Congruences for modular form coefficients

Ken Ono

(University of Wisconsin at Madison).

Fact. Modular form coefficients are <u>**important**</u>.

They are a source of interesting problems:

- Ramanujan-Petersson Conjecture (a.k.a Deligne's Theorem).
- Taniyama-Shimura Conjecture.
- Lehmer's Conjecture.
- Serre's Conjectures.
- etc.

These coefficients **also** play central roles in many applications such as:

- Ramanujan's work on partitions.

- Quadratic forms and sphere packing.

- Artin's L-function Conjecture.

- Proof of Fermat's Last Theorem.

- Birch and Swinnerton-Dyer Conjecture.

- Monstrous Moonshine.

- Class field theory of CM fields.

- Elliptic curves in so **many many** ways....etc.

Goal. We recall some classical **congruences** for modular form coefficients, and give one modern application to elliptic curves.

. . . .

underbar**Ramanujan's works.**

We begin with Ramanujan's work on $p(n)$ and $\tau(n)$, examples which "inspired" much of the early history of work on modular forms.

I. Partitions.

Definition. A **partition** of an integer N is a sequence of non-increasing positive integers with sum N.

$$p(N) := \#\{\text{partitions of } N\}$$

N	Partitions of N	$p(N)$
1	1	$p(1) = 1$
2	2	$p(2) = 2$
	1 1	
3	3	$p(3) = 3$
	2 1	
	1 1 1	
4	4	$p(4) = 5$
	3 1	
	2 2	
	2 1 1	
	1 1 1 1	

Question. What is the size of $p(N)$?

N	$p(N)$
10	42
100	190569292
1000	24061467864032622473692149727991
...	...

The Hardy-Ramanujan Asymptotic Formula.

Inventing the "circle method", they proved:

$$p(N) \sim \frac{e^{\pi\sqrt{2N/3}}}{4N\sqrt{3}}.$$

Theorem (Ramanujan).
If $n \geq 0$, then

$$p(5n+4) \equiv 0 \pmod{5},$$
$$p(7n+5) \equiv 0 \pmod{7},$$
$$p(11n+6) \equiv 0 \pmod{11}.$$

. . . .

Remark. These results require "modularity".

Theorem (Euler).

$$\sum_{n=0}^{\infty} p(n)q^n = \prod_{n=1}^{\infty} \frac{1}{1-q^n}.$$

As a weight $-\frac{1}{2}$ modular form, we have

$$\frac{1}{\eta(24z)} = \sum_{n=0}^{\infty} p(n)q^{24n-1}.$$

II. The tau-function.

Following Ramanujan, define integers $\tau(n)$ by:

$$\Delta(z) = \sum_{n=1}^{\infty} \tau(n) q^n = q \prod_{n=1}^{\infty} (1 - q^n)^{24}$$

$$= q - 24q^2 + 252q^3 - 1472q^4 + 4830q^5 - \cdots .$$

Remarks.

1. Throughout, we let $q = e^{2\pi i z}$.

2. This function is a weight 12 modular form.

3. This function drove much of the early history in the study of modular forms.

Some examples of important results for $\tau(n)$:

1. (Ramanujan) For every $n \geq 1$, we have

$$\tau(n) \equiv \sum_{d|n} d^{11} \pmod{691}.$$

2. (Mordell) If n and m are coprime positive integers, then

$$\tau(n)\tau(m) = \tau(nm).$$

This marked the birth of Hecke operators.

3. (Deligne) If p is prime, then

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

This follows from the Weil Conjectures.

Remark. Although Ramanujan proved the "691 congruence" using a simple q-series identity, it is a special case of a very deep theory.

Galois representations.

By work of Deligne (and others), we have:

Theorem. If $f(z) = \sum_{n=1}^{\infty} a(n)q^n \cap \mathbb{Z}[[q]]$ is an **integer weight** Hecke eigenform, then for each prime ℓ there is an ℓ-adic representation

$$\rho_{f,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}_\ell)$$

such that for every prime $p \nmid \ell N$ we have

$$\mathrm{Tr}(\rho_{f,\ell}(\mathrm{Frob}(p)) = a(p).$$

Remarks.

