Algebra & Number Theory

Volume 15
2021
No. 7

Sporadic cubic torsion

Maarten Derickx, Anastassia Etropolski, Mark van Hoeij,
Jackson S. Morrow and David Zureick-Brown

msp

ALGEBRA AND NUMBER THEORY 15:7 (2021)
https://doi.org/10.2140/ant.2021.15.1837

Sporadic cubic torsion

Maarten Derickx, Anastassia Etropolski, Mark van Hoeij,
Jackson S. Morrow and David Zureick-Brown

Let K be a number field, and let E/K be an elliptic curve over K. The Mordell–Weil theorem asserts that the K-rational points $E(K)$ of E form a finitely generated abelian group. In this work, we complete the classification of the finite groups which appear as the torsion subgroup of $E(K)$ for K a cubic number field.

To do so, we determine the cubic points on the modular curves $X_1(N)$ for

$$N = 21, 22, 24, 25, 26, 28, 30, 32, 33, 35, 36, 39, 45, 65, 121.$$

As part of our analysis, we determine the complete lists of N for which $J_0(N)$, $J_1(N)$, and $J_1(2, 2N)$ have rank 0. We also provide evidence to a generalized version of a conjecture of Conrad, Edixhoven, and Stein by proving that the torsion on $J_1(N)(\mathbb{Q})$ is generated by $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-orbits of cusps of $X_1(N)_{\overline{\mathbb{Q}}}$ for $N \leq 55$, $N \neq 54$.

1. Introduction

Let $E/\mathbb{Q}$ be an elliptic curve defined over the rationals $\mathbb{Q}$. Poincaré [1910] conjectured that the set $E(\mathbb{Q})$ of $\mathbb{Q}$-rational points on E is a finitely generated abelian group. Mordell [1922] proved this conjecture and Weil [1929] generalized it to an arbitrary abelian variety defined over a number field.

Theorem 1.1 (Mordell–Weil). *For an elliptic curve defined over a number field K,*

$$E(K) \cong \mathbb{Z}^r \oplus E(K)_{\mathrm{tors}}.$$

The free rank r of $E(K)$ is the *rank of E over K* and the finite group $E(K)_{\mathrm{tors}}$ is the *torsion subgroup of $E(K)$*. Since $E(K)_{\mathrm{tors}}$ is isomorphic to a finite subgroup of $(\mathbb{Q}/\mathbb{Z})^2$, we know that this group must be isomorphic to a group of the form

$$\mathbb{Z}/N\mathbb{Z} \oplus \mathbb{Z}/NM\mathbb{Z},$$

for positive integers N, M. The celebrated result of Mazur classified which N, M appear for $K = \mathbb{Q}$.

Theorem 1.2 [Mazur 1977]. *Let $E/\mathbb{Q}$ be an elliptic curve. Then $E(\mathbb{Q})_{\mathrm{tors}}$ is isomorphic to one of the following* 15 *groups*:

$$\mathbb{Z}/N_1\mathbb{Z} \qquad \text{with } 1 \leq N_1 \leq 12,\ N_1 \neq 11,$$
$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N_2\mathbb{Z} \qquad \text{with } 1 \leq N_2 \leq 4.$$

Furthermore, there exist infinitely many $\overline{\mathbb{Q}}$-isomorphism classes for each such torsion subgroup.

MSC2020: primary 11G18; secondary 11G05, 11Y50, 14H45.
Keywords: modular curves, elliptic curves, finitely many cubic points.

The modular curves $X_1(M, MN)$ classify elliptic curves (and degenerations) together with independent points P, Q of order M and MN. In this language, Mazur's theorem asserts that $X_1(M, MN)(\mathbb{Q})$ has no noncuspidal rational points for (M, MN) outside of the above set.

Merel [1996] proved the existence of a uniform bound on the size of $E(K)_{\text{tors}}$ that depends only on the degree of the number field K. Merel's result leads to the natural question of classifying (up to isomorphism) the torsion subgroups of elliptic curves defined over number fields of degree d, for a fixed integer $d \geq 1$.

For $d = 2$, this classification was started by Kenku and Momose and completed by Kamienny.

Theorem 1.3 [Kenku and Momose 1988; Kamienny 1992a]. *Let $K/\mathbb{Q}$ be a quadratic extension and E/K be an elliptic curve. Then $E(K)_{\text{tors}}$ is isomorphic to one of the following* 26 *groups*:

$$\begin{aligned}
&\mathbb{Z}/N_1\mathbb{Z} && \text{with } 1 \leq N_1 \leq 18,\ N_1 \neq 17,\\
&\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N_2\mathbb{Z} && \text{with } 1 \leq N_2 \leq 6,\\
&\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3N_3\mathbb{Z} && \text{with } N_3 = 1, 2,\\
&\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}.
\end{aligned}$$

Furthermore, there exist infinitely many $\overline{\mathbb{Q}}$-isomorphism classes for each such torsion subgroup.

The modular curves $X_1(M, MN)$ for this list all have genus ≤ 2; all have infinitely many quadratic points.

1.4. ***Statement of main results.*** In this paper, we shall be concerned with the case of $d = 3$. Jeon, Kim, and Schweizer [2004] determined the torsion structures that appear infinitely often as one varies over all elliptic curves over all cubic number fields (i.e., they classified the pairs (M, MN) for which $X_1(M, MN)$ is trigonal, and show there are no $X_1(M, MN)$ which admit a degree 3 map to a positive rank elliptic curve over $\mathbb{Q}$). Jeon, Kim, and Lee [2011] constructed infinite families of elliptic curves realizing each of these torsion structures by finding models of the relevant trigonal modular curves. The first author and Najman [Derickx and Najman 2019] classified the torsion groups of elliptic curves over cubic fields with Galois group $\mathbb{Z}/3\mathbb{Z}$, complex cubic fields, and totally real cubic fields with Galois group S_3.

Najman [2016] discovered the first example of *sporadic* torsion: the elliptic curve $E/\mathbb{Q}$ with Cremona label `162b1` satisfies $E(\mathbb{Q}(\zeta_9)^+)_{\text{tors}} \cong \mathbb{Z}/21\mathbb{Z}$, and is the only elliptic curve defined over $\mathbb{Q}$ which admits a K-rational 21-torsion point. He then classified the possible torsion subgroups of elliptic curves defined over $\mathbb{Q}$ when considered over some cubic number field K. The consideration of the base change of elliptic curves defined over $\mathbb{Q}$ to other number fields leads to sharper results concerning the torsion subgroups which appear over number fields K (see [Lozano-Robledo 2013]). A computer generated table of sporadic points is given in [van Hoeij 2014].

Parent [2000; 2003] proved that cubic torsion points of prime order p do not exist for $p > 13$ (reliant on Kato's [2004] subsequent generalization of Kolyvagyn's theorem to quotients of $J_1(N)$). Momose [1984, Theorem B] ruled out the cyclic torsion for the cases $N_1 = 27, 64$. It was formally conjectured in [Wang 2015, Conjecture 1.1.2] that the only possible torsion structures for elliptic curves over K are

the ones identified in [Jeon, Kim, and Schweizer 2004; Najman 2016]. Wang made progress on this conjecture in his thesis (see [Wang 2018; 2019; 2020] for updated versions), and ruled out the existence of cyclic torsion for $N_1 = 77, 91, 143, 169$. Bruin and Najman [2016, Theorem 7] ruled out the cyclic cases $N_1 = 40, 49, 55$ and the noncyclic case $N_2 = 10$.

Our main theorem completes the classification of torsion over cubic number fields.

Theorem A. *Let $K/\mathbb{Q}$ be a cubic extension and E/K be an elliptic curve. Then $E(K)_{\mathrm{tors}}$ is isomorphic to one of the following 26 groups*:

$$\begin{aligned} &\mathbb{Z}/N_1\mathbb{Z} && \text{with } N_1 = 1, \dots, 16, 18, 20, 21, \\ &\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N_2\mathbb{Z} && \text{with } N_2 = 1, \dots, 7. \end{aligned}$$

There exist infinitely many $\overline{\mathbb{Q}}$-isomorphism classes for each such torsion subgroup except for $\mathbb{Z}/21\mathbb{Z}$. In this case, the elliptic curve with Cremona label `162b1` and minimal Weierstrass equation $y^2 + xy + y = x^3 - x^2 - 5x + 5$ over $\mathbb{Q}(\zeta_9)^+ \cong \mathbb{Q}[x]/(x^3 - 3x + 1)$ is the unique elliptic curve over a cubic field with $\mathbb{Z}/21\mathbb{Z}$-torsion, in particular the point $(2\alpha - 3, 2\alpha - 2)$ has order 21 where α is a root of $x^3 - 3x + 1$.

Remark 1.5 (enumeration of remaining cases). Combining the above work of Parent, Momose, Wang, and Bruin and Najman, the remaining task[1] is to determine the cubic points on the modular curves $X_1(N_1)$ for

$$N_1 = 21, 22, 24, 25, 26, 28, 30, 32, 33, 35, 36, 39, 45, 65, 121$$

and on $X_1(2, 2N_2)$ for $N_2 = 8, 9$. (Note that there is a natural map $X_1(4N) \to X_1(2, 2N)$ by [Jeon and Kim 2005, Section 1], and thus the determination of the cubic points on $X_1(2, 16)$ and $X_1(2, 18)$ determines the cubic points on $X_1(32)$ and $X_1(36)$.)

1.6. ***Strategy.*** We first determine the complete lists of N for which $J_0(N)$, $J_1(N)$ and $J_1(2, 2N))$ have rank 0 (Section 3). For the N_i from Remark 1.5, $J_1(N_1)(\mathbb{Q})$ has rank 0, unless $N_1 = 65, 121$.

For the rank 0 cases, we use a variety of techniques:

- local arguments (Section 5.1),
- direct computation of preimages of an Abel–Jacobi map $X_1(N)^{(3)}(\mathbb{Q}) \to J_1(N)(\mathbb{Q})$ (Section 5.2),
- passage to modular curve quotients (Section 5.3),
- results on the cuspidal subgroup of $J_1(N)(\mathbb{Q})$ (Section 4), and
- explicit description of cusps on $X_1(N)$ via modular units (Section 2.9).

For the rank 1 cases, we use a modified formal immersion criterion (Sections 7.1 and 7.3). These methods are expounded on in Sections 4 and 5.

[1] Wang's proofs for $N_1 = 22, 25, 39, 40, 49, 55, 65$ contain an error, which we address in Remark 7.5. (The remaining cases from Wang's papers are correct.)

1.7. ***Outline of paper.*** In Section 2, we recall background on the arithmetic of curves, modular curves, cuspidal subschemes of modular curves, and modular units. In Section 3, we determine the complete lists of N for which $J_0(N)$, $J_1(N)$, and $J_1(2, 2N))$ have rank 0, and in Section 4, we investigate the torsion subgroup of $J_1(N)(\mathbb{Q})$ via modular symbols. We describe the various techniques used to determine the cubic points on $X_1(N)$ in Section 5, and we conclude with the determination of cubic points on modular curves in Sections 6 and 7.

1.8. ***Conventions.*** Let K be a field and let X/K be a nice curve, i.e., a smooth, proper, geometrically integral scheme of dimension one. For such an X, let $K(X)$ denote its function field and let J_X denote its Jacobian. For a field $L \supset K$, let X_L denote the base change of X to L. In some cases, we will use this notation when the curve X is defined over a ring R. Let $\mathrm{Div}\, X$ be the group of all divisors of X, and let $\mathrm{Div}^0 X$ be the subgroup of divisors of degree 0. Let $\mathrm{Div}_L X$ (resp. $\mathrm{Div}^0_L X$) be the group of all divisors (resp. the subgroup of divisors of degree 0) of the curve X_L. We note that base change gives inclusions $\mathrm{Div}\, X \hookrightarrow \mathrm{Div}_L X$ and $\mathrm{Div}^0 X \hookrightarrow \mathrm{Div}^0_L X$. For abelian varieties A_1, A_2 over K, we will use the notation $A_1 \sim_{\mathbb{Q}} A_2$ to denote that A_1 is $\mathbb{Q}$-isogenous to A_2. We will typically refer to a finite abelian group by its invariants $[n_1, \ldots, n_m]$ (ordered by divisibility).

1.9. ***Comments on code.*** This paper has a large computational component. We use the computer algebra programs `Maple` [Maple 2005], `Magma` [Magma 1997], and `Sage` [Sage 2017] to perform these computations. The code verifying our claims is available as an online supplement to this paper.

1.10. ***Summary of cases and techniques.*** In Table 1, we summarize the modular curves from Remark 1.5, their genera, and the proof technique we use to determine the cubic points on these modular curves.

2. Background

Here we recall some basic definitions concerning curves and the definition of certain modular curves.

2.1. ***Geometry of curves.*** First, we review a few definitions from the geometry of curves. Let X be a smooth proper geometrically connected curve defined over a field K.

Definition 2.2. The *gonality* $\gamma(X)$ of X is the minimal degree among all finite morphisms $X \to \mathbb{P}^1_K$. We say that a closed point $P \in X$ has *degree* d if $[K(P) : K] = d$.

