FIELDS OF DEFINITION OF ELLIPTIC CURVES WITH PRESCRIBED TORSION

PETER BRUIN AND FILIP NAJMAN

Abstract. We prove that all elliptic curves over quadratic fields with a subgroup isomorphic to C_{16}, as well as all elliptic curves over cubic fields with a subgroup isomorphic to $C_2 \times C_{14}$, are base changes of elliptic curves defined over $\mathbb{Q}$. We obtain these results by studying geometric properties of modular curves and maps between modular curves, and then obtaining a modular description of these curves and maps.

1. Introduction

By the Mordell–Weil theorem, the Abelian group $E(K)$ of K-rational points on an elliptic curve E over a number field K is finitely generated. This group can therefore be decomposed as $E(K) \simeq E(K)_{\mathrm{tor}} \oplus \mathbb{Z}^r$, where r is the rank of E over K.

Let $\Phi(d)$ denote the set of isomorphism classes of finite groups G with the property that there exists an elliptic curve E over a number field K of degree d such that $E(K)_{\mathrm{tor}} \simeq G$. In this paper we will show that for $d = 2$ and $d = 3$ and for certain groups $G \in \Phi(d)$, if $E(K)_{\mathrm{tor}} \simeq G$, it turns out that E is a base change of an elliptic curve over $\mathbb{Q}$.

The first example of a result where the torsion of an elliptic curve over a number field of given degree yields information about its field of definition can be found in [2]. There it was shown that if an elliptic curve over a quadratic field K has a point of order 13 or 18, then K is a real quadratic field. In other words, there are no elliptic curves over imaginary quadratic fields with a point of order 13 or 18. Another result in the same paper shows that if an elliptic curve over a quartic field K has a point of order 22, then K has a quadratic subfield over which the modular curve $Y_1(11)$ has points; note that "most" quartic fields do not have quadratic subfields. In [3], it is proved that if an elliptic curve over a quartic field K has a point of order 17 and L is the normal closure of K over $\mathbb{Q}$, then $\mathrm{Gal}(L/\mathbb{Q})$ is isomorphic to D_4 or S_4.

The goal of this paper is to prove the following two theorems.

2010 *Mathematics Subject Classification.* Primary 11G05; Secondary 11G18.

Key words and phrases. Elliptic curves, modular curves.

The first author was supported by the Netherlands Organisation for Scientific Research (NWO) through Veni grant 639.031.346.

The second author gratefully acknowledges support from the QuantiXLie Center of Excellence.

Theorem 1.1. *Every elliptic curve over a quadratic field with a subgroup isomorphic to C_{16} is a base change of an elliptic curve over $\mathbb{Q}$ with a subgroup isomorphic to C_8.*

Theorem 1.2. *If E is an elliptic curve over a cubic field K with a subgroup isomorphic to $C_2 \times C_{14}$, then K is normal over $\mathbb{Q}$ and E is a base change of an elliptic curve over $\mathbb{Q}$.*

We found examples of elliptic curves that are not base changes of elliptic curves over $\mathbb{Q}$ with all possible torsion groups over quadratic fields apart from C_{16}, and with all possible torsion groups over cubic fields apart from $C_2 \times C_{14}$ and C_{21}. The case of C_{21} is somewhat special: there is a unique curve over a cubic field with this torsion group, and the curve is a base change of an elliptic curve (with Cremona label 162b1) over $\mathbb{Q}$. This curve was found by the second author [10] and was proved to be the only such curve in yet unpublished work of Derickx, Etropolski, Morrow and Zureick-Brown.

In Section 2 we prove Theorem 1.1; in Section 3 we prove the more difficult Theorem 1.2. We deduce these results from geometric properties of modular curves and maps between modular curves, combinined with the modular description of these curves and maps. For a congruence subgroup $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$, let X_Γ be the corresponding modular curve and let Y_Γ be the complement of the cusps in X_Γ.

The idea of the proof of Theorem 1.1 is as follows. There exists a congruence subgroup $\Gamma' \subset \mathrm{SL}_2(\mathbb{Z})$, containing $\Gamma_1(16)$ as a subgroup of index 2, such that all the degree 2 points on $Y_1(16)$ map to $\mathbb{Q}$-rational points of $Y_{\Gamma'}$ under the natural morphism $X_1(16) \to X_{\Gamma'}$. The modular descriptions of $X_1(16)$ and $X_{\Gamma'}$ then allow us to conclude that the points of degree 2 on $Y_1(16)$ in fact parameterize elliptic curves defined over $\mathbb{Q}$.

