RANKS OF ELLIPTIC CURVES WITH PRESCRIBED TORSION OVER NUMBER FIELDS

JOHAN BOSMAN, PETER BRUIN, ANDREJ DUJELLA, AND FILIP NAJMAN

Abstract. We study the structure of the Mordell–Weil group of elliptic curves over number fields of degree 2, 3, and 4. We show that if T is a group, then either the class of all elliptic curves over quadratic fields with torsion subgroup T is empty, or it contains curves of rank 0 as well as curves of positive rank. We prove a similar but slightly weaker result for cubic and quartic fields. On the other hand, we find a group T and a quartic field K such that among the elliptic curves over K with torsion subgroup T, there are curves of positive rank, but none of rank 0. We find examples of elliptic curves with positive rank and given torsion in many previously unknown cases. We also prove that all elliptic curves over quadratic fields with a point of order 13 or 18 and all elliptic curves over quartic fields with a point of order 22 are isogenous to one of their Galois conjugates and, by a phenomenon that we call *false complex multiplication*, have even rank. Finally, we discuss connections with elliptic curves over finite fields and applications to integer factorization.

1. Introduction

For an elliptic curve E over a number field K, the Mordell–Weil theorem states that the Abelian group $E(K)$ of K-rational points on E is finitely generated. The group $E(K)$ is isomorphic to $T \oplus \mathbb{Z}^r$, where T is the torsion subgroup and r is a non-negative integer called the *rank* of the elliptic curve.

The aim of this paper is to study the interplay of the rank and torsion group of elliptic curves over quadratic, cubic, and quartic number fields. More explicitly, we will be interested in the following question: given a torsion group T and an elliptic curve E over a number field K of degree 2, 3, or 4 such that $E(K)_{\mathrm{tors}} \simeq T$, what can we say about the rank of $E(K)$?

A natural starting point is to wonder what can be said over $\mathbb{Q}$. Let T be a possible torsion group of an elliptic curve over $\mathbb{Q}$, i.e. it is one of the 15 groups from Mazur's torsion theorem [20, Theorem 8]. What can be said about the rank? The short answer is: nothing. For all we know, it might be 0, it might be positive, it might be even, or it might be odd. As we will later show, this is in stark contrast with what happens over number fields. Note that already in [15] torsion groups T and number fields K are given such that every elliptic curve over K with torsion T has rank 0.

We start by examining a very basic question: how many points can an elliptic curve have over a quadratic, cubic, or quartic field and what group structure can

2010 *Mathematics Subject Classification.* 11G05, 11R11, 11R16, 14H52.

Key words and phrases. Elliptic curves, number fields, rank, torsion group.

J.B. was supported by Marie Curie FP7 grant 252058.

P.B. was supported by the program "Points entiers et points rationnels" (Agence nationale de la recherche, France), I.H.É.S., and Swiss National Science Foundation grant 124737.

A.D. and F.N. were supported by the Ministry of Science, Education, and Sports, Republic of Croatia, grant 037-0372781-2821. A.D. was also supported by the Croatian Science Foundation under the project no. 6422.

F.N. was also supported by the National Foundation for Science, Higher Education, and Technological Development of the Republic of Croatia.

these points have? As there exist elliptic curves with infinitely many points over $\mathbb{Q}$, it is clear that an elliptic curve can possibly have infinitely many points over any number field. So, this question is closely related to determining for which finite groups T there exists an elliptic curve over a field of degree 2, 3, or 4 with torsion T and rank 0.

Over $\mathbb{Q}$, the answer to this question is known by Mazur's torsion theorem [20, Theorem 8]; it is an easy exercise to find an elliptic curve with fixed torsion and rank 0 over $\mathbb{Q}$. An elliptic curve over $\mathbb{Q}$ has $1, \ldots, 10, 12, 16$, or infinitely many rational points.

We prove a similar result over all the quadratic fields using a theorem of Kamienny, Kenku, and Momose [14, Theorem 3.1], [18, Theorem (0.1)], which tells us which groups appear as torsion of elliptic curves over quadratic fields. We find, for each of these torsion groups, an elliptic curve over some quadratic field having that particular torsion group and rank 0.

Note that if one fixes a number field and not just the degree, the situation is a bit different. Mazur and Rubin [21, Theorem 1.1] have proved that for each number field K there exists an elliptic curve over K such that the rank of $E(K)$ is 0. A natural question is whether the following generalization is true: if T is a group that appears as a torsion group of an elliptic curve over K, does there exist some elliptic curve with torsion T and rank 0? We prove that the answer is no, by giving an example of a quartic field K such that every elliptic curve with torsion $\mathbb{Z}/15\mathbb{Z}$ over K has positive rank.

It is known which groups appear *infinitely often* as a torsion group of an elliptic curve over a cubic field [12, Theorem 3.4]. For each group T from this list, we find a curve over a cubic field with rank 0 and torsion group T. We do the same for quartic fields, using the analogous result [11, Theorem 3.6]. It is not known if any other groups can appear as torsion groups of elliptic curves over cubic or quartic fields.

Next, we examine elliptic curves with given torsion and positive rank over fields of degree 2, 3, and 4. This problem has been extensively studied over $\mathbb{Q}$; see for example [6] for a list of references and rank records with given torsion. Over quadratic fields Rabarison [25, Section 4] found examples of elliptic curves with given torsion and positive rank for all except possibly 4 torsion groups. We find examples of elliptic curves with positive rank unconditionally for all these groups.

We do the same for cubic and quartic fields and find many instances of elliptic curves with previously unknown Mordell–Weil groups.

When searching for elliptic curves with given torsion and positive rank, we noticed that all constructed elliptic curves with 13-torsion and 18-torsion over quadratic fields and all constructed elliptic curves with 22-torsion over quartic fields appeared to have even rank. In Section 4 we prove that this is not a coincidence and that all elliptic curves with 13-torsion and 18-torsion over quadratic fields and all elliptic curves with 22-torsion over quartic fields have even rank indeed. The explanation involves $\mathbb{Q}$-curves and K-curves, where K is a quadratic field, and a phenomenon that we call *false complex multiplication*.

In Section 5 we examine the connections and applications of our results to elliptic curves over finite fields. In the elliptic curve factoring method [19], one looks for elliptic curves whose number of points over $\mathbb{F}_p$ for p prime is likely to be smooth, i.e. divisible only by small primes. It is now a classical method (see [1] and [23]) to use elliptic curves E with large rational torsion, as the torsion injects into $E(\mathbb{F}_p)$ for all primes $p \geq 3$ of good reduction. This in turn makes the order of $E(\mathbb{F}_p)$ more likely to be smooth.

One can get more information about the heuristic probability of an elliptic curve to have smooth order if the torsion of the curve is examined over both the rationals and number fields of small degree. We give an explicit example of two curves such that the one with smaller rational torsion has smooth order more often and discuss the implications of this for choosing elliptic curves for factoring.

We used Magma [3], Pari [24], and Sage [28] for most of our computations.

Acknowledgments. We are greatly indebted to Hendrik W. Lenstra, Jr. for ideas that motivated much of Section 4, including the terminology "false complex multiplication". We thank Thomas Preu for finding points of infinite order on the elliptic curve with torsion $\mathbb{Z}/18\mathbb{Z}$ over a quadratic field mentioned in Theorem 6.

2. Curves with prescribed torsion and rank 0

We first examine elliptic curves over quadratic fields. By a theorem of Kamienny [14, Theorem 3.1], Kenku, and Momose [18, Theorem (0.1)], the following 26 groups can appear as a torsion group of an elliptic curve over a quadratic field:

$$\begin{gathered}\mathbb{Z}/m\mathbb{Z} \text{ for } 1 \le m \le 18,\ m \ne 17,\\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z} \text{ for } 1 \le m \le 6,\\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3m\mathbb{Z} \text{ for } m = 1, 2,\\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}.\end{gathered} \tag{1}$$

We used the RankBound() function in Magma and the program mwrank [5] for rank computations. Over quadratic fields Magma can easily prove that the rank of the curves we are going to list in Theorem 1 is 0, so one does not have to employ any tricks to check the rank that will be needed in higher degree cases.

Note that it is easy to find examples with a torsion group that appears over $\mathbb{Q}$ and rank 0. By standard conjectures (see [8]), half of all elliptic curves should have rank 0. One first finds a curve $E/\mathbb{Q}$ with given torsion and rank 0. Then one finds a squarefree $d \in \mathbb{Z}$ such that the quadratic twist $E^{(d)}$ has rank 0. The curve $E_{\mathbb{Q}(\sqrt{d})}$ has rank 0 as well, and its torsion is likely the same as that of $E_{\mathbb{Q}}$. We still give explicit examples, as we feel that this is in the spirit of this paper. For the rest of the groups, one can find infinite families of elliptic curves with given torsion in [10] and [25, Section 4] and then search for rank 0 examples.

Theorem 1. *For each group T from (1), there exists an elliptic curve over a quadratic field with torsion T and rank 0.*

Proof. In Table 1 we give explicit examples of elliptic curves with rank 0. For all the curves listed, one checks that the rank is indeed 0 using a 2-descent. □

It is known which torsion groups appear infinitely often over cubic fields [12, Theorem 3.4]:

$$\begin{gathered}\mathbb{Z}/m\mathbb{Z} \text{ for } 1 \le m \le 20,\ m \ne 17, 19,\\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z} \text{ for } 1 \le m \le 7.\end{gathered} \tag{2}$$

There is no known example of an elliptic curve over a cubic field with a torsion subgroup that is not in the list (2), although it has not been proved that there are no such curves.

As the computation of rank bounds becomes more time-consuming in the cubic case, we first compute the parity (assuming the Birch–Swinnerton-Dyer conjecture) of the rank of the elliptic curve using the RootNumber() function in Magma and eliminate the curves with odd rank.

Theorem 2. *For each group T from (2), there exists an elliptic curve over a cubic field with torsion T and rank 0.*

Proof. We give explicit examples in Table 2; again, one can easily check that each curve has rank 0. We obtained our curves from [9]. □

As with cubic fields, it is known which torsion groups appear infinitely often over quartic fields [11, Theorem 3.6]:

$$\begin{gathered}\mathbb{Z}/m\mathbb{Z} \text{ for } 1 \leq m \leq 24,\ m \neq 19, 23,\\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z} \text{ for } 1 \leq m \leq 9,\\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3m\mathbb{Z} \text{ for } 1 \leq m \leq 3,\\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4m\mathbb{Z} \text{ for } 1 \leq m \leq 2,\\ \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z},\\ \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}.\end{gathered} \tag{3}$$

Again it is unknown whether there exists an elliptic curve over a quartic field with a torsion subgroup that is not in the list (3).

The computation of upper bounds on the rank of elliptic curves over quartic fields becomes much harder if it is done directly over the quartic field. However, we will use the fact that if an elliptic curve E is defined over a number field K and L is an extension of K of degree 2, i.e. $L = K(\sqrt{d}),\ d \in K$ and d is not a square, then the rank of $E(L)$ is the sum of the rank of $E(K)$ and the rank of $E^{(d)}(K)$. This can reduce the computation of the rank of an elliptic curve over a quartic field down to the computation of two ranks over quadratic fields or four computations over $\mathbb{Q}$. Again, we always compute the conjectural parity of the rank of the elliptic curve before the actual computation of the rank.

Theorem 3. *For each group T from (3) there exists an elliptic curve over a quartic field with torsion T and rank 0.*

Proof. We give explicit examples of such curves in Table 3. We used curves defined over smaller fields wherever possible. Curves that could not be obtained in such a way were obtained from [10].

Unlike in Tables 1 and 2, here the computation of the rank is usually very hard. We solve one example, $(2, 16)$, in detail to give a flavor of how our curves were obtained.

