Torsion of elliptic curves over cubic fields

Filip Najman

Abstract

Although it is not known which groups can appear as torsion groups of elliptic curves over cubic number fields, it is known which groups can appear for infinitely many non-isomorphic curves. We denote the set of these groups as S. In this paper we deal with three problems concerning the torsion of elliptic curves over cubic fields. First, we study the possible torsion groups of elliptic curves that appear over the field with smallest absolute value of its discriminant and having Galois group S_3 and over the field with smallest absolute value of its discriminant and having Galois group $\mathbb{Z}/3\mathbb{Z}$. Secondly, for all except two groups $G \in S$, we find the field K with smallest absolute value of its discriminant such that there exists an elliptic curve over K having G as torsion. Finally, for every $G \in S$ and every cubic field K we determine whether there exists infinitely many non-isomorphic elliptic curves with torsion G.

Keywords Torsion Group, Elliptic Curves, Cubic Fields
Mathematics Subject Classification (2010) 11G05, 11G18, 11R16, 14H52

1 Introduction.

The possible torsion groups of an elliptic curve over the rational numbers are known by a theorem of Mazur, who actually gave two different proofs of the theorem [13] and [14]. These groups are:

$$\mathbb{Z}/n\mathbb{Z},\ n = 1, \ldots, 10, 12,$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 1, \ldots, 4.$$

In a similar manner all the possible torsion groups over the collection of all quadratic fields were determined by Kenku and Momose [11] and Kamienny [8]. The author determined the possible torsion groups over the quadratic cyclotomic fields $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-3})$ [17, 18], which are also the two quadratic fields with the smallest discriminant.

It was proven by Parent [21, 22] that 13 is the largest prime that can divide the order of the torsion of an elliptic curve over a cubic field. Jeon, Kim and Schweizer [5] found all the groups that appear as torsion for infinitely many non-isomorphic curves over cubic fields. These are the following groups:

$$\mathbb{Z}/n\mathbb{Z},\ n = 1, \ldots, 16, 18, 20,$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z},\ n = 1, \ldots 7$$

We denote the set of the above groups as S. Unfortunately, it is not known whether there are other groups that appear as torsion for only finitely many curves. For a cubic field K, we will denote by $T(K)$ the set of all groups that appear as torsion of an elliptic curve over K but are not contained in the set S. Note that the union of all $T(K)$ over all cubic fields is still a finite set, and one could use [20] to give an effective bound. But this bound would be huge and would not be of help for practical purposes.

Since over the rationals and over quadratic fields all the groups that appear as torsion, do so for infinitely many curves, the possibility that $T(K)$ is empty for all cubic fields is not unreasonable.

In this paper we focus more on the torsion of elliptic curves over a single cubic field (as opposed to looking at all cubic fields simultaneously). We deal with three problems:

1) Determine the possible torsion groups of an elliptic curve over the field with smallest discriminant and having Galois group S_3 and over the field with smallest discriminant and having Galois group $\mathbb{Z}/3\mathbb{Z}$.

2) Find for every group from S the field with the smallest discriminant having it as a torsion of an elliptic curve,

3) Determine for how many non-isomorphic curves does each of the groups from S appear as torsion for any fixed cubic field K.

Note that a similar problem to 1) was solved by the author in [17, 18] for quadratic fields. The analogues of 2) and 3) for quadratic fields were dealt with successfully by Kamienny and the author in [9].

We succeed in 1) under the assumptions that $T(K)$ is empty for these fields K. We also eliminate some possibilities for $T(K)$.

We succeed in 2) for all the groups except for $\mathbb{Z}/20\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$. The reason we fail for these groups is that the modular curves X_1 corresponding to these groups are non-hyperelliptic of genus 3 and 4, and thus it is extremely hard to determine the existence of a cubic point on them.

We solve problem 3) completely. When counting curves throughout this paper, we will always count them up to isomorphisms.

Although we follow the general strategy of [9] and [18] to handle these problems, since the problems are much harder over cubic than over quadratic fields, we will use various other methods, not previously used in [9, 18].

2 Torsion over cubic fields with smallest discriminant

As we will be mentioning certain cubic fields many times in the remainder of the paper, for the convenience of the reader we list the first seven cubic fields (taken from [7]) ordered by ascending absolute value of the discriminant in the table below. In the table, i is the position of the field in the table, Δ the discriminant of the field, G its Galois group (the Galois group of its normal closure, to be precise) and in the last column in the table is the generating polynomial of the field.

i	Δ	G	Polynomial
1	-23	S_3	$x^3 - x^2 + 1$
2	-31	S_3	$x^3 + x - 1$
3	-44	S_3	$x^3 - x^2 + x + 1$
4	49	$\mathbb{Z}/3\mathbb{Z}$	$x^3 - x^2 - 2x + 1$
5	-59	S_3	$x^3 + 2x - 1$
6	-76	S_3	$x^3 - 2x - 2$
7	81	$\mathbb{Z}/3\mathbb{Z}$	$x^3 - 3x - 1$

Table 1.

We will denote the i-th field in the table as K_i. We will focus on two fields, K_1 and K_4. The field K_1 is the cubic field with the smallest discriminant, while K_4 is both the field with smallest discriminant having $\mathbb{Z}/3\mathbb{Z}$ as a Galois group and the totally real field with smallest discriminant. Note that both fields have class number 1 and that K_4 is the maximal real subfield of the cyclotomic field $\mathbb{Q}(\zeta_7)$. By α_i we denote the element generating K_i.

