Classification of Genus 0 Modular Curves with a Rational Point

Rakvi

Cornell University

CTNT, June 2020

Let E be a non-CM elliptic curve over $\mathbb{Q}$. Let $N \geq 1$ be an integer. The natural action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $E[N] \subseteq E(\overline{\mathbb{Q}})$ gives a representation,

$$\rho_{E,N} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[N]) \simeq \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}).$$

By choosing compatible bases for $E[N]$ with $N \geq 1$, these representations combine to give a representation

$$\rho_E : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\hat{\mathbb{Z}}).$$

From Serre, we know that $\rho_E(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ is an open subgroup of $\mathrm{GL}_2(\hat{\mathbb{Z}})$ that has full determinant.

Hard Problem (Mazur's Program B)

Describe the possible images of ρ_E.

- Let G be an open subgroup of $\mathrm{GL}_2(\hat{\mathbb{Z}})$ such that $\det(G) = \hat{\mathbb{Z}}^*$ and $-I \in G$. We will assume these conditions on G unless otherwise mentioned. The level of G, is the smallest positive integer N such that G is the inverse image of its image under the projection map $\mathrm{GL}_2(\hat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$.
- Associated to G, there is a modular curve X_G which is a nice curve over $\mathbb{Q}$ with a morphism

$$\pi_G : X_G \to \mathbb{P}^1_{\mathbb{Q}}$$

which *loosely* parametrizes elliptic curves E such that $\rho_E(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ is contained in G^t.

For an elliptic curve E defined over $\mathbb{Q}$ such that $j(E) \notin \{0, 1728\}$, the group $\rho_E(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ is conjugate in $\mathrm{GL}_2(\hat{\mathbb{Z}})$ to a subgroup of G^t if and only if $j(E) \in \pi_G(X_G(\mathbb{Q}))$.

Recap: Given an open subgroup G of $\mathrm{GL}_2(\hat{\mathbb{Z}})$ that contains $-I$ and has full determinant, we can associate a pair (X_G, π_G) to it.

Problem

Give a classification of all genus 0 modular curves with a rational point.

There is a classification of genus 0 and genus 1 modular curves of prime power levels with infinitely many rational points due to Sutherland and Zywina.

Issue

There are infinitely many of them if we do not restrict the level!

Let us see a "quadratic family" of examples.

A family of Modular Curves

- Let d be a square free integer.
- For each d, there is an associated open index 2 subgroup G_d of $\mathrm{GL}_2(\hat{\mathbb{Z}})$ whose modular curve X_{G_d} is isomorphic to $\mathbb{P}^1_{\mathbb{Q}}$ with the associated morphism $\pi_{G_d} : X_{G_d} \to \mathbb{P}^1_{\mathbb{Q}}$ described by the rational function

$$\pi_{G_d}(t) = dt^2 + 1728.$$

Remark: Since any rational number is of the form $dt^2 + 1728$ for some $d, t \in \mathbb{Q}$, the representation ρ_E is never surjective. In particular, $\rho_E(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})) \subseteq G_d \subsetneq \mathrm{GL}_2(\hat{\mathbb{Z}})$ for some d.

A family of Modular Curves(contd.)

- The curves $\{(X_{G_d}, \pi_{G_d})\}_d$ are twists of each other, i.e., over $\mathbb{Q}(\sqrt{d})$ we have a commutative diagram

$$\begin{array}{ccc} X_{G_d} & \xrightarrow{\sim} & X_{G_1}. \\ & {\scriptstyle \pi_{G_d}} \searrow \quad \swarrow {\scriptstyle \pi_{G_1}} & \\ & \mathbb{P}^1_{\mathbb{Q}(\sqrt{d})} & \end{array}$$

- For each d, $G_d \cap \mathrm{SL}_2(\mathbb{Z})$ is the unique index 2 congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$.

Theorem (R.)

The genus 0 modular curves with a rational point lie in finitely many explicit families.

Cubic family of modular curves

- Let $v \in \mathbb{Q}$. Consider $X_v := \mathbb{P}^1_{\mathbb{Q}}$ with the morphism $\pi_v : X_v \to \mathbb{P}^1_{\mathbb{Q}}$ given by

$$\pi_v(t) = \frac{(-v+3)t^3 + (-3v^2+9v-9)t^2 + (-3v^3+9v^2-15v)t + (-v^4+3v^3-6v^2-v+3)}{t^3+2vt^2+(v^2+v-3)t+(v^2-3v+1)}.$$

- This describes a modular curve. Given a v, we can explicitly compute the group G_v corresponding to (X_v, π_v).
- Moreover, (X_v, π_v) is a twist of $(X_{3/2}, \pi_{3/2})$ over $\mathbb{Q}(\alpha)$ where α is a solution of the cubic equation $(T^3 - 3T + 1)/(T^2 - T) = v$.

Towards a definition of Modular Curves

We compute modular curves by computing their function fields.
Let $N \geq 1$ be an integer. Let $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ be a congruence subgroup.

