# TORSION SUBGROUPS OF ELLIPTIC CURVES
# OVER QUINTIC AND SEXTIC NUMBER FIELDS

MAARTEN DERICKX AND ANDREW V. SUTHERLAND

(Communicated by Romyar T. Sharifi)

ABSTRACT. Let $\Phi^\infty(d)$ denote the set of finite abelian groups that occur infinitely often as the torsion subgroup of an elliptic curve over a number field of degree $d$. The sets $\Phi^\infty(d)$ are known for $d \le 4$. In this article we determine $\Phi^\infty(5)$ and $\Phi^\infty(6)$.

## 1. INTRODUCTION

Let $E$ be an elliptic curve over a number field $K$. By the Mordell-Weil theorem [29], the set of $K$-rational points on $E$ forms a finitely generated abelian group $E(K)$. In particular, its torsion subgroup $E(K)_{\mathrm{tors}}$ is finite, and it is well known that it can be generated by two elements [27]. There thus exist integers $m, n \ge 1$ such that

$$E(K)_{\mathrm{tors}} \simeq \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/mn\mathbb{Z}.$$

The uniform boundedness conjecture states that for every number field $K$ there exists a bound $B$ such that $\#E(K)_{\mathrm{tors}} \le B$ for every elliptic curve $E$ over $K$. This conjecture is now a theorem due to Merel [25], who actually proved the strong version of this conjecture in which the bound $B$ depends only on the degree $d :=$ $[K : \mathbb{Q}]$. It follows that for every positive integer $d$, there is a finite set $\Phi(d)$ of isomorphism classes of torsion subgroups that arise for elliptic curves over number fields of degree $d$; we may identify elements of $\Phi(d)$ by pairs of positive integers $(m, mn)$.

The set $\Phi(1)$ was famously determined by Mazur [24], who proved that

$$\Phi(1) = \{(1, n) : 1 \le n \le 12, \ n \ne 11\} \ \cup \ \{(2, 2n) : 1 \le n \le 4\}.$$

The set $\Phi(2)$ was determined in a series of papers by Kenku, Momose, and Kamienny, culminating in [17, 19], which yield the result

$$\Phi(2) = \{(1, n) : 1 \le n \le 18, \ n \ne 17\} \cup \{(2, 2n) : 1 \le n \le 6\} \cup \{(3, 3), (3, 6), (4, 4)\}.$$

For $d > 2$ the sets $\Phi(d)$ have yet to be completely determined. However, if we distinguish the subset $\Phi^\infty(d) \subseteq \Phi(d)$ of torsion subgroups that arise for infinitely many $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves defined over number fields of degree $d$, we can say more.

We have $\Phi^\infty(1) = \Phi(1)$ and $\Phi^\infty(2) = \Phi(2)$. In [16] Jeon, Kim, and Schweizer found that

$$\Phi^\infty(3) = \{(1, n) : 1 \le n \le 20, \ n \ne 17, 19\} \ \cup \ \{(2, 2n) : 1 \le n \le 7\},$$

and in [15] Jeon, Kim and Park obtained

$$\Phi^\infty(4) = \{(1, n) : 1 \le n \le 24, \ n \ne 19, 23\} \ \cup \ \{(2, 2n) : 1 \le n \le 9\}$$
$$\cup \ \{(3, 3n) : 1 \le n \le 3\} \ \cup \{(4, 4), (4, 8), (5, 5), (6, 6)\}.$$

In this article we determine the sets $\Phi^\infty(5)$ and $\Phi^\infty(6)$.

**Theorem 1.1.** *Let $\Phi^\infty(d)$ denote the set of pairs $(m, mn)$ for which $E(K)_{\text{tors}} \simeq \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/mn\mathbb{Z}$ for infinitely many non-isomorphic elliptic curves $E$ over number fields $K$ of degree $d$. Then*

$$\Phi^\infty(5) = \{(1, n) : 1 \le n \le 25, \ n \ne 23\} \ \cup \ \{(2, 2n) : 1 \le n \le 8\},$$

*and*

$$\Phi^\infty(6) = \{(1, n) : 1 \le n \le 30, \ n \ne 23, 25, 29\} \ \cup \ \{(2, 2n) : 1 \le n \le 10\}$$
$$\cup \ \{(3, 3n) : 1 \le n \le 4\} \ \cup \{(4, 4), (4, 8), (6, 6)\}.$$

For $d = 5, 6, 7, 8$, the elements $(1, n) \in \Phi^\infty(d)$ were determined in [6] using a strategy that we generalize here. The key steps involve computing (or at least bounding) the gonalities of certain modular curves and determining whether their Jacobians have rank zero or not. To obtain gonality bounds we require explicit models for the modular curves $X_1(m, mn)$ that parametrize triples $(E, P, Q)$, where $E$ is an elliptic curve with independent points $P$ of order $m$ and $Q$ of order $mn$; for our approach to be computationally feasible, it is important that these models have low degree and reasonably small coefficients. Optimized models for $X_1(n) = X(1, n)$ for $n \le 50$ were constructed in [28]. Here we extend the approach of [28] to construct optimized models for $X_1(m, mn)$ for $m^2 n \le 120$, as described in §3; these can be found in [10]. These models are necessarily defined only over the cyclotomic field $\mathbb{Q}(\zeta_m)$. The need to work over $\mathbb{Q}(\zeta_m)$ requires us to develop some new techniques for determining when the Jacobian of $X_1(m, mn)$ has rank zero over $\mathbb{Q}(\zeta_m)$; these are described in §4. The case $X_1(2, 30)$ proved to be computationally challenging, so we used an alternative strategy based on ideas in [8], as explained in §5.

In principle our methods can also determine $\Phi^\infty(7)$; we have computed explicit models for all of the relevant modular curves and proved that their Jacobians have rank zero. We can prove $(2, 2n) \in \Phi^\infty(7)$ for $1 \le n \le 10$ and not for $n > 15$; it remains only to determine for $11 \le n \le 15$ whether the gonality of $X_1(2, 2n)$ is greater than 7 or not (we expect the answer is yes in each case). Similar comments apply to $\Phi^\infty(8)$ but not to $\Phi^\infty(9)$, which requires new techniques, as explained in Remark 5.2.

The source code for computations on which results of this article depend is available in [9].

## 2. BACKGROUND

In this section we briefly recall background material and introduce some notation. Let $K$ be a field and let $X/K$ be a *nice curve*, by which we mean that $X/K$ is of dimension 1, smooth, projective, and geometrically integral. The *gonality* $\gamma(X)$ of $X$ is the minimal degree of a finite $K$-morphism $X \to \mathbb{P}^1_K$. If $L/K$ is a field

extension and $X_L := X \times_K L$ is the base change of $X$ to $L$, we necessarily have $\gamma(X_L) \leq \gamma(X)$, and we call $\gamma(X_L)$ the $L$-*gonality* of $X$. If $K$ is a number field, $\mathfrak{p}$ is a prime of $K$ of good reduction for $X$, and $X_{\mathbb{F}_\mathfrak{p}}$ is the reduction of $X$ to the residue field $\mathbb{F}_\mathfrak{p}$ of $\mathfrak{p}$, then $\gamma(X_{\mathbb{F}_\mathfrak{p}}) \leq \gamma(X)$, and we call $\gamma(X_{\mathbb{F}_\mathfrak{p}})$ the $\mathbb{F}_\mathfrak{p}$-*gonality* of $X$.

