# 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 $E(K) \simeq$ $E(K)_{\text {tor }} \oplus \mathbb{Z}^{r}$, 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 $E(K)_{\text {tor }} \simeq G$. In this paper we will show that for $d=2$ and $d=3$ and for certain groups $G \in \Phi(d)$, if $E(K)_{\text {tor }} \simeq G$, 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 $\operatorname{Gal}(L / \mathbb{Q})$ is isomorphic to $D_{4}$ or $S_{4}$.

The goal of this paper is to prove the following two theorems.
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 $\mathbb{Q}$.
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 obtain these results by studying geometric properties of modular curves and maps between modular curves, and combining these with the modular description of these curves and maps. The basic idea is as follows. For a congruence subgroup $\Gamma \subseteq \mathrm{SL}_{2}(\mathbb{Z})$, let $X_{\Gamma}$ be the corresponding

[^0]modular curve, let $g\left(X_{\Gamma}\right)$ denote its genus, and let $Y_{\Gamma}$ be the complement of the cusps in $X_{\Gamma}$. Let $\Gamma \supseteq \Gamma^{\prime}$ be two congruence subgroups of $\mathrm{SL}_{2}(\mathbb{Z})$ not containing the matrix $\left(\begin{array}{cc}-1 & 0 \\ 0 & -1\end{array}\right)$. For the pairs $\Gamma \supseteq \Gamma^{\prime}$ that we will study, it turns out that for a suitable $d$, all points of degree $d$ on $Y_{\Gamma}$ map to $\mathbb{Q}$-rational points of $Y_{\Gamma^{\prime}}$ under the natural morphism $X_{\Gamma} \rightarrow X_{\Gamma^{\prime}}$. The modular descriptions of $X_{\Gamma}$ and $X_{\Gamma^{\prime}}$ then allow us to conclude that the points of degree $d$ on $Y_{\Gamma}$ in fact parametrize elliptic curves defined over $\mathbb{Q}$.

## 2. Elliptic curves with 16 -Torsion over quadratic fields

In this section we will prove Theorem 1.1. We start by taking $\Gamma=\Gamma_{1}(16)$ and

$$
\Gamma^{\prime}=\left\{\left(\begin{array}{ll}
a & b \\
c & d
\end{array}\right) \in \mathrm{SL}_{2}(\mathbb{Z}) \left\lvert\, \begin{array}{rr}
a \equiv d \equiv 1 & (\bmod 8), \\
c \equiv 0 & (\bmod 16)
\end{array}\right.\right\} .
$$

The curves $X_{1}(16)$ and $X_{\Gamma^{\prime}}$ have genus 2 and 0 , respectively, and the map

$$
\pi: X_{1}(16) \rightarrow X_{\Gamma^{\prime}}
$$

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 $\pi$ of $\mathbb{Q}$-rational points of $Y_{\Gamma^{\prime}}$.

Now 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 $\sigma$ be the generator of $\operatorname{Gal}(K / \mathbb{Q})$. Using the fact that the hyperelliptic involution on $X_{1}(16)$ is the diamond automorphism $\langle 9\rangle$, it was proved in [2] that there exists an isomorphism

$$
\mu: E^{\sigma} \rightarrow E
$$

satisfying $\mu \circ \mu^{\sigma}=$ id. Replacing $\mu$ by $-\mu$ if necessary, we may assume in addition

$$
\mu\left(P^{\sigma}\right)=9 P .
$$

Noting that $9(2 P)=18 P=2 P$, we deduce that the isomorphism $\mu$ maps $(2 P)^{\sigma}$ to $2 P$. This shows that not only $E$, but also the pair $(E, 2 P)$ is defined over $\mathbb{Q}$.

The above argument can be made explicit as follows. The modular curve $X_{1}(16)$ admits the equation

$$
X_{1}(16): v^{2}-\left(u^{3}+u^{2}-u+1\right) v+u^{2}=0 .
$$

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 $E$, and then descend the pair $(E, 2 P)$ to $\mathbb{Q}$ by writing $E$ in Tate normal form with respect to the point $2 P$. This gives the Weierstrass equation

$$
E: y^{2}+a x y+b y=x^{3}+b x \text { with } 2 P=(0,0)
$$

where $a$ and $b$ are given by

$$
\begin{aligned}
& a=1-\frac{u^{2}(u-1)(u+1)}{u^{2}+1}, \\
& b=\frac{-u^{2}(u-1)(u+1)}{\left(u^{2}+1\right)^{2}} .
\end{aligned}
$$

