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 $E(K) \cong E(K)_{\text{tor}} \oplus \mathbb{Z}^r$, 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 $E(K)_{\text{tor}} \cong G$. In this paper we will show that for $d = 2$ and $d = 3$ and for certain groups $G \in \Phi(d)$, if $E(K)_{\text{tor}} \cong G$, 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 $\text{Gal}(L/\mathbb{Q})$ is isomorphic to $D_4$ or $S_4$.

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.
modular curve, let \( g(X_\Gamma) \) denote its genus, and let \( Y_\Gamma \) be the complement of the cusps in \( X_\Gamma \). Let \( \Gamma \supseteq \Gamma' \) be two congruence subgroups of \( \text{SL}_2(\mathbb{Z}) \) not containing the matrix \( \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \). For the pairs \( \Gamma \supseteq \Gamma' \) 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 \( Y_{\Gamma'} \) under the natural morphism \( X_\Gamma \to X_{\Gamma'} \). The modular descriptions of \( X_\Gamma \) and \( X_{\Gamma'} \) 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

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

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

\[ \pi : X_1(16) \to X_{\Gamma'} \]

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 \( \pi \) of \( \mathbb{Q} \)-rational points of \( Y_{\Gamma'} \).

Now consider a point on \( Y_1(16)(K) \) 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 \( \text{Gal}(K/\mathbb{Q}) \).

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 \( \mu : E^\sigma \to E \) satisfying \( \mu \circ \mu^\sigma = \text{id} \). Replacing \( \mu \) by \( -\mu \) if necessary, we may assume in addition

\[ \mu(P^\sigma) = 9P. \]

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

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

\[ X_1(16) : v^2 - (u^3 + u^2 - u + 1)v + u^2 = 0. \]

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 \( E \), and 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

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

where \( a \) and \( b \) are given by

\[
a = 1 - \frac{u^2(u-1)(u+1)}{u^2 + 1},
\]

\[
b = \frac{-u^2(u-1)(u+1)}{(u^2 + 1)^2}.
\]

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 \(\Gamma\) and the corresponding modular curve \(X_\Gamma\) using several auxiliary congruence subgroups. Let \(\Gamma_*(2)\) be the unique subgroup of \(\text{SL}_2(\mathbb{Z})\) that contains \(\Gamma(2)\) and such that \((\Gamma_*(2) : \Gamma(2)) = 3\); more precisely,

\[
\Gamma_*(2) = \left\{ \Gamma \in \text{SL}_2(\mathbb{Z}) \mid \gamma \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \\ \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \\ \end{pmatrix} \pmod{2} \right\}.
\]

We also define \(\Gamma_*(7) = \left\{ \begin{pmatrix} a & b \\ c & b \end{pmatrix} \in \text{SL}_2(\mathbb{Z}) \mid a, d \equiv 1, 2, 4 \pmod{7}, c \equiv 0 \pmod{7} \right\}\).

This will play the role of the group denoted by \(\Gamma'\) in the introduction. We note that \(\Gamma_*(7)\) does not contain the matrix \(\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\). 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

\[
A_3 = (\Gamma_*(2) \cap \Gamma_1(7))/\Gamma, \\
C_3 = (\Gamma(2) \cap \Gamma_*(7))/\Gamma, \\
A_3 \times C_3 = (\Gamma_*(2) \cap \Gamma_*(7))/\Gamma.
\]

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 \(X_\Gamma\) 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 \textit{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.

\textbf{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 $X_\Gamma \to X_1(14)$ 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. \hfill \Box

**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 $\{ (1), (9), (11) \}$. Under any identification of $X_1(14)$ with an elliptic curve, the automorphisms $(9)$ and $(11)$ 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 $A_3$. \hfill \Box

**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 $X_\Gamma / A_3$ 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. \hfill \Box

**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 $X_\Gamma$ (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 $Y_1(7)$, since $Y_1(7)$ is a fine moduli space. This implies that the map $X_\Gamma / (A_3 \times C_3) \to X_4(7)$ is unramified outside the cusps. Since $X_4(7)$ has genus 0, the Hurwitz formula implies that this last map is ramified above the two cusps of $X_4(7)$ and that $X_\Gamma / (A_3 \times C_3)$ has genus 0. This proves (1).

