MATHEMATICS OF COMPUTATION
Volume 88, Number 319, September 2019, Pages 2443–2459
https://doi.org/10.1090/mcom/3408
Article electronically published on December 27, 2018

TORSION OF ELLIPTIC CURVES OVER CYCLIC CUBIC FIELDS

MAARTEN DERICKX AND FILIP NAJMAN

Abstract. We determine all the possible torsion groups of elliptic curves over cyclic cubic fields, over non-cyclic totally real cubic fields, and over complex cubic fields.

1. Introduction

An important problem in the theory of elliptic curves is to determine the possible torsion groups of elliptic curves over number fields of degree d. Mazur solved the problem for $d = 1$ [15] and Kamienny [12], building on the work of Kenku and Momose [13], solved the problem for $d = 2$. Recently, Derickx, Etropolski, van Hoeij, Morrow, and Zuerick-Brown announced the solution of the problem for $d = 3$ [5], building on the work of Parent [18,19]. For $d > 3$ the problem remains unsolved at the moment.

A question that naturally arises is which of the groups that arise as torsion groups of elliptic curves over number fields of degree d arise over some natural subset of the set of number fields of degree d. These subsets of the set of all number fields of degree d can be chosen to be, perhaps most naturally, the subset of real (or totally real) number fields, the subset of complex number fields, and the subset of number fields whose normal closure over $\mathbb{Q}$ has Galois group isomorphic to some prescribed group G. Throughout the paper, by abuse of language we say that a number field K has Galois group G over $\mathbb{Q}$ if the Galois group over $\mathbb{Q}$ of the normal closure of K over $\mathbb{Q}$ is G.

These problems are of course meaningless for the case $d = 1$, and for $d = 2$ one can only consider the subdivision of quadratic fields into real and imaginary quadratic fields. The possibilities in each of these cases (for $d = 2$) follow directly from [3] and are summed up in Theorem 3.1. Thus the problem has been solved completely for $d = 2$, so it is natural to consider the case $d = 3$, which is the last case where all the possible torsion groups are known. The main result of the paper is the determination of all possible torsion groups of elliptic curves over

a) all cubic fields with Galois group $\mathbb{Z}/3\mathbb{Z}$,
b) all complex cubic fields,
c) all totally real cubic fields with Galois group S_3.

Received by the editor April 30, 2018, and, in revised form, September 28, 2018.
2010 *Mathematics Subject Classification.* Primary 11G05.
Key words and phrases. Elliptic curves, modular curves, rational points.
The second author was supported by the QuantiXLie Centre of Excellence, a project co-financed by the Croatian Government and European Union through the European Regional Development Fund—the Competitiveness and Cohesion Operational Programme (Grant KK.01.1.1.01.0004).

Parts of some proofs of our results are based on computations in Magma [1]. Some of these computations depend on a Magma package written by Solomon Vishkautsan and the first author [7]. All computations done in Magma for this paper can be found at `https://github.com/wishcow79/chabauty/tree/master/papers/cyclic_cubic`. When referring to specific elliptic curves, we will use their LMFDB labels [14], instead of giving their defining equations.

2. Strategy for determining the Galois groups of degree d points on a curve

The problem described in the introduction easily translates into the question of which cubic fields can occur as the field of definition of degree 3 points on certain modular curves. Ignoring the totally real and complex cubic field questions for a moment and only focusing on the Galois group, one is then led to the more general question of which Galois groups can occur as the Galois group of a degree d point on some curve $X/\mathbb{Q}$. For the rest of this section $X/\mathbb{Q}$ will be a smooth projective and geometrically irreducible curve.

Let $L/\mathbb{Q}$ be a degree d extension, let $\widetilde{L}$ be its normal closure, and let $G := \mathrm{Gal}(\widetilde{L}/\mathbb{Q})$ be its Galois group. A choice of an enumeration $\sigma_1, \dots, \sigma_d$ of the d elements in $\mathrm{Hom}_{\mathbb{Q}}(L, \widetilde{L})$ allows one to see G which naturally acts on $\mathrm{Hom}_{\mathbb{Q}}(L, \widetilde{L})$ as acting on $1, \dots, d$ so that $G \subseteq S_d$. Now let $H \subset S_d$ be any subgroup. Then H naturally acts on X^d by permuting the factors of the direct product; the corresponding quotient X^d/H will be called the H-symmetric product of X and denoted by $X^{(H)} := X^d/H$. If $H = S_d$, then the H-symmetric product $X^{(S_d)}$ is nothing other than the dth symmetric product $X^{(d)}$. Note that contrary to $X^{(d)}$ it is not always true that $X^{(H)}$ is smooth. The simplest non-smooth example is $X^{(\mathbb{Z}/3\mathbb{Z})}$; however, $X^{(H)}$ is smooth if one stays away from the fixed points of H, in particular it is smooth away from the image of $\Delta(X^d)$, the locus in X^d where at least two coordinates coincide. If one lets $s \in X(L)$ be a point and define $s^{(\sigma)} := (\sigma_1(s), \dots, \sigma_d(s)) \in X^d(\widetilde{L})$, and lets $s^{(H)}$ be its image in $X^{(H)}(\widetilde{L})$, then by definition one has that $s^{(H)} \in X^{(H)}(\mathbb{Q})$ if one has that the action of $G = \mathrm{Gal}(\widetilde{L}/\mathbb{Q})$ on $s^{(H)}$ is trivial. By construction the latter happens if $G \subseteq H$ as subgroups of S_d, and if additionally $s \in X(L)$ is not definable over any subfield of L, then one even has that the action of G on $s^{(H)}$ is trivial if and only if $G \subseteq H$.

Remark 2.1. In fact there is a converse to this construction, namely every $x \in X^{(H)}(\mathbb{Q})$ that does not come from some $X^{(H')}(\mathbb{Q})$ for some $H' \subsetneq H$ has to be of the form $s^{(H)}$ as above.

So this turns the study of degree d points on X whose Galois group is isomorphic to H to a study of the rational points of $X^{(H)}$ (that do not come from $X^{(H')}(\mathbb{Q})$ for some $H' \subsetneq H$). This can be a difficult problem in general depending on what X, d, and H are. For example for $X = \mathbb{P}^1$ this problem is equivalent to the inverse Galois problem for H, and for $X = E$ an elliptic curve and $H = \mathbb{Z}/d\mathbb{Z}$ this is closely related to the rank growth of E over cyclic extensions; see for example [8, Section 4].

The cases that need to be dealt with in this paper are however more feasible than the general problem, because we restrict only to $d = 3$. In this case there are only the groups S_3 and $\mathbb{Z}/3\mathbb{Z}$ to consider and the question becomes which points

on $X^{(3)}(\mathbb{Q})$ come from $X^{(\mathbb{Z}/3\mathbb{Z})}(\mathbb{Q})$ and which do not. For most of the relevant modular curves that actually have a cubic point it is easy to construct infinitely many points on $X^{(3)}(\mathbb{Q})$ that come from $X^{(\mathbb{Z}/3\mathbb{Z})}(\mathbb{Q})$ as well as infinitely many that don't (see Theorems 4.1, 6.1, and 6.2 and their proofs, as well as [9]). This is done for example by constructing functions $f \in \mathbb{Q}(X)$ such that the function field extension $\mathbb{Q}(f) \subset \mathbb{Q}(X)$ has Galois group either $\mathbb{Z}/3\mathbb{Z}$ or S_3. The most problematic cases are $X_1(16)$ and $X_1(20)$, both of which have functions of degree 3 where the function field extension has Galois group S_3, but there are no obvious constructions for cubic points with Galois group $\mathbb{Z}/3\mathbb{Z}$. However, in these two cases one can prove that every point of degree 3 on $X_1(N)$ comes from a function $f : X_1(N) \to \mathbb{P}^1$ of degree 3 (see Corollary 4.8) and that additionally there are only finitely many functions of degree 3 (see Lemmas 4.9 and 4.11). So the question is now what the Galois group of $f^{-1}(t)$ can be for $t \in \mathbb{P}^1(\mathbb{Q})$.

