theorem 7. As in b) there are only 2 cases when a twist can have torsion C_5 [20, Theorem 2 c)]. There exist elliptic curves $E/\mathbb{Q}$ with torsion $E(\mathbb{Q})_{tors} \simeq C_3$ with a twist $E^d(\mathbb{Q})_{tors} \simeq C_3$. For example, all curves of the form

$$x^3 + y^3 + z^3 = 3\alpha xyz, \ \alpha^3 \neq 1$$

have this property (see [13, Table 1.]). Likewise, there exist elliptic curves with 3-torsion and all quadratic twists with trivial torsion, for example $19a3$ [4, Table 2]. The case iii) follows from Corollary 4 and [20, Theorem 2 c)].

d) The case i) is for example $11a2$ [4, Table 2], while the cases ii), iii), iv), v) and the impossibility of any other case follow from a), b) and c).   □

4. Quadratic twists of curves with even order torsion

Lemma 9. *If* $E(\mathbb{Q})_{tors} \simeq C_{4n}$, *then there exists exactly one quadratic twist* E^d *such that* $E^d(\mathbb{Q}) \supset C_4$.

Proof. There exists exactly one quadratic field $\mathbb{Q}(\sqrt{d})$ over which E has full 2-torsion; the elliptic curves E and E^d are isomorphic over this field and $E(\mathbb{Q}(\sqrt{d})) \simeq E^d(\mathbb{Q}(\sqrt{d})) \supset C_2 \oplus C_4$. By [4, Theorem 5 iii)] it follows that $E^d(\mathbb{Q}) \supset C_4$. Hence we have proven that there exists one quadratic twist with torsion C_4; it remains to prove it is the only one. Suppose there exists a different one E^{d_1}. Since $E(\mathbb{Q}(\sqrt{d_1})) \simeq C_{4m}$, for some integer m, from Lemma 3 we have the exact sequence

$$0 \to \operatorname{Ker} \phi \to E(\mathbb{Q}(\sqrt{d})) \xrightarrow{\phi} E(\mathbb{Q}) \oplus E^d(\mathbb{Q}) \to \operatorname{coker} \phi \to 0.$$

As coker ϕ is a quotient of a group isomorphic to the quotient of $C_{4n} \oplus C_{4m}$ by Im ϕ, which is a subgroup of C_{4k} for some integer k. Since C_{4n} and C_{4m} have to be subgroups of C_{4k}, the only possibility that the cokernel is annihilated by 2 (which is necessary by Lemma 3) is that $k = n = m = 1$ and that the quotient is isomorphic to $C_2 \oplus C_2$.

But this also leads to a contradiction, as the quotient of $C_4 \oplus C_4$ by C_4 cannot be isomorphic to $C_2 \oplus C_2$, and hence annihilated by 2, which contradicts Lemma 3.   □

We use this lemma to count the possible number of quadratic twists with large torsion of an elliptic curve with even order torsion.

Proposition 10. *Let* $E(\mathbb{Q})_{tors} \simeq C_{2n}$.

 a) *If* $n = 1$ *then the following* 5 *cases are possible:*
  i) *All the quadratic twists of* E *have just 2-torsion.*
  ii) *E has 1 quadratic twist with a point of odd order and every other quadratic twist has only 2-torsion.*

      iii) *E has 2 quadratic twists with 3-torsion and every other quadratic twist has only 2-torsion.*
      iv) *E has 2 quadratic twists with 4-torsion and every other quadratic twist has only 2-torsion.*
      v) *E has 2 quadratic twists with 4-torsion and 1 quadratic twist with 3-torsion, and every other quadratic twist has only 2-torsion.*

b) *If $n = 2$ then E has 1 quadratic twist with 4-torsion. The curve E has 0 or 1 quadratic twists with 3-torsion. All other quadratic twists have only 2-torsion.*