Let K be a number field. Denote by $Y_1(m,n)$ the affine modular curve whose K-rational points classify isomorphism classes of triples (E, P_m, P_n), where E is an elliptic curve (over K) and P_m and P_n are torsion points (over K) which generate a subgroup isomorphic to $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$. For simplicity, we write $Y_1(n)$ instead of $Y_1(1,n)$. Let $X_1(m,n)$ be the compactification of the curve $Y_1(m,n)$ obtained by adjoining its cusps.

Similarly, let $Y_0(N)$ be the affine curve whose K-rational points classify isomorphism classes of pairs (E, C), where E is an elliptic curve and C is a

cyclic $Gal(\overline{K}/K)$-invariant subgroup of $E(\overline{K})$ of order N, or a *N-cycle*. We obtain $X_0(N)$ by adjoining the cusps to $Y_0(N)$.

Nice models of the curves $X_0(n)$ and $X_1(n)$ can be found for example in [1, 25], while the curves $X_1(2,10)$ and $X_1(2,12)$ can be found in [23].

We will use *division polynomials* in many places in this paper. For a definition and more information on division polynomials see [24]. We denote by ψ_n the n-th division polynomial, which satisfies that, for a point P on an elliptic curve in Weierstrass form, $\psi_n(x(P)) = 0$ if and only if $nP = 0$. Note that for even n one has to work with ψ_n/ψ_2 to get a polynomial only in one variable.

We do our rank and torsion computations on elliptic curves and Jacobians of genus 2 curves throughout this paper using MAGMA.

We first prove a useful lemma.

Lemma 1. *If the torsion group of an elliptic curve E over $\mathbb{Q}$ has a nontrivial 2-Sylow subgroup, then over any number field of odd degree the torsion of E will have the same 2-Sylow subgroup as over $\mathbb{Q}$.*

Proof. Let K be a number field of odd degree. If $E(\mathbb{Q}) \simeq \mathbb{Z}/2nZ$, then the rest of the 2-torsion is defined over a quadratic field and hence not over K. So if the 2-Sylow group increases there must be a K-rational (but not $\mathbb{Q}$-rational) point P such that $2P = Q$, where $Q \in E(\mathbb{Q})$ is a nontrivial torsion point whose order is a power of 2. But for fixed Q the equation $2P = Q$ has exactly 4 solutions and it is easy to see that the orbits under the action of $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ can only have lengths of 2 or 4. □

Theorem 2. *Let T be a torsion group from Mazur's theorem and K a cubic number field. There exist infinitely many elliptic curves with torsion T over K.*

Proof. First note that by [5, Theorem 3.2] there are infinitely many elliptic curves over $\mathbb{Q}$ with each of the torsion groups from Mazur's theorem.

Let K be a fixed cubic field. Let E be an elliptic curve defined over $\mathbb{Q}$, such that $E(\mathbb{Q})_{tors} \simeq \mathbb{Z}/2\mathbb{Z}$. By Lemma 1, $E(K)_{tors} \simeq \mathbb{Z}/2n\mathbb{Z}$, where n is odd. From [15, Lemma 5.5] only finitely many quadratic twists of $E(K)$ have any odd-order torsion and (since twisting does not change the 2-torsion) hence all but finitely many twists will have torsion $\mathbb{Z}/2\mathbb{Z}$. In exactly the same manner one proves that there are infinitely many curves with $E(K)_{tors} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

The only groups apart of the ones from Mazur's theorem that can a priori appear as the torsion of infinitely many elliptic curves over K are the

ones such that the corresponding modular curve has genus ≤ 1 and that they appear on the list in [5, Theorem 3.4]. One can see that these are the groups $\mathbb{Z}/11\mathbb{Z}$, $\mathbb{Z}/14\mathbb{Z}$, $\mathbb{Z}/15\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$.

Let E be an elliptic curve over $\mathbb{Q}$ with torsion $T = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$. Then by Lemma 1, the 2-Sylow subgroups of $E(\mathbb{Q})$ and $E(K)$ are equal. Thus the torsion of $E(K)$ is larger than $E(\mathbb{Q})$ for only finitely many rational elliptic curves satisfying $E(\mathbb{Q})_{tors} \simeq T$.

By invoking Lemma 1 when needed, it also follows that there are only finitely many elliptic curves defined over $\mathbb{Q}$ with torsion $\mathbb{Z}/n\mathbb{Z}$, where $n = 6, 8, 9, 10$ or 12 whose torsion becomes larger in K.

Take $E(t)$ to be the family of rational elliptic curves

$$E(t) : y^2 + xy + (5t + 3)y = x^3 + (5t + 3)x^2,$$

$t \in \mathbb{Z}$, with 4-torsion over $\mathbb{Q}$. All elliptic curves in this family have good reduction at 5, and $E(t)(\mathbb{F}_5) \simeq \mathbb{Z}/4\mathbb{Z}$ for all $t \in \mathbb{Z}$. This shows that $E(t)(\mathbb{Q})$ cannot have any 8-torsion, 12-torsion or torsion containing $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$, for all $t \in \mathbb{Z}$. As the 3-division polynomial of $E(t)$ is an irreducible degree 4 polynomial (over $\mathbb{Q}(t)$), by Hilbert's irreducibility theorem, there are infinitely many t such that $E(t)(K)$ has no 3-torsion. Since by Lemma 1, the 2-Sylow subgroups of $E(t)(\mathbb{Q})$ and $E(t)(K)$ are equal, we have proved that there are infinitely many $E(t)$ with torsion group $\mathbb{Z}/4\mathbb{Z}$ over K.