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 $\Gamma$ and the corresponding modular curve $X_{\Gamma}$ 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 $\left(\Gamma_{*}(2): \Gamma(2)\right)=3$; more precisely,

$$
\Gamma_{*}(2)=\left\{\Gamma \in \mathrm{SL}_{2}(\mathbb{Z}) \left\lvert\, \gamma \equiv\left(\begin{array}{ll}
1 & 0 \\
0 & 1
\end{array}\right)\right.,\left(\begin{array}{ll}
1 & 1 \\
1 & 0
\end{array}\right),\left(\begin{array}{ll}
0 & 1 \\
1 & 1
\end{array}\right) \quad(\bmod 2)\right\} .
$$

We also define

$$
\Gamma_{*}(7)=\left\{\left(\begin{array}{ll}
a & b \\
c & b
\end{array}\right) \in \mathrm{SL}_{2}(\mathbb{Z}) \left\lvert\, \begin{array}{c}
a, d \equiv 1,2,4 \quad(\bmod 7), \\
c \equiv 0 \quad(\bmod 7)
\end{array}\right.\right\}
$$

This will play the role of the group denoted by $\Gamma^{\prime}$ in the introduction. We note that $\Gamma_{*}(7)$ does not contain the matrix $\left(\begin{array}{cc}-1 & 0 \\ 0 & -1\end{array}\right)$. 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

$$
\begin{aligned}
A_{3} & =\left(\Gamma_{*}(2) \cap \Gamma_{1}(7)\right) / \Gamma, \\
C_{3} & =\left(\Gamma(2) \cap \Gamma_{*}(7)\right) / \Gamma, \\
A_{3} \times C_{3} & =\left(\Gamma_{*}(2) \cap \Gamma_{*}(7)\right) / \Gamma .
\end{aligned}
$$

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 $H^{\prime}$.
3.1. Geometric properties of modular curves. The modular curve $X_{\Gamma}$ 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 $X_{\Gamma}$. The action of the various subgroups of interest gives rise to the following diagram, where the numbers next to the arrows indicate the degrees:


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 $X \rightarrow X(1)$, at this cusp.

Lemma 3.1. The curve $X_{\Gamma}$ has genus 4 . It has 18 cusps: 9 of index 2 and 9 of index 14.

Proof. The map $X_{\Gamma} \rightarrow X_{1}(14)$ 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

$$
2 g\left(X_{\Gamma}\right)-2=2\left(2 g\left(X_{1}(14)\right)-2\right)+6 .
$$

Both statements now follow easily.
Lemma 3.2. The groups $A_{3}$ and $C_{3}$ act freely on $X_{\Gamma}$.
Proof. The action of the group $C_{3}$ on $X_{\Gamma}$ 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 $X_{\Gamma}$.

The group $A_{3}$ acts freely on $Y_{\Gamma}$ because $Y_{\Gamma}$ is a fine modular curve. 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

$$
\begin{aligned}
& X_{\Gamma} \rightarrow X_{\Gamma} / A_{3} \\
& X_{\Gamma} \rightarrow X_{\Gamma} / C_{3}
\end{aligned}
$$

are unramified. Each of the curves $X_{\Gamma} / A_{3}$ and $X_{\Gamma} / C_{3}$ 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 the lemma; the last one follows from the Hurwitz formula.
Lemma 3.4. (1) The curve $X_{\Gamma} /\left(A_{3} \times C_{3}\right)$ has genus 0 . It has two cusps: one of index 2 and one of index 14.
(2) The map $X_{\Gamma} \rightarrow X_{\Gamma} /\left(A_{3} \times C_{3}\right)$ has ramification index 3 at 12 points of $X_{\Gamma}$ (lying above 4 points of $\left.X_{\Gamma} /\left(A_{3} \times C_{3}\right)\right)$ and is unramified everywhere else.
Proof. The map $X_{\Gamma} / A_{3} \rightarrow X_{1}(7)$ is unramified over $Y_{1}(7)$, since $Y_{1}(7)$ is a fine moduli space. This implies that the map $X_{\Gamma} /\left(A_{3} \times C_{3}\right) \rightarrow X_{*}(7)$ 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 $X_{\Gamma} /\left(A_{3} \times C_{3}\right)$ has genus 0 . This proves (1).