Going back to the more general case, let $f : X \to \mathbb{P}^1$ be a function of degree d, and let $\widetilde{\mathbb{Q}(X)}$ be the normal closure of $\mathbb{Q}(X)$ seen as a finite extension of $\mathbb{Q}(\mathbb{P}^1)$, and let $H \subset S_d$ be its Galois group. The generic point of X gives a point $\eta \in X(\mathbb{Q}(X))$. Since $\mathrm{Gal}(\widetilde{\mathbb{Q}(X)}/\mathbb{Q}(\mathbb{P}^1)) = H$ one has that $\eta^{(H)} \in X^{(H)}(\widetilde{\mathbb{Q}(X)})$ is actually a $\mathbb{Q}(\mathbb{P}^1)$-valued point. Define $f^* : \mathbb{P}^1 \to X^{(H)}$ to be the morphism corresponding to $\eta^{(H)}$. Now if $t \in \mathbb{P}^1(\mathbb{Q})$ is not a ramification point and $s \in f^{-1}(t)$ is a point whose field of definition L is of degree d, then one has $f^*(t) = s^{(H)}$. So the question of whether the Galois group of L is smaller than H becomes equivalent to whether $f^*(t) \in X^{(H)}(\mathbb{Q})$ comes from a rational point on $X^{(H')}$ for some $H' \subsetneq H$. Now for an $H' \subsetneq H$ define $C_{H'} := X^{(H')} \times_{X(H)} \mathbb{P}^1$:

$$\begin{array}{ccc} C_{H'} & \longrightarrow & \mathbb{P}^1 \\ \downarrow & & \downarrow{\scriptstyle f^*} \\ X^{(H')} & \longrightarrow & X^{(H)} \end{array} \qquad \begin{array}{ccc} \mathrm{Spec}\,\widetilde{\mathbb{Q}(X)}^{H'} & \longrightarrow & \mathrm{Spec}\,\mathbb{Q}(\mathbb{P}^1) = \mathrm{Spec}\,\widetilde{\mathbb{Q}(X)}^{H} \\ \downarrow{\scriptstyle \eta^{(H')}} & & \downarrow{\scriptstyle \eta^{(H)}} \\ X^{(H')} & \longrightarrow & X^{(H)} \end{array}$$

Now $C_{H'}$ is a curve, so the question of whether the Galois group can get smaller than H has been turned into a question about rational points on curves. The generic fiber of $C_{H'}$ is just $\widetilde{\mathbb{Q}(X)}^{H'}$ with the map $\eta^{(H')}$. This means that it is possible to compute explicit equations for the normalization of $C_{H'}$. In the case that $H = S_d$ and $H' = A_d$ one can even be more explicit. Indeed if one writes $\mathbb{Q}(X) \cong \mathbb{Q}(f)[t]/g$ for some g of degree d in t, then $\mathbb{Q}(C_{A_d}) \cong \mathbb{Q}(f)[t]/(t^2 - \Delta(g))$.

3. Previously known results

In this section we describe known results, some of which we will use in our proofs.

As mentioned in the introduction, for quadratic fields we have a classification of which torsion groups appear over real and which over imaginary quadratic fields. Although the result is not used in this paper, we state it for completeness, as it is not explicitly stated in [3], although it follows directly from the results proved in this paper.

Theorem 3.1 ([3])**.**

a) *Let E be an elliptic curve over an imaginary quadratic number field K. Then $E(K)_{tors}$ is isomorphic to one of the following groups:*

$$\begin{aligned} &\mathbb{Z}/n\mathbb{Z} \text{ for } n = 1, \dots, 12, 14, 15, 16, \\ &\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z} \text{ for } n = 1, \dots, 6, \\ &\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z} \text{ for } n = 1, 2, \\ &\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}. \end{aligned}$$

Each of the cases arises for infinitely many non-isomorphic elliptic curves.

b) *Let E be an elliptic curve over a real quadratic number field K. Then $E(K)_{tors}$ is isomorphic to one of the following groups:*

$$\begin{aligned} &\mathbb{Z}/n\mathbb{Z} \text{ for } n = 1, \dots, 16, 18, \\ &\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z} \text{ for } n = 1, \dots, 6. \end{aligned}$$

Each of the cases arises for infinitely many non-isomorphic elliptic curves.

The following result tells us which are the possible torsion groups of elliptic curves over all cubic fields.

Theorem 3.2 ([5])**.** *The possible torsion groups of elliptic curves over cubic fields are*

$$\mathbb{Z}/n\mathbb{Z} \text{ for } n = 1, \dots, 16, 18, 20, 21,$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z} \text{ for } m = 1, \dots, 7.$$

There exists one curve with torsion $\mathbb{Z}/21\mathbb{Z}$.

Remark 3.3. The one curve with $\mathbb{Z}/21\mathbb{Z}$ torsion was found in [17] and is defined over a cyclic cubic field.

Jeon [9] found infinite families of elliptic curves over cyclic cubic fields with prescribed torsion groups.

Theorem 3.4 ([9])**.** *There exist infinitely many elliptic curves over cyclic cubic fields with torsion:*

$$\mathbb{Z}/n\mathbb{Z} \text{ for } n = 1, \dots, 15, 18,$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z} \text{ for } m = 1, \dots, 7.$$

In this paper we will show that the groups from the above theorem are the only ones that appear infinitely often, and also solve the problem of which torsion groups appear at all (not just infinitely often) over cyclic cubic fields.

A recent result of Bruin and the second author shows that the torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z}$ appears only over cyclic cubic fields.

Theorem 3.5 ([4, Theorem 1.2])**.** *If an elliptic curve E over a cubic field K has torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/14\mathbb{Z}$, then K is cyclic.*

4. Torsion groups over cyclic cubic fields

In this section we classify the possible torsion groups of elliptic curves over cyclic cubic fields.

We want to prove the following.

Theorem 4.1. *Let E be an elliptic curve over a cyclic cubic field K. Then $E(K)_{tors}$ is isomorphic to one of the following groups:*

$$\mathbb{Z}/n\mathbb{Z} \text{ for } n = 1, \dots, 16, 18, 21,$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z} \text{ for } m = 1, \dots, 7.$$

For each of the groups $G = \mathbb{Z}/16\mathbb{Z}$ and $\mathbb{Z}/21\mathbb{Z}$ there is a unique (up to the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$) pair (E, K), where K is a cyclic cubic field and E/K is an elliptic curve, such that $E(K)_{tors} \simeq G$, while for each of the other groups G from the list above there exist infinitely many such pairs.

From Theorem 3.4, it follows that all of the groups in the list apart from $\mathbb{Z}/16\mathbb{Z}$ and $\mathbb{Z}/21\mathbb{Z}$ appear infinitely often. The group $\mathbb{Z}/21\mathbb{Z}$ appears once by Remark 3.3. Thus, by Theorem 3.2, it remains to show that $\mathbb{Z}/16\mathbb{Z}$ appears once and $\mathbb{Z}/20\mathbb{Z}$ does not appear at all. To do this we have to show that $X_1(20)$ has no non-cuspidal cubic points over any cyclic cubic field and find all such points on $X_1(16)$.

Definition 4.2. Let C be a curve over a perfect field K. Then the *new part* of $C^{(d)}(K)$ is defined to be

$$C^{(d)}(K)^{new} := C^{(d)}(K) \setminus \bigcup_{i=1}^{d-1} \iota_i(C^{(i)}(K) \times C^{(d-i)}(K)),$$

where $\iota_i : C^{(i)} \times C^{(d-i)} \to C^{(d)}$ is the map sending effective divisors of degree i and $d - i$ to their sum.

