

GONALITY AND QUINTIC POINTS ON INTERMEDIATE MODULAR CURVES

MARIN VARIVODA

ABSTRACT. For $\{\pm 1\} \subseteq \Delta \subseteq (\mathbb{Z}/N\mathbb{Z})^\times$ let $X_\Delta(N)$ be the intermediate modular curve between $X_1(N)$ and $X_0(N)$. We determine the $\mathbb{Q}$ -gonality of every strict intermediate curve $X_\Delta(N)$ with $N \leq 50$, and of $X_1(N)$ for $41 \leq N \leq 50$, where it equals the upper bound of Derickx and van Hoeij at every level. We also settle the thirty levels left open by Derickx, Hwang, Jeon and Orlić, completing the list of curves $X_0(N)$ with infinitely many points of degree 5, and we show that exactly 43 strict intermediate curves have infinitely many points of degree 5. As a consequence, the strict intermediate curves of density degree 5 are exactly the four $\mathbb{Q}$ -pentagonal curves found by Orlić. The proofs use published classifications, the Castelnuovo–Severi inequality, and three computational methods; all computations can be rerun from the accompanying code.

1. INTRODUCTION

Let N be a positive integer and Δ a subgroup with $\{\pm 1\} \subseteq \Delta \subseteq (\mathbb{Z}/N\mathbb{Z})^\times$. The intermediate modular curve $X_\Delta(N)$ is the modular curve attached to

$$\Gamma_\Delta(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \pmod{N}, a \pmod{N} \in \Delta \right\}.$$

It lies between $X_1(N) = X_{\{\pm 1\}}(N)$ and $X_0(N) = X_{(\mathbb{Z}/N\mathbb{Z})^\times}(N)$, and it is defined over $\mathbb{Q}$. We call $X_\Delta(N)$ *strict* if both inclusions $\{\pm 1\} \subsetneq \Delta \subsetneq (\mathbb{Z}/N\mathbb{Z})^\times$ are strict. We follow the notation of Jeon, Kim and Schweizer [25], Orlić [36] and Derickx and Orlić [13], and we name curves by their LMFDB labels [42, 38].

For a curve C over a field k , the k -gonality $\mathrm{gon}_k C$ is the least degree of a nonconstant morphism $C \rightarrow \mathbb{P}^1$ defined over k . A *point of degree d* on $C/\mathbb{Q}$ is a closed point whose residue field has degree d over $\mathbb{Q}$. The *density degree* of C is the least d such that C has infinitely many points of degree d . By Hilbert irreducibility, C has infinitely many points of degree $\mathrm{gon}_{\mathbb{Q}} C$, so the density degree is at most the $\mathbb{Q}$ -gonality.

1.1. Previous work. Points of low degree on modular curves have been studied intensively, with the degree going up one at a time. For $X_0(N)$, the curves with infinitely many points of degree 2 follow from Ogg’s classification of hyperelliptic curves [35] and Bars’ classification of bielliptic curves [3]; degree 3 is due to Jeon [23]; degree 4 to Hwang and Jeon [21] and independently to Derickx and Orlić [12]; and degree 5 to Derickx, Hwang, Jeon and Orlić [10], except for thirty levels that their methods did not reach. For intermediate curves, degree 2 is due to Jeon, Kim and Schweizer [25], degree 3 to Dalal [5], and degree 4 to Derickx and Orlić [13]. In [13] the authors explain the obstacles to extending their methods to degree 5; Theorem B below settles that case.

For gonality, the hyperelliptic and trigonal intermediate curves were found by Ishii and Momose [22] and Jeon and Kim [24]. Orlić [36] determined all intermediate curves of $\mathbb{Q}$ -gonality at most

Date: October 13, 2026.

2020 Mathematics Subject Classification. 11G18, 14H51, 11G05, 14G05.

Key words and phrases. modular curves, gonality, points of low degree, density degree.

5, and the $\mathbb{Q}$ -gonality of every strict curve with $N \leq 40$. The $\mathbb{Q}$ -gonality of $X_0(N)$ is known for $N < 145$ by Najman and Orlić [33], and that of $X_1(N)$ for $N \leq 40$ by Derickx and van Hoeij [16], who also gave upper bounds for $N \leq 250$.

1.2. Results.

Theorem C. *Let $X_\Delta(N)$ be a strict intermediate curve with $N \leq 50$. Its $\mathbb{Q}$ -gonality is given in Table 3. For $N \leq 40$ these values are due to Orlić [36], as are those of 6 of the 24 curves with $41 \leq N \leq 50$, which have gonality 4 or 5; two more have genus 3 and 4 and are trigonal. The values for the other 16 curves are new.*

Theorem D. *For $41 \leq N \leq 50$, the $\mathbb{Q}$ -gonality of $X_1(N)$ equals the upper bound of Derickx and van Hoeij [16]:*

N	41	42	43	44	45	46	47	48	49	50
$\text{gon}_{\mathbb{Q}} X_1(N)$	22	12	24	15	18	19	29	16	21	15

Theorem A. *For each of the thirty levels*

$$N \in \{74, 77, 79, 82, 83, 85, 86, 88, 89, 92, 96, 98, 99, 100, 101, \\ 103, 107, 111, 118, 123, 128, 131, 141, 142, 143, 145, 155, 159, 167, 191\}$$

left open in [10, Remark 1.11 and §7], the curve $X_0(N)$ has only finitely many points of degree 5, and no morphism of degree 5 to $\mathbb{P}^1$ over $\mathbb{Q}$. Together with [10, Theorem 1.10], this completes the list of curves $X_0(N)$ with infinitely many points of degree 5.

Theorem B. *Exactly 43 strict intermediate curves $X_\Delta(N)$ have infinitely many points of degree 5. They are listed in Table 4, and each of them has a morphism of degree 5 to $\mathbb{P}^1$ over $\mathbb{Q}$.*

Corollary E. *The strict intermediate curves of density degree 5 are exactly the four $\mathbb{Q}$ -pentagonal curves of Orlić [36, Theorems 1.4–1.5]: $X_\Delta(31)$ with $\Delta = \langle -1, 2 \rangle$ and $\Delta = \langle -1, 5 \rangle$, $X_\Delta(44)$ with $\Delta = \langle -1, 5 \rangle$, and $X_\Delta(125)$ with $\Delta = \langle -1, 4 \rangle$.*

This parallels the case of $X_0(N)$, where $X_0(109)$ is the only curve of density degree 5 [10].

1.3. Methods. We have tried to keep the new mathematical input to a minimum, so that the paper can be checked by a human reader. Wherever a published result or an inequality settles a case, we use it: Castelnuovo–Severi, the classifications of curves of small gonality [22, 24, 36], and the classifications of curves with infinitely many points of degree at most 4 [25, 5, 13, 10]. Everything else is done by three methods, each stated once:

- I. *Explicit pencils:* an explicit divisor D with $\ell(D) \geq 2$ gives $\text{gon}_{\mathbb{Q}} \leq \deg D$ (§3.1).
- II. *Finite-field exclusion:* at a prime of good reduction, a complete search over $\mathbb{F}_p$ shows that there is no function of degree at most d (§3.2). We use the gonality algorithm of Derickx and Terao [15] and their package CurveArith. For the large curves $X_1(N)$ we keep their first phase (places and expansions of differentials) unchanged and replace their second phase by a search over a smaller family of divisors, run in compiled code (§3.3). For $X_1(48)$ we search instead on the quotient by a diamond involution (§5.1).
- III. *Lifting arguments:* when a finite field allows more than $\mathbb{Q}$ does, a Mordell–Weil or local argument decides which classes over $\mathbb{F}_p$ come from $\mathbb{Q}$. This is needed for Theorems A and B and for one curve in Theorem C.

All computations were done in Magma V2.29-4 [4] and SageMath 10.7. The code, data and logs that verify all computations in this paper can be found on

<https://github.com/marin-varivoda/intermediate-modular-curves>;

§8 describes how to rerun them.

2. PRELIMINARIES

2.1. Curves and models. The groups Δ and the curves $X_\Delta(N)$ are enumerated with Derickx's package MD Sage [8] (`intermediate_modular_groups`), as in [36, 13]. We identify each curve with its LMFDB label by checking that the corresponding open subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$,

$$H_\Delta = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) : a \in \Delta \right\},$$

is conjugate to the group of the label. Rational Fourier expansions at the cusp ∞ describe the model of $X_\Delta(N)$ that parametrizes μ_N -markings; since $\Delta = \Delta^{-1}$, it is $\mathbb{Q}$ -isomorphic to the model parametrizing points of order N : quotienting by the marked subgroup and dualizing interchanges the two moduli problems over $\mathbb{Q}$ and carries the diamond operator $\langle a \rangle$ to $\langle a^{-1} \rangle$, so it descends to $X_\Delta(N)$ because $\Delta^{-1} = \Delta$. In particular the cusp ∞ is a rational point of $X_\Delta(N)$.

For genus $g \geq 5$ we use the canonical model computed by MD Sage (`vanishing_quadratic_forms` with `minimize_strategy="LLL"`); all lower bounds over finite fields for Theorems C and D are computed on these models or on the models of $X_1(N)$ below (for Theorem A, on Magma's canonical models of $X_0(N)$). For $X_1(N)$ we use the plane models of Sutherland and van Hoeij [40]: each comes with explicit Tate normal form data (E, P) over its function field with P of order N , which gives the birational map to $X_1(N)$ (compare [41]).

2.2. Good reduction. All lower bounds over $\mathbb{Q}$ in this paper come from a prime of good reduction.

Lemma 2.1 (Specialization). *Let $C/\mathbb{Q}$ be a smooth projective geometrically integral curve, and let $\mathcal{C}$ be a smooth proper model of C over $\mathbb{Z}_{(p)}$. Then $\mathrm{gon}_{\mathbb{Q}} C \geq \mathrm{gon}_{\mathbb{F}_p} \mathcal{C}_{\mathbb{F}_p}$. More generally, if L is a line bundle on C with $h^0(L) \geq 2$, then its extension to $\mathcal{C}$ has $h^0 \geq 2$ on $\mathcal{C}_{\mathbb{F}_p}$.*

Proof. The second statement is upper semicontinuity of h^0 [20, III.12.8], applied to the extension of L (which exists because $\mathcal{C}$ is regular). If $f: C \rightarrow \mathbb{P}^1$ has degree d , take $L = f^*\mathcal{O}(1)$: its extension has degree d and at least two sections on the special fibre, so $\mathrm{gon}_{\mathbb{F}_p} \mathcal{C}_{\mathbb{F}_p} \leq d$. This is standard; see for example [37] and [33]. $\square$

We certify that a given model has good reduction at p in one of two ways.

- (1) For the canonical model of an intermediate curve of genus g , we check that the reduction of the MD Sage equations modulo p is an integral curve with the Hilbert polynomial $(2g - 2)t + 1 - g$ of the generic canonical curve, whose normalization has genus g , and which contains the reduction $(1 : 0 : \dots : 0)$ of the cusp ∞ . Then the flat closure of C in the integral model has the same special fibre (both have the same Hilbert polynomial and one contains the other); equality of arithmetic and geometric genus makes it normal, hence smooth, and the rational point makes it geometrically integral. (The primes $p \nmid N$ at which this can fail are controlled by Derickx and Najman [11]; we only use primes where the check passes.)
- (2) For $X_1(N)$ with $p \nmid N$: the curve $X_1(N)$ has good reduction at p [7]. Its function field is $\mathbb{Q}(x, y)$ with $F(x, y) = 0$ the plane model of [40], scaled to a primitive polynomial in $\mathbb{Z}[x, y]$. We reduce F modulo p and check that $\deg_y \bar{F} = \deg_y F$, that $\bar{F}$ is irreducible over $\mathbb{F}_p(x)$, that $\mathbb{F}_p$ is algebraically closed in $K_p = \mathbb{F}_p(x)[y]/(\bar{F})$, and that K_p has genus $g(X_1(N))$. The field K_p is the residue field of the Gauss valuation of $\mathbb{Q}(x, y)$ extending the p -adic valuation, so it is the function field of a component of the special fibre of some normal model of $X_1(N)$. Every such model is dominated by a blow-up of the smooth model, whose exceptional components are rational [31, §9.3, §10.1]; as $g(K_p) = g(X_1(N)) \geq 2$, K_p is the function field of $X_1(N)_{\mathbb{F}_p}$.

2.3. Tools from the geometry of curves.

Lemma 2.2 (Castelnuovo–Severi [39, Theorem 3.11.3]). *Let C be a curve of genus g over a perfect field, with morphisms $C \rightarrow C_1$ and $C \rightarrow C_2$ of degrees d_1, d_2 to curves of genera g_1, g_2 . If the two morphisms do not both factor through a common morphism of degree > 1 , then $g \leq d_1 g_1 + d_2 g_2 + (d_1 - 1)(d_2 - 1)$.*

We use it mainly with $C_2 = \mathbb{P}^1$: a morphism $C \rightarrow \mathbb{P}^1$ of degree d that does not factor through a morphism $C \rightarrow C_1$ of degree m to a curve of genus h satisfies $g \leq mh + (m - 1)(d - 1)$. If $\gcd(d, m) = 1$ the factorization condition holds automatically.

