Computing modular forms

Eran Assaf

Dartmouth College

Québec Vermont Number Theory Seminar, February 2020

Structure of the talk

Structure of the talk

1. Elliptic Curves

Structure of the talk

1. Elliptic Curves
2. Modular Forms

Structure of the talk

1. Elliptic Curves
2. Modular Forms
3. Results

Structure of the talk

1. Elliptic Curves
2. Modular Forms
3. Results
4. Modular Symbols

Structure of the talk

1. Elliptic Curves
2. Modular Forms
3. Results
4. Modular Symbols
5. Hecke Operators

Structure of the talk

1. Elliptic Curves
2. Modular Forms
3. Results
4. Modular Symbols
5. Hecke Operators
6. Computational Aspects

Elliptic Curves

Diophantine Equations

Elliptic Curves

Diophantine Equations

- $x^2 + y^2 = z^2$ - Babylonians, Euclid

Elliptic Curves

Diophantine Equations

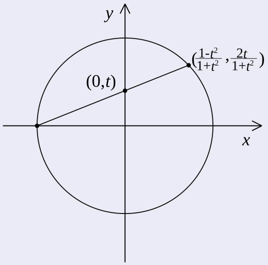
- $x^2 + y^2 = z^2$ - Babylonians, Euclid
- $ax^2 + by^2 + cz^2 + dxy + eyz + fzx = 0$

Elliptic Curves

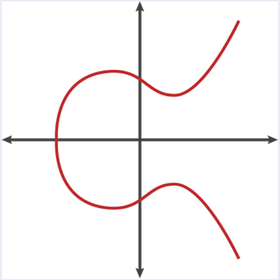
Diophantine Equations

- $x^2 + y^2 = z^2$ - Babylonians, Euclid
- $ax^2 + by^2 + cz^2 + dxy + eyz + fzx = 0$
- $y^2 = ax^3 + bx^2 + cx + d$

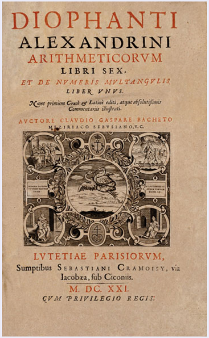
Rational Parameterization



Elliptic Curves



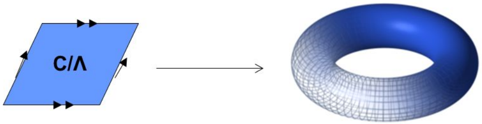
Arithmetica


DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX,
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
Nunc primum Græcè & Latinè editi, atque absolutissimis Commentariis illustrati.
AVCTORE CLAVDIO GASPARE BACHETO
LVTETIAE PARISIORVM,
Sumptibus SEBASTIANI CRAMOISY, via Iacobæa, sub Ciconiis.
M. DC. XXI.
CVM PRIVILEGIO REGIS.

Elliptic Curves

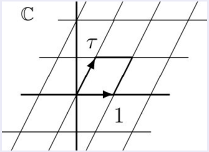
Over $\mathbb{C}$

Elliptic Curves over Complex Numbers

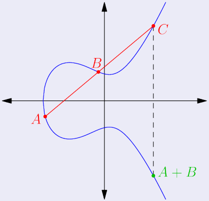


$$\mathbb{C}/\Lambda \longrightarrow E : y^2 = x^3 + Ax + B$$
$$z \longmapsto (\wp(z), -\wp'(z)/2)$$

$\Lambda = \mathbb{Z} + \mathbb{Z}\tau$



Addition Law



Elliptic Curves

Over $\mathbb{Q}$

Theorem (Mordell, 1922)

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

Elliptic Curves

Over $\mathbb{Q}$

Theorem (Mordell, 1922)

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

- $\text{rank}(E(\mathbb{Q})) = \ ?$

Elliptic Curves

Over $\mathbb{Q}$

Theorem (Mordell, 1922)

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

- $\text{rank}(E(\mathbb{Q})) = ?$
- $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts on $E(\bar{\mathbb{Q}})$.