We start our search by looking for elliptic curves E over the rationals with torsion $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ and rank 0, where P is a point of order 8 and Q is of order 2 such that P and Q generate the complete torsion. Next, we search for a point $R \in E(\overline{\mathbb{Q}})$ with $2R = P$. There will be 4 such choices for R. We can obtain the field of definition of the points R by factoring the 16th division polynomial of our elliptic curve. There will be five factors of degree 4: one for each choice of R, and a fifth one that will generate the field of definition of the point Q_1 satisfying $2Q_1 = Q$ (over the field of definition of Q_1, our elliptic curve will have torsion isomorphic to $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$). Over each field K we check the conjectural parity of our starting elliptic curve over K. If it is odd, we eliminate the field and move to the next. If we get a curve E that has even rank over $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$, then we check the parity of the curves $E^{(d_1)}, E^{(d_2)}, E^{(d_1 \cdot d_2)}$ and eliminate the field if any of the curves have odd rank. If all the fields are eliminated, we move to the next elliptic curve.

After some searching we find the elliptic curve

$$y^2 = x^3 + 12974641/13176900x^2 + 16/14641x$$

over the field $\mathbb{Q}(\sqrt{-330}, \sqrt{-671})$. One can easily compute that the ranks of E and $E^{(-671)}$ are 0 by 2-descent in mwrank, but proving that the other two twists, $E^{(-330)}$ and $E^{(1871)}$, have rank 0 can not be done by 2-descent. Actually, both curves have the 2-primary part of their Tate–Shafarevich group isomorphic to

$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$, which can be checked by doing an 8-descent in Magma. In fact, the Tate–Shafarevich group of $E^{(-330)}$ is conjecturally isomorphic to $\mathbb{Z}/12\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$. However, one can prove that the twisted curves have rank 0 by approximating the L-value $L(E,1)$ and using Kolyvagin's result that an elliptic curve E over $\mathbb{Q}$ with $L(E,1) \neq 0$ has rank 0. We used Sage for this computation. □

From Theorems 1, 2, and 3 we obtain the following result about the number of points of an elliptic curve over a number fields of degree 2, 3, and 4.

Corollary 4. (1) *An elliptic curve over a quadratic field has* 1, ..., 16, 18, 20, 24, *or infinitely many points. All of the cases occur.*
(2) *There exist elliptic curves over cubic fields with* 1, ..., 15, 16, 18, 20, 24, 28, *and infinitely many points.*
(3) *There exist elliptic curves over quartic fields with* 1, ..., 17, 18, 20, 21, 22, 24, 25, 27, 28, 32, 36, *and infinitely many points.*
(4) *Up to isomorphism, there exist only finitely many elliptic curves over cubic and quartic fields for which the number of points is not in these lists.*

The last part depends on Merel's theorem [22]: for all $d \geq 1$, there are only finitely many groups that occur as torsion subgroups of elliptic curves over number fields of degree d. We also note that no curves with a different number of points are currently known. Furthermore, we do not know whether all the listed possibilities occur infinitely often.

3. Curves with prescribed torsion and positive rank

As mentioned in the introduction, Mazur and Rubin [21, Theorem 1.1] proved that over each number field there exists an elliptic curve with rank 0. We can reinterpret this theorem in the following way: if we look among all elliptic curves over a number field K, we will find a rank 0 curve. It is natural to ask whether this statement holds true if one only looks among elliptic curves satisfying some condition. We prove that the statement is not true if one looks only at elliptic curves with prescribed torsion over some fixed number field.

Theorem 5. *There is exactly one elliptic curve up to isomorphism over the quartic field* $\mathbb{Q}(i,\sqrt{5})$ *having torsion subgroup* $\mathbb{Z}/15\mathbb{Z}$*, and it has positive rank.*

Proof. (Compare [15, Theorem 5].) Over $\mathbb{Q}(\sqrt{5})$ there is exactly one curve with torsion $\mathbb{Z}/15\mathbb{Z}$, namely

$$E\colon y^2 = x^3 + (281880\sqrt{5} - 630315)x + 328392630 - 146861640\sqrt{5},$$

and one of the points of order 15 is

$$P = (315 - 132\sqrt{5}, 5400 - 2376\sqrt{5}).$$

We take an explicit affine model of $\mathrm{X}_1(15)$,

$$\mathrm{X}_1(15)\colon y^2 + xy + y = x^3 + x^2,$$

which can be found in [30], and compute

$$\mathrm{X}_1(15)(\mathbb{Q}(\sqrt{5})) \simeq \mathbb{Z}/8\mathbb{Z}.$$

Four of the points are cusps. The other four correspond to the pairs $(E, \pm P)$, $(E, \pm 2P)$, $(E, \pm 4P)$, $(E, \pm 7P)$. Over $\mathbb{Q}(\sqrt{5}, i)$, no extra points of $\mathrm{X}_1(15)$ appear, so E remains the only curve with torsion $\mathbb{Z}/15\mathbb{Z}$. In addition, E acquires the point $(-675 + 300\sqrt{5}, (2052\sqrt{5} - 4590)i)$ of infinite order over $\mathbb{Q}(i,\sqrt{5})$. □

Finding elliptic curves with high rank and prescribed torsion has a long history, which can be seen at the webpage [6], where there is a list of over 50 references about this problem.

Finding elliptic curves over number fields with prescribed torsion and positive rank has first been done by Rabarison [25], who studied elliptic curves over quadratic fields. He managed to find elliptic curves over quadratic fields with positive rank and torsion $\mathbb{Z}/11\mathbb{Z}$, $\mathbb{Z}/13\mathbb{Z}$, $\mathbb{Z}/14\mathbb{Z}$, $\mathbb{Z}/16\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$, and $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$.

Theorem 6. *There exist elliptic curves over quadratic fields whose Mordell–Weil groups contain* $\mathbb{Z}/15\mathbb{Z}\oplus\mathbb{Z}$, $\mathbb{Z}/18\mathbb{Z}\oplus\mathbb{Z}^2$, $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/10\mathbb{Z}\oplus\mathbb{Z}^4$, *and* $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/12\mathbb{Z}\oplus\mathbb{Z}^4$.

Proof. We give explicit examples of such curves in Table 6.

Suppose E is an elliptic curve with exactly one point of order 2 over some number field K. Note that the 2-division polynomial of E, ψ_2, is of degree 3, so ψ_2 factors over K as a linear polynomial times a quadratic polynomial. This implies that there is exactly one quadratic extension of K over which E has full 2-torsion, which can easily be found (the splitting field of the quadratic factor).

We start with elliptic curves with high rank over $\mathbb{Q}$ and torsion $\mathbb{Z}/10\mathbb{Z}$ and $\mathbb{Z}/12\mathbb{Z}$ over $\mathbb{Q}$. Explicit examples of such curves are given in [6]. We take such a curve and use the fact that it has exactly one rational 2-torsion point. We then apply the above method to construct elliptic curves with high rank and torsion $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$ over some quadratic field. In this way, we find the two corresponding curves in Table 6.

To find an elliptic curve with torsion $\mathbb{Z}/15\mathbb{Z}$ and positive rank, we search for points on $\mathrm{X}_1(15)$ and then from them construct elliptic curves. Among those elliptic curves, we sieve for the ones that have conjecturally odd rank. Then we are left with the problem of finding a point of infinite order on such a curve. We managed to find such a point by looking at small multiples of divisors of the discriminant of the curve.

For elliptic curves over quadratic fields with torsion $\mathbb{Z}/18\mathbb{Z}$, the rank is always even, as will be shown in Theorem 9. For curves constructed from points of $\mathrm{X}_1(18)$ over quadratic fields, therefore, instead of computing the root number to find candidates for curves with positive rank, we approximate the value of the L-function $L(E, s)$ at $s = 1$; if this vanishes, then E should have rank at least 2 by the Birch–Swinnerton-Dyer conjecture. In this way we obtain the elliptic curve in Table 6. The first point of infinite order was found by T. Preu using the PseudoMordellWeilGroup() function in Magma after a change of coordinates to simplify the Weierstrass equation. The second point of infinite order can be found using the action of $\mathbb{Z}[\sqrt{-2}]$ on $E(K)$ described in Subsection 4.6. □

We study the same problem over cubic and quartic fields, and find many new examples of Mordell–Weil groups of elliptic curves. We will not give examples for the torsion groups T such that it is trivial to find an elliptic curve with torsion T and positive rank. Let us explain what we mean by "trivial" for cubic and for quartic fields.

Over cubic fields, the trivial T are those that already appear as torsion groups of elliptic curves over $\mathbb{Q}$, as well as $\mathbb{Z}/14\mathbb{Z}$ and $\mathbb{Z}/18\mathbb{Z}$. Namely, let E be an elliptic curve over $\mathbb{Q}$ with positive rank and torsion $\mathbb{Z}/7\mathbb{Z}$ or $\mathbb{Z}/9\mathbb{Z}$. Then over the cubic field generated by a root of the 2-division polynomial, E has torsion $\mathbb{Z}/14\mathbb{Z}$ or $\mathbb{Z}/18\mathbb{Z}$, respectively. In this way, one can construct elliptic curves with Mordell–Weil groups $\mathbb{Z}/14\mathbb{Z} \oplus \mathbb{Z}^5$ and $\mathbb{Z}/18\mathbb{Z} \oplus \mathbb{Z}^4$; see [6].

Over quartic fields, the trivial T are those that already occur over the rational numbers or a quadratic field, those of the form $\mathbb{Z}/4n\mathbb{Z}$, where $\mathbb{Z}/2n\mathbb{Z}$ occurs over $\mathbb{Q}$,

and those of the form $\mathbb{Z}/2\mathbb{Z} \oplus T'$, where T' occurs over a quadratic field and has exactly one element of order 2. Let E be an elliptic curve over $\mathbb{Q}$ with positive rank and torsion $\mathbb{Z}/2n\mathbb{Z}$, and let $R \in E(\overline{\mathbb{Q}})$ be a point such that $2R$ generates this torsion group. Then E has torsion at least $\mathbb{Z}/4n\mathbb{Z}$ over the field of definition of R. In this way, one can construct elliptic curves with Mordell–Weil group containing $\mathbb{Z}/16\mathbb{Z} \oplus \mathbb{Z}^6$, $\mathbb{Z}/20\mathbb{Z} \oplus \mathbb{Z}^4$, and $\mathbb{Z}/24\mathbb{Z} \oplus \mathbb{Z}^4$. Now let E be an elliptic curve over a quadratic field K with positive rank and torsion T', with T' as above. Then E has torsion at least $\mathbb{Z}/2\mathbb{Z} \oplus T'$ over the quartic field $K(E[2])$. In this way, one can construct elliptic curves over quartic fields with Mordell–Weil groups containing $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z} \oplus \mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z} \oplus \mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/18\mathbb{Z} \oplus \mathbb{Z}^2$, and $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}^6$. (See [13] for an example of an elliptic curve with Mordell–Weil group containing $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}^6$ over $\mathbb{Q}(\sqrt{-3})$.)

Theorem 7. *There exist elliptic curves over cubic fields whose Mordell–Weil groups contain* $\mathbb{Z}/11\mathbb{Z} \oplus \mathbb{Z}^2$, $\mathbb{Z}/13\mathbb{Z} \oplus \mathbb{Z}$, $\mathbb{Z}/15\mathbb{Z} \oplus \mathbb{Z}$, $\mathbb{Z}/16\mathbb{Z} \oplus \mathbb{Z}$, $\mathbb{Z}/20\mathbb{Z} \oplus \mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z} \oplus \mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z} \oplus \mathbb{Z}$ *and* $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z} \oplus \mathbb{Z}$.