c) *If $n = 3$ then there are 3 cases:*
      i) *All the quadratic twists have just 2-torsion.*
      ii) *E has 1 quadratic twist with 6-torsion and every other quadratic twist has 2-torsion.*
      iii) *E has 2 quadratic twists with 4-torsion and every other quadratic twist has only 2-torsion.*

d) *If $n = 4$ then E has exactly one quadratic twist which has torsion C_4 and all the other twists have just 2-torsion.*

e) *If $n = 5$ then all the quadratic twists of E have just 2-torsion.*

f) *If $n = 6$ then E has exactly one quadratic twist which has 4-torsion and all the other quadratic twists have just 2-torsion.*

Proof. **a)** To prove that each of these cases is possible, we simply list the curves which fall into the respective case. Examples for each of the cases can be found in Table 1. That they have the appropriate number of quadratic twists with given torsion is easy to determine by checking their division polynomials or by checking their isogeny diagrams in [2].

As can be seen from Proposition 9, E can have either 0 or 2 quadratic twists with 4-torsion. From Corollary 4 and Theorem 7, it can be seen that if E has a point of order 5, then it cannot have any other quadratic twist with large torsion. Using again Corollary 4 and Theorem 7, we see that E can have at most 2 quadratic twists with a point of order 3. Note that if it has 2 quadratic twists with a point of order 3, then it cannot have a quadratic twist with order 4, because in this case E would have 2 independent isogenies of degrees 3 and 12. This would imply that E is isogenous to a curve with a 36-isogeny, which is a contradiction with Theorem 6.

The cases **b)**, **c)** and **e)** are proven in the same manner as **a)**, using Corollary 4 and Theorems 6 and 7.

In the case **d)** one has to additionally check that the quadratic twist of E which contains 4-torsion has torsion isomorphic to C_4 (and not C_8). But that can be seen from the fact (Lemma 3) that the kernel of the map $E^d(\mathbb{Q}) \oplus E(\mathbb{Q}) \to E(\mathbb{Q}(\sqrt{d}))$ has to be annihilated by 2, and that $(C_8 \oplus C_8)/(C_2 \oplus C_2) \simeq C_4 \oplus C_4$, which leads to a contradiction with $E(\mathbb{Q}) \subset E(\mathbb{Q}(\sqrt{d}))$.

□

Finally, we list the possibilities when $E(\mathbb{Q})$ has full 2-torsion, which were proven by Kwon.

Proposition 11 ([14], Theorem 2)**.** *Let $E(\mathbb{Q})_{tors} \simeq C_2 \oplus C_{2n}$.*

  i) *If $n = 1$, then E can have either no large torsion quadratic twists, or 1 or 2 quadratic twists with torsion $C_2 \oplus C_4$ and no other large torsion quadratic twists, or 1 quadratic twist with torsion $C_2 \oplus C_{2m}$ for $m = 3$ or 4 and no other large torsion quadratic twists.*
  ii) *If $n = 2$, then E can have 0 or 1 quadratic twists with torsion $C_2 \oplus C_4$.*
  iii) *If $n = 3$ or 4 then E has no quadratic twists with large torsion.*

Propositions 8, 10 and 11 together prove Theorem 1.

Finally, we will prove that there are finitely many large torsion quadratic twists over any number field. This is a generalization of [5, Proposition 1], where it was shown that there are finitely many large torsion quadratic twists over $\mathbb{Q}$ and [18, Lemma 5.5], where it was shown that there are finitely many quadratic twists with a point of odd order over a general number field K. We will simultaneously prove that $E(K)_{tors}$, where K is a number field, grows in finitely many quadratic extensions, generalizing [4, Theorem 6] and [6, Lemma 3.4 a)].