Let $E(t)$ be the family of rational elliptic curves

$$E(t) : y^2 + 5txy + (5t - 1)y = x^3 + (5t - 1)x^2,$$

$t \in \mathbb{Z}$, with 5-torsion over $\mathbb{Q}$. All elliptic curves in this family have good reduction at 5, and $E(t)(\mathbb{F}_5) \simeq \mathbb{Z}/5\mathbb{Z}$ for all $t \in \mathbb{Z}$. This rules out the possibility of 10-torsion in $E(\mathbb{Q})$. If $E(t)(K)$ had any 3-torsion, it would inject into the residue field of (a prime over) 5. But $|E(t)(\mathbb{F}_{125})| = 140$, implying that there is no 3-torsion in the residue field of (a prime over) 5, whatever the splitting behavior of 5 in K. This implies that $E(t)(K)$ has no 15-torsion, for all $t \in \mathbb{Z}$. If $E(t)$ is written in short Weierstrass form $y^2 = x^3 + a(t)x + b(t)$, then the discriminant of $x^3 + a(t)x + b(t)$ is a degree 7 polynomial in t. This implies that there are infinitely many values t such that this polynomial generates a totally real cubic field and infinitely many values for which the same polynomial generates a complex cubic field. This now implies that infinitely many $E(t)$ will not have any 2-torsion in K.

A similar argumentation proves that infinitely many rational elliptic curves E with $E(\mathbb{Q})_{tors} \simeq \mathbb{Z}/7\mathbb{Z}$ will have no 2-torsion in K and thus have $E(K)_{tors} \simeq \mathbb{Z}/7\mathbb{Z}$.

We take the families of elliptic curves with 3-torsion

$$E_i(t) : y^2 + ((-1)^i 10t + 2)xy + (10t + 1)y = x^3,$$

where $i = 1$ or 2 and t is a non-zero integer. Note that all curves from both families have good reduction at 5, and $E_i(t)(\mathbb{F}_5) \simeq \mathbb{Z}/3\mathbb{Z}$, and hence $E_i(t)(\mathbb{Q})$ has no 2-torsion or 9-torsion. Thus all curves from these two families have torsion group isomorphic to $\mathbb{Z}/3\mathbb{Z}$. If K is complex, then we choose $E_2(t)$ and if K is totally real, we choose $E_1(t)$. The discriminant of $E_i(t)$ will then be of opposite sign than the discriminant of K (implying that there is no 2-torsion in $E_i(t)(K)$). All curves from both families have good reduction at (a prime over) 2, and have either 3 or 9 points in the residue field of (the prime over) 2. This rules out the possibility of 15-torsion in any $E_i(t)(K)$. By factoring the 9-division polynomial of $E_i(t)$ and taking out the factors belonging to the 3-division polynomial, we are left with factors of degree larger than 9 (as polynomials over $\mathbb{Q}(t)$). This means that, by Hilbert's irreducibility theorem, for infinitely many values t, there will be no 9-torsion in $E_i(t)(K)$.

Let $E(t)$ be the family of rational elliptic curves with

$$E(t) : y^2 + xy - ((5t + 2)^2 - \frac{1}{16})y = x^3 - ((5t + 2)^2 - \frac{1}{16})x^2,$$

where $t \in \mathbb{Z}$, containing $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ as a torsion subgroup over $\mathbb{Q}$. All curves in the family have good reduction at 5, and all curves have 8 points in $\mathbb{F}_5$. This proves that none of the curves have torsion $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ and that $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ is the whole torsion group over $\mathbb{Q}$. The 3-division polynomial is irreducible (over $\mathbb{Q}(t)$) and by Hilbert's irreducibility theorem, there are infinitely many curves $E(t)$ that have no 3-torsion over any cubic field. Finally, after applying Lemma 1, we have proved that there are infinitely many curves with torsion $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ over K.

As we have already proved that there are infinitely many elliptic curves with odd torsion over K, from [15, Lemma 5.5] we conclude that each of these curves has a twist with trivial torsion. Thus there are infinitely many elliptic curves with trivial torsion over K. □

Theorem 3. *Suppose $T(K_1) = \emptyset$. Then the torsion of an elliptic curve over K_1 is isomorphic to one of the groups*

$$\mathbb{Z}/n\mathbb{Z}, \ n = 1, \dots 10, 12,$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \ n = 1, \dots 4, 6.$$

All of the groups actually appear as a torsion of infinitely many curves over K_1.

Proof. By Theorem 2, all the torsion groups from Mazur's theorem appear infinitely often over K_1.

The modular curve $X_1(11)$ is an elliptic curve with an affine model $y^2-y=x^3-x^2$. We compute that $X_1(11)(K_1)$ has rank 0 and $X_1(11)(K_1) \simeq X_1(11)(\mathbb{Q}) \simeq \mathbb{Z}/5\mathbb{Z}$, so all the points $X_1(11)(K_1)$ correspond to cusps, implying the non-existence of an elliptic curve with 11-torsion over K_1.

The modular curve $X_1(14)$ is an elliptic curve with an affine model $y^2+xy+y=x^3-x$. We compute that $X_1(14)(K_1)$ has rank 0 and $X_1(14)(K_1) \simeq X_1(14)(\mathbb{Q}) \simeq \mathbb{Z}/6\mathbb{Z}$, so all the points $X_1(11)(K_1)$ correspond to cusps, implying the non-existence of an elliptic curve with 14-torsion over K_1.