For (2), we observe that by the Hurwitz formula and the fact that the map $X_{\Gamma} / A_{3} \rightarrow X_{\Gamma} /\left(A_{3} \times C_{3}\right)$ is cyclic of degree 3 , this map is totally ramified at 4 points. The claim now follows from the fact that the map $X_{\Gamma} \rightarrow X_{\Gamma} / A_{3}$ is unramified (the same argument works for $C_{3}$ ).
Lemma 3.5. The curves $X_{\Gamma} / H$ and $X_{\Gamma} / H^{\prime}$ have genus 0 .
Proof. Let $P$ be one of the 12 ramification points of the map $X_{\Gamma} \rightarrow X_{\Gamma} /\left(A_{3} \times C_{3}\right)$. Then the stabilizer (decomposition group) $G_{P}$ 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 $X_{\Gamma}$. Therefore $G_{P}$ is either $H$ or $H^{\prime}$. Let $n_{H}$ be the number of points $P \in X_{\Gamma}$ with stabilizer $H$, and similarly for $n_{H^{\prime}}$. The Hurwitz formula gives

$$
\begin{gathered}
2 g\left(X_{\Gamma}\right)-2=3\left(g\left(X_{\Gamma} / H\right)-2\right)+2 n_{H} \\
2 g\left(X_{\Gamma}\right)-2=3\left(g\left(X_{\Gamma} / H^{\prime}\right)-2\right)+2 n_{H^{\prime}} .
\end{gathered}
$$

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

We conclude that the curve $X_{\Gamma}$ admits two maps of degree 3 to a curve of genus 0 , namely the quotient maps

$$
q_{H}: X_{\Gamma} \rightarrow X_{\Gamma} / H, \quad q_{H^{\prime}}: X_{\Gamma} \rightarrow X_{\Gamma} / H^{\prime} .
$$

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

We fix one rational cusp, say $O=(0,0)$, and we consider the Jacobian $J_{\Gamma}$ of $X_{\Gamma}$ and the (nondominant) rational map

$$
\begin{align*}
\phi: \mathrm{Sym}^{3} X_{\Gamma} & \rightarrow J_{\Gamma} \\
D & \mapsto[D-3 O] \tag{1}
\end{align*}
$$

Lemma 3.6. The map $\phi$ contracts the lines $L$ and $L^{\prime}$ and is injective outside $L \cup L^{\prime}$.
Proof. Consider two distinct points of $\mathrm{Sym}^{3} X_{\Gamma}$ corresponding to effective divisors $D, D^{\prime}$ of degree 3 on $X_{\Gamma}$. Then $\phi(D)=\phi\left(D^{\prime}\right)$ if and only if $D$ and $D^{\prime}$ are linearly equivalent. In this case, there exists a rational function $f$ on $X_{\Gamma}$ such that $\operatorname{div}(f)=D-D^{\prime}$. Such an $f$ gives a map of degree at most 3 to $\mathbb{P}_{\mathbb{Q}}^{1}$; this can be identified with either $q_{H}$ or $q_{H^{\prime}}$, since $X_{\Gamma}$ is not hyperelliptic. This implies that $\phi(D)=\phi\left(D^{\prime}\right)$ if and only if either both $D$ and $D^{\prime}$ are pull-backs of points under $q_{H}: X_{\Gamma} \rightarrow X_{\Gamma} / H$, or both are pull-backs of points under $q_{H^{\prime}}: X_{\Gamma} \rightarrow X_{\Gamma} / H^{\prime}$.
3.2. Modular description of $X_{1}(7)$ and $X_{*}(7)$. The curve $X_{1}(7)$ is isomorphic to $\mathbb{P}_{\mathbb{Q}}^{1}$. In terms of a suitable coordinate $d$ on $X_{1}(7)$, the universal elliptic curve over $Y_{1}(7)$ is given by

$$
E_{1}(7): y^{2}+\left(1+d-d^{2}\right) x y+\left(d^{2}-d^{3}\right) y=x^{3}+\left(d^{2}-d^{3}\right) x^{2},
$$

equipped with the distinguished point $(0,0)$ of order 7 . The cusps are given by $d=0, d=1, d=\infty$ and $d^{3}-8 d^{2}+5 d+1=0$. The diamond automorphisms are given by

$$
\begin{aligned}
& \langle \pm 1\rangle d=d, \\
& \langle \pm 2\rangle d=(d-1) / d, \\
& \langle \pm 3\rangle d=-1 /(d-1) .
\end{aligned}
$$

The locus of common fixed points of these automorphisms is given by $d^{2}-d+1=0$.
The curve $X_{*}(7)$ is the quotient of $X_{1}(7)$ by the group of diamond automorphisms $\{\langle 1\rangle,\langle 2\rangle,\langle 4\rangle\}$. The fixed points of these automorphisms on $X_{1}(7)$ map to two elliptic points on $X_{*}(7)$. Let $U_{*}(7)$ be the complement of the cusps and the elliptic points on $X_{*}(7)$. Then $U$ is the fine part of the modular curve classifying elliptic curves equipped with a subscheme that is étale locally of the form $P+2 P+4 P$ with $P$ a point of order 7 , and the universal elliptic curve over $X_{1}(7)$ descends to $U$.