Theorem 12. *Let E/K be an elliptic curve over a number field K.*
  a) *There exists finitely many quadratic extensions L/K such that $E(L)_{tors} \supsetneq E(K)_{tors}$.*
  b) *There exists finitely many E^d/K with large torsion.*

Proof. **a)** By [19], there exists a bound n such that $\#E(L)_{tors} < n$ for all quadratic extensions L of K. It suffices to prove that for any $n_1 < n$ there will be finitely many quadratic extensions L of K such that there exists a point of order n_1 over L, but which is not defined over K. But this follows trivially from the fact that $E[n_1]$ has n_1^2 (and hence finitely many) elements.

b) By [18, Lemma 5.5], it suffices to prove that there exist only finitely many quadratic twist $E^d(K)$ does not contain C_4. First note that if $E(K)_{tors} = E(K(\sqrt{d}))_{tors}$, then $E^d(K)$ cannot contain C_4, for otherwise the map $E^d(K) \oplus E(K) \to E(K(\sqrt{d}))$ from Lemma 3 could not be annihilated by 2. Now from a), it follows that this assumption is true for all but finitely many $d \in K^*/(K^*)^2$, proving the claim. $\square$

5. NUMBER OF QUADRATIC FIELDS WHERE THE TORSION GROWS

We introduce the following notation: for $E/\mathbb{Q}$ by $g(E)$ we denote the number of quadratic fields K such that $E(K)_{tors} \supsetneq E(\mathbb{Q})_{tors}$.

We first deal with the case when the order of the torsion is odd.

Proposition 13. *Let $E/\mathbb{Q}$ such that $|E(\mathbb{Q})_{tors}|$ is odd. Then $g(E)$ is equal to the number of quadratic twists of E with large torsion.*

Proof. This follows directly from Corollary 4. $\square$

Determining $g(E)$ when $|E(\mathbb{Q})_{tors}|$ is even is much harder. We start with the following lemma.

Lemma 14. *If $E(\mathbb{Q})_{tors} \simeq C_{2n}$, $n \neq 2$, then there are either 0 or 2 quadratic fields K such that $E(K)_{tors} \simeq C_{4n}$. If $n = 2$, then there can be either 0, 1 or 2 such quadratic fields, and if there is exactly one such quadratic field then $g(E) = 1$.*

Proof. We first look at the case $n \neq 2$. Let P be the generator of $E(\mathbb{Q})_{tors}$. Now the equation $2Q = P$ has 4 solutions in $E(\overline{\mathbb{Q}})$ and $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on the solutions. Since the solutions are by assumption not defined over $\mathbb{Q}$, it follows that they have either one orbit of length 4 or 2 orbits of length 2 under the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. In the former case, there will not exist a quadratic field K such that $E(K) \supset C_{4n}$. In the latter case it follows that $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on the solutions through 2 automorphisms of $\overline{\mathbb{Q}}$ of order 2, say σ and τ. It remains to show that $\sigma \neq \tau$ or equivalently that all the solutions of $2Q = P$ are defined over the same field K, giving $E(K) \supset C_2 \oplus C_4$.

Suppose $\sigma = \tau$. It follows that all the solutions of $2Q = P$ are defined over a quadratic field K, from which it follows that $E(K) \supset C_2 \oplus C_{4n}$. The cases $n = 1$ and $n = 3$ are impossible by [4, Theorem 5 iii)], while the cases $n \geq 4$ are impossible by Theorem 7.

In the case $n = 2$, it is possible that $\sigma = \tau$; the curve 1344m5 is such a curve. It remains to prove that in the case $\sigma = \tau$, or equivalently $E(K)_{tors} \simeq C_2 \oplus C_8$ for some quadratic field K, that for all quadratic fields $F \neq K$, it is true that $E(F)_{tors} \simeq C_4$. It is obvious that E cannot gain even order torsion in any quadratic field apart from K, so it remains to show that it does not gain any odd order torsion in any quadratic extension. First note that such a curve has a Galois-invariant subgroup of order 8 (say the one generated by a Q satisfying $2Q = P$). If it gained n-order torsion, where n is odd, in a quadratic extension, then it would mean that over $\mathbb{Q}$ it has an n-isogeny. Now it follows that there exists an elliptic curve with an $8n$-isogeny over $\mathbb{Q}$, which is in contradiction with Theorem 6. $\qquad\qquad\square$