1. Proving congruences are reduced to the computation of Galois representations.

2. "Nice" representations give congruences.

   In particular, for primes $p \neq 691$ we have

   $$\rho_{\Delta,691}(\mathrm{Frob}(p)) \equiv \begin{pmatrix} 1 & * \\ 0 & p^{11} \end{pmatrix} \pmod{691}.$$

3. These representations play a central role in Wiles' proof of Fermat's Last Theorem.

Basics about modular forms.

$\mathsf{SL}_2(\mathbb{Z})$-action on $\mathcal{H}$.

If $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathsf{SL}_2(\mathbb{Z})$ and $z \in \mathcal{H}$, then we let

$$Az = \frac{az+b}{cz+d}.$$

. . . .

Congruence Subgroups.

The level N **congruence subgroups** are

$$\Gamma_0(N) := \left\{ A \in \mathsf{SL}_2(\mathbb{Z}) \ : \ A \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N} \right\}$$

$$\Gamma_1(N) := \left\{ A \in \mathsf{SL}_2(\mathbb{Z}) \ : A \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}.$$

Integer weight modular forms.

Definition. A holomorphic function $f(z)$ on $\mathcal{H}$ is a **modular form** of integer weight k on a congruence subgroup Γ if

1. We have
$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$$
for all $z \in \mathcal{H}$ and all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$.

2. If $f(z)$ is holomorphic at each cusp.

Half-integral weight modular forms

Notation. If d is odd and $c \in \mathbb{Z}$, then let

$$\left(\frac{c}{d}\right) := \begin{cases} \left(\frac{c}{|d|}\right) & \text{if } \ d < 0 \text{ and } c > 0, \\ -\left(\frac{c}{|d|}\right) & \text{if } \ d < 0 \text{ and } c < 0, \\ \left(\frac{c}{|d|}\right) & \text{if } d > 0 \text{ and } c \neq 0, \\ 1 & \text{if } c = 0 \text{ and } d = \pm 1, \end{cases}$$

$$\epsilon_d := \begin{cases} 1 & \text{if } d \equiv 1 \mod 4 \\ i & \text{if } d \equiv 3 \mod 4. \end{cases}$$

. . . .

$\sqrt{z} =$ branch of $\sqrt{z}$ with argument in $(-\pi/2, \pi/2]$.

Definition. Suppose that $\lambda \geq 0$ and that Γ is a congruence subgroup of level $4N$.

A holomorphic function $f(z)$ on $\mathcal{H}$ is a **half-integral weight modular form** of weight $\lambda + \frac{1}{2}$ on Γ if

1) If $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$, then

$$f\left(\frac{az+b}{cz+d}\right) = \left(\frac{c}{d}\right)^{2\lambda+1} \epsilon_d^{-1-2\lambda} (cz+d)^{\lambda+\frac{1}{2}} f(z).$$

2) If $f(z)$ is holomorphic at each cusp.

Terminology. Suppose that

$$f(z) \text{ is a modular form.}$$

1) If $k = 0$, then $f(z)$ is a **modular function**.

2) If $f(z)$ is a holomorphic modular form which vanishes at the cusps, then it is a **cusp form.**

Notation.

$M_k(\Gamma) := \{$holomorphic modular forms of weight k on $\Gamma\}$,

$S_k(\Gamma) := \{$cusp forms of weight k on $\Gamma\}$.

. . . .

Fourier expansion at infinity. Modular forms have a **Fourier expansion at infinity**

$$f(z) = \sum_{n \geq n_0}^{\infty} a(n) q^n,$$

where $q := e^{2\pi i z}$.

Nonvanishing of L-functions

Notation for the main objects

- An **even weight newform**:

$$f(z) = \sum_{n=1}^{\infty} a(n) q^n \in S_{2k}^{\mathrm{new}}(\Gamma_0(M))$$

- Its L-function

$$L(f, s) = \sum_{n=1}^{\infty} \frac{a(n)}{n^s}$$

- If D is a fundamental discriminant and $\chi_D = \left(\frac{D}{\bullet}\right)$, then the **quadratic twists** are:

$$f_D(z) = \sum_{n=1}^{\infty} \chi_D(n) a(n) q^n,$$

$$L(f_D, s) = \sum_{n=1}^{\infty} \frac{\chi_D(n) a(n)}{n^s}.$$

Remark. These values are related to the Birch and Swinnerton-Dyer Conjecutre.