Elliptic Curves

Over $\mathbb{Q}$

Theorem (Mordell, 1922)

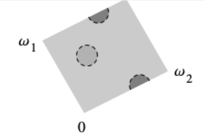
$E : y^2 = f(x)$, $f(x) \in \mathbb{Q}[x] \Rightarrow E(\mathbb{Q})$ is finitely generated.

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

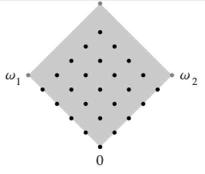
Question

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, 1972)

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, 1972)

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

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

Elliptic Curves

Theorem (Serre's Open Image Theorem, 1972)

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, 1972)

$\exists c$, 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 - $\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}$

Elliptic Curves

Theorem (Serre's Open Image Theorem, 1972)

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, 1972)

$\exists c$, 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 - $\begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix}$

Elliptic Curves

Theorem (Serre's Open Image Theorem, 1972)

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, 1972)

$\exists c$, 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 - $\mathbb{F}_{p^2}^\times \hookrightarrow GL_2(\mathbb{F}_p)$

Elliptic Curves

Theorem (Serre's Open Image Theorem, 1972)

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, 1972)

$\exists c$, *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

$$SL_2(\mathbb{Z})\backslash\mathcal{H} \xrightarrow{\sim} \{\Lambda \subseteq \mathbb{C}\}/\sim \longrightarrow \{\text{Elliptic curves over } \mathbb{C}\}/\sim$$
$$\tau \mapsto \Lambda_\tau = \mathbb{Z}\tau + \mathbb{Z} \mapsto E_\tau = \mathbb{C}/\Lambda_\tau$$

Modular Curves

Moduli Spaces

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

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

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

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

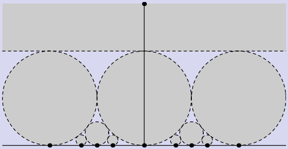
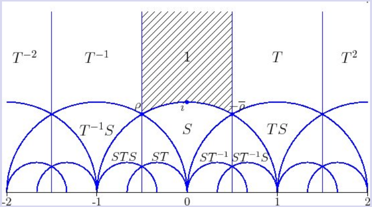


Figure 2.5. Neighborhoods of ∞ and of some rational points

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



Modular Curves

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

$H \subseteq GL_2(\mathbb{Z}/N\mathbb{Z}), \phi : E[N] \to \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$

$(E, \phi) \sim_H (E', \phi') \iff \exists h \in H, \iota : E \to E' \text{ s.t. } h \circ \phi = \phi' \circ \iota$

Modular Curves

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

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

- $S(H) = \{(E, \phi)\}/ \sim_H$

Modular Curves

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

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

- $S(H) = \{(E, \phi)\}/ \sim_H$
- $(E, \phi)^\sigma = (E^\sigma, \phi \circ \sigma^{-1}) \quad \sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$

Modular Curves

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

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

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

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

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

- $\Gamma(N) = \ker(SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/N\mathbb{Z}))$

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 - $\Gamma_0(p)$

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 - $\Gamma_0(p)$
- Normalizer of split (non-split) Cartan - $\Gamma_s^+(p)$, $\Gamma_{ns}^+(p)$

Theorem (Serre, 1972)

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

Theorem (Mazur, 1978)

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

Theorem (Bilu, Parent, Rebolledo, 2011)

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, 2017)

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

Theorem (Mercuri, Schoof, 2018)

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, 2014)

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

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

Modular Forms

Meromorphic differentials

Modular Forms

Meromorphic differentials

- $\mathcal{A}_k(\Gamma) = \pi^\star \Omega^{\otimes k/2}(X_\Gamma)$

Modular Forms

Meromorphic differentials

- $\mathcal{A}_k(\Gamma) = \pi^\star \Omega^{\otimes k/2}(X_\Gamma)$
- Holomorphic - $\mathcal{M}_k(\Gamma)$, Cuspidal - $\mathcal{S}_k(\Gamma)$

Modular Forms

Meromorphic differentials

- $\mathcal{A}_k(\Gamma) = \pi^\star \Omega^{\otimes k/2}(X_\Gamma)$
- Holomorphic - $\mathcal{M}_k(\Gamma)$, Cuspidal - $\mathcal{S}_k(\Gamma)$
- $\mathcal{S}_2(\Gamma) \cong \Omega^1_{hol}(X_\Gamma)$, $(\omega_1, \ldots, \omega_g) : X(\Gamma) \to \mathbb{P}^{g-1}$

