Gonality of the modular curve $X_0(N)$

Dubrovnik, Croatia

Petar Orlić

Faculty of Science
Department of Mathematics
University of Zagreb

7. 10. 2022.

Funding

EUROPSKA UNIJA
Zajedno do fondova EU
EUROPSKI STRUKTURNI I INVESTICIJSKI FONDOVI
Operativni program KONKURENTNOST I KOHEZIJA

Sadržaj ove prezentacije isključiva je odgovornost Prirodoslovno-matematičkog fakulteta Sveučilišta u Zagrebu te ne predstavlja nužno stajalište Europske unije.

Projekt sufinancira Europska unija iz Europskog fonda za regionalni razvoj.

Supported by the QuantiXLie Centre of Excellence, a project cofinanced by the Croatian Government and European Union through the European Regional Development Fund - the Competitiveness and Cohesion Operational Programme (KK.01.1.1.01.0004).

Projekt:KK.01.1.1.01.0004
Provedba vrhunskih istraživanja u sklopu Znanstvenog centra izvrsnosti (ZCI) za kvantne i kompleksne sustave te reprezentacije Liejevih algebri

Introduction

For a curve C over a field k, the gonality $\mathrm{gon}_k C$ is the least degree of a non-constant morphism $f : C \to \mathbb{P}^1$ defined over k.
Abramovich gave a lower bound for the gonality over $\mathbb{C}$ for any modular curve.

Theorem (Abramovich; 1996)

Let $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup and X_Γ the corresponding modular curve. Let $D_\Gamma = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma]$ and let $d_\mathbb{C}(X_\Gamma)$ be a $\mathbb{C}$-gonality of X_Γ. Then

$$\frac{7}{800} D_\Gamma \leq d_\mathbb{C}(X_\Gamma).$$

This bound is usually not sharp.

The modular curve $X_0(N)$ corresponds to the congruence subgroup

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

The noncuspidal points of $X_0(N)$ represent classes $[(E, C_N)]$, where E is an elliptic curve with a cyclic Galois-invariant subgroup C_N of order N.
We study the gonalities of the modular curves $X_0(N)$ over $\mathbb{Q}$ and $\mathbb{C}$. The cases when the $\mathbb{C}$-gonality is ≤ 4 have already been determined.

The modular curve $X_0(N)$ corresponds to the congruence subgroup

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

The noncuspidal points of $X_0(N)$ represent classes $[(E, C_N)]$, where E is an elliptic curve with a cyclic Galois-invariant subgroup C_N of order N.
We study the gonalities of the modular curves $X_0(N)$ over $\mathbb{Q}$ and $\mathbb{C}$. The cases when the $\mathbb{C}$-gonality is ≤ 4 have already been determined.

Theorem

The modular curve $X_0(N)$ is isomorphic to $\mathbb{P}^1$ (i.e. of genus 0) if and only if

$$N \in \{1, \dots, 10, 12, 13, 16, 18, 25\}.$$

Theorem

The modular curve $X_0(N)$ is elliptic (i.e. of genus 1) if and only if

$$N \in \{11, 14, 15, 17, 19, 20, 21, 24, 27, 32, 36, 49\}.$$

Theorem (Ogg; 1974)

The modular curve $X_0(N)$ is hyperelliptic if and only if

$$N \in \{22, 23, 26, 28, 29, 30, 31, 33, 35, 37, 39, 40, 41, 46, 47, 48, 50, 59, 71\}.$$

Theorem (Hasegawa, Shimura; 1999)

The modular curve $X_0(N)$ has $\mathbb{C}$-gonality equal to 3 if and only if

$$N \in \{34, 38, 43, 44, 45, 53, 54, 61, 64, 81\}.$$

Theorem (Jeon, Park; 2005)

The modular curve $X_0(N)$ has $\mathbb{C}$-gonality equal to 4 if and only if

$$N \in \{38, 42, 44, 51, 52, 53, 55, 56, 57, 58, 60, 61, 62, 63, 65, 66, 67, 68, 69, 70, 72, 73, 74, 7577, 78, 79, 80, 83, 85, 87, 88, 89, 91, 92, 94, 95, 96, 98, 99, 100, 101, 103, 104, 107, 109, 111, 119, 121, 125, 131, 142, 143, 167, 191\}$$

The question of determining the trigonal and tetragonal curves over $\mathbb{Q}$ as well as the pentagonal curves over $\mathbb{Q}$ and $\mathbb{C}$ naturally arises.

