University of Zagreb

FACULTY OF SCIENCE

DEPARTMENT OF MATHEMATICS

Petar Orlić

Gonality of modular curves and their quotients

DOCTORAL DISSERTATION

Zagreb, 2025.

University of Zagreb

FACULTY OF SCIENCE

DEPARTMENT OF MATHEMATICS

Petar Orlić

Gonality of modular curves and their quotients

DOCTORAL DISSERTATION

Supervisor:

prof. dr. sc. Filip Najman

Zagreb, 2025.

Sveučilište u Zagrebu

PRIRODOSLOVNO–MATEMATIČKI FAKULTET
MATEMATIČKI ODSJEK

Petar Orlić

Gonalnost modularnih krivulja i njihovih kvocijenata

DOKTORSKI RAD

Mentor:

prof. dr. sc. Filip Najman

Zagreb, 2025.

ACKNOWLEDGEMENTS

I thank my advisor Filip Najman for his steady guidance, patience, many helpful comments, and productive cooperation throughout my doctoral studies.

I also thank Maarten Derickx for useful discussions and collaboration on our joint project.

The author is grateful for the support and funding from the QuantiXLie Center of Excellence, a project co-financed by the Croatian Government and European Union through the European Regional Development Fund - the Competitiveness and Cohesion Operational Programme (Grant KK.01.1.1.01.0004), and by the Croatian Science Foundation under the projects no. IP-2018-01-1313 and IP-2022-10-5008.

SUMMARY

Modular curves are one of the significant objects in number theory. One of their important properties is that points on modular curves represent classes of elliptic curves with some additional structure. Therefore, we can answer some questions regarding elliptic curves by studying modular curves.

The central topic of this thesis is the modular curve $X_0(N)$ and its quotient curves. Points on the curve $X_0(N)$ parametrize classes of elliptic curves together with a cyclic subgroup of order N (or equivalently, a cyclic isogeny of degree N).

For an algebraic curve defined over a field k, its k-gonality is the minimal possible degree of a morphism from that curve to the projective line $\mathbb{P}^1$. Problems concerning determining the $\mathbb{Q}$-gonality and $\mathbb{C}$-gonality of curves defined over $\mathbb{Q}$ are particularly interesting. One of the reasons for that is that preimages of degree d rational morphisms to $\mathbb{P}^1$ are the source of degree d points on curves.

All cases when the $\mathbb{C}$-gonality of the curve $X_0(N)$ is $2,3$, or 4 were determined by Ogg, Hasegawa and Shimura, and Jeon and Park in [37, 53, 80]. All $\mathbb{Q}$-trigonal curves $X_0(N)$ were also determined by Hasegawa and Shimura in the same paper. The author's paper in collaboration with Filip Najman [76] determines all cases when the $\mathbb{Q}$-gonality of the curve $X_0(N)$ is $4,5$, or 6. The $\mathbb{Q}$-gonality of all curves $X_0(N)$ for $N \leq 144$ is also determined there, along with the $\mathbb{C}$-gonality for many of these curves. These results can be found in Section 2.1.

For every divisor d of N such that $\gcd(d,N/d) = 1$ there exists an involution w_d on $X_0(N)$ defined over $\mathbb{Q}$, called an Atkin-Lehner involution. The curve $X_0^{+d}(N)$ is a quotient curve of the modular curve $X_0(N)$ by w_d. If $d = N$, we denote this curve as $X_0^+(N)$.

All cases when the $\mathbb{C}$-gonality of the curve $X_0^{+d}(N)$ is 2 or 3 were determined by Furumoto and Hasegawa and Hasegawa and Shimura in [32, 38]. The author's papers

[81, 83] determine all cases when the $\mathbb{Q}$-gonality of the curve $X_0^{+d}(N)$ is 3 or 4 and all cases when the $\mathbb{C}$-gonality of the curve $X_0^{+d}(N)$ is equal to 4. These results can be found in Section 2.2.

For every group $\{\pm 1\} \subsetneq \Delta \subsetneq (\mathbb{Z}/N\mathbb{Z})^\times$, there exists an intermediate modular curve $X_\Delta(N)$ between the curves $X_1(N)$ and $X_0(N)$. Since the $\mathbb{Q}$-gonality of curves $X_1(N)$ has been determined for $N \leq 40$ in [23] and we know the $\mathbb{Q}$-gonality of curves $X_0(N)$ for $N \leq 144$, the question of determininng the $\mathbb{Q}$-gonality of intermediate curves $X_\Delta(N)$ naturally arises.

All cases when the $\mathbb{C}$-gonality of the curve $X_\Delta(N)$ is 2 or 3 were determined by Ishii and Momose and Jeon and Kim in [43, 48]. The author's paper [82] determines all cases when the $\mathbb{Q}$-gonality of the curve $X_\Delta(N)$ is 4 or 5 and all cases when the $\mathbb{C}$-gonality of the curve $X_\Delta(N)$ is equal to 4. These results can be found in Section 2.3.

The existence of rational maps to $\mathbb{P}^1$ and elliptic curves is closely related to the existence of infinitely many points of a certain degree over $\mathbb{Q}$. Bars [6] determined all cases when the curve $X_0(N)$ has infinitely quadratic points and Jeon [45] determined all cases when the curve $X_0(N)$ has infinitely many cubic points. The author's paper in collaboration with Maarten Derickx [21] determines all cases when the curve $X_0(N)$ has infinitely many quartic points. These results can be found in Chapter 3.

A lot of the results in this thesis rely on `Magma` [11] and Sage computations. The codes that verify all computations in this thesis can be found on

`https://github.com/orlic1`

and

`https://github.com/koffie/mdsage/tree/main/articles/derickx_orlic-quartic_X0`.

Key words: Elliptic curve, Modular curves, Gonality

SAŽETAK

Modularne krivulje jedan su od značajnijih predmeta istraživanja u teoriji brojeva. Jedno od njihovih važnijih svojstava je to da točke na modularnim krivuljama reprezentiraju klase eliptičkih krivulja s nekom dodatnom strukturom. Stoga na neka pitanja koja se tiču eliptičkih krivulja možemo odgovoriti proučavajući modularne krivulje.

Središnji objekt ove disertacije je modularna krivulja $X_0(N)$ i njezine kvocijentne krivulje. Točke na krivulji $X_0(N)$ parametriziraju klase eliptičkih krivulja zajedno s cikličkom podgrupom reda N (ili ekvivalentno, s cikličkom izogenijom stupnja N).

Za algebarsku krivulju definiranu nad poljem k, njezina k-gonalnost je minimalni mogući stupanj preslikavanja iz te krivulje u projektivni pravac $\mathbb{P}^1$. Osobito su zanimljivi problemi određivanja $\mathbb{Q}$-gonalnosti i $\mathbb{C}$-gonalnosti krivulja definiranih nad $\mathbb{Q}$. Jedan od razloga za to što su praslike racionalnih preslikavanja stupnja d u $\mathbb{P}^1$ izvor točaka stupnja d nad $\mathbb{Q}$ na krivuljama.

Sve slučajeve kada je $\mathbb{C}$-gonalnost krivulje $X_0(N)$ jednaka $2,3$ ili 4 odredili su Ogg, Hasegawa i Shimura te Jeon i Park u [37, 53, 80]. Hasegawa i Shimura su u istom članku odredili i sve slučajeve kad je krivulja $X_0(N)$ $\mathbb{Q}$-trigonalna. Autorov članak u suradnji s Filipom Najmanom [76] određuje sve slučajeve kada je $\mathbb{Q}$-gonalnost krivulje $X_0(N)$ jednaka $4,5$ ili 6. $\mathbb{Q}$-gonalnost krivulja $X_0(N)$ za $N \leq 144$ je također određena u tom članku, kao i $\mathbb{C}$-gonalnost mnogih of tih krivulja. Ovi rezultati se mogu naći u Poglavlju 2.1.

Za svaki djelitelj d od N za koji je $M(d,N/d) = 1$ postoji involucija w_d krivulje $X_0(N)$ definirana nad $\mathbb{Q}$ koju zovemo Atkin-Lehnerova involucija. Krivulja $X_0^{+d}(N)$ je kvocijentna krivulja modularne krivulje $X_0(N)$ po w_d. Ako je $d = N$, označavamo ovu krivulju s $X_0^+(N)$.

Sve slučajeve kada je $\mathbb{C}$-gonalnost krivulje $X_0^{+d}(N)$ jednaka 2 ili 3 odredili su Furu-

moto i Hasegawa te Hasegawa i Shimura u [32, 38]. Autorovi članci [81, 83] određuju sve slučajeve kada je $\mathbb{Q}$-gonalnost krivulje $X_0^{+d}(N)$ jednaka 3 ili 4 te sve slučajeve kada je $\mathbb{C}$-gonalnost krivulje $X_0^{+d}(N)$ jednaka 4. Ovi rezultati se mogu naći u Poglavlju 2.2.

Za svaku grupu $\{\pm 1\} \subsetneq \Delta \subsetneq (\mathbb{Z}/N\mathbb{Z})^\times$ postoji modularna međukrivulja $X_\Delta(N)$ koja se nalazi između krivulja $X_1(N)$ i $X_0(N)$. Kako je $\mathbb{Q}$-gonalnost krivulja $X_1(N)$ određena za $N \leq 40$ u [23] i kako znamo kolika je $\mathbb{Q}$-gonalnost krivulja $X_0(N)$ za $N \leq 144$, prirodno se postavlja pitanje određivanja $\mathbb{Q}$-gonalnosti krivulja $X_\Delta(N)$.

Sve slučajeve kada je $\mathbb{C}$-gonalnost krivulje $X_\Delta(N)$ jednaka 2 ili 3 odredili su Ishii i Momose te Jeon i Kim u [43, 48]. Autorov članak [82] određuje sve slučajeve kada je $\mathbb{Q}$-gonalnost krivulje $X_\Delta(N)$ jednaka 4 ili 5 te sve slučajeve kada je $\mathbb{C}$-gonalnost krivulje $X_\Delta(N)$ jednaka 4. Ovi rezultati se mogu naći u Poglavlju 2.3.

Postojanje racionalnog preslikavanja u $\mathbb{P}^1$ i eliptičke krivulje je usko povezano s postojanjem beskonačno mnogo točaka određenog stupnja nad $\mathbb{Q}$. Bars [6] je odredio sve slučajeve kada krivulja $X_0(N)$ ima beskonačno mnogo kvadratnih točaka, a Jeon [45] je odredio sve slučajeve kada krivulja $X_0(N)$ ima beskonačno kubičnih točaka. Autorov članak u suradnji s Maartenom Derickxom [21] određuje sve slučajeve kada krivulja $X_0(N)$ ima beskonalno mnogo kvartičnih točaka. Ovi rezultati se mogu naći u Poglavlju 3.

Dosta rezultata u ovoj disertaciji se oslanja na izračune u računalnim sustavima `Magma` [11] i Sage. Kodovi koji opravdavaju sve izračune u ovoj disertaciji se nalaze na

`https://github.com/orlic1`

i

`https://github.com/koffie/mdsage/tree/main/articles/derickx_orlic-quartic_X0`.

Ključne riječi: Eliptičke krivulje, Modularne krivulje, Gonalnost

CONTENTS

1. INTRODUCTION

1.1. ELLIPTIC CURVES

Definition 1.1.1. Let k be a field. An elliptic curve over k is a smooth, projective, algebraic curve of genus 1 defined over k on which there is a specified k-rational point $\mathscr{O}$.

It is well known that every elliptic curve E has a model of the form

$$E : y^2z + a_1xyz + a_3yz^3 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3,$$

called the long Weierstrass model. Additionally, if char $k \neq 2,3$, then it also has a simpler model of the form

$$E : y^2z = x^3 + axz^2 + bz^3,$$

called the short Weierstrass model. Here $\mathscr{O}$ is the unique point at infinity $(0:1:0)$. The elliptic curve is required to be non-singular which is equivalent to the condition that the discriminant of the curve $\Delta(E)$ is non-zero. For elliptic curves in the long Weierstrass model the formula for $\Delta(E)$ is

$$\begin{aligned}\Delta(E) = &-(a_1^2+4a_2)^2(a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2) - 8(a_1a_3+2a_4)^3 - \\ &- 27(a_3^2+4a_6)^2 + 9(a_1^2+4a_2)(a_1a_3+2a_4)(a_3^2+4a_6).\end{aligned}$$

In the short Weierstrass model this just translates to $\Delta(E) = -16(4a^3+27b^2) \neq 0$. We

also define the j-invariant of an elliptic curve as

$$j(E) = \frac{((a_1^2+4a_2)^2 - 24(a_1a_3+2a_4))^3}{\Delta(E)}.$$

In the short Weierstrass form we have $j(E) = \dfrac{1728a^3}{4a^3+27b^2}$. The name j-invariant comes from the fact that the two elliptic curves over k are isomorphic over $\bar{k}$ if and only if their j-invariants are equal.

One of the characterizations of the genus of an algebraic curve is as follows. Every algebraic curve over $\mathbb{C}$ is as a Riemann surface homeomorphic to the sphere with g handles, where g is the genus of that curve. Therefore, every elliptic curve over $\mathbb{C}$ is homeomorphic to a torus.

On the set of k-rational points of E, denoted by $E(k)$, we can define the operation $+ : E(k) \times E(k) \to E(k)$. This operation is defined algebraically over k and with it $E(k)$ becomes an abelian group with an identity element $\mathcal{O}$. Moreover, we have the following result.

Theorem 1.1.2 (Mordell)**.** For an elliptic curve E defined over a number field k, the group $E(k)$ is a finitely generated abelian group.

This means that for an elliptic curve E over a number field k we have

$$E(k) \cong E(k)_{\text{tors}} \times \mathbb{Z}^r.$$

Here $E(k)_{\text{tors}}$ is a torsion group, i.e., the group of points of finite order, and r is the rank of E over k. It is natural to ask what are the possibilities for $E(k)_{\text{tors}}$ and r. All possible torsion groups have been determined for elliptic curves over $\mathbb{Q}$ and number fields of small degree.

Theorem 1.1.3 (Mazur [70])**.** Let E be an elliptic curve defined over $\mathbb{Q}$. Then the torsion group of $E(\mathbb{Q})$ is isomorphic to one of the following groups:

$$\begin{aligned} &\mathbb{Z}/m\mathbb{Z}, && m = 1,\ldots,10,12 \\ &\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}, && m = 1,2,3,4. \end{aligned}$$

Theorem 1.1.4 (Kamienny, Kenku, Momose [55,62])**.** Let E be an elliptic curve defined over a quadratic field k. Then the torsion group of $E(k)$ is isomorphic to one of the following groups:

$$\begin{aligned}
&\mathbb{Z}/m\mathbb{Z}, && m = 1,\dots,16,18\\
&\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2m\mathbb{Z}, && m = 1,\dots,6,\\
&\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3m\mathbb{Z}, && m = 1,2,\\
&\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}.
\end{aligned}$$

Theorem 1.1.5 (Derickx, Etropolski, van Hoeij, Morrow, Zureick-Brown [18])**.** Let E be an elliptic curve defined over a cubic field k. Then the torsion group of $E(k)$ is isomorphic to one of the following groups:

$$\begin{aligned}
&\mathbb{Z}/m\mathbb{Z}, && m = 1,\dots,16,18,20,21,\\
&\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2m\mathbb{Z}, && m = 1,\dots,7.
\end{aligned}$$

Theorem 1.1.6 (Derickx, Najman [19])**.** Let E be an elliptic curve defined over a quartic field k. Then the torsion group of $E(k)$ is isomorphic to one of the following groups:

$$\begin{aligned}
&\mathbb{Z}/m\mathbb{Z}, && m = 1,\dots,18,20,21,22,24\\
&\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2m\mathbb{Z}, && m = 1,\dots,9,\\
&\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3m\mathbb{Z}, && m = 1,2,3,\\
&\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4m\mathbb{Z}, && m = 1,2,\\
&\mathbb{Z}/5\mathbb{Z}\times\mathbb{Z}/5\mathbb{Z},\\
&\mathbb{Z}/6\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}.
\end{aligned}$$

Interestingly, in all these cases except for $m = 21$ in the cubic field case, there exist infinitely many elliptic curves over $\mathbb{Q}$ with the given torsion. The only elliptic curve over $\mathbb{Q}$ with a torsion group $\mathbb{Z}/21\mathbb{Z}$ over some cubic field is the elliptic curve with LMFDB label 162.c3. Over a cubic field $\mathbb{Q}(\zeta_9)^+$, this curve has a torsion group $\mathbb{Z}/21\mathbb{Z}$ [75].

Less is known about the possible ranks for elliptic curves, even over $\mathbb{Q}$. It is not even

known whether it is bounded or not. The current highest known $\mathbb{Q}$-rank of an elliptic curve is $r = 29$ due to Elkies and Klagsbrun in 2024. Prior to this recent result, the highest known rank was $r = 28$ due to Elkies in 2006.

1.1.1. Reduction mod p

Definition 1.1.7. Let E be an elliptic curve over $\mathbb{Q}$ let and p be a prime. By changing the coordinates we can obtain an isomorphic curve E' with coefficients in $\mathbb{Z}$ and with a minimal Weierstrass model (i.e., with minimal discriminant Δ). The (possibly singular) curve $\tilde{E}$ with coefficients over $\mathbb{F}_p$ obtained by reducing all coefficients of E' mod p is called the reduction of E modulo p.

We say that the reduction mod p is

(a) good (or stable) if $\tilde{E}$ is non-singular.

(b) multiplicative (or semistable) if $\tilde{E}$ has a node.

(c) additive (or unstable) if $\tilde{E}$ has a cusp.

In cases (b) and (c) the curve $\tilde{E}$ is singular and we say that the reduction mod p is bad.

The following result gives us an easily computable criterion for determining the reduction type mod p.

Proposition 1.1.8. [90, Proposition VII.5.1] Let $E/\mathbb{Q}$ be an elliptic curve given by its minimal Weierstrass model

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

We define the value $c_4 = (a_1^2 + 4a_2)^2 - 24(a_1a_3 + 2a_4)$.

(a) E has good reduction mod p if and only if $p \nmid \Delta$.

(b) E has multiplicative reduction mod p if and only if $p \mid \Delta$ and $p \nmid c_4$.

(c) E has additive reduction mod p if and only if $p \mid \Delta$ and $p \mid c_4$.

Therefore, for each elliptic curve $E/\mathbb{Q}$ there are only finitely many bad primes p.

It is also possible to define the good and bad reduction mod p for general algebraic curves over $\mathbb{Q}$. The reduction will be good if the resulting reduced curve is non-singular and bad otherwise. In later chapters we will extensively use the reduction mod p properties of curves.

1.2. ISOGENIES OF ELLIPTIC CURVES

Definition 1.2.1. Let V_1 and V_2 be projective varieties over a field k. A rational map from V_1 to V_2 is a map of the form

$$\phi : V_1 \to V_2,\ \phi = [f_0, \ldots, f_n],$$

where $f_0, \ldots, f_n \in \overline{k}(V_1)$. A morphism is a rational map that is regular everywhere on V_1.

A morphism ϕ is an isomorphism if there exists a morphism $\psi : V_2 \to V_1$ such that $\psi \circ \phi = \mathrm{id}_{V_1}$ and $\phi \circ \psi = \mathrm{id}_{V_2}$.

Theorem 1.2.2 ([90, Teorem II.2.3]). Let $\phi : C_1 \to C_2$ be a morphism of curves. Then ϕ is either constant or surjective.

Let C_1 and C_2 be curves over k and let $\phi : C_1 \to C_2$ be a non-constant k-rational map. Then we have an injection of function fields

$$\phi^* : k(C_2) \to k(C_1),\ \phi^* f = f \circ \phi.$$

Theorem 1.2.3 ([90, Theorem II.2.4 (a)]). Let C_1 and C_2 be curves over k and let $\phi : C_1 \to C_2$ be a non-constant morphism over k. Then $k(C_1)$ is a finite extension of $\phi^* k(C_2)$.

Definition 1.2.4. Let $\phi : C_1 \to C_2$ be a non-constant morphism of curves defined over k. We define the degree of ϕ as

$$\deg \phi = [k(C_1) : \phi^* k(C_2)].$$

We say that a morphism ϕ is separable, inseparable, or purely inseparable if the field extension $k(C_1)/\phi^* k(C_2)$ has the corresponding property.

If ϕ is separable (which is always true if $\mathrm{char}\, k = 0$), we can calculate $\deg \phi$ as the size of the preimage of a generic point on C_2. This is an easier alternative to working with the function fields.

Proposition 1.2.5. [90, Corollary II.2.4.1] Let C_1 and C_2 be smooth curves and let $\phi : C_1 \to C_2$ be a degree 1 morphism. Then ϕ is an isomorphism.

Definition 1.2.6. Let E_1 and E_2 be elliptic curves. An isogeny from E_1 to E_2 is a morphism $\phi : E_1 \to E_2$ satisfying $\phi(\mathcal{O}_{E_1}) = \mathcal{O}_{E_2}$. We say that E_1 and E_2 are isogenous if there exists a non-zero isogeny from E_1 to E_2.

Example 1.2.7. For every elliptic curve E over k and every $m \in \mathbb{Z}$ there is a multiplication-by-m isogeny $[m] : E \to E$. For $m \geq 0$ we define it as

$$[m] : E \to E,\ P \mapsto mP = \underbrace{P + \ldots + P}_{m \text{ times}},$$

and for $m < 0$, we set $[m]P = [-m](-P)$. For $m > 0$, the kernel of this isogeny is the m-torsion subgroup of E

$$E[m] = \{P \in E(\overline{k}) : mP = \mathcal{O}\},$$

i.e., the set of points of E of order m.

If we have two isogenies $\phi, \psi : E \to E$, we can pointwise define the isogenies $\phi \pm \psi$ and $\phi \circ \psi$. Therefore, the endomorphism group $\mathrm{End}(E)$ is a ring. It is of characteristic zero with no zero divisors. If $\mathrm{char}\, k = 0$, then we usually have $\mathrm{End}(E) \cong \mathbb{Z}$. If the endomorphism ring is strictly larger than $\mathbb{Z}$, then we say that E has complex multiplication (CM). We will mention more results regarding the endomorphism rings and CM elliptic curves at the end of this section.

Proposition 1.2.8 ([90, Corollary III.6.4])**.** Let E be an elliptic curve over a field k and $m \in \mathbb{Z}$ with $m \neq 0$.

(a) $\deg[m] = m^2$.

(b) If either $\mathrm{char}\, k \neq 0$ or $\mathrm{char}\, k = p \nmid m$, then

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

(c) If $\mathrm{char}\, k = p$, then one of the following is true:

(i) $E[p^e] \cong 0$ for all $e = 1, 2, 3, \ldots$

(ii) $E[p^e] \cong \mathbb{Z}/p^e\mathbb{Z}$ for all $e = 1,2,3,\ldots$

Example 1.2.9. Let $\phi : E_1 \to E_2$ be a non-constant isogeny of degree m. Then there exists a unique isogeny $\hat{\phi} : E_2 \to E_1$ such that $\hat{\phi} \circ \phi = [m]$. This isogeny $\hat{\phi}$ is called the dual isogeny of ϕ and it is defined over the same field as ϕ. Also, the kernel of the dual isogeny is $\ker \hat{\phi} = \phi(E_1[m])$.

It follows that "being isogenous" is an equivalence relation on the set of elliptic curves. Furthermore, it is a consequence of Shafarevich's theorem [89] that for elliptic curves defined over a number field k, up to isomorphism there are only finitely many elliptic curves in each isogeny class. For example, for $k = \mathbb{Q}$, Kenku [61] showed that there are at most 8 $\mathbb{Q}$-isomorphism classes of elliptic curves in each $\mathbb{Q}$-isogeny class.

Isogenies of elliptic curves have more interesting properties. We list some of them below.

Theorem 1.2.10 ([90, Theorem III.4.8])**.** Let $\phi : E_1 \to E_2$ be an isogeny. Then $\phi(P+Q) = \phi(P) + \phi(Q)$ for all $P, Q \in E_1$.

We see from Theorem 1.2.2 that every non-zero isogeny $\phi : E_1 \to E_2$ is surjective. Also, its kernel $\operatorname{Ker} \phi = \phi^{-1}(\mathcal{O}_{E_2})$ is a finite group. It is a group because of Theorem 1.2.10 and finite since it is a preimage of a point $\mathcal{O}_{E_2}$ on E_2.

Theorem 1.2.11 ([90, Theorem III.6.2])**.** The dual isogeny has the following properties:

(a) If $\phi : E_1 \to E_2$ and $\lambda : E_2 \to E_3$ are isogenies, then

$$\widehat{\lambda \circ \phi} = \hat{\phi} \circ \hat{\lambda}.$$

(b) If $\phi, \psi : E_1 \to E_2$ are isogenies, then

$$\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}.$$

(c) $\widehat{[m]} = [m]$ for all $m \in \mathbb{Z}$.

(d) $\deg \hat{\phi} = \deg \phi$.

(e) $\hat{\hat{\phi}} = \phi$.

Proposition 1.2.12 ([90, Proposition III.4.12, Remark III.4.13])**.** Let E be an elliptic curve and let Φ be a finite subgroup of E. Then there are a unique elliptic curve E' and a separable isogeny

$$\phi : E \to E' \text{ satisfying } \ker\phi = \Phi.$$

Furthermore, suppose that E is defined over k and that Φ is $G_{\overline{k}/k}$-invariant. Then E' and ϕ can be defined over k.

This elliptic curve E' is often denoted as E/Φ to signify that it is determined by E and Φ and that Φ is the kernel of the isogeny. In the spirit of this notation we will also denote $\phi(C)$ as C/Φ for subgroups C that contain Φ. For example, for dual isogenies in Example 1.2.9 we will write $\ker\hat{\phi} = E_1[m]/\ker\phi$.

Definition 1.2.13. We say that an isogeny $\phi : E_1 \to E_2$ is cyclic if $\ker\phi$ is a cyclic group.

Every isogeny $\phi : E_1 \to E_2$ is a composition of a cyclic isogeny and a multiplication-by-m isogeny. More precisely, there exists a cyclic isogeny $\psi : E_1 \to E_2$ and $m \in \mathbb{Z}$ such that

$$\phi = [m] \circ \psi.$$

For the end of this section we give a brief discussion regarding the CM properties of elliptic curves.

Proposition 1.2.14 ([90, Corollary 9.4])**.** The endomorphism ring of an elliptic curve E/k is either $\mathbb{Z}$, an order of an imaginary quadratic field, or an order in a quaternion algebra. If $\mathrm{char}(k) = 0$, then only the first two cases are possible.

Therefore, if an elliptic curve $E/\mathbb{Q}$ is CM, then $R = \mathrm{End}(E)$ is an order of an imaginary quadratic field. This means that the field of fractions $\mathbb{Q}(R)$ is equal to $\mathbb{Q}(\sqrt{-d})$ for some $d \in \mathbb{N}$. Furthermore, the ring of integers of this field $\mathbb{Q}(\sqrt{-d})$ has class number 1, i.e., it is a principal ideal domain.

Theorem 1.2.15 (Baker-Stark-Heegner, [90, Example C.11.3.1])**.** The imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$ has class number 1 exactly for the following 9 values of $-d$:

$$-d \in \{-1, -2, -3, -7, -11, -19, -43, -67, -163\}.$$

All elliptic curves isomorphic to an elliptic curve E have the same endomorphism ring as E. Therefore, the CM property depends only on the j-invariant. Interestingly, there are finitely many (exactly 13) CM j-invariants of elliptic curves over $\mathbb{Q}$ [90, Example C.11.3.2].

Table 1.1: j-invariants of CM elliptic curves over $\mathbb{Q}$ along with their corresponding endomorphism rings.

$\mathrm{End}(E)$	j
$\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$	0
$\mathbb{Z}[1+\sqrt{-3}]$	$2^4 \cdot 3^3 \cdot 5^3$
$\mathbb{Z}\left[\frac{3(1+\sqrt{-3})}{2}\right]$	$2^{15} \cdot 3^3 \cdot 5^2$
$\mathbb{Z}[\sqrt{-1}]$	$2^4 \cdot 3^3$
$\mathbb{Z}[2\sqrt{-1}]$	$2^4 \cdot 3^3 \cdot 11^3$
$\mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$	$-3^3 \cdot 5^3$
$\mathbb{Z}[1+\sqrt{-7}]$	$3^3 \cdot 5^3 \cdot 17^3$
$\mathbb{Z}[\sqrt{-2}]$	$2^4 \cdot 5^3$
$\mathbb{Z}\left[\frac{1+\sqrt{-11}}{2}\right]$	-2^{15}
$\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$	$-2^{15} \cdot 3^3$
$\mathbb{Z}\left[\frac{1+\sqrt{-43}}{2}\right]$	$-2^{18} \cdot 3^3 \cdot 5^3$
$\mathbb{Z}\left[\frac{1+\sqrt{-67}}{2}\right]$	$-2^{15} \cdot 3^3 \cdot 5^3 \cdot 11^3$
$\mathbb{Z}\left[\frac{1+\sqrt{-163}}{2}\right]$	$-2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3$

1.3. MODULAR CURVES

Let $\mathscr{H} = \{z \in \mathbb{C} : \operatorname{Im} z > 0\}$ be the upper half-plane of the complex numbers and let $\mathscr{H}^* = \mathscr{H} \cup \mathbb{P}^1(\mathbb{Q})$ be the compactified half-plane. The modular group $\mathrm{SL}_2(\mathbb{Z})$ acts on $\mathscr{H}^*$ as

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} z = \frac{az+b}{cz+d}.$$

Definition 1.3.1. A principal congruence subgroup of level N is the group

$$\Gamma(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : a,d \equiv 1 \pmod{N}, b,c \equiv 0 \pmod{N} \right\}.$$

A subgroup $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ is called a congruence subgroup if there exists $N \in \mathbb{N}$ such that $\Gamma(N) \leq \Gamma$.

Examples of congruence subgroups are

$$\Gamma_0(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \pmod{N} \right\},$$

$$\Gamma_1(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : a,d \equiv 1 \pmod{N}, c \equiv 0 \pmod{N} \right\},$$

$$\Gamma_1(M,N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : a,d \equiv 1 \pmod{N}, c \equiv 0 \pmod{N}, b \equiv 0 \pmod{M} \right\}$$

for $M \mid N$.

Modular curves $X(\Gamma)$ are a type of algebraic curves which can be constructed as quotients of of the upper half-plane $\mathscr{H}^*$ with a congruence subgroup Γ. Examples of modular curves are $X(N)$, $X_0(N)$, $X_1(N)$, and $X_1(M,N)$ which correspond to congruence subgroups $\Gamma(N)$, $\Gamma_0(N)$, $\Gamma_1(N)$, and $\Gamma_1(M,N)$. As algebraic curves, $X_0(N)$ and $X_1(N)$ are defined over $\mathbb{Q}$, $X(N)$ is defined over the cyclotomic field $\mathbb{Q}(\zeta_N)$, and $X_1(M,N)$ is defined over the cyclotomic field $\mathbb{Q}(\zeta_M)$. Notice that the curve $X_1(1,N)$ is isomorphic to $X_1(N)$.

The value N present in the modular curves $X(N)$, $X_0(N)$, $X_1(N)$ is called the level of these modular curves.

Modular curves $X(\Gamma)$ are very important because they are also moduli spaces of elliptic curves, i.e., points on modular curves represent isomorphism classes of elliptic curves with some additional property depending on the group Γ.

For example, non-cuspidal points on $X(N)$ represent k-isomorphism classes $[(E,P,Q)]$, where E is an elliptic curve and P,Q form a basis for the N-torsion group $E[N]$. Non-cuspidal points on $X_1(N)$ represent k-isomorphism classes $[(E,P)]$, where E is an elliptic curve and P is a point on E of order N. Non-cuspidal points on $X_1(M,N)$ represent k-isomorphism classes $[(E,P,Q)]$, where E is an elliptic curve and P,Q are independent points of orders M and N, respectively. Non-cuspidal points on $X_0(N)$ represent $\overline{k}$-isomorphism classes $[(E,C_N)]$, where E is an elliptic curve and C_N is a cyclic subgroup of points on E of order N (or equivalently due to Proposition 1.2.12, classes $[(E,\phi)]$, where ϕ is a degree N cyclic isogeny from E).

We say that $X(N)$, $X_1(N)$, and $X_1(M,N)$ are fine moduli spaces and that $X_0(N)$ is a coarse moduli space (due to isomorphism classes being over $\overline{k}$ and not k).

Therefore, we can look at the modular curves from three perspectives: as smooth projective algebraic curves defined over $\mathbb{Q}$, as quotients of $\mathscr{H}^*$, and as moduli spaces.

An additional very important property of modular curves is their cusps. Cusps are points corresponding to classes $\Gamma\backslash\mathbb{P}^1(\mathbb{Q})$. The following results give the number of cusps on the curves $X(N)$, $X_1(N)$, and $X_0(N)$.

Proposition 1.3.2. [25, p. 101–103] The number of cusps on the curve $X(N)$ is equal to

$$\begin{cases} 1 & \text{for } N=1, \\ 3 & \text{for } N=2, \\ \dfrac{N^2}{2}\displaystyle\prod_{p\mid N}\left(1-\frac{1}{p^2}\right) & \text{for } N>2. \end{cases}$$

The number of cusps on the curve $X_1(N)$ is equal to

$$\begin{cases} 1 & \text{for } N = 1, \\ 2 & \text{for } N = 2, \\ 3 & \text{for } N = 4, \\ \dfrac{N^2}{2}\displaystyle\prod_{p|N}\left(1-\frac{1}{p^2}\right) & \text{otherwise.} \end{cases}$$

The number of cusps on the curve $X_0(N)$ is equal to

$$\sum_{d|N} \phi((d,N/d)),$$

where ϕ is the Euler's totient function. Moreover, the cusps in each summand are defined over $\mathbb{Q}(\zeta_{\phi((d,N/d))})$.

As we can see, the cusps on these modular curves are a source of rational points. This is very important since algebraic curves are not generally expected to contain a rational point.

Modular curves are a very active area of mathematics. One of the reasons for that is that we can solve some problems concerning elliptic curves by studying a single modular curve. For example, Theorem 1.1.3 can be rephrased as follows.

Theorem 1.3.3 (Mazur [70])**.** The modular curve $X_1(M,N)$ has a non-cuspidal rational point if and only if $(M,N) = (1,n)$ for $n = 1,\dots,10,12$ or $(M,N) = (2,2n)$ for $n = 1,2,3,4$.

Theorems 1.1.3, 1.1.4, and 1.1.5 give us all modular curves $X_1(M,N)$ that contain non-cuspidal points of degree ≤ 3. Less is known about the points on $X_0(N)$. Mazur and Kenku determined all curves $X_0(N)$ containing a non-cuspidal rational point.

Theorem 1.3.4 ([57–60, 71])**.** The modular curve $X_0(N)$ has a non-cuspidal rational point if and only if

$$N \in \{1,\dots,19,21,25,27,37,43,67,163\}.$$

The problem of determining all quadratic points on curves $X_0(N)$ is still open, al-

though there are some results in that direction.

1.3.1. Atkin-Lehner involutions

Let d be a divisor of N such that $\gcd(d,N/d) = 1$. Then there exists an involution w_d of the modular curve $X_0(N)$. This curve is called an Atkin-Lehner involution and it is defined over $\mathbb{Q}$. The involution w_d is defined on $X_0(N)$ through its moduli interpretation as follows. Take an elliptic curve E with a cyclic subgroup C_N. We can decompose C_N as a sum of subgroups $C_d + C_{N/d}$. Then

$$w_d(E,C_N) = w_d(E,C_d,C_{N/d}) = (E/C_d, E[d]/C_d, C_N/C_d).$$

The involution w_N is also called the Fricke involution. From the definition of w_d for general d we see that

$$w_N(E,C_N) = (E/C_N, E[N]/C_N).$$

It is not hard to see that w_d is an involution because

$$\begin{aligned} w_d(E/C_d, E[d]/C_d, C_N/C_d) &= (E/E[d], (E/C_d)[d]/(E[d]/C_d), (E[d]+C_N)/E[d]) \\ &= (E, C_d, C_{N/d}). \end{aligned}$$

This is because $E[d]/C_d$ is the kernel of the dual isogeny (see Example 1.2.9 and Proposition 1.2.12) and $E[d]$ is the kernel of the multiplication-by-d isogeny $[d]$.

Atkin-Lehner involutions of a curve $X_0(N)$ form an abelian group $B(N)$ with composition as the group operation [24, Section 4]. The group $B(N)$ has 2^{ω_N} elements, where ω_N is the number of different prime divisors of N. For every subgroup of $B(N)$ there exists a corresponding quotient curve defined over $\mathbb{Q}$ with the rational quotient map from $X_0(N)$ to that quotient curve.

For example, the curve $X_0^{+d}(N)$ is the quotient curve by the involution w_d and the quotient map $X_0(N) \to X_0^{+d}(N)$ has degree 2. When $d = N$, we write $X_0^+(N)$ instead. The curve $X_0^*(N)$ is the quotient curve by the entire group $B(N)$ and the quotient map $X_0(N) \to X_0^*(N)$ has degree 2^{ω_N}.

1.4. DIVISORS AND JACOBIANS

Before we define divisors on a curve, we first introduce function fields which will be needed in the definition of a special class of divisors, principal divisors.

We can define function fields for general algebraic varieties, but we will restrict ourselves to curves. First, we define function fields of affine curves, then we will do the same for the projective curves.

Definition 1.4.1. Let C/k be an affine curve. The affine coordinate ring of C/k is

$$k[C] = k[X]/I(C).$$

Its field of fractions is denoted by $k(C)$ and is called the function field of C/k.

Example 1.4.2. Suppose we have an elliptic curve

$$E : y^2 = x^3 + ax + b$$

defined over $\mathbb{Q}$. Its function ring over $\mathbb{Q}$ is $\mathbb{Q}[x,y]/\langle y^2 - x^3 - ax - b\rangle$.

Definition 1.4.3. [90, Section I.2] Let C/k be a projective curve in $\mathbb{P}^n$. Choose $\mathbb{A}^n \subset \mathbb{P}^n$ such that $C \cap \mathbb{A}^n \neq \emptyset$. The function field of C, denoted by $k(C)$, is the function field of $C \cap \mathbb{A}^n$. We note that for different choices of $\mathbb{A}^n$, the different $k(C)$ are canonically isomorphic, so we may identify them.

Remark 1.4.4. [90, Remark I.2.9] The function field of a projective curve C may also be described as the subfield of $k(X)$ consisting of rational functions $F(X) = f(X)/g(X)$ such that:

(i) f and g are homogenous of the same degree,

(ii) $g \notin I(C)$,

(iii) two functions f_1/g_1 and f_2/g_2 are identified if $f_1 g_2 - f_2 g_1 \in I(C)$.

Definition 1.4.5. A divisor on an algebraic curve C is a finite combination of points on C with integer coefficients. For a divisor $D = \sum_P a_P P$, we define its degree $\deg D = \sum_P a_P$

(the sum is well defined since only finitely many a_P are $\neq 0$). We say that a divisor D is effective, denoted by $D \geq 0$, if all its coefficients are non-negative.

If $f \in k(C)^\times$ is a non-zero element of a function field, we can define its divisor $\operatorname{div} f = \sum_P \operatorname{ord}_P f$. We can write this divisor in the form

$$\operatorname{div} f = D_0 - D_\infty,$$

where D_0, called the zero divisor, is the sum of all zeros of f counting multiplicities, and D_∞, called the polar divisor, is the sum of all poles of f counting multiplicities.

We say that a divisor D is principal if it is a divisor of some function, i.e., if there exists some $f \in k(C)^\times$ such that $D = \operatorname{div} f$. The divisors D_1 and D_2 are linearly equivalent if there exists a function f such that $D_1 = \operatorname{div} f + D_2$.

If we have a degree d morphism $f = (f_1 : f_2) : C \to \mathbb{P}^1$, where $f_1, f_2 \in k(C)^\times$, we can define its divisor as

$$\operatorname{div} f = \operatorname{div} f_1 - \operatorname{div} f_2.$$

It is not hard to see that this definition does not depend on the choice of f_1 and f_2. We will use this slight abuse of notation throughout the thesis and look at divisors of morphisms from C to $\mathbb{P}^1$.

Proposition 1.4.6. Let $f : C \to \mathbb{P}^1$ be a degree d morphism and let $\operatorname{div} f = D_0 - D_\infty$. Then D_0 and D_∞ are both degree d effective divisors. Therefore, all principal divisors have degree 0.

Proof. The degree of f is the size of the preimage of any point in $\mathbb{P}^1(\mathbb{Q})$, counting multiplicities. Therefore, $\deg D_0 = \#f^{-1}(0) = d$ and $\deg D_\infty = \#f^{-1}(\infty) = d$. Now we have $\deg \operatorname{div} f = d - d = 0$. ■

We denote the set of degree d divisors as $\operatorname{Div}^d(C)$ and the set of principal divisors as $\operatorname{Princ}(C)$. It follows that $\operatorname{Princ}(C) \leq \operatorname{Div}^0(C)$. We define the zero Picard group

$$\operatorname{Pic}^0(C) = \operatorname{Div}^0(C)/\operatorname{Princ}(C).$$

We also define the Picard group

$$\mathrm{Pic}(C) = \mathrm{Div}(C)/\mathrm{Princ}(C)$$

and $\mathrm{Pic}^d(C)$ as the set of classes of degree d divisors, similarly to $\mathrm{Pic}^0(C)$.

Definition 1.4.7. An abelian variety is a projective algebraic variety that is also an abelian group with the group operation defined with regular functions.

Elliptic curves are an example of abelian varieties. In fact, they are the only abelian varieties of dimension 1.

Theorem 1.4.8 (Mordell-Weil)**.** For an abelian variety A defined over a number field k, the group $A(k)$ is a finitely generated abelian group.

This theorem is a generalization of the Mordell theorem for elliptic curves.

We will not define the Jacobian variety $J(C)$ here, the definition can be found in [74, Section 1]. Instead, we give a characterization.

Theorem 1.4.9. [74, Theorem 1.1] Let C be a curve over a field k such that $C(k) \neq \emptyset$. Then $J(C)(k) \cong \mathrm{Pic}^0(C)(k)$.

The Jacobian $J(C)$ is an abelian variety, but its defining equations are not of interest to us. Instead, it is much more useful as a zero Picard group or as a finitely generated abelian group (due to Mordell-Weil theorem). It has many other important properties which will be discussed later in this thesis.

The Jacobians of modular curves $X(N)$, $X_0(N)$, $X_1(N)$, and $X_1(M,N)$ are usually denoted by $J(N)$, $J_0(N)$, $J_1(N)$, and $J_1(M,N)$, respectively.

Definition 1.4.10. The Riemann-Roch space of a divisor D is

$$L(D) = \{f : C \to \mathbb{P}^1 : \mathrm{div}\ f + D \geq 0\} \cup \{0\}.$$

This is a finitely dimensional vector space of dimension $\ell(D)$.

Notice that for all $D \geq 0$ we have $\ell(D) \geq 1$ since the constant functions are in $L(D)$. Also, it is not hard to see that linearly equivalent divisors have the same dimension $\ell(D)$ and that $\ell(D) = 0$ for divisors D with negative degree.

We say that a divisor D on a curve C is canonical if there exists a differential ω on C such that $D = \operatorname{div}\omega$. We will not define differentials on a curve here, the definition can be found in [90, Section II.4]. Instead we give two results that give a characterization of canonical divisors.

Proposition 1.4.11. [90, Remark II.4.4] If ω_1, ω_2 are non-zero differentials, then there is a function f such that

$$\operatorname{div}\omega_1 = \operatorname{div} f + \operatorname{div}\omega_2.$$

Therefore, any two canonical divisors differ by a principal divisor.

Proposition 1.4.12. A divisor D on a genus g curve C is canonical if and only if $\deg D = 2g-2$ and $\ell(D) = g$.

Now we state the Riemann-Roch theorem and Clifford's theorem on special divisors. The Riemann-Roch theorem is a very important result and it will be heavily used throughout this thesis. For example, we will use it to prove Proposition 1.4.12.

Theorem 1.4.13 (Riemann-Roch, [36, Theorem IV.1.3])**.** Let D be a divisor on a genus g curve C and let K be a canonical divisor on C. Then we have

$$\ell(D) - \ell(K-D) = \deg D - g + 1.$$

Theorem 1.4.14 (Clifford's theorem on special divisors, [36, Theorem IV.5.4])**.** A divisor D is called special if $\ell(K-D) \geq 1$ (K is again the canonical divisor). For an effective degree d special divisor D on a curve C we have

$$2(\ell(D)-1) \leq d.$$

The equality holds if and only if D is zero or a canonical divisor, or if C is a hyperelliptic curve and D is linearly equivalent to an integral multiple of a hyperelliptic divisor.

Proof of Proposition 1.4.12. Apply the Riemann-Roch theorem with $D = 0$. Since $L(0)$ contains only constant functions, we get

$$1 - \ell(K) = 0 - g + 1 = 1.$$

Therefore, $\ell(K) = g$. Now apply the theorem with $D = K$. We get

$$g - 1 = \ell(K) - \ell(0) = \deg K - g + 1.$$

Therefore, $\deg K = 2g - 2$. Suppose now that there is a divisor D such that $\deg D = 2g - 2$ and $\ell(D) = g$. Applying the theorem again we get

$$g - \ell(K - D) = g - 1,$$

meaning that $\ell(K - D) = 1$. Therefore, there exists a morphism f such that $K - D + \operatorname{div} f \geq 0$. Since $\deg(K - D) = 0$, this implies that $K - D$ is principal and D must be canonical by Proposition 1.4.11 as a difference of a canonical and a principal divisor. ■

1.4.1. Hyperelliptic and bielliptic curves

Hyperelliptic curves were mentioned in Clifford's theorem. We will now define them and mention some of their properties because we will consider them in later chapters.

Definition 1.4.15. A curve C of genus $g \geq 2$ is hyperelliptic if there exists a degree 2 morphism $f : C \to \mathbb{P}^1$.

Every hyperelliptic curve of genus g can be given by an equation of the form

$$C : y^2 + h(x)y = f(x),$$

where $f(x)$ is a polynomial of degree $2g + 1$ or $2g + 2$ without multiple roots and $h(x)$ is a polynomial of degree $\leq g + 1$. If the field of definition is not of characteristic 2, we can take $h = 0$. From this equation we can easily see that the map $x : C \to \mathbb{P}^1$, $(x, y) \mapsto x$ is a desired degree 2 morphism.

A hyperelliptic divisor, mentioned in Clifford's theorem, is a divisor of the for $(x, y) + (x, y')$ for some x. If $h = 0$, this divisor is just $(x, y) + (x, -y)$.

The hyperelliptic curve $y^2 = f(x) = a_{2g+2}x^{2g+2} + \ldots + a_0$ is actually a projective curve, but it is singular in the standard projective space $\mathbb{P}^2$. Therefore, we must use the weighted projective space where y has weight $g + 1$ and x, z have weight 1. The projective

model of the curve is

$$y^2 = a_{2g+2}x^{2g+2} + \ldots + a_0 z^{2g+2}.$$

We can see that the curve has a single point at infinity $\infty = (1:0:0)$ if $a_{2g+2} = 0$ and two points at infinity $\infty_\pm = (1 : \pm\sqrt{a_{2g+2}} : 0)$ if $a_{2g+2} \neq 0$ (or none, depending on the field of definition).

Proposition 1.4.16. Every genus 2 curve is hyperelliptic.

Proof. By Proposition 1.4.12, the canonical divisor K of this curve C is of degree 2 and Riemann-Roch dimension 2. Therefore, there exists a non-constant morphism $f : C \to \mathbb{P}^1$.

Since $\operatorname{div} f + K \geq 0$, the degree of f is at most 2. It cannot be 1, otherwise C would be isomorphic to a genus 0 curve $\mathbb{P}^1$. Therefore, $\deg f = 2$ and C is hyperelliptic. ■

For the end of this section, we prove Proposition 1.4.18 to demonstrate the usefulness of the Riemann-Roch theorem.

Proposition 1.4.17 (Corollary of [14, Theorem 2.1])**.** Let $C/\mathbb{Q}$ be a smooth projective curve of genus $g \geq 1$, and let $P \in C(\mathbb{Q})$. Then for all $d \geq 2g$, the curve C has infinitely many points of degree d.

Proposition 1.4.18. Let $C/\mathbb{Q}$ be a smooth projective curve of genus $g = 2$ with a point $P \in C(\mathbb{Q})$. If $J(C)(\mathbb{Q})$ is nontrivial, then C has infinitely many cubic points.