Lemma 2.3 (Pullback). *If $\pi: C \rightarrow D$ has degree m over $\mathbb{Q}$, then $\text{gon}_{\mathbb{Q}} C \leq m \cdot \text{gon}_{\mathbb{Q}} D$.*

Lemma 2.4 (Hilbert irreducibility). *If a curve $C/\mathbb{Q}$ has a morphism $C \rightarrow \mathbb{P}^1$ of degree d over $\mathbb{Q}$, then it has infinitely many points of degree d .*

Proof. By Hilbert’s irreducibility theorem, the set of $t \in \mathbb{P}^1(\mathbb{Q})$ whose fibre is a single closed point of degree d is the complement of a thin set, and in particular infinite. $\square$

Lemma 2.5 (Frey [19], Abramovich [1]). *If $C/\mathbb{Q}$ has infinitely many points of degree d , then $\text{gon}_{\mathbb{Q}} C \leq 2d$. For a modular curve of index μ in $\text{PSL}_2(\mathbb{Z})$, $\text{gon}_{\mathbb{C}} \geq \frac{\lambda_1}{24}\mu$ with $\lambda_1 \geq \frac{975}{4096}$ by Kim and Sarnak [29, Appendix 2].*

In particular, a modular curve with $119\mu > 120000$ has $\text{gon}_{\mathbb{C}} > 10$ and so only finitely many points of degree 5; this is the form used in [36, Theorem 3.16] and below.

3. THREE METHODS

Throughout, C is a smooth projective geometrically integral curve of genus g over a field k , and for a divisor D we write $L(D) = \{f \in k(C)^{\times} : \text{div } f + D \geq 0\} \cup \{0\}$ and $\ell(D) = \dim L(D)$. A nonconstant $f \in k(C)$ has degree $\deg f = \deg(f)_{\infty}$, the degree of its pole divisor, and $\text{gon}_k C \leq d$ if and only if there is an effective divisor D of degree at most d with $\ell(D) \geq 2$.

3.1. Method I: explicit pencils. To prove $\text{gon}_{\mathbb{Q}} C \leq d$ we exhibit a rational effective divisor D of degree d and compute $\ell(D) \geq 2$ with Magma’s Riemann–Roch routine. The divisors used are of three kinds:

- (1) divisors supported on rational cusps, or on cusps and other low-degree points, whose Riemann–Roch spaces we compute from q -expansions at all cusps, using Zywin’s package [44];
- (2) pullbacks along a forgetful map $X_{\Delta}(N) \rightarrow X_{\Delta'}(M)$ of a pencil of minimal degree on the target, whose gonality is known (Theorem 2.3);
- (3) low genus: if $g \geq 2$ and $P \in C(\mathbb{Q})$, then $\ell(K - (g - 2)P) = \ell((g - 2)P) + 1 \geq 2$ by Riemann–Roch, so $\text{gon}_{\mathbb{Q}} C \leq g$; if $g \leq 1$ and $P \in C(\mathbb{Q})$, then $\ell(2P) \geq 2$ (and $\ell(P) = 2$ if $g = 0$).

For $X_1(N)$ the upper bounds in Theorem D are the degrees of the modular units of Derickx and van Hoeij [16, Table 1], which also equal the degree in y of the model of [40].

3.2. Method II: finite-field exclusion. To prove $\text{gon}_{\mathbb{Q}} C > d$, we choose a prime p of good reduction (Theorem 2.1) and show that $C_{\mathbb{F}_p}$ has no nonconstant function of degree at most d . For this we use the algorithm of Derickx and Terao [15], implemented in their Magma package CurveArith; it works over any finite field $\mathbb{F}_q$ (here $q = p$) and has two phases.

Phase 1 (places and expansions). Let $N_1 = \#C(\mathbb{F}_q)$ and $n = \lceil N_1/(q + 1) \rceil$. CurveArith enumerates the places of $C_{\mathbb{F}_q}$ of degree at most $d - \min(n, d - 1)$, fixes a basis $\omega_1, \dots, \omega_g$ of $H^0(C, \Omega^1)$, and at each place P computes the first m_P coefficients of the expansions of the ω_i

in a uniformizer at P , as vectors over $\mathbb{F}_q$ ($\deg P$ coordinates per coefficient). For an effective divisor $D = \sum a_P P$ with $a_P \leq m_P$ this gives a $g \times \deg D$ matrix M_D , whose columns are the coefficients of index $< a_P$ at each P in its support.

Lemma 3.1 ([15]). $\ell(D) = \deg D + 1 - \text{rank } M_D$.

Proof. By Riemann–Roch, $\ell(D) = \deg D + 1 - g + \ell(K - D)$, and $\ell(K - D) = g - \text{rank } M_D$ is the dimension of the space of holomorphic differentials vanishing on D . $\square$

Lemma 3.2 ([15, 16]). *If $C_{\mathbb{F}_q}$ has a nonconstant function f of degree at most d , it has one whose pole divisor contains at least n distinct rational places.*

Proof. The N_1 rational points are distributed among the $q + 1$ fibres of f over $\mathbb{P}^1(\mathbb{F}_q)$, so one fibre contains at least n of them. Compose f with an automorphism of $\mathbb{P}^1$ over $\mathbb{F}_q$ moving that fibre to ∞ . $\square$

Phase 2 (search). CurveArith tests all effective divisors D of degree d containing at least n rational places for $\ell(D) \geq 2$ (Theorem 3.1). This is enough for every strict intermediate curve in this paper. For the curves $X_1(N)$ with $41 \leq N \leq 50$ there are far too many such divisors, and we use instead a smaller family of larger divisors, as follows.

3.3. A smaller search family. Let $S = \{P_1, \dots, P_{N_1}\}$ be the rational places, and also write $S = \sum P_i$. Fix an integer $b \geq 1$. For an effective divisor Q with no rational place in its support and an effective divisor E supported on S , put $s = \# \text{supp } E$ and

$$(1) \quad c(E, Q) = bs + \max(n - s, 0) + \deg E + \deg Q.$$

Let $\mathcal{F}_b(d)$ be the set of divisors $H = bS + E + Q$ with $\deg Q \leq d - n$, $c(E, Q) \leq d$, and E maximal with this property for its Q (for the order $E \leq E'$).

Proposition 3.3. *Suppose $n \geq 1$. If $C_{\mathbb{F}_q}$ has a nonconstant function of degree at most d , then there is $H \in \mathcal{F}_b(d)$ such that $L(H)$ contains a nonconstant function of degree at most d .*

Proof. By Theorem 3.2 there is such an f whose pole divisor $D = A + Q$ has at least n distinct rational places in its support, where A is supported on S and Q on the other places. Put $E = \sum_{P \in S} \max(v_P(A) - b, 0)P$ and $s = \# \text{supp } E$. A place in $\text{supp } E$ contributes $b + v_P(E)$ to $\deg A$, and $\text{supp } A$ has at least $\max(n - s, 0)$ further places, each contributing at least 1. Hence $c(E, Q) \leq \deg A + \deg Q = \deg f \leq d$, and in particular $\deg Q \leq d - n$. Since $v_P(A) \leq b + v_P(E)$ for every $P \in S$, we have $D \leq bS + E + Q$. Enlarging E to a maximal E' with $c(E', Q) \leq d$ keeps $D \leq bS + E' + Q$, so $f \in L(bS + E' + Q)$ with $bS + E' + Q \in \mathcal{F}_b(d)$. $\square$

The divisors in $\mathcal{F}_b(d)$ have degree larger than d , so $\ell(H) \geq 2$ is not enough: we need the least degree of a nonconstant function in $L(H)$. It can be read off from the same matrix M_H .

Lemma 3.4. *Let H be effective. The space $L(H)/k$ is isomorphic to the space of vectors x with $M_H x = 0$. Under this isomorphism, the order of the pole of f at $P \in \text{supp } H$ is the largest $j \leq v_P(H)$ such that the coordinates of x belonging to the coefficient of index $j - 1$ at P are not all zero.*

Proof. For each $P \in \text{supp } H$ let $V_P = \mathcal{O}_P / \mathfrak{m}_P^{v_P(H)}$ and $V = \bigoplus V_P$. Write each ω_i as $g_i du_P$ with u_P the uniformizer chosen by CurveArith at P ; the columns of M_H are the coordinates (over k , using a k -basis of the residue field at P) of the jets of the g_i in V , in which, for every j , the subspace $\mathfrak{m}_P^j / \mathfrak{m}_P^{v_P(H)}$ is cut out by the vanishing of the coordinates of index $< j$; indeed, CurveArith computes the coefficients one at a time, subtracting a lift of each coefficient and dividing by the uniformizer, and this is k -linear. The pairing $(\phi, \eta) \mapsto \sum_P \text{Tr}_{k(P)/k} \text{Res}_P(\phi \eta du_P)$

identifies the principal parts $\bigoplus_P \mathfrak{m}_P^{-v_P(H)}/\mathcal{O}_P$ with the dual of V , a principal part having pole order $\leq j$ at P exactly when it annihilates $\mathfrak{m}_P^j/\mathfrak{m}_P^{v_P(H)}$. By the residue theorem and Serre duality, a principal part is the principal part of a function in $L(H)$ (unique up to constants) if and only if it annihilates the image of $H^0(C, \Omega^1)$ in V , that is, if and only if its coordinate vector x satisfies $M_H x = 0$. $\square$

Precision. The expansions computed in Phase 1 suffice for every $H \in \mathcal{F}_b(d)$: at a rational place $P \in \text{supp } E$ we have $v_P(H) = b + v_P(E) \leq bs + \deg E \leq d$, which is CurveArith's precision there, and at a place P of degree $e \geq 2$ we have $ev_P(H) \leq \deg Q \leq d - n$, so $v_P(H) \leq \lfloor (d - \min(n, d - 1))/e \rfloor$, which is CurveArith's precision there. (The program checks this before searching.)

So for $H \in \mathcal{F}_b(d)$ we compute the kernel of M_H and check whether some nonzero kernel vector, up to scalars, gives a pole divisor of degree at most d . By Theorem 3.3, if this fails for every $H \in \mathcal{F}_b(d)$, then $\text{gon}_{\mathbb{F}_q} C > d$. The same argument with $b = 0$ and all effective divisors of degree at most d handles curves without rational points; we did not need this case.

Remark 3.5. Theorem 3.3 and Theorem 3.4 are an elementary variation on the second phase of [15]; the first phase is used unchanged. The point is that $\mathcal{F}_b(d)$ is much smaller than the set of divisors of degree d with n rational places: the rational part is fixed to bS up to the small excess E , and the kernels of M_H have dimension at most 2 or 3 in all our computations. For a fixed Q , the divisors $bS + E + Q$ share the block of rows of $bS + Q$, so we eliminate those once and add the rows of E incrementally. This variation was first implemented as an option `A1:="Cover"` of CurveArith's `CAHasFunctionOfDegreeAtMost`; for the curves $X_1(N)$ we run the same search in a short C++ program (§8).

3.4. Method III: lifting. When $C_{\mathbb{F}_p}$ has more functions or divisor classes of a given kind than can come from $\mathbb{Q}$, we use the structure of $J(\mathbb{Q})$, where $J = \text{Jac } C$, to decide which of them lift. The arguments are of three types, each explained where it is used:

- (1) *rank zero*: if $J(\mathbb{Q})$ is finite, reduction at an odd good prime is injective on $J(\mathbb{Q})$, and a finite list of classes over $\mathbb{F}_p$ can be compared with explicit rational classes (§6, §7);
- (2) *a known positive-rank part*: if $J(\mathbb{Q}) = A(\mathbb{Q}) + T$ for an explicit abelian subvariety A and an explicit finite group T , the reduction of $J(\mathbb{Q})$ is contained in an explicit subgroup of $J(\mathbb{F}_p)$ (the curve 43.132.9.a.2 in §4, and Route Q in §6, Table 9);
- (3) *local rigidity*: if over $\mathbb{F}_p$ the relevant locus agrees, to first order, with a known family defined over $\mathbb{Q}$, a formal implicit function argument shows that it agrees over $\mathbb{Z}_p$ (Theorem 6.2).

4. GONALITY OF INTERMEDIATE CURVES: PROOF OF THEOREM C

There are 76 strict intermediate curves with $N \leq 50$, of which 52 have $N \leq 40$; for the 39 of these of genus ≥ 3 both bounds are in [36, Theorem 1.2, Table 1], the other 13 have genus ≤ 1 , and we only recall them in Table 3. The remaining 24 curves, with $41 \leq N \leq 50$, are treated as follows.

4.1. Upper bounds. Each upper bound is Method I.

- *Pullbacks.* Fourteen curves map, by a forgetful map of degree m , to a curve whose gonality γ is known, with $m\gamma$ equal to the lower bound. The targets have genus at most 3, or are hyperelliptic, or are curves $X_1(M)$ with $M \leq 40$ [16]; the degree and target of each map are listed in the data file of the accompanying repository.
- *Cuspidal divisors.* For five curves (41.168.11.b.1, 41.210.11.b.1, 41.420.21.d.1, 45.432.21.g.2, 49.392.19.i.2), a rational divisor D supported on the cusps has degree equal to the lower bound and $\ell(D) \geq 2$. We compute $\ell(D) = \deg D + 1 - g + \ell(K - D)$, where $H^0(K - D)$

is the space of weight-2 cusp forms vanishing to the prescribed orders at the cusps, from q -expansions at all cusps computed with Zywin's package [44]. Conditions at one cusp of each Galois orbit suffice, since the basis is rational.