The question of determining the trigonal and tetragonal curves over $\mathbb{Q}$ as well as the pentagonal curves over $\mathbb{Q}$ and $\mathbb{C}$ naturally arises.

Theorem (O., Najman)

The modular curve $X_0(N)$ has $\mathbb{Q}$-gonality equal to 3 if and only if

$$N \in \{34, 43, 45, 54, 64, 81\}.$$

The modular curve $X_0(N)$ has $\mathbb{Q}$-gonality equal to 4 if and only if

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

The modular curve $X_0(N)$ has $\mathbb{Q}$-gonality equal to 5 if and only if $N = 109$.

Further, we determine the $\mathbb{Q}$-gonality of $X_0(N)$ for all $N < 150$ except $135, 145$ and some N larger than 150. For many of those curves we also determine the $\mathbb{C}$-gonality.
As a byproduct of our results, we obtain that $X_0(N)$ is pentagonal over $\mathbb{C}$ for $N = 97, 169$, the first known such curves.
A lot of our results rely on extensive computations in `Magma`. The codes that verify our computations can be found on:

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

Lower bounds

In this section we give the results used to obtain lower bounds for the gonality of $X_0(N)$. We first mention the obvious inequality

$$\mathrm{gon}_{\mathbb{C}} C \leq \mathrm{gon}_{\mathbb{Q}} C.$$

Lower bounds

In this section we give the results used to obtain lower bounds for the gonality of $X_0(N)$. We first mention the obvious inequality

$$\operatorname{gon}_{\mathbb{C}} C \leq \operatorname{gon}_{\mathbb{Q}} C.$$

Proposition

For a curve C over $\mathbb{Q}$ and a rational prime p of good reduction of C, the following inequality holds:

$$\operatorname{gon}_{\mathbb{F}_p} C \leq \operatorname{gon}_{\mathbb{Q}} C.$$

For a curve $X_0(N)$, the primes of good reduction are all p not dividing N.

Proposition

Let $f : X \to Y$ be a non-constant morphism over k of degree d. Then

$$\operatorname{gon}_k Y \leq \operatorname{gon}_k X \leq d \cdot \operatorname{gon}_k Y.$$

Proposition (Castelnuovo-Severi inequality)

Let k be a perfect field and let X, Y, Z be curves over k. Let non-constant morphisms $f : X \to Y$ and $g : X \to Z$ over k be given of degrees m and n, respectively. Assume that there is no morphism $X \to X'$ over k of degree > 1 through which both f and g factor. Then

$$g(x) \leq m \cdot g(Y) + n \cdot g(Z) + (m-1)(n-1).$$

Fields of characteristic 0 (such as $\mathbb{Q}$ and $\mathbb{C}$) and finite fields $\mathbb{F}_q$ are perfect.

Proposition (Castelnuovo-Severi inequality)

Let k be a perfect field and let X, Y, Z be curves over k. Let non-constant morphisms $f : X \to Y$ and $g : X \to Z$ over k be given of degrees m and n, respectively. Assume that there is no morphism $X \to X'$ over k of degree > 1 through which both f and g factor. Then

$$g(x) \leq m \cdot g(Y) + n \cdot g(Z) + (m-1)(n-1).$$

Fields of characteristic 0 (such as $\mathbb{Q}$ and $\mathbb{C}$) and finite fields $\mathbb{F}_q$ are perfect.

Proposition

Let X be a curve and p a prime of good reduction for X. Suppose $X(\mathbb{F}_q) > d(q+1)$ for some d. Then $\operatorname{gon}_{\mathbb{Q}}(X) \geq d+1$.

Proof.

Let $f \in \mathbb{F}_q(X)$ be a function 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 $X(\mathbb{F}_q)$ into $\mathbb{P}^1(\mathbb{F}_q)$, it follows that $\#X(\mathbb{F}_q) \leq d(q+1)$, contradiction. □

Theorem (Hasegawa, Shimura; 1999)

If the modular curve $X_0(N)$ has $\mathbb{C}$-gonality equal to 4 then $N \leq 191$.
If the modular curve $X_0(N)$ has $\mathbb{C}$-gonality equal to 5 then $N \leq 197$.

