Modular curves $X_0(N)$ with infinitely many points of degree d

Joint work with Maarten Derickx

Petar Orlić

Faculty of Science
Department of Mathematics
University of Zagreb

Modular curves and Galois representations, Zagreb 2023

Introduction

We want to determine the curves $X_0(N)$ with infinitely many points of degree d.

Definition

Let C be a curve defined over a number field k. The arithmetic degree of rationality $\mathrm{a.irr}_k C$ is the smallest integer d such that C has infinitely many closed points of degree d over k, i.e.

$$\mathrm{a.irr}_k C := \left\{ \min \left(d, \# \left\{ \cup_{[F:k] \leq d} C(F) \right\} = \infty \right) \right\}.$$

Therefore, we want to determine all curves $X_0(N)$ such that $\mathrm{a.irr}_{\mathbb{Q}} X_0(N) = d$.

This problem is closely related to finding a rational degree d map from $X_0(N)$ to $\mathbb{P}^1$ or a positive $\mathbb{Q}$-rank elliptic curve.

Theorem (Kadets, Vogt 2022)

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 $\epsilon := 3d - 1 - 6m < 6$. 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. $g \leq \max\left(\frac{d(d-1)}{2} + 1, 3m(m-1) + m\epsilon\right)$.

Special case: $d = 4$

Corollary

Suppose $C/\mathbb{Q}$ is a curve of genus $g \geq 8$ and $\text{a.irr}_{\mathbb{Q}} X = 4$. Then there exists a nonconstant rational morphism of degree 4 from C to $\mathbb{P}^1$ or an elliptic curve defined over $\mathbb{Q}$ with a positive $\mathbb{Q}$-rank.

Proof.

We compute $m = 1$ and $\epsilon = 5$. Therefore, case (2) of the previous theorem is impossible and we have a morphism $f : C \to Y$ of degree 2 or 4.
If $\deg f = 2$, then we have $\text{a.irr}_{\mathbb{Q}} Y = 2$ and Y must be a double cover of $\mathbb{P}^1$ or an elliptic curve with a positive $\mathbb{Q}$-rank (Harris-Silverman).
If $\deg f = 4$, then we have $\text{a.irr}_{\mathbb{Q}} Y = 1$ and Y must be isomorphic to $\mathbb{P}^1$ or an elliptic curve with a positive $\mathbb{Q}$-rank (Faltings' theorem). □

Degree 4 map to an elliptic curve

After eliminating the tetragonal curves, our problem of finding infinitely many quartic points reduces to finding a degree 4 rational map to a positive $\mathbb{Q}$-rank elliptic curve.

Theorem (Modularity theorem)

For every elliptic curve $E/\mathbb{Q}$, for some N there exists a rational map from $X_0(N)$ to E.

A minimal such N is called the conductor of E. We will denote it by $\mathrm{Cond}(E)$. We call the corresponding rational map $f : X_0(\mathrm{Cond}(E)) \to E$ a modular parametrization of E.
All primes of bad reduction for E are those that divide $\mathrm{Cond}(E)$. Also, every N such that there exists a rational map from $X_0(N)$ to E must be a multiple of $\mathrm{Cond}(E)$.

Jacobians

For every non-singular algebraic curve C its Jacobian variety $J(C)$ is an abelian variety with the Albanese property.
This implies that any morphism from $X_0(N)$ to E that sends ∞ to 0 factors uniquely through $J_0(N)$.
Furthermore, if there exists a nonconstant morphism from $J_0(N)$ to E, then E must (up to isogeny) appear in the decomposition of $J_0(N)$. This means that there are only finitely many such elliptic curves E.

Jacobians

For every non-singular algebraic curve C its Jacobian variety $J(C)$ is an abelian variety with the Albanese property.
This implies that any morphism from $X_0(N)$ to E that sends ∞ to 0 factors uniquely through $J_0(N)$.
Furthermore, if there exists a nonconstant morphism from $J_0(N)$ to E, then E must (up to isogeny) appear in the decomposition of $J_0(N)$. This means that there are only finitely many such elliptic curves E.

Proposition

Let $C/\mathbb{Q}$ be a curve with at least one rational point and $E/\mathbb{Q}$ an elliptic curve 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* $\mathrm{Hom}_{\mathbb{Q}}(J(C), E) \cong \mathbb{Z}^n$.