Proof. We give explicit examples of such curves in Table 6. For torsion group $\mathbb{Z}/11\mathbb{Z}$, we search through the curves constructed in [12], and quickly find a rank two curve among the smallest cases. For the other torsion groups, we construct elliptic curves with given torsion using [9], sieve for elliptic curve with conjecturally odd (and thus positive) rank, and then find points on the curves obtained. □

Theorem 8. *There exist elliptic curves over quartic fields whose Mordell–Weil groups contain* $\mathbb{Z}/17\mathbb{Z} \oplus \mathbb{Z}$, $\mathbb{Z}/21\mathbb{Z} \oplus \mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}$, *and* $\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}$.

Proof. Explicit examples of such curves are given in Table 6. We obtain our curves from [10] and use the same strategy as in Theorem 7 to obtain points of infinite order on them. □

From the results in this section, we can draw the following conclusion. Let $d \leq 4$, and let T be a group that occurs infinitely often as the torsion group of an elliptic curve over a number field of degree d. Then there exists an elliptic curve with positive rank and torsion T over a number field of degree d, except possibly for $d = 4$ and $T = \mathbb{Z}/22\mathbb{Z}$.

4. False complex multiplication

In this section we describe a phenomenon that, for an elliptic curve E over a quadratic field L having torsion $\mathbb{Z}/13\mathbb{Z}$, $\mathbb{Z}/16\mathbb{Z}$, or $\mathbb{Z}/18\mathbb{Z}$, gives $E(L)$ a module structure over the ring $\mathbb{Z}[t]/(t^2-a)$ for some $a \in \mathbb{Z}$. We say that E has *false complex multiplication* by $\mathbb{Q}[t]/(t^2-a)$; a precise definition of false complex multiplication will be given in Subsection 4.1. A similar phenomenon occurs for elliptic curves with torsion $\mathbb{Z}/22\mathbb{Z}$ over quartic fields.

Theorem 9. *Let E be an elliptic curve over a number field L.*

1. *If $[L : \mathbb{Q}] = 2$ and E has a rational point of order 13, then L is real and E has false complex multiplication by $\mathbb{Q}(\sqrt{-1})$.*
2. *If $[L : \mathbb{Q}] = 2$ and E has a rational point of order 16, then E has false complex multiplication by $\mathbb{Q} \times \mathbb{Q}$.*
3. *If $[L : \mathbb{Q}] = 2$ and E has a rational point of order 18, then L is real and E has false complex multiplication by $\mathbb{Q}(\sqrt{-2})$.*
4. *If $[L : \mathbb{Q}] = 4$ and E has a rational point of order 22, then L has a quadratic subfield K such that E is a K-curve over L with false complex multiplication by $\mathbb{Q}(\sqrt{-2})$.*

Corollary 10. *Any elliptic curve over a quadratic number field with a point of order* 13 *or order* 18*, as well as any elliptic curve over a quartic number field with a point of order* 22*, has even rank.*

Theorem 11. *Let E be an elliptic curve defined over a quadratic field L with a point of order $n = 13$ or 16, and let σ be the generator of* $\mathrm{Gal}(L/\mathbb{Q})$*. Then*

(1) *E is L-isomorphic to E^σ.*
(2) *E has a quadratic twist (by an element d of O_L) $E^{(d)}$ that is defined over $\mathbb{Q}$. For any such d, the curve $E^{(d)}$ has an n-isogeny defined over $\mathbb{Q}$.*

4.1. **Preliminaries.** Let L/K be a finite Galois extension of number fields, and let E be an elliptic curve over L. Let $\mathrm{Res}_{L/K}$ denote the Weil restriction functor. We let B denote the Abelian variety

$$B = \mathrm{Res}_{L/K} E$$

of dimension $[L : K]$ over K. It is known that the base change B_L of B to L is given by

$$B_L \simeq \prod_{\sigma \in \mathrm{Gal}(L/K)} {}^\sigma E.$$

From this we get an isomorphism

$$\mathrm{End}_L B_L \simeq \bigoplus_{\sigma,\tau \in \mathrm{Gal}(L/K)} \mathrm{Hom}_L({}^\sigma E, {}^\tau E).$$

where the multiplication on the left-hand side corresponds to "matrix multiplication" on the right-hand side. Taking Galois invariants, we get an isomorphism

$$\mathrm{End}_K B \simeq \bigoplus_{\sigma \in \mathrm{Gal}(L/K)} \mathrm{Hom}_L({}^\sigma E, E),$$

where the multiplication on the right-hand side is the bilinear extension of the maps

$$\begin{aligned} \mathrm{Hom}({}^\sigma E, E) \times \mathrm{Hom}({}^\tau E, E) &\longrightarrow \mathrm{Hom}({}^{\sigma\tau} E, E) \\ (\mu, \nu) &\longmapsto \mu \circ {}^\sigma \nu. \end{aligned}$$

Definition. Let L/K be a finite Galois extension of number fields. A *K-curve over L* is an elliptic curve E over L that is isogenous to its Galois conjugates ${}^\sigma E$ for all $\sigma \in \mathrm{Gal}(L/K)$.

Let E be a K-curve over L, and write $R_E = \mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}_L E$; this is either $\mathbb{Q}$ or an imaginary quadratic field. Then $\mathrm{Hom}_L({}^\sigma E, E)$ is a one-dimensional R_E-vector space for all $\sigma \in \mathrm{Gal}(L/K)$, and hence $\mathbb{Q} \otimes_{\mathbb{Z}} \mathrm{End}_K(\mathrm{Res}_{L/K} E)$ is an R_E-vector space of dimension $[L : K]$.

In the sequel, we will only be interested in the case where L is a quadratic extension of K. For this we introduce the following terminology.

Definition. Let L be a number field, let E be an elliptic curve over L, and let F be an étale $\mathbb{Q}$-algebra of degree 2. We say that E has *false complex multiplication* by F if there exists a subfield $K \subset L$ with $[L : K] = 2$ such that $\mathbb{Q} \otimes \mathrm{End}_K(\mathrm{Res}_{L/K} E)$ contains a $\mathbb{Q}$-algebra isomorphic to F.

Remarks. Let E, L, F, and K be as in the above definition.

(1) An elliptic curve E over a number field L has false complex multiplication if and only if E has complex multiplication or there is a subfield $K \subset L$ with $[L : K] = 2$ such that E is a K-curve.

(2) Note that F is either $\mathbb{Q} \times \mathbb{Q}$ or a quadratic field. If E is an elliptic curve over L with false complex multiplication by F, then the $\mathbb{Q}$-vector space

$$\mathbb{Q} \otimes_{\mathbb{Z}} E(L) \simeq \mathbb{Q} \otimes_{\mathbb{Z}} (\mathrm{Res}_{L/K} E)(K)$$

has a natural F-module structure. If F is a field, this implies that the finitely generated Abelian group $E(L)$ has even rank.

4.2. **Families of curves with false complex multiplication constructed from involutions on modular curves.** Let n be a positive integer, and let $\mathrm{Y}_0(n)$ be the (coarse) modular curve over $\mathbb{Q}$ classifying elliptic curves with a cyclic subgroup of order n, i.e. a subgroup scheme that is locally isomorphic to $\mathbb{Z}/n\mathbb{Z}$ in the étale topology. Let Y be a smooth affine curve over $\mathbb{Q}$, let E be an elliptic curve over Y, and let G be a cyclic subgroup of order n in E. Then we obtain a morphism

$$Y \to \mathrm{Y}_0(n).$$

We assume that this morphism is finite. Furthermore, we suppose given an involution

$$\iota \colon Y \xrightarrow{\sim} Y$$

that lifts the automorphism w_n of $\mathrm{Y}_0(n)$.

Pulling back E via ι gives a second elliptic curve $\iota^* E$ over Y. By the assumption that ι lifts w_n, we have

$$\iota^* E \simeq E/G.$$

Symmetrically, $\iota^* E$ is equipped with the cyclic subgroup $\iota^* G$ of order n, which corresponds to the subgroup $E[n]/G$ of E/G; we have

$$(\iota^* E)/(\iota^* G) \simeq E.$$

In view of this, we may fix an isogeny

$$\mu \colon \iota^* E \to E$$

with kernel $\iota^* G$. Since the morphism $Y \to \mathrm{Y}_0(n)$ is finite and therefore dominant, we have $\mathrm{Aut}_Y E = \{\pm 1\}$, and so μ is unique up to sign. Pulling back μ via ι and using the canonical isomorphism $\iota^* \iota^* E \simeq E$, we get a second isogeny

$$\iota^* \mu \colon E \to \iota^* E$$

with kernel G. Composing these, we get an endomorphism

$$a = \mu \circ \iota^* \mu \in \mathrm{End}_Y E. \tag{4}$$

Note that this endomorphism does not depend on the choice of μ. Its kernel is $E[n]$, so again using $\mathrm{Aut}_Y E = \{\pm 1\}$, we conclude that

$$a = \pm n.$$

In particular, up to sign, $\iota^* \mu$ is the dual isogeny of μ.

Let U be the complement of the scheme of fixed points of the involution ι on Y, let U/ι denote the quotient, and let $\mathrm{Res}_{U/(U/\iota)}$ denote the Weil restriction functor from U-schemes to (U/ι)-schemes [2, Section 7.6]. We write

$$B = \mathrm{Res}_{U/(U/\iota)} E.$$

Because the quotient map $U \to U/\iota$ is étale of degree 2, this is an Abelian scheme of relative dimension 2 over U/ι. As in Subsection 4.1, we have

$$\mathrm{End}_{U/\iota} B \simeq \mathrm{End}_U L \oplus \mathrm{Hom}_U(\iota^* E, E).$$

We get an injective homomorphism

$$\mathbb{Z}[t]/(t^2 - a) \rightarrowtail \mathrm{End}_{U/\iota} B$$

mapping t to the endomorphism of B corresponding to $\mu \in \mathrm{Hom}_U(\iota^* E, E)$ under the above isomorphism.

Now let K be a number field. Specializing to arbitrary K-points of U/ι gives a construction of K-curves, as follows. Let $u \in (U/\iota)(K)$. Suppose that the inverse image v of u in U is irreducible, so it is of the form $\operatorname{Spec} L$ with L a quadratic extension of L. Then the fiber E_v is a K-curve over L and has false complex multiplication by $\mathbb{Q}[t]/(t^2 - a)$. In particular, if a is not a square, then $E_v(L)$ has even rank.

4.3. **The modular curves $\mathrm{Y}_1(n)$.** Let $n \geq 6$ be an integer. The affine modular curve $\mathrm{Y}_1(n)$ classifying elliptic curves with a point of order n can be described as

$$\mathrm{Y}_1(n) \simeq \operatorname{Spec}\big(\mathbb{Z}[s, t, 1/n, 1/\Delta]/(\phi_n)\big),$$

where

$$\Delta = -s^4 t^3 (t-1)^5 \big(s(s+4)^2 t^2 - s(2s^2 + 5s + 20)t + (s-1)^3\big)$$

and where

$$\phi_n \in \mathbb{Z}[s, t]$$

is an irreducible polynomial depending on n. The universal elliptic curve over $\mathrm{Y}_1(n)$ is given by the Weierstrass equation

$$E\colon y^2 + (1 + (t-1)s)xy + t(t-1)sy = x^3 + t(t-1)sx^2$$

with the distinguished point $(0, 0)$, and ϕ_n is such that its vanishing is equivalent to the condition that $(0, 0)$ is of order n.

Since the polynomial ϕ_n is rather complicated for all but the smallest values of n, it pays to introduce a change of variables giving a simpler-looking equation for $\mathrm{Y}_1(n)$. The new variables are called u and v in the examples below.

4.4. **Torsion subgroup $\mathbb{Z}/13\mathbb{Z}$.** We consider the modular curve $\mathrm{Y}_1(13)$ over $\mathbb{Q}$. Its compactification $\mathrm{X}_1(13)$ has genus 2 and in particular is hyperelliptic. There are six rational cusps and six cusps with field of definition $\mathbb{Q}(\zeta_{13} + \zeta_{13}^{-1})$.