Remark 2.3. If X admits a map $f : X \to \mathbb{P}^1_K$ of degree d, or a map $f : X \to E$ of degree d, where E is an elliptic curve with positive rank over K, then X also admits infinitely many points of degree d (arising from fibers of f). Conversely, if $d < \gamma(X)/2$, then X admits only finitely many points of degree d [Frey 1994, Proposition 1]; if the Jacobian of X has rank 0 over K (and in particular X does not admit a nonconstant map to an elliptic curve with positive rank over K), then in fact for $d < \gamma(X)$, X admits only finitely many points of degree d [Derickx and Sutherland 2017, Proposition 2.3].

Level	Genus	Method of proof	Genus of quotient
32	17	Maps to another curve in this table	$g(X_1(2,16)) = 5$
36	17	Maps to another curve in this table	$g(X_1(2,18)) = 7$
22	6	Local methods at $p = 3$ (Section 6.1)	N/A
25	12	Local methods at $p = 3$	N/A
21	5	Direct analysis over $\mathbb{Q}$ (Section 6.2)	N/A
26	10	Direct analysis over $\mathbb{F}_3$	N/A
30	9	Direct analysis over $\mathbb{Q}$ on $X_0(30)$ (Section 6.4)	$g(X_0(30)) = 3$
33	21	Direct analysis over $\mathbb{Q}$ on $X_0(33)$	$g(X_0(33)) = 3$
35	25	Direct analysis over $\mathbb{Q}$ on $X_0(35)$	$g(X_0(35)) = 3$
39	33	Direct analysis over $\mathbb{Q}$ on $X_0(39)$	$g(X_0(39)) = 3$
(2,16)	5	Hecke bound + direct analysis over $\mathbb{F}_3$ (Section 6.5)	N/A
(2,18)	7	Hecke bound + direct analysis over $\mathbb{F}_5$	N/A
28	10	Hecke bound + direct analysis over $\mathbb{F}_3$ (Section 6.6)	N/A
24	5	Hecke bound + additional argument (Theorem 4.13) + direct analysis over $\mathbb{F}_5$	N/A
45	41	Hecke bound + direct analysis over $\mathbb{Q}$ on $X_H(45)$ (Section 6.7)	$g(X_H(45)) = 5$
65	121	Formal immersion criteria (Section 7.3)	$g(X_0(65)) = 5$
121	526	Formal immersion criteria (Section 7.1)	$g(X_0(121)) = 6$

Table 1. Summary of genera of modular curves and proof techniques.

Definition 2.4. For a positive integer d, we define the *d-th symmetric power of X* to be $X^{(d)} := X^d/S_d$, where S_d is the symmetric group on d letters. The K-points of $X^{(d)}$ correspond to effective K-rational divisors on X of degree d. In particular, a point of X/K of degree d gives rise to a divisor of degree d, and thus a point of $X^{(d)}(K)$, and we will often identify a degree d point of X with a divisor of degree d without distinguishing notation.

If $X^{(d)}(K)$ is nonempty, then a fixed K-rational divisor E of degree d gives rise to a corresponding *Abel–Jacobi map*

$$f_{d,E} : X^{(d)} \to J_X, \quad D \mapsto D - E.$$

2.5. ***Modular curves.*** We now list the various modular curves we will study.

The modular curve $X_1(M, MN)$ is the moduli space whose noncuspidal K-rational points classify elliptic curves over K together with independent points P, Q of order M and MN. By setting $M = 1$, we encounter the modular curves $X_1(N) := X_1(1, N)$ whose noncuspidal K-rational points parametrize elliptic curves over K which have a torsion point of exact order N defined over K.

The modular curve $X_0(N)$ is the moduli space whose noncuspidal K-rational points classify elliptic curves with a cyclic subgroup of order N (or equivalently, a cyclic isogeny of degree N).

For a subgroup $\Gamma_1(N) \subseteq H \subseteq \Gamma_0(N)$, we can form the "intermediate" modular curve $X_H(N)$. This curve is a quotient of $X_1(N)$ by a subgroup of $\mathrm{Aut}(X_1(N))$, and (roughly) parametrizes elliptic curves whose mod N Galois representation has image contained in H (see [Rouse and Zureick-Brown 2015, Lemma 2.1]).

Remark 2.6 (models of X_H). For computational purposes, we need explicit equations for many of these modular curves. For small values of N, the `Magma` intrinsic `SmallModularCurve(N)` produces smooth models for the modular curves $X_0(N)$. For larger values of N (e.g., $N = 65, 121$), we use work of Ozman and Siksek [2019] to find canonical models for $X_0(N)$. We use the algorithm from [Derickx et al. 2013, Section 2] to compute an equation for a quotient of $X_1(45)$ via relations between modular units; see Section 6.7.

There are several ways to compute models for $X_1(M, MN)$. We use [Sutherland 2012a] for the equations for $X_1(N)$ and for the j-map $j : X_1(N) \to X(1)$. These models are generally singular. We can compute models for $X_1(M, MN)$ by taking the normalization of (a particular component of) the fiber product $X_1(M) \times_{X(1)} X_1(MN)$. A priori, the fiber product produces a singular model X. We can desingularize using the canonical map and the `Magma` intrinsic `CanonicalImage(X,CanonicalMap(X))`. We can also compute a model for $X_1(2, 2N)$ by computing a quotient of $X_1(4N)$ with [Derickx et al. 2013, Section 2], or we can use [Derickx and Sutherland 2017, Section 3] (we checked that our models are birational to theirs).

2.7. ***Cuspidal subschemes of modular curves.*** Our analysis of cubic points will heavily rely on understanding the cuspidal *subscheme* of $X_1(N)$ and $X_0(N)$.

Lemma 2.8. *Let $N \geq 5$ be a positive integer, and let $R = \mathbb{Z}[1/2N]$.*

(1) *The cuspidal subscheme of $X_1(N)_R$ is isomorphic to*

$$\coprod_{d|N} (\mu_{N/d} \times \mathbb{Z}/d\mathbb{Z})'/[-1],$$

where the prime notation refers to points of maximal order.

(2) *The cuspidal subscheme of $X_0(N)_R$ is isomorphic to*

$$\coprod_{d|N} (\mu_{\gcd(d,N/d)})',$$

where the prime notation refers to points of maximal order.

Proof. This can be directly computed from [Derickx 2016, Chapter 1, Sections 1.3, 1.4, and 2.2] and [Derickx and van Hoeij 2014, Footnote 5]. □

2.9. ***Modular units.*** In practice, we will work with some model of $X_1(N)$ (canonical or singular), and will need to explicitly determine the cusps on our model (e.g., to find an explicit basis for $J_1(N)(\mathbb{Q})_{\mathrm{tors}}$). The naive approach is to compute the poles of the j-map but it has high degree when N is large. Modular units are a useful alternative.

Definition 2.10. A nonzero element of $\mathbb{Q}(X_1(N))$ is called a *modular unit* if all of its poles and roots are cusps. Let $\mathcal{F}_1(N) \subset \mathbb{Q}(X_1(N))/\mathbb{Q}^\times$ be *the group of modular units modulo* $\mathbb{Q}^\times$.

A basis of $\mathcal{F}_1(N)$ mod $\mathbb{Q}^\times$ is given in [Derickx and van Hoeij 2014, Conjecture 1] which was proved by Streng [2015, Theorem 1]. The relevance for our purposes is that this basis is expressed in terms of the same coordinates used in the defining equations for $X_1(N)$ from [Sutherland 2012b], and we have their divisors as well [van Hoeij and Smith 2021]. For further discussion of modular units, we refer the reader to [Derickx and van Hoeij 2014, Section 2; Kubert and Lang 1981].

3. Modular Jacobians of rank 0

In this section, we compute, with proof, the complete lists of N for which $J_0(N)(\mathbb{Q})$, $J_1(N)(\mathbb{Q})$, and $J_1(2, 2N)(\mathbb{Q})$ have rank 0. This extends the computation of [Derickx and van Hoeij 2014, Lemma 1(3)] and [Derickx and Sutherland 2017, Theorem 4.1].

Theorem 3.1. *Let S_0 be the set*

$$\{1, \ldots, 36, 38, \ldots, 42, 44, \ldots, 52, 54, 55, 56, 59, 60, 62, 63, 64, 66, 68, 69, 70, 71, 72, 75, 76, 78,$$
$$80, 81, 84, 87, 90, 94, 95, 96, 98, 100, 104, 105, 108, 110, 119, 120, 126, 132, 140, 144, 150, 168, 180\},$$

and let S_1 be the set

$$\{1, \ldots, 21, 24, 25, 26, 27, 30, 33, 35, 42, 45\}.$$

Then the following are true.

(1) *The rank of $J_0(N)(\mathbb{Q})$ is zero if and only if $N \in S_0$.*

(2) *The rank of $J_1(N)(\mathbb{Q})$ is zero if and only if $N \in S_0 - \{63, 80, 95, 104, 105, 126, 144\}$.*

(3) *The rank of $J_1(2, 2N)(\mathbb{Q})$ is zero if and only if $N \in S_1$.*

In preparation of the proof, we make a series of remarks about computing ranks of modular abelian varieties.

Remark 3.2 (analytic ranks). Let A be a simple factor of $J_1(N)$. By Kolyvagyn's theorem (improved to $J_1(N)$ by Kato [2004, Corollary 14.3]), the rank of $A(\mathbb{Q})$ is zero if and only if the L-series of A, $L(A, s)$, evaluated at 1 is nonzero. A provably correct computation of whether $L(A, 1) \neq 0$ is implemented in Magma: `Decomposition(JOne(N))` computes the simple factors of $J_1(N)$, and for a simple factor A, `IsZeroAt(LSeries(A),1)` provably computes whether $L(A, 1) \neq 0$. (This is similar to the approach of [Derickx and Sutherland 2017, Theorem 4.1].)

For simple factors of $J_0(N)$ this computation is quite fast, even for relatively large N. For factors of $J_1(N)$ this computation is much slower, even for N in the $100, \ldots, 180$ range.

Remark 3.3 (winding quotients). A faster alternative to working directly with the L-series of the simple factors of $J_*(N)$, where $*$ is either 0 or 1, is the following. The *winding quotient* $J_e(N)$ of $J_*(N)$ is the largest quotient with analytic rank zero, and may be described as $J_e(N) = J_*(N)/I_e J_*(N)$, where $e = \{0, \infty\} \in H_1(X_*(N)(\mathbb{C}), \mathbb{Q})$ is the "winding element" and I_e is the annihilator of e in the Hecke algebra $\mathbf{T}$ (see [Merel 1996, Proposition 1; Derickx et al. 2017, Definition 4.1 and Theorem 4.2]). In particular, $J_*(N)(\mathbb{Q})$ has rank zero if and only if the projection of the image of e under the Hecke algebra $\mathbf{T}$ onto the cuspidal subspace spans it.

By [Lario and Schoof 2002, Theorem 5.1], the Hecke algebra $\mathbf{T}$ on $\Gamma_*(N)$ is generated by T_n with

$$n \leq \frac{k}{12} \cdot [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_*(N)]$$

(where we note that their proof, as written, also works for $\Gamma_1(N)$), so this computation is finite and easily implemented in `Magma`; see `master-ranks.m` for more detail.

Remark 3.4 (moonshine and Ogg's Jack Daniels challenge). The subspace of weight 2 newforms with sign of functional equation equal to -1 is the subspace fixed by the Fricke involution, and thus for p prime, $J_0(p)$ is isogenous to a product $A \times J_0^+(p)$, where $J_0^+(p)$ is the Jacobian of the quotient $X_0^+(p)$ of $X_0(p)$ by the Fricke involution, and where, necessarily, each factor of A has even rank and each factor of $J_0(p)$ has odd rank. In particular, if $J_0(p)(\mathbb{Q})$ has rank 0, then $X_0^+(p)$ has genus 0.

As is well celebrated, Ogg [1975, Remarque 1] proved that for p prime, $X_0^+(p)$ has genus 0 if and only if p divides the order of the Monster group. Hence, if $J_0(N)(\mathbb{Q})$ has rank 0 and p is a prime divisor of N, then p divides

$$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$$

(and offered a bottle of Jack Daniels for an explanation of the coincidence).

We note that this approach does not generalize to composite level N. For example, $J_0(28)(\mathbb{Q})$ has rank 0, but $X_0^+(28)$ is the elliptic curve $X_0(14)$. It is still true that one can deduce the signs of the functional equations of newforms via Atkin–Lehner, but the presence of oldforms contributes additional genus to $X_0^+(N)$.

Proof of Theorem 3.1. For $N \in S_0$, we compute that $J_0(N)(\mathbb{Q})$ has rank 0 via Remark 3.2 (using Remark 3.3 to check our computation), and for any integer of the form $N \cdot p$ with $N \in S_0$ and p a prime divisor of the order of the Monster group, we again similarly compute that the rank is nonzero via `Magma`. This proves part (1).

For part (2), if $J_1(N)(\mathbb{Q})$ has rank 0, then $J_0(N)(\mathbb{Q})$ also has rank 0 (but not conversely), so we again check using Remark 3.2 (and Remark 3.3 for some of the larger N) for which $N \in S_0$ $J_1(N)(\mathbb{Q})$ has rank 0.

