SMOOTH PLANE MODELS OF MODULAR CURVES

1. Introduction

This story begins four years ago, when I just joined the Simons collaboration on Arithmetic Geometry, Number Theory and computation. Started my position on September 1st, and on September 2nd already going to a conference in Rennes with John Voight about computational methods in the p-adic local Langlands program. (Related to the topic of my PhD thesis).

John is giving the first talk about computing equations for modular curves using modular symbols, and someone in the crowd is asking about doing that more generally (for congruence subgroups that are not $\Gamma_0(N), \Gamma_1(N)$). I ask her and John some questions, and John suggests that I'll start with this project - compute modular symbols for any congruence subgroup. It seems like a small, easy project - something very appealing after years of graduate degree and no publications. Let me start by telling you several motivatiosn we had to start working on this project.

2. Elliptic Curves

Consider an elliptic curve $E : y^2 = f(x)$ defined over $\mathbb{Q}$ (i.e. $f \in \mathbb{Q}[x]$), where $\deg(f) = 3$. Then by Mordell's theorem $E(\mathbb{Q})$ is finitely generated (Mordell, 1922). Write $\overline{\mathbb{Q}}$ for the field of algebraic numbers (all α that are roots of some polynomial $m_\alpha(x) \in \mathbb{Q}[x]$), and $\mathrm{Gal}_{\mathbb{Q}} = \mathrm{Aut}(\overline{\mathbb{Q}})$ for the absolute Galois group of $\mathbb{Q}$.

If $P = (x, y) \in E(\overline{\mathbb{Q}})$, and $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$, then since $f(x) \in \mathbb{Q}[x]$, we have $\sigma(P) = (\sigma(x), \sigma(y)) \in E(\overline{\mathbb{Q}})$. Note that since $[N] : E \to E$ is algebraic, if $P \in E[N](\mathbb{C})$ then $P \in E(\overline{\mathbb{Q}})$. (The coordinates satisfy the N-th division polynomial). Also, if $[N]P = 0$, then $[N]\sigma(P) = 0$, showing that $\mathrm{Gal}_{\mathbb{Q}}$ acts on $E[N] = E[N](\mathbb{C}) \simeq (\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})$. Since addition is defined over $\mathbb{Q}$, the action is linear, yielding a representation $\overline{\rho}_{E,N} : \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$.

Example 2.1. If $E : y^2 = x^3 + x$, then $E[2] = \{0, (i, 0), (-i, 0), (0, 0)\}$, which we identify with $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ via $(i, 0) \mapsto (1, 0)$ and $(-i, 0) \mapsto (0, 1)$. Then if $\sigma(i) = -i$, $\overline{\rho}_{E,2}(\sigma) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

Question 2.2. *What can one say about* $\mathrm{Im}\,\overline{\rho}_{E,N}$ *How large is it?*

Example 2.3. In the above example, $\#\,\mathrm{Im}\,\overline{\rho}_{E,2} = 2$, while $\#\,\mathrm{GL}(2, \mathbb{Z}/2\mathbb{Z}) = 6$. This is a special case, since E has CM by i, hence $\overline{\rho}_{E,2}$ must commute with multiplication by i, which in our chosen basis is $[i] = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

Theorem 2.4 (Serre's Open Image Theorem, 1972)**.** *If $E/\mathbb{Q}$ is an elliptic curve without CM, then there exists a constant c_E such that* $[\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}) : \mathrm{Im}\,\overline{\rho}_{E,p}] \leq c_E$.

Conjecture 2.5 (Serre's uniformity conjecture, 1972)**.** *There exists c, independent of E, such that* $[\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z}) : \mathrm{Im}\,\overline{\rho}_{E,p}] \leq c$.

Question 2.6 (Mazur's Program B, 1977)**.** *Classify all options for* $\mathrm{Im}\,\overline{\rho}_{E,N}$.

3. Modular curves

The way we found to try and answer these questions is to look at moduli spaces of elliptic curves.