Proof. Suppose first that $\ell(2P) = 1$. Applying the Riemann-Roch theorem on $D = 3P$ we get

$$\ell(3P) = \ell(3P) - \ell(K - 3P) = 3 - 2 + 1 = 2.$$

Therefore, there exists a non-constant function $f : C \to \mathbb{P}^1$ of degree ≤ 3. However, its degree cannot be ≤ 2, otherwise we would have $\operatorname{div} f + 2P \geq 0$, a contradiction with $\ell(2P) = 1$. This means that $\deg f = 3$. We can now use [14, Theorem 2.1, Step 2] to find infinitely many cubic points on C as preimages of points in $\mathbb{P}^1(\mathbb{Q})$.

Suppose now that $\ell(2P) \geq 2$. Applying the Riemann-Roch theorem on $D = 2P$ we get

$$\ell(2P) - \ell(K - 2P) = 2 - 2 + 1 = 1 \implies \ell(K - 2P) \geq 1.$$

Since $K-2P$ is of degree 0 and $\ell(K-2P) \geq 1$, it is principal. Therefore, $2P$ must be canonical as a difference of a canonical and a principal divisor.

Since $J(C)(\mathbb{Q})$ is nontrivial, there exists an effective rational divisor D of degree 2 such that the divisor $D-2P$ is not principal. We again use the Riemann-Roch theorem to get (since $2P$ is canonical we may plug in $2P$ instead of K)

$$\ell(D+P)-\ell(P-D) = 3-2+1 = 2 \implies \ell(D+P) = 2,$$

$$\ell(D)-\ell(2P-D) = 2-2+1 = 1 \implies \ell(D) = 1.$$

Therefore, there exists a function f such that $D+P+\operatorname{div} f \geq 0$ and $D+\operatorname{div} f \ngeq 0$. We immediately see that $\deg f \leq 3$. If $\deg f = 3$, we may apply [14, Theorem 2.1, Step 2] to conclude that C has infinitely many cubic points. Since $g = 2$, we have $\deg f > 1$. It remains to prove that f cannot have degree 2.

Suppose that $\deg f = 2$ and let us write $D = D_1 + D_2$ for $D_1, D_2 \in C(\bar{k})$. Since $D+P+\operatorname{div} f \geq 0$ and $D+\operatorname{div} f \ngeq 0$, we see that $\operatorname{div} f = X+Y-D_1-P$ for some $X, Y \in C(\bar{k})$. This means that $\ell(D_1+P) \geq 2$ (one function is f and the other is a constant function) and so, again by Riemann-Roch, D_1+P must be canonical.

However, since D_1+P and $2P$ are both canonical, their difference $D_1+P-2P = D_1-P$ must be principal and we get a contradiction. ■

Therefore, by Proposition 1.4.17 every genus 2 curve over $\mathbb{Q}$ containing at least 1 rational point has infinitely many points of degree d for every $d \geq 4$. Since every genus 2 curve is hyperelliptic, it also has infinitely many quadratic points of the form $(x, \sqrt{f(x)})$. Furthermore, if its Jacobian is nontrivial over $\mathbb{Q}$ (automatically true if the curve has at least 2 rational points P, Q since $[P-Q] \neq 0$), it also has infinitely many cubic points by Proposition 1.4.18.

At the end of this section, we will define the bielliptic curves.

Definition 1.4.19. A curve C of genus $g \geq 2$ is bielliptic if there exists a degree 2 morphism from C to an elliptic curve.

Proposition 1.4.20. [35, Proposition 1] If C is a bielliptic curve and $f : C \to C'$ is a non-constant morphism, then C' is either of genus 0, elliptic, hyperelliptic, or bielliptic.

1.5. MODULAR FORMS

Definition 1.5.1. Let $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup. A modular form of level Γ and weight k is a holomorphic function $f : \mathscr{H} \to \mathbb{C}$ such that

$$f(\gamma(\tau)) = (c\tau + d)^k f(\tau) \text{ for every } \gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma, \tau \in \mathscr{H}$$

and which is also holomorphic at ∞. The set of modular forms of level Γ and weight k is denoted by $M_k(\Gamma)$.

The set $M_k(\Gamma)$ is a finitely dimensional vector space over $\mathbb{C}$ [25, Section 1.1]. If $-I \in \Gamma$ (as is the case for $\Gamma = \Gamma_0(N)$, for example), then $M_k(\Gamma)$ is trivial for odd k. This is because in that case

$$f(\tau) = f(-I\tau) = (-1)^k f(\tau) = -f(\tau) \text{ for every } \tau \in \mathscr{H},$$

implying that $f = 0$. From the fact that $\lim_{\tau \to \infty} e^{2\pi i \tau} = 0$ and because modular forms are by definition holomorphic at ∞, every modular form has a Fourier expansion

$$f(\tau) = \sum_{n=0}^{\infty} a_n q^n, q = e^{2\pi i \tau}.$$

Definition 1.5.2. A cusp form of level Γ and weight k is a modular form whose Fourier expansion has leading coefficient $a_0 = 0$, i.e.,

$$f(\tau) = \sum_{n=1}^{\infty} a_n q^n, q = e^{2\pi i \tau}.$$

The set of cusp forms of level Γ and weight k is denoted by $S_k(\Gamma)$.

The cusp forms $S_k(\Gamma)$ form a vector subspace of $M_k(\Gamma)$.

We will particularly be interested in the modular forms associated with the congruence subgroup $\Gamma_0(N)$. We say that these modular forms are of level N and accordingly define $M_k(N) := M_k(\Gamma_0(N))$, $S_k(N) := S_k(\Gamma_0(N))$.

Definition 1.5.3. Let $n \in \mathbb{N}$. The Hecke operator T_n is a linear operator on $M_k(N)$ defined

as follows. For $f = a_0 + a_1 q + \ldots$ the Fourier coefficients of $T_n f$ are defined as

$$a_m(T_n f) := \sum_{d \mid \gcd(m,n)} d^{k-1} a_{mn/d^2}.$$

The Hecke operators pairwise commute. Furthermore, they satisfy the following relations [25, Section 5.3]:

$$\begin{aligned} T_{p^r} &= T_{p^{r-1}} T_p - p T_{p^{r-2}} && \text{for primes } p \nmid M \text{ and } r > 1, \\ T_{p^r} &= T_p^r && \text{for primes } p \mid M \text{ and } r > 0, \\ T_{mn} &= T_m T_n && \text{if } \gcd(m,n) = 1. \end{aligned}$$

Let M be a divisor of N. Since $\Gamma_0(N) \subset \Gamma_0(N)$, we immediately get that $M_k(M) \subset M_k(N)$. Thus we define the space $M_k^{\text{old}}(N) = \bigcup_{M \mid N, M \neq N} M_k(M)$. The orthogonal complement of $M_k^{\text{old}}(N)$ with respect to the Petersson inner product (we will not define it here as we do not use it later, its definition can be found in [25, Section 5.4]) is the space $M_k^{\text{new}}(N)$, Therefore, we have

$$M_k(N) = M_k^{\text{old}}(N) \bigoplus M_k^{\text{new}}(N).$$

If we restrict ourselves to cusp forms, we have a corresponding decomposition into spaces of oldforms and newforms

$$S_k(N) = S_k^{\text{old}}(N) \bigoplus S_k^{\text{new}}(N).$$

Definition 1.5.4. A cusp form $f \in S_k(N)$ is an eigenform of a Hecke operator T_n if there is some $a \in \mathbb{C}$ such that $T_n f = a \cdot f$.

A newform is a cusp form $f \in S_k^{\text{new}}(N)$, normalized so that $a_1 = 1$, that is also an eigenform of all Hecke operators T_n.

Theorem 1.5.5 ([25, Theorem 5.8.2])**.** For every $N \in \mathbb{N}$ the set of newforms $S_k^{\text{new}}(N)$ has a basis of newforms. For each such newform f we have $T_n f = a_n(f) f$ for all $n \in \mathbb{N}$, that is, its Fourier coefficients are its eigenvalues.

Elliptic curves are closely linked to newforms. To see that, we first need to define the

trace of Frobenius.

Definition 1.5.6. Let E be an elliptic curve over $\mathbb{F}_q$. Then $a_q = q + 1 - \#E(\mathbb{F}_q)$ is the trace of Frobenius of E over $\mathbb{F}_q$.

Theorem 1.5.7 (Hasse-Weil Bound, [94])**.** Let $C/\mathbb{F}_q$ be a curve of genus g. Then $|q + 1 - \#C(\mathbb{F}_q)| \leq 2g\sqrt{q}$.

As an immediate consequence we get a bound $|a_q| \leq 2\sqrt{q}$.

Definition 1.5.8. An elliptic curve E is modular if there exists $N \in \mathbb{N}$ and a non-constant morphism $X_0(N) \to E$.

Theorem 1.5.9 (Modularity Theorem, [25, Theorem 2.5.1])**.** Let $E/\mathbb{Q}$ be an elliptic curve. Then there exists $N \in \mathbb{N}$ and a non-constant rational morphism $f : X_0(N) \to E$.

A minimal such N is called the conductor of E and is denoted by $\mathrm{cond}(E)$. The primes of bad reduction for E are precisely those primes that divide $\mathrm{cond}(E)$. Also, if there is a non-constant rational morphism $X_0(N) \to E$ for some N, then $\mathrm{cond}(E) \mid N$.

A morphism $f : X_0(\mathrm{cond}(E)) \to E$ of a minimal degree is called a modular parametrization of E and its degree is called a modular degree of E.

Lemma 1.5.10. Elliptic curves over $\mathbb{Q}$ that are in the same $\mathbb{Q}$-isogeny class have the same conductor.

Proof. Let us take $E/\mathbb{Q}$ and $E'/\mathbb{Q}$ together with a rational isogeny $\psi : E \to E'$. Then there exists a dual isogeny $\hat{\psi} : E' \to E$. Now any morphism $f : X_0(N) \to E$ generates a morphism $\psi \circ f : X_0(N) \to E'$ and any morphism $h : X_0(N) \to E'$ generates a morphism $\hat{\psi} : X_0(N) \to E$. ■

Theorem 1.5.11 (Modularity Theorem, alternative formulation, [25, Theorem 8.8.1])**.** Let $E/\mathbb{Q}$ be an elliptic curve with conductor N. Then there exists a newform $f \in S_2^{\mathrm{new}}(N)$ such that $a_p(f) = a_p(E)$ for all primes p.

Remark 1.5.12. The converse is also true. Namely, every rational newform $f \in S_2^{\mathrm{new}}(N)$ arises from some elliptic curve $E/\mathbb{Q}$ with conductor N.

Notice that this correspondence is not bijective because elliptic curves over $\mathbb{Q}$ that are in the same $\mathbb{Q}$-isogeny class will have the same associated newform. This is because isogenous elliptic curves have the same traces of Frobenius $a_q(E)$ as a consequence of Tate's Isogeny Theorem [93, Theorem 3.1]. We have the following bijection:

$$\text{rational newforms } f \in S_2^{\text{new}}(N) \iff \mathbb{Q}-\text{isogeny classes of elliptic curves over } \mathbb{Q} \text{ with conductor } N.$$

From now on we will work only with modular forms of weight 2.

The modularity theorem tells us that all elliptic curves over $\mathbb{Q}$ are modular. This was an important step in proving Fermat's Last Theorem. Another result used in that proof was the following proposition.

Proposition 1.5.13. There exist newforms $f \in S_2^{\text{new}}(N)$ if and only if

$$N \notin \{1,2,3,4,5,6,7,8,9,10,12,13,16,18,22,25,28,60\}.$$

Therefore, there are no elliptic curves over $\mathbb{Q}$ with conductor N in this set.

It is a conjecture that all elliptic curves over number fields are modular. This is still an open problem, although some special cases have been solved. For example, Freitas, Le Hung, and Siksek have proved that all elliptic curves over real quadratic fields are modular [30].

2. GONALITY OF ALGEBRAIC CURVES

Definition 2.0.1. Let k be a field and C a smooth projective curve over k. The k-gonality $\mathrm{gon}_k(C)$ of C is defined to be the least degree of a non-constant morphism $f : C \to \mathbb{P}^1$.

Gonality of algebraic curves has been the subject of research by many researchers. The topic of this chapter will be the computation of the $\mathbb{Q}$ and $\mathbb{C}$-gonalities of modular curves and their quotients. First, we give two obvious lower bounds on the $\mathbb{Q}$-gonality of a curve C defined over $\mathbb{Q}$.

$$\mathrm{gon}_{\mathbb{C}}(C) \leq \mathrm{gon}_{\mathbb{Q}}(C) \text{ and}$$
$$\mathrm{gon}_{\mathbb{F}_p}(C) \leq \mathrm{gon}_{\mathbb{Q}}(C).$$

In the second inequality p is a prime of good reduction of C. Now we present a result that gives bounds on the gonality of a general algebraic curve. This result will be very important to us and we will use it throughout the thesis.

Proposition 2.0.2 ([85, Proposition A.1])**.** Let X be a curve of genus g over a field k.

(i) If L is a field extension of k, then $\mathrm{gon}_L(X) \leq \mathrm{gon}_k(X)$.

(ii) If k is algebraically closed and L is a field extension of k, then $\mathrm{gon}_L(X) = \mathrm{gon}_k(X)$.

(iii) If $g \geq 2$, then $\mathrm{gon}_k(X) \leq 2g-2$.

(iv) If $g \geq 2$ and $X(k) \neq \emptyset$, then $\mathrm{gon}_k(X) \leq g$.

(v) If k is algebraically closed, then $\mathrm{gon}_k(X) \leq \dfrac{g+3}{2}$.

(vi) If $\pi : X \to Y$ is a non-constant k-rational morphism, then $\mathrm{gon}_k(X) \leq \deg \pi \cdot \mathrm{gon}_k(Y)$.

(vii) If $\pi : X \to Y$ is a non-constant k-rational morphism, then $\mathrm{gon}_k(X) \geq \mathrm{gon}_k(Y)$.

Since all modular curves $X_0(N)$, and $X_1(N)$ as well as all quotients of the curve $X_0(N)$ have at least 1 rational cusp, by Proposition 2.0.2(iv) their $\mathbb{Q}$-gonality is bounded from above by their genus.

There exists a lower bound on the $\mathbb{C}$-gonality of any modular curve $X(\Gamma)$, linear in terms of the index of the congruence subgroup Γ. This was proven by Zograf [95]. Later, Abramovich [1] and Kim and Sarnak [64, Appendix 2] improved the constant in that bound. We here present the result obtained by combining these results.

Theorem 2.0.3. [50, Theorem 1.2.] Let $X(\Gamma)$ be the algebraic curve corresponding to a congruence subgroup $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ of index

$$D_\Gamma = [\mathrm{SL}_2(\mathbb{Z}) : \pm\Gamma].$$

Then

$$D_\Gamma \leq \frac{12000}{119}\mathrm{gon}_{\mathbb{C}}(X(\Gamma)).$$

Remark 2.0.4. From Kim and Sarnak's arguments in [64] we can get that the constant $\frac{12000}{119}$ can be replaced with a slightly better constant $\frac{2^{15}}{325}$. However, their difference is ~ 0.01572 which does not make any difference in our calculations (we would need to work with gonality > 100 for it to make a difference). The constant $\frac{12000}{119}$ is given here because it appears in other papers, for example, in [50].

The constant $\frac{2^{15}}{325}$ is the best one so far. We should also mention that the constant in Zograf's inequality was 128 and this constant was improved to $\frac{800}{7}$ in Abramovich's inequality.

2.1. GONALITY OF THE MODULAR CURVE $X_0(N)$

The study of gonalities of the classical modular curve $X_0(N)$ started with Ogg [80], who determined the hyperelliptic modular curves $X_0(N)$. Hasegawa and Shimura [37] determined both the $X_0(N)$ that are trigonal over $\mathbb{C}$ and the $X_0(N)$ that are trigonal over $\mathbb{Q}$ and Jeon and Park [53] determined the $X_0(N)$ that are tetragonal over $\mathbb{C}$.

In this thesis we will study the gonalities of the modular curves $X_0(N)$ over $\mathbb{Q}$ instead of over $\mathbb{C}$. The motivation for this comes from two directions.

First, the $\mathbb{Q}$-gonality of a curve is arguably more interesting from an arithmetical point of view than its $\mathbb{C}$-gonality. For example, when one wants to determine the modular curves $X_0(N)$ and $X_1(M,N)$ with infinitely many degree d points (over $\mathbb{Q}$), a question of fundamental arithmetical importance, as these curves parametrize elliptic curves with level structures, then determining all such curves of gonality d plays a key role.

Using the gonality of the modular curves as one of the main ingredients, all the modular curves $X_1(M,N)$ with infinitely many degree d points have been determined for $d = 2$ by Mestre [72], $d = 3$ by Jeon, Kim and Schweizer [51], for $d = 4$ by Jeon, Kim and Park [50] and for $d = 5,6$ by Derickx and Sutherland [22]. The same problem has been solved for the modular curves $X_0(N)$ for $d = 2$ by Bars [6] and for $d = 3$ by Jeon [45].

The other motivation comes from the database, which is in construction, of modular curves that will be incorporated in the LMFDB [67], which tabulates L-functions, modular forms, elliptic curves and related objects. At the moment of writing of this thesis, there were 235 modular curves $X_0(N)$ in LMFDB, all with $N \leq 331$. The exact $\mathbb{Q}$-gonality was listed as known for less than half of them. Our work determines the $\mathbb{Q}$-gonality for all $N \leq 144$ and many other N in this database.

Although our interest lies primarily in $\mathbb{Q}$-gonalities, we compute and document the $\mathbb{C}$-gonality wherever possible. Our main result is the following theorem.

Theorem 2.1.1. [76, Theorem 1.1] The $\mathbb{Q}$-gonalities and $\mathbb{C}$-gonalities of modular curves $X_0(N)$ are as listed in Table A.1.

One immediate consequence of this result is the determination of all $X_0(N)$ that are tetragonal over $\mathbb{Q}$. A curve that is tetragonal over $\mathbb{Q}$ has to have gonality ≤ 4 over $\mathbb{C}$

and all curves satisfying this are known by the aforementioned results [37, 53, 80]. As we determine in Theorem 2.1.1 the $\mathbb{Q}$-gonalities for all N satisfying this, the following result immediately follows.

Theorem 2.1.2. [76, Theorem 1.2] The modular curve $X_0(N)$ is tetragonal over $\mathbb{Q}$ if and only if

$$N \in \{38, 42, 44, 51, 52, 53, 55, 56, 57, 58, 60, 61, 62, 63, 65, 66, 67, 68, 69, 70, 72, 73, 74, 75, 77, 78, 79, 80, 83, 85, 87, 88, 89, 91, 92, 94, 95, 96, 98, 100, 101, 103, 104, 107, 111, 119, 121, 125, 131, 142, 143, 167, 191\}.$$

After Theorem 2.1.2 and the aforementioned results [37, 53, 80] which determine all $X_0(N)$ of $\mathbb{C}$-gonality ≤ 4, the question of determining the pentagonal, and after that, hexagonal (both over $\mathbb{Q}$ and over $\mathbb{C}$) curves $X_0(N)$ naturally arises. Surprisingly, there seems to have been no known curve that is pentagonal either over $\mathbb{Q}$ or over $\mathbb{C}$ (at least to our knowledge); see [37, p.139-140] for a short discussion stating this. As a byproduct of our results and with some additional work, we determine all $X_0(N)$ that are pentagonal or hexagonal over $\mathbb{Q}$.

Theorem 2.1.3. [76, Theorem 1.3] The modular curve $X_0(N)$ is pentagonal over $\mathbb{Q}$ if and only if $N = 109$.

Theorem 2.1.4. [76, Theorem 1.4] The modular curve $X_0(N)$ is hexagonal over $\mathbb{Q}$ if and only if

$$N \in \{76, 82, 84, 86, 90, 93, 97, 99, 108, 112, 113, 115-118, 122-124, 127-129, 135, 137, 139, 141, 144, 146, 147, 149, 151, 155, 159, 162, 164, 169, 179, 181, 215, 227, 239\}.$$

We also show that $X_0(N)$ is pentagonal over $\mathbb{C}$ for $N = 97$ and 169, obtaining the first known such curves.

Some of our methods will be similar to the ones in the work of Derickx and Van Hoeij [23], where they compute the exact $\mathbb{Q}$-gonalities of the modular curves $X_1(N)$ for $N \leq 40$ and give upper bounds for $N \leq 250$, but some will be different. The differences

arise out of the intrinsic properties of the different modular curves. In particular, on one hand the properties that make $X_0(N)$ easier to deal with are its lower genus and an abundance of involutions (especially for highly composite N). On the other hand, $X_0(N)$ has much fewer cusps and hence much fewer modular units, the main tool in [23] for obtaining upper bounds. Another difficulty with $X_0(N)$, as opposed to $X_1(N)$, is that it is in general hard to obtain reasonable plane models, making computations in function fields much more computationally demanding.

We now give a brief description of our methods and compare them to the methods of [23]. The way to determine the exact gonality of a modular curve is to give a lower bound and an upper bound for the gonality which match each other. We explain both in more detail and rigor in Sections.

The authors of [23] were (perhaps surprisingly) able to use a single method to obtain lower bounds and a single method to obtain upper bounds. The lower bounds were obtained using the well-known fact that $\mathrm{gon}_{\mathbb{F}_p}(C) \leq \mathrm{gon}_{\mathbb{Q}}(C)$ for a prime of good reduction p of C and by then computing $\mathrm{gon}_{\mathbb{F}_p}(C)$, which is a finite computation. This will be one of our main tools too, together with the Castelnuovo-Severi inequality (see Proposition 2.1.5) and using $\mathrm{gon}_{\mathbb{C}}(C) \leq \mathrm{gon}_{\mathbb{Q}}(C)$ together with known results about $\mathbb{C}$-gonalities. An especially interesting method, described in Section 2.1.4, is Mordell-Weil sieving on the Brill-Noether varieties $W_d^1(X)$, which we use to show to determine the $\mathbb{Q}$-gonalities of curves $X_0(N)$ for $N = 97, 133, 145$. To produce lower bounds on the $\mathbb{C}$-gonality, we will also use computations on Betti numbers and proven parts of the Green conjecture (see e.g. Corollary 2.1.14 and Corollary 2.1.15). There will be a few instances in which we use other methods as well.

Derickx and van Hoeij obtained their upper bounds by constructing *modular units* (morphisms to $\mathbb{P}^1$ whose zero and polar divisor are supported only on cusps) of a certain degree. In certain instances we will also obtain upper bounds by explicitly constructing morphisms of degree d by searching in Riemann-Roch spaces of sets of divisors with some fixed support. For us, the set of divisors through which we will search will not be supported only on cusps, but will also include CM points and even non-CM non-cuspidal rational points. We will also construct morphisms on $X_0(N)$ by finding morphisms g of degree k on curves $X_0(N)/w_d$ or $X_0(d)$ for $d|N$ and then pulling them back via the quotient

map $f : X_0(N) \to X_0(N)/w_d$ or $f : X_0(N) \to X_0(d)$, thus obtaining a map f^*g of degree $k \cdot \deg f$. Apart from this, we will also use the Tower theorem (see Corollary 2.1.17) which allows us to determine the $\mathbb{Q}$-gonality from the $\mathbb{C}$-gonality under certain assumptions.

A lot of our results rely on extensive computation in `Magma` [11]. To compute models for $X_0(N)$ and their quotients by Atkin-Lehner involutions, we used the code written by Philippe Michaud-Jacobs as part of a collaborative project on computing points of low degree on modular curves [3].

It is natural to wonder why we stopped at the point where we did and whether one can determine $\mathbb{Q}$-gonalities of $X_0(N)$ for larger N. We discuss this, the complexity of the most computationally demanding parts of our computations, and possible further work briefly in Section 2.1.6.

The code that verifies all our computations can be found on:

`https://github.com/orlic1/gonality_X0`.

All of our computations were performed on the *Euler* server at the Department of Mathematics, University of Zagreb with an Intel Xeon W-2133 CPU running at 3.60GHz and with 64 GB of RAM.

2.1.1. Lower bounds

In this section we give all the results used to obtain lower bounds for the gonality of the curve $X_0(N)$.

A very useful tool for producing a lower bound on the gonality is the Castelnuovo-Severi inequality (see [92, Theorem 3.11.3] for a proof).

Proposition 2.1.5 (Castelnuovo-Severi inequality)**.** Let k be a perfect field, and let X, Y, Z be curves over k. Let non-constant morphisms $\pi_Y : X \to Y$ and $\pi_Z : X \to Z$ over k be given, and let their degrees be m and n, respectively. Assume that there is no morphism $X \to X'$ of degree > 1 through which both π_Y and π_Z factor. Then the following inequality holds:

$$g(X) \leq m \cdot g(Y) + n \cdot g(Z) + (m-1)(n-1). \tag{2.1}$$

A field k is called separable if every irreducible polynomial over k has no multiple

roots over any field extension of k. Since $\mathbb{C}$ and $\mathbb{Q}$ are both perfect fields as fields of characteristic 0, we can use Castelnuovo-Severi inequality to get lower bounds on both $\mathbb{C}$ and $\mathbb{Q}$-gonalities.

Remark 2.1.6. One of the assumptions of Castelnuovo-Severi inequality is that there is no morphism $X \to X'$ through which both π_Y and π_Z factor. This morphism could, however, be defined over $\overline{k}$ and not over k. However, Khawaja and Siksek have recently shown [63, Theorem 14] that we can weaken this assumption. Namely, that there is no morphism $X \to X'$ over k through which both π_Y and π_Z factor.

Another important tool used here is the following inequality of Ogg. It originally appeared as [80, Theorem 3.1], but we state it in the simpler form as in [37, Lemma 3.1].

Lemma 2.1.7 (Ogg)**.** For a prime $p \nmid N$, let

$$L_p(N) := \frac{p-1}{12}\psi(N) + 2^{\omega(N)},$$

where $\psi(N) = N\prod_{q|N}(1+\frac{1}{q})$ is the index of the congruence subgroup $\Gamma_0(N)$ is $\mathrm{SL}_2(\mathbb{Z})$ and $\omega(N)$ is the number of distinct prime divisors of N. Then

$$L_p(N) \leq \#X_0(N)(\mathbb{F}_{p^2}).$$

Lemma 2.1.8. Let C be a curve over $\mathbb{Q}$, p a prime of good reduction for C and q a power of p. Suppose $\#C(\mathbb{F}_q) > d(q+1)$ for some d. Then $\mathrm{gon}_{\mathbb{Q}}(C) > d$.

Proof. Suppose on the contrary that there exists a rational morphism $f : C \to \mathbb{P}^1$ of degree $\leq d$. Then for any $c \in \mathbb{P}^1(\mathbb{F}_q)$ we have $\#f^{-1}(c) \leq d$. Since f sends $C(\mathbb{F}_q)$ into $\mathbb{P}^1(\mathbb{F}_q)$, it follows that $\#X(\mathbb{F}_q) \leq d(q+1)$. ■

We will use Lemma 2.1.7 in combination with Lemma 2.1.8 to get a reasonable bound on N such that the curve $X_0(N)$ has $\mathbb{Q}$-gonality at most 6. This is a better bound for the $\mathbb{Q}$-gonality than the one we can obtain from Theorem 2.0.3.

Proposition 2.1.9. If $N > 336$, then the curve $X_0(N)$ has $\mathbb{Q}$-gonality at least 7.

Proof. The proof is similar to the proof of [37, Lemma 3.2]. Primes of good reduction for $X_0(N)$ are all $p \nmid N$. It is sufficient to show that there is a prime $p \nmid N$ such that

$$\frac{p-1}{12}\psi(N) + 2^{\omega(N)} > 6(p^2+1).$$

Suppose that the $\mathbb{Q}$-gonality of $X_0(N)$ is ≤ 6. Now we have 6 cases.

(i) $2 \nmid N$: take $p = 2$, from $\frac{\psi(N)}{12} + 2 \leq 30$ we get $N \leq \psi(N) \leq 336$.

(ii) $2 \mid N$, $3 \nmid N$: take $p = 2$, from $\frac{\psi(N)}{6} + 2 \leq 60$ we get $\frac{3N}{2} \leq \psi(N) \leq 348$, or $N \leq 232$.

(iii) $2,3 \mid N$, $5 \nmid N$: take $p = 5$, from $\frac{\psi(N)}{3} + 4 \leq 156$ we get $2N \leq \psi(N) \leq 456$, or $N \leq 228$.

(iv) $2,3,5 \mid N$, $7 \nmid N$: take $p = 7$, from $\frac{\psi(N)}{2} + 8 \leq 300$ we get $\frac{5N}{2} \leq \psi(N) \leq 584$, or $N \leq 234$.

(v) $2,3,5,7 \mid N$, $11 \nmid N$: take $p = 11$, from $\frac{5\psi(N)}{6} + 16 \leq 732$ we get $\frac{20N}{7} \leq \psi(N) \leq 716$, or $N \leq 251$.

(vi) $2,3,5,7,11 \mid N$: take $p = p_0$, the smallest prime not dividing N. Let q_0 be the largest prime dividing N. We have

$$\frac{p_0-1}{12} \cdot \frac{240 \cdot 210 q_0}{77} + 32 \leq \frac{p_0-1}{12} \cdot \frac{240N}{77} + 32 \leq \frac{(p_0-1)\psi(N)}{12} + 2^{\omega(N)} \leq 6(p_0^2+1).$$

Simplifying this we get $\frac{600(p_0-1)q_0}{11} \leq 6p_0^2 - 26$. Due to Bertrand's postulate we have $p_0 < 2q_0$, therefore $\frac{300(p_0-1)p_0}{11} \leq 6p_0^2 - 26$. However, this quadratic inequality never holds and we get a contradiction in this case.

Therefore, for $N > 336$ we can always find a suitable prime p. ■

Now we use proven parts of Green's conjecture to obtain a lower bound on the $\mathbb{C}$-gonality, which in turn gives us a lower bound on the $\mathbb{Q}$-gonality. We mostly follow the notation of [53], stated in the language of divisors instead of line bundles.

Definition 2.1.10. A g^r_d is a subspace V of $L(D)$, for a divisor D on a curve C, such that $\deg D = d$ and $\dim V = r+1$.

Since removing the base locus of a linear series decreases the degree while preserving r, the gonality $\mathrm{gon}_{\mathbb{C}}C$ is the smallest d such that C has a g^1_d. This will be further elaborated in the proof of Corollary 2.1.14.

Definition 2.1.11. Let D be a divisor on C and K a canonical divisor on C. The *Clifford index of D* is the integer

$$\mathrm{Cliff}(D) := \deg D - 2(\ell(D)-1),$$

and the *Clifford index of C* is

$$\mathrm{Cliff}(C) := \min\{\mathrm{Cliff}(D) \mid \ell(D) \geq 2 \text{ and } \ell(K-D) \geq 2\}.$$

The *Clifford dimension of C* is defined to be

$$\mathrm{CD}(C) := \min\{\ell(D)-1 \mid \ell(D) \geq 2, \ell(K-D) \geq 2, \mathrm{Cliff}(D) = \mathrm{Cliff}(C)\}.$$

For every such divisor D that achieves the minimum we say that it computes the Clifford dimension.

The Clifford index gives bounds for the $\mathbb{C}$-gonality of X (see [15]):

$$\mathrm{Cliff}(C)+2 \leq \mathrm{gon}_{\mathbb{C}}X \leq \mathrm{Cliff}(C)+3. \tag{2.2}$$

We can see that $\mathrm{CD}(X) \geq 1$ immediately from the definition. In most cases we have $\mathrm{CD}(X) = 1$. It is a classical result that $\mathrm{CD}(X) = 2$ if and only if X is a smooth plane curve of degree ≥ 5 [53, Page 309]. Martens [69] proved that $\mathrm{CD}(X) = 3$ if and only if X is a complete intersection of two irreducible cubic surfaces in $\mathbb{P}^3$, and hence its genus is 10.

Let C be a non-hyperelliptic curve. It has a canonical embedding $C \hookrightarrow \mathbb{P}^{g-1}$. Let $S := \mathbb{C}[X_0, \ldots X_{g-1}]$, let I_C be the ideal of C and S_C be S-module $S_C := S/I_C$. Let

$$0 \to F_{g-1} \to \cdots F_2 \to F_1 \to S \to S_C \to 0 \tag{2.3}$$

be the minimal free resolution of S_C, where

$$F_i = \bigoplus_{j\in\mathbb{Z}} S(-i-j)^{\beta_{i,j}}.$$

The numbers $\beta_{i,j}$ are called *graded Betti numbers*. Green's conjecture relates graded Betti numbers with the existence of g^r_d. We state it as in [88, p.84] (note that the indices of Betti numbers are defined differently there).

Conjecture 2.1.12 (Green [33])**.** Let C be a curve of genus g. Then $\beta_{p,2} \neq 0$ if and only if there exists a divisor D on C of degree d such that a subspace g^r_d of $L(D)$ satisfies $d \leq g-1$, $r = \ell(D)-1 \geq 1$ and $d-2r \leq p$.

The "if" part of the statement has been proved by Green and Lazarsfeld in the appendix to [33].

Theorem 2.1.13 (Green and Lazarsfeld, Appendix to [33])**.** Let C be a curve of genus g. If $\beta_{p,2} = 0$, then there does not exist a divisor D on C of degree d such that a subspace g^r_d of $L(D)$ satisfies $d \leq g-1$, $r = \ell(D)-1 \geq 1$ and $d-2r \leq p$.

For the ease of the reader we state the direct consequences of this theorem that we are going to use.

Corollary 2.1.14. Let C be a curve of genus $g \geq 5$ with $\beta_{2,2} = 0$. Suppose that C is neither hyperelliptic nor trigonal. Then $\mathrm{gon}_{\mathbb{C}}(C) \geq 5$.

Proof. Suppose that $\mathrm{gon}_{\mathbb{C}}(C) = 4$. Then there is a degree 4 morphism $f : C \to \mathbb{P}^1$. We have $\mathrm{div}(f) = P - Q$, where P is a zero divisor and Q is a polar divisor. This means that $\ell(Q) \geq 2$.

Suppose that $\ell(Q) = 2$. Since $d = \deg Q = 4$, this implies the existence of g^1_4. However, from the assumptions we have $\beta_{2,2} = 0$ and by Theorem 2.1.13 (by plugging in $d = 4$, $r = 1$, $p = 2$) this is impossible. Therefore, we must have $\ell(Q) \geq 3$ and there exists another morphism $g : C \to \mathbb{P}^1$ such that $\mathrm{div}(g) = R - Q$ and $1, f, g$ are linearly independent.

Let us fix $P_0 \in C(\overline{\mathbb{Q}})$. Then the morphisms $f' := f - f(P_0)$ and $g' := g - g(P_0)$ are in $L(D)$ and have a common zero P_0. We now have

$$\operatorname{div}(f') = P_0 + P' - Q,\ \operatorname{div}(g') = P_0 + R' - Q$$

for some effective degree 3 divisors P', R'. Also, $P' \neq R'$ since the morphisms $1, f, g$ are linearly independent. Therefore, $\operatorname{div}(f'/g') = P' - R'$ and f'/g' is a non-constant morphism from C to $\mathbb{P}^1$ of degree ≤ 3, a contradiction. ■

Corollary 2.1.15. Let C be a curve of genus $g \geq 6$ with $\beta_{3,2} = 0$. Suppose that $\operatorname{gon}_{\mathbb{C}}(C) \geq 5$. Then $\operatorname{gon}_{\mathbb{C}}(C) \geq 6$.

Proof. The proof is similar to the proof of Corollary 2.1.14. ■

2.1.2. Upper bounds

In this section we give the results used to obtain upper bounds on the gonality of the curve $X_0(N)$. Most upper bounds were obtained using Proposition 2.0.2 with known rational maps from curves $X_0(N)$. We now state the Tower theorem and its two very useful corollaries.

Theorem 2.1.16 (The Tower theorem, [78, Theorem 2.1])**.** Let C be a curve defined over a perfect field k and $f : C \to \mathbb{P}^1$ be a non-constant morphism over $\overline{k}$ of degree d. Then there exists a curve C' defined over k and a non-constant morphism $C \to C'$ defined over k of degree d' dividing d such that

$$g(C') \leq \left(\frac{d}{d'} - 1\right)^2.$$

Proof. For a published proof, see [85, Proposition 2.4]. ■

Corollary 2.1.17. Let C be a curve defined over a perfect field k such that $C(k) \neq \emptyset$ and let $f : C \to \mathbb{P}^1$ be a non-constant morphism over $\overline{k}$ of prime degree d such that $g(C) > (d-1)^2$. Then there exists a non-constant morphism $C \to \mathbb{P}^1$ of degree d defined over k.

Proof. From [37, Corollary 1.7.] it immediately follows that there exists a curve C' of

genus 0 and a non-constant morphism $C \to C'$ of degree d defined over k. Since $C(k) \neq \emptyset$, it follows $C'(k) \neq \emptyset$. Hence C' is isomorphic to $\mathbb{P}^1$ over k, proving our claim. ■

Corollary 2.1.18. (i) Let C be a curve over $\mathbb{Q}$ of genus ≥ 5 which is trigonal over $\mathbb{C}$ and such that $C(\mathbb{Q}) \neq \emptyset$. Then C is trigonal over $\mathbb{Q}$.

(ii) Let C be a curve defined over $\mathbb{Q}$ with $\mathrm{gon}_{\mathbb{C}}(X) = 4$ and $g(X) \geq 10$ and such that $C(\mathbb{Q}) \neq \emptyset$. Then $\mathrm{gon}_{\mathbb{Q}}(X) = 4$.

Proof. Part (i) follows immediately from Corollary 2.1.17 by specializing C' to be $\mathbb{P}^1$ and d to be 3.

To prove part (ii) we note that, by Theorem 2.1.16, C will have a map of degree d' over $\mathbb{Q}$ dividing 4 to a curve of genus $\leq (4/d'-1)^2$, so d' cannot be 1. If d' is 2, then C is bielliptic because it admits a degree 2 rational map to an elliptic curve defined over $\mathbb{Q}$. Since every elliptic curve $E/\mathbb{Q}$ admits a degree 2 rational morphism to $\mathbb{P}^1$ (for curves in the long Weierstrass model this morphism is simply x), the curve is tetragonal over $\mathbb{Q}$ with a morphism $C \to E \to \mathbb{P}^1$. If d' is 4, then C is tetragonal over $\mathbb{Q}$, as required. ■

2.1.3. Results

In this section we apply the results of Section 2.1.1 and Section 2.1.2 to the modular curves $X_0(N)$ to obtain upper and lower bounds for their $\mathbb{Q}$ and $\mathbb{C}$-gonality. An overview of the results and the location of the proofs for each curve can be found in Appendix A, Table A.1.

Proposition 2.1.19. The $\mathbb{C}$-gonality of the curve $X_0(N)$ is at least 6 for $N \geq 198$ and

$$N \in \{114, 132, 134, 135, 140, 145, 150, 151, 152, 160, 165, 166, 168, 170, 171,$$
$$172, 174, 175, 176, 178, 182, 183, 185, 186, 189, 192, 194, 195, 196\}.$$

Proof. This is [37, Proposition 4.4]. ■

Upper bounds obtained by searching in Riemann-Roch spaces

One way of obtaining an upper bound of d on the gonality over $\mathbb{Q}$ of modular curves is to explicitly construct a morphism f of degree d. This can be done by finding an effective $\mathbb{Q}$-rational divisor D such that $\ell(D) \geq 2$.

Proposition 2.1.20. The $\mathbb{Q}$-gonality of $X_0(N)$ for $N = 85$ and 88 is at most 4.

Proof. To prove the upper bound, we construct a morphism to $\mathbb{P}^1$ of degree 4 by looking at the Riemann-Roch spaces of $\mathbb{Q}$-rational divisors of degree 4 whose support is in the quadratic points obtained by the pullbacks of rational points on $X_0^*(85)$ and $X_0^+(88)$, respectively. We note that in the case $N = 85$ we were unable to obtain such morphisms by looking at pullbacks from rational points on $X_0(N)/w_d$, for any of the Atkin-Lehner involutions. ■

Proposition 2.1.21. The $\mathbb{Q}$-gonality of $X_0(109)$ for $N = 109$ is at most 5.

Proof. We construct a morphism to $\mathbb{P}^1$ of degree 5 by looking at the Riemann-Roch spaces of $\mathbb{Q}$-rational divisors of degree 5 whose support is in the quadratic points obtained by the pullbacks of rational points on $X_0^+(109)$. ■

Proposition 2.1.22. The $\mathbb{Q}$-gonality of $X_0(112)$ is at most 6.

Proof. We explicitly find a modular unit of degree 6 whose polar divisor is supported on the 8 rational cusps (Proposition 1.3.2 tells us that the curve $X_0(112)$ has 8 rational cusps and 4 cusps defined over $\mathbb{Q}(i)$). The `Magma` computations took 10 hours to finish; see the accompanying code on Github. ■

Proposition 2.1.23. The curve $X_0(N)$ has $\mathbb{Q}$-gonality at most 6 for

$$N = 84, 93, 115, 116, 129, 137, 155, 159.$$

Proof. The quotients $X_0^+(N)$ have genus 4. We find degree 3 morphisms in $\mathbb{Q}(X_0^+(N))$ by searching the Riemann-Roch spaces of divisors of the form $P_1 + P_2 + P_3$, where $P_i \in X_0^+(N)(\mathbb{Q})$. It follows that $\mathrm{gon}_{\mathbb{Q}} X_0(N) \leq 2 \cdot \mathrm{gon}_{\mathbb{Q}} X_0^+(N) = 6$ by Proposition 2.0.2 (vi). ■

Upper bounds obtained by considering a dominant map

Another way of obtaining an upper bound is to explicitly construct a morphism $f := X_0(N) \to Y$, where $\mathrm{gon}_{\mathbb{Q}} Y$ is known. Then $\mathrm{gon}_{\mathbb{Q}} X_0(N) \leq \deg f \cdot \mathrm{gon}_{\mathbb{Q}} Y$ by Proposition 2.0.2 (vi).

Proposition 2.1.24. The $\mathbb{Q}$-gonality of $X_0(N)$ is at most 4 for

$$N = 51, 55, 56, 60, 62, 63, 65, 69, 75, 79, 83, 89, 92, 95, 101.$$

Proof. This was proved in [37, p.139]; but as the proof is short and instructive, we repeat it here. By [6] all these curves are bielliptic and have a bielliptic involution w of Atkin-Lehner type. Hence the maps $\pi : X \to X/w$ are defined over $\mathbb{Q}$, and hence so is the degree 4 morphism obtained by composing π with a degree 2 rational morphism from the elliptic curve X/w to $\mathbb{P}^1$. ■

Proposition 2.1.25. The $\mathbb{Q}$-gonality of $X_0(N)$ is at most 4 for the following values of N, with $Y := X_0(N)/w_d$.

Table 2.1: The values of N in Proposition 2.1.25.

N	$g(X_0(N))$	d	$g(Y)$	N	$g(X_0(N))$	d	$g(Y)$
42	5	42	2	77	7	77	2
52	5	52	2	80	7	80	2
57	5	57	2	87	9	87	2
58	6	29	2	91	7	91	2
66	9	11	2	98	7	98	2
67	5	67	2	100	7	4	2
68	7	68	2	103	8	103	2
70	9	35	2	107	9	107	2
73	5	73	2	121	6	121	2
74	8	74	2	125	8	125	2

Proof. This is proved in [37, p.139] and the argument of the proof is the same as of Proposition 2.1.24, with the only difference being that the quotients $X_0(N)/w_d$ are of genus 2 and hence necessarily hyperelliptic. ■

Now we produce upper bounds on the $\mathbb{Q}$-gonality by considering the degeneracy maps $X_0(N) \to X_0(d)$ for $d|N$. We will elaborate more on the degeneracy maps in Chapter 3.

For now, it is enough to know that the projection map $X_0(N) \to X_0(d)$

$$(E,C) \mapsto (E,C[d])$$

is one of the degeneracy maps and that it is defined over $\mathbb{Q}$.

Also, for a prime p, the degree of the degeneracy map $X_0(Np) \to X_0(N)$ is p if $p \mid N$ and $p+1$ if $p \nmid N$ since this is a number of groups C that have the same subgroup $C[d]$. Therefore, for $M \mid N$, it is an easy calculation that the degree of the degeneracy map $X_0(N) \to X_0(M)$ is equal to $\dfrac{\psi(N)}{\psi(M)}$ (the function ψ is defined in Lemma 2.1.7).

Proposition 2.1.26. The $\mathbb{Q}$-gonality of $X_0(N)$ is bounded from above for the following values of N, where deg denotes the degree of the degeneracy map $X_0(N) \to X_0(d)$.

Table 2.2: The values of N for Proposition 2.1.26.

N	$\mathrm{gon}_{\mathbb{Q}}(X_0(N)) \leq$	d	deg	N	$\mathrm{gon}_{\mathbb{Q}}(X_0(N)) \leq$	d	deg
72	4	36	2	144	6	48	3
82	6	41	3	148	8	74	2
90	6	30	3	150	8	50	4
96	4	48	2	156	8	78	2
99	6	33	3	160	8	80	2
108	6	36	3	175	8	25	8
117	6	39	3	176	8	88	2
118	6	59	3	184	8	92	2
132	8	66	2	192	8	96	2
136	8	68	2	196	8	98	2
140	8	70	2	200	8	100	2

Proof. There exists a morphism $f : X_0(N) \to X_0(d)$ of degree deg over $\mathbb{Q}$ by the above discussion. Therefore, $\mathrm{gon}_{\mathbb{Q}}(X_0(N)) \leq \deg \cdot \mathrm{gon}_{\mathbb{Q}}(X_0(d))$. ■

Next, we obtain upper bounds on $\mathrm{gon}_{\mathbb{Q}} X_0(N)$ by considering Atkin-Lehner quotients.

Proposition 2.1.27. The $\mathbb{C}$-gonality of $X_0(N)$ is bounded above by 6 and the $\mathbb{Q}$-gonality is bounded from above for the following values of N, with $X := X_0(N)$ and $Y := X_0(N)/w_d$.

Table 2.3: The values of N for Proposition 2.1.27.

N	$\mathrm{gon}_{\mathbb{Q}}(X) \leq$	d	$g(Y)$	$\mathrm{gon}_{\mathbb{Q}}Y \leq$	N	$\mathrm{gon}_{\mathbb{Q}}(X) \leq$	d	$g(Y)$	$\mathrm{gon}_{\mathbb{Q}}Y$
76	6	76	3	3	145	8	29	4	4
86	6	86	3	3	149	6	149	3	3
97	6	97	3	3	151	6	151	3	3
105	6	35	3	3	161	8	161	4	4
110	8	55	4	4	169	6	169	3	3
113	6	113	3	3	173	8	173	4	4
123	6	41	3	3	177	8	59	4	4
124	6	31	3	3	179	6	179	3	3
127	6	127	3	3	188	8	47	4	4
128	6	128	3	3	199	8	199	4	4
133	8	19	4	4	215	6	215	4	3
135	6	135	4	3	239	6	239	3	3
139	6	139	3	3	251	8	251	4	4
141	6	47	3	3	311	8	311	4	4

Proof. In all the above cases Y is known to not be hyperelliptic. As there exists a morphism of degree 2 over $\mathbb{Q}$ to $X_0(N)/w_d$, it follows from Proposition 2.0.2 (v),(vi) that

$$\mathrm{gon}_{\mathbb{Q}}(X_0(N)) \leq 2\mathrm{gon}_{\mathbb{Q}}(Y) \leq 2g(Y).$$

In the cases $N = 135$ and 215 in the table above where we have $\mathrm{gon}_{\mathbb{Q}}Y \leq 3 < g(Y) = 4$, this was obtained by explicitly computing the trigonal map $Y \to \mathbb{P}^1$ and observing that it is defined over $\mathbb{Q}$. ■

Proposition 2.1.28. The $\mathbb{Q}$-gonality of $X_0(N)$ is ≤ 8 for the following values of N, with $Y := X_0(N)/\langle w_{d_1}, w_{d_2} \rangle$.

Table 2.4: The values of N for Proposition 2.1.28.