In terms of the coordinate

$$
s=d+\frac{d-1}{d}-\frac{1}{d-1}=\frac{d^{3}-3 d+1}{d(d-1)}
$$

on $X_{*}(7)$, the cusps are $s=8$ and $s=\infty$, and the elliptic points are given by $s^{2}-3 s+9=0$. Starting from $E_{1}(7)$ and the distinguished point $P$ of order 7 , we can obtain an equation for the universal elliptic curve $E_{*}(7)$ over $U$ via the unique change of variables bringing the equation for $E_{1}(7)$ into the form

$$
y^{2}+x y=x^{3}+a_{2} x^{2}+a_{4} x+a_{6}
$$

with the points $P, 2 P$ and $4 P$ lying on the line $y=0$ and the points $3 P, 5 P$ and $6 P$ lying on the line $y=-x$. We obtain

$$
\begin{aligned}
& a_{2}=-\frac{d(d-1)\left(d^{3}-3 d+1\right)}{\left(d^{2}-d+1\right)^{3}}=-\frac{s}{s^{2}-3 s+9} \\
& a_{4}=\frac{d^{3}(d-1)^{3}\left(d^{3}-3 d^{2}+1\right)}{\left(d^{2}-d+1\right)^{6}}=\frac{s-3}{\left(s^{2}-3 s+9\right)^{2}} \\
& a_{6}=\frac{d^{6}(d-1)^{6}}{\left(d^{2}-d+1\right)^{9}}=\frac{1}{\left(s^{2}-3 s+9\right)^{3}}
\end{aligned}
$$

and hence $E_{*}(7)$ is given by

$$
\begin{equation*}
E_{*}(7): y^{2}+x y=x^{3}-\frac{s}{s^{2}-3 s+9} x^{2}+\frac{s-3}{\left(s^{2}-3 s+9\right)^{2}} x+\frac{1}{\left(s^{2}-3 s+9\right)^{3}} \tag{2}
\end{equation*}
$$

3.3. Modular description of $X_{\Gamma}$. We view $X_{\Gamma}$ 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 $\{0,1,2\}$.

In view of the action of the diamond automorphisms on $X_{1}(7)$, we put

$$
\delta_{0}=d, \quad \delta_{1}=\frac{d-1}{d}, \quad \delta_{2}=\frac{1}{1-d}
$$

Let $\xi_{0}, \xi_{1}, \xi_{2}$ be the $x$-coordinates of the three points of order 2 with respect to the above model for the universal elliptic curve $E_{1}(7)$ over $Y_{1}(7)$. Then $\xi_{0}, \xi_{1}, \xi_{2}$ are the three zeroes of the 2-division polynomial of $E_{1}(7)$, i.e.
$4\left(x-\xi_{0}\right)\left(x-\xi_{1}\right)\left(x-\xi_{2}\right)=4 x^{3}+\left(d^{4}-6 d^{3}+3 d^{2}+2 d+1\right) x^{2}+2 d^{2}(d-1)\left(d^{2}-d-1\right) x+d^{4}(d-1)^{2}$.
We define

$$
\zeta_{i}=\xi_{i} \frac{d^{2}-d+1}{d^{2}(d-1)^{2}}+\frac{1}{1-d} \quad \text { for } i=1,2,3
$$

and

$$
\begin{aligned}
t & =\frac{4}{d^{4}(d-1)^{4}}\left(\xi_{1}-\xi_{0}\right)\left(\xi_{0}-\xi_{2}\right)\left(\xi_{2}-\xi_{1}\right) \\
& =4 \frac{d^{2}(d-1)^{2}}{\left(d^{2}-d+1\right)^{3}}\left(\zeta_{1}-\zeta_{0}\right)\left(\zeta_{0}-\zeta_{2}\right)\left(\zeta_{2}-\zeta_{1}\right)
\end{aligned}
$$

Then we have the identities

$$
\begin{equation*}
t^{2}=\frac{d^{3}-8 d^{2}+5 d+1}{d(d-1)} \tag{3}
\end{equation*}
$$

and

$$
4\left(\zeta_{0}-\zeta_{1}\right)\left(\zeta_{0}-\zeta_{2}\right)\left(\zeta_{1}-\zeta_{2}\right)=t\left(t^{2}-t+7\right)\left(t^{2}+t+7\right)
$$

and $\zeta_{0}, \zeta_{1}, \zeta_{2}$ are the three zeroes of the polynomial

$$
4\left(x-\zeta_{0}\right)\left(x-\zeta_{1}\right)\left(x-\zeta_{2}\right)=4 x^{3}+\left(t^{4}+9 t^{2}+17\right) x^{2}+\left(4 t^{2}+20\right) x+4
$$