Moving on to the setting of Theorem 1.2, let $\Gamma = \Gamma_1(2,14)$. The proof of Theorem 1.2 follows the same lines, with the difference that in this case there will be two maps $q_H \colon X_\Gamma \to X_\Gamma/H$ and $q_{H'} \colon X_\Gamma \to X_\Gamma/H'$ of degree 3, where the quotient curves X_Γ/H and X_Γ/H' of genus 0 are constructed in Section 3.1. We prove that all cubic points of Y_Γ are inverse images of rational points of Y_Γ/H or Y_Γ/H' under the maps q_H and $q_{H'}$. Using an explicit equation for X_Γ, we compute the group of $\mathbb{Q}$-points of the Jacobian of X_Γ (Proposition 3.8) and describe the set of effective divisors of degree 3 on X_Γ (Proposition 3.9). It is then not hard to deduce that all cubic points on $Y(\Gamma)$ arise from $\mathbb{Q}$-rational points on Y_Γ/H or Y_Γ/H'.

2. Elliptic curves with 16-torsion over quadratic fields

In this section we will prove Theorem 1.1. We write

$$\Gamma' = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; \begin{array}{r} a \equiv d \equiv 1 \pmod{8}, \\ c \equiv 0 \pmod{16} \end{array} \right\}.$$

The curves $X_1(16)$ and $X_{\Gamma'}$ have genus 2 and 0, respectively, and the map

$$\pi\colon X_1(16) \to X_{\Gamma'}$$

of degree 2 is a quotient map for the diamond automorphism $\langle 9\rangle$ on $X_1(16)$. It was already shown in [2] that all quadratic points on $Y_1(16)$ are inverse images under π of $\mathbb{Q}$-rational points of $Y_{\Gamma'}$.

Proof of Theorem 1.1. Consider a point of $Y_1(16)(K)$ corresponding to a pair (E, P), where E is an elliptic curve over a quadratic field K and $P \in E(K)$ is a point of order 16. Let σ be the generator of $\mathrm{Gal}(K/\mathbb{Q})$. Using the fact that the hyperelliptic involution on $X_1(16)$ is the diamond automorphism $\langle 9\rangle$, it was proved in [2, § 4.5] that there exists an isomorphism

$$\mu\colon E^\sigma \xrightarrow{\sim} E$$

satisfying

$$\mu \circ \mu^\sigma = \mathrm{id} \quad \text{and} \quad \mu(P^\sigma) = 9P.$$

(This μ differs from the one in [2] by a sign.) It follows, although this was not explicitly stated in [2], that E can be descended to $\mathbb{Q}$. The isomorphism μ maps $(2P)^\sigma$ to $2(9P) = 18P = 2P$. Therefore not only E, but also the point $2P$ of order 8 is defined over $\mathbb{Q}$. □

The above argument can be made explicit as follows. The modular curve $X_1(16)$ admits the equation

$$X_1(16)\colon v^2 - (u^3 + u^2 - u + 1)v + u^2 = 0.$$

From [2], it follows that all quadratic points (u, v) on $Y_1(16)$ satisfy $u \in \mathbb{Q}$. One can write down, in terms of the coordinates (u, v), equations for the universal elliptic curve E and for the universal point P of order 16 on E. (The resulting equations are the same as those obtained by Rabarison [12, Section 4.4], up to a change of variables in the equation for $X_1(16)$.) One can then descend the pair $(E, 2P)$ to $\mathbb{Q}$ by writing E in Tate normal form with respect to the point $2P$. This gives the Weierstrass equation

$$E\colon y^2 + axy + by = x^3 + bx^2 \text{ with } 2P = (0, 0),$$

where

$$a = 1 - \frac{u^2(u-1)(u+1)}{u^2+1} \quad \text{and} \quad b = \frac{-u^2(u-1)(u+1)}{(u^2+1)^2}.$$

Since these expressions do not contain v, we obtain a Weierstrass equation for E with coefficients in $\mathbb{Q}$.