For part (3), by [Jeon and Kim 2005, Section 1], there is an isomorphism $X_\Delta(4N) \to X_1(2, 2N)$, with $\Delta := \{\pm 1, \pm(2N+1)\}$, and thus a surjection $X_1(4N) \to X_1(2, 2N)$. Thus, if $J_1(4N)(\mathbb{Q})$ has rank 0, then $J_1(2, 2N)(\mathbb{Q})$ also has rank 0. On the other hand, there are surjective maps $X_1(2, 2N) \cong X_\Delta(4N) \to X_0(4N)$ and $X_1(2, 2N) \to X_1(2N)$, so if either $J_0(4N)(\mathbb{Q})$ or $J_1(2N)(\mathbb{Q})$ have positive rank,

then $J_1(2, 2N)(\mathbb{Q})$ also has positive rank. Cases (1) and (2) thus determine the rank of $J_1(2, 2N)(\mathbb{Q})$ unless $N = 20, 26, 36$. The remaining three cases we do by hand using the isomorphism $X_\Delta(4N) \to X_1(2, 2N)$ and `Magma`'s intrinsic `JH` to compute the rank of $J_\Delta(4N)$ via Remark 3.2. □

See the file `master-ranks.m` for code verifying these computations.

4. Computing rational torsion on modular Jacobians

This section explains how to compute the rational torsion of a modular Jacobian. For an additional technique see [Ozman and Siksek 2019, Section 4].

4.1. ***Local bounds on torsion via reduction.*** Let K be a number field, $\mathfrak{p}$ a prime of K lying over a rational prime $p > 2$, and A/K an abelian variety with good reduction at $\mathfrak{p}$. Then by [Katz 1981, Appendix], if the ramification index $e_\mathfrak{p}$ is less than $p-1$, the reduction map $A(K)_{\text{tors}} \to A(\mathbb{F}_\mathfrak{p})$ is injective. The GCD of $\#A(\mathbb{F}_\mathfrak{p})$, as $\mathfrak{p}$ ranges over such primes, gives a naive upper bound on $A(K)_{\text{tors}}$. For rational torsion on modular Jacobians, one can quickly compute $\#A(\mathbb{F}_p)$ via the coefficients of the corresponding modular forms, which `Magma` has packaged into the intrinsic `TorsionMultiple`.

Comparing orders is usually insufficient (e.g., if $A(\mathbb{Q})_{\text{tors}}$ is cyclic and $A(\mathbb{F}_p)$ is non cyclic, the output of `TorsionMultiple` is usually larger than $\#A(\mathbb{Q})_{\text{tors}}$; see Example 4.2). To improve these bounds, we compute the "GCD" of the groups $A(\mathbb{F}_p)$ for various p; more precisely, given abelian groups $A_1, \ldots, A_n$, we define the $\mathrm{GCD}(A_1, \ldots, A_n)$ to be the largest abelian group A such that each A_i contains a subgroup isomorphic to A.

Example 4.2 (torsion on $J_1(21)$). To demonstrate this, we consider the rational torsion on $A = J_1(21)$, which is a 5-dimensional modular abelian variety. The output of the intrinsic `TorsionMultiple(JOne(21))` yields a bound of 728, but $A(\mathbb{F}_5)$ has invariants [2184] and $A(\mathbb{F}_{11})$ has invariants [14, 6916], and these groups have GCD [364]. We computed $A(\mathbb{F}_p)$ by reducing a model for $X_1(21)$ modulo p and using `Magma`'s `ClassGroup` intrinsic; see the `Magma` file `master-21.m`.

4.3. ***Better local bounds on torsion via Eichler–Shimura and modular symbols.*** The naive approach above does not incorporate the action of complex conjugation, and slows quickly as the genus grows. We describe here a substantial improvement, derived from the Eichler–Shimura relation. For an intermediate modular curve $X_H(N)$, let $J_H(N)$ denote its Jacobian.

For a prime $q \nmid 2N$, let T_q be the q-th Hecke operator. By the Eichler–Shimura relation, the kernel of the operator

$$T_q - q\langle q \rangle - 1 : J_H(N)(\overline{\mathbb{Q}})_{\text{tors}} \to J_H(N)(\overline{\mathbb{Q}})_{\text{tors}}$$

contains the prime to q torsion in $J_H(N)(\mathbb{Q})$ (cf. [Derickx et al. 2017, Proposition 5.2; Diamond and Im 1995, p. 87)]. Additionally, let

$$\tau : J_H(N)(\overline{\mathbb{Q}}) \to J_H(N)(\overline{\mathbb{Q}})$$

be complex conjugation. Then it is clear that $\tau - 1$ vanishes on $J_H(N)(\mathbb{Q})$, and thus also vanishes on $J_H(N)(\mathbb{Q})_{\text{tors}}$.

Thus, for a finite set of primes $q_1, \dots, q_n$ (still coprime to $2N$) with $n \geq 2$,

$$M_H := J_H(N)(\overline{\mathbb{Q}})_{\mathrm{tors}}[T_{q_1} - q_1\langle q_1\rangle - 1, \dots, T_{q_n} - q_n\langle q_n\rangle - 1, \tau - 1] \tag{4.3.1}$$

contains $J_H(N)(\mathbb{Q})_{\mathrm{tors}}$. We can efficiently compute M_H as follows. Under the uniformization

$$J_H(N)(\mathbb{C}) \cong H_1(X_H(N)(\mathbb{C}), \mathbb{C})/H_1(X_H(N)(\mathbb{C}), \mathbb{Z})$$

we can identify the geometric torsion as

$$J_H(N)(\overline{\mathbb{Q}})_{\mathrm{tors}} \cong H_1(X_H(N)(\mathbb{C}), \mathbb{Q})/H_1(X_H(N)(\mathbb{C}), \mathbb{Z}).$$

While it does not make sense to ask this identification to be Galois equivariant, it does commute with the Hecke and diamond operators, and with complex conjugation. The right-hand side lends itself very well to explicit computations with `Sage` using modular symbols (and is very fast, since the computations are now essentially linear algebra). This is implemented in the module `CuspidalClassgroup` from [Derickx 2017], and is also available in our accompanying code (see Section 1.9).

We will call this upper bound on rational torsion we get from computing M_H the *Hecke bound*.

To demonstrate how the Hecke bound produces better bounds than the local bounds from Section 4.1, we will consider the following two examples.

Example 4.4 (torsion on $J_1(28)$). Consider the rational torsion on $A = J_1(28)$, which is a 10-dimensional modular abelian variety. The intrinsic `TorsionMultiple(JOne(28))` produces a bound of 359424. We compute that $A(\mathbb{F}_3)$ has invariants $[4, 4, 24, 936]$ and $A(\mathbb{F}_5)$ has invariants $[2, 2, 8, 8, 312, 936]$, which have GCD $[4, 4, 24, 936]$. The Hecke bound give an upper bound of $[2, 4, 12, 936]$, which improves upon the GCD bound; see the `Sage` file `torsionComputations.py`.

Example 4.5 (torsion on $J_1(2, 18)$). Consider the rational torsion on $A = J_1(2, 18)$, which is a 7-dimensional modular abelian variety. We compute that $A(\mathbb{F}_5)$ has invariants $[6, 84, 252]$ and $A(\mathbb{F}_7)$ has invariants $[3, 6, 6, 126, 126]$, which have GCD $[6, 42, 126]$. The Hecke bound give an upper bound of $[2, 42, 126]$, which improves upon the GCD bound; see the `Sage` file `torsionComputations.py`.

4.6. ***Cuspidal torsion and a generalized Conrad–Edixhoven–Stein conjecture.*** By the Manin–Drinfeld theorem [Manin 1972; Drinfeld 1973], cuspidal divisors are torsion; conversely, it is expected that $J(\mathbb{Q})_{\mathrm{tors}}$ is cuspidal for a modular Jacobian J. More precisely, we conjecture that the torsion on $J_1(N)(\mathbb{Q})$ is generated by the $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-orbits of cusps (see Conjecture 4.15).

This is a conjecture of Conrad, Edixhoven and Stein [Conrad et al. 2003, Conjecture 6.2.2] for the modular Jacobian $J_1(p)$ where p is a prime. The authors proved this conjecture for all primes $p \leq 157$ except for $p = 29, 97, 101, 109$, and 113, and the case of $p = 29$ was proved in [Derickx et al. 2017, Theorem 6.4]. Moreover, their conjecture is true for all primes p such that $J_1(p)(\mathbb{Q})$ has rank 0. For composite N, the torsion subgroup of $J_1(N)$ generated by $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-orbits of cusps has been studied, and in some special cases, the Conrad–Edixhoven–Stein conjecture has been proved; see [Yu 1980; Takagi 1992; 1995; 2008; 2012; 2014; Hazama 1998; Csirik 2002; Yang 2009; Yang and Yu 2010; Sun 2010; Chen 2011; Ohta 2013].

In this subsection, we will use the construction of M_H from equation (4.3.1) and the results from Section 2.9 to determine when the rational torsion on certain modular Jacobians is cuspidal. First, we need to establish some definitions.

Definition 4.7. We define the following subgroups of $\operatorname{Div} X_H(N)$.

- Let $\operatorname{Div}^{\mathrm{c}} X_H(N)$ denote the free abelian group generated by the cusps of $X_{H_{\overline{\mathbb{Q}}}}$.
- Let $\operatorname{Div}^{\mathrm{c}}_{\mathbb{Q}} X_H(N) := \operatorname{Div}^{\mathrm{c}} X_H(N) \cap \operatorname{Div}_{\mathbb{Q}} X_H(N)$ denote the subgroup generated by the $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-orbits of cusps.

Definition 4.8. We define the following quotients of the divisor groups from Definition 4.7.

- Let $\operatorname{prin}^{\mathrm{c}} X_H(N)$ denote the principal divisors in $\operatorname{Div}^{0,\mathrm{c}} X_H(N)$, and let
$$\operatorname{Cl}^{\mathrm{c}} X_H(N) := \operatorname{Div}^{0,\mathrm{c}} X_H(N)/\operatorname{prin}^{\mathrm{c}} X_H(N)$$
denote the quotient.
- Let $\operatorname{prin}^{\mathrm{c}}_{\mathbb{Q}} X_H(N)$ denote the principal divisors in $\operatorname{Div}^{0,\mathrm{c}}_{\mathbb{Q}} X_H(N)$, and let
$$\operatorname{Cl}^{\mathrm{c}}_{\mathbb{Q}} X_H(N) := \operatorname{Div}^{0,\mathrm{c}}_{\mathbb{Q}} X_H(N)/\operatorname{prin}^{\mathrm{c}} X_H(N)$$
denote the quotient.

With these definitions it is clear that determining if the rational torsion on the modular Jacobian J_H is cuspidal boils down to whether $\operatorname{Cl}^{\mathrm{c}}_{\mathbb{Q}} X_H(N) = J_H(\mathbb{Q})_{\mathrm{tors}}$.

Section 4.3 gave an inclusion $J_H(\mathbb{Q})_{\mathrm{tors}} \subset M_H$ (the "Hecke bound"). In order to get lower bounds, we need to compute $\operatorname{Cl}^{\mathrm{c}}_{\mathbb{Q}} X_H(N)$, which we now describe. Let $G := \operatorname{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^\times$ be the Galois group of the cyclotomic field obtained by adjoining an N-th root of unity to $\mathbb{Q}$. To determine the group $\operatorname{Cl}^{\mathrm{c}}_{\mathbb{Q}} X_H(N)$, we first use results and code from [Derickx and van Hoeij 2014] and actions of diamond operators to compute $\operatorname{Cl}^{\mathrm{c}} X_H(N)$, and from here we take G-invariants as $\operatorname{Div}^{0,\mathrm{c}}_{\mathbb{Q}} X_H(N) = (\operatorname{Div}^{0,\mathrm{c}} X_H(N))^G$. An implementation to compute $\operatorname{Cl}^{\mathrm{c}}_{\mathbb{Q}} X_1(N)$ is available at [van Hoeij 2013], explained in [van Hoeij and Smith 2021], and a `Sage` version extending this to $\operatorname{Cl}^{\mathrm{c}}_{\mathbb{Q}} X_H(N)$ can be found in the module `MiscellaneousFunctions` from [Derickx 2017]. We illustrate the utility of this code in the following examples.

Example 4.9 (torsion on $J_1(28)$). The code finds $\operatorname{Cl}^{\mathrm{c}}_{\mathbb{Q}} X_1(28) \cong [2, 4, 12, 936]$. Combining this with the Hecke bound from Example 4.4 gives $\operatorname{Cl}^{\mathrm{c}}_{\mathbb{Q}} X_1(28) = J_1(28)(\mathbb{Q})_{\mathrm{tors}}$, and in particular, all of the rational torsion on $J_1(28)$ is cuspidal; see the `Sage` file `torsionComputations.py`.

Example 4.10 (torsion on $J_1(2, 18)$). The code finds $\operatorname{Cl}^{\mathrm{c}}_{\mathbb{Q}} X_1(2, 18) \cong [2, 42, 126]$. Combining this with the Hecke bound from Example 4.5 gives $\operatorname{Cl}^{\mathrm{c}}_{\mathbb{Q}} X_1(2, 18) = J_1(2, 18)(\mathbb{Q})_{\mathrm{tors}}$, and in particular, all of the rational torsion on $J_1(2, 18)$ is cuspidal; see the `Sage` file `torsionComputations.py`.

To study the question of whether the rational torsion on the modular Jacobian is cuspidal in more generality, we proceed as follows. Since $(\mathrm{Cl}^{\mathrm{c}} X_H(N))^G \subset J_H(\mathbb{Q})$, it is necessary that the map

$$\mathrm{Div}^{0,\mathrm{c}}_{\mathbb{Q}} X_H(N) = (\mathrm{Div}^{0,\mathrm{c}} X_H(N))^G \to (\mathrm{Cl}^{\mathrm{c}} X_H(N))^G$$

is surjective in order for the rational torsion to be cuspidal.