For each of these finitely many levels N and elliptic curves E we determined the basis for $\mathrm{Hom}_{\mathbb{Q}}(J_0(N), E)$ and its quadratic form.

Let $P \in C(\mathbb{Q})$, $f \in \mathrm{Hom}(C, E)$, and

$$\mathrm{Hom}_P(C, E) := \{g : C \to E \mid g(P) = 0\}.$$

We extend the degree map as follows.

$$\mathrm{Hom}(C, E) \xrightarrow{f - f(P)} \mathrm{Hom}_P(C, E) \xrightarrow{x \mapsto [x-P]} \mathrm{Hom}(J(C), E)$$

Note that the translated map $f - f(P)$ has the same degree as f.

We construct the quadratic form as a pairing map

$$\langle \cdot, \cdot \rangle : \mathrm{Hom}_{\mathbb{Q}}(J_0(N), E) \times \mathrm{Hom}_{\mathbb{Q}}(J_0(N), E) \to \mathrm{Hom}_{\mathbb{Q}}(E, E) \equiv \mathbb{Z}.$$

On $\mathrm{Hom}_{\mathbb{Q}}(X_0(N), E)$ this pairing is defined as

$$\langle f, g \rangle = f_* \circ g^*.$$

Therefore, we have that $\langle f, f \rangle = f_* \circ f^* = [\deg f]$ and this is indeed an extension of the degree map.

Degeneracy maps

Let E be a strong Weil curve, $M := \mathrm{Cond}(E) \mid N$, and let $f : X_0(M) \to E$ be the modular parametrization of E.
For each divisor d of $\frac{N}{M}$ there exists a degeneracy map
$\iota_{d,N,M} : X_0(N) \to X_0(M)$,

$$\iota_{d,N,M} : X_0(N) \to X_0(M),\ (E, G) \to (E/G[d], (G/G[d])[M]).$$

Using Sage, we proved that in all our cases the maps $f \circ \iota_{d,N,M}$ form a basis for $\mathrm{Hom}_{\mathbb{Q}}(J_0(N), E)$.

Degeneracy maps

Let E be a strong Weil curve, $M := \mathrm{Cond}(E) \mid N$, and let $f : X_0(M) \to E$ be the modular parametrization of E.
For each divisor d of $\frac{N}{M}$ there exists a degeneracy map
$\iota_{d,N,M} : X_0(N) \to X_0(M)$,

$$\iota_{d,N,M} : X_0(N) \to X_0(M),\ (E, G) \to (E/G[d], (G/G[d])[M]).$$

Using Sage, we proved that in all our cases the maps $f \circ \iota_{d,N,M}$ form a basis for $\mathrm{Hom}_{\mathbb{Q}}(J_0(N), E)$.

Proposition (Coefficients of the quadratic form - squarefree case)

Suppose $\frac{N}{M}$ is squarefree and let d_1, d_2 be divisors of $\frac{N}{M}$. We write $\gcd := \gcd(d_1, d_2)$ *and* $\mathrm{lcm} = \mathrm{lcm}(d_1, d_2)$, *then the coefficients of the quadratic form are*

$$\langle f \circ \iota_{d_1,N,M}, f \circ \iota_{d_2,N,M} \rangle = a_{d_1 d_2/\gcd^2} \cdot \psi\left(\frac{N \gcd}{M\ \mathrm{lcm}}\right) \cdot \deg f,$$

where $a_{d_1 d_2/\gcd^2}$ is the coefficient of the modular form corresponding to E.

Sketch of the proof.

We begin by proving

$$\left\langle \iota_{1,N,M}, \iota_{N/M,N,M} \right\rangle (E,G) = \sum_{\substack{\#C=N/M \\ C\cap G=\{0\}}} (E/C,(G+C)/C) = T_{N/M}(E,G).$$

Sketch of the proof.

We begin by proving

$$\left\langle \iota_{1,N,M}, \iota_{N/M,N,M} \right\rangle (E,G) = \sum_{\substack{\#C=N/M \\ C\cap G=\{0\}}} (E/C,(G+C)/C) = T_{N/M}(E,G).$$

We prove (after much tedious work with similar sums) that

$$\left\langle f\circ \iota_{d_1,N,M}, f\circ \iota_{d_2,N,M} \right\rangle =$$

$$= w_M \circ T_{d_1/\gcd} \circ w_M \circ T_{d_2/\gcd} \circ [\deg \iota_{\gcd,N,M\mathrm{lcm}/\gcd}] \circ [\deg f].$$

Sketch of the proof.