- Let $\mathcal{H}^*$ be the extended upper half plane and X_Γ be the complex curve $\Gamma \setminus \mathcal{H}^*$. We will use the notation $X(N)$ for X_Γ when $\Gamma = \Gamma(N)$.
- Let $\mathcal{F}_N$ be the field of meromorphic functions on $X(N)$ whose q-expansions have coefficients in $K_N := \mathbb{Q}(\zeta_N)$.
- We have $\mathcal{F}_1 = \mathbb{Q}(j)$, where

$$j = q^{-1} + 744 + 196884q + 21493760q^2 + \cdots .$$

- If N' is a divisor of N then $\mathcal{F}_{N'} \subseteq \mathcal{F}_N$. In particular, we have that $\mathcal{F}_1 \subseteq \mathcal{F}_N$.

Towards a definition of Modular Curves

The following propeties hold.

- The field extension $\mathcal{F}_1 \subseteq \mathcal{F}_N$ is Galois and

$$\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\} \simeq \mathrm{Gal}(\mathcal{F}_N/\mathcal{F}_1)^{op}.$$

- The field K_N is algebraically closed in $\mathcal{F}_N$, i.e., $\overline{\mathbb{Q}} \cap \mathcal{F}_N = K_N$.

Towards a definition of Modular Curves

Let G be an open subgroup of $\mathrm{GL}_2(\hat{\mathbb{Z}})$. Let N be the level of G, i.e., N is the smallest positive integer such that G is the inverse image of its image under the projection map $\mathrm{GL}_2(\hat{\mathbb{Z}}) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$.

Definition

The modular curve X_G is the nice curve over $\mathbb{Q}$ with the function field $\mathcal{F}_N^G$.

Let $\pi_G : X_G \to \mathbb{P}^1_{\mathbb{Q}}$ be the morphism corresponding to the inclusion of fields $\mathcal{F}_1 \subseteq \mathcal{F}_N^G$.

For an elliptic curve E defined over $\mathbb{Q}$ such that $j(E) \notin \{0, 1728\}$, we have $\rho_E(\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}))$ is conjugate in $\mathrm{GL}_2(\hat{\mathbb{Z}})$ to a subgroup of G^t if and only if $j(E) \in \pi_G(X_G(\mathbb{Q}))$.

Congruence Subgroups

Let G be an open subgroup of $\mathrm{GL}_2(\hat{\mathbb{Z}})$.

- The subgroup $\Gamma := G \cap \mathrm{SL}_2(\mathbb{Z}) \subseteq \mathrm{SL}_2(\mathbb{Z})$ is a congruence subgroup of level $M|N$.
- The curve X_G over $\mathbb{C}$ is naturally isomorphic to the curve X_Γ.
- In particular, the genus of the curve X_Γ is equal to the genus of the curve X_G.
- For a given g there are only finitely many congruence subgroups $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ such that X_Γ has genus g.
  For $0 \leq g \leq 24$, a complete classification of these can be found in Cummins-Pauli database available at `http://www.uncg.edu/mat/faculty/pauli/congruence/`.
- However, recall that there may be infinitely many modular curves X_G of a given genus.

- In general, given a congruence subgroup $\Gamma \subseteq \mathsf{SL}_2(\mathbb{Z})$ containing $-I$ of index m and level M there may exist infinitely many $G \subseteq \mathsf{GL}_2(\hat{\mathbb{Z}})$ containing $-I$, $\det(G) = \hat{\mathbb{Z}}^\times$ of index m and level N which is a multiple of M such that $G \cap \mathsf{SL}_2(\mathbb{Z})$ is Γ.
- These curves are not all the same. In particular, the sets $\pi_G(X_G(\mathbb{Q}))$ and $\pi_{G'}(X_{G'}(\mathbb{Q}))$ differ.
- These pairs (X_G, π_G) are all twists of each other over cyclotomic extensions.

Idea of Classification

Step 0

Fix a genus 0 congruence subgroup $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ containing $-I$ of level M. Our goal is to compute all the pairs (X_G, π_G) such that X_G is $\mathbb{P}^1_{\mathbb{Q}}$ and $G \cap \mathrm{SL}_2(\mathbb{Z}) = \Gamma$.

Step 1

- We compute an explicit modular function $h \in \mathcal{F}_M$ such that $\mathbb{C}(X_\Gamma) = \mathbb{C}(h)$. Moreover, our h is a hauptmodul of Γ given explicitly in terms of Siegel functions.
- We compute the function $J_\Gamma \in K_M(t)$ which satisfies $J_\Gamma(h) = j$.
- This function describes the morphism $\pi_\Gamma : X_\Gamma \to \mathbb{P}^1$.