For the remainder of this section, we will focus our attention on determining the rational torsion on modular curves $X_1(N)$ and $X_1(2, 2N)$ with modular Jacobians $J_1(N)$ and $J_1(2, 2N)$, respectively. As a first step, we show that for $N \leq 55$, the above map on divisors is surjective.

Proposition 4.11. *Let $N \leq 55$ be an integer. Then $\mathrm{Cl}^{\mathrm{c}}_{\mathbb{Q}} X_1(N) = (\mathrm{Cl}^{\mathrm{c}} X_1(N))^G$.*

Proof. We verify the result by computing the maps

$$(\mathrm{Div}^{0,\mathrm{c}} X_1(N))^G \to (\mathrm{Cl}^{\mathrm{c}} X_1(N))^G$$

in terms of modular symbols and the computation showed it was surjective in all cases. □

For code verifying these claims as well as those in Theorem 4.13, Corollary 4.14, and Proposition 4.16 see the `Sage` file `torsionComputations.py`.

For the main theorem in this section, we will also need the following lemma.

Lemma 4.12. *Let R be a commutative ring M be an R-module whose cardinality is finite and C, M', T be R-submodules of M such that $C \subseteq M'$, $C \subseteq T$ and $M' \cap T = C$. Assume that for all maximal ideals m of R one has $(M/C)[m] = (M'/C)[m]$, then $T = C$.*

Proof. By taking the quotient by C, one may assume that $C = 0$. Since T is of finite cardinality, it is isomorphic to $\otimes_{i=1}^{k} T[m_i^{\infty}]$ for some finite sequence of maximal ideals $m_1, \ldots, m_k$. Let $m = m_i$ be one of these maximal ideals. Due to the equalities $M[m] = M'[m]$ and $M' \cap T = 0$, one gets $T[m] = M[m] \cap T = M'[m] \cap T = 0$, and thence $T[m^{\infty}] = 0$. Since this holds for all m_i, $T = 0$. □

Theorem 4.13. *Let $N \leq 55$, $N \neq 54$ be an integer. Then*

$$\mathrm{Cl}^{\mathrm{c}}_{\mathbb{Q}} X_1(N) = J_1(N)(\mathbb{Q})_{\mathrm{tors}}$$

If $N = 54$, then the index of $\mathrm{Cl}^{\mathrm{c}}_{\mathbb{Q}} X_1(N)$ in $J_1(N)(\mathbb{Q})_{\mathrm{tors}}$ is a divisor of 3.

Proof. This was verified using a `Sage` computation, which we now describe. We compute the M from equation (4.3.1) for the modular Jacobians $J_1(N)$ for $N \leq 55$. For $N \neq 24, 32, 33, 40, 48, 54$, our computation shows that $M \subseteq \mathrm{Cl}^{\mathrm{c}} X_1(N)$ holds and hence

$$(\mathrm{Cl}^{\mathrm{c}} X_1(N))^G \subseteq J_1(N)(\mathbb{Q})_{\mathrm{tors}} \subseteq M^G \subseteq (\mathrm{Cl}^{\mathrm{c}} X_1(N))^G.$$

Therefore, the result follows from Proposition 4.11 except for the cases of $N = 24, 24, 32, 33, 40, 48, 54$. For these cases, define $M' = M \cap \mathrm{Cl}^{\mathrm{c}} X_1(N)$. The `Sage` computation then shows that for all primes p that divide $\#M$, we have $(M/\mathrm{Cl}^{\mathrm{c}}_{\mathbb{Q}} X_1(N))[p] = (M'/\mathrm{Cl}^{\mathrm{c}}_{\mathbb{Q}} X_1(N))[p]$ holds for all the above N except for 54. The theorem follows by applying Lemma 4.12 with $C = \mathrm{Cl}^{\mathrm{c}}_{\mathbb{Q}} X_1(N)$ and $T = J_1(N)(\mathbb{Q})_{\mathrm{tors}}$.

For the $N = 54$, we computed the index $i := [M + \mathrm{Cl}^{\mathrm{c}}\, X_1(N) : \mathrm{Cl}^{\mathrm{c}}\, X_1(N)]$; taking $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-invariants of the sequence

$$0 \to \mathrm{Cl}^{\mathrm{c}}\, X_1(N) \to M + \mathrm{Cl}^{\mathrm{c}}\, X_1(N) \to (M + \mathrm{Cl}^{\mathrm{c}}\, X_1(N))/\,\mathrm{Cl}^{\mathrm{c}}\, X_1(N) \to 0$$

shows that $[(M + \mathrm{Cl}^{\mathrm{c}}\, X_1(N))^{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})} : (\mathrm{Cl}^{\mathrm{c}}\, X_1(N))^{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})}]$ divides 3. Since

$$J_1(\mathbb{Q})_{\mathrm{tors}} = (M + \mathrm{Cl}^{\mathrm{c}}\, X_1(N))^{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})} \quad \text{and} \quad \mathrm{Cl}^{\mathrm{c}}\, X_1(N)^{\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})} = \mathrm{Cl}^{\mathrm{c}}_{\mathbb{Q}}\, X_1(N),$$

we use this index to get the multiplicative upper bound of 3 mentioned in the second statement. □

The only $N \leq 55$ such that $J_1(N)$ has positive rank are 37, 43 and 53 so as a corollary we immediately get that:

Corollary 4.14. *Let $N \leq 55$ be an integer. If $N \neq 37, 43, 53,$ or $54,$ then*

$$\mathrm{Cl}^{\mathrm{c}}_{\mathbb{Q}}\, X_1(N) = J_1(N)(\mathbb{Q}).$$

Based on the results of Theorem 4.13, we make the following conjecture, which is a generalization of [Conrad et al. 2003, Conjecture 6.2.2].

Conjecture 4.15. For any integer N, we have that

$$\mathrm{Cl}^{\mathrm{c}}_{\mathbb{Q}}\, X_1(N) = J_1(N)(\mathbb{Q})_{\mathrm{tors}}.$$

Using the same proof as in Theorem 4.13, we can prove the following.

Proposition 4.16. *Let $N \leq 16$ be an integer. Then*

$$\mathrm{Cl}^{\mathrm{c}}_{\mathbb{Q}}\, X_1(2, 2N) = J_1(2, 2N)(\mathbb{Q})_{\mathrm{tors}}.$$

Again see the `Sage` file `torsionComputations.py`.

4.17. ***Local to global failures.*** For $J_0(N)$, the local methods described above often give only an upper bound instead of the true torsion. With enough work one can sometimes fix this; see Example 4.18 below. For another compelling example see [Ozman and Siksek 2019, Subsection 5.5] — the curve $X_0(45)$ is a plane quartic, and they use the explicit description of $J_0(45)(\overline{\mathbb{Q}})[2]$ via bitangents to bridge the discrepancy between their local bounds and the true torsion.

Example 4.18 (torsion on $J_0(30)$). Consider the rational torsion on $A = J_0(30)$, which is a 3-dimensional modular abelian variety. The rational cuspidal divisors generate a subgroup with invariants $[2, 4, 24]$. Locally, $A(\mathbb{F}_7)$ has invariants $[2, 2, 4, 48]$ and $A(\mathbb{F}_{23})$ has invariants $[2, 12, 24, 24]$; these groups have GCD $[2, 2, 4, 24]$. The Hecke bound and the additional argument from Theorem 4.13 do not improve this.

N	$\mathrm{Cl}^{\mathrm{c}}_{\mathbb{Q}}\, X_1(N)$	N	$\mathrm{Cl}^{\mathrm{c}}_{\mathbb{Q}}\, X_1(N)$	N	$\mathrm{Cl}^{\mathrm{c}}_{\mathbb{Q}}\, X_1(N)$
11	[5]	27	[3,3,52497]	42	[182,1092,131040]
13	[19]	28	[2,4,12,936]	43	[2,1563552532984879906]
14	[6]	29	[4,4,64427244]	44	[4,620,3100,6575100]
15	[4]	30	[4,8160]	45	[3,9,36,16592750496]
16	[2,10]	31	[10,1772833370]	46	[408991,546949390174]
17	[584]	32	[2,2,2,4,120,11640]	47	[3279937688802933030787]
18	[21]	33	[5,42373650]	48	[2,2,2,2,4,40,40,240,1436640]
19	[4383]	34	[8760,595680]	49	[7,52367710906884085342]
20	[60]	35	[13,109148520]	50	[5,1137775,47721696825]
21	[364]	36	[12,252,7812]	51	[8,1168,7211322610146240]
22	[5,775]	37	[160516686697605]	52	[4,28,532,7980,17470957140]
23	[408991]	38	[9,4383,33595695]	53	[18242730287918375982989 1277]
24	[2,2,120]	39	[7,31122,3236688]	54′	[3,3,3,9,9,1102437,1529080119]
25	[227555]	40	[2,2,2,8,120,895440]	55	[5,550,89723967399178860 00]
26	[133,1995]	41	[107768799408099440]		

Table 2. Cuspidal torsion in $J_1(N)(\mathbb{Q})$ for $N = 11$ and $13 \leq N \leq 55$ (all torsion if $N \neq 54$).

The curve $X_0(30)$ is hyperelliptic and admits the model $y^2 = f(x)$, where

$$f(x) = (x^2 + 3x + 1) \cdot (x^2 + 6x + 4) \cdot (x^4 + 5x^3 + 11x^2 + 10x + 4),$$

and we can exploit the explicit description of the 2-torsion of the Jacobian of a hyperelliptic curve. The geometric 2-torsion $J_0(30)(\overline{\mathbb{Q}})[2]$ is Galois-equivariantly in bijection with even order subsets of the set of Weierstrass points modulo the subset of all Weierstrass points (see, e.g., [Gross 2012, Section 6]), and one can compute the rational torsion by taking Galois invariants. See the file `functions.m` for a short routine `twoTorsionRank` which computes $J(\mathbb{Q})[2]$ for the Jacobian of a hyperelliptic curve. Using this routine, we find that $\mathrm{rank}_{\mathbb{F}_2} J_0(30)(\mathbb{Q})[2] = 3$, and hence the rational torsion on $J_0(30)$ is cuspidal and isomorphic to $[2, 4, 24]$.

Note that if J is the Jacobian of a hyperelliptic curve defined by an odd degree polynomial $f(x)$, $\mathrm{rank}_{\mathbb{F}_2} J(\mathbb{Q})[2] = i$, where $i + 1$ is the number of factors $f(x)$; this is no longer true in general, as $J_0(30)$ demonstrates.

See the `Magma` file `master-30.m` for more details.

4.19. ***Tables of cuspidal torsion subgroups for $J_1(N)$ and $J_1(2, 2N)$.*** We conclude this section by giving the structure of $\mathrm{Cl}^{\mathrm{c}}_{\mathbb{Q}}\, X_1(N)$ for $10 \leq N \leq 55$ and of $\mathrm{Cl}^{\mathrm{c}}_{\mathbb{Q}}\, X_1(2, 2N)$ for $5 \leq N \leq 16$ in terms of its invariant factor decomposition in Tables 2 and 3. For code, see the `Sage` file `torsionComputations.py`.

$(2, 2N)$	$\mathrm{Cl}^{\mathrm{c}}_{\mathbb{Q}}\, X_1(2, 2N)$	$(2, 2N)$	$\mathrm{Cl}^{\mathrm{c}}_{\mathbb{Q}}\, X_1(2, 2N)$	$(2, 2N)$	$\mathrm{Cl}^{\mathrm{c}}_{\mathbb{Q}}\, X_1(2, 2N)$
(2, 10)	[6]	(2, 18)	[2,42,126]	(2, 26)	[2,14,266,3990,11970]
(2, 12)	[4]	(2, 20)	[4,60,120]	(2, 28)	[2,4,4,4,8,24,936,936]
(2, 14)	[2,2,6,18]	(2, 22)	[2,10,1550,4650]	(2, 30)	[2,2,2,2,2,24,8160,8160]
(2, 16)	[2,20,20]	(2, 24)	[2,4,4,120,240]	(2, 32)	[2,2,2,4,4,24,120,23280,23280]

Table 3. (Cuspidal) torsion on $J_1(2, 2N)(\mathbb{Q})$ for $5 \le N \le 16$.

Remark 4.20. Yang [2009] determined the cuspidal torsion on $J_1(N)$ generated by ∞-cusps (cf. [Derickx et al. 2017, Definition 5.4]). By comparing his results with Table 2, we can find N for which one needs non-∞ cusps and/or nonrational cusps to generate the torsion on $J_1(N)(\mathbb{Q})$. For example, by [Yang 2009, Table 1], the ∞-cusps on $X_1(20)$ generate a subgroup isomorphic to [20], but by Theorem 4.13 and Table 2, we see that $J_1(20)(\mathbb{Q})$ is cuspidal and isomorphic to [60]; in particular, the ∞-cusps do not generate all of the rational torsion on $J_1(20)$. A similar situation occurs for $X_1(21)$, which we discuss in Section 6.2.

5. Methods for determining cubic points on curves

In this section, we describe the variety of methods we utilize to determine the cubic points on the modular curves $X_1(N)$.

5.1. ***Local methods.*** In some cases, we can deduce that there are no noncuspidal cubic points on $X_1(N)$ simply by determining points on $X_1(N)(\mathbb{F}_{p^i})$ for $i = 1, 2$, and 3 for some prime $p \nmid 2N$.