**Proposition 2.1** (Abramovich, Kim-Sarnak)**.** *Let* $\Gamma \subseteq \mathrm{PSL}_2(\mathbb{Z})$ *be a congruence subgroup. The* $\mathbb{C}$-*gonality of the modular curve* $X_\Gamma$ *is at least* $(\lambda_1/24)[\mathrm{PSL}_2(\mathbb{Z}) : \Gamma]$, *where* $\lambda_1 \geq 975/4096$.

*Proof.* See [1, Thm. 0.1] for the first statement and [20, p. 176] for the lower bound on $\lambda_1$. $\qquad\square$

Let $d(X)$ denote the least integer for which the set $\{a \in X(\overline{K}) : [K(a) : K] = d\}$ of *points of degree $d$* on $X$ is infinite. We have the following result of Frey [11], which can be viewed as a corollary of Faltings' proof of Lang's conjecture [12].

**Proposition 2.2** (Frey)**.** *Let $X$ be a nice curve over a number field. Then* $d(X) \leq \gamma(X) \leq 2d(X)$.

*Proof.* If $f \in K(X)$ is a function of degree $d$, then by Hilbert irreducibility there are infinitely many points of degree $d$ over $K$ among the roots of $f - c$ as $c$ varies over $K$. This proves the first inequality, and the second is [11, Prop. 1]. $\qquad\square$

There is one situation in which the lower bound of Proposition 2.2 is known to be tight.

**Proposition 2.3.** *Let $X/K$ be a nice curve whose Jacobian has rank zero. Then* $d(X) = \gamma(X)$.

*Proof.* Let $d < \gamma(X)$ be a positive integer. The map $\pi\colon X^{(d)} \to \mathrm{Jac}(X)$ from the $d$th symmetric power of $X$ to its Jacobian is injective, since otherwise we could construct a function $f \in K(X)$ of degree $d < \gamma(X)$ from the difference of two linearly equivalent divisors of degree $d$ and view $f$ as a map $X \to \mathbb{P}^1_K$. If $\mathrm{rk}(\mathrm{Jac}(X)(K)) = 0$, then $\pi(X^{(d)}(K))$ is finite, and so is $X^{(d)}(K)$. It follows that $X$ has only finitely many points of degree $d$. $\qquad\square$

The proofs of Propositions 2.2 and 2.3 together imply the following corollary.

**Corollary 2.4.** *Let $X/K$ be a nice curve over a number field. If $K(X)$ contains a function of degree $d$, then $X$ has infinitely many points of degree $d$. When* $\mathrm{rk}(\mathrm{Jac}(X)(K)) = 0$ *the converse also holds.*

For positive integers $m$ and $n$ we use $Y_1(m, mn)$ to denote the modular curve that parameterizes triples $(E, P, Q)$, where $E$ is an elliptic curve with independent points $P$ of order $m$ and $Q$ of order $mn$, and $X_1(m, mn)$ is its projectivization obtained by adding cusps. We view $X_1(m, mn)$ as a $\mathbb{Z}[\frac{1}{mn}]$-scheme that is isomorphic to the coarse moduli space for the corresponding algebraic stack $\mathcal{X}_1(m, mn)$ in the sense of [5]; all the cases of interest to us have $mn \geq 5$ and are also fine moduli spaces. By fixing a primitive $m$th root of unity $\zeta_m$ in the function field of $X_1(m, mn)$, we may also view $X_1(m, mn)$ as a nice curve over $\mathbb{Q}(\zeta_m)$ that has good reduction at all primes not dividing $mn$, and we write $J_1(m, mn)$ for the Jacobian of $X_1(m, mn)$ as a curve over $\mathbb{Q}(\zeta_m)$. There is an associated congruence subgroup

$\Gamma_1(m, mn)$

$$:= \left\{ \left( \begin{smallmatrix} a & b \\ c & d \end{smallmatrix} \right) \in \mathrm{SL}_2(\mathbb{Z}) : a \equiv d \equiv 1 \bmod mn, \ c \equiv 0 \bmod mn, \ b \equiv 0 \bmod m \right\},$$

and after fixing an embedding $\mathbb{Q}(\zeta_m) \hookrightarrow \mathbb{C}$, the quotient $\mathbb{H}^*/\Gamma_1(m, mn)$ of the extended upper half-plane by the action of $\Gamma_1(m, mn)$ is a compact Riemann surface isomorphic to $X_1(m, mn)(\mathbb{C})$. The image of $\Gamma_1(m, mn)$ in $\mathrm{PSL}_2(\mathbb{Z})$ has index $\frac{m^3 n^2}{2} \prod_{p|mn}(1 - \frac{1}{p^2}) \geq m^2 n - 1$.

Let $X_{0,1}(m, mn)$ be the projectivization of the modular curve that parametrizes triples $(E, G, Q)$, where $E$ is an elliptic curve, $G$ is a cyclic subgroup of order $m$ (or equivalently, a cyclic isogeny of degree $m$) and $Q$ is an independent point of order $mn$ (so $G \cap \langle Q \rangle = \{0\}$). The curve $X_{0,1}(m, mn)_{\mathbb{Q}(\zeta_m)}$ is isomorphic to $X_1(m, mn)$ (as can be seen by considering the corresponding congruence subgroups or by writing a natural transformation between the two functors on schemes over $\mathbb{Z}/nm\mathbb{Z}$, where we view $X_{0,1}(m, mn)_{\mathbb{Q}(\zeta_m)}$ as parametrizing quadruples $(E, G, Q, \zeta_m)$ with $E, G, Q$ as above and $\zeta_m$ a chosen primitive $m$th root of unity). Unlike $X_1(m, mn)$, the curve $X_{0,1}(m, mn)$ has the advantage of always being defined over $\mathbb{Q}$. Now let $X_1(m^2 n) := X_1(1, m^2 n)$ parameterize pairs $(E, Q)$ in which $E$ is an elliptic curve with a point $Q$ of order $m^2 n$, and consider the map

$$\varphi \colon X_1(m^2 n) \to X_{0,1}(m, mn)$$

that sends the pair $(E, Q)$ to the triple $(E/\langle mnQ \rangle, E[m]/\langle mnQ \rangle, Q \bmod \langle mnQ \rangle)$. The group $E[m]/\langle mnQ \rangle$ and the point $Q \bmod \langle mnQ \rangle$ are independent because $Q \bmod \langle mnQ \rangle$ has the same order $mn$ as $Q \bmod E[m]$. The map $\varphi$ is defined over $\mathbb{Q}$ and has degree $m$. The group $(\mathbb{Z}/m^2 n\mathbb{Z})^\times$ acts on $X_1(m^2 n)$ via the diamond operators $\langle a \rangle \colon (E, P) \mapsto (E, aP)$. We have $a \equiv 1 \bmod mn$ precisely when $\langle a \rangle$ stabilizes $\varphi$, meaning $\varphi = \varphi \circ \langle a \rangle$, and the quotient of $X_1(m^2 n)$ by this automorphism subgroup is isomorphic to $X_{0,1}(m, mn)$.

