

**Non-vanishing of the
partition function modulo
small primes.**

Matt Boylan
University of South Carolina
October, 2006.

Partitions.

Definition: A **partition** of a positive integer n is a non-increasing sequence of positive integers whose sum is n .

• $p(n) := \#$ partitions of n ; $p(0) := 1$.

• **Example:** $p(4) = 5$:

$$\begin{array}{cccccc} & & & & & & & 4 \\ & & & & & & & 3 + 1 \\ & & & & & & & 2 + 2 \\ & & & & & & & 2 + 1 + 1 \\ & & & & & & & 1 + 1 + 1 + 1 \\ 1 & + & 1 & + & 1 & + & 1 & + & 1 \end{array}$$

.....

• **Some other values:**

n	$p(n)$
0	1
1	1
2	2
3	3
4	5
32	8349
200	397299029388

- **MacMahon (~1910):** Calculated $p(200)$.
- **Hardy, Ramanujan (1917):** As $n \rightarrow \infty$,

$$p(n) \sim \frac{1}{4n\sqrt{3}} \cdot e^{\pi\sqrt{\frac{2n}{3}}}.$$

They used the “**circle method**” from analytic number theory.

- **Rademacher (1930's):**

Exact formula for $p(n)$:

$$p(n) = \frac{2\pi}{(24n-1)^{\frac{3}{4}}} \sum_{k=1}^{\infty} \frac{A_k(n)}{k} I_{\frac{3}{2}} \left(\frac{\pi\sqrt{24n-1}}{6k} \right).$$

$A_k(n)$'s : exponential sums.

$I_{\frac{3}{2}}$: modified Bessel function of 1st kind.

Euler.

- **Generating function for $p(n)$:**

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

$$= \left(\sum_{n_1=0}^{\infty} q^{n_1} \right) \left(\sum_{n_2=0}^{\infty} q^{2n_2} \right) \left(\sum_{n_3=0}^{\infty} q^{3n_3} \right) \dots$$

- **Pentagonal Number Theorem:**

$$1 + \sum_{n=0}^{\infty} (-1)^n q^{\frac{n(3n\pm 1)}{2}} = \prod_{m=1}^{\infty} (1 - q^m). \quad (2)$$

- **Recursion:** $(1) \times (2) = 1 \implies$

$$p(n) = \sum_{k=1}^{\infty} (-1)^{k+1} p\left(n - \frac{k(3k \pm 1)}{2}\right) \quad \forall n.$$

Distribution of $p(n)$ modulo M .

- Question: How often is $p(n) \equiv r \pmod{M}$?

- Define:

$$\delta_r(M; X) := \frac{\#\{0 < n < X : p(n) \equiv r \pmod{M}\}}{X}.$$

- Example: $X = 10,000$, $M \in \{2, 3, 5, 7\}$.

		M			
		2	3	5	7
r	0	.4996	.3313	.3611	.2744
	1	.5004	.3325	.1531	.1198
	2		.3362	.1657	.1214
	3			.1562	.1202
	4			.1639	.1247
	5				.1187
	6				.1208

- $p(n)$ seems to be **equidistributed** in residue classes modulo 2 and 3. What is going on modulo 5 and 7?

Answer.

Ramanujan (1919):

I have proved a number of arithmetical properties of $p(n)$... in particular that

$$p(5n + 4) \equiv 0 \pmod{5},$$

and

$$p(7n + 5) \equiv 0 \pmod{7} \dots$$

I have since found another method which enables me to prove all of these properties and a variety of others, of which the most striking is

$$p(11n + 6) \equiv 0 \pmod{11}.$$

There are corresponding properties in which the moduli are powers of 5, 7, or 11...

It appears that there are no equally simple properties for any moduli involving primes other than these three.

Ramanujan's Congruences. $\forall n$

$$p(5n + 4) \equiv 0 \pmod{5},$$

$$p(7n + 5) \equiv 0 \pmod{7},$$

$$p(11n + 6) \equiv 0 \pmod{11}.$$

- **Are there other congruences for $p(n)$?**

.....

On one hand, Ramanujan's quote \implies

Conjecture R: Let $\ell \geq 5$ be prime, $a \in \mathbb{Z}$.

If $p(\ell n + a) \equiv 0 \pmod{\ell} \forall n$, then

$$(\ell, a) \in \{(5, 4), (7, 5), (11, 6)\}.$$

.....

Thm. (Ahlgren, B., Invent. Math., 2003):

Conjecture R is true.