Suppose that X is a curve of gonality at least 4 and at least one rational point, and that its Jacobian J_X satisfies $\mathrm{rank}\, J(\mathbb{Q}) = 0$. Fix a point $\infty \in X(\mathbb{Q})$. Since X has gonality at least 4, the Abel–Jacobi maps

$$f_{i,i\infty} : X^{(i)} \hookrightarrow J_X, \quad D \mapsto D - i\infty$$

are injective for $i = 1, 2, 3$. Moreover, since the rank of $J_X(\mathbb{Q})$ is zero, the reduction map $J_X(\mathbb{Q}) \hookrightarrow J_X(\mathbb{F}_p)$ is injective for $p > 2$ (see Section 4.1). We thus get a commutative diagram

$$\begin{array}{ccc} X^{(i)}(\mathbb{Q}) & \hookrightarrow & J_X(\mathbb{Q}) \\ \downarrow & & \downarrow \\ X^{(i)}(\mathbb{F}_p) & \hookrightarrow & J_X(\mathbb{F}_p) \end{array}$$

of injections. In particular, the reduction maps $X^{(i)}(\mathbb{Q}) \hookrightarrow X^{(i)}(\mathbb{F}_p)$ are injective for $i = 1, 2, 3$; if there is a prime p such that these maps are also surjective, then we have determined $X^{(i)}(\mathbb{Q})$. One can verify surjectivity by checking cardinalities, i.e., checking if

$$\#X^{(i)}(\mathbb{Q}) \ge \#X^{(i)}(\mathbb{F}_p).$$

In practice, $\#X^{(i)}(\mathbb{F}_p)$ can be determined very quickly in `Magma` (even using a singular model, by working with places instead of points), and we often a priori have a lower bound on $\#X^{(i)}(\mathbb{Q})$ coming from an explicit description of cusps (e.g., Lemma 2.8).

See Section 6.1 for examples.

5.2. ***Direct analysis of preimages of an Abel–Jacobi map.*** When $X_1(N)$ has gonality at least 4 and $J_1(N)(\mathbb{Q})$ has rank 0, one is able to compute the finitely many preimages of an Abel–Jacobi map $\iota : X_1(N)^{(3)}(\mathbb{Q}) \to J_1(N)(\mathbb{Q})$. For values of N such that the genus of $X_1(N)$ and the size of $J_1(N)(\mathbb{Q})$ is not too large, it is possible to do this directly over $\mathbb{Q}$: fixing a base point $\infty \in X_1(N)(\mathbb{Q})$, a divisor $D \in J_1(N)(\mathbb{Q})$ is in the image of the Abel–Jacobi map $E \mapsto E - 3\infty$ if and only if the linear system $|D + 3\infty| \neq \varnothing$. One can compute $|D + 3\infty|$ via `Magma`'s `RiemannRoch` intrinsic. If $|D + 3\infty| = \varnothing$ then we disregard it; otherwise it will contain a single effective divisor E of degree 3. Thus as D ranges over $J_1(N)(\mathbb{Q})$, we eventually compute all of the effective degree 3 divisors (and hence the image of Abel–Jacobi). We will refer to this as *direct analysis over* $\mathbb{Q}$.

Direct analysis over $\mathbb{Q}$ can be very slow (cf. Remark 6.3). A much faster method from [van Hoeij 2014, Footnote 1] works as follows. The diagram from Section 5.1

$$\begin{array}{ccc} X^{(3)}(\mathbb{Q}) & \xhookrightarrow{\iota} & J_X(\mathbb{Q}) \\ \downarrow{\scriptstyle \mathrm{red}_X} & & \downarrow{\scriptstyle \mathrm{red}_J} \\ X^{(3)}(\mathbb{F}_p) & \xhookrightarrow{\iota_p} & J_X(\mathbb{F}_p) \end{array}$$

commutes, so the image of ι_p contains the reduction of the image of ι. It thus suffices to

(1) compute the image of ι_p (which is generally very fast),

(2) compute the preimage of $\operatorname{im} \iota_p$ under red_J (also fast), and

(3) compute which elements of $\mathrm{red}_J^{-1}(\operatorname{im} \iota_p)$ are in the image of ι.

We will refer to this approach as *direct analysis over* $\mathbb{F}_p$. The set $\mathrm{red}_J^{-1}(\operatorname{im} \iota_p)$ of divisors which are "locally in the image of Abel–Jacobi" is generally much smaller than $J_X(\mathbb{Q})$, so step (3) is much faster. (Equivalently, since each map is injective, one can compute the intersection $(\operatorname{im} \mathrm{red}_J) \cap (\operatorname{im} \iota_p)$.) One could further speed up the computation by repeating this procedure at several primes; see the Mordell–Weil sieve [Ozman and Siksek 2019, Section 6]. Implementing this was unnecessary for our results.

See Sections 6.2 and 6.5 for examples.

5.3. ***Direct analysis on nontrigonal curve quotients.*** While direct analysis works in principle, we encounter many values of N where the genus of $X_1(N)$ and the size of $J_1(N)$ are large (for example, $g(X_1(45)) = 41$ and $16128153482112 \mid \#J_1(45)(\mathbb{Q})$), and hence working directly with $X_1(N)^{(3)}(\mathbb{Q})$ and $J_1(N)(\mathbb{Q})$ is hard. Instead, we consider a morphism $X_1(N) \to X$ where X is nontrigonal and perform the direct analysis on X. For details on how to find a model for X, see Remark 2.6.

Remark 5.4 (cubic points on hyperelliptic curves). A curve X of genus $g \leq 2$ is trigonal as it admits a base-point free g^1_3 by Riemann–Roch, and a nonhyperelliptic curve of genus $g = 3$ or 4 is trigonal. However, a hyperelliptic curve of $g \geq 3$ is not trigonal, and thus has finitely many cubic points. In this case, $X^{(3)}(\mathbb{Q})$ is still infinite; it contains the image of $X(\mathbb{Q}) \times X^{(2)}(\mathbb{Q})$ (i.e., divisors of the form $P + Q + Q^\iota$, where $P \in X(\mathbb{Q})$ and where ι is the hyperelliptic involution), and the complement of this subset contains the finitely many cubic points. Therefore, when we search for nontrigonal curve quotients, we either need a genus $g \geq 3$ hyperelliptic curve or certain nonhyperelliptic curves of $g \geq 5$.

In the hyperelliptic case, we need to know that the image of a cubic point does not reduce to a noncuspidal rational point plus another divisor. We encounter four genus 3 hyperelliptic cases, namely $X_0(N)$ for $N = 30$, 33, 35, and 39. By [Kenku 1982, Theorem 1], we know that the rational points on the curves $X_0(N)$ for these N are all cuspidal.

See Section 6.4 for examples.

5.5. ***Formal immersion criteria.*** When the rank of $J_1(N)(\mathbb{Q})$ is positive, we apply formal immersion criteria of [Derickx et al. 2017] to determine all of the points on $X_1(N)^{(3)}(\mathbb{Q})$. The underlying ideas of using formal immersion in the study of rational and higher degree points on modular curves comes from the foundational works [Mazur 1978; Kamienny 1992b].

To begin, we define formal immersions. Throughout this subsection, let R be a discrete valuation ring with perfect residue field κ and fraction field K.

Definition 5.6. Let $\phi : X \to Y$ be a morphism of Noetherian schemes and $x \in X$ a point and $y = f(x) \in Y$. Then ϕ is a *formal immersion at* x if the induced morphism of complete local rings $\widehat{\phi^*} : \widehat{\mathcal{O}_{Y,y}} \to \widehat{\mathcal{O}_{X,x}}$ is surjective.

The main reason we consider formal immersions is the following lemma.

Lemma 5.7 [Derickx et al. 2017, Lemma 2.2]. *Let X, Y be Noetherian schemes. Let R be a Noetherian local ring with maximal ideal $\mathfrak{m}$ and residue field $\kappa = R/\mathfrak{m}$. Suppose that $f : X \to Y$ is a formal immersion at a point $x \in X(\kappa)$ and suppose that $P, Q \in X(R)$ are two points such that $x = P_\kappa = Q_\kappa$ and $f(P) = f(Q)$. Then $P = Q$.*

To verify that a morphism is a formal immersion at a point, we will use the following criterion.

Proposition 5.8 [Derickx et al. 2017, Proposition 3.7]. *Let C be a smooth projective curve over R with geometrically connected generic fiber and Jacobian J. Let $y \in C^{(d)}(\kappa)$ be a point and write $y = \sum_{j=1}^{m} n_j y_j$ with $y_j \in C^{(d_j)}(\bar{\kappa})$ distinct and $m, n_1, \ldots, n_m \in \mathbb{N}$. Let $t : J \to A$ be a map of abelian schemes over R such that $t(J^1(R)) = \{0\}$, where $J^1(R)$ denotes the kernel of the reduction map $J(R) \to J(\kappa)$. Let q_j be a uniformizer at y_j, e be a positive integer and $\omega_1, \ldots, \omega_e \in t^*(\mathrm{Cot}_0 A_{\bar{\kappa}}) \subset \mathrm{Cot}_0(J_{\bar{\kappa}})$. For $1 \leq i \leq e$ and $1 \leq j \leq m$, let $a(\omega_i, q_j, n_j) := (a_1(\omega_i), \ldots, a_{n_j}(\omega_i))$ be the row vector of the first n_j coefficients of ω_i's q_j-expansion.*

Then $t \circ f_{d,y} : C_\kappa^{(d)} \to A_\kappa$ is a formal immersion at y if the matrix

$$A := \begin{pmatrix} a(\omega_1, q_1, n_1) & a(\omega_1, q_2, n_2) & \cdots & a(\omega_1, q_1, n_m) \\ a(\omega_2, q_1, n_1) & a(\omega_2, q_2, n_2) & \cdots & a(\omega_2, q_1, n_m) \\ \vdots & \vdots & \ddots & \vdots \\ a(\omega_e, q_1, n_1) & a(\omega_e, q_2, n_2) & \cdots & a(\omega_e, q_1, n_m) \end{pmatrix} \tag{5.8.1}$$

has rank d. If $\omega_1, \ldots, \omega_e$ generate $t^* \operatorname{Cot}_0(A_{\bar\kappa})$, then the previous statement is an equivalence.

To apply Proposition 5.8, we will take κ to have odd characteristic and A to be a rank 0 abelian variety; since torsion injects under reduction, the hypothesis $t(J^1(R)) = \{0\}$ is satisfied.

Our plan for $N = 65$ and 121 is as follows. We first show, either via a brute force search or using the Hasse bound, that a cubic point on $X_1(N)$ will reduce modulo some prime $p \nmid 2N$ to a degree 3 divisor which is supported on cusps. Then, we know that the reduction modulo p of a cubic point on $X_1(N)$ will map to a degree 3 cuspidal divisor on $X_0(N)$. Using `Magma`'s intrinsic `Decomposition(JZero(N))`, we find a rank zero quotient A of $J_0(N)$, and then we verify that the morphism $X_0(N)^{(3)} \to A$ is a formal immersion at these degree 3 divisors.

See Sections 7.1 and 7.3 for greater detail.

6. Cubic points on modular curves with rank 0 Jacobians

In this section, we determine the cubic points on the modular curves $X_1(N)$ from Remark 1.5 which have Jacobians $J_1(N)$ of rank 0.

For claims about gonality of $X_1(N)$, see [Derickx and van Hoeij 2014, Table 1], for claims about the number and degrees of cusps on $X_1(N)$ or $X_0(N)$, see Lemma 2.8, and for claims about the torsion on $J_1(N)(\mathbb{Q})$ and $J_1(2, 2N)(\mathbb{Q})$ see Corollary 4.14, Proposition 4.16, and Tables 2 and 3.

6.1. ***Local methods — the cases $X_1(22)$ and $X_1(25)$.*** The modular curve $X_1(22)$ is a genus 6 tetragonal curve with 10 rational cusps. Using `Magma`, we determine that modulo 3, $X_1(22)$ has 10 degree 1 places, 0 degree 2 places, and 0 degree 3 places. Since we found 10 rational points, we immediately conclude that $X_1(22)$ has no cubic points. An identical argument handles $X_1(25)$.

See the `Magma` files `master-22.m` and `master-25.m` for code verifying these claims.

6.2. ***Direct analysis over $\mathbb{Q}$ — the case of $X_1(21)$.*** The modular curve $X_1(21)$ has genus 5 and is tetragonal. We prove that the only $\mathbb{Q}$-rational points of $X_1(21)^{(3)}$ arise from combinations of the 6 rational cusps, the 2 quadratic cusps, and the 2 cubic points D_0 and D_0' corresponding to the elliptic curve $E/\mathbb{Q}$ with Cremona label `162b1`, which has a point of exact order 21 over $\mathbb{Q}(\zeta_9)^+$. We follow the method of Section 5.2.

From Example 4.2, we know that $J_1(21)(\mathbb{Q})$ is cyclic of order 364. Differences of the *rational* cusps only generate the subgroup of order 364/2, but $D := D_0 - 3\infty$ has order 364 (where ∞ is any rational cusp).

