Equations for modular curves

Eran Assaf

Dartmouth College

Dartmouth Algebra and Number Theory Seminar, October 2020

Elliptic Curves

Over $\mathbb{Q}$

Theorem (Mordell, [Mor22])

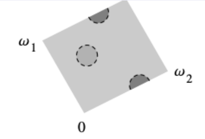
$E : y^2 = f(x)$, $f(x) \in \mathbb{Q}[x] \Rightarrow E(\mathbb{Q})$ *is finitely generated.*

- $\mathrm{rank}(E(\mathbb{Q})) = ?$
- $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts on $E(\bar{\mathbb{Q}})$.
- $\rho_{E,p} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to GL(E[p]) \cong GL_2(\mathbb{F}_p)$.

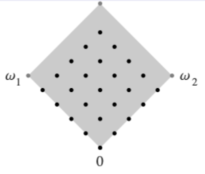
Question

What can we say about $\rho_{E,p}$ *?*

$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$



$E[5]$



Elliptic Curves

Theorem (Serre's Open Image Theorem, [Ser72])

E defined over $\mathbb{Q}$ without complex multiplication. Then $[GL_2(\mathbb{F}_p) : \operatorname{Im} \rho_{E,p}] \leqslant c_E$.

Conjecture (Serre's uniformity conjecture, [Ser72])

$\exists c$, independent of E, such that $[GL_2(\mathbb{F}_p) : \operatorname{Im} \rho_{E,p}] \leqslant c$.

Maximal subgroups of $PGL_2(\mathbb{F}_p)$

- Borel subgroups - $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$
- Normalizer of a split Cartan - $\begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}$
- Normalizer of a non-split Cartan - $\mathbb{F}_{p^2}^{\times} \hookrightarrow GL_2(\mathbb{F}_p)$
- Exceptional - A_4, S_4, A_5

Modular Curves

Moduli Spaces

$$SL_2(\mathbb{Z})\backslash\mathcal{H} \xrightarrow{\sim} \{\Lambda \subseteq \mathbb{C}\}/\sim \longrightarrow \{\text{Elliptic curves over } \mathbb{C}\}/\sim$$

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

- $Y_\Gamma(\mathbb{C}) = \Gamma\backslash\mathcal{H}$, $\Gamma \subseteq SL_2(\mathbb{Z})$
- $X_\Gamma(\mathbb{C}) = \Gamma\backslash\mathcal{H}^*$

Cusps

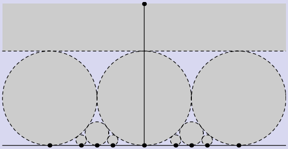
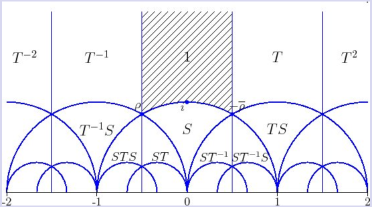


Figure 2.5. Neighborhoods of ∞ and of some rational points

$SL_2(\mathbb{Z})\backslash\mathcal{H}$



Modular Curves

Moduli Spaces Over $\bar{\mathbb{Q}}$

$$H \subseteq GL_2(\mathbb{Z}/N\mathbb{Z}), \phi : E[N] \to \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$$
$$(E, \phi) \sim_H (E', \phi') \iff \exists h \in H, \iota : E \to E' \text{ s.t. } h \circ \phi = \phi' \circ \iota$$

- $S(H) = \{(E, \phi)\}/ \sim_H$
- $(E, \phi)^\sigma = (E^\sigma, \phi \circ \sigma^{-1}) \quad \sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$
- (E, ϕ) rational iff E rational and $\phi \circ \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \circ \phi^{-1} \subseteq H$
- $\Gamma_H \subseteq SL_2(\mathbb{Z})$, $Y_{\Gamma_H} = S(H)$

Congruence subgroups

- $\Gamma(N) = \ker(SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/N\mathbb{Z}))$
- Borel - $\Gamma_0(N)$
- Normalizer of split (non-split) Cartan - $\Gamma_s^+(N)$, $\Gamma_{ns}^+(N)$

Theorem (Serre, [Ser72])

For $p > 13$, $H \subseteq GL_2(\mathbb{F}_p)$ exceptional, the modular curve X_{Γ_H} has no rational points.

Theorem (Mazur, [Maz77])

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

Theorem (Bilu, Parent, Rebolledo, [BPR13])

For $p > 13$, the modular curve $X_s^+(p)$ has no non-CM, non-cuspidal rational points.

Conjecture (Serre's uniformity conjecture)

For $p > 11$, the only $\mathbb{Q}$-points of the modular curve $X_{ns}^+(p)$ are CM.

