A CRITERION TO RULE OUT TORSION GROUPS FOR ELLIPTIC CURVES OVER NUMBER FIELDS

PETER BRUIN AND FILIP NAJMAN

Abstract. We present a criterion for proving that certain groups of the form $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ do not occur as the torsion subgroup of any elliptic curve over suitable (families of) number fields. We apply this criterion to eliminate certain groups as torsion groups of elliptic curves over cubic and quartic fields. We also use this criterion to give the list of all torsion groups of elliptic curves occurring over a specific cubic field and over a specific quartic field.

1. Introduction

A fundamental result in the theory of elliptic curves, the Mordell–Weil theorem, states that the Abelian group of points of an elliptic curve (or more generally an Abelian variety) E over a number field K is finitely generated. Thus, $E(K)$ is isomorphic to $E(K)_{\mathrm{tors}} \oplus \mathbb{Z}^r$, where $E(K)_{\mathrm{tors}}$ is the torsion subgroup of $E(K)$ and $r \geq 0$ is the rank of $E(K)$.

We will denote by $\Phi(d)$, where d is a positive integer, the set of all the possible isomorphism types of $E(K)_{\mathrm{tors}}$, where K runs through all number fields K of degree d and E runs through all elliptic curves over K. Similarly, for a fixed number field K, we will denote by $\Phi(K)$ the set of all the possible isomorphism types of $E(K)_{\mathrm{tors}}$ where E runs through all elliptic curves over this fixed field K. Obviously, if K is a number field of degree d, then $\Phi(K) \subseteq \Phi(d)$, and $\Phi(d)$ is the union of the $\Phi(K)$ with K running over all number fields of degree d. It is interesting to determine the set $\Phi(d)$ for fixed integers d, as well as the set $\Phi(K) \subseteq \Phi(d)$ for fixed number fields K of degree d.

Let C_m be a cyclic group of order m. Mazur's torsion theorem [23, 24] tells us that $\Phi(\mathbb{Q}) = \Phi(1)$ consists of the following 15 groups:

$$\begin{aligned} &C_m, && m = 1, \dots, 10, 12, \\ &C_2 \oplus C_{2m}, && m = 1, \dots, 4. \end{aligned} \tag{1}$$

Similarly, by a theorem of Kamienny [15, Theorem 3.1] and Kenku and Momose [19, Theorem (0.1)], $\Phi(2)$ consists of the following 26 groups:

$$\begin{aligned} &C_m, && m = 1, \dots, 16, 18, \\ &C_2 \oplus C_{2m}, && m = 1, \dots, 6, \\ &C_3 \oplus C_{3m}, && m = 1, 2, \\ &C_4 \oplus C_4. \end{aligned} \tag{2}$$

Over cubic fields, we know that if a point on an elliptic curve has prime order p, then $p \leq 13$ [31, 32], we know all the isomorphism types in $\Phi(3)$ that appear as the torsion groups of infinitely many non-isomorphic elliptic curves [11], and we know that this list is strictly smaller than $\Phi(3)$ [29], as opposed to what happens in the

rational and quadratic cases. Unfortunately, $\Phi(d)$ has as yet not been determined for any $d \geq 3$, although Maarten Derickx (personal communication) has told us that the computation of $\Phi(3)$ should be within reach.

As for results on $\Phi(K)$ for specific K, Mazur [23] determined $\Phi(\mathbb{Q}) = \Phi(1)$, the second author determined $\Phi(\mathbb{Q}(\zeta_3))$ and $\Phi(\mathbb{Q}(\zeta_4))$ [26], and methods of determining $\Phi(K)$ for other quadratic fields K were given by Kamienny and the second author [16]. The second author also tried to determine $\Phi(K)$ for certain cubic fields K with small discriminant, but managed to obtain only partial results [28].

In this paper we develop a criterion, based on a careful study of the cusps of modular curves $X_1(m, n)$, which can tell us that certain groups do not occur as torsion groups of elliptic curves over a number field K. This criterion is essentially a generalization of a criterion of Kamienny [13]. Kamienny showed that for certain n, the curve $X_1(n)$ cannot have non-cuspidal points over an extension of degree d of $\mathbb{Q}$, where d is less than the gonality of $X_1(n)$, as points of degree d on $X_1(n)$ would force functions of a smaller degree than the gonality to exist, which is impossible.

We generalize Kamienny's approach both by using the modular curves $X_1(m, n)$ instead of $X_1(n)$ and by viewing the number fields K as extensions of a suitable subfield L of $\mathbb{Q}(\zeta_m)$. This generalization is somewhat technical (for example, it requires a careful consideration of the fields of definitions of cusps), but gives us more flexibility in ruling out torsion groups of the form $C_m \oplus C_n$. Our criterion, on its own or in combination with other techniques, allows us to advance our understanding of the torsion groups of elliptic curves over K, both when K is a fixed number field and when K runs through all number fields of degree d. In particular, we make progress in determining $\Phi(3)$ and $\Phi(4)$ by ruling out a number of possibilities for torsion groups of elliptic curves over cubic and quartic fields. As for determining $\Phi(K)$ for a fixed cubic or quartic field K, a natural choice for a quartic field K, in view of [26], is the 'next' cyclotomic field, $\mathbb{Q}(\zeta_5)$. Since there are no cubic cyclotomic fields, we choose the cyclic cubic field $\mathbb{Q}(\zeta_{13} + \zeta_{13}^5 + \zeta_{13}^8 + \zeta_{13}^{12})$.

In Section 2, we state and prove our main results (Theorem 1 and Corollary 3). In Sections 3 and 4, we use Theorem 1 to determine $\Phi(\mathbb{Q}(\zeta_{13} + \zeta_{13}^5 + \zeta_{13}^8 + \zeta_{13}^{12}))$ and $\Phi(\mathbb{Q}(\zeta_5))$, achieving to our knowledge the first determination of $\Phi(K)$ for a cubic and a quartic field, respectively. In Sections 5 and 6, we use Corollary 3, together with other techniques, to prove that a large number of finite groups do not occur as torsion groups of elliptic curves over cubic and quartic fields, respectively.

The computer calculations were done using Magma [22]. Showing that the rank of Jacobians over $\mathbb{Q}$ is 0, unless otherwise mentioned, has been done by showing that the L-function of (the factors of) J is non-zero. By results of Kato [17], the Birch-Swinnerton–Dyer conjecture is true for quotients of modular Jacobians, so this computation unconditionally proves that the rank is 0.

2. Main results

Notation. If K is a number field, $\mathcal{O}_K$ denotes its ring of integers. If $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$, we write $k(\mathfrak{p})$ for the residue field $\mathcal{O}_K/\mathfrak{p}$, and $\mathrm{Nm}(\mathfrak{p}) = \#k(\mathfrak{p})$. Furthermore, we denote by $\mathcal{O}_{K,\mathfrak{p}}$ the localization of $\mathcal{O}_K$ at $\mathfrak{p}$.