3. Elliptic curves with $(2,14)$-torsion over cubic fields

Next, we take $\Gamma = \Gamma_1(2,14) = \Gamma(2) \cap \Gamma_1(7)$. We will study Γ and the corresponding modular curve X_Γ using several auxiliary congruence subgroups. Let $\Gamma_*(2)$ be the unique subgroup of $\mathrm{SL}_2(\mathbb{Z})$ that contains $\Gamma(2)$ and such that $(\Gamma_*(2) : \Gamma(2)) = 3$; more precisely,

$$\Gamma_*(2) = \left\{ \Gamma \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; \gamma \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \pmod 2 \right\}.$$

We also define

$$\Gamma_*(7) = \left\{ \begin{pmatrix} a & b \\ c & b \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; \begin{matrix} a, d \equiv 1, 2, 4 \pmod 7, \\ c \equiv 0 \pmod 7 \end{matrix} \right\}.$$

We note that $\Gamma_*(7)$ does not contain the matrix $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. It does have two conjugacy classes of elliptic elements of order 3, corresponding to two specific $\Gamma_*(7)$-structures on an elliptic curve with j-invariant 0.

The groups $\Gamma_*(2)$ and $\Gamma_*(7)$ contain $\Gamma(2)$ and $\Gamma_1(7)$, respectively, as normal subgroups of index 3. We define A_3 and C_3 as the respective quotients $\Gamma_*(2)/\Gamma(2)$ and $\Gamma_*(7)/\Gamma_1(7)$, and we make the identifications

$$\begin{aligned} A_3 &= (\Gamma_*(2) \cap \Gamma_1(7))/\Gamma, \\ C_3 &= (\Gamma(2) \cap \Gamma_*(7))/\Gamma, \\ A_3 \times C_3 &= (\Gamma_*(2) \cap \Gamma_*(7))/\Gamma. \end{aligned}$$

The group $A_3 \times C_3$ has four subgroups of order 3; besides A_3 and C_3, there are two further subgroups H and H'.

3.1. Geometric properties of modular curves.

The modular curve X_Γ equals $X_1(2,14)$. Furthermore, the modular curve $X_{\Gamma_*(7)}$ is just $X_0(7)$, but we will denote it by $X_*(7)$ in view of the fact that it is defined using $\Gamma_*(7)$ instead of $\Gamma_0(7)$, which is essential to our method. We will also need the modular curves $X_1(7)$ and $X_1(14)$. The curves $X_*(7)$ and $X_1(7)$ have genus 0. The curve $X_1(14)$ has genus 1, and is isomorphic to the elliptic curve over $\mathbb{Q}$ with Cremona label 14a4.

The group $\Gamma_*(7)/\Gamma$ acts on X_Γ. The action of the various subgroups of interest gives rise to the following diagram, where the numbers next to the arrows indicate the degrees:

$$\begin{tikzcd}
 & & & X_\Gamma \arrow[dlll, "2"'] \arrow[dll, "3"] \arrow[dl, "3"] \arrow[dr, "3"'] \arrow[drr, "3"] & & \\
X_1(14) \arrow[dr, "3"'] & X_\Gamma/A_3 \arrow[d, "2"] \arrow[drr, "3"'] & X_\Gamma/H \arrow[dr, "3"] & & X_\Gamma/H' \arrow[dl, "3"'] & X_\Gamma/C_3 \arrow[dll, "3"] \\
 & X_1(7) \arrow[drr, "3"'] & & X_\Gamma/(A_3 \times C_3) \arrow[d, "2"] & & \\
 & & & X_*(7) & &
\end{tikzcd}$$

The *index* of a cusp on a modular curve X is the order of vanishing of the discriminant modular form, or equivalently the ramification index of the canonical map $X \to X(1)$, at this cusp.