Throughout this article $\overline{\mathbb{Q}}$ denotes a fixed algebraic closure of $\mathbb{Q}$ that contains all number fields $K$ under consideration, and we identify $\overline{K} = \overline{\mathbb{Q}}$. For a modular curve $X$ defined over a number field $K$, we define the *degree over* $\mathbb{Q}$ of a point $a \in X(\overline{\mathbb{Q}})$ to be the absolute degree $[L : \mathbb{Q}]$ of the minimal extension $L/K$ for which $a \in X(L)$ and let $\mathbb{Q}(a)$ denote the field $L$ (which contains $K$). For the sake of clarity we may refer to $[L : K]$ as the *degree of a over* $K$.

Finally, we use $\phi(m) := [\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \#(\mathbb{Z}/m\mathbb{Z})^\times$ throughout to denote the Euler function.

## 3. Constructing models of $X_1(m, mn)$

Our method for constructing explicit methods of $X_1(m, mn)$ is a generalization of the technique used in [28] to construct models for $X_1(n) := X_1(1, n)$, which we now briefly recall. Given $n > 3$ one begins as in [26] with the universal family of elliptic curves

$$E(b, c) := y^2 + (1 - c)y - by = x^3 - bx^2$$

in Tate normal form with rational point $P = (0, 0)$ and imposes the constraint

$$\left\lceil \frac{n+1}{2} \right\rceil P + \left\lfloor \frac{n-1}{2} \right\rfloor P = 0$$

by requiring the $x$-coordinates of the two summands to coincide (the $y$-coordinates of the summands cannot coincide because $\lceil (n+1)/2 \rceil \neq \lfloor (n-1)/2 \rfloor$, so the points must sum to zero). After clearing denominators and removing spurious factors corresponding to torsion points whose order properly divides $n$, one obtains a (singular) affine plane curve $C/\mathbb{Q}$ with the same function field as $X_1(n)$. Each non-singular

point $(b_0, c_0)$ on this curve determines an elliptic curve $E(b_0, c_0)$ on which $P = (0,0)$ is a point of order $n$. The equations obtained by this method are typically much larger than necessary, but the algorithm in [28] can be used to obtain models with lower degrees, fewer terms, and smaller coefficients.

3.1. **Constructing models using elliptic surfaces.** We use a similar approach to construct equations for $X_1(m, mn)$. For $m = 2$ we use the parameterized family of elliptic curves constructed by Jain in [13], in which the elliptic curve

$$E_2(q, t): \quad y^2 = x^3 + (t^2 - qt - 2)x^2 - (t^2 - 1)(qt + 1)^2 x$$

has the rational point $P_2 := (0, 0)$ of order 2 and the rational point

$$Q_2(q, t) := \big((t + 1)(qt + 1),\, t(qt + 1)(t + 1)\big)$$

of infinite order; see [13, Thm. 1.ii]. As suggested to us by Noam Elkies, for any $n > 1$, setting

$$\left\lceil \frac{2n + 1}{2} \right\rceil Q_2(q, t) + \left\lfloor \frac{2n - 1}{2} \right\rfloor Q_2(q, t) = 0$$

allows us to construct a model for $X_1(2, 2n)$. As above, it is enough to equate the $x$-coordinates of the two summands, and this yields a polynomial equation in $q$ and $t$. With $n = 7$, for example, after clearing denominators and removing spurious factors we obtain the equation

$$7q^{12}t^4 + 56q^{11}t^3 + 70q^{10}t^4 + 112q^{10}t^2 + 208q^9t^3 + 64q^9t - 111q^8t^4 + 144q^8t^2$$
$$- 624q^7t^3 - 156q^6t^4 - 1104q^6t^2 - 512q^5t^3 - 832q^5t - 55q^4t^4 - 592q^4t^2$$
$$- 256q^4 - 136q^3t^3 - 256q^3t - 10q^2t^4 - 96q^2t^2 - 16qt^3 - t^4 = 0.$$

This equation is not as compact as we might wish, and its degree in both $q$ and $t$ is greater than the gonality of $X_1(2, 14)$, which is 3. However, after applying the optimizations described in [28] we obtain the equation

$$(u^2 + u)v^3 + (u^3 + 2u^2 - u - 1)v^2 + (u^3 - u^2 - 4u - 1)v - u^2 - u = 0,$$

whose degree in $u$ and $v$ matches the gonality of $X_1(2, 14)$. The relation between the $(u, v)$ coordinates and the $(q, t)$ coordinates is given by

$$q = \frac{u + v}{v - u}, \qquad t = \frac{(u - v)(u + v)(u + v + 2)}{u^3 + u^2v + 2u^2 + uv^2 + 2uv + v^3 + 2v^2}.$$

The reader may wish to compare this model for $X_1(2, 14)$ with the one given in [14, p. 589].

A similar approach can be used to obtain equations for $X_1(3, 3n)$. From [13, Thm. 4.ii] we have the parameterized family of elliptic curves

$$E_3(q, t): \quad y^2 + (qt - q + t + 2)xy + (qt^2 - qt + t)y = x^3,$$

with the rational point $P_3 := (0, 0)$ of order 3 and the rational point

$$Q_3(q, t) := (-t, t^2)$$

of infinite order. For $n \geq 1$, equating the $x$-coordinates of $\left\lceil \frac{3n+1}{2} \right\rceil Q_3(q, t)$ and $\left\lfloor \frac{3n-1}{2} \right\rfloor Q_3(q, t)$ yields an equation $F(q, t) = 0$ that we may use to construct a model for $X_1(3, 3n)$. In order to obtain a geometrically integral curve we must factor $F$ over $\mathbb{Q}(\zeta_3)$ rather than $\mathbb{Q}$ (if we only factor over $\mathbb{Q}$, over $\mathbb{Q}(\zeta_3)$ we will have the union of two curves that are both birationally equivalent to $X_1(3, 3n)$).

To obtain equations for $X_1(4, 4n)$ we use a parameterization due to Kumar and Shioda; see the example following [23, Rem. 10]. We have the family

$$E_4(q, t): \quad y^2 + xy + (1/16)(q^2 - 1)(t^2 - 1)y = x^3 + (1/16)(q^2 - 1)(t^2 - 1)x^2,$$

with the rational point $P_4 := (0, 0)$ of order 4 and the rational point

$$Q_4(q, t) := \big((q + 1)(t^2 - 1)/8, \, (q + 1)^2(t - 1)^2(t + 1)/32\big)$$

of infinite order. For any $n \geq 1$, equating the $x$-coordinates of $\lceil \frac{4n+1}{2} \rceil Q_4(q, t)$ and $\lfloor \frac{4n-1}{2} \rfloor Q_4(q, t)$ yields an equation $F(q, t) = 0$ that we may use to construct a model for $X_1(4, 4n)$ after factoring $F(q, t)$ over $\mathbb{Q}(\zeta_4) = \mathbb{Q}(i)$.

*Remark* 3.1. It is usually obvious which factor of $F(q, t)$ is the correct choice (the biggest one), but one can verify the correct choice by checking that it yields a curve of the same genus as $X_1(m, mn)$. The other non-conjugate factors of $F(q, t)$ correspond to modular curves $X$ that admit a non-constant map from $X_1(m, mn)$ of degree greater than 1. Provided $X_1(m, mn)$ has genus $g > 1$, the Riemann-Hurwitz formula implies that $g > g(X)$. For $g \leq 1$ one can instead prove that none of the non-conjugate factors yield a model for $X_1(m, mn)$ by finding a non-singular point that does not yield a triple $E(E, P, Q)$ with $P$ and $Q$ of the correct order (always possible).