Definition. Let m and n be positive integers with $m \mid n$. Let L be a subfield of $\mathbb{Q}(\zeta_m)$, and let $\mathfrak{p}_0$ be a prime of L. Let X be the curve $X_1(m, n)_{\mathbb{Q}(\zeta_m)}$ viewed as a (proper, smooth, but possibly geometrically disconnected) curve over L. We consider triples $(\mathcal{X}, \mathcal{X}', \pi)$, where

- $\mathcal{X}$ is a flat, proper model of X over $\mathcal{O}_{L,\mathfrak{p}_0}$ such that the j-invariant extends to a map $j\colon \mathcal{X} \to \mathbb{P}^1_{\mathcal{O}_{L,\mathfrak{p}_0}}$;
- $\mathcal{X}'$ is a flat, proper and regular curve over $\mathcal{O}_{L,\mathfrak{p}_0}$ such that the curve $X' = \mathcal{X}'_L$ over L is geometrically connected;
- $\pi\colon \mathcal{X} \to \mathcal{X}'$ is a proper and generically finite map of $\mathcal{O}_{L,\mathfrak{p}_0}$-schemes.

Given such a triple $(\mathcal{X}, \mathcal{X}', \pi)$, we write $\mathcal{C}$ for the topological inverse image of the section ∞ under the map $j\colon \mathcal{X} \to \mathbb{P}^1_{\mathcal{O}_{L,\mathfrak{p}_0}}$, and $\mathcal{C}'$ for the topological image of $\mathcal{C}$ under π equipped with the reduced induced subscheme structure. With this notation, we call $(\mathcal{X}, \mathcal{X}', \pi)$ a *nice* $(L, \mathfrak{p}_0)$*-quotient* of $X_1(m,n)$ if the following conditions are satisfied:

(1) The scheme $\mathcal{C}'$ is normal and lies in the smooth locus of $\mathcal{X}'$ over $\mathcal{O}_{L,\mathfrak{p}_0}$.
(2) The image of the open subscheme $\mathcal{X} \setminus \mathcal{C}$ under π equals $\mathcal{X}' \setminus \mathcal{C}'$.

For our applications, the curve X' will also be a modular curve and π will have a moduli interpretation (e.g. forgetting part of the level structure). In this setting (X, X', π) is automatically a nice $(L, \mathfrak{p}_0)$-quotient.

Theorem 1. *Let A be a group of the form $C_m \oplus C_n$ with $m \mid n$, let K and L be number fields with $L \subseteq \mathbb{Q}(\zeta_m) \subseteq K$, and let $d = [K : L]$. Let $\mathfrak{p}_0$ be a prime of L, let p be the residue characteristic of $\mathfrak{p}_0$, and let e be the largest absolute ramification index of a prime of K dividing $\mathfrak{p}_0$. Let $S_{K,\mathfrak{p}_0}$ be the set*

$$S_{K,\mathfrak{p}_0} = \{\delta \geq 1 \mid \delta \text{ divides } [k(\mathfrak{p}) : k(\mathfrak{p}_0)] \text{ for some prime } \mathfrak{p} \text{ of } K \text{ over } \mathfrak{p}_0\}.$$

Let

$$A' = \begin{cases} A & \text{if } p > e+1 \\ \text{maximal } p\text{-divisible subgroup of } A & \text{if } p \leq e+1. \end{cases}$$

Let $(\mathcal{X}, \mathcal{X}', \pi)$ be a nice $(L, \mathfrak{p}_0)$-quotient of $X_1(m,n)$. Let $X' = \mathcal{X}'_L$, and let J' be the Jacobian of X'. Let h be the least common multiple of the ramification indices $e(\mathfrak{q}/\mathfrak{p}_0)$ where $L(C)$ is the function field of an irreducible component C of $\mathcal{C}'$ and $\mathfrak{q}$ is a prime of $L(C)$ over $\mathfrak{p}_0$. Assume that the following conditions are satisfied:

i) *The gonality of X' over L is at least $dh+1$.*
ii) *The group $J'(L)$ has rank 0.*
iii) *If $p = 2$, then the 2-torsion subgroup of $J'(L)$ is trivial.*
iv) *For all primes $\mathfrak{p} \mid \mathfrak{p}_0$ of K, there does not exist an elliptic curve over $k(\mathfrak{p})$ with a subgroup isomorphic to A'.*
v) *For all primes $\mathfrak{p} \mid \mathfrak{p}_0$ of K, neither $3\,\mathrm{Nm}(\mathfrak{p})$ nor $4\,\mathrm{Nm}(\mathfrak{p})$ is divisible by $\#A'$.*
vi) *For all irreducible components C of $\mathcal{C}'$, if the function field $L(C)$ has a prime $\mathfrak{q}$ over $\mathfrak{p}_0$ such that $[k(\mathfrak{q}) : k(\mathfrak{p}_0)]$ is in $S_{K,\mathfrak{p}_0}$, then $\mathfrak{q}$ is the* unique *prime of $L(C)$ over $\mathfrak{p}_0$.*

Then there does not exist an elliptic curve over K with a subgroup isomorphic to A.

We will prove Theorem 1 below; we begin with an auxiliary result.

Lemma 2. *Let A, K, L and $\mathfrak{p}_0$ be as in Theorem 1. Under the conditions iv) and v) of Theorem 1, any elliptic curve E over K equipped with an embedding $\iota\colon A \hookrightarrow E(K)$ has multiplicative reduction at all primes of K lying over $\mathfrak{p}_0$.*

Proof. Let $\mathfrak{p}$ be a prime of K over $\mathfrak{p}_0$. By $\tilde{E}_\mathfrak{p}$ we denote the reduction of E modulo $\mathfrak{p}$, i.e. the special fibre of the Néron model of E at $\mathfrak{p}$. Then we have a reduction map

$$E(K) \to \tilde{E}_\mathfrak{p}(k(\mathfrak{p})).$$

This map is injective on $\iota(A')$ by [18, Appendix] and the definition of A'. The group $\tilde{E}_{\mathfrak{p}}(k(\mathfrak{p}))$ therefore contains a subgroup isomorphic to A'.

By assumption iv), E does not have good reduction at $\mathfrak{p}$. If E had additive reduction, then by the Kodaira–Néron classification [33, Appendix C, §15], $\tilde{E}_{\mathfrak{p}}(k(\mathfrak{p}))$ would be a product of the additive group of $k(\mathfrak{p})$ and a group of order ≤ 4, contradicting assumption v). We conclude that E has multiplicative reduction at $\mathfrak{p}$. □

Proof of Theorem 1. Let $\mathcal{X}_{\mathfrak{p}_0}$ and $\mathcal{X}'_{\mathfrak{p}_0}$ be the special fibres of $\mathcal{X}$ and $\mathcal{X}'$ over $\mathfrak{p}_0$. Let $\mathcal{J}'$ be the Néron model of J' over $\mathcal{O}_{L,\mathfrak{p}_0}$. It is known [2, §9.5, Theorem 4] that $\mathcal{J}'$ represents the functor P/E, where P is the open subfunctor of $\mathrm{Pic}_{\mathcal{X}'/\mathcal{O}_{L,\mathfrak{p}_0}}$ given by line bundles of total degree 0 and E is the schematic closure in P of the unit section in $P(L)$. We have a commutative diagram

$$\begin{array}{ccccc} & & P(\mathcal{O}_{L,\mathfrak{p}_0}) & \longrightarrow & P(k(\mathfrak{p}_0)) \\ & & \downarrow & & \downarrow \\ J'(L) & = & \mathcal{J}'(\mathcal{O}_{L,\mathfrak{p}_0}) & \longrightarrow & \mathcal{J}'(k(\mathfrak{p}_0)). \end{array}$$

By assumptions ii) and iii) and [18, Appendix], the bottom horizontal map is injective.