Let $\mathcal{H} = \{z \in \mathbb{C} : \operatorname{Im} z > 0\}$ be the complex upper half plane. It admits a natural action of $\mathrm{GL}_2^+(\mathbb{R})$. For a discrete subgroup $\Gamma \leq \mathrm{GL}_2^+(\mathbb{R})$ we can consider the quotient $Y_\Gamma(\mathbb{C}) = \Gamma\backslash\mathcal{H}$, which admits a natural compactification $X_\Gamma(\mathbb{C}) = Y_\Gamma(\mathbb{C}) \cup \{\Gamma\backslash\mathbb{P}^1(\mathbb{Q})\}$. As an example, if $\Gamma = \mathrm{SL}_2(\mathbb{Z}) = \mathrm{GL}_2^+(\mathbb{Z})$, then $\Gamma\backslash\mathcal{H}$ is the well-known fundamental domain D (draw), and $X_\Gamma(\mathbb{C})$ is birational to the Riemann sphere $\mathbb{P}^1(\mathbb{C})$. In this case, $X_\Gamma(\mathbb{C})$ parametrizes isomorphism classes of elliptic curves over $\mathbb{C}$ (or of homothety classes of lattices), through the map

$$\tau \mapsto \Lambda_\tau = \mathbb{Z} \cdot \tau + \mathbb{Z} \cdot 1 \mapsto E_\tau = \mathbb{C}/\Lambda_\tau.$$

Denote by $\Gamma(N) = \ker(\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}))$ the principal congruence subgroup of level N. Then $\Gamma(N)\backslash\mathcal{H}$ is a finite (Galois) cover of $\Gamma(1)\backslash\mathcal{H}$, ramified only at 3 points, parametrizing isomorphism classes of elliptic curves, with full level structure, i.e. a choice of basis for their N-torsion. More generally, if $\Gamma(N) \leq \Gamma$, we say that Γ is a congruence subgroup, and $X_\Gamma(\mathbb{C})$ is a Riemann surface, parametrizing isomorphism classes of elliptic curves with additional data. Important examples of congruence subgroups include

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid c \in N\mathbb{Z} \right\},$$

and

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \mid a - 1 \in N\mathbb{Z} \right\},$$

with $X_0(N)(\mathbb{C}) = X_{\Gamma_0(N)}(\mathbb{C})$ parametrizing elliptic curves with a cyclic N-isogeny, and $X_1(N)(\mathbb{C}) = X_{\Gamma_1(N)}(\mathbb{C})$ parametrizing elliptic curves with an N-torsion point, via

$$\tau \mapsto \left(\Lambda_\tau, \frac{1}{N} + \Lambda_\tau\right) = (c\tau + d)\left(\Lambda_{\gamma\tau}, \frac{1}{N} + \Lambda_{\gamma\tau}\right).$$

However, in number theory we care about the moduli space of elliptic curves, which are defined over $\mathbb{Q}$, and optimally one would like to have a curve X defined over $\mathbb{Q}$ such that its $\mathbb{Q}$-points parametrize elliptic curves over $\mathbb{Q}$. In fact, we have the following theorem of Shimura.

Theorem 3.1 (Shimura)**.** *There exists an algebraic curve X_Γ defined over $\mathbb{Q}(\zeta_N)$ such that $X_\Gamma(\mathbb{C}) = (\Gamma\backslash\mathcal{H}) \cup \{\Gamma\backslash\mathbb{P}^1(\mathbb{Q})\}$.*

But we want to bring this down to $\mathbb{Q}$. The way to do this is to keep track of the Galois action. For example, if (E, P) is an elliptic curve defined over $\mathbb{Q}$ with an N-torsion point, then it follows that $\operatorname{Im}\overline{\rho}_{E,N} \subseteq \begin{pmatrix} * & * \\ 0 & \pm 1 \end{pmatrix}$. (and for a pair (E, C) the image is in the Borel subgroup), with the Galois group acting on the Weil pairing through the determinant.