Lemma 3.7. Let $f=x^{3}+p x^{2}+q x+r$ be a separable monic cubic polynomial over a field $K$, and let $\alpha, \beta$, $\gamma$ be the roots of $f$ in some splitting field of $f$ over $K$. Let $\delta=(\beta-\alpha)(\alpha-\gamma)(\gamma-\beta)$, so that $\delta^{2}$ equals the discriminant of $f$. Then we have

$$
\begin{aligned}
& \beta=\frac{-(p q-9 r-\delta) \alpha+\left(6 p r-2 q^{2}\right)}{\left(2 p^{2}-6 q\right) \alpha+(p q-9 r+\delta)}, \\
& \gamma=\frac{-(p q-9 r+\delta) \alpha+\left(6 p r-2 q^{2}\right)}{\left(2 p^{2}-6 q\right) \alpha+(p q-9 r-\delta)} .
\end{aligned}
$$

Proof. This is a straightforward verification.
With $(\alpha, \beta, \gamma)=\left(\zeta_{0}, \zeta_{1}, \zeta_{2}\right)$, Lemma 3.7 implies the identities

$$
\begin{aligned}
& \zeta_{1}=-2 \frac{\left(t^{2}-t+1\right) \zeta_{0}+2}{\left(t^{4}+5 t^{2}+1\right) \zeta_{0}+2\left(t^{2}+t+1\right)}, \\
& \zeta_{2}=-2 \frac{\left(t^{2}+t+1\right) \zeta_{0}+2}{\left(t^{4}+5 t^{2}+1\right) \zeta_{0}+2\left(t^{2}-t+1\right)} .
\end{aligned}
$$

Our definitions imply that $\delta_{0}, \delta_{1}, \delta_{2}$ are the three solutions of the equation

$$
\delta^{3}-\left(t^{2}+8\right) \delta^{2}+\left(t^{2}+5\right) \delta+1=0
$$

and $\zeta_{0}, \zeta_{1}, \zeta_{2}$ are the three solutions of the equation

$$
\zeta^{3}+\frac{1}{4}\left(t^{4}+9 t^{2}+17\right) \zeta^{2}+\left(t^{2}+5\right) \zeta+1=0
$$

To study the quotients $X_{\Gamma} / H$ and $X_{\Gamma} / H^{\prime}$, which are isomorphic to $\mathbb{P}_{\mathbb{Q}}^{1}$, we define

$$
\begin{aligned}
& \eta_{+}=4\left(\delta_{0} \zeta_{0}+\delta_{1} \zeta_{1}+\delta_{2} \zeta_{2}\right), \\
& \eta_{-}=4\left(\delta_{0} \zeta_{0}+\delta_{1} \zeta_{2}+\delta_{2} \zeta_{1}\right)
\end{aligned}
$$

Then one computes the minimal polynomials of $\eta_{+}$and $\eta_{-}$over $\mathbb{Q}(t)$ as

$$
\begin{aligned}
F_{+}=x^{3} & +\left(t^{6}+17 t^{4}+89 t^{2}+136\right) x^{2}+\left(t^{10}+23 t^{8}+221 t^{6}+1169 t^{4}+3643 t^{2}+5365\right) x \\
& -\left(t^{12}+19 t^{10}+8 t^{9}+78 t^{8}+208 t^{7}-761 t^{6}+2136 t^{5}\right. \\
& \left.-8866 t^{4}+10192 t^{3}-33885 t^{2}+19208 t-48791\right)
\end{aligned}
$$

and

$$
\begin{gathered}
F_{-}=x^{3}+\left(t^{6}+17 t^{4}+89 t^{2}+136\right) x^{2}+\left(t^{10}+23 t^{8}+221 t^{6}+1169 t^{4}+3643 t^{2}+5365\right) x \\
-\left(t^{12}+19 t^{10}-8 t^{9}+78 t^{8}-208 t^{7}-761 t^{6}-2136 t^{5}\right. \\
\left.-8866 t^{4}-10192 t^{3}-33885 t^{2}-19208 t-48791\right) .
\end{gathered}
$$