Example

Modular Forms

Meromorphic differentials

- $\mathcal{A}_k(\Gamma) = \pi^\star \Omega^{\otimes k/2}(X_\Gamma)$
- Holomorphic - $\mathcal{M}_k(\Gamma)$, Cuspidal - $\mathcal{S}_k(\Gamma)$
- $\mathcal{S}_2(\Gamma) \cong \Omega^1_{hol}(X_\Gamma)$, $(\omega_1, \dots, \omega_g) : X(\Gamma) \to \mathbb{P}^{g-1}$

Example

- $G_k(\tau) = \sum'_{(c,d)} \frac{1}{(c\tau+d)^k} \in \mathcal{M}_k(SL_2(\mathbb{Z}))$

Modular Forms

Meromorphic differentials

- $\mathcal{A}_k(\Gamma) = \pi^\star \Omega^{\otimes k/2}(X_\Gamma)$
- Holomorphic - $\mathcal{M}_k(\Gamma)$, Cuspidal - $\mathcal{S}_k(\Gamma)$
- $\mathcal{S}_2(\Gamma) \cong \Omega^1_{hol}(X_\Gamma)$, $(\omega_1, \ldots, \omega_g) : X(\Gamma) \to \mathbb{P}^{g-1}$

Example

- $G_k(\tau) = \sum'_{(c,d)} \frac{1}{(c\tau+d)^k} \in \mathcal{M}_k(SL_2(\mathbb{Z}))$
- Fourier expansion - $G_k(\tau) = 2\zeta(k) \cdot \left(1 - \frac{2k}{B_k} \sum_{n=1}^\infty \sigma_{k-1}(n) q^n\right)$

Modular Forms

Meromorphic differentials

- $\mathcal{A}_k(\Gamma) = \pi^\star \Omega^{\otimes k/2}(X_\Gamma)$
- Holomorphic - $\mathcal{M}_k(\Gamma)$, Cuspidal - $\mathcal{S}_k(\Gamma)$
- $\mathcal{S}_2(\Gamma) \cong \Omega^1_{hol}(X_\Gamma)$, $(\omega_1, \ldots, \omega_g) : X(\Gamma) \to \mathbb{P}^{g-1}$

Example

- $G_k(\tau) = \sum'_{(c,d)} \frac{1}{(c\tau+d)^k} \in \mathcal{M}_k(SL_2(\mathbb{Z}))$
- Fourier expansion - $G_k(\tau) = 2\zeta(k) \cdot \left(1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n\right)$
- $\dim \mathcal{M}_8(SL_2(\mathbb{Z})) = 1 \Rightarrow G_8 = C \cdot G_4^2$

Modular Forms

Meromorphic differentials

- $\mathcal{A}_k(\Gamma) = \pi^\star \Omega^{\otimes k/2}(X_\Gamma)$
- Holomorphic - $\mathcal{M}_k(\Gamma)$, Cuspidal - $\mathcal{S}_k(\Gamma)$
- $\mathcal{S}_2(\Gamma) \cong \Omega^1_{hol}(X_\Gamma)$, $(\omega_1, \ldots, \omega_g) : X(\Gamma) \to \mathbb{P}^{g-1}$

Example

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

Modular Forms

Meromorphic differentials

- $\mathcal{A}_k(\Gamma) = \pi^\star \Omega^{\otimes k/2}(X_\Gamma)$
- Holomorphic - $\mathcal{M}_k(\Gamma)$, Cuspidal - $\mathcal{S}_k(\Gamma)$
- $\mathcal{S}_2(\Gamma) \cong \Omega^1_{hol}(X_\Gamma)$, $(\omega_1, \ldots, \omega_g) : X(\Gamma) \to \mathbb{P}^{g-1}$

Example

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

Results

Problem

Given a group $H \subseteq GL_2(\mathbb{Z}/N\mathbb{Z})$, an integer $k \geqslant 2$ and a positive integer L, find the q-expansion of a basis for $S_k(\Gamma_H)$ up to precision q^L. (Known for $\Gamma_0(N), \Gamma_1(N)$ - Stein, Cremona)

Theorem (A., 2020)

There exists an algorithm that given a group $H \subseteq GL_2(\mathbb{Z}/N\mathbb{Z})$ satisfying (*), an integer $k \geqslant 2$, and a positive integer L, returns the q-expansions of a basis of $S_k(\Gamma_H)$ up to precision q^L.