For $N \geq 198$ the $\mathbb{Q}$ and $\mathbb{C}$-gonality are $\geq 6 \implies$ there are only finitely many possible pentagonal curves.
Jeon and Park have determined all curves $X_0(N)$ with $\mathbb{C}$-gonality equal to 4. The question of finding all curves $X_0(N)$ with $\mathbb{C}$-gonality equal to 5 is still open.

Divisors

Let C be a smooth curve over a field k. A divisor on C is a finite linear combination of points on C with integer coefficients. The degree of a divisor is a sum of its coefficients.

Divisors

Let C be a smooth curve over a field k. A divisor on C is a finite linear combination of points on C with integer coefficients. The degree of a divisor is a sum of its coefficients.
The divisor of a function $f : C \to \mathbb{P}^1$ is defined as

$$\mathrm{div}(f) = \sum_{P \in C} \mathrm{ord}_P(f) P$$

where $\mathrm{ord}_P(f)$ is the order of vanishing of f at P (negative if P is a pole).

Divisors

Let C be a smooth curve over a field k. A divisor on C is a finite linear combination of points on C with integer coefficients. The degree of a divisor is a sum of its coefficients.
The divisor of a function $f : C \to \mathbb{P}^1$ is defined as

$$\mathrm{div}(f) = \sum_{P \in C} \mathrm{ord}_P(f) P$$

where $\mathrm{ord}_P(f)$ is the order of vanishing of f at P (negative if P is a pole).
A divisor D is principal if there exists a function f such that $\mathrm{div}(f) = P$.
Note that every principal divisor has degree 0. Divisors D_1 and D_2 are linearly equivalent if $D_1 - D_2$ is principal.

Divisors

Let C be a smooth curve over a field k. A divisor on C is a finite linear combination of points on C with integer coefficients. The degree of a divisor is a sum of its coefficients.
The divisor of a function $f : C \to \mathbb{P}^1$ is defined as

$$\operatorname{div}(f) = \sum_{P \in C} \operatorname{ord}_P(f) P$$

where $\operatorname{ord}_P(f)$ is the order of vanishing of f at P (negative if P is a pole).
A divisor D is principal if there exists a function f such that $\operatorname{div}(f) = P$.
Note that every principal divisor has degree 0. Divisors D_1 and D_2 are linearly equivalent if $D_1 - D_2$ is principal.
A divisor D is effective (denoted by $D \geq 0$) if all its coefficients are nonnegative.

Riemann-Roch spaces

Let D be a divisor on a smooth curve f. The Riemann-Roch space of D, denoted by $\mathrm{L}(D)$, is the set of all functions $f : C \to \mathbb{P}^1$ such that

$$\mathrm{div}(f) + D \geq 0.$$

This set is a finite-dimensional vector space, we denote its dimension by $\ell(D)$.

Riemann-Roch spaces

Let D be a divisor on a smooth curve f. The Riemann-Roch space of D, denoted by $\mathrm{L}(D)$, is the set of all functions $f : C \to \mathbb{P}^1$ such that

$$\mathrm{div}(f) + D \geq 0.$$

This set is a finite-dimensional vector space, we denote its dimension by $\ell(D)$.

Theorem (Riemann-Roch)

Let X be a smooth curve of genus g with a divisor D and a canonical divisor K. Then

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

Mordell-Weil sieving

We use this method for solving the cases $N = 97$ and $N = 133$.
Notation:

- X - the curve $X_0(N)$
- $\mathrm{Pic}^d(X)$ - divisor classes of divisors of degree d (recall that $\mathrm{Pic}^0(X)$ is the Jacobian of the curve X)
- $W_d^r(X) := \{[D] \in \mathrm{Pic}^d(X) : D \geq 0, \ell(D) \geq r+1\}$
- $J_0(N)$ - the Jacobian of $X_0(N)$
- $J_0(N)^- := (1 - w_N)J_0(N)$ (w_N being the Atkin-Lehner involution)
- red_p - reduction modulo p
- $\mu : \mathrm{Pic}^d(X) \to J_0(N)^-$, $\mu(D) = (1 - w_N)(D)$