3.2. **A general method.** The methods in the previous section for $m = 2, 3, 4$ rely on parameterizations obtained from elliptic surfaces that do not exist in general. We now sketch a general method that works for any $m > 3$. Rather than constructing a model for the curve $X_1(m, n)$, we will construct a model for its quotient by the involution $(E, P, Q) \to (E, -P, Q)$, which we denote $X_1(m, n)^+$. The curve $X_1(m, n)^+$ is defined over $\mathbb{Q}(\zeta_m)^+$, the maximal real subfield of $\mathbb{Q}(\zeta_m)$, and its base change from $\mathbb{Q}(\zeta_m)^+$ to $\mathbb{Q}(\zeta_m)$ is isomorphic to $X_1(m, n)$; for $m = 1, 2, 3, 4, 6$ we have $\mathbb{Q}(\zeta_m)^+ = \mathbb{Q}$ and $X_1(m, n)^+ \simeq X_{0,1}(m, n)$. For the sake of brevity we give details only for the cases in which $X_1(m)$ has genus 0, which suffices for our purposes.

Let us fix $m > 3$ and $n \geq 1$. We may view $E(b, c)$ as the universal elliptic curve with rational points $P = (0, 0)$ and $Q = (x, y)$; let $e(b, c, x, y) = 0$ be the equation defining $E(b, c)$. Let $f(b, c) = 0$ be an equation for $X_1(m)$ constructed as in [28], and let $h(b, c, x)$ denote the irreducible polynomial obtained by equating the $x$-coordinates of $\lceil (mn + 1)/2 \rceil Q$ and $\lfloor (mn - 1)/2 \rfloor Q$ and removing spurious factors as above. The equations $e(b, c, x, y) = f(b, c) = h(b, c, x) = 0$ define a curve in $\mathbb{A}^4[b, c, x, y]$; this curve is not reduced (because there are two choices for the unconstrained $y$-coordinate), but it contains the curve we seek.

Let us now assume that $m \in \{4, 5, 6, 7, 8, 9, 10, 12\}$ so that $g(X_1(m)) = 0$, in which case we may write $b = b(t)$ and $c = c(t)$ as functions of a single rational parameter $t$, as in [22, Table 3]. In this case there is no $f(b, c)$ to compute, our curve equation becomes $e(t, x, y) = 0$, and we compute $h(t, x)$ by equating the $x$-coordinates of $\lceil (mn + 1)/2 \rceil Q$ and $\lfloor (mn - 1)/2 \rfloor Q$ and removing spurious factors as above. Let $H$ be the resultant of $e$ and $h$ with respect to the variable $y$; the polynomial $H(t, x)$ is the square of a polynomial $F \in \mathbb{Z}[t, x]$ that is irreducible over $\mathbb{Q}$ but splits into $\phi(m)/2$ geometrically irreducible factors over $\mathbb{Q}(\zeta_m)^+$ that are $\text{Gal}(\mathbb{Q}(\zeta_m)^+/\mathbb{Q})$-conjugates. We may take any of these factors as our model for $X_1(m, n)^+$. The base change of this model from $\mathbb{Q}(\zeta_m)^+$ to $\mathbb{Q}(\zeta_m)$ is then a model for $X_1(m, mn)$.

By combining this method with §3.1 and applying the algorithm in [28], we have constructed optimized models for $X_1(m, mn)$ for $m^2n \le 120$ and verified them as explained in Remark 3.1. These models are available in electronic form at [10].

## 4. Modular Jacobians of rank zero over cyclotomic fields

In [4], Conrad, Edixhoven, and Stein give an explicit method for computing $L$-ratios for modular forms on $X_1(n)$. By applying the proven parts of the Birch and Swinnerton-Dyer conjecture (see [18, Cor. 14.3] or [21]) they are then able to prove that the rank of $J_1(p) := \mathrm{Jac}(X_1(p))$ is zero over $\mathbb{Q}$ for all primes $p < 73$ except for $p = 37, 43, 53, 61, 67$; see [4, §6.1.3, §6.2.2]. The software developed by Stein for performing these computations is available in the computer algebra system Magma [3], which can compute provably correct bounds on $L$-ratios as exact rational numbers; in particular, one can unconditionally determine when the $L$-ratio is non-zero, in which case the rank is provably zero.

Here we adapt this method to prove that $J_1(m, mn)$ has rank zero over $\mathbb{Q}(\zeta_m)$ for suitable values of $m$ and $n$. For the sake of brevity we focus on the cases $m = 2, 3, 4, 6$ in which $\mathbb{Q}(\zeta_m)$ has degree at most 2, which suffices for our application; the method generalizes to arbitrary $m$ and abelian extensions $K/\mathbb{Q}$ that contain an $m$th root of unity. This includes $m = 5$, which we list below for reference but do not need to prove our main result.

**Theorem 4.1.** *The rank of $J_1(m, mn)$ is zero over $\mathbb{Q}(\zeta_m)$ if any of the following hold:*

- *$m = 1$ and $n \le 36$;*
- *$m = 2$ and $n \le 21$;*
- *$m = 3$ and $n \le 10$;*
- *$m = 4$ and $n \le 6$;*
- *$m = 5$ and $n \le 4$;*
- *$m = 6$ and $n \le 5$.*

All computations referred to in the proof below were performed using the `IsX1mnRankZero` function implemented in [9], which uses the `LRatio` function in Magma [3] to determine when the $L$-ratio is non-zero.

*Proof.* Let $J$ be the Jacobian of the quotient of the curve $X_1(m^2n)$ by the subgroup of diamond operators that stabilize the map $\varphi \colon X_1(m^2n) \to X_{0,1}(m, mn)$, as described in §2. We then have $J_1(m, mn) \simeq J_{\mathbb{Q}(\zeta_m)}$, and it suffices to prove that the rank of $J_{\mathbb{Q}(\zeta_m)}(\mathbb{Q}(\zeta_m)) = J(\mathbb{Q}(\zeta_m))$ is zero.

For $m \le 2$ we have $\mathbb{Q}(\zeta_m) = \mathbb{Q}$ and the strategy of [4] can be applied directly; the desired result follows from a computation that finds the $L$-ratios to be non-zero for all modular forms $f$ corresponding to simple isogeny factors of $J$, for $m \le 2$ and $n$ as in the theorem.

We now assume $m \in \{3, 4, 6\}$ so that $\mathbb{Q}(\zeta_m)$ is a quadratic extension of $\mathbb{Q}$. Let $f$ be a newform of level dividing $m^2n$ such that the abelian variety $A_f$ associated to $f$ is an isogeny factor of $J$. Proving that $\mathrm{rk}(J(\mathbb{Q}(\zeta_m))) = 0$ is equivalent to proving that $\mathrm{rk}(A_f(\mathbb{Q}(\zeta_m))) = 0$ for all such $f$.