Corollary (Banwait, Cremona, 2014)

The modular curve $X_{S_4}(13)$ is a genus 3 curve whose canonical embedding in $\mathbb{P}^2_{\mathbb{Q}}$ has the model

$$4x^3y - 3x^2y^2 + 3xy^3 - x^3z + 16x^2yz - 11xy^2z + \\ +5y^3z + 3x^2z^2 + 9xyz^2 + y^2z^2 + xz^3 + 2yz^3 = 0.$$

Results

Corollary (Baran, 2014)

The modular curves $X_{ns}^{+}(13)$ and $X_{s}^{+}(13)$ are defined by the equation

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

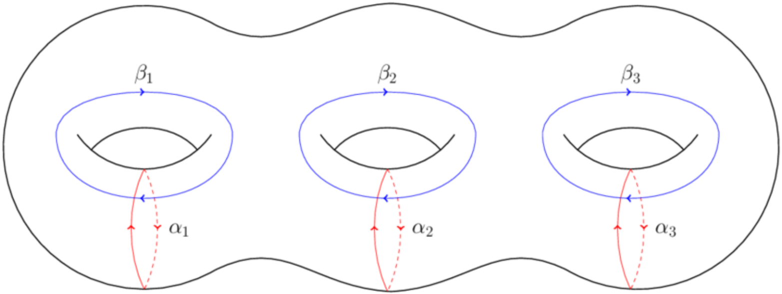
Similar results for $X_{ns}^{+}(17), X_{ns}^{+}(19)$ and $X_{ns}^{+}(23)$.

Corollary (A., 2020)

The Jacobian of the modular curve $X_{ns}^{+}(97)$ decomposes as the direct sum of 13 Hecke irreducible subspaces, of dimensions $3, 4, 4, 6, 7, 7, 12, 14, 24, 24, 24, 56, 168$. *In particular, it has no elliptic curve factor.*