In a **broader sense**, there are many linear congruences for $p(n)$.

.....

- **1960's**: Sporadic examples.

Atkin (1967): $\forall n$

$$p(103^3 \cdot 97^3 \cdot 13^2 n - 6950975499604) \equiv 0 \pmod{13^2}.$$

.....

- **Theorem (Ahlgren, Ono, 1999-2001)**:

$\forall M$ coprime to 6, \exists ∞ -ly many progressions $An + B$, none contained in any other, for which

$$p(An + B) \equiv 0 \pmod{M} \quad \forall n.$$

Typical examples. $\forall N$

$$p(48037937 \cdot N + 1122838) \equiv 0 \pmod{17}.$$

$$p(1977147619 \cdot N + 815655) \equiv 0 \pmod{19}.$$

$$p(14375 \cdot N + 3474) \equiv 0 \pmod{23}.$$

$$p(348104768909 \cdot N + 43819835) \equiv 0 \pmod{29}.$$

$$p(4063467631 \cdot N + 30064597) \equiv 0 \pmod{31}.$$

.....

Question: What about $p(n)$ modulo 2 or 3?

Computations suggest $p(n)$ behaves much differently in these cases, but **less is known.**

Parity.

- **Kolberg (1959):** $p(n)$ is infinitely often even and infinitely often odd.

.....

Conjecture 1 (Parkin and Shanks, 1967):

Let $r \in \{0, 1\}$. As $X \mapsto \infty$,

$$\frac{\#\{0 < n < X : p(n) \equiv r \pmod{2}\}}{X} \sim \frac{1}{2}.$$

.....

Results:

- “Even” case (Serre, 1998):

$$\lim_{X \rightarrow \infty} \frac{\#\{0 < n < X : p(n) \equiv 0 \pmod{2}\}}{\sqrt{X}} = +\infty.$$

- “Odd” case (Ono, 2006):

$$\#\{0 < n < X : p(n) \equiv 1 \pmod{2}\} \gg \frac{X}{\log X}.$$

Conjecture 2 (Subbarao, 1966): $\forall r, t \in \mathbb{Z}$
with $0 \leq r < t$, there are ∞ -ly many n with

$$p(tn + r) \not\equiv 0 \pmod{2}.$$

• **Remark:** Conjecture 2 \implies no congruences
of the form $p(An + B) \equiv 0 \pmod{2} \forall n$.

.....

• **Results (1960's - early 1990's):**

Conjecture 2 is true for every $r \pmod{t}$ with

$$t \in \{1, 2, 3, 4, 5, 6, 8, 10, 12, 16, 20, 40\}.$$

Theorem 1 (B., Ono, BLMS, 2001):

Let $s \geq 1$. Conjecture 2 is true $\forall r \pmod{2^s}$.

i.e., for all $0 \leq r < 2^s$, $\exists \infty$ -ly many n with

$$p(2^s n + r) \not\equiv 0 \pmod{2}.$$

.....

More is true: Theorem 1 + estimate
(due to Ahlgren) \implies

$$\#\{n \leq X : n \equiv r \pmod{2^s}, 2 \nmid p(n)\} \gg_s \frac{\sqrt{X}}{\log X}.$$

Remarks.

(1) Ono (Crelle, 1996): Conj. 2 holds for a residue class $r \pmod{t}$ provided there is **at least one** $n \equiv r \pmod{t}$ with $p(n)$ odd.

.....

Consequence: Fix t . To prove Conj. 2 for the modulus t , it suffices, $\forall r \pmod{t}$, to find an $n \equiv r \pmod{t}$ with $p(n)$ odd.

- **Ono:** True $\forall r \pmod{t}$ with $t \leq 10^5$.

- **B., Ono (Theorem 1):**

True $\forall r \pmod{t}$ with $t = \text{power of } 2$.

.....

(2) “Even” analogue. Ono also proved:
 $\forall r, t$ with $0 \leq r < t$, there are ∞ -ly many $n \equiv r \pmod{t}$ with $p(n)$ **even**.

The partition function modulo 3.

- **Ono (2006):** $p(n) \equiv 0 \pmod{3}$ for infinitely many n .

He used a generalization of Borcherd's theory of automorphic infinite products.

.....