Suppose the theorem is false. Let E be an elliptic curve over K equipped with an embedding $A \rightarrowtail E(K)$. These data determine a point of $X(K)$ whose Zariski closure is a prime divisor D on $\mathcal{X}$. Let $D_{\mathfrak{p}_0}$ be the schematic intersection of the divisor D with $\mathcal{X}_{\mathfrak{p}_0}$, and let $(\pi_* D)_{\mathfrak{p}_0}$ be the schematic intersection of $\pi_* D$ with $\mathcal{X}'_{\mathfrak{p}_0}$. By Lemma 2, E has multiplicative reduction at all primes of K over $\mathfrak{p}_0$, so the support of $D_{\mathfrak{p}_0}$ is contained in $\mathcal{C}$. Let Z be the support of $(\pi_* D)_{\mathfrak{p}_0}$; then the definition of $\mathcal{C}'$ implies that Z is contained in $\mathcal{C}'$. We can write $(\pi_* D)_{\mathfrak{p}_0}$ as a linear combination $\sum_{z \in Z} n_z z$, where the n_z are positive integers.

Let z be a point of Z. Since $(\mathcal{X}, \mathcal{X}', \pi)$ is a nice $(L, \mathfrak{p}_0)$-quotient, there is a unique irreducible component C_z of $\mathcal{C}'$ containing z, and the coordinate ring of C_z is the integral closure of $\mathcal{O}_{L,\mathfrak{p}_0}$ in the function field $L(C_z)$ of C_z. Hence $k(z)$ can be identified with the residue field $k(\mathfrak{q}_z)$ of some prime $\mathfrak{q}_z$ of $L(C_z)$ over $\mathfrak{p}_0$; in particular, $[k(\mathfrak{q}_z) : k(\mathfrak{p}_0)]$ equals $[k(z) : k(\mathfrak{p}_0)]$. On the other hand, $k(z)$ can also be identified with a subfield of the residue field $k(\mathfrak{p}_z)$ of some prime $\mathfrak{p}_z$ of K over $\mathfrak{p}_0$, so $[k(z) : k(\mathfrak{p}_0)]$ divides $[k(\mathfrak{p}_z) : k(\mathfrak{p}_0)]$. This implies that $[k(\mathfrak{q}_z) : k(\mathfrak{p}_0)] = [k(z) : k(\mathfrak{p}_0)]$ is in $S_{K,\mathfrak{p}_0}$. By assumption vi), $\mathfrak{q}_z$ is the only prime of $L(C_z)$ over $\mathfrak{p}_0$. This implies that the schematic intersection of C_z with $\mathcal{X}'_{\mathfrak{p}_0}$ equals $e_z z$, where $e_z = e(\mathfrak{q}_z/\mathfrak{p}_0)$. We note that e_z divides h.

We consider the effective divisor D' on $\mathcal{X}'$ defined by

$$D' = \sum_z \frac{n_z h}{e_z} C_z.$$

By the above description of the intersections of D and the C_z with $\mathcal{X}'_{\mathfrak{p}_0}$, the divisor $h\pi_* D - D'$ on $\mathcal{X}'$ specializes to the zero divisor on $\mathcal{X}'_{\mathfrak{p}_0}$. This implies that the class of $h\pi_* D - D'$ in $P(k(\mathfrak{p}_0))$ is zero. By the commutativity of the above diagram and the injectivity of the bottom map, the class of $h\pi_* D - D'$ in $J'(L)$ is also zero. By assumption i), we conclude that the divisors $h\pi_* D$ and D' are equal. The generic fibre of D is supported outside $\mathcal{C}$; since $(\mathcal{X}, \mathcal{X}', \pi)$ is a nice $(L, \mathfrak{p}_0)$-quotient, the

generic fibre of $\pi_* D$ is supported outside $\mathcal{C}'$. On the other hand, the generic fibre of D' is supported on $\mathcal{C}'$, a contradiction. □

The following corollary of Theorem 1 is useful for eliminating groups from $\Phi(d)$.

Corollary 3. *Let A be a group of the form $C_m \oplus C_n$ with $m \mid n$, let $d \geq 1$ be an integer, and let L be a subfield of $\mathbb{Q}(\zeta_m)$. Let $\mathfrak{p}_0$ be a prime of L, let p be the residue characteristic of $\mathfrak{p}_0$, and let $q = \mathrm{Nm}(\mathfrak{p}_0)$. Let*

$$S_{\mathfrak{p}_0} = \left\{ \delta \geq 1 \;\middle|\; \begin{array}{l} K \text{ is an extension of } \mathbb{Q}(\zeta_m) \text{ with } [K:L] = d, \\ \mathfrak{p} \text{ is a prime of } K \text{ over } \mathfrak{p}_0, \text{ and } \delta \text{ divides } [k(\mathfrak{p}) : k(\mathfrak{p}_0)] \end{array} \right\}.$$

Let

$$A' = \begin{cases} A & \text{if } p > d+1 \\ \text{maximal } p\text{-divisible subgroup of } A & \text{if } p \leq d+1. \end{cases}$$

Let $(\mathcal{X}, \mathcal{X}', \pi)$ be a nice $(L, \mathfrak{p}_0)$-quotient of $X_1(m,n)$. Let $X' = \mathcal{X}'_L$, and let J' be the Jacobian of X'. Let h be the least common multiple of the ramification indices $e(\mathfrak{q}/\mathfrak{p}_0)$ where $L(C)$ is the function field of an irreducible component C of $\mathcal{C}'$ and $\mathfrak{q}$ is a prime of $L(C)$ over $\mathfrak{p}_0$. Assume that the following conditions are satisfied:

i) *The gonality of X' over L is at least $dh+1$.*
ii) *The group $J'(L)$ has rank 0.*
iii) *If $p = 2$, then the 2-torsion subgroup of $J'(L)$ is trivial.*
iv) *For all $i \in S_{\mathfrak{p}_0}$, there does not exist an elliptic curve over a field of q^i elements with a subgroup isomorphic to A'.*
v) *Neither $3q^d$ nor $4q^d$ is divisible by $\#A'$.*
vi) *For all irreducible components C of $\mathcal{C}'$, if the function field $L(C)$ has a prime $\mathfrak{q}$ over $\mathfrak{p}_0$ such that $[k(\mathfrak{q}) : k(\mathfrak{p}_0)]$ is in $S_{\mathfrak{p}_0}$, then $\mathfrak{q}$ is the* unique *prime of $L(C)$ over $\mathfrak{p}_0$.*

Then there does not exist an elliptic curve over an extension of degree d of L with a subgroup isomorphic to A.