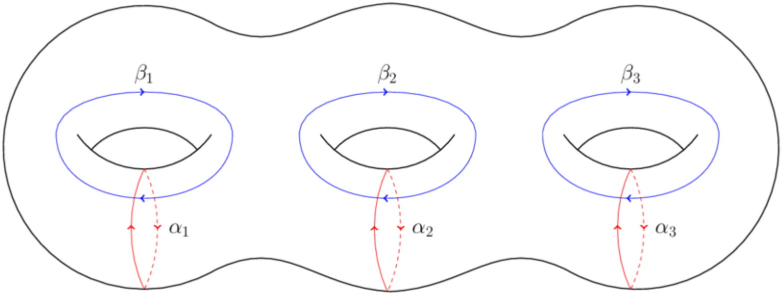
Modular Symbols

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



Modular Symbols

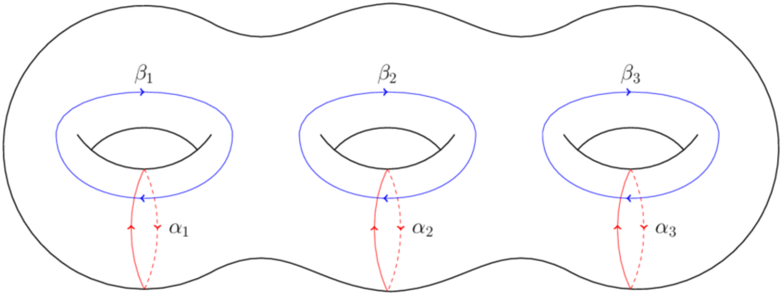
$H_1(X_0(39), \mathbb{Z})$



- $H_1(X_\Gamma; \mathbb{R}) = \Omega^1_{hol}(X_\Gamma)^\vee$

Modular Symbols

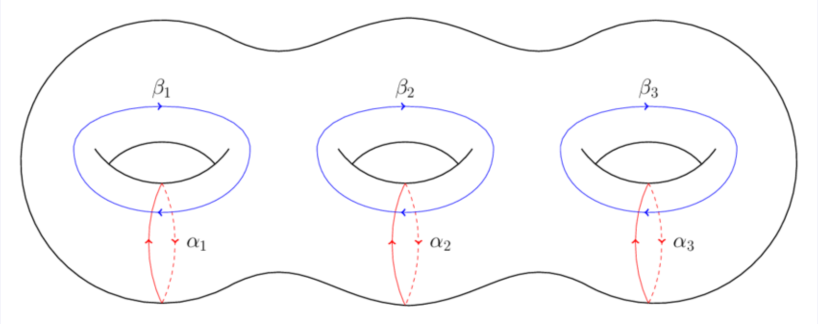
$H_1(X_0(39), \mathbb{Z})$



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

Modular Symbols

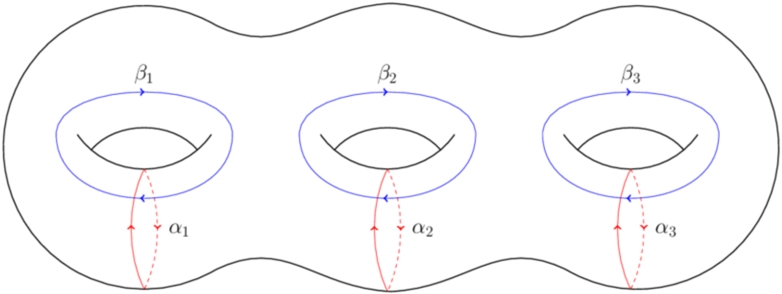
$H_1(X_0(39), \mathbb{Z})$



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

Modular Symbols

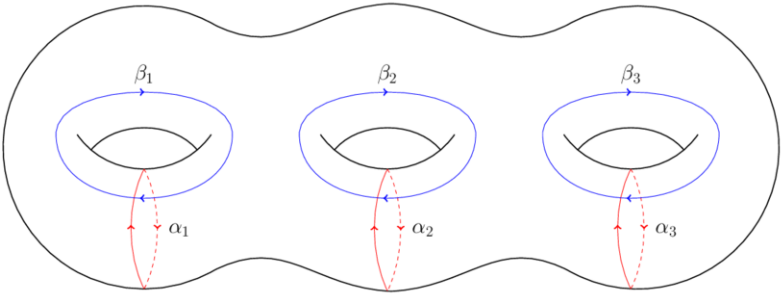
$H_1(X_0(39), \mathbb{Z})$



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

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

Modular Symbols

Modular Symbols

- $F = \bigoplus_{\alpha,\beta \in \mathbb{P}^1(\mathbb{Q})} \mathbb{Z} \cdot \{\alpha, \beta\}$, $R = \{\alpha, \beta\} + \{\beta, \gamma\} + \{\gamma, \alpha\}$

Modular Symbols

Modular Symbols

- $F = \bigoplus_{\alpha,\beta \in \mathbb{P}^1(\mathbb{Q})} \mathbb{Z} \cdot \{\alpha, \beta\}$, $R = \{\alpha, \beta\} + \{\beta, \gamma\} + \{\gamma, \alpha\}$
- $\mathbb{M}_2 = (F/R)/(F/R)_{\text{tor}}$

Modular Symbols

Modular Symbols

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

Modular Symbols

Modular Symbols

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

Example

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

Theorem (Manin, 1972)

$\varphi : \mathbb{M}_2(\Gamma) \to H_1(X_\Gamma, cusps, \mathbb{Z})$ 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

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

- $\mathbb{B}_2 = \bigoplus_{\alpha \in \mathbb{P}^1(\mathbb{Q})} \mathbb{Z} \cdot \{\alpha\}$, $\mathbb{B}_k = \mathbb{Z}[X, Y]_{k-2} \otimes \mathbb{B}_2$

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.