Conjectures: (Ahlgren, Ono, 2000):

Conjecture 3: Let $r \in \{0, 1, 2\}$. As $X \mapsto \infty$,

$$\frac{\#\{0 < n < X : p(n) \equiv r \pmod{3}\}}{X} \sim \frac{1}{3}.$$

Conjecture 4: $\forall r, t \in \mathbb{Z}$ with $0 \leq r < t$, there are ∞ -ly many n with

$$p(tn + r) \not\equiv 0 \pmod{3}.$$

- **Remark:** Conjecture 4 \implies no congruences of the form $p(An + B) \equiv 0 \pmod{3}$.

Theorem 2 (B., to appear in IMRN):

Let $r, s \in \mathbb{Z}$ with $s \geq 1$ and $0 \leq r < 3^s$. Then:

$$\#\{n \leq X : n \equiv r \pmod{3^s}, 3 \nmid p(n)\} \gg_s \frac{\sqrt{X}}{\log X}.$$

.....

Remarks.

(1) Theorem 2 settles Conjecture 4 for every $r \pmod{3^s}$. This is the only infinite family of moduli for which Conjecture 4 is known.

(2) Let l be prime. We say that r is a **good residue class** for l modulo t if

$$\#\{n \leq X : n \equiv r \pmod{t}, l \nmid p(n)\} \gg_{r,t} \frac{\sqrt{X}}{\log X}.$$

Theorem 3: Let $l \in \{5, 7, 11\}$, $s \geq 1$. Then

$$\frac{\#\{\text{good res. classes for } l \pmod{l^s}\}}{l^s} \geq \frac{1}{l}.$$

Proof of Theorem 2.

Important Preliminary Fact:

Theorem (Ahlgren, 1999):

Let ℓ be an odd prime and $r, t \in \mathbb{Z}$ with $0 \leq r < t$. Suppose also that $\exists n \equiv r \pmod{t}$ with $p(n) \not\equiv 0 \pmod{\ell}$. Then

$$\#\{n \leq X : n \equiv r \pmod{t}, \ell \nmid p(n)\} \gg_t \frac{\sqrt{X}}{\log X}.$$

Result: To prove Theorem 2, it suffices,

$\forall r \pmod{3^s}$, to find $n \equiv r \pmod{3^s}$

with $p(n) \not\equiv 0 \pmod{3}$.

.....

The proof uses facts about **modular forms** and **Galois representations**.

Modular Forms.

Objects:

- $SL_2(\mathbb{Z}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}; ad - bc = 1 \right\}.$

- **Upper half-plane:** $\mathfrak{h} := \{z \in \mathbb{C} : \text{Im } z > 0\}.$

.....

Properties of $SL_2(\mathbb{Z})$:

Acts on \mathfrak{h} by **Möbius transformations:**

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az + b}{cz + d}.$$

Generators:

$$S := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ and } T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Definition: Let $k \in \mathbb{Z}$. A function $f : \mathfrak{h} \rightarrow \mathbb{C}$ is a **modular form of weight k** on $SL_2(\mathbb{Z})$ if

(1) $\forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}),$

$$f\left(\frac{az + b}{cz + d}\right) = (cz + d)^k f(z).$$

(2) f is **holomorphic** on \mathfrak{h} .

(3) f is **holomorphic** at ∞ :

i.e., $\lim_{z \rightarrow i\infty} f(z)$ exists.

Notation: The set of such forms is M_k .

.....

If $f \in M_k$ has $\lim_{z \rightarrow i\infty} f(z) = 0$, then f is a **cuspidal form**.

The set of cuspidal forms in M_k is denoted by S_k .

Fact: M_k and S_k are finite-dimensional \mathbb{C} -vector spaces.

.....

Fourier series:

(1) $f(z) = f(z + 1)$. (by transformation law)

(2) $f(z)$ is holomorphic on \mathfrak{h} .

$$\implies f(z) = \sum_{n=0}^{\infty} a(n)e^{2\pi inz}.$$

Set $q := e^{2\pi iz}$.

We identify $f(z)$ with its **q-expansion:**

$$f(z) = \sum_{n=0}^{\infty} a(n)q^n.$$

Example: Ramanujan's Delta function.

$$\begin{aligned}\Delta(z) &:= q \prod_{n=1}^{\infty} (1 - q^n)^{24} = \sum_{n=1}^{\infty} \tau(n)q^n \\ &= q - 24q^2 + 252q^3 - \dots \in S_{12}.\end{aligned}$$

.....