We begin by proving

$$\left\langle \iota_{1,N,M}, \iota_{N/M,N,M} \right\rangle (E,G) = \sum_{\substack{\#C=N/M \\ C\cap G=\{0\}}} (E/C,(G+C)/C) = T_{N/M}(E,G).$$

We prove (after much tedious work with similar sums) that

$$\langle f \circ \iota_{d_1,N,M}, f \circ \iota_{d_2,N,M} \rangle =$$

$$= w_M \circ T_{d_1/\gcd} \circ w_M \circ T_{d_2/\gcd} \circ [\deg \iota_{\gcd,N,M\mathrm{lcm}/\gcd}] \circ [\deg f].$$

As the Atkin-Lehner involution w_M acts on $E \subset J_0(M)$ as ± 1, it cancels itself out. Also, Hecke operators T_m act on $E \subset J_0(M)$ as multiplication by a_m (the coefficient in the corresponding newform).
Furthermore, since $(\frac{d_1}{\gcd}, \frac{d_2}{\gcd}) = 1$, we know that $a_{d_1/\gcd} \cdot a_{d_2/\gcd} = a_{d_1 d_2/\gcd^2}$. We finish the proof by noting that $\deg \iota_{d,N_1,N_2} = \psi(\frac{N_1}{N_2})$ for any positive integers d, N_1, N_2. □

In the non-squarefree case, we get a similar result

$$\langle f \circ \iota_{d_1,N,M}, f \circ \iota_{d_2,N,M} \rangle = a \cdot \psi\left(\frac{N \gcd}{M \mathrm{lcm}}\right) \cdot \deg f,$$

where

$$a = \sum_{m^2 | (d_1 d_2 / \gcd^2)} \mu(m) a_{d_1 d_2 / (gcd^2 m^2)}.$$

The Möbius sum comes from the properties of the Hecke operators.

In the non-squarefree case, we get a similar result

$$\langle f \circ \iota_{d_1,N,M}, f \circ \iota_{d_2,N,M} \rangle = a \cdot \psi\left(\frac{N \gcd}{M \mathrm{lcm}}\right) \cdot \deg f,$$

where

$$a = \sum_{m^2 | (d_1 d_2 / \gcd^2)} \mu(m) a_{d_1 d_2/(gcd^2 m^2)}.$$

The Möbius sum comes from the properties of the Hecke operators. This formula is useful because all factors are easily computable and available on LMFDB.

In the non-squarefree case, we get a similar result

$$\langle f \circ \iota_{d_1,N,M}, f \circ \iota_{d_2,N,M} \rangle = a \cdot \psi\left(\frac{N \gcd}{M \mathrm{lcm}}\right) \cdot \deg f,$$

where

$$a = \sum_{m^2 | (d_1 d_2 / \gcd^2)} \mu(m) a_{d_1 d_2/(gcd^2 m^2)}.$$

The Möbius sum comes from the properties of the Hecke operators.
This formula is useful because all factors are easily computable and available on LMFDB.
Now that we know the coefficients of the quadratic form, it is enough to show that it can never attain the value 4.

In the non-squarefree case, we get a similar result

$$\langle f \circ \iota_{d_1,N,M}, f \circ \iota_{d_2,N,M} \rangle = a \cdot \psi\left(\frac{N \gcd}{M \mathrm{lcm}}\right) \cdot \deg f,$$

where

$$a = \sum_{m^2 | (d_1 d_2 / \gcd^2)} \mu(m) a_{d_1 d_2 / (gcd^2 m^2)}.$$

The Möbius sum comes from the properties of the Hecke operators.
This formula is useful because all factors are easily computable and available on LMFDB.
Now that we know the coefficients of the quadratic form, it is enough to show that it can never attain the value 4.
If E is not a strong Weil curve, let E' be a strong Weil curve in its isogeny class. We proved (in our cases) that the maps from $J_0(N)$ to E factor through E'.

