Finite index subgroups of the modular group and their modular forms

Ling Long

Iowa State University

February 2010

Finite index subgroups of $SL_2(\mathbb{Z})$ and their modular forms

The subject is related to the following area:

- Group theory
- Function theory
- Combinatorics
- Algebraic geometry including algebraic curves, covering, and higher analogues
- Representation theory
- Differential equation, such as Picard-Fuch equations for elliptic surfaces
- *p*-adic analysis
- $\cdots$

Finite index subgroups (FIS) of the modular group $SL_2(\mathbb{Z})$

- The modular group
  $SL_2(\mathbb{Z}) = \left\langle E = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, V = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} \right\rangle.$
- Principal congruence subgroups
  $\Gamma(N) = \{\gamma \in SL_2(\mathbb{Z}) \mid \gamma \equiv I_2 \mod N\}$
- A finite index subgroup is said to be congruence if it contains a $\Gamma(N)$, otherwise, it is said to be noncongruence.
- Noncongruence subgroups dominate congruence subgroups.

Description of FIS

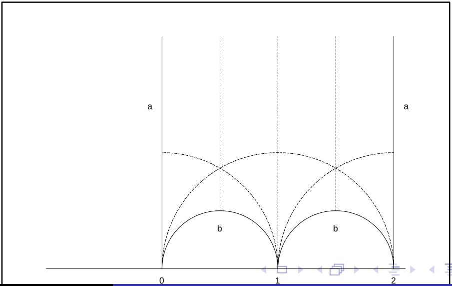
- Below we consider $\pm\Gamma / \pm I_2$ in $PSL_2(\mathbb{Z})$.
- (Millington) Up to isomorphisms the set of index-n FIS corresponds 1-1 to pairs of permutations (e, v) in S_n such that $e^2 = id = v^3$ and $\langle e, v\rangle$ acts transitively on S_n.
- (Kulkarni) FIS can be described algorithmically using generalized Farey symbols, which specifies a special hyperbolic polygon as the fundamental domain of Γ with pairing information for the boundary arcs.

Example: $\Gamma(2)$

- It corresponds to the isomorphism class of $(e, v) \in S_6^2$ where $e = (12)(34)(56)$, $v = (145)(263)$.
- Generalized Farey symbol for $\Gamma(2)$:

$$-\infty \underbrace{\quad}_{1} \frac{0}{1} \underbrace{\quad}_{2} \frac{1}{1} \underbrace{\quad}_{2} \frac{2}{1} \underbrace{\quad}_{1} \infty$$

- A special polygon for $\Gamma(2)$ is as below.



Algorithms for computing FIS

Inputs: either (e, v) or generalized Farey symbols of a FIS

- Minimal set of generators
- Basic invariants like index, genus, elliptic points
- Modular symbols
- Identifying congruence subgroups (Lang-Lim-Tan, Hsu)
- Intersection, union
- Group of normalizers in $SL_2(\mathbb{R})$ (Lang)
- $\cdots$

Chris Kurth implemented a SAGE package “KFarey" for computing FIS.

Modular curve

Let Γ be a FIS. It acts on the upper half plane $\mathbb{H}$ by linearly fractional transformation.
$X_\Gamma := (\mathbb{H}/\Gamma)^*$ its *modular curve*.

Theorem (Belyi)

Any smooth projective irreducible complex curve C defined over a number field is isomorphic to a modular curve for some finite index subgroup Γ of $SL_2(\mathbb{Z})$.

Variables on the curve C correspond to modular functions for Γ. These are meromorphic functions defined on $\mathbb{H}$ and cusps s. t.

$$f(z) = f(\frac{az+b}{cz+d}), \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma, z \in \mathbb{H}.$$

Examples: $j(z)$ for $SL_2(\mathbb{Z})$ and $\lambda(z)$ for $\Gamma(2)$.

Modular functions

Theorem (Atkin and Swinnerton-Dyer, Birch)

A function $f(z)$ on $\mathbb{H}$ is a modular function for some $\Gamma \subset \Gamma(2)$ iff it is an algebraic function of $\lambda(z)$ with only branched points at $\lambda(z) = 0, 1, \infty$.