Numerical Evidence

Theorem (Balakrishnan, Dogra, Müller, Tuitman, Vonk, [BDM+19])

The modular curve $X_{ns}^{+}(13)$ has exactly 7 rational points, all of which are CM.

Theorem (Mercuri, Schoof, [MS20])

For $p = 17, 19, 23$, there are no "small" rational points on $X_{ns}^{+}(p)$, other than the seven CM points.

Explicit equations

Theorem (Baran, [Bar14])

The modular curve $X_{ns}^{+}(13)$ is defined by the equation

$$(-y - z)x^3 + (2y^2 + zy)x^2 +$$
$$(-y^3 + zy^2 - 2z^2y + z^3)x + (2z^2y^2 - 3z^3y) = 0.$$

Equations and the canonical map

Theorem (Petri's Theorem*)

X curve over k of genus g. $\omega_1, \ldots, \omega_g \in H^0(X, \Omega^1)$ define

$$(\omega_1, \ldots, \omega_g) : \varphi : X \to \mathbb{P}^{g-1}.$$

If X is not hyperelliptic, φ is an embedding. Let $I(X) = \bigoplus_{d=0}^{\infty} I_d(X)$ be the ideal of relations. Then

1. $\dim_k I_2(X) = (g-2)(g-3)/2$ *and* $\dim_k I_3(X) = (g-3)(g^2+6g-10)/6$.
2. *If $g \geqslant 4$, $I(X)$ is generated by $I_2(X)$ and $I_3(X)$.*
3. *If $g = 3$, $I(X)$ is generated by $I_4(X)$ and $\dim_k I_4(X) = 1$.*

Strategy

Compute a basis for $H^0(X, \Omega^1)$, look for enough polynomial relations of small degrees.

Modular Forms

weight k action

$\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$, $f : \mathcal{H} \to \mathbb{C}$

$$f|_{[\alpha]_k}(z) = (cz+d)^{-k} f(\alpha z).$$

Definition (Modular form of weight k for Γ)

$f : \mathcal{H} \to \mathbb{C}$ holomorphic s.t. $f|_{[\gamma]_k} = f$ for all $\gamma \in \Gamma$ and $f|_{[\alpha]_k}$ is holomorphic at ∞ for all $\alpha \in SL_2(\mathbb{Z})$.

q-expansion

If $\Gamma(N) \subseteq \Gamma$, $\begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix} \in \Gamma$, $f(z+N) = f(z)$, so

$$f(z) = \sum_{n=0}^{\infty} a_n q_N^n \quad q_N = e^{\frac{2\pi i z}{N}}.$$

Modular forms as differentials

Holomorphic differentials

- $\mathcal{A}_k(\Gamma) = \pi^\star \Omega_{mer}^{\otimes k/2}(X_\Gamma)$ $(\pi : \mathcal{H}^* \to X_\Gamma)$
- $\mathcal{M}_K(\Gamma) \cong H^0(X_\Gamma, \Omega^1(\Delta)^{\otimes k/2})$, $\mathcal{S}_k(\Gamma) \cong H^0(X_\Gamma, \Omega^{\otimes k/2})$
- $\mathcal{S}_2(\Gamma) \cong \Omega^1_{hol}(X_\Gamma)$, $(\omega_1, \ldots, \omega_g) : X_\Gamma \to \mathbb{P}^{g-1}$

Example

- $G_k(\tau) = \sum'_{(c,d)} \frac{1}{(c\tau+d)^k} \in \mathcal{M}_k(SL_2(\mathbb{Z}))$
- Fourier expansion - $G_k(\tau) = 2\zeta(k) \cdot \left(1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n\right)$
- $\dim \mathcal{M}_8(SL_2(\mathbb{Z})) = 1 \Rightarrow G_8 = C \cdot G_4^2$
- $\Delta(\tau) = (60 G_4(\tau))^3 - 27(140 G_6(\tau))^2 \in \mathcal{S}_{12}(SL_2(\mathbb{Z}))$
- $j(\tau) = 1728 \frac{(60 G_4(\tau))^3}{\Delta(\tau)} \in \mathcal{A}_0(SL_2(\mathbb{Z}))$

Computing q-expansions

Theorem ([MS20], [Zyw20])

Let $G \subseteq GL_2(\mathbb{Z}/N\mathbb{Z})$ be s.t. $-1 \in G$ and $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$. Then $X_G = X_{\Gamma_G}$ is defined over $\mathbb{Q}$ and

$$\mathcal{S}_k(\Gamma(N), \mathbb{Q}(\zeta_N))^G \cong \mathcal{S}_k(\Gamma, \mathbb{Q}).$$