Therefore, instead of considering a congruence subgroup $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$, we consider a group $G \leq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. Then there is an algebraic (not necessarily irreducible) curve X_G parameterizing G-isomorphism classes of pairs (E, ϕ) where $\phi : E[N] \to (\mathbb{Z}/N\mathbb{Z}) \times (\mathbb{Z}/N\mathbb{Z})$ is an isomorphism, and a G-isomorphism $\iota : (E, \phi) \to (E', \phi')$ is such that there exists $g \in G$ with $\phi' \circ \iota = g \circ \phi$. Its $\mathbb{Q}$-points are elliptic curves E defined over $\mathbb{Q}$ with $\operatorname{Im}\overline{\rho}_{E,N} \leq G$ (up to conjugation). Then X_G is defined over $\mathbb{Q}$,

it has $[(\mathbb{Z}/N\mathbb{Z})^\times : \det(G)]$ components, each of which is isomorphic to X_{Γ_G} where Γ_G is the pullback of $G \cap \mathrm{SL}(\mathbb{Z}/N\mathbb{Z})$.

A different way - look at $X(N)^{big}$ and take its quotient by G. This curve parametrizes (E, P, Q) where P, Q are basis points, and it has geometric components indexed by $(\mathbb{Z}/N\mathbb{Z})^\times$ according to the Weil pairing of P, Q. An element $\sigma \in G$ identifies components differing by $\det(\sigma)$, hence $X(N)/G$ has $[(\mathbb{Z}/N\mathbb{Z})^\times : G]$ components. In particular, if $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$, then there is a single component, isomorphic to X_{Γ_G}.

We have the following progress on Serre's uniformity conjecture.

Theorem 3.2 (Serre, 1972)**.** *For $p > 13$, $G \leq \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ exceptional (S_4, A_4, A_5), the modular curve X_{Γ_G} has no rational points.*

Theorem 3.3 (Mazur, 1977)**.** *For $p > 37$, the modular curve $X_0(p)$ has no non-CM, non-cuspidal rational points.*

Theorem 3.4 (Bilu, Parent, Reboledom 2013)**.** *For $p > 13$, the modular curve $X_s^+(p)$ has no non-CM, non-cuspidal rational points.*

Serre's uniformity conjecture then restricts to showing that the only rational points on $X_{ns}^+(p)$ are CM for $p > 11$.

A few steps were taking in this direction in recent years. Eran: [Add here some more recent progress]

Theorem 3.5 (Balakrishnan, Dogra, Müller, Tuitman, Vonk, 2019)**.** *The modular curve $X_{ns}^+(13)$ has no non-CM rational points.*

Do I want to present some explicit models in the service of modularity? Maybe.

Can present some cool examples for models that had use, e.g. the proof of modularity (original, real quadratic fields, cubic fields, but also now imaginary quadratic fields).

Want to relate to previous work on models of modular curves and LMFDB effort on modular curves.

Theorem 3.6. *There exists an algorithm to compute a model over $\mathbb{Q}$ for $X_0(N)$.*

Model is an algebraic curve isomorphic to our curve.

Say something about canonical models.

Theorem 3.7 (Zywina (2020), Box (2021), A. (2022))**.** *Let $G \leq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ be such that $\det(G) = (\mathbb{Z}/N/Z)^\times$, $-1 \in G$ and $\eta G \eta^{-1} = G$, where $\eta = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$. Then there exists an algorithm to compute a canonical model over $\mathbb{Q}$ for X_G.*

Question 3.8. *When does X_Γ admit a smooth plane model defined over $\mathbb{Q}$?*

Theorem 3.9 (Badr, Bars, Garcia 2019)**.** *Let C be a smooth $\overline{\mathbb{Q}}$ plane curve defined over $\mathbb{Q}$ of degree d such that either d is coprime to 3 or $C(\mathbb{Q}) \neq \emptyset$. Then every twist of C is a smooth plane curve over $\mathbb{Q}$.*

Idea : the twists are classified by $H^1(k, PGL_3 = Aut(\mathbb{P}^2))$, which are the 3-torsion elements in the Brauer group.

4. Plane Curves

What is a smooth plane model of a curve X? It is a morphism $X \to \mathbb{P}^2$. Since each such morphism corresponds to a 2-dimensional linear system, induced from a divisor D on X. Let $d = \deg D$. Then $h^0(X, D) = 3$, and if we write

$$g^r_d(X) = \{D \in \mathrm{Pic}(X) : \deg(D) = d, h^0(X, D) = r + 1\},$$

it follows that $D \in g^2_d(X)$.

Thus, we may replace our question by a question of finding a divisor $D \in g^2_d(X)$ defined over $\mathbb{Q}$.