E.g. for any integer $n \geq 2$, $\sqrt[n]{\lambda(z)}$, $\sqrt[n]{1-\lambda(z)}$ are modular functions. Here we may replace by $\lambda(z)$ or $1-\lambda(z)$ by any modular unit (i.e. modular function with poles and zeros at the cusps). Meanwhile $\sqrt[n]{2-\lambda(z)}$ is not modular function.
The field of all modular functions for Γ, denoted by $\mathfrak{M}_\Gamma$, form a field. To describe X_Γ it is equivalent to describe $\mathfrak{M}_\Gamma$.

A review of congruence cusp forms

Recall that

$$\begin{aligned}\Delta(z) &= q\prod_{n=1}^{\infty}(1-q^n)^{24} \\ &= \sum_{n=1}^{\infty}\tau(n)q^n = q - 24q^2 + 252q^3 - 1472q^4 + \cdots\end{aligned}$$

Ramanujan discovered empirically that

$$\tau(np^r) - \tau(p)\tau(np^{r-1}) + p^{11}\tau(np^{r-2}) = 0, \forall n, r \geq 1 \qquad (1)$$

$$|\tau(p)| < 2p^{11/2}. \qquad (2)$$

- The recursion comes from *Hecke theory*.
- The inequality is proved by Deligne by constructing a *Galois representation* ρ_ℓ attached to $\Delta(z)$:

$$\rho_\ell : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\mathbb{Q}_\ell)$$

which is a continuous homomorphism for a fixed prime ℓ. It satisfies that for any $p \neq \ell$,

$$\mathrm{Tr}(\rho_\ell(\mathrm{Fr}_p)) = \tau(p), \quad \det(\rho_\ell(\mathrm{Fr}_p)) = p^{11}$$

where Fr_p denote the conjugacy class of the arithmetic Frobenius at p.

Bounded denominator property

Let $f(z) = \sum a(n)q^n$ be a integral weight congruence modular form, holomorphic on $\mathbb{H}$, meromorphic at the cusps, with alg. coefficients. Then $\exists\ c \neq 0$ s. t. $c \cdot a(n)$ are alg. integral $\forall n$. Congruence cusp forms are like that due to Hecke theory. An example of Eisenstein series:

$$E_{12}(z) = 1 + \frac{65520}{691} \sum_{n \geq 1} \sigma_{11}(n)q^n.$$

Reason: When n is large, $f(z) \cdot \Delta(z)^n$ is a congruence cusp form, where $\Delta = q \prod_{n \geq 1}(1 - q^n)^{24} = q - 24q^2 + \cdots$. In particular, Δ^{-1} also have integer coefficients. So $f = (f \cdot \Delta^n) \cdot \Delta^{-n}$ satisfies the bounded denominator property.

A glimpse of noncongruence Modular Form

The elliptic curve
$$X^3 + Y^3 = 1$$
is isomorphic to an index-9 subgroup $\Phi(3)$ of $\Gamma(2)$ (i.e. $X = \sqrt[3]{\lambda(z)}, Y = \sqrt[3]{1-\lambda(z)}$). Its invariant differential corresponds to a weight 2 cusp form for $\Phi(3)$

$$\begin{aligned} f(z) &= \sum_{n=1}^{\infty} a(n) q^{n/2} = q^{1/2} + \ldots + 70 q^{5/2} + \ldots \\ &\quad + \frac{23000}{3^2} q^{7/2} + \ldots + \frac{6850312202}{3^5} q^{13/2} + \cdots \end{aligned}$$

Remarks:

- UBD: $a(n) \in \mathbb{Q}$ and they have unbounded denominators (i.e $\nexists n \in \mathbb{Z}_{\neq 0}$ s.t. $nf(z) \in \mathbb{Z}[[q]]$)
- Atkin and Swinnerton-Dyer (ASD) congruence: For every prime $p \neq 3$,

$$a(np^r) - A_p a(np^{r-1}) + pa(np^{r-2}) \equiv 0 \mod p^{(2-1)r}$$

  for all integers $n, r \geq 1$, where $A_p = p + 1 - \#(F_n/\mathbb{F}_p)$
- Modularity/Automorphy: $L(s, f)" = " \prod_{p \text{ prime}} (1 - A_p p^{-s} + p^{1-2s})^{-1}$ is the L-series of a *congruence* modular form. (Wiles, Taylor-Wiles, et al.)

