Atkin-Swinnerton-Dyer Congruences on Modular Forms for Noncongruence Subgroups

in memory of A. O. L. Atkin

Winnie Li

Pennsylvania State University, U.S.A.
and
National Center for Theoretical Sciences, Taiwan

Modular forms

- A modular form is a holomorphic function on the Poincaré upper half-plane $\mathfrak{H}$ with a lot of symmetries w.r.t. a finite-index subgroup Γ of $SL_2(\mathbb{Z})$.
- Γ is called a *congruence* subgroup if it contains the group

$$\Gamma(N) = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \ : \ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod N \}$$

  for some positive integer N.

  Forms for such Γ are called congruence modular forms.
- Otherwise Γ is called a *noncongruence* subgroup, and forms are called noncongruence modular forms.
- Congruence forms well-studied; noncongruence forms much less understood.

Modular curves

- The group Γ acts on $\mathfrak{H}$ by fractional linear transformations. We compactify the orbit space $\Gamma\backslash\mathfrak{H}$ by joining finitely many cusps to get a Riemann surface, called the modular curve X_Γ for Γ. It has a model defined over a number field.

- The modular curves for congruence subgroups are defined over $\mathbb{Q}$ or cyclotomic fields $\mathbb{Q}(\zeta_N)$.

- Belyi: Every smooth projective irreducible curve defined over a number field is isomorphic to a modular curve X_Γ (for infinitely many finite-index subgroups Γ of $SL_2(\mathbb{Z})$).

- $SL_2(\mathbb{Z})$ has far more noncongruence subgroups than congruence subgroups.

Modular forms for congruence subgroups

Let $g = \sum_{n\geq 1} a_n(g)q^n$, where $q = e^{2\pi i\tau}$, be a normalized ($a_1(g) = 1$) newform of weight $k \geq 2$ level N and character χ. Key properties:

- The Fourier coefficients are multiplicative, i.e.,

$$a_{mn}(g) = a_m(g)a_n(g)$$

  whenever m and n are coprime.

- (Hecke) It is an eigenfunction of the Hecke operators T_p with eigenvalue $a_p(g)$ for all primes $p \nmid N$, i.e., for all $n \geq 1$,

$$a_{np}(g) - a_p(g)a_n(g) + \chi(p)p^{k-1}a_{n/p}(g) = 0.$$

  For primes $p|N$ and all $n \geq 1$,

$$a_{np}(g) = a_n(g)a_p(g).$$

- The Fourier coefficients of a newform are algebraic integers. Given a congruence subgroup and weight, there is a basis of cusp forms with integral Fourier coefficients. An algebraic cusp form has bounded denominators.

- (Eichler-Shimura, Deligne) There exists a compatible family of l-adic deg. 2 rep'ns $\rho_{g,l}$ of the Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ such that

$$\begin{aligned} \mathrm{Tr}(\rho_{g,l}(\mathrm{Frob}_p)) &= a_p(g), \\ \det(\rho_{g,l}(\mathrm{Frob}_p)) &= \chi(p)p^{k-1}, \end{aligned}$$

for all primes p not dividing lN.

The char. poly.

$$H_p(T) = T^2 - A_p T + B_p$$

of $\rho_{g,l}(\mathrm{Frob}_p)$ is indep. of l, and

$$a_{np}(g) - A_p\, a_n(g) + B_p\, a_{n/p}(g) = 0$$

for $n \geq 1$ and primes $p \nmid lN$.

- Ramanujan-Petersson conjecture holds for newforms. That is, $|a_p(g)| \leq 2p^{(k-1)/2}$ for all primes $p \nmid N$.

Modular forms for noncongruence subgroups

Γ : a noncongruence subgroup of $SL_2(\mathbb{Z})$ with finite index

$S_k(\Gamma)$: space of cusp forms of weight $k \geq 2$ for Γ of dim d

A cusp form has an expansion in powers of $q^{1/\mu}$.

Assume the modular curve X_Γ is defined over $\mathbb{Q}$ and the cusp at infinity is $\mathbb{Q}$-rational.