Let $A$ be the Weil descent of $A_{f, \mathbb{Q}(\zeta_m)}$ down to $\mathbb{Q}$. From the definition of the Weil descent we have $A(\mathbb{Q}) = A_f(\mathbb{Q}(\zeta_m))$, and the identity map $A_{f, \mathbb{Q}(\zeta_m)} \to A_{f, \mathbb{Q}(\zeta_m)}$ over $\mathbb{Q}(\zeta_m)$ induces a morphism $A_f \to A$ over $\mathbb{Q}$; it follows that $A$ is isogenous to $A_f \oplus A/A_f$. Let $\chi_m \colon (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{Q}^\times$ denote the quadratic character of $\mathbb{Q}(\zeta_m)$. One sees that $A/A_f$ is isogenous to $A_{f_{\chi_m}}$ by comparing traces of Frobenius on their

Tate modules. In particular, $\mathrm{rk}(A_f(\mathbb{Q}(\zeta_m))) = 0$ if and only if both $\mathrm{rk}(A_f(\mathbb{Q})) = 0$ and $\mathrm{rk}(A_{f_{\chi_m}}(\mathbb{Q})) = 0$ hold.

The theorem now follows from a computation: we find that the $L$-ratios of $f$ and $f_{\chi_m}$ are non-zero for $m = 3, 4, 6$ and $n$ as in the theorem and all newforms $f$ of level dividing $m^2 n$ such that the abelian variety $A_f$ associated to $f$ is an isogeny factor of $J$.

In fact (as kindly pointed out to us by the referee), it suffices to compute the $L$-ratios of the forms $f$; the twists $f_{\chi_m}$ already arise among the untwisted $f$ under consideration. Indeed, it follows from [2, Prop. 3.1] that for any Dirichlet character $\varepsilon$ of conductor dividing $mn$, if $f$ is a modular form in $S_2(\Gamma_0(m^2 n), \varepsilon)$, then so is $f_{\chi_m}$, since $\chi_m^2 = 1$.                                                                  □

*Remark* 4.2. We also computed the relevant $L$-ratios for $m \leq 6$ and $n$ just past the range listed in Theorem 4.1. For each of these $(m, n)$ we found that at least one relevant $L$-ratio was zero.

## 5. PROOF OF THE MAIN THEOREM

The first step in our proof of Theorem 1.1 is to show for $d = 5, 6$ that $\mathbb{Q}(\zeta_m)(X_1(m, mn))$ contains a function of degree $d/\phi(m)$ if and only if $(m, mn)$ is one of the pairs for $\Phi^\infty(d)$ appearing in the theorem. The following lemma illustrates why the forward implication is useful.

**Lemma 5.1.** *If* $\mathbb{Q}(\zeta_m)(X_1(m, mn))$ *contains a function of degree* $\frac{d}{\phi(m)}$, *then* $(m, mn) \in \Phi^\infty(d)$.

*Proof.* We first note that for $mn \leq 4$, either $\phi(m) = 1$ and $(m, mn) \in \Phi(1) = \Phi^\infty(1) \subseteq \Phi^\infty(d)$ or $\phi(m) = 2$ divides $d$ and $(m, mn) \in \Phi(2) = \Phi^\infty(2) \subseteq \Phi^\infty(d)$. In both cases the lemma holds.

We now assume $mn \geq 5$, in which case $X_1(m, mn)$ is a fine moduli space. By Merel's proof of the uniform boundedness conjecture [25] there is a positive integer $B$ such that for all number fields $K$ of degree $d$ and elliptic curves $E/K$ we have $E(K)_{\mathrm{tors}} \subseteq E[B]$. The integer $B$ is necessarily divisible by $mn$, since $X_1(m, mn)$ has points of degree $d$ over $\mathbb{Q}$.

Now let $f \in \mathbb{Q}(\zeta_m)(X_1(m, mn))$ be a function of degree $d/\phi(m)$. For each $a \in \mathbb{Q}(\zeta_m)$ the points in $f^{-1}(a)$ have degree at most $d/\phi(m)$ over $\mathbb{Q}(\zeta_m)$, hence degree at most $d$ over $\mathbb{Q}$. By Hilbert irreducibility, there are infinitely many $a$ for which the points in $f^{-1}(a)$ have degree exactly $d$, but we also need to show that there are infinitely many $a$ for which the torsion subgroups of the elliptic curves corresponding to the points in $f^{-1}(a)$ are actually isomorphic to $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/mn\mathbb{Z}$ and not any larger. In order to show this we consider the maps

$$X_1(B, B) \xrightarrow{\pi} X_1(m, mn) \xrightarrow{f} \mathbb{P}^1,$$

where $\pi$ sends $(E, P, Q)$ to $(E, (B/m)P, B/(mn)Q)$, and let $\varphi := f \circ \pi$. Let $A \subseteq \mathbb{P}^1(\mathbb{Q}(\zeta_m))$ be the set of $a$ for which every $b \in \varphi^{-1}(a)$ has degree $d \deg \pi$ over $\mathbb{Q}$. The set $A$ is infinite, by Hilbert irreducibility, and for $a \in A$ every $c \in f^{-1}(a)$ has degree $d$ over $\mathbb{Q}$. We claim that for all such $c = (E, P, Q)$ we have $E(\mathbb{Q}(c))_{\mathrm{tors}} = \langle P, Q \rangle$, which implies $(m, mn) \in \Phi^\infty(d)$ as desired.

Suppose not. Then we can construct a point $c' = (E, P', Q')$ on $X_1(m', m'n')$ of degree $d$ over $\mathbb{Q}$ with $P \in \langle P' \rangle$, $Q \in \langle Q' \rangle$, and $\langle P, Q \rangle \subsetneq \langle P', Q' \rangle$, and we have maps

$$X_1(B, B) \xrightarrow{\pi_1} X_1(m', m'n') \xrightarrow{\pi_2} X_1(m, mn) \xrightarrow{f} \mathbb{P}^1,$$

in which $\pi = \pi_2 \circ \pi_1$, with $\deg \pi_1 < \deg \pi$, and $c = \pi_2(c')$. If we now consider $b \in \pi_1^{-1}(c')$, then $b \in \varphi^{-1}(a)$ has degree $d \deg \pi_1 < d \deg \pi$ over $\mathbb{Q}$, a contradiction. $\quad\square$

We now outline the strategy of the proof. Let $T$ be the set of pairs $(m, mn)$ identifying torsion subgroups that we wish to prove is equal to $\Phi^\infty(d)$. To prove $\Phi^\infty(d) = T$ we proceed as follows.

(1) Prove that $\mathbb{Q}(\zeta_m)(X_1(m, mn))$ contains a function of degree $d/\phi(m)$ for all $(m, mn) \in T$.

(2) Compute the set $T_1 := \{(m, mn) : \phi(m)|d \text{ and } B(m, mn) \leq 2d\}$ where $B(m, mn)$ is the lower bound on $\gamma(X_1(m, mn))$ given by Proposition 2.1 (we have $\Phi^\infty(d) \subseteq T_1$).

(3) Verify that $\mathrm{rk}(J_1(m, mn)(\mathbb{Q}(\zeta_m))) = 0$ for all $(m, mn) \in T_1$ via Theorem 4.1.

(4) Compute the set $T_2 := \{(m, mn) : \phi(m)|d \text{ and } B(m, mn) \leq d\} \subseteq T_1$ (now $\Phi^\infty(d) \subseteq T_2$).