- *Published.* 44.144.8.c.4 is in Orlić's list of $\mathbb{Q}$ -pentagonal curves [36, Theorems 1.4–1.5], and 45.144.5.a.1 in the list of $\mathbb{Q}$ -tetragonal curves [36, Theorem 1.3]; 49.168.3.b.1 is a nonhyperelliptic genus-3 curve with a rational point.
- *Two special divisors at level 43.* For 43.308.15.b.1 (genus 15) we take $D = 3C_3 + C_4 + P_5$, where C_3, C_4 are rational cusps and P_5 is a point of degree 5, the image of a point of degree 15 on $X_1(43)$ found by van Hoeij [43]; then $\deg D = 9$ and $\ell(D) = 2$. For 43.132.9.a.2 (genus 9), let $\pi: X \rightarrow X_0^+(43) = E$ be the map of degree 6 to the elliptic curve 43a1; with rational cusps C_1, C_2, C_3 , the divisor $D = 3C_3 + 7C_2 - 3C_1 + \pi^*(G) - \pi^*(O)$ for a point $G \in E(\mathbb{Q})$ of infinite order has degree 7 and $\ell(D) = 2$.

4.2. Lower bounds. Twenty-one of the 24 lower bounds are Method II, using CurveArith's **CAGonality** unchanged at a prime of good reduction (Table 3). Six of these curves (41.84.5.a.1, 44.144.8.c.4, 45.144.5.a.1 and the three curves of genus 5 and 7 at level 48) are also covered by Orlić's classification [36]; we recompute them as a check. The longest computation, for 48.384.19.bc.1 at $p = 7$, takes about an hour; all others take at most eleven minutes. The curves 49.168.3.b.1 and 50.180.4.a.2 have genus 3 and 4 and are not hyperelliptic [22], hence have gonality at least 3.

The remaining curve, 43.132.9.a.2, needs Method III.

4.3. The curve 43.132.9.a.2. Let $X = X_\Delta(43)$ with $\Delta = \langle -1, 2 \rangle = \{\pm 1, \pm 2, \pm 4, \pm 8, \pm 11, \pm 16, \pm 21\}$. It has genus 9, three rational cusps C_1, C_2, C_3 and one cusp orbit $C_{(3)}$ of degree 3. The forgetful map $X \rightarrow X_0(43)$ has degree 3, and composing with the quotient by the Atkin–Lehner involution gives $\pi: X \rightarrow X_0^+(43) = E$, of degree 6, where E is the elliptic curve 43a1 of rank 1.

Proposition 4.1. $\text{gon}_{\mathbb{Q}} X = 7$.

The Castelnuovo–Severi inequality does not help here: the maps to $X_0(43)$ (genus 3, degree 3) and to E (degree 6) exclude nothing in degrees 2 to 6. Over $\mathbb{F}_2$ the gonality is 5 and over $\mathbb{F}_5$ it is 4; we use $p = 3$, where X has good reduction.

Proof. The upper bound is the divisor above. For the lower bound, let $J = \text{Jac } X$, and let $c = C_3$ be the base point of the Abel–Jacobi map.

Step 1: over $\mathbb{F}_3$. **CAGonality** gives $\text{gon}_{\mathbb{F}_3} X_{\mathbb{F}_3} = 6$, so by Theorem 2.1 there is no function of degree at most 5 over $\mathbb{Q}$. Here $n = \lceil 4/4 \rceil = 1$, and testing the 845 effective divisors of degree 6 over $\mathbb{F}_3$ containing a rational place shows that exactly four have $\ell \geq 2$, and that they are linearly equivalent. So $W_6^1(X_{\mathbb{F}_3})(\mathbb{F}_3)$ is a single class T , and $T - 6c$ has order 1596 in $J(\mathbb{F}_3)$, a group of order 19152.

Step 2: the rational points of J . Let $A = \pi^*E \subseteq J$ and $B = J/A$. The pullback π^* is injective: a nontrivial kernel would make π factor through an isogeny onto E of degree dividing 6, but 43a1 has no rational cyclic isogeny and $E(\mathbb{Q})_{\text{tors}} = 0$. So $A(\mathbb{Q}) \cong E(\mathbb{Q}) \cong \mathbb{Z}$. The abelian variety B is isogenous to a product of modular abelian varieties of dimensions 2, 2 and 4 whose L -values at 1 are nonzero (exact modular-symbol computations of L -ratios 2/7, 3/16, 1/361); by Kato [27, Corollary 14.3], $B(\mathbb{Q})$ is finite. Its order divides $\gcd_p \#B(\mathbb{F}_p)$ over odd primes $p \neq 43$, since reduction is injective on rational torsion at such primes [28, Appendix]; the gcd over $p = 3, 5, 23$ is already 532. (Point counts are invariant under isogeny, so we may compute them on the modular abelian variety isogenous to B .) On the other hand, the subgroup $\mathcal{C} \subseteq J(\mathbb{Q})$ generated by $[C_2 - C_1]$, $[C_3 - C_1]$ and $[C_{(3)} - 3C_3]$ is finite (its generators are torsion, as checked below; this is also an instance of the theorem of Manin and Drinfeld [32, 17]), of order at least 532 (its

reduction modulo 3 has order 532), and it meets $A(\mathbb{Q})$ trivially, as $A(\mathbb{Q})$ is torsion-free. So $\mathcal{C}$ maps isomorphically onto $B(\mathbb{Q})$, and

$$J(\mathbb{Q}) = A(\mathbb{Q}) + \mathcal{C}.$$

Step 3: conclusion. Let $H_3 \subseteq J(\mathbb{F}_3)$ be the subgroup generated by $\pi^*E(\mathbb{F}_3)$ and the reduction of $\mathcal{C}$. It has order 3192, and $T - 6c \notin H_3$. If $f: X \rightarrow \mathbb{P}^1$ had degree 6 over $\mathbb{Q}$, the class of $L = f^*\mathcal{O}(1)$ would satisfy $[L - 6c] \in J(\mathbb{Q})$, so its reduction would lie in H_3 ; but by Theorem 2.1 the reduction of L is a degree-6 class with two sections, that is T . This contradiction shows $\text{gon}_{\mathbb{Q}} X \geq 7$. $\square$

Remark 4.2. The saturation in Step 2 cannot be avoided: $J(\mathbb{F}_3)$ has cyclic 3-part, and the 3-component of $T - 6c$ lies in $\pi^*E(\mathbb{F}_3)$, so $T - 6c \notin H_3$ only because of its 2-, 7- and 19-parts. In particular the coarser statement “ $532 \cdot J(\mathbb{Q}) \subseteq A(\mathbb{Q})$ ” would not suffice.

The certificate for Theorem 4.1 runs in about 12 seconds; the computations of L -ratios and of $\#B(\mathbb{F}_p)$ take a few minutes. The scripts work with the LMFDB model of X , its map to $X_0(43)$ and its cusps; the script `identify_model.m` shows that this model is isomorphic over $\mathbb{Q}$ to the MD Sage model, by an explicit linear change of coordinates (found by matching points over $\mathbb{F}_{101}$ and $\mathbb{F}_{103}$, and checked exactly). The three classes generating $\mathcal{C}$ are certified to be torsion directly over $\mathbb{Q}$ (`torsion_classes.m`): with $D_1 = C_2 - C_1$, $D_2 = C_3 - C_1$ and $E = C_{(3)} - (C_1 + C_2 + C_3)$, the divisors $38D_1$, $38D_2$ and $7E$ are principal, and $C_{(3)} - 3C_3 = E + D_1 - 2D_2$. So the proof does not depend on knowing that these points are cusps.

5. GONALITY OF $X_1(N)$: PROOF OF THEOREM D

Proof of Theorem D. Upper bounds. Derickx and van Hoeij [16, Table 1] give, for each N , a modular unit on $X_1(N)$ over $\mathbb{Q}$ whose degree is the value in Theorem D; it is also the degree in y of the plane model of [40], i.e. the degree of the coordinate function x .

Lower bounds. Let u be the value in Theorem D and $d = u - 1$. For $N = 48$ see §5.1. For the other N we apply Method II to $X_1(N)$ at the prime p of Table 1, which does not divide N ; §2 explains why the reduction of the plane model of [40] computes $X_1(N)_{\mathbb{F}_p}$, and we check its genus. Phase 1 is CurveArith’s: the places of degree at most $R = d - \min(n, d - 1)$ and the expansions of a basis of holomorphic differentials at them, with CurveArith’s precisions. Phase 2 is the search of §3.3 over the family $\mathcal{F}_b(d)$. In every case it finds no function of degree at most d . By Theorem 3.3 and Theorem 3.4, $\text{gon}_{\mathbb{F}_p} X_1(N)_{\mathbb{F}_p} > d$, and by Theorem 2.1, $\text{gon}_{\mathbb{Q}} X_1(N) \geq u$. $\square$

TABLE 1. Theorem D: Method II for $X_1(N)$. $n = \lceil N_1/(p+1) \rceil$; places up to degree $R = d - \min(n, d - 1)$; b the baseline; $\#\mathcal{F}_b(d)$ the number of divisors searched. Time: Phase 1 (its longest process, on a shared machine) + Phase 2.

N	g	p	d	N_1	n	R	places	b	$\#\mathcal{F}_b(d)$	time
41	51	2	21	20	7	14	2669	2	2643150	171 min + 14 s
42	25	5	11	12	2	9	277397	1	3860784	648 min + 153 s
43	57	2	23	21	7	16	8515	2	17156720	367 min + 50 s
44	36	3	14	15	4	10	9518	1	3133892	49 min + 25 s
45	41	2	17	12	4	13	1608	2	265608	86 min + 1 s
46	45	3	18	22	6	12	69995	1	374417725	884 min + 950 s
47	70	2	28	23	8	20	110354	2	651609964	1813 min + 3565 s
49	69	2	20	21	7	13	1497	2	2167431	207 min + 13 s
50	48	3	14	20	5	9	3369	2	41835	161 min + 1 s

The second phase also counts the divisors it tests and compares the total with an independent count of $\#\mathcal{F}_b(d)$ computed from the numbers of places of each degree; they agree in every case. As a check of the whole pipeline, the same programs reproduce $\text{gon}_{\mathbb{F}_2} X_1(29) = 11$ (degree 10 is excluded after testing 8568 divisors, and a function of degree 11 is found). For $X_1(47)$, an independent earlier computation, with a different implementation of the first phase (a different enumeration of places and expansions), tested exactly the same number 651,609,964 of divisors and also found no function of degree at most 28.

5.1. The level 48: a double cover. For $N = 48$ Method II over $\mathbb{F}_5$ or $\mathbb{F}_7$ would need all places of degree up to 12, which is out of reach. We use instead the quotient of $X = X_1(48)$ by the diamond operator $\langle 23 \rangle$, an involution; the quotient is $Y = X_{\{\pm 1, \pm 23\}}(48)$, of genus 13, and X has genus 37. Everything is computed on Y .

Let k be a finite field of odd characteristic, and $\pi: X \rightarrow Y$ a morphism of degree 2 of smooth curves over k , the quotient by an involution σ . For a function a on Y write $\pi^*a = a \circ \pi$; these are exactly the σ -invariant functions on X . Fix a function w on X with $\sigma w = -w$; then $w^2 = \pi^*\delta$ for a function δ on Y . Write $\text{div}_Y \delta = B - 2H$ with B the sum of the branch points, so that $c := \deg H = \frac{1}{2} \deg B = g_X - 2g_Y + 1$. (For a hyperelliptic curve $w^2 = \delta(x)$ over $Y = \mathbb{P}^1$, all of this is classical: every function is $a(x) + b(x)w$.)

Lemma 5.1. (1) *Every function f on X is uniquely $f = \pi^*a + \pi^*b \cdot w$ with a, b functions on Y , and f comes from Y if and only if $b = 0$.*
(2) *Put $t = 2a$ and $n = a^2 - b^2\delta$. Then $f + \sigma f = \pi^*t$, $f \cdot \sigma f = \pi^*n$, and for every place P of Y the total pole order of f above P is $\deg P \cdot \max(0, -v_P(t), -v_P(n))$. In particular $\deg_X f \geq \deg_Y n$ and $\deg_X f \geq \deg_Y t$.*
(3) *If $\deg_X f = d$ and $b \neq 0$, there are an effective divisor E on Y of degree $d - c$ and $u \neq 0$, h in $L_Y(E + H)$ with $f = (\pi^*h + w)/\pi^*u$.*

Proof. (1) Take $\pi^*a = (f + \sigma f)/2$ and $\pi^*b = (f - \sigma f)/(2w)$, both σ -invariant. (2) The first two identities are direct. Measure the orders of the two values of f above P in units of v_P , say α, β (if a single ramified point Q lies above P , then $\alpha = \beta = v_Q(f)/2$; if a single unramified point Q of degree $2 \deg P$ lies above P , then $\alpha = \beta = v_Q(f)$). The pole order above P is $\deg P(\max(0, -\alpha) + \max(0, -\beta))$, while $v_P(n) = \alpha + \beta$ and $v_P(t) \geq \min(\alpha, \beta)$ with equality if $\alpha \neq \beta$. If $\alpha, \beta \geq 0$ both sides vanish; if $\alpha < 0 \leq \beta$ then $v_P(t) = \alpha \leq v_P(n)$ and both sides are $-\alpha$; if $\alpha, \beta < 0$ then $v_P(n) < v_P(t)$ and both sides are $-\alpha - \beta$. (3) Since $\text{div}_X w = R - \pi^*H$ with R the ramification divisor, for every divisor A on Y the poles of f are bounded by π^*A if and only if $a \in L_Y(A)$ and $b \in L_Y(A - H)$. Take $A = \pi_*$ of the pole divisor of f , of degree d , and $E = \text{div } b + A - H \geq 0$, $u = 1/b$, $h = a/b$. $\square$