N	d_1, d_2	$g(Y)$	N	d_1, d_2	$g(Y)$
102	2, 51	2	171	9, 19	3
106	2, 53	2	190	19, 95	2
114	3, 38	2	195	5, 39	3
120	8, 15	2	205	5, 41	2
126	2, 63	2	206	2, 103	2
130	10, 26	2	209	11, 19	2
134	2, 67	2	213	3, 71	2
138	3, 69	2	221	13, 17	2
153	9, 17	2	279	9, 31	5
158	2, 79	2	284	4, 71	2
165	11, 15	3	287	7, 41	2
166	2, 83	2	299	13, 23	2
168	24, 56	4			

Proof. There exists a morphism of degree 4 over $\mathbb{Q}$ to $X_0(N)/\langle w_{d_1}, w_{d_2}\rangle$. All these quotients are hyperelliptic by [32]. Therefore, $\mathrm{gon}_{\mathbb{Q}}(X_0(N)) \leq 4 \cdot 2 = 8$. ■

Proposition 2.1.29. The $\mathbb{Q}$-gonality of $X_0(N)$ is at most 6 for the following values of N, where $Y := X_0(N)/w_d$.

Table 2.5: The values of N for Proposition 2.1.29.

N	$g(X_0(N))$	d	$g(Y)$	N	$g(X_0(N))$	d	$g(Y)$
105	13	35	3	147	11	3	5
118	14	59	3	149	12	149	3
122	14	122	5	162	16	162	7
123	13	41	3	164	19	164	6
124	14	31	3	181	14	181	5

139	11	139	3	227	19	227	5
141	15	47	3	239	20	239	3
146	17	146	5				

Proof. For $N = 105, 118, 123, 124, 139, 141, 149, 239$ the quotients $Y = X_0(N)/w_d$ are trigonal over $\mathbb{Q}$ since they are of genus 3. For $N = 122, 146, 147, 162, 164, 181, 227$, the quotients are trigonal over $\mathbb{Q}$ since they are trigonal over $\mathbb{C}$ of genus ≥ 5 by [38] and we can apply Corollary 2.1.18 (i). It follows that $\mathrm{gon}_{\mathbb{Q}} X_0(N) \leq 6$. ■

Proposition 2.1.30. The curve $X_0(N)$ has $\mathbb{Q}$-gonality at most 8 for

$$N = 152, 157, 163, 183, 185, 197, 203, 211, 223, 263, 269, 359.$$

Proof. The quotients $X_0^+(N)$ have genus 5 or 6 and are not trigonal by [38]. We explicitly find degree 4 functions in $\mathbb{Q}(X_0^+(N))$ using the `Magma` functions Genus5GonalMap(C) and Genus6GonalMap(C). It follows that $\mathrm{gon}_{\mathbb{Q}} X_0(N) \leq 2 \cdot \mathrm{gon}_{\mathbb{Q}} X_0^+(N) \leq 8$. ■

Lower bounds obtained by reduction modulo p

An important technique for obtaining a lower bound for the $\mathbb{Q}$-gonality is computing the $\mathbb{F}_p$-gonality. We will use certain tricks to greatly reduce the computational time needed to give a lower bound for the $\mathbb{F}_p$-gonality. The following propositions explain how we do this in more detail. The following lemma will be useful in making the computation of $\mathrm{gon}_{\mathbb{F}_p} C$ much quicker.

Lemma 2.1.31. Let $C/\mathbb{F}_p$ be a curve such that $\#C(\mathbb{F}_p) = n$. Suppose that there exists a morphism $f : C \to \mathbb{P}^1$ of degree d. Then

(a) there exists a morphism g of degree d such that its polar divisor is supported on at most $\left\lfloor \frac{n}{p+1} \right\rfloor$ points $P \in C(\mathbb{F}_p)$.

(b) there exists a morphism h of degree d such that its polar divisor is supported on at least $\left\lceil \frac{n}{p+1} \right\rceil$ points $P \in C(\mathbb{F}_p)$.

Proof. We will prove (a), as (b) is proved analogously. As f maps $C(\mathbb{F}_p)$ into $\mathbb{P}^1(\mathbb{F}_p)$, it follows by the pigeonhole principle that there exists a $c \in \mathbb{P}^1(\mathbb{F}_p)$ such that $f^{-1}(c)$ consists of at most $\left\lfloor \frac{n}{p+1} \right\rfloor$ points. If $c = \infty$, then let $g := f$, otherwise we define $g(x) := \frac{1}{f(x)-c}$. The morphism g obviously satisfies the claim. ■

Proposition 2.1.32. The $\mathbb{Q}$-gonality of $X_0(N)$ for $N = 99$ is at least 6.

Proof. Let $C := X_0(99)$. We compute $\#C(\mathbb{F}_5) = 6$. Suppose f is an $\mathbb{F}_5$-rational morphism of degree ≤ 5. By the pigeonhole principle (as in Lemma 2.1.31), it follows that either there is a point $c \in \mathbb{P}^1(\mathbb{F}_5)$ such that $f^{-1}(c)$ contains no $\mathbb{F}_5$-rational points, or $\#f^{-1}(c)(\mathbb{F}_5) = 1$ for every $c \in \mathbb{P}^1(\mathbb{F}_5)$.

Suppose the former and let $g(x) := \frac{1}{f(x)-c}$. Therefore $g^{-1}(\infty)$ has no $\mathbb{F}_5$-rational points. Hence g lies in the Riemann-Roch space of a divisor of one of the following forms: D_5, D_4, $D_3 + D_2$ or $D_2 + D_2'$, where D_i is an irreducible $\mathbb{F}_5$-rational effective divisor of degree i. Searching among the Riemann-Roch spaces of such divisors, we find that there are no such non-constant morphisms.

Suppose now the latter. Now we can fix a $P \in C(\mathbb{F}_5)$ and suppose without loss of generality that $g^{-1}(\infty)(\mathbb{F}_5) = P$. Hence g will be found in the Riemann-Roch spaces of $P + D_4$, $P + D_2 + D_2'$ or $P + D_3$, where the notation is as before. Searching among the Riemann-Roch spaces of such divisors, we find that there are no such non-constant morphisms. ■

Proposition 2.1.33. The $\mathbb{Q}$-gonality of $X_0(N)$ for $N = 130$ is at least 8.

Proof. Let $C := X_0(130)$. We compute $\#C(\mathbb{F}_3) = 8$. Suppose f is an $\mathbb{F}_3$-rational function of degree ≤ 7. By the pigeonhole principle (as in Lemma 2.1.31), it follows that either there is a point $c \in \mathbb{P}^1(\mathbb{F}_3)$ such that $f^{-1}(c)(\mathbb{F}_3)$ contains at most one $\mathbb{F}_3$-rational point or $\#f^{-1}(c)(\mathbb{F}_3) = 2$ for every $c \in \mathbb{P}^1(\mathbb{F}_3)$.

Suppose the former and let $g(x) := \frac{1}{f(x)-c}$. Therefore $g^{-1}(\infty)$ has one $\mathbb{F}_3$-rational point. Hence f lies in the Riemann-Roch space of an effective degree 7 divisor supported on at most 1 rational point. Searching among the Riemann-Roch spaces of such divisors, we find that there are no such non-constant morphisms.

Suppose now the latter. Now we can fix a $P \in C(\mathbb{F}_3)$ and suppose without loss of generality that $g^{-1}(\infty)(\mathbb{F}_3) = \{P, Q\}$ for some $Q \in C(\mathbb{F}_3)$. Hence g will be found in the

Riemann-Roch space of an effective degree 7 divisor for which the set of rational points in the support is exactly $\{P,Q\}$, with Q varying through all $Q \in C(\mathbb{F}_3)$. Searching among the Riemann-Roch spaces of such divisors, we find that there are no such non-constant functions. ■

We apply a similar approach by producing a lower bound for the $\mathbb{F}_p$-gonality to obtain a lower bound for the $\mathbb{Q}$-gonality for a large number of N.

Proposition 2.1.34. A lower bound (LB) for the $\mathbb{Q}$-gonality of $X_0(N)$ is given in the following table, where p is a prime of good reduction for $X_0(N)$

Table 2.6: The values of N for Proposition 2.1.34 along with the running times of corresponding `Magma` programs.

N	LB	p	time	N	LB	p	time	N	LB	p	time
38	4	5	2 sec	44	4	5	4 sec	53	4	5	9 sec
61	4	3	1 sec	76	6	5	8 sec	82	6	5	62 sec
84	6	5	67 min	86	6	3	135 sec	93	6	5	4 sec
99	6	5	94 sec	102	8	5	3.3 hrs	106	8	7	35 hrs
108	6	5	27 min	109	5	3	83 sec	112	6	3	10 hrs
113	6	3	4 sec	114	8	5	53.2 hrs	115	6	3	56 sec
116	6	3	10 sec	117	6	5	10 sec	118	6	3	12 sec
122	6	3	55 sec	127	6	3	24 sec	128	6	3	4 sec
130	8	3	20 min	132	8	5	22.2 hrs	134	8	3	1.2 hrs
136	8	5	13.4 hrs	137	6	3	4 sec	140	8	3	25.6 hrs
144	6	5	56 sec	147	6	5	4.5 min	148	8	5	3.2 hrs
150	8	7	34.5 hrs	151	6	5	94 sec	152	8	3	20.5 min
153	8	5	2 hrs	154	8	5	2 days	157	8	3	37 sec
160	8	7	173 sec	162	6	5	53 sec	163	7	5	3 min
169	6	5	2.5 min	170	8	3	100.5 hrs	172	8	3	3.3 hrs
175	2	2	18.7 sec	176	8	3	12 min	178	8	3	4.5 hrs
179	6	5	10 min	180	7	7	9 days	181	6	3	9 sec

187	8	2	1.5 hrs	189	8	2	3 min	192	8	5	4 days
193	6	3	28 sec	196	8	5	2.9 hrs	197	6	3	36 min
198	8	5	7 days	200	8	3	1.6 hrs	201	8	2	4 hrs
217	8	2	2 min	229	8	3	6.5 min	233	8	2	2 hrs
241	8	2	2.5 min	247	8	2	4 hrs	277	8	5	7 days

Proof. In all the cases we compute that there are no functions of degree $< d$ in $\mathbb{F}_p(X_0(N))$, where p is as listed in the table. In computationally more demanding cases, i.e. when d, p and the genus of $X_0(N)$ are larger, we use techniques as in Propositions 2.1.32 and 2.1.33. All the `Magma` computations proving this can be found in our repository. ■

Corollary 2.1.35. The curve $X_0(212)$ is not hexagonal over $\mathbb{Q}$.

Proof. The curve $X_0(106)$ has $\mathbb{Q}$-gonality equal to 8 by Proposition 2.1.28 and Proposition 2.1.34. Therefore, the $\mathbb{Q}$-gonality of the curve $X_0(212)$ must be at least 8 by Proposition 2.0.2 (vii). ■

Proposition 2.1.36. The following genus 4 quotients $X_0(N)/w_d$ are **not** trigonal over $\mathbb{Q}$, where p is a prime of good reduction for $X_0(N)$.

Table 2.7: The values of N for Proposition 2.1.36.

N	d	p	N	d	p
110	55	7	188	47	3
145	29	11	199	199	5
161	161	5	251	251	3
173	173	5	311	311	5
177	59	5			

Proof. We find that the quotients $X_0(N)/w_d$ have no functions of degree 3 over $\mathbb{F}_p$ for d and p listed in the table above. ■

Remark 2.1.37. It is worth mentioning that Bars and Dalal [7] determined all quotients $X_0^+(N)$ which are trigonal over $\mathbb{Q}$, thereby independently obtaining the results for $N = 161, 173, 199, 251, 311$ in Proposition 2.1.36.

We can also directly use Lemma 2.1.7 and Lemma 2.1.8 to compute the number of $\mathbb{F}_{p^2}$-points on $X_0(N)$ get a lower bound on the $\mathbb{F}_p$-gonality.

Proposition 2.1.38. The curve $X_0(N)$ is not hexagonal over $\mathbb{Q}$ for $N > 335$ and

$$\begin{aligned} N \in \{&220, 222, 224-226, 228, 230-232, 234, 236-238, 242, 244-246, 248, 250, 252, \\ &254-256, 258, 260-262, 264-268, 270, 272-276, 278, 280, 282, 285, 286, 288, \\ &290, 292, 294-298, 300-306, 308-310, 312, 314-316, 318-330, 332-335\}. \end{aligned}$$

Proof. If the curve $X_0(N)$ were hexagonal over $\mathbb{Q}$, we must have $\#X_0(N)(\mathbb{F}_{p^2}) \leq 6(p^2+1)$ by setting $q = p^2$ in Lemma 2.1.8. Therefore, the inequality $L_p(N) \leq 6(p^2+1)$ must hold for every prime $p \nmid N$. Now, using the same technique as in Proposition 2.1.9 we complete the proof. ■

Proposition 2.1.39. The curve $X_0(N)$ is not hexagonal over $\mathbb{Q}$ for the following N.

Table 2.8: The values of N for Proposition 2.1.39.

N	p	$\#X_0(N)(\mathbb{F}_{p^2})$	N	p	$\#X_0(N)(\mathbb{F}_{p^2})$
182	3	64	253	2	32
207	2	32	259	2	34
208	3	68	283	3	64
216	5	168	289	2	32
218	3	64	307	3	68
235	2	32	313	3	68
240	7	312	317	2	35
243	2	33	331	2	37

Proof. For each of these N we have that $\#X_0(N)(\mathbb{F}_{p^2}) > 6(p^2+1)$ from which it follows by Lemma 2.1.8 that $X_0(N)$ is not hexagonal over $\mathbb{Q}$. ■

Lower bounds obtained by the Castelnuovo-Severi inequality

Proposition 2.1.40. The $\mathbb{Q}$-gonality and $\mathbb{C}$-gonality of $X_0(N)$ are at least 6 for N in the table below, where $Y := X_0(N)/w_d$.

Table 2.9: The values N for Proposition 2.1.40.

N	$g(X_0(N))$	d	$g(Y)$	N	$g(X_0(N))$	d	$g(Y)$
105	13	35	3	141	15	47	3
116	13	116	4	146	17	146	5
118	14	59	3	149	12	149	3
123	13	41	3	164	19	164	6
124	14	31	3	227	19	227	5
139	11	139	3	239	20	239	3

Proof. By [53] it follows that $\mathrm{gon}_{\mathbb{C}} X_0(N) \geq 5$. Suppose that $\mathrm{gon}_{\mathbb{C}} X_0(N) = 5$. We apply Castelnuovo-Severi inequality with this hypothetical degree 5 morphism to $\mathbb{P}^1$ and the degree 2 quotient map to $Y = X_0(N)/w_d$ and get

$$g(X_0(N)) \leq 5 \cdot 0 + 2 \cdot g(Y) + 4 \cdot 1.$$

These two morphisms definitely do not factor through a same morphism of degree > 1 since their degrees are 5 and 2, respectively.

However, from the table we can easily see that this is not true. Therefore, this hypothetical degree 5 morphism does not exist and we have $\mathrm{gon}_{\mathbb{C}} X_0(N) \geq 6$. ■

Proposition 2.1.41. The $\mathbb{Q}$-gonality of $X_0(N)$ is at least 8 and the $\mathbb{C}$-gonality of $X_0(N)$ is at least 6 for

$$N \in \{110, 161, 173, 177, 188, 199, 251, 311\}.$$

Proof. All these curves $X_0(N)$ have genus 4 quotients $X_0(N)/w_d$ as mentioned in Proposition 2.1.36, genus $g \geq 14$, and $\mathbb{C}$-gonality at least 5 by [53]. These genus 4 quotients $X_0(N)/w_d$ are not trigonal over $\mathbb{Q}$.

Applying Castelnuovo-Severi inequality with the hypothetical degree 5 morphism to $\mathbb{P}^1$ and the degree 2 quotient map proves $\mathrm{gon}_{\mathbb{C}} \geq 6$, similarly as in Proposition 2.1.40.

For $N \neq 173$ we repeat this procedure to prove $\mathrm{gon}_{\mathbb{Q}} X_0(N) \neq 6,7$. For $\mathrm{gon} = 7$ the application of CS is exactly the same and for $\mathrm{gon} = 6$ we need to check that the rational degree 6 morphism to $\mathbb{P}^1$ and the degree 2 quotient map do not factor through the same rational morphism of degree > 1 (we use Remark 2.1.6 here). However, if that were true, then the curve $X_0(N)/w_d$ would have to be $\mathbb{Q}$-trigonal, which is not the case by Proposition 2.1.36. Therefore, $\mathrm{gon}_{\mathbb{Q}} X_0(N) \geq 8$ in these cases.

For $N = 173$, using the same method as above we obtain $\mathrm{gon}_{\mathbb{Q}}(X_0(173)) \neq 6$. However, Castelnuovo-Severi inequality will not prove that $\mathrm{gon}_{\mathbb{Q}} \neq 7$ since $g(X_0(173)) = 14$. We explicitly compute that there are no degree 7 morphisms over $\mathbb{F}_3$ as in Proposition 2.1.34 (the computation takes 26 seconds). Therefore, $\mathrm{gon}_{\mathbb{Q}} X_0(173) \geq 8$. ■

Proposition 2.1.42. The $\mathbb{Q}$-gonality and $\mathbb{C}$-gonality of $X_0(N)$ are at least 8 for the following values of N, where $Y := X_0(N)/w_d$.

Table 2.10: The values of N for Proposition 2.1.42.

N	$g(X_0(N))$	d	$g(Y)$	N	$g(X_0(N))$	d	$g(Y)$
120	17	15	5	203	19	203	6
126	17	63	5	205	19	41	6
138	21	23	5	206	25	206	8
156	23	39	6	209	19	209	5
158	19	79	5	213	23	71	5
165	21	11	7	221	19	221	6
166	20	83	6	263	22	263	5
168	25	56	9	269	22	269	6
171	17	171	5	279	29	279	9
183	19	183	6	284	34	71	7

184	21	23	5	287	27	287	7
185	17	185	5	299	27	299	6
190	27	95	6	359	30	359	6
195	25	39	9				

Proof. Since the quotients $Y = X_0(N)/w_d$ are not trigonal over $\mathbb{C}$ by [38], by applying Castelnuvo-Severi inequality in the same way as in Proposition 2.1.41 the result follows. ■

Proposition 2.1.43. The $\mathbb{Q}$-gonality of $X_0(N)$ for $N = 271$ is 10 and the $\mathbb{C}$-gonality is 8.

Proof. The quotient $X_0^+(271)$ is of genus 6 and pentagonal over $\mathbb{Q}$ (we found a function of degree 5 using the `Magma` function Genus6GonalMap(C)). Furthermore, the quotient is not tetragonal over $\mathbb{Q}$ since it is not tetragonal over $\mathbb{F}_3$, but it is tetragonal over $\mathbb{C}$ because of Proposition 2.0.2(v). It now follows from Castelunovo-Severi and Remark 2.1.6 that there are no morphisms $f : X_0(271) \to \mathbb{P}^1$ of degree ≤ 7 defined over $\mathbb{C}$ and that there are no morphisms $f : X_0(271) \to \mathbb{P}^1$ of degree ≤ 9 defined over $\mathbb{Q}$. ■

Proposition 2.1.44. The $\mathbb{C}$-gonality for is bounded from below for the following values of N, where $Y := X_0(N)/w_d$.

Table 2.11: The levels N for Proposition 2.1.44.

N	$g(X_0(N))$	d	$g(Y)$	$\text{gon}_{\mathbb{C}} \geq$	N	$g(X_0(N))$	d	$g(Y)$	$\text{gon}_{\mathbb{C}} \geq$
102	15	51	5	6	202	24	101	9	7
129	13	129	4	6	204	31	68	12	8
150	19	75	7	6	210	41	35	15	8
152	17	152	6	6	211	17	211	6	6
155	15	155	4	6	214	26	107	9	8
159	17	159	4	6	219	23	219	8	7
174	27	87	8	8	223	18	223	6	7
175	15	175	5	6	257	21	257	7	7

186	29	62	11	8	281	23	281	7	8
194	23	97	7	8	293	24	293	8	8

Proof. Using the degree 2 quotient maps to $X_0(N)/w_d$, we can apply the Castelnuovo-Severi inequality similarly as in Proposition 2.1.41 and get the lower bound for $\mathrm{gon}_{\mathbb{C}}(X_0(N))$. ■

Lower bounds by Green's conjecture

Proposition 2.1.45. The $\mathbb{C}$-gonality and the $\mathbb{Q}$-gonality of $X_0(90)$ are equal to 6.

Proof. Let $X := X_0(90)$. We first note that the degree 3 degeneracy map to a hyperelliptic curve $X_0(30)$ gives an upper bound on the $\mathbb{Q}$-gonality. From [53, Theorem 0.1], it follows that $\mathrm{gon}_{\mathbb{C}}X > 4$. By [50, Table 1], we see that $\beta_{3,2} = 0$, and we conclude by Corollary 2.1.15 that X has no g^1_5 and that $\mathrm{gon}_{\mathbb{C}}X \geq 6$. Hence $\mathrm{gon}_{\mathbb{C}}X = \mathrm{gon}_{\mathbb{Q}}X = 6$. ■

Proposition 2.1.46. The $\mathbb{C}$-gonality of $X_0(N)$ is at least 6 for

$$N \in \{84, 86, 93, 106, 115, 127, 128, 133, 137\}.$$

Proof. By [53], $\mathrm{gon}_{\mathbb{C}}X_0(N) \geq 5$. By [50, Table 1], we see that $\beta_{3,2} = 0$ for all N in this list except 86 and 127, while for $N = 86, 127$ we compute $\beta_{3,2} = 0$ in `Magma` (the computations take 3.5 and 1.5 hours, respectively). Similarly as in Proposition 2.1.45, we conclude by Corollary 2.1.15 that $X_0(N)$ has no g^1_5 and that $\mathrm{gon}_{\mathbb{C}}X_0(N) \geq 6$. ■

2.1.4. Mordell-Weil sieving on Brill-Noether varieties

The only cases for $N < 145$ when we still have not determined the $\mathbb{Q}$-gonality of $X_0(N)$ are $N = 97$, 133. So far, we have $5 \leq \mathrm{gon}_{\mathbb{Q}}X_0(97) \leq 6$ and $\mathrm{gon}_{\mathbb{Q}}X_0(133) \leq 8$. In this section we show that the upper bound is correct in both cases and also prove that $7 \leq \mathrm{gon}_{\mathbb{Q}}X_0(145)$.

Definition 2.1.47. For a curve X, we define

$$W^r_d(X) = \{[D] : D \geq 0, \deg D = d, \ell(D) \geq r+1\}.$$

This is a closed subvariety of $\mathrm{Pic}^d(X)$.

Obviously a curve X with $X(\mathbb{Q}) \neq \emptyset$ has a function of degree d over $\mathbb{Q}$ if and only if $W_d^1(X)(\mathbb{Q}) \neq \emptyset$.

Let $X := X_0(N)$ and $\mu : \mathrm{Pic}^d X \to J_0(N)$ be the map defined by $\mu(D) := D - w(D)$. For every level N the Jacobian $J_0(N)$ can be decomposed (up to isogeny) as

$$J_0(N) \simeq J_0(N)^+ \times J_0(N)^-,$$

where

$$J_0(N)^+ = (1 + w_N)J_0(N) \subset J_0(N),$$

$$J_0(N)^- = (1 - w_N)J_0(N) \subset J_0(N).$$

These are sub-abelian varieties, defined over $\mathbb{Q}$. The subvarieties $J_0(N)^+$ and $J_0(N)^-$ are also isomorphic to quotients of $J_0(N)$ on which w_N acts as $+1$, and -1 respectively [70, Section 10]. The abelian variety $J_0(N)^+$ can be identified with the Jacobian of the quotient curve $X_0^+(N)$.

Therefore, we obviously have that $\mu(J_0(N)) \subset J_0(N)^-$. For $N = 97$ and 133, we compute that $J_0(N)^-(\mathbb{Q})$ is of rank 0 by computing that its analytic rank is 0 (see e.g. [18, Section 3]). Actually, it is a conjecture that $J_0(N)^-(\mathbb{Q})$ is of rank 0 for almost all levels N.

Suppose $D \in W_d^1(X)(\mathbb{Q})$ and let $p > 2$ be a prime of good reduction for X. We have the commutative diagram

$$\begin{array}{ccc} W_d^1(X)(\mathbb{Q}) & \xrightarrow{\mu} & J_0(N)^-(\mathbb{Q}) \\ \downarrow{\scriptstyle \mathrm{red}_p} & & \downarrow{\scriptstyle \mathrm{red}_p} \\ W_d^1(X)(\mathbb{F}_p) & \xrightarrow{\mu} & J_0(N)^-(\mathbb{F}_p) \end{array},$$

where the vertical maps are reduction modulo p. Suppose now that there exists a $D \in W_d^1(X)(\mathbb{Q})$. Then $\mu(D)$ lies in $\mathrm{red}_p^{-1}(\mu(W_d^1(X)(\mathbb{F}_p)))$. The set $W_d^1(X)(\mathbb{F}_p)$ can be computed in practice by simply finding all the effective degree d divisors whose Riemann-Roch spaces have dimension ≥ 2. Note that in our cases $J_0(N)^-(\mathbb{Q})$ is a torsion group and red_p is injective on the torsion of $J_0(N)(\mathbb{Q})$ [56, Appendix]. The same procedure can

be applied for a set S of multiple primes $p > 2$ of good reduction, in which case we get

$$\mu(D) \in \bigcap_{p \in S} \mathrm{red}_p^{-1}(\mu(W_d^1(X)(\mathbb{F}_p))).$$

If

$$\bigcap_{p \in S} \mathrm{red}_p^{-1}(\mu(W_d^1(X)(\mathbb{F}_p))) = \emptyset$$

it follows that $W_d^1(X)(\mathbb{Q}) = \emptyset$ and indeed this is what we will show. In our cases it will be enough to take S consisting of a single prime.

Proposition 2.1.48. The $\mathbb{Q}$-gonality of $X_0(97)$ is 6 and the $\mathbb{Q}$-gonality of $X_0(133)$ is 8. The $\mathbb{Q}$-gonality of $X_0(145)$ is ≥ 7.

Proof. By [70, Theorem 4] we know that for primes p the torsion is $J_0(p)_{\mathrm{tors}} \simeq \mathbb{Z}/m\mathbb{Z}$, where p is the numerator of $\frac{p-1}{12}$. It is generated by $D_0 = [0-\infty]$, where 0 and ∞ are the two cusps of $X_0(p)$. Therefore, $J_0(97)^-(\mathbb{Q}) \simeq \mathbb{Z}/8\mathbb{Z}$. We compute

$$\mathrm{red}_3^{-1}(\mu(W_5^1(X_0(97)(\mathbb{F}_3)))) = \{0\}, \quad \mathrm{red}_5^{-1}(\mu(W_5^1(X_0(97)(\mathbb{F}_5)))) = \{D_0, 7D_0\},$$

$$\mathrm{red}_7^{-1}(\mu(W_5^1(X_0(97)(\mathbb{F}_7)))) = \emptyset.$$

Hence sieving with either $\{3,5\}$ or just the prime 7 proves that $W_5^1(X_0(97))(\mathbb{Q}) = \emptyset$. It follows that $X_0(97)$ is of gonality 6 over $\mathbb{Q}$.

The cases of $X_0(133)$ and $X_0(145)$ are more involved than $X_0(97)$ because we cannot compute the torsion group exactly. The rank of $J_0(N)^-(\mathbb{Q})$ is 0 in both cases, so $J_0(N)^-(\mathbb{Q})$ is contained in $J_0(N)(\mathbb{Q})_{\mathrm{tors}}$.

First, we solve the case $N = 133$. Using the methods of [18, Section 4], we obtain that $J_0(N)(\mathbb{Q})_{\mathrm{tors}}$ is isomorphic to a subgroup of $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/360\mathbb{Z}$. We find cuspidal divisors (i.e. divisors supported on cusps of $X_0(N)$) A, B which generate a subgroup $T := \langle A, B \rangle \simeq \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/180\mathbb{Z}$. Thus it follows that for any $x \in J_0(N)^-(\mathbb{Q})$, we have $2x \in T$. Hence we use the map 2μ, sending a divisor D to $2(D - w(D))$ instead of μ (which we used for $X_0(97)$). For sieving, we will just need to use the prime 3.

We observe that $\#X_0(133)(\mathbb{F}_3) = 8$, so if there exists a function of degree 7 on $X_0(133)$ over $\mathbb{Q}$, then there has to exist a function of degree 7 over $\mathbb{Q}$ whose reduction modulo

3 has a polar divisor that is supported on at most 2 $\mathbb{F}_3$-rational points, using the same arguments as in Lemma 2.1.31. Thus we need only search effective divisors supported on at most 2 $\mathbb{F}_3$-rational points; if $R \subset W_7^1(X_0(133))(\mathbb{F}_3)$ is the set of all divisors classes in $W_7^1(X_0(133))(\mathbb{F}_3)$ represented by divisors supported on at most 2 $\mathbb{F}_3$-rational points, then

$$\mathrm{red}_3^{-1}(2\cdot\mu(R)) = \emptyset \quad \text{implying that} \quad \mathrm{red}_3^{-1}(2\cdot\mu(W_7^1(X_0(133))(\mathbb{F}_3))) = \emptyset.$$

This proves that $\mathrm{gon}_{\mathbb{Q}}(X_0(133)) = 8$.

Now we give a lower bound for $N = 145$. Using the methods of [18, Section 4] again, we obtain that $J_0(N)(\mathbb{Q})_{\mathrm{tors}}$ is isomorphic to a subgroup of $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/14\mathbb{Z}\times\mathbb{Z}/140\mathbb{Z}$.

We find cuspidal divisors A, B which generate a subgroup $T := \langle A, B\rangle \simeq \mathbb{Z}/14\mathbb{Z}\times\mathbb{Z}/140\mathbb{Z}$. Hence we use the map 2μ as in the case $N = 133$. For sieving, we will again just need to use the prime 3. Using the same techniques as for the $N = 133$ we obtain

$$\mathrm{red}_3^{-1}(2\cdot\mu(R)) = \emptyset \quad \text{implying that} \quad \mathrm{red}_3^{-1}(2\cdot\mu(W_6^1(X_0(145))(\mathbb{F}_3))) = \emptyset$$

which proves that the $\mathbb{Q}$-gonality of $X_0(145)$ is ≥ 7 as desired. ■

For $N = 97$, the program described in Proposition 2.1.48 terminates after 7.6 minutes, for $N = 133$ after 6.3 hours, and for $N = 145$ after 1.6 minutes.

Remark 2.1.49. The Mordell-Weil sieve fails to prove that $\mathrm{gon}_{\mathbb{Q}}X_0(145) \geq 8$ because

$$\bigcap_{p\leq 19} \mathrm{red}_p^{-1}(2\cdot\mu(W_7^1(X_0(145))(\mathbb{F}_p))) \neq \emptyset.$$

The computations take too long for the larger primes and would likely give the same result. On the other hand, we were unable to find a degree 7 rational morphism to $\mathbb{P}^1$.

All rational points on $X_0(145)$ are the 4 rational cusps by Theorem 1.3.4. There are finitely many quadratic points on $X_0(145)$ since it is neither hyperelliptic nor bielliptic [35, Corollary 3]. However, all degree 7 rational effective divisors supported on the rational cusps and quadratic points we found have Riemann-Roch dimension 1.

2.1.5. Proofs of the main theorems

First, observe that Theorem 2.1.1 follows from the fact that the upper and lower bounds in Table A.1 agree. We now prove Theorems 2.1.2, 2.1.3 and 2.1.4. Before proceeding with the proofs, recall that Ogg [80] determined the hyperelliptic curves $X_0(N)$ and Hasegawa and Shimura [37] determined all $X_0(N)$ that are trigonal over $\mathbb{Q}$.

Proof of Theorem 2.1.2. By [37, Proposition 4.4] the $\mathbb{C}$-gonality (and therefore the $\mathbb{Q}$-gonality) of $X_0(N)$ is ≥ 5 for $N \geq 192$. Hence, we only need to consider the $N \leq 191$ such that $X_0(N)$ is not of gonality ≤ 3 over $\mathbb{Q}$ and such that the gonality over $\mathbb{C}$ is not ≥ 5. For these values, the results follow from Theorem 2.1.1. ■

Proof of Theorem 2.1.3. In Theorem 2.1.2 we determined all the curves $X_0(N)$ that are tetragonal over $\mathbb{Q}$. Proposition 2.1.21 and Proposition 2.1.34 tell us that for $N = 109$ the curve is pentagonal over $\mathbb{Q}$.

Hasegawa and Shimura [37, Proposition 4.4] have proved that the $\mathbb{C}$-gonality (and therefore the $\mathbb{Q}$-gonality) of the curve $X_0(N)$ is ≥ 6 for $N \geq 198$. In Theorem 2.1.1 we proved that for the remaining (i.e. those not of $\mathbb{Q}$-gonality ≤ 4) $X_0(N)$ with $N \leq 197$, the $\mathbb{Q}$-gonality is ≥ 6. Hence it follows that for $N \neq 109$ the $\mathbb{Q}$-gonality is either smaller or larger than 5, proving the result. ■

Proof of Theorem 2.1.4. The proof is similar to the proofs of Theorems 2.1.2 and 2.1.3. It follows from Theorem 2.1.1 and Propositions 2.1.19 - 2.1.48. ■

2.1.6. Limits of our methods

It is a natural question what stopped us from going further, i.e. determining the gonality for larger N. Unfortunately, as N gets larger, computations get much harder. As the genus of $X_0(N)$ becomes larger, computing models, their quotients, and computations in Riemann-Roch spaces over $\mathbb{Q}$ all become much more difficult. Furthermore, as the gonalities get larger, the degrees of divisors and the sheer number of divisors needed to be considered (as in Proposition 2.1.34) makes computations of the $\mathbb{F}_p$-gonality far more difficult.

In particular, the most computationally demanding computations that we do are the ones to determine a lower bound for the $\mathbb{F}_p$-gonality. This requires computing the dimension of a huge number of Riemann-Roch spaces. While the complexity of computing a single Riemann-Roch space is polynomial in the size of the input (see [41]), the number of Riemann-Roch spaces that need to be computed to give a lower bound of d for the $\mathbb{F}_p$-gonality is $O(p^d)$. By [1, Theorem 0.1] we can expect the gonality of $X_0(N)$ to grow linearly in N, which suggests that the number of Riemann-Roch spaces that need to be checked grows exponentially with N (and doubly exponentially with the size of N). The necessity of choosing (very) small p when computing the $\mathbb{F}_p$-gonality is clear from the complexity discussion above.

It should be clear that our methods do not give an algorithm for computing the gonality of $X_0(N)$. They produce a lower bound and an upper bound, but there is no guarantee that they will be equal. In practice, this (the bounds not matching) is exactly what happens for N larger than the ones that we list in our results. It often happens that for a curve X, one has $\mathrm{gon}_{\mathbb{F}_p} X < \mathrm{gon}_{\mathbb{Q}} X$. For example, this happens when $n = \mathrm{gon}_{\mathbb{C}} X < \mathrm{gon}_{\mathbb{Q}} X$, and a degree n map to $\mathbb{P}^1$ is defined over a number field K in which p splits completely. Then it follows that $\mathrm{gon}_{\mathbb{F}_p} X \leq n$, hence the lower bound obtained by computing $\mathrm{gon}_{\mathbb{F}_p} X$ will not be sharp.

In practice, for the levels N where we started encountering difficulties and could not compute the exact gonality, the bounds not matching was the more common problem than the computations being too demanding.

2.2. TETRAGONAL MODULAR QUOTIENTS $X_0^{+d}(N)$

After determining the gonality of modular curves $X_0(N)$, we now consider quotient curves $X_0^{+d}(N) = X_0(N)/w_d$. Much progress has been made in studying the $\mathbb{Q}$-gonality of the quotients of $X_0(N)$ as well. Furumoto and Hasegawa [32] determined all hyperelliptic quotients of $X_0(N)$, Hasegawa and Shimura [38–40] determined all trigonal quotients of $X_0(N)$ over $\mathbb{C}$ and partially determined the $\mathbb{Q}$-trigonal quotients (more precisely, they solved all cases when the genus is not equal to 4). Furthermore, Bars, Gonzalez and Kamel [8] determined all bielliptic quotients of $X_0(N)$ for squarefree levels, Jeon [44] determined all bielliptic curves $X_0^+(N)$, and Bars, Kamel and Schweizer [9] determined all bielliptic quotients of $X_0(N)$ for non-squarefree levels.

The next logical step is determining all tetragonal quotients of $X_0(N)$. In this thesis we will study the $\mathbb{Q}$ and $\mathbb{C}$-gonality of quotient curves $X_0^{+d}(N) = X_0(N)/w_d$ (w_d being an Atkin-Lehner involution).

One of the reasons we study the gonality of $X_0^{+d}(N)$, apart from being an interesting question in itself, is that it can help us to determine the gonality of $X_0(N)$. The reason for that is, of course, that we have a natural rational quotient map $X_0(N) \to X_0^{+d}(N)$ of degree 2. Therefore, any map $X_0^{+d}(N) \to \mathbb{P}^1$ of degree d induces a map $X_0(N) \to \mathbb{P}^1$ of degree $2d$ defined over the same base field.

Also, the existence of rational degree d maps to $\mathbb{P}^1$ is closely linked to the problem of determining whether that curve has infinitely many points of degree d, as can for example be seen in [2, 35], and, more recently, Theorems 3.0.4 and 3.4.1.

For a field K, a K-curve is an elliptic curve defined over some finite separable extension of K which is isogenous over $\overline{K}$ to all its $\mathrm{Gal}(\overline{K}/K)$ conjugates [27, Page 81]. The $\mathbb{Q}$-curves are the most studied of the K-curves. There is a number of papers which use Frey $\mathbb{Q}$-curves defined over quadratic fields to solve Diophantine equations. Some of the more recent ones are [68, 84].

Non-cuspidal rational points on the curve $X_0^+(N)$ correspond to a pair of elliptic curves with a degree N isogeny between them. Furthermore, these two elliptic curves are either

[77, Section 2]

- a $\mathbb{Q}$-curve defined over a quadratic field together with its Galois conjugate, or
- two elliptic curves over $\mathbb{Q}$.

Similarly, for a number field K, K-rational points on the curve $X_0^+(N)$ represent pairs of K-curves of degree N defined over a quadratic extension of K and pairs of elliptic curves over K with a degree N isogeny between them. Therefore, determining the $\mathbb{Q}$-gonality of curves $X_0^+(N)$ could be useful in determining whether there are infinitely many K-curves of a certain degree defined over a quadratic extension of K (see Section 3 for further explanation).

Our main results are the following theorems (though the first theorem was already mostly proved by Hasegawa and Shimura).

Theorem 2.2.1. The curve $X_0^{+d}(N) := X_0(N)/w_d$ is of genus 4 and has $\mathbb{Q}$-gonality equal to 3 if and only if

$$\begin{aligned}(N,d) \in \{&(66,33),(74,37),(84,84),(86,43),(88,88),(93,93),(108,4),(112,7),\\ &(115,115),(116,116),(129,129),(135,135),(137,137),(147,147),\\ &(155,155),(159,159),(215,215)\}.\end{aligned}$$

Theorem 2.2.2. The curve $X_0^{+d}(N) := X_0(N)/w_d$ has $\mathbb{Q}$-gonality equal to 4 if and only if the pair (N,d) is in the following table. In all cases when the genus of the curve $X_0^{+d}(N)$ is not 4 (all genus 4 cases are listed in Proposition 2.2.6), the $\mathbb{C}$-gonality is also equal to 4.

Additionally, for $N = 243, 271$, the curve $X_0^+(N)$ is tetragonal over $\mathbb{C}$, but not over $\mathbb{Q}$.

Table 2.12: $\mathbb{Q}$-tetragonal curves $X_0^{+d}(N)$.

N	d	N	d	N	d
60	3, 5	66	2, 3, 22	68	17
70	2, 5, 7, 70	74	2	76	4
77	11	78	2, 3, 6, 13, 78	80	5
82	2, 82	84	3,4,7,12,21,28	85	5, 17
88	8, 11	90	2,5,9,10,18,45,90	91	7
93	3, 31	96	3	98	2
99	9	100	25	102	2, 3, 17, 51, 102
104	8, 13	105	3,5,7,15,21,35,105	106	2,53,106
108	27, 108	110	2,5,10,11,22,55,110	111	3, 37
112	16, 112	114	2, 3, 19, 38, 114	115	5, 23
116	4, 29	117	9, 117	118	2, 59, 118
120	5, 8, 15, 24, 40, 120	122	2, 61	123	3, 41, 123
124	4, 31, 124	126	2,7,9,14,18,63,126	129	3, 43
130	2, 10, 13, 26, 65	132	4, 11, 44	133	19, 133
134	2, 67, 134	135	5, 27	136	8, 17, 136
138	3, 6, 23, 69, 138	140	4, 35, 140	141	3, 47, 141
142	2, 71, 142	143	11, 13	144	9, 16, 144
145	29, 145	146	2, 73	147	49
148	4, 148	152	152	153	9, 17
155	5, 31	156	4, 39, 156	157	157
158	2, 79, 158	159	3, 53	160	32, 160
161	7, 23, 161	163	163	165	11, 15, 165
166	2, 83, 166	168	21, 24, 56	171	9, 19, 171
173	173	175	175	176	11, 16, 176
177	3, 59, 177	183	183	184	8, 23, 184
185	185	188	4, 47, 188	190	5, 10, 19, 95
192	192	193	193	194	194
195	5, 39, 195	196	4	197	197

199	199	200	200	203	203
205	5, 41, 205	206	2, 103, 206	207	9, 23, 207
209	11, 19, 209	211	211	213	3, 71, 213
215	5, 43	221	13, 17, 221	223	223
224	224	229	229	241	241
251	251	257	257	263	263
269	269	279	9, 31, 279	281	281
284	4, 71, 284	287	7, 41, 287	299	13, 23, 299
311	311	359	359		

As a consequence, in Corollary 2.2.19 we were able to determine the $\mathbb{Q}$-gonality of $X_0(N)$ for several new levels N that were not previously solved in [76].

It is perhaps surprising that we were able to determine all tetragonal curves $X_0^+(N)$ using mostly previously known methods. One of the reasons for that is that in many cases we can get the degree 4 map from a degree 2 quotient map to $X_0(N)/\langle w_d, w_N\rangle$, as presented in Proposition 2.2.10 and Proposition 2.2.11. If one would, for example, search for all pentagonal curves $X_0^+(N)$, there is no such natural source of degree 5 maps.

We use similar methods to the ones used in Section 2.1 to determine the tetragonal curves $X_0^{+d}(N)$. In Section 2.2.1, we give lower bounds on the $\mathbb{Q}$-gonality by computing the gonality over finite fields. In Section 2.2.2, we give lower bounds on the $\mathbb{C}$-gonality via the Castelnuovo-Severi inequality. In Section 2.2.3, we construct degree 4 rational morphisms to $\mathbb{P}^1$, either via quotient maps to curves $X_0(N)/\langle w_d, w_{d'}\rangle$ or by finding degree 4 effective rational divisors of Riemann-Roch dimension 2 using `Magma`. In Section 2.2.4, we use Theorem 2.0.3 and graded Betti numbers to disprove the existence of degree 4 morphisms to $\mathbb{P}^1$.

Note that for each level N that is not a prime power, there are multiple quotients $X_0^{+d}(N)$ that need to be checked. For example, for $N = 210$ which has four different prime factors, there are 15 such quotients. Therefore, it can be hard to track whether all quotients have been solved.

For the reader's convenience, in Appendix B at the end of the thesis we put Table B.1.

In this table, for each level N, we give the links to all propositions used to solve the quotients at that level.

A lot of the results in this section rely on `Magma` computations. The codes that verify all computations in this section can be found on

https://github.com/orlic1/gonality_X0_quotients.

Additionally, code and data associated with the paper [86] by Jeremy Rouse, Andrew V. Sutherland, and David Zureick-Brown was used in Proposition 2.2.3 and Proposition 2.2.4. Their code can be found on

https://github.com/AndrewVSutherland/ell-adic-galois-images/tree/209c2f888669785151174f472ea2c9eafb6daaa9.

2.2.1. $\mathbb{F}_p$-gonality

From Lemma 2.1.7 and Lemma 2.1.8 we can get a lower bound on the $\mathbb{Q}$-gonality of the curve $X_0^{+d}(N)$. Namely, if the quotient curve $X_0^{+d}(N)$ is tetragonal over $\mathbb{Q}$, then there exists a rational composition map $X_0(N) \to X_0^{+d}(N) \to \mathbb{P}^1$ of degree 8. Therefore, we must have

$$L_p(N) \leq 8(p^2+1) \tag{2.4}$$

for all primes $p \nmid N$. However, similarly as in Proposition 2.1.9, we get that for $N \geq 456$ there exists a prime p for which this inequality does not hold. This means that we have eliminated all but finitely many levels N. This inequality can in the same way be used to eliminate

$$\begin{aligned} N \in \{&255, 260, 266, 276, 280, 282, 285, 286, 290, 292, 294, 296, 304, 306, 308, 310, 312, 314, \\ &315, 316, 318, 320, 322, 324, 326, 327, 328, 330, 332, 333, 334, 336, 338, 339, 340, 342, \\ &344, 345, 346, 348, 350, 351, 352, 354, 356, 357, 358, 360, 362-366, 368, 369, 370, \\ &372, 374, 375, 376, 378, 380, 381, 382, 384-388, 390, 392-396, 398, 399, 400, \\ &402-408, 410-418, 422-430, 432, 434-438, 440, 441, 442, 444-448, 450-455\}. \end{aligned}$$

We can also use Lemma 2.1.8 directly to deal with some cases.

Proposition 2.2.3. The curve $X_0^+(N)$ is not tetragonal over $\mathbb{Q}$ for the following values of N.

Table 2.13: The values of N in Proposition 2.2.3.

N	p	$\#X_0^+(N)(\mathbb{F}_{p^2})$	N	p	$\#X_0^+(N)(\mathbb{F}_{p^2})$	N	p	$\#X_0^+(N)(\mathbb{F}_{p^2})$
268	3	46	272	3	42	273	2	26
274	3	48	288	5	116	291	2	21
297	2	27	298	3	45	301	2	21
305	2	24	309	2	23	323	2	23
325	2	23	341	2	25	343	3	43
347	2	21	349	2	22	353	2	22
355	2	22	361	2	22	367	2	46
371	2	25	373	2	21	377	2	24
379	2	22	389	2	24	391	2	24
397	3	41	401	2	24	409	2	25
419	2	23	421	2	25	433	2	23
439	2	22	443	2	25	449	2	26

Proof. Using `Magma`, we calculate the number of $\mathbb{F}_{p^2}$ points on $X_0^+(N)$. It is now easy to check that $\#X_0^+(N)(\mathbb{F}_{p^2}) > 4(p^2+1)$ in all these cases. ■

Proposition 2.2.4. The curve $X_0^{+d}(N)$ is not tetragonal over $\mathbb{Q}$ for $N = 420$ and all 15 possible values of d.

Proof. Using `Magma`, we calculate that the curve $X_0(420)$ has 1128 points over $\mathbb{F}_{11^2}$. Lemma 2.1.8 now tells us that the $\mathbb{Q}$-gonality of the curve $X_0(420)$ is at least 10. Therefore, the $\mathbb{Q}$-gonality of all quotient curves $X_0^{+d}(420)$ is at least 5. ■

We continue computing the $\mathbb{F}_p$-gonality of curves $X_0^{+d}(N)$, similarly as in Proposition 2.1.34.

Proposition 2.2.5. The $\mathbb{F}_p$-gonality of the curve $X_0^+(N)$ is bounded from below for the following values of N.

Table 2.14: The values of N in Proposition 2.2.5.

N	p	$\text{gon}_{\mathbb{F}_p} \geq$	N	p	$\text{gon}_{\mathbb{F}_p} \geq$	N	p	$\text{gon}_{\mathbb{F}_p} \geq$	N	p	$\text{gon}_{\mathbb{F}_p} \geq$
70	11	4	82	3	4	90	11	4	108	5	4
117	7	4	130	3	5	132	5	5	150	7	5
154	3	5	161	2	4	168	5	5	170	3	5
172	3	5	173	5	4	174	5	5	178	3	5
180	7	5	182	3	5	187	3	5	189	2	5
196	3	5	198	5	5	199	5	4	201	2	5
202	3	5	204	5	5	208	3	5	212	3	5
216	5	5	217	2	5	218	3	5	219	2	5
225	2	5	226	3	5	228	5	5	230	3	5
231	2	5	232	3	5	233	2	5	234	5	5
235	2	5	237	2	5	240	7	5	242	3	5
243	7	5	244	3	5	245	2	5	247	3	5
250	3	5	251	2	4	253	2	5	256	3	5
259	2	5	261	2	5	265	2	5	271	3	5
275	2	5	277	2	5	283	2	5	289	2	5
293	2	5	307	2	5	311	2	4	313	2	5
317	2	5	319	2	5	331	2	5	335	2	5
337	2	5	383	2	5						

Proof. Using `Magma`, we compute that there are no functions of degree $< d$ in $\mathbb{F}_p(X_0^+(N))$. We can reduce the number of divisors that need to be checked by noting the following: If there exists a function f over a field k of a certain degree and if $c \in k$, then the function $g(x) := \frac{1}{f(x)-c}$ has the same degree and its polar divisor contains a k-rational point. ■

Proposition 2.2.6. The $\mathbb{Q}$-gonality of the genus 4 curve $X_0^{+d}(N)$ is equal to 4 for the following values of N and d.