(5) For $(m, mn) \in T_2 - T$ prove that $\mathbb{Q}(\zeta_m)(X_1(m, mn))$ has no functions of degree $d/\phi(m)$.

In step (2) the restriction on $m$ follows from the Weil pairing, and the restriction on $n$ is from Proposition 2.2; the tighter restriction on $n$ in step (4) is Proposition 2.3. If the verification in step (3) succeeds, then Corollary 2.4 and Lemma 5.1 together imply that each pair $(m, mn) \in T_2$ lies in $\Phi^\infty(d)$ if and only if $\mathbb{Q}(\zeta_m)(X_1(m, mn))$ contains a function of degree $d/\phi(m)$.

*Remark* 5.2. We have completed steps (1)-(4) for $d = 5, 6, 7, 8$. This strategy cannot be applied with $d = 9$ because (3) fails; as proved in [6], we have $\gamma(X_1(37)) = 18$ and $\mathrm{rk}(J_1(37)(\mathbb{Q})) \neq 0$.

We now prove Theorem 1.1, beginning with the case $d = 5$, following the strategy above.

**Proposition 5.3.** $\Phi^\infty(5) = \{(1, n) : 1 \leq n \leq 25, n \neq 23\} \cup \{(2, 2n) : 1 \leq n \leq 8\}$.

*Proof.* The existence of the Weil pairing implies that $(m, mn) \in \Phi^\infty(5)$ only if $\phi(m)$ divides 5; we thus have $m \leq 2$. The elements $(1, n) \in \Phi^\infty(5)$ are determined in [6, Thm. 3], so we only need to consider $m = 2$.

For $1 \leq n \leq 6$ the genus of $X_1(2, 2n)$ is either 0 or 1 and $X_1(2, 2n)(\mathbb{Q}) \neq \emptyset$; it follows that $\mathbb{Q}(X_1(2, 2n))$ contains functions of every degree $d \geq 2$, including $d = 5$.

For $n = 7$ we used the method of §3.1 and a modified version of the algorithm in [28] to construct the model

$$X_1(2, 14) : v^3 - (u^3 + u^2 + u - 1)v^2 - (u^5 + 3u^4 + 3u^3 + u^2 + u)v + u^5 + u^4 = 0,$$

with maps

$$q = \frac{v+1}{v - 2u + 1}, \qquad t = \frac{(v+1)(2u - v + 1)(2u(u+1) + v + 1)}{v^3 + (2u^2 + 1)v^2 - (2u^3 - 2u^2 - 2u - 1)v + u^4 + (u+1)^4}$$

that give points $(E_2(q, t), P_2(q, 2), Q_2(q, t))$ on $X_1(2, 14)$ as defined in §3.1. We may then take $u$ as a function of degree 5 in $\mathbb{Q}(X_1(2, 14))$.

For $n = 8$ we similarly constructed

$$X_1(2, 16) : v^4 + (u^3 - 2u)v^3 - (2u^4 + 2)v^2 + (u^5 + u^3 + 2u)v + 1 = 0,$$

which also has $u$ as a function of degree 5 in $\mathbb{Q}(X_1(2, 16))$ (we omit the maps $q(u, v)$ and $t(u, v)$ for reasons of space). This completes step (1) of our proof strategy.

Proceeding to steps (2)–(4), from Proposition 2.1 we find that $\gamma(X_1(2, 2n)) > 10$ for $n > 18$, and $\gamma(X_1(2, 2n)) > 5$ for $n > 13$. By Theorem 4.1 we have $\mathrm{rk}(J_1(2, 2n)(\mathbb{Q})) = 0$ for $n \leq 18$; thus by Proposition 2.3 it suffices to prove that $\mathbb{Q}(X_1(2, 2n))$ contains no functions of degree 5 for $9 \leq n \leq 13$.

For step (5) we begin by proving that $\gamma(X_1(2, 2n)_{\mathbb{F}_3}) > 5$ for $n = 10, 11, 13$ and that $\gamma(X_1(2, 24)_{\mathbb{F}_5}) > 5$ for $n = 12$, using methods similar to those in [6]. This involves exhaustively searching the Reimann–Roch spaces of a suitable set of divisors for functions of degree $d \leq 5$. The Magma code we used to perform these computations can be found in [9].

For $n = 9$ we actually have $\gamma(X_1(2, 18)) = 4$, so in this case we need to show that $\mathbb{Q}(X_1(2, 18))$ contains no functions of degree exactly equal to 5; this is addressed by Proposition 5.4 below. $\qquad\square$

**Proposition 5.4.** $\mathbb{Q}(X_1(2, 18))$ *does not contain a function of degree* 5.

*Proof.* We proceed by verifying conditions 1–5 of [6, Prop. 7] for $p = d = 5$. For $k = \mathbb{Q}, \mathbb{F}_5$, let $W_d^r(k)$ denote the closed subscheme of $\mathrm{Pic}^d(X_1(2, 18)_k(k))$ corresponding to line bundles of degree $d$ whose global sections form a $k$-vector space of dimension strictly greater than $r$.

1. The map $J_1(2, 18)(\mathbb{Q}) \to J_1(2, 18)_{\mathbb{F}_5}(\mathbb{F}_5)$ is injective because $J_1(2, 18)(\mathbb{Q})$ is finite.
2. Using Magma, a brute force search of the Riemann–Roch space of all effective divisors of degree 5 on $X_1(2, 18)_{\mathbb{F}_5}$ finds that $\mathbb{F}_5(X_1(2, 18)_{\mathbb{F}_5})$ contains no functions of degree 5.
3. A similar brute force computation shows that $W_5^2(\mathbb{F}_5) = \emptyset$.
4. A brute force computation finds that $5 - \gamma(X_1(2, 18)_{\mathbb{F}_5}) = 5 - 4 = 1$ and $\#W_4^1(\mathbb{F}_5) = 3$. The surjectivity of the map $W_4^1(\mathbb{Q}) \to W_4^1(\mathbb{F}_5)$ is verified in [9] by finding three modular units of degree 4 on $X_1(2, 18)$ with linearly independent pole divisors.
5. The reduction map $X_1(2, 18)(\mathbb{Q}) \to X_1(2, 18)_{\mathbb{F}_5}(\mathbb{F}_5)$ is surjective because the 9 elements of $X_1(2, 18)_{\mathbb{F}_5}(\mathbb{F}_5)$ are precisely the reductions of the 9 cusps in $X_1(2, 18)(\mathbb{Q})$.

It follows from [6, Prop. 7] that $\mathbb{Q}(X_1(2, 18))$ contains no functions of degree 5. $\quad\square$

We now address $d = 6$ using the same proof strategy.

**Proposition 5.5.** *We have*

$$\Phi^\infty(6) = \{(1, n) : 1 \leq n \leq 30, n \neq 23, 25, 29\} \ \cup \ \{(2, 2n) : 1 \leq n \leq 10\}$$
$$\cup \ \{(3, 3n) : 1 \leq n \leq 4\} \ \cup \ \{(4, 4), (4, 8), (6, 6)\}.$$

*Proof.* We have $\phi(m)$ dividing 6 for $m = 1, 2, 3, 4, 6, 7, 9, 14, 18$. The elements $(1, n) \in \Phi^\infty(6)$ are determined in [6, Thm. 3], and we can immediately rule out $m = 7, 9, 14, 18$, since for these $m$ we have $\phi(m) = 6$ and $d/\phi(m) = 1$, but $g(X_1(m, mn)) > 1$ for all $m > 6$ and $n \geq 1$. Faltings' theorem implies that $X_1(m, mn)(\mathbb{Q}(\zeta_m))$ is finite for $m > 6$. This leaves only $m = 2, 3, 4, 6$.