Let (E, P) denote the universal pair of an elliptic curve and a point of order 13 over $\mathrm{Y}_1(13)$. The diamond automorphism

$$\iota = \langle 5 \rangle = \langle -5 \rangle$$

of $\mathrm{Y}_1(13)$ is an involution since 5^2 is the identity element of $(\mathbb{Z}/13\mathbb{Z})^\times/\{\pm 1\}$. It is a lift of the "Atkin–Lehner involution w_1" on $\mathrm{X}(1)$ (i.e. the identity). We note that the fixed points of ι lie outside the cusps.

Pulling back (E, P) via ι yields a second pair $\iota^*(E, P)$, and the definition of ι gives an isomorphism

$$\mu\colon \iota^*(E, P) \xrightarrow{\sim} (E, 5P)$$

over $\mathrm{Y}_1(13)$. Pulling back μ via ι gives another isomorphism

$$\iota^*\mu\colon (E, P) \xrightarrow{\sim} \iota^*(E, 5P).$$

We have

$$\mu \circ \iota^*\mu\colon (E, P) \xrightarrow{\sim} (E, 5^2 P) = (E, -P).$$

This implies that, in the notation introduced above, we have

$$a = -1,$$

so the Abelian variety B has the property that

$$\operatorname{End} B \simeq \mathbb{Z}[\sqrt{-1}].$$

In coordinates, the situation looks as follows. We have

$$\phi_{13} = t^3 - (s^4 + 5s^3 + 9s^2 + 4s + 2)t^2 + (s^3 + 6s^2 + 3s + 1)t + s^3.$$

We use the change of variables

$$u = 1/(s+1) + 1/(t-1), \quad v = u^4(t-1) + u^2;$$
$$s = \frac{v+u}{u(u+1)^2} - 1, \quad t = \frac{v-u^2}{u^4} + 1.$$

The modular curve $\mathrm{Y}_1(13)$ is isomorphic to the affine curve given by

$$v^2 - (u^3 + 2u^2 + u + 1)v + u^2(u+1) = 0,$$
$$u(u+1)(u^3 - u^2 - 4u - 1) \neq 0.$$

The six rational cusps are given by $u = 0$, $u = -1$, and $u = \infty$; the six cusps defined over $\mathbb{Q}(\zeta_{13} + \zeta_{13}^{-1})$ are given by $u^3 - u^2 - 4u - 1 = 0$.

The hyperelliptic involution sends (u, v) to $(u, u^3+2u^2+u+1-v)$. A computation using the moduli interpretation shows that the hyperelliptic involution coincides with $\langle 5 \rangle = \langle -5 \rangle$.

The specialization construction explained in Subsection 4.2 gives a family of $\mathbb{Q}$-curves. Let $c \in \mathbb{Q} \setminus \{0, -1\}$. The inverse image of the point defined by c under the map

$$u \colon \mathrm{Y}_1(13) \to \operatorname{Spec} \mathbb{Q}[u, 1/(u(u+1)(u^3 - u^2 - 4u - 1))]$$

is the spectrum of the quadratic $\mathbb{Q}$-algebra

$$L = \mathbb{Q}[v]/(v^2 - (c^3 + 2c^2 + c + 1)v + c^2(c+1)).$$

Since $\mathrm{Y}_1(13)$ does not have any $\mathbb{Q}$-rational points, L is a field, and we obtain an elliptic curve over L with false complex multiplication by $\mathbb{Q}(\sqrt{-1})$.

In fact, *any* elliptic curve over a quadratic field with a point of order 13 comes from the above construction, as we will now show.

Lemma 12. *Let X be a proper, smooth, geometrically connected curve of genus 2 over a field k, let ι be the hyperelliptic involution on X, let K be a canonical divisor on X, and let J be the Jacobian of X.*

1. *An effective divisor of degree 2 on X is in the canonical linear equivalence class if and only it is the pull-back of a k-rational point of X/ι.*
2. *Let S be a finite set of closed points of X such that every k-point of J is of the form $[D' - K]$, where D' is an effective divisor of degree 2 with support in S. Let D be an effective divisor of degree 2 on X. Then either D has support in S, or D lies in the canonical linear equivalence class.*

Proof. The first part is well known. For the second part, let D be an effective divisor of degree 2. By assumption, D is linearly equivalent to an effective divisor D' with support in S. If D is not in the canonical linear equivalence class, then the complete linear system $|D|$ has dimension 0, so $D = D'$. □

Lemma 13. *Let $\mathrm{J}_1(13)$ denote the Jacobian of $\mathrm{X}_1(13)$, and let K be a canonical divisor on $\mathrm{X}_1(13)$. The group $\mathrm{J}_1(13)(\mathbb{Q})$ is isomorphic to $\mathbb{Z}/19\mathbb{Z}$, and every element of $\mathrm{J}_1(13)(\mathbb{Q})$ is of the form $[D-K]$ with D an effective divisor of degree 2 supported on the cusps of $\mathrm{X}_1(13)$.*

Proof. Two distinct effective divisors of degree 2 on a curve of genus 2 are linearly equivalent if and only if they are both in the canonical linear equivalence class. The set of effective divisors of degree 2 supported at the cusps, which has $\binom{6+2-1}{2} = 21$ elements, therefore splits up into the canonical linear equivalence class consisting of 3 divisors (defined concretely by $u = 0$, $u = -1$, and $u = \infty$) and 18 linear equivalence classes consisting of a single divisor. We deduce that the effective divisors of degree 2 supported at the cusps yield 19 rational points of $\mathrm{J}_1(13)$.

One can show by a 2-descent (implemented for instance in Magma that $\mathrm{J}_1(13)$ has trivial 2-Selmer group. It follows that $\mathrm{J}_1(13)(\mathbb{Q})$ is a finite group of odd order. Together with the fact that $\mathrm{J}_1(13)$ has good reduction at 2, this implies that $\mathrm{J}_1(13)(\mathbb{Q})$ injects into $\mathrm{J}_1(13)(\mathbb{F}_2)$. One computes the zeta function of $\mathrm{X}_1(13)_{\mathbb{F}_2}$ as

$$Z(\mathrm{X}_1(13)_{\mathbb{F}_2}, t) = \frac{1 + 3t + 5t^2 + 6t^3 + 4t^4}{(1-t)(1-2t)}.$$

Setting $t = 1$ in the numerator, we see that $\mathrm{J}_1(13)$ has 19 points over $\mathbb{F}_2$. This proves that $\mathrm{J}_1(13)$ has no other rational points than the 19 found above. □

Proof of Theorem 9(1). Let (E, P) be a pair consisting of an elliptic curve and a point of order 13 over a quadratic field L. Let y be the closed point of $\mathrm{Y}_1(13)$ defined by (E, P). Since $\mathrm{Y}_1(13)$ has no $\mathbb{Q}$-rational points, the residue field of y is a quadratic extension of $\mathbb{Q}$, so y defines a divisor of degree 2 on $\mathrm{Y}_1(13)$. Combining Lemma 13 and Lemma 12, with S equal to the set of cusps of $\mathrm{X}_1(13)$, we see that y lies in the canonical linear equivalence class. This implies that there is a $\mathbb{Q}$-rational point $x \in \mathrm{Y}_1(13)/\iota$ such that y is the inverse image of x under the quotient map $\mathrm{Y}_1(13) \to \mathrm{Y}_1(13)/\iota$. Therefore (E, P) arises from the specialization construction described above, and E has false complex multiplication by $\mathbb{Q}(\sqrt{-1})$.

The modular curve $\mathrm{Y}_1(13)$ can be rewritten in the form

$$v^2 = f(u) = u^6 - 2u^5 + u^4 - 2u^3 + 6u^2 - 4u + 1,$$

$$u(u-1)(u^3 - 4u^2 + u + 1) \neq 0.$$

The description of the points on $\mathrm{Y}_1(13)$ implies that for $y = (u, v) \in \mathrm{Y}_1(13)(L)$, u is $\mathbb{Q}$-rational. As $f(u) > 0$ for all $u \in \mathbb{R}$, we conclude that v is a square root of a positive rational number, and hence v is defined over a real quadratic field. □

4.5. **The modular curve $\mathrm{Y}_1(16)$ and quadratic $\mathbb{Q}$-curves with odd rank.** As noted in Subsection 4.2, a $\mathbb{Q}$-curve has even rank if the value a defined in (4) is not a square. In this subsection we show that for every elliptic curve defined over a quadratic field with torsion $\mathbb{Z}/16\mathbb{Z}$, the value a is equal to 1. As opposed to the $\mathbb{Z}/13\mathbb{Z}$ or $\mathbb{Z}/18\mathbb{Z}$ cases, there do exist elliptic curves with torsion $\mathbb{Z}/16\mathbb{Z}$ and odd rank.

Let (E, P) denote the universal pair consisting of an elliptic curve and a point of order 16 over $\mathrm{Y}_1(16)$. The diamond automorphism

$$\iota = \langle 7 \rangle = \langle -7 \rangle$$

of $\mathrm{Y}_1(16)$ is an involution since 7^2 is the identity element in $(\mathbb{Z}/16\mathbb{Z})^\times$. As in Subsection 4.4, ι is a lift of w_1 on $\mathrm{X}(1)$.

Pulling back (E, P) via ι yields a second pair $\iota^*(E, P)$, and the definition of ι gives an isomorphism

$$\mu \colon \iota^*(E, P) \xrightarrow{\sim} (E, 7P)$$

over $\mathrm{Y}_1(16)$. Pulling back μ via ι gives another isomorphism

$$\iota^*\mu \colon (E, P) \xrightarrow{\sim} \iota^*(E, 7P).$$

We have

$$\mu \circ \iota^*\mu \colon (E, P) \xrightarrow{\sim} (E, 7^2 P) = (E, P).$$

This implies that we have $a = 1$, so the Abelian variety B has the property that

$$\operatorname{End} B \simeq \mathbb{Z} \times \mathbb{Z}.$$

Using this construction, we can in fact obtain $\mathbb{Q}$-curves with odd rank: the elliptic curve

$$E \colon y^2 + (121 + 39\sqrt{10})xy - (3510 + 1107\sqrt{10})y = x^3 - (3510 + 1107\sqrt{10})x^2,$$

taken from [25, Théorème 10] has Mordell–Weil group

$$E(\mathbb{Q}(\sqrt{10})) \simeq \mathbb{Z}/16\mathbb{Z} \oplus \mathbb{Z}.$$

It is also a $\mathbb{Q}$-curve, isomorphic to E^σ.

As in the previous subsections, we prove that all elliptic curves with torsion $\mathbb{Z}/16\mathbb{Z}$ are $\mathbb{Q}$-curves. In fact, as with curves having torsion $\mathbb{Z}/13\mathbb{Z}$, they will be isomorphic, not just isogenous, to their Galois conjugates.

Lemma 14. *Let* $\mathrm{J}_1(16)$ *denote the Jacobian of* $\mathrm{X}_1(16)$*, and let* K *be a canonical divisor on* $\mathrm{X}_1(18)$*. The group* $\mathrm{J}_1(16)(\mathbb{Q})$ *is isomorphic to* $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$*, and every element of* $\mathrm{J}_1(16)(\mathbb{Q})$ *is of the form* $[D - K]$ *with* D *an effective divisor of degree* 2 *supported on the cusps of* $\mathrm{X}_1(16)$*.*

Proof. This is again similar to Lemma 13. The set of effective divisors of degree 2 supported at the cusps has $\binom{6+2-1}{2} + 2 = 23$ elements and splits up into the canonical linear equivalence class, consisting of 4 divisors (with support in the cusps corresponding to 8-gons and 16-gons), and 19 linear equivalence classes consisting of a single divisor. We deduce that the effective divisors of degree 2 supported at the cusps yield 20 rational points of $\mathrm{J}_1(16)$. Moreover, there are at least three such divisors D (with support in the cusps corresponding to 2-, 4-, and 8-gons) such that $[D - K]$ has order 2.