Properties of $\tau(n)$:

- (1) $\gcd(m, n) = 1 \implies \tau(mn) = \tau(m)\tau(n)$.
- (2) $\tau(n) \equiv \sum_{d|n} d^{11} \pmod{691}$. (**Ramanujan**)
- (3) If p is prime, $|\tau(p)| \leq 2p^{\frac{11}{2}}$. (**Deligne**)
- (4) **Conjecture (Lehmer)**: $\forall n, \tau(n) \neq 0$.

Back to the proof of Theorem 2.

(1) Euler's generating function:

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

• Let $s \geq 1$. $\forall n, j \geq 0$, define $a_s(n), r_s(j) \in \mathbb{Z}$:

(2) $\sum_{n=1}^{\infty} a_s(n)q^n := \Delta(z)^{\frac{9^s-1}{8}} \in S_{\frac{3(9^s-1)}{2}}$.

(3) $\sum_{j=0}^{\infty} r_s(j)q^{3 \cdot 9^s j} := \prod_{n=1}^{\infty} (1 - q^{3 \cdot 9^s j})$.

.....

• Modular forms and $p(n) \pmod{3}$:

Proposition 1: $\forall n$

$$a_s(n) \equiv \sum_{j=0}^{\infty} r_s(j)p\left(\frac{n - \frac{9^s-1}{8}}{3} - 9^s j\right) \pmod{3}.$$

Idea: Non-vanishing of $a_s(n) \pmod{3}$

\implies non-vanishing of $p(n) \pmod{3}$.

.....

Proof of Proposition 1: Compute mod 3:

$$\begin{aligned} \Delta^{\frac{9^s-1}{8}} &= \left(q \cdot \prod_{n=1}^{\infty} (1 - q^n)^{24} \right)^{\frac{9^s-1}{8}} \\ &\equiv q^{\frac{9^s-1}{8}} \prod_{n=1}^{\infty} (1 - q^{3 \cdot 9^s}) \cdot \prod_{m=1}^{\infty} \frac{1}{1 - q^{3m}} \\ &\equiv \left(\sum_{j=0}^{\infty} r_s(j) q^{3 \cdot 9^s j} \right) \cdot \left(\sum_{k=0}^{\infty} p(k) q^{3k + \frac{9^s-1}{8}} \right) \\ &\equiv \sum_{n=0}^{\infty} \left(\sum_{j=0}^{\infty} r_s(j) p \left(\frac{n - \frac{9^s-1}{8}}{3} - 9^s j \right) \right) q^n. \end{aligned}$$

A crucial non-vanishing lemma.

Lemma 2: Let $s \geq 1$. Then $\exists n_s \geq 1$ with

- $n_s \equiv 1 \pmod{3}$.
- $a_s(n_s) \not\equiv 0 \pmod{3}$.
- \forall prime $\ell \nmid n_s$ with $\ell \equiv 2 \pmod{3}$,
$$a_s(n_s \ell^2) \not\equiv 0 \pmod{3}.$$

.....

Significance: Uniformly describes ∞ -ly many coefficients of a modular form which are not divisible by 3.

Proposition 3: Lemma 2 \implies Theorem 2.

i.e., Lemma 2 $\implies \exists \infty$ -ly many $n \equiv r \pmod{3^s}$ with $3 \nmid p(n)$.

Proof of Proposition 3: It suffices to show:

If $0 \leq r < 9^s$, then $\exists M \equiv r \pmod{9^s}$
with $p(M) \not\equiv 0 \pmod{3}$.

• **Lemma 2** $\implies \exists n_s$ such that $\forall \ell \nmid n_s$ with
 $\ell \equiv 2 \pmod{3}$, $a_s(n_s \ell^2) \not\equiv 0 \pmod{3}$.

• **Proposition 1** $\implies \exists j \geq 0$ with

$$p\left(\frac{n_s \ell^2 - \frac{9^s - 1}{8}}{3} - 9^s j\right) \not\equiv 0 \pmod{3}.$$

Vary ℓ over $\{\text{primes } \ell : \ell \nmid n_s \text{ and } \ell \equiv 2 \pmod{3}\}$.

• **Hensel's Lemma + Dirichlet's Thm.** \implies
the numbers $\frac{n_s \ell^2 - \frac{9^s - 1}{8}}{3}$ cover all $r \pmod{9^s}$.

Tools for the proof of Lemma 2.

(1) Modular forms modulo N.

From here on, set $M_k := M_k \cap \mathbb{Z}[[q]]$.