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

**Lemma 3.5.** The curves $X_\Gamma / H$ and $X_\Gamma / H'$ 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 (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 $H'$. 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 \( g(X_{1}) = 4 \) and \( n_{H} + n_{H'} = 12 \), we get \( g(X_{1}/H) + g(X_{1}/H') = 0 \), which implies the claim. \( \square \)

We conclude that the curve \( X_{1} \) admits two maps of degree 3 to a curve of genus 0, namely the quotient maps

\[
q_{H} : X_{1} \to X_{1}/H, \quad q_{H'} : X_{1} \to X_{1}/H'.
\]

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 \( \text{Sym}^{3} X_{1} \). 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 \( X_{1} \) embeds as a smooth curve of bidegree \( (3,3) \) in \( X_{1}/H \times X_{1}/H' \simeq \mathbb{P}^{1}_{\mathbb{Q}} \times \mathbb{P}^{1}_{\mathbb{Q}} \), 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 [4, IV, Example 5.2.2]), every non-constant map \( X_{1} \to \mathbb{P}^{1}_{\mathbb{Q}} \) of degree 3 can be identified with either \( q_{H} \) or \( q_{H'} \) via an isomorphism of \( \mathbb{P}^{1}_{\mathbb{Q}} \) with \( X_{1}/H \) or \( X_{1}/H' \), respectively.

We fix one rational cusp, say \( O = (0,0) \), and we consider the Jacobian \( J_{1} \) of \( X_{1} \) and the (non-dominant) rational map

\[
\phi : \text{Sym}^{3} X_{1} \to J_{1}
\]

\[
D \mapsto [D - 3O]
\]

**Lemma 3.6.** The map \( \phi \) contracts the lines \( L \) and \( L' \) and is injective outside \( L \cup L' \).

**Proof.** Consider two distinct points of \( \text{Sym}^{3} X_{1} \) corresponding to effective divisors \( D, D' \) of degree 3 on \( X_{1} \). 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 \( X_{1} \) such that \( \text{div}(f) = D - D' \). 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 \( X_{1} \) is not hyperelliptic. This implies that \( \phi(D) = \phi(D') \) if and only if both \( D \) and \( D' \) are pull-backs of points under \( q_{H} : X_{1} \to X_{1}/H \), or both are pull-backs of points under \( q_{H'} : X_{1} \to X_{1}/H' \). \( \square \)

### 3.2. Modular description of \( X_{1}(7) \) and \( X_{s}(7) \).

The curve \( X_{1}(7) \) is isomorphic to \( \mathbb{P}^{1}_{\mathbb{Q}} \). In terms of a suitable coordinate \( d \) on \( X_{1}(7) \), the universal elliptic curve over \( Y_{1}(7) \) is given by

\[
E_{1}(7) : y^{2} + (1 + d - d^{2})xy + (d^{2} - d^{3})y = x^{3} + (d^{2} - d^{3})x^{2},
\]

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

\[
(\pm 1)d = d, \\
(\pm 2)d = (d - 1)/d, \\
(\pm 3)d = -1/(d - 1).
\]

The locus of common fixed points of these automorphisms is given by \(d^2 - d + 1 = 0\).