Mordell-Weil sieving

We use this method for solving the cases $N = 97$ and $N = 133$.
Notation:

- X - the curve $X_0(N)$
- $\mathrm{Pic}^d(X)$ - divisor classes of divisors of degree d (recall that $\mathrm{Pic}^0(X)$ is the Jacobian of the curve X)
- $W_d^r(X) := \{[D] \in \mathrm{Pic}^d(X) : D \geq 0, \ell(D) \geq r+1\}$
- $J_0(N)$ - the Jacobian of $X_0(N)$
- $J_0(N)^- := (1 - w_N)J_0(N)$ (w_N being the Atkin-Lehner involution)
- red_p - reduction modulo p
- $\mu : \mathrm{Pic}^d(X) \to J_0(N)^-$, $\mu(D) = (1 - w_N)(D)$

A curve X has a non-constant function of degree d over $\mathbb{Q}$ only if $W_d^1(X)(\mathbb{Q}) \neq \emptyset$ (since $f = c$ is in the Riemann-Roch space of every $D \geq 0$).
Suppose $D \in W_d^1(X)(\mathbb{Q})$ and $p > 2$ is a prime of good reduction for X.

We have the following commutative diagram

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

- $W_d^1(X)(\mathbb{F}_p)$ can be computed using `Magma`
- in our case $\mathrm{rank}(J_0(N)^-(\mathbb{Q})) = 0 \implies J_0(N)^-(\mathbb{Q}) \subset J_0(N)(\mathbb{Q})_{\mathrm{tors}}$
- red_p is injective on $J_0(N)(\mathbb{Q})_{\mathrm{tors}}$
- hence $\mu(D) \in \mathrm{red}_p^{-1}(\mu(W_d^1(X)(\mathbb{F}_p)))$

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 $W_d^1(X)(\mathbb{Q}) = \emptyset$.

Upper bounds

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

Proposition

Let X be a curve of genus $g \geq 2$ over a field k such that $X(k) \neq \emptyset$, then $\mathrm{gon}_k(X) \leq g$*. If k is algebraically closed, then* $\mathrm{gon}_k(X) \leq \lfloor \frac{g+3}{2} \rfloor$*.*

$X_0(N)(\mathbb{Q}) \neq \emptyset$ since for each N at least 2 cusps are defined over $\mathbb{Q}$. The same is true for the quotients $X_0(N)/\langle w_d \rangle$ and $X_0(N)/\langle w_{d_1}, w_{d_2} \rangle$.

Proof.

We fix $P \in X(k)$. The Riemann-Roch theorem tells us that

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

Since the divisor $(g-2)P$ is effective, we have $\ell((g-2)P) \geq 1$ and $\ell(K-(g-2)P) \geq 2$.
There exists a function f such that $D := \operatorname{div}(f)+K-(g-2)P \geq 0$. Since $\ell(D)=\ell(K-(g-2)P) \geq 2$, there exists a non-constant function g such that $\operatorname{div}(g)+D \geq 0$. This function has degree $\leq d$ because D has degree d. □

Proposition

Let p be a rational prime. There exists a morphism from $X_0(pN)$ to $X_0(N)$ defined over $\mathbb{Q}$ which is of degree $p+1$ if $p \nmid N$ and of degree p if $p \mid N$.

Proof.

The map $\pi_p : X_0(pN) \to X_0(N)$ sends the point corresponding to (E, C_{pN}), where C_{pN} is a cyclic subgroup of E of order pN, to (E, pC_{pN}). Thus the degree of π_p is the number of points (E, X) that satisfy $\pi_p((E, X)) = (E, C_N)$ for a given a fixed subgroup C_N of E. This is equal to the number of cyclic subgroups X of $(\mathbb{Z}/pN\mathbb{Z})^2$ that satisfy $pX = C_N$, which is as claimed. □

The morphisms $X_0(N) \to X_0(N)/w_d$ and $X_0(N) \to X_0(N)/\langle w_{d_1}, w_{d_2}\rangle$ defined over $\mathbb{Q}$ of degrees 2 and 4, respectively, also give us the upper bound in many cases.