Remark 4.3. If K is algebraically closed, then $C^{(d)}(K)^{new} = \emptyset$ for all $d > 1$ because each ι_i is finite surjective and hence surjective on $K = \overline{K}$ points.

Remark 4.4. If one thinks about $C^{(d)}(K)$ as effective divisors of degree D on $C(\overline{K})$ that are stable under the action of Galois, then $C^{(d)}(K)^{new}$ are exactly those divisors $D = \sum_{i=1}^{n} m_i P_i$ of degree d where all the multiplicities m_i of the points are 1 and the action of $\mathrm{Gal}(K)$ is transitive on the points $P_1, \dots, P_n$. In particular $C^{(d)}(K)^{new}$ consists exactly of those points in $C^{(d)}(K)$ of the form $x^{(d)}$, where $x \in C(\overline{K})$ is a point whose field of definition is of degree d over K.

Lemma 4.5. *Let C be a curve over a field K and $Z \subset C$ a closed subscheme with $Z(K) \neq \emptyset$, and suppose that d is an integer such that $\mu_d : Z^{(d)}(K) \to \mathrm{Pic}^d(C)(K)$ given by $D \mapsto \mathcal{O}_C(D)$ is surjective. Then $\mu_e : Z^{(e)}(K) \to \mathrm{Pic}^e(C)(K)$ is surjective for all integers $e > d$ as well.*

Proof. Let $x \in Z(K)$ be a point and define $\phi_x : \mathrm{Pic}^d(C) \to \mathrm{Pic}^e(C)$ to be the map given by $\phi_x(\mathcal{L}) = \mathcal{L}((e-d)x)$. Then ϕ_x is an isomorphism and hence any $\in \mathrm{Pic}^e(C)(K)$ can be written as $\mathcal{L}'((e-d)x)$ with $\mathcal{L}' \in \mathrm{Pic}^d(C)(K)$. By the surjectiveness assumption on μ_d we can even take $\mathcal{L}' = \mathcal{O}_C(D)$ with $D \in Z^{(d)}(K)$. This gives

$$L = L'((e-d)x) = O_C((e-d)x + D) = \mu_e((e-d)x + D),$$

where $(e-d)x + D$ is in the domain of μ_e because $e - d > 0$. It follows that μ_e is surjective. □

Lemma 4.6. *Let C be a curve over a field K with $C(K) \neq \emptyset$, let d be an integer, and let $S \subset C^{(d)}(K)$ be a subset such that $\mu_{|S} : S \to \mathrm{Pic}^d(C)(K)$ given by $D \mapsto \mathcal{O}_C(D)$ is surjective. Then every point in $C^{(d)}(K)^{new} \setminus S$ is of the form $f^*(x)$, where $f \in K(C)$ is a function of degree d, $x \in \mathbb{P}^1(K)$, and $f^*(x)$ denotes the pullback of x along f as a divisor.*

Proof. Let $D \in C^{(d)}(K)^{new} \setminus S$. Then by the surjectiveness assumption there is an$= D' \in S$ such that $\mu(D') = \mu(D)$. Let f be a function such that $\operatorname{div} f = D - D'$. Then by definition one has $D \neq D'$, and because $D \in C^{(d)}(K)^{new}$ one even has that the supports of D and D' have to be disjoint. In particular f has to have degree exactly d, and $D = f^*(0)$ by construction. □

Proposition 4.7. *Let $C_1(N) := X_1(N) \setminus Y_1(N)$ be the closed subscheme consisting of the cusps. Then the maps $\mu_3 : C_1(16)^{(3)}(\mathbb{Q}) \to \mathrm{Pic}^3 X_1(16)(\mathbb{Q})$ and $\mu_3 : C_1(20)^{(3)}(\mathbb{Q}) \to \mathrm{Pic}^3 X_1(20)(\mathbb{Q})$ are surjective.*

Proof. For $X_1(16)$ this follows from Lemma 4.5 because according to [3, Lemma 4.8] the conditions of Lemma 4.5 are satisfied for $d = 2$.

For $X_1(20)$ this is slightly more work. To determine $J_1(20)(\mathbb{Q})$, an easy computation in Magma shows that $J_1(20)(\mathbb{F}_3) \simeq \mathbb{Z}/60\mathbb{Z}$, and the subgroup of $J_1(20)(\mathbb{Q})$ generated by $\mathbb{Q}$-rational divisors supported on the cusps is isomorphic to $\mathbb{Z}/60\mathbb{Z}$, showing that $J_1(20)(\mathbb{Q})$ and hence $\mathrm{Pic}^3 X_1(20)(\mathbb{Q})$ have cardinality 60.

So it suffices to compute the cardinality of the image of $\mu_3 : C_1(20)^{(3)}(\mathbb{Q}) \to \mathrm{Pic}^3 X_1(20)(\mathbb{Q})$. The curve $X_1(20)$ has six rational cusps, three pairs of Galois conjugate cusps over quadratic extensions, and no cusps with a cubic field of definition. Hence the cardinality of $C_1(20)^{(3)}(\mathbb{Q})$ is $74 = 56 + 18$ with a contribution of $\binom{6+3-1}{3} = 56$ coming from triples of rational cusps and a contribution of $6 \cdot 3 = 18$ coming from a rational cusp together with a pair of Galois conjugate cusps. Computing the map $\mu_3 : C_1(20)^{(3)}(\mathbb{Q}) \to \mathrm{Pic}^3 X_1(20)(\mathbb{Q})$ can be done using modular symbols as in [6, Section 4]. This shows that μ_3 has 54 fibers containing exactly one element, two fibers with four elements (these two fibers are swapped by the action of the diamond operators), and four fibers containing three elements (these four fibers are again permuted by the diamond operators). This gives a total of 60 non-empty fibers and hence μ_3 is surjective. □

Combining Lemma 4.6 and Proposition 4.7 one gets the following corollary.

Corollary 4.8. *Let $N = 16$ or 20. Then any point of degree 3 over $\mathbb{Q}$ on $Y_1(N)$ occurs in an inverse image of the form $f^{-1}(t)$, with $f \in \mathbb{Q}(X_1(N))$ a function of degree 3 and $t \in \mathbb{P}^1(\mathbb{Q})$.*

The above corollary says that in order to explicitly describe all degree 3 points on either $X_1(N)$ for $N = 16$ or 20 one just needs to find all $\mathbb{Q}$-rational functions of degree 3 on these curves. However Proposition 4.7 also gives a hint on how to find all these functions explicitly; indeed it says that every degree 3 function is (up to an automorphism of $\mathbb{P}^1$) a pole supported at the cusps. This means that Lemmas 4.9 and 4.11 can now easily be proved by computing which elements $C \in C_1(N)^{(3)}(\mathbb{Q})$ are the pole divisor of a function of degree 3, and then grouping these elements together by linear equivalence and taking one of them under the action of the

diamond operators. What follows is a description of what happens for $X_1(16)$ and $X_1(20)$ when doing this computation.