By 2-descent, we find that the 2-Selmer group of $\mathrm{J}_1(16)$ has dimension 2 over $\mathbb{F}_2$. Since we have three distinct points of order 2, we conclude that $\mathrm{J}_1(16)(\mathbb{Q})$ is finite. As in the proof of Lemma 15, we use the fact that reduction modulo 3 is injective on torsion. The zeta function of $\mathrm{X}_1(16)$ over $\mathbb{F}_3$ is

$$Z(\mathrm{X}_1(16)_{\mathbb{F}_3}, t) = \frac{1 + 2t + 2t^2 + 6t^3 + 9t^4}{(1-t)(1-3t)}.$$

Setting $t = 1$ in the numerator, we see that $\mathrm{J}_1(16)$ has 20 points over $\mathbb{F}_3$. This proves that $\mathrm{J}_1(16)$ has no other rational points than the 20 found above. The only possible group structure is $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$ in view of the three 2-torsion points. □

Proof of Theorem 9(2). This is proved in the same way as Theorem 9(1), using Lemma 14 instead of Lemma 13. □

Proof of Theorem 11. Part (1) follows from Subsections 4.4 and 4.5. Since E and E^σ are isomorphic, E has to have a rational j-invariant, meaning that a twist $E^{(d)}$ of can be defined over $\mathbb{Q}$. As E/L has an n-isogeny, so does $E^{(d)}/L$. Let C be an n-cycle on E. As E and E^σ are isomorphic and μ sends C^σ to C, one can see that (E, C) and (E^σ, C^σ) represent the same point on $\mathrm{Y}_0(n)(L)$. As Y_0 is a coarse moduli space, the same point on $\mathrm{Y}_0(n)(L)$ is also represented by $(E^{(d)}, C')$, where C' is the corresponding n-cycle on $E^{(d)}$ over L and $((E^\sigma)^{(d)}, (C')^\sigma)$. Thus, one can see that C' is σ-invariant, and hence $E^{(d)}$ has a $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-invariant cyclic subgroup of order n (and hence a rational n-isogeny). □

4.6. **Torsion subgroup** $\mathbb{Z}/18\mathbb{Z}$**.** We consider the modular curve $\mathrm{Y}_1(18)$ over $\mathbb{Q}$. Its compactification $\mathrm{X}_1(18)$ has genus 2 and in particular is hyperelliptic. There are six rational cusps, four cusps with field of definition $\mathbb{Q}(\zeta_3)$, and six cusps with field of definition $\mathbb{Q}(\zeta_9 + \zeta_9^{-1})$.

We view $\mathrm{Y}_1(18)$ as classifying triples (E, P_2, P_9) with E an an elliptic curve, P_2 a point of order 2, and P_9 a point of order 9. We define an involution ι of $\mathrm{Y}_1(18)$ by

$$\iota(E, P_2, P_9) = (E/\langle P_2\rangle, Q_2, 2P_9 \bmod \langle P_2\rangle),$$

where Q_2 is the generator of the isogeny dual to the quotient map $E \to E/\langle P_2\rangle$.

We denote the universal triple over $\mathrm{Y}_1(18)$ by (E, P_2, P_9). The definition of ι gives an isogeny of degree 2:

$$\begin{aligned}\mu\colon \iota^*(E,P_2,P_9) &\xrightarrow{\sim} (E/\langle P_2\rangle, Q_2, 2P_9 \bmod \langle P_2\rangle)\\ &\longrightarrow (E/E[2], 0, 2P_9 \bmod E[2])\\ &\xrightarrow{\sim} (E,0,4P_9).\end{aligned}$$

Pulling back μ via ι gives a second isomorphism

$$\iota^*\mu\colon (E,P_2,P_9) \longrightarrow \iota^*(E,0,4P_9).$$

We have

$$\mu\circ\iota^*\mu\colon (E,P_9) \xrightarrow{\sim} (E,4^2P_9) = (E,-2P_9).$$

This implies that in the notation introduced above, we have

$$a = -2,$$

so the Abelian variety B has the property that

$$\operatorname{End} B \simeq \mathbb{Z}[\sqrt{-2}].$$

In coordinates, the situation looks as follows. We have

$$\begin{aligned}\phi_{18} = {}&(s^3+6s^2+9s+1)t^4 + (s^5+7s^4+20s^3+19s^2-8s-1)t^3\\ &- s^2(s^2+11s+28)t^2 - s^2(s^2+5s-8)t - s^2(s^2-s+1).\end{aligned}$$

We use the change of variables

$$\begin{aligned}u = {}&-\frac{s^6+10s^5+38s^4+68s^3+55s^2+14s+1}{s(s+1)^6}t^3\\ &-\frac{s^8+11s^7+53s^6+135s^5+176s^4+88s^3-16s^2-12s-1}{s(s+1)^6}t^2\\ &+\frac{s^6+13s^5+63s^4+132s^3+116s^2+26s}{(s+1)^6}t+\frac{2s^5+3s^4-8s^3-17s^2-5s}{(s+1)^6},\end{aligned}$$

$$v = u - s; \qquad s = u - v, \quad t = \frac{(u^2-1)v - u^5 - 2u^4 - 2u^3 + u^2 + u}{u^3+3u^2-1}.$$

The modular curve $\mathrm{Y}_1(18)$ is isomorphic to the affine curve given by

$$\begin{aligned}v^2 - (u^3+2u^2+3u+1)v + u(u+1)^2 = 0,\\ u(u+1)(u^2+u+1)(u^3+3u^2-1) \neq 0.\end{aligned}$$

The hyperelliptic involution sends (u,v) to $(u, u^3+2u^2+3u+1-v)$. A computation using the moduli interpretation shows that the hyperelliptic involution coincides with the involution ι defined above.

By specialization we obtain a family of elliptic curves with false complex multiplication by $\mathbb{Q}(\sqrt{-2})$.

Lemma 15. *Let* $\mathrm{J}_1(18)$ *denote the Jacobian of* $\mathrm{X}_1(18)$*, and let* K *be a canonical divisor on* $\mathrm{X}_1(18)$*. The group* $\mathrm{J}_1(18)(\mathbb{Q})$ *is isomorphic to* $\mathbb{Z}/18\mathbb{Z}$*, and every element of* $\mathrm{J}_1(18)(\mathbb{Q})$ *is of the form* $[D-K]$ *with* D *an effective divisor of degree* 2 *supported on the cusps of* $\mathrm{X}_1(18)$*.*

Proof. This is proved in the same way as Lemma 13. The set of effective divisors of degree 2 supported at the cusps has $\binom{6+2-1}{2} + 4 = 25$ elements and splits up into the canonical linear equivalence class, consisting of 5 divisors, and 20 linear equivalence classes consisting of a single divisor. We deduce that the effective divisors of degree 2 supported at the cusps yield 21 rational points of $\mathrm{J}_1(18)$.

Again by 2-descent, $\mathrm{J}_1(18)$ has trivial 2-Selmer group, so $\mathrm{J}_1(18)(\mathbb{Q})$ is finite. In general, if A is an Abelian variety over a number field K and $\mathfrak{p} \mid p$ is a prime of

good reduction with $e(\mathfrak{p}/p) < p-1$, then reduction modulo $\mathfrak{p}$ is injective on the torsion of $A(K_\mathfrak{p})$; see for instance [17, Appendix]. Using this, we see that $\mathrm{J}_1(18)(\mathbb{Q})$ injects into $\mathrm{J}_1(18)(\mathbb{F}_5)$. One computes the zeta function of $\mathrm{X}_1(18)_{\mathbb{F}_5}$ as

$$Z(\mathrm{X}_1(18)_{\mathbb{F}_5}, t) = \frac{1-5t^2+25t^4}{(1-t)(1-5t)}.$$

Setting $t=1$ in the numerator, we see that $\mathrm{J}_1(18)$ has 21 points over $\mathbb{F}_5$. This proves that $\mathrm{J}_1(18)$ has no other rational points than the 21 found above. □

Proof of Theorem 9(3). In the same way as in Theorem 9(1), one proves that E has false complex multiplication by $\mathbb{Q}(\sqrt{-2})$, using Lemma 15 instead of Lemma 13. As in the proof of Theorem 9(1), we conclude that any quadratic point on $\mathrm{Y}_1(18)$ is the inverse image under the quotient map $\mathrm{Y}_1(18) \to \mathrm{Y}_1(18)/\iota$ of a $\mathbb{Q}$-rational point on $\mathrm{Y}_1(18)/\iota$.

The modular curve $\mathrm{Y}_1(18)$ can be rewritten as

$$v^2 = f(u) = u^6 + 2u^5 + 5u^4 + 10u^3 + 10u^2 + 4u + 1,$$
$$u(u+1)(u^2+u+1)(u^2-3u-1) = 0.$$

We conclude that for any quadratic point $y = (u, v) \in \mathrm{Y}_1(18)$, u has to be $\mathbb{Q}$-rational, and since $f(u) > 0$ for all $u \in \mathbb{R}$, this implies that v is a square root of a positive rational number and hence an element of a real quadratic field. □

4.7. **Torsion subgroup $\mathbb{Z}/22\mathbb{Z}$.** In this subsection, we will prove Theorem 9(4). Throughout this subsection we will denote the modular curve $\mathrm{X}_1(22)$ by C and its Jacobian by J. The genus of C is equal to 6; this fact will play a crucial role.

Unless stated otherwise, curves are assumed to be complete, smooth, and geometrically integral.

To prove Theorem 9(4), we will characterize the points on $\mathrm{Y}_1(22)$ that are defined over quartic number fields. One way of finding quartic points on $\mathrm{Y}_1(22)$ is by choosing a degree 4 morphism $C \to \mathbb{P}^1$. The fibers of rational points then consist of points defined over number fields of degree at most 4. Amongst other things, we will prove the following proposition.

Proposition 16. *Each non-cuspidal quartic point of C lies in a fiber of a rational point for some morphism $C \to \mathbb{P}^1$ of degree 4. Furthermore, each non-cuspidal point of C that lies in such a fiber has quartic field of definition.*

Along the way we will characterize all degree 4 morphisms $C \to \mathbb{P}^1$; the K-curve property in the theorem will then follow from this characterization.

The curve C parametrizes triples (E, P_2, P_{11}) with E a generalized elliptic curve, P_2 a point of order 2, and P_{11} a point of order 11. Let us mention that C has 20 cusps: 10 cusps defined over $\mathbb{Q}$, whose moduli correspond to Néron 11-gons and 22-gons, and 10 cusps defined over the quintic field $\mathbb{Q}(\zeta_{11} + \zeta_{11}^{-1})$, whose moduli correspond to Néron 1-gons and 2-gons.

Let ι be the following involution on C:

$$\iota\colon (E, P_2, P_{11}) \mapsto (E/\langle P_2\rangle, Q_2,\ 4P_{11} \bmod \langle P_2\rangle)\,,$$

where Q_2 is the generator of the isogeny dual to $E \to E/\langle P_2\rangle$.

Lemma 17. *The quotient $C/\langle\iota\rangle$ is isomorphic to an elliptic curve with 5 rational points.*

Proof. Put $\Lambda = \mathbb{Z} + \sqrt{-2}\mathbb{Z}$, $E = \mathbb{C}/\Lambda$, and $P_2 = \sqrt{-2}/2 \bmod \Lambda$. If P_{11} is $1/11 \pm 4/11\sqrt{-2} \bmod \Lambda$ or any multiple thereof, then (E, P_2, P_{11}) is a fixed point of ι. This gives 10 fixed points; the Riemann-Hurwitz formula now implies $g(C/\langle\iota\rangle) \leq 1$. If there were more fixed points, then $g(C/\langle\iota\rangle)$ would be 0 and thus C would

be hyperelliptic, which contradicts the fact that there are no elliptic curves over quadratic fields with a 22-torsion point.