The Unbounded Denominator Conjecture

Unbounded Denominator Conjecture (UBD)

An integral weight modular form holomorphic on $\mathbb{H}$ with algebraic Fourier coefficients is a congruence form if and only if its Fourier coefficients have bounded denominators.

This is a widely believe folklore. It implies a “theorem" of physicists: any C_2-cofinite, rational vertex operator algebra over $\mathbb{C}$ is a congruence modular function.

First Evidence of the UBD Conjecture

Let $\eta(z) = q^{1/24} \prod_{i \geq 1}(1 - q^i)$

Weight 0 eta quotient: $f(z) = \prod_{i=1}^m \eta(a_i z)^{e_i}$ for some integers e_i and $a_i \geq 1$ with $\sum e_i = 0$. E.g. $\eta(11z)^{12}\eta(z)^{-12}$

Let $f(z)$ be an eta quotient. For any integer $n \geq 1$, $\sqrt[n]{f(z)}$ is a modular function. Let

$$\Gamma_{f,n} = \left\{ \gamma \in SL_2(\mathbb{Z}) \mid \sqrt[n]{f}|_\gamma = \sqrt[n]{f} \right\}.$$

Theorem (Kurth, L-)

The UBD conjecture holds for every integral weight modular form of $\Gamma_{f,n}$ with algebraic coefficients.

Atkin and Swinnerton-Dyer congruences: “p-adic" Hecke theory

Atkin, Serre, G. Berger: Hecke operators act ineffectively on noncongr. modular forms.

Atkin and Swinnerton-Dyer conjectured that for a given $S_k(\Gamma)$ and almost all primes p, $S_k(\Gamma)$ possesses a basis consists of “p-adic" Hecke eigenforms $f(z) = \sum a(n)q^{n/\mu} \in E[[q]]$ (where $E/\mathbb{Q}_p$ a finite extn with maximal ideal $\mathfrak{m}$) s. t.

$$a(np^r) - A(p)a(np^{r-1}) + B(p)a(np^{r-2}) \equiv 0 \mod \mathfrak{m}^{(k-1)r}, \forall n, r \geq 1,$$

for some $A(p), B(p) \in E$.

A related issue: supercongruence

Let

$$F_3(z) = q + 4q^2 + 8q^3 + 16q^4 + 26q^5 + 32q^6 + 48q^7 + \cdots = \sum_{n \geq 1} c(n) q^n,$$

is a weight 3 level Eisenstein series with character $\left(\frac{-1}{\cdot}\right))$ such that for each prime $p > 2$,

$$c(p) = p^2 + \left(\frac{-1}{p}\right)$$

$$c(np^r) + -c(p)c(np^{r-1}) + \left(\frac{-1}{p}\right) p^2 c(np^{r-2}) = 0, \forall n, r \geq 1.$$

Supercongruence continued

Lambda function: $\lambda(2z) = 16q\prod_{n\geq 1}(1-q^{2n})^{16}(1-q^{2n-1})^8$.
$\lambda(z)/16$ is a another local uniformizer of $X_{\Gamma(2)}$ at infinity.
Rewrite $F(z)\frac{dq}{q}$ in term of λ, i.e.

$$F(z)\frac{dq}{q} = \sum a_\lambda(n)\lambda^n\frac{d\lambda}{\lambda}, \quad a_\lambda(n) = \sum_{k=0}^{n-1}\binom{2k}{k}^2 2^{-4k}$$

Conjecture

Let p be an odd prime, then

$$a_\lambda(np^r) + \left(\left(\frac{-1}{p}\right) + p^2\right)a_\lambda(np^{r-1}) + \left(\frac{-1}{p}\right)p^2 a_\lambda(np^{r-2}) \equiv 0 \mod p^{2r}, \forall n, r \geq 1.$$

Beukers proved it when modulo p^r (and λ can be replaced by any local uniformizer at infinity), Mortenson proved the case when $r = 1$ and modulo p^2.