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, 1980 + Merel, 1994)

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

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

Modular Symbols

Manin symbols

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

- $\{[X^{k-2-i}Y^i, \Gamma g]\}_{i=0, g \in \Gamma \backslash SL_2(\mathbb{Z})}^{k-2}$ generate $\mathbb{M}_k(\Gamma)$.

Modular Symbols

Manin symbols

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

- $\{[X^{k-2-i}Y^i, \Gamma g]\}_{i=0, g \in \Gamma \backslash SL_2(\mathbb{Z})}^{k-2}$ generate $\mathbb{M}_k(\Gamma)$.
- $x + xS = 0$, $x + x(ST) + x(ST)^2 = 0$, $x - xJ = 0$

Modular Symbols

Manin symbols

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

- $\{[X^{k-2-i}Y^i, \Gamma g]\}_{i=0, g \in \Gamma \backslash SL_2(\mathbb{Z})}^{k-2}$ generate $\mathbb{M}_k(\Gamma)$.
- $x + xS = 0$, $x + x(ST) + x(ST)^2 = 0$, $x - xJ = 0$
- Great for computation!

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 $\mathbb{S}_k(\Gamma) = \left(\mathcal{S}_k(\Gamma) \oplus \bar{\mathcal{S}}_k(\Gamma)\right)^\vee$.

Modular Symbols

Manin symbols

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

- $\{[X^{k-2-i}Y^i, \Gamma g]\}_{i=0, g \in \Gamma \backslash SL_2(\mathbb{Z})}^{k-2}$ 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?

Hecke Operators

Hecke operators

$$T_\Delta : \mathcal{M}_k(\Gamma) \to \mathcal{M}_k(\Gamma)$$
$$T_\Delta(f) = \sum_{\delta \in \Gamma \backslash \Delta} f|_\delta$$

Hecke Operators

Hecke operators

$$T_\Delta : \mathcal{M}_k(\Gamma) \to \mathcal{M}_k(\Gamma)$$
$$T_\Delta(f) = \sum_{\delta \in \Gamma \backslash \Delta} f|_\delta$$

- $T_\alpha = T_{\Gamma\alpha\Gamma}$, can compute dual on $\mathbb{M}_k(\Gamma)$.

Hecke Operators

Hecke operators

$$T_\Delta : \mathcal{M}_k(\Gamma) \to \mathcal{M}_k(\Gamma)$$
$$T_\Delta(f) = \sum_{\delta \in \Gamma \backslash \Delta} f|_\delta$$

- $T_\alpha = T_{\Gamma\alpha\Gamma}$, can compute dual on $\mathbb{M}_k(\Gamma)$.
- Commuting normal operators $\Rightarrow$ basis of common eigenvectors

Hecke Operators

Hecke operators

$$T_\Delta : \mathcal{M}_k(\Gamma) \to \mathcal{M}_k(\Gamma)$$
$$T_\Delta(f) = \sum_{\delta \in \Gamma \backslash \Delta} f|_\delta$$

- $T_\alpha = T_{\Gamma\alpha\Gamma}$, can compute dual on $\mathbb{M}_k(\Gamma)$.
- Commuting normal operators $\Rightarrow$ basis of common eigenvectors
- For $\Gamma = \Gamma_0(N), \Gamma_1(N),\ T_p = T_{\alpha_p}$ satisfies $T_p f = a_p(f) f$

That's great, but what about arbitrary Γ?

Hecke Operators

Proposition

Assume $p \nmid N$. Let $\alpha \in M_2(\mathbb{Z})$ be such that $\det(\alpha) = p$ and $\lambda_N(\alpha) \in H$. Then T_α is independent of α, and if $f = \sum_{n=1}^{\infty} a_n q^n$ is an eigenform of the Hecke algebra then $T_\alpha f = a_p f$.

Question

What about $p \mid N$?

Computational Aspects

Merel pair

Δ, $\phi : \tilde{\Delta} \cdot SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z})$ s.t.

Computational Aspects

Merel pair

Δ, $\phi : \tilde{\Delta} \cdot SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z})$ s.t.

- $\Gamma \cdot \phi(\gamma g) = \Gamma \cdot \phi(\gamma) \cdot g$

Computational Aspects

Merel pair

Δ, $\phi : \tilde{\Delta} \cdot SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z})$ s.t.