. . . .

Elliptic curves. If $K/\mathbb{Q}$ is a field, then we shall consider elliptic curves

$$E: \; y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad a_i \in K$$

Theorem (Poincare)
The set of points $E(K)$ togther with the the point at infinity forms an abelian group.

Group Law on $E: \quad y^2 = x^3 + 17$

Theorem (Mordell-Weil)
Every elliptic curve $E(K)$ over a number field K is a finitely generated abelian group.

$$E(K) \cong E_{tor}(K) \oplus \mathbb{Z}^{\mathrm{rk}(E,K)}.$$

. . . .

Example. If E is the elliptic curve

$$E: \quad y^2 = x^3 + 17,$$

then we have

$$E(\mathbb{Q}) \cong \mathbb{Z}^2.$$

(i.e. $\mathrm{rk}(E, \mathbb{Q}) = 2$)

The Birch and Swinnerton-Dyer Conjecture.

Notation.

$$E/\mathbb{Q} \quad \text{an elliptic curve}$$

$$L(E,s) = \sum_{n=1}^{\infty} \frac{a_E(n)}{n^s} \text{ its Hasse-Weil } L\text{-function.}$$

. . . .

Remark. For primes p of good reduction

$$N_E(p) = p + 1 - a_E(p),$$

where $N_E(p)$ is # points on E modulo p.

Birch and Swinnerton-Dyer Conjecture.
If $\mathrm{rk}(E)$ is the rank of $E(\mathbb{Q})$, then

$$\mathrm{ord}_{s=1}(L(E,s)) = \mathrm{rk}(E).$$

. . . .

Remarks.

1) For E with CM, Coates and Wiles proved

(1977) $\quad L(E,1) \neq 0 \implies \mathrm{rk}(E) = 0.$

2) Kolyvagin's breakthrough in the 1980s.

Subject to hypotheses on the nonvanishing of central L-values and derivatives of **quadratic twists**, for **modular** E he proved

$$\mathrm{ord}_{s=1}(L(E,s)) \leq 1$$

$$\implies \quad \mathrm{ord}_{s=1}(L(E,s)) = \mathrm{rk}(E).$$

Happily we have:

Theorem.
If $E/\mathbb{Q}$ has conductor $N(E)$, then there is a newform $f_E(z) \in S_2^{\text{new}}(\Gamma_0(N(E))$ for which

$$L(E,s) = L(f_E,s).$$

. . . .

Hence, we have:

Theorem (Kolyvagin)
If $E/\mathbb{Q}$ is an elliptic curve, then

$$\text{ord}_{s=1}(L(E,s)) \leq 1$$

$$\Longrightarrow \quad \text{ord}_{s=1}(L(E,s)) = \text{rk}(E)$$

$$\text{and } |\text{Ш}(E)| < +\infty.$$

Quadratic twists of elliptic curves.

If $E/\mathbb{Q}$ is an elliptic curve given

$$E: \quad y^2 = x^3 + ax^2 + bx + c,$$

then its $D-$**quadratic twist of** E is given by

$$E(D): \quad Dy^2 = x^3 + ax^2 + bx + c.$$

. . . .

Lemma. Suppose that $E/\mathbb{Q}$ is an elliptic curve and that $f = f_E(z)$ has the property that

$$L(E, s) = L(f, s).$$

If D is coprime to the conductor of E, then

$$L(E(D), s) = L(f_D, s).$$

Main Problem. Given E, we wish to estimate

$$\#\{|D| \le X \ : \ \mathrm{rk}(E(D)) = 0\}.$$

. . . .

<u>Congruent Numbers.</u> A positive integer D is a "congruent number" if it is the area of a right triangle with rational sidelengths.

Remark. This problem remains open, and is a special case of the Main Problem above since

$$D \text{ is congruent} \iff \mathrm{rk}(E(D)) > 0,$$

where $E:\ y^2 = x^3 - x$.

"Conjecture" (Goldfeld).