Key players: Fricke, Kline, Atkin and Swinnerton-Dyer, Scholl

Atkin and Swinnerton-Dyer: there exists a positive integer M such that $S_k(\Gamma)$ has a basis consisting of forms with coeffs. in $\mathbb{Z}[\frac{1}{M}]$ (called M-integral) :

$$f(\tau) = \sum_{n \geq 1} a_n(f) q^{n/\mu}.$$

No efficient Hecke operators on noncongruence forms

- Let Γ' be the smallest congruence subgroup containing Γ. Naturally, $S_k(\Gamma') \subset S_k(\Gamma)$.
- $Tr_{\Gamma'}^{\Gamma} : S_k(\Gamma) \to S_k(\Gamma')$ such that its restriction on $S_k(\Gamma')$ is multiplication by $[\Gamma' : \Gamma]$.
- The kernel of $Tr_{\Gamma'}^{\Gamma}$ consists of genuine noncongruence forms in $S_k(\Gamma)$.

Conjecture (Atkin). The Hecke operators on $S_k(\Gamma)$ for $p \nmid M$ defined using double cosets as for congruence forms is zero on genuine noncongruence forms in $S_k(\Gamma)$.

This was proved by Serre, Berger.

Atkin-Swinnerton-Dyer congruences

Let E be an elliptic curve defined over $\mathbb{Q}$ with conductor M. By Belyi, $E \simeq X_\Gamma$ for a finite index subgroup Γ of $SL_2(\mathbb{Z})$. Eg. $E : x^3 + y^3 = z^3$, Γ is an index-9 noncongruence subgp of $\Gamma(2)$.

Atkin and Swinnerton-Dyer: The normalized holomorphic differential 1-form $f\frac{dq}{q} = \sum_{n\geq 1} a_n q^n \frac{dq}{q}$ on E satisfies the congruence relation

$$a_{np} - [p + 1 - \#E(\mathbb{F}_p)]a_n + pa_{n/p} \equiv 0 \mod p^{1+\mathrm{ord}_p n}$$

for all primes $p \nmid M$ and all $n \geq 1$.

Note that $f \in S_2(\Gamma)$.

Taniyama-Shimura modularity theorem: There is a normalized congruence newform $g = \sum_{n\geq 1} b_n q^n$ with $b_p = p + 1 - \#E(\mathbb{F}_p)$. This gives congruence relations between f and g.

Back to general case where X_Γ has a model over $\mathbb{Q}$, and the d-dim'l space $S_k(\Gamma)$ has a basis of M-integral forms.

ASD congruences: for each prime $p \nmid M$, $S_k(\Gamma, \mathbb{Z}_p)$ has a p-adic basis $\{h_j\}_{1 \le j \le d}$ such that the Fourier coefficients of h_j satisfy a three-term congruence relation

$$a_{np}(h_j) - A_p(j) a_n(h_j) + B_p(j) a_{n/p}(h_j) \equiv 0 \mod p^{(k-1)(1+\mathrm{ord}_p n)}$$

for all $n \ge 1$. Here

- $A_p(j)$ is an algebraic integer with $|A_p(j)| \le 2p^{(k-1)/2}$, and
- $B_p(j)$ is equal to p^{k-1} times a root of unity.

This is proved to hold for $k = 2$ and $d = 1$ by ASD.

Their data also show that the A_p's satisfy the Sato-Tate distribution.

Remarks. (1) The basis varies with p.

(2) The three-term congruence relations for noncongruence forms capture the spirit of the Hecke operators in essence.

(3) From where do $A_p(j)$ and $B_p(j)$ arise? Any modularity interpretations?

Belyi's theorem tells us that, viewed simply as algebraic curves, noncongruence modular curves are very general, and that we should not expect them to have any special arithmetic properties. On the other hand, the uniformization of noncongruence curves by the upper half-plane is quite special, and leads to surprising consequences.