We have $\Phi^\infty(2), \Phi^\infty(3) \subseteq \Phi^\infty(6)$ (given a degree 2 or 3 point $(E, P, Q)$ on $X_1(m, mn)$ we can always base change $E$ to a number field of degree 6). It thus suffices to show that $\mathbb{Q}(\zeta_m)(X_1(m, mn))$ contains a function of degree 6 for the pairs $(2, 16), (2, 18), (2, 20)$, and a function of degree 3 for the pairs $(3, 9), (3, 12), (4, 8)$, $(6, 6)$.

The map $\pi \colon X_1(2, 2n) \to X_1(2n)$ given by $(E, P, Q) \mapsto (E, Q)$ has degree 2. For $n = 8, 9, 10$ we have a function $f$ of degree 3 in $\mathbb{Q}(X_1(2n))$, because $(1, 2n) \in \Phi^\infty(3)$ and $\mathrm{rk}(J_1(2n)(\mathbb{Q})) = 0$ (by Theorem 4.1), and $\pi \circ f$ is then a function of degree 6 in $\mathbb{Q}(X_1(2, 2n))$.

The curves $X_1(3, 9)$, $X_1(4, 8)$, $X_1(6, 6)$ all have genus 1 and a $\mathbb{Q}(\zeta_m)$-rational point (take a rational cusp); hence they are isomorphic to elliptic curves and admit functions of every degree $d \geq 2$. The map $: X_1(3, 12) \to X_1(12)_{\mathbb{Q}(\zeta_3)}$ given by $(E, P, Q) \mapsto (E, Q)$ has degree 3, and $X_1(12)_{\mathbb{Q}(\zeta_3)}$ has genus 0 and a $\mathbb{Q}(\zeta_3)$-rational point; hence it is isomorphic to $\mathbb{P}^1_{\mathbb{Q}(\zeta_m)}$. It follows that $\mathbb{Q}(\zeta_3)(X_1(3, 12))$ contains a function of degree 3.

This completes step (1) of our proof strategy. We now proceed to steps (2)–(5) for each $m = 2, 3, 4, 6$ in turn.

We begin with $m = 2$. From Proposition 2.1 we find that $\gamma(X_1(2, 2n)) > 12$ for $n > 21$, and $\gamma(X_1(2, 2n)) > 6$ for $n > 15$. By Theorem 4.1 we have $\mathrm{rk}(J_1(2, 2n)(\mathbb{Q})) = 0$ for $n \leq 21$; thus by Proposition 2.3 it suffices to prove that $\mathbb{Q}(X_1(2, 2n))$ contains no functions of degree 6 for $11 \leq n \leq 15$. For $11 \leq n \leq 14$ we proceed as in Proposition 5.3 to prove $\gamma(X_1(2, 2n)_{\mathbb{F}_p}) > 6$ using $p = 3$ for $n = 11, 13, 14$ and $p = 5$ for $n = 12$, which was done with a computation in Magma. The code written for these and the subsequent computations can be found in [9]. For $n = 15$ we instead apply Lemma 5.6 and Proposition 5.7.

We next consider $m = 3$. We have $\gamma(X_1(3, 3n)) > 6$ for $n > 8$ and $\gamma(X_1(3, 3n)) > 3$ for $n > 5$, and $\mathrm{rk}(J_1(3, 3n)(\mathbb{Q}(\zeta_3))) = 0$ for $n \leq 8$. It suffices to show that $\mathbb{Q}(\zeta_3)(X_1(3, 15))$ contains no functions of degree 3, which again follows from a Magma computation.

The cases $m = 4, 6$ are similar. For $m = 4$ we have $\gamma(X_1(4, 4n)) > 6$ for $n > 6$ and $\gamma(X_1(4, 4n)) > 3$ for $n > 3$, and $\mathrm{rk}(J_1(4, 4n)(\mathbb{Q}(\zeta_4))) = 0$ for $n \leq 6$; a computation shows that $\gamma(X_1(4, 12)_{\mathbb{F}_5}) > 3$. For $m = 6$ we have $\gamma(X_1(6, 6n)) > 6$ for $n > 2$ and $\mathrm{rk}(J_1(6, 6n)(\mathbb{Q}(\zeta_6))) = 0$ for $n \leq 2$; a Magma computation shows that $\gamma(X_1(6, 12)_{\mathbb{F}_5}) > 3$. $\qquad \square$

**Lemma 5.6.** $X_1(2, 30)$ *has no non-cuspidal points of degree less than 6.*

*Proof.* $X_1(2, 30)$ has a degree two map to $X_1(30)$ given by $(E, P, Q) \mapsto (E, Q)$, so we start by considering the points of degree less than 6 on $X_1(30)$.

Theorem 3 of [6] states that $X_1(30)$ has only finitely many points of degree less than 6, and these points are explicitly determined in [7]. The non-cuspidal points on $X_1(30)$ of degree less than 6 all have degree 5 and arise from two Galois conjugacy classes of elliptic curves that we now describe.

Let $x_1, x_2 \in \overline{\mathbb{Q}}$ be zeros of $x^5 + x^4 - 3x^3 + 3x + 1$ and $x^5 + x^4 - 7x^3 + x^2 + 12x + 3$, respectively, and define

$$y_1 := 2x_1^4 + x_1^3 - 6x_1^2 + 4x_1 + 4, \quad y_2 := \frac{3x_2^4 + 7x_2^3 + 6x_2^2 + 11x_2 - 73}{53}.$$

Let $E_{x,y}$ denote the curve $E(b, c)$ in Tate normal form with $b = rs(r-1)$ and $c = s(r-1)$, where $r = (x^2y - xy + y - 1)/(x^2y - x)$ and $s := (xy - y + 1)/(xy)$.

The point $P_0 := (0,0)$ is a point of order 30 on both $E_{x_1,y_1}$ and $E_{x_2,y_2}$. Moreover, every non-cuspidal point $(E, P) \in X_1(30)(\overline{\mathbb{Q}})$ of degree less than 6 over $\mathbb{Q}$ can be obtained as either $(E_{\sigma(x_1),\sigma(y_1)}, dP_0)$ or $(E_{\sigma(x_2),\sigma(y_2)}, dP_0)$ for some $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and $d \in (\mathbb{Z}/30\mathbb{Z})^\times$; thus every such point has degree 5.

The 2-division polynomials of $E_{x_1,y_1}$ and $E_{x_2,y_2}$ each have just one root in $\mathbb{Q}(x_1)$ and $\mathbb{Q}(x_2)$, respectively, corresponding to $x(15P_0)$; it follows that $E_{x_1,y_1}(\mathbb{Q}(x_1))$ and $E_{x_2,y_2}(\mathbb{Q}(x_2))$ contain no other points of order 2. Thus every non-cuspidal point in $X_1(2,30)(\overline{\mathbb{Q}})$ that maps to a point of degree less than 6 in $X_1(30)(\overline{\mathbb{Q}})$ has degree at least $2 \cdot 5 = 10$. The lemma follows. $\square$

**Proposition 5.7.** $X_1(2,30)$ *has only finitely many points of degree* 6.

The proof below is based on ideas presented in [8, §4].