Proof. Under the conditions of the corollary, the conditions of Theorem 1 are satisfied for every extension K of degree d over L such that $L \subseteq \mathbb{Q}(\zeta_m) \subseteq K$. □

We end this section with some remarks on checking the conditions of Theorem 1 and Corollary 3. The conditions are straightforward to check in practice, apart from condition ii) if $L \neq \mathbb{Q}$. An easy way to make sure that condition vi) holds is to choose $\mathfrak{p}_0$ totally inert in $\mathbb{Q}(\zeta_n)$.

An important special case occurs when L equals $\mathbb{Q}(\zeta_m)$, the prime $\mathfrak{p}_0$ does not divide n, the curve X' equals X and π is the identity on X. In this case the conditions simplify as follows: (X, X', π) automatically extends to a nice $(L, \mathfrak{p}_0)$-quotient, and we have $A' = A$ and $h = 1$. Moreover, the following remarks are useful to check condition vi) in these cases.

Let r be a divisor of n. The cusps of $X_1(m,n)$ represented by points $(a : b) \in \mathbb{P}^1(\mathbb{Q})$, where a, b are coprime integers with $\gcd(b,n) = r$, all have the same field of definition, which we denote by $F_{m,n,r}$. By generalities on cusps and by the existence of the Weil pairing, we have $\mathbb{Q}(\zeta_m) \subseteq F_{m,n,r} \subseteq \mathbb{Q}(\zeta_n)$. Explicitly, the field $F_{m,n,r}$ can be described as follows. We consider the subgroups $H^0_{m,n,r} \subseteq H_{m,n,r} \subseteq G_{m,n} \subseteq$

$(\mathbb{Z}/n\mathbb{Z})^\times$ defined by

$$\begin{aligned} G_{m,n} &= \{s \in (\mathbb{Z}/n\mathbb{Z})^\times \mid s \equiv 1 \pmod{m}\}, \\ H^0_{m,n,r} &= \{s \in (\mathbb{Z}/n\mathbb{Z})^\times \mid s \equiv 1 \pmod{\operatorname{lcm}(m, n/r)}\}, \\ H_{m,n,r} &= \begin{cases} H^0_{m,n,r} & \text{if } \gcd(mr, n) > 2, \\ H^0_{m,n,r} \cdot \{\pm 1\} & \text{if } \gcd(mr, n) \leq 2. \end{cases} \end{aligned}$$

(Note that in the latter case m is 1 or 2, so -1 is in $G_{m,n}$.) Using the canonical identification of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ with $(\mathbb{Z}/n\mathbb{Z})^\times$, the field $F_{m,n,r}$ is then the field of invariants of $H_{m,n,r}$ acting on $\mathbb{Q}(\zeta_n)$.

The set $\{L(C) : C \text{ is a cusp of } X_1(m,n)\}$ is now equal to $\{F_{m,n,r} : r|n\}$ and condition vi) can now be checked by computing the defining polynomials for $F_{m,n,r}$ over L and factoring them modulo $\mathfrak{p}_0$.

In the case $m = 1$, we have

$$F_{1,n,r} = \begin{cases} \mathbb{Q}(\zeta_{n/r}) & \text{if } r > 2, \\ \mathbb{Q}(\zeta_{n/r})^+ & \text{if } r \leq 2. \end{cases}$$

3. Torsion groups of elliptic curves over $\mathbb{Q}(\zeta_{13} + \zeta_{13}^5 + \zeta_{13}^8 + \zeta_{13}^{12})$

In this section, we consider the cyclic cubic field

$$K = \mathbb{Q}(\zeta_{13} + \zeta_{13}^5 + \zeta_{13}^8 + \zeta_{13}^{12})$$

of discriminant 13^2. This field can be written as $K = \mathbb{Q}(\omega)$ where ω has minimal polynomial $x^3 + x^2 - 4x + 1$.

Theorem 4. *For every elliptic curve E over K, the torsion group $E(K)_{\mathrm{tors}}$ is one of the groups from Mazur's torsion theorem.*

Proof. By results of Parent [31, 32], we know that no prime $p > 13$ divides the torsion order of an elliptic curve over a cubic field. It therefore remains to prove that $E(K)$ does not contain any of the following groups:

$$\begin{aligned} &C_n && \text{where } n = 11, 13, 14, 15, 16, 18, 20, 21, 24, 25, 27, 35, 49, \\ &C_2 \oplus C_{2m} && \text{where } m = 5, 6. \end{aligned}$$

For later use, we note that 3 is totally inert, 5 is totally split and 13 is totally ramified in K. Let $\mathfrak{p}_5$ be one of the primes above 5, and let $\mathfrak{p}_{13}$ be the unique prime above 13.

3.1. **The cases C_{11}, C_{14} and C_{15}.** In these cases, the modular curve $X_1(n)$ is an elliptic curve, and an easy computation in Magma shows that $X_1(n)(K) = X_1(n)(\mathbb{Q})$. It is well known that $X_1(n)(\mathbb{Q})$ contains only cusps (see for example [23]), hence $Y_1(n)(K) = \emptyset$.

3.2. **The cases C_{20}, C_{24}, $C_2 \oplus C_{10}$ and $C_2 \oplus C_{12}$.** Recall that $X_0(20)$ and $X_0(24)$ are elliptic curves. A computation in Magma shows that $X_0(20)(K) = X_0(20)(\mathbb{Q})$ and $X_0(24)(K) = X_0(24)(\mathbb{Q})$, and it is known that $X_0(20)(\mathbb{Q})$ and $X_0(24)(\mathbb{Q})$ consist purely of cusps (see for example [24]). As an elliptic curve with a point of order n admits a cyclic isogeny of degree n, it follows that $Y_1(20)(K) = \mathrm{Y}_1(24)(K) = \emptyset$. Similarly, an elliptic curve with torsion $C_2 \oplus C_{2m}$ over K is 2-isogenous to a curve with a cyclic $2m$-isogeny, and hence it follows that $Y_1(2,10)(K) = \mathrm{Y}_1(2,12)(K) = \emptyset$.

3.3. **The cases C_{13}, C_{16} and C_{18}.** The modular curves $X_1(n)$ are all hyperelliptic curves of genus 2. Magma computations show that $\operatorname{rk} J_1(13)(k) = \operatorname{rk} J_1(16)(K) = \operatorname{rk} J_1(18)(K) = 0$.

We compute $J_1(13)(\mathbb{F}_5) \simeq C_{19}$, and as $J_1(13)(K) \rightarrowtail J_1(k(\mathfrak{p}_5)) = J_1(\mathbb{F}_5)$ and $J_1(\mathbb{Q}) \simeq C_{19}$, it follows that $J_1(13)(K) = J_1(13)(\mathbb{Q}) \simeq C_{19}$. It follows that $Y_1(13)(K) = \emptyset$. A similar argument deals with the case $n = 18$.