Lemma 4.9. *There are four (up to the action of the diamond operators on $X_1(16)$ and automorphisms of $\mathbb{P}^1$) maps $X_1(16) \to \mathbb{P}^1$ of degree 3.*

Proof. The modular curve $X_1(16)$ has an affine model (see [21])

$$X_1(16) : y^2 = x(x^2+1)(x^2+2x-1).$$

We can identify $C_1(16)(\mathbb{C})$ with $\Gamma_1(16)\backslash\mathbb{P}^1(\mathbb{Q})$ an explicit set of representatives of this given by

$$\{0, 1/8, 1/7, 1/6, 1/5, 1/4, 1/3, 1/2, 3/4, 3/8, 3/16, 5/16, 7/16, \infty\}.$$

Under the action of Galois this splits up into nine orbits, namely:

$$\{0, 1/7, 1/5, 1/3\}, \{1/6, 1/2\}, \{1/4, 3/4\}, \{1/8\}, \{3/8\}, \{3/16\}, \{5/16\}, \{7/16\}, \{\infty\}.$$

This means that $C_1(16)^{(3)}(\mathbb{Q})$ consists of $\binom{6+3-1}{3} = 56$ divisors supported at the six rational cusps and $6 \cdot 2$ divisors of the form $P_1 + P_2$, where P_1 is one of the six rational cusps and P_2 is the sum of the points in either of the two pairs of Galois conjugate cusps. By explicit computation one checks that each of the 12 effective divisors of degree 3 not supported at the rational cusps is linearly equivalent to a divisor supported on the rational cusps, so that up to automorphisms of $\mathbb{P}^1$ every function of degree 3 has a pole divisor supported on the rational cusps. It turns out that of the 56 effective divisors of degree 3 supported on the rational cusps, there are exactly 32 that are the pole of a degree 3 function. These 32 divisors are divided into 10 linear equivalence classes of size 2 and 4 linear equivalence classes of size 3, for a total of 14 linear equivalence classes, hence up to the automorphisms of $\mathbb{P}^1$ there are exactly 10+4 = 14 functions of degree 3 on $X_1(16)$. The 10 linear equivalence classes of size 2 form one orbit of size 2 and two orbits of size 4 under the diamond operators, while the four linear equivalence classes of size 3 are one diamond orbit. So that the 14 functions form four distinct orbits under the action of the diamond operators. Finally the explicit equations for these functions were obtained by finding an f whose divisor is the difference between divisors in the same linear equivalence class. Given a degree 3 function g_i,

$$g_i \in \mathbb{Q}(x)[y]/(y^2 - x(x^2+1)(x^2+2x-1)) \simeq \mathbb{Q}(X_1(16)),$$

one can compute its minimal polynomial over $\mathbb{Q}(x)$ as an element $f_i \in \mathbb{Q}(x)[t]$. If the degree of f_i in t is $[\mathbb{Q}(X_1(16)) : \mathbb{Q}(x)] = 2$, then $t \mapsto g_i$ gives an isomorphism $\mathbb{Q}(x)[t]/f_i \to \mathbb{Q}(X_1(16))$.

The explicit equations for the four maps $X_1(16) \to \mathbb{P}^1$ of degree 3 that we obtain are:

$$g_1(x,y) = (x^3 + x^2 + 3x - 1 + 2y)/(2x^3 - 2x^2 - 2x + 2), \tag{1}$$

$$f_1(x,t) = (4x^3 - 4x^2 - 4x + 4)y^2 + (-4x^3 - 4x^2 - 12x + 4)y + x^3 - x^2 - x + 1, \tag{2}$$

$$g_2(x,y) = \frac{y + 2x^2}{x^2 - 1}, \tag{3}$$

$$f_2(x,t) = (x^2 - 1)t^2 - 4x^2 t - x^3 + 2x^2 - x, \tag{4}$$

$$g_3(x,y) = \frac{y - 2x^2}{x^3 - x}, \tag{5}$$

$$f_3(x,t) = (x^3 - x)t^2 + 4x^2 t - x^2 + 2x - 1, \tag{6}$$

$$g_4(x,y) = \frac{2x^2 + y}{x^2 - x}, \tag{7}$$

$$f_4(x,t) = (x^2 - x)t^2 - 4x^2 t - x^3 + x^2 + x - 1. \tag{8}$$

□

Remark 4.10. Notice that from the computations in the proof of Lemma 4.9 one can also see that the image of $\mu_3 : C_1(16)^{(3)}(\mathbb{Q}) \to \mathrm{Pic}^3 X_1(16)(\mathbb{Q})$ has 20 elements and hence is surjective.

Lemma 4.11. *There are two (up to the action of the diamond operators on $X_1(20)$ and automorphisms of $\mathbb{P}^1$) maps $X_1(20) \to \mathbb{P}^1$ of degree 3.*

Proof. The modular curve $X_1(20)$ has an affine model (see [21])

$$X_1(20) : y^3 = x^3 y^2 + x^2 y - x.$$

We can identify $C_1(20)(\mathbb{C})$ with $\Gamma_1(20)\backslash\mathbb{P}^1(\mathbb{Q})$ an explicit set of representatives of this given by

$$\{0, 1/10, 1/9, 1/8, 1/7, 1/6, 1/5, 1/4, 1/3, 1/2, 2/5, 3/4, 3/5, 3/8, 3/10, 3/20, 4/5, 7/20, 9/20, \infty\}.$$

Under the action of Galois this splits up into eleven orbits, namely:

$$\{0, 1/9, 1/7, 1/3\}, \{1/8, 1/4, 3/8, 3/4\},$$
$$\{1/6, 1/2\}, \{1/5, 4/5\}, \{2/5, 3/5\},$$
$$\{1/10\}, \{3/10\}, \{3/20\}, \{7/20\}, \{9/20\}, \{\infty\}.$$

This means that $C_1(20)^{(3)}(\mathbb{Q})$ consists of $\binom{6+3-1}{3} = 56$ divisors supported at the six rational cusps and $6 \cdot 3$ divisors of the form $P_1 + P_2$, where P_1 is one of the six rational cusps and P_2 is the sum of the points in either of the three pairs of Galois conjugate cusps. By explicit computation one checks that 12 of the 18 effective divisors of degree 3 not supported at the rational cusps do not occur as the pole of a function of degree 3 and that the other six are linearly equivalent to a divisor supported on the rational cusps, so that up to automorphisms of $\mathbb{P}^1$ every function of degree 3 has a pole divisor supported on the rational cusps. It turns out that of the 56 effective divisors of degree 3 supported on the rational cusps, there are exactly 14 that are the pole of a degree 3 function. These 14 divisors are divided into four linear equivalence classes of size 2 and two linear equivalence classes of size 3, for a total of six linear equivalence classes, hence up to the automorphisms of $\mathbb{P}^1$

there are exactly six functions of degree 3 on $X_1(20)$. The four linear equivalence classes of size 2 form one orbit under the diamond operators, as do the two linear equivalence classes of size 3. So that the six functions form only two distinct orbits under the action of the diamond operators. Finally the explicit equations for these functions were obtained by finding an f whose divisor is the difference between divisors in the same linear equivalence class.

As in the proof of Lemma 4.9, the degree 3 functions g_i will be written down as elements,

$$g_i \in \mathbb{Q}(x)[y]/(y^3 - x^3y^2 - x^2y + x) \simeq \mathbb{Q}(X_1(20)),$$

and $f_i \in \mathbb{Q}(x)[t]$ will denote the minimal polynomial of g_i over $\mathbb{Q}(x)$.

The explicit equations for the two maps $X_1(20) \to \mathbb{P}^1$ of degree 3 that we obtain are:

$$g_1(x, y) = y - 1, \tag{9}$$

$$f_1(y, t) = t - y + 1, \tag{10}$$

$$g_2(x, y) = \frac{xy + y}{y + 1}, \tag{11}$$

$$\begin{aligned} f_2(y, t) = {} & (y^3 - y)t^3 + (-3y^2 + 2y + 1)t^2 \\ & + (3y^2 + 2y - 1)t - y^2 - 2y - 1. \end{aligned} \tag{12}$$

□

Remark 4.12. Notice that from the computations in the proof of Lemma 4.11 one can also see that the image of $\mu_3 : C_1(20)^{(3)}(\mathbb{Q}) \to \mathrm{Pic}^3 X_1(20)(\mathbb{Q})$ has 60 elements and hence is surjective.