Galois representations attached to $S_k(\Gamma)$ and congruences

Theorem[Scholl] *Suppose that the modular curve X_Γ has a model over $\mathbb{Q}$. Attached to $S_k(\Gamma)$ is a compatible family of* $2d$*-dim'l l-adic rep'ns ρ_l of the Galois group* $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ *unramified outside lM such that for primes $p > k+1$ not dividing Ml, the following hold.*

(i) The char. polynomial

$$H_p(T) = \sum_{0 \le r \le 2d} B_r(p) T^{2d-r}$$

of $\rho_l(\mathrm{Frob}_p)$ lies in $\mathbb{Z}[T]$, is indep. of l, and its roots are algebraic integers with absolute value $p^{(k-1)/2}$;

(ii) For any form f in $S_k(\Gamma)$ integral outside M, its Fourier coeffs satisfy the $(2d+1)$-term congruence relation

$$\begin{aligned} & a_{np^d}(f) + B_1(p)a_{np^{d-1}}(f) + \cdots + \\ & + B_{2d-1}(p)a_{n/p^{d-1}}(f) + B_{2d}(p)a_{n/p^d}(f) \\ & \equiv 0 \mod p^{(k-1)(1+\mathrm{ord}_p n)} \end{aligned}$$

for $n \geq 1$.

The Scholl rep'ns ρ_l are generalizations of Deligne's construction to the noncongruence case. The congruence in (ii) follows from comparing l-adic theory to an analogous p-adic de Rham/crystalline theory; the action of $Frob_p$ on both sides have the same characteristic polynomials.

Scholl's theorem establishes the ASD congruences if $d = 1$.

In general, to go from Scholl congruences to ASD congruences, ideally one hopes to factorize

$$H_p(T) = \prod_{1\le j\le d} (T^2 - A_p(j)T + B_p(j))$$

and find a p-adic basis $\{h_j\}_{1\le j\le d}$, depending on p, for $S_k(\Gamma, \mathbb{Z}_p)$ such that each h_j satisfies the three-term ASD congruence relations given by $A_p(j)$ and $B_p(j)$.

For a congruence group Γ, this is achieved by using Hecke operators to further break the l-adic and p-adic spaces into pieces. For a noncongruence Γ, no such tools are available.

Scholl representations, being motivic, should correspond to automorphic forms for reductive groups according to Langlands philosophy. They are the link between the noncongruence and congruence worlds.

Modularity of Scholl representations when $d = 1$

Scholl: the rep'n attached to $S_4(\Gamma_{7,1,1})$ is modular, coming from a newform of wt 4 for $\Gamma_0(14)$; ditto for $S_4(\Gamma_{4,3})$ and $S_4(\Gamma_{5,2})$.

Li-Long-Yang: True for wt 3 noncongruence forms assoc. with K3 surfaces defined over $\mathbb{Q}$.

In 2006 Kahre, Wintenberger and Kisin established Serre's conjecture on modular representations. This leads to

Theorem *If* $S_k(\Gamma)$ *is* 1*-dimensional, then the degree two l-adic Scholl representations of* $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ *are modular.*

Therefore for $S_k(\Gamma)$ with dimension one, we have both ASD congruences and modularity. Consequently, every $f \in S_k(\Gamma)$ with algebraic Fourier coefficients satisfies three-term congruence relations with a wt k congruence form.

ASD congruences and modularity for $d \geq 2$

For each $n \geq 1$, there is an index-n subgroup Γ_n of $\Gamma^1(5)$ whose modular curve is defined over $\mathbb{Q}$ and $S_3(\Gamma_n)$ is $(n-1)$-dim'l with explicit basis and attached Scholl rep'n $\rho_{n,l}$.

Case $d = 2$.

Theorem[L-Long-Yang, 2005, for Γ_3]

(1) The space $S_3(\Gamma_3)$ has a basis consisting of 3-integral forms

$$f_{\pm}(\tau) = q^{1/15} \pm iq^{2/15} - \frac{11}{3}q^{4/15} \mp i\frac{16}{3}q^{5/15} - \\ -\frac{4}{9}q^{7/15} \pm i\frac{71}{9}q^{8/15} + \frac{932}{81}q^{10/15} + \cdots .$$

(2) (Modularity) There are two cuspidal newforms of weight 3 level 27 and character χ_{-3} given by

$$
\begin{aligned}
g_{\pm}(\tau) \;=\; & q \mp 3iq^2 - 5q^4 \pm 3iq^5 + 5q^7 \pm 3iq^8 + \\
& +9q^{10} \pm 15iq^{11} - 10q^{13} \mp 15iq^{14} - \\
& -11q^{16} \mp 18iq^{17} - 16q^{19} \mp 15iq^{20} + \\
& 45q^{22} \pm 12iq^{23} + \cdots .
\end{aligned}
$$

such that $\rho_{3,l} = \rho_{g_+,l} \oplus \rho_{g_-,l}$ *over* $\mathbb{Q}_l(\sqrt{-1})$.