For $n = 16$, it is not enough to use just one prime. We compute $\#J_1(16)(\mathbb{F}_5) = 40$, $\#J_1(16)(\mathbb{F}_{27}) = 1220$ and $J_1(16)(\mathbb{Q}) \simeq C_2 \oplus C_{10}$. Since $\gcd(40, 1220) = 20$, it follows that $J_1(16)(K) = J_1(16)(\mathbb{Q})$. We conclude that $Y_1(16)(K) = \emptyset$.

3.4. **The cases C_n for $n = 21, 25, 27, 35, 49$.** We apply Theorem 1 using $L = \mathbb{Q}$, $\mathfrak{p}_0 = (5)$ for $n = 21, 27, 49$ and $\mathfrak{p}_0 = (13)$ for $n = 25, 35$, $X' = X$ and $\pi = \mathrm{id}$. Conditions i), ii) and iii) are satisfied since in all cases $X_1(n)$ is of gonality ≥ 4 [11] and $\operatorname{rk} J_1(n)(\mathbb{Q}) = 0$. Condition iv) holds because of the Hasse bound over $\mathbb{F}_5$ and $\mathbb{F}_{13}$. Condition v) clearly holds. For $n \in \{27, 35, 49\}$, condition vi) holds because $\mathfrak{p}_0$ is totally inert in $\mathbb{Q}(\zeta_n)$. For $n = 21$, condition vi) holds because $S_{K,(5)} = \{1\}$ and there are no primes of degree 1 above 5 in $\mathbb{Q}(\zeta_3)$, $\mathbb{Q}(\zeta_7)$ and $\mathbb{Q}(\zeta_{21})^+$. Finally, for $n = 35$, condition vi) holds because $S_{K,(13)} = \{1\}$ and there are no primes of degree 1 above 13 in $\mathbb{Q}(\zeta_5)$, $\mathbb{Q}(\zeta_7)$ and $\mathbb{Q}(\zeta_{35})^+$.

Theorem 4 follows by combining the above cases. □

4. Torsion groups of elliptic curves over $\mathbb{Q}(\zeta_5)$

In this section, we will determine $\Phi(K)$, where K is the field $\mathbb{Q}(\zeta_5)$. We will use the (as of yet unpublished) result that the largest prime dividing the order of a point over a quartic field is 17 [6], and the fact that there is no 17-torsion over cyclic quartic extensions of $\mathbb{Q}$ [5].

Theorem 5. *Let $K = \mathbb{Q}(\zeta_5)$. Then for every elliptic curve E over K, the torsion group $E(K)_{\mathrm{tors}}$ is one of the following groups:*

$$\begin{array}{ll} C_n & \text{where } n = 1, \ldots, 10, 12, 15, 16, \\ C_2 \oplus C_{2m} & \text{where } m = 1, \ldots, 4, \\ C_5 \oplus C_5. & \end{array} \tag{3}$$

There exist infinitely many elliptic curves with each of the torsion groups from the list (3)*, except for C_{15} and C_{16}.*

Proof. As mentioned at the beginning of this section, we need only consider primes $p \leq 13$ as possible divisors of the order of a torsion point.

Before proceeding further, we find all elliptic curves over K containing a point of order 15 and show that the torsion subgroup of these curves is exactly C_{15}. Recall that $X_1(15)$ is isomorphic to the elliptic curve with Cremona label 15a8. We compute that the group of K-points of this elliptic curve is isomorphic to C_{16}. Of the 16 points, 8 are cusps, and we compute that the remaining 8 points correspond to elliptic curves over K with torsion subgroup C_{15}. In particular, there exist no curves with torsion C_{15n} for any integer $n > 1$ and no curves with torsion $C_5 \oplus C_{15}$.

There exist elliptic curves with points of order 16 over K; one such example is the elliptic curve

$$y^2 + (6\zeta_5^3 + \zeta_5^2 + 3\zeta_5 + 6)xy + (-10\zeta_5^3 - 2\zeta_5^2 - 5\zeta_5 - 8)y = x^3 + (-10\zeta_5^3 - 2\zeta_5^2 - 5\zeta_5 - 8)x^2,$$

on which $(0,0)$ is a point of order 16. Since $X_1(16)$ has genus 2, the set $X_1(16)(K)$ is finite by Faltings's theorem.

It remains to prove that $E(K)$ does not have a subgroup isomorphic to one of the following groups:

$$\begin{aligned} &C_n && \text{where } n = 11, 13, 14, 17, 18, 20, 21, 24, 25, 27, 32, 35, 49, \\ &C_2 \oplus C_{2m} && \text{where } m = 5, 6, 8, \\ &C_5 \oplus C_{10}. \end{aligned}$$

4.1. **The cases C_n for $n = 11$, 14, 20, 49 and $C_2 \oplus C_{2m}$ for $m = 5$, 6.** These cases are dealt with by simply computing $X_1(n)(K) = X_1(n)(\mathbb{Q})$, for $n = 11$, 14, $X_0(20)(K) = X_0(20)(\mathbb{Q})$ for C_{20} and $C_2 \oplus C_{10}$, $X_0(24)(K) = X_0(24)(\mathbb{Q})$ for C_{24} and $C_2 \oplus C_{12}$ as in the proof of Theorem 4. Similarly, noting that $X_0(49)$ is an elliptic curve, we compute $X_0(49)(K) = X_0(49)(\mathbb{Q})$, which consists only of cusps.

4.2. **The case C_{21}.** The curve $X_0(21)$ is an elliptic curve and we compute that $X_0(21)(K) = X_0(21)(\mathbb{Q})$. However, the difference between this case and the previous ones is that $Y_0(21)(K)$ is not empty and hence one needs also to check that the elliptic curves with 21-isogenies do not have any K-rational points over K. This can be done by using division polynomials; see [28, 29] for details.

4.3. **The cases C_{13} and C_{18}.** These cases are dealt with exactly as in the proof of Theorem 4.

4.4. **The cases C_{27}, C_{32} and $C_2 \oplus C_{16}$.** We apply Theorem 1 with $L = \mathbb{Q}$, $\mathfrak{p}_0 = (11)$ (which is totally split in K), $X' = X$ and $\pi = \mathrm{id}$. The curves $X_1(27)$, $X_1(32)$ and $X_1(2,16)$ all have gonality ≥ 5 by [12, Theorem 2.6] (see also [7]), and their Jacobians all have rank 0. This implies conditions i), ii) and iii). Condition iv) follows from the Hasse bound over $\mathbb{F}_{11}$, and condition v) clearly holds. Finally, condition vi) holds in the case C_{27} because 11 is totally inert in $\mathbb{Q}(\zeta_{27})$, and in the cases C_{32} and $C_2 \oplus C_{16}$ because $S_{K,11} = \{1\}$ and there are no primes of degree 1 above 11 in the fields $\mathbb{Q}(\zeta_4)$, $\mathbb{Q}(\zeta_8)$, $\mathbb{Q}(\zeta_{16})^+$ and $\mathbb{Q}(\zeta_{32})^+$.