Proposition 5.2. *X has no nonconstant function of degree at most m if $2 \text{gon}_k Y > m$ and, for every effective divisor E on Y of degree $m - c$, every $u \neq 0$ and every h in $L_Y(E + H)$, the function $(\pi^*h + w)/\pi^*u$ has degree $> m$.*

Proof. Functions with $b = 0$ are π^*a , of degree $2 \deg_Y a$. For the others use Theorem 5.1(3) and enlarge E by $m - d$ points, which only enlarges $L_Y(E + H)$. $\square$

For $X_1(48)$ we take $k = \mathbb{F}_7$ and $m = 15$, so $c = 12$ and E has degree 3. The diamond operator $\langle 23 \rangle$ is defined over $\mathbb{Q}$ and extends to the smooth model of $X_1(48)$ over $\mathbb{Z}_{(7)}$; since 2 is invertible, the quotient commutes with base change, so $Y_{\mathbb{F}_7} = X_1(48)_{\mathbb{F}_7}/\langle 23 \rangle$ is the reduction of Y . We use MD Sage's canonical model of Y (coordinates $y_0, \dots, y_{12}$, a basis of $S_2(\Gamma_Y)$ with integral q -expansions, $y_0 = q + O(q^2)$), checked to have good reduction at 7 as in §2. Let $\psi \in S_2(\Gamma_1(48))$ have integral q -expansion, nonzero modulo 7, with $\langle 23 \rangle \psi = -\psi$, and put $w = \psi/y_0$, a function on $X_1(48)$ with $\sigma w = -w$. Then $\delta = w^2 = \psi^2/y_0^2$ is a ratio of two forms of weight 8 on Y ,

$\delta = \text{Nm}(y)/\text{Dn}(y)$, from an identity $\psi^2 \text{Dn}(y) = y_0^2 \text{Nm}(y)$ with integral coefficients checked to the Sturm bound. Reducing modulo 7, $\bar{w}$ is a function on $X_1(48)_{\mathbb{F}_7}$ with $\sigma\bar{w} = -\bar{w}$ and $\bar{w}^2 = \bar{\delta}$, so the function field of $X_1(48)_{\mathbb{F}_7}$ is $\mathbb{F}_7(Y)(\sqrt{\bar{\delta}})$; as a check, Magma computes its genus as 37. **CAGonality** gives $\text{gon}_{\mathbb{F}_7} Y = 8$, so $2 \text{gon} Y = 16 > 15$. There are 1328 effective divisors E of degree 3 on $Y_{\mathbb{F}_7}$; each $L_Y(E + H)$ has dimension 3, giving 57 choices of u up to scalars and 49 of h modulo u , and 3,709,104 functions in all. The bound $\deg_X f \geq \deg_Y n$ of Theorem 5.1(2) excludes all but 18 of them, and for those the exact degree, computed on Y , is at least 16. Hence $\text{gon}_{\mathbb{F}_7} X_1(48) > 15$, and $\text{gon}_{\mathbb{Q}} X_1(48) = 16$ by Theorem 2.1. The divisors E are split into parts by a key that depends only on E (not on the order in which Magma lists places), so the parts cover every E exactly once; the longest part took 12.5 hours. The degree formula of Theorem 5.1(2) was checked against Magma's degree computation on X itself for a sample of the candidates, and the whole procedure was tested on $X_1(24)$ and $X_1(26)$, where it reproduces the known gonality.

6. POINTS OF DEGREE 5 ON $X_0(N)$: PROOF OF THEOREM A

Let $C = X_0(N)$ for one of the thirty levels of Theorem A, of genus g , and $J = \text{Jac } C$. The rational cusp ∞ identifies $\text{Pic}^5(C)$ with J . For $r \geq 0$ let $W_5^r \subseteq \text{Pic}^5(C)$ be the locus of classes with $h^0 \geq r + 1$. Table 2 lists, for every level, the argument for each of the two assertions of Theorem A.

6.1. The framework.

Lemma 6.1. *If C has no function of degree 5 over $\mathbb{Q}$, then the points of degree 5 inject into $W_5^0(\mathbb{Q})$, and a point of degree 5 is the unique effective divisor in its class.*

Proof. If D is a point of degree 5 and $h^0(D) \geq 2$, a nonconstant $f \in L(D)$ over $\mathbb{Q}$ has a nonzero rational pole divisor bounded by D ; since D is irreducible, it equals D , so $\deg f = 5$. $\square$

Up to isogeny, J is a product of modular abelian varieties. Let $\mathcal{A} \subseteq J$ be the sum of the isotypic components whose L -function vanishes at $s = 1$; the vanishing is decided by exact modular-symbol computations. By Kolyvagin and Logachev [30], $(J/\mathcal{A})(\mathbb{Q})$ is finite. By Faltings [18], the Zariski closure of $W_5^0(\mathbb{Q})$ is a finite union of translates of abelian subvarieties; a positive-dimensional component with dense rational points has its direction in $\mathcal{A}$. So it suffices to show, in addition to excluding functions of degree 5, that every positive-dimensional translate $T \subseteq W_5^0$ with $T(\mathbb{Q})$ dense has a fixed proper subdivisor on its locus with $h^0 = 1$: then only finitely many classes can contain an irreducible divisor.

At each working prime $p \nmid N$ we check that the reduction of Magma's canonical model is an integral curve of arithmetic genus g , with normalization of genus g and a rational point (§2), and we enumerate all effective divisors of degree 5 over $\mathbb{F}_p$, for every partition of 5 into degrees of places. If $x + B \subseteq W_5^0$ over $\mathbb{Q}$, then the reduction contains the entire coset $\bar{x} + B(\mathbb{F}_p)$ in $W_5^0(\mathbb{F}_p)$.

Lemma 6.2 (Local rigidity). *Let $R = \mathbb{Z}_p$, let Z be a closed subscheme of a scheme smooth over R , and let $U \rightarrow Z$ be a morphism from a smooth R -scheme of relative dimension n . Let $u \mapsto z$ be rational points of the special fibres. If $\dim T_z Z_{\mathbb{F}_p} = n$ and $T_u U_{\mathbb{F}_p} \rightarrow T_z Z_{\mathbb{F}_p}$ is an isomorphism, then $U \rightarrow Z$ induces an isomorphism of completed local rings at u and z .*

Proof. Lifting cotangent generators gives a surjection $R[[x_1, \dots, x_n]] \rightarrow \hat{\mathcal{O}}_{Z,z}$; its composite with $\hat{\mathcal{O}}_{Z,z} \rightarrow \hat{\mathcal{O}}_{U,u} \cong R[[t_1, \dots, t_n]]$ has invertible linear part modulo p , so it is an isomorphism, and the surjection is injective. $\square$

We apply this to $Z_S = \bigcap_{s \in S} (W_5^0 - s)$ for a finite subgroup $S \subseteq J(\mathbb{F}_p)$, after lifting S to $J(\mathbb{Z}_p)$: prime-to- p torsion points lift uniquely to torsion points over $\mathbb{Z}_p$ (and if S lies in the reduction of both a candidate direction and a known abelian subvariety B , the lifts lie in both); when the

direction is already known to be B , we may lift points of $B(\mathbb{F}_p)$ arbitrarily to $B(\mathbb{Z}_p)$, including p -primary points, since both families are stable under all of B . At a class with $h^0(D) = 1$ the annihilator of $T_{[D]}W_5^0$ in $H^0(K_C)$ is $H^0(K_C - D)$, and at a class with $h^0 \geq 2$ the tangent space is everything. A known family $V \subseteq W_5^0$ defined over $\mathbb{Q}$ which fills the local branch then contains every candidate translate through that residue class. (For the tangent space of W_5^1 and the base-point-free pencil trick used below see [2, Chapter IV].)

6.2. Excluding functions of degree 5. *The double-cover inequality.* If C has an involution w with quotient of genus h and $g > 2h + 4$, a morphism of degree 5 cannot exist, even over $\overline{\mathbb{Q}}$, by Theorem 2.2 (the degrees 2 and 5 are coprime). This applies to 17 levels (Table 2). For 12 of them, namely 83, 89, 92, 101, 107, 111, 131, 141, 142, 143, 167, 191, these levels are already excluded in [10, Proposition 5.2] (for 142, 143, 167, 191 via a map of degree 4 to $\mathbb{P}^1$); it is new for 118, 123, 145, 155, 159.

Published gonality. $\text{gon}_{\mathbb{Q}} X_0(82) = 6$ [33, Theorem 1.4].

Empty special loci. At $N = 86, 99, 128$ and $p = 7, 5, 3$ respectively, the numbers of effective divisors of degree 5 over $\mathbb{F}_p$ and of their classes are equal, so $W_5^1(\mathbb{F}_p) = \emptyset$, and Theorem 2.1 applies.

Local pencils. At $N = 77, 85, 88$ the curve has $\mathbb{Q}$ -gonality 4 [33, Theorem 1.2]. At $p = 5, 7, 3$, every special divisor of degree 5 has $h^0 = 2$ and is $A_4 + P$ for the unique class A_4 of degree 4 with two sections, and $\dim T_{[D]}W_5^1 = 8 - g + h^0(K - D - A_4) = 1$ (the base-point-free pencil trick). The rational tetragonal pencil reduces to a class of degree 4 with two sections, which must be A_4 (an extra section would give a class of degree 5 with $h^0 \geq 3$ after adding a rational point); so it lifts A_4 , the Abel map $P \mapsto A_4 + P$ is an immersion, and Theorem 6.2 identifies W_5^1 near every relevant point with this family. Its sections come from A_4 , so a rational class in W_5^1 has a base point. Level 74 uses the same argument at the two primes 3 and 5. The possible positive-rank part A is isogenous to E_{37}^2 , and the rank-zero quotient $R = J/A$ has $\#R(\mathbb{Q})$ dividing 513 (the gcd of its point counts at $q \leq 31$). Since $\#E_{37}(\mathbb{F}_3) = 7$ and $\#E_{37}(\mathbb{F}_5) = 8$, $A(\mathbb{F}_3)$ is a 7-group and $A(\mathbb{F}_5)$ a 2-group, so $A(\mathbb{Q})_{\text{tors}}$, which injects into both, is trivial. The four rational cusps generate a torsion group $\mathcal{C}$ whose reductions modulo 3 and 5 have order 513; it meets the torsion-free $A(\mathbb{Q})$ trivially, so it maps onto $R(\mathbb{Q})$, and every rational class lies in $\mathcal{C} + A(\mathbb{Q})$, whose reduction lies in $\bar{\mathcal{C}} + A(\mathbb{F}_p) \subseteq \bar{\mathcal{C}} + J(\mathbb{F}_p)[\ell^\infty]$ with $\ell = 7, 2$. At $p = 3$ (using $J(\mathbb{F}_3)[7^\infty]$, of order 49) and at $p = 5$ (using $J(\mathbb{F}_5)[2^\infty]$, of order 256) the local pencil argument applies outside two exceptional cusp labels each, and the exceptional labels at the two primes are disjoint; so every rational class is covered at one of the primes.

The remaining levels are treated with the finiteness argument below: rank-zero lifting at 96, 98, 100 and the quotient sieve at 79, 103.

6.3. Route R: direct reduction. *Rank zero* (96, 98, 100). Here $L(J, 1) \neq 0$, so $J(\mathbb{Q})$ is finite and reduction is injective on it at the odd good primes $p = 7, 3, 3$. This is the situation of [34, Proposition 5.5]. The computation shows that every special class of degree 5 over $\mathbb{F}_p$ has $h^0 = 2$ and is $\bar{A}_4 + \bar{P}$ for a class $\bar{A}_4$ of degree 4 with two sections and a point $\bar{P} \in C(\mathbb{F}_p)$, and it lifts every such $\bar{A}_4$ to a rational class A_4 . At 96 and 100 every point of $C(\mathbb{F}_p)$ is the reduction of a rational point P , and injectivity forces a rational special class to be $A_4 + P$, which has the base point P . At 98 only four of the six points of $C(\mathbb{F}_3)$ (the cusps) lift. If L is a rational special class, then $L - A_4$ is a rational class of degree 1 whose reduction is $\bar{P}$; its push-forward along the degeneracy map $X_0(98) \rightarrow X_0(49) = E$ is a point of $E(\mathbb{Q}) \cong \mathbb{Z}/2$ reducing to the image of $\bar{P}$. For a noncuspidal $\bar{P}$ that image is a noncuspidal point of $E(\mathbb{F}_3) \cong \mathbb{Z}/4$ (degeneracy maps send noncusps to noncusps), of order 4, which is not the reduction of a point of $E(\mathbb{Q})$. So $\bar{P}$ is a cusp, and $L = A_4 + P$ with a fixed rational cusp P .

Empty cosets (85, 88, 92). Here $\mathcal{A}$ is simple, of dimension 2, 1, 1. At $p = 3$, the ℓ -primary subgroup of $\mathcal{A}(\mathbb{F}_3)$, for $\ell = 17, 7, 7$, has no full coset inside $W_5^0(\mathbb{F}_3)$; so no translate exists.