The modular curve $X_1(15)$ is an elliptic curve with an affine model $y^2+xy+y=x^3+x^2$. We compute that $X_1(15)(K_1) \simeq X_1(15)(\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z}$, the points on $X_1(15)(K_1)$ again being cusps, thus proving the non-existence of 15-torsion over K_1.

The modular curve $X_1(2,10)$ is an elliptic curve with an affine model $y^2=x^3+x^2-x$. We compute that $X_1(2,10)(K_1) \simeq X_1(2,10)(\mathbb{Q}) \simeq \mathbb{Z}/6\mathbb{Z}$, the points on $X_1(2,10)(K_1)$ being cusps, implying that there does not exist an elliptic curve with torsion $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$ over K_1.

The modular curve $X_1(2,12)$ is an elliptic curve with an affine model $y^2=x^3-x^2+x$. We compute $X_1(2,12)(K_1) \simeq \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}$, where $(2\alpha_1^2-1, 2\alpha_1^2-2\alpha_1-3)$ is an element of infinite order. Since each point on $X_1(2,12)(K_1)$ corresponds to an isomorphism class of elliptic curves with torsion $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$ over K_1, it is easy to see that there are infinitely many curves with this torsion.

The modular curve $X_1(13)$ is a hyperelliptic curve of genus 2 having an affine model $y^2=x^6-2x^5+x^4-2x^3+6x^2-4x+1$. Denote by $J_1(N)$ the Jacobian of $X_1(N)$. We embed the curve into its Jacobian $J_1(13)(K_1)$, and compute that $J_1(13)(K_1) \simeq \mathbb{Z}/19\mathbb{Z}$. The rank of the Jacobian can be computed in MAGMA, while for the computation of the torsion, we use the MAGMA code of S. Siksek that can be found at `http://www.warwick.ac.uk/staff/S.Siksek/progs/chabnf/g2-jac.m` (although we could manage to compute the torsion by examining the Jacobian over finite fields, as in [18]). We then proceed to compute the fiber of the map $X_1(13)(K_1) \to J_1(13)(K_1)$ and thus find that all the points on $X_1(13)(K_1)$ are cusps.

The modular curve $X_1(16)$ is a hyperelliptic curve of genus 2 having an affine model $y^2=x^5+2x^4+2x^2-x$. In a similar way as above we compute

$J_1(16)(K_1) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$, and find that all the points on $X_1(16)(K_1)$ are cusps.

The modular curve $X_1(18)$ is a hyperelliptic curve of genus 2 having an affine model $y^2 = x^6 + 2x^5 + 5x^4 + 10x^3 + 10x^2 + 4x + 1$. In a similar way as above we compute $J_1(18)(K_1) \simeq \mathbb{Z}/21\mathbb{Z}$, and find that all points on $X_1(18)(K_1)$ are cusps.

As there is no 14-torsion over K_1, there obviously does not exist a curve with torsion $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$.

It remains to prove that there is no 20-torsion. As we mentioned in the introduction, the methods used above are hard to use on $X_1(20)$ as it is a non-hyperelliptic curve of genus 3. We will instead work with $X_0(20)$, and prove a stronger statement, i.e. that there is no 20-cycle over K_1. The modular curve $X_0(20)$ is an elliptic curve with an affine model $y^2 = (x+1)(x^2+4)$ (see [25]), and we compute $X_0(20)(K_1) \simeq X_0(20)(\mathbb{Q}) \simeq \mathbb{Z}/6\mathbb{Z}$. It is known (see [19]) that $X_0(4p)$ has 6 rational cusps when p is a prime, so we conclude that all the points on $X_0(20)(K_1)$ are cusps. □

In general, for any cubic field K, it is known that there are no points of order 55 [11, Remark (2.3)], 27 or 64 [16, Theorem B] over K.

Remark 1. One could also easily prove that there is also no 21-torsion over K_1 in a similar same way as it was proven that there is no 20-torsion. One finds that $X_0(21)(K_1) = X_0(21)(\mathbb{Q})$, having 4 noncuspidal points, corresponding to the 4 rational curves having a 21-cycle, and none of them having 21-torsion. Unfortunately, this is all we can say about $T(K_1)$.

Theorem 4. *Suppose $T(K_4) = \emptyset$. Then the torsion of an elliptic curve over K_4 is isomorphic to one of the groups*

$$\mathbb{Z}/n\mathbb{Z}, \ n = 1, \dots 10, 12, 13, 14, 18$$

$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}, \ n = 1, \dots 4.$$

The groups that appear over $\mathbb{Q}$ appear infinitely many times as torsion, while all the other groups appear only finitely many times.

Proof. We first compute in a similar manner as in the proof of Theorem 3 that $Y_1(11)(K_4)$ is empty.

Next we find that the rank of $X_1(14)(K_4)$ is 0 and the torsion is $\mathbb{Z}/18\mathbb{Z}$. These 18 points comprise all the cusps of $X_1(14)$ (6 rational over $\mathbb{Q}$ and 6 rational over K_4), and the 6 noncuspidal points generate exactly two curves (if P is a point of order 14 on E, then $(E, \pm P)$, $(E, \pm 3P)$ and $(E, \pm 5P)$ are

three distinct points on $X_1(14)$ corresponding to the same curve E), which are

$$y^2 + \frac{9\alpha_4^2 - 13\alpha_4 + 1}{7}xy + \frac{8\alpha_4^2 - 4\alpha_4 - 19}{7}y = x^3 + \frac{8\alpha_4^2 - 4\alpha_4 - 19}{7}x^2 \quad (1)$$

and

$$y^2 + \frac{3\alpha_4^2 + 5\alpha_4 + 5}{7}xy + \frac{8\alpha_4^2 + 7\alpha_4 - 4}{7}y = x^3 + \frac{8\alpha_4^2 + 7\alpha_4 - 4}{7}x^2, \quad (2)$$

both with the 14-torsion point $(0, 0)$. The curves (1) and (2) have j-invariants 255^3 and -15^3 respectively, and both are CM curves. Note that $X_1(14)$ is itself an elliptic curve, so we have simultaneously proved that there also exists an elliptic curve with 18-torsion over K_4! As the curves above are the only ones with 14-torsion, by checking that they do not have another 2-torsion point, we prove that there are no curves over K_4 with torsion $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$. Both curves have rank 0, so over K_4 there are no elliptic curves having $\mathbb{Z}/14\mathbb{Z} \oplus \mathbb{Z}$ as a subgroup.