Lemma 4.13. *The only (up to the action of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$*) elliptic curve* E *with* $\mathbb{Z}/16\mathbb{Z}$ *torsion over a cyclic cubic field* K *is*

$$y^2 + axy + by = x^3 + bx^2,$$

where

$$a = \frac{119\alpha^2 - 760\alpha - 6139}{10044}, b = \frac{917\alpha^2 - 8734\alpha - 106531}{700569}, \tag{13}$$

α *is a root of* $x^3 - 201x - 1072$*, and* $K = \mathbb{Q}(\alpha)$.

Proof. Since we've proved in Corollary 4.8 that all cubic points on $X_1(16)$ can be obtained by the action of diamond operators on the inverse images of $\mathbb{P}^1(\mathbb{Q})$ under the maps (1), (3), (5), and (7), this allows us to describe all elliptic curves with $\mathbb{Z}/16\mathbb{Z}$ torsion over cubic fields as a union of parametric families E_t/K_t, where each curve E_t is defined over the cubic field K_t.

Thus we have to find all values t such that $\Delta(K_t)$ is a square, since these will correspond to values of t for which K_t is cyclic. This is equivalent to finding all the values t such that the discriminant $\Delta(f_i)$ is a square for $1 \le i \le 4$, and where the f_i are given in (2), (4), (6), and (8).

This leads us to consider the following four hyperelliptic curves; each curve C_i is obtained by having $y^2 = \Delta(f_i)$:

$$C_1 = C_1(16) : y^2 = 128t^7 - 240t^6 + 112t^5 - 12t^4 + 80t^3 - 88t^2 + 32t - 4, \tag{14}$$

$$C_2 = C_2(16) : y^2 = t^8 - 12t^7 + 54t^6 - 112t^5 + 97t^4 - 32t^3 + 4t^2 - 4t, \tag{15}$$

$$C_3 = C_3(16) : y^2 = t(t^7 - 2t^5 + 16t^4 - 15t^3 + 36t^2 - 32t + 4), \tag{16}$$

$$C_4 = C_4(16) : y^2 = t^6 - 4t^5 - 4t^4 - 40t^3 + 20t^2 - 32t. \tag{17}$$

The curve C_4 has genus 2, while the other three curves have genus 3. Using 2-descent for hyperelliptic curves in Magma we get that the Jacobian of the curve C_1 has rank 0, while the Jacobians of the remaining three curves have rank 1.

Since the Jacobian of the curve C_1 has rank 0, it is easy to find all the rational points on C_1. We find that $\#\operatorname{Aut}(C_1) = 4$, so C_1 has automorphisms which are not the identity and not the hyperelliptic involution. Let w of C_1 be the automorphism defined by $w(x, y) = \left(\frac{x}{x-1}, \frac{y}{x-1}\right)$. The quotient curve $C_1/\langle w\rangle$ is isomorphic to the elliptic curve with LMFDB label 26a2 (Cremona label 26a1). This elliptic curve has three rational points and the only rational points on C_1 in the preimages of the rational points on 26a2 are

$$C_1(\mathbb{Q}) = \{(1/2, 0), \infty\}.$$

We obtain that the cubic points corresponding to $C_1(\mathbb{Q})$ are cusps.

Computing the rational points on the curve C_4 is straightforward—since C_4 has genus 2, the Chabauty method is implemented in Magma, and Magma returns all the rational points. We get that

$$C_4(\mathbb{Q}) = \{(-1/4, \pm 201/4), (0, 0), \pm\infty\}.$$

From the value $t = -1/4$ we get the exceptional curve (13), while the values $t = 0$ and $\pm\infty$ correspond to cusps of $X_1(16)$.

Finding $C_2(\mathbb{Q})$ and $C_3(\mathbb{Q})$ is much more technically difficult and requires the combined use of the Mordell-Weil sieve and the Chabauty method. An additional difficulty is that the Chabauty method is not implemented in Magma for genus > 2 curves; this required us to write our own implementation for the Chabauty method for genus > 2 hyperelliptic curves in Magma. As the methods used in the determination of the rational points on C_2 and C_3 are similar to what we use in determining the points on a curve in Lemma 4.15, we give a detailed explanation of the determination of rational points on C_2 and C_3 in Section 5 and in particular in Theorem 5.3.

We obtain

$$C_2(\mathbb{Q}) = \{(0, 0), \pm\infty\} \text{ and } C_3(\mathbb{Q}) = \{(0, 0), \pm\infty\},$$

and that the cubic points on $X_1(16)$ corresponding to $C_2(\mathbb{Q})$ and $C_3(\mathbb{Q})$ are cusps. □

Remark 4.14. The number field that appears in Lemma 4.13 can be found in LMFDB: 3.3.363609.2. The point $(0, 0)$ on the curve in Lemma 4.13 is of order 16.

Lemma 4.15. *There are no elliptic curves with torsion $\mathbb{Z}/20\mathbb{Z}$ over cyclic cubic fields.*

Proof. Since we've proved in Corollary 4.8 that all cubic points on $X_1(20)$ can be obtained by the action of diamond operators on the inverse images of $\mathbb{P}^1(\mathbb{Q})$ under the maps (9) and (11), this allows us to describe all elliptic curves with $\mathbb{Z}/20\mathbb{Z}$ torsion over cubic fields as a union of parametric families E_t/K_t, where each curve E_t is defined over the cubic field K_t.

Thus, as in the proof of Lemma 4.13 we have to find all values t such that $\Delta(K_t)$ is a square, since these will correspond to values of t for which K_t is cyclic. This is equivalent to finding all the values t such that the discriminant $\Delta(f_i)$ is a square for $i = 1, 2$, and where the f_i are given in (10) and (12).

We obtain the following hyperelliptic curves; each curve C_i is obtained by taking $y^2 = \Delta(f_i)$:

$$C_1 = C_1(20) : y^2 = -27t^8 + 22t^4 + 5, \tag{18}$$

$$C_2 = C_2(20) : y^2 = t^{10} - 6t^9 + 15t^8 - 32t^7 + 51t^6 - 54t^5 + 65t^4 - 64t^3 + 24t^2 - 4t. \tag{19}$$

The genus 3 curve C_1 has an obvious degree 2 map f to the rank 0 elliptic curve

$$E : y^2 = -27t^4 + t^2 + 5.$$

We find that $E(\mathbb{Q}) \simeq \mathbb{Z}/6\mathbb{Z}$ and the only $\mathbb{Q}$-rational points in $f^{-1}(E(\mathbb{Q}))$ are

$$C_1(\mathbb{Q}) = \{(\pm 1, 0)\}.$$

Finding $C_2(\mathbb{Q})$ is much more technically difficult and requires the combined use of the Mordell-Weil sieve and the Chabauty method. We describe these methods and how they were used in detail in Section 5 and in particular in Theorem 5.3 (as they are similar to the ones used in the proof of Lemma 4.13).

We obtain

$$C_2(\mathbb{Q}) = \{(0, 0), \pm\infty\}$$

and that the cubic points on $X_1(20)$ corresponding to $C_2(\mathbb{Q})$ are cusps. □

5. Explicit rational point computations

In the previous section we determined the rational points on $C_1(16), C_4(16)$, and $C_1(20)$. This was relatively easy since they either had a map to a rank 0 elliptic curve whose rational points are easy to compute, or were of genus 2 and the Jacobian had rank 1 so that Magma could compute the set of rational points using explicit Chabauty. For the remaining three curves $C_2(16)$, $C_3(16)$, and $C_2(20)$ the $r < g$ condition needed for explicit Chabauty is satisfied, so from a theoretical point of view it should be easy to compute all rational points on these three curves using Chabauty-Coleman (see [16]) in combination with some Mordell-Weil sieving (see [2]). However a general implementation for explicit Chabauty for hyperelliptic curves of genus > 2 is not implemented in Magma yet so we briefly describe how we manually computed all rational points on these three curves. Before the actual computations, we briefly describe how to do Mordell-Weil sieving without knowing the full Mordell-Weil group.