6.4. Route Q: a rank-zero quotient (nine prime levels). For $N \in \{79, 83, 89, 101, 103, 107, 131, 167, 191\}$ let $Y = C/w_N$, $A = \pi^* \text{Jac } Y$ and $R = J/A$; here $\mathcal{A} = A$ is simple of multiplicity one and R has rank 0. With $t = [w_N(\infty) - \infty]$, the gcd m of $\#R(\mathbb{F}_q)$ over $q \leq 19$ odd equals the order of $\bar{t}$ in $R(\mathbb{F}_p)$ at the working prime, so $R(\mathbb{Q}) = \langle t \rangle$ is cyclic of order m . Every rational class of degree 5 lies on some $T_i = [5\infty] + it + A$, $0 \leq i < m$, and only the following indices survive the coset test over $\mathbb{F}_p$: $i \in \{1, 2, 3, 4\}$ for $N = 79, 89, 101, 131$; $\{1, 2, 3, 4, 23\}$ for $N = 83$; $\{2, 3\}$ for $N = 103, 107, 167, 191$. For $g(Y) = 1$ these are the families $\pi^* \text{Pic}^1(Y) + 3P$, $\pi^* \text{Pic}^2(Y) + P$, $\pi^* \text{Pic}^2(Y) + Q$, $\pi^* \text{Pic}^1(Y) + 3Q$ with $P = \infty$, $Q = w_N(\infty)$, and for $g(Y) = 2$ only the middle two. The cusp is a fixed subdivisor: if D contains no full fibre of π and $d + \deg D < g - 2g(Y) + 1$, then $H^0(C, \pi^* M(D)) = H^0(Y, M)$ for every M of degree d . At $N = 83$ the index 23 is the family $\pi^* \text{Pic}^1(Y) + D$ through an explicit w_{83} -fixed cubic point D : with $F = \infty + w_{83}(\infty)$ and $c = [F + D - 5\infty]$, invariance of $F + D$ under w_{83} , which acts as -1 on R , gives $2c = 5t$ in $R(\mathbb{Q}) \cong \mathbb{Z}/41$, so $c = 23t$; the fixed subdivisor is D . At 79 and 103 the same sieve shows that all classes of $W_5^1(\mathbb{F}_p)$ lie over the indices 2, 3, whose families have fixed cusps; so there is no function of degree 5.

6.5. Route T: known families (fifteen levels). For the remaining levels, C has a double cover $C \rightarrow Y$ with $g(Y) = 2$ or a map of degree 4 to a curve of genus 1, giving a family $V = B + [F_4] + C \subseteq W_5^0$ with B the pulled-back Jacobian and F_4 a fibre (or twice a fibre). For every tested subgroup S and every full coset $x + S \subseteq W_5^0(\mathbb{F}_p)$, the certificate checks (Table 8) that $S \subseteq B(\mathbb{F}_p)$, that $x + S \subseteq B(\mathbb{F}_p) + [F_4] + C(\mathbb{F}_p)$, that $\dim T_x Z_S = \dim B + 1$, and that the differential of $B \times C \rightarrow \text{Pic}^5(C)$ has rank $\dim B + 1$. The subgroups tested cover every possible direction in $\mathcal{A}$: for each prime order $\ell \neq p$ tested, every simple factor of $\mathcal{A}$ has Frobenius order divisible by some tested ℓ , and all subgroups of that order in $J(\mathbb{F}_p)$ are tested. At 82, 99, 128 the unique positive elliptic part is identified with B through its newform, so the whole of $B(\mathbb{F}_p)$ may be used. At 86 the repeated elliptic factor is isogenous to $E_{43}: y^2 + y = x^3 + x^2$, which has no rational 2-isogeny, so every curve in its isogeny class is linked to it by an odd-degree isogeny and has cyclic group of order 8 over $\mathbb{F}_7$; all 192 cyclic subgroups of order 8 of $J(\mathbb{F}_7)$ are tested. By Theorem 6.2, every translate T lies in V . Projecting to J/B , which has dimension > 1 , shows $T \subseteq B + [F_4] + P$ for a fixed point P , whose Galois orbit is then a proper fixed subdivisor.

Proof of Theorem A. Combine the function exclusions with the three routes, as in Table 2. The 36 certificates are in the accompanying repository (`certificates/A_x0_quintic`), with a list of the data per level. $\square$

7. POINTS OF DEGREE 5 ON INTERMEDIATE CURVES: PROOF OF THEOREM B

7.1. Reduction to finitely many curves.

Lemma 7.1 (Projection). *Let $C \rightarrow D$ be a finite morphism over $\mathbb{Q}$. If D has only finitely many points of degree 1 and of degree 5, then C has only finitely many points of degree 5.*

Proof. The image of a point of degree 5 has degree dividing 5, and fibres are finite. $\square$

Forgetful maps $X_\Delta(N) \rightarrow X_{\Delta'}(M)$, for $M \mid N$ and Δ mapping into Δ' , are defined over $\mathbb{Q}$; in particular every $X_\Delta(N)$ maps to $X_0(N)$. By Theorem A and [10, Theorem 1.10], $X_0(N)$ has finitely many points of degree 5 unless

$$N \in \{1, \dots, 45\} \cup \{47, \dots, 58\} \cup \{61, 63, 64, 65, 67, 68, 72, 73, 75, 80, 81, 91, 109, 121, 125\},$$

TABLE 2. Theorem A: the thirty levels. The route proves finiteness of the points of degree 5 assuming there is no function of degree 5; the last column is the separate argument excluding functions of degree 5 (“double cover”: the inequality $g > 2h + 4$).

N	g	route	degree-5 functions	N	g	route	degree-5 functions
74	8	T	local pencil, 2 primes	107	9	Q	double cover
77	7	T	local pencil	111	11	T	double cover
79	6	Q	quotient sieve	118	14	T	double cover
82	9	T	[33]	123	13	T	double cover
83	7	Q	double cover	128	9	T	$W_5^1(\mathbb{F}_3) = \emptyset$
85	7	R	local pencil	131	11	Q	double cover
86	10	T	$W_5^1(\mathbb{F}_7) = \emptyset$	141	15	T	double cover
88	9	R	local pencil	142	17	T	double cover
89	7	Q	double cover	143	13	T	double cover
92	10	R	double cover	145	13	T	double cover
96	9	R	rank zero	155	15	T	double cover
98	7	R	rank zero	159	17	T	double cover
99	9	T	$W_5^1(\mathbb{F}_5) = \emptyset$	167	14	Q	double cover
100	7	R	rank zero	191	16	Q	double cover
101	8	Q	double cover				
103	8	Q	quotient sieve				

and every $X_0(N)$ with N outside this list has genus > 1 (otherwise its rational cusp would give a function of degree 5, §3.1), hence finitely many rational points by Faltings [18]; so these $X_0(N)$ can serve as targets in Theorem 7.1. So every strict pair with $N \geq 192$, and 807 of the 1011 strict pairs with $N \leq 191$, have finitely many points of degree 5. The strict pairs with $N \leq 191$ are enumerated twice, once from primitive rows (c, d) modulo N up to Δ and once with Sage’s **GammaH**; full sets of elements, not orders or genera, are used to identify them. Seven more pairs map to intermediate curves already shown to be negative (Table 6), and fifteen more, of genus 57 to 256, satisfy $119\mu > 120000$, so they have $\text{gon}_{\mathbb{C}} > 10$ and finitely many points of degree 5 by Theorem 2.5 and [14, Proposition 2.2]. This leaves 182 strict pairs.

7.2. The 43 positive curves. Each curve in Table 4 has a function of degree 5 over $\mathbb{Q}$, hence infinitely many points of degree 5 (Theorem 2.4):

- L (13 curves, $g \leq 2$): for a rational cusp P , $\ell(5P) = 6 - g > \ell(4P)$;
- K (14 curves, $g = 3, 4$): in genus 3, 5 is not a Weierstrass gap at the cusp ∞ (read off from the orders of vanishing of a basis of cusp forms); in genus 4 the curve is not hyperelliptic (the quadrics in the canonical ideal have the right rank), so $K - P$ is base-point free of degree 5;
- W (12 curves): an explicit divisor D of degree 5 with $\ell(D) = 2$ and no base point, on a canonical model certified through the Sturm bound and a Hilbert polynomial comparison;
- P (4 curves): the $\mathbb{Q}$ -pentagonal curves of [36, Theorems 1.4–1.5].

7.3. The negative curves. For the remaining 139 curves we show finiteness. The arguments are listed by code in Table 5.

Lemma 7.2 (Rank zero). *If $C(\mathbb{Q}) \neq \emptyset$, $J(C)(\mathbb{Q})$ is finite and C has no function of degree 5 over $\mathbb{Q}$, then C has finitely many points of degree 5.*

Proof. As in Theorem 6.1, each point of degree 5 is the unique effective divisor in its class, and there are finitely many classes. $\square$

Rank zero (82 curves). We show $J(\mathbb{Q})$ finite from nonvanishing L -values (exact modular-symbol L -ratios), using Kato [27, Corollary 14.3] as applied to modular Jacobians with nontrivial character in [14, §4]. The absence of a function of degree 5 comes from

- Z (74 curves) Orlic's classification: genus ≥ 5 and not in Orlic's lists of curves of $\mathbb{Q}$ -gonality at most 5, so $\text{gon}_{\mathbb{Q}} \geq 6$ [36];
- B (2 curves, $35\langle -1, 8 \rangle$ and $55\langle -1, 4 \rangle$, of genus 7 and 9) the curves are bielliptic [25, Theorem 0.2], so a function of degree 5 would violate Theorem 2.2: $g \leq 2 + 4 = 6$;
- T (3 curves) Petri lifting: over $\mathbb{F}_p$ every class of W_5^1 is $A + P$ for an explicit rational base-point free class A of degree 4, with Petri tangent dimension 1; Theorem 6.2 identifies W_5^1 near each such class with the Abel curve $A + C$, so a rational pencil of degree 5 has a base point;
- R (3 curves) a complete sieve of rational divisor classes: an explicit subgroup of $J(\mathbb{Q})$ generated by differences of rational points is shown to be all of $J(\mathbb{Q})$, and every class of $W_5^1(\mathbb{F}_p)$ in its reduction is lifted and checked over $\mathbb{Q}$. At level 40 the explicit subgroup has order 4032, and $\#J(\mathbb{Q})$ is bounded above by the Hecke method of [9, §4.3]: rational torsion is fixed by complex conjugation, and for $\ell \nmid 40$ the Eichler–Shimura relation shows that $1 - T_\ell + \ell\langle \ell \rangle$ kills rational torsion of order prime to ℓ ; both operators act on the integral homology, computed from Manin symbols. Since the relation at ℓ says nothing about ℓ -primary torsion, for each $\ell \in \{3, 7, 11, 13\}$ we bound the ℓ -primary part using only the relations at the other three primes, and the remaining primary parts using all four; each of these computations gives a group of order $8064 = 2^7 \cdot 3^2 \cdot 7$. Point counts over finite fields give $\#J(\mathbb{Q}) \mid 28224$, so $\#J(\mathbb{Q}) \mid \gcd(8064, 28224) = 4032$; at level 48 the bounds 2304 and 12800 come from the description of $J_1(48)(\mathbb{Q})_{\text{tors}}$ by cuspidal divisors [9, Theorem 4.13], transferred along the forgetful map.

Positive rank (57 curves). None of these curves has a function of degree 5 over $\mathbb{Q}$: they have genus at least 8 and are not in the classification of curves of $\mathbb{Q}$ -gonality at most 5 [22, 24], [36, Theorems 1.3–1.5], except $43\langle -1, 2 \rangle$, which has $\mathbb{Q}$ -gonality 7 by Theorem 4.1. Here we use the classification of curves with infinitely many points of degree at most 4 [13, Theorems 1.4–1.6]: none of these curves has infinitely many points of degree ≤ 4 , so if it had infinitely many points of degree 5, its minimum density degree $\min \delta(X/\mathbb{Q})$ would be 5. By Kadets and Vogt [26, Theorem 1.3], applied with $d = 5$ (so $m = \lceil d/2 \rceil - 1 = 2$ and $\varepsilon = 3d - 1 - 6m = 2$), either $g \leq \max(d(d-1)/2 + 1, 3m(m-1) + m\varepsilon) = 11$, or there is a morphism $X \rightarrow Y$ of degree 5 to a curve Y with infinitely many rational points, that is, to $\mathbb{P}^1$ or to an elliptic curve of positive rank. So for $g \geq 12$ it suffices to exclude these two kinds of maps. For $9 \leq g \leq 11$, the classification of curves of minimum density degree 5 [26, Proposition 6.3 and Table 1] leaves, besides these covers (and curves of genus at most 8), only normalizations of Debarre–Fahlaoui curves: the points may then come from a curve in $\text{Sym}^2 E$ of class $(5+j)H - jF$ with $1 \leq j \leq 5$ (Debarre–Fahlaoui [6], [26, Definition 5.1]); adjunction gives arithmetic genus $11 - j(j-1)/2$, so $j \leq 2$ and the addition map to E has degree 6 or 7.