One finds in exactly the same way as in Theorem 3 that there are no elliptic curves over K_4 with torsion subgroups $\mathbb{Z}/15\mathbb{Z}$, $\mathbb{Z}/16\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$.

As $X_1(4N)$ is a cover of $X_1(2, 2N)$, and $Y_1(2, 10)(K_4) = \emptyset$, one sees that $Y_1(20)(K_4) = \emptyset$.

We find noncuspidal points on $X_1(13)$ and construct from one of them the curve (which has rational j-invariant)

$$y^2 + (4\alpha_4^2 - 2\alpha_4 - 8)xy + (20\alpha_4^2 - 11\alpha_4 - 45)y = x^3 + (20\alpha_4^2 - 11\alpha_4 - 45)x^2,$$

with the point $(0, 0)$ of order 13.

Note that since $X_1(13)$ and $X_1(18)$ are curves of genus 2, by Faltings' theorem there are only finitely many points on them over K_4 and hence only finitely many elliptic curves with 13-torsion and 18-torsion. □

We can say more about $T(K_4)$ than we did for $T(K_1)$.

Proposition 5. *The groups $\mathbb{Z}/21\mathbb{Z}$, $\mathbb{Z}/24\mathbb{Z}$, $\mathbb{Z}/28\mathbb{Z}$, $\mathbb{Z}/32\mathbb{Z}$, $\mathbb{Z}/35\mathbb{Z}$, $\mathbb{Z}/36\mathbb{Z}$, $\mathbb{Z}/49\mathbb{Z}, \mathbb{Z}/52\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/26\mathbb{Z}$ are not in $T(K_4)$.*

Proof. One proves the non-existence of 21-torsion exactly the same way as over K_1. The non-existence of 24-torsion follows from $Y_1(2, 12) = \emptyset$.

As proven in Theorem 4, there are only two curves having $\mathbb{Z}/14\mathbb{Z}$ as a subgroup, and one easily checks that neither of them contains $\mathbb{Z}/28\mathbb{Z}$.

The non-existence of N-torsion for $N = 32, 36$ and 49 is proven by showing that the elliptic curve $X_0(N)$ has rank 0 and checking that all the torsion points are actually cusps. For all the curves except $X_0(32)$, MAGMA easily computes the rank using 2-descent. For $X_0(32)$ it only gives an upper bound of 2. However we can compute that the analytic rank is equal to 0, and since K_4 is a totally real field of odd degree, [26] implies that the algebraic rank is also equal to 0.

Since $X_0(35)$ is a genus 3 (hyperelliptic) curve, it is better not to work with $X_0(35)$ directly. Instead, we can redo the proof of Kubert [12, Proposition IV.3.5.] over K_4. We work with $X_0(35)/w_5$, where w_5 is an Atkin-Lehner involution. There is a nice model of $X_0(35)/w_5$:

$$E : y^2 + y = x^3 + x^2 + 9x + 1.$$

We compute that $E(K_4) = E(\mathbb{Q}) \simeq \mathbb{Z}/3\mathbb{Z}$, and as already shown in [12], these 3 points come from cusps of $X_0(35)$, thus proving that there is no 35-cycle over K_4.

By [2] for a rational elliptic curve E of conductor N there exists a morphism

$$X_0(N) \longrightarrow E$$

called *modular parametrization*. To eliminate $\mathbb{Z}/52\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/26\mathbb{Z}$ we more or less follow the strategy of the proof of [4, Theorem 4.2]. We easily compute that for the elliptic curve

$$E : y^2 = x^3 + x - 10$$

with conductor 52 it holds $E(K_4) \simeq E(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$ and that the degree of the modular parametrization is 3. Thus there are at most 6 points on $X_0(52)(K_4)$, but (see [19]) $X_0(52)$ has 6 rational cusps, so $Y_0(52)(K_4) = \emptyset$, implying $\mathbb{Z}/52\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/26\mathbb{Z} \notin T(K_4)$.

□

Remark 2. One can prove that if $\mathbb{Z}/25\mathbb{Z} \notin T(K_7)$, then $T(K_7) = \emptyset$ in the following way. First, one uses the same methods as in the proofs of Theorems 3 and 4 to prove that there are no elliptic curves with points of order 11, 13, 14, 15, 16, 18 and that no curve contains $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$ as a subgroup. We find that there are infinitely many curves containing $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$ and are unfortunately unable to determine whether there exists a curve with 20-torsion. The non-existence of an elliptic curve having a point of order 21, 24, 35 or 49 is proved in exactly the same way as in the proof of Proposition 5. Finally, we use the modular parametrization (of

degree 4) $X_0(40) \to E$, where E is the elliptic curve $y^2 = x^3 - 107x - 426$ with $E(K_7) = E(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z}$, to prove the non-existence of a 40-cycle, ruling out $\mathbb{Z}/40\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/20\mathbb{Z}$ as possible subgroups. Note that all other non-cyclic torsion groups are ruled out by the Weil pairing.