Proposition 15. *Let $E(\mathbb{Q})_{tors} \simeq C_{2n}$.*

    a) *If $n = 1$, then $g(E) = 1, 2, 3$ or 4.*
    b) *If $n = 2$ then $g(E) = 1, 2$ or 3.*
    c) *If $n = 3$ then $g(E) = 1, 2$ or 3.*
    d) *If $n = 4$ then $g(E) = 1$ or 3.*
    e) *If $n = 5$ or 6 then $g(E) = 1$.*

Proof. **a)** Lemma 14 shows that E can have 0 or 2 extensions over which E contains C_4, and there has to be exactly 1 extension over which E has torsion $C_2 \oplus C_2$ and this extension is necessarily different from the ones over which E has torsion C_4 ([4, Theorem 5 iii)]). In addition, there can exist a quadratic field over which E has torsion C_6. Examples of curves E such that $g(E) = 1, 2, 3$ and 4 can be found in Table 2.

It is impossible that E gains 4-torsion in a quadratic extension and odd order torsion in 2 quadratic extensions (of degree m and n, respectively). To see that, first note that, for a quadratic field K, if $E(K)$ contained C_4, (but not $C_2 \oplus C_4$, since that is impossible), then $\mathrm{Gal}(K/\mathbb{Q})$ would act on $E[4](K)$ by permuting the 2 points of order 4, and hence E would have a 4-isogeny over $\mathbb{Q}$. The curve E would also have an m-isogeny and an (independent) n-isogeny, and hence there would exist an elliptic curve with a $4mn$-isogeny (see [20, Lemma 7]) over $\mathbb{Q}$, which is impossible by Theorem 6. This proves that $g(E) \leq 4$.

b) In the case $n = 2$, it follows by Lemma 14 that the torsion of E contains C_8 in $0, 1$ or 2 quadratic fields. If it contains C_8 in one extension, then as we have shown $g(E) = 1$.

If it contains C_8 in 2 extensions, then E has an 8-isogeny over $\mathbb{Q}$ (this can be shown using the same argument as in a)), and from Theorem 6 it follows that there are no extensions where E gains points of odd order because otherwise Lemma 5 would lead to a contradiction with Theorem 6. In addition there will be one quadratic field, different from the ones where the torsion is C_8, where the torsion will be $C_2 \oplus C_4$. In this case $g(E) = 3$; for example the curve 15a7 is such a curve.

If E contains C_8 in 0 quadratic fields, then it is possible that there exist 1 quadratic field where E has torsion C_{12}. Together with the field with torsion $C_2 \oplus C_4$, this means that $g(E) = 2$; 150c1 is such a curve.

c) By Lemma 14, there are 0 or 2 quadratic fields K such that $E(K)_{tors} \simeq C_{12}$ and there is exactly one quadratic field K such that $E(K)_{tors} \simeq C_2 \oplus C_6$. In addition, it is possible that $E(\mathbb{Q}(\sqrt{-3}) \simeq C_3 \oplus C_6$. Examples of curves with $g(E) = 1, 2$ and 3 can be found in Table 2.

To complete the proof, it remains to show that $g(E) \leq 3$, or in other words, that it is impossible that $E(\mathbb{Q}(\sqrt{-3})) \simeq C_3 \oplus C_6$ and that there exists a quadratic field K such that $E(K)_{tors} \simeq C_{12}$. If such a K existed, it would follow that $E/\mathbb{Q}$ has a 12-isogeny and from the fact that $E(\mathbb{Q}(\sqrt{-3})) \simeq C_3 \oplus C_6$ it would follow that $E/\mathbb{Q}$ has 2 independent 3-isogenies. Combining these 2 facts we would get that $E/\mathbb{Q}$ has a 12-isogeny and an independent 3-isogeny. By [20, Lemma 7], it follows that there exists an elliptic curve over $\mathbb{Q}$, isogenous to E, with a 36-isogeny. But this is impossible by Theorem 6.

d) This follows from the fact that there exists exactly 1 quadratic field over which E has torsion $C_2 \oplus C_{2n}$ and, by Lemma 14, 0 or 2 quadratic extensions with 16-torsion.

e) As before, by Theorem 7, there exists exactly 1 quadratic field over which E has torsion $C_2 \oplus C_{2n}$.