The curve \( X_{s}(7) \) is the quotient of \( X_{1}(7) \) by the group of diamond automorphisms \( \{ (1), (2), (4) \} \). The fixed points of these automorphisms on \( X_{1}(7) \) map to two elliptic points on \( X_{s}(7) \). Let \( U_{s}(7) \) be the complement of the cusps and the elliptic points on \( X_{s}(7) \). Then \( U \) is the fine part of the modular curve classifying elliptic curves equipped with a subscheme that is étale locally of the form \( P + 2P + 4P \) with \( P \) a point of order 7, and the universal elliptic curve over \( X_{1}(7) \) descends to \( U \).
In terms of the coordinate
\[ s = d + \frac{d - 1}{d} - \frac{1}{d - 1} = \frac{d^3 - 3d + 1}{d(d - 1)} \]
on \( X_*(7) \), the cusps are \( s = 8 \) and \( s = \infty \), and the elliptic points are given by \( s^2 - 3s + 9 = 0 \).
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
\[ y^2 + xy = x^3 + a_2x^2 + a_4x + a_6 \]
with the points \( P, 2P \) and \( 4P \) lying on the line \( y = 0 \) and the points \( 3P, 5P \) and \( 6P \) lying on the line \( y = -x \). We obtain
\[
\begin{align*}
a_2 &= -\frac{d(d - 1)(d^3 - 3d + 1)}{(d^2 - d + 1)^3} = -\frac{s}{s^2 - 3s + 9}, \\
a_4 &= \frac{d^6(d - 1)^3(d^3 - 3d^2 + 1)}{(d^2 - d + 1)^6} = \frac{s - 3}{(s^2 - 3s + 9)^2}, \\
a_6 &= \frac{d^8(d - 1)^6}{(d^2 - d + 1)^9} = \frac{1}{(s^2 - 3s + 9)^3}.
\end{align*}
\]
and hence \( E_*(7) \) is given by
\[ E_*(7): y^2 + xy = x^3 - \frac{s}{s^2 - 3s + 9}x^2 + \frac{s - 3}{(s^2 - 3s + 9)^2}x + \frac{1}{(s^2 - 3s + 9)^3}. \]

### 3.3. Modular description of \( X_1(7) \)

We view \( X_1(7) \) 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.
\[
4(x - \xi_0)(x - \xi_1)(x - \xi_2) = 4x^3 + (d^4 - 6d^3 + 3d^2 + 2d + 1)x^2 + 2d^2(d - 1)(d^2 - d - 1)x + d^4(d - 1)^2.
\]

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
\[
t = \frac{4}{d^4(d - 1)^4}(\xi_1 - \xi_0)(\xi_0 - \xi_2)(\xi_2 - \xi_1)
\]
\[
= 4\frac{d^2(d - 1)^2}{(d^2 - d + 1)^3}(\zeta_1 - \zeta_0)(\zeta_0 - \zeta_2)(\zeta_2 - \zeta_1).
\]

Then we have the identities
\[ t^2 = \frac{d^3 - 8d^2 + 5d + 1}{d(d - 1)} \]
and
\[ 4(\zeta_0 - \zeta_1)(\zeta_0 - \zeta_2)(\zeta_1 - \zeta_2) = t(t^2 - t + 7)(t^2 + t + 7), \]
and \( \zeta_0, \zeta_1, \zeta_2 \) are the three zeroes of the polynomial
\[ 4(x - \zeta_0)(x - \zeta_1)(x - \zeta_2) = 4x^3 + (t^4 + 9t^2 + 17)x^2 + (4t^2 + 20)x + 4. \]

**Lemma 3.7.** Let \( f = x^3 + px^2 + qx + r \) 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
\[ \beta = \frac{-(pq - 9r - \delta)\alpha + (6pr - 2q^2)}{(2p^2 - 6q)\alpha + (pq - 9r + \delta)}, \]
\[ \gamma = \frac{-(pq - 9r + \delta)\alpha + (6pr - 2q^2)}{(2p^2 - 6q)\alpha + (pq - 9r - \delta)}. \]

**Proof.** This is a straightforward verification. \( \square \)

With \((\alpha, \beta, \gamma) = (\zeta_0, \zeta_1, \zeta_2)\), Lemma 3.7 implies the identities
\[ \zeta_1 = -2\frac{(t^2 - t + 1)\zeta_0 + 2}{(t^4 + 5t^2 + 1)\zeta_0 + 2(t^2 + t + 1)}, \]
\[ \zeta_2 = -2\frac{(t^2 + t + 1)\zeta_0 + 2}{(t^4 + 5t^2 + 1)\zeta_0 + 2(t^2 - t + 1)}. \]

Our definitions imply that \( \delta_0, \delta_1, \delta_2 \) are the three solutions of the equation
\[ \delta^3 - (t^2 + 8)\delta^2 + (t^2 + 5)\delta + 1 = 0 \]
and \( \zeta_0, \zeta_1, \zeta_2 \) are the three solutions of the equation
\[ \zeta^3 + \frac{1}{4}(t^4 + 9t^2 + 17)\zeta^2 + (t^2 + 5)\zeta + 1 = 0. \]