For any cubic field K it seems hardest to rule out the existence of 25-torsion in $T(K)$, as $X_0(25)$ has genus 0 (and infinitely many points) and $X_1(25)$ has genus 12. There is an intermediate curve B

$$X_1(25) \xrightarrow{2} B \xrightarrow{5} X_0(25)$$

(where the numbers above the arrows denote the degrees of the maps), which was used by Kubert [12] to prove the non-existence of rational 25-torsion and by Kenku [10] to show that there is no 25-torsion over quadratic fields. However this is still a curve of genus 4, and is thus not suited for the methods used in this paper.

3 Cubic fields with smallest discriminant with a given torsion group appearing over them

In this section we will find, for a given group $G \in S - \{\mathbb{Z}/20\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}\}$ the cubic field K with smallest absolute value of its discriminant such that G appears as torsion of some elliptic curve $E(K)$. We will follow the same general strategy as Kamienny and the author [9], by examining fields by ascending $|\Delta(K)|$ and for each field either finding an elliptic curve with given torsion or proving the non-existence of such a curve. For a group $G \in S$, we denote that field by $M(G)$.

Proposition 6. $M(\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}) = K_1$.

Proof. This follows directly from Theorem 3. □

Proposition 7. $M(\mathbb{Z}/14\mathbb{Z}) = M(\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}) = K_2$.

Proof. From Theorem 3, we see that $\mathbb{Z}/14\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$ do not appear as torsion groups over K_1. We compute $rank(X_1(14)(K_2)) = 1$, and find the elliptic curve

$$y^2 + \frac{13\alpha_2^2 + 8\alpha_2 + 29}{9}xy + \frac{-35\alpha_2^2 - 25\alpha_2 - 49}{27}y = x^3 + \frac{-35\alpha_2^2 - 25\alpha_2 - 49}{27}x^2$$

with the point $(0, 0)$ having order 14.

In a similar way we compute $rank(X_1(2,10)(K_2)) = 1$ and find an elliptic curve with torsion $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$, for example

$$y^2+\frac{-\alpha_2^2-9\alpha_2+6}{11}xy+\frac{-84\alpha_2^2-52\alpha_2-145}{121}y = x^3+\frac{-84\alpha_2^2-52\alpha_2-145}{121}x^2.$$

□

Proposition 8. $M(\mathbb{Z}/11\mathbb{Z}) = M(\mathbb{Z}/13\mathbb{Z}) = M(\mathbb{Z}/15\mathbb{Z}) = K_3$.

Proof. One easily computes that $X_1(11)(K_i) \simeq \mathbb{Z}/5\mathbb{Z}$ has only cusps for $i = 1, 2$ and $X_1(11)(K_3) \simeq \mathbb{Z}/10\mathbb{Z}$ (the rank of $X_1(11)$ is 0 over K_3). We obtain that there is exactly one (up to isomorphism) elliptic curve with 11-torsion over K_3, this curve being

$$y^2 + (3\alpha_3^2 - 5\alpha_3 - 3)xy + (8\alpha_3^2 + 8\alpha_3 + 2)y = x^3 + (2\alpha_3^2 - 10\alpha_3 - 6)x^2 \quad (3)$$

Note that this curve has rank 0.

One can compute that $Y_1(15)(K_i) = \emptyset$ for $i = 1, 2$ and that the rank of $X_1(15)(K_3)$ is 1. We find an elliptic curve

$$y^2 + (\alpha_3^2 + \alpha_3 + 5)xy + (8\alpha_3^2 - 4\alpha_3 + 4)y = x^3 + (2\alpha_3^2 - \alpha_3 + 1)x^2$$

with 15-torsion.

We compute that $rank(J_1(13)) = 0$ over the fields with smaller discriminant. Then it is easy to check that there are no elliptic curves with 13-torsion over those fields. Over K_3 we find that $J_1(13)$ has positive rank, and by a simple search we find points on $Y_1(13)$, obtaining the elliptic curve

$$y^2 + (-\alpha_3^2 + 2)xy + (\alpha_3^2 - 2\alpha_3 + 1)y = x^3 + (\alpha_3^2 - 2\alpha_3 + 1)x^2.$$

□

Proposition 9. $M(\mathbb{Z}/18\mathbb{Z}) = K_4$.

Proof. One computes that the rank of the $J_1(18)(K_i)$ is 0 and $Y_1(18)(K_i) = \emptyset$ for $i < 4$. In Theorem 4, it was already proved that 18-torsion appears over K_4. □

Proposition 10. $M(\mathbb{Z}/16\mathbb{Z}) = K_5$.

Proof. This is proved exactly as the previous proposition. We give a curve with 16-torsion over K_5:

$$y^2 + (-\alpha_5 + 2)xy + (-\alpha_5^2 - 2\alpha_5 + 1)y = x^3 + (-\alpha_5^2 - 2\alpha_5 + 1)x^2.$$

□

Proposition 11. *Let* $M(\mathbb{Z}/20\mathbb{Z}) = L_1$ *and* $M(\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}) = L_2$. *Then* $|\Delta(L_1)| \leq 316$ *and* $|\Delta(L_2)| \leq 961$.