$\square$

Remark 16. Note that if $E(\mathbb{Q})_{tors} \simeq C_2$, it is impossible that the torsion of E grows to C_4 in one extension and to C_{2n}, where $n \geq 5$ is odd in another extension. One can see this as if $E(\mathbb{Q})_{tors} \simeq C_2$ and $E(K)_{tors} \supset C_4$ for some quadratic field K, it follows that E has a 4-isogeny over $\mathbb{Q}$. Also, by Lemma

5, it follows that E has a $4n$-isogeny over $\mathbb{Q}$, which is a contradiction with Theorem 6.

Proposition 17. *Let $E(\mathbb{Q})_{tors} \simeq C_2 \oplus C_{2n}$.*

    a) *If $n = 1$, then $g(E) = 0, 1, 2$ or 3.*
    b) *If $n = 2$, then $g(E) = 0, 1, 2$ or 3.*
    c) *If $n = 3$ then $g(E) = 0$ or 1.*
    d) *If $n = 4$ then $g(E) = 0$.*

Proof. **a)** We first note that E can gain torsion $C_2 \oplus C_4$ over either $0, 1, 2$ or 3 quadratic fields; there are 12 points of order 4 in $E(\overline{\mathbb{Q}})$, so it is obvious that there cannot be more than 3 extensions with torsion $C_2 \oplus C_4$, since E gains 4 points of order 4 in each of them.

Next we observe that it is impossible that E can gain points of odd order in more than 1 extension, since Lemma 5 would give a contradiction with Theorem 6.

We claim that if E gains torsion $C_2 \oplus C_4$ in 3 extensions, that then E gains no odd order points in any quadratic extension. Let $G = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Suppose the opposite. Then by Lemma 5 it follows that E has an n-isogeny, for some odd value n. In this case $K := \mathbb{Q}(E[4])$ is a biquadratic field and hence the image of the mod 4 Galois representation $\rho_{E,4}(G)$ has to be isomorphic to $\mathrm{Gal}(K/\mathbb{Q}) \simeq C_2 \oplus C_2$. Let $\mathrm{Gal}(K/\mathbb{Q}) = \{\mathrm{id}, \sigma_1, \sigma_2, \sigma_3\}$. All the σ_i have to have the property that they fix the complete 2 torsion, as $E(\mathbb{Q}) \supset C_2 \oplus C_2$, and that they fix a different point of order 4, as $E(F_i) \supset C_2 \oplus C_4$, where F_i is the quadratic field fixed by σ_i. By running through (in Magma [1]) all the subgroups of $\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ isomorphic to $C_2 \oplus C_2$ we obtain that the only possibility, up to conjugacy, for $\rho_{E,4}(G)$ is the group

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix} \right\}.$$

We see that this group is contained in a Borel subgroup, hence it follows that E has a cyclic 4-isogeny over $\mathbb{Q}$. As E also has an independent 2-isogeny, this implies that there is an elliptic curve $E'/\mathbb{Q}$, 2-isogenous to E over $\mathbb{Q}$, with an $8n$-isogeny, which is impossible.

Thus, we have proven that $g(E) \leq 3$. Furthermore, one can find examples of curves $E/\mathbb{Q}$ such that $g(E) = 0, 1, 2$ or 3 in Table 2, proving a).

b) First note that by [14, Theorem 2], the torsion of E over a quadratic field can grow into either $C_4 \oplus C_4$ or into $C_2 \oplus C_8$.