Idea of Classification

Step 2

We search for a modular curve (X_{G_0}, π_{G_0}) such that we have the following commutative diagram over K_N, where N is a multiple of M.

$$\begin{array}{ccc} \mathbb{P}^1_{K_N} & \xrightarrow{\quad f \quad} & (X_{G_0})_{K_N} \\ & {\scriptstyle \pi_\Gamma} \searrow \quad \swarrow {\scriptstyle \pi_{G_0}} & \\ & \mathbb{P}^1_{K_N} & \end{array}$$

The commutative diagram shown above gives us the following condition that f should satisfy

$$\sigma(\pi_\Gamma) = \pi_\Gamma \circ f^{-1} \circ \sigma(f)$$

for every $\sigma \in \mathrm{Gal}(K_N/\mathbb{Q})$.

Idea of Classification

Step 2 (contd.)

- The map $\zeta : \mathrm{Gal}(K_N/\mathbb{Q}) \to \mathrm{PGL}_2(K_N)$ given by $\zeta(\sigma) = f^{-1}\sigma(f)$ is a 1-cocycle and there are finitely many of them (with N fixed).
- The cocyle gives a twist $C/\mathbb{Q}$ of $\mathbb{P}^1_{\mathbb{Q}}$ that can be explicitly computed as a conic Q; we can check if it has a rational point.
- If Q has a rational point then, we compute a matrix $C \in \mathrm{PGL}_2(K)$ that realizes ζ as a coboundary. Composing C^{-1} with π_Γ gives us the element π_{G_0} corresponding to X_{G_0}.
- Moreover, We can also compute a set of generators for G_0 using the hauptmodul h and matrix C.

Idea of Classification

Step 3

We then search for modular curves (X_G, π_G) which become isomorphic to (X_{G_0}, π_{G_0}) over $\mathbb{Q}^{ab}$, where $\mathbb{Q}^{ab}$ is the maximal abelian extension of $\mathbb{Q}$.

$$\begin{array}{ccc} (X_{G_0})_{\mathbb{Q}^{ab}} & \xrightarrow{\quad f \quad} & (X_G)_{\mathbb{Q}^{ab}} \\ & {}_{\pi_{G_0}}\searrow \quad \swarrow_{\pi_G} & \\ & \mathbb{P}^1_{\mathbb{Q}^{ab}} & \end{array}$$

The commutative diagram shown above gives us the following condition that f should satisfy

$$\pi_{G_0} = \pi_{G_0} \circ f^{-1} \circ \sigma(f)$$

for every $\sigma \in \mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q})$.

Idea of Classification

The set $\mathrm{Aut}(X_G, \pi_G)$ is the group of all automorphisms of X_G which preserve the map π_G. The set $\mathrm{Aut}_{\mathbb{Q}}(X_G, \pi_G)$ is the group of all elements of $\mathrm{Aut}(X_G, \pi_G)$ defined over $\mathbb{Q}$.

Step 3 (contd.)

- There exists a finite number of twists (X_G, π_G) such that all the modular curves that are isomorphic to $\mathbb{P}^1_{\mathbb{Q}}$ and come from Γ are described by homomorphisms $\phi : \mathrm{Gal}(\mathbb{Q}^{ab}/\mathbb{Q}) \to \mathrm{Aut}_{\mathbb{Q}}(X_G, \pi_G)$.

The cubic family of modular curves discussed before arises when $\mathrm{Aut}_{\mathbb{Q}}(X_G, \pi_G)$ is described by $\{t, -1/(t-1), (t-1)/t\}$.
We will use the notation $\mathcal{A}$ for $\mathrm{Aut}_{\mathbb{Q}}(X_G, \pi_G)$.

Theorem (R.)

Our classification breaks down as following:

- *There are 31 families of genus 0 modular curves with a rational point described by* $\mathcal{A} = \{t\}$.
- *There are 145 families of genus 0 modular curves with a rational point described by* $\mathcal{A} = \{t, -t\}$ *which is cyclic of order 2.*
- *There are 27 families of genus 0 modular curves with a rational point described by* $\mathcal{A} = \{t, \alpha/t\}$ *(cyclic of order 2), where* α *is a non-zero rational number which is not a square.*
- *There are 8 families of genus 0 modular curves with a rational point described by* $\mathcal{A} = \{t, -1/(t-1), (t-1)/t\}$ *which is cyclic of order 3.*

- There are 17 families of genus 0 modular curves with a rational point described by $\mathcal{A} = \{t, -1/t, (-t-1)/(t-1), (t-1)/(t+1)\}$ which is cyclic of order 4.
- There are 57 families of genus 0 modular curves with a rational point described by $\mathcal{A}$ which is isomorphic to Klein-4 group.

Examples of non conjugate Klein-4 groups are
$\mathcal{A} = \{t, \alpha/t, -t, -\alpha/t\}$, where α is a non-zero rational number,
$\mathcal{A} = \{t, -1/t, (t+1)/(t-1), (-t+1)/(t+1)\}$,
$\mathcal{A} = \{t, -1/(5t), (-t+1)/(5t+1), (t+1/5)/(t-1)\}$.

THANK YOU

Thank you for listening.