4.5. **The case C_{25}.** We apply Theorem 1 with $L = \mathbb{Q}$, $\mathfrak{p}_0 = (2)$ (which is totally inert in K), $X' = X$ and $\pi = \mathrm{id}$. The modular curve $X_1(25)$ has gonality at least 5 [12, Theorem 2.6], and $J_1(25)(\mathbb{Q})$ has rank 0 [21] and trivial 2-torsion; this implies conditions i), ii) and iii). Although 25 is in the Hasse interval of $\mathbb{F}_{16}$, a search among all elliptic curves over $\mathbb{F}_{16}$ shows that all such curves E with 25 points satisfy $E(\mathbb{F}_{16}) \simeq C_5 \oplus C_5$. This shows that condition iv) holds. Condition v) clearly holds. Finally, condition vi) is satisfied because 2 is totally inert in $\mathbb{Q}(\zeta_{25})$.

4.6. **The case C_{35}.** We apply Theorem 1 with $L = \mathbb{Q}$, $\mathfrak{p}_0 = (3)$ (which is totally inert in K), $X' = X$ and $\pi = \mathrm{id}$. The curve $X_1(35)$ has gonality at least 5 [12, Theorem 2.6], and $J_1(35)(\mathbb{Q})$ has rank 0; this shows that conditions i) and ii) hold. One easily checks conditions iii) and v). By [35, Theorem 4.1], there are no elliptic curves with order a multiple of 35 over $k(\mathfrak{p}) = \mathbb{F}_{81}$; this implies condition iv). The prime 3 is totally inert in $\mathbb{Q}(\zeta_5)$, $\mathbb{Q}(\zeta_7)$ and $\mathbb{Q}(\zeta_{35})^+$, which implies condition vi).

4.7. **The case $C_5 \oplus C_{10}$.** We apply Theorem 1 with $L = \mathbb{Q}(\zeta_5)$, $\mathfrak{p}_0$ one of the primes above 11 (which is totally split in L), $X' = \mathrm{X}_0(50)_L$ and π the map defined by the inclusion $\alpha^{-1}\Gamma_1(5,10)\alpha \subset \Gamma_0(50)$, where $\alpha = \left(\begin{smallmatrix} 5 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. The gonality of X' is 2, and we compute in Magma that $J_0(50)(K)$ has rank 0; this implies conditions i) and ii). One easily checks conditions iii) and v). Condition iv) follows from the Hasse bound over $k(\mathfrak{p}_0) = \mathbb{F}_{11}$. Finally, condition vi) follows from the fact that all cusps of X' are defined over L.

Theorem 5 follows by combining the above cases. □

5. Results for all cubic fields

We now apply the results of Section 2 to prove that certain groups are not in $\Phi(3)$. We note that the cases C_{40}, C_{49} and C_{55} (and more) were also proved independently by Wang [34].

Theorem 6. *The groups $C_2 \oplus C_{20}$, C_{40}, C_{49} and C_{55} do not occur as subgroups of elliptic curves over cubic fields.*

Proof. To prove the cases $C_2 \oplus C_{20}$, C_{49} and C_{55}, we apply Corollary 3 with $L = \mathbb{Q}$, $\mathfrak{p}_0 = (3)$, $X' = X$ and $\pi = \mathrm{id}$. We have $S_{\mathfrak{p}_0} = \{1, 2, 3\}$. Conditions i) and ii) hold because $X_1(2,20)$, $X_1(49)$ and $X_1(55)$ have gonality at least 4 and their Jacobians have rank 0 over $\mathbb{Q}$. Condition iv) holds because 40, 49 and 55 are all outside the Hasse intervals of $\mathbb{F}_3$, $\mathbb{F}_9$ and $\mathbb{F}_{27}$. Condition iii) and v) clearly hold. Condition vi) follows from the fact that there are no primes of degree 1, 2 or 3 above 3 in the fields $\mathbb{Q}(\zeta_n)$ for $n \in \{5, 7, 11\}$ and $\mathbb{Q}(\zeta_n)^+$ for $n \in \{20, 49, 55\}$. Finally, the case C_{40} follows from the case $C_2 \oplus C_{20}$ in view of the covering $X_1(40) \to X_1(2,20)$. □

6. Results for quartic fields

In this section, we show that certain groups of the form $C_m \oplus C_n$, with $m \mid n$ and $m \geq 3$, are not in $\Phi(4)$. Recall that an elliptic curve E with a subgroup isomorphic to $C_m \oplus C_n$ has to be defined over a field containing $\mathbb{Q}(\zeta_m)$.

Theorem 7. *The following groups do not occur as subgroups of elliptic curves over quartic fields:*

$$C_3 \oplus C_{12}, \quad C_3 \oplus C_{18}, \quad C_3 \oplus C_{27}, \quad C_3 \oplus C_{33}, \quad C_3 \oplus C_{39}, \quad C_4 \oplus C_{12},$$
$$C_4 \oplus C_{16}, \quad C_4 \oplus C_{28}, \quad C_4 \oplus C_{44}, \quad C_4 \oplus C_{52}, \quad C_4 \oplus C_{68}, \quad C_8 \oplus C_8 \ .$$

Proof. We consider each of the above cases separately.

6.1. **The case $C_3 \oplus C_{12}$.** The curve $X = X_1(3,12)$ has genus 3 and is non-hyperelliptic [8]. We apply Corollary 3 with $L = \mathbb{Q}(\zeta_3)$, $\mathfrak{p}_0$ one of the primes of norm 7 in L, $X' = X$ and $\pi = \mathrm{id}$. We compute that the Jacobian of X has rank 0 over $\mathbb{Q}(\zeta_3)$ (see [9, proof of Lemma 4.4] for details). This shows that conditions i), ii) and iii) are satisfied. For all elliptic curves over fields of 49 elements with 36 points, the group of points is isomorphic to $C_6 \oplus C_6$, proving iv). Condition v) clearly holds. Finally, condition vi) holds because $\mathfrak{p}_0$ is inert in $\mathbb{Q}(\zeta_{12})$.

6.2. **The case $C_3 \oplus C_{18}$.** The curve $X = X_1(3,18)$ has genus 10, and its gonality over $\mathbb{C}$ is at least 4 by the results of [1] and [20, Appendix 2] (see also [12, Theorem 1.2]). We use Corollary 3, choosing $L = \mathbb{Q}(\zeta_3)$, $\mathfrak{p}_0 = (2)$, $X' = X$ and $\pi = \mathrm{id}$. The Jacobian $J = J_1(3,18)$ over $\mathbb{Q}(\zeta_3)$ decomposes up to isogeny as

$$J \sim \bigoplus_{i=1}^{7} B_i,$$

where B_i is an elliptic curve for $1 \leq i \leq 4$ and B_i is an Abelian surface for $5 \leq i \leq 7$. A number of 2-descent and L-series computations in Magma shows that the rank of all these B_i is 0. This shows that condition ii) is satisfied. If $\mathfrak{q}$ is one of the primes of norm 7 in L, then $J(k(\mathfrak{q}))$ has order $3^{14} \cdot 7^3$. This implies that the 2-torsion of $J(L)$ is trivial, so condition iii) holds. The Hasse bound implies condition iv). Condition v) clearly holds, and condition vi) holds because 2 is totally inert in $\mathbb{Q}(\zeta_{18}) = \mathbb{Q}(\zeta_9)$.

