Modular curves $X_0(N)$ with infinitely many quartic points

Joint work with Maarten Derickx

Petar Orlić

Faculty of Science
Department of Mathematics
University of Zagreb

Representation Theory XVIII, 2023

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

The modular curve $X_0(N)$ is the moduli space for elliptic curves E with cyclic subgroups C_N of order N. It is known that $X_0(N)$ can be defined over $\mathbb{Q}$.
If $P = [(E, C_N)] \in X_0(N)(k)$ for a number field k, then E and C_N are also defined over k.

Introduction

The modular curve $X_0(N)$ is the moduli space for elliptic curves E with cyclic subgroups C_N of order N. It is known that $X_0(N)$ can be defined over $\mathbb{Q}$.
If $P = [(E, C_N)] \in X_0(N)(k)$ for a number field k, then E and C_N are also defined over k.
We want to determine the curves $X_0(N)$ with infinitely many points of degree d. This problem has been solved for $d \leq 3$.

Theorem (Mazur 1978, Kenku 1979-1981: $d = 1$)

The modular curve $X_0(N)$ has infinitely many rational points if and only if $g(X_0(N)) = 0$, i.e. when

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

Theorem (Faltings 1983)

Let k be a number field and let C/k be a non-singular curve of genus $g \geq 2$. Then C has only finitely many rational points.

Theorem (Harris, Silverman 1991)

Let k be a number field. The curve C/k of genus $g \geq 1$ has infinitely many quadratic points if and only if there exists a degree 2 morphism from C to $\mathbb{P}^1$ or to an elliptic curve with positive rank.

Therefore, all curves of genus $g \geq 1$ with infinitely many quadratic points must be elliptic, hyperelliptic, or bielliptic.

Theorem (Harris, Silverman 1991)

Let k be a number field. The curve C/k of genus $g \geq 1$ has infinitely many quadratic points if and only if there exists a degree 2 morphism from C to $\mathbb{P}^1$ or to an elliptic curve with positive rank.

Therefore, all curves of genus $g \geq 1$ with infinitely many quadratic points must be elliptic, hyperelliptic, or bielliptic.
Ogg determined all hyperelliptic, and Bars determined all bielliptic curves $X_0(N)$.

Theorem (Bars 1998: $d = 2$)

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 (Harris, Silverman 1991)

Let k be a number field. The curve C/k of genus $g \geq 1$ has infinitely many quadratic points if and only if there exists a degree 2 morphism from C to $\mathbb{P}^1$ or to an elliptic curve with positive rank.

Therefore, all curves of genus $g \geq 1$ with infinitely many quadratic points must be elliptic, hyperelliptic, or bielliptic.
Ogg determined all hyperelliptic, and Bars determined all bielliptic curves $X_0(N)$.

Theorem (Bars 1998: $d = 2$)

The modular curve $X_0(N)$ has infinitely many points of degree 2 over $\mathbb{Q}$ if and only if

$$N \in \{1–33, 35–37, 39–41, 43, 46–50, 53, 59, 61, 65, 71, 79, 83, 89, 101, 131\}.$$

Furthermore, for curves $X_0(N)$ that are of genus $<= 8$, of genus $<= 10$ with N prime, or bielliptic, all quadratic points have been described.

Theorem (Jeon 2021: $d = 3$)

The modular curve $X_0(N)$ has infinitely many points of degree 3 over $\mathbb{Q}$ if and only if

$$N \in \{1 - 29, 31, 32, 34, 36, 37, 43, 45, 49, 50, 54, 64, 81\}.$$

Theorem (Jeon 2021: $d = 3$)

The modular curve $X_0(N)$ has infinitely many points of degree 3 over $\mathbb{Q}$ if and only if

$$N \in \{1 - 29, 31, 32, 34, 36, 37, 43, 45, 49, 50, 54, 64, 81\}.$$

Theorem (Abramovich, Harris 1991)

Let k be a number field. If the curve C/k of genus $g \geq 1$ has infinitely many cubic points, then there exists a morphism of degree ≤ 3 over $\overline{k}$ to $\mathbb{P}^1$ or an elliptic curve.

Theorem (Jeon 2021: $d = 3$)

The modular curve $X_0(N)$ has infinitely many points of degree 3 over $\mathbb{Q}$ if and only if

$$N \in \{1 - 29, 31, 32, 34, 36, 37, 43, 45, 49, 50, 54, 64, 81\}.$$

Theorem (Abramovich, Harris 1991)

Let k be a number field. If the curve C/k of genus $g \geq 1$ has infinitely many cubic points, then there exists a morphism of degree ≤ 3 over $\overline{k}$ to $\mathbb{P}^1$ or an elliptic curve.

After proving the result for $d = 3$, Abramovich and Harris gave a conjecture that a curve C/k with infinitely many points of degree d has a map of degree $\leq d$ over $\overline{k}$ to $\mathbb{P}^1$ or an elliptic curve.
This was, however, disproved for $d \geq 4$ by Debarre and Fahlaoui.

Definition

Let C/k be a curve. The k-gonality of C $\mathrm{gon}_k C$ is the minimal degree of a nonconstant morphism $g : C \to \mathbb{P}^1$ defined over k.