Proof. One finds an elliptic curve with 20-torsion over K_{40}, the 40-th field in the table [7], generated by the polynomial $x^3 - x^2 - 4x + 2$ by putting $t = 2$ into [6, Table 1, $N = 20$]. Note that the polynomials $4x^3 + 8x^2 + x - 2$ obtained from [6, Table 1, $N = 20$] and $x^3 - x^2 - 4x + 2$ (from [7]) differ but they generate the same field. The field K_{40} is a S_3 cubic field.

We find an elliptic curve with torsion $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$ over K_{143}, the 143-th field from [7], generated by $x^3 - x^2 - 10x + 8$, using [6, Example 4.3]. The polynomials from [7] and [6, Example 4.3] differ, but they generate the same field. The field K_{143} is a cyclic cubic field. □

4 The number of elliptic curves with given torsion over a number field

In this section we examine the number (up to isomorphism) of elliptic curves over cubic number fields. We will ignore the groups that appear as torsion already over $\mathbb{Q}$ as by Theorem 2 they appear as torsion over every cubic field infinitely many times.

The same problem (again ignoring the groups from Mazur's theorem) for quadratic fields was dealt with in [9]. It was shown that for some groups, if there is one curve with given torsion there are infinitely many, for some groups there are always finitely many, while for some groups, over some quadratic fields there will be finitely many, and over others infinitely many.

We obtain the following result for cubic fields.

Theorem 12. *a) There are only finitely many elliptic curves with torsion* $\mathbb{Z}/13\mathbb{Z}$, $\mathbb{Z}/16\mathbb{Z}$, $\mathbb{Z}/18\mathbb{Z}$, $\mathbb{Z}/20\mathbb{Z}$ *and* $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$ *over any fixed cubic field.*
b) Over any cubic field there is either no curve with torsion $\mathbb{Z}/15\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$ *and* $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$ *or there are infinitely many.*
c) There is exactly one curve with 11-torsion over K_3. *This is the curve (3). Over any other cubic field there are either no elliptic curves with 11-torsion or there are infinitely many.*
d) There are exactly two curves with 14-torsion over K_4. *These are the curves (1) and (2). Over any other cubic field there are either no or infinitely many such curves.*
e) For each of the groups $\mathbb{Z}/11\mathbb{Z}$, $\mathbb{Z}/14\mathbb{Z}$, $\mathbb{Z}/15\mathbb{Z}$ *and* $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$ *there exist infinitely many cubic fields with Galois group* S_3 *over which there exist infinitely many elliptic curves with that torsion. There exist infinitely many*

totally real cubic fields over which there exist infinitely many elliptic curves with torsion $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$.

Proof. a) Since all the modular curves parameterizing these torsions are of genus ≥ 2, the result follows trivially from Faltings' theorem. Actually, the statement is true over a number field of any degree.

b) The only way it is possible that there is a finite number of curves with a torsion group parameterized by a modular curve X_1 of genus 1 is that over some cubic field the torsion of $X_1(K)$ is larger than $X_1(\mathbb{Q})$ and that $rank(X_1(K)) = 0$. We can find the possible candidates for this by examining the division polynomials of X_1.

By [21, 22] the only primes that can divide the order of the torsion are the primes up to and including 13.

We start with $X_1(15)$. Note that $X_1(15)(\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z}$. We easily compute that $\psi_n(X_1(15))$ for $n = 3, 5, 7, 11, 13$ are all irreducible of degree larger than 3, and hence $\psi_n(X_1(15))$ will not have a root over any cubic field. By Lemma 1 the 2-Sylow subgroups of $X_1(15)(\mathbb{Q})$ and $X_1(15)(K)$ are equal for all cubic fields K.

We compute $X_1(2,10)(\mathbb{Q}) \simeq \mathbb{Z}/6\mathbb{Z}$ and $\psi_n(X_1(2,10))$ for $n = 5, 7, 11, 13$ are all irreducible of degree larger than 3, and hence $\psi_n(X_1(2,10))$ will not have a root over any cubic field. By Lemma 1 there are no additional cubic points of order 2^n. The polynomial $\psi_9(X_1(2,10))$ factors as $(x-1)(x^3 + 7/3x^2 + 1/3x + 1/3)f_9 f_{27}$, where f_9 and f_{27} are irreducible polynomials of degree 9 and 27. The points with $x = 1$ correspond to the rational points of order 3. We see that there is a factor of degree 3 in the factorization implying that the x-coordinate of an additional element of order dividing 9 satisfies $x^3+7/3x^2+1/3x+1/3$. We examine $X_1(2,10)(\mathbb{Q}(\alpha))$, where α is the root of $x^3+7/3x^2+1/3x+1/3$. We check that the torsion of $X_1(2,10)(\mathbb{Q}(\alpha))$ is still $\mathbb{Z}/6\mathbb{Z}$. This is because the y-coordinate of the point corresponding to this polynomial is not defined over $\mathbb{Q}(\alpha)$. It is in fact defined over $\mathbb{Q}(\alpha, \sqrt{-3})$, over which $X_1(2,10)$ has torsion $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$. We conclude that there are no noncuspidal cubic torsion points on $X_1(2,10)$ that are not defined over $\mathbb{Q}$.