Each of the polynomials $F_{+}$and $F_{-}$defines a singular curve that is birational to $\mathbb{P}_{\mathbb{Q}}^{1}$. More precisely, we consider the functions

$$
\begin{aligned}
& y_{+}=-\frac{\left(t^{3}+6 t+1\right) \eta_{+}+\left(t^{7}-t^{6}+14 t^{5}-11 t^{4}+70 t^{3}-27 t^{2}+125 t+78\right)}{\left(t^{2}+t+3\right) \eta_{+}+\left(t^{7}+15 t^{5}+t^{4}+71 t^{3}+33 t^{2}+78 t+185\right)} \\
& y_{-}=\frac{\left(t^{3}+6 t-1\right) \eta_{-}+\left(t^{7}+t^{6}+14 t^{5}+11 t^{4}+70 t^{3}+27 t^{2}+125 t-78\right)}{\left(t^{2}-t+3\right) \eta_{-}+\left(-t^{7}-15 t^{5}+t^{4}-71 t^{3}+33 t^{2}-78 t+185\right)}
\end{aligned}
$$

Then $y_{+}$and $y_{-}$are rational parameters for the curves defined by $F_{+}$and $F_{-}$, respectively, and one can write

$$
\begin{aligned}
\eta_{+} & =-\frac{y_{+}^{12}+2 y_{+}^{11}+5 y_{+}^{10}+14 y_{+}^{9}+24 y_{+}^{8}+32 y_{+}^{7}+37 y_{+}^{6}+28 y_{+}^{5}+14 y_{+}^{4}+16 y_{+}^{3}+15 y_{+}^{2}+6 y_{+}+1}{y_{+}^{4}\left(y_{+}+1\right)^{2}} \\
t & =-\frac{y_{+}^{3}+y_{+}^{2}-2 y_{+}-1}{y_{+}\left(y_{+}+1\right)}
\end{aligned}
$$

and

$$
\begin{aligned}
\eta_{-} & =-\frac{y_{-}^{12}+2 y_{-}^{11}+5 y_{-}^{10}+14 y_{-}^{9}+24 y_{-}^{8}+32 y_{-}^{7}+37 y_{-}^{6}+28 y_{-}^{5}+14 y_{-}^{4}+16 y_{-}^{3}+15 y_{-}^{2}+6 y_{-}+1}{y_{-}^{4}\left(y_{-}+1\right)^{2}} \\
t & =\frac{y_{-}^{3}+y_{-}^{2}-2 y_{-}-1}{y_{-}\left(y_{-}+1\right)}
\end{aligned}
$$

Taking $(u, v)=\left(y_{+}, y_{-}\right)$as coordinates on $X_{\Gamma}$, we see that $X_{\Gamma}$ is the smooth curve of bidegree $(3,3)$ in $\mathbb{P}_{\mathbb{Q}}^{1} \times \mathbb{P}_{\mathbb{Q}}^{1}$ given by the equation

$$
X_{\Gamma}: \frac{u^{3}+u^{2}-2 u-1}{u(u+1)}+\frac{v^{3}+v^{2}-2 v-1}{v(v+1)}=0
$$

or equivalently

$$
\begin{equation*}
X_{\Gamma}:\left(u^{3}+u^{2}-2 u-1\right) v(v+1)+\left(v^{3}+v^{2}-2 v-1\right) u(u+1)=0 \tag{4}
\end{equation*}
$$

As noted in Lemma 3.1, $X_{\Gamma}=X_{1}(2,14)$ has 9 cusps over $\mathbb{Q}$ (and no other rational points) and 9 cusps over the cubic subfield of $\mathbb{Q}\left(\zeta_{7}\right)$. The $(u, v)$-coordinates of the 9 rational cusps are

$$
\begin{array}{cll}
(0,0), & (0,-1), & (0, \infty) \\
(-1,0), & (-1,-1), & (-1, \infty) \\
(\infty, 0), & (\infty,-1), & (\infty, \infty)
\end{array}
$$

The 9 cusps with field of definition $\mathbb{Q}\left(\zeta_{7}\right)^{+}$are defined by

$$
u^{3}+u^{2}-2 u-1=v^{3}+v^{2}-2 v-1=0
$$

3.4. Proof of the main result. We first determine the structure of $J_{\Gamma}(\mathbb{Q})$.

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 $J_{\Gamma}$ over $\mathbb{Q}$ decomposes up to isogeny as $J_{\Gamma} \sim E \times E \times B$, where $E$ is the elliptic curve $J_{1}(14)$ of conductor 14 and $B$ is the Jacobian of the smooth curve of genus 2 defined by the equation

$$
e^{2}=d(d-1)\left(d^{3}-8 d^{2}+5 d+1\right)
$$

which is obtained from (3) by the change of variables $e=d(d-1) t$. Using the Magma function RankBound [1], one computes the ranks of $E$ and $B$ to be 0 . Alternatively, a computation with newforms in either Magma or Sage [9] shows that the $L$-functions of $E$ and $B$ do not vanish at 1. By results of Kato [5], the Birch-Swinnerton-Dyer conjecture is true for quotients of modular Jacobians. Either way, we conclude that the rank of $J_{\Gamma}(\mathbb{Q})$ is 0 .