Let $N \in \mathbb{Z}$ and let

$$f(z) = \sum a(n)q^n,$$

$$g(z) = \sum b(n)q^n \in M_k.$$

Congruence of modular forms:

$$f(z) \equiv g(z) \pmod{N}$$

$$\iff \forall n, a(n) \equiv b(n) \pmod{N}.$$

(2) Hecke operators.

Definition: \forall primes p , $\exists T_{p,k} : M_k \mapsto M_k$,

$$\sum a(n)q^n | T_{p,k} := \sum \left(a(np) + p^{k-1} a\left(\frac{n}{p}\right) \right) q^n,$$

where $a\left(\frac{n}{p}\right) = 0$ if $p \nmid n$.

Definition: Let p be prime. If $\exists \lambda_p \in \mathbb{Z}$ such that $f \in M_k$ has

$$f | T_{p,k} = \lambda_p f,$$

then f is an **eigenform** for $T_{p,k}$.

.....

Proposition 4: Let $\ell \in \{2, 3, 5, 7\}$. Suppose that \forall prime $p \neq \ell$, f is an eigenform for $T_{p,k}$. If $p \equiv -1 \pmod{\ell}$, then $\lambda_p \equiv 0 \pmod{\ell}$.

$$\text{i.e., } f | T_{p,k} \equiv 0 \pmod{\ell}.$$

Galois representations.

Suppose: \forall primes p , $f(z) = \sum_{n=1}^{\infty} a(n)q^n \in S_k$

is an eigenform for $T_{p,k}$ with eigenvalue $\lambda_p \in \mathbb{Z}$.

.....

• **Deligne:** \forall primes ℓ , there is a continuous semisimple mod ℓ **Galois representation** ramified only at ℓ ,

$$\rho_{\ell,f} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \mapsto \text{GL}_2(\mathbb{Z}/\ell\mathbb{Z}),$$

such that \forall primes $p \neq \ell$,

$$\text{Tr} \rho_{\ell,f}(\text{Frob}_p) \equiv \lambda_p \pmod{\ell}$$

$$\text{Det} \rho_{\ell,f}(\text{Frob}_p) \equiv p^{k-1} \pmod{\ell}.$$

.....

• **Atkin, Serre, Tate:** If $\ell \in \{2, 3, 5, 7\}$, then $\rho_{\ell,f}$ must be **reducible**.

Proof of Proposition 4 for $\ell = 3$:

- Let χ_3 be the mod 3 **cyclotomic character**:

If $p \neq 3$ is prime, then $\chi_3(p) \equiv 0 \pmod{3}$.

- $\rho_{3,f}$ **reducible** implies that

$$\rho_{3,f} = 1 \oplus \chi_3.$$

- If $p \equiv -1 \pmod{3}$ is prime, then

Deligne's Theorem \implies

$$\lambda_p \equiv \text{Tr} \rho_{3,f}(\text{Frob}_p) \equiv 1 + p \equiv 0 \pmod{3}.$$

.....

Consequence: \forall primes $p \equiv 2 \pmod{3}$,

$T_{p,k} : M_k \mapsto M_k$ is **nilpotent** mod 3.

An important definition:

Let $f(z) \in M_k$ with $f(z) \not\equiv 0 \pmod{3}$.

.....

• $f(z)$ has **nilpotency degree** $i = 1$ if

\forall prime $p \not\equiv 1 \pmod{3}$, $f \mid T_{p,k} \equiv 0 \pmod{3}$.

• $f(z)$ has **nilpotency degree** $i \geq 2$ if

(1) \exists distinct primes $p_1, \dots, p_{i-1} \not\equiv 1 \pmod{3}$

such that $f \mid T_{p_1,k} \mid \dots \mid T_{p_{i-1},k} \not\equiv 0 \pmod{3}$.

(2) \forall coll. of distinct primes $\ell_1, \dots, \ell_i \not\equiv 1 \pmod{3}$,

$f \mid T_{\ell_1,k} \mid \dots \mid T_{\ell_i,k} \equiv 0 \pmod{3}$.

.....

Summary: The **nilpotency degree** of f is the smallest number of $T_{p,k}$'s guaranteed to always annihilate $f \pmod{3}$.

Notation:

$\text{nil}(f) :=$ nilpotency degree of $f(z)$.

Examples:

(1) $f \in M_k \implies \text{nil}(f) \leq \dim(S_k)$.

(2) $\text{nil}(\Delta) = 1; \text{nil}(\Delta^7) = 5$.