Theorem (The Tower theorem)

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 $f' : C \to C'$ defined over k of degree d' dividing d such that

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

Corollary

(i) *Let C be a curve defined over $\mathbb{Q}$ with* $\mathrm{gon}_{\mathbb{C}}(X) = 3$ *and* $g(X) \geq 5$. *Then* $\mathrm{gon}_{\mathbb{Q}}(X) = 3$.

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

Proof.

Part (i) follows immediately by specializing C' to be $\mathbb{P}^1$ and d to be 3. To prove part (ii) we note that 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 X is bielliptic (and is tetragonal over $\mathbb{Q}$). If d' is 4, then X is tetragonal over $\mathbb{Q}$, as required. □

Summary of methods

Lower bounds

- $\text{gon}_{\mathbb{C}} C \leq \text{gon}_{\mathbb{Q}} C$
- $\text{gon}_{\mathbb{F}_p} C \leq \text{gon}_{\mathbb{Q}} C$
- $f : X \to Y$ over k of degree d $\implies \text{gon}_k Y \leq \text{gon}_k X$
- Castelnuovo-Severi inequality
- $X(\mathbb{F}_q) > d(q+1)$ for some d $\implies \text{gon}_{\mathbb{Q}}(X) \geq d+1$.
- $N \geq 198 \implies \text{gon}_{\mathbb{C}}(X_0(N)) \geq 6$
- Mordell-Weil sieving

Upper bounds

- $\text{gon}_{\mathbb{Q}}(X) \leq g$, $\text{gon}_{\mathbb{C}}(X) \leq \lfloor \frac{g+3}{2} \rfloor$
- $f : X \to Y$ over k of degree d $\implies \text{gon}_k X \leq d \cdot \text{gon}_k Y$
- $X_0(pN) \to X_0(N)$
- $X_0(N) \to X_0(N)/w_d$, $X_0(N) \to X_0(N)/\langle w_{d_1}, w_{d_2} \rangle$
- the Tower theorem

Examples

- $N = 34, 43, 45, 64$
  $3 = \text{gon}_{\mathbb{C}} \leq \text{gon}_{\mathbb{Q}} \leq g = 3 \implies \text{gon}_{\mathbb{C}} = \text{gon}_{\mathbb{Q}} = 3$

Examples

- $N = 34, 43, 45, 64$
  $3 = \mathrm{gon}_{\mathbb{C}} \leq \mathrm{gon}_{\mathbb{Q}} \leq g = 3 \implies \mathrm{gon}_{\mathbb{C}} = \mathrm{gon}_{\mathbb{Q}} = 3$
- $N = 38, 44, 53, 61$
  $4 \leq \mathrm{gon}_{\mathbb{F}_p} \leq \mathrm{gon}_{\mathbb{Q}} \leq g = 4$ ($p = 3$ for 61 and $p = 5$ for $38, 44, 53$)
  $\implies \mathrm{gon}_{\mathbb{C}} = 3$, $\mathrm{gon}_{\mathbb{Q}} = 4$

Examples

- $N = 34, 43, 45, 64$
  $3 = \mathrm{gon}_{\mathbb{C}} \leq \mathrm{gon}_{\mathbb{Q}} \leq g = 3 \implies \mathrm{gon}_{\mathbb{C}} = \mathrm{gon}_{\mathbb{Q}} = 3$
- $N = 38, 44, 53, 61$
  $4 \leq \mathrm{gon}_{\mathbb{F}_p} \leq \mathrm{gon}_{\mathbb{Q}} \leq g = 4$ ($p = 3$ for 61 and $p = 5$ for $38, 44, 53$)
  $\implies \mathrm{gon}_{\mathbb{C}} = 3$, $\mathrm{gon}_{\mathbb{Q}} = 4$
- $N = 42, 52, 57, 67, 68, 73, 74, 77, 80, 87, 91, 98, 103, 107, 121, 125$
  $4 = \mathrm{gon}_{\mathbb{C}} \leq \mathrm{gon}_{\mathbb{Q}}$, the quotients $X_0(N)/w_N$ are hyperelliptic
  $\implies \mathrm{gon}_{\mathbb{Q}} \leq 2 \cdot 2 = 4$. Therefore, $\mathrm{gon}_{\mathbb{C}} = \mathrm{gon}_{\mathbb{Q}} = 4$.