We claim that there exist at most two quadratic fields over which E has torsion $C_2 \oplus C_8$. Let $\langle P, Q \rangle \simeq E(\mathbb{Q})_{tors}$, where P is of order 2 and Q of order 4. If E gains points of order 8 over a quadratic field, it gains 8 of them in each quadratic field. The only way in which this can happen is that a point of order 4 becomes divisible by 2. Over one quadratic field K, E can possibly gain the 4 solutions of the equation $2X = Q$ and the 4 solutions of the equation $2X = 3Q$, and over another field F, E can gain the 4 solutions

of $2X = P + Q$ and the 4 solutions of $2X = P + 3Q$. This exhausts all the possible quadratic points of order 8, proving our claim.

It follows that $g(E) \leq 3$ (at most two extension with torsion $C_2 \oplus C_8$ and one with $C_4 \oplus C_4$). Examples of curve $E/\mathbb{Q}$ such that $g(E) = 0, 1, 2$ and 3 are given in Table 2, completing the proof of b).

Part **c)** is [14, Theorem 1 (ii)] and **d)** is [14, Theorem 1 (iii)]. $\square$

6. TORSION OF CUBIC AND QUARTIC TWISTS

To complete the study of large torsion in twists, we have to study cubic and quartic twists of elliptic curves. This is a much easier problem, since we have to study only the elliptic curves with j-invariant 0 and 1728. There is a difference in cubic and quartic twisting compared to quadratic twisting in the sense that the 2-torsion can change upon quartic and cubic twisting. In particular, the elliptic curve $E_2 : y^2 = x^3 + 2$ has trivial torsion, while its cubic twist $E_1 : y^2 = x^3 + 1$ and all quadratic twists of E_1 have non-trivial 2-torsion.

We state the results for elliptic curves with j-invariant 0 in the following proposition.

Proposition 18. *Among all the curves with j-invariant 0, there exists infinitely many with trivial torsion, infinitely many with torsion C_2, infinitely many with torsion C_3, and 1 with torsion C_6.*

Proof. An elliptic curve with j-invariant 0 is of the form

$$E_D : y^2 = x^3 + D, \text{ where } D \in \mathbb{Q}^*/(\mathbb{Q}^*)^6.$$

It follows that $E_D(\mathbb{Q})[2] \simeq \mathbb{Z}/2\mathbb{Z}$ if D is a cube and and $E_D(\mathbb{Q})[2]$ is trivial otherwise. A computation using division polynomials proves that there is no 4-torsion in $E_D(\mathbb{Q})$.

By [3, Theorem 3] it follows that $E_D(\mathbb{Q})[3] \simeq \mathbb{Z}/3\mathbb{Z}$ if D is a square and $E_D(\mathbb{Q})[3]$ is trivial otherwise.

There can be no other torsion in $E_D(\mathbb{Q})$ by [21, Proposition 1]. $\square$

Remark 19. Note that elliptic curves with j-invariant 0 are the only curves that have infinitely many large torsion twists, if one does not restrict twisting only to quadratic twisting.

We deal in a similar way with elliptic curves with j-invariant 1728.

Proposition 20. *Among all the curves with j-invariant 1728, there exists infinitely many with torsion C_2, infinitely many with torsion $C_2 \oplus C_2$ and 1 with torsion C_4.*

Proof. An elliptic curve with j-invariant 1728 is of the form

$$E_D : y^2 = x^3 + Dx, \text{ where } D \in \mathbb{Q}^*/(\mathbb{Q}^*)^4.$$

It follows that $E_D(\mathbb{Q})[2] \simeq \mathbb{Z}/2\mathbb{Z}$ if D is not a square and $E_D(\mathbb{Q})[2] \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ if D is a square. A computation using division polynomials

shows that the only elliptic curve with 4-torsion in this family is $E_4 : y^2 = x^3 + 4x$ with $E_4(\mathbb{Q})_{tors} \simeq \mathbb{Z}/4\mathbb{Z}$. By [3, Theorem 3], there is no p-torsion in $E_D(\mathbb{Q})$ for any odd primes p.