- E (43 curves, genus ≥ 12 , so only elliptic maps of degree 5 need to be excluded) every positive-rank elliptic factor E has conductor N , multiplicity one and odd analytic rank, and for $N \leq 800$ the parametrization through $X_0(N)$ is optimal [13, Corollary 4.10]; so every morphism $X_\Delta(N) \rightarrow E'$ with E' isogenous to E has degree divisible by $t \cdot d_E$, where $t = [(\mathbb{Z}/N\mathbb{Z})^\times : \Delta]$ and d_E is the optimal modular degree, and $t, d_E > 1$ in all these cases (Table 10; see also [13, Corollary 4.12]); so $t d_E$ is composite and the degree is not 5;

- E0 (5 curves, at levels 109 and 125) the decomposition of the Jacobian has no positive-rank elliptic factor;
- D (3 curves of genus 9 or 10: $37\langle -1, 10 \rangle$, $57\langle -1, 2 \rangle$, $73\langle -1, 6 \rangle$) here a Debarre–Fahlaoui configuration must also be excluded, that is, elliptic maps of degree 5, 6 or 7: at level 73 there is no positive-rank elliptic factor, and at levels 37 and 57 every elliptic map of positive rank has degree at least 12 and 8 respectively [13, Corollary 4.10];
- C (1 curve, $43\langle -1, 2 \rangle$) the only possibly positive-rank factor is an elliptic curve A ; at $p = 2$, $A(\mathbb{F}_2)$ has order 5, and no full coset of it lies in $W_5^0(\mathbb{F}_2)$, which has 2133 elements. A positive-dimensional translate in W_5^0 over $\mathbb{Q}$ would reduce to such a coset (prime-to-2 torsion specializes injectively), so $W_5^0(\mathbb{Q})$ is finite;
- F (5 curves, levels 53, 61, 65) there is a map $f: C \rightarrow E$ of degree 4 whose pullback is the positive-rank part A , and the surface $Z = \{f^*Q + P\}$ of reducible divisors lies in W_5^0 . At a good odd prime p , with $B = A(\mathbb{F}_p)$, we check that every full B -coset in $W_5^0(\mathbb{F}_p)$ lies in Z , that the intersection of the corresponding tangent spaces has dimension at most 2, and that $A \times C \rightarrow \text{Pic}^5 C$ has injective differential at the relevant points. Since $f_*f^* = [4]$ and p is odd, A has a smooth model over $\mathbb{Z}_p$; lifting B to $A(\mathbb{Z}_p)$ and applying Theorem 6.2 puts every rational translate of A in W_5^0 into Z . A point of degree 5 in Z would be $f^*Q + P$ with a unique, hence rational, point P , which is impossible.

Proof of Theorem B. The 43 positive curves, the 139 curves above, the 7 further projections, the 15 curves with large index and the 807 projections to $X_0(N)$ account for all 1011 strict pairs with $N \leq 191$, and projection to $X_0(N)$ handles $N \geq 192$. $\square$

Proof of Corollary E. The 39 positive curves other than Orlic’s four $\mathbb{Q}$ -pentagonal curves have $\mathbb{Q}$ -gonality at most 4: those of genus $g \leq 4$ have a rational cusp, so $\text{gon}_{\mathbb{Q}} \leq \max(g, 2) \leq 4$ (§3.1), and the twelve curves of type W are $\mathbb{Q}$ -tetragonal [36, Theorem 1.3]. By Theorem 2.4 they have density degree at most 4. The four pentagonal curves have genus 6, 6, 8 and 16, so finitely many rational points by Faltings [18], and none of them occurs in the lists of [13, Theorems 1.4, 1.5 and 1.6] of curves with infinitely many points of degree 2, 3 or 4. By Theorem B they have infinitely many points of degree 5. $\square$

Every case has a certificate or a precise citation in the accompanying repository (`certificates/B_intermediate_quintic`), which also contains the full case list.

8. COMPUTATIONS

All computations use Magma V2.29-4 [4], SageMath 10.7 with MD Sage [8] (commit 6022429), CurveArith [15] (commit b7c6192) and Zywin’s package [44] (commit ce31d78); the three packages are pinned as git submodules of the accompanying repository. The repository is organized by theorem:

folder	contents
data/	one row per curve: bounds, methods, certificates or citations
certificates/A_x0_quintic/	Theorem A: 36 Magma certificates and logs
certificates/B_intermediate_quintic/	Theorem B and Corollary E: all 1388 pairs (N, Δ) , $N \leq 191$ (1011 strict)
certificates/C_intermediate_gonality/	Theorem C: models, CurveArith runs, upper-bound certificates
certificates/C_43.132.9.a.2/	Theorem 4.1
certificates/D_x1_gonality/	Theorem D: Phase 1 driver, Phase 2 program, logs
verify.py	checks that every row of data/ has a passing log or a citation

Method II for $X_1(N)$. Phase 1 is a short Magma script that loads CurveArith and calls its internal function `PrecomputePowerSeriesExpansions` with exactly the places and precisions that `CAHasFunctionOfDegreeAtMost` would use; no CurveArith code is modified. It runs in several Magma processes. Every process enumerates all places, as CurveArith does, and computes the expansions only at the places assigned to it: the place's key (the irreducible polynomial $g(t) \in \mathbb{F}_p[t]$ below it, encoded as an integer, or 0 at infinity) is hashed by a fixed integer function, and the hash determines the process. This assignment does not depend on the order in which Magma lists the places, so the processes together treat every place exactly once; the merge checks that the counts add up, and that the processes agree on the curve, the place counts and the basis of differentials. (Splitting by position in the list instead is not safe: Magma does not always list the places in the same order in different processes.) Its output is the list of matrices of Theorem 3.1.

Phase 2 is a C++ program of about 1000 lines (with GMP) that enumerates $\mathcal{F}_b(d)$, performs the incremental Gaussian elimination of §3.3 over $\mathbb{F}_p$, and enumerates the kernel vectors up to scalars (Theorem 3.4). It is a reimplementaion, for speed, of the option `A1:="Cover"` of a modified CurveArith, which we used to cross-check it on small curves. The baseline b is chosen to minimize the number of divisors times the size of the kernels. For any b the result is correct; it only affects the running time.

Validation. The pipeline was tested in both directions against CurveArith's unmodified `CAGonality`: on $X_1(26)$ over $\mathbb{F}_3, \mathbb{F}_5, \mathbb{F}_7$ and on $X_1(29)$ over $\mathbb{F}_2, \mathbb{F}_3$, it finds no function of degree $\text{gon}_{\mathbb{F}_p} - 1$ and finds one of degree $\text{gon}_{\mathbb{F}_p}$. When a function is found, its divisor is checked independently by a rank computation. Each Phase 1 process also computes a few Riemann–Roch dimensions with Magma's `Dimension`, for divisors supported on its own places; Phase 2 checks them against Theorem 3.1 before searching.

Running times. The 36 certificates of Theorem A take 40 minutes of CPU time in total, the longest ($N = 86$) 16 minutes. The certificates of Theorem 4.1 take a few minutes. The lower bounds of Theorem C take about 2 hours in total, dominated by 48.384.19.bc.1 (66 minutes). The running times for Theorem D are in Table 1.

Acknowledgements. The computations rest on software written by others: I thank Maarten Derickx for MD Sage and for permission to build on its code, Maarten Derickx and Kenji Terao for CurveArith, Andrew Sutherland and Mark van Hoeij for their optimized models of $X_1(N)$, David Zywna for his Magma package for modular curves, and the LMFDB collaboration, whose database was used to find examples and to name curves; its model of one curve is used in

Theorem 4.1, and otherwise the LMFDB is not a source of proofs. I thank Petar Orlić for the tables of [36], on which much of this paper builds.

Use of AI tools. Large language model assistants (OpenAI’s GPT-6 Astra, through Codex, and Anthropic’s Claude, through Claude Code) were used to write and optimize code, to organize the certificates, and to draft parts of the text. The proofs are built to be checked without trusting these tools: each step is a cited published result, a short argument written out in full, or a computation backed by a certificate in the accompanying repository that can be rerun independently. The author takes responsibility for the content of this paper.

REFERENCES

1. Dan Abramovich, *A linear lower bound on the gonality of modular curves*, Internat. Math. Res. Notices (1996), no. 20, 1005–1011.
2. E. Arbarello, M. Cornalba, P. A. Griffiths, and J. Harris, *Geometry of algebraic curves. Vol. I*, Grundlehren der mathematischen Wissenschaften, vol. 267, Springer-Verlag, New York, 1985.
3. Francesc Bars, *Bielliptic modular curves*, J. Number Theory **76** (1999), 154–165.
4. Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), 235–265.
5. Tarun Dalal, *Intermediate modular curves with infinitely many cubic points over $\mathbb{Q}$* , Int. J. Number Theory **20** (2024), no. 3, 701–713.
6. Olivier Debarre and Rachid Fahlouai, *Abelian varieties in $W_d^r(C)$ and points of bounded degree on algebraic curves*, Compositio Math. **88** (1993), 235–249.
7. P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*, Modular functions of one variable, II, Lecture Notes in Math., vol. 349, Springer, Berlin, 1973, pp. 143–316.
8. Maarten Derickx, *MD Sage: a SageMath package for modular curves*, <https://github.com/koffie/mdsage>, commit 6022429.
9. Maarten Derickx, Anastassia Etropolski, Mark van Hoeij, Jackson S. Morrow, and David Zureick-Brown, *Sporadic cubic torsion*, Algebra Number Theory **15** (2021), no. 7, 1837–1864.
10. Maarten Derickx, Wontae Hwang, Daeyeol Jeon, and Petar Orlić, *Modular curves $X_0(N)$ of density degree 5*, Math. Comp. (2026), published electronically 27 July 2026, doi:10.1090/mcom/4221, arXiv:2503.08975.
11. Maarten Derickx and Filip Najman, *Hyperelliptic and trigonal modular curves in characteristic p* , Q. J. Math. **76** (2025), no. 1, 1–18.
12. Maarten Derickx and Petar Orlić, *Modular curves $X_0(N)$ with infinitely many quartic points*, Res. Number Theory **10** (2024), no. 2, Paper No. 42.
13. ———, *Intermediate modular curves with infinitely many quartic points*, Int. J. Number Theory **22** (2026), no. 5, 1053–1074.
14. Maarten Derickx and Andrew V. Sutherland, *Torsion subgroups of elliptic curves over quintic and sextic number fields*, Proc. Amer. Math. Soc. **145** (2017), no. 10, 4233–4245.
15. Maarten Derickx and Kenji Terao, *Computing class groups and gonalitys of algebraic curves over finite fields*, 2026, arXiv:2602.17417; software CurveArith, <https://github.com/nt-lib/CurveArith>.
16. Maarten Derickx and Mark van Hoeij, *Gonality of the modular curve $X_1(N)$* , J. Algebra **417** (2014), 52–71.
17. V. G. Drinfeld, *Two theorems on modular curves*, Funkcional. Anal. i Priložen. **7** (1973), no. 2, 83–84.
18. Gerd Faltings, *Diophantine approximation on abelian varieties*, Ann. of Math. (2) **133** (1991), 549–576.
19. Gerhard Frey, *Curves with infinitely many points of fixed degree*, Israel J. Math. **85** (1994), 79–83.
20. Robin Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics, vol. 52, Springer-Verlag, New York-Heidelberg, 1977.
21. Wontae Hwang and Daeyeol Jeon, *Modular curves with infinitely many quartic points*, Math. Comp. **93** (2024), 383–395.
22. Noburo Ishii and Fumiyuki Momose, *Hyperelliptic modular curves*, Tsukuba J. Math. **15** (1991), no. 2, 413–423.
23. Daeyeol Jeon, *Modular curves with infinitely many cubic points*, J. Number Theory **219** (2021), 344–355.
24. Daeyeol Jeon and Chang Heon Kim, *On the arithmetic of certain modular curves*, Acta Arith. **130** (2007), 181–193.
25. Daeyeol Jeon, Chang Heon Kim, and Andreas Schweizer, *Bielliptic intermediate modular curves*, J. Pure Appl. Algebra **224** (2020), no. 1, 272–299.
26. Borys Kadets and Isabel Vogt, *Subspace configurations and low degree points on curves*, Adv. Math. **460** (2025), Paper No. 110021.

27. Kazuya Kato, *p-adic Hodge theory and values of zeta functions of modular forms*, Astérisque **295** (2004), 117–290.
28. Nicholas M. Katz, *Galois properties of torsion points on abelian varieties*, Invent. Math. **62** (1981), 481–502.
29. Henry H. Kim, *Functoriality for the exterior square of GL_4 and the symmetric fourth of GL_2* , J. Amer. Math. Soc. **16** (2003), 139–183, With Appendix 1 by D. Ramakrishnan and Appendix 2 by H. Kim and P. Sarnak.
30. V. A. Kolyvagin and D. Yu. Logachëv, *Finiteness of the Shafarevich–Tate group and the group of rational points for some modular abelian varieties*, Leningrad Math. J. **1** (1990), 1229–1253.
31. Qing Liu, *Algebraic geometry and arithmetic curves*, Oxford Graduate Texts in Mathematics, vol. 6, Oxford University Press, Oxford, 2002.
32. Ju. I. Manin, *Parabolic points and zeta functions of modular curves*, Izv. Akad. Nauk SSSR Ser. Mat. **36** (1972), 19–66.
33. Filip Najman and Petar Orlić, *Gonality of the modular curve $X_0(N)$* , Math. Comp. **93** (2024), 863–886.
34. Filip Najman and Marin Varivoda, *Torsion groups of elliptic curves that appear infinitely often over septic, octic and nonic fields*, 2026, arXiv:2602.03513v4.
35. Andrew P. Ogg, *Hyperelliptic modular curves*, Bull. Soc. Math. France **102** (1974), 449–462.
36. Petar Orlić, *Tetragonal intermediate modular curves*, Acta Arith. **220** (2025), 263–288.
37. Bjorn Poonen, *Gonality of modular curves in characteristic p* , Math. Res. Lett. **14** (2007), 691–701.
38. Jeremy Rouse, Andrew V. Sutherland, and David Zureick-Brown, *ℓ -adic images of Galois for elliptic curves over $\mathbb{Q}$* , Forum Math. Sigma **10** (2022), e62, With an appendix by John Voight.
39. Henning Stichtenoth, *Algebraic function fields and codes*, second ed., Graduate Texts in Mathematics, vol. 254, Springer-Verlag, Berlin, 2009.
40. Andrew V. Sutherland, *Optimized equations for $X_1(N)$* , https://math.mit.edu/~drew/X1_optcurves.html, models of Sutherland and van Hoeij.
41. ———, *Constructing elliptic curves over finite fields with prescribed torsion*, Math. Comp. **81** (2012), no. 278, 1131–1147.
42. The LMFDB Collaboration, *The L-functions and modular forms database*, <https://www.lmfdb.org>, 2026.
43. Mark van Hoeij, *Low degree places on the modular curve $X_1(N)$* , 2012, arXiv:1202.4355; the places are in the data files on the author’s web page.
44. David Zywina, *Modular: a Magma package for modular forms and modular curves*, <https://github.com/davidzywina/Modular>, commit ce31d78.