To study the quotients \( X_\Gamma/H \) and \( X_\Gamma/H' \), which are isomorphic to \( \mathbb{P}^1_\mathbb{Q} \), we define
\[ \eta_+ = 4(\delta_0\zeta_0 + \delta_1\zeta_1 + \delta_2\zeta_2), \]
\[ \eta_- = 4(\delta_0\zeta_0 + \delta_1\zeta_2 + \delta_2\zeta_1). \]

Then one computes the minimal polynomials of \( \eta_+ \) and \( \eta_- \) over \( \mathbb{Q}(t) \) as
\[ F_+ = x^3 + (t^6 + 17t^4 + 89t^2 + 136)x^2 + (t^{10} + 23t^8 + 221t^6 + 1169t^4 + 3643t^2 + 5365)x \]
\[ - (t^{12} + 19t^{10} + 8t^9 + 78t^8 + 208t^7 - 761t^6 + 2136t^5) \]
\[ - 8866t^4 + 10192t^3 - 33885t^2 + 19208t - 48791) \]
and
\[ F_- = x^3 + (t^6 + 17t^4 + 89t^2 + 136)x^2 + (t^{10} + 23t^8 + 221t^6 + 1169t^4 + 3643t^2 + 5365)x \]
\[ - (t^{12} + 19t^{10} - 8t^9 + 78t^8 - 208t^7 - 761t^6 - 2136t^5) \]
\[ - 8866t^4 - 10192t^3 - 33885t^2 - 19208t - 48791). \]
Each of the polynomials $F_+$ and $F_-$ defines a singular curve that is birational to $\mathbb{P}_Q^1$. More precisely, we consider the functions

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

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

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

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

and

$$\eta_- = \frac{y_{-1}^2 + 2y_-^{11} + 5y_-^{10} + 14y_-^9 + 24y_-^8 + 32y_-^7 + 37y_-^6 + 28y_-^5 + 14y_-^4 + 16y_-^3 + 15y_-^2 + 6y_- + 1}{y_-^4(y_- + 1)^2},$$
$$t = \frac{y_-^3 + y_-^2 - 2y_- - 1}{y_-(y_+ + 1)}.$$

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

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

or equivalently

$$(4) \quad X_\Gamma: (u^3 + u^2 - 2u - 1)v(v + 1) + (v^3 + v^2 - 2v - 1)u(u + 1) = 0.$$

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 $\mathbb{Q}(\zeta_7)$. The $(u, v)$-coordinates of the 9 rational cusps are

$$(0, 0), \quad (0, -1), \quad (0, \infty),$$
$$(1, 0), \quad (-1, 1), \quad (-1, \infty),$$
$$(\infty, 0), \quad (\infty, -1), \quad (\infty, \infty).$$

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

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

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

$$e^2 = d(d - 1)(d^3 - 8d^2 + 5d + 1),$$

where $d$ is a parameter.

The structure of $J_\Gamma$ is then determined by considering the isogenies and the action of the automorphisms of $E$, $E$, and $B$. The details of this proof are beyond the scope of this summary.
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 \( J \) is 0.

Let \( \text{red}_3 \) denote the reduction map \( J(\mathbb{Q}) \to J(\mathbb{F}_3) \). Then \( \text{red}_3 \) is injective. One computes the numerator of the zeta function of \( J \) 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 \( #X(\mathbb{F}_3) = 1 + 5 + 3 = 9 \); substituting \( x = 1 \), we obtain \( #J(\mathbb{F}_3) = 432 = 2^4 \cdot 3^3 \). We deduce that \( #J(\mathbb{Q}) \) divides 432.

Let \( A \) be the subgroup of \( J(\mathbb{Q}) \) 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 \( #J(\mathbb{Q}) \) 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 \( \text{red}_3 \).