Let $\operatorname{red}_{3}$ denote the reduction map $J_{\Gamma}(\mathbb{Q}) \rightarrow J_{\Gamma}\left(\mathbb{F}_{3}\right)$. Then red ${ }_{3}$ is injective. One computes the numerator of the zeta function of $X_{\Gamma}$ over $\mathbb{F}_{3}$ to be $1+5 x+12 x^{2}+17 x^{3}+22 x^{4}+51 x^{5}+108 x^{6}+$ $135 x^{7}+81 x^{8}$. Looking at the coefficient of $x$, we obtain $\# X_{\Gamma}\left(\mathbb{F}_{3}\right)=1+5+3=9$; substituting $x=1$, we obtain $\# J_{\Gamma}\left(\mathbb{F}_{3}\right)=432=2^{4} \cdot 3^{3}$. 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 $J_{\Gamma}\left(\mathbb{F}_{3}\right)$, we use Khuri-Makdisi's algorithmic framework for computing in Picard groups of projective curves $[6,7]$. 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 $x=0$ (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 [ $D-r O$ ] 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 [8]. For this we need to determine the space of global sections of a line bundle of sufficiently high degree. Starting from the equation (4) 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 ( $\left.1, u, v, u v, u^{2}, v^{2}, u v(u+v)\right)$ for the space of global sections.

For every point $P \in X_{\Gamma}\left(\mathbb{F}_{3}\right)$, we consider the corresponding point $[P-(0,0)] \in J_{\Gamma}\left(\mathbb{F}_{3}\right)$. We define the following elements of $J_{\Gamma}\left(\mathbb{F}_{3}\right)$ :

$$
\begin{array}{ll}
x_{1}=9[(0,-1)-(0,0)], & y_{1}=2[(-1,0)-(0,0)], \\
x_{2}=9[(0, \infty)-(0,0)], & y_{2}=2[(-1,-1)-(0,0)] . \\
x_{3}=9[(-1,0)-(0,0)], & \\
x_{4}=9[(-1,-1)-(0,0)], &
\end{array}
$$

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

$$
\begin{aligned}
\lambda_{2}:(\mathbb{Z} / 2 \mathbb{Z})^{4} & \longrightarrow \operatorname{red}_{3}\left(A_{2}\right) \\
\left(a_{1}, a_{2}, a_{3}, a_{4}\right) & \longmapsto \sum_{i=1}^{4} a_{i} x_{i} .
\end{aligned}
$$

and

$$
\begin{aligned}
\lambda_{3}: \mathbb{Z} / 9 \mathbb{Z} \times \mathbb{Z} / 3 \mathbb{Z} & \longrightarrow \operatorname{red}_{3}\left(A_{3}\right) \\
\left(b_{1}, b_{2}\right) & \longmapsto b_{1} y_{1}+b_{2} y_{2} .
\end{aligned}
$$

These fit in the following commutative diagrams:

where the vertical maps $A_{2} \rightarrow \operatorname{red}_{3}\left(A_{2}\right)$ and $A_{3} \rightarrow \operatorname{red}_{3}\left(A_{3}\right)$ are isomorphisms. We show that $\lambda_{2}$ is injective by evaluating $\lambda_{2}$ on each element of $(\mathbb{Z} / 2 \mathbb{Z})^{4}$ and testing whether the result is zero. In a similar way, we show that $\lambda_{3}$ is injective. Comparing orders, we see that $\lambda_{2}$ and $\lambda_{3}$ are isomorphisms. Therefore both $A$ and $\operatorname{red}_{3}(A)$ are isomorphic to $C_{2} \times C_{2} \times C_{6} \times C_{18}$, and in particular have order 432 . Finally, we deduce $J_{\Gamma}\left(\mathbb{F}_{3}\right)=\operatorname{red}_{3}(A)$ and $J_{\Gamma}(\mathbb{Q})=A$.

We now determine the image of the set of divisors of degree 3 under the map $\phi$ defined by (1).
Proposition 3.9. The image of $\left(\operatorname{Sym}^{3} X_{\Gamma}\right)(\mathbb{Q})$ under $\phi$ equals the set of points in $J_{\Gamma}(\mathbb{Q})$ represented by effective divisors of degree 3 supported on the cusps.