Let

$$f_{3,3\infty} : X_1(21)^{(3)}(\mathbb{Q}) \to J_1(21)(\mathbb{Q}), \quad E \mapsto E - 3\infty$$

be an Abel–Jacobi map. For each point $nD \in J_1(21)(\mathbb{Q})$, nD is in the image of $f_{3,3\infty}$ if and only if the linear system $|nD + 3\infty|$ is nonempty, and the `Magma` intrinsic `RiemannRochSpace` will check whether this is true. Moreover, since $X_1(21)$ is tetragonal, $\dim |nD + 3\infty| \leq 0$, so if it is nonempty, it follows that $|nD + 3\infty| = \{E\}$ for some effective divisor E of degree 3; in `Magma` one can easily compute E and its support. We find that nD is in the image of $f_{3,3\infty}$ if and only if

$$\begin{aligned} n \in \big\{&0, 1, 5, 8, 12, 14, 16, 22, 38, 40, 42, 58, 60, 64, 65, 67, 76, 84, 91, 92, 94, 101, 104, 111,\\ &118, 121, 123, 138, 145, 147, 167, 172, 183, 188, 190, 200, 201, 202, 204, 206, 214, 226, 228,\\ &230, 234, 241, 246, 248, 250, 252, 254, 268, 272, 274, 278, 280, 282, 284, 289, 291, 292, 294,\\ &297, 298, 306, 308, 315, 318, 326, 328, 332, 335, 338, 352, 360, 362\big\}; \end{aligned}$$

each of these correspond to combinations of known rational, quadratic, and cubic points, and in particular nD is the image of a cubic point (under $f_{3,3\infty}$) if and only if $n = 1, 183$.

See the `Magma` file `master-21.m` for code verifying these claims.

Remark 6.3. While direct analysis over $\mathbb{Q}$ works in this example, it took over a week to complete. In contrast, we quickly verify our results via a direct analysis over $\mathbb{F}_5$, which took around 8 seconds.

6.4. ***Direct analysis over $\mathbb{Q}$ on a nontrigonal curve quotient — the cases $X_1(N)$ for $N \in \{30, 33, 35, 39\}$.*** The curve $X_1(30)$ has genus 9 and is 6-gonal. While the genus is not prohibitively large, we instead work on the genus 3, hyperelliptic curve $X_0(30)$, which is not trigonal. Using the `Magma` intrinsic `SmallModularCurve(30)`, we have the affine equation

$$X_0(30) : y^2 + (-x^4 - x^3 - x^2)y = 3x^7 + 19x^6 + 60x^5 + 110x^4 + 121x^3 + 79x^2 + 28x + 4.$$

We note that the map $X_0(30)^{(3)} \to J_0(30)$ is not injective since $X_0(30)^{(2)}$ contains a rational curve (see Remark 5.4). However, the map is still injective on cubic points of $X_0(30)$, which suffices for our purposes.

In Example 4.18, we proved that $J_0(30)(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z}$, and so next we perform a direct analysis over $\mathbb{Q}$ and find 48 cubic points on $X_0(30)$, which are all necessarily noncuspidal by Lemma 2.8(2). To conclude, we compute the j-invariants of the cubic points and check to see if there is a 30-torsion point on a twist of the corresponding curve E. To check this, it suffices to show that for some prime p not dividing $30N_E\Delta$, where N_E is the conductor of the elliptic curve E and Δ the discriminant of the cubic number field where E is defined, and for all primes $\mathfrak{p}$ above p, E modulo $\mathfrak{p}$ and its twists do not have an $\mathbb{F}_\mathfrak{p}$-rational point of order 30. For each of the 48 cubic points, we verify this, which tells us that these cubic points on $X_0(30)$ do not lift to $X_1(30)$, and thus, there are no cubic points on $X_1(30)$. We use a similar combination of methods to handle $N = 33$, 35 and 39.

See the `Magma` files `master-30.m`, `master-33.m`, `master-35.m`, and `master-39.m` for code.

6.5. ***Hecke bounds and direct analysis over $\mathbb{F}_p$ — the cases $X_1(2,16)$, $X_1(24)$, and $X_1(2,18)$.*** The modular curve $X_1(2,16)$ has genus 5 and is tetragonal. Using the model from [Derickx and Sutherland 2017], we find 8 rational cusps and 2 quadratic cusps on $X_1(2,16)$. The local bound on the torsion is $[2,2,20,20]$, and the Hecke bound improves this to $[2,20,20]$. The cusps generate a subgroup isomorphic to $[2,20,20]$ and hence they generate all of the torsion on $J_1(2,16)(\mathbb{Q})$. We also know that these cusps give rise to 136 rational points on $X_1(2,16)^{(3)}$.

To conclude, we compute the intersection of the image of an Abel–Jacobi with our known subgroup modulo 3. This gives 136 cubic divisors, and so by Section 5.1, we have completely determined the rational points on $X_1(2,16)^{(3)}$. A very similar argument handles $X_1(24)$ and $X_1(2,18)$.

See the `Magma` files `master-2-16.m`, `master-24.m` and `master-2-18.m` as well as the `Sage` file `torsionComputations.py` for code verifying these claims.

6.6. ***Hecke bounds and direct analysis over $\mathbb{F}_3$ — the cases $X_1(28)$ and $X_1(26)$.*** The modular curve $X_1(28)$ has genus 10 and is 6-gonal. A direct analysis over $\mathbb{Q}$ takes too much time, and we have no suitable quotient curve.

We know that $J_1(28)(\mathbb{Q})$ is cuspidal, but we would like to find explicit generators for $J_1(28)(\mathbb{Q})$. Via the results on modular units in Section 2.9, we determine that the cuspidal divisors on $J_1(28)(\mathbb{Q})$ are generated by the principal divisors together with the cuspidal divisors of degree 1, 2, and 3 (i.e., we do not need cuspidal divisors of degree 6 to generate the torsion). Following Section 5.2, we perform direct analysis over $\mathbb{F}_3$ and determine that there is only one cubic point locally in the image of Abel–Jacobi, namely the known cubic cusp (strictly speaking: "*Galois orbit* of cubic cusps"). Therefore, we can conclude that the only cubic point on $X_1(28)$ is the known cubic cusp. A similar argument handles $X_1(26)$.

See the `Magma` files `master-28.m` and `master-26.m`, and the `Sage` file `torsionComputations.py` for code verifying these claims.

6.7. ***Hecke bounds and direct analysis over $\mathbb{Q}$ on a nontrigonal curve quotient — the case of $X_1(45)$.*** The curve $X_1(45)$ has genus 41, so we look for a quotient. It maps to $X_0(45)$, a nonhyperelliptic genus 3 curve, which is necessarily trigonal and thus has infinitely many cubic points. We work instead with the intermediate genus 5 nonhyperelliptic nontrigonal curve $X_H(45)$, where H is the subgroup

$$H = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in \Gamma_0(45) : a \text{ is a square modulo } 15 \right\}.$$

We use the algorithm from [Derickx et al. 2013] to compute an equation $P(x,y)=0$ for $X_H(45)$ as follows. (See also [Derickx and van Hoeij 2014, Example 1].) We construct modular units $x, y \in \mathbb{Q}(X_1(45))$ that are invariant under the diamond action $\langle 4 \rangle$, and compute a relation $P(x,y)=0$; we then check its genus to verify that x, y generate $\mathbb{Q}(X_H(45))$. We chose y to be the image of x under the diamond action $\langle 2 \rangle$ so that P is symmetric, allowing it to be written as $P(x,y) = Q(xy, x+y) = 0$ for some Q. Here

$$Q(u,v) = u^3 + (v^2+7v+7)u^2 + (2v+3)(v^2+5v+3)u + (v^2+3v)^2$$

is an equation for $X_0(45)$. As a check for correctness, we computed an alternative model of $X_H(45)$ using [Zywina 2020], and checked in `Magma` that they are isomorphic.

Next, we determine the cubic points on $X_H(45)$. Since $X_1(45)$ dominates $X_H(45)$, $J_H(45)(\mathbb{Q})$ has rank 0, and local computations tell us that $J_H(45)(\mathbb{Q})$ is isomorphic to a subgroup of

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/48\mathbb{Z}.$$

The Galois orbits of cusps generate a subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/48\mathbb{Z}$, and the Hecke bounds from Section 4.3 prove that this generates $J_H(45)(\mathbb{Q})$.

We fix a known rational point $\infty \in X_H(45)(\mathbb{Q})$. Via direct analysis over $\mathbb{Q}$, we determine that $f_{3,3\infty}(X_H(45)(\mathbb{Q})) = f_{3,3\infty}(X_H(45)(\mathbb{Q})) \cap J_H(45)(\mathbb{Q})$ and find that there are 8 noncuspidal cubic points on $X_H(45)$. Finally, we lift the cubic points back to $X_1(45)$ to verify that they do not come from degree 3 points on $X_1(45)$.

See the `Maple` files `FindModel-XH-45-input` and `Lift-XY-back-to-X1-45-input`, the `Magma` file `master-45.m` and the `Sage` file `torsionComputations.py` for code verifying these computations.

7. Cubic points on modular curves with positive rank Jacobians

In this section, we use the formal immersion criterion of Section 5.5 to determine the cubic points on modular curves $X_1(N)$ for $N = 65, 121$.

7.1. ***The case of $X_1(121)$.*** We will prove that the cubic points on $X_1(121)$ are cuspidal. Consider the morphism $\phi : X_1(121) \to X_0(121)$, and let $\phi^{(3)} : X_1(121)^{(3)} \to X_0(121)^{(3)}$. The algorithm for $X_0(N)$ from [Ozman and Siksek 2019] provides the canonical model of $X_0(121)$. This genus 6 curve is not trigonal by [Hasegawa and Shimura 1999, Theorem 3.3]. By Lemma 2.8(2), the cuspidal subscheme of $X_0(121)$ is isomorphic to the disjoint union of μ_1, μ_1, and $(\mu_{11})'$, where the prime notation refers to points of exact order 11, i.e., $X_0(121)$ has 12 cusps: 2 rational cusps $\{c_0, c_\infty\}$ and a Galois orbit of size 10 defined over $\mathbb{Q}(\zeta_{11})$.

To begin, we claim that for a cubic point x on $X_1(121)$, $\phi^{(3)}(x_{\mathbb{F}_5})$ is equal (as a divisor) to one of

$$3[c_{\infty,\mathbb{F}_5}], \quad 2[c_{\infty,\mathbb{F}_5}] + [c_{0,\mathbb{F}_5}], \quad [c_{\infty,\mathbb{F}_5}] + 2[c_{0,\mathbb{F}_5}], \quad \text{or} \quad 3[c_{0,\mathbb{F}_5}].$$

Indeed, by a brute force search, we see that there are no elliptic curves over $\mathbb{F}_{5^i}$ for $i = 1, 2, 3$ with a rational 121 torsion point, and so a cubic point on $X_1(121)$ has bad reduction at each prime above 5, i.e., it must reduce to a sum of cusps (considered as a degree 3 divisor). (The Hasse bound at the prime 5 unfortunately does not a priori exclude the existence of such an elliptic curve.) The image $\phi^{(3)}(x_{\mathbb{F}_5})$ is thus also a sum of cusps. The cuspidal subscheme of $X_0(121)$ further decomposes modulo 5: the prime 5 splits in $\mathbb{Q}(\zeta_{11})$ as 2 primes each with inertia degree 5, and so the component $(\mu_{11})'_{\mathbb{F}_5}$ splits as two copies of $\operatorname{Spec} \mathbb{F}_{5^5}$, i.e., the modulo 5 reduction of the Galois orbit of size 10 is defined over $\mathbb{F}_{5^5}$. Now, our claim follows since $c_{0,\mathbb{F}_5}$ and $c_{\infty,\mathbb{F}_5}$ are the only cusps defined over $\mathbb{F}_{5^2}$ or $\mathbb{F}_{5^3}$.

Using Magma's intrinsic `Decomposition(JZero(121))`, we find that

$$J_0(121) \sim_{\mathbb{Q}} E_1 \times E_2 \times E_3 \times E_4 \times X_0(11) \times X_1(11),$$

and we compute that $E_1(\mathbb{Q})$ has rank 1 and $X_0(11)(\mathbb{Q})$, $X_1(11)(\mathbb{Q})$, and $E_i(\mathbb{Q})$ have rank 0 for $i = 2, 3, 4$. Let $A := E_2 \times E_3 \times E_4 \times X_1(11)$. Let $C_1 := 3[c_\infty]$, $C_2 := 2[c_\infty] + [c_0]$, $C_3 := [c_\infty] + 2[c_0]$, and $C_4 := 3[c_0]$. Define for $i = 1, \ldots, 4$, the morphisms $\mu_i : X_0(121)^{(3)} \to J_0(121)$ given by $z \mapsto [z - C_i]$ and $t : J_0(121) \to A$, where the latter is projection. By our first claim, we know that $\phi^{(3)}(x_{\mathbb{F}_5})$ is equal to one of $C_{1,\mathbb{F}_5}$, $C_{2,\mathbb{F}_5}$, $C_{3,\mathbb{F}_5}$ or $C_{4,\mathbb{F}_5}$, and so for the appropriate i, the image of $(t \circ \mu_i)(\phi^{(3)}(x))$ belongs to the kernel of reduction $A(\mathbb{Q}) \to A(\mathbb{F}_5)$. However, since $A(\mathbb{Q})$ is torsion, the kernel of reduction is trivial [Katz 1981, Appendix], and so for each appropriate i, $(t \circ \mu_i)(\phi^{(3)}(x)) = 0$.