We compute $X_1(2,12)(\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z}$ and $\psi_n(X_1(2,12))$ for $n = 3, 5, 7, 11, 13$ are all irreducible of degree larger than 3, and hence $\psi_n(X_1(2,12))$ will not have a root over any cubic field. By Lemma 1 there are no cubic points of even order apart from the ones defined over $\mathbb{Q}$.

c) From the short Weierstrass form we see that K_3 is the only cubic field over which $X_1(11)$ has a 2-torsion point. Over any other cubic field, X_1 has odd torsion. As $X_1(11)$ has good reduction at (a prime over) 2, its whole

torsion subgroup embeds into the residue field of (a prime over) 2. By the Hasse-Weil bound, an elliptic curve can have at most 13 points over that field, so only $\mathbb{Z}/5\mathbb{Z}$ ($\simeq X_1(11)(\mathbb{Q})$) is possible.

d) We compute $X_1(14)(\mathbb{Q}) \simeq \mathbb{Z}/6\mathbb{Z}$ and $\psi_n(X_1(14))$ for $n = 5, 7, 11, 13$ are all irreducible of degree larger than 3, and hence $\psi_n(X_1(14))$ will not have a root over any cubic field. By Lemma 1 there are no additional cubic 2^n-torsion points. The polynomial $\psi_9(X_1(14))$ factors as $x(x^3 - 2x^2 - x + 1)(x^3 + x^2/3 - x + 1)f_6 f_{27}$, where f_6 and f_{27} are irreducible polynomials of degree 6 and 27. Note that the first polynomial generates K_4 and, as shown in Theorem 4, $X_1(14)(K_4) \simeq \mathbb{Z}/18\mathbb{Z}$ and the additional torsion generates just the curves (1) and (2). Let K be the field generated by $x^3 + x^2/3 - x + 1$. We check that although the x-coordinate of additional torsion points is defined over K, the y-coordinate is not. Actually, the situation is similar to $X_1(2, 10)$, i.e. $X_1(14)(K(\sqrt{-3})) \simeq \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$.

e) We use the proof of [5, Lemma 3.3. (b)], where it is proved that if an elliptic curve E is written in the form $Y^2 = X^3 + Ax + B$, $A, B \in \mathbb{Z}$, then one can construct an infinite sequence of primes p_i such that the roots ξ_i of $X^3 + Ax + B - p_i^{-20}$ generate distinct cubic fields $\mathbb{Q}(\xi_i)$, such that $E(\mathbb{Q}(\xi_i))$ has positive rank. For the modular curve $X_1(2, 10)$, the discriminant of $X^3 + Ax + B$ is positive, so for all but finitely many p_i, the discriminant of $X^3 + Ax + B - p_i^{-20}$ will also be positive. Hence $X_1(2, 10)$ will have positive rank over infinitely many totally real cubic fields. On the other hand, for the remaining modular curves of genus 1, the discriminant of $X^3 + Ax + B$ is negative, implying that for all but finitely many p_i, the discriminant of $X^3 + Ax + B - p_i^{-20}$ will also be negative. Hence these modular curves will have positive rank over infinitely many cubic fields with Galois group S_3.

□

Acknowledgements. The author was supported by the National Foundation for Science, Higher Education and Technological Development of the Republic of Croatia. We are grateful to Andrej Dujella and Peter Stevenhagen for their helpful comments. We are greatly indebted to the anonymous referee whose numerous comments significantly improved this paper both in presentation and mathematical content.

References

[1] H. Baaziz, *Equations for the modular curve $X_1(N)$ and models of elliptic curves with torsion points*, Math. Comp. **79** (2010), 2371–2386.

[2] C. Breuil, B. Conrad, F. Diamond, R. Taylor, *On the modularity of elliptic curves over Q: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), 843–939.

[3] J. Cremona, Algorithms for Modular Elliptic Curves, 2nd ed. Cambridge University Press, Cambridge, 1997., `http://www.warwick.ac.uk/~masgaj/ftp/data/`

[4] F. Jarvis, P. Meekin, *The Fermat equation over* $\mathbb{Q}(\sqrt{2})$, J. Number Theory **109** (2004), 182–196.

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

[6] 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.

[7] J. Jones, `http://hobbes.la.asu.edu/NFDB/`

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

[9] S. Kamienny, F. Najman, *Torsion groups of elliptic curves over quadratic fields*, preprint.

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

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

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

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

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

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

[16] F. Momose, *p-torsion on elliptic curves defined over quadratic fields*, Nagoya Math. J. **96** (1984), 139–165.

[17] F. Najman, *Torsion of elliptic curves over quadratic cyclotomic fields*, Math J. Okayama U. **53**, (2011) 75–82.

[18] F. Najman, *Complete classification of torsion of elliptic curves over quadratic cyclotomic fields*, J. Number Theory **130** (2010), 1964–1968.

[19] A. Ogg, *Rational points on certain elliptic modular curves*, Proc. Symp. Pure Math **24**, AMS, Providence, R.I. (1973), 221–231.

[20] P. Parent, *Bornes effectives pour la torsion des courbes elliptiques sur les corps de nombres*, J. Reine Angew. Math. **506** (1999), 85–116.

[21] P. Parent, *Torsion des courbes elliptiques sur les corps cubiques*, Ann. Inst. Fourier **50** (2000), 723–749.

[22] P. Parent, *No 17-torsion on elliptic curves over cubic number fields*, J. Theor. Nombres Bordeaux **15** (2003), 831–838.

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

[24] L. Washington, Elliptic Curves. Number Theory and Cryptography, Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, 2003.

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

[26] S. Zhang, *Heights of Heegner points on Shimura curves*, Ann. of Math. (2) **153** (2001), 27–147.

MATHEMATISCH INSTITUUT, P.O. BOX 9512, 2300 RA LEIDEN, THE NETHERLANDS

E-mail: fnajman@math.leidenuniv.nl

AND

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ZAGREB, BIJENIČKA CESTA 30, 10000 ZAGREB, CROATIA

E-mail: fnajman@math.hr