If $E/\mathbb{Q}$ is an elliptic curve, then

$$\sum_{|D|\le X} \mathsf{rk}(E(D)) \sim \frac{1}{2}\#\{D \;:\; |D| < X\}.$$

Theorem 1 ('98 Invent. Math., O-Skinner).

If $f(z) \in S_{2k}^{\mathrm{new}}(\Gamma_0(M))$ *is a newform, then*

$$\#\{|D| \leq X \ : \ L(f_D, k) \neq 0\} \gg \frac{X}{\log X}.$$

. . . .

Corollary. If $E/\mathbb{Q}$ is an elliptic curve, then

$$\#\{|D| \leq X \ : \ \mathrm{rk}(E(D)) = 0\} \gg \frac{X}{\log X}.$$

For most newforms, more is true:

"**Theorem 2.**" ['01 Crelle, O]
If there is a prime $p \nmid 2M$ with

$$a(p) \equiv 1 \pmod 2,$$

then $\exists\ D_f$ and a set of primes S_f, with positive density, such that for every j

$$L(f_{p_1 p_2 \cdots p_{2j} D_f}, k) \neq 0,$$

whenever $p_1, p_2, \ldots, p_{2j} \in S_f$ are distinct.

Corollary. If $2 \nmid \#E_{\text{tor}}$, then $\exists\ D_E$ and a set of primes S_E, with positive density, such that for every $j \geq 1$ we have

$$\text{rk}(E(D_E p_1 p_2 \cdots p_{2j})) = 0,$$

whenever $p_1, p_2, \ldots p_{2j} \in S_E$ are distinct.

. . . .

Remark. In Thm 2 and the corollary above, $\exists\ 0 < \alpha < 1$ for which

$$\#\{|D| \leq X \ : \ L(f_D, k) \neq 0\} \gg \frac{X}{(\log X)^{1-\alpha}},$$

$$\#\{-X < D < X \ : \ \text{rk}(E(D)) = 0\} \gg \frac{X}{\log^{1-\alpha} X}.$$

Example. Let $E/\mathbb{Q}$ be the elliptic curve

$$E : \quad y^2 = x^3 - 432.$$

Then $D_E := 1$ and

$S_E := \{p > 3 \ : \ 2 \text{ is not a cubic residue in } \mathbb{F}_p\}$.

Sketch of the proof of Theorem 2

Kohnen and Zagier, and Waldspurger proved

"arithmetic formulas" for $L(f_D, k)$.

Notation. For every fundamental discriminant D let

$$D_0 := \begin{cases} |D| & \text{if } D \text{ is odd,} \\ |D|/4 & \text{if } D \text{ if even.} \end{cases}$$

Theorem (Waldspurger).
If $f(z) \in S_{2k}^{\text{new}}(\Gamma_0(M))$ is a newform, then there is a $\delta \in \{\pm\}$ and a

$$g(z) = \sum_{n=1}^{\infty} b(n)q^n \in S_{k+\frac{1}{2}}(\Gamma_0(4N), \chi)$$

with the property that if $\delta D > 0$, then

$$b(D_0)^2 = \begin{cases} \epsilon_D \cdot \frac{L(f_D,k)D_0^{k-\frac{1}{2}}}{\Omega_f} & \text{if } \gcd(D_0, 4N) = 1, \\ 0 & \text{otherwise.} \end{cases}$$

. . . .

Remark. By Kolyvagin, we need to show that

$$b(D_0) \neq 0$$

for the D we have identified.

Using Galois representations, one can show:

"Theorem". Let $f_1(z), f_2(z), \ldots, f_y(z)$ be integer weight cusp forms

$$f_i(z) = \sum_{n=1}^{\infty} a_i(n) q^n \in S_{k_i}(\Gamma_0(M_i)).$$

If $p_0 \nmid \ell M_1 M_2 \cdots M_y$ is prime and $j \geq 1$, then there is a set of primes p with positive density such that for every $1 \leq i \leq y$ we have

$$f_i(z) \mid T_{p_0,k_i} \equiv f_i(z) \mid T_{p,k_i} \pmod{\ell^{j+1}}.$$

Here $T_{p,k}$ is the weight k Hecke operator for p.