Examples

- $N = 34, 43, 45, 64$
  $3 = \text{gon}_{\mathbb{C}} \leq \text{gon}_{\mathbb{Q}} \leq g = 3 \implies \text{gon}_{\mathbb{C}} = \text{gon}_{\mathbb{Q}} = 3$
- $N = 38, 44, 53, 61$
  $4 \leq \text{gon}_{\mathbb{F}_p} \leq \text{gon}_{\mathbb{Q}} \leq g = 4$ ($p = 3$ for 61 and $p = 5$ for $38, 44, 53$)
  $\implies \text{gon}_{\mathbb{C}} = 3, \text{gon}_{\mathbb{Q}} = 4$
- $N = 42, 52, 57, 67, 68, 73, 74, 77, 80, 87, 91, 98, 103, 107, 121, 125$
  $4 = \text{gon}_{\mathbb{C}} \leq \text{gon}_{\mathbb{Q}}$, the quotients $X_0(N)/w_N$ are hyperelliptic
  $\implies \text{gon}_{\mathbb{Q}} \leq 2 \cdot 2 = 4$. Therefore, $\text{gon}_{\mathbb{C}} = \text{gon}_{\mathbb{Q}} = 4$.
- $N = 117$
  $6 \leq \text{gon}_{\mathbb{F}_5} \leq \text{gon}_{\mathbb{Q}}$, degree 3 map to $X_0(39)$
  $\implies \text{gon}_{\mathbb{Q}} \leq 3 \cdot g(X_0(39)) = 3 \cdot 2 = 6$. Therefore, $\text{gon}_{\mathbb{Q}} = 6$.

- $N = 109$

  Jeon and Park have already proven that $\text{gon}_{\mathbb{C}} = 4$.
  We construct a rational function 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 $X_0^+(109)$.
  To be precise, we found rational divisors P, Q, R such that $\deg(P) = 1$, $\deg(Q) = \deg(R) = 2$ and $\ell(P + Q + R) = 2$.
  Furthermore, $5 \leq \text{gon}_{\mathbb{F}_3} \leq \text{gon}_{\mathbb{Q}}$ and it follows that $\text{gon}_{\mathbb{Q}} = 5$.

- $N = 146$
  The quotient $X_0(146)/w_{146}$ is of genus 5 and trigonal over $\mathbb{C}$. Therefore, it is trigonal over $\mathbb{Q}$ by the Tower theorem and $\text{gon}_{\mathbb{Q}} \leq 2 \times 3 = 6$.
  We know that $\text{gon}_{\mathbb{C}} \geq 5$ from the theorems in the Introduction. On the other hand, suppose that there is a map $X_0(146) \to \mathbb{P}^1$ of degree 5. Then by applying the CS-inequality we get

$$g(X_0(146)) \leq 5 \cdot 0 + 2 \cdot 5 + (5-1)(2-1) \leq 14$$

  which is impossible since $g(X_0(146)) = 17$. Therefore, $\text{gon}_{\mathbb{C}} = \text{gon}_{\mathbb{Q}} = 6$.

- $N = 169$
  The curve $X_0(169)$ is of genus 8. Therefore, $\mathrm{gon}_{\mathbb{C}} \leq \lfloor \frac{8+3}{2} \rfloor = 5$. Since $\mathrm{gon}_{\mathbb{C}} \geq 5$ from the theorems in the Introduction, we get $\mathrm{gon}_{\mathbb{C}} = 5$.
  Let us now determine the $\mathbb{Q}$-gonality.