The 10 rational cusps of C map down to 5 rational points on $C/\langle\iota\rangle$. The modular curve C has level 22, thus the quotient $C/\langle\iota\rangle$ is an elliptic curve of conductor dividing 22. According to [5, Table 1] there are 3 such elliptic curves; they all have conductor 11 and at most 5 rational points. □

Remark. The elliptic curve in question is in fact isomorphic to $\mathrm{X}_1(11)$, but we will not need this in the sequel.

A curve X that has a degree 2 morphism to an elliptic curve is called a *bi-elliptic* curve. An involution on X that gives such a morphism by dividing it out, is called a bi-elliptic involution. The so-called Castelnuovo–Severi inequality is useful in the study of bi-elliptic curves.

Proposition 18 (Castelnuovo–Severi inequality, [29, Theorem III.10.3])**.** *Let k be a perfect field, and let X, Y, and Z be curves over k. Let non-constant morphisms $\pi_Y\colon X \to Y$ and $\pi_Z\colon X \to Z$ be given, and let their degrees be m and n, respectively. Assume that there is no morphism $X \to X'$ of degree > 1 through which both π_Y and π_Z factor. Then the following inequality holds:*

$$g(X) \leq m{\cdot}g(Y) + n{\cdot}g(Z) + (m-1)(n-1).$$

Corollary 19. *Let k be a perfect field, and let X be a bi-elliptic curve over k of genus at least 6. Then X has a unique bi-elliptic involution ι. Furthermore, there are no non-constant morphisms $X \to \mathbb{P}^1$ of degree less than 4, and every degree 4 morphism $X \to \mathbb{P}^1$ factors through $X \to X/\langle\iota\rangle$.*

Proof. If there were two bi-elliptic involutions, ι and ι' say, then $\pi_Y\colon X \to X/\langle\iota\rangle$ and $\pi_Z\colon X \to X/\langle\iota'\rangle$ would contradict Proposition 18. For the other two assertions, apply Proposition 18 with $\pi_Y\colon X \to X/\langle\iota\rangle$ and π_Z any non-constant morphism $X \to \mathbb{P}^1$ of degree at most 4. □

So we see that the degree 4 morphisms $C \to \mathbb{P}^1$ are in bijection with the degree 2 morphisms $C/\langle\iota\rangle \to \mathbb{P}^1$.

If we identify morphisms to $\mathbb{P}^1$ whenever they differ by an automorphism of $\mathbb{P}^1$, then a degree 2 morphism $C/\langle\iota\rangle \to \mathbb{P}^1$ is given by a base-point-free linear system of divisors of degree 2 and dimension 1 on $C/\langle\iota\rangle$. Since $C/\langle\iota\rangle$ is an elliptic curve, any complete linear system of divisors of degree 2 is base-point-free and of dimension 1. These are in turn in bijection with the set $\mathrm{Pic}^2(C)$ of linear equivalence classes of degree 2 divisors on $C/\langle\iota\rangle$. An elliptic curve is its own Jacobian, so for any degree d the set $\mathrm{Pic}^d(C)$ is in bijection with $C/\langle\iota\rangle(\mathbb{Q})$, which consists of 5 points.

A quartic point on C defines a rational point on $\mathrm{Sym}^4 C$, and a morphism $C \to \mathbb{P}^1$ defines a closed immersion $\mathbb{P}^1 \rightarrowtail \mathrm{Sym}^4 C$. So the 5 degree 4 morphisms $C \to \mathbb{P}^1$ give us 5 copies of $\mathbb{P}^1$ in $\mathrm{Sym}^4 C$ that are defined over $\mathbb{Q}$. We wish to prove that all rational points of $\mathrm{Sym}^4 C$ outside these $\mathbb{P}^1$'s are supported on the cusps of C.

Fix any point of $C(\mathbb{Q})$; this gives us a morphism

$$\phi\colon \mathrm{Sym}^4 C \to J.$$

If D is an effective divisor of degree 4 on C, then the fiber $\phi^{-1}(\phi(D))$ is isomorphic to a projective space whose rational points form the complete linear system $|D|$ of effective divisors that are linearly equivalent to D.

Lemma 20. *Let k be a perfect field, and let X be a bi-elliptic curve over k of genus at least 6. Let D be a divisor on X of degree at most 4. Then the dimension of the*

complete linear system $|D|$ of divisors satisfies the following:

$$\dim |D| = \begin{cases} 1 & \text{if } D \text{ is a fiber of a degree 4 morphism } X \to \mathbb{P}^1; \\ 0 & \text{otherwise.} \end{cases}$$

In the former case, $|D|$ consists of all fibers of the same degree 4 morphism $X \to \mathbb{P}^1$.

Proof. Assume $|D|$ has positive dimension. Let Y be any subspace of $|D|$ of dimension 1, and let $F \leq D$ be the fixed divisor of Y. Subtracting F from all elements of Y, we obtain a base-point-free linear system of dimension 1 and degree $\deg(D - F)$ and thus a morphism $X \to \mathbb{P}^1$ of degree $\deg(D - F)$. By Corollary 19 we have $\deg D = 4$ and $F = 0$. Since linear systems of degree less than 4 over any algebraic extension of k have dimension 0, it follows that $\dim |D|$ cannot exceed 1. We thus have $Y = |D|$, and the last assertion is immediate. □

This lemma immediately implies that the five $\mathbb{P}^1$'s described above are fibers of ϕ and furthermore that outside these $\mathbb{P}^1$'s the rational points of $\operatorname{Sym}^4 C$ map injectively into $J(\mathbb{Q})$. It is thus interesting to know what $J(\mathbb{Q})$ looks like.

Lemma 21. *The Mordell–Weil rank of J is zero.*

Proof. Each isogeny factor of J is a modular Abelian variety A_f, where is a newform of $S_2(\Gamma_1(N))$ with $N \mid 22$. We must prove that these A_f all have Mordell–Weil rank 0. There are two such A_f: one for the unique newform of level 11 and one for the unique newform of level 22. For f of level 11 we have $A_f = \mathrm{J}_1(11)$, which is an elliptic curve with 5 rational points. For f of level 22, proven instances of the Birch–Swinnerton-Dyer Conjecture [16, Corollary 14.3] ensure us that $\operatorname{rk} A_f(\mathbb{Q}) = 0$ if $L(f, 1) \neq 0$. Symbolic methods involving modular symbols can be used to verify $L(f, 1) \neq 0$ (see for instance [27, Section 3.10]); it turns out that this is indeed the case here. □

To further study the Diophantine properties of $\operatorname{Sym}^4 C$ and J, we will use reduction modulo 3; this will enable us to prove Proposition 16. In general, if A is an Abelian variety over a number field K and $\mathfrak{p} \mid p$ is a prime of good reduction with $e(\mathfrak{p}/p) < p - 1$, then reduction modulo $\mathfrak{p}$ is injective on the torsion of $A(K_\mathfrak{p})$; see for instance [17, Appendix]. For us this means that $J(\mathbb{Q})$ injects into $J(\mathbb{F}_3)$.

Proof of Proposition 16. We can compute the zeta function of $C_{\mathbb{F}_3}$, either by direct point counting over extensions of $\mathbb{F}_3$ or by expressing the Frobenius action on the Tate module in terms of the Hecke operator T_3, and find

$$Z(C_{\mathbb{F}_3}, t) = \frac{P(t)}{(1 - t)(1 - 3t)}$$

with

$$P(t) = (1 + t + 3t^2)^2 \cdot (1 + 4t + 3t^2 - 10t^3 - 29t^4 - 30t^5 + 27t^6 + 108t^7 + 81t^8).$$

The 10 rational cusps of C reduce to distinct points of $C(\mathbb{F}_3)$. If we expand $Z(C_{\mathbb{F}_3}, t)$ as a power series, then the coefficient of t^d is equal to the number of effective divisors of degree d on $C_{\mathbb{F}_3}$. So from

$$Z(C_{\mathbb{F}_3}, t) = 1 + 10t + 55t^2 + 220t^3 + 720t^4 + O(t^5)$$

we can immediately read off that all points of $C(\mathbb{F}_3)$ are cusps. The number of unordered n-tuples of cusps is $\binom{10+n-1}{n}$, which is equal to 55, 220, and 715 for $n = 2, 3, 4$, respectively. It follows that all divisors of degree 2 and 3 are supported on the cusps and that there are precisely 5 divisors of degree 4 that are not supported on the cusps.

We will now show that these 5 points of $\mathrm{Sym}^4(C)(\mathbb{F}_3)$ are in the non-trivial fibers of $\mathrm{Sym}^4(C) \to J$. This would immediately imply that all points of $\mathrm{Sym}^4(C)(\mathbb{Q})$ outside these fibers are cuspidal, because of the injectivity of $\mathrm{Sym}^4(\mathbb{Q}) \to J(\mathbb{F}_3)$ outside these fibers. To do this, we can simply count the number of non-cuspidal points in the non-trivial fibers over $\mathbb{F}_3$. Let a morphism $C \to \mathbb{P}^1$ of degree 4 be given. The proof of Lemma 17 implies that the 10 cusps of C are mapped to $\mathbb{P}^1$ in fibers of 4, 4, and 2 points, respectively. Hence, in each of the 5 rational projective lines that we have in $\mathrm{Sym}^4(C)$, there are precisely 3 points supported on the cusps. Over $\mathbb{F}_3$ these lines have $\#\mathbb{P}^1(\mathbb{F}_3) = 4$ rational points, thus each of the 5 lines has exactly 1 non-cuspidal point, giving us 5 points in total. □

Corollary 22. *Each point on C with quartic field of definition maps to a point of $C/\langle\iota\rangle$ that is defined over a quadratic field.* □

Proof of Theorem 9(4). Let (E, P_2, P_{11}) be the universal elliptic curve with points of order 2 and 11 over $\mathrm{Y}_1(22)$. The construction in Subsection 4.2 gives us an isogeny $\mu\colon \iota^*(E, P_2, P_{11}) \to (E, 0, 8P_{11})$ of degree 2. From this we obtain an isomorphism

$$\mu \circ \iota^*\mu\colon (E, P_{11}) \xrightarrow{\sim} (E, 8^2 P_{11}) = (E, -2P_{11}).$$

Let P be a point of $\mathrm{Y}_1(22)$ defined over a quartic number field L. From the above it follows that there is a degree 4 morphism $C \to \mathbb{P}^1$ mapping P to a rational point and thus that P lies above a point of $C/\langle\iota\rangle$ defined over a quadratic number field K that is necessarily a subfield of L. The results from Subsection 4.2 now immediately imply that the elliptic curve E associated with P is a K-curve with false complex multiplication by $\mathbb{Q}(\sqrt{-2})$. □

5. Applications to elliptic curves over finite fields

Finding elliptic curves with positive rank and large torsion over number fields is not just a curiosity. As mentioned in the introduction, elliptic curves with large torsion and positive rank over the rationals have long been used for factorization, starting with Montgomery [23], Atkin and Morain [1]. In this section we argue that examining the torsion of an elliptic curve over number fields of small degree is beneficial in addition to examining the rational torsion.

A nice explicit example of the factorization of large numbers (Cunningham numbers in this case) using elliptic curves over number fields of small degree can be found in [4]. The authors used elliptic curves over cyclotomic fields with torsion groups $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. Also, they tried to construct elliptic curves over cyclotomic fields with torsion $\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ and positive rank (see [4, 4.4 and 4.5]), but failed. Note that one can find such curves in Theorem 8.