Table 2.15: The values of N and d in Proposition 2.2.6.

$(N,d))$	p	(N,d)	p	(N,d)	p	(N,d)	p
$(60,3)$	7	$(60,5)$	7	$(66,2)$	13	$(68,17)$	3
$(70,5)$	17	$(74,2)$	3	$(76,4)$	5	$(77,11)$	3
$(80,5)$	7	$(82,2)$	7	$(85,5)$	23	$(85,17)$	7
$(88,8)$	5	$(91,7)$	11	$(93,3)$	5	$(98,2)$	11
$(100,25)$	3	$(108,27)$	5	$(110,55)$	7	$(133,19)$	5
$(145,29)$	11	$(177,59)$	5	$(188,47)$	3		

Proof. Using `Magma`, we compute that there are no functions of degree ≤ 3 in $\mathbb{F}_p(X_0^{+d}(N))$, similarly as in Proposition 2.2.5.

On the other hand, all these curves are of genus 4 and have at least one rational cusp. By Proposition 2.0.2(iv), this implies that their $\mathbb{Q}$-gonality is at most 4. ■

Proposition 2.2.7. The $\mathbb{Q}$-gonality of the curve $X_0^{+d}(N)$ is at least 5 for the following values of N and d.

Table 2.16: The values of N and d in Proposition 2.2.7.

(N,d)	p	(N,d)	p	(N,d)	p	(N,d)	p	(N,d)	p
$(132,33)$	5	$(140,5)$	3	$(140,28)$	3	$(150,25)$	7	$(154,2)$	3
$(154,7)$	3	$(154,11)$	3	$(154,14)$	5	$(154,22)$	5	$(154,77)$	3
$(164,41)$	3	$(165,3)$	2	$(165,5)$	2	$(165,33)$	7	$(165,55)$	2
$(168,3)$	5	$(168,7)$	5	$(168,8)$	5	$(170,2)$	7	$(170,5)$	3
$(170,10)$	3	$(170,17)$	3	$(170,34)$	3	$(170,85)$	3	$(172,4)$	3
$(180,4)$	7	$(180,5)$	7	$(180,9)$	7	$(180,20)$	7	$(180,36)$	7
$(180,45)$	7	$(186,2)$	5	$(186,31)$	5	$(186,62)$	5	$(192,3)$	5

$(192,64)$	5	$(195,13)$	2	$(198,11)$	5	$(198,22)$	5	$(198,99)$	5
$(200,8)$	3	$(200,25)$	3	$(201,3)$	2	$(201,67)$	2	$(204,68)$	5
$(208,13)$	3	$(210,35)$	11	$(212,4)$	3	$(212,53)$	5	$(216,8)$	5
$(216,27)$	5	$(218,2)$	5	$(218,109)$	5	$(219,3)$	5	$(219,73)$	2
$(220,55)$	3	$(224,7)$	5	$(225,25)$	2	$(226,2)$	3	$(226,113)$	3
$(232,8)$	3	$(232,29)$	3	$(234,13)$	5	$(234,26)$	5	$(234,117)$	5
$(235,5)$	7	$(235,47)$	3	$(237,3)$	2	$(232,79)$	7	$(240,80)$	11
$(242,2)$	3	$(242,121)$	3	$(244,4)$	3	$(244,61)$	3	$(247,13)$	5
$(247,19)$	5	$(250,125)$	3	$(252,63)$	5	$(253,11)$	2	$(253,23)$	3
$(254,127)$	3	$(258,86)$	5	$(259,7)$	5	$(261,29)$	2	$(265,5)$	3
$(265,53)$	3	$(268,4)$	3	$(268,67)$	3	$(272,16)$	3	$(274,137)$	3
$(275,11)$	2	$(278,139)$	3	$(288,9)$	5	$(288,32)$	5	$(291,3)$	5
$(297,11)$	2	$(298,149)$	3	$(301,7)$	3	$(301,43)$	3	$(302,151)$	3
$(323,19)$	3	$(325,25)$	7	$(355,71)$	3				

Proof. Similarly as in the previous proposition, we use `Magma` to compute that there are no functions of degree ≤ 4 in $\mathbb{F}_p(X_0^{+d}(N))$. ■

Some computations in Proposition 2.2.7 were running for more than an hour, especially in the higher genus cases. This approach is not feasible for the curves in the next proposition which are all of high genus. For example, the curve $X_0^{+6}(246)$ is of genus 20 and the curve $X_0^{+3}(300)$ is of genus 22. Instead, we can prove that the quotient curve $X_0(N)/\langle w_d, w_{d'}\rangle$, which is of smaller genus, is not tetragonal.

Proposition 2.2.8. The $\mathbb{Q}$-gonality of the curve $X_0^{+d}(N)$ is at least 5 for the following values of N and d.

Table 2.17: The values of N and d in Proposition 2.2.8.

N	d	p	Y	N	d	p	Y
228	3, 19, 57	5	$X_0(228)/\langle w_3, w_{19}\rangle$	228	12, 57, 76	5	$X_0(228)/\langle w_{12}, w_{57}\rangle$
228	4, 57	5	$X_0(228)/\langle w_4, w_{57}\rangle$	240	3, 5, 15	11	$X_0(240)/\langle w_3, w_5\rangle$
240	3, 16, 48	11	$X_0(240)/\langle w_3, w_{16}\rangle$	246	6, 82, 123	5	$X_0(246)/\langle w_6, w_{82}\rangle$
246	3, 82	5	$X_0(246)/\langle w_3, w_{82}\rangle$	264	3, 8, 24	5	$X_0(264)/\langle w_3, w_8\rangle$
264	3, 11, 33	5	$X_0(264)/\langle w_3, w_{11}\rangle$	264	8, 11, 88	5	$X_0(264)/\langle w_8, w_{11}\rangle$
270	5, 27, 135	7	$X_0(270)/\langle w_5, w_{27}\rangle$	300	3, 100	7	$X_0(300)/\langle w_3, w_{100}\rangle$
300	12, 25	7	$X_0(300)/\langle w_{12}, w_{25}\rangle$	309	3, 103	5	$X_0(309)/\langle w_3, w_{103}\rangle$

Proof. Using `Magma`, we compute that there are no $\mathbb{F}_p$-rational functions of degree ≤ 4 from Y to $\mathbb{P}^1$. in $\mathbb{F}_p(X_0(N)/\langle w_d, w_{d'}\rangle)$. Since there is a rational degree 2 quotient map $X_0^{+d}(N) \to Y$, Proposition 2.0.2(vii) tells us that $\mathbb{F}_p$-gonality of $X_0^{+d}(N)$ is ≥ 5. ■

In Section 2.2.4, we will use Corollary 2.1.18 to see that all curves of genus at least 10 that are not $\mathbb{Q}$-tetragonal are also not $\mathbb{C}$-tetragonal. Furthermore, all such curves have been solved in this section.

2.2.2. Castelnuovo-Severi inequality

In this section we use the Castelnuovo-Severi inequality (Proposition 2.1.5) to obtain a lower bound on the $\mathbb{Q}$ and $\mathbb{C}$-gonality of curves $X_0^{+d}(N)$.

Proposition 2.2.9. The $\mathbb{C}$-gonality of the curve $X_0^{+d}(N)$ is at least 5 for the following values of N and d. Here g denotes the genus of the curve $X_0^{+d}(N)$ and g' denotes the genus of the quotient curve $X_0(N)/\langle w_d, w_{d'}\rangle$.

Table 2.18: The values of N and d in Proposition 2.2.9.

(N,d)	g	d'	g'	(N,d)	g	d'	g'	(N,d)	g	d'	g'
$(132,3)$	10	44	3	$(132,12)$	10	11	3	$(138,2)$	11	23	3
$(138,46)$	11	2	3	$(140,7)$	10	20	3	$(150,2)$	10	75	3
$(150,3)$	10	50	3	$(156,3)$	11	13	3	$(156,12)$	11	52	3
$(156,13)$	12	3	3	$(156,52)$	12	12	3	$(174,2)$	14	87	3
$(174,3)$	14	29	3	$(174,6)$	13	58	4	$(174,29)$	13	3	3
$(174,58)$	14	6	4	$(182,2)$	13	91	4	$(182,7)$	13	26	4
$(182,13)$	12	14	4	$(182,14)$	11	26	3	$(182,26)$	10	14	3
$(182,91)$	10	14	3	$(183,61)$	10	3	3	$(186,3)$	14	62	4
$(186,6)$	14	62	5	$(186,62)$	14	6	5	$(186,186)$	12	3	3
$(190,2)$	14	95	3	$(190,38)$	14	10	3	$(190,190)$	13	2	3
$(195,3)$	13	65	3	$(195,15)$	13	39	3	$(198,2)$	14	99	5
$(198,9)$	15	11	5	$(204,3)$	16	68	5	$(204,4)$	15	51	5
$(204,12)$	16	51	5	$(204,17)$	16	4	6	$(210,2)$	21	35	8
$(210,3)$	21	35	7	$(210,5)$	19	7	7	$(210,6)$	19	35	6
$(210,7)$	21	5	7	$(210,10)$	21	14	6	$(210,14)$	16	10	6
$(210,15)$	21	21	7	$(210,21)$	19	15	7	$(210,30)$	21	35	8
$(210,42)$	21	35	8	$(210,70)$	21	2	8	$(210,105)$	19	3	7
$(210,210)$	19	6	6	$(214,214)$	12	4	4	$(220,4)$	16	55	4
$(220,5)$	16	11	3	$(220,11)$	13	5	4	$(220,20)$	16	44	4
$(220,44)$	13	20	4	$(220,220)$	14	4	4	$(222,2)$	18	111	4
$(222,3)$	17	37	5	$(222,6)$	18	74	3	$(222,37)$	18	3	5
$(222,74)$	13	6	3	$(222,111)$	10	6	3	$(222,222)$	15	2	4
$(230,2)$	17	115	5	$(230,5)$	16	46	5	$(230,10)$	16	23	6
$(230,23)$	17	10	6	$(230,46)$	15	5	5	$(230,115)$	14	2	5
$(231,3)$	15	77	3	$(231,7)$	15	33	4	$(231,11)$	15	21	4
$(231,21)$	13	33	4	$(231,33)$	13	21	4	$(231,77)$	11	3	3
$(234,18)$	18	117	7	$(234,9)$	17	26	6	$(234,18)$	18	26	7
$(236,236)$	10	4	3	$(238,2)$	17	119	3	$(238,7)$	17	17	3

$(238,14)$	17	34	3	$(238,17)$	15	7	3	$(238,34)$	15	14	3
$(238,238)$	15	3	3	$(245,5)$	10	49	3	$(246,2)$	19	123	7
$(246,3)$	20	41	7	$(246,6)$	20	41	7	$(246,82)$	20	2	8
$(248,8)$	15	31	3	$(248,248)$	11	8	3	$(249,3)$	14	83	3
$(249,249)$	11	3	3	$(250,2)$	14	125	5	$(252,4)$	17	63	5
$(252,7)$	19	9	7	$(252,9)$	19	7	7	$(252,28)$	19	36	7
$(252,36)$	19	28	7	$(252,252)$	17	4	5	$(254,2)$	16	127	4
$(254,254)$	12	2	4	$(258,2)$	20	43	8	$(258,3)$	20	86	7
$(258,6)$	21	86	7	$(258,43)$	21	2	8	$(258,129)$	18	6	7
$(258,258)$	19	3	7	$(259,37)$	12	7	4	$(261,9)$	13	29	4
$(262,2)$	16	131	4	$(262,262)$	15	2	4	$(266,266)$	14	14	5
$(267,3)$	15	89	4	$(267,267)$	13	3	4	$(270,2)$	22	135	7
$(270,5)$	21	27	8	$(270,10)$	22	54	7	$(270,27)$	22	5	8
$(270,54)$	19	10	7	$(270,270)$	19	2	7	$(272,17)$	16	16	6
$(274,2)$	16	137	6	$(275,25)$	13	11	4	$(276,276)$	18	12	5
$(278,2)$	17	139	5	$(278,278)$	14	2	5	$(282,282)$	21	6	6
$(286,286)$	17	2	4	$(291,97)$	16	3	6	$(295,5)$	15	59	3
$(295,295)$	11	5	3	$(297,27)$	16	11	6	$(298,2)$	18	149	7
$(300,4)$	19	75	7	$(300,75)$	19	4	7	$(300,300)$	19	4	7
$(302,2)$	19	151	5	$(302,302)$	16	2	5	$(303,3)$	17	101	3
$(303,101)$	10	3	3	$(303,303)$	12	3	3	$(305,5)$	14	61	4
$(305,61)$	12	5	4	$(310,310)$	21	3	8	$(312,312)$	23	8	8
$(316,316)$	17	4	5	$(318,318)$	23	2	7	$(319,11)$	15	29	4
$(319,29)$	12	11	4	$(321,3)$	18	107	4	$(321,107)$	12	3	4
$(323,17)$	15	19	5	$(329,7)$	16	47	3	$(329,47)$	11	7	3
$(329,329)$	10	7	3	$(330,330)$	31	3	13	$(335,5)$	16	67	4
$(335,67)$	17	5	4	$(341,11)$	14	31	4	$(341,31)$	16	11	4
$(355,5)$	18	71	4	$(371,7)$	17	53	5	$(371,53)$	18	7	5
$(377,13)$	16	29	5	$(377,29)$	14	13	5	$(391,17)$	16	23	5
$(391,23)$	18	17	5								

Proof. The results of [32] and [38] tell us that these curves $X_0^{+d}(N)$ are not hyperelliptic nor trigonal over $\mathbb{C}$.

We have a degree 2 quotient map from $X_0^{+d}(N)$ to $X_0(N)/\langle w_d, w_{d'}\rangle$. If there existed a degree 4 map from $X_0^{+d}(N)$ to $\mathbb{P}^1$, then we apply the Castelnuovo-Severi inequality to this hypothetical degree 4 map and the degree 2 quotient map. Since $g(X_0^{+d}(N)) > 4\cdot 0 + 2\cdot g(X_0(N)/\langle w_d, w_{d'}\rangle) + 3\cdot 1$, we conclude that the degree 4 map would have to factor through the quotient map $X_0^{+d}(N) \to X_0(N)/\langle w_d, w_{d'}\rangle$ and the curve $X_0(N)/\langle w_d, w_{d'}\rangle$ would need to be elliptic or hyperelliptic. However, we can again use [32] to eliminate this possibility. ■

2.2.3. Rational morphisms to $\mathbb{P}^1$

In Section 2.2.1 and Section 2.2.2, we were proving that the curve $X_0^{+d}(N)$ is not $\mathbb{Q}$-tetragonal by arguing that $\mathbb{C}$ or $\mathbb{F}_p$-gonalities are too large. Now we find degree 4 rational morphisms from $X_0^{+d}(N)$ to $\mathbb{P}^1$ for all levels N listed in Theorem 2.2.2.

In most cases, when there exists a degree 4 morphism $X_0^{+d}(N) \to \mathbb{P}^1$, we can realise it via the quotient map to the curve $X_0(N)/\langle w_d, w_{d'}\rangle$, as the following two propositions show.

Proposition 2.2.10. The quotient curve $X_0(N)/\langle w_d, w_{d'}\rangle$ is an elliptic curve for the following values of N, d, d'.

Table 2.18: The values of N, d, d' in Proposition 2.2.10.

N	(d,d')	N	(d,d')	N	(d,d')	N	(d,d')
70	$(2,35)$	86	$(2,43)$	96	$(3,32)$	99	$(9,11)$
105	$(3,35)$	110	$(2,5)$	111	$(3,37)$	118	$(2,59)$
123	$(3,41)$	124	$(4,31)$	141	$(3,47)$	142	$(2,71)$
143	$(11,13)$	145	$(5,29)$	155	$(5,31)$	159	$(3,53)$
188	$(4,47)$						

Proposition 2.2.11. The quotient curve $X_0(N)/\langle w_d, w_{d'}\rangle$ is a hyperelliptic curve for the following values of N, d, d'. Here g denotes the genus of the curve $X_0(N)/\langle w_d, w_{d'}\rangle$.

Table 2.19: The values of N, d, d' in Proposition 2.2.11.

N	(d,d')	g	N	(d,d')	g	N	(d,d')	g
66	$(3,22)$	2	70	$(7,10)$	2	78	$(2,3)$	3
84	$(3,4),(7,12),$ $(4,21),(3,28)$	2	88	$(8,11)$	2	90	$(2,45),(5,18),(9,10)$	2
93	$(3,31)$	2	102	$(2,51),(3,17)$	2	104	$(8,13)$	2
105	$(3,5),(3,7),(7,15)$	3	106	$(2,53)$	2	110	$(2,5),(2,11),(5,22)$	3
112	$(7,16)$	2	114	$(2,19)$	3	114	$(3,38)$	2
115	$(5,23)$	2	116	$(4,29)$	2	117	$(9,13)$	2
120	$(8,15),(15,24)$	2	120	$(5,24)$	3	122	$(2,61)$	2
126	$(2,63),(14,18)$	2	126	$(7,9),(9,14)$	3	129	$(3,43)$	2
130	$(10,26)$	2	130	$(2,13)$	3	132	$(4,11)$	2
133	$(7,19)$	2	134	$(2,67)$	2	135	$(5,27)$	2
136	$(8,17)$	3	138	$(3,23),(6,23)$	2	140	$(4,35)$	2
146	$(2,73)$	2	147	$(3,49)$	2	150	$(6,50)$	2
153	$(9,17)$	2	156	$(4,39)$	2	158	$(2,79)$	2
161	$(7,23)$	2	165	$(11,15)$	3	166	$(2,83)$	2
168	$(21,24)$	4	171	$(9,19)$	3	176	$(11,16)$	4
177	$(3,59)$	2	184	$(8,23)$	2	190	$(5,19)$	2
195	$(5,39)$	3	205	$(5,41)$	2	206	$(2,103)$	2
207	$(9,23)$	3	209	$(11,19)$	2	213	$(3,71)$	2
215	$(5,42)$	2	221	$(13,17)$	2	279	$(9,31)$	5
284	$(4,71)$	2	287	$(7,41)$	2	299	$(13,23)$	2

Proof. Every curve of genus 2 is hyperelliptic and [32] gives us all hyperelliptic quotients of genus $g \geq 3$. ■

Now we deal with the cases when there does not exist such a quotient map.

Proposition 2.2.12. There exists a degree 3 rational morphism from $X_0^{+d}(N)$ to $\mathbb{P}^1$ for

$$\begin{aligned}(N,d) \in \{&(66,33),(74,37),(84,84),(86,43),(88,88),(93,93),(108,4),(112,7),\\ &(115,115),(116,116),(129,129),(135,135),(137,137),(147,147),\\ &(155,155),(159,159),(215,215)\}.\end{aligned}$$

Proof. The curve $X_0^{+d}(N)$ is of genus 4 in these cases and we can use the inbuilt `Magma` function Genus4GonalMap(C) to get the desired morphism.

It is good to mention here that this function always returns a morphism of degree ≤ 3 to $\mathbb{P}^1$ since all genus 4 curves have $\mathbb{C}$-gonality at most 3 by Proposition 2.0.2 (v). In the cases listed in this proposition, that morphism will be defined over $\mathbb{Q}$. However, the degree 3 morphism can, in the general case, be defined over a quadratic field. ■

Proposition 2.2.13. There exists a degree 4 rational morphism from $X_0^{+}(N)$ to $\mathbb{P}^1$ for

$$N \in \{136,152,163,183,197,203,211,223,269,359\}.$$

Proof. The curve $X_0^{+}(N)$ is of genus 6 in these cases and we can use the inbuilt `Magma` function Genus6GonalMap(C) to get the desired morphism.

Similarly to the function Genus4GonalMap(C), this function always returns a morphism of degree ≤ 4 to $\mathbb{P}^1$ since all genus 6 curves have $\mathbb{C}$-gonality at most 4 by Proposition 2.0.2 (v). In these cases, that morphism will be defined over $\mathbb{Q}$. However, not all genus 6 curves are $\mathbb{Q}$-tetragonal, for example $X_0^{+}(243)$, as we have seen in Proposition 2.2.18. ■

Proposition 2.2.14. There exists a degree 4 rational morphism from $X_0^{+d}(N)$ to $\mathbb{P}^1$ for

$$\begin{aligned}(N,d) \in \{&(144,9),(144,16),(144,144),(148,148),(157,157),(171.171),(175,175),\\ &(176,176),(185,185),(193,193),(194.194),(196,4),(200,200),(263,263)\}.\end{aligned}$$

Proof. We find a morphism of degree 4 by searching the Riemann-Roch spaces of divisors of the form $P_1+P_2+P_3+P_4$, where $P_i \in X_0^{+}(N)(\mathbb{Q})$. ■

Proposition 2.2.15. There exists a degree 4 rational morphism from $X_0^{+d}(N)$ to $\mathbb{P}^1$ for

$$(N,d) \in \{(148,4),(160,32),(160,160),(192,192),(208,16),(217,31),$$
$$(224,224),(229,229),(241,241),(257,257),(281,281)\}.$$

Proof. In these cases we were not able to find a degree 4 morphism whose polar divisor is supported on rational points so we had to search for quadratic points.

We searched for quadratic points by intersecting the curve $X_0^{+d}(N)$ with hyperplanes of the form

$$b_0x_0 + \ldots + b_kx_k = 0,$$

where $b_0,\ldots,b_k \in \mathbb{Z}$ are coprime and chosen up to a certain bound, a similar idea as in [13, Section 3.2]. We can improve this by noting that, in a quadratic point $(x_0,\ldots,x_k)$, already its first three coordinates must be linearly dependent over $\mathbb{Q}$. Therefore, it is enough to check the hyperplanes

$$b_0x_0 + b_1x_1 + b_2x_2 = 0.$$

In all of these cases we found a function of degree 4 lying in the Riemann-Roch space of a divisor of the form $P_1 + P_2 + Q + \sigma(Q)$, where $P_1, P_2 \in X_0^{+d}(N)(\mathbb{Q})$, and Q is one of the quadratic points we found. ■

It is worth mentioning here that the running time was ~ 20 minutes for $(N,d) = (192,192)$ and ~ 4.5 hours for $(N,d) = (224,224)$. Most of that time was spent on searching for points. Other computations in this section were faster.

2.2.4. Betti numbers

In this section we will prove that the remaining curves $X_0^{+d}(N)$ are not $\mathbb{C}$-tetragonal. A helpful tool here is the Tower theorem (Theorem 2.1.16). We use Corollary 2.1.18 which says that for curves of genus ≥ 10, the existence of a map to $\mathbb{P}^1$ over $\mathbb{C}$ is equivalent with the existence of a rational map to $\mathbb{P}^1$.

Since in Section 2.2.1 we solved all cases when $g \geq 10$, the only curves we need to

look at are those of genus at most 9. In order to bound the number of levels we need to check, we can use the following corollary of Theorem 2.0.3.

Corollary 2.2.16. The curve $X_0^{+d}(N)$ is not $\mathbb{C}$-tetragonal for $N \geq 807$.

Proof. Suppose $X_0^{+d}(N)$ is $\mathbb{C}$-tetragonal. Then $X_0(N)$ has a degree 8 map to $\mathbb{P}^1$. Since $-I \in \Gamma_0(N)$, we have that $\psi(N) = D_{\Gamma_0(N)} \leq \frac{12000}{119} \cdot 8$ (here $\psi(N) = N\prod_{q|N}(1+\frac{1}{q})$, as mentioned in Lemma 2.1.7). ■

This leaves us with reasonably many cases that are not yet solved. The only pairs (N,d) we need to check are in the table below.

Table 2.20: Curves $X_0^{+d}(N)$ of genus at most 9 that are not $\mathbb{Q}$-tetragonal.

(N,d)	$g(X_0^{+d}(N))$	(N,d)	$g(X_0^{+d}(N))$	(N,d)	$g(X_0^{+d}(N))$
$(102,6)$	8	$(102,34)$	8	$(114,6)$	9
$(114,57)$	8	$(120,3)$	9	$(130,5)$	9
$(130,130)$	8	$(132,132)$	8	$(140,20)$	8
$(148,37)$	9	$(150,150)$	8	$(152,8)$	8
$(152,19)$	9	$(154,7)$	9	$(154,77)$	9
$(154,154)$	9	$(160,5)$	9	$(162,2)$	8
$(162,81)$	7	$(164,4)$	9	$(170,170)$	9
$(172,43)$	9	$(172,172)$	9	$(174,87)$	8
$(175,7)$	8	$(175,25)$	8	$(178,89)$	8
$(178,178)$	9	$(183,3)$	9	$(185,5)$	9
$(185,37)$	9	$(187,11)$	9	$(187,17)$	7
$(187,187)$	7	$(189,189)$	7	$(196,49)$	9
$(196,196)$	7	$(201,201)$	8	$(202,101)$	9
$(203,7)$	9	$(214,107)$	9	$(217,217)$	8
$(219,219)$	8	$(225,9)$	9	$(225,225)$	8
$(231,231)$	9	$(233,233)$	7	$(238,119)$	7
$(242,242)$	9	$(243,243)$	7	$(245,49)$	9

$(247,247)$	8	$(248,31)$	9	$(249,83)$	8
$(256,256)$	9	$(259,259)$	8	$(262,131)$	9
$(267,89)$	9	$(271,271)$	6	$(275,275)$	9
(283.283)	9	$(289,289)$	7	$(293,293)$	8
$(295,59)$	9	$(335,335)$	8	$(341,341)$	9
$(361,361)$	9	$(383,383)$	8	$(419,419)$	9
$(431,431)$	9	$(479,479)$	8		

By Proposition 2.0.2(v), we immediately see that for $N = 271$ there exists a degree 4 morphism since the genus is 6. For the other cases we will use graded Betti numbers $\beta_{i,j}$.

Proposition 2.2.17. The curve $X_0^{+d}(N)$ is not tetragonal for all (N,d) in Table 2.20 except $(243,243)$ and $(271,271)$.

Proof. For all these curves we compute $\beta_{2,2} = 0$ using `Magma` and use Corollary 2.1.14 to finish the proof.

The computation time for $(N,d) = (361,361)$ was around 1 hour, the other computations were much faster and took less than 10 minutes. ■

To prove that the curve $X_0^+(243)$ is $\mathbb{C}$-tetragonal, we will use the Clifford index and Clifford dimension, defined in Definition 2.1.11.

Proposition 2.2.18. The curve $X_0^+(243)$ is tetragonal over $\mathbb{C}$.

Proof. We compute the genus $g(X_0^+(243)) = 7$ and the Betti table. In particular, we get $\beta_{2,2} = 9$. By [87, Table 1.], this implies the existence of g_6^2. Now we use a similar argument as in [53, Page 310, Case 3].

Since there exists a g_6^2, there is a divisor D such that $\deg D = 6$ and $\ell(D) = 3$. By definition, for this D we have $\mathrm{Cliff}(D) = 2$. We now apply Riemann-Roch theorem to get

$$3 - \ell(K-D) = \ell(D) - \ell(K-D) = 6 - 7 + 1 = 0.$$

Therefore, $\ell(K-D) = 3$ and we have proven that $\mathrm{Cliff}(X_0^+(243)) \leq 2$.

The homogenous ideal of the canonical embedding of this curve is generated by quadrics (`Magma` function X0NQuotient(243,[243]) gives the canonical embedding for example). By [53, Theorem 1.1], this implies that $\mathrm{Cliff}(X_0^+(243)) \geq 2$ and we conclude that $\mathrm{Cliff}(X_0^+(243)) = 2$.

Since $\mathrm{Cliff}(X_0^+(243)) = \mathrm{Cliff}(D) = 2$, from the definition of the Clifford dimension $\mathrm{CD}(X)$ we get that $\mathrm{CD}(X_0^+(243)) \leq 2$. Since $g(X_0^+(243)) = 7$, it is not a smooth plane curve of degree $d \geq 5$ (a smooth plane curve of dimension d has genus $(d-1)(d-2)/2$) and we have that $\mathrm{CD}(X_0^+(243)) = 1$.

Let us now take a divisor D' that computed the Clifford dimension. We have $\ell(D') = 2$ and $\mathrm{Cliff}(D') = \mathrm{Cliff}(X_0^+(243)) = 2$. Therefore, from the definition of $\mathrm{Cliff}(D')$ we compute that $\deg D' = 4$. We may assume that $D' > 0$, otherwise we can take an effective divisor linearly equivalent to D' (which exists because $\ell(D') \geq 1$) and it will also compute the Clifford dimension of $X_0^+(243)$.

There exists a non-constant morphism $f \in L(D')$ and its degree is at most 4, otherwise $\mathrm{div}(f) + D' \ngeq 0$ (here we used that D' is effective). Since $\mathrm{gon}_{\mathbb{C}}(X_0^+(243)) \geq 4$ by [38], f is the desired degree 4 morphism from $X_0^+(243)$ to $\mathbb{P}^1$. ■

2.2.5. Proofs of the main theorems

Proof of Theorem 2.2.1. Hasegawa and Shimura [38, Proposition 1] already solved the cases when $g(X_0^{+d}(N)) \neq 4$. Proposition 2.2.6 and Proposition 2.2.12 solve the cases when the genus is equal to 4. ■

Proof of Theorem 2.2.2. We can suppose that the genus of the curve $X_0^{+d}(N)$ is at least 4, otherwise the $\mathbb{Q}$-gonality is at most 3 due to Proposition 2.0.2(iv).

The results of [32] give us all hyperelliptic quotients of $X_0(N)$ and the results of [38] give us all $\mathbb{C}$-trigonal curves $X_0^{+d}(N)$. There are exactly 8 cases when the curve $X_0^{+d}(N)$ is $\mathbb{C}$-trigonal of genus $g \geq 5$, namely [38, Theorem 1]

$$(N,d) \in \{(117,13),(122,122),(146,146),(147,3),\\ (162,162),(164,164),(181,181),(227,227)\},$$

and in these cases the Tower theorem implies that the $\mathbb{Q}$-gonality is also equal to 3.

For genus 4 curves listed in the statement of the theorem, we used Proposition 2.2.6 to prove that there are no degree 3 rational maps to $\mathbb{P}^1$. Therefore, the $\mathbb{Q}$-gonality of these curves must be equal to 4.

We can now suppose that the curve $X_0^{+d}(N)$ is of genus $g \geq 5$ and is not hyperelliptic nor trigonal over $\mathbb{C}$. For the curves listed in the theorem, in Section 2.2.3 we find a rational degree 4 map to $\mathbb{P}^1$. In the remaining cases, we prove in Sections 2.2.1, 2.2.2, and 2.2.4 that there are no degree 4 rational maps to $\mathbb{P}^1$, and so $\mathrm{gon}_{\mathbb{Q}} X_0^{+d}(N) > 4$ in these cases. Moreover, in Section 2.2.4, we prove that $\mathrm{gon}_{\mathbb{C}} X_0^{+d}(N) > 4$ for $(N,d) \notin \{(243,243),(271,271)\}$.

The curve $X_0^+(243)$ is $\mathbb{C}$-tetragonal due to Proposition 2.2.18 and the genus 6 curve $X_0^+(271)$ is $\mathbb{C}$-tetragonal due to Proposition 2.0.2(v). ■

Corollary 2.2.19. The $\mathbb{Q}$-gonality of the curve $X_0(N)$ is equal to 8 for

$$N \in \{193, 194, 207, 224, 229, 241, 257, 281\}.$$

For $N \in \{194, 224, 257, 281\}$ the $\mathbb{C}$-gonality of the curve $X_0(N)$ is also 8.

Proof. The composition map $X_0(N) \to X_0^+(N) \to \mathbb{P}^1$ is a degree 8 rational map and from [76, Tables 1,2,3] we get that $\mathrm{gon}_{\mathbb{Q}}(X_0(N)) > 7$. For $N = 193, 207, 229, 241$ this follows from the bound on $\mathbb{F}_p$-gonality; codes for that can be found on

`https://github.com/orlic1/gonality_X0/tree/main/Fp_gonality`).

For $N = 194, 224, 257, 281$ we can use the Castelnuovo-Severi inequality to prove it, meaning that we also get the lower bound on $\mathbb{C}$-gonality in these cases. ■

2.3. TETRAGONAL INTERMEDIATE MODULAR CURVES

For every group $\Delta \subseteq (\mathbb{Z}/N\mathbb{Z})^\times$, there exists a modular curve $X_\Delta(N)$ defined over $\mathbb{Q}$. It corresponds to the congruence subgroup

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

Since $-I$ acts trivially on the upper half plane $\mathscr{H}^*$ (where $I \in \mathrm{SL}_2(\mathbb{Z})$ is an identity matrix), the curves $X_\Delta(N)$ and $X_{\pm\Delta}(N)$ are isomorphic. Therefore, in this section we will always assume that $-1 \in \Delta$.

For every group $\{\pm 1\} \subseteq \Delta \subseteq (\mathbb{Z}/N\mathbb{Z})^\times$, there exists a modular curve $X_\Delta(N)$ lying between the curves $X_1(N)$ and $X_0(N)$. Notice that, when $\Delta = (\mathbb{Z}/N\mathbb{Z})^\times$, the curve $X_\Delta(N)$ is actually the curve $X_0(N)$ and that, when $\Delta = \{\pm 1\}$, the curve $X_\Delta(N)$ is the curve $X_{\pm 1}(N)$ which is isomorphic to the curve $X_1(N)$. Moreover, if

$$\{\pm 1\} \subseteq \Delta_1 \subseteq \Delta_2 \subseteq (\mathbb{Z}/N\mathbb{Z})^\times,$$

then we have natural projections

$$X_1(N) \to X_{\Delta_1}(N) \to X_{\Delta_2}(N) \to X_0(N)$$

defined over $\mathbb{Q}$. If $\{\pm 1\} \subsetneq \Delta \subsetneq (\mathbb{Z}/N\mathbb{Z})^\times$, then we call the curve $X_\Delta(N)$ an intermediate modular curve.

It is also possible to define modular curves in another way. For every group $H \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, there exists a modular curve X_H defined over $\mathbb{Q}$. Using the same argument as before with the curves $X_\Delta(N)$, we may assume that $-I \in H$ without loss of generality. If H has full determinant (that is, if $\det H = (\mathbb{Z}/N\mathbb{Z})^\times$), the curve X_H is ensured to be geometrically irreducible.

Suppose that $H \subseteq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ such that $-I \in H$ and that H has full determinant.

Then there is a congruence subgroup Γ such that the curves X_H and $X(\Gamma)$ are isomorphic. It is defined as follows:

$$H_0 := \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \cap H,\ \Gamma := \{A \in \mathrm{SL}_2(\mathbb{Z}) : (A \bmod N) \in H_0\}.$$

It is not hard to check that $\Gamma(N) \subseteq \Gamma$, therefore Γ is indeed a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. Conversely, in the case of intermediate modular curves $X_\Delta(N)$, its isomorphic curve X_H is defined as

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

We can easily see that $-I \in H$ and that H has full determinant.

Recall from Section 2.1 that the $\mathbb{Q}$-gonality of the curve $X_0(N)$ has been determined for all $N \leq 144$ (Theorem 2.1.1). Also, we know all curves $X_0(N)$ with $\mathbb{Q}$-gonality at most 6 (Theorems 2.1.2, 2.1.3, 2.1.4) and all curves $X_0(N)$ with $\mathbb{C}$-gonality at most 4 ([37, 53, 80]).

Regarding the curve $X_1(N)$, Kenku and Momose [62, p. 126] determined all hyperelliptic, Jeon, Kim, and Schweizer [51, Theorem 2.3] determined all trigonal curves $X_1(N)$ over $\mathbb{C}$ and $\mathbb{Q}$, Jeon, Kim, and Park [50, Theorem 2.6] determined all tetragonal curves $X_1(N)$ over $\mathbb{C}$ and $\mathbb{Q}$, and Derickx and van Hoeij [23, Proposition 6] determined all curves $X_1(N)$ with $\mathbb{Q}$-gonality equal to d for $d = 5, 6, 7, 8$. They also determined the $\mathbb{Q}$-gonality of the curve $X_1(N)$ for $N \leq 40$ and gave upper bounds on the $\mathbb{Q}$-gonality of $X_1(N)$ for $N \leq 250$.

Now we move on to the intermediate modular curves $X_\Delta(N)$. Ishii and Momose [43] determined (although with a slight error regarding the curve $X_{\Delta_1}(21)$) all hyperelliptic curves $X_\Delta(N)$ and Jeon and Kim [49] determined all trigonal curves $X_\Delta(N)$ over $\mathbb{C}$ and fixed this error. Jeon, Kim, and Schweizer [52] also determined all bielliptic curves $X_\Delta(N)$. Derickx and Najman [20, Table 1] determined the fields of definition of trigonal maps for genus 4 curves $X_\Delta(N)$. This, together with the information about $\mathbb{C}$-trigonal curves $X_\Delta(N)$ from [49], determines all curves $X_\Delta(N)$ which are trigonal over $\mathbb{Q}$.

Theorem 2.3.1. [20, Table 1] The genus 4 intermediate modular curves $X_\Delta(N)$ that are

trigonal over $\mathbb{Q}$ are

$$(N,\Delta) \in \{(26,\{\pm1,\pm5\}),(26,\{\pm1,\pm3,\pm9\}),(28,\pm1,\pm3,\pm9),(28,\{\pm1,\pm13\}),$$
$$(29,\langle -1,4\rangle),(37,\langle -1,8\rangle),(37,\langle -1,4\rangle),(50,\{\pm1,\pm9,\pm11,\pm19,\pm21\})\}.$$

The only genus 4 intermediate modular curve that is not trigonal over $\mathbb{Q}$ is $(N,\Delta) = (25,\{\pm1,\pm7\})$. For expository reasons, for larger groups Δ we give only their generators instead of all their elements.

The next logical step is to determine all tetragonal curves $X_\Delta(N)$ over $\mathbb{C}$ and $\mathbb{Q}$. Also, since we know the $\mathbb{Q}$-gonality of curves $X_0(N)$ for $N \leq 144$ and the $\mathbb{Q}$-gonality of curves $X_1(N)$ for $N \leq 40$, we would like to obtain a similar result for intermediate curves $X_\Delta(N)$ for $N \leq 40$.

The main results of this section are the following theorems.

Theorem 2.3.2. The $\mathbb{Q}$-gonalities of intermediate modular curves $X_\Delta(N)$ for all $N \leq 40$ and $\{\pm1\} \subsetneq \Delta \subsetneq (\mathbb{Z}/N\mathbb{Z})^\times$ are given in Table C.1.

Theorem 2.3.3. The intermediate modular curve $X_\Delta(N)$ is tetragonal over $\mathbb{Q}$ if and only if N and Δ are listed in the following table. For expository reasons, we do not list all elements of larger groups Δ. Instead, we give the generators and the number of elements of such groups Δ.

Table 2.21: The values of N and Δ for Theorem 2.3.3.

N	Δ	N	Δ
25	$\{\pm1,\pm7\}$	30	$\{\pm1,\pm11\}$
32	$\{\pm1,\pm15\}$	33	$\{\pm1,\pm2,\pm4,\pm8,\pm16\}$
34	$\{\pm1,\pm9,\pm13,\pm15\}$	35	$\{\pm1,\pm6,\pm8,\pm13\}$
35	$\langle -1,4\rangle$, $\#\Delta = 12$	36	$\{\pm1,\pm17\}$
39	$\{\pm1,\pm5,\pm8,\pm14\}$	39	$\langle -1,4\rangle$, $\#\Delta = 12$
40	$\{\pm1,\pm3,\pm9,\pm13\}$	40	$\{\pm1,\pm7,\pm9,\pm17\}$
40	$\{\pm1,\pm9,\pm11,\pm19\}$	41	$\langle -1,2\rangle$, $\#\Delta = 20$

45	$\langle -1,4\rangle$, $\#\Delta = 12$	48	$\{\pm 1, \pm 5, \pm 19, \pm 23\}$
48	$\{\pm 1, \pm 7, \pm 17, \pm 23\}$	48	$\{\pm 1, \pm 11, \pm 13, \pm 23\}$
55	$\langle -1,4\rangle$, $\#\Delta = 20$	64	$\langle -1,9\rangle$, $\#\Delta = 16$
75	$\langle -1,4\rangle$, $\#\Delta = 20$		

Theorem 2.3.4. The intermediate modular curve $X_\Delta(N)$ is tetragonal over $\mathbb{C}$ and has $\mathbb{Q}$-gonality at least 5 if and only if

$$(N,\Delta) \in \{(31, \{\pm 1, \pm 5, \pm 6\}), (31, \{\pm 1, \pm 2, \pm 4, \pm 8, \pm 15\})\}.$$

Moreover, the $\mathbb{Q}$-gonality of both these curves is equal to 5.

Theorem 2.3.5. The intermediate modular curve $X_\Delta(N)$ is pentagonal over $\mathbb{Q}$ and over $\mathbb{C}$ if and only if

$$(N,\Delta) \in \{(44, \{\pm 1, \pm 5, \pm 7, \pm 9, \pm 19\}), (125, \langle -1,4\rangle)\}.$$

For $N = 125$, this group Δ has 50 elements.

In Section 2.3.1 we present the results needed to prove the above theorems. More precisely, in Section 2.3.2 we give lower bounds on the $\mathbb{Q}$-gonality of curves $X_\Delta(N)$ via $\mathbb{F}_p$-gonality, in Section 2.3.3 we give lower bounds on the $\mathbb{C}$-gonality obtained using the Castelnuovo-Severi inequality (Proposition 2.1.5), in Section 2.3.4 we give rational morphisms from $X_\Delta(N)$ to $\mathbb{P}^1$, and in Section 2.3.5 we determine the $\mathbb{C}$-tetragonal curves $X_\Delta(N)$. After that, in Section 2.3.6 we prove the main theorems of this section.

For the reader's convenience, in Appendix C at the end of the thesis we put Table C.1. There we list the curves $X_\Delta(N)$ for all levels N studied in the section (the list of these levels N is given and explained at the beginning of Section 2.3.1). For these curves $X_\Delta(N)$ we also give their $\mathbb{C}$ and $\mathbb{Q}$-gonality with the links to all results used to determine the gonality of that curve.

A lot of the results in this section rely on `Magma` [11] and Sage computations as well. An important part in determining the gonality of algebraic curves is finding their mod-

els, preferably non-singular ones. For the modular curve $X_0(N)$ and its quotient curves $X_0(N)/W$ (where W is some group of Atkin-Lehner involutions w_d) there exists an inbuilt `Magma` function X0NQuotient() that gives a canonical model. However, this is not the case for the intermediate curves $X_\Delta(N)$. Therefore, we have to manually find a regular model for them.

Let C/k be a curve of genus g. Then its space of regular differentials has dimension g with a basis $\omega_1,\ldots,\omega_g$. The canonical map of C is the map

$$(\omega_1 : \ldots : \omega_g) : C \to \mathbb{P}^{g-1}.$$

For non-hyperelliptic curves of genus $g \geq 3$, this map is an embedding, and its image is called the canonical model of C.

There is also an equivalent definition of the canonical map which does not use differentials. Let K be a canonical divisor on C. We know from Proposition 1.4.12 that $\deg K = 2g-2$ and $\ell(D) = g$. Let $f_1,\ldots,f_g$ be a basis for $L(D)$. The canonical map of C is the map

$$(f_1 : \ldots : f_g) : C \to \mathbb{P}^{g-1}.$$

For $i \geq 2$, we denote by $\mathscr{L}_i$ the $\mathbb{Q}$-vector space of homogenous degree d polynomials $P \in \mathbb{Q}[x_1,\ldots,x_g]$ such that $P(\omega_1,\ldots,\omega_g) = 0$.

Theorem 2.3.6 (Noether, [26, Section 8B])**.** $\dim \mathscr{L}_2 = \dfrac{(g-2)(g-3)}{2}$.

Theorem 2.3.7 (Petri, [5, 79])**.** Let C/k be a smooth non-hyperelliptic curve of genus $g \geq 3$.

(a) If $g = 3$, then $\dim \mathscr{L}_2 = \dim \mathscr{L}_3 = 0, \dim \mathscr{L}_4 = 1$. Any generator of $\mathscr{L}_4$ provides an equation of C. In other words, any genus 3 non-hyperelliptic curve $C/\mathbb{Q}$ is a smooth plane quartic.

(b) If $g > 3$, then the basis of $\mathscr{L}_2 \bigoplus \mathscr{L}_3$ provides a canonical model of C. Furthermore, if C is neither trigonal nor a smooth plane quintic (only possible if $g = 6$), then the basis of $\mathscr{L}_2$ provides a canonical model of C

Example 2.3.8. Any non-hyperelliptic curve of genus 4 is an intersection of a cubic and

a quadric (that is, a common zero locus of two homogenous polynomials of degrees 3 and 2, respectively).

Since we are only interested in curves of genus $g \geq 5$ (none of them are trigonal by [49]) and there are no intermediate modular curves that are smooth plane quintics by [4, Theorem 1.1], the $\frac{(g-2)(g-3)}{2}$ quadrics will give canonical models of these curves $X_\Delta(N)$.

We used a function vanishing_quadratic_forms() from Maarten Derickx's Sage package MD Sage to find these quadrics and, consequently, canonical models of intermediate curves $X_\Delta(N)$. Following that, we loaded these models into `Magma` codes for giving bounds on $\mathbb{Q}$ and $\mathbb{C}$-gonality.

Another reason we use Sage instead of `Magma` for finding the models of curves $X_\Delta(N)$ is that in Sage it is easier to work with congruence subgroups. We can use a Sage function GammaH() to get congruence subgroups Γ_H. For example, GammaH(29,[12,-1]) gives a subgroup $\Gamma_{\{\pm 1,\pm 12\}}(29)$. On the other hand, `Magma` only has such functions for subgroups $\Gamma(N)$, $\Gamma_0(N)$, $\Gamma_1(N)$, and $\Gamma_1(M,N)$.

It should also be mentioned that David Zwyina's `Magma` function FindCanonicalModel() on

`https://github.com/davidzywina/ActionsOnCuspForms`,

used in [96], also gives canonical models of modular curves X_Γ for groups $\Gamma \leq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. However, this function is much slower than the MD Sage function vanishing_quadratic_forms() used here.

The codes that verify all computations in this section can be found on

`https://github.com/orlic1/gonality_X_Delta`.

Additionally, code and data associated to the paper [86] by Jeremy Rouse, Andrew V. Sutherland, and David Zureick-Brown was used in Proposition 2.3.9. Their code can be found on

`https://github.com/AndrewVSutherland/ell-adic-galois-images/tree/209c2f888669785151174f472ea2c9eafb6daaa9`.

