

NON-VANISHING OF THE PARTITION FUNCTION MODULO SMALL PRIMES

MATTHEW BOYLAN

ABSTRACT. Let $p(n)$ be the ordinary partition function. We show, for all integers r and s with $s \geq 1$ and $0 \leq r < 3^s$, that

$$\#\{n \leq X : n \equiv r \pmod{3^s} \text{ and } p(n) \not\equiv 0 \pmod{3}\} \gg_{r,s} \frac{\sqrt{X}}{\log X}.$$

We also prove a similar result on the non-vanishing of $p(n)$ modulo $\ell \in \{5, 7, 11\}$.

1. INTRODUCTION AND STATEMENT OF RESULTS.

A *partition* of a positive integer n is a non-increasing sequence of positive integers whose sum is n . We denote by $p(n)$ the number of partitions of n . By convention, we set $p(0) := 1$. Euler showed that the generating function for $p(n)$ satisfies

$$(1.1) \quad \sum_{n=0}^{\infty} p(n)q^n = \prod_{m=1}^{\infty} \frac{1}{1 - q^m}.$$

Among the most well-known contributions of Ramanujan to the study of partitions are the congruences which now bear his name. These are, for all integers $n \geq 0$,

$$(1.2) \quad p(5n + 4) \equiv 0 \pmod{5}$$

$$(1.3) \quad p(7n + 5) \equiv 0 \pmod{7}$$

$$(1.4) \quad p(11n + 6) \equiv 0 \pmod{11}.$$

After Ramanujan, relatively few linear congruences for $p(n)$ beyond (1.2), (1.3), (1.4), and their extensions modulo powers of 5, 7, and 11 had been discovered until recent work of Ahlgren and Ono [3, 5, 11]. They proved, for every modulus M coprime to 6, that there are infinitely many arithmetic progressions $An + B$, none contained in any other, such that

$$p(An + B) \equiv 0 \pmod{M} \text{ for all } n.$$

By contrast, less is known about $p(n)$ modulo 2 or 3. In this paper, we consider the following conjecture.

Conjecture S. *Let r and t be integers with $0 \leq r < t$.*

(1) *There are infinitely many integers $n \equiv r \pmod{t}$ such that $p(n) \not\equiv 0 \pmod{2}$.*

(2) *There are infinitely many integers $m \equiv r \pmod{t}$ such that $p(m) \not\equiv 0 \pmod{3}$.*

Remark 1. Subbarao [15] conjectured (1) in 1966, while Ahlgren and Ono conjectured (2) in 2001 [4, Conjecture 5.2]. For other conjectures and problems on the arithmetic of $p(n)$, many of which remain unsettled, the reader should consult [12, Section 5.4].

Date: May 31, 2006.

2000 Mathematics Subject Classification. 11P83, 11F11.

Remark 2. Conjecture S implies that there are no linear congruences for $p(n)$ modulo 2 or 3.

Remark 3. In earlier work, Ono [10] proved the “even” analogue of (1): For all integers r and t with $0 \leq r < t$, there are infinitely many $n \equiv r \pmod{t}$ such that $p(n) \equiv 0 \pmod{2}$. Combined with an estimate of Serre [9], this work gives

$$\#\{n \leq X : n \equiv r \pmod{t} \text{ and } p(n) \equiv 0 \pmod{2}\} \gg_{r,t} \sqrt{X}.$$

In recent unpublished work, Ono has also proved that there are infinitely many n for which $p(n) \equiv 0 \pmod{3}$ using a generalization of Borchers’ theory of automorphic infinite products. However, his result is not refined to the point where one knows that there are infinitely many such n in any fixed arithmetic progression.

We now summarize the main results on Conjecture S. Prior to the mid 1990’s, part (1) was known (see [10] for references) for every arithmetic progression $r \pmod{t}$ with

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

In [10], Ono showed that if there is at least one integer $n \equiv r \pmod{t}$ with $p(n) \not\equiv 0 \pmod{2}$, then there are infinitely many such n . Hence, to verify part (1) of Conjecture S for a fixed arithmetic progression $r \pmod{t}$, it suffices to give a single integer $n \equiv r \pmod{t}$ for which $p(n) \not\equiv 0 \pmod{2}$. This was done by Ono in [10] for every arithmetic progression $r \pmod{t}$ with $t \leq 10^5$ and by Ono and the author in [6] for every arithmetic progression whose modulus is a power of 2, thus providing the first infinite family of arithmetic progressions for which part (1) of Conjecture S is true.

Theorem 1.1. *Let r and s be integers with $s \geq 1$ and $0 \leq r < 2^s$. Then part (1) of Conjecture S holds for the arithmetic progression $r \pmod{2^s}$. Moreover, we have*

$$\#\{n \leq X : n \equiv r \pmod{2^s} \text{ and } p(n) \not\equiv 0 \pmod{2}\} \gg_{r,s} \frac{\sqrt{X}}{\log X}.$$

The estimate in Theorem 1.1 follows from our work together with a theorem of Ahlgren [1, Theorem 1.4].