Theorem 23. *Let m and n be positive integers such that m divides n. Let E be an elliptic curve over $\mathbb{Q}$, let p be a prime number not dividing n such that E has good reduction at p, and let d be a positive integer. Suppose there exists a number field K such that $E(K)$ contains a subgroup isomorphic to $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ and such that K has a prime of residue characteristic p and inertia degree dividing d. Then $E(\mathbb{F}_{p^d})$ contains a subgroup isomorphic to $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$.*

Proof. This follows from the fact that the n-torsion of $E(K)$ reduces injectively modulo any prime of good reduction that does not divide n; see for example [26, VII, Proposition 3.1]. □

We can apply Theorem 23 with a fixed number field K, such as the splitting field of $E[n]$. Then Chebotarev's density theorem gives a lower bound for the density of the set of primes p such that $E(\mathbb{F}_p)$ contains a subgroup isomorphic to $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$.

The relevance for the elliptic curve factoring method is as follows. One looks for elliptic curves over fields of small degree having a given torsion subgroup G. If E is such a curve, then $E(\mathbb{F}_p)$ contains a subgroup isomorphic to G for a large density of primes p. We say that an integer m is *n-smooth* for some fixed value of n if all the prime divisors of m are less than or equal to n. As mentioned in the introduction, for the elliptic curve factoring method, one wants to choose elliptic curves E such that $|E(\mathbb{F}_p)|$ is smooth for many p.

The standard heuristic is that the larger the torsion subgroup T of $E(\mathbb{Q})$, the greater the probability that $|E(\mathbb{F}_p)|$ is smooth. This is because T injects into $E(\mathbb{F}_p)$ for all primes p of good reduction that do not divide $|T|$, making $|E(\mathbb{F}_p)|$ divisible by $|T|$. However, this heuristic is too simplistic, as a curve with smaller $E(\mathbb{Q})_{\text{tors}}$ can have much larger torsion over fields of small degree, giving altogether a greater probability of $|E(\mathbb{F}_p)|$ to be smooth. We give an example of this phenomenon.

Example 1. One can use [10, Theorem 4.14] (using $t = 3$) to obtain an elliptic curve over $\mathbb{Q}$ with torsion $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ over the field $K = \mathbb{Q}(\sqrt{-3}, \sqrt{217})$ and torsion $\mathbb{Z}/6\mathbb{Z}$ over $\mathbb{Q}$. The curve is:

$$E_1 : y^2 = x^3 - 17811145/19683x - 81827811574/14348907.$$

For example, 61, 67, and 73 are primes of good reduction that completely split in K, so the complete torsion group of $E(K)$ injects into the finite fields with 61, 67, and 73 elements. One easily checks that the curve has 72 points over all the fields and that the groups are isomorphic to $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$. Now take

$$E_2 : y^2 = x^3 - 25081083x + 44503996374.$$

The torsion of $E_2(\mathbb{Q})$ is isomorphic to $\mathbb{Z}/7\mathbb{Z}$, implying that by standard heuristics (examining only the rational torsion), $|E_2(\mathbb{F}_p)|$ should be more often smooth than $|E_1(\mathbb{F}_p)|$. Note that both curves have rank 1 over $\mathbb{Q}$, so the rank should not play a role.

We examine how often $|E_1(\mathbb{F}_p)|$ and $|E_2(\mathbb{F}_p)|$ are 100-smooth and 200-smooth if p runs through the first 1000, 10000, and 100000 primes, excluding the first ten primes to get rid of the primes of bad reduction. For comparison, we also take the elliptic curve

$$E_3 : y^2 = x^3 + 3,$$

with trivial torsion group and rank 1. In the following table, p_n denotes the n-th prime number.

	$30 < p < p_{1010}$	$30 < p < p_{10010}$	$30 < p < p_{100010}$
#100-smooth $\lvert E_1(\mathbb{F}_p)\rvert$	812	4843	22872
#100-smooth $\lvert E_2(\mathbb{F}_p)\rvert$	768	4302	20379
#100-smooth $\lvert E_3(\mathbb{F}_p)\rvert$	553	2851	12344
#200-smooth $\lvert E_1(\mathbb{F}_p)\rvert$	903	6216	35036
#200-smooth $\lvert E_2(\mathbb{F}_p)\rvert$	877	5690	32000
#200-smooth $\lvert E_3(\mathbb{F}_p)\rvert$	699	4134	21221

We see that, contrary to what one would expect if examining only the rational torsion, E_1 is consistently more likely to be smooth than E_2. Why does this happen? Examine the behavior of the torsion of $E_1(K)$ and $E_2(K)$ as K varies through all quadratic fields. The torsion of $E_2(K)$ will always be $\mathbb{Z}/7\mathbb{Z}$ (see [7, Theorem 2]), while $E_1(\mathbb{Q}(\sqrt{-3}))_{\text{tors}} \simeq \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ and $E_1(\mathbb{Q}(\sqrt{217}))_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$. One fourth of the primes will split in $\mathbb{Q}(\sqrt{-3})$ and not in $\mathbb{Q}(\sqrt{217})$, one fourth vice versa, one fourth will split in neither field, and one fourth will split in both fields (and thus splitting completely in $\mathbb{Q}(\sqrt{-3}, \sqrt{217})$). This implies that $|E_1(\mathbb{F}_p)|$ is divisible

by 6, 12, 18, and 36, each for one fourth of the primes, while all we can say for $|E_2(\mathbb{F}_p)|$ is that it is divisible by 7. We also see that $|E_3(\mathbb{F}_p)|$ is much less likely to be smooth than both E_1 and E_2.

Note that these curves are by no means special; a similar result will be obtained if one chooses three other elliptic curves defined over $\mathbb{Q}$ of the same type, one with torsion $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ over a quartic field, one with torsion $\mathbb{Z}/7\mathbb{Z}$ over $\mathbb{Q}$, and one with trivial torsion over the rationals.

6. Examples of curves with prescribed torsion

The tables are arranged as follows. In the first column we give a pair (m, n), meaning that the given elliptic curve has torsion isomorphic to $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$. In Table 1, the second column contains a squarefree integer d indicating the base field $\mathbb{Q}(\sqrt{d})$. In all other tables, the second column contains an irreducible polynomial $f \in \mathbb{Q}[x]$ defining the base field, and w denotes a root of f. The curve is given in the third column, either by a quintuple $(a_1, a_2, a_3, a_4, a_6)$ representing a curve in long Weierstrass form or by a pair (a, b) representing a curve in Tate form $y^2 + axy + by = x^3 + bx^2$.

Table 1. Curves with prescribed torsion and rank 0 over quadratic fields.

(m, n)	d	Curve
$(1, 1)$	-1	$(0, 0, 0, 0, 6)$
$(1, 2)$	5	$(0, 0, 0, 1, 0)$
$(1, 3)$	-2	$(0, 0, 0, 0, 4)$
$(1, 4)$	-2	$(1, \frac{1}{8})$
$(1, 5)$	-1	$(-2, -3)$
$(1, 6)$	-1	$(-2, -12)$
$(1, 7)$	-1	$(-1, 2)$
$(1, 8)$	-2	$(7, -6)$
$(1, 9)$	-2	$(3, 6)$
$(1, 10)$	-2	$(-5, -24)$
$(1, 11)$	2	$(\sqrt{2} + 1, -\sqrt{2} + 2)$
$(1, 12)$	-3	$(43, -210)$
$(1, 13)$	17	$(2\sqrt{17} - 9, 18\sqrt{17} - 74)$
$(1, 14)$	-7	$(\sqrt{-7} + 2, \sqrt{-7} + 5)$
$(1, 15)$	5	$(3, 2)$
$(1, 16)$	70	$(-\frac{31}{5}, -\frac{18}{25})$
$(1, 18)$	33	$(6 + \sqrt{33}, -5 - \sqrt{33})$
$(2, 2)$	-1	$(0, 0, 0, 1, 0)$
$(2, 4)$	-3	$(1, \frac{1}{18})$
$(2, 6)$	-3	$(\frac{11}{10}, \frac{9}{100})$
$(2, 8)$	-3	$(-\frac{23}{7}, -\frac{30}{49})$
$(2, 10)$	-2	$(-\frac{7}{2}, -\frac{9}{2})$
$(2, 12)$	6	$(\frac{29}{27}, \frac{50}{729})$
$(3, 3)$	-3	$(1, -1, 0, 12, 8)$
$(3, 6)$	-3	$(\frac{9}{8}, \frac{7}{64})$
$(4, 4)$	-1	$(1, \frac{15}{256})$

TABLE 2. Curves with prescribed torsion and rank 0 over cubic fields.

(m,n)	f	Curve
$(1,1)$	x^3+x^2+2	$(0,0,0,0,-3)$
$(1,2)$	x^3+x^2+10	$(0,0,0,1,0)$
$(1,3)$	x^3+x^2+x-1	$(0,0,0,0,4)$
$(1,4)$	x^3+x^2-1	$(1,\frac{1}{2})$
$(1,5)$	x^3+x+1	$(-2,-3)$
$(1,6)$	x^3+2	$(\frac{4}{3},\frac{2}{9})$
$(1,7)$	x^3+x+1	$(-1,-4)$
$(1,8)$	x^3+2x^2+1	$(-\frac{1}{2},-3)$
$(1,9)$	x^3+2x^2+1	$(-3,-12)$
$(1,10)$	x^3+x^2+3	$(-5,-24)$
$(1,11)$	x^3-x^2-2	$(-2w^2+2w+3,2w^2-2w-2)$
$(1,12)$	x^3+2	$(43,-210)$
$(1,13)$	x^3-x-2	$(-w^2-w-1,-w^2+w+2)$
$(1,14)$	x^3-x-2	$(-1,-4)$
$(1,15)$	x^3+2x-1	$\left(\frac{w^2-2w+3}{2},\frac{-2w^2-w+1}{2}\right)$
$(1,16)$	x^3-x^2+2x+8	$(-4w-5,-7w^2-3w+10)$
$(1,18)$	x^3+3x-2	$(-3,-12)$
$(1,20)$	x^3-x^2-2x-2	$\left(\frac{-5w^2-w}{2},-14w^2-12w-8\right)$
$(2,2)$	x^3+2	$(0,0,0,-1,0)$
$(2,4)$	x^3+2	$(1,-\frac{1}{2})$
$(2,6)$	x^3+2	$(\frac{5}{2},-\frac{3}{4})$
$(2,8)$	x^3+2	$(\frac{17}{2},-15)$
$(2,10)$	x^3-x^2-1	$(-5w^2-3w-3,-5w^2-3w-4)$
$(2,12)$	x^3-2x-2	$\left(\frac{12w^2+24w+17}{2},\frac{-309w^2-546w-348}{4}\right)$
$(2,14)$	x^3+2x^2-9x-2	$(3w^2-7w-1,-55w^2+115w+26)$

TABLE 3. Curves with prescribed torsion and rank 0 over quartic fields.