5.1. **Mordell-Weil sieving with partial Mordell-Weil information.**

Mordell-Weil sieving, as explained for example in [2], is a useful tool that helps find all rational points on a curve C using the Mordell-Weil group of its Jacobian J. In order to simplify the exposition[1] we fix a rational point $\infty \in C(\mathbb{Q})$ and a finite set of primes $S = \{p_1, \ldots, p_k\}$ of good reduction for C and use the point ∞ as a base point for the maps $\mu : C(\mathbb{Q}) \to J(\mathbb{Q})$ and $\mu : C(\mathbb{F}_p) \to J(\mathbb{F}_p)$ for all primes $p \in S$.

[1] At the cost of some technical difficulties one could drop the assumption on the existence of a rational point and the assumption that the primes in S are of good reduction. Additionally one can even let S consist of prime powers instead of primes.

Then for every integer N we have the following commutative diagram:

$$\begin{array}{ccc} C(\mathbb{Q}) & \longrightarrow & J(\mathbb{Q})/NJ(\mathbb{Q}) \\ \downarrow & & \downarrow \\ \prod_{p\in S} C(\mathbb{F}_p) & \longrightarrow & \prod_{p\in S} J(\mathbb{F}_p)/NJ(\mathbb{F}_p). \end{array}$$

The usefulness of this commutative diagram is that one can show that for a fixed $q \in S$ one has that $C(\mathbb{Q}) \to C(\mathbb{F}_q)$ factors via

$$\prod_{p\in S} C(\mathbb{F}_p) \times_{\prod_{p\in S} J(\mathbb{F}_p)/NJ(\mathbb{F}_p)} J(\mathbb{Q})/NJ(\mathbb{Q}) \to C(\mathbb{F}_q). \tag{20}$$

In particular one can show that certain points in $C(\mathbb{F}_q)$ have no rational points reducing to them if the map in (20) is not surjective. However in order to compute the fiber product in (20) one has to know all of $J(\mathbb{Q})$. In practice (for example for the curves relevant to his article) one sometimes can find explicit generators of a finite index subgroup $\Gamma \subseteq J(\mathbb{Q})$. Even though computing $J(\mathbb{Q})$ using the knowledge of Γ is a finite computation, this is not always that easy in practice. This is where the following lemma comes in useful.

Lemma 5.1. *Let C be a curve with Jacobian J, let $S := \{p_1, \dots, p_k\}$ be a finite set of primes of good reduction, let N be a positive integer, let $\Gamma \subseteq J(\mathbb{Q})$ be a subgroup of finite index, let e be such that $eJ(\mathbb{Q}) \subseteq \Gamma$, and let $d := \gcd(N, e)$. Then for every $q \in S$ the map $C(\mathbb{Q}) \to C(\mathbb{F}_q)$ factors via:*

$$\mathrm{MWS}_{\Gamma,N,S,d} := \prod_{p\in S} C(\mathbb{F}_p) \times_{\prod_{p\in S} J(\mathbb{F}_p)/NJ(\mathbb{F}_p)} \Gamma/N\Gamma \to C(\mathbb{F}_q)., \tag{21}$$

where in the above fiber product the map $\prod_{p\in S} C(\mathbb{F}_p) \to \prod_{p\in S} J(\mathbb{F}_p)/NJ(\mathbb{F}_p)$ is $[d] \circ \mu$ on each coordinate and $\Gamma/N\Gamma \to \prod_S J(\mathbb{F}_p)/NJ(\mathbb{F}_p)$ is just the reduction map.

Proof. The definition of d assures the existence of an integer f such that $d \equiv ef \bmod N$, so the lemma follows from the following commutative diagram:

$$\begin{array}{ccccc} C(\mathbb{Q}) & \xrightarrow{\mu} & J(\mathbb{Q})/NJ(\mathbb{Q}) & \xrightarrow{[ef]=[d]} & \Gamma/N\Gamma \\ \downarrow & & \downarrow & & \downarrow \\ \prod_{p\in S} C(\mathbb{F}_p) & \xrightarrow{\mu} & \prod_{p\in S} J(\mathbb{F}_p)/NJ(\mathbb{F}_p) & \xrightarrow{[ef]=[d]} & \prod_{p\in S} J(\mathbb{F}_p)/NJ(\mathbb{F}_p). \end{array}$$

□

The above lemma allows one to circumvent the computation of $J(\mathbb{Q})$ because one can often compute d without knowing $J(\mathbb{Q})$ or e.

Example 5.2. Suppose $J(\mathbb{Q})$ has rank 1 and $x \in J(\mathbb{Q})$ is a generator of the free part. Let d_{tors} be such that $d_{tors}J(\mathbb{Q})_{tors} \subseteq \Gamma_{tors}$, and let d_{free} be such that N/d_{free} is the order of x in $\prod_{p\in S} J(\mathbb{F}_p)/NJ(\mathbb{F}_p)$. Then one can find an e such that $d = \gcd(\mathrm{lcm}(d_{tors}, N), d_{free})$.

5.2. **Rational points on $C_2(16), C_3(16)$, and $C_2(20)$.**

Theorem 5.3. *The hyperelliptic curves*

$$C_2(16): y^2 = t^8 - 12t^7 + 54t^6 - 112t^5 + 97t^4 - 32t^3 + 4t^2 - 4t, \tag{22}$$

$$C_3(16): y^2 = t(t^7 - 2t^5 + 16t^4 - 15t^3 + 36t^2 - 32t + 4), \tag{23}$$

$$C_2(20): y^2 = t^{10} - 6t^9 + 15t^8 - 32t^7 + 51t^6 - 54t^5 + 65t^4 - 64t^3 + 24t^2 - 4t \tag{24}$$

each have exactly three rational points, namely the affine point $P_1 = (0,0)$ and the two points $P_2 = (1:1:0), P_3 = (1:-1:0) \in C(\mathbb{Q})$ at infinity. Furthermore, their Jacobians are of rank 1 over $\mathbb{Q}$ and the three rational points generate a finite index subgroup of the Jacobian.

Proof. In the parts of the proof below which are the same for all three curves we will just write C for the curve and J for the Jacobian of C.

Magma has an implementation of two-descent for hyperelliptic curves, and the result of a two-descent computation is that the rank is at most one for each of the three curves, and one easily checks that $[P_1 - P_2] = -[P_1 - P_3]$ is a point of infinite order on $J(\mathbb{Q})$ for all three curves. So this proves the "furthermore" part of Theorem 5.3. What remains is to do explicit Chabauty and then some Mordell-Weil sieving to actually compute the rational points.

Since these curves are hyperelliptic, it is easy to give a basis for the Kähler differentials, namely

$$\omega_0 := \frac{x^0 \mathrm{d}x}{y}, \omega_1 := \frac{x^1 \mathrm{d}x}{y}, \ldots, \omega_{g-1} := \frac{x^{g-1}\mathrm{d}x}{y},$$

where g is the genus of the curve. If p is a prime of good reduction this is even a $\mathbb{Z}_p$-basis.