$\square$

References

[1] W. Bosma, J. J. Cannon, C. Fieker, A. Steel (eds.), Handbook of Magma functions, Edition 2.18 (2012).

[2] J. Cremona, Algorithms for Modular Elliptic Curves, 2nd ed. Cambridge University Press, Cambridge, 1997.

[3] L. Dieulefait, E. González-Jiménez and J. Jiménez Urroz, *On fields of definition of torsion points of elliptic curves with complex multiplication*, Proc. Amer. Math. Soc. **139** (2011), 1961–1969.

[4] 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, **108** (2014), 923–934.

[5] F. Gouvêa and B. Mazur, *The square-free sieve and the rank of elliptic curves*, J. Amer. Math. Soc. **4** (1991), 1–23.

[6] D. Jeon, C. H. Kim and E. Park, *On the torsion of elliptic curves over quartic number fields*, J. London Math. Soc. (2) **74** (2006), 1–12.

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

[8] M. A. Kenku, *The modular curves $X_0(65)$ and $X_0(91)$ and rational isogeny*, Math. Proc. Cambridge Philos. Soc. **87** (1980), 15–20.

[9] M. A. Kenku, *The modular curve $X_0(169)$ and rational isogeny*, J. London Math. Soc. (2) **22** (1980), 239–244.

[10] M. A. Kenku, *On the modular curves $X_0(125)$, $X_1(25)$ and $X_1(49)$*, J. London Math. Soc. (2) **23** (1981), 415–427.

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

[12] Z. Klagsbrun, B. Mazur and K.Rubin, *Disparity in Selmer ranks of quadratic twists of elliptic curves*, Ann. of Math. (2) **178** (2013), 287–320.

[13] D. S. Kubert, *Universal bounds on the torsion of elliptic curves*, Proc. London. Math. Soc. **33** (1976), 193–237.

[14] S. Kwon, *Torsion Subgroups of Elliptic Curves over Quadratic Extensions*, J. Number Theory, **62** (1997), 144–162.

[15] M. Laska and M. Lorenz, *Rational points on elliptic curves over $\mathbb{Q}$ in elementary abelian 2-extensions of $\mathbb{Q}$*, J. Reine Angew. Math. **355** (1985), 163–172.

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

[17] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), 129–162.

[18] B. Mazur and K. Rubin *Ranks of twists of elliptic curves and Hilbert's tenth problem*, Invent. Math. **181** (2010), 541–575.

[19] L. Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres*, Invent. Math. **124** (1996), 437–449.

[20] F. Najman, *Torsion of rational elliptic curves over cubic fields and sporadic points on $X_1(n)$*, Math. Res. Letters, to appear.

[21] J. L. Parish, *Rational Torsion in Complex-Multiplication Elliptic Curves*, J. Number Theory, **33** (1989), 257–265.

[22] L. C. Washington, Elliptic Curves: Number Theory and Cryptography, Second Edition, Chapman & Hall, Boca Ranton, 2008.

Appendix

Table 1 gives examples for every case possible from Theorem 1, excluding those when the choice of $E(\mathbb{Q})_{tors}$ uniquely determines the number of twists with large torsion. The second column gives an example of such an elliptic curve, the third column gives the number of quadratic twists of E, and in the fourth column all the d-s such that $E^d(\mathbb{Q})$ has large torsion are listed, with $E^d(\mathbb{Q})_{tors}$ given in brackets for every listed d.