6.3. **The case $C_3 \oplus C_{27}$.** We use Corollary 3, taking $L = \mathbb{Q}$, $\mathfrak{p}_0 = (2)$, $X' = X_1(27)$ and $\pi\colon X \to X'$ the canonical map. Condition i) holds because X' has gonality 6 by [7]. A computation using L-functions shows that $\operatorname{rk} J'(\mathbb{Q}) = 0$, which implies condition ii). Condition iii) follows from $\#J'(\mathbb{F}_7) = 242518973481$. Condition iv) and v) clearly hold. Condition vi) holds since 2 is inert in $\mathbb{Q}(\zeta_{27})$.

6.4. **The cases $C_3 \oplus C_{33}$ and $C_3 \oplus C_{39}$.** These cases require a slightly different approach, following the lines of [14]. Let K be a quadratic extension of $\mathbb{Q}(\zeta_3)$, let σ be the non-trivial element of $\mathrm{Gal}(K/\mathbb{Q}(\zeta_3))$, and let $\mathfrak{p}$ be a prime of K above 7.

We first decribe the case $C_3 \oplus C_{33}$. We take the hyperelliptic curve $X' = X_0(33)$ of genus 3, with hyperelliptic involution w_{11}. Suppose that y is a non-cuspidal point on $X_1(3,33)$. By Lemma 2, y maps to the cusp at ∞ mod $\mathfrak{p}$, and y^σ maps to ∞ mod $\mathfrak{p}$. The points y and y^σ on $X_1(3,33)$ map to x and x^σ on X', which likewise map to ∞ mod $\mathfrak{p}$. Consider the map

$$\begin{aligned} f\colon X' &\to J' \\ t &\mapsto [t + t^\sigma - 2\infty]. \end{aligned}$$

Then $f(x)$ is $\mathbb{Q}(\zeta_3)$-rational, and $f(x)$ mod $\mathfrak{p}$ is 0. We compute that $J'(\mathbb{Q}(\zeta_3))$ is finite. Since reduction modulo $\mathfrak{p}$ is injective on the torsion, it follows that $f(x) = 0$ over $\mathbb{Q}(\zeta_3)$, so there is a function g whose divisor is $x + x^\sigma - 2\infty$. Since g has degree 2, it is fixed by the hyperelliptic involution. It follows that ∞ is fixed by the hyperelliptic involution. But w_{11} acts freely on the cusps of X', leading to a contradiction.

We now deal with the case $C_3 \oplus C_{39}$. We take

$$X' = X_0(39)/w_{13}\colon y^2 = x^6 - 20x^4 - 6x^3 + 64x^2 - 48x + 9.$$

The curve X' is hyperelliptic of genus 2, and the hyperelliptic involution on X' is induced by w_3. We compute that $J'(\mathbb{Q}(\zeta_3))$ is finite. Using the same arguments as above, we conclude that w_3 fixes the cusp at ∞ of X', but w_3 acts by switching the two cusps 0 and ∞, which leads to a contradiction.

6.5. **The case $C_4 \oplus C_{12}$.** We apply Corollary 3 with $L = \mathbb{Q}(i)$, $\mathfrak{p}_0 = (2+i)$, $X' = X = X_1(4,12)$ and $\pi = \mathrm{id}$. The curve X has genus 5 and is non-hyperelliptic [8]. It is the base change of the curve $X_{\Delta'}(48)$ over $\mathbb{Q}$, where Δ' is the subgroup $\{\pm 1, \pm 13, \pm 25, \pm 37\}$ of $(\mathbb{Z}/48\mathbb{Z})^\times$. By [9, pages 464–465], the Jacobian $J_{\Delta'}$ of $X_{\Delta'}$ decomposes over $\mathbb{Q}$ as

$$J_{\Delta'} \sim B_1^2 \oplus B_2 \oplus B_3,$$

where

$$B_1 \colon y^2 = x^3 - x^2 - 4x + 4,$$
$$B_2 \colon y^2 = x^3 + x^2 - 4x - 4$$

and B_3 is the Jacobian of the curve

$$C_3 \colon y^2 = x^5 - 10x^3 + 9x.$$

Note that B_2 is a -1-twist of B_1, and hence B_1 and B_2 are isomorphic over $\mathbb{Q}(i)$. A computation in Magma shows that

$$\operatorname{rk} B_1(\mathbb{Q}(i)) = \operatorname{rk} B_2(\mathbb{Q}(i)) = \operatorname{rk} B_3(\mathbb{Q}(i)) = 0,$$

so condition ii) is satisfied. Condition iii) holds trivially. The Hasse bound implies condition iv). Condition v) is clearly satisfied. Finally, condition vi) holds because $\mathfrak{p}_0$ is totally inert in $\mathbb{Q}(\zeta_{12})$.

6.6. **The case $C_4 \oplus C_{16}$.** We take the genus 5 curve $X' = X_1(2,16)$ of gonality 4 [12, Theorem 2.8.], $L = \mathbb{Q}(i)$ and $\mathfrak{p}_0 = (2+i)\mathbb{Z}[i]$. The Jacobian J' of X' factors over $\mathbb{Q}$ as

$$J' \sim E_1 \oplus J_1(16)^2,$$

where E_1 is the elliptic curve over $\mathbb{Q}$ with Cremona label 32a1. A computation using 2-descent shows that $\operatorname{rk} J'(\mathbb{Q}(i)) = 0$ and $\mathfrak{p}_0$ is inert in $\mathbb{Q}(\zeta_{16})$. As all the assumptions of Corollary 3 are satisfied, the result follows.

6.7. **The case $C_4 \oplus C_{28}$.** We take $X' = X_1(28)$ of gonality 6 [7], $L = \mathbb{Q}$ and $\mathfrak{p}_0 = (3)$. We compute $\operatorname{rk} J'(\mathbb{Q}) = 0$, showing that condition ii) holds. Condition vi) is satisfied because $S_{K,\mathfrak{p}_0} = \{1,2,4\}$, while 3 is inert in $\mathbb{Q}(i)$ and none of the fields $\mathbb{Q}(\zeta_7)$, $\mathbb{Q}(\zeta_{14})^+$ and $\mathbb{Q}(\zeta_{28})^+$ have any primes of degree 1, 2 or 4 above 3.

6.8. **The case $C_4 \oplus C_{44}$.** We take $X' = X_1(44)$ of gonality ≥ 7 [1], $L = \mathbb{Q}$ and $\mathfrak{p}_0 = (3)$. Condition vi) is satisfied because $S_{K,\mathfrak{p}_0} = \{1,2,4\}$, while 3 is inert in $\mathbb{Q}(i)$ and none of the fields $\mathbb{Q}(\zeta_{11})$, $\mathbb{Q}(\zeta_{22})^+$ and $\mathbb{Q}(\zeta_{44})^+$ have any primes of degree 1, 2 or 4 above 3. After computing $\operatorname{rk} J'(\mathbb{Q}) = 0$, we are done.