To conclude our analysis, we verify that the morphism

$$\tau \circ \mu_i : X_0(121)^{(3)} \to A$$

is a formal immersion at the point $C_{i,\mathbb{F}_5}$ using Proposition 5.8. Via Magma's intrinsic `Newform`, we can compute a basis for the 1-forms on A, and so to verify the formal immersion criterion, we need to check that certain 4×3 matrices (see (5.8.1)) have rank 3. We can compute the q-expansion at c_∞ in Magma, and since the Atkin–Lehner involution ω_{121} swaps c_0 and c_∞, we can also directly compute the q-expansion at c_0 in Magma. We then observe the four matrices (modulo 5) defined in Proposition 5.8 all have rank 3, and thus, $(t \circ \mu_i)$ is a formal immersion at the above points. Finally, by Lemma 5.7, $\phi^{(3)}(x)$ is equal to one of $3[c_\infty]$, $2[c_\infty] + [c_0]$, $[c_\infty] + 2[c_0]$, or $3[c_0]$, and therefore we can conclude that any cubic point on $X_1(121)$ must be cuspidal.

See the Magma file `master-121.m` for code verifying these claims.

Remark 7.2. The argument that $\phi^{(3)}(x_{\mathbb{F}_5})$ is a sum of reductions of rational cusps proceeded by brute force. Typically, one would work at a smaller prime (in this case, 3) and apply the Hasse bound as in Lemma 7.4 below. It turns out that $X_0(121)^{(3)} \to A$ is not a formal immersion modulo 3, forcing us to work at a larger prime.

7.3. ***The case of $X_1(65)$.*** We will prove that the cubic points on $X_1(65)$ must be cuspidal. Consider the morphism $\phi : X_1(65) \to X_0(65)$, and let $\phi^{(3)} : X_1(65)^{(3)} \to X_0(65)^{(3)}$. Using equations from [Ozman and Siksek 2019], we have a model for the genus 5 curve $X_0(65)$, which is not trigonal [Hasegawa and Shimura 1999, Theorem 3.3]. By Lemma 2.8(2), we have that $X_0(65)$ has 4 cusps, c_0, c_∞, $c_{1/5}$, and $c_{1/13}$, all of which are rational.

Unlike the case of $N = 121$, the map $X_0(65)^{(3)} \to J_e(65)$ to the winding quotient is *not* a formal immersion at all cuspidal divisors. Fortunately, the following lemma tells us that we only need to verify the formal immersion criterion at particular sums of cusps on $X_0(65)$.

Lemma 7.4. *Let $\phi^{(3)} : X_1(65)^{(3)} \to X_0(65)^{(3)}$, and let x be a cubic point on $X_1(65)$. Then, $\phi^{(3)}(x_{\mathbb{F}_3})$ is equal to $3[c_{\mathbb{F}_3}]$ for some rational cusp $c \in X_0(65)(\mathbb{Q})$.*

Proof. First, we claim that $x_{\mathbb{F}_3}$ must be supported on a sum of cusps using the following Hasse bound computation.

If E is an elliptic curve over a cubic field K and $\mathfrak{p}$ is a prime of K over a rational prime p, then, if its reduction modulo $\mathfrak{p}$ is smooth, it has (by the Hasse bound) at most

$$\#E(\mathbb{F}_q) \leq 2\sqrt{q} + (q+1)$$

points, where $q \leq p^3$. In our setting of $N = 65$, the Hasse bound tells us that there cannot exist an elliptic curve over $\mathbb{F}_{3^i}$ for $i = 1, 2, 3$ with a rational 65-torsion point, and thus $x_{\mathbb{F}_3}$ must be a degree 3 cuspidal divisor on $X_1(65)_{\mathbb{F}_3}$.

By Lemma 2.8(1), the cuspidal subscheme of $X_1(65)$ is isomorphic to

$$(\mathbb{Z}/65\mathbb{Z})'/[-1] \sqcup (\mathbb{Z}/5\mathbb{Z} \times \mu_{13})'/[-1] \sqcup (\mu_5 \times \mathbb{Z}/13\mathbb{Z})'/[-1] \sqcup (\mu_{65})'/[-1],$$

where the prime notation means points of exact order 65, and each piece reduces to a distinct rational cusp on $X_0(65)$. We need to analyze the reduction modulo 3 of each piece.

First, no cubic point can reduce to either of the last two pieces. The scheme $(\mu_5 \times \mathbb{Z}/13\mathbb{Z})'$ is isomorphic to 12 copies of $(\mu_5)'$; the $[-1]$ action identifies pairs of copies of $(\mu_5)'$, thus the $(\mu_5 \times \mathbb{Z}/13\mathbb{Z})'/[-1]$ piece is isomorphic to 6 copies of μ_5'. Since the 5-th cyclotomic polynomial is irreducible modulo 3, $(\mu_5)'_{\mathbb{F}_3}$ is still irreducible; $(\mu_5 \times \mathbb{Z}/13\mathbb{Z})'/[-1]$ is thus a sum of quartic points, and our cubic point x cannot reduce to this component. A similar argument shows that our cubic point x cannot reduce to $((\mu_{65})'/[-1])_{\mathbb{F}_3}$.

Next, the $(\mathbb{Z}/5\mathbb{Z} \times \mu_{13})'/[-1]$ part breaks up as 4 copies of μ_{13}', and the $[-1]$ action identifies pairs of copies of $(\mu_{13})'$. The image of $(\mathbb{Z}/5\mathbb{Z} \times \mu_{13})'/[-1]$ in $X_0(65)$ is supported at a single rational cusp. Since each component is isomorphic to μ_{13}' and the 13-th cyclotomic polynomial factors into four cubics over $\mathbb{F}_3$, $(\mu_{13})'_{\mathbb{F}_3}$ breaks up into four pieces each defined over $\mathbb{F}_{3^3}$. The $(\mathbb{Z}/65\mathbb{Z})'/[-1]$ part corresponds to the $\phi(65)/2 = 24$ rational cusps on $X_1(65)$, and these cusps have the same image in $X_0(65)$. A cubic point (considered as a degree 3 divisor) thus reduces either to a sum of three $\mathbb{F}_3$-rational cusps, which have the same image in $X_0(65)$, or a single cubic cusp (again, considered as a degree 3 divisor), whose image in $X_0(65)^{(3)}$ is $3[c_{\mathbb{F}_3}]$ for a rational cusp c. □

We now analyze the decomposition of $J_0(65)$. Using `Magma`'s intrinsic `Decomposition(JZero(65))`, we find that

$$J \sim_{\mathbb{Q}} E \times A_1 \times A_2,$$

where $E(\mathbb{Q})$ has rank 1 and A_i are modular abelian surfaces with analytic rank 0. Let A be the winding quotient. Let $C_1 := 3[c_\infty]$, $C_2 := 3[c_0]$, $C_3 := 3[c_{1/5}]$, and $C_4 := 3[c_{1/13}]$. For $i = 1, \ldots, 4$, define the morphisms $\mu_i : X_0(65)^{(3)} \to J_0(65)$ given by $z \mapsto [z - C_i]$ and $t : J_0(65) \to A$, where the latter is projection. Since $\phi^{(3)}(x_{\mathbb{F}_3})$ is equal to $C_{i,\mathbb{F}_3}$ for some i, the point $(t \circ \mu_i)(\phi^{(3)}(x)) \in A(\mathbb{Q})$ belongs to the kernel of reduction $A(\mathbb{Q}) \to A(\mathbb{F}_3)$ for the appropriate i. However, since $A(\mathbb{Q})$ is torsion, the kernel of reduction is trivial [Katz 1981, Appendix], so $(t \circ \mu_i)(\phi^{(3)}(x)) = 0$ for the appropriate i.

To conclude, we verify that the morphism

$$\tau \circ \mu_i : X_0(65)^{(3)} \to A$$

a formal immersion at $C_{i,\mathbb{F}_3}$ using Proposition 5.8. Via `Magma`'s intrinsic `Newform`, we can compute a basis $\{\omega_1, \ldots, \omega_5\}$ for the 1-forms on $J_0(65)$. The initial basis has q-expansions with noninteger coefficients; to find a basis with integer q-expansions, we simultaneously diagonalize these 1-forms with respect to the action of the Hecke operators. The Hecke action also identifies the subspace pulled back from A. To verify that the formal immersion criterion holds at $C_{i,\mathbb{F}_3}$, we check that certain 4×3 matrices (see (5.8.1)) have rank 3; we can compute the expansions of the ω at the other cusps via the Atkin–Lehner involutions. Finally, Lemma 5.7 asserts that $\phi^{(3)}(x)$ is equal to either $3[c_0]$, $3[c_\infty]$, $3[c_{1/5}]$, or $3[c_{1/13}]$; we conclude that x is cuspidal.

See the `Magma` file `master-65.m` for code verifying these claims.

Remark 7.5. Wang addresses the cases of $N_1 = 22, 25, 40, 49$ in [Wang 2019, Theorem 1.2], $N_1 = 55, 65$ in [Wang 2018, Theorem 1.2], and $N_1 = 39$ in a recent preprint [Wang 2020, Theorem 0.3]. However, his proofs of these cases are incorrect. For instance, [Wang 2019, Lemma 3.5] claims that for $N > 4$ and a prime $p \nmid N$, when the gonality of $X_1(N) > d$ and $J_1(N)(\mathbb{Q})$ is finite, the moduli of each noncuspidal, degree d point of $X_1(N)$ has good reduction at *every* prime $\mathfrak{p}$ over p. (The proofs for $N_1 = 22, 25, 40, 49$ and 39 rely on this claim.)

We provide a counter-example to this. By [Derickx and van Hoeij 2014, Table 1], the gonality of $X_1(31)$ is 12. Over the number field $\mathbb{Q}[a]/(a^{11} - 4a^{10} + 9a^9 - 15a^8 + 21a^7 - 21a^6 + 17a^5 - 8a^4 + 3a^2 - 3a + 1)$, the elliptic curve

$$\begin{aligned} y^2 &+ (a^{10} - 2a^9 + 3a^8 - 3a^7 + 5a^6 + a^5 + a^4 + 3a^3 - 2a^2 + a - 1)xy \\ &+ (a^{10} + 3a^9 + 4a^8 + 6a^7 + 6a^6 + a^5 + 6a^4 - 6a^3 + 2a^2 - 3a - 1)(y - x^2) - x^3 = 0 \end{aligned}$$

has a point of order 31, namely $(0, 0)$. However the norm of the j-invariant of this elliptic curve has 311 in its denominator, and hence, this curve has multiplicative reduction for at least one prime above 311; it cannot have additive reduction because it has a point of order 31. Indeed the prime 311 splits into three primes in this degree 11 number field, one of degree 9 and two of degree 1, and this elliptic curve has good reduction at the prime of degree 9 and one prime of degree 1, but multiplicative reduction at the other prime of degree 1.

Similarly, for $N_1 = 55, 65$, while [Wang 2018, Lemma 3.6] is correct, its application to [Wang 2018, Theorem 3.7] contains an error. Wang applies [loc. cit., Lemma 3.6] to conclude that the points $(\omega_n(x_1), \ldots, \omega_n(x_d))$ and $(\infty, \ldots, \infty)$ on the d-th symmetric power $X_0(N_1)^{(d)}$ of the modular curve $X_0(N_1)$ reduce to the same point modulo p, where ω_n is some Atkin–Lehner involution on $X_0(N_1)$. The correct condition that one needs to check is that $\gcd(N_1, 3^{2i} - 1) = 1$ for $i = 1, 2$, which succeeds for $N_1 = 143, 91, 77$, however it fails for $N_1 = 55, 65$. (In Lemma 7.4, we circumvent this issue for $N_1 = 65$ by verifying the formal immersion criteria at more general cuspidal divisors.)

Remark 7.6. For each i, the morphism $(t \circ \mu_i)$ in Section 7.3 is not a formal immersion at *every* cuspidal divisor on $X_0(65)^{(3)}(\mathbb{F}_3)$. The failure of the formal immersion criterion is due to the fact that the Atkin–Lehner quotient $X_0^+(65)$ is a rank 1 elliptic curve and the quotient map $X_0(65) \to X_0^+(65)$ has degree 2. Since $X_0(65)$ has rational points (the 4 rational cusps), there are 4 "copies" of $X_0(65)^{(2)}(\mathbb{Q})$ lying on $X_0(65)^{(3)}(\mathbb{Q})$. In particular, $X_0(65)^{(3)}(\mathbb{Q})$ is infinite, but only finitely many rational points of $X_0(65)^{(3)}$ do not lie on one of the copies of $X_0(65)^{(2)}(\mathbb{Q})$. Moreover, the reduction modulo 3 of these copies of $X_0(65)^{(2)}(\mathbb{Q})$ correspond to some of the points on $X_0(65)^{(3)}(\mathbb{F}_3)$ where the formal immersion criterion fails. In fact, even more is true: one can compute (in `Magma`, via cotangent spaces) that the map $X_0(65)^{(3)} \to J_e(65)$ to the winding quotient (which has dimension 4) is not an immersion at all points of $X_0(65)^{(3)}$.

Acknowledgements

We thank Lea Beneish, Nils Bruin, John Duncan, Bjorn Poonen, Jeremy Rouse, Andrew Sutherland, and Bianca Viray for helpful discussions. We also thank Lea Beneish, Abbey Bourdon, Bas Edixhoven, Álvaro Lozano-Robledo, and Filip Najman for useful comments on an earlier draft. The third author was supported by NSF grant 1618657. The last author was partially supported by NSF grant DMS-1555048. Finally, we thank the referee for their comments.