In this paper, we furnish the first infinite family of arithmetic progressions for which part (2) of Conjecture S is true. Our methods also apply to the study of the non-vanishing of $p(n)$ modulo 5 and 7. We prove

Theorem 1.2. *Let $s \geq 1$ be an integer.*

- (1) *Suppose that r is an integer with $0 \leq r < 3^s$. Then part (2) of Conjecture S holds for the arithmetic progression $r \pmod{3^s}$. Moreover, we have*

$$\#\{n \leq X : n \equiv r \pmod{3^s} \text{ and } p(n) \not\equiv 0 \pmod{3}\} \gg_{r,s} \frac{\sqrt{X}}{\log X}.$$

- (2) *There is an integer $g_s \not\equiv 4 \pmod{5}$ such that for all integers u with $0 \leq 5u + g_s < 5^s$, we have*

$$\#\{n \leq X : n \equiv 5u + g_s \pmod{5^s} \text{ and } p(n) \not\equiv 0 \pmod{5}\} \gg_{u,s} \frac{\sqrt{X}}{\log X}.$$

- (3) *There is an integer $h_s \not\equiv 5 \pmod{7}$ such that for all integers v with $0 \leq 7v + h_s < 7^s$, we have*

$$\#\{n \leq X : n \equiv 7v + h_s \pmod{7^s} \text{ and } p(n) \not\equiv 0 \pmod{7}\} \gg_{v,s} \frac{\sqrt{X}}{\log X}.$$

Remark 1. The methods we use to prove Theorem 1.2 are natural adaptations and generalizations of the methods used to prove Theorem 1.1. Most (if not all) of the results in Sections 2-4 are stated for $\ell \in \{3, 5, 7\}$, but also hold for $\ell = 2$.

Remark 2. Theorem 1.2 continues to hold for $\ell = 11$, and the proof in this case is a modification of the proof for $\ell \in \{5, 7\}$. In particular, one can show that if $s \geq 1$ is an integer, then there is an integer $i_s \not\equiv 6 \pmod{11}$ such that for all integers w with $0 \leq 11w + i_s < 11^s$, we have

$$\#\{n \leq X : n \equiv 11w + i_s \pmod{11^s} \text{ and } p(n) \not\equiv 0 \pmod{11}\} \gg_{w,s} \frac{\sqrt{X}}{\log X}.$$

To see this, one observes that the proof of Theorem 1.2 for $\ell \in \{5, 7\}$ depends on Lemma 2.2. In turn, Lemma 2.2 relies crucially on the existence of the Ramanujan congruences modulo $\ell \in \{5, 7\}$ and the fact that, for $\ell \in \{5, 7\}$, a modular mod ℓ Galois representation ramified only at ℓ must be reducible. Therefore, in view of the Ramanujan congruence modulo 11, to produce a generalization of Lemma 2.2 to $\ell = 11$, we need to study modular mod 11 Galois representations ramified only at 11. Unfortunately, there is an irreducible modular Galois representation of this type arising from the fact that

$$\Delta(z) \equiv \eta^2(z)\eta^2(11z) \pmod{11},$$

where $\eta(z)$ is Dedekind's eta-function. This representation is induced by the Galois action on the 11-torsion points of $X_0(11)$. Using fundamental lemmas of Swinnerton-Dyer [16, Lemma 7] and Ono and Skinner [13], one can show that there exists a set of primes $m \equiv -1 \pmod{11}$ (which satisfy some other complicated conditions coming from the properties of $X_0(11)$) for which the conclusion of Lemma 2.2 holds for $\ell = 11$. We emphasize that for the purpose of proving Theorem 1.2 and its analogue for $\ell = 11$, we merely require the existence of such primes; a simple, explicit description is not necessary. However, a simple, explicit description of the primes m in Lemma 2.2 is possible when $\ell \in \{5, 7\}$ since the associated modular mod ℓ Galois representations are reducible in these cases.

Before giving the proof of Theorem 1.2, we cite an important fact due to Ahlgren [2].

Theorem 1.3. *Let ℓ be an odd prime, and let r and t be integers with $0 \leq r < t$. Suppose that there is an integer $n \equiv r \pmod{t}$ such that $p(n) \not\equiv 0 \pmod{\ell}$. Then we have*

$$\#\{n \leq X : n \equiv r \pmod{t} \text{ and } p(n) \not\equiv 0 \pmod{\ell}\} \gg_{r,t} \frac{\sqrt{X}}{\log X}.$$

Let $\ell \in \{3, 5, 7\}$, and let $s \geq 1$. In view of Theorem 1.3, to prove Theorem 1.2 for a fixed arithmetic progression $r \pmod{\ell^s}$, it suffices to exhibit a single $n \equiv r \pmod{\ell^s}$ with $p(n) \not\equiv 0 \pmod{\ell}$. We devote Sections 2-4 of this paper to this task. In Section 2, we relate modular forms to partitions. In particular, we state a precise lemma on the non-vanishing of modular form coefficients modulo ℓ , and we show that its truth implies Theorem 1.2. In Section 3, we study the non-vanishing of modular form coefficients modulo ℓ , and in Section 4, we use the results from Section 3 to complete the proof of Theorem 1.2.