2.3.1. Preliminaries

If we have

$$\{\pm 1\} \subseteq \Delta_1 \subseteq \Delta_2 \subseteq (\mathbb{Z}/N\mathbb{Z})^\times,$$

then, due to the natural projections

$$X_1(N) \to X_{\Delta_1}(N) \to X_{\Delta_2}(N) \to X_0(N)$$

and Proposition 2.0.2(vii), we conclude that

$$\operatorname{gon}_{\mathbb{Q}}(X_1(N)) \geq \operatorname{gon}_{\mathbb{Q}}(X_{\Delta_1}(N)) \geq \operatorname{gon}_{\mathbb{Q}}(X_{\Delta_2}(N)) \geq \operatorname{gon}_{\mathbb{Q}}(X_0(N)), \tag{2.5}$$

$$\operatorname{gon}_{\mathbb{C}}(X_1(N)) \geq \operatorname{gon}_{\mathbb{C}}(X_{\Delta_1}(N)) \geq \operatorname{gon}_{\mathbb{C}}(X_{\Delta_2}(N)) \geq \operatorname{gon}_{\mathbb{C}}(X_0(N)). \tag{2.6}$$

Therefore, when searching for tetragonal curves $X_\Delta(N)$, we may restrict ourselves to the levels N for which the curve $X_0(N)$ has $\mathbb{C}$-gonality at most 4. Similarly, when searching for $\mathbb{Q}$-pentagonal curves $X_\Delta(N)$, we may restrict ourselves to the levels N for which the curve $X_0(N)$ has $\mathbb{Q}$-gonality at most 5. These levels N are listed in [53] and Theorem 2.1.3. They are

$$N \in \{1-75, 77-81, 83, 85, 87-89, 91, 92, 94-96, 98, 100, 101,$$
$$103, 104, 107, 109, 111, 119, 121, 125, 131, 142, 143, 167, 191\}.$$

We can also eliminate those levels N for which the $\mathbb{Q}$-gonality of the curve $X_1(N)$ is at most 3, namely [23, Table 1]

$$N \in \{1-16, 18, 20\}.$$

Therefore, there are only finitely many intermediate modular curves $X_\Delta(N)$ we need to deal with. Moreover, from the group structure of the group $(\mathbb{Z}/N\mathbb{Z})^\times$, we can easily see that for

$$N \in \{22, 23, 46, 47, 59, 83, 94, 107, 167\},$$

there are actually no intermediate modular curves $X_\Delta(N)$ because in these cases $(\mathbb{Z}/N\mathbb{Z})^\times \cong \mathbb{Z}/2p\mathbb{Z}$ for some prime p.

2.3.2. $\mathbb{F}_p$-gonality

In this section we use the results on the $\mathbb{F}_p$-gonality to get a lower bound on the $\mathbb{Q}$-gonality of the modular curves $X_\Delta(N)$.

Proposition 2.3.9. The modular curve $X_\Delta(N)$ has $\mathbb{Q}$-gonality at least 6 for the following values of N and Δ:

Table 2.22: The values of N and Δ for Proposition 2.3.9.

N	Δ	p	$\#X_\Delta(N)(\mathbb{F}_{p^2})$
71	$\langle -1,5\rangle$	5	182
78	$\langle -1,5,31\rangle$	5	192
80	$\langle -1,3,49\rangle$	3	68
88	$\langle -1,21,25\rangle$	3	68
91	$\langle -1,2\rangle$	2	38
96	$\langle -1,5\rangle$	5	160
104	$\langle -1,3,25\rangle$	3	72
104	$\langle -1,5,27\rangle$	5	192
143	$\langle -1,8\rangle$	5	180

Proof. We use `Magma` to compute the number of $\mathbb{F}_{p^2}$ rational points on these curves $X_\Delta(N)$. It is easy to check that $\#X_\Delta(N)(\mathbb{F}_{p^2}) > 5(p^2+1)$ and we can use Lemma 2.1.8 with $q = p^2$ to finish the proof. ■

Here we used Andrew Sutherland's `Magma` function GL2PointCount(Γ, q) which, for $\Gamma \leq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, returns the number of $\mathbb{F}_q$-rational points of X_Γ. For a given group $\Delta \leq (\mathbb{Z}/N\mathbb{Z})^\times$, the corresponding group Γ (from the discussion at the beginning of Section 2.3) has the following generators:

$$\begin{bmatrix} a & 0 \\ 0 & 1 \end{bmatrix} : a \text{ is a generator of } \Delta,$$
$$\begin{bmatrix} 1 & 0 \\ 0 & d \end{bmatrix} : d \text{ is a generator of } (\mathbb{Z}/N\mathbb{Z})^{\times},$$
$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

We can also directly obtain the lower bound on the $\mathbb{F}_p$-gonality of $X_\Delta(N)$ by checking that the dimensions of Riemann-Roch spaces of all degree $\leq d$ effective $\mathbb{F}_p$-rational divisors are equal to 1. This is a finite task since the number of such divisors is finite. We can also use certain tricks (like the ones used in Propositions 2.1.32, 2.1.33, 2.2.5) to reduce the number of divisors that need to be checked.

Proposition 2.3.10. The $\mathbb{F}_p$-gonality of the curve $X_\Delta(N)$ at least 5 for the following values of N and Δ:

Table 2.23: The values of N and Δ for Proposition 2.3.10.

N	Δ	p
31	$\{\pm 1, \pm 5, \pm 6\}$	7
31	$\{\pm 1, \pm 2, \pm 4, \pm 8, \pm 16\}$	2
125	$\langle -1, 4\rangle$	2

Proof. Using `Magma`, we compute that there are no functions of degree ≤ 4 in $\mathbb{F}_p(X_\Delta(N))$. ■

Proposition 2.3.11. The $\mathbb{F}_p$-gonality of the curve $X_\Delta(N)$ at least 6 for the following values of N and Δ:

Table 2.24: The values of N and Δ for Proposition 2.3.11.

N	Δ	p	N	Δ	p
29	$\{\pm1,\pm12\}$	3	33	$\{\pm1,\pm10\}$	5
34	$\{\pm1,\pm13\}$	3	35	$\{\pm1,\pm11,\pm16\}$	3
37	$\{\pm1,\pm10,\pm11\}$	3	38	$\{\pm1,\pm7,\pm11\}$	3
39	$\{\pm1,\pm16,\pm17\}$	5	40	$\{\pm1,\pm19\}$	3
41	$\langle-1,4\rangle$	3	41	$\{\pm1,\pm3,\pm9,\pm14\}$	2
42	$\{\pm1,\pm5,\pm17\}$	5	42	$\{\pm1,\pm13\}$	5
43	$\{\pm1,\pm2\}$	3	43	$\{\pm1,\pm6,\pm7\}$	3
44	$\{\pm1,\pm21\}$	3	45	$\{\pm1,\pm8,\pm17,\pm19\}$	2
45	$\{\pm1,\pm14,\pm16\}$	2	48	$\{\pm1,\pm23\}$	5
49	$\{\pm1,\pm18,\pm19\}$	2	51	$\langle-1,2\rangle$	2
52	$\langle-1,21\rangle$	3	52	$\langle-1,3\rangle$	3
53	$\langle-1,4\rangle$	19	54	$\{\pm1,\pm17,\pm19\}$	5
55	$\langle-1,16\rangle$	2	55	$\{\pm1,\pm12,\pm21,\pm23\}$	2
56	$\langle-1,3\rangle$	3	56	$\langle-1,9,15\rangle$	3
56	$\langle-1,5,9\rangle$	3	56	$\{\pm1,\pm13,\pm15,\pm27\}$	3
57	$\langle-1,8,20\rangle$	2	57	$\langle-1,2\rangle$	3
58	$\langle-1,9\rangle$	3	60	$\{\pm1,\pm11,\pm19,\pm29\}$	7
60	$\{\pm1,\pm11,\pm13,\pm23\}$	7	60	$\{\pm1,\pm7,\pm11,\pm17\}$	7
61	$\langle-1,4\rangle$	5	61	$\langle-1,8\rangle$	2
61	$\langle-1,29\rangle$	2	62	$\langle-1,27\rangle$	2
63	$\langle-1,4,5\rangle$	2	63	$\langle-1,8,20\rangle$	2
63	$\langle-1,8,10\rangle$	2	63	$\langle-1,5,8\rangle$	2
63	$\langle-1,2\rangle$	2	64	$\{\pm1,\pm15,\pm17,\pm31\}$	3
65	$\langle-1,2,7\rangle$	2	65	$\langle-1,4,6\rangle$	2
65	$\langle-1,3,4\rangle$	2	65	$\langle-1,8,12\rangle$	2
66	$\langle-1,25\rangle$	5	67	$\langle-1,8\rangle$	2
68	$\langle-1,9\rangle$	3	69	$\langle-1.4\rangle$	2

70	$\langle -1,27\rangle$	3	70	$\langle -1,9\rangle$	3
71	$\langle -1,20\rangle$	3	72	$\langle {}^{-}1,13,25\rangle$	5
72	$\langle -1,17,25\rangle$	5	72	$\langle -1,5\rangle$	5
73	$\langle -1,21\rangle$	2	73	$\langle -1,25\rangle$	3
74	$\langle -1,25\rangle$	3	75	$\langle -1,16\rangle$	2
77	$\langle -1,32\rangle$	2	77	$\langle -1,8\rangle$	2
77	$\langle -1,4\rangle$	2	78	$\langle -1,35,49\rangle$	5
79	$\langle -1,27\rangle$	2	80	$\langle -1,7,9\rangle$	3
80	$\langle -1,21,49\rangle$	3	81	$\langle -1,8\rangle$	2
85	$\langle -1,2,9\rangle$	2	85	$\langle -1,3,4\rangle$	3
87	$\langle -1,4\rangle$	2	88	$\langle -1,5\rangle$	3
88	$\langle -1,25,105\rangle$	3	89	$\langle -1,9\rangle$	2
91	$\langle -1,8,12\rangle$	2	91	$\langle -1,8,24\rangle$	2
91	$\langle -1,8,48\rangle$	2	91	$\langle -1,4,12\rangle$	2
92	$\langle -1,9\rangle$	3	95	$\langle -1,4\rangle$	2
95	$\langle -1,8\rangle$	2	96	$\langle -1,17,25\rangle$	5
96	$\langle -1,11,25\rangle$	5	100	$\langle -1,9\rangle$	3
101	$\langle -1,4\rangle$	2	103	$\langle -1,22\rangle$	2
104	$\langle -1,5,9\rangle$	3	109	$\langle -1,2\rangle$	2
109	$\langle -1,36\rangle$	2	111	$\langle -1,8\rangle$	2
111	$\langle -1,4\rangle$	2	119	$\langle -1,27\rangle$	2
119	$\langle -1,9\rangle$	2			

Proof. Using `Magma`, we compute that there are no functions of degree ≤ 5 in $\mathbb{F}_p(X_\Delta(N))$. ■

Proposition 2.3.12. The $\mathbb{F}_p$-gonality of the curve $X_\Delta(N)$ is bounded from below by d for the following values of N and Δ:

Table 2.24: The values of N and Δ for Proposition 2.3.12.

N	Δ	p	d
35	$\{\pm 1, \pm 6\}$	2	8
37	$\{\pm 1, \pm 6\}$	2	9
39	$\{\pm 1, \pm 14\}$	2	8
40	$\{\pm 1, \pm 11\}$	3	7
40	$\{\pm 1, \pm 9\}$	3	8

Proof. Using `Magma`, we compute that there are no functions of degree $\leq d-1$ in $\mathbb{F}_p(X_\Delta(N))$. ■

Remark 2.3.13. Most computations for Propositions 2.3.10, 2.3.11, and 2.3.12 were relatively fast (several minutes). However, there were some cases that took longer to finish, For example, the cases $(N,\Delta) = (78, \langle -1, 35, 49\rangle), (96, \langle -1, 11, 25\rangle), (104, \langle -1, 5, 9\rangle)$ took around 2 hours to finish.

Also, the computation time for $(N,\Delta) = (53, \langle -1, 4\rangle)$ was around 4 hours, mostly due to the larger field $\mathbb{F}_{19}$ the program was working with. This is because the number of Riemann-Roch spaces that need to be computed to give a lower bound of d on the $\mathbb{F}_p$-gonality is $O(p^d)$ (see Section 2.1.6)) and it is therefore advisable to choose small values of p when computing the $\mathbb{F}_p$-gonality.

From this we can also see that the complexity grows exponentially with d, meaning that computing the $\mathbb{F}_p$-gonality using this method becomes more difficult and increasingly unfeasible as the gonality grows, especially in the high genus cases.

2.3.3. Castelnuovo-Severi inequality

Proposition 2.3.14. The $\mathbb{C}$-gonality of the curve $X_\Delta(N)$ is at least 6 for the following values of N and Δ:

Table 2.25: The values of N and Δ for Proposition 2.3.14.

N	Δ	$X_\Delta(N)$ - LMFDB label	$g(X_\Delta(N))$	Y	deg	$g(Y)$
48	$\{\pm1,\pm7\}$	48.384.19.bj.1	19	$X_{\{\pm1,\pm7,\pm17,\pm23\}}(48)$	2	7
48	$\{\pm1,\pm17\}$	48.384.19.bc.1	19	$X_{\{\pm1,\pm7,\pm17,\pm23\}}(48)$	2	7
50	$\{\pm1,\pm7\}$	50.450.22.f.1	22	25.150.4.f.1	3	4
62	$\{\pm1,\pm5,\pm25\}$	62.480.31.c.1	31	31.160.6.c.1	3	6
72	$\{\pm1,\pm17,\pm19,\pm35\}$	72.432.21.tx.1	21	36.216.7.u.1	2	7
74	$\langle-1,23\rangle$	74.342.22.b.1	22	37.114.4.b.2	3	4
98	$\langle-1,27\rangle$	98.504.19.b.1	19	49.168.3.b.1	3	3

Proof. We know from [43] and [49] that these curves $X_\Delta(N)$ are neither hyperelliptic nor trigonal. Therefore, their $\mathbb{C}$-gonality is at least 4.

Suppose that the curve $X_\Delta(N)$ is tetragonal for some values of N and Δ from this table. This would mean that there is a degree 4 morphism from $X_\Delta(N)$ to $\mathbb{P}^1$. We can easily check on LMFDB that there is a degree deg morphism from $X_\Delta(N)$ to the curve Y.

If $\deg = 3$, then these two morphisms surely do not factor through a morphism of degree > 1. If $\deg = 2$ and these two morphisms factor through a morphism $X_\Delta(N) \to X'$, then this morphism $X_\Delta(N) \to X'$ must be of degree 2 and we must have $X' \cong Y$. Therefore, we must have

$$X_\Delta(N) \xrightarrow{2} Y \xrightarrow{2} \mathbb{P}^1,$$

meaning that the curve Y is hyperelliptic. However, we can easily check on LMFDB that this is not the case and we get a contradiction.

This means that we can apply Castelnuovo-Severi inequality to these two morphisms to get

$$g(X_\Delta(N)) \leq 4 \cdot 0 + \deg \cdot g(Y) + 3(\deg - 1).$$

This inequality does not hold for these values of N and Δ, however, meaning that there is no degree 4 morphism from $X_\Delta(N)$ to $\mathbb{P}^1$.

Suppose now that the curve $X_\Delta(N)$ is pentagonal for some values of N and Δ from

the table. This would mean that there is a degree 5 morphism from $X_\Delta(N)$ to $\mathbb{P}^1$. Since deg $= 2,3$ for all entries in the table, this hypothetical morphism and the degree deg morphism to Y surely do not factor through a morphism of degree > 1.

This means that we can apply Castelnuovo-Severi inequality to these two morphisms to get

$$g(X_\Delta(N)) \leq 5 \cdot 0 + \deg \cdot g(Y) + 4(\deg -1).$$

This inequality does not hold for these values of N and Δ, however, meaning that there is no degree 5 morphism from $X_\Delta(N)$ to $\mathbb{P}^1$. ■

2.3.4. Rational morphisms to $\mathbb{P}^1$

In Section 2.3.2 and Section 2.3.3, we were giving lower bounds on the $\mathbb{C}$ and $\mathbb{Q}$-gonality of curves $X_\Delta(N)$. Now we give upper bounds by finding rational morphisms from $X_\Delta(N)$ to $\mathbb{P}^1$.

Proposition 2.3.15. There exists a degree 4 rational morphism from $X_\Delta(N)$ to $\mathbb{P}^1$ for the following values of N and Δ:

Table 2.26: The values of N and Δ for Proposition 2.3.15.

N	Δ
30	$\{\pm 1, \pm 11\}$
32	$\{\pm 1, \pm 15\}$
33	$\{\pm 1, \pm 2, \pm 4, \pm 8, \pm 16\}$
35	$\{\pm 1, \pm 4, \pm 6, \pm 9, \pm 11, \pm 16\}$
36	$\{\pm 1, \pm 17\}$
39	$\{\pm 1, \pm 4, \pm 10, \pm 14, \pm 16, \pm 17\}$
40	$\{\pm 1, \pm 9, \pm 11, \pm 19\}$
41	$\langle -1, 2\rangle$
45	$\{\pm 1, \pm 4, \pm 11, \pm 14, \pm 16, \pm 19\}$
64	$\langle -1, 9\rangle$

Proof. All these curves $X_\Delta(N)$ are of genus 5 and from the discussion at the end of the introduction of Section 2.3 we know that their canonical models are intersections of three quadrics. Using Sage, we obtained canonical models for these curves. With these models, we used a `Magma` function Genus5GonalMap(C) which returned that the $\mathbb{C}$-gonality of the curve $X_\Delta(N)$ is 4 and also gave the equations of this degree 4 morphism. The equations were all defined over $\mathbb{Q}$, therefore these curves $X_\Delta(N)$ are all $\mathbb{Q}$-tetragonal. ■

Remark 2.3.16. `Magma` has inbuilt functions Genus2GonalMap(C), Genus3GonalMap(C), Genus4GonalMap(C), Genus5GonalMap(C), and Genus6GonalMap(C) which return the $\mathbb{C}$-gonality of the curve C (required to be of that genus) and a gonal map to $\mathbb{P}^1$, defined over some number field.

However, these functions seem to expect the 'usual' model of C. For example, they expect the model of a genus 3 curve to be a single quartic and a model of a genus 5 curve to be an intersection of three quadrics (models mentioned in Theorem 2.3.7). Otherwise, `Magma` can return an error (the current version of `Magma` at the time of writing of this thesis was V2.28-14).

For example, for genus 5 quotients of the modular curve $X_0(N)$, the inbuilt `Magma` function X0NQuotient() returns a canonical model that is an intersection of cubics instead of an intersection of three quadrics.

Proposition 2.3.17. There exists a degree d rational morphism from $X_\Delta(N)$ to $\mathbb{P}^1$ for the following values of N and Δ:

Table 2.27: The values of N and Δ for Proposition 2.3.17.

N	Δ	d
29	$\{\pm1,\pm12\}$	6
31	$\{\pm1,\pm2\}$	5
31	$\{\pm1,\pm5,\pm6\}$	5
33	$\{\pm1,\pm10\}$	6
34	$\{\pm1,\pm13\}$	6
35	$\{\pm1,\pm11,\pm16\}$	6

35	$\{\pm 1, \pm 6, \pm 8, \pm 13\}$	4
37	$\{\pm 1, \pm 10, \pm 11\}$	6
39	$\{\pm 1, \pm 16, \pm 17\}$	6
40	$\{\pm 1, \pm 11\}$	7
44	$\{\pm 1, \pm 5, \pm 7, \pm 9, \pm 19\}$	5
55	$\langle -1, 4 \rangle$	4

Proof. We used Sage to find a canonical model for these curves $X_\Delta(N)$. After that, we used `Magma` to find a degree d rational effective divisor with Riemann-Roch dimension at least 2. In all cases except for $(N, \Delta) = (37, \{\pm 1, \pm 10, \pm 11\})$ this divisor was a sum of d rational points.

For $(N, \Delta) = (37, \{\pm 1, \pm 10, \pm 11\})$ we were not able to find a degree 6 function whose polar divisor is supported on rational points so we had to search for quadratic points.

We searched for quadratic points by intersecting the curve with hyperplanes of the form

$$b_0 x_0 + b_1 x_1 + b_2 x_2 = 0,$$

where $b_0, b_1, b_2 \in \mathbb{Z}$ are coprime and chosen up to a certain bound, a similar idea as in Proposition 2.2.15. Following that, we found a degree d effective rational divisor with Riemann-Roch dimension 2. This divisor is a sum of rational points and divisors of the form $Q + \sigma(Q)$, where Q is one of the quadratic points. ■

Proposition 2.3.18. There exists a degree d rational morphism from $X_\Delta(N)$ to $\mathbb{P}^1$ for the following values of N and Δ:

Table 2.28: The values of N and Δ for Proposition 2.3.18.

N	Δ	d	$X_\Delta(N)$ - LMFDB label	Y	deg	$\mathrm{gon}_{\mathbb{Q}}(Y)$
33	$\{\pm1,\pm2,\pm4,\pm8,\pm16\}$	4	33.96.5.a.4	$X_0(33)$	2	2
34	$\{\pm1,\pm13\}$	6	34.216.9.a.1	17.72.1.a.2	3	2
35	$\{\pm1,\pm6\}$	8	35.288.13.a.2	$X_{\{\pm1,\pm6,\pm8,\pm13\}}(35)$	2	4
36	$\{\pm1,\pm17\}$	4	36.216.7.u.1	$X_{\pm1}(18)$	2	2
37	$\{\pm1,\pm6\}$	9	37.342.16.c.2	$X_{\langle-1,8\rangle}(37)$	3	3
38	$\{\pm1,\pm7,\pm11\}$	6	38.180.10.a.1	19.60.1.a.2	3	2
39	$\{\pm1,\pm5,\pm8,\pm14\}$	4	39.168.9.a.1	13.42.0.a.2	4	1
39	$\{\pm1,\pm14\}$	8	39.336.17.c.1	$X_{\pm1}(13)$	4	2
40	$\{\pm1,\pm3,\pm9,\pm13\}$	4	40.144.7.fp.1	$X_0(40)$	2	2
40	$\{\pm1,\pm7,\pm9,\pm17\}$	4	40.144.7.fs.1	$X_0(40)$	2	2
40	$\{\pm1,\pm19\}$	6	40.288.9.bh.1	$X_{\pm1}(20)$	2	3
40	$\{\pm1,\pm9\}$	8	40.288.13.sp.1	$X_{\{\pm1,\pm9,\pm11,\pm19\}}(40)$	2	4
48	$\{\pm1,\pm5,\pm19,\pm23\}$	4	48.192.7.hj.1	$X_0(48)$	2	2
48	$\{\pm1,\pm7,\pm17,\pm23\}$	4	48.192.7.ho.1	$X_0(48)$	2	2
125	$\langle-1,4\rangle$	5	125.300.16.a.1	25.60.0.a.1	5	1

Proof. This degree d morphism is obtained as a composition map

$$X_\Delta(N) \xrightarrow{\deg} Y \xrightarrow{\mathrm{gon}_{\mathbb{Q}}(Y)} \mathbb{P}^1.$$

The map from $X_\Delta(N)$ to Y is a rational projection map and can be checked on LMFDB. It only remains to discuss the $\mathbb{Q}$-gonality of the curve Y.

If Y is of genus $0,1$ or is hyperelliptic, this is obvious. The $\mathbb{Q}$-gonalities of the curves $X_{\{\pm1,\pm6,\pm8,\pm13\}}(35)$ and $X_{\{\pm1,\pm9,\pm11,\pm19\}}(40)$ were proved in Propositions 2.3.17 and 2.3.15. The $\mathbb{Q}$-gonality of the curve $X_{\langle-1,8\rangle}(37)$ was proved in Theorem 2.3.1 and the $\mathbb{Q}$-gonalities of the curves $X_{\pm1}(N) \cong X_1(N)$ were proved in [23]. ■

2.3.5. $\mathbb{C}$-gonalities

In this section we will determine the cases when $\mathrm{gon}_{\mathbb{C}}(X_\Delta(N)) = 4$.

Proposition 2.3.19. The modular curve $X_\Delta(N)$ has $\mathbb{C}$-gonality at least 6 for the following values of N and Δ:

Table 2.29: The values of N and Δ for Proposition 2.3.19.

N	Δ	$[\mathrm{SL}_2(\mathbb{Z}) : \Delta]$	N	Δ	$[\mathrm{SL}_2(\mathbb{Z}) : \Delta]$
53	$\langle -1, 2^{13} \rangle$	702	58	$\langle -1, 3^7 \rangle$	630
66	$\langle -1, 5^5 \rangle$	720	67	$\langle -1, 2^{11} \rangle$	748
69	$\langle -1, 2^{11} \rangle$	1056	75	$\langle -1, 2^5 \rangle$	600
79	$\langle -1, 3^{13} \rangle$	1040	87	$\langle -1, 2^7 \rangle$	840
88	$\langle -1, 21, 5^5 \rangle$	720	89	$\langle -1, 3^{11} \rangle$	990
92	$\langle -1, 3^{11} \rangle$	1584	98	$\langle -1, 3^7 \rangle$	1176
100	$\langle -1, 3^5 \rangle$	900	101	$\langle -1, 2^5 \rangle$	510
103	$\langle -1, 5^{17} \rangle$	1763	121	$\langle -1, 32 \rangle$	660
121	$\langle -1, 2^{11} \rangle$	1452	125	$\langle -1, 32 \rangle$	750
131	$\langle -1, 2^5 \rangle$	660	131	$\langle -1, 2^{13} \rangle$	1716
142	$\langle -1, 7^5 \rangle$	1080	142	$\langle -1, 7^7 \rangle$	1512
143	$\langle -1, 2^5 \rangle$	840	191	$\langle -1, 19^5 \rangle$	960
191	$\langle -1, 19^{19} \rangle$	3648			

Proof. From Theorem 2.0.3, we can see that $X_\Delta(N)$ cannot be d-gonal for $d \leq 5$ because $[\mathrm{SL}_2(\mathbb{Z}) : \Delta] > \lfloor 5 \cdot \frac{12000}{119} \rfloor = 504$ in all these cases. ■

Proposition 2.3.20. The curves $X_\Delta(N)$ are $\mathbb{C}$-tetragonal for

$$(N, \Delta) \in \{(31, \{\pm 1, \pm 5, \pm 6\}), (31, \{\pm 1, \pm 2, \pm 4, \pm 8, \pm 15\})\}.$$

Proof. These curves are of genus 6. Therefore, they have $\mathbb{C}$-gonality at most 4 by Proposition 2.0.2(v). We also know that they are neither hyperelliptic nor trigonal by [43]

and [49]. Hence their $\mathbb{C}$-gonality is equal to 4. ■

From Theorem 2.1.16 and Corollary 2.1.17 we see that in order to prove that a curve of genus $g \geq 10$ has $\mathbb{C}$-gonality at least 5, it is enough to prove that its $\mathbb{Q}$-gonality is at least 5. All such non-tetragonal curves $X_\Delta(N)$ have been dealt with in Sections 2.3.2, 2.3.3, and Proposition 2.3.19. Therefore, the remaining curves are those with genus ≤ 9.

In order to prove that these curves are not tetragonal, we will use graded Betti numbers $\beta_{i,j}$.

Proposition 2.3.21. The modular curve $X_\Delta(N)$ has $\mathbb{C}$-gonality at least 5 for the following values of N and Δ:

Table 2.30: The values of N and Δ for Proposition 2.3.21.

N	Δ	N	Δ	N	Δ
29	$\{\pm1,\pm12\}$	34	$\{\pm1,\pm13\}$	35	$\{\pm1,\pm11,\pm16\}$
39	$\{\pm1,\pm16,\pm17\}$	40	$\{\pm1,\pm19\}$	42	$\{\pm1,\pm5,\pm17\}$
43	$\langle -1,2\rangle$	44	$\{\pm1,\pm5,\pm7,\pm9,\pm19\}$	45	$\{\pm1,\pm14,\pm16\}$
51	$\langle -1,2\rangle$	52	$\langle -1,3\rangle$	53	$\langle -1,4\rangle$
55	$\langle -1,4\rangle$	56	$\langle -1,3\rangle$	57	$\langle -1,2\rangle$
61	$\langle -1,4\rangle$	63	$\langle -1,4,5\rangle$	65	$\langle -1,2,7\rangle$
72	$\langle -1,11,25\rangle$	73	$\langle -1,25\rangle$		

Proof. In all these cases we use `Magma` to compute $\beta_{2,2} = 0$ and the result follows from Corollary 2.1.14 since these curves are neither hyperelliptic nor trigonal. ■

2.3.6. Proofs of the main theorems

By the results of Ishii and Momose [43] and Jeon and Kim [49], we know that the only hyperelliptic curve $X_\Delta(N) \neq X_0(N), X_1(N)$ is a curve $X_{\{\pm1,\pm8\}}(21)$ and that all $\mathbb{C}$-trigonal curves $X_\Delta(N) \neq X_0(N), X_1(N)$ are of genus 3 or 4. Moreover, Theorem 2.3.1 tells us which genus 4 curves are $\mathbb{Q}$-trigonal (we know from Proposition 2.0.2(iv) that genus 3

curves have $\mathbb{Q}$-gonality ≤ 3). In the proofs of the main theorems, we may now suppose that all remaining curves we consider have $\mathbb{C}$-gonality at least 4.

Proof of Theorem 2.3.3. The curve $X_{\{\pm 1,\pm 7\}}$ is tetragonal over $\mathbb{Q}$ due to Theorem 2.3.1. Other listed curves are tetragonal over $\mathbb{Q}$ due to Propositions 2.3.15, 2.3.17, and 2.3.18.

Suppose now that $X_\Delta(N)$ is a curve of $\mathbb{C}$-gonality at least 4 not listed in the theorem. In the first case, we prove that the $\mathbb{Q}$-gonality of this curve is at least 5 in Propositions 2.3.9, 2.3.10, 2.3.11, 2.3.12, and Proposition 2.3.14, Otherwise, there is a projection map

$$X_\Delta(N) \to X_{\Delta_1}(N)$$

to a curve $X_{\Delta_1}(N)$ for which we have already proven that it is not $\mathbb{Q}$-tetragonal. In that case we can use Proposition 2.0.2(vii) to prove that the curve $X_\Delta(N)$ is not $\mathbb{Q}$-tetragonal.

For example, we consider the case $N = 41$. Since $(\mathbb{Z}/41\mathbb{Z})^\times \cong \mathbb{Z}/40\mathbb{Z}$, there are 4 intermediate modular curves $X_\Delta(41)$, namely

$$\Delta \in \{\{\pm 1,\pm 9\},\{\pm 1,\pm 3,\pm 9,\pm 14\},\{\pm 1,\pm 4,\pm 10,\pm 16,\pm 18\},\langle -1,2\rangle\}.$$

The curve with $\Delta = \langle -1,2\rangle$ is $\mathbb{Q}$-tetragonal due to Proposition 2.3.15 and the curves with $\Delta = \{\pm 1,\pm 3,\pm 9,\pm 14\},\{\pm 1,\pm 4,\pm 10,\pm 16,\pm 18\}$ are not $\mathbb{Q}$-tetragonal due to Proposition 2.3.11. Then the curve with $\Delta = \{\pm 1,\pm 9\}$ is automatically not $\mathbb{Q}$-tetragonal since it maps to a curve with $\Delta = \{\pm 1,\pm 3,\pm 9,\pm 14\}$. ■

Proof of Theorem 2.3.4. The two listed curves are $\mathbb{C}$-tetragonal due to Proposition 2.3.20 and they admit a degree 5 rational morphism to $\mathbb{P}^1$ due to Proposition 2.3.17. However, they are not $\mathbb{Q}$-tetragonal due to Proposition 2.3.10.

Suppose now that $X_\Delta(N)$ is a curve of $\mathbb{C}$-gonality at least 4 not listed in Theorems 2.3.3 and 2.3.4. Then we either prove that its $\mathbb{C}$-gonality is at least 5 using Proposition 2.3.14, Proposition 2.3.19, Proposition 2.3.21, the bound on $\mathbb{F}_p$-gonality in Section 2.3.2 along with Corollary 2.1.17 for curves of genus $g \geq 10$, or we use Proposition 2.0.2(vii) with a map $X_\Delta(N) \to X_{\Delta_1}(N)$, similarly as in the proof of the previous theorem. ■

Proof of Theorem 2.3.5. The two listed curves are $\mathbb{Q}$-pentagonal due to Propositions 2.3.17 and 2.3.18. We proved that the curve with $N = 44$ has $\mathbb{C}$-gonality at least 5 in Proposi-

tion 2.3.21 and that the curve with $N = 125$ has $\mathbb{Q}$-gonality at least 5 in Proposition 2.3.10. Since the genus of the curve $X_{\langle -1,4\rangle}(125)$ is equal to 16, we can use Corollary 2.1.17 to prove that its $\mathbb{C}$-gonality is at least 5.

Suppose now that $X_\Delta(N)$ is a curve of $\mathbb{C}$-gonality at least 4 not listed in Theorems 2.3.3, 2.3.4, and 2.3.5. Then we know that its $\mathbb{C}$-gonality is at least 5. It remains to prove that its $\mathbb{Q}$-gonality is at least 6.

In the first case, we either use Propositions 2.3.11, 2.3.12, 2.3.14, or Proposition 2.3.19 to prove that the $\mathbb{Q}$-gonality is at least 6. Otherwise, we use Proposition 2.0.2(vii) with a map $X_\Delta(N) \to X_{\Delta_1}(N)$, similarly as in the previous two proofs. ■

3. DEGREE d POINTS ON CURVES

Let C be a smooth, projective, and geometrically integral curve defined over a number field k. Determining whether the set of points of degree $\leq d$ over k on C is finite or infinite is an important problem in arithmetic geometry. Faltings' Theorem solves the base case $d = 1$.

Theorem 3.0.1 (Faltings' Theorem, [28])**.** Let k be a number field and let C be a non-singular curve defined over k of genus $g \geq 2$. Then the set $C(k)$ is finite.

Therefore, if $C(k) \neq \emptyset$, then it is infinite if and only if C is isomorphic to $\mathbb{P}^1$ ($g = 0$) or C is an elliptic curve ($g = 1$) with positive k-rank. The next step is considering the same problem for $d > 1$.

Definition 3.0.2. Let C be a curve defined over a number field k. The arithmetic degree of irrationality $\text{a.irr}_k C$ is the smallest integer d such that C has infinitely many points of degree d over k, i.e.

$$\text{a.irr}_k C := \min\left(d, \#\left\{\cup_{[F:k]\leq d} C(F)\right\} = \infty\right).$$

We also define

$$\text{a.irr}_{\bar{k}}\, C := \min_{[L:k]<\infty} \text{a.irr}_L\, C.$$

It is obvious that $\text{a.irr}_k C \geq \text{a.irr}_{\bar{k}}\, C$.

Harris and Silverman [35, Corollary 3] proved that if a curve of genus $g \geq 2$ has infinitely many quadratic points, then it must be either hyperelliptic or bielliptic. Also, Abramovich and Harris [2, Theorem 1] gave a conjecture

$$\text{a.irr}_{\bar{k}}\, C \leq d \iff C \text{ admits a map of degree} \leq d \text{ to } \mathbb{P}^1 \text{ or an elliptic curve}$$

which they proved for $d = 2, 3$. However, Debarre and Fahlaoui constructed counterexamples for $d \geq 4$ [17]. One way to characterize when there are infinitely many points of degree d on C is the following theorem.

Theorem 3.0.3 ([12, Theorem 4.2. (1)])**.** Let C be a curve over a number field. There are infinitely many degree d points on C if and only if either there exists a map $C \to \mathbb{P}^1$ of degree d or the image of $\mathrm{Sym}^d C$ in $\mathrm{Pic}^d C$ contains a translate of a positive rank abelian variety.

It can be hard to check, however, whether the image of $\mathrm{Sym}^d C$ in $\mathrm{Pic}^d C$ contains a translate of a positive rank abelian variety. Kadets and Vogt gave a simpler characterization for $d = 2, 3$, which encompasses the previous results of Harris-Silverman [35] and Abramovich-Harris [2].

Theorem 3.0.4 ([54], Theorem 1.2)**.** Suppose X/k is a smooth, projective, and geometrically integral curve. Then the following statements hold:

(1) If $\mathrm{a.irr}_k X = 2$, then X is a double cover of $\mathbb{P}^1$ or an elliptic curve of positive rank over k.

(2) If $\mathrm{a.irr}_k X = 3$, then one of the following three cases holds:

   (a) X is a triple cover of $\mathbb{P}^1$ or an elliptic curve of positive rank over k.

   (b) X is a smooth plane quartic with no rational points, positive rank Jacobian, and at least one cubic point.

   (c) X is a genus 4 Debarre-Fahlaoui curve [17, Section 4].

(3) If $\mathrm{a.irr}_{\bar{k}} X = d \leq 3$, then $X_{\bar{k}}$ is a degree d cover of $\mathbb{P}^1$ or an elliptic curve.

(4) If $\mathrm{a.irr}_{\bar{k}} X = d = 4, 5$, then either $X_{\bar{k}}$ is a Debarre-Fahlaoui curve [17, Section 4], or $X_{\bar{k}}$ is a degree d cover of $\mathbb{P}^1$ or an elliptic curve.

The question of determining $\mathrm{a.irr}_k C$ is closely related to the k-gonality of C and degree k maps to elliptic curves. Frey [31, Proposition 2] proved that if a curve C defined over a number field k has infinitely many points of degree $\leq d$ over k, then $\mathrm{gon}_k C \leq 2d$.

Regarding the curves $C = X_1(M,N)$ and $k = \mathbb{Q}$, all cases when C has infinitely many points of degree $d \leq 6$ were determined by Mazur [70] (for $d = 1$), Kenku, Momose, and Kamienny [55,62] (for $d = 2$), Jeon, Kim, and Schweizer [51] (for $d = 3$), Jeon, Kim, and Park [50] (for $d = 4$), and Derickx and Sutherland [22] (for $d = 5,6$). Additionally, Derickx and van Hoeij [23] determined all curves $X_1(N)$ which have infinitely many points of degree $d = 7,8$ and Jeon determined all trielliptic [46] and tetraelliptic [47] curves $X_1(N)$ over $\mathbb{Q}$.

In this thesis, we will study the curve $C = X_0(N)$ and $k = \mathbb{Q}$. The curve $X_0(N)$ has infinitely many rational points if and only if $N \in \{1-10,12,13,16,18,25\}$ (i.e. when $g(X_0(N)) = 0$). This was proved by Mazur [71] and Kenku [57–60].

Ogg [80] determined all hyperelliptic curves $X_0(N)$, Bars [6] determined all bielliptic curves $X_0(N)$, as well as all curves $X_0(N)$ with infinitely many quadratic points, and Jeon [45] determined all curves $X_0(N)$ with infinitely many cubic points.

Theorem 3.0.5 (Bars)**.** The modular curve $X_0(N)$ has infinitely many points of degree 2 over $\mathbb{Q}$ if and only if

$$N \in \{1-33,35-37,39-41,43,46-50,53,59,61,65,71,79,83,89,101,131\}.$$

Theorem 3.0.6 (Jeon)**.** The modular curve $X_0(N)$ has infinitely many points of degree 3 over $\mathbb{Q}$ if and only if

$$N \in \{1-29,31,32,34,36,37,43,45,49,50,54,64,81\}.$$

We here determine all curves $X_0(N)$ with infinitely many quartic points. Our main result is the following theorem.

Theorem 3.0.7. The modular curve $X_0(N)$ has infinitely many points of degree 4 over $\mathbb{Q}$ if and only if

$$N \in \{1-75,77-83,85-89,91,92,94-96,98-101,103,104,107,111,$$
$$118,119,121,123,125,128,131,141-143,145,155,159,167,191\}.$$

For N in the above set, we prove in Section 3.3 that $X_0(N)$ has infinitely many quartic points. The harder part of the proof is proving that for the other N, there are only finitely many quartic points on $X_0(N)$.

Remark 3.0.8. This result has in the meantime been proven by Jeon and Hwang in [42] using different methods. However, the methods presented here could be used to solve the higher degree cases (i.e. $d = 5$). Moreover, with some modifications, our methods could be used to determine all trielliptic and tetraelliptic curves $X_0(N)$ and also all trielliptic quotients of $X_0(N)$ (all bielliptic quotients of $X_0(N)$ were determined in [9]).

Thus, we put emphasis on our method of determining the possible degrees of a rational morphism to an elliptic curve. The classification of curves $X_0(N)$ with infinitely many quartic points is given afterwards as an application.

Section 3.1 contains the technical results used in Section 3.2, where we determine all positive rank tetraelliptic curves $X_0(N)$. Our main tool for proving that a curve C over $\mathbb{Q}$ does not admit a degree 4 morphism to an elliptic curve E over $\mathbb{Q}$ is the representation of rational morphisms from $J_0(N)$ to E by a quadratic form.

Proposition 3.0.9 (Part of the proof of Theorem 3.0.11)**.** Let C be a curve over $\mathbb{Q}$ with at least one rational point and E an elliptic curve over $\mathbb{Q}$ that occurs as an isogeny factor of $J(C)$ with multiplicity $n \geq 1$. Then the degree map $\deg : \mathrm{Hom}_{\mathbb{Q}}(C,E) \to \mathbb{Z}$ can be extended to a positive definite quadratic form on $\mathrm{Hom}_{\mathbb{Q}}(J_0(N),E) \cong \mathbb{Z}^n$.

This statement is a generalization of [90, Corollary III.6.3], which deals with the case when C is an elliptic curve. The proof uses optimal E-isogenous quotients defined in Section 3.2 to prove that $\mathrm{Hom}_{\mathbb{Q}}(J(C),E) \cong \mathrm{Hom}_{\mathbb{Q}}(E^n,E) \cong \mathbb{Z}^n$. We do not give the proof here because we do not need Proposition 3.0.9 to prove Theorem 3.0.11, but are instead able to manually construct a desired quadratic form in all our cases.

In Section 3.1.2 we define a pairing on $\mathrm{Hom}_{\mathbb{Q}}(J(C),E)$ which is an extension of the degree map. Proposition 3.1.5 tells us that it is a positive definite symmetric bilinear quadratic form. It turns out that, in all our cases, the degeneracy maps $\iota_{d,N,M}$ (defined in Section 3.1.3) form a basis for $\mathrm{Hom}_{\mathbb{Q}}(J(C),E)$. More precisely, we have the following result.

Proposition 3.0.10. Take a positive integer $N < 408$. Let E be an elliptic curve of positive $\mathbb{Q}$-rank and conductor $\mathrm{Cond}(E) = M \mid N$, and let $f : X_0(M) \to E$ be a modular parametrization of E. Then (with the natural embedding $X_0(N) \to J_0(N)$), the maps $f \circ \iota_{d,N,M}$ form a basis for $\mathrm{Hom}_{\mathbb{Q}}(J(C), E)$, where d ranges over all divisors of $\frac{N}{M}$.

Therefore, the coefficients of the quadratic form are the values of the pairing on the base elements $f \circ \iota_{d,N,M}$. The main result of Section 3.1, Theorem 3.1.13, allows us to explicitly compute these coefficients in terms of the q-expansion of the modular form associated with E. We use these quadratic forms in Section 3.4 to prove the following theorem.

Theorem 3.0.11. The curve $X_0(N)$ is positive rank tetraelliptic over $\mathbb{Q}$ if and only if

$$N \in \{57, 58, 65, 74, 77, 82, 86, 91, 99, 111, 118, 121, 123, 128, 141, 142, 143, 145, 155, 159\}.$$

One step of the proof of Theorem 3.0.11 is to check for finitely many cases that the suitable quadratic form does not take 4 as a value and conclude that there are no degree 4 rational morphisms from $X_0(N)$ to E. The quadratic forms considered are listed in Appendix D.

The last two sections are an application of our methods developed in Section 3.1 and Section 3.2. In Section 3.3, we find degree 4 morphisms for all levels N when curve $X_0(N)$ has infinitely many quartic points.

In Section 3.4, we prove that any curve $C/\mathbb{Q}$ of genus $g \geq 8$ with infinitely many quartic points and finitely many cubic points has a degree 4 morphism to $\mathbb{P}^1$ or a positive rank elliptic curve. Using this result for $C = X_0(N)$, along with the fact that all curves $X_0(N)$ with infinitely many cubic points are tetragonal over $\mathbb{Q}$ (since all of them either have genus 0 or 1, or are hyperelliptic or bielliptic), we get that any curve $X_0(N)$ of genus $g \geq 8$ with infinitely many quartic points must admit a degree 4 rational morphism to a positive rank elliptic curve (we will call such curves positive rank tetraelliptic). Therefore, only finitely many levels N (actually, only $N = 97$) need to be solved separately.

Finally, at the end of Section 3.4, we prove Theorem 3.0.11 and Theorem 3.0.7 and give a few examples to illustrate the application of our methods.

The reason why we only solved the case $d = 4$ is the following. Although we could

get a similar result as in Theorem 3.0.11 for $d \geq 5$, there is a large number of small genus curves $X_0(N)$ for which we cannot use Theorem 3.4.1 to connect the degree d maps with the points of degree $\leq d$.

For example, when $d = 5$, Theorem 3.4.1 can only be used for curves of genus $g \geq 12$. Although we can use the Jacobi inversion theorem to deal with the cases $g \leq 5$, there are 34 curves $X_0(N)$ with genus $g \in [6, 11]$ such that $J_0(N)$ has positive rank over $\mathbb{Q}$ (for $d = 4$ we were lucky to have only one such small genus case, $N = 97$). Furthermore, there exists only one pentagonal curve $X_0(N)$, namely $X_0(109)$ (Theorem 2.1.3), and we did not find any degree 5 maps from $X_0(N)$ to an elliptic curve. Therefore, we expect that in most $g \geq 6$ cases the curve $X_0(N)$ will have only finitely many degree 5 points.

3.1. PROPERTIES OF JACOBIANS

3.1.1. Notation and definitions

Let C, C' be curves over a field k. A morphism $f : C \to C'$ induces maps $f_* : J(C) \to J(C')$ and $f^* : J(C') \to J(C)$ which are defined as follows. If $D = \sum n_i P_i$ and $D' = \sum n'_i P'_i$ are divisors on C and C' respectively, then

$$f_*([D]) = [\sum n_i f(P_i)] \text{ and}$$
$$f^*([D']) = [\sum n'_i f^{-1}(P'_i)].$$

When seeing $J(C)$ not as divisors modulo principal divisors but as $\mathrm{Pic}^0(C)$, the map f^* is sometimes also denoted as $f^\vee$ or $\mathrm{Pic}(f)$.

Lemma 3.1.1. $f_* \circ f^* = [\deg f]$.

Proof. $f_*(f^*([D'])) = f_*(f^*([\sum n'_i P'_i])) = f_*([\sum n'_i f^{-1}(P'_i)]) = [\sum n'_i \cdot (\deg f) P'_i] = [(\deg f) D']$. ■

By [74, Theorem 6.6], the abelian variety $J(C)$ comes with a canonical principal polarization

$$\phi_{\Theta_C} : J(C) \to J(C)^\vee$$

induced by the theta divisor of C. This map is an isomorphism.

If $P \in C(k)$, then we can define the embedding morphism

$$f_P : C \to J(C),$$
$$x \mapsto [x - P].$$

If A is an abelian variety over k, we can use this point to define

$$\mathrm{Hom}_P(C, A) := \{f \in \mathrm{Hom}(C, A) \mid f(P) = 0\}.$$

With this definition, the universal property of the Jacobian [74, Theorem 6.1] states that

the map

$$\iota_P : \mathrm{Hom}(J(C),A) \to \mathrm{Hom}_P(C,A),$$
$$h \mapsto h \circ f_P$$

is an isomorphism. The map

$$s_P : \mathrm{Hom}(C,A) \to \mathrm{Hom}_P(C,A),$$
$$f \mapsto t_{-f(P)} \circ f,$$

where $t_{-f(P)}$ denotes the translation by $-f(P)$ map, is a retraction of the canonical inclusion $\mathrm{Hom}_P(C,A) \to \mathrm{Hom}(C,A)$ whose kernel are the constant maps. Since the constant maps can be identified with $A(k)$, we have a direct sum decomposition

$$\mathrm{Hom}(C,A) \cong \mathrm{Hom}_P(C,A) \times A(k).$$

If A is an elliptic curve, then f and $s_P(f)$ have the same degree because $t_{-f(p)}$ is an isomorphism. In particular, if one wants to study the possible degrees that occur for elements in $\mathrm{Hom}(C,A)$, it suffices to restrict to those in $\mathrm{Hom}_P(C,A)$.

Note that the maps $f_P^\vee : J(C)^\vee \to J(C)$ and $\phi_{\Theta_C} : J(C) \to J(C)^\vee$ are closely related to each other, namely $f_P^\vee \circ \phi_{\Theta_C} = -\mathrm{Id}_{J(C)}$. For elliptic curves, one often takes $P = 0_E$ to be the zero section of the elliptic curve, and then the map $f_{0_E} : E \to J(E)$ is used to identify E with its Jacobian/dual. So the above means that this identification differs by the one coming from the polarization $\phi_{\Theta_E} : J(E) \to J(E)^\vee = E^{\vee\vee} \cong E$ by a minus sign.