The question of finding divisors in $g^1_d(X)$ turns out to be related and extensively studied. Indeed, if $D \in g^1_d$, then it induces a non-constant morphism $\varphi_D : X \to \mathbb{P}^1$. The minimum number $\gamma(X)$ such that $g^1_{\gamma(X)} \neq \emptyset$ is the gonality of the curve X.

Proposition 4.1 (Serrano, 1987)**.** *Let $X \subseteq \mathbb{P}^2$ be a smooth plane curve of degree d. Then $\gamma(X) = d - 1$ and the unique g^2_d on X is $O(1)|_X$.*

Proof. Eran: [Does that work over $\mathbb{Q}$?] First, note that if E is a divisor of degree e, then if $n \geq e$, $O(n)|_X - E$ is base-point-free. Indeed, take the union of n distinct lines, e of which pass through the support of E. Let $D \in g^1_e(X)$. Then by Riemann-Roch $h^0(K_X - D) = h^0(D) - e + g - 1 = g - e + 1$. But $K_X = O(d-3)|_X$, so for any $f \leq d - 3$, for a divisor E of degree f, $O(n)|_X - E$ is base-point-free. In particular, for any $e \leq d - 2$, $h^0(O(n)|_X - D) = h^0(O(n)|_X) - e$. It follows that

$$g - e + 1 = h^0(O(d-3) - D) = h^0(O(d-3)) - e = h^0(K_X) - e = g - e,$$

contradiction. Therefore, there is no such divisor for $e \leq d - 2$. For $e = d - 1$, clearly projection from a point has the required properties, but we can show more. If $D \in g^1_d(X)$, then all points in the support lie on a line, so it must be the projection from a point. □

5. Bounds

Note that models for X_Γ defined over $\mathbb{Q}$ come from groups $G \leq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ such that $G \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ pulls back to Γ. An important observation is the following.

Theorem 5.1. *Let G_1, G_2 be such that $G_1 \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) = G_2 \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. If X_{G_1} has a smooth plane model defined over $\mathbb{Q}$, then so does X_{G_2}.*

Therefore, this question does not depend on G, but only on Γ.

The following theorem was known, but was not made precise quantitatively before.

Theorem 5.2 (Anni, A., Garcia, 2022)**.** *There exist finitely many modular curves that admit a smooth plane model over $\mathbb{Q}$.*

Proof. The idea is the same as in the proof from [Abramovich, 1996], using the relation we have between the gonality of the curve and the degree when it is a plane curve.

Let γ be the gonality of X_Γ, i.e. the minimum degree of a non-constant map $X_\Gamma \to \mathbb{P}^1$. Let $h = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma]$. Using the Yang-Yau inequality for the first eigenvalue of a compact Riemann surface [Li, Yau 1982], one bounds the first eigenvalue of the Laplacian on X_Γ by $\lambda_1 < \frac{24\gamma}{h}$.

On the other hand, Selberg's inequality, improved by [Kim, Sarnak, 2003], yields a lower bound $\lambda_1 \geq \alpha = \frac{975}{4096}$.

For a smooth plane curve of degree d we have $\gamma = d-1$ and $g = \frac{1}{2}(d-1)(d-2)$. From Gauss-Bonnet we get $g \leq \frac{1}{12}h + 1$ hence the inequality yields

$$\frac{1}{2}(d-1)(d-2) = g \leq \frac{1}{12}h + 1 \leq \frac{2(d-1)}{\alpha}.$$

so $d \leq \frac{4}{\alpha} + 2$, hence $d \leq 18$. Finally, the number of Γ of a given genus is finite, by [Cox, Parry, 1984]. □

Remark 5.3. Even if we knew Selberg's conjecture, that $\lambda_1 \geq \frac{1}{4}$, the bound on d would not improve.

Corollary 5.4.

Previous work - mention Abramovich, relate Selberg's inequality to the shortest geodesic (JJ), see if I have a better estimate for these families.

Maarten - The same arguments can also work to make the case in characteristic p (with Elisa's paper even shorter).

6. Canonical models

Noether-Enriques-Petri, work on models - Assaf, Box, Zywina

7. Smooth plane models

Brill-Noether, Green Theorem. Maybe go into more details here?