.....

Question : Suppose that $\sum a(n)q^n \in M_k$
has $\text{nil}(f) = i \geq 1$.

What can one say about which coefficients
 $a(n) \not\equiv 0 \pmod{3}$?

Proposition 5: Let $f(z) = \sum a(n)q^n \in M_k$ have $\text{nil}(f) = i$.

.....

• If $i = 1$, then $\exists s \geq 1$ such that

(1) s is divisible only by primes $p \equiv 1 \pmod{3}$.

(2) $a(s) \not\equiv 0 \pmod{3}$.

.....

• If $i \geq 2$, then $\exists n_0 \geq 1$ and distinct primes $p_1, \dots, p_{i-1} \not\equiv 1 \pmod{3}$ such that

(1) $n_0 \equiv 1 \pmod{3}$.

(2) $\gcd(n_0, p_1 \cdots p_{i-1}) = 1$.

(3) $a(n_0 p_1 \cdots p_{i-1}) \not\equiv 0 \pmod{3}$.

.....

Point: $\text{nil}(f)$ tells us something about indices of non-vanishing coefficients mod 3.

Proof of Lemma 2.

Recall:

$$(1) \quad \sum a_s(n)q^n = \Delta(z)^{\frac{9^s-1}{8}}.$$

(2) **Lemma 2:** Let $s \geq 1$. $\exists n_s \equiv 1 \pmod{3}$,

- $a_s(n_s) \not\equiv 0 \pmod{3}$.

- \forall prime $\ell \nmid n_s$ with $\ell \equiv 2 \pmod{3}$,

$$a_s(n_s \ell^2) \not\equiv 0 \pmod{3}.$$

.....

Set $i := \text{nil}(\Delta^{\frac{9^s-1}{8}}) \geq 1$.

Prop. 5 $\implies \exists n_0 \equiv 1 \pmod{3}$ and distinct primes $p_1, \dots, p_{i-1} \equiv 2 \pmod{3}$ such that

- $\text{gcd}(n_0, p_1 \cdots p_{i-1}) = 1$.

- $a_s(n_0 p_1 \cdots p_{i-1}) \not\equiv 0 \pmod{3}$.

$$\text{nil}(\Delta^{\frac{9^s-1}{8}}) = i \implies \forall n, c_{i-1}(n) \equiv 0 \pmod{3}.$$

Set $n = n_0\ell$. Then, in particular, we have

$$c_{i-1}(n_0\ell) \equiv 0 \pmod{3}.$$

.....

Recall:

$$\sum a(n)q^n \mid T_{p,k} = \sum \left(a(pn) + p^{k-1}a\left(\frac{n}{p}\right) \right) q^n.$$

Observe:

- $\sum c_{i-1}(n)q^n \equiv \sum c_{i-2}(n)q^n \mid T_{p_{i-1},k}$.

- Since $p_{i-1} \nmid n_0\ell$, formula for $T_{p,k}$'s \implies

$$\begin{aligned} 0 &\equiv c_{i-1}(n_0\ell) \equiv c_{i-2}(n_0\ell p_{i-1}) + 2c_{i-2}\left(\frac{n_0\ell}{p_{i-1}}\right) \\ &\equiv c_{i-2}(n_0 p_{i-1} \ell) \pmod{3}. \end{aligned}$$

Repeat this “unwinding” process.

Since $\ell, p_1, \dots, p_{i-1}$ are distinct primes and $\gcd(n_0, \ell p_1 \cdots p_{i-1}) = 1$, we obtain:

.....

$$\begin{aligned}
 0 &\equiv c_{i-1}(n_0\ell) \\
 &\equiv c_{i-2}(n_0p_{i-1}\ell) \\
 &\equiv c_{i-3}(n_0p_{i-2}p_{i-1}\ell) \\
 &\quad \vdots \\
 &\equiv c_0(n_0p_1 \cdots p_{i-1}\ell) \\
 &\equiv a_s(n_0p_1 \cdots p_{i-1}\ell^2) + 2a_s(n_0p_1 \cdots p_{i-1}) \pmod{3}.
 \end{aligned}$$

.....

Therefore,

$$a_s(n_0p_1 \cdots p_{i-1}\ell^2) \equiv a_s(n_0p_1 \cdots p_{i-1}) \not\equiv 0 \pmod{3}.$$

Lemma 2 follows with $n_s = n_0p_1 \cdots p_{i-1}$.