Lemma 3.1. *The curve X_Γ has genus 4. It has 18 cusps: 9 of index 2 and 9 of index 14.*

Proof. The map $X_\Gamma \to X_1(14)$ of degree 2 is unramified over the open subset $Y_1(14)$; this follows for example from the fact that there is a universal elliptic curve over $Y_1(14)$ and that its 2-torsion is étale. As for the cusps, for each $d \in \{1, 2, 7, 14\}$ there are three cusps of index d on $X_1(14)$, and the above covering is ramified exactly above the six cusps of index 1 or 7 on $X_1(14)$. The Hurwitz formula gives

$$2g(X_\Gamma) - 2 = 2(2g(X_1(14)) - 2) + 6.$$

Both statements now follow easily. □

Lemma 3.2. *The groups A_3 and C_3 act freely on X_Γ.*

Proof. The action of the group C_3 on X_Γ descends to an action on $X_1(14)$ via the group of diamond automorphisms $\{\langle 1\rangle, \langle 9\rangle, \langle 11\rangle\}$. Under any identification of $X_1(14)$ with an elliptic curve, the automorphisms $\langle 9\rangle$ and $\langle 11\rangle$ act as translations by 3-torsion points and hence have no fixed points. It follows that C_3 acts freely on $X_1(14)$, and hence also on X_Γ.

The group A_3 acts freely on Y_Γ because $Y_1(7)$ is a fine moduli space. The cusps also have trivial stabilizer; this follows from the fact that the indices of all cusps are coprime to the order of A_3. □

Corollary 3.3. *The quotient maps*

$$X_\Gamma \to X_\Gamma/A_3,$$
$$X_\Gamma \to X_\Gamma/C_3$$

are unramified. Each of the curves X_Γ/A_3 and X_Γ/C_3 has 6 cusps: 3 of index 2 and 3 of index 14. Both curves have genus 2.

Proof. The first two statements are immediate from Lemma 3.2; the last one follows from the Hurwitz formula. □

Lemma 3.4.
(1) *The curve $X_\Gamma/(A_3 \times C_3)$ has genus 0. It has two cusps: one of index 2 and one of index 14.*
(2) *The map $X_\Gamma \to X_\Gamma/(A_3 \times C_3)$ has ramification index 3 at 12 points of X_Γ (lying above 4 points of $X_\Gamma/(A_3 \times C_3)$) and is unramified everywhere else.*

Proof. The map $X_\Gamma/A_3 \to X_1(7)$ is unramified over $Y_1(7)$ by Lemma 3.2, so the map $X_\Gamma/(A_3 \times C_3) \to X_*(7)$ is unramified outside the cusps. Since $X_*(7)$ has genus 0, the Hurwitz formula implies that this last map is ramified above the two cusps of $X_*(7)$ and that $X_\Gamma/(A_3 \times C_3)$ has genus 0. This proves (1).

By the Hurwitz formula and the fact that the map $X_\Gamma/A_3 \to X_\Gamma/(A_3 \times C_3)$ is cyclic of degree 3, this map is totally ramified at 4 points. The claim (2) now follows from the fact that the map $X_\Gamma \to X_\Gamma/A_3$ is unramified (the same argument works for C_3). $\square$

Lemma 3.5. *The curves X_Γ/H and X_Γ/H' have genus 0.*

Proof. Let P be one of the 12 ramification points of the map $X_\Gamma \to X_\Gamma/(A_3 \times C_3)$. Then the stabilizer G_P of P in $A_3 \times C_3$ is of order 3 and different from A_3 and C_3 since the latter two groups act freely on X_Γ by Lemma 3.2. Therefore G_P is either H or H'. Let n_H be the number of points $P \in X_\Gamma$ with stabilizer H, and similarly for $n_{H'}$. The Hurwitz formula gives

$$2g(X_\Gamma) - 2 = 3(g(X_\Gamma/H) - 2) + 2n_H,$$

$$2g(X_\Gamma) - 2 = 3(g(X_\Gamma/H') - 2) + 2n_{H'}.$$

Adding the two equations and using $g(X_\Gamma) = 4$ and $n_H + n_{H'} = 12$, we get $g(X_\Gamma/H) + g(X_\Gamma/H') = 0$, which implies the claim. $\square$

We conclude that the curve X_Γ admits two maps of degree 3 to a curve of genus 0, namely the quotient maps

$$q_H\colon X_\Gamma \to X_\Gamma/H, \quad q_{H'}\colon X_\Gamma \to X_\Gamma/H'.$$