As we have seen, the existence of infinitely many points of degree d is related to the gonality of the curve.

Theorem (Frey 1994)

Let k be a number field. If a curve C/k has infinitely many points of degree $\leq d$, then $\mathrm{gon}_k C \leq 2d$.

After solving the cases $d \leq 3$, the next logical step is to determine the curves $X_0(N)$ with infinitely many points of degree 4 over $\mathbb{Q}$.

After solving the cases $d \leq 3$, the next logical step is to determine the curves $X_0(N)$ with infinitely many points of degree 4 over $\mathbb{Q}$.

Theorem (Derickx, O. 2023.)

The modular curve $X_0(N)$ has infinitely many points of degree 4 over $\mathbb{Q}$ if and only if

$$N \in \{1-75, 77-83, 85-89, 91, 92, 94-96, 98-101, 103, 104, 107, 111, 118, 119, 121, 123, 125, 128, 131, 141-143, 145, 155, 159, 167, 191\}.$$

Curves with infinitely many quartic points

In all cases when $X_0(N)$ has infinitely many quartic points, we obtain them as pullbacks of rational and quadratic points. We get the desired map $f : X_0(N) \to C'$ in several ways.

Curves with infinitely many quartic points

In all cases when $X_0(N)$ has infinitely many quartic points, we obtain them as pullbacks of rational and quadratic points. We get the desired map $f : X_0(N) \to C'$ in several ways.

- When $X_0(N)$ has $\mathbb{Q}$-gonality equal to 4 (all such cases were determined by Najman, O. in 2022), we can use the degree 4 rational map $f : C \to \mathbb{P}^1$.

Curves with infinitely many quartic points

In all cases when $X_0(N)$ has infinitely many quartic points, we obtain them as pullbacks of rational and quadratic points. We get the desired map $f : X_0(N) \to C'$ in several ways.

- When $X_0(N)$ has $\mathbb{Q}$-gonality equal to 4 (all such cases were determined by Najman, O. in 2022), we can use the degree 4 rational map $f : C \to \mathbb{P}^1$.
- When $X_0^+(N) := X_0(N)/w_N$ is an elliptic or hyperelliptic curve, we can use the degree 2 quotient map $\pi : X_0(N) \to X_0^+(N)$.

Curves with infinitely many quartic points

In all cases when $X_0(N)$ has infinitely many quartic points, we obtain them as pullbacks of rational and quadratic points. We get the desired map $f: X_0(N) \to C'$ in several ways.

- When $X_0(N)$ has $\mathbb{Q}$-gonality equal to 4 (all such cases were determined by Najman, O. in 2022), we can use the degree 4 rational map $f: C \to \mathbb{P}^1$.
- When $X_0^+(N) := X_0(N)/w_N$ is an elliptic or hyperelliptic curve, we can use the degree 2 quotient map $\pi: X_0(N) \to X_0^+(N)$.
- When N has exactly 2 different prime divisors and $X_0^*(N) := X_0(N)/B(N)$ is an elliptic curve of positive $\mathbb{Q}$-rank, we can use the degree 4 quotient map $\pi: X_0(N) \to X_0^*(N)$.

Curves with infinitely many quartic points

In all cases when $X_0(N)$ has infinitely many quartic points, we obtain them as pullbacks of rational and quadratic points. We get the desired map $f : X_0(N) \to C'$ in several ways.

- When $X_0(N)$ has $\mathbb{Q}$-gonality equal to 4 (all such cases were determined by Najman, O. in 2022), we can use the degree 4 rational map $f : C \to \mathbb{P}^1$.
- When $X_0^+(N) := X_0(N)/w_N$ is an elliptic or hyperelliptic curve, we can use the degree 2 quotient map $\pi : X_0(N) \to X_0^+(N)$.
- When N has exactly 2 different prime divisors and $X_0^*(N) := X_0(N)/B(N)$ is an elliptic curve of positive $\mathbb{Q}$-rank, we can use the degree 4 quotient map $\pi : X_0(N) \to X_0^*(N)$.
- When $N = 121$, the curve $X_{ns}^+(11)$ is an elliptic curve of rank 1 over $\mathbb{Q}$, and there exists a degree 4 rational map $X_0(121) \to X_{ns}^+(11)$.
- When $N = 128$, an elliptic curve $E : y^2 = x^3 + x^2 + x + 1$ (LMFDB label 128.a2) is of rank 1 over $\mathbb{Q}$, and there exists a degree 4 rational map $X_0(128) \to E$.

Curves with finitely many quartic points

As we have seen, we can obtain quartic points on a curve C as pullbacks of rational and quadratic points. It turns out that this is the only way to obtain them when $g(C)$ is high enough.

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 $\mathrm{a.irr}_{\mathbb{Q}} X_0(N) = 4$.