- $N = 169$

  The curve $X_0(169)$ is of genus 8. Therefore, $\mathrm{gon}_{\mathbb{C}} \leq \lfloor \frac{8+3}{2} \rfloor = 5$. Since $\mathrm{gon}_{\mathbb{C}} \geq 5$ from the theorems in the Introduction, we get $\mathrm{gon}_{\mathbb{C}} = 5$.
  Let us now determine the $\mathbb{Q}$-gonality.
  The quotient $X_0(169)/w_{169}$ is of genus 3. Therefore,
  $\mathrm{gon}_{\mathbb{Q}} \leq 2 \cdot 3 = 6$. On the other hand, we have $6 \leq \mathrm{gon}_{\mathbb{F}_p} \leq \mathrm{gon}_{\mathbb{Q}}$ which implies that $\mathrm{gon}_{\mathbb{Q}} = 6$.

- $N = 97$
  The curve $X_0(97)$ is of genus 7. Therefore, $\text{gon}_{\mathbb{C}} \leq \lfloor \frac{7+3}{2} \rfloor = 5$. Since $\text{gon}_{\mathbb{C}} \geq 5$ from the theorems in the Introduction, we get $\text{gon}_{\mathbb{C}} = 5$. Let us now determine the $\mathbb{Q}$-gonality.

- $N = 97$
  The curve $X_0(97)$ is of genus 7. Therefore, $\text{gon}_{\mathbb{C}} \leq \lfloor \frac{7+3}{2} \rfloor = 5$. Since $\text{gon}_{\mathbb{C}} \geq 5$ from the theorems in the Introduction, we get $\text{gon}_{\mathbb{C}} = 5$.
  Let us now determine the $\mathbb{Q}$-gonality.
  The quotient $X_0(97)/w_{97}$ is of genus 3. Therefore, we have $\text{gon}_{\mathbb{Q}} \leq 2 \cdot 3 = 6$. For the lower bound we do the Mordell-Weil sieving.

The rank of $J_0(97)^-(\mathbb{Q})$ is 0.
For a prime p, $J_0(p)^-_{tors}(\mathbb{Q}) \simeq \mathbb{Z}/\frac{p-1}{12}\mathbb{Z}$ and is generated by $D_0 = [0 - \infty]$, where 0 and ∞ are the two cusps of $X_0(p)$.
Therefore, $J_0(97)^-(\mathbb{Q}) \simeq \mathbb{Z}/8\mathbb{Z}$ and is generated by D_0.
We compute

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

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

Therefore $W_5^1(X_0(97))(\mathbb{Q}) = \emptyset$ and we get $\mathrm{gon}_{\mathbb{Q}} = 6$.

The rank of $J_0(97)^-(\mathbb{Q})$ is 0.
For a prime p, $J_0(p)^-_{tors}(\mathbb{Q}) \simeq \mathbb{Z}/\frac{p-1}{12}\mathbb{Z}$ and is generated by $D_0 = [0 - \infty]$, where 0 and ∞ are the two cusps of $X_0(p)$.
Therefore, $J_0(97)^-(\mathbb{Q}) \simeq \mathbb{Z}/8\mathbb{Z}$ and is generated by D_0.
We compute

$$\text{red}_3^{-1}(\mu(W_5^1(X_0(97)(\mathbb{F}_3)))) = \{0\},$$

$$\text{red}_5^{-1}(\mu(W_5^1(X_0(97)(\mathbb{F}_5)))) = \{D_0, 7D_0\}.$$

Therefore $W_5^1(X_0(97))(\mathbb{Q}) = \emptyset$ and we get $\text{gon}_{\mathbb{Q}} = 6$.
Later we noticed that

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

so it was possible to do the sieving with just one prime.

- $N = 133$

  This case is more involved than 97 because we couldn't compute the torsion group exactly.
  The rank of $J_0(133)^-(\mathbb{Q})$ is 0, so $J_0(133)^-(\mathbb{Q}) \subset J_0(133)(\mathbb{Q})_{\text{tors}}$.
  We proved that $J_0(133)(\mathbb{Q})_{\text{tors}}$ is isomorphic to a subgroup of $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/360\mathbb{Z}$.
  We found rational divisors 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 $x \in J_0(133)^-(\mathbb{Q})$, 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 97).
  We compute

  $$\text{red}_3^{-1}(2\mu(W_7^1(X_0(133))(\mathbb{F}_3))) = \emptyset.$$

  Therefore, $W_7^1(X_0(133))(\mathbb{Q}) = \emptyset$ and we get $\text{gon}_\mathbb{Q} = 8$.