APPENDIX A. TABLES

Table 3: $\mathbb{Q}$ -gonality of the strict curves $X_\Delta(N)$, $N \leq 50$.
Lower and upper bound: method (§3), or “genus” for $g \leq 1$
or the low-genus arguments of §3.1. For $N \leq 40$ and $g \geq 3$
both bounds are from [36, Theorem 1.2, Table 1].

label	Δ	g	$\text{gon}_{\mathbb{Q}}$	lower bound	upper bound
13.28.0.a.1	$\langle -1, 3 \rangle$	0	1	genus	genus
13.42.0.a.2	$\langle -1, 5 \rangle$	0	1	genus	genus
15.48.1.a.1	$\langle -1, 4 \rangle$	1	2	genus	genus
16.48.0.v.1	$\langle -1, 7 \rangle$	0	1	genus	genus
17.36.1.a.2	$\langle -1, 2 \rangle$	1	2	genus	genus
17.72.1.a.2	$\langle -1, 4 \rangle$	1	2	genus	genus
19.60.1.a.2	$\langle -1, 7 \rangle$	1	2	genus	genus
20.72.1.f.2	$\langle -1, 9 \rangle$	1	2	genus	genus
21.64.1.a.3	$\langle -1, 4 \rangle$	1	2	genus	genus
21.96.3.a.1	$\langle -1, 8 \rangle$	3	2	[36]	[36]
24.96.1.dg.2	$\langle -1, 11 \rangle$	1	2	genus	genus
24.96.3.ge.2	$\langle -1, 5 \rangle$	3	3	[36]	[36]
24.96.3.gi.1	$\langle -1, 7 \rangle$	3	3	[36]	[36]
25.60.0.a.1	$\langle -1, 4 \rangle$	0	1	genus	genus

label	Δ	g	$\text{gon}_{\mathbb{Q}}$	lower bound	upper bound
25.150.4.f.1	$\langle -1, 7 \rangle$	4	4	[36]	[36]
26.84.4.a.1	$\langle -1, 3 \rangle$	4	3	[36]	[36]
26.126.4.a.1	$\langle -1, 5 \rangle$	4	3	[36]	[36]
27.108.1.a.1	$\langle -1, 8 \rangle$	1	2	genus	genus
28.96.4.c.4	$\langle -1, 3 \rangle$	4	3	[36]	[36]
28.144.4.d.1	$\langle -1, 13 \rangle$	4	3	[36]	[36]
29.60.4.a.1	$\langle -1, 4 \rangle$	4	3	[36]	[36]
29.210.8.b.2	$\langle -1, 12 \rangle$	8	6	[36]	[36]
30.144.5.a.1	$\langle -1, 11 \rangle$	5	4	[36]	[36]
31.96.6.a.1	$\langle -1, 2 \rangle$	6	5	[36]	[36]
31.160.6.c.1	$\langle -1, 5 \rangle$	6	5	[36]	[36]
32.96.1.f.1	$\langle -1, 7 \rangle$	1	2	genus	genus
32.192.5.bu.1	$\langle -1, 15 \rangle$	5	4	[36]	[36]
33.96.5.a.4	$\langle -1, 2 \rangle$	5	4	[36]	[36]
33.240.11.a.1	$\langle -1, 10 \rangle$	11	6	[36]	[36]
34.108.5.a.2	$\langle -1, 9 \rangle$	5	4	[36]	[36]
34.216.9.a.1	$\langle -1, 13 \rangle$	9	6	[36]	[36]
35.96.5.a.2	$\langle -1, 4 \rangle$	5	4	[36]	[36]
35.144.7.a.2	$\langle -1, 8 \rangle$	7	4	[36]	[36]
35.192.9.b.3	$\langle -1, 11 \rangle$	9	6	[36]	[36]
35.288.13.a.2	$\langle -1, 6 \rangle$	13	8	[36]	[36]
36.144.3.c.1	$\langle -1, 11 \rangle$	3	3	[36]	[36]
36.216.7.u.1	$\langle -1, 17 \rangle$	7	4	[36]	[36]
37.76.4.a.2	$\langle -1, 3 \rangle$	4	3	[36]	[36]
37.114.4.b.1	$\langle -1, 8 \rangle$	4	3	[36]	[36]
37.228.10.a.2	$\langle -1, 10 \rangle$	10	6	[36]	[36]
37.342.16.c.2	$\langle -1, 6 \rangle$	16	9	[36]	[36]
38.180.10.a.1	$\langle -1, 7 \rangle$	10	6	[36]	[36]
39.112.5.a.2	$\langle -1, 4 \rangle$	5	4	[36]	[36]
39.168.9.a.1	$\langle -1, 5 \rangle$	9	4	[36]	[36]
39.224.9.a.3	$\langle -1, 16 \rangle$	9	6	[36]	[36]
39.336.17.c.1	$\langle -1, 14 \rangle$	17	8	[36]	[36]
40.144.5.gn.1	$\langle -1, 9, 11 \rangle$	5	4	[36]	[36]
40.144.7.fp.1	$\langle -1, 3 \rangle$	7	4	[36]	[36]
40.144.7.fs.1	$\langle -1, 7 \rangle$	7	4	[36]	[36]
40.288.13.sp.1	$\langle -1, 9 \rangle$	13	8	[36]	[36]
40.288.13.sq.2	$\langle -1, 11 \rangle$	13	7	[36]	[36]
40.288.9.bh.1	$\langle -1, 19 \rangle$	9	6	[36]	[36]
41.84.5.a.1	$\langle -1, 2 \rangle$	5	4	II, $p = 3$	I (pullback)
41.168.11.b.1	$\langle -1, 4 \rangle$	11	6	II, $p = 2$	I (cusps)
41.210.11.b.1	$\langle -1, 3 \rangle$	11	8	II, $p = 5$	I (cusps)
41.420.21.d.1	$\langle -1, 9 \rangle$	21	11	II, $p = 2$	I (cusps)
42.192.9.c.2	$\langle -1, 5 \rangle$	9	6	II, $p = 5$	I (pullback)
42.288.13.a.1	$\langle -1, 13 \rangle$	13	6	II, $p = 5$	I (pullback)
43.132.9.a.2	$\langle -1, 2 \rangle$	9	7	II+III, $p = 3$	I (special)
43.308.15.b.1	$\langle -1, 6 \rangle$	15	9	II, $p = 2$	I (special)
44.144.8.c.4	$\langle -1, 5 \rangle$	8	5	II, $p = 3$	[36]

label	Δ	g	$\text{gon}_{\mathbb{Q}}$	lower bound	upper bound
44.360.16.e.1	$\langle -1, 21 \rangle$	16	8	II, $p = 3$	I (pullback)
45.144.5.a.1	$\langle -1, 4 \rangle$	5	4	II, $p = 2$	[36]
45.216.11.d.2	$\langle -1, 8 \rangle$	11	6	II, $p = 2$	I (pullback)
45.288.9.a.4	$\langle -1, 14 \rangle$	9	6	II, $p = 2$	I (pullback)
45.432.21.g.2	$\langle -1, 19 \rangle$	21	10	II, $p = 2$	I (cusps)
48.192.5.ky.2	$\langle -1, 11 \rangle$	5	4	II, $p = 5$	I (pullback)
48.192.7.hj.1	$\langle -1, 5 \rangle$	7	4	II, $p = 5$	I (pullback)
48.192.7.ho.1	$\langle -1, 7, 17 \rangle$	7	4	II, $p = 5$	I (pullback)
48.384.13.nt.1	$\langle -1, 23 \rangle$	13	8	II, $p = 7$	I (pullback)
48.384.19.bc.1	$\langle -1, 7 \rangle$	19	8	II, $p = 7$	I (pullback)
48.384.19.bj.1	$\langle -1, 17 \rangle$	19	8	II, $p = 5$	I (pullback)
49.168.3.b.1	$\langle -1, 6 \rangle$	3	3	genus	genus
49.392.19.i.2	$\langle -1, 18 \rangle$	19	11	II, $p = 2$	I (cusps)
50.180.4.a.2	$\langle -1, 9 \rangle$	4	3	genus	I (pullback)
50.450.22.f.1	$\langle -1, 7 \rangle$	22	10	II, $p = 3$	I (pullback)

Table 4: Positive strict intermediate pairs.

N	Generators of Δ	g	Proof
13	$\langle -1, 3 \rangle$	0	L
13	$\langle -1, 5 \rangle$	0	L
15	$\langle -1, 4 \rangle$	1	L
16	$\langle -1, 7 \rangle$	0	L
17	$\langle -1, 2 \rangle$	1	L
17	$\langle -1, 4 \rangle$	1	L
19	$\langle -1, 7 \rangle$	1	L
20	$\langle -1, 9 \rangle$	1	L
21	$\langle -1, 4 \rangle$	1	L
21	$\langle -1, 8 \rangle$	3	K
24	$\langle -1, 5 \rangle$	3	K
24	$\langle -1, 7 \rangle$	3	K
24	$\langle -1, 11 \rangle$	1	L
25	$\langle -1, 4 \rangle$	0	L
25	$\langle -1, 7 \rangle$	4	K
26	$\langle -1, 3 \rangle$	4	K
26	$\langle -1, 5 \rangle$	4	K
27	$\langle -1, 8 \rangle$	1	L
28	$\langle -1, 3 \rangle$	4	K
28	$\langle -1, 13 \rangle$	4	K
29	$\langle -1, 4 \rangle$	4	K
30	$\langle -1, 11 \rangle$	5	W
31	$\langle -1, 2 \rangle$	6	P
31	$\langle -1, 5 \rangle$	6	P
32	$\langle -1, 7 \rangle$	1	L
32	$\langle -1, 15 \rangle$	5	W
33	$\langle -1, 2 \rangle$	5	W
34	$\langle -1, 9 \rangle$	5	W
35	$\langle -1, 4 \rangle$	5	W

N	Generators of Δ	g	Proof
36	$\langle -1, 11 \rangle$	3	K
37	$\langle -1, 3 \rangle$	4	K
37	$\langle -1, 8 \rangle$	4	K
39	$\langle -1, 4 \rangle$	5	W
40	$\langle -1, 7 \rangle$	7	W
40	$\langle -1, 9, 11 \rangle$	5	W
41	$\langle -1, 2 \rangle$	5	W
44	$\langle -1, 5 \rangle$	8	P
45	$\langle -1, 4 \rangle$	5	W
48	$\langle -1, 11 \rangle$	5	W
49	$\langle -1, 6 \rangle$	3	K
50	$\langle -1, 9 \rangle$	4	K
64	$\langle -1, 7 \rangle$	5	W
125	$\langle -1, 4 \rangle$	16	P

Table 5: All direct negative assignments (excluding projection).

N	Generators of Δ	g	μ	Proof
29	$\langle -1, 12 \rangle$	8	210	Z
33	$\langle -1, 10 \rangle$	11	240	Z
34	$\langle -1, 13 \rangle$	9	216	Z
35	$\langle -1, 8 \rangle$	7	144	B
35	$\langle -1, 11 \rangle$	9	192	Z
35	$\langle -1, 6 \rangle$	13	288	Z
36	$\langle -1, 17 \rangle$	7	216	T
37	$\langle -1, 10 \rangle$	10	228	D
37	$\langle -1, 6 \rangle$	16	342	E
38	$\langle -1, 7 \rangle$	10	180	Z
39	$\langle -1, 5 \rangle$	9	168	T
39	$\langle -1, 16 \rangle$	9	224	Z
39	$\langle -1, 14 \rangle$	17	336	Z
40	$\langle -1, 3 \rangle$	7	144	R
40	$\langle -1, 9 \rangle$	13	288	Z
40	$\langle -1, 11 \rangle$	13	288	Z
40	$\langle -1, 19 \rangle$	9	288	Z
41	$\langle -1, 4 \rangle$	11	168	Z
41	$\langle -1, 3 \rangle$	11	210	Z
41	$\langle -1, 9 \rangle$	21	420	Z
42	$\langle -1, 5 \rangle$	9	192	Z
42	$\langle -1, 13 \rangle$	13	288	Z
43	$\langle -1, 2 \rangle$	9	132	C
43	$\langle -1, 6 \rangle$	15	308	E
44	$\langle -1, 21 \rangle$	16	360	Z
45	$\langle -1, 8 \rangle$	11	216	Z
45	$\langle -1, 14 \rangle$	9	288	Z
45	$\langle -1, 19 \rangle$	21	432	Z
48	$\langle -1, 5 \rangle$	7	192	R
48	$\langle -1, 7, 17 \rangle$	7	192	R
48	$\langle -1, 7 \rangle$	19	384	Z
48	$\langle -1, 17 \rangle$	19	384	Z