*Proof.* We have $d(X_1(2,30)) = \gamma(X_1(2,30))$ by Proposition 2.3, since $\mathrm{rk}(J_1(2,30)(\mathbb{Q})) = 0$, by Theorem 4.1, and $d(X_1(2,30)) = \gamma(X_1(2,30)) \geq 6$, by Lemma 5.6. It thus suffices to prove there are no functions of degree 6 in $\mathbb{Q}(X_1(2,30))$.

We first show that if $\mathbb{Q}(X_1(2,30))$ contains a function of degree 6, then it contains a function whose pole and zero divisors consist entirely of cusps. Let $f \in \mathbb{Q}(X_1(2,30))$ be a function of degree 6 and let $c \in X_1(2,30)(\mathbb{Q})$ be any of its 12 rational cusps. We may assume $f$ has a pole at $c$ by replacing $f$ with $1/(f-f(c))$ if necessary. The pole divisor of $f$ can then be written as $c + D$, where $D$ is a divisor of degree 5. Now let $c' \neq c$ be a rational cusp not in the support of $D$, and define $f' := f - f(c')$. The function $f'$ has the same poles as $f$, and its zero divisor can be written as $c' + D'$ with $D'$ a divisor of degree 5. The divisors $D$ and $D'$ must consist entirely of cusps, by Lemma 5.6, and the claim follows.

An enumeration of all $f \in \mathbb{Q}(X_1(2,30))$ of degree at most 6 with $\mathrm{div}(f)$ supported on cusps computed as in [6, Footnote 7] finds none with degree exactly 6; the proposition follows. $\square$

## Acknowledgement

## References

[1] Dan Abramovich, *A linear lower bound on the gonality of modular curves*, Internat. Math. Res. Notices **no. 20** (1996), 1005–1011. MR1422373

[2] A. O. L. Atkin and Wen Ch'ing Winnie Li, *Twists of newforms and pseudo-eigenvalues of W-operators*, Invent. Math. **48** (1978), no. 3, 221–243. MR508986

[3] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, Computational algebra and number theory (London, 1993), J. Symbolic Comput. **24** (1997), no. 3-4, 235–265. MR1484478

[4] Brian Conrad, Bas Edixhoven, and William Stein, $J_1(p)$ *has connected fibers*, Doc. Math. **8** (2003), 331–408. MR2029169

[5] P. Deligne and M. Rapoport, *Modular functions of one variable, II* (French), Lecture Notes in Math., Vol. 349, 1973, pp. 143–316. MR0337993

[6] Maarten Derickx and Mark van Hoeij, *Gonality of the modular curve $X_1(N)$*, J. Algebra **417** (2014), 52–71. MR3244637

[7] Maarten Derickx and Mark van Hoeij, data related to [6], available at `www.math.fsu.edu/~hoeij/files/X1N`, 2013.

[8] Maarten Derickx, Sheldon Kamienny, and Barry Mazur, *Rational families of 17-torsion points of elliptic curves over number fields*, Contemporary Mathematics, AMS, to appear.

[9] Maarten Derickx and Andrew V. Sutherland, GitHub repository related to *Torsion subgroups of elliptic curves over quintic and sextic number fields*, available at `https://github.com/koffie/mdmagma/`, 2016.

[10] Maarten Derickx and Andrew V. Sutherland, *Explicit models of $X_1(m, mn)$*, available at `http://math.mit.edu/~drew/X1mn.html`, 2016.

[11] Gerhard Frey, *Curves with infinitely many points of fixed degree*, Israel J. Math. **85** (1994), no. 1-3, 79–83. MR1264340

[12] Gerd Faltings, *The general case of S. Lang's conjecture*, Barsotti Symposium in Algebraic Geometry (Abano Terme, 1991), Perspect. Math., vol. 15, Academic Press, San Diego, CA, 1994, pp. 175–182. MR1307396

[13] Sonal Jain, *Points of low height on elliptic surfaces with torsion*, LMS J. Comput. Math. **13** (2010), 370–387. MR2685131

[14] Daeyeol Jeon, Chang Heon Kim, and Yoonjin Lee, *Families of elliptic curves over cubic number fields with prescribed torsion subgroups*, Math. Comp. **80** (2011), no. 273, 579–591. MR2728995

[15] Daeyeol Jeon, Chang Heon Kim, and Euisung Park, *On the torsion of elliptic curves over quartic number fields*, J. London Math. Soc. (2) **74** (2006), no. 1, 1–12. MR2254548

[16] Daeyeol Jeon, Chang Heon Kim, and Andreas Schweizer, *On the torsion of elliptic curves over cubic number fields*, Acta Arith. **113** (2004), no. 3, 291–301. MR2069117

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

[18] Kazuya Kato, *p-adic Hodge theory and values of zeta functions of modular forms* (English, with English and French summaries), Cohomologies $p$-adiques et applications arithmétiques. III, Astérisque **No. 295** (2004), ix, 117–290. MR2104361

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

[20] Henry H. Kim, *Functoriality for the exterior square of $GL_4$ and the symmetric fourth of $GL_2$*, with appendix 1 by Dinakar Ramakrishnan and appendix 2 by Kim and Peter Sarnak, J. Amer. Math. Soc. **16** (2003), no. 1, 139–183. MR1937203

[21] V. A. Kolyvagin and D. Yu. Logachëv, *Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties* (Russian), Algebra i Analiz **1** (1989), no. 5, 171–196; English transl., Leningrad Math. J. **1** (1990), no. 5, 1229–1253. MR1036843

[22] Daniel Sion Kubert, *Universal bounds on the torsion of elliptic curves*, Proc. London Math. Soc. (3) **33** (1976), no. 2, 193–237. MR0434947

[23] Abhinav Kumar and Tetsuji Shioda, *Multiplicative excellent families of elliptic surfaces of type $E_7$ or $E_8$*, Algebra Number Theory **7** (2013), no. 7, 1613–1641. MR3117502

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

[25] Loïc Merel, *Bornes pour la torsion des courbes elliptiques sur les corps de nombres* (French), Invent. Math. **124** (1996), no. 1-3, 437–449. MR1369424

[26] Markus A. Reichert, *Explicit determination of nontrivial torsion structures of elliptic curves over quadratic number fields*, Math. Comp. **46** (1986), no. 174, 637–658. MR829635

[27] Joseph H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR2514094

[28] Andrew V. Sutherland, *Constructing elliptic curves over finite fields with prescribed torsion*, Math. Comp. **81** (2012), no. 278, 1131–1147. MR2869053

[29] André Weil, *L'arithmétique sur les courbes algébriques* (French), Acta Math. **52** (1929), no. 1, 281–315. MR1555278

Mathematisch Instituut, Universiteit Leiden, Postbus 9512, 2300 RA Leiden, Netherlands

Department of Mathematics, Massachusetts Institute of Technology, 77 Massachsuetts Avenue, Cambridge, Massachusetts 02139