6.9. **The case $C_4 \oplus C_{52}$.** We take $X' = X_1(26)$ of gonality 6 [7], $L = \mathbb{Q}$ and $\mathfrak{p}_0 = (3)$. We check that 3 splits into 4 primes of degree 3 in $\mathbb{Q}(\zeta_{13})$, all of which remain inert in $\mathbb{Q}(\zeta_{52})$. As (3) is inert in $\mathbb{Q}(i)$, the primes of any quartic field containing $\mathbb{Q}(i)$ above it are of degree 2 or 4, this proves vi). We compute $\operatorname{rk} J'(\mathbb{Q}) = 0$ and $\#J'(\mathbb{F}_5) = 3^2 5^2 7^3 19^2$, proving that all the assumptions are satisfied.

6.10. **The case $C_4 \oplus C_{68}$.** We use Corollary 3, taking $X' = X_1(34)$ of gonality 10 [7], $L = \mathbb{Q}$ and $\mathfrak{p}_0 = (3)$. Since 3 splits into 2 primes of degree 16 over $\mathbb{Q}(\zeta_{68})$ and is inert in $\mathbb{Q}(\zeta_{17})$ and $\mathbb{Q}(i)$, it easily follows that condition vi) is satisfied. We compute $\operatorname{rk} J'(\mathbb{Q}) = 0$, completing the proof.

6.11. **The case $C_8 \oplus C_8$.** The only field over which there could exist an elliptic curve with full 8-torsion is $\mathbb{Q}(\zeta_8) = \mathbb{Q}(i, \sqrt{2})$. To show that such curves do not exist, we will in fact prove the stronger statement that there does not exist an elliptic curve over $\mathbb{Q}(\zeta_8)$ with a subgroup isomorphic to $C_4 \oplus C_8$. To prove this, we note that the modular curve $X_1(4,8)$ is isomorphic (over $\mathbb{Q}(i)$) to the elliptic curve with Cremona label 32a2 [27, Lemma 13]. We compute

$$X_1(4,8)(\mathbb{Q}(\zeta_8)) \simeq C_4 \oplus C_4,$$

and all the points are cusps, which proves our claim.

This finishes the proof of Theorem 7. □

Acknowledgments. We would like to thank Maarten Derickx for useful discussions on the topic of this paper.

References

[1] D. Abramovich, *A linear lower bound on the gonality of modular curves*, Int. Math. Res. Notices **20** (1996), 1005–1011.
[2] S. Bosch, W. Lütkebohmert and M. Raynaud, Néron Models. Springer-Verlag, Berlin/Heidelberg, 1990.
[3] J. G. Bosman, P. J. Bruin, A. Dujella and F. Najman, *Ranks of elliptic curves with prescribed torsion over number fields*, Int. Math. Res. Notices **2014** (2014), 2885–2923.
[4] M. Derickx, *Torsion points on elliptic curves and gonalities of modular curves*, master's thesis, Universiteit Leiden, 2012, `http://www.math.leidenuniv.nl/nl/theses/324/`
[5] M. Derickx, S. Kamienny and B. Mazur, *Rational families of 17-torsion points of elliptic curves over number fields*, preprint, `http://www.math.harvard.edu/~mazur/papers/For.Momose20.pdf`
[6] M. Derickx, S. Kamienny, W. A. Stein and M. Stoll, *Torsion points on elliptic curves over fields of small degree*, preprint.
[7] M. Derickx and M. van Hoeij, *Gonality of the modular curve $X_1(N)$*, J. Algebra **417** (2014), 52–71.
[8] N. Ishii and F. Momose, *Hyperelliptic modular curves*, Tsukuba J. Math. **15** (1991), 413–423.
[9] D. Jeon and C. H. Kim, *Bielliptic modular curves $X_1(m,n)$*, manuscripta math. **118** (2005), 455–466.
[10] D. Jeon and C. H. Kim, *On the arithmetic of certain modular curves*, Acta Arith. **130** (2007), 181–193.
[11] D. Jeon, C. H. Kim and A. Schweizer, *On the torsion of elliptic curves over cubic number fields*, Acta Arith. **113** (2004) 291–301.
[12] 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.
[13] S. Kamienny, *Torsion points on elliptic curves over all quadratic fields*, Duke Math J. **53** (1986), 157–162.
[14] S. Kamienny, *Torsion points on elliptic curves over all quadratic fields. II.*, Bull. Soc. Math. France **114** (1986), 119–122.
[15] S. Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms*, Invent. Math. **109** (1992), 221–229.
[16] S. Kamienny and F. Najman, *Torsion groups of elliptic curves over quadratic fields*, Acta. Arith. **152** (2012), 291–305.
[17] K. Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, Cohomologies p-adiques et applications arithmétiques. III. Astrisque **295** (2004), 117–290.
[18] N. M. Katz, *Galois properties of torsion points on abelian varieties*, Invent. Math. **62** (1981), 481–502.
[19] M. A. Kenku and F. Momose, *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. **109** (1988), 125–149.

[20] H. H. Kim, *Functoriality for the exterior square of* GL_4 *and the symmetric fourth of* GL_2, J. Amer. Math. Soc. **16** (2003), 139–184, With appendix 1 by D. Ramakrishnan and appendix 2 by H. H. Kim and P. Sarnak.
[21] D. S. Kubert, *Universal bounds on the torsion of elliptic curves*, Proc. London Math. Soc. **33** (1976), 193–237.
[22] W. Bosma, J. J. Cannon, C. Fieker, A. Steel (eds.), Handbook of Magma functions, Edition 2.19 (2013).
[23] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. **47** (1978), 33–186.
[24] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), 129–162.
[25] B. Mazur and J. Tate, *Points of order 13 on elliptic curves*, Invent. Math. **22** (1973), 41–49.
[26] F. Najman, *Complete classification of torsion of elliptic curves over quadratic cyclotomic fields*, J. Number Theory **130** (2010), 1964–1968.
[27] F. Najman, *Exceptional elliptic curves over quartic fields*, Int. J. Number Theory **8** (2012), 1231–1246
[28] F. Najman, *Torsion of elliptic curves over cubic fields*, J. Number Theory, **132** (2012), 26–36.
[29] F. Najman, *Torsion of rational elliptic curves over cubic fields and sporadic points on* $X_1(n)$, Math. Res. Letters, to appear.
[30] A. P. Ogg, *Hyperelliptic Modular Curves*, Bull. Soc. Math. France, **102** (1974), 449–462.
[31] P. Parent, *Torsion des courbes elliptiques sur les corps cubiques*, Ann. Inst. Fourier **50** (2000), 723–749.
[32] P. Parent, *No 17-torsion on elliptic curves over cubic number fields*, J. Theor. Nombres Bordeaux **15** (2003), 831–838.
[33] J. H. Silverman, Arithmetic of elliptic curves, 2nd edition, Springer-Verlag, New York, 2009.
[34] J. Wang, *On the cyclic torsion of elliptic curves over cubic number fields*, preprint, `http://arxiv.org/abs/1502.06873`
[35] W. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup. **4** (1969), 521–560.

Mathematisch Instituut, Universiteit Leiden, Postbus 9512, 2300 RA Leiden, Netherlands
E-mail address: `P.J.Bruin@math.leidenuniv.nl`

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

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA
E-mail address: `fnajman@mit.edu`