To compute in \( J(\mathbb{F}_3) \), 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 \( J(k) \cong \text{Pic}^0 X \) 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 \([D - rO]\) 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 \([8]\). 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 \( \mathcal{O}_{X_1}(2((0, \infty) + (-1, \infty) + (\infty, 0) + (\infty, -1) + (\infty, \infty))) \) 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 \( P \in X_1(\mathbb{F}_3) \), we consider the corresponding point \([P - (0, 0)] \in J(\mathbb{F}_3)\). We define the following elements of \( J(\mathbb{F}_3) \):

\[
x_1 = 9[(0, -1) - (0, 0)], \quad y_1 = 2[(-1, 0) - (0, 0)],
\]
\[
x_2 = 9[(0, \infty) - (0, 0)], \quad y_2 = 2[(-1, -1) - (0, 0)],
\]
\[
x_3 = 9[(-1, 0) - (0, 0)],
\]
\[
x_4 = 9[(-1, -1) - (0, 0)],
\]

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

\[
\lambda_2: (\mathbb{Z}/2\mathbb{Z})^4 \to \text{red}_3(A_2)
\]
\[
(a_1, a_2, a_3, a_4) \mapsto \sum_{i=1}^4 a_i x_i.
\]
and
\[ \lambda_3 : \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \longrightarrow \text{red}_3(A_3) \]
\[ (b_1, b_2) \longmapsto b_1y_1 + b_2y_2. \]
These fit in the following commutative diagrams:
\[
\begin{array}{ccc}
(\mathbb{Z}/2\mathbb{Z})^4 & \xrightarrow{\lambda_2} & A_2 \\
\downarrow \text{red}_3 & & \downarrow \text{red}_3 \\
\text{red}_3(A_2) & \xrightarrow{\lambda_3} & A_3
\end{array}
\]
where the vertical maps \( A_2 \to \text{red}_3(A_2) \) and \( A_3 \to \text{red}_3(A_3) \) 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 \( \text{red}_3(A) \) are isomorphic to \( C_2 \times C_2 \times C_2 \times C_14 \), and in particular have order 342. Finally, we deduce \( J_\Gamma(\mathbb{F}_3) = \text{red}_3(A) \) 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 \((\text{Sym}^3 X_\Gamma)(\mathbb{Q})\) 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 \( \mathbb{Q}(\zeta_3)^+ \), there are \((9 + 3 - 1)/3 + 3 = 168\) 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 \( X_\Gamma/H' \). Furthermore, none of the three Galois orbits of cusps with field of definition \( \mathbb{Q}(\zeta_7)^+ \) lies over a single rational point of \( X_\Gamma/H \) or \( X_\Gamma/H' \). 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 \( X_\Gamma \), which we can view as a \( \mathbb{Q} \)-rational point of \( \text{Sym}^3 X_\Gamma \). Then \( \phi(D) \) is a \( \mathbb{Q} \)-rational point of the subvariety \( \text{im}(\phi) \) 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 \( \mathbb{P}^1_{\mathbb{Q}} \) inside \( \text{Sym}^3 X_\Gamma \) 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 \( X_\Gamma/H' \) under the maps \( q_H \) and \( q_{H'} \), 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 $P$, $2P$ 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

$$y^2 + xy + y = x^3 - x^2 + (-3737\alpha^2 - 8584\alpha + 9067)x + (203770\alpha^2 + 468074\alpha - 494427)$$

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 the fibre of the family $E_s(7)$ 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).
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.
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](http://www.math.harvard.edu/~mazur/papers/For.Momose20.pdf)
4. R. Hartshorne, *Algebraic Geometry*, Springer-Verlag, New York, 1977.
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.
6. K. Khuri-Makdisi, *Linear algebra algorithms for divisors on an algebraic curve*, Math. Comp. 73 (2004), no. 245, 333–357.
7. K. Khuri-Makdisi, *Asymptotically fast group operations on Jacobians of general curves*, Math. Comp. 76 (2007), no. 260, 2213–2239.
8. The PARI Group, *PARI/GP (version 2.7.6)*, Bordeaux, 2016, [http://pari.math.u-bordeaux.fr/](http://pari.math.u-bordeaux.fr/).
9. The Sage Developers, *SageMath, the Sage Mathematics Software System (version 7.2)*, 2016, [http://www.sagemath.org/](http://www.sagemath.org/).