By construction, both are cyclic with Galois groups H and H', respectively. Pull-back of divisors along the two maps q_H and $q_{H'}$ gives rise to two lines L and L' (copies of $\mathbb{P}^1_{\mathbb{Q}}$) inside $\operatorname{Sym}^3 X_\Gamma$. Both maps are ramified at exactly 6 points, and the two sets of 6 points are disjoint because of Lemma 3.4(2). This implies that X_Γ embeds as a smooth curve of bidegree $(3,3)$ in $X_\Gamma/H \times X_\Gamma/H' \simeq \mathbb{P}^1_{\mathbb{Q}} \times \mathbb{P}^1_{\mathbb{Q}}$, and that L and L' are disjoint. Furthermore, because a curve of genus 4 admits at most two linear systems of degree 3 and dimension 1 (see [6, IV, Example 5.2.2]), every non-constant map $X_\Gamma \to \mathbb{P}^1_{\mathbb{Q}}$ of degree 3 can be identified with either q_H or $q_{H'}$ via an isomorphism of $\mathbb{P}^1_{\mathbb{Q}}$ with X_Γ/H or X_Γ/H', respectively.

We fix one rational cusp, say $O = (0,0)$, and we consider the Jacobian J_Γ of X_Γ and the (non-dominant) rational map

$$\begin{aligned} \phi\colon \operatorname{Sym}^3 X_\Gamma &\to J_\Gamma \\ D &\mapsto [D - 3O] \end{aligned} \tag{1}$$

Lemma 3.6. *The map ϕ contracts the lines L and L' and is injective outside $L \cup L'$.*

Proof. Consider two distinct points of $\operatorname{Sym}^3 X_\Gamma$ corresponding to effective divisors D, D' of degree 3 on X_Γ. Then $\phi(D) = \phi(D')$ if and only if D and D' are linearly equivalent. In this case, there exists a rational function f on X_Γ with divisor $D - D'$. Such an f gives a map of degree at most 3 to $\mathbb{P}^1_{\mathbb{Q}}$; this can be identified with either q_H or $q_{H'}$, since X_Γ is not hyperelliptic. This implies that $\phi(D) = \phi(D')$ if and only if either both D and D' are pull-backs of points under $q_H\colon X_\Gamma \to X_\Gamma/H$, or both are pull-backs of points under $q_{H'}\colon X_\Gamma \to X_\Gamma/H'$. $\square$

Proposition 3.7. *The modular curve X_Γ is isomorphic to the smooth projective curve of bidegree $(3,3)$ in $\mathbb{P}^1_{\mathbb{Q}} \times \mathbb{P}^1_{\mathbb{Q}}$ given by the equation*

$$X_\Gamma \colon (u^3+u^2-2u-1)v(v+1)+(v^3+v^2-2v-1)u(u+1)=0. \tag{2}$$

The (u,v)-coordinates of the 9 rational cusps are

$$\begin{gathered}(0,0),\quad (0,-1),\quad (0,\infty),\\ (-1,0),\quad (-1,-1),\quad (-1,\infty),\\ (\infty,0),\quad (\infty,-1),\quad (\infty,\infty).\end{gathered}$$

The 9 cusps with field of definition $\mathbb{Q}(\zeta_7)^+$ are defined by

$$u^3+u^2-2u-1=v^3+v^2-2v-1=0.$$

Our initial proof of the above proposition proceeded by viewing X_Γ as the S_3-cover of the curve $X_1(7)$ corresponding to the moduli problem of labelling the three points of order 2 by the set $\{0,1,2\}$. As this proof involves rather long calculations, we do not give it here, but refer to the independent derivation of the above equation for X_Γ by Derickx and Sutherland [4, § 3.1].

3.2. **Proof of the main result.** We first determine the structure of $J_\Gamma(\mathbb{Q})$. As X_Γ is a non-hyperelliptic genus 4 curve, note that $J_\Gamma(\mathbb{Q})$ cannot be computed directly in any current computer algebra system.

Proposition 3.8. *The group $J_\Gamma(\mathbb{Q})$ is generated by differences of rational cusps and is isomorphic to $C_2 \times C_2 \times C_6 \times C_{18}$.*

Proof. The modular Abelian variety J_Γ over $\mathbb{Q}$ decomposes up to isogeny as $J_\Gamma \sim E \times E \times B$, where E is an elliptic curve and B is an Abelian surface. A computation with newforms in either Magma or Sage [13] shows that the L-functions of E and B do not vanish at 1. By results of Kato [7], the Birch–Swinnerton-Dyer conjecture is true for modular Abelian varieties. We conclude that $J_\Gamma(\mathbb{Q})$ has rank 0.