3.1.2. Degree pairing

We already saw in Section 3.1.1 that if $f : C \to C'$ is a map of curves, then $f_* \circ f^* = [\deg f]$. This motivates the following definition:

Definition 3.1.2. Let C, E be curves over a field k with E being an elliptic curve. The

degree pairing is defined on $\mathrm{Hom}(C,E)$ as

$$\begin{aligned}\langle \_,\_\rangle : \mathrm{Hom}(C,E)\times\mathrm{Hom}(C,E) &\to \mathrm{End}(J(E))\\ f,g &\mapsto f_*\circ g^*.\end{aligned}$$

If $P\in C(k)$, then we can define the degree pairing on $\mathrm{Hom}(J(C),E)$ as

$$\begin{aligned}\langle \_,\_\rangle : \mathrm{Hom}(J(C),E)\times\mathrm{Hom}(J(C),E) &\to \mathrm{End}(J(E)),\\ f,g &\mapsto (f\circ f_P)_*\circ(g\circ f_P)^*.\end{aligned}$$

We will also write $\langle f,g\rangle := f_*\circ g^*$ for $f,g\in\mathrm{Hom}(C,C')$ (this is not a pairing when C' is not elliptic since $\mathrm{Hom}(C,C')$ is not an abelian group in that case). With this notation we have $\langle f,f\rangle = [\deg f]$ for $f\in\mathrm{Hom}(C,C')$.

Note that the definition on $\mathrm{Hom}(J(C),E)$ is slightly unsatisfactory since a priori it seems to depend on the base point P. Additionally, it is not defined in terms of intrinsic properties of the abelian variety $J(C)$, but instead just defined by using $f_P : C\to J(C)$ to transport the definition on $\mathrm{Hom}(C,E)$ to that on $\mathrm{Hom}(J(C),E)$. So let's try to give a more intrinsic definition.

Let A and B be two polarized abelian varieties over k with polarizations ϕ_A and ϕ_B respectively and assume the polarization ϕ_A is principal. Then one can define the map

$$\begin{aligned}\_^\dagger : \mathrm{Hom}(A,B) &\to \mathrm{Hom}(B,A),\\ f &\mapsto \phi_A^{-1}\circ f^\vee\circ\phi_B.\end{aligned}$$

When $A=B$ this is just the Rosati involution, defined in Section 17 of [73].

Definition 3.1.3. Let (A,ϕ_A) and (B,ϕ_B) be two polarized abelian varieties over k with ϕ_A a principal polarization. Then the dagger pairing on $\mathrm{Hom}(A,B)$ is defined as

$$\begin{aligned}\langle \_,\_\rangle_\dagger : \mathrm{Hom}(A,B)\times\mathrm{Hom}(A,B) &\to \mathrm{End}(B),\\ f,g &\mapsto f\circ g^\dagger.\end{aligned}$$

The following lemma shows how the dagger pairing relates to the degree pairing.

Lemma 3.1.4. Let C, E be curves over a field k with E being an elliptic curve, and let $P \in C(k)$. Then for $f, g \in \mathrm{Hom}(J(C), J(E))$ we have

$$\langle f, g \rangle_\dagger = \langle f_{0_E}^{-1} \circ f \circ f_P,\ f_{0_E}^{-1} \circ g \circ f_P \rangle,$$

where the principal polarizations on $J(C)$ and $J(E)$ needed for the definition of $\langle \_, \_ \rangle_\dagger$ are taken to be those coming from the theta divisors on C and E.

Proof. We prove this by showing $(f_{0_E}^{-1} \circ f \circ f_P)_* = f$ and $(f_{0_E}^{-1} \circ g \circ f_P)^* = g^\dagger$.

For the equality $(f_{0_E}^{-1} \circ f \circ f_P)_* = f$ it suffices to show equality on points over the algebraic closure of k. So let $D = \sum n_i P_i$ be a degree zero divisor representing a point in $J(C)(\overline{k})$. Then

$$(f_{0_E}^{-1} \circ f \circ f_P)_*(\sum n_i P_i) = \sum n_i (f_{0_E}^{-1} \circ f)(P_i - P) = (f_{0_E}^{-1} \circ f)(\sum n_i (P_i - P)) = \dots$$
$$\dots = f_{0_E}^{-1}(f(\sum n_i P_i) - f(\sum n_i P)) = f_{0_E}^{-1}(f(\sum n_i P_i) - f(0)) = f(\sum n_i P_i).$$

The equality $(f_{0_E}^{-1} \circ g \circ f_P)^* = g^\dagger$ follows since * and $^\vee$ denote the same operation and

$$(f_{0_E}^{-1} \circ g \circ f_P)^\vee = f_P^\vee \circ g^\vee \circ (f_{0_E}^{-1})^\vee = (-\phi_{\Theta_C})^{-1} \circ g^\vee \circ (-\phi_{\Theta_E}) = \phi_{\Theta_C}^{-1} \circ g^\vee \circ \phi_{\Theta_E} = g^\dagger,$$

where the second equality follows by applying Lemma 6.8 of [74] twice.

■

Proposition 3.1.5. Let C, E be curves over $\mathbb{Q}$ with E being an elliptic curve. Then the dagger pairing is a positive definite symmetric bilinear form on $\mathrm{Hom}_\mathbb{Q}(J(C), J(E))$ taking values in $\mathrm{End}_\mathbb{Q}(J(E)) = \mathbb{Z}$.

Proof. The dagger pairing is obviously bilinear. It is also symmetric because for $f, g \in \mathrm{Hom}_\mathbb{Q}(J(C), J(E))$ we have

$$\langle f, g \rangle_\dagger = f \circ g^\dagger = (g \circ f^\dagger)^\dagger = g \circ f^\dagger.$$

Here the last equality holds because $g \circ f^\dagger \in \mathrm{End}_\mathbb{Q}(J(E))$ is of the form $[n]$ for some $n \in \mathbb{Z}$ and $[n]^\dagger = [n]$. The positive definiteness follows from Lemma 3.1.4 since we can compute

$\langle f,f\rangle_\dagger$ over $\overline{\mathbb{Q}}$ by choosing a $P \in C(\overline{\mathbb{Q}})$ as follows:

$$\langle f,f\rangle_\dagger = \langle f_{0_E}^{-1} \circ f \circ f_P,\ f_{0_E}^{-1} \circ f \circ f_P \rangle = [\deg f_{0_E}^{-1} \circ f \circ f_P],$$

and $\deg f_{0_E}^{-1} \circ f \circ f_P > 0$ if $f \neq 0$. ■

Remark 3.1.6. If E is a CM elliptic curve over $\mathbb{C}$, we could also consider the dagger pairing $\mathrm{Hom}_{\mathbb{C}}(J(C),J(E)) \times \mathrm{Hom}_{\mathbb{C}}(J(C),J(E)) \to \mathrm{End}_{\mathbb{C}}(J(E))$. This is a positive definite *hermitian* form instead of a symmetric one since the Rosati involution $\_^\dagger$ acts as complex conjugation on $\mathrm{End}_{\mathbb{C}}(J(E))$.

3.1.3. Degeneracy maps

Let M and N be positive integers such that $M \mid N$. For every divisor d of $\dfrac{N}{M}$ there exists a degeneracy map

$$\iota_{d,N,M} : X_0(N) \to X_0(M), (E,G) \mapsto (E/G[d], (G/G[d])[M]).$$

The degeneracy map acts on $\tau \in \mathscr{H}^*$ in the extended upper half-plane as

$$\iota_{d,N,M}(\tau) = d\tau.$$

From this or directly from the definition, we can easily see that when $dM \mid N$ and $d'N \mid N'$, then

$$\iota_{d,N,M} \circ \iota_{d',N',N} = \iota_{dd',N',M}. \tag{3.1}$$

We want to describe $\left\langle \iota_{d_1,N,M}, \iota_{d_2,N,M} \right\rangle$ for different divisors d_1, d_2 of $\dfrac{N}{M}$ in terms of Hecke operators on $J_0(M)$ (the case $d_1 = d_2$ is solved by Lemma 3.1.1). We recall from Section 7.3 of [24] that Hecke operators T_n act on $Y_0(M)$ as

$$T_n(E,G) = \sum_{\substack{\#C=n \\ C\cap G=\{0\}}} (E/C, (G+C)/C)$$

and have the following properties (mentioned previously in Section 1.5):

$$\begin{aligned} T_{p^r} &= T_{p^{r-1}}T_p - pT_{p^{r-2}} && \text{for primes } p \nmid M \text{ and } r > 1, \\ T_{p^r} &= T_p^r && \text{for primes } p \mid M \text{ and } r > 0, \\ T_{mn} &= T_m T_n && \text{if } \gcd(m,n) = 1. \end{aligned}$$

We want to determine $\langle \iota_{d_1,N,M}, \iota_{d_2,N,M} \rangle$. When $N = Mp$ for a prime p, we already know from Section 7.3 of [24] that $\langle \iota_{1,N,M}, \iota_{p,N,M} \rangle = T_p$. The remaining case is when $\frac{N}{M}$ is a composite number. Before we consider that case, we prove a technical group theory lemma.

Lemma 3.1.7. Let G be an abelian group of order N that has a cyclic subgroup G' of order d. If $dG \cong \mathbb{Z}/\left(\frac{N}{d}\mathbb{Z}\right)$, then G is cyclic.

Proof. We know that $G \cong (\mathbb{Z}/(d_1\mathbb{Z})) \times \ldots \times (\mathbb{Z}/(d_k\mathbb{Z}))$, where d_i are integers such that $d_1 \mid \ldots \mid d_k$, $d_1 \ldots d_k = N$ and $d \mid d_k$. Thus,

$$dG \leq (\mathbb{Z}/(d_1\mathbb{Z})) \times \ldots \times \left(\mathbb{Z}/\left(\frac{d_k}{d}\mathbb{Z}\right)\right).$$

However, $dG \cong \mathbb{Z}/\left(\frac{N}{d}\mathbb{Z}\right)$ implying that $d_1 = \ldots = d_{k-1} = 1$ and $d_k = N$. ■

Lemma 3.1.8. If $\frac{N}{M}$ is square-free, then $\langle \iota_{1,N,M}, \iota_{N/M,N,M} \rangle = T_{N/M}$.

Proof. Suppose that (E,G) represents a point on $Y_0(M)$. We compute

$$\begin{aligned} \langle \iota_{1,N,M}, \iota_{N/M,N,M} \rangle (E,G) &= \sum_{\substack{E'/G'[N/M]=E \\ G'/G'[N/M]=G}} (E', G'[M]), \\ T_{N/M}(E,G) &= \sum_{\substack{\#C=N/M \\ C\cap G=\{0\}}} (E/C, (G+C)/C). \end{aligned}$$

In order to prove that these sums are equal, it is enough to find a bijection between the summands. We will now construct a map that sends $(E', G'[M])$ to $(E/C, (G+C)/C)$ (i.e. define C in terms of E' and G') and prove that it is a bijection.

By definition, there is a map $f : E' \to E$ such that $\ker f = G'[N/M]$. We set

$$C := \ker f^\vee.$$

This means that for the map $f^\vee : E \to E'$ we have $E' = E/C$. Further,

$$(G+C)/C = f^\vee(G) = f^\vee(f(G')) = \frac{N}{M}G' = G'[M],$$

meaning that $G \cap C = \{0\}$ (since $f^\vee(G)$ is a group of order M) and $(E/C, (G+C)/C = (E', G'[M]))$. To prove bijectivity, we define the inverse map, i.e. we define E' and G' in terms of C.

By definition, there is a map $g : E \to E/C$. We set

$$E' := E/C,$$
$$G' := (g^\vee)^{-1}(G).$$

First, we need to prove that G' is a cyclic subgroup of order N. It is obviously a group of order N. We have

$$\frac{N}{M}G' = (g \circ g^\vee)(g^\vee)^{-1}(G) = g(G) = (G+C)/C.$$

Also, $\mathbb{Z}/\left(\frac{N}{M}\mathbb{Z}\right) \cong \ker g^\vee \leq G'$ so we can use Lemma 3.1.7 to conclude that G' is a cyclic subgroup of order N. This further implies that $G'[M] = \frac{N}{M}G' = (G+C)/C$.

To prove that these two maps are inverse to each other it is enough to prove $g = f^\vee$. This holds because

$$\ker f = G'[N/M] = (g^\vee)^{-1}(G)[N/M] = M(g^\vee)^{-1}(G) = (g^\vee)^{-1}(MG) = (g^\vee)^{-1}(0) = \ker g^\vee.$$

■

Lemma 3.1.9. If $\frac{N}{M}$ is square-free, then $\left\langle \iota_{N/M,N,M}, \iota_{1,N,M} \right\rangle = w_M \circ T_{N/M} \circ w_M$.

Proof. We will prove the equivalent statement $w_M \circ \left\langle \iota_{N/M,N,M}, \iota_{1,N,M} \right\rangle = T_{N/M} \circ w_M$. Suppose that (E, G) represents a point on $Y_0(M)$. We compute (similarly as in the previous

lemma)

$$\left\langle \iota_{N/M,N,M}, \iota_{1,N,M} \right\rangle (E,G) = \sum_{\substack{\#G'=N \\ G'[M]=G}} (E/G'[N/M], G'/G'[N/M]) = \sum (E', G''),$$

$$w_M \circ \left\langle \iota_{N/M,N,M}, \iota_{1,N,M} \right\rangle (E,G) = \sum_{\substack{\#G'=N \\ G'[M]=G}} (E'/G'', E'[M]/G''),$$

$$T_{N/M} \circ w_M(E,G) = \sum_{\substack{\#H=N/M \\ (E[M]/G)\cap H=\{0\}}} (E/G/H, ((E[M]/G)+H)/H).$$

It remains to prove that there is a bijection between the summands. We have the following situation:

$$E \overset{f_1}{\to} E' \overset{f_2}{\to} E'/G'',$$

$$E \overset{g_1}{\to} E/G \overset{g_2}{\to} E/G/H$$

where we know that $G' = \ker(f_2 \circ f_1)$ because $\ker f_2 = G'/G'[N/M] = G'/\ker f_1$.

We can express G' in terms of H as $G' := g_1^{-1}(H) = \ker(g_2 \circ g_1)$. By Lemma 3.1.7, this is a cyclic group of order N because $\mathbb{Z}/(M\mathbb{Z}) \cong G \leq G'$ and

$$MG' = (g_1^\vee \circ g_1) g_1^{-1}(H) = g_1^\vee(H) \cong H \cong \mathbb{Z}/\left(\frac{N}{M}\mathbb{Z}\right).$$

Here the third equality holds because $(E[M]/G) \cap H = \{0\}$. Now, since $G' = g_1^{-1}(H) = \ker(g_2 \circ g_1)$, we get $f_2 \circ f_1 = g_2 \circ g_1$. Further, $G = \ker g_1 \subset G'$ implying that $G'[M] = G$.

Let us now express H in terms of G'. Since G is a subgroup of $G' = \ker(f_2 \circ f_1)$, there exist isogenies g_1 and g_2 such that $g_2 \circ g_1 = f_2 \circ f_1$ and $G = \ker g_1$. We set $H := \ker g_2$. It remains to prove that $(E[M]/G) \cap H = \{0\}$. This holds because

$$g_2(E[M]/G) = g_2(g_1(E[M])) = f_2(f_1(E[M])) = E[M]/(E[M] \cap G') \cong E[M]/G.$$

■

Remark 3.1.10. When the number $\dfrac{N}{M}$ is not square-free, then the proofs of Lemma 3.1.8 and Lemma 3.1.9 still work provided one replaces the Hecke operator $T_{N/M}$ by a slightly

different operator $T'_{N/M}$, which is defined as

$$T'_n(E,G) := \sum_{\substack{\#C=n \\ C \text{ cyclic} \\ C\cap G=\{0\}}} (E/C,(G+C)/C).$$

Note that the only difference between T' and T is that the sum in T' is restricted to cyclic subgroups. If N/M is coprime to M, then $T_{N/M}$, seen as element of $\mathrm{End}(J_0(M))$, can be easily expressed as $T_{N/M} = \sum_{m^2|N/M} \mu(m) T'_{N/(Mm^2)}$. Using the Möbius inversion formula one then gets

$$\left\langle \iota_{1,N,M}, \iota_{N/M,N,M} \right\rangle = T'_{N/M} = \sum_{m^2|N/M} \mu(m) T_{N/(Mm^2)},$$

$$\left\langle \iota_{N/M,N,M}, \iota_{1,N,M} \right\rangle = w_M \circ T'_{N/M} \circ w_M = w_M \circ \sum_{m^2|N/M} \mu(m) T_{N/(Mm^2)} \circ w_M,$$

where μ denotes the Möbius function.

Proposition 3.1.11. Let M, d_1, d_2 be positive integers with $\gcd(d_1,d_2) = 1$. Then

$$\iota_{1,d_1d_2M,d_1M,*} \circ \iota^*_{1,d_1d_2M,d_2M} = \iota^*_{1,d_1M,M} \circ \iota_{1,d_2M,M,*} \quad \text{and}$$
$$\left\langle \iota_{d_1,d_1d_2M,M}, \iota_{d_2,d_1d_2M,M} \right\rangle = \left\langle \iota_{d_1,d_1M,M}, \iota_{1,d_1M,M} \right\rangle \circ \left\langle \iota_{1,d_2M,M}, \iota_{d_2,d_2M,M} \right\rangle.$$

Proof. Let E be an elliptic curve with a cyclic subgroup G of order d_2M. The first equality can be verified on a pair (E,G) since

$$\begin{aligned} \iota_{1,d_1d_2M,d_1M,*} \circ \iota^*_{1,d_1d_2M,d_2M}(E,G) &= \sum_{\substack{H_1\supseteq G \text{ cyclic} \\ \#H_1=d_1d_2M}} (E, H_1[d_1M]) \\ &= \sum_{\substack{H_2\supseteq G[M] \text{ cyclic} \\ \#H_2=d_1M}} (E,H_2) \\ &= \iota^*_{1,d_1M,M} \circ \iota_{1,d_2M,M,*}(E,G). \end{aligned}$$

Furthermore, H_1 and H_2 are related to each other via $H_2 = H_1[d_1M]$ and $H_1 = H_2 + G$.

The second equality follows from the first because

$$\begin{aligned}\left\langle \iota_{d_1,d_1d_2M,M}, \iota_{d_2,d_1d_2M,M}\right\rangle &= \iota_{d_1,d_1d_2M,M,*}\circ \iota^*_{d_2,d_1d_2M,M}\\ &= \iota_{d_1,d_1M,M,*}\circ \iota_{1,d_1d_2M,d_1M,*}\circ \iota^*_{1,d_1d_2M,d_2M}\circ \iota^*_{d_2,d_2M,M}\\ &= \iota_{d_1,d_1M,M,*}\circ \iota^*_{1,d_1M,M}\circ \iota_{1,d_2M,M,*}\circ \iota^*_{d_2,d_2M,M}\\ &= \left\langle \iota_{d_1,d_1M,M}, \iota_{1,d_1M,M}\right\rangle \circ \left\langle \iota_{1,d_2M,M}, \iota_{d_2,d_2M,M}\right\rangle .\end{aligned}$$

■

Combining the previous results we get the following proposition.

Proposition 3.1.12. Assume that $\frac{N}{M}$ is either squarefree or coprime to M and let d_1 and d_2 be divisors of $\frac{N}{M}$. We write just gcd instead of $\gcd(d_1,d_2)$ and lcm instead of $\operatorname{lcm}(d_1,d_2)$ for simplicity. Then

$$\begin{aligned}\left\langle \iota_{d_1,N,M}, \iota_{d_2,N,M}\right\rangle = w_M\circ \left(\sum_{m^2\mid d_1/\gcd} \mu(m) T_{d_1/(m^2\gcd)}\right)\circ w_M\circ\\ \circ \left(\sum_{m^2\mid d_1/\gcd} \mu(m) T_{d_2/(m^2\gcd)}\right)\circ [\deg \iota_{\gcd,N,M\operatorname{lcm}/\gcd}].\end{aligned}$$

Proof. Note that

$$\iota_{d_1,N,M} = \iota_{d_1/\gcd,M\operatorname{lcm}/\gcd,M}\circ \iota_{\gcd,N,M\operatorname{lcm}/\gcd}$$

and similarly for d_2. This shows that $\iota_{d_1,N,M}$ and $\iota_{d_2,N,M}$ both factor through the map $\iota_{\gcd,N,M\operatorname{lcm}/\gcd}$ allowing us to write

$$\begin{aligned}\left\langle \iota_{d_1,N,M}, \iota_{d_2,N,M}\right\rangle &= \iota_{d_1/\gcd,M\operatorname{lcm}/\gcd,M,*}\circ \iota_{\gcd,N,M\operatorname{lcm}/\gcd,*}\circ \iota^*_{\gcd,N,M\operatorname{lcm}/\gcd}\circ \iota^*_{d_2/\gcd,M\operatorname{lcm}/\gcd,M}\\ &= \iota_{d_1/\gcd.M\operatorname{lcm}/\gcd,M,*}\circ [\deg \iota_{\gcd,N,M\operatorname{lcm}/\gcd}]\circ \iota^*_{d_2/\gcd,M\operatorname{lcm}/\gcd,M}\\ &= \left\langle \iota_{d_1/\gcd,M\operatorname{lcm}/\gcd,M}, \iota_{d_2/\gcd,M\operatorname{lcm}/\gcd,M}\right\rangle \circ [\deg \iota_{\gcd,N,M\operatorname{lcm}/\gcd}].\end{aligned}$$

Further, by Proposition 3.1.11 we have

$$\left\langle \iota_{d_1/\gcd,M\operatorname{lcm}/\gcd,M}, \iota_{d_2/\gcd,M\operatorname{lcm}/\gcd,M}\right\rangle =$$

$$= \left\langle \iota_{d_1/\gcd, Md_1/\gcd, M}, \iota_{1, Md_1/\gcd, M} \right\rangle \circ \left\langle \iota_{1, Md_2/\gcd, M}, \iota_{d_2/\gcd, Md_2/\gcd, M} \right\rangle.$$

Now we get the desired result by applying Lemma 3.1.8, Lemma 3.1.9, and Remark 3.1.10.

■

Theorem 3.1.13. Using the assumptions and notation of Proposition 3.1.12, let E be an elliptic curve of conductor M with corresponding newform $\sum_{n=1}^{\infty} a_n q^n$ and let $f : X_0(M) \to E$ be the modular parametrization of E. If we define

$$a = \left(\sum_{m^2 | (d_1/\gcd)} \mu(m) a_{d_1/(\gcd m^2)} \right) \left(\sum_{m^2 | (d_2/\gcd)} \mu(m) a_{d_2/(\gcd m^2)} \right),$$

where μ is the Möbius function (when $\dfrac{d_1 d_2}{\gcd^2}$ is squarefree, a is equal to $a_{d_1 d_2/\gcd^2}$, similarly as in Remark 3.1.10), then

$$\left\langle f \circ \iota_{d_1, N, M}, f \circ \iota_{d_2, N, M} \right\rangle = \left[a \cdot \frac{\psi(N)}{\psi\left(\frac{M \operatorname{lcm}}{\gcd}\right)} \cdot \deg f \right].$$

Here $\psi(N) = N \prod_{q|N} (1 + \dfrac{1}{q})$, as in Lemma 2.1.7.

Proof. For the sake of simplicity, we will assume that $\dfrac{d_1 d_2}{\gcd^2}$ is squarefree. We have

$$\left\langle f \circ \iota_{d_1, N, M}, f \circ \iota_{d_2, N, M} \right\rangle = f_* \circ \iota_{d_1, N, M, *} \circ \iota^*_{d_2, N, M} \circ f^* = f_* \circ \left\langle \iota_{d_1, N, M}, \iota_{d_2, N, M} \right\rangle \circ f^*.$$

Let E' be $f^*(E) \subset J_0(M)$. Then E' is an elliptic curve isogenous to E. Since, up to isogeny, E occurs with multiplicity one in the factorization of $J_0(M)$ (because $\operatorname{cond}(E) = M$), it follows that $\left\langle \iota_{d_1, N, M}, \iota_{d_2, N, M} \right\rangle$ is a rational endomorphism of E'. Therefore, $\left\langle \iota_{d_1, N, M}, \iota_{d_2, N, M} \right\rangle$ is of the form $[k]$ for some $k \in \mathbb{Z}$ and we get that

$$f_* \circ \left\langle \iota_{d_1, N, M}, \iota_{d_2, N, M} \right\rangle \circ f^* = f_* \circ f^* \circ \left\langle \iota_{d_1, N, M}, \iota_{d_2, N, M} \right\rangle = [\deg f] \circ \left\langle \iota_{d_1, N, M}, \iota_{d_2, N, M} \right\rangle.$$

Proposition 3.1.12 now tells us that

$$\left\langle f \circ \iota_{d_1,N,M}, f \circ \iota_{d_2,N,M} \right\rangle = w_M \circ T_{d_1/\gcd} \circ w_M \circ T_{d_2/\gcd} \circ [\deg \iota_{\gcd,N,M\mathrm{lcm}/\gcd}] \circ [\deg f]. \tag{3.2}$$

We see that here both the Atkin-Lehner involution w_M and Hecke operators act on E. As w_M acts as ± 1 on E, the action of w_M cancels itself. Furthermore, the Hecke operators T_n act on E as multiplication by a_n (the coefficient in the corresponding newform). Therefore,

$$\begin{aligned}\left\langle f \circ \iota_{d_1,N,M}, f \circ \iota_{d_2,N,M} \right\rangle &= [a_{d_1/\gcd}] \circ [a_{d_2/\gcd}] \circ [\deg \iota_{\gcd,N,M\mathrm{lcm}/\gcd}] \circ [\deg f] \\ &= [a_{d_1 d_2/\gcd^2} \cdot \deg \iota_{\gcd,N,M\mathrm{lcm}/\gcd} \cdot \deg f].\end{aligned}$$

The last equality holds due to the fact that $a_n a_m = a_{nm}$ for relatively prime m, n. Finally, since the degrees of all degeneracy maps from $X_0(N)$ to $X_0(M\mathrm{lcm}/\gcd)$ are equal to $\dfrac{\psi(N)}{\psi\left(\frac{M\mathrm{lcm}}{\gcd}\right)}$ by Proposition 2.1.26, we get the desired formula.

If $\dfrac{d_1 d_2}{\gcd^2}$ is not squarefree, in Equation (3.2) we will get the Möbius sums from Remark 3.1.10 instead of $T_{d_i/\gcd}$. We can then use the same argument to get the desired result since the sums $\sum_{m^2|(d_i/\gcd)} \mu(m) T_{d_i/(\gcd m^2)}$ act on E as $\sum_{m^2|(d_i/\gcd)} \mu(m) a_{d_i/(\gcd m^2)}$. ■

This result is useful because all items on the right-hand side are easily computable ($\deg f$ is the modular degree of E and a is determined by the coefficients of the corresponding newform of E), and in fact already have been computed for all elliptic curves of conductor $\leq 500{,}000$ and $\mathrm{lcm}(d_1,d_2)/\gcd(d_1,d_2) \leq 1{,}000$. This data is available in the LMFDB [67].

Remark 3.1.14. Alternatively, we can compute $\left\langle f \circ \iota_{d_1,N,M}, f \circ \iota_{d_2,N,M} \right\rangle$ using either Sage or Magma since $\iota_{d_1,N,M,*}$ and $\iota^*_{d_2,N,M}$ are explicitly computable on modular symbols, see Proposition 8.26 of [91].

3.2. d-ELLIPTIC MODULAR CURVES

Definition 3.2.1. Let d be a positive integer. We call a curve C over a field k d-elliptic if there exists an elliptic curve E over k and a morphism $C \to E$ of degree d defined over k. If in addition k is a number field and E has positive Mordell-Weil rank over k, then we call C positive rank d-elliptic.

In this section, we will describe some ideas that allow one to determine for given integers N and d whether $X_0(N)$ is d-elliptic over $\mathbb{Q}$.

If we fix a point $P \in X_0(N)(\mathbb{Q})$, then, as we have seen in Section 3.1.1, there exists an element of $\mathrm{Hom}_{\mathbb{Q}}(X_0(N), E)$ of degree d if and only if there exists an element of $\mathrm{Hom}_{\mathbb{Q},P}(X_0(N), E)$ of degree d. Furthermore, by the universal property of $J_0(N)$, every $f \in \mathrm{Hom}_{\mathbb{Q},P}(X_0(N), E)$ factors uniquely through $J_0(N)$ via the map f_P.

We define a map $\mathrm{Hom}_{\mathbb{Q}}(X_0(N), E) \to \mathrm{Hom}_{\mathbb{Q}}(J_0(N), E)$ as follows:

$f \mapsto t_{-f(P)} \circ f \mapsto$ homomorphism induced from $t_{-f(P)} \circ f$ by the universal property of $J_0(N)$.

In this section, to make the text more readable, we sometimes use a slight abuse of notation. We will sometimes work with maps defined on $X_0(N)$ as if they were defined on $J_0(N)$. For example, in the proof of Theorem 3.0.11, we will say that the maps $f \circ d_i : X_0(N) \to E$ form a basis for $\mathrm{Hom}_{\mathbb{Q}}(J_0(N), E)$, but this will actually hold for the images of $f \circ d_i$ via the above map.

Definition 3.2.2. An abelian variety is called simple if it is not isogenous to a product of abelian varieties of lower dimension.

Definition 3.2.3. Let A and B be abelian varieties over a field k with B simple. An abelian variety A' together with a quotient map $\pi : A \to A'$ is an optimal B-isogenous quotient if A' is isogenous to B^n for some integer n and every morphism $A \to B'$ with B' isogenous to B^m for some integer m uniquely factors via π.

Proposition 3.2.4. Optimal B-isogenous quotients exist, and are unique up to a unique isomorphism.

Proof. By the Poincaré reducibility theorem [73, Chapter 12], [10, Theorem 5.3.7], there exists an integer s and simple abelian subvarieties $A_1,\dots,A_s$ of A such that the sum map $A_1 \times \cdots \times A_s \to A$ is an isogeny. By reordering the A_i if necessary we can let $n \leq s$ be the integer such that $A_1,\dots,A_n$ are isogenous to B while $A_{n+1},\dots,A_s$ are not. Define $A' = A/(A_{n+1} + \cdots + A_s)$ then A' is isogenous to B^n since the composition of the maps $A_1 \times \cdots \times A_n \to A \to A'$ is an isogeny.

To show that the quotient $\pi : A \to A'$ is an optimal B-isogenous quotient, let B' be an abelian variety isogenous to B^m and let $f : A \to B'$ be a morphism. Since B' is isogenous to B^m but all the A_i for $i > n$ are not isogenous to B, meaning that for $i > n$, $A_i \subset \ker f$. However, A' was obtained by quotienting out the A_i with $i > n$ meaning that f factors uniquely via π which is what we needed to prove.

The uniqueness up to unique isomorphism follows formally because optimal B-isogenous quotients are defined using a universal property. ■

Remark 3.2.5. An elliptic curve over $\mathbb{Q}$ of conductor M is called the strong Weil curve if it is an optimal E-isogenous quotient of $J_0(M)$ with the quotient map induced from the modular parametrization $f : X_0(M) \to E$ as in Section 3.1.1. Every $\mathbb{Q}$-isogeny class contains a unique strong Weil curve and for any curve E' in the $\mathbb{Q}$-isogeny class of E the modular parametrization of E' factors through f.

The dual notion of optimal B-isogenous quotient is the following:

Definition 3.2.6. Let A and B be abelian varieties over a field k with B simple. An abelian variety A' together with an isogeny $\iota : A' \to A$ is a maximal B-isogenous subvariety if A' is isogenous to B^n for some integer n and every morphism $B' \to A$ with B' isogenous to B^m for some integer m uniquely factors via ι.

The following follows formally from duality since we can just take $\iota = \pi^\vee$ where π is an optimal B-isogenous quotient of $A^\vee$. The reason for calling A' a subvariety is because, by the universal property, ι actually induces an isomorphism between A' and $\iota(A')$.

Proposition 3.2.7. Maximal B-isogenous subvarieties exist, and are unique up to a unique isomorphism.

Remark 3.2.8. The above proposition can also be proved constructively. Namely, if $A_1,\dots,A_s$ are simple abelian subvarieties of A such that the sum map $A_1\times\cdots\times A_s\to A$ is an isogeny and additionally $A_1,\dots,A_n$ are isogenous to B while $A_{n+1},\dots,A_s$ are not. Then $A_1+\cdots+A_n\subseteq A$ is a maximal B-isogenous subvariety.

Definition 3.2.9. Let N and M be positive integers with $M\mid N$ and let n denote the number of divisors of N/M. Then we define the maps $\tau_{N,M}: J_0(N)\to J_0(M)^n$, $\tau^*_{N,M}: J_0(M)^n\to J_0(N)$ as

$$\tau_{N,M} := (\iota_{1,N,M,*},\dots,\iota_{N/M,N,M,*}),$$
$$\tau^*_{N,M} := (\iota^*_{1,N,M},\dots,\iota^*_{N/M,N,M}),$$

where the first subscript of ι runs over all divisors of N/M. Further, let A be an abelian variety and $f: J_0(M)\to A$ a morphism. Then we define the map $\xi_{f,N}: J_0(N)\to A^n$ as

$$\xi_{f,N} := f^n\circ\tau_{N,M}.$$

If A is a strong Weil curve E of conductor M and f is its modular parametrization, then we use the notation $\xi_{E,N}:=\xi_{f,N}$.

With the above notation we have $\tau_{N,M}=\xi_{id_{J_0(M)},N}$.

Proposition 3.2.10. Suppose $N<408$ and let E be a strong Weil curve over $\mathbb{Q}$ of positive rank and conductor $\mathrm{Cond}(E)=M\mid N$. If n is the number of divisors of N/M, then $\xi^\vee_{E,N}: E^n\to J_0(N)$ has a trivial kernel. Hence $\xi^\vee_{E,N}: E^n\to J_0(N)$ is a maximal E-isogenous abelian subvariety and $\xi_{E,N}: J_0(N)\to E^n$ is an optimal E-isogenous quotient of $J_0(N)$.

Proof. The claim that $\xi^\vee_{E,N}: E^n\to J_0(N)$ is injective for $N<408$ was verified computationally using Sage. It is a finite computation since the restriction on N means there are only finitely pairs (N,E) for which we need to verify that $\xi^\vee_{E,N}: E^n\to J_0(N)$ is injective.

The second part follows from Atkin-Lehner-Li Theory. The decomposition

$$S_2(\Gamma_0(N)) = \bigoplus_{M\mid N}\bigoplus_{d\mid N/M}\iota^*_{d,N,M}(S_2(\Gamma_0(M))_{\mathrm{new}})$$

from [91, Theorem 9.4] yields the isogeny decomposition

$$J_0(N) = \bigoplus_{M|N} \bigoplus_{d|N/M} \iota_{d,N,M}^*(J_0(M)_{\text{new}}).$$

If $E/\mathbb{Q}$ is an elliptic curve of conductor M, then M is the only integer such that E occurs as an isogeny factor of $J_0(M)_{\text{new}}$, and does so with multiplicity one. In particular, this decomposition implies that if E is an elliptic curve of conductor M and $f : J_0(M) \to E$ is its modular parametrization, then the maps $(f \circ \iota_{d,N,M})^\vee : E \to J_0(N)$ give all the isogeny factors of $J_0(N)$ that are isogenous to E, where d ranges over all divisors of N/M. From Remark 3.2.8 it then follows that the image of $\xi_{E,N}^\vee$ inside $J_0(N)$ is a maximal E-isogenous subvariety of $J_0(N)$. However, since we already verified that $\xi_{E,N}^\vee$ has a trivial kernel, we have that $\xi_{E,N}^\vee$ is an isomorphism onto its image. In particular, $\xi_{E,N}^\vee$ is also a maximal E-isogenous subvariety of $J_0(N)$. ■

The fact that the map $\xi_{E,N}^\vee$ has a trivial kernel for the cases in which the above proposition is applicable makes it significantly easier to determine the positive rank tetraelliptic $X_0(N)$. All elliptic curves of positive $\mathbb{Q}$-rank and conductor at most 408 have rank 1, with the exception of the curve $389.a1$ which has rank 2. Proposition 3.2.14 is not needed for the classification of the positive rank tetraelliptic curves $X_0(N)$ in Theorem 3.0.11. Instead, it is an attempt to explain why we observed that the kernel of $\xi_{E,N}^\vee$ was always trivial in Proposition 3.2.10.

We now introduce the analytic rank of an elliptic curve and mention some of its properties.

Definition 3.2.11. The L-function of an elliptic curve $E/\mathbb{Q}$ of conductor N is defined as

$$L(E,s) = \prod_p (1 - a_p p^{-s} + \mathbf{1}_{p\nmid N} p^{1-2s})^{-1}.$$

This product converges for $\Re(s) > \frac{3}{2}$ and can be analytically extended to the whole $\mathbb{C}$ [25, Chapter 5.9]. The analytic rank of E is the order of vanishing of $L(E,1)$.

Let f be a rational newform. We define its L-function $L(f,s) = L(E,s)$, where E is a corresponding elliptic curve over $\mathbb{Q}$.

Lemma 3.2.12. We have $a_p = \pm 1$ when the reduction mod p is multiplicative and $a_p = 0$ when the reduction mod p is additive.

Proof. For an elliptic curve $\tilde{E} : y^2 = x^3 + \tilde{a}x + \tilde{b}$ defined over $\mathbb{F}_p$ we have

$$\#\tilde{E}(\mathbb{F}_p) = p + 1 + \sum_{i=0}^{p-1} \left(\frac{i^3 + ai + b}{p} \right).$$

Here $\left(\frac{x}{p}\right)$ denotes the Legendre symbol. If the reduction mod p is multiplicative, then the equation of the reduced curve is of the form

$$\tilde{E} : y^2 = (x-s)(x-t)^2$$

for some $s \neq t \in \mathbb{F}_p$ and the formula for the number of $\mathbb{F}_p$-points becomes

$$\#\tilde{E}(\mathbb{F}_p) = p + 1 + \sum_{i=0}^{p-1} \left(\frac{(i-s)(i-t)^2}{p} \right).$$

There are exactly $\frac{p-1}{2}$ quadratic residues and non-residues mod p. If $s-t$ is a quadratic residue, then $\#\tilde{E}(\mathbb{F}_p) = 2 \cdot \frac{p-1}{2} - 1 + 1 + 1 = p$. The last three summands are for the points $(t,0)$, $(0,0)$, and $\mathscr{O}$, respectively. Therefore, $a_p = p + 1 - p = 1$. If $s-t$ is not a quadratic residue, we similarly get $\#\tilde{E}(\mathbb{F}_p) = 2 \cdot \frac{p-1}{2} + 1 + 1 + 1 = p + 2$ and $a_p = p + 1 - (p+2) = -1$.

If the reduction mod p is additive, then the equation of the reduced curve is of the form

$$\tilde{E} : y^2 = (x-t)^3$$

for some $t \in \mathbb{F}_p$ and the formula for the number of $\mathbb{F}_p$-points becomes

$$\#\tilde{E}(\mathbb{F}_p) = p + 1 + \sum_{i=0}^{p-1} \left(\frac{(i-t)^3}{p} \right) = 2 \cdot \frac{p-1}{2} + 1 + 1 = p + 1.$$

The last two summands are for the points $(t,0)$ and $\mathscr{O}$, respectively. Therefore, $a_p = p + 1 - (p+1) = 0$. ■

Conjecture 3.2.13 (Birch and Swinnerton-Dyer conjecture)**.** Let $E/\mathbb{Q}$ be an elliptic

curve. Then its algebraic and analytic ranks are equal.

Only some special cases of this conjecture have been proven. Gross and Zagier [34] proved that

$$\text{analytic rank} = 1 \implies \text{algebraic rank} \geq 1$$

and Kolyvagin [65] improved this result. He proved that for $r = 0, 1$ we have

$$\text{analytic rank} = r \implies \text{algebraic rank} = r.$$

Proposition 3.2.14. Let E be a strong Weil curve over $\mathbb{Q}$ of conductor $M \mid N$ and let us suppose that $\dfrac{N}{M}$ is squarefree and coprime to M. If E has an odd analytic rank, then the kernel of $\xi_{E,N}^{\vee} : E^n \to J_0(N)$ is a 2-group (n is again the number of divisors of $\dfrac{N}{M}$).

The main ingredient in the proof of this proposition is Theorem 3.2.16.

Definition 3.2.15. Let M be a positive integer and let $\pi : X_1(M) \to X_0(M)$ be the natural map $(E,P) \mapsto (E,\langle P\rangle)$. The Shimura subgroup $\Sigma(M)$ is the kernel of the map $\pi^* : J_0(M) \to J_1(M)$. For an abelian subvariety $A \subseteq J_0(M)$ we define the Shimura subgroup of A to be $A \cap \Sigma(M)$

Theorem 3.2.16 ([66, Theorem 4])**.** Let N be a positive integer, and let M be a divisor of N such that $\dfrac{N}{M} = q_1 \dots q_t$ (distinct primes) and $\gcd\left(M, \dfrac{N}{M}\right) = 1$. We define

$$\Sigma(M)_0^{2^t} := \left\{ (x_1, \dots, x_{2^t}) : x_i \in \Sigma(M), \sum_1^{2^t} x_i = 0 \right\}.$$

We recall from Definition 3.2.9 the map $\tau_{N,M}^* := (\iota_{1,N,M}^*, \dots, \iota_{N/M,N,M}^*) : J_0(M)^{2^t} \to J_0(N)$.

(i) If M is odd or $\dfrac{N}{M}$ is a prime, then $\ker \tau_{N,M}^* = \Sigma(M)_0^{2^t}$.

(ii) If M is even and $\dfrac{N}{M}$ is not a prime, then $\ker \tau_{N,M}^*$ and $\Sigma(M)_0^{2^t}$ are equal up to a 2-group.

Lemma 3.2.17. Let E be an elliptic curve with conductor M. Then the Atkin-Lehner involution w_M acts on $E \subset J_0(M)$ as 1 if the analytic rank of E is odd and as -1 if the analytic rank of E is even.

Proof. E occurs with multiplicity 1 in the factorisation of $J_0(M)$. Therefore, we have that w_M acts on E. Moreover, by taking the corresponding cusp form f, we get that (since f is an eigenform for Atkin-Lehner involutions and Hecke operators) w_M acts on E as multiplication by a constant ε. Since w_M is an involution, we get $\varepsilon^2 = 1$, i.e. $\varepsilon = \pm 1$.

For a rational newform f of level N we define the function

$$\Lambda(f,s) = N^{s/2}(2\pi)^{-s}\Gamma(s)L(f,s),$$

where $\Gamma(s) = \int_0^\infty t^{s-1}e^{-t}dt$ is the usual Gamma function. From Section 10.5.1 of [91] we have the functional equation

$$\Lambda(f,s) = -\varepsilon\Lambda(f,2-s).$$

If we define $\Lambda'(f,s) := \Lambda(f,s+1)$, the equation becomes

$$\Lambda'(f,s) = -\varepsilon\Lambda'(f,-s).$$

Now, if $\varepsilon = 1$, then $\Lambda'(f,\cdot)$ is an odd function so only odd powers appear in the series expansion. Since $\Gamma(1) = 1$, the analytic rank of E is odd. We similarly conclude that $\varepsilon = -1$ implies that the analytic rank of E is even. ■

Proof of Proposition 3.2.14. Theorem 3.2.16 tells us that the kernel of $\tau_{N,M}^*$ is equal to $\Sigma(M)_0^{2^t}$ up to a 2-group. Since E is a strong Weil curve, we have that $f^\vee : E \to J_0(M)$ actually turns E into a subvariety of $J_0(M)$. Therefore, we have $\ker \xi_{E,N}^\vee = \ker \tau_{N,M}^* \cap E^{2^t}$. This is, up to a 2-group, equal to $\Sigma(M)_0^{2^t} \cap E^{2^t}$, which is isomorphic to $(\Sigma(M) \cap E)^{2^t-1}$. Now it is enough to prove that $\Sigma(M) \cap E$ is a 2-group.

By [70, Chapter II, Proposition 11.7], the Atkin-Lehner involution w_M acts as -1 on $\Sigma(M)$. Further, since E has an odd analytic rank, it follows by looking at the functional equation for $L(E,s)$ that w_M acts as 1 on E. Therefore, $-1 = 1$ on $\Sigma(M) \cap E$ meaning that $\Sigma(M) \cap E$ must be a 2-group. ■

Theorem 3.2.16 is not enough to prove that $\xi_{E,N}^\vee$ is always injective for strong Weil curves of odd analytic rank. However, the computational evidence of Proposition 3.2.10

seems to indicate the possibility that the 2-group admitted by Theorem 3.2.16 cannot actually occur. We therefore make the following conjecture.

Conjecture 3.2.18. Let E be a strong Weil curve over $\mathbb{Q}$ of conductor $M \mid N$. If E has an odd analytic rank, then $\xi_{E,N}^{\vee}$ is injective.

All but one of the strong Weil curves E considered in the proof of Proposition 3.2.10 have analytic rank 1, the exception being the curve $389.a1$ with analytic rank 2. Therefore, if this conjecture turns out to be correct, in the first part of Proposition 3.2.10, Sage will only be needed to prove that $\xi_{E,N}$ has a trivial kernel for the elliptic curve $389.a1$.

Note that the above conjecture, if true, makes the determination of all positive rank d-elliptic $X_0(N)$ significantly easier. Since the above conjecture together with Theorem 3.1.13 implies the following:

Corollary 3.2.19. Assume Conjecture 3.2.18. Let E be a strong Weil curve over $\mathbb{Q}$ of odd analytic rank, conductor M, and parametrization $f : X_0(M) \to E$. If N is a multiple of M and $g : X_0(N) \to E'$ is a map with E' isogenous to E, then $\deg f \mid \deg g$.

This would give us a lower bound on $\deg g$, allowing us to consider significantly fewer elliptic curves E in the determination of positive rank d-elliptic $X_0(N)$.

3.3. CURVES $X_0(N)$ WITH INFINITELY MANY QUARTIC POINTS

In this section, we will prove that for levels N listed in the Theorem 3.0.7 the curve $X_0(N)$ has infinitely many quartic points. When $X_0(N)$ already has infinitely many quadratic points (these N are listed in Theorem 3.0.5), this is trivial. Now we consider the other cases.

We will use two methods for obtaining quartic points on a curve C defined over a number field k. Both methods obtain quartic points as pullback via rational maps from C. The first method uses a degree 4 morphism to a curve C' with infinitely many rational points (recall that Faltings' theorem implies that the only such curves C' are of genus 0 or genus 1 with positive k-rank), and the second method uses a degree 2 morphism to a curve C' with infinitely many quadratic points. The following proposition verifies these methods.

Proposition 3.3.1. Let k be a number field and let d be a positive integer. Suppose C and C' are smooth, projective, and geometrically integral curves defined over k and let $f : C \to C'$ be a morphism of degree $d' \mid d$ defined over k. If C' has infinitely many points of degree $\frac{d}{d'}$ over k, then C has infinitely many points of degree $\leq d$ over k.

Proof. Let P be a point on C' of degree $\frac{d}{d'}$ over k and let $K \supset k$ be its field of definition. Then the preimage $f^{-1}(P)$ has size $\leq d'$. Let $Q \in C(\overline{\mathbb{Q}})$ be an element of $f^{-1}(P)$. For every automorphism $\sigma \in G_K$, where G_K is an absolute Galois group over K, we have

$$f(\sigma(Q)) = \sigma(f(Q)) = \sigma(P) = P.$$

Therefore, $\sigma(Q) \in f^{-1}(P)$ for every $\sigma \in G_K$. This means that, since $\#f^{-1}(P) \leq d'$, Q must be defined over some field L such that $[L : K] \leq d'$, or equivalently $[L : k] \leq d$. ■

As we can see, this pullback method gives points of degree $\leq d$ over k. Therefore, if there are infinitely many points of degree $\leq d-1$ on C, we cannot immediately conclude that C has infinitely many points of degree d. This can be resolved, however, using The-

orems 4.2 and 4.3 of [12] which tell us that, as soon as one of the points in the pullback has degree d, there will be infinitely many points of degree d on C. We will use this proposition to find infinitely many quartic points $X_0(N)$ by taking $d = 4$ and $d' = 1$ or 2.

Remark 3.3.2. Interestingly, from Theorems 3.0.5 and 3.0.6 it follows that if $X_0(N)$ has infinitely many cubic points, then $X_0(N)$ also has infinitely many quadratic points. This means that the curve $X_0(N)$ has infinitely many points of degree ≤ 4 if and only if it has infinitely many points of degree 4.