1) Let $g(z) = \sum_{n=1}^{\infty} b(n)q^n$ satisfy

$$b(D_0)^2 = \text{stuff} \times L(f_D, k).$$

2) If $p \nmid 4N$ is a prime, then $\exists \lambda(p)$ with

$$b(np^2) = \left(\lambda(p) - \chi^\star(p)p^{\lambda-1}\left(\frac{n}{p}\right)\right) b(n)$$

$$- \chi^\star(p^2)p^{2\lambda-1}b(n/p^2).$$

3) Define the **integer weight** form $G(z)$ by

$$G(z) = \sum_{n=1}^{\infty} b_g(n)q^n = g(z) \cdot \left(1 + 2\sum_{n=1}^{\infty} q^{n^2}\right)$$

$$\equiv g(z) \pmod 2.$$

4) By hypothesis, $\exists \;\; p_0 \nmid 4N$ for which

$$\lambda(p_0) \equiv 1 \pmod 2.$$

. . . .

5) By "Theorem" for $G(z)$ and $f(z)$, we have:

For $j \geq 1$, there is a set of odd primes $S_{p_0,j}$ with positive density satisfying:

- If $p \in S_{p_0,j}$, then

$$\lambda(p) \equiv \lambda(p_0) \equiv 1 \pmod 2.$$

- If $p \in S_{p_0,j}$ then

$$G(z) \mid T_{p,\lambda+1} \equiv G(z) \mid T_{p_0,\lambda+1} \pmod{2^{j+1}}.$$

6) If $\mathrm{ord}_2(b(m)) = s_0$, and $q_1 \in S_{p_0,s_0}$ is coprime to m, then Hecke operators give

$$\big(\text{Coeff. of } q^{mq_1} \text{ in } G(z) \mid T_{q_1}\big) = b_g(mq_1^2) \pm \chi(q_1) q_1^k b_g(m).$$

7) Replacing $b_g(mq_1^2)$, using 2), this is

$$\equiv \lambda(q_1) b_g(m) + b_g(m)\chi^\star(q_1) q_1^{k-1}(\pm q_1 \pm 1) \pmod{2^{s_0+1}}$$

8) Since $\pm q_1 \pm 1 \equiv 0 \pmod 2$, we get

$$\mathrm{ord}_2(\text{Coeff. of } q^{mq_1} \text{ in } G(z) \mid T_{q_1}) = s_0.$$

9) Now 5) implies that if $q_2 \in S_{p_0,s_0}$, then

$$G \mid T_{q_1} \equiv G \mid T_{q_2} \pmod{2^{s_0+1}}$$

$$\Longrightarrow \quad \text{ord}_2(\text{Coeff. of } q^{mq_1} \text{ in } G(z) \mid T_{q_2}) = s_0$$

$$\underset{\text{hecke}}{\Longrightarrow} \text{ord}_2\left(b_g(mq_1q_2) \pm \chi(q_2)q_2^k b_g(mq_1/q_2)\right) = s_0$$

$$\Longrightarrow \quad \text{ord}_2(b_g(mq_1q_2)) = s_0$$

$$\underset{\text{def. } G}{\Longrightarrow} \text{ord}_2(b(mq_1q_2)) = s_0$$

$$\underset{\text{Wald}}{\Longrightarrow} L(f_{\delta mq_1q_2}, k) \neq 0.$$

12) Iterate 6)-9) with pairs q_3, q_4, etc...

$\square$

Summary

Works of Kolyvagin, Shimura, and Waldspurger, and "congruence properties" of modular form coefficients imply:

1) For generic f and $E/\mathbb{Q}$, we have

$$\#\{|D| \le X \ : \ L(f_D, k) \neq 0\} \gg \frac{X}{\log X}$$

$$\#\{|D| \le X \ : \ \mathrm{rk}(E(D)) = 0\} \gg \frac{X}{\log X}.$$

. . . .

2) For E with $2 \nmid \#E_{\mathrm{tor}}$, we have

$$\mathrm{rk}(E(D_E p_1 p_2 \cdots p_{2j})) = 0$$

whenever $p_1, \ldots, p_{2j} \in S_E$.