(3) $f_{\pm}$ *satisfy the 3-term ASD congruences with* $A_p = a_p(g_{\pm})$ *and* $B_p = \chi_{-3}(p)p^2$ *for all primes* $p \geq 5$.

Here χ_{-3} is the quadratic character attached to $\mathbb{Q}(\sqrt{-3})$.

Basis functions $f_{\pm}$ indep. of p, best one can hope for.

Hoffman, Verrill and students: an index 3 subgp of $\Gamma_0(8) \cap \Gamma_1(4)$, wt 3 forms, $\rho = \tau \oplus \tau$ and τ modular, one family of A_p and B_p.

Case $d = 3$.

- $S_3(\Gamma_4)$ has an explicit basis h_1, h_2, h_3 of 2-integral forms.
- $\Gamma_4 \subset \Gamma_2 \subset \Gamma^1(5)$ and $S_3(\Gamma_2) =< h_2 >$.

Theorem[L-Long-Yang, 2005, for Γ_2]

The 2-dim'l Scholl representation $\rho_{2,l}$ attached to $S_3(\Gamma_2)$ is modular, isomorphic to $\rho_{g_2,l}$ attached to the cuspidal newform $g_2 = \eta(4z)^6$. Consequently, h_2 satisfies the ASD congruences with $A_p = a_p(g_2)$ and $B_p = p^2$.

It remains to describe the ASD congruence on the space $< h_1, h_3 >$. Let

$$f_1(z) = \frac{\eta(2z)^{12}}{\eta(z)\eta(4z)^5} = q^{1/8}(1 + q - 10q^2 + \cdots) = \sum_{n\geq 1} a_1(n)q^{n/8},$$
$$f_3(z) = \eta(z)^5\eta(4z) = q^{3/8}(1 - 5q + 5q^2 + \cdots) = \sum_{n\geq 1} a_3(n)q^{n/8},$$
$$f_5(z) = \frac{\eta(2z)^{12}}{\eta(z)^5\eta(4z)} = q^{5/8}(1 + 5q + 8q^2 + \cdots) = \sum_{n\geq 1} a_5(n)q^{n/8},$$
$$f_7(z) = \eta(z)\eta(4z)^5 = q^{7/8}(1 - q - q^2 + \cdots) = \sum_{n\geq 1} a_7(n)q^{n/8}.$$

Theorem[Atkin-L-Long, 2008] [ASD congruence for the space $< h_1, h_3 >$]

1. *If* $p \equiv 1 \mod 8$, *then both* h_1 *and* h_3 *satisfy the three-term ASD congruence at* p *with* $A_p = sgn(p)a_1(p)$ *and* $B_p = p^2$, *where* $sgn(p) = \pm 1 \equiv 2^{(p-1)/4} \mod p$ *;*
2. *If* $p \equiv 5 \mod 8$, *then* h_1 *(resp.* h_3*) satisfies the three-term ASD-congruence at* p *with* $A_p = -4ia_5(p)$ *(resp.* $A_p = 4ia_5(p)$*) and* $B_p = -p^2$*;*
3. *If* $p \equiv 3 \mod 8$, *then* $h_1 \pm h_3$ *satisfy the three-term ASD congruence at* p *with* $A_p = \mp 2\sqrt{-2}a_3(p)$ *and* $B_p = -p^2$*;*
4. *If* $p \equiv 7 \mod 8$, *then* $h_1 \pm ih_3$ *satisfy the three-term ASD congruence at* p *given by* $A_p = \pm 8\sqrt{-2}a_7(p)$ *and* $B_p = -p^2$.