Let red_3 denote the reduction map $J_\Gamma(\mathbb{Q}) \to J_\Gamma(\mathbb{F}_3)$. Then red_3 is injective. One computes the numerator of the zeta function of X_Γ over $\mathbb{F}_3$ to be $1+5x+12x^2+17x^3+22x^4+51x^5+108x^6+135x^7+81x^8$. Looking at the coefficient of x, we obtain $\#X_\Gamma(\mathbb{F}_3)=1+5+3=9$; substituting $x=1$, we obtain $\#J_\Gamma(\mathbb{F}_3)=432=2^4\cdot 3^3$. We deduce that $\#J_\Gamma(\mathbb{Q})$ divides 432.

Let A be the subgroup of $J_\Gamma(\mathbb{Q})$ generated by all differences of two rational cusps. Then A can be written as $A_2 \times A_3$, where A_2 and A_3 are the 2-primary and 3-primary subgroups of A, respectively, and it suffices to compute A_2 and A_3. The above bound on $\#J_\Gamma(\mathbb{Q})$ implies that $\#A_2$ divides 2^4 and $\#A_3$ divides 3^3. We claim that there are isomorphisms

$$(\mathbb{Z}/2\mathbb{Z})^4 \xrightarrow{\sim} A_2, \quad \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \xrightarrow{\sim} A_3.$$

We will prove this by computing the images of A_2 and A_3 under red_3.

To compute in $J_\Gamma(\mathbb{F}_3)$, we use Khuri-Makdisi's algorithmic framework for computing in Picard groups of projective curves [8, 9]. For a curve X over a field k, with Jacobian J, this gives us a way to represent elements of $J(k) \simeq \operatorname{Pic}^0 X$ and algorithms to perform the following operations:

- given two points $P, Q \in X(k)$, compute the divisor class $[P - Q] \in J(k)$;
- given two elements $x, y \in J(k)$, compute $-x - y$ (which also allows us to perform addition and negation);
- given an element $x \in J(k)$, test whether x is the zero element (which also allows us to test whether two elements are equal);
- given elements $x \in J(k)$ and $O \in X(k)$, compute the least $r \geq 0$ such that x is of the form $[D - rO]$ for some effective divisor D of degree r.

We used an unpublished implementation of Khuri-Makdisi's algorithms over finite fields by the first named author in PARI/GP [11]. For this we need to determine the space of global sections of a line bundle of sufficiently high degree. Starting from the equation (2) and using the line bundle $\mathcal{O}_{X_\Gamma}(2((0,\infty) + (-1,\infty) + (\infty,0) + (\infty,-1) + (\infty,\infty)))$ of degree 10, we obtain the basis $(1, u, v, uv, u^2, v^2, uv(u+v))$ for the space of global sections.

For every point $P \in X_\Gamma(\mathbb{F}_3)$, we consider the corresponding point $[P - (0,0)] \in J_\Gamma(\mathbb{F}_3)$. We define the following elements of $J_\Gamma(\mathbb{F}_3)$:

$$\begin{aligned} x_1 &= 9[(0,-1) - (0,0)], & y_1 &= 2[(-1,0) - (0,0)],\\ x_2 &= 9[(0,\infty) - (0,0)], & y_2 &= 2[(-1,-1) - (0,0)].\\ x_3 &= 9[(-1,0) - (0,0)], & &\\ x_4 &= 9[(-1,-1) - (0,0)], & & \end{aligned}$$

Then the points x_i have order 2, the point y_1 has order 9, and the point y_2 has order 3. We consider the group homomorphisms

$$\begin{aligned} \lambda_2\colon (\mathbb{Z}/2\mathbb{Z})^4 &\longrightarrow \operatorname{red}_3(A_2)\\ (a_1, a_2, a_3, a_4) &\longmapsto \sum_{i=1}^4 a_i x_i. \end{aligned}$$

and

$$\begin{aligned} \lambda_3\colon \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} &\longrightarrow \operatorname{red}_3(A_3)\\ (b_1, b_2) &\longmapsto b_1 y_1 + b_2 y_2. \end{aligned}$$