Proposition 3.3.3. The curve $X_0(N)$ has infinitely many quartic points for

$$N \in \{34, 45, 54, 64, 81\}.$$

Proof. For each of these N, the quotient $X_0(N)/\langle w_N \rangle$ is an elliptic curve and therefore has infinitely many quadratic points. Now we use Proposition 3.3.1 for the degree 2 quotient map from $X_0(N)$ to $X_0(N)/\langle w_N \rangle$. ■

Proposition 3.3.4. The curve $X_0(N)$ has infinitely many quartic points for

$$\begin{aligned} N \in \{&38, 42, 44, 51, 52, 55-58, 60, 62, 63, 66-70, 72-75, 77, 78, 80, 85, 87, 88, \\ &91, 92, 94-96, 98, 100, 103, 104, 107, 111, 119, 121, 125, 142, 143, 167, 191\}. \end{aligned}$$

Proof. For each of these N the curve $X_0(N)$ has $\mathbb{Q}$-gonality equal to 4 by [76, Tables 1,2,3]. Using Proposition 3.3.1 we now conclude that there are infinitely many points of degree ≤ 4 on $X_0(N)$ for these N. Therefore, these curves $X_0(N)$ have infinitely many quartic points by Remark 3.3.2. ■

Proposition 3.3.5. The curve $X_0(N)$ has infinitely many quartic points for the following values of N:

Table 3.1: The values of N for Proposition 3.3.5.

N	LMFDB label of $X_0^*(N)$
82	82.a2
86	43.a1
99	99.a2
118	118.a1
123	123.b1
141	141.d1
145	145.a1
155	155.c1
159	53.a1

Proof. For each of these N we can use the Magma function X0NQuotient() to prove that the quotient $X_0^*(N)$ is an elliptic curve with the LMFDB label as in the table above. LMFDB also tells us that this elliptic curve is of rank 1 over $\mathbb{Q}$. Now we use Proposition 3.3.1 for the degree 4 quotient map from $X_0(N)$ to $X_0^*(N)$. ■

Remark 3.3.6. The proof of Proposition 3.3.5 applies to the following levels N as well:

Table 3.2: The values of N for Remark 3.3.6.

N	LMFDB label of $X_0^*(N)$
57	57.a1
58	58.a1
74	37.a1
77	77.a1
91	91.a1
111	37.a1
142	142.a1

143	143.a1

Also, the curve $X_{\text{ns}}^+(11)$ is an elliptic curve with LMFDB label 121.b2. It has conductor 121, modular degree 4, and rank 1 over $\mathbb{Q}$. Therefore, we have a degree 4 rational morphism from $X_0(121)$ to a positive rank elliptic curve.

We list these cases here separately since they have already been solved in Proposition 3.3.4, but we need a morphism to a positive rank elliptic curve for Theorem 3.0.11.

Proposition 3.3.7. The curve $X_0(128)$ has infinitely many quartic points.

Proof. The elliptic curve $y^2 = x^3 + x^2 + x + 1$ has conductor 128, modular degree 4, and rank 1 over $\mathbb{Q}$. This curve has Cremona label 128a1 [16] and LMFDB label128.a2. Now we use Proposition 3.3.1 for the degree 4 morphism from $X_0(128)$ to this elliptic curve. ■

3.4. CURVES $X_0(N)$ WITH FINITELY MANY QUARTIC POINTS

In this section, we will prove that for levels N not listed in the Theorem 3.0.7 the curve $X_0(N)$ has only finitely many quartic points. The first step to do that is to reduce this problem to a finite problem by giving an upper bound for N such that the curve $X_0(N)$ has infinitely many quartic points.

As we mentioned in the introduction of Chapter 3, Frey's result [31, Proposition 2] gives us that any curve defined over $\mathbb{Q}$ with infinitely many quartic points must have $\mathbb{Q}$-gonality ≤ 8. Furthermore, Theorem 2.0.3 gives us the lower bound on the $\mathbb{C}$-gonality of any modular curve. In our case, we get $\mathrm{gon}_{\mathbb{C}} X_0(N) \geq \frac{119}{12000}N$ which means that for $N > \frac{8 \cdot 12000}{119}$ the curve $X_0(N)$ has only finitely many quartic points (here we used a trivial fact that $\mathrm{gon}_{\mathbb{Q}} C \geq \mathrm{gon}_{\mathbb{C}} C$ for any curve C defined over $\mathbb{Q}$). However, this bound is impractical here.

When the genus of C is high enough, the following theorem by Kadets and Vogt tells us that this pullback method is the only way to obtain points of a certain degree.

Theorem 3.4.1 ([54], Theorem 1.3)**.** Suppose X/k is a curve of genus g and $\mathrm{a.irr}_k X = d$. Let $m := \lceil d/2 \rceil - 1$ and let $\varepsilon := 3d - 1 - 6m < 6$. Then one of the following holds:

(1) There exists a nonconstant morphism of curves $\phi : X \to Y$ of degree at least 2 such that $d = \mathrm{a.irr}_k Y \cdot \deg \phi$.

(2) $g \leq \max\left(\frac{d(d-1)}{2} + 1, 3m(m-1) + m\varepsilon\right)$.

Corollary 3.4.2. Suppose $C/\mathbb{Q}$ is a curve of genus $g \geq 8$ and $\mathrm{a.irr}_{\mathbb{Q}} C = 4$. Then there exists a nonconstant morphism of degree 4 from C to $\mathbb{P}^1$ or an elliptic curve defined over $\mathbb{Q}$ with positive $\mathbb{Q}$-rank.

Proof. We compute $m = 1$ and $\varepsilon = 5$. Therefore, case (2) of the previous theorem is impossible and we have a morphism $f : C \to Y$ of degree 2 or 4.

If the degree of f is 2, then we have $\mathrm{a.irr}_{\mathbb{Q}} Y = 2$ and Y is a double cover of $\mathbb{P}^1$ or an elliptic curve with a positive $\mathbb{Q}$-rank by Theorem 3.0.4. If the degree of f is 4, then we

have $\text{a.irr}_{\mathbb{Q}} Y = 1$ and Y is isomorphic to $\mathbb{P}^1$ or an elliptic curve with a positive $\mathbb{Q}$-rank by Faltings' theorem. ■

This means that for levels N such that the genus of the curve $X_0(N)$ is at least 8 the existence of infinitely many quartic points is equivalent with the existence of a degree 4 morphism to $\mathbb{P}^1$ or to an elliptic curve with a positive $\mathbb{Q}$-rank.

Since for all levels N not listed in Theorem 3.0.7 the curve $X_0(N)$ has $\mathbb{Q}$-gonality > 4 by Theorem 2.1.2 and since $g(X_0(N)) > 7$ for all $N > 100$, Corollary 3.4.2 gives us that any potential $X_0(N)$ with infinitely many quartic points must be tetraelliptic. Now we can get a much better bound for N using Lemma 2.1.7.

Corollary 3.4.3. If the curve $X_0(N)$ is tetraelliptic, then for every prime $p \nmid N$ we must have

$$4(p+1)^2 \geq L_p(N) = \frac{p-1}{12}\psi(N) + 2^{\omega(N)}.$$

Proof. Suppose we have a degree 4 rational morphism $X_0(N) \to E$ for some elliptic curve $E/\mathbb{Q}$. Therefore $\text{cond}(E) \mid N$ and p is a prime of good reduction for E.

Theorem 1.5.7 tells us that the number of $\mathbb{F}_{p^2}$-rational points on E is at most $p^2 + 1 + 2 \cdot 1 \cdot p = (p+1)^2$. We conclude that $\#X_0(N)(\mathbb{F}_{p^2}) \leq 4(p+1)^2$ similarly as in Lemma 2.1.8. Lemma 2.1.7 tells us that $\#X_0(N)(\mathbb{F}_p^2) \geq L_p(N)$, completing the proof. ■

Now, applying Corollary 3.4.3 in the same way as in Proposition 2.1.9, we get

Corollary 3.4.4. The curve $X_0(N)$ is not tetraelliptic for all $N \geq 402$ and

$$\begin{aligned} N \in \{&154, 174, 190, 198, 202, 204, 212, 222, 224, 228, 231, 232, 234, 236, 244, 246, \\ &248, 256, 258, 260, 262, 270, 272, 273, 276, 279, 282, 284-287, 290, 296, 301, \\ &303-306, 308, 310, 312, 316, 318, 320-322, 324-328, 330, 332-336, \\ &338-340, 342, 344-346, 348, 350-352, 354-358, 360, 362-366, \\ &368-372, 374-378, 380-382, 384-388, 390-396, 398-400\}. \end{aligned}$$

This means that we only need to check a reasonably small number of levels N for tetraellipticity. First, though, we separately solve the cases when $g(X_0(N)) \leq 7$ and we

cannot use Theorem 3.4.1. The only N not discussed already for which $g(X_0(N)) \leq 7$ is $N = 97$.

Proposition 3.4.5. The curve $X_0(97)$ has only finitely many quartic points.

Proof. Suppose that there are infinitely many quartic points on $X_0(97)$. Since the curve $X_0(97)$ has $\mathbb{Q}$-gonality 6 by Theorem 2.1.4 and genus 7, we can apply [50, Proposition 1.6] and get that the Jacobian $J_0(97)$ must contain an elliptic curve with a positive $\mathbb{Q}$-rank. However, up to isogeny, $J_0(97)$ only contains abelian varieties of dimension 3 and 4 and we get a contradiction. ■

It is worth mentioning here that for levels N in the following table there exist morphisms of degree 4 to elliptic curves. For $N \neq 109$, these morphisms are quotient maps which are, for N divisible by 4, composed with degree 2 degeneracy maps from $X_0(N)$ to $X_0\left(\frac{N}{2}\right)$. However, these elliptic curves are of rank 0 over $\mathbb{Q}$ and therefore generate only finitely many quartic points.

Table 3.3: Levels N for which there exist morphisms of degree 4 to an elliptic curve E of rank 0 over $\mathbb{Q}$

N	E
76	$X_0(38)/\langle w_{38}\rangle$, $X_0(38)/\langle w_{19}\rangle$
105	$X_0(105)/\langle w_3, w_{35}\rangle$
108	$X_0(54)/\langle w_{54}\rangle$, $X_0(54)/\langle w_{27}\rangle$
109	$y^2+xy = x^3-x^2-8x-7$ (LMFDB label 109.a1)
110	$X_0(110)/\langle w_2, w_{55}\rangle$
112	$X_0(56)/\langle w_{56}\rangle$, $X_0(56)/\langle w_7\rangle$
124	$X_0(62)/\langle w_{31}\rangle$
184	$X_0(92)/\langle w_{23}\rangle$
188	$X_0(94)/\langle w_{47}\rangle$

Now we are ready to prove the two main theorems: Theorem 3.0.7 and Theorem 3.0.11.

Proof of Theorem 3.0.11. The proofs of Propositions 3.3.5, 3.3.7 and Remark 3.3.6 tell us that $X_0(N)$ is positive rank tetraelliptic for all levels N listed in Theorem 3.0.11. Now we prove that for the other N the curve $X_0(N)$ is not positive rank tetraelliptic. We only need to consider $N < 408$ not already eliminated in Corollary 3.4.4 for which there exists an elliptic curve of conductor $M \mid N$ of positive $\mathbb{Q}$-rank. Further, if $M = N$, then any morphism from $X_0(N)$ factors through the modular parametrization of a strong Weil curve in the corresponding isogeny class. However, the modular degree is strictly greater than 4 in all such cases. Therefore, we may suppose $M < N$.

Let E be a strong Weil curve of conductor $M \mid N$ and positive $\mathbb{Q}$-rank, n the number of divisors of N/M, and $f : X_0(M) \to E$ its modular parametrization. Since $\xi_{E,N} : J_0(N) \to E^n$ for $N < 408$ is an E-isogenous optimal quotient by Proposition 3.2.10, every map from $J_0(N)$ to E uniquely factors through E^n. Therefore, we get that the maps $f \circ d_i$, where d_i runs over the degeneracy maps $X_0(N) \to X_0(M)$, form a basis for $\mathrm{Hom}_{\mathbb{Q}}(J_0(N), E) \cong \mathrm{Hom}_{\mathbb{Q}}(E^n, E) \cong \mathbb{Z}^n$. Theorem 3.1.13 and Remark 3.1.14 allow us to compute the degree pairing on this basis. Now, the degree of a map $\sum_{i|N/M} x_i(f \circ d_i)$ is given by a positive definite quadratic form

$$\sum_{i|N/M} \sum_{j|N/M} x_i x_j \left\langle f \circ d_i, f \circ d_j \right\rangle .$$

All levels N and strong Weil curves E which were considered in this proof are given in the Table D.1.

Using the norm induced by this quadratic form, we can use the Fincke-Pohst algorithm for enumerating integer vectors of small norm [29] to determine that there are no nonconstant elements of $\mathrm{Hom}_{\mathbb{Q}}(J_0(N), E)$ of degree ≤ 4, and hence no elements of $\mathrm{Hom}_{\mathbb{Q}}(X_0(N), E)$ of degree ≤ 4. So this proves the statement for strong Weil curves.

If E is not a strong Weil curve, let E' be a strong Weil curve in the isogeny class of E. Then by the E-isogenous optimality of $\xi_{E',N} : J_0(N) \to (E')^n$ we have that any $g \in \mathrm{Hom}_{\mathbb{Q}}(J_0(N), E)$ factors as $h \circ \xi_{E',N}$ for some $h \in \mathrm{Hom}_{\mathbb{Q}}((E')^n, E)$. Also, the map

$$\pi : \mathrm{Hom}_{\mathbb{Q}}((E')^n, E) \to \mathrm{Hom}_{\mathbb{Q}}(E', E)^n,\ \pi(f) = (f \restriction_{E'_1}, \ldots, f \restriction_{E'_n}),$$

where E_i' is the i-th component of $(E')^n$, is an isomorphism with an inverse map

$$\pi^{-1}((f_1,\ldots,f_n))(x_1,\ldots,x_n) = f_1(x_1)+\ldots+f_n(x_n).$$

Furthermore, we have that $\mathrm{Hom}_{\mathbb{Q}}(E',E)$ is a free $\mathrm{Hom}_{\mathbb{Q}}(E',E')(\cong\mathbb{Z})$-module of rank 1, generated by a single element g_2. In particular, any $f\in\mathrm{Hom}_{\mathbb{Q}}(E',E)$ can be written as $g_2\circ[m]$ for some $m\in\mathbb{Z}$.

Therefore, we have $\pi(h)=(f_1,\ldots,f_n)=g_2\circ([m_1],\ldots,[m_n])$ and $h(x_1,\ldots,x_n)=g_2(m_1x_1+\ldots+m_nx_n)$. This means that $h=g_2\circ m$ for some $m\in\mathrm{Hom}_{\mathbb{Q}}((E')^n,E')$. Returning back to our $g\in\mathrm{Hom}_{\mathbb{Q}}(J_0(N),E)$, we see that it factors as $g_2\circ m\circ\xi_{E',N}$. It follows that

$$\deg g=\deg g_2\cdot\deg(m\circ\xi_{E',N})\geq\deg(m\circ\xi_{E',N})>4$$

since E' is a strong Weil curve and $m\circ\xi_{E',N}$ is a rational map. ■

In most cases, especially when we have only 2 degeneracy maps, we do not actually need the Fincke-Pohst algorithm to prove that there are no nonconstant elements of $\mathrm{Hom}_{\mathbb{Q}}(J_0(N),E)$ of degree ≤ 4. We show several examples where we prove that with elementary methods.

Example 3.4.6. We take $N=122$. There exist two elliptic curves E of positive $\mathbb{Q}$-rank and conductor $\mathrm{cond}(E)\mid N$. One of them has conductor equal to N and modular degree 8 and can therefore be eliminated. The other one is $E=X_0^+(61)$. Its modular parametrization f is the quotient map $X_0(61)\to X_0^+(61)$.

By the proof of Theorem 3.0.11, the basis for $\mathrm{Hom}_{\mathbb{Q}}(J_0(122),E)$ is $\{f\circ d_1, f\circ d_2\}$ and both of these maps have degree $2\cdot 3=6$. Further, by Theorem 3.1.13, we have

$$\langle f\circ d_1, f\circ d_2\rangle=[a_2\cdot 1\cdot 2]=[-2].$$

This means that any map $J_0(122)\to E$ must have degree equal to

$$6x^2-4xy+6y^2$$

for some integers x,y. It remains to prove that this expression can never be equal to 4.

Let us suppose the contrary. If both x and y are not 0, then $6x^2 - 4xy + 6y^2 = 4x^2 + 2(x-y)^2 + 4y^2 \geq 8$. Therefore, we may without loss of generality set $y = 0$. However, the expression now becomes $6x^2$ which cannot be equal to 4, contradiction.

Example 3.4.7. We take $N = 129$. There exist two elliptic curves E of positive $\mathbb{Q}$-rank and conductor $\mathrm{cond}(E) \mid N$. One of them has conductor equal to N and modular degree 8 and can therefore be eliminated. The other one is $E = X_0^+(43)$. Its modular parametrization f is the quotient map $X_0(43) \to X_0^+(43)$.

By the proof of Theorem 3.0.11, the basis for $\mathrm{Hom}_{\mathbb{Q}}(J_0(129), E)$ is $\{f \circ d_1, f \circ d_3\}$ and both of these maps have degree $2 \cdot 4 = 8$. Further, by Theorem 3.1.13, we have

$$\langle f \circ d_1, f \circ d_3 \rangle = [a_3 \cdot 1 \cdot 2] = [-4].$$

This means that any map $J_0(129) \to E$ must have degree equal to

$$8x^2 - 8xy + 8y^2$$

for some integers x, y. This expression is divisible by 8 and cannot therefore be equal to 4.

Example 3.4.8. We take $N = 148$. There exist two elliptic curves E of positive $\mathbb{Q}$-rank and conductor $\mathrm{cond}(E) \mid N$. One of them has conductor equal to N and modular degree 12 and can therefore be eliminated. The other one is $E = X_0^+(37)$. Its modular parametrization f is the quotient map $X_0(37) \to X_0^+(37)$.

In this case N/M is not squarefree like in the previous two examples. However, N/M and M are coprime and we can still use Theorem 3.1.13.

By the proof of Theorem 3.0.11, the basis for $\mathrm{Hom}_{\mathbb{Q}}(J_0(148), E)$ is $\{f \circ d_1, f \circ d_2, f \circ d_4\}$ and these maps have degree $2 \cdot 6 = 12$. Further, by Theorem 3.1.13, we have

$$\langle f \circ d_1, f \circ d_2 \rangle = [a_2 \cdot 2 \cdot 2] = [-8],$$

$$\langle f \circ d_1, f \circ d_4 \rangle = [(a_4 - a_1)) \cdot 1 \cdot 2] = [2],$$

$$\langle f \circ d_2, f \circ d_4 \rangle = [a_2 \cdot 2 \cdot 2] = [-8].$$

This means that any map $J_0(148) \to E$ must have degree equal to

$$12x^2 + 12y^2 + 12z^2 - 16xy + 4xz - 16yz$$

for some integers x, y, z. This expression is equal to

$$2(x+z-2y)^2 + 2(2x-y)^2 + 2(2z-y)^2 + 2x^2 + 2z^2.$$

Let us suppose that it is equal to 4 for some x, y, z. If both x and z are not 0, then $2x^2 + 2z^2 \geq 4$ and the other terms must be equal to 0. This would mean that $x+z-2y = 2x-y = 2z-y = 0$. We can easily check that this is impossible.

Therefore, we may without loss of generality set $z = 0$. The expression now becomes $12x^2 - 16xy + 12y^2 = 8(x-y)^2 + 4x^2 + 4y^2$. As before, we see that x or y must be 0 (otherwise $4x^2 + 4y^2 \geq 8$) and that $x = y$ (otherwise $8(x-y)^2 \geq 8$). This means that $x = y = z = 0$ and we get a contradiction.

Proof of Theorem 3.0.7. The results in Section 3.3 give us the cases when $X_0(N)$ has infinitely many quartic points and Proposition 3.4.5 tells us that the curve $X_0(97)$ has only finitely many quartic points.

For the other levels N, we have $g(X_0(N)) \geq 8$, $\text{a.irr}_{\mathbb{Q}}(X_0(N)) > 3$, $\text{gon}_{\mathbb{Q}}(X_0(N)) > 4$ by [76, Tables 1,2,3], and that $X_0(N)$ is not positive rank tetraelliptic over $\mathbb{Q}$ by Theorem 3.0.11. Therefore, Corollary 3.4.2 tells us that $X_0(N)$ has only finitely many quartic points for these levels N. ■

APPENDIX A

This appendix contains the tables with the $\mathbb{Q}$-gonalities of modular curves $X_0(N)$ associated with Section 2.1. For each value of N, there are 7 entries, listed in the order that they appear in: the genus g, the gonality of $X_0(N)$ over $\mathbb{Q}$ (denoted by $\text{gon}_{\mathbb{Q}}$), references to how the lower and upper bound for the $\mathbb{Q}$-gonality were obtained (denoted by LB and UB, respectively), the gonality of $X_0(N)$ over $\mathbb{C}$ (denoted by $\text{gon}_{\mathbb{C}}$) and finally references to how the lower and upper bound for the $\mathbb{C}$-gonality were obtained (again denoted by LB and UB, respectively).

For larger N, we show only those whose $\mathbb{Q}$-gonality we have determined and skip the others.

Table A.1: Gonality of the curve $X_0(N)$.

N	g	$\text{gon}_{\mathbb{Q}}$	LB	UB	$\text{gon}_{\mathbb{C}}$	LB	UB
≤ 10	0	1			1		
11	1	2	[80]	[80]	2	[80]	[80]
12	0	1			1		
13	0	1			1		
14	1	2	[80]	[80]	2	[80]	[80]
15	1	2	[80]	[80]	2	[80]	[80]
16	0	1			1		
17	1	2	[80]	[80]	2	[80]	[80]
18	0	1			1		
19	1	2	[80]	[80]	2	[80]	[80]
20	1	2	[80]	[80]	2	[80]	[80]

21	1	2	[80]	[80]	2	[80]	[80]
22	2	2	[80]	[80]	2	[80]	[80]
23	2	2	[80]	[80]	2	[80]	[80]
24	1	2	[80]	[80]	2	[80]	[80]
25	0	1			1		
26	2	2	[80]	[80]	2	[80]	[80]
27	1	2	[80]	[80]	2	[80]	[80]
28	2	2	[80]	[80]	2	[80]	[80]
29	2	2	[80]	[80]	2	[80]	[80]
30	3	2	[80]	[80]	2	[80]	[80]
31	2	2	[80]	[80]	2	[80]	[80]
32	1	2	[80]	[80]	2	[80]	[80]
33	3	2	[80]	[80]	2	[80]	[80]
34	3	3	$\mathrm{gon}_{\mathbb{C}}$	[37]	3	[37]	[37]
35	3	2	[80]	[80]	2	[80]	[80]
36	1	2	[80]	[80]	2	[80]	[80]
37	2	2	[80]	[80]	2	[80]	[80]
38	4	4	2.1.34	[37]	3	[37]	[37]
39	3	2	[80]	[80]	2	[80]	[80]
40	3	2	[80]	[80]	2	[80]	[80]
41	3	2	[80]	[80]	2	[80]	[80]
42	5	4	$\mathrm{gon}_{\mathbb{C}}$	2.1.25	4	[53]	[53]
43	3	3	$\mathrm{gon}_{\mathbb{C}}$	[37]	3	[37]	[37]
44	4	4	2.1.34	[37]	3	[37]	[37]
45	3	3	$\mathrm{gon}_{\mathbb{C}}$	[37]	3	[37]	[37]
46	5	2	[80]	[80]	2	[80]	[80]
47	4	2	[80]	[80]	2	[80]	[80]
48	3	2	[80]	[80]	2	[80]	[80]
49	1	2	[80]	[80]	2	[80]	[80]
50	2	2	[80]	[80]	2	[80]	[80]
51	5	4	$\mathrm{gon}_{\mathbb{C}}$	2.1.24	4	[53]	[53]

52	5	4	$\mathrm{gon}_{\mathbb{C}}$	2.1.25	4	[53]	[53]
53	4	4	2.1.34	[37]	3	[37]	[37]
54	4	3	$\mathrm{gon}_{\mathbb{C}}$	[37]	3	[37]	[37]
55	5	4	$\mathrm{gon}_{\mathbb{C}}$	2.1.24	4	[53]	[53]
56	5	4	$\mathrm{gon}_{\mathbb{C}}$	2.1.24	4	[53]	[53]
57	5	4	$\mathrm{gon}_{\mathbb{C}}$	2.1.25	4	[53]	[53]
58	6	4	$\mathrm{gon}_{\mathbb{C}}$	2.1.25	4	[53]	[53]
59	5	2	[80]	[80]	2	[80]	[80]
60	7	4	$\mathrm{gon}_{\mathbb{C}}$	2.1.25	4	[53]	[53]
61	4	4	2.1.34	[37]	3	[37]	[37]
62	7	4	$\mathrm{gon}_{\mathbb{C}}$	2.1.24	4	[53]	[53]
63	5	4	$\mathrm{gon}_{\mathbb{C}}$	2.1.24	4	[53]	[53]
64	3	3	$\mathrm{gon}_{\mathbb{C}}$	[37]	3	[37]	[37]
65	5	4	$\mathrm{gon}_{\mathbb{C}}$	2.1.24	4	[53]	[53]
66	9	4	$\mathrm{gon}_{\mathbb{C}}$	2.1.25	4	[53]	[53]
67	5	4	$\mathrm{gon}_{\mathbb{C}}$	2.1.25	4	[53]	[53]
68	7	4	$\mathrm{gon}_{\mathbb{C}}$	2.1.25	4	[53]	[53]
69	7	4	$\mathrm{gon}_{\mathbb{C}}$	2.1.24	4	[53]	[53]
70	9	4	$\mathrm{gon}_{\mathbb{C}}$	2.1.25	4	[53]	[53]
71	6	2	[80]	[80]	2	[80]	[80]
72	5	4	$\mathrm{gon}_{\mathbb{C}}$	2.1.26	4	[53]	[53]
73	5	4	$\mathrm{gon}_{\mathbb{C}}$	2.1.25	4	[53]	[53]
74	8	4	$\mathrm{gon}_{\mathbb{C}}$	2.1.25	4	[53]	[53]
75	5	4	$\mathrm{gon}_{\mathbb{C}}$	2.1.24	4	[53]	[53]
76	8	6	2.1.34	2.1.27	5	[53]	2.0.2(v)
77	7	4	$\mathrm{gon}_{\mathbb{C}}$	2.1.25	4	[53]	[53]
78	11	4	$\mathrm{gon}_{\mathbb{C}}$	[37]	4	[53]	[53]
79	6	4	$\mathrm{gon}_{\mathbb{C}}$	2.1.24	4	[53]	[53]
80	7	4	$\mathrm{gon}_{\mathbb{C}}$	2.1.25	4	[53]	[53]
81	4	3	$\mathrm{gon}_{\mathbb{C}}$	[37]	3	[37]	[37]
82	9	6	2.1.34	2.1.26	[5,6]	[53]	$\mathrm{gon}_{\mathbb{Q}}$

83	5	4	$\mathrm{gon}_{\mathbb{C}}$	2.1.24	4	[53]	[53]
84	11	6	2.1.34	2.1.23	6	2.1.46	$\mathrm{gon}_{\mathbb{Q}}$
85	7	4	$\mathrm{gon}_{\mathbb{C}}$	2.1.20	4	[53]	[53]
86	10	6	2.1.34	2.1.27	6	2.1.46	$\mathrm{gon}_{\mathbb{Q}}$
87	9	4	$\mathrm{gon}_{\mathbb{C}}$	2.1.25	4	[53]	[53]
88	9	4	$\mathrm{gon}_{\mathbb{C}}$	2.1.20	4	[53]	[53]
89	7	4	$\mathrm{gon}_{\mathbb{C}}$	2.1.24	4	[53]	[53]
90	11	6	$\mathrm{gon}_{\mathbb{C}}$	2.1.26	6	2.1.45	$\mathrm{gon}_{\mathbb{Q}}$
91	7	4	$\mathrm{gon}_{\mathbb{C}}$	2.1.25	4	[53]	[53]
92	10	4	$\mathrm{gon}_{\mathbb{C}}$	2.1.24	4	[53]	[53]
93	9	6	2.1.34	2.1.23	6	2.1.46	$\mathrm{gon}_{\mathbb{Q}}$
94	11	4	$\mathrm{gon}_{\mathbb{C}}$	[37]	4	[53]	[53]
95	9	4	$\mathrm{gon}_{\mathbb{C}}$	2.1.24	4	[53]	[53]
96	9	4	$\mathrm{gon}_{\mathbb{C}}$	2.1.26	4	[53]	[53]
97	7	6	2.1.48	2.1.27	5	[53]	2.0.2(v)
98	7	4	$\mathrm{gon}_{\mathbb{C}}$	2.1.25	4	[53]	[53]
99	9	6	2.1.32	2.1.26	4	[53]	[53]
100	7	4	$\mathrm{gon}_{\mathbb{C}}$	2.1.25	4	[53]	[53]
101	8	4	$\mathrm{gon}_{\mathbb{C}}$	2.1.24	4	[53]	[53]
102	15	8	2.1.34	2.1.28	[6,8]	2.1.44	$\mathrm{gon}_{\mathbb{Q}}$
103	8	4	$\mathrm{gon}_{\mathbb{C}}$	2.1.25	4	[53]	[53]
104	11	4	$\mathrm{gon}_{\mathbb{C}}$	[37]	4	[53]	[53]
105	13	6	2.1.40	2.1.29	6	2.1.40	$\mathrm{gon}_{\mathbb{Q}}$
106	12	8	2.1.34	2.1.28	[6,7]	2.1.46	2.0.2(v)
107	9	4	$\mathrm{gon}_{\mathbb{C}}$	2.1.25	4	[53]	[53]
108	10	6	2.1.34	2.1.24	[5,6]	[53]	$\mathrm{gon}_{\mathbb{Q}}$
109	8	5	2.1.34	2.1.21	4	[53]	[53]
110	15	8	2.1.41	2.1.27	6	2.1.41	2.1.27
111	9	4	$\mathrm{gon}_{\mathbb{C}}$	[37]	4	[53]	[53]
112	11	6	2.1.34	2.1.22	[5,6]	[53]	$\mathrm{gon}_{\mathbb{Q}}$
113	9	6	2.1.34	2.1.27	[5,6]	[53]	$\mathrm{gon}_{\mathbb{Q}}$

114	17	8	2.1.34	2.1.28	[6,8]	2.1.19	$\mathrm{gon}_{\mathbb{Q}}$
115	11	6	2.1.34	2.1.23	6	2.1.46	$\mathrm{gon}_{\mathbb{Q}}$
116	13	6	2.1.40	2.1.23	6	2.1.40	$\mathrm{gon}_{\mathbb{Q}}$
117	11	6	2.1.34	2.1.26	[5,6]	[53]	$\mathrm{gon}_{\mathbb{Q}}$
118	14	6	2.1.40	2.1.29	6	2.1.40	$\mathrm{gon}_{\mathbb{Q}}$
119	11	4	$\mathrm{gon}_{\mathbb{C}}$	[37]	4	[53]	[53]
120	17	8	2.1.42	2.1.28	8	2.1.42	$\mathrm{gon}_{\mathbb{Q}}$
121	6	4	$\mathrm{gon}_{\mathbb{C}}$	2.1.25	4	[53]	[53]
122	14	6	2.1.34	2.1.29	[5,6]	[53]	$\mathrm{gon}_{\mathbb{Q}}$
123	13	6	2.1.40	2.1.29	6	2.1.40	$\mathrm{gon}_{\mathbb{Q}}$
124	14	6	2.1.40	2.1.29	6	2.1.40	$\mathrm{gon}_{\mathbb{Q}}$
125	8	4	$\mathrm{gon}_{\mathbb{C}}$	2.1.25	4	[53]	[53]
126	17	8	2.1.42	2.1.28	8	2.1.42	$\mathrm{gon}_{\mathbb{Q}}$
127	10	6	2.1.34	2.1.27	6	2.1.46	$\mathrm{gon}_{\mathbb{Q}}$
128	9	6	2.1.34	2.1.27	6	2.1.46	$\mathrm{gon}_{\mathbb{Q}}$
129	13	6	2.1.34	2.1.23	6	2.1.44	$\mathrm{gon}_{\mathbb{Q}}$
130	17	8	2.1.33	2.1.28	[6,8]	2.1.19	$\mathrm{gon}_{\mathbb{Q}}$
131	11	4	$\mathrm{gon}_{\mathbb{C}}$	[37]	4	[53]	[53]
132	19	8	2.1.34	2.1.26	[6,8]	2.1.19	$\mathrm{gon}_{\mathbb{Q}}$
133	11	8	2.1.48	2.1.27	6	2.1.46	2.1.27
134	16	8	2.1.34	2.1.27	[6,8]	2.1.19	$\mathrm{gon}_{\mathbb{Q}}$
135	13	6	$\mathrm{gon}_{\mathbb{C}}$	2.1.27	6	2.1.19	$\mathrm{gon}_{\mathbb{Q}}$
136	15	8	2.1.34	2.1.26	[5,8]	[53]	$\mathrm{gon}_{\mathbb{Q}}$
137	11	6	2.1.34	2.1.23	6	2.1.46	$\mathrm{gon}_{\mathbb{Q}}$
138	21	8	2.1.42	2.1.28	8	2.1.42	$\mathrm{gon}_{\mathbb{C}}$
139	11	6	2.1.40	2.1.27	6	2.1.40	$\mathrm{gon}_{\mathbb{Q}}$
140	19	8	2.1.34	2.1.26	[6,8]	2.1.19	$\mathrm{gon}_{\mathbb{Q}}$
141	15	6	2.1.40	2.1.27	6	2.1.40	$\mathrm{gon}_{\mathbb{Q}}$
142	17	4	$\mathrm{gon}_{\mathbb{C}}$	[37]	4	[53]	[53]
143	13	4	$\mathrm{gon}_{\mathbb{C}}$	[37]	4	[53]	[53]
144	13	6	2.1.34	2.1.26	[5,6]	[53]	$\mathrm{gon}_{\mathbb{Q}}$

145	13	[7,8]	2.1.48	2.1.27	6	2.1.19	2.1.27
146	17	6	2.1.40	2.1.29	6	2.1.40	$\mathrm{gon}_{\mathbb{Q}}$
147	11	6	2.1.34	2.1.29	[5,6]	[53]	$\mathrm{gon}_{\mathbb{Q}}$
148	17	8	2.1.34	2.1.26	[5,8]	[53]	$\mathrm{gon}_{\mathbb{Q}}$
149	12	6	2.1.40	2.1.27	6	2.1.40	$\mathrm{gon}_{\mathbb{Q}}$
150	19	8	2.1.34	2.1.26	[6,8]	2.1.44	$\mathrm{gon}_{\mathbb{Q}}$
151	12	6	2.1.34	2.1.27	6	2.1.19	$\mathrm{gon}_{\mathbb{Q}}$
152	17	8	2.1.34	2.1.30	[6,8]	2.1.44	$\mathrm{gon}_{\mathbb{Q}}$
153	15	8	2.1.34	2.1.28	[5,8]	[53]	$\mathrm{gon}_{\mathbb{Q}}$
154	21	[8,12]	2.1.34	2.1.26	[5,12]	[53]	$\mathrm{gon}_{\mathbb{Q}}$
155	15	6	$\mathrm{gon}_{\mathbb{C}}$	2.1.23	6	2.1.44	$\mathrm{gon}_{\mathbb{Q}}$
156	23	8	2.1.42	2.1.26	8	2.1.42	$\mathrm{gon}_{\mathbb{Q}}$
157	12	8	2.1.34	2.1.30	[5,7]	[53]	2.0.2(v)
158	19	8	2.1.42	2.1.28	8	2.1.42	$\mathrm{gon}_{\mathbb{Q}}$
159	17	6	$\mathrm{gon}_{\mathbb{C}}$	2.1.23	6	2.1.44	$\mathrm{gon}_{\mathbb{Q}}$
160	17	8	2.1.34	2.1.26	[6,8]	2.1.19	$\mathrm{gon}_{\mathbb{Q}}$
161	15	8	2.1.41	2.1.27	6	2.1.41	2.1.27
162	16	6	2.1.34	2.1.29	[5,6]	[53]	$\mathrm{gon}_{\mathbb{Q}}$
163	13	[7,8]	2.1.34	2.1.30	[5,8]	[53]	$\mathrm{gon}_{\mathbb{Q}}$
164	19	6	2.1.40	2.1.29	6	2.1.40	$\mathrm{gon}_{\mathbb{Q}}$
165	21	8	2.1.42	2.1.28	8	2.1.42	$\mathrm{gon}_{\mathbb{Q}}$
166	20	8	2.1.42	2.1.28	8	2.1.42	$\mathrm{gon}_{\mathbb{Q}}$
167	14	4	[37]	[37]	4	[53]	[53]
168	25	8	2.1.42	2.1.28	8	2.1.42	$\mathrm{gon}_{\mathbb{Q}}$
169	8	6	2.1.34	2.1.27	5	[53]	2.0.2(v)
171	17	8	2.1.42	2.1.28	8	2.1.42	$\mathrm{gon}_{\mathbb{Q}}$
173	14	8	2.1.41	2.1.27	6	2.1.41	2.1.27
175	15	8	2.1.34	2.1.26	[6,8]	2.1.44	$\mathrm{gon}_{\mathbb{Q}}$
176	19	8	2.1.34	2.1.26	[6,8]	2.1.19	$\mathrm{gon}_{\mathbb{Q}}$
177	19	8	2.1.41	2.1.27	6	2.1.41	2.1.27
179	15	6	2.1.34	2.1.27	[5,6]	[53]	$\mathrm{gon}_{\mathbb{Q}}$

181	14	6	2.1.34	2.1.29	[5,6]	[53]	$\mathrm{gon}_{\mathbb{Q}}$
183	19	8	2.1.42	2.1.30	8	2.1.42	$\mathrm{gon}_{\mathbb{Q}}$
184	21	8	2.1.42	2.1.26	8	2.1.42	$\mathrm{gon}_{\mathbb{Q}}$
185	17	8	2.1.42	2.1.30	8	2.1.42	$\mathrm{gon}_{\mathbb{Q}}$
188	22	8	2.1.41	2.1.27	6	2.1.41	2.1.27
190	27	8	2.1.42	2.1.28	8	2.1.42	$\mathrm{gon}_{\mathbb{Q}}$
191	16	4	[37]	[37]	4	[53]	[53]
192	21	8	2.1.34	2.1.26	[6,8]	[37]	$\mathrm{gon}_{\mathbb{Q}}$
195	25	8	2.1.42	2.1.28	8	2.1.42	$\mathrm{gon}_{\mathbb{Q}}$
196	17	8	2.1.34	2.1.26	[6,8]	2.1.19	$\mathrm{gon}_{\mathbb{Q}}$
197	16	8	2.1.42	2.1.30	8	2.1.42	$\mathrm{gon}_{\mathbb{Q}}$
199	16	8	2.1.41	2.1.41	6	2.1.41	$\mathrm{gon}_{\mathbb{Q}}$
200	19	8	2.1.34	2.1.26	[6,8]	2.1.19	$\mathrm{gon}_{\mathbb{Q}}$
203	19	8	2.1.42	2.1.30	8	2.1.42	$\mathrm{gon}_{\mathbb{Q}}$
205	19	8	2.1.42	2.1.28	8	2.1.42	$\mathrm{gon}_{\mathbb{Q}}$
206	25	8	2.1.42	2.1.28	8	2.1.42	$\mathrm{gon}_{\mathbb{Q}}$
209	19	8	2.1.42	2.1.28	8	2.1.42	$\mathrm{gon}_{\mathbb{Q}}$
211	17	8	2.1.34	2.1.30	[6,8]	2.1.44	$\mathrm{gon}_{\mathbb{Q}}$
213	23	8	2.1.42	2.1.28	8	2.1.42	$\mathrm{gon}_{\mathbb{Q}}$
215	21	6	$\mathrm{gon}_{\mathbb{C}}$	2.1.27	6	2.1.19	$\mathrm{gon}_{\mathbb{Q}}$
221	19	8	2.1.42	2.1.28	8	2.1.42	$\mathrm{gon}_{\mathbb{Q}}$
223	18	8	2.1.34	2.1.30	[7,8]	2.1.44	$\mathrm{gon}_{\mathbb{Q}}$
227	19	6	2.1.40	2.1.29	6	2.1.40	$\mathrm{gon}_{\mathbb{Q}}$
239	20	6	2.1.40	2.1.29	6	2.1.40	$\mathrm{gon}_{\mathbb{Q}}$
251	21	8	2.1.41	2.1.27	6	2.1.41	2.1.27
263	22	8	2.1.42	2.1.30	8	2.1.42	$\mathrm{gon}_{\mathbb{Q}}$
269	22	8	2.1.42	2.1.30	8	2.1.42	$\mathrm{gon}_{\mathbb{Q}}$
271	22	10	2.1.43	2.1.43	8	2.1.43	2.1.43
279	29	8	2.1.42	2.1.28	8	2.1.42	$\mathrm{gon}_{\mathbb{Q}}$
284	34	8	2.1.42	2.1.28	8	2.1.42	$\mathrm{gon}_{\mathbb{Q}}$
287	27	8	2.1.42	2.1.28	8	2.1.42	$\mathrm{gon}_{\mathbb{Q}}$

299	27	8	2.1.42	2.1.28	8	2.1.42	$\text{gon}_{\mathbb{Q}}$
311	26	8	2.1.41	2.1.27	6	2.1.41	2.1.27
359	30	8	2.1.42	2.1.30	8	2.1.42	$\text{gon}_{\mathbb{Q}}$

APPENDIX B

This appendix contains the results of Section 2.2. We summarize the results in the following table. For each value of N, we give links to all results used to solve the curves $X_0^{+d}(N)$. We skip the curves of genus at most 3 and in the table we write $g \leq 3$ when we want to say that all curves $X_0^{+d}(N)$ for that level N are of genus $g \leq 3$.

Table B.1: Methods used to find tetragonal curves $X_0^{+d}(N)$.
Levels N eliminated by Equation (2.4) are omitted.

N	Results used	N	Results used
≤ 59	$g \leq 3$	60	$g \leq 3$ for $d = 4, 15, 20$, 2.2.7, [32]
61	$g \leq 3$	62	$g \leq 3$ for $d = 31$, [32]
63	$g \leq 3$	64	$g \leq 3$
65	$g \leq 3$	66	2.2.7, 2.2.11, 2.2.12, [32]
67	[32]	68	$g \leq 3$ for $d = 4$, 2.2.7
69	$g \leq 3$ for $d = 23$, [32]	70	$g \leq 3 (d = 14, 35)$, 2.2.5, 2.2.7, 2.2.10, 2.2.11, [32]
71	$g \leq 3$	72	$g \leq 3$
73	[32]	74	2.2.7, 2.2.12
75	$g \leq 3$	76	$g \leq 3$ for $d = 19$, 2.2.7
77	$g \leq 3$ for $d = 7$, 2.2.7	78	2.2.11, [32]
79	$g \leq 3$	80	$g \leq 3$ for $d = 16$, 2.2.7
81	$g \leq 3$	82	$g \leq 3$ for $d = 41$, 2.2.5, 2.2.7
83	$g \leq 3$	84	2.2.11, 2.2.12
85	2.2.7	86	2.2.10, 2.2.12
87	[32]	88	2.2.7, 2.2.11, 2.2.12

89	$g \leq 3$	90	2.2.5, 2.2.7, 2.2.11
91	$g \leq 3$ for $d = 13$, 2.2.7	92	[32]
93	2.2.7, 2.2.11, 2.2.12	94	[32]
95	[32]	96	$g \leq 3$ for $d = 32$, 2.2.10
97	[38]	98	$g \leq 3$ for $d = 49$, 2.2.7
99	$g \leq 3$ for $d = 11$, 2.2.10	100	$g \leq 3$ for $d = 4$, 2.2.7
101	$g \leq 3$	102	2.2.11, 2.2.17
103	[32]	104	2.2.11
105	2.2.10, 2.2.11	106	2.2.11
107	[32]	108	2.2.5, 2.2.7, 2.2.12
109	[38]	110	2.2.7, 2.2.10, 2.2.11
111	2.2.10	112	2.2.11, 2.2.12, 2.2.15
113	[38]	114	2.2.11, 2.2.17
115	2.2.11, 2.2.12	116	2.2.11, 2.2.12
117	2.2.5, 2.2.7, 2.2.11, [38]	118	2.2.10
119	[32]	120	2.2.11, 2.2.17
121	[32]	122	2.2.11
123	2.2.10	124	2.2.10
125	[32]	126	2.2.11
127	[38]	128	[38]
129	2.2.11, 2.2.12	130	2.2.7, 2.2.11, 2.2.17
131	$g \leq 3$	132	2.2.7, 2.2.7, 2.2.9, 2.2.11, 2.2.17
133	2.2.7, 2.2.11	134	2.2.11
135	2.2.11, 2.2.12	136	2.2.11, 2.2.13
137	2.2.12	138	2.2.9, 2.2.11
139	[38]	140	2.2.7, 2.2.9, 2.2.11, 2.2.17
141	2.2.10	142	2.2.10
143	2.2.10	144	2.2.14
145	2.2.6, 2.2.10	146	2.2.11
147	2.2.11, 2.2.12, [38]	148	2.2.14, 2.2.15 2.2.17
149	[38]	150	2.2.5, 2.2.7, 2.2.9, 2.2.11, 2.2.17

151	[38]	152	2.2.13, 2.2.17
153	2.2.11	154	2.2.5, 2.2.7, 2.2.17
155	2.2.10, 2.2.12	156	2.2.9, 2.2.11
157	2.2.14	158	2.2.11
159	2.2.10, 2.2.12	160	2.2.7, 2.2.15
161	2.2.5, 2.2.11	162	2.2.17
163	2.2.13	164	2.2.7, 2.2.17
165	2.2.7, 2.2.11	166	2.2.11
167	[32]	168	2.2.5, 2.2.7, 2.2.11
169	[38]	170	2.2.5, 2.2.7, 2.2.17
171	2.2.11, 2.2.14	172	2.2.5, 2.2.7, 2.2.17
173	2.2.5	174	2.2.5, 2.2.9, 2.2.17
175	2.2.14, 2.2.17	176	2.2.11, 2.2.14
177	2.2.6, 2.2.11	178	2.2.5, 2.2.9, 2.2.17
179	[38]	180	2.2.5, 2.2.7
181	[38]	182	2.2.5, 2.2.9
183	2.2.9, 2.2.13, 2.2.17	184	2.2.11
185	2.2.7, 2.2.14, 2.2.17	186	2.2.7, 2.2.9
187	2.2.5, 2.2.17	188	2.2.6, 2.2.10
189	2.2.5, 2.2.9, 2.2.17	190	2.2.9, 2.2.11
191	[32]	192	2.2.7, 2.2.15
193	2.2.14	194	2.2.9, 2.2.14
195	2.2.7, 2.2.9, 2.2.11, 2.2.17	196	2.2.5, 2.2.14, 2.2.17
197	2.2.13	198	2.2.5, 2.2.7, 2.2.9
199	2.2.5	200	2.2.7, 2.2.14
201	2.2.5, 2.2.7	202	2.2.5, 2.2.9, 2.2.17
203	2.2.9, 2.2.13, 2.2.17	204	2.2.5, 2.2.7, 2.2.9
205	2.2.11	206	2.2.11
207	2.2.11	208	2.2.5, 2.2.7, 2.2.15
209	2.2.11	210	2.2.7, 2.2.9
211	2.2.13	212	2.2.5, 2.2.7

213	2.2.11	214	2.2.9, 2.2.17
215	2.2.11, 2.2.12	216	2.2.5, 2.2.7
217	2.2.5, 2.2.9, 2.2.15, 2.2.17	218	2.2.5, 2.2.7
219	2.2.5, 2.2.7, 2.2.17	220	2.2.7, 2.2.9
221	2.2.11	222	2.2.9
223	2.2.13	224	2.2.7, 2.2.9, 2.2.15
225	2.2.5, 2.2.7, 2.2.17	226	2.2.5, 2.2.7
227	[38]	228	2.2.5, 2.2.8
229	2.2.15	230	2.2.5, 2.2.9
231	2.2.5, 2.2.9, 2.2.17	232	2.2.5, 2.2.7
233	2.2.5, 2.2.17	234	2.2.5, 2.2.7, 2.2.9
235	2.2.5, 2.2.7	236	2.2.9
237	2.2.5, 2.2.7	238	2.2.9, 2.2.17
239	[38]	240	2.2.5, 2.2.7, 2.2.8
241	2.2.15	242	2.2.5, 2.2.7, 2.2.17
243	2.2.5, 2.2.18	244	2.2.5, 2.2.7
245	2.2.5, 2.2.9, 2.2.17	246	2.2.8, 2.2.9
247	2.2.5, 2.2.7, 2.2.17	248	2.2.9, 2.2.17
249	2.2.9, 2.2.17	250	2.2.5, 2.2.7, 2.2.9
251	2.2.5	252	2.2.7, 2.2.9
253	2.2.5, 2.2.7	254	2.2.7, 2.2.9
255	2.4	256	2.2.5, 2.2.17
257	2.2.15	258	2.2.7, 2.2.9
259	2.2.5, 2.2.7, 2.2.9, 2.2.17	260	2.4
261	2.2.5, 2.2.7, 2.2.9	262	2.2.9, 2.2.17
263	2.2.14	264	2.2.8
265	2.2.5, 2.2.7	266	2.4
267	2.2.9, 2.2.17	268	2.2.3, 2.2.7
269	2.2.13	270	2.2.8, 2.2.9
271	2.2.5, 2.0.2(v)	272	2.2.3, 2.2.7, 2.2.9
273	2.2.3, 2.2.7, 2.2.8	274	2.2.3, 2.2.7, 2.2.9

275	2.2.5, 2.2.7, 2.2.9, 2.2.17	276	2.4
277	2.2.5	278	2.2.7, 2.2.9
279	2.2.11	280	2.4
281	2.2.15	282	2.4
283	2.2.5, 2.2.17	284	2.2.11
285	2.4	286	2.4
287	2.2.11	288	2.2.3, 2.2.7
289	2.2.5, 2.2.17	290	2.4
291	2.2.3, 2.2.7, 2.2.9	292	2.4
293	2.2.5, 2.2.17	294	2.4
295	2.2.9, 2.2.17	296	2.4
297	2.2.3, 2.2.7, 2.2.9	298	2.2.3, 2.2.7, 2.2.9
299	2.2.11	300	2.2.8, 2.2.9
301	2.2.3, 2.2.7	302	2.2.7, 2.2.9
303	2.2.9	304	2.4
305	2.2.3, 2.2.9	307	2.2.5
309	2.2.3, 2.2.8	311	2.2.5
313	2.2.5	317	2.2.5
319	2.2.5, 2.2.9	321	2.2.9
323	2.2.3, 2.2.7, 2.2.9	325	2.2.3, 2.2.7
329	2.2.9	331	2.2.5
335	2.2.5, 2.2.9	337	2.2.5
341	2.2.3, 2.2.9	343	2.2.3
347	2.2.3	349	2.2.3
353	2.2.3	355	2.2.3, 2.2.7, 2.2.9
359	2.2.13	361	2.2.3
367	2.2.3	371	2.2.3, 2.2.9
373	2.2.3	377	2.2.3, 2.2.9
379	2.2.3	383	2.2.5
389	2.2.3	391	2.2.3, 2.2.9
397	2.2.3	401	2.2.3

409	2.2.3	419	2.2.3
420	2.2.4	421	2.2.3
431	2.2.5, 2.2.17	433	2.2.3
439	2.2.3	443	2.2.3
449	2.2.3		

APPENDIX C

This appendix contains the results of Section 2.3. For each level N, there are 7 entries, listed in the order they appear in: the structure of the group $(\mathbb{Z}/N\mathbb{Z})^\times$ along with its generators, the group Δ, the genus g of $X_\Delta(N)$, the $\mathbb{Q}$-gonality of $X_\Delta(N)$, the $\mathbb{C}$-gonality of $X_\Delta(N)$ (if determined), and all results used to obtain the gonalities.