Some supercongruences I proved

Let $p > 3$ be a prime. Then

$$\sum_{k=0}^{\frac{p-1}{2}} (4k+1) \left(\frac{(\frac{1}{2})_k}{k!} \right)^6 \equiv p \cdot \gamma_p \mod p^4. \qquad (3)$$

where γ_p is the pth coefficient of $\eta(2z)^4\eta(4z)^4$.
A conjecture of van Hamme:

$$\sum_{k=0}^{\frac{p-1}{2}} (6k+1) \left(\frac{(\frac{1}{2})_k}{k!} \right)^3 4^{-k} \equiv (-1)^{\frac{p-1}{2}} p \mod p^4. \qquad (4)$$

This is a p-adic analogue of the following by Ramanujan:

$$\sum_{k=0}^{\infty} (6k+1) \left(\frac{(\frac{1}{2})_k}{k!} \right)^3 4^{-k} = \frac{4}{\pi}.$$

Scholl Galois rep'ns attached to noncong. cuspforms

Let Γ be a noncongruence gp. s. t. $X_\Gamma := (\mathbb{H}/\Gamma)^*$ is defined over $\mathbb{Q}$ with infinity as a rational point.
For $k \in \mathbb{Z}_{\geq 2}$, $d = \dim S_k(\Gamma)$. Scholl constructed a compatible family of ℓ-adic Galois representations attached to $S_k(\Gamma)$:

$$\rho_{\ell,\Gamma,k} : G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(W_{\ell,\Gamma,k}), \quad \dim_{\mathbb{Q}_\ell} W_{\ell,\Gamma,k} = 2d$$

As Scholl representations are motivic, following Langlands philosophy, the L-function of the dual of $\rho_{\ell,\Gamma,k}$ $L(s, \rho^\vee_{\ell,\Gamma,k})$ "$=$" $\prod_p H_p(p^{-s})^{-1}$ should agree with the L-function of an automorphic representation of some adelic reductive group. If so, we say that $\rho_{\ell,\Gamma,k}$ is *automorphic*.

Conjecture

Absolutely irreducible Scholl representations attached to noncongruence cusp forms are automorphic.

Difference between Deligne and Scholl rep'ns

- Due to the Hecke theory, when Γ is congruence, $\rho_{\ell,\Gamma,k}$ can be decomposed into a direct sum of 2 dimensional representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.
- If Γ is noncongruence, irreducible component of $\rho_{\ell,\Gamma,k}$ could be any dimensional. They make up an amiable variety of motivic representations. Scholl representation becomes a fertile testing ground for Langlands philosophy.

Theorem

Any 2-dimensional Scholl representation of $G_{\mathbb{Q}}$ attached to 1-dimensional space of cusp forms is isomorphic to a Galois representation arising from classical newforms.

The theorem follows from Serre's conjecture, which was proved by Khare and Wintenberger recently.
This theorem applies to our first example: weight 2 cusp form for the Fermat group $\Phi(3)$.

An Application

Theorem (Li and L-)

Suppose $k \geq 2$, X_Γ is defined over $\mathbb{Q}$, and $S_k(\Gamma)$ is 1-dimensional, generated by a cusp form f with rational coefficients. Then the UBD conjecture holds for f.

Idea of the proof

- There are 2 different L-functions associated to a given weight k noncongruence cusp form $f = \sum a(n)q^{n/\mu}$ (where μ is the cusp width of Γ at infinity): $L(s, \rho_{\ell,\Gamma,k})$ and $L(s, f) = \sum_{n\geq 1} \frac{a(n)}{n^s}$.
- $L(s, \rho_{\ell,\Gamma,k})$ is automorphic.
- Under the assumptions, if f have bounded denominators, then $L(s, \rho_{\ell,\Gamma,k})$ and $L(s, f)$ agree up to a twist due to ASD congruence and $a(n) \sim O(n^{k/2-1/5})$, by Selberg.
- The above implies f is congruence.

Higher dim'l Scholl rep'n

- Here, we consider those Scholl representations, up to restriction to subgroups $G_K := \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ of $G_{\mathbb{Q}}$, that can be decomposed into 2-dim'l rep'ns.
- In addition, we consider those 2-dim'l rep's of G_K that are ultimately related to congruence new forms.