N	Generators of Δ	g	μ	Proof
48	$\langle -1, 23 \rangle$	13	384	Z
49	$\langle -1, 18 \rangle$	19	392	Z
50	$\langle -1, 7 \rangle$	22	450	Z
51	$\langle -1, 2 \rangle$	9	144	Z
51	$\langle -1, 4 \rangle$	17	288	Z
51	$\langle -1, 16 \rangle$	33	576	Z
52	$\langle -1, 3 \rangle$	9	168	Z
52	$\langle -1, 5 \rangle$	13	252	Z
52	$\langle -1, 9 \rangle$	19	336	Z
52	$\langle -1, 25 \rangle$	25	504	Z
53	$\langle -1, 4 \rangle$	8	108	F
53	$\langle -1, 23 \rangle$	40	702	E
54	$\langle -1, 17 \rangle$	10	324	Z
55	$\langle -1, 4 \rangle$	9	144	B
55	$\langle -1, 16 \rangle$	17	288	Z
55	$\langle -1, 12 \rangle$	21	360	Z
55	$\langle -1, 21 \rangle$	41	720	Z
56	$\langle -1, 3 \rangle$	9	192	Z
56	$\langle -1, 5 \rangle$	11	192	Z
56	$\langle -1, 17 \rangle$	11	192	Z
56	$\langle -1, 13, 15 \rangle$	13	288	Z
56	$\langle -1, 9 \rangle$	21	384	Z
56	$\langle -1, 13 \rangle$	31	576	Z
56	$\langle -1, 15 \rangle$	31	576	Z
56	$\langle -1, 27 \rangle$	25	576	Z
57	$\langle -1, 2 \rangle$	9	160	D
57	$\langle -1, 11 \rangle$	13	240	E
57	$\langle -1, 7 \rangle$	25	480	E
57	$\langle -1, 20 \rangle$	43	720	E
58	$\langle -1, 5 \rangle$	12	180	E
58	$\langle -1, 17 \rangle$	36	630	E
61	$\langle -1, 4 \rangle$	8	124	F
61	$\langle -1, 8 \rangle$	12	186	E
61	$\langle -1, 21 \rangle$	16	310	E
61	$\langle -1, 3 \rangle$	26	372	E
61	$\langle -1, 13 \rangle$	36	620	E
61	$\langle -1, 11 \rangle$	56	930	E
63	$\langle -1, 4, 5 \rangle$	9	192	Z
63	$\langle -1, 2 \rangle$	17	288	Z
63	$\langle -1, 11 \rangle$	17	288	Z
63	$\langle -1, 10 \rangle$	17	288	Z
63	$\langle -1, 13 \rangle$	13	288	Z
63	$\langle -1, 4 \rangle$	33	576	Z
63	$\langle -1, 17 \rangle$	33	576	Z
63	$\langle -1, 20 \rangle$	25	576	Z
63	$\langle -1, 8 \rangle$	49	864	Z
64	$\langle -1, 15 \rangle$	13	384	Z
64	$\langle -1, 31 \rangle$	37	768	Z
65	$\langle -1, 2, 7 \rangle$	9	168	F
65	$\langle -1, 3 \rangle$	11	168	F
65	$\langle -1, 6 \rangle$	11	168	F

N	Generators of Δ	g	μ	Proof
65	$\langle -1, 8, 12 \rangle$	13	252	E
65	$\langle -1, 2 \rangle$	19	336	E
65	$\langle -1, 7 \rangle$	19	336	E
65	$\langle -1, 9 \rangle$	21	336	E
65	$\langle -1, 8, 14 \rangle$	25	504	E
65	$\langle -1, 12 \rangle$	31	504	E
65	$\langle -1, 21 \rangle$	31	504	E
65	$\langle -1, 4 \rangle$	41	672	E
65	$\langle -1, 8 \rangle$	55	1008	E
65	$\langle -1, 14 \rangle$	61	1008	E
65	$\langle -1, 18 \rangle$	55	1008	E
67	$\langle -1, 3 \rangle$	15	204	E
67	$\langle -1, 29 \rangle$	45	748	E
68	$\langle -1, 9 \rangle$	13	216	Z
72	$\langle -1, 5 \rangle$	13	288	Z
72	$\langle -1, 7 \rangle$	13	288	Z
72	$\langle -1, 11 \rangle$	9	288	Z
72	$\langle -1, 17, 19 \rangle$	21	432	Z
72	$\langle -1, 23 \rangle$	25	576	Z
72	$\langle -1, 17 \rangle$	49	864	Z
72	$\langle -1, 19 \rangle$	49	864	Z
72	$\langle -1, 35 \rangle$	41	864	Z
73	$\langle -1, 6 \rangle$	9	148	D
73	$\langle -1, 7 \rangle$	13	222	E
73	$\langle -1, 2 \rangle$	19	296	E
73	$\langle -1, 3 \rangle$	25	444	E
73	$\langle -1, 10 \rangle$	43	666	E
73	$\langle -1, 8 \rangle$	55	888	E
73	$\langle -1, 27 \rangle$	85	1332	S
75	$\langle -1, 4 \rangle$	9	240	T
75	$\langle -1, 14 \rangle$	17	480	Z
75	$\langle -1, 7 \rangle$	37	600	Z
75	$\langle -1, 26 \rangle$	73	1200	S
80	$\langle -1, 3, 13 \rangle$	15	288	Z
80	$\langle -1, 7, 9 \rangle$	15	288	Z
80	$\langle -1, 9, 11 \rangle$	13	288	Z
80	$\langle -1, 7 \rangle$	35	576	Z
80	$\langle -1, 13 \rangle$	35	576	Z
80	$\langle -1, 17 \rangle$	35	576	Z
80	$\langle -1, 9 \rangle$	69	1152	S
80	$\langle -1, 31 \rangle$	69	1152	S
80	$\langle -1, 39 \rangle$	57	1152	S
81	$\langle -1, 8 \rangle$	10	324	Z
81	$\langle -1, 26 \rangle$	46	972	Z
91	$\langle -1, 3, 4 \rangle$	13	224	E
91	$\langle -1, 2 \rangle$	21	336	E
91	$\langle -1, 11 \rangle$	21	336	E
91	$\langle -1, 5 \rangle$	23	336	E
91	$\langle -1, 6 \rangle$	23	336	E
91	$\langle -1, 9, 12 \rangle$	25	448	E
91	$\langle -1, 3 \rangle$	41	672	E

N	Generators of Δ	g	μ	Proof
91	$\langle -1, 4 \rangle$	41	672	E
91	$\langle -1, 25 \rangle$	45	672	E
91	$\langle -1, 36 \rangle$	45	672	E
91	$\langle -1, 8 \rangle$	67	1008	E
91	$\langle -1, 9 \rangle$	81	1344	S
91	$\langle -1, 12 \rangle$	89	1344	S
91	$\langle -1, 16 \rangle$	81	1344	S
91	$\langle -1, 22 \rangle$	89	1344	S
91	$\langle -1, 27 \rangle$	133	2016	S
109	$\langle -1, 3 \rangle$	16	220	E0
109	$\langle -1, 2 \rangle$	22	330	E0
109	$\langle -1, 4 \rangle$	46	660	E0
109	$\langle -1, 8 \rangle$	64	990	E0
109	$\langle -1, 45 \rangle$	136	1980	S
109	$\langle -1, 33 \rangle$	208	2970	S
121	$\langle -1, 10 \rangle$	26	660	E
121	$\langle -1, 3 \rangle$	106	1452	S
125	$\langle -1, 7 \rangle$	36	750	E0
125	$\langle -1, 24 \rangle$	76	1500	S
125	$\langle -1, 57 \rangle$	256	3750	S

TABLE 6. Projections to intermediate curves (other than X_0) used in the proof of Theorem B.

N	Source generators	M	Target generators
63	$\langle -1, 5 \rangle$	63	$\langle -1, 4, 5 \rangle$
68	$\langle -1, 13 \rangle$	34	$\langle -1, 13 \rangle$
68	$\langle -1, 33 \rangle$	34	$\langle -1, 13 \rangle$
80	$\langle -1, 3 \rangle$	40	$\langle -1, 3 \rangle$
80	$\langle -1, 9, 31 \rangle$	40	$\langle -1, 3 \rangle$
80	$\langle -1, 11 \rangle$	40	$\langle -1, 11 \rangle$
80	$\langle -1, 19 \rangle$	40	$\langle -1, 19 \rangle$

DEPARTMENT OF MATHEMATICS, FACULTY OF SCIENCE, UNIVERSITY OF ZAGREB, BIJENIČKA CESTA 30, 10000 ZAGREB, CROATIA

Email address: `marin.varivoda@math.hr`

TABLE 7. The twelve exceptional negative certificates.

N	Generators of Δ	g	Method
36	$\langle -1, 17 \rangle$	7	Petri lifting
39	$\langle -1, 5 \rangle$	9	Petri lifting
40	$\langle -1, 3 \rangle$	7	Rational classes
43	$\langle -1, 2 \rangle$	9	Empty cosets
48	$\langle -1, 5 \rangle$	7	Rational classes
48	$\langle -1, 7, 17 \rangle$	7	Rational classes
53	$\langle -1, 4 \rangle$	8	Elliptic families
61	$\langle -1, 4 \rangle$	8	Elliptic families
65	$\langle -1, 2, 7 \rangle$	9	Elliptic families
65	$\langle -1, 3 \rangle$	11	Elliptic families
65	$\langle -1, 6 \rangle$	11	Elliptic families
75	$\langle -1, 4 \rangle$	9	Petri lifting

TABLE 8. Theorem A, Route T: the known family $V = B + [F_4] + C$, the subgroups S tested over $\mathbb{F}_p$, and the counts. “Divisors” and “classes” are the effective divisors of degree 5 over $\mathbb{F}_p$ and their classes.

N	p	quotient by	$\dim B$	$\#B(\mathbb{F}_p)$	subgroups tested	divisors	classes	cosets	$\dim TZ_S$
74	3	w_{74}	2	21	all of order 7	1340	1316	18	3
77	5	w_{77}	2	35	all of order 7	12528	12488	40	3
82	3	w_2, w_{41}	1	6	$B(\mathbb{F}_3)$	2574	2568	6	2
86	7	w_2, w_{43}	1	8	cyclic of order 8 (192)	64384	64384	12	2
99	5	w_9, w_{11}	1	10	$B(\mathbb{F}_5)$	8504	8504	6	2
111	2	w_{111}	2	15	all of order 5	328	320	12	3
118	3	w_2, w_{59}	1	5	all of order 5	3104	3104	6	2
123	2	w_3, w_{41}	1	3	order 3 or 5	842	842	6	2
128	3	$w_{128}, sw_{128}s^{-1}$	1	6	$B(\mathbb{F}_3)$	1812	1812	4	2
141	2	w_3, w_{47}	1	3	order 3 or 5	566	566	4	2
142	3	w_{71}	2	15	order 5 or 7	1668	1656	12	3
143	2	w_{143}	2	15	all of order 3	332	324	20	3
145	3	w_5, w_{29}	1	4	all of order 2	1552	1552	24	2
155	2	w_5, w_{31}	1	3	order 3 or 5	536	536	4	2
159	5	w_3, w_{53}	1	6	all of order 3	23476	23476	16	2

TABLE 9. Theorem A, Route Q: $Y = X_0(N)/w_N$, $A = \pi^* \text{Jac } Y$, $R = J/A$ with $R(\mathbb{Q})$ cyclic of order m , and the surviving indices i of the translates $T_i = [5\infty] + it + A$.

N	g	$g(Y)$	p	m	$\#A(\mathbb{F}_p)$	surviving i
79	6	1	3	13	5	1, 2, 3, 4
83	7	1	7	41	11	1, 2, 3, 4, 23
89	7	1	3	22	5	1, 2, 3, 4
101	8	1	5	25	7	1, 2, 3, 4
103	8	2	5	17	55	2, 3
107	9	2	3	53	29	2, 3
131	11	1	3	65	5	1, 2, 3, 4
167	14	2	3	83	19	2, 3
191	16	2	2	95	11	2, 3

TABLE 10. Theorem B, class E: for each level N and index $t = [(\mathbb{Z}/N\mathbb{Z})^\times : \Delta]$, the number of curves, their genera, the elliptic curves of conductor N with odd analytic rank, and their optimal modular degree d_E (Cremona's database). At $N = 67, 73$ there are none. Every positive-rank elliptic quotient has degree divisible by $t d_E$ [13, Corollary 4.10], which is composite, hence $\neq 5$.

N	t	curves	genera	E	d_E
37	9	1	16	37a1	2
43	7	1	15	43a1	2
53	13	1	40	53a1	2
57	3	1	13	57a1	4
57	6	1	25	57a1	4
57	9	1	43	57a1	4
58	2	1	12	58a1	4
58	7	1	36	58a1	4
61	3	1	12	61a1	2
61	5	1	16	61a1	2
61	6	1	26	61a1	2
61	10	1	36	61a1	2
61	15	1	56	61a1	2
65	3	1	13	65a1	2
65	4	3	19, 19, 21	65a1	2
65	6	3	25, 31, 31	65a1	2
65	8	1	41	65a1	2
65	12	3	55, 55, 61	65a1	2
67	3	1	15	—	—
67	11	1	45	—	—
73	3	1	13	—	—
73	4	1	19	—	—
73	6	1	25	—	—
73	9	1	43	—	—
73	12	1	55	—	—
91	2	1	13	91a1, 91b1	4
91	3	4	21, 21, 23, 23	91a1, 91b1	4
91	4	1	25	91a1, 91b1	4
91	6	4	41, 41, 45, 45	91a1, 91b1	4
91	9	1	67	91a1, 91b1	4
121	5	1	26	121b1	4