We only list the curves $X_\Delta(N)$ with genus $g \geq 3$. Some information about the genera of curves $X_\Delta(N)$ was taken from [52, Table 6]. Some groups Δ have been omitted from the table, especially for bigger N when there are many groups Δ, since we can use Proposition 2.0.2(vii) for them to prove that they are neither $\mathbb{C}$-tetragonal nor $\mathbb{Q}$-pentagonal. For non-tetragonal curves with genus $g \geq 10$ we also omit their $\mathbb{C}$-gonality if the bound $\mathrm{gon}_{\mathbb{C}} \geq 5$ can be deduced from Corollary 2.1.17.

Table C.1: The $\mathbb{Q}$-gonalities of curves $X_\Delta(N)$ for $N \leq 40$.

N	$(\mathbb{Z}/N\mathbb{Z})^\times$	generators	Δ	g	$\mathrm{gon}_{\mathbb{Q}}$	$\mathrm{gon}_{\mathbb{C}}$	results used
21	$C_2 \times C_6$	$-1, 2$	$\{\pm 1, \pm 8\}$	3	2	2	[43], [49]
24	$C_2 \times C_2 \times C_2$	$-1, 5, 7$	$\{\pm 1, \pm 5\}$	3	3	3	$g = 3$, 2.0.2(iv)
			$\{\pm 1, \pm 7\}$	3	3	3	$g = 3$, 2.0.2(iv)
25	C_{20}	2	$\{\pm 1, \pm 7\}$	4	4	3	2.3.1
26	C_{12}	7	$\{\pm 1, \pm 5\}$	4	3	3	2.3.1
			$\{\pm 1, \pm 3, \pm 9\}$	4	3	3	2.3.1
28	$C_2 \times C_6$	$3, 13$	$\{\pm 1, \pm 13\}$	4	3	3	2.3.1
			$\{\pm 1, \pm 3, \pm 9\}$	4	3	3	2.3.1
29	C_{28}	2	$\{\pm 1, \pm 12\}$	8	6	5	2.3.11, 2.3.17, 2.3.21

			$\langle -1,4\rangle$	4	3	3	2.3.1
30	$C_2\times C_4$	$7,11$	$\{\pm1,\pm11\}$	5	4	4	2.3.15
31	C_{30}	3	$\{\pm1,\pm5,\pm6\}$	6	5	4	2.3.10, 2.3.17, 2.3.20
			$\{\pm1,\pm2,\pm4,\pm8,\pm15\}$	6	5	4	2.3.10, 2.3.17, 2.3.20
32	$C_2\times C_8$	$-1,3$	$\{\pm1,\pm15\}$	5	4	4	2.3.15
33	$C_2\times C_{10}$	$2,10$	$\{\pm1,\pm10\}$	11	6	≥ 5	2.3.11, 2.3.17, 2.1.17
			$\{\pm1,\pm2,\pm4,\pm8,\pm16\}$	5	4	4	2.3.15
34	C_{16}	3	$\{\pm1,\pm13\}$	9	6	≥ 5	2.3.11, 2.3.17, 2.3.21
			$\{\pm1,\pm9,\pm13,\pm15\}$	5	4	4	2.3.15
35	$C_2\times C_{12}$	$-1,2$	$\{\pm1,\pm6\}$	13	8	≥ 5	2.3.12, 2.3.18, 2.1.17
			$\{\pm1,\pm11,\pm16\}$	9	6	≥ 5	2.3.11, 2.3.17 2.3.21
			$\{\pm1,\pm6,\pm8,\pm13\}$	7	4	4	2.3.17
			$\langle -1,4\rangle$	5	4	4	2.3.15
36	$C_2\times C_6$	$5,19$	$\{\pm1,\pm17\}$	7	4	4	2.3.18
			$\{\pm1,\pm11,\pm13\}$	3	3	3	$g=3$, 2.0.2(iv)
37	C_{36}	2	$\{\pm1,\pm6\}$	16	9	≥ 5	2.3.12, 2.3.18
			$\{\pm1,\pm10,\pm11\}$	10	6	≥ 5	2.3.11, 2.3.17, 2.1.17
			$\langle -1,8\rangle$	4	3	3	2.3.1
			$\langle -1,4\rangle$	4	3	3	2.3.1
38	C_{18}	3	$\{\pm1,\pm7,\pm11\}$	10	6	≥ 5	2.3.11, 2.3.18, 2.1.17
39	$C_2\times C_{12}$	$-1,2$	$\{\pm1,\pm14\}$	17	8	≥ 5	2.3.12, 2.3.18, 2.1.17
			$\{\pm1,\pm16,\pm17\}$	9	6	≥ 5	2.3.11, 2.3.17, 2.3.21
			$\{\pm1,\pm5,\pm8,\pm14\}$	9	4	4	2.3.18
			$\langle -1,4\rangle$	5	4	4	2.3.15
40	$C_2\times C_2\times C_4$	$-1,3,11$	$\{\pm1,\pm9\}$	13	8	≥ 5	2.3.12, 2.3.18, 2.1.17
			$\{\pm1,\pm11\}$	13	7	≥ 5	2.3.12, 2.3.17, 2.1.17
			$\{\pm1,\pm19\}$	9	6	≥ 5	2.3.11, 2.3.18, 2.3.21
			$\{\pm1,\pm3,\pm9,\pm13\}$	7	4	4	2.3.18
			$\{\pm1,\pm7,\pm9,\pm17\}$	7	4	4	2.3.18
			$\{\pm1,\pm9,\pm11,\pm19\}$	5	4	4	2.3.15
41	C_{40}	6	$\{\pm1,\pm9\}$	21	≥ 6		2.0.2(vii)

			$\{\pm1,\pm3,\pm9,\pm14\}$	11	≥ 6		2.3.11, 2.1.17
			$\{\pm1,\pm4,\pm10,\pm16,\pm18\}$	11	≥ 6		2.3.11, 2.1.17
			$\langle -1,5\rangle$	5	4	4	2.3.15
42	$C_2\times C_6$	$5,13$	$\{\pm1,\pm13\}$	13	≥ 6		2.3.11
			$\{\pm1,\pm5,\pm17\}$	9	≥ 6	≥ 5	2.3.11, 2.3.21
43	C_{42}	3	$\{\pm1,\pm6,\pm7\}$	15	≥ 6		2.3.11
			$\langle -1,27\rangle$	9	≥ 6	≥ 5	2.3.11, 2.3.21
44	$C_2\times C_{10}$	$-1,3$	$\{\pm1,\pm21\}$	16	≥ 6		2.3.11
			$\{\pm1,\pm5,\pm7,\pm9,\pm19\}$	8	5	5	2.3.17, 2.3.21
45	$C_2\times C_{12}$	$-1,2$	$\{\pm1,\pm19\}$	21	≥ 6		2.0.2(vii)
			$\{\pm1,\pm14,\pm16\}$	9	≥ 6	≥ 5	2.3.11, 2.3.21
			$\{\pm1,\pm8,\pm17,\pm19\}$	11	≥ 6		2.3.11
			$\langle -1,4\rangle$	5	4	4	2.3.15
48	$C_2\times C_2\times C_4$	$-1,5,7$	$\{\pm1,\pm7\}$	19	≥ 6	≥ 6	2.3.14
			$\{\pm1,\pm17\}$	19	≥ 6	≥ 6	2.3.14
			$\{\pm1,\pm23\}$	13	≥ 6		2.3.11
			$\{\pm1,\pm5,\pm19,\pm23\}$	7	4	4	2.3.18
			$\{\pm1,\pm7,\pm17,\pm23\}$	7	4	4	2.3.18
			$\{\pm1,\pm11,\pm13,\pm23\}$	5	4	4	2.3.15
49	C_{42}	3	$\{\pm1,\pm18,\pm19\}$	19	≥ 6		2.3.11
			$\langle -1,27\rangle$	3	3	3	$g=3$, 2.0.2(iv)
50	C_{20}	3	$\{\pm1,\pm7\}$	22	≥ 6	≥ 6	2.3.14
			$\{\pm1,\pm9,\pm11,\pm19,\pm21\}$	4	3	3	2.3.1
51	$C_2\times C_{16}$	$-1,3$	$\{\pm1,\pm16\}$	33	≥ 6		2.0.2(vii)
			$\{\pm1,\pm4,\pm13,\pm16\}$	17	≥ 6		2.0.2(vii)
			$\langle -1,9\rangle$	9	≥ 6	≥ 5	2.3.11, 2.3.21
52	$C_2\times C_{12}$	$-1,7$	$\langle -1,7^3\rangle$	13	≥ 6		2.3.11
			$\langle -1,3\rangle$	9	≥ 6	≥ 5	2.3.11, 2.3.21
			other				2.0.2(vii)
53	C_{52}	2	$\{\pm1,\pm23\}$	40	≥ 6		2.3.19

			$\langle -1,4\rangle$	8	≥ 6	≥ 5	2.3.11, 2.3.21
54	C_{18}	5	$\{\pm 1,\pm 17,\pm 19\}$	10	≥ 6		2.3.11
55	$C_2 \times C_{20}$	2, 21	$\{\pm 1,\pm 21\}$	41	≥ 6		2.0.2(vii)
			$\{\pm 1,\pm 12,\pm 21,\pm 23\}$	21	≥ 6		2.3.11
			$\{\pm 1,\pm 16,\pm 19,\pm 24,\pm 26\}$	17	≥ 6		2.3.11
			$\langle -1,4,21\rangle$	9	4	4	2.3.17
56	$C_2 \times C_2 \times C_6$	3, 13, 29	$\{\pm 1,\pm 13,\pm 15,\pm 27\}$	13	≥ 6		2.3.11
			$\langle -1,9,13\rangle$	11	≥ 6		2.3.11
			$\langle -1,9,15\rangle$	11	≥ 6		2.3.11
			$\langle -1,3\rangle$	9	≥ 6	≥ 5	2.3.11, 2.3.21
			other				2.0.2(vii)
57	$C_2 \times C_{18}$	2, 20	$\langle -1,8,20\rangle$	13	≥ 6		2.3.11
			$\langle -1,2\rangle$	9	≥ 6	≥ 5	2.3.11, 2.3.21
			other				2.0.2(vii)
58	C_{28}	3	$\langle -1,3^7\rangle$		≥ 6	≥ 6	2.3.19
			$\langle -1,9\rangle$	12	≥ 6		2.3.11
60	$C_2 \times C_2 \times C_4$	7, 11, 19	$\{\pm 1,\pm 7,\pm 11,\pm 17\}$	15	≥ 6		2.3.11
			$\{\pm 1,\pm 11,\pm 13,\pm 23\}$	15	≥ 6		2.3.11
			$\{\pm 1,\pm 11,\pm 19,\pm 29\}$	13	≥ 6		2.3.11
			other				2.0.2(vii)
61	C_{60}	2	$\langle -1,2^5\rangle$	16	≥ 6		2.3.11
			$\langle -1,8\rangle$	12	≥ 6		2.3.11
			$\langle -1,4\rangle$	8	≥ 6	≥ 5	2.3.11, 2.3.21
			other				2.0.2(vii)
62	C_{30}	3	$\{\pm 1,\pm 5,\pm 25\}$	31	≥ 6	≥ 6	2.3.14
			$\{\pm 1,\pm 15,\pm 23,\pm 27,\pm 29\}$	19	≥ 6		2.3.11
63	$C_6 \times C_6$	2, 5	$\langle -1,2\rangle$	17	≥ 6		2.3.11
			$\langle -1,5\rangle$	17	≥ 6		2.3.11
			$\langle -1,8,10\rangle$	17	≥ 6		2.3.11
			$\langle -1,8,20\rangle$	13	≥ 6		2.3.11
			$\langle -1,4,5\rangle$	9	≥ 6	≥ 5	2.3.11, 2.3.21

			other				2.0.2(vii)
64	$C_2 \times C_{16}$	$-1,3$	$\{\pm 1, \pm 31\}$	37	≥ 6		2.0.2(vii)
			$\{\pm 1, \pm 15, \pm 17, \pm 31\}$	13	≥ 6		2.3.11
			$\langle -1, 9 \rangle$	5	4	4	2.3.15
65	$C_4 \times C_{12}$	$2,12$	$\langle -1, 8, 12 \rangle$	13	≥ 6		2.3.11
			$\langle -1, 4, 12 \rangle$	11	≥ 6		2.3.11
			$\langle -1, 4, 24 \rangle$	11	≥ 6		2.3.11
			$\langle -1, 2 \rangle$	9	≥ 6	≥ 5	2.3.11, 2.3.21
			other				2.0.2(vii)
66	$C_2 \times C_{10}$	$-1,5$	$\langle -1, 25 \rangle$	17	≥ 6		2.3.11
			$\langle -1, 5^5 \rangle$		≥ 6	≥ 6	2.3.19
67	C_{66}	2	$\langle -1, 2^{11} \rangle$		≥ 6	≥ 6	2.3.19
			$\langle -1, 8 \rangle$	15	≥ 6		2.3.11
68	$C_2 \times C_{16}$	$-1,3$	$\langle -1, 9 \rangle$	13	≥ 6		2.3.11
69	$C_2 \times C_{22}$	$-1,2$	$\{\pm 1, \pm 22\}$	67	≥ 6	≥ 6	2.3.19
			$\langle -1, 4 \rangle$	13	≥ 6		2.3.11
70	$C_2 \times C_{12}$	$-1,3$	$\langle -1, 27 \rangle$	25	≥ 6		2.3.11
			$\langle -1, 9 \rangle$	17	≥ 6		2.3.11
			other				2.0.2(vii)
71	C_{70}	7	$\{\pm 1, \pm 5 \pm 14, \pm 17, \pm 25\}$	36	≥ 6		2.3.9
			$\langle -1, 7^5 \rangle$	26	≥ 6		2.3.11
72	$C_2 \times C_2 \times C_6$	$-1,5,17$	$\{\pm 1, \pm 17, \pm 19, \pm 35\}$	21	≥ 6	≥ 6	2.3.14
			$\langle -1, 5 \rangle$	13	≥ 6		2.3.11
			$\langle -1, 17, 25 \rangle$	13	≥ 6		2.3.11
			$\langle -1, 13, 25 \rangle$	9	≥ 6	≥ 5	2.3.11, 2.3.21
			other				2.0.2(vii)
73	C_{72}	5	$\langle -1, 5^3 \rangle$	13	≥ 6		2.3.11
			$\langle -1, 25 \rangle$	9	≥ 6	≥ 5	2.3.11, 2.3.21
			other				2.0.2(vii)
74	C_{36}	5	$\langle -1, 5^3 \rangle$	22	≥ 6	≥ 6	2.3.14
			$\langle -1, 25 \rangle$	16	≥ 6		2.3.11

			other				2.0.2(vii)
75	$C_2 \times C_{20}$	$-1,2$	$\{\pm1,\pm26\}$	73	≥ 6		2.0.2(vii)
			$\{\pm1,\pm7,\pm26,\pm32\}$	37	≥ 6	≥ 6	2.3.19
			$\{\pm1,\pm14,\pm16,\pm29,\pm31\}$	17	≥ 6		2.3.11
			$\langle -1,4\rangle$	9	4	4	2.3.18
77	$C_2 \times C_{30}$	$-1,2$	$\langle -1,32\rangle$	31	≥ 6		2.3.11
			$\langle -1,8\rangle$	19	≥ 6		2.3.11
			$\langle -1,4\rangle$	13	≥ 6		2.3.11
			other				2.0.2(vii)
78	$C_2 \times C_{12}$	$5,7$	$\langle -1,5,7^3\rangle$	31	≥ 6		2.3.9
			$\langle -1,35,49\rangle$	31	≥ 6		2.3.11
			other				2.0.2(vii)
79	C_{78}	3	$\{\pm1,\pm23,\pm24\}$	66	≥ 6	≥ 6	2.3.19
			$\langle -1,27\rangle$	18	≥ 6		2.3.11
80	$C_2 \times C_4 \times C_4$	$-1,3,7$	$\langle -1,7,9\rangle$	15	≥ 6		2.3.11
			$\langle -1,3,49\rangle$	15	≥ 6		2.3.11
			$\langle -1,21,49\rangle$	13	≥ 6		2.3.11
			other				2.0.2(vii)
81	C_{54}	2	$\{\pm1,\pm26,\pm28\}$	46			2.0.2(vii)
			$\langle -1,8\rangle$	10	≥ 6		2.3.11
85	$C_4 \times C_{16}$	$3,13$	$\langle -1,3\rangle$	15	≥ 6		2.3.11
			$\langle -1,9,13\rangle$	13	≥ 6		2.3.11
			other				2.0.2(vii)
87	$C_2 \times C_{28}$	$-1,2$	$\langle -1,2^7\rangle$		≥ 6	≥ 6	2.3.19
			$\langle -1,4\rangle$	17	≥ 6		2.3.11
88	$C_2 \times C_2 \times C_{10}$	$-1,5,21$	$\langle -1,21,5^5\rangle$	41	≥ 6	≥ 6	2.3.19
			$\langle -1,21,25\rangle$	19	≥ 6		2.3.9
			$\langle -1,25,105\rangle$	19	≥ 6		2.3.11
			$\langle -1,5\rangle$	17	≥ 6		2.3.11
			other				2.0.2(vii)
89	C_{88}	3	$\{\pm1,\pm34\}$	133	≥ 6		2.0.2(vii)

			$\{\pm1,\pm12,\pm34,\pm37\}$	67	≥ 6	≥ 6	2.3.19
			$\langle -1,3^4\rangle$	27	≥ 6		2.0.2(vii)
			$\langle -1,9\rangle$	13	≥ 6		2.3.11
91	$C_6\times C_{12}$	$2,12$	$\langle -1,8,12\rangle$	23	≥ 6		2.3.11
			$\langle -1,8,48\rangle$	23	≥ 6		2.3.11
			$\langle -1,8,24\rangle$	21	≥ 6		2.3.11
			$\langle -1,2\rangle$	21	≥ 6		2.3.9
			$\langle -1,4,12\rangle$	13	≥ 6		2.3.11
			other				2.0.2(vii)
92	$C_2\times C_{22}$	$-1,3$	$\{\pm1,\pm45\}$	100	≥ 6	≥ 6	2.3.19
			$\langle -1,9\rangle$	20	≥ 6		2.3.11
95	$C_2\times C_{36}$	$-1,2$	$\langle -1,8\rangle$	25	≥ 6		2.3.11
			$\langle -1,4\rangle$	17	≥ 6		2.3.11
			other				2.0.2(vii)
96	$C_2\times C_2\times C_8$	$-1,5,17$	$\langle -1,17,25\rangle$	17	≥ 6		2.3.11
			$\langle -1,25,85\rangle$	17	≥ 6		2.3.11
			$\langle -1,5\rangle$	17	≥ 6		2.3.9
			other				2.0.2(vii)
98	C_{42}	3	$\langle -1,3^7\rangle$		≥ 6	≥ 6	2.3.19
			$\langle -1,27\rangle$	19	≥ 6	≥ 6	2.3.14
100	$C_2\times C_{20}$	$-1,3$	$\langle -1,3^5\rangle$		≥ 6	≥ 6	2.3.19
			$\langle -1,9\rangle$	12	≥ 6		2.3.11
101	C_{100}	2	$\langle -1,32\rangle$	36	≥ 6	≥ 6	2.3.19
			$\langle -1,4\rangle$	16	≥ 6		2.3.11
			other				2.0.2(vii)
103	C_{102}	5	$\langle 5^{17}\rangle$		≥ 6	≥ 6	2.3.19
			$\langle -1,5^3\rangle$	24	≥ 6		2.3.11
			other				2.0.2(vii)
104	$C_2\times C_2\times C_{12}$	$-1,15,51$	$\langle -1,15^3,51\rangle$	31	≥ 6		2.3.9
			$\langle -1,15\rangle$	23	≥ 6		2.3.11
			$\langle -1,15^2,15\cdot 51\rangle$	23	≥ 6		2.3.11

			$\langle -1, 15^2, 51 \rangle$	21	≥ 6		2.3.9
			other				2.0.2(vii)
109	C_{108}	6	$\langle -1, 6^3 \rangle$	22	≥ 6		2.3.11
			$\langle -1, 36 \rangle$	16	≥ 6		2.3.11
			other				2.0.2(vii)
111	$C_2 \times C_{36}$	$-1, 2$	$\langle -1, 8 \rangle$	31	≥ 6		2.3.11
			$\langle -1, 4 \rangle$	21	≥ 6		2.3.11
			other				2.0.2(vii)
119	$C_2 \cdot C_{48}$	$-1, 3$	$\langle -1, 27 \rangle$	31	≥ 6		2.3.11
			$\langle -1, 9 \rangle$	21	≥ 6		2.3.11
			other				2.0.2(vii)
121	C_{110}	2	$\langle -1, 2^{11} \rangle$		≥ 6	≥ 6	2.3.19
			$\langle -1, 32 \rangle$		≥ 6	≥ 6	2.3.19
125	C_{100}	2	$\langle -1, 32 \rangle$		≥ 6	≥ 6	2.3.19
			$\langle -1, 4 \rangle$	16	5	5	2.3.11, 2.3.18
			other				2.0.2(vii)
131	C_{130}	2	all Δ		≥ 6	≥ 6	2.3.19
142	C_{70}	7	all Δ		≥ 6	≥ 6	2.3.19
143	$C_2 \times C_{60}$	$-1, 2$	$\langle -1, 32 \rangle$		≥ 6	≥ 6	2.3.19
			$\langle -1, 8 \rangle$	37	≥ 6		2.3.9
			$\langle -1, 4 \rangle$	25	≥ 6		2.3.11
			other				2.0.2(vii)
191	C_{190}	19	all Δ		≥ 6	≥ 6	2.3.19

APPENDIX D

Table D.1: Levels N and strong Weil curves E (given by their LMFDB labels) considered in the proof of Theorem 3.0.11.

N	E	Modular Degree	Quadratic Form
106	53.a1	2	$6x^2-4xy+6y^2$
114	57.a1	4	$12x^2-16xy+12y^2$
116	58.a1	4	$8x^2-8xy+8y^2$
122	61.a1	2	$6x^2-4xy+6y^2$
129	43.a1	2	$8x^2-8xy+8y^2$
130	65.a1	2	$6x^2-4xy+6y^2$
148	37.a1	2	$12x^2+12y^2+12z^2-16xy+4xz-16yz$
158	79.a1	2	$6x^2-4xy+6y^2$
164	82.a1	4	$8x^2-8xy+8y^2$
166	83.a1	2	$6x^2-4xy+6y^2$
171	57.a1	4	$12x^2-8xy+12y^2$
172	43.a1	2	$12x^2+12y^2+12z^2-16xy+4xz-16yz$
176	88.a1	8	$16x^2+16y^2$
178	89.a1	2	$6x^2-4xy+6y^2$
182	91.a1	4	$12x^2-16xy+12y^2$
	91.b2	4	$12x^2+12y^2$
183	61.a1	2	$8x^2-8xy+8y^2$
184	92.a1	6	$12x^2+12y^2$

185	37.a1	2	$12x^2 - 8xy + 12y^2$
195	65.a1	2	$8x^2 - 8xy + 8y^2$
215	43.a1	2	$12x^2 - 16xy + 12y^2$
237	79.a1	2	$8x^2 - 4xy + 8y^2$
242	121.b2	4	$12x^2 + 12y^2$
249	83.a1	2	$8x^2 - 4xy + 8y^2$
259	37.a1	2	$16x^2 - 4xy + 16y^2$
264	88.a1	8	$32x^2 - 48xy + 32y^2$
265	53.a1	2	$12x^2 + 12y^2$
267	89.a1	2	$8x^2 - 4xy + 8y^2$
297	99.a2	4	$12x^2 + 12y^2$

CONCLUSION

In this thesis we have two main chapters, one about the gonality of modular curves, the second about the modular curves with infinitely many degree d points. These are Chapter 2 and Chapter 3, respectively. Here we will give an overview of the main results in those chapters.

In Section 2.1 we determined the $\mathbb{Q}$ and $\mathbb{C}$-gonality of the modular curve $X_0(N)$. The results are given in Table A.1. We determined the $\mathbb{Q}$-gonality of the curve $X_0(N)$ for all $N \leq 144$. Also, we determined all curves $X_0(N)$ with $\mathbb{Q}$-gonality equal to d for $d = 4,5,6$ in Theorems 2.1.2, 2.1.3, 2.1.4. Interestingly, there exists only one curve $X_0(N)$ with $\mathbb{Q}$-gonality equal to 5, namely $X_0(109)$. We used a variety of methods to obtain these results and computations in `Magma` computer algebra system were of great help to us.

In Section 2.2 we computed the $\mathbb{Q}$ and $\mathbb{C}$-gonality of quotient curves $X_0^{+d}(N)$. The results are given in Table B.1. In Theorem 2.2.2 we determined all $\mathbb{Q}$-tetragonal curves $X_0^{+d}(N)$ as well as all $\mathbb{C}$-tetragonal curves $X_0^{+d}(N)$. As a consequence of these results, we were able to compute the $\mathbb{Q}$-gonality of the curve $X_0(N)$ for several new levels N in Corollary 2.2.19.

In Section 2.3 we computed the $\mathbb{Q}$ and $\mathbb{C}$-gonality of intermediate modular curves $X_\Delta(N)$. The results are given in Table C.1. In Theorems 2.3.1, 2.3.3, 2.3.4, 2.3.5 we determined all curves $X_\Delta(N)$ with $\mathbb{Q}$-gonality equal to d for $d = 4,5$ as well as all curves $X_\Delta(N)$ with $\mathbb{C}$-gonality equal to 4.

In Chapter 3 we studied the problem of determining the existence of infinitely many degree d points on a curve. Our results mostly deal with the modular curve $X_0(N)$. In Theorem 3.0.7 we determine all curves $X_0(N)$ with infinitely many quartic points. To prove this result, we used results about the $\mathbb{Q}$-gonality from Section 2.1. A big part of the proof was finding all curves $X_0(N)$ that admit a degree 4 rational morphism to

a positive rank elliptic curve $E/\mathbb{Q}$. This was solved in Theorem 3.0.11 by finding a quadratic form that represents all possible degrees of such morphisms. We used the Sage computer algebra system to prove that these quadratic forms (listed in Table D.1) represent all possible degrees of morphisms.

BIBLIOGRAPHY

[1] D. Abramovich. A linear lower bound on the gonality of modular curves. *Internat. Math. Res. Notices*, 1996(20):1005–1011, 1996. ↑ 28, 57.

[2] D. Abramovich and J. Harris. Abelian varieties and curves in $W_d(C)$. *Compos. Math.*, 78(2):227–238, 1991. ↑ 58, 99, 100.

[3] N. Adžaga, T. Keller, P. Michaud-Jacobs, F. Najman, E. Ozman, and B. Vukorepa. Computing quadratic points on modular curves $X_0(N)$. *Math. Comp.*, 93:1371–1397, 2024. ↑ 32.

[4] S. Anni, E. Assaf, and E. Lorenzo García. On smooth plane models for modular curves of shimura type. *Res. Number Theory*, 9(2), 2023. ↑ 83.

[5] D. Babbage. A note on the quadrics through a canonical curve. *J. London Math. Soc.*, 14, 1939. ↑ 82.

[6] F. Bars. Bielliptic modular curves. *J. Number Theory*, 76(1):154–165, 1999. ↑ iv, vi, 29, 40, 101.

[7] F. Bars and T. Dalal. Infinitely many cubic points for $X_0^+(N)$ over $\mathbb{Q}$. *Acta Arith.*, 206(4):373–388, 2022. ↑ 48.

[8] F. Bars, J. González, and M. Kamel. Bielliptic quotient modular curves with N square-free. *J. Number Theory*, 216:380–402, 2020. ↑ 58.

[9] F. Bars, M. Kamel, and A. Schweizer. Bielliptic quotient modular curves of $X_0(N)$. *Math. Comp.*, 92(340):895–929, 2022. ↑ 58, 102.

[10] C. Birkenhake and H. Lange. *Complex Abelian Varieties*. Springer Berlin Heidelberg, 2004. ↑ 118.

[11] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I: The user language. *J. Symb. Comput.*, 24(3-4):235–265, 1997. ↑ iv, vi, 32, 81.

[12] A. Bourdon, Ö. Ejder, Y. Liu, F. Odumodu, and B. Viray. On the level of modular curves that give rise to isolated j-invariants. *Adv. Math.*, 357:106824, 33, 2019. ↑ 100, 126.

[13] J. Box. Quadratic points on modular curves with infinite Mordell-Weil group. *Math. Comp.*, 90(327):321–343, 2021. ↑ 73.

[14] P. L. Clark, M. Milosevic, and P. Pollack. Typically bounding torsion. *J. Number Theory*, 192:150–167, 2018. ↑ 20, 21.

[15] M. Coppens and G. Martens. Secant spaces and Clifford's theorem. *Compos. Math.*, 78(2):193–212, 1991. ↑ 35.

[16] J. Cremona. Elliptic curve data. `http://homepages.warwick.ac.uk/staff/J.E.Cremona/ftp/data/INDEX.html`, 2020. ↑ 128.

[17] O. Debarre and R. Fahlaoui. Abelian varieties in $W_d^r(C)$ and points of bounded degree on algebraic curves. *Compositio Math.*, 88(3):235–249, 1993. ↑ 100.

[18] M. Derickx, A. Etropolski, M. van Hoeij, J. S. Morrow, and D. Zureick-Brown. Sporadic cubic torsion. *Algebra Number Theory*, 15(7):1837–1864, 2021. ↑ 3, 53, 54, 55.

[19] M. Derickx and F. Najman. Classification of torsion of elliptic curves over quartic fields, 2024. preprint. available at: `https://arxiv.org/abs/2412.16016`. ↑ 3.

[20] M. Derickx and F. Najman. Hyperelliptic and trigonal modular curves in characteristic p. *Q. J. Math.*, 00:1–18, 2024. ↑ 79.

[21] M. Derickx and P. Orlić. Modular curves $X_0(N)$ with infinitely many quartic points. *Res. Number Theory*, 10(42), 2024. ↑ iv, vi.

[22] M. Derickx and A. V. Sutherland. Torsion subgroups of elliptic curves over quintic and sextic number fields. *Proc. Am. Math. Soc.*, 145(10):4233–4245, 2017. ↑ 29, 101.

[23] M. Derickx and M. van Hoeij. Gonality of the modular curve $X_1(N)$. *J. Algebra*, 417:52–71, 2014. ↑ iv, vi, 30, 31, 79, 84, 94, 101.

[24] F. Diamond and J. Im. Modular forms and modular curves. *Conference proceedings, Can. Math. Soc.*, 17, 1995. ↑ 14, 109, 110.

[25] F. Diamond and J. Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005. ↑ 12, 22, 23, 24, 120.

[26] D. Eisenbud. *The Geometry of Syzygies: A Second Course in Algebraic Geometry and Commutative Algebra*. Graduate Texts in Mathematics. Springer, 2005. ↑ 82.

[27] N. D. Elkies. On elliptic K-curves. In *Modular curves and Abelian varieties. Based on lectures of the conference, Bellaterra, Barcelona, July 15–18, 2002*, pages 81–91. Basel: Birkhäuser, 2004. ↑ 58.

[28] G. Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983. ↑ 99.

[29] U. Fincke and M. Pohst. Improved methods for calculating vectors of short length in a lattice, including a complexity analysis. *Math. Comp.*, 44(170):463–471, 1985. ↑ 132.

[30] N. Freitas, B. V. Le Hung, and S. Siksek. Elliptic curves over real quadratic fields are modular. *Invent. math.*, 201(1):159–206, 2014. ↑ 25.

[31] G. Frey. Curves with infinitely many points of fixed degree. *Israel J. Math.*, 85(1-3):79–83, 1994. ↑ 100, 129.

[32] M. Furumoto and Y. Hasegawa. Hyperelliptic Quotients of Modular Curves $X_0(N)$. *Tokyo J. Math.*, 22(1):105 – 125, 1999. ↑ iii, vi, 43, 58, 70, 71, 76, 145, 146, 147.

[33] M. L. Green. Koszul cohomology and the geometry of projective varieties. Appendix: The nonvanishing of certain Koszul cohomology groups (by Mark Green and Robert Lazarsfeld). *J. Differ. Geom.*, 19:125–167, 168–171, 1984. ↑ 36.

[34] B. H. Gross and D. B. Zagier. Heegner points and derivatives of l-series. *Invent. Math.*, 84(2):225–320, 1986. ↑ 122.

[35] J. Harris and J. H. Silverman. Bielliptic curves and symmetric products. *Proc. Amer. Math. Soc.*, 112(2):347–356, 1991. ↑ 21, 55, 58, 99, 100.

[36] R. Hartshorne. *Algebraic Geometry*. Graduate Texts in Mathematics. Springer, 1977. ↑ 18.

[37] Y. Hasegawa and M. Shimura. Trigonal modular curves. *Acta Arith.*, 88(2):129–140, 1999. ↑ iii, v, 29, 30, 33, 34, 37, 38, 40, 56, 79, 138, 139, 140, 141, 142, 143.

[38] Y. Hasegawa and M. Shimura. Trigonal modular curves $X_0^{+d}(N)$. *Proc. Japan Acad., Ser. A*, 75(9):172–175, 1999. ↑ iii, vi, 44, 51, 58, 70, 76, 146, 147, 148.

[39] Y. Hasegawa and M. Shimura. Trigonal modular curves $X_0^*(N)$. *Proc. Japan Acad., Ser. A*, 76(6):83–86, 2000. ↑ 58.

[40] Y. Hasegawa and M. Shimura. Trigonal quotients of modular curves $X_0(N)$. *Proc. Japan Acad., Ser. A*, 82(2):15–17, 2006. ↑ 58.

[41] F. Hess. Computing Riemann-Roch spaces in algebraic function fields and related topics. *J. Symb. Comput.*, 33(4):425–445, 2002. ↑ 57.

[42] W. Hwang and D. Jeon. Modular curves with infinitely many quartic points. *Math. Comp.*, August 2023. ↑ 102.

[43] N. Ishii and F. Momose. Hyperelliptic modular curves. *Tsukuba J. Math.*, 15(2):413–423, 1991. ↑ iv, vi, 79, 90, 95, 96, 151.

[44] D. Jeon. Bielliptic modular curves $X_0^+(N)$. *J. Number Theory*, 185:319–338, 2018. ↑ 58.

[45] D. Jeon. Modular curves with infinitely many cubic points. *J. Number Theory*, 219:344–355, 2021. ↑ iv, vi, 29, 101.

[46] D. Jeon. Trielliptic modular curves $X_1(N)$. *Acta Arith.*, 206(2):171–188, 2022. ↑ 101.

[47] D. Jeon. Tetraelliptic modular curves $X_1(N)$, 2023. preprint. available at: `https://arxiv.org/abs/2305.05851`. ↑ 101.

[48] D. Jeon and C. H. Kim. On the arithmetic of certain modular curves. *Acta Arith.*, 130(2):181–193, 2007. ↑ iv, vi.

[49] D. Jeon and C. H. Kim. On the arithmetic of certain modular curves. *Acta Arith.*, 130(2):181–193, 2007. ↑ 79, 83, 90, 96, 151.

[50] D. Jeon, C. H. Kim, and E. Park. On the torsion of elliptic curves over quartic number fields. *J. London Math. Soc. (2)*, 74(1):1–12, 2006. ↑ 28, 29, 52, 79, 101, 131.

[51] D. Jeon, C. H. Kim, and A. Schweizer. On the torsion of elliptic curves over cubic number fields. *Acta Arith.*, 113(3):291–301, 2004. ↑ 29, 79, 101.

[52] D. Jeon, C. H. Kim, and A. Schweizer. Bielliptic intermediate modular curves. *J. Pure Appl. Algebra*, 224(1):272–299, 2020. ↑ 79, 151.

[53] D. Jeon and E. Park. Tetragonal modular curves. *Acta Arith.*, 120(3):307–312, 2005. ↑ iii, v, 29, 30, 34, 35, 49, 50, 52, 75, 76, 79, 84, 138, 139, 140, 141, 142, 143.

[54] B. Kadets and I. Vogt. Subspace configurations and low degree points on curves. *Adv. Math.*, 460:110021, 2025. ↑ 100, 129.

[55] S. Kamienny. Torsion points on elliptic curves and q-coefficients of modular forms. *Invent. Math.*, 109(2):221–229, 1992. ↑ 3, 101.

[56] N. M. Katz. Galois properties of torsion points on abelian varieties. *Invent. Math.*, 62(3):481–502, 1981. ↑ 53.

[57] M. A. Kenku. The modular curve $X_0(39)$ and rational isogeny. *Math. Proc. Cambridge Philos. Soc.*, 85(1):21–23, 1979. ↑ 13, 101.

[58] M. A. Kenku. The modular curve $X_0(169)$ and rational isogeny. *J. Lond. Math. Soc.*, s2-22(2):239–244, 10 1980. ↑ 13, 101.

[59] M. A. Kenku. The modular curves $X_0(65)$ and $X_0(91)$ and rational isogeny. *Math. Proc. Cambridge Philos. Soc.*, 87(1):15–20, 1980. ↑ 13, 101.

[60] M. A. Kenku. On the modular curves $X_0(125)$, $X_1(25)$ and $X_1(49)$. *J. Lond. Math. Soc., II. Ser.*, 23:415–427, 1981. ↑ 13, 101.

[61] M. A. Kenku. On the number of $\mathbf{Q}$-isomorphism classes of elliptic curves in each $\mathbf{Q}$-isogeny class. *J. Number Theory*, 15(2):199–202, 1982. ↑ 8.

[62] M. A. Kenku and F. Momose. Torsion points on elliptic curves defined over quadratic fields. *Nagoya Math. J.*, 109:125–149, 1988. ↑ 3, 79, 101.

[63] M. Khawaja and S. Siksek. Primitive algebraic points on curves. *Res. Number Theory*, 10(57), 2024. ↑ 33.

[64] H. Kim. Functoriality for the exterior square of GL_4 and the symmetric fourth of GL_2. Appendix 2: Refined estimates towards the Ramanujan and Selberg conjectures (by H. Kim and P. Sarnak). *J. Amer. Math. Soc.*, 16(1):139–183, 2002. ↑ 28.

[65] V Kolyvagin. Finiteness of $E(Q)$ and $X(E,Q)$ for a class of Weil curves. *Math. USSR Izv.*, 32(3):523–541, 1989. ↑ 122.

[66] S. Ling. Shimura subgroups and degeneracy maps. *J. Number Theory*, 54(1):39–59, 1995. ↑ 122.

[67] LMFDB Collaboration. The L-functions and modular forms database. `http://www.lmfdb.org`, 2022. [Online; accessed 15 July 2024]. ↑ 29, 116.

[68] F. G. Madriaga, A. Pacetti, and L. Villagra Torcomian. On the equation $x^2+dy^6=z^p$ for square-free $1 \leq d \leq 20$. *Int. J. Number Theory*, 19(05):1129–1165, 2023. ↑ 58.

[69] G. Martens. Über den Clifford-Index algebraischer Kurven. *J. Reine Angew. Math.*, 336:83–90, 1982. ↑ 35.

[70] B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, 47(1):33–186, 1977. ↑ 2, 13, 53, 54, 101, 123.

[71] B. Mazur. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.*, 44(2):129–162, 1978. ↑ 13, 101.

[72] J.-F. Mestre. Corps euclidiens, unites exceptionnelles et courbes elliptiques. *J. Number Theory*, 13:123–137, 1981. ↑ 29.

[73] J. S. Milne. Abelian varieties. In *Arithmetic Geometry*, chapter V, pages 103–150. Springer New York, NY, 1986. ↑ 107, 118.

[74] J. S. Milne. Jacobian varieties. In *Arithmetic Geometry*, chapter VII, pages 167–212. Springer New York, NY, 1986. ↑ 17, 105, 108.

[75] F. Najman. Torsion of rational elliptic curves over cubic fields and sporadic points on $X_1(n)$. *Math. Res. Lett.*, 23(1):245–272, 2016. ↑ 3.

[76] F. Najman and P. Orlić. Gonality of the modular curve $X_0(N)$. *Math. Comp*, 93:863–886, 2023. ↑ iii, v, 29, 30, 61, 77, 126, 135.

[77] F. Najman and B. Vukorepa. Quadratic points on bielliptic modular curves. *Math. Comp.*, 92(342):1791–1816, 2023. ↑ 59.

[78] K. V. Nguyen and M.-H. Saito. d-gonality of modular curves and bounding torsions. preprint, available at: `https://arxiv.org/abs/alg-geom/9603024`, 1996. ↑ 37.

[79] M. Noether. Ueber invariante darstellung algebraischer funktionen. *Math. Ann*, 17, 1880. ↑ 82.

[80] A. P. Ogg. Hyperelliptic modular curves. *Bull. Soc. Math. France*, 102:449–462, 1974. ↑ iii, v, 29, 30, 33, 56, 79, 101, 137, 138, 139.

[81] P. Orlić. Tetragonal modular quotients $X_0^+(N)$, 2023. preprint, available at: `arxiv.org/abs/2311.09955`. ↑ iv, vi.

[82] P. Orlić. Tetragonal intermediate modular curves, 2024. preprint, available at: `arxiv.org/abs/2407.14512`. ↑ iv, vi.

[83] P. Orlić. Tetragonal modular quotients $X_0^{+d}(N)$, 2024. preprint, available at: arxiv.org/abs/2404.08014. ↑ iv, vi.

[84] A. Pacetti and L. Villagra Torcomian. $\mathbb{Q}$-Curves, Hecke characters and some Diophantine equations. *Math. Comp*, August 2022. ↑ 58.

[85] B. Poonen. Gonality of modular curves in characteristic p. *Math. Res. Lett.*, 14(4):691–701, 2007. ↑ 27, 37.

[86] J. Rouse, A. V. Sutherland, and D. Zureick-Brown. ℓ -adic images of Galois for elliptic curves over $\mathbb{Q}$ (and an appendix with John Voight). *Forum Math. Sigma*, 10:e62, 2022. ↑ 62, 83.

[87] F.-O. Schreyer. Syzygies of canonical curves and special linear series. *Math. Ann.*, 275(1):105–137, March 1986. ↑ 75.

[88] F.-O. Schreyer. A standard basis approach to syzygies of canonical curves. *J. Reine Angew. Math.*, 421:83–123, 1991. ↑ 36.

[89] I. R. Shafarevich. Algebraic number fields. *Transl., Ser. 2, Am. Math. Soc.*, 31:25–39, 1963. ↑ 8.

[90] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, 2nd edition, 2009. ↑ 4, 6, 7, 8, 9, 10, 15, 18, 102.

[91] W. A. Stein. *Modular forms, a computational approach*, volume 79 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2007. ↑ 116, 120, 123.

[92] H. Stichtenoth. *Algebraic function fields and codes*, volume 254 of *Graduate Texts in Mathematics*. Berlin: Springer, 2nd edition, 2009. ↑ 32.

[93] J. Tate. Endomorphisms of abelian varieties over finite fields. *Invent. Math.*, 2(2):134–144, 1966. ↑ 25.

[94] A. Weil. Numbers of solutions of equations in finite fields. *Bull. Amer. Math. Soc.*, 55:497–508, 1949. ↑ 24.

[95] P. G. Zograf. Small eigenvalues of automorphic laplacians in spaces of parabolic forms. *J. Soviet Math.*, 36(1):106–114, 1987. ↑ 28.

[96] D. Zywina. Computing actions on cusp forms. preprint, available at https://arxiv.org/abs/2001.07270, 2020. ↑ 83.

CURRICULUM VITAE

Petar Orlić was born on July 11th 1998 in Zagreb. He attended elementary school and XV Gymnasium in Zagreb and started his studies at the University of Zagreb, Faculty of Science, Department of Mathematics in 2016. In 2019 he finished the Undergraduate University Programme and in 2021 he finished the Graduate University Programme and was awarded the title summa cum laude. His Master's thesis was entitled *Isogenies of elliptic curves* and was written under the supervision of prof.dr.sc. Filip Najman.

During his high school education he participated in International Mathematical Olympiad three times, in 2014, 2015, and 2016. He was awarded a silver medal in 2015 and a bronze medal in 2016. During his studies he participated in Vojtéch Jarnik International Mathematics Competition where he got 5th place in 2017 and 2nd place in 2018. He also participated in the International Mathematics Competition where he won two gold medals.

In 2019 he was awarded the Special rector's award of the University of Zagreb for the two gold medals at the International Mathematics Competition and in 2020 he got the award for best students in the final year of graduate programmes.

In 2021 he started a doctoral programme in mathematics and is working as a teaching assistant at the University of Zagreb, where he is a member of the Seminar for Number Theory and Algebra. He has participated in several international conferences and research schools and has written a number of papers. Two of them have been published:

- F. Najman and P. Orlić. Gonality of the modular curve $X_0(N)$. *Math. Comp,* 93:863-886, 2023

- M. Derickx and P. Orlić, Modular curves $X_0(N)$ with infinitely many quartic points. *Res. Number Theory,* 10(42), 2024

Additionally, one paper has been accepted for publishing:

- P. Orlić. Tetragonal modular quotients $X_0^+(N)$, to appear in *Acta Arith.*