The next step in the Chabauty method is to find p-adic differentials $\omega \in H^0(C, \Omega^1_{C/\mathbb{Z}_p})$ that vanish on $J(\mathbb{Q})$ under the p-adic integration pairing

$$\langle -, - \rangle : J(\mathbb{Q}_p) \times H^0(C, \Omega^1_{C/\mathbb{Z}_p}) \to \mathbb{Q}_p,$$
$$(D, \omega) \mapsto \int_0^D \omega.$$

Since $[P_1 - P_2]$ generates a subgroup of $J(\mathbb{Q})$ of finite index one has that a p-adic 1-form ω vanishes on all of $J(\mathbb{Q})$ if and only if $\int_{P_2}^{P_1} \omega = 0$. Explicitly computing $\int_{P_2}^{P_1} \omega_i$ up to some p-adic precision allows one to find $a_i \in \mathbb{Z}_p$ such that $\sum_{i=0}^{g-1} a_i \int_{P_2}^{P_1} \omega_i = \int_{P_2}^{P_1} \sum_{i=0}^{g-1} a_i \omega_i = 0$. For $C = C_2(16)$ we use $p = 5$ from now on, and for $C = C_3(16)$ and $C = C_2(20)$ we use $p = 3$. The result of this computation gives

$$\int_{P_2}^{P_1} \omega \equiv 0 \mod p^5 = 5^5 \qquad \text{for } \omega := \omega_2 + 2983\omega_0 \in \Omega^1_{C_2(16)/\mathbb{Z}_5},$$

$$\int_{P_2}^{P_1} \omega \equiv 0 \mod p^5 = 3^5 \qquad \text{for } \omega := \omega_2 + 118\omega_0 \in \Omega^1_{C_3(16)/\mathbb{Z}_3},$$

$$\int_{P_2}^{P_1} \omega \equiv 0 \mod p^5 = 3^5 \qquad \text{for } \omega := \omega_3 + 4\omega_1 + \omega_0 \in \Omega^1_{C_2(20)/\mathbb{Z}_3}.$$

One easily verifies that these ω have no zeros at the $P_{i,\mathbb{F}_p} \in C(\mathbb{F}_p)$ so that the conclusion of the Chabauty computation is that the residue discs of the $P_{i,\mathbb{F}_p}$ contain

exactly one rational point. What remains to do in order to show that $C(\mathbb{Q}) = \{P_1, P_2, P_3\}$ is to show that there are no rational points reducing to the points in $C(\mathbb{F}_p) \setminus \{P_{1,\mathbb{F}_p}, P_{2,\mathbb{F}_p}, P_{3,\mathbb{F}_p}\}$; this is done using Mordell-Weil sieving.

Computing $\#J(\mathbb{F}_p)$ for the first 20 primes of good reduction shows that $\#J(\mathbb{Q})_{tors}$ is either 1 or 3. Instead of computing the exact 3-torsion we will use Lemma 5.1 in order to do Mordell-Weil sieving without computing the 3-torsion. In all three cases the finite index subgroup Γ will be the group

$$\Gamma := \langle [P_1 - P_2] \rangle \subseteq J(\mathbb{Q}).$$

Mordell-Weil sieving for $C_2(16)$. The primes we will use to sieve with are 5 and 11. The group structures of the Jacobian at these primes are $J(\mathbb{F}_5) \cong \mathbb{Z}/3 \cdot 11^2\mathbb{Z}$ and $J(\mathbb{F}_{11}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^5 \cdot 3 \cdot 11\mathbb{Z}$. For N we will take 22 in order to exploit the interference between the 11-torsion of $J(\mathbb{F}_5)$ and $J(\mathbb{F}_{11})$ and the non-cyclicity of the 2-torsion of $J(\mathbb{F}_{11})$.

The image of $x = [P_1 - P_2]$ in $J(\mathbb{F}_5)/22J(\mathbb{F}_5)$ is of order 11 and a generator. The 11 points in $C_2(16)(\mathbb{F}_5)$ map to $0x, 2x, 2x, 4x, 4x, 5x, 5x, 7x, 7x, 9x$, and $10x$ in $J(\mathbb{F}_5)/22J(\mathbb{F}_5)$ respectively, where $0x, 9x$, and $10x$ correspond to the three known rational points. The image of x in $J(\mathbb{F}_{11})/22J(\mathbb{F}_{11})$ is of order 22 so that as in Example 5.2 we can use $d = 1$. It is also clear that x generates a subgroup of index 2. Of the 16 points in $C_2(16)(\mathbb{F}_{11})$ there are eight that map to a multiple of x; the multiples are $0, 3, 10, 10, 17, 20, 21$, and 21. In particular the image of

$$\mathrm{MWS}_{\Gamma,22,\{5,11\},1} \to C(\mathbb{F}_5) \tag{25}$$

consists exactly of the rational points so that we are done by Lemma 5.1.

Mordell-Weil sieving for $C_3(16)$. In this case only a single prime, namely $p = 3$, is used for sieving, but we use the auxiliary prime 17 in order to show that $\Gamma \subseteq J(\mathbb{Q})$ is saturated at 2. The group structures of the Jacobian at these two primes are $J(\mathbb{F}_3) \cong \mathbb{Z}/2 \cdot 3^3\mathbb{Z}$ and $J(\mathbb{F}_{17}) \cong \mathbb{Z}/2 \cdot 3^2 \cdot 293\mathbb{Z}$.

In this case there is the nice coincidence that the three points in $C_3(16)(\mathbb{F}_3)$ having a known rational point in their residue class are all sent to 0 in $J(\mathbb{F}_3)/2J(\mathbb{F}_3) \cong \mathbb{Z}/2\mathbb{Z}$ while the two other points in $C_3(16)(\mathbb{F}_3)$ are sent to the non-zero element. Furthermore, the image of Γ in $J(\mathbb{F}_3)/2J(\mathbb{F}_3)$ is 0 so that just using the Mordell-Weil sieve at the prime 3 using $N = 2$ gives the desired answer as soon as we can prove that the finite index submodule $\Gamma \subseteq J(\mathbb{Q})$ is saturated at 2. But the latter is indeed saturated at 2 since $J(\mathbb{Q})$ has no 2-torsion and the generator of Γ is sent to the non-zero element in $J(\mathbb{F}_{17})/2J(\mathbb{F}_{17})$.

Mordell-Weil sieving for $C_2(20)$. The primes we will use to sieve with are 3 and 37. The group structures of the Jacobian at these primes are $J(\mathbb{F}_3) \cong \mathbb{Z}/3 \cdot 47\mathbb{Z}$ and $J(\mathbb{F}_{37}) \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3 \cdot 47 \cdot 4651\mathbb{Z}$. For N we will take 47 in order to exploit the interference between the 47-torsion of $J(\mathbb{F}_3)$ and $J(\mathbb{F}_{37})$.

The image of $x = [P_1 - P_2]$ in $J(\mathbb{F}_3)/47J(\mathbb{F}_3)$ is of order 47 and a hence a generator, so that due to Example 5.2 we can use $d = 1$. The five points in $C_2(20)(\mathbb{F}_3)$ map to $0x, 19x, 26x, 45x$, and $46x$ in $J(\mathbb{F}_3)/47J(\mathbb{F}_3)$, respectively, where $0x, 45x$ and $46x$ correspond to the known rational points. Each of the 39 points in $C_2(20)(\mathbb{F}_{37})$ is mapped to a multiple nx of x, where the values of n are as follows:

$$0, 1, 1, 1, 2, 2, 3, 3, 6, 6, 7, 9, 12, 14, 14, 16, 17, 18, 22, 23, 27,$$
$$28, 29, 31, 31, 33, 36, 38, 39, 39, 42, 42, 43, 43, 44, 44, 44, 45, 46.$$

Now one sees that 19 and 26 are not in this list, so that in particular the image of

$$\mathrm{MWS}_{\Gamma,47,\{3,37\},1} \to C(\mathbb{F}_3) \tag{26}$$

consists exactly of the rational points so we are done by Lemma 5.1. □

6. Torsion groups over complex and over totally real and non-Galois cubic fields

Theorem 6.1. *Suppose E/K is an elliptic curve over a complex cubic field K. Then $E(K)_{tors}$ is isomorphic to one of the following groups:*

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

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z} \text{ for } m = 1, \ldots, 6.$$

Each of the listed groups occurs for infinitely many distinct j-invariants.