Theorem (A.O.L. Atkin, W.C. Li., T. Liu, L-)

Let ℓ be a large prime, $K/\mathbb{Q}$ be a deg. d cyclic extension and ρ_ℓ be a $2d$-dim'l Scholl representation of $G_{\mathbb{Q}}$ to some $S_k(\Gamma)$. Assume that

(a) ρ_ℓ is induced from a 2-dim'l absolutely irreducible rep'n $\widetilde{\rho}$ of G_K;

(b) There exists a finite character χ of G_K such that $(\widetilde{\rho}\otimes\chi)^{ss} = \hat{\rho}|_{G_K}$ for some 2-dimensional $\hat{\rho}$ of $G_{\mathbb{Q}}$.

If further $\hat{\rho}$ is an odd and absolute irreducible representation, then $\hat{\rho}$ is isomorphic to ρ_g attached to a weight k cuspidal newform g, and

$$L(s,\rho_\ell^\vee) = L(s,\widetilde{\rho}^\vee) = L(s,(\rho_g|_{G_K})\otimes\chi^{-1}).$$

An example

The universal elliptic curve with 5 torsion point:

$$y^2 = t\left(x^3 - \frac{1+12t+14t^2-12t^3+t^4}{48t^2}x + \frac{1+18t+75t^2+75t^4-18t^5+t^6}{864t^3}\right). \tag{5}$$

Let $t=(t_4)^4$, i.e. we consider a ramified 4-fold cover of the base curve and then pull back the universal family of elliptic curve to get an elliptic surface $\mathcal{E}_4$. It corresponds to an index-4 normal subgroup Γ_4 of $\Gamma^1(5)$. In particular, $\dim S_3(\Gamma_4)=3$. A piece of the 2nd etale cohomology of $\mathcal{E}_4$ gives rise to a 6-dim'l rep'n ρ_ℓ of $G_{\mathbb{Q}}$, which is isomorphic to Scholl representation attached to $S_3(\Gamma)$. ρ_ℓ is a direct sum of a 2-dim'l ρ_+ and a 4-dim'l ρ_-.

On $\mathcal{E}_4$, there are two finite order maps:

$$A : (x, y, t_4) \mapsto (-x, iy, \frac{\omega_8}{t_4}).$$

$$\zeta : (x, y, t_4) \mapsto (x, y, \omega_8^{-2} \cdot t_4).$$

Let A^*, ζ^* be the maps on cohomology level. They generate an automorphism group which is isomorphic to Q_8. Consequently, ρ_- is induced from 2-dim'l representations of some index-2 subgroups in three different ways. I.e. $\rho_- = \mathrm{Ind}_{G_{\mathbb{Q}(\sqrt{s})}}^{G_{\mathbb{Q}}} \rho_{-,s}$, $s = -1, 2, -2$.

Further, it is shown that for $s = -1, 2, -2$, there exists a character χ_s of $G_{\mathbb{Q}(\sqrt{s})}$ such that $(\rho_{-,s} \otimes \chi_s)^\vee = \rho_{g_s}|_{G_{\mathbb{Q}(\sqrt{s})}}$ for some Deligne representations attached to new form g_s.
As an application, for each odd prime p $S_3(\Gamma)$ has a basis f_1, f_2, f_3, depending only $p \mod 8$ s. t. the coeff.s of f_i satisfies 3-term Atkin and Swinnerton-Dyer congruences. The characteristic poly. of these congruences (i.e coefficients $A(p)$ and $B(p)$) are coming from an explicit automorphic form.

The following table summarizes the state of knowledge for congruence and noncongruence subgroups.

	Congr Γ, level N	Noncongr Γ
Defn Field of X_Γ	$\mathbb{Q}$ or $\mathbb{Q}(\mu_N)$	Some number field
Moduli interpre.	Yes	No
Hecke operators	Eigenforms $\{f_i\}$	conj'l ASD congruences
Galois Reps	2 dim'l ρ_{f_i} for each i	One for each $S_k(\Gamma)$
Automorphy	Yes	Langlands conj ??
L-fcn of Gal. Rep	Analy cont + fcnl eqn	??
L-fcn of cuspform	same as above for f_i	Fcnl eqn on different group
q-exp of $f \in S_k(\Gamma)$	Bounded denom.	UBD Conjecture