In order to prove that the maps $f \circ \iota_{d,N,M}$ form a basis for $\mathrm{Hom}_{\mathbb{Q}}(J_0(N), E)$, we needed to prove that a map $\xi^{\vee}_{E,N} : E^n \to J_0(N)$ (defined via these maps $f \circ \iota_{d,N,M}$) is injective. We verified this for all our cases using Sage.

Proposition

Let E be a strong Weil curve over $\mathbb{Q}$ of conductor $M \mid N$ and let us suppose that $\frac{N}{M}$ is squarefree and coprime to M. If E has an odd analytic rank, then the kernel of $\xi^{\vee}_{E,N} : E^n \to J_0(N)$ is a 2-group.

In order to prove that the maps $f \circ \iota_{d,N,M}$ form a basis for $\mathrm{Hom}_{\mathbb{Q}}(J_0(N), E)$, we needed to prove that a map $\xi^{\vee}_{E,N} : E^n \to J_0(N)$ (defined via these maps $f \circ \iota_{d,N,M}$) is injective. We verified this for all our cases using Sage.

Proposition

Let E be a strong Weil curve over $\mathbb{Q}$ of conductor $M \mid N$ and let us suppose that $\frac{N}{M}$ is squarefree and coprime to M. If E has an odd analytic rank, then the kernel of $\xi^{\vee}_{E,N} : E^n \to J_0(N)$ is a 2-group.

We suspect that the kernel of this map is trivial, but so far we have not been able to prove it. If this turns out to be correct, we will no longer need Sage to find the basis.

Examples

We take $N = 122$. There exists only one elliptic curve E of positive $\mathbb{Q}$-rank and $\mathrm{cond}(E) \mid N$, namely $X_0^+(61)$. Its modular parametrization f is the degree 2 quotient map $X_0(61) \to X_0^+(61)$.
The basis for $\mathrm{Hom}_{\mathbb{Q}}(J_0(122), E)$ is $\{f \circ d_1, f \circ d_2\}$. We compute

$$\langle f \circ d_1, f \circ d_1 \rangle = \langle f \circ d_2, f \circ d_2 \rangle = a_1 \cdot \psi(2) \cdot 2 = 6,$$

$$\langle f \circ d_1, f \circ d_2 \rangle = \langle f \circ d_2, f \circ d_1 \rangle = a_2 \cdot \psi(1) \cdot 2 = -2.$$

This means that our quadratic form is $6x^2 - 4xy + 6y^2$. However, we can easily check that this can never be equal to 4 when $x, y \in \mathbb{Z}$.

We take $N = 129$. There exists only one elliptic curve E of positive $\mathbb{Q}$-rank and $\mathrm{cond}(E) \mid N$, namely $X_0^+(43)$. Its modular parametrization f is the degree 2 quotient map $X_0(43) \mapsto X_0^+(43)$.
The basis for $\mathrm{Hom}_{\mathbb{Q}}(J_0(129), E)$ is $\{f \circ d_1, f \circ d_3\}$. We compute

$$\langle f \circ d_1, f \circ d_1 \rangle = \langle f \circ d_3, f \circ d_3 \rangle = a_1 \cdot \psi(3) \cdot 2 = 8,$$

$$\langle f \circ d_1, f \circ d_3 \rangle = \langle f \circ d_3, f \circ d_1 \rangle = a_3 \cdot \psi(1) \cdot 2 = -4.$$

This means that our quadratic form $8x^2 - 8xy + 8y^2$. This expression is divisible by 8 when $x, y \in \mathbb{Z}$ and can therefore never be equal to 4.

- $N = 148$, $E = X_0^+(37)$, $M = 37$, $\deg f = 2$
  The basis for $\mathrm{Hom}_{\mathbb{Q}}(J_0(148), E)$ is $\{f \circ d_1, f \circ d_2, f \circ d_4\}$. The quadratic form is

$$12x^2 + 12y^2 + 12z^2 - 16xy + 4xz - 16yz.$$

- $N = 172$, $E = X_0^+(43)$, $M = 43$, $\deg f = 2$
  The basis for $\mathrm{Hom}_{\mathbb{Q}}(J_0(172), E)$ is $\{f \circ d_1, f \circ d_2, f \circ d_4\}$. The quadratic form is

$$12x^2 + 12y^2 + 12z^2 - 16xy + 4xz - 16yz.$$

Thank you for your attention!