- $\Gamma \cdot \phi(\gamma g) = \Gamma \cdot \phi(\gamma) \cdot g$
- $\gamma \cdot \phi(\gamma)^{-1} \in \tilde{\Delta}$

Computational Aspects

Merel pair

Δ, $\phi : \tilde{\Delta} \cdot SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z})$ s.t.

- $\Gamma \cdot \phi(\gamma g) = \Gamma \cdot \phi(\gamma) \cdot g$
- $\gamma \cdot \phi(\gamma)^{-1} \in \tilde{\Delta}$
- $\Gamma \backslash \Delta \hookrightarrow \tilde{\Delta} \cdot SL_2(\mathbb{Z}) / SL_2(\mathbb{Z})$

Theorem (Merel, 1994)

(Δ_n, ϕ_n) Merel pair for Γ with $\Delta_n \subseteq M_2(\mathbb{Z})_n$. Let $\sum_M u_M M$ satisfy

$$\sum_{M \in K} u_M([M\infty] - [M0]) = [\infty] - [0].$$

in $\mathbb{C}[\mathbb{P}^1(\mathbb{Q})]$. Then in $\mathbb{M}_k(\Gamma)$

$$T^{\vee}_{\Delta_n}([P, g]) = \sum_M u_M [P|_{\tilde{M}}, \phi_n(gM)]$$

where the sum is over M such that $gM \in \tilde{\Delta}_n SL_2(\mathbb{Z})$.

Computational Aspects

Corollary (A., 2020)

Computation of the Hecke operator T_p on $\mathcal{S}_k(\Gamma_H)$, for $p \in \det(H)$, can be done in $O(p \log p)$ basic CosetIndex *operations.*

Complexity of T_α with $(\det(\alpha), N) > 1$ is dominated by the cost of conjugation, done using Farey symbols -

Theorem (A., 2020)

There exists an algorithm that given a congruence subgroup of real type $\Gamma \subseteq SL_2(\mathbb{Z})$ of level N, an element $\alpha \in GL_2^+(\mathbb{Q})$ such that $\eta^{-1}\alpha\eta \in \Gamma\alpha\Gamma$ and an integer $k \geqslant 2$, computes the Hecke operator T_α corresponding to the double coset $\Gamma\alpha\Gamma$, on the space of cusp forms $S_k(\Gamma)$, in complexity

$$O(C \cdot I_{\alpha,\Gamma} \log(N^2 \cdot D(\alpha)) + [SL_2(\mathbb{Z}) : \Gamma]^2 \cdot \mathrm{In}).$$

Computational Aspects

Corollary (A., 2020)

There exists an algorithm that given a group of real type $H \subseteq GL_2(\mathbb{Z}/N\mathbb{Z})$ with surjective determinant such that for all $p \mid N$ the Hecke operator is effectively computable, an integer $k \geqslant 2$, and a positive integer L, returns the q-expansions of a basis of eigenforms for $\mathcal{S}_k(\Gamma_H)$ using

$$O(d(C \log N(L \log L + N) + NI_H^2 \cdot \mathrm{In} + kI_H \log(kI_H)) + d^3)$$

field operations, where $d := \dim S_k(\Gamma_H)$, $I_H := [SL_2(\mathbb{Z}) : \Gamma_H]$, C is the cost of a CosetIndex *operation, and* In *is the cost of membership testing in H.*

Other issues

Computational Aspects

Other issues

- Characters, diamond operators

Computational Aspects

Other issues

- Characters, diamond operators
- Degeneracy maps and newforms

Other issues

- Characters, diamond operators
- Degeneracy maps and newforms
- Real type

Computational Aspects

Other issues

- Characters, diamond operators
- Degeneracy maps and newforms
- Real type
- Non-surjective determinant. ($p \notin \det(H)$)

Computational Aspects

Other issues

- Characters, diamond operators
- Degeneracy maps and newforms
- Real type
- Non-surjective determinant. ($p \notin \det(H)$)
- Fast implementation (boundary map, sparse linear algebra, computing intersection and conjugation)

Thanks for listening!