Proof. Because $X_{\Gamma}$ has 9 rational cusps and 3 Galois orbits of cusps with field of definition $\mathbb{Q}\left(\zeta_{3}\right)^{+}$, there are $\left({ }_{3}^{9+3-1}\right)+3=168$ effective divisors of degree 3 supported on the cusps. The nine $\mathbb{Q}$-rational cusps of $X_{\Gamma}$ lie above three rational points of $X_{\Gamma} / H$, and also above three rational points of $X_{\Gamma} / H^{\prime}$. Furthermore, none of the three Galois orbits of cusps with field of definition $\mathbb{Q}\left(\zeta_{7}\right)^{+}$lies over a single rational point of $X_{\Gamma} / H$ or $X_{\Gamma} / H^{\prime}$. 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 $x \in J_{\Gamma}\left(\mathbb{F}_{3}\right)$, we compute the least $r \geq 0$ such that $x$ is of the form [ $D-r O$ ] for some effective divisor $D$ of degree $r$ on $\left(X_{\Gamma}\right)_{\mathbb{F}_{3}}$. This yields exactly 164 points in $J_{\Gamma}\left(\mathbb{F}_{3}\right)$ of the form $[D-3 O]$ with $D$ an effective divisor of degree 3 on $\left(X_{\Gamma}\right)_{\mathbb{F}_{3}}$. 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 $X_{\Gamma}$, which we can view as a $\mathbb{Q}$-rational point of $\operatorname{Sym}^{3} X_{\Gamma}$. Then $\phi(D)$ is a $\mathbb{Q}$-rational point of the subvariety $\operatorname{im}(\phi)$ of $J_{\Gamma}$. 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 $\mathbb{P}_{\mathbb{Q}}^{1}$ inside $\operatorname{Sym}^{3} X_{\Gamma}$ that are contracted under $\phi$. It follows that $D$ is the inverse image of some $\mathbb{Q}$-rational point on one of the two rational curves $X_{\Gamma} / H$ and $X_{\Gamma} / H^{\prime}$ under the maps $q_{H}$ and $q_{H^{\prime}}$, respectively. This implies that $K$ is normal over $\mathbb{Q}$. Furthermore, mapping $D$ to $X_{*}(7)$ and noting that the elliptic points of $X_{*}(7)$ are not defined over $\mathbb{Q}$, we obtain an element $s \in \mathbb{Q}$ such that $E$ is the base change to $K$ of the fibre at $s$ of the family $E_{*}(7)$ given by (2). 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 $P, 2 P$ and $4 P$ lie on the line $y=0$ and the points $3 P, 5 P$ and $6 P$ 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

$$
y^{2}+x y+y=x^{3}-x^{2}+\left(-3737 \alpha^{2}-8584 \alpha+9067\right) x+\left(203770 \alpha^{2}+468074 \alpha-494427\right)
$$

has torsion subgroup isomorphic to $C_{2} \times C_{14}$, and the point $P=\left(14 \alpha^{2}+32 \alpha-33,59 \alpha^{2}+136 \alpha-144\right)$ 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 the fibre of the family $E_{*}(7)$ given by (2) at $s=33 / 4$. Finally, we note that $E$ is the base change of the elliptic curve over $\mathbb{Q}$ with Cremona label 1922c1.

## References

[1] W. Bosma, J. J. Cannon, C. Fieker, A. Steel (eds.), Handbook of Magma functions, Edition 2.20 (2014). 3.4
[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. http://www.math.harvard.edu/~mazur/papers/For.Momose20.pdf 1
[4] R. Hartshorne, Algebraic Geometry, Springer-Verlag, New York, 1977. 3.1
[5] 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. 3.4
[6] K. Khuri-Makdisi, Linear algebra algorithms for divisors on an algebraic curve, Math. Comp. 73 (2004), no. 245, 333-357. 3.4
[7] K. Khuri-Makdisi, Asymptotically fast group operations on Jacobians of general curves, Math. Comp. 76 (2007), no. 260, 2213-2239. 3.4
[8] The PARI Group, PARI/GP (version 2.7.6), Bordeaux, 2016, http://pari.math.u-bordeaux.fr/. 3.4
[9] The Sage Developers, SageMath, the Sage Mathematics Software System (version 7.2), 2016, http://www.sagemath.org/. 3.4

Mathematisch Instituut, Universiteit Leiden, Postbus 9512, 2300 RA Leiden, Netherlands
E-mail address: P.J.Bruin@math.leidenuniv.nl
Department of Mathematics, University of Zagreb, Bijenička cesta 30, 10000 Zagreb, Croatia
E-mail address: fnajman@math.hr


[^0]:    The first author was partially supported by a Veni grant from the Netherlands Organisation for Scientific Research (NWO).

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