References

[Bruin and Najman 2016] P. Bruin and F. Najman, "A criterion to rule out torsion groups for elliptic curves over number fields", *Res. Number Theory* **2** (2016), Art. 3, 13. MR Zbl

[Chen 2011] Y.-H. Chen, "Cuspidal $\mathbb{Q}$-rational torsion subgroup of $J(\Gamma)$ of level P", *Taiwanese J. Math.* **15**:3 (2011), 1305–1323.

[Conrad et al. 2003] B. Conrad, B. Edixhoven, and W. Stein, "$J_1(p)$ has connected fibers", *Doc. Math.* **8** (2003), 331–408. MR Zbl

[Csirik 2002] J. A. Csirik, "The kernel of the Eisenstein ideal", *J. Number Theory* **92**:2 (2002), 348–375.

[Derickx 2016] M. Derickx, *Torsion points on elliptic curves over number fields of small degree*, Ph.D. thesis, Leiden University, 2016.

[Derickx 2017] M. Derickx, MD Sage Package, 2017, https://koffie.github.io/mdsage/doc/html/index.html.

[Derickx and Najman 2019] M. Derickx and F. Najman, "Torsion of elliptic curves over cyclic cubic fields", *Math. Comp.* **88**:319 (2019), 2443–2459. MR Zbl

[Derickx and Sutherland 2017] M. Derickx and A. V. Sutherland, "Torsion subgroups of elliptic curves over quintic and sextic number fields", *Proc. Amer. Math. Soc.* **145**:10 (2017), 4233–4245. MR Zbl

[Derickx and van Hoeij 2014] M. Derickx and M. van Hoeij, "Gonality of the modular curve $X_1(N)$", *J. Algebra* **417** (2014), 52–71. MR Zbl

[Derickx et al. 2013] M. Derickx, M. van Hoeij, and J. Zeng, "Computing Galois representations and equations for modular curves $X_H(\ell)$", preprint, 2013. arXiv

[Derickx et al. 2017] M. Derickx, S. Kamienny, W. Stein, and M. Stoll, "Torsion points on elliptic curves over number fields of small degree", preprint, 2017. arXiv

[Diamond and Im 1995] F. Diamond and J. Im, "Modular forms and modular curves", pp. 39–133 in *Seminar on Fermat's Last Theorem* (Toronto, 1993–1994), edited by V. K. Murty, CMS Conf. Proc. **17**, Amer. Math. Soc., Providence, RI, 1995. MR Zbl

[Drinfeld 1973] V. G. Drinfeld, "Two theorems on modular curves", *Funkcional. Anal. i Priložen.* **7**:2 (1973), 83–84. In Russian; translated in *Funct. Anal. Appl.* **7** (1973), 155–156. MR Zbl

[Frey 1994] G. Frey, "Curves with infinitely many points of fixed degree", *Israel J. Math.* **85**:1-3 (1994), 79–83. MR Zbl

[Gross 2012] B. H. Gross, "Hanoi lectures on the arithmetic of hyperelliptic curves", *Acta Math. Vietnam.* **37**:4 (2012), 579–588. MR Zbl

[Hasegawa and Shimura 1999] Y. Hasegawa and M. Shimura, "Trigonal modular curves", *Acta Arith.* **88**:2 (1999), 129–140. MR Zbl

[Hazama 1998] F. Hazama, "Determinantal formula for the cuspidal class number of the modular curve $X_1(m)$", *J. Number Theory* **68**:2 (1998), 229–242.

[van Hoeij 2013] M. van Hoeij, Minformula (in file: cusp_divisors_program), 2013, www.math.fsu.edu/~hoeij/files/X1N/.

[van Hoeij 2014] M. van Hoeij, "Low degree places on the modular curve $X_1(N)$", preprint, 2014. arXiv

[van Hoeij and Smith 2021] M. van Hoeij and H. Smith, "A divisor formula and a bound on the $\mathbb{Q}$-gonality of the modular curve $X_1(N)$", *Res. Number Theory* **7**:2 (2021). MR Zbl

[Jeon and Kim 2005] D. Jeon and C. H. Kim, "Bielliptic modular curves $X_1(M, N)$", *Manuscripta Math.* **118**:4 (2005), 455–466. MR Zbl

[Jeon, Kim, and Lee 2011] D. Jeon, C. H. Kim, and Y. Lee, "Families of elliptic curves over cubic number fields with prescribed torsion subgroups", *Math. Comp.* **80**:273 (2011), 579–591. MR Zbl

[Jeon, Kim, and Schweizer 2004] D. Jeon, C. H. Kim, and A. Schweizer, "On the torsion of elliptic curves over cubic number fields", *Acta Arith.* **113**:3 (2004), 291–301. MR Zbl

[Kamienny 1992a] S. Kamienny, "Torsion points on elliptic curves and q-coefficients of modular forms", *Invent. Math.* **109**:1 (1992), 221–229. MR Zbl

[Kamienny 1992b] S. Kamienny, "Torsion points on elliptic curves over fields of higher degree", *Internat. Math. Res. Notices* 6 (1992), 129–133. MR Zbl

[Kato 2004] K. Kato, "p-adic Hodge theory and values of zeta functions of modular forms", pp. 117–290 in *Cohomologies p-adiques et applications arithmétiques*, vol. III, edited by P. Berthelot et al., Astérisque **295**, 2004. MR Zbl

[Katz 1981] N. M. Katz, "Galois properties of torsion points on abelian varieties", *Invent. Math.* **62**:3 (1981), 481–502. MR Zbl

[Kenku 1982] M. A. Kenku, "On the number of **Q**-isomorphism classes of elliptic curves in each **Q**-isogeny class", *J. Number Theory* **15**:2 (1982), 199–202. MR Zbl

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

[Kubert and Lang 1981] D. S. Kubert and S. Lang, *Modular units*, Grundlehren der Math. Wissenschaften **244**, Springer, 1981. MR Zbl

[Lario and Schoof 2002] J.-C. Lario and R. Schoof, "Some computations with Hecke rings and deformation rings", *Experiment. Math.* **11**:2 (2002), 303–311. MR Zbl

[Lozano-Robledo 2013] A. Lozano-Robledo, "On the field of definition of p-torsion points on elliptic curves over the rationals", *Math. Ann.* **357**:1 (2013), 279–305. MR

[Magma 1997] W. Bosma, J. Cannon, and C. Playoust, "The Magma algebra system, I. The user language", *J. Symbolic Comput.* **24**:3-4 (1997), 235–265. MR Zbl

[Manin 1972] Ju. I. Manin, "Parabolic points and zeta functions of modular curves", *Izv. Akad. Nauk SSSR Ser. Mat.* **36**:1 (1972), 19–66. In Russian; translated in *Math. USSR-Izv.* **6**:1 (1972), 19–64. MR Zbl

[Maple 2005] M. B. Monagan, K. O. Geddes, K. M. Heal, G. Labahn, S. M. Vorkoetter, J. McCarron, and P. DeMarco, *Maple* 10 *Programming Guide*, Maplesoft, Waterloo ON, Canada, 2005.

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

[Mazur 1978] B. Mazur, "Rational isogenies of prime degree", *Invent. Math.* **44**:2 (1978), 129–162. MR Zbl

[Merel 1996] L. Merel, "Bornes pour la torsion des courbes elliptiques sur les corps de nombres", *Invent. Math.* **124**:1-3 (1996), 437–449. MR Zbl

[Momose 1984] F. Momose, "p-torsion points on elliptic curves defined over quadratic fields", *Nagoya Math. J.* **96** (1984), 139–165.

[Mordell 1922] L. J. Mordell, "On the rational solutions of the indeterminate equations of the third and fourth degrees", *Proc. Cambridge Philos. Soc* **21** (1922), 179–192.

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

[Ogg 1975] A. P. Ogg, "Automorphismes de courbes modulaires", in *Séminaire Delange–Pisot–Poitou*, *Théorie des nombres*, vol. 16, Secrétariat mathématique, 1975. MR Zbl

[Ohta 2013] M. Ohta, "Eisenstein ideals and the rational torsion subgroups of modular Jacobian varieties", *J. Math. Soc. Japan* **65**:3 (2013), 733–772.

[Ozman and Siksek 2019] E. Ozman and S. Siksek, "Quadratic points on modular curves", *Math. Comp.* **88**:319 (2019), 2461–2484. MR Zbl

[Parent 2000] P. Parent, "Torsion des courbes elliptiques sur les corps cubiques", *Ann. Inst. Fourier* (*Grenoble*) **50**:3 (2000), 723–749. MR Zbl

[Parent 2003] P. Parent, "No 17-torsion on elliptic curves over cubic number fields", *J. Théor. Nombres Bordeaux* **15**:3 (2003), 831–838.

[Poincaré 1910] H. Poincaré, "Sur les courbes tracées sur les surfaces algébriques", *Ann. Sci. École Norm. Sup.* (3) **27** (1910), 55–108. MR Zbl

[Rouse and Zureick-Brown 2015] J. Rouse and D. Zureick-Brown, "Elliptic curves over $\mathbb{Q}$ and 2-adic images of Galois", *Res. Number Theory* **1** (2015), art. id. 12. MR Zbl

[Sage 2017] The Sage Developers, *SageMath, the Sage Mathematics Software System*, 2017, http://www.sagemath.org.

[Streng 2015] M. Streng, "Generators of the group of modular units for $\Gamma_1(N)$ over $\mathbb{Q}$", preprint, 2015. arXiv

[Sun 2010] H.-S. Sun, "Cuspidal class number of the tower of modular curves $X_1(Np^n)$", *Math. Ann.* **348**:4 (2010), 909–927.

[Sutherland 2012a] A. V. Sutherland, "Constructing elliptic curves over finite fields with prescribed torsion", *Math. Comp.* **81**:278 (2012), 1131–1147. MR

[Sutherland 2012b] A. V. Sutherland, "Defining equations for $X_1(N)$", 2012, http://math.mit.edu/~drew/X1_altcurves.html.

[Takagi 1992] T. Takagi, "Cuspidal class number formula for the modular curves $X_1(p)$", *J. Algebra* **151**:2 (1992), 348–374.

[Takagi 1995] T. Takagi, "The cuspidal class number formula for the modular curves $X_1(3^m)$", *J. Math. Soc. Japan* **47**:4 (1995), 671–686.

[Takagi 2008] T. Takagi, "The cuspidal class number formula for the modular curves $X_1(2^{2n+1})$", *J. Algebra* **319**:9 (2008), 3535–3566.

[Takagi 2012] T. Takagi, "The cuspidal class number formula for the modular curves $X_1(2p)$", *J. Math. Soc. Japan* **64**:1 (2012), 23–85.

[Takagi 2014] T. Takagi, "The $\mathbb{Q}$-rational cuspidal group of $J_1(2p)$", *J. Math. Soc. Japan* **66**:4 (2014), 1249–1301.

[Wang 2015] J. Wang, *On the torsion structure of elliptic curves over cubic number fields*, Ph.D. thesis, University of Southern California, 2015, https://www.proquest.com/docview/1728322697.

[Wang 2018] J. Wang, "On the cyclic torsion of elliptic curves over cubic number fields", *J. Number Theory* **183** (2018), 291–308. MR Zbl

[Wang 2019] J. Wang, "On the cyclic torsion of elliptic curves over cubic number fields, II", *J. Théor. Nombres Bordeaux* **31**:3 (2019), 663–670. MR Zbl

[Wang 2020] J. Wang, "On the cyclic torsion of elliptic curves over cubic number fields, III", (2020). arXiv

[Weil 1929] A. Weil, "L'arithmétique sur les courbes algébriques", *Acta Math.* **52**:1 (1929), 281–315. MR Zbl

[Yang 2009] Y. Yang, "Modular units and cuspidal divisor class groups of $X_1(N)$", *J. Algebra* **322**:2 (2009), 514–553. MR Zbl

[Yang and Yu 2010] Y. Yang and J.-D. Yu, "Structure of the cuspidal rational torsion subgroup of $J_1(p^n)$", *J. Lond. Math. Soc.* (2) **82**:1 (2010), 203–228.

[Yu 1980] J. Yu, "A cuspidal class number formula for the modular curves $X_1(N)$", *Math. Ann.* **252**:3 (1980), 197–216. MR Zbl

[Zywina 2020] D. Zywina, "Computing actions on cusp forms", preprint, 2020. arXiv

Communicated by Frank Calegari
Received 2020-08-10 Revised 2020-11-05 Accepted 2020-12-20

maarten@mderickx.nl *Mathematisch Instituut, Universiteit Leiden, Leiden, Netherlands*

aetropolski@rice.edu *Department of Mathematics, Rice University, Houston, TX, United States*

hoeij@math.fsu.edu *Department of Mathematics, Florida State University, Tallahassee, FL, United States*

jmorrow4692@gmail.com *Department of Mathematics, Emory University, Atlanta, GA, United States*

dzb@mathcs.emory.edu *Department of Mathematics, Emory University, Atlanta, GA, United States*

Algebra & Number Theory

msp.org/ant

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2021 is US $415/year for the electronic version, and $620/year (+$60, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

ANT peer review and production are managed by EditFLOW® from MSP.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

Algebra & Number Theory

Volume 15 No. 7 2021