Action on cusp forms

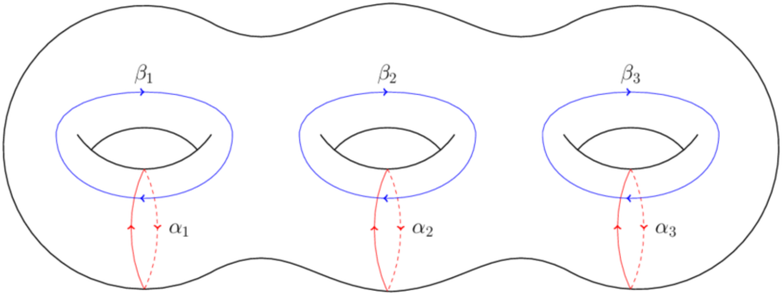
Zywina [Zyw20] computes the action of $GL_2(\mathbb{Z}/N\mathbb{Z})$ on q-expansions. Computes a basis for $\mathcal{S}_2(\Gamma(N), \mathbb{Q}(\zeta_N))^G$.

Issues

- The space $\mathcal{S}_2(\Gamma(N), \mathbb{Q}(\zeta_N))$ is much larger than $\mathcal{S}_2(\Gamma, \mathbb{Q})$.
- Uses numerical approximation with large denominators.

Modular Symbols

$H_1(X_0(39), \mathbb{Z})$



- $H_1(X_\Gamma; \mathbb{R}) = \Omega^1_{hol}(X_\Gamma)^\vee$
- $\{z_1, z_2\} \mapsto \left(\omega \mapsto \int_{z_1}^{z_2} \omega\right)$
- $\{z_1, z_2\} + \{z_2, z_3\} + \{z_3, z_1\} = 0$
- $\{z_1, z_1\} = 0$
- $\langle \{\alpha z_1, \alpha z_2\}, \omega \rangle = \langle \{z_1, z_2\}, \omega \circ \alpha \rangle$

Modular Symbols

Modular Symbols

- $F = \bigoplus_{\alpha,\beta\in\mathbb{P}^1(\mathbb{Q})} \mathbb{Z}\cdot\{\alpha,\beta\}$, $R = \{\alpha,\beta\}+\{\beta,\gamma\}+\{\gamma,\alpha\}$
- $\mathbb{M}_2 = (F/R)/(F/R)_{\mathrm{tor}}$
- $\mathbb{M}_k = \mathbb{Z}[X,Y]_{k-2}\otimes\mathbb{M}_2$
- $\mathbb{M}_k(\Gamma) = (\mathbb{M}_k)_\Gamma$ modulo torsion.

Example

$X^3\otimes\{0,1/2\} - 17XY^2\otimes\{\infty,1/7\}\in\mathbb{M}_5$

Theorem (Manin, [Man72])

$\varphi : \mathbb{M}_2(\Gamma)\to H_1(X_\Gamma, cusps, \mathbb{Z})$ *is an isomorphism.*

Modular Symbols

Pairing with modular forms

$$\left(\mathcal{S}_k(\Gamma) \oplus \bar{\mathcal{S}}_k(\Gamma)\right) \times \mathbb{M}_k(\Gamma) \to \mathbb{C}$$

$$\langle (f_1, f_2), P\{\alpha, \beta\} \rangle = \int_\alpha^\beta f_1(z) P(z,1) dz + \int_\alpha^\beta f_2(z) P(\bar{z}, 1) d\bar{z}$$

Cuspidal modular symbols

- $\mathbb{B}_2 = \bigoplus_{\alpha \in \mathbb{P}^1(\mathbb{Q})} \mathbb{Z} \cdot \{\alpha\}$, $\mathbb{B}_k = \mathbb{Z}[X, Y]_{k-2} \otimes \mathbb{B}_2$
- $\mathbb{B}_k(\Gamma) = (\mathbb{B}_k)_\Gamma$ modulo torsion.
- $\mathbb{S}_k(\Gamma) = \ker(\partial : \mathbb{M}_k(\Gamma) \to \mathbb{B}_k(\Gamma))$

Theorem (Shokurov, [Sho80] + Merel, [Mer94])