(m,n)	f	Curve
$(1,1)$	x^4+8x^2+4	$(0,0,0,0,6)$
$(1,2)$	x^4+3x^2+1	$(0,0,0,1,0)$
$(1,3)$	x^4-2x^2+4	$(0,0,0,0,4)$
$(1,4)$	x^4-3x^2+4	$(1,-2)$
$(1,5)$	x^4+3x^2+1	$(-2,-3)$
$(1,6)$	x^4+3x^2+1	$(-2,-12)$
$(1,7)$	x^4-3x^2+4	$(-1,-4)$
$(1,8)$	x^4+26x^2+49	$(7,-6)$
$(1,9)$	x^4-7x^2+4	$(3,6)$
$(1,10)$	x^4-x^2+1	$(-5,-24)$
$(1,11)$	x^4+2x^2+4	$(-w^3-1,-3w^3-8)$
$(1,12)$	x^4-x^2+1	$(43,-210)$
$(1,13)$	x^4-38x^2+225	$\left(\frac{w^3-53w-135}{15},\frac{3w^3-159w-370}{5}\right)$
$(1,14)$	x^4-3x^2+4	$(-2w^2+5,-2w^2+8)$
$(1,15)$	x^4-x^2+4	$(3,2)$
$(1,16)$	x^4+9x^2+9	$(-\frac{7}{5},-\frac{12}{25})$
$(1,17)$	$x^4-x^3+x^2-5x-4$	$\left(\frac{5w^3-12w^2+9w-40}{4},-4w^3+2w^2-10w+12\right)$
$(1,18)$	x^4+17x^2+64	$(2w^2+23,-2w^2-22)$
$(1,20)$	$x^4-2x^3+x^2+2$	$(-5,-24)$
$(1,21)$	x^4-x^3+2x-8	$\left(\frac{-w^3-6w^2-26w+80}{8},\frac{-53w^3+118w^2-154w+200}{2}\right)$
$(1,22)$	$x^4-2x^3-x^2+2x+8$	$\left(\frac{w^3-12w^2+31w-20}{8},3w^3-13w^2+18w-4\right)$
$(1,24)$	x^4-18x^2-15	$(1,\frac{8}{3})$
$(2,2)$	x^4+3x^2+1	$(0,0,0,1,0)$
$(2,4)$	x^4-3x^2+4	$(1,\frac{1}{18})$
$(2,6)$	x^4+2x^2+4	$(\frac{5}{2},\frac{3}{4})$
$(2,8)$	x^4+6x^2+4	$(-\frac{7}{3},-10)$
$(2,10)$	x^4+18x^2+25	$(-\frac{7}{2},-\frac{9}{2})$
$(2,12)$	x^4+9x^2+9	$(1,\frac{8}{3})$
$(2,14)$	$x^4-x^3+3x^2+3x+2$	$(w^3-2w^2+3w+3,w^3-2w^2+3w+6)$
$(2,16)$	$x^4+2002x^2+116281$	$\left(\frac{2329}{2695},-\frac{366}{2401}\right)$
$(2,18)$	x^4-x^2-8	$(2w^2+5,-2w^2-4)$
$(3,3)$	x^4-x^2+4	$(1,-1,0,12,8)$
$(3,6)$	x^4-x^2+4	$(\frac{9}{8},\frac{7}{64})$
$(3,9)$	x^4+294x^2+2601	$\left(\frac{11w^2+129}{24},\frac{269w^2+2463}{24}\right)$
$(4,4)$	x^4+1	$(1,\frac{1}{8})$
$(4,8)$	$x^4+541x^2+72900$	$\left(\frac{431}{690},-\frac{259}{529}\right)$
$(5,5)$	$x^4+x^3+x^2+x+1$	$(-10,-11)$
$(6,6)$	x^4+5x^2+1	$(\frac{9}{8},\frac{7}{64})$

TABLE 4. Curves with prescribed torsion and positive rank over quadratic fields.

(m,n)	f or d	Curve	Independent points of infinite order
$(1,15)$	x^2-x-86	$\left(\frac{10w+493}{448},\frac{10w+45}{448}\right)$	$\left(\frac{-w-274}{3584},\frac{-2455w-20382}{200704}\right)$
$(1,18)$	$x^2+163x+12$	$\left(\frac{25105w+2071}{216},\frac{634768555w+46752805}{7776}\right)$	$\left(\frac{3673w+223}{486},\frac{150110959w+11056609}{8748}\right)$, $\left(\frac{-112579w-8293}{6},\frac{-3011095399w-221775913}{288}\right)$
$(2,10)$	55325286553	$\left(-\frac{1001929453}{87419475},-\frac{1089348928}{87419475}\right)$	$\left(-\frac{76249664}{9062625},-\frac{3294239461376}{55961709375}\right)$, $\left(-\frac{1378903694270734}{47323818070815},-\frac{233856747339051186962702}{6331823076742017702705}\right)$, $\left(-\frac{317897024}{55559933},-\frac{54763043233792}{3408435209751}\right)$, $\left(-\frac{10158696384}{631362875},-\frac{66880771114752}{779733150625}\right)$
$(2,12)$	2947271015	$\left(\frac{1024873209359}{27734204981},-\frac{543206429719981170}{2187369012646489}\right)$	rank ≥ 4, see [6]

TABLE 5. Curves with prescribed torsion and positive rank over cubic fields.

(m,n)	f	Curve	Independent points of infinite order
$(1,11)$	x^3-x^2-12	$\left(\frac{-3w^2+3w-8}{4},-3w^2+3w-12\right)$	$(2w^2-2w,3w^2+15w-30)$, $\left(4w^2+6w+14,\frac{-29w^2-35w-116}{2}\right)$
$(1,13)$	$x^3-x^2-2x-24$	$\left(\frac{-w^2-3w+3}{3},\frac{-5w^2-5w-24}{3}\right)$	$\left(\frac{12w^2+10w+30}{9},\frac{20w^2+88w+516}{27}\right)$
$(1,15)$	x^3+x^2-2x-6	$\left(\frac{7w^2+20w-58}{8},\frac{7w^2+20w-66}{8}\right)$	$\left(5w^2+4w-24,\frac{21w^2+108w-270}{2}\right)$
$(1,16)$	x^3-5x^2+8	$\left(\frac{-w^2-2w+2}{2},-4w^2-w+4\right)$	$\left(\frac{173w^2-62w-296}{2},\frac{8039w^2-3000w-13896}{2}\right)$
$(1,20)$	$x^3-17x-6$	$\left(\frac{3w^2-3w-118}{80},\frac{75w^2+114w-1872}{320}\right)$	$\left(\frac{-21w^2-33w+522}{64},\frac{351w^2+414w-8316}{1280}\right)$
$(2,10)$	x^3-x^2-3	$\left(\frac{-5w^2+2w-1}{5},\frac{-42w^2-42w-81}{25}\right)$	$\left(\frac{9w^2-3w+18}{5},\frac{30w^2+6w+27}{5}\right)$
$(2,12)$	x^3-x^2+x-16	$\left(1,\frac{-532w^2+27560w-106048}{88209}\right)$	$\left(\frac{38w^2-10w+512}{243},\frac{1566w^2+2810w+7264}{6561}\right)$
$(2,14)$	$x^3-x^2-166x-536$	$\left(\frac{7w^2+108w+322}{26},\frac{-631w^2-8667w-22964}{169}\right)$	$\left(\frac{315061w^2+4358637w+11743820}{3237013},\frac{-289420914w^2-3975201306w-10528526328}{42081169}\right)$

TABLE 6. Curves with prescribed torsion and positive rank over quartic fields.

(m,n)	f	Curve	Independent points of infinite order
$(1,17)$	$x^4-2x^3+2x^2+2x-4$	$(-w^3+w^2+2w-1,3w^3-6w^2-2w+6)$	$(-w^3+2w^2+2w-2,2w^3-4w^2-4w+4)$
$(1,21)$	$x^4-x^3-2x^2+10x-4$	$\left(\frac{-2w^3+7w^2-23w+17}{7},\frac{-135w^3+440w^2-715w+246}{7}\right)$	$\left(\frac{8w^3-23w^2+35w-4}{7},\frac{-190w^3+610w^2-984w+316}{7}\right)$
$(3,9)$	x^4-2x^2+4	$(w^3-5w^2+8w-3,28w^3-59w^2+32w+20)$	$(-w^2+4w-4,32w^3-32w^2-52w+96)$
$(4,8)$	x^4-3x^2+4	$(\frac{17}{2},-15)$	$(\frac{5}{2},\frac{25w^2-50}{4})$
$(5,5)$	$x^4+x^3+x^2+x+1$	$(-\frac{88}{93},-\frac{181}{93})$	$(\frac{2}{3},\frac{7}{3})$

References

[1] A. O. L. Atkin, F. Morain, *Finding suitable curves for the elliptic curve method of factorization*, Math. Comp. **60** (1993), 399–405.

[2] S. Bosch, W. Lütkebohmert, M. Raynaud, *Néron Models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) **21**, Springer-Verlag, Berlin, 1990.

[3] W. Bosma, J. J. Cannon, C. Fieker, A. Steel (eds.), Handbook of Magma functions, Edition 2.18 (2011).

[4] É. Brier, C. Clavier, *New families of ECM curves for Cunningham numbers*. in: Proceedings of ANTS IX, Lecture Notes in Comput. Sci. **6197**, Springer, Heidelberg, 2010, pp. 96–109.

[5] J. E. Cremona, *Algorithms for modular elliptic curves*, second edition, Cambridge University Press, Cambridge, 1997.

[6] A. Dujella, High rank elliptic curves with prescribed torsion, `http://web.math.hr/~duje/tors/tors.html`.

[7] Y. Fujita, *Torsion subgroups of elliptic curves in elementary abelian 2-extensions of* $\mathbb{Q}$, J. Number Theory **114** (2005), 124–134.

[8] D. Goldfeld, *Conjectures on elliptic curves over quadratic fields*, in: Number Theory, Carbondale 1979, Lecture Notes in Math. **751**, Springer, Berlin, 1979, pp. 108–118.

[9] D. Jeon, C. H. Kim, Y. Lee, *Families of elliptic curves over cubic number fields with prescribed torsion subgroups*, Math. Comp. **80** (2011), 579–591.

[10] D. Jeon, C. H. Kim, Y. Lee, *Families of elliptic curves over quartic number fields with prescribed torsion subgroups*, Math. Comp. **80** (2011), 2395–2410.

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

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

[13] M. Jukić Bokun, *On the rank of elliptic curves over* $\mathbb{Q}(\sqrt{-3})$ *with torsion groups* $\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/3\mathbb{Z}$ *and* $\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/6\mathbb{Z}$, Proc. Japan Acad. Ser. A Math Sci. **87** (2011), 61–64.

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

[15] S. Kamienny, F. Najman, *Torsion groups of elliptic curves over quadratic fields*, Acta Arith., to appear.

[16] K. Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, in: Cohomologies p-adiques et applications arithmétiques (III), Astérisque **295** (2004), 117–290.

[17] N. M. Katz, *Galois properties of torsion points on Abelian varieties*, Invent. Math. **62** (1981), 481–502.

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

[19] H. W. Lenstra, Jr., *Factoring integers with elliptic curves*, Ann. of Math. **126** (1987), 649–673.

[20] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. **47** (1977), 33–186.

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

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

[23] P. L. Montgomery, *Speeding the Pollard and elliptic curve methods of factorization*, Math. Comp. **48** (1987), 243–264.

[24] The PARI-group, *PARI/GP mathematics software (version 2.5.0)*, Bordeaux, 2011, `http://pari.math.u-bordeaux.fr/`.

[25] F. P. Rabarison, *Structure de torsion des courbes elliptiques sur les corps quadratiques*, Acta Arith. **144** (2010), 17–52.

[26] J. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, Springer-Verlag, New York, 1986.

[27] W. A. Stein, *Explicit approaches to modular abelian varieties*, Ph.D. thesis, University of California, Berkeley (2000).

[28] W. A. Stein et al., *Sage mathematics software (version 4.7.2)*, The Sage Development Team, 2011, `http://www.sagemath.org/`.

[29] H. Stichtenoth, *Algebraic function fields and codes*, Universitext, Springer-Verlag, Berlin, 1993.

[30] Y. Yang, *Defining equations of modular curves*, Adv. Math. **204** (2006), 481–508.

Mathematics Institute, University of Warwick, Coventry CV4 7AL, United Kingdom
E-mail address: J.Bosman@warwick.ac.uk

Institut für Mathematik, Universität Zürich, Winterthurerstrasse 190, 8057 Zürich, Switzerland
E-mail address: peter.bruin@math.uzh.ch

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

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