Here $a_1(p), a_3(p), a_5(p), a_7(p)$ *are given above.*

To describe the modularity of $\rho_{4,l}$, let

$$f(z) = f_1(z) + 4f_5(z) + 2\sqrt{-2}(f_3(z) - 4f_7(z)) = \sum_{n\geq 1} a(n)q^{n/8}.$$

$f(8z)$ is a newform of level dividing 256, weight 3, and quadratic character χ_{-4} associated to $\mathbb{Q}(i)$.

Let $K = \mathbb{Q}(i, 2^{1/4})$ and χ a character of $Gal(K/\mathbb{Q}(i))$ of order 4. Denote by $h(\chi)$ the associated (weight 1) cusp form.

Theorem[Atkin-L-Long, 2008][Modularity of $\rho_{4,l}$]

The degree 6 Scholl rep'n $\rho_{4,l}$ decomposes over $\mathbb{Q}_l$ into the sum of $\rho_{2,l}$ (2-dim'l) and $\rho_{-,l}$ (4-dim'l). Further, $L(s, \rho_{2,l}) = L(s, g_2)$ and $L(s, \rho_{-,l}) = L(s, f \times h(\chi))$ (same local L-factors).

Proof uses Faltings-Serre method.

Representations with quaternion multiplications

Joint work with A.O.L. Atkin, T. Liu and L. Long

ρ_l : a 4-dim'l Scholl representation of $G_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ assoc. to a 2-dim'l subspace $S \subset S_k(\Gamma)$.

Suppose ρ_l has *quaternion multiplications* (QM) over $\mathbb{Q}(\sqrt{s}, \sqrt{t})$, i.e., there are two operators J_s and J_t on $\rho_l \otimes_{\mathbb{Q}_l} \bar{\mathbb{Q}}_l$, parametrized by two non-square integers s and t, satisfying

(a) $J_s^2 = J_t^2 = -id, J_{st} := J_s J_t = -J_t J_s$;

(b) For $u \in \{s, t\}$ and $g \in G_{\mathbb{Q}}$, we have $J_u \rho_l(g) = \varepsilon_u(g) \rho_l(g) J_u$, where ε_u is the quadratic character of $\mathrm{Gal}(\mathbb{Q}(\sqrt{u})/\mathbb{Q})$.

For Γ_3, Scholl representations have QM over $\mathbb{Q}(\sqrt{s}, \sqrt{t}) = \mathbb{Q}(\sqrt{-3})$, and for Γ_4, we have QM over $\mathbb{Q}(\sqrt{s}, \sqrt{t}) = \mathbb{Q}(\sqrt{-1}, \sqrt{2}) = \mathbb{Q}(\zeta_8)$.

Theorem [Atkin-L-Liu-Long] (Modularity)

(a) *If* $\mathbb{Q}(\sqrt{s}, \sqrt{t})$ *is a quadratic extension, then over* $\mathbb{Q}_l(\sqrt{-1})$, ρ_l *decomposes as a sum of two degree* 2 *representations assoc. to two congruence forms of weight* k.

(b) *If* $\mathbb{Q}(\sqrt{s}, \sqrt{t})$ *is biquadratic over* $\mathbb{Q}$, *then for each* $u \in \{s, t, st\}$, *there is an automorphic form* g_u *for* GL_2 *over* $\mathbb{Q}(\sqrt{u})$ *such that the* L*-functions attached to* ρ_l *and* g_u *agree locally at all* p. *Consequently,* $L(s, \rho_l)$ *is automorphic.*

$L(s, \rho_l)$ also agrees with the L-function of an automorphic form of $GL_2 \times GL_2$ over $\mathbb{Q}$, and hence also agrees with the L-function of a form on GL_4 over $\mathbb{Q}$ by Ramakrishnan.

The proof uses descent and modern modularity criteria.