The pairing

$$\langle \cdot, \cdot \rangle : \left(\mathcal{S}_k(\Gamma) \oplus \bar{\mathcal{S}}_k(\Gamma)\right) \times \mathbb{S}_k(\Gamma; \mathbb{C}) \to \mathbb{C}$$

is a nondegenerate pairing of complex vector spaces

Modular Symbols

Manin symbols

$$[P, \Gamma g] = g(P\{0, \infty\}) \in \mathbb{M}_k(\Gamma)$$

- $\left\{\left[X^{k-2-i}Y^i, \Gamma g\right]\right\}_{i=0, g \in \Gamma \backslash SL_2(\mathbb{Z})}^{k-2}$ generate $\mathbb{M}_k(\Gamma)$.
- $x + xS = 0$, $x + x(ST) + x(ST)^2 = 0$, $x - xJ = 0$
- Great for computation!
- Can compute the vector space $\mathbb{S}_k(\Gamma) = \left(\mathcal{S}_k(\Gamma) \oplus \bar{\mathcal{S}}_k(\Gamma)\right)^\vee$.
- If Γ is of real type, $\mathcal{S}_k(\Gamma) = (\mathbb{S}_k(\Gamma)^+)^\vee$, so also $\mathcal{S}_k(\Gamma)$.

That's great, but what about q-expansions?

Twisting method

Definition (twist of a modular form)

Let $f = \sum_{n=0}^{\infty} a_n q^n$, $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}$ *primitive. Write*

$$f_\chi = \sum_{n=1}^{\infty} a_n \chi(n) q^n.$$

Let

$$S_N = \begin{pmatrix} N & 1 \\ 0 & N \end{pmatrix}, \quad R_\chi = \sum_{u \bmod N} \overline{\chi}(u) S_N^u.$$

Then $R_\chi(f) = g(\overline{\chi}) \cdot f_\chi$.

Theorem (Atkin, Li, [A+78] + Box [Box20])

Let $V \subseteq S_2(\Gamma(N), \mathbb{Q}(\zeta_N))$ *be an irrep of* $GL_2(\mathbb{Z}/N\mathbb{Z})$*. Then there exists a newform* f *such that* V *is spanned by* $\{R_\chi \circ \alpha_d(f)\}_{\chi,d}$.

From modular symbols to q-expansions

Twisting modular symbols

Box in [Box20] computes $\mathbb{S}_2(\Gamma(N))^G \cap V_i$ for each irrep. V_i, finds the newform f_i, and thus computes a basis of q-expansions.

Working directly with Γ

- In [Ass20], can compute* Hecke operators for $\mathbb{S}_k(\Gamma)$.
- Finds systems of eigenvalues.
- Computes the action of Hecke operators on the q-expansions at all the cusps.
- In particular, recovers the above elements f_i.
- Given a q-expansion, can compute the period map.
- Also computes Eisenstein series - could that be of use?

Demonstration...

Thanks for listening!

A Oliver L Atkin et al.
Twists of newforms and pseudo-eigenvalues ofw-operators.
Inventiones mathematicae, 48(3):221–243, 1978.

Eran Assaf.
Computing classical modular forms for arbitrary congruence subgroups.
arXiv preprint arXiv:2002.07212, 2020.

Burcu Baran.
An exceptional isomorphism between modular curves of level 13.
Journal of Number Theory, 145:273–300, 2014.

Jennifer S Balakrishnan, Netan Dogra, J Steffen Müller, Jan Tuitman, and Jan Vonk.
Explicit chabauty—kim for the split cartan modular curve of level 13.
Annals of mathematics, 189(3):885–944, 2019.

Josha Box.

q-expansions of modular forms for general congruence subgroups using twist orbits.
to be published, 2020.

Yuri Bilu, Pierre Parent, and Marusia Rebolledo.
Rational points on $x_0^+(p^r)$.
In *Annales de l'Institut Fourier*, volume 63, pages 957–984, 2013.

Ju I Manin.
Parabolic points and zeta-functions of modular curves.
Mathematics of the USSR-Izvestiya, 6(1):19, 1972.

Barry Mazur.
Rational points on modular curves.
In *Modular functions of one variable V*, pages 107–148. Springer, 1977.

Loïc Merel.
Universal Fourier expansions of modular forms.

In *On Artin's Conjecture for Odd 2-Dimensional Representations*, pages 59–94. Springer, 1994.

Louis Mordell.
On the rational solutions of the indeterminate equation of the third and fourth degree.
In *Proc. Camb. Phil. Soc.*, volume 21, pages 179–192, 1922.

Pietro Mercuri and René Schoof.
Modular forms invariant under non-split Cartan subgroups.
Mathematics of Computation, 89(324):1969–1991, 2020.

Jean-Pierre Serre.
Propriétés galoisiennes des points d'ordre fini des courbes elliptiques.
Invent. math, 15:259–331, 1972.

Vyacheslav Vladimirovich Shokurov.
The study of the homology of Kuga varieties.
Izvestiya Rossiiskoi Akademii Nauk. Seriya Matematicheskaya, 44(2):443–464, 1980.

David Zywina.
Computing actions on cusp forms.
arXiv preprint arXiv:2001.07270, 2020.