Proof. We prove this theorem by explicit computation. We use the infinite families E_t/K_t from [10], where for each torsion group from the statement of the theorem, an infinite family of elliptic curves with such torsion is given. For each family we have to determine whether there exists a value $t \in \mathbb{Q}$ such that $\Delta(K_t) < 0$ (which is equivalent to K_t being complex).

If there exists at least one value $t \in \mathbb{R}$ such that $\Delta(K_t) < 0$, then this immediately means that there are infinitely many $t \in \mathbb{Q}$ such that $\Delta(K_t) < 0$. For all the families we explicitly find a value t such that $\Delta(K_t) < 0$ and we are done. □

Theorem 6.2. *Suppose E/K is an elliptic curve over a totally real cubic field K whose Galois group is S_3. Then $E(K)_{tors}$ is isomorphic to one of the following groups:*

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

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z} \text{ for } m = 1, \ldots, 6.$$

Each of the listed groups occurs for infinitely many distinct j-invariants.

Proof. Recall that totally real cubic fields K that are not Galois over $\mathbb{Q}$ have $\Delta(K) > 0$ and $\Delta(K)$ is not a square. The proof of this theorem follows from similar computations as Theorem 6.1. We use the same families E_t/K_t as in Theorem 6.1, and only need to find values $t \in \mathbb{R}$ such that $\Delta(K_t) > 0$, by using the same argument as in the proof of Theorem 6.1. Once we find such a value, by the same argument as before, we see that there are infinitely many $t \in \mathbb{Q}$ such that $\Delta(K_t) > 0$.

It remains to prove that for infinitely many of those t such that $\Delta(K_t) > 0$, it is true that $\Delta(K_t)$ is not a square (in $\mathbb{Q}$). Let

$$C_1 : y = \Delta(K_t) \text{ and } C_2 : y^2 = \Delta(K_t).$$

Now there is an obvious degree 2 map $\phi : C_2 \to C_1$ and hence $\phi(C_2(\mathbb{Q}))$ is a *thin set* (see [20, Chapter 9]) in $C_1(\mathbb{Q})$ and $C_1(\mathbb{Q})\backslash\phi(C_2(\mathbb{Q}))$ is dense, hence there are infinitely many $t \in \mathbb{Q}$ such that $\Delta(K_t) > 0$.

We managed to find a $t \in \mathbb{Q}$ such that $\Delta(K_t) > 0$ for every group apart from $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$. For $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$, we check that $X_1(2, 12)$ (which is the elliptic curve 24a5 (Cremona label 24a4)) has positive rank over the totally real cubic field K with LMFDB label 3.3.148.1, which is the unique cubic field with discriminant 148, the minimal discriminant for a totally real cubic S_3-extension of $\mathbb{Q}$. □

Acknowledgments

We would like to thank Solomon Vishkautsan for making his Chabauty code public and for his help in explaining how to use it, and John Cremona and Andrew Sutherland for helpful comments regarding a previous version of the paper.

References

[1] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, DOI 10.1006/jsco.1996.0125. Computational algebra and number theory (London, 1993). MR1484478

[2] N. Bruin and M. Stoll, *The Mordell-Weil sieve: proving non-existence of rational points on curves*, LMS J. Comput. Math. **13** (2010), 272–306, DOI 10.1112/S1461157009000187. MR2685127

[3] J. Bosman, P. Bruin, A. Dujella, and F. Najman, *Ranks of elliptic curves with prescribed torsion over number fields*, Int. Math. Res. Not. IMRN **11** (2014), 2885–2923, DOI 10.1093/imrn/rnt013. MR3214308

[4] P. Bruin and F. Najman, *Fields of definition of elliptic curves with prescribed torsion*, Acta Arith. **181** (2017), no. 1, 85–95, DOI 10.4064/aa170323-20-9. MR3720004

[5] M. Derickx. A. Etropolski, M. van Hoeij, J. Morrow, and D. Zuerick-Brown, *Sporadic cubic torsion*, preprint.

[6] M. Derickx, B. Mazur, and S. Kamienny, *Rational families of 17-torsion points of elliptic curves over number fields*, Number Theory Related to Modular Curves—Momose Memorial Volume, Contemp. Math., vol. 701, Amer. Math. Soc., Providence, RI, 2018, pp. 81–104, DOI 10.1090/conm/701/14142. MR3755909

[7] M. Derickx and S. Vishkautsan, *Magma package for the Chabauty method*, `https://github.com/wishcow79/chabauty`.

[8] J. Fearnley, H. Kisilevsky, and M. Kuwata, *Vanishing and non-vanishing Dirichlet twists of L-functions of elliptic curves*, J. Lond. Math. Soc. (2) **86** (2012), no. 2, 539–557, DOI 10.1112/jlms/jds018. MR2980924

[9] D. Jeon, *Families of elliptic curves over cyclic cubic number fields with prescribed torsion*, Math. Comp. **85** (2016), no. 299, 1485–1502, DOI 10.1090/mcom/3012. MR3454372

[10] D. Jeon, C. H. Kim, and Y. Lee, *Families of elliptic curves over cubic number fields with prescribed torsion subgroups*, Math. Comp. **80** (2011), no. 273, 579–591, DOI 10.1090/S0025-5718-10-02369-0. MR2728995

[11] D. Jeon, C. H. Kim, and A. Schweizer, *On the torsion of elliptic curves over cubic number fields*, Acta Arith. **113** (2004), no. 3, 291–301, DOI 10.4064/aa113-3-6. MR2069117

[12] S. Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms*, Invent. Math. **109** (1992), no. 2, 221–229, DOI 10.1007/BF01232025. MR1172689

[13] M. A. Kenku and F. Momose, *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. **109** (1988), 125–149, DOI 10.1017/S0027763000002816. MR931956

[14] The LMFDB Collaboration, *The L-functions and modular forms database*, `http://www.lmfdb.org`, 2013 [Online; accessed 20 April 2018].

[15] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. **47** (1977), 33–186 (1978). MR488287

[16] W. McCallum and B. Poonen, *The method of Chabauty and Coleman* (English, with English and French summaries), Explicit Methods in Number Theory, Panor. Synthèses, vol. 36, Soc. Math. France, Paris, 2012, pp. 99–117. MR3098132

[17] F. Najman, *Torsion of rational elliptic curves over cubic fields and sporadic points on $X_1(n)$*, Math. Res. Lett. **23** (2016), no. 1, 245–272, DOI 10.4310/MRL.2016.v23.n1.a12. MR3512885

[18] P. Parent, *Torsion des courbes elliptiques sur les corps cubiques* (French, with English and French summaries), Ann. Inst. Fourier (Grenoble) **50** (2000), no. 3, 723–749. MR1779891

[19] P. Parent, *No 17-torsion on elliptic curves over cubic number fields* (English, with English and French summaries), J. Théor. Nombres Bordeaux **15** (2003), no. 3, 831–838. MR2142238

[20] J.-P. Serre, *Lectures on the Mordell-Weil Theorem*, 3rd ed., Aspects of Mathematics, Friedr. Vieweg & Sohn, Braunschweig, 1997. Translated from the French and edited by Martin Brown from notes by Michel Waldschmidt; With a foreword by Brown and Serre. MR1757192

[21] A. V. Sutherland, *Constructing elliptic curves over finite fields with prescribed torsion*, Math. Comp. **81** (2012), no. 278, 1131–1147, DOI 10.1090/S0025-5718-2011-02538-X. MR2869053

Johann Bernoulli Institute, Universiteit Groningen, Nijenborgh 9, 9747 AG Groningen, The Netherlands

Email address: maarten@mderickx.nl

Department of Mathematics, University of Zagreb, Bijenička cesta 30, 10000 Zagreb, Croatia

Email address: fnajman@math.hr