8. Involutions

Here I want to spend some time. Maybe prove Haruki-Kato-Komeda-Ohbuchi. Then we list all curves up to the bounds with genus and level.

There are a total of 8282 groups of Shimura type of level up to 2234 and genus up to 136. Restricting to genera which are triangular numbers, there are only 965 of these.

Main Point #1 : The involution test

Theorem 8.1 (Harui, Kato, Komeda, Ohbuchi, 2010)**.** *Let C be a smooth plane curve of degree d, σ an involution of C. Then σ has has either d or $d+1$ fixed points (whichever is even), and $\gamma(C/\sigma) = [d/2]$.*

Proof. Since C has a unique g^2_d, so σ extends to an automorphism of $\mathbb{P}^2$, which we may assume to be $diag(1,1,-1)$. Then the quotient $S = \mathbb{P}(1,1,2)$ embeds into $\mathbb{P}^3$ as a cone over the rational normal curve $[s:t:u] \mapsto (s^2 : st : t^2 : u)$ with vertex $[0:0:0:1]$. It is the image of the Hirzebruch surface $\mathbb{F}_2 = \mathbb{P}(O(2) \oplus O)$ under $\varphi_{e_2+2e_0}$ where e_2, e_0 form a basis for $\operatorname{Pic}\mathbb{F}_2$ with $e_0^2 = 0, e_2^2 = -2, e_2 \cdot e_0 = 1$. Let P_0 be the unique point of the fiber of Q_0 under π, and blow up $\mathbb{P}^2$ at P_0 to get $\mathbb{F}_1$. Identify the curve C with its strict transform, and note that it is the pullback of the quotient, and that e_2 pulls back to $2e_1$. If C passes through P_0, then $C \cdot e_1 = 1, C \cdot e_0 = d-1$, so that $C = (d-1)e_1 + de_0$, and otherwise $C \cdot e_1 = 0, C \cdot e_0 = d$, so that $C = de_1 + de_0$. But also if $\pi(C) \sim ae_2 + be_0$, then $C \simeq 2ae_1 + be_0$, hence $a = [d/2], b = d$. Using that $K_{\mathbb{F}_2} = -2e_2 - 4e_0$, and adjunction, get $2g(\pi(C)) - 2 = K(K + \pi(C))$, leading to $2g - 2 = [d/2](d-3) - 2$ if d is odd and $d(d/2-2)$ if d is even. From Riemann Hurwitz, we have that the number of fixed points is $f = 2g(C) - 2 - 2(2g-2)$, but $2g(C) = (d-1)(d-2)$, yielding the result. □

On these we can run the involution test for all Atkin-Lehner involutions, leaving us with 187 curves.

(Do I want to include the dihedral group action case? maybe)

Main Point #2: The supersingular point count gonality test

Leaving only 4 curves - $X_0(256), X_0(547), X_H(91, [27, 54])$ and $X_H(127, [27])$.

Point #3: Gonality bounds, reduction and Riemann-Roch spaces

For $X_0(547)$, Looking at the Atkin-Lehner quotient $Y = X_0(547)^+$, (a curve of genus 20), we can actually write down the equations for it. Doing that, reducing modulo 5, and counting points, we see that $\#Y(\mathbb{F}_5) = 33 > 5 \cdot 6 = 5\#\mathbb{P}^1(\mathbb{F}_5)$. In particular, it means that the $\mathbb{Q}$-gonality of Y is at least 6. We have to be careful here, because Theorem 4.3 shows only that the $\mathbb{C}$-gonality of Y is 5, but looking at the proof (Theorem 2.2. in Harui, Keto and Komeda), it seems that the gonal map can be written over the field of definition of the curve. (Their working assumption over $\mathbb{C}$ seems to be only required to allow for roots of unity of higher orders, i.e. $n > 2$). This should give us a contradiction.

For $X = X_H(91, [27, 54])$ we win for gonality reasons - we can compute that modulo 5 there is no function of degree at most 7 with at most one rational point in the fiber, and as $\#X(\mathbb{F}_5) = 6$, it follows that the gonality of the curve is at least 8. In particular, can't be a smooth plane curve fo degree 8.

For $X_0(256)$ we really need to bring out the big guns - compute the Betti numbers of the quotient under the Atkin-Lehner involution...