$E(\mathbb{Q})_{tors}$	E	#	$d(E^d(\mathbb{Q})_{tors})$
C_1	11a2	0	-
C_1	832f1	1	$2(C_7)$
C_1	1600c1	2	$2(C_5), 10(C_3)$
C_2	52a1	0	-
C_2	4800l3	1	$2(C_{10})$
C_2	75b4	2	$5(C_4), 3(C_4)$
C_2	450g1	3	$-3(C_4), 5(C_4), -15(C_6)$
C_3	19a3	0	-
C_3	19a1	1	$-3(C_3)$
C_4	15a7	1	$15(C_4)$
C_4	150c1	2	$-15(C_4), 5(C_6)$
C_5	11a1	0	-
C_5	50b1	1	$5(C_3)$
C_6	20a1	0	-
C_6	14a2	1	$-3(C_6)$
C_6	30a1	2	$5(C_4), -3(C_4)$
$C_2 \oplus C_2$	120b2	0	-
$C_2 \oplus C_2$	150c2	1	$5(C_2 \oplus C_6)$
$C_2 \oplus C_4$	24a1	0	-
$C_2 \oplus C_4$	15a1	1	$-1(C_2 \oplus C_4)$

Table 1.

Table 2 gives examples for every case possible from Theorem 2, excluding those when the choice of $E(\mathbb{Q})_{tors}$ uniquely determines the number of quadratic fields in which the torsion of E grows. The values in the columns are listed in a similar manner as in Table 1.

$E(\mathbb{Q})_{tors}$	E	$g(E)$	$d(E(\mathbb{Q}(\sqrt{d}))_{tors})$
C_1	11a2	0	-
C_1	832f1	1	$2(C_7)$
C_1	1600c1	2	$2(C_5), 10(C_3)$
C_2	52a1	1	$-1(C_2 \oplus C_2)$
C_2	480l3	2	$-15(C_2 \oplus C_2), 2(C_{10})$
C_2	75b4	3	$15(C_2 \oplus C_2), 5(C_8), 3(C_4)$
C_2	2880n1	4	$-6(C_6), 2(C_4), -30(C_4), -15(C_2 \oplus C_2),$
C_3	19a3	0	-
C_3	19a1	1	$-3(C_3 \oplus C_3)$
C_4	222c4	1	$3(C_2 \oplus C_4)$
C_4	90c1	2	$-15(C_2 \oplus C_4), -3(C_{12})$
C_4	15a7	3	$5(C_8), 3(C_8), 15(C_2 \oplus C_4)$
C_5	11a1	0	-
C_5	50b1	1	$5(C_{15})$
C_6	20a1	1	$-1(C_2 \oplus C_6)$
C_6	14a2	2	$2(C_2 \oplus C_6), -3(C_3 \oplus C_6)$
C_6	30a1	3	$5(C_{12}), -3(C_{12}), -15(C_2 \oplus C_6)$
C_8	15a4	1	$-1(C_2 \oplus C_8)$
C_8	210e1	3	$-7(C_2 \oplus C_8), -15(C_{16}), 105(C_{16})$
$C_2 \oplus C_2$	120b2	0	-
$C_2 \oplus C_2$	33a1	1	$-1(C_2 \oplus C_4)$
$C_2 \oplus C_2$	960o2	2	$6(C_2 \oplus C_4), -2(C_2 \oplus C_6)$
$C_2 \oplus C_2$	15a2	3	$5(C_2 \oplus C_4), -5(C_2 \oplus C_4), -1(C_2 \oplus C_4)$
$C_2 \oplus C_4$	24a1	0	-
$C_2 \oplus C_4$	21a1	1	$-3(C_2 \oplus C_8)$
$C_2 \oplus C_4$	15a1	2	$-1(C_4 \oplus C_4), 5(C_2 \oplus C_8)$
$C_2 \oplus C_4$	210e3	3	$-1(C_4 \oplus C_4), 6(C_2 \oplus C_8), -6(C_2 \oplus C_8)$
$C_2 \oplus C_6$	30a2	0	-
$C_2 \oplus C_6$	90c6	1	$6(C_2 \oplus C_{12})$

Table 2.

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