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

Corollary

Suppose $C/\mathbb{Q}$ is a curve of genus $g \geq 8$ and $\mathrm{a.irr}_{\mathbb{Q}} X = 4$. 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 $\mathrm{a.irr}_{\mathbb{Q}} Y = 2$ 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 $\mathrm{a.irr}_{\mathbb{Q}} Y = 1$ and Y must be isomorphic to $\mathbb{P}^1$ or an elliptic curve with a positive $\mathbb{Q}$-rank (Faltings' theorem). □

The only value of N with finitely many quartic points and $g(X_0(N)) \leq 7$ is $N = 97$. For all the other N, it is enough to prove that there is no degree 4 rational morphism to $\mathbb{P}^1$ or a positive $\mathbb{Q}$-rank elliptic curve.

The only value of N with finitely many quartic points and $g(X_0(N)) \leq 7$ is $N = 97$. For all the other N, it is enough to prove that there is no degree 4 rational morphism to $\mathbb{P}^1$ or a positive $\mathbb{Q}$-rank elliptic curve.

Proposition (Jeon, Kim, Park)

Let $X/\mathbb{Q}$ be a curve with infinitely many quartic points. If $g(X) \geq 7$ and $\mathrm{gon}_{\mathbb{Q}}(X) \geq 5$, then the Jacobian variety $J(X)$ must contain a positive $\mathbb{Q}$-rank elliptic curve.

Corollary

The modular curve $X_0(97)$ has only finitely many quartic points.

Proof.

We have $g(X_0(97)) = 7$ and $\mathrm{Gon}_{\mathbb{Q}}(X_0(97)) = 6$. However, the Jacobian variety $J_0(97)$ only contains (up to isogeny) abelian varieties of dimension 3 and 4. $\square$

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 $\mathrm{Cond}(E)$.

Proposition (Ogg)

For a prime $p \nmid N$, we have

$$\#X_0(N)(\mathbb{F}_{p^2}) \geq \frac{p-1}{12}\psi(N) + 2^{\omega(N)},$$

where $\psi(N) = N\prod_{q|N}(1+\frac{1}{q})$ *and* $\omega(N)$ *is the number of distinct prime divisors of* N.

Corollary

If the curve $X_0(N)$ *is tetraelliptic, then for every prime* $p \nmid N$ *we must have*

$$4(p+1)^2 \geq \frac{p-1}{12}\psi(N) + 2^{\omega(N)}.$$

Proof.

We have a morphism $f : X_0(N) \mapsto E$ of degree 4. Both $X_0(N)$ and E have good reduction at p since $p \nmid N$. Therefore, we have a morphism $\tilde{f} : \tilde{X}_0(N) \mapsto E_p$ of degree 4 defined over $\mathbb{F}_p$.
Hasse's theorem gives us that $\#E_p(\mathbb{F}_{p^2}) \leq (p+1)^2$. Moreover, every point in $\tilde{X}_0(N)(\mathbb{F}_{p^2})$ maps to $E_p(\mathbb{F}_{p^2})$ meaning that $\#\tilde{X}_0(N)(\mathbb{F}_{p^2}) \leq 4(p+1)^2$. □

Proof.

We have a morphism $f : X_0(N) \mapsto E$ of degree 4. Both $X_0(N)$ and E have good reduction at p since $p \nmid N$. Therefore, we have a morphism $\tilde{f} : \tilde{X}_0(N) \mapsto E_p$ of degree 4 defined over $\mathbb{F}_p$.

Hasse's theorem gives us that $\#E_p(\mathbb{F}_{p^2}) \leq (p+1)^2$. Moreover, every point in $\tilde{X}_0(N)(\mathbb{F}_{p^2})$ maps to $E_p(\mathbb{F}_{p^2})$ meaning that $\#\tilde{X}_0(N)(\mathbb{F}_{p^2}) \leq 4(p+1)^2$. $\square$

Using this inequality, we can eliminate all N except

$$N \in \{106, 113, 116, 122, 129, 130, 148, 158, 164, 166, 171, 172, 176, 178, \\ 182, 183, 184, 185, 195, 215, 237, 242, 249, 259, 264, 265, 267, 297\}.$$

Jacobians

For every non-singular algebraic curve C there exists a Jacobian variety $J(C)$. It is an abelian variety and has the Albanese property, i.e. any morphism from C to an abelian variety factors uniquely through $J(C)$.
Since elliptic curves are abelian varieties of dimension 1, this means that any morphism from $X_0(N)$ to an elliptic curve E factors uniquely through $J_0(N)$.
Furthermore, if there exists a 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 there exists a Jacobian variety $J(C)$. It is an abelian variety and has the Albanese property, i.e. any morphism from C to an abelian variety factors uniquely through $J(C)$.
Since elliptic curves are abelian varieties of dimension 1, this means that any morphism from $X_0(N)$ to an elliptic curve E factors uniquely through $J_0(N)$.
Furthermore, if there exists a 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 N and elliptic curves E we determined the basis for $\mathrm{Hom}_{\mathbb{Q}}(J_0(N), E)$ and its quadratic form.

We construct this 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 one of these elliptic curves, $M := \mathrm{Cond}(E) \mid N$, 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 one of these elliptic curves, $M := \mathrm{Cond}(E) \mid N$, 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

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

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

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

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

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

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

where

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

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

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

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.

Examples

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

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