Theorem [Atkin-L-Liu-Long] (ASD congruences)

Assume $\mathbb{Q}(\sqrt{s}, \sqrt{t})$ is biquadratic. Suppose that the QM operators J_s and J_t arise from real algebraic linear combinations of normalizers of Γ so that they also act on forms in S. For each $u \in \{s, t, st\}$, let $f_{u,j}$, $j = 1, 2$, be linearly independent eigenfunctions of J_u. For almost all primes p split in $\mathbb{Q}(\sqrt{u})$, $f_{u,j}$ are p-adically integral basis of S and the ASD congruences at p hold for $f_{u,j}$ with $A_{u,p}(j)$ and $B_{u,p}(j)$ coming from the two local factors

$$(1 - A_{u,p}(j)p^{-s} + B_{u,p}(j)p^{-2s})^{-1}, \qquad j = 1, 2,$$

of $L(s, g_u)$ at the two places of $\mathbb{Q}(\sqrt{u})$ above p.

Note that the basis functions for ASD congruences depend on p modulo the conductor of $\mathbb{Q}(\sqrt{s}, \sqrt{t})$.

ASD congruences in general

Now suppose $S_k(\Gamma)$ has dimension d. Scholl representations ρ_l are $2d$-dimensional. For almost all p the characteristic polynomial $H_p(T)$ of $\rho_l(\mathrm{Frob}_p)$ has degree $2d$. The representations are called *strongly regular* at p if $H_p(T)$ has d roots which are distinct p-adic units (and the remaining d roots are p^{k-1} times units).

Scholl: ASD congruences at p hold if ρ_l is strongly regular at p.

But if the representations are not regular at p, then the situation is quite different. We exhibit 2 examples computed by J. Kibelbek.

Ex 1. $X : y^2 = x^5 + 1$, genus 2 curve defined over $\mathbb{Q}$. By Belyi, $X \simeq X_\Gamma$ for a finite index subgroup $\Gamma < SL_2(\mathbb{Z})$. Put

$$w = -\frac{x^2}{y}, \quad \frac{dx}{y} = f_1 \frac{dw}{w}, \quad x\frac{dx}{y} = f_2 \frac{dw}{w}.$$

Then $S_2(\Gamma) =< f_1, f_2 >$, where

$$f_1 = \sum_{n \geq 0} \binom{5n+1}{n} w^{10n+3}, \quad f_2 = \sum_{n \geq 0} \binom{5n}{n} w^{10n+1}.$$

The l-adic representations for wt 2 forms are the dual of the Tate modules on the Jacobian of X.

For primes $p \equiv 2, 3 \mod 5$, $H_p(T) = T^4 + p^2$, but no 3-term congruences exist.

Ex 2. $X : \; y^2 = x^5 + 2x^4 + 1$, genus 2 curve defined over $\mathbb{Q}$. Again, $X \simeq X_\Gamma$ for a finite index subgroup $\Gamma < SL_2(\mathbb{Z})$. Define

$$w = -\frac{x^2}{y}, \quad \frac{dx}{y} = f_1 \frac{dw}{w}, \quad x\frac{dx}{y} = f_2 \frac{dw}{w}.$$

Then $S_2(\Gamma) =< f_1, f_2 >$, where

$$f_1 = \sum_{n \geq 3, \mathrm{odd}} \; \sum_{4i+j=(n-3)/2} \binom{(n-1)/2}{i, j, 3i+1} w^n,$$

and

$$f_2 = \sum_{n \geq 1, \mathrm{odd}} \; \sum_{4i+j=(n-1)/2} \binom{(n-1)/2}{i, j, 3i} w^n.$$

$H_3(T) = T^4 + T^3 + 3T^2 + 3T + 9$ has roots α_1, ..., α_4.

Modulo 3^9, they are

$\alpha_1 = 18530$ (3-adic unit) ; $\alpha_2 = 15603 = 3/\alpha_1$ (divisible by 3);
$\alpha_3 = 2616 + 18926\sqrt{6}$, $\alpha_4 = 2616 - 18926\sqrt{6} = 3/\alpha_3$
(both have 3-adic valuation $1/2$).

$f_2 - 695 f_1$ satisfies the ASD congruence at 3 with A_3 and $B_3 = 3$ coming from $(T - \alpha_3)(T - \alpha_4) = T^2 - A_3 T + 3$.

However, no form in $S_2(\Gamma)$ linearly independent of $f_2 - 695 f_1$ will satisfy a 3-term ASD congruence at 3.