These fit in the following commutative diagrams:

$$\begin{tikzcd} (\mathbb{Z}/2\mathbb{Z})^4 \arrow[r] \arrow[dr, "\lambda_2"'] & A_2 \arrow[d, "\operatorname{red}_3"] \\ & \operatorname{red}_3(A_2) \end{tikzcd} \qquad \begin{tikzcd} \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \arrow[r] \arrow[dr, "\lambda_3"'] & A_3 \arrow[d, "\operatorname{red}_3"] \\ & \operatorname{red}_3(A_3) \end{tikzcd}$$

where the vertical maps $A_2 \to \operatorname{red}_3(A_2)$ and $A_3 \to \operatorname{red}_3(A_3)$ are isomorphisms. We show that λ_2 is injective by evaluating λ_2 on each element of $(\mathbb{Z}/2\mathbb{Z})^4$ and testing whether the result is zero. In a similar way, we show that λ_3 is injective. Comparing orders, we see that λ_2 and λ_3 are isomorphisms. Therefore both A and $\mathrm{red}_3(A)$ are isomorphic to $C_2 \times C_2 \times C_6 \times C_{18}$, and in particular have order 432. Finally, we deduce $J_\Gamma(\mathbb{F}_3) = \mathrm{red}_3(A)$ and $J_\Gamma(\mathbb{Q}) = A$. □

We now determine the image of the set of divisors of degree 3 under the map ϕ defined by (1).

Proposition 3.9. *The image of* $(\mathrm{Sym}^3 X_\Gamma)(\mathbb{Q})$ *under* ϕ *equals the set of points in* $J_\Gamma(\mathbb{Q})$ *represented by effective divisors of degree* 3 *supported on the cusps.*

Proof. Because X_Γ has 9 rational cusps and 3 Galois orbits of cusps with field of definition $\mathbb{Q}(\zeta_3)^+$, there are $\binom{9+3-1}{3} + 3 = 168$ effective divisors of degree 3 supported on the cusps. The nine $\mathbb{Q}$-rational cusps of X_Γ lie above three rational points of X_Γ/H, and also above three rational points of X_Γ/H'. Furthermore, none of the three Galois orbits of cusps with field of definition $\mathbb{Q}(\zeta_7)^+$ lies over a single rational point of X_Γ/H or X_Γ/H'. This implies that the 168 effective divisors of degree 3 supported on the cusps form 164 linear equivalence classes, namely 162 consisting of 1 divisor and 2 consisting of 3 divisors.

For each of the 432 points $x \in J_\Gamma(\mathbb{F}_3)$, we compute the least $r \geq 0$ such that x is of the form $[D - rO]$ for some effective divisor D of degree r on $(X_\Gamma)_{\mathbb{F}_3}$. This yields exactly 164 points in $J_\Gamma(\mathbb{F}_3)$ of the form $[D - 3O]$ with D an effective divisor of degree 3 on $(X_\Gamma)_{\mathbb{F}_3}$. Therefore at most 164 points in $J_\Gamma(\mathbb{Q})$ have this property, and since we already have 164 points in $J_\Gamma(\mathbb{Q})$ that are represented by effective divisors of degree 3 supported on the cusps, we are done. □

Proof of Theorem 1.2. An elliptic curve E over a cubic field K with an embedding of $C_2 \times C_{14}$ defines an effective divisor D of degree 3 on X_Γ, which we can view as a $\mathbb{Q}$-rational point of $\mathrm{Sym}^3 X_\Gamma$. Then $\phi(D)$ is a $\mathbb{Q}$-rational point of the image of ϕ in J_Γ. By Proposition 3.9 and the fact that D is evidently not supported on the cusps, D lies in one of the two copies of $\mathbb{P}^1_{\mathbb{Q}}$ inside $\mathrm{Sym}^3 X_\Gamma$ that are contracted under ϕ. It follows that D is the inverse image of a $\mathbb{Q}$-rational point on one of the two rational curves X_Γ/H and X_Γ/H' under the maps q_H and $q_{H'}$, respectively. This implies that K is normal over $\mathbb{Q}$. It is known that the field of definition of the two elliptic points of $X_*(7)$ equals $\mathbb{Q}(\zeta_3)$; see for example [5, § 4.4]. Thus D lies above a non-elliptic point $s \in X_*(7)(\mathbb{Q})$, and E is the base change to K of the fibre at s of the universal elliptic curve over the complement of the cusps and elliptic points in $X_*(7)$. We conclude that E is defined over $\mathbb{Q}$. □

Remark 3.10. Given an elliptic curve E over a cubic field K with a subgroup isomorphic to $C_2 \times C_{14}$, the proof of Theorem 1.2 yields the following procedure to determine a model of E over $\mathbb{Q}$. Choose a point P of order 7 in $E(K)$, and write down the unique Weierstrass equation for E such that the points P, $2P$ and $4P$ lie on the line $y = 0$ and the points $3P$, $5P$ and $6P$ lie on the line $y = -x$. Then this Weierstrass equation has coefficients in $\mathbb{Q}$.

Example 3.11. Consider the cubic field $K = \mathbb{Q}(\alpha)$ of discriminant 31^2, where $\alpha^3 - \alpha^2 - 10\alpha + 8 = 0$. The elliptic curve E over K defined by the Weierstrass equation

$$\begin{aligned} y^2 + xy + y = x^3 - x^2 &+ (-3737\alpha^2 - 8584\alpha + 9067)x \\ &+ (203770\alpha^2 + 468074\alpha - 494427) \end{aligned}$$

has torsion subgroup isomorphic to $C_2 \times C_{14}$, and the point $P = (14\alpha^2 + 32\alpha - 33, 59\alpha^2 + 136\alpha - 144)$ has order 7. After a change of variables to bring E in the form described by Remark 3.10 with respect to P, we obtain a Weierstrass equation with coefficients in $\mathbb{Q}$, namely

$$y^2 + xy = x^3 - \frac{2^2 \cdot 11}{3^2 \cdot 31}x^2 + \frac{2^6 \cdot 7}{3^5 \cdot 31^2}x + \frac{2^{12}}{3^9 \cdot 31^3}.$$

In fact, E is the base change of the elliptic curve over $\mathbb{Q}$ with Cremona label 1922c1.

Acknowledgements. We thank the referee for some helpful suggestions.

References

[1] W. Bosma, J. J. Cannon, C. Fieker, A. Steel (eds.), Handbook of Magma functions, Edition 2.20 (2014).

[2] J. G. Bosman, P. J. Bruin, A. Dujella and F. Najman, *Ranks of elliptic curves with prescribed torsion over number fields*, Int. Math. Res. Notices 2014 (2014), 2885–2923. 1, 2

[3] M. Derickx, S. Kamienny and B. Mazur, *Rational families of 17-torsion points of elliptic curves over number fields*, in: V. Kumar Murty (ed.), Momose Memorial Volume, Contemp. Math., to appear, http://www.math.harvard.edu/~mazur/papers/For.Momose20.pdf 1

[4] M. Derickx and A. V. Sutherland, *Torsion subgroups of elliptic curves over quintic and sextic number fields*, Proc. Amer. Math. Soc., to appear. 3.1

[5] N. D. Elkies, *The Klein quartic in number theory*, in: S. Levy (ed.), *The eightfold way. The beauty of Klein's quartic curve*, Cambridge University Press, Cambridge, 1999. 3.2

[6] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag, New York, 1977. 3.1

[7] K. Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, Cohomologies p-adiques et applications arithmétiques. III. Astérisque 295 (2004), 117–290. 3.2

[8] K. Khuri-Makdisi, *Linear algebra algorithms for divisors on an algebraic curve*, Math. Comp. 73 (2004), 333–357. 3.2

[9] K. Khuri-Makdisi, *Asymptotically fast group operations on Jacobians of general curves*, Math. Comp. 76 (2007), 2213–2239. 3.2

[10] F. Najman, *Torsion of rational elliptic curves over cubic fields and sporadic points on $X_1(n)$*, Math. Res. Letters 23 (2016), 245–272. 1

[11] The PARI Group, PARI/GP (version 2.7.6), Bordeaux, 2016, http://pari.math.u-bordeaux.fr/. 3.2

[12] F. P. Rabarison, *Structure de torsion des courbes elliptiques sur les corps quadratiques*, Acta Arith. 144 (2010), 17–52. 2

[13] The Sage Developers, SageMath, the Sage Mathematics Software System (version 7.2), 2016, http://www.sagemath.org/. 3.2

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

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