Acknowledgments. The author thanks K. Ono for several helpful conversations in the preparation of this paper.

2. MODULAR FORMS AND PARTITIONS.

The proofs of our theorems require the theory of modular forms (see, for example, [8] for details). We begin by fixing notation. Let $k \geq 4$ be an even integer. We denote by M_k the finite-dimensional complex vector space of holomorphic modular forms of weight k on $\mathrm{SL}_2(\mathbb{Z})$. Setting $q := e^{2\pi iz}$, we identify a modular form $f(z) \in M_k$ with its q -expansion,

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

The subspace of cusp forms in M_k , denoted by S_k , consists of forms $f(z)$ with $a_f(0) = 0$. The principal cusp form of interest to us is the Delta function of Ramanujan, given by

$$(2.1) \quad \Delta(z) := q \prod_{n=1}^{\infty} (1 - q^n)^{24} \in S_{12}.$$

Let $s \geq 1$ be an integer, and let $\ell \in \{3, 5, 7\}$. For integers $n \geq 1$, we define integers $a_{s,\ell}(n)$ by

$$(2.2) \quad \sum_{n=1}^{\infty} a_{s,\ell}(n)q^n := \begin{cases} \Delta(z)^{\frac{\ell^{2s}-1}{8}} & \text{if } \ell = 3 \\ \Delta(z)^{\frac{\ell^{2s}-1}{24}} & \text{if } \ell \in \{5, 7\}. \end{cases}$$

We also define, for every integer $j \geq 0$, integers $r_{s,\ell}(j)$ by

$$(2.3) \quad \sum_{j=0}^{\infty} r_{s,3}(j)q^{3 \cdot 9^s j} := \prod_{n=1}^{\infty} (1 - q^{3 \cdot 9^s n}),$$

$$(2.4) \quad \sum_{j=0}^{\infty} r_{s,\ell}(j)q^{\ell^{2s} j} := \prod_{n=1}^{\infty} (1 - q^{\ell^{2s} n}) \quad \text{if } \ell \in \{5, 7\}.$$

The following proposition establishes a recursive formula modulo ℓ for the modular form coefficients $a_{s,\ell}(n)$ in terms of partition values in certain arithmetic progressions modulo powers of ℓ^2 .

Proposition 2.1. *Let $n \geq 1$ be an integer, and let $\ell \in \{3, 5, 7\}$.*

(1) *We have*

$$a_{s,\ell}(n) \equiv \begin{cases} \sum_{j=0}^{\infty} r_{s,\ell}(j)p \left(\frac{n - \frac{\ell^{2s}-1}{8}}{3} - \ell^{2s} j \right) & \pmod{\ell} \quad \text{if } \ell = 3 \\ \sum_{j=0}^{\infty} r_{s,\ell}(j)p \left(n - \left(\frac{\ell^{2s}-1}{24} \right) - \ell^{2s} j \right) & \pmod{\ell} \quad \text{if } \ell \in \{5, 7\}. \end{cases}$$

(2) *If $n \equiv 0$ or $2 \pmod{3}$, then we have $a_{s,3}(n) \equiv 0 \pmod{3}$.*

(3) *If $\ell \in \{5, 7\}$ and $n \equiv 0 \pmod{\ell}$, then we have $a_{s,\ell}(n) \equiv 0 \pmod{\ell}$.*

Proof. We prove the $\ell = 3$ case of (1). The proofs of the $\ell = 5$ and 7 cases are similar. Computing modulo 3 using (1.1), (2.1), (2.2), and (2.3), we obtain

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

To prove (2), we note that $\frac{9^s-1}{8} \equiv 1 \pmod{3}$ for all $s \geq 1$. Therefore, if $n \equiv 0, 2 \pmod{3}$, part (1) of the proposition implies that $a_{s,3}(n) \equiv 0 \pmod{3}$. To prove (3) for $\ell = 5$ (respectively $\ell = 7$), we observe by (1.2) (respectively (1.3)) that for every integer n ,

$$p \left(\ell n - \frac{\ell^{2s} - 1}{24} - \ell^{2s} j \right) \equiv 0 \pmod{\ell}.$$

For $\ell \in \{5, 7\}$, it now follows by part (1) of the proposition that $a_{s,\ell}(\ell n) \equiv 0 \pmod{\ell}$. \square

The following lemma gives, for our purposes, the crucial non-vanishing properties modulo ℓ of the coefficients $a_{s,\ell}(n)$.

Lemma 2.2. *Let $s \geq 1$ be an integer, and let $\ell \in \{3, 5, 7\}$. There is an integer $n_{s,\ell} \geq 1$ such that*

- (1) $n_{s,\ell} \not\equiv \begin{cases} 0, 2 & \pmod{\ell} \text{ if } \ell = 3 \\ 0 & \pmod{\ell} \text{ if } \ell \in \{5, 7\}. \end{cases}$
- (2) $a_{s,\ell}(n_{s,\ell}) \not\equiv 0 \pmod{\ell}$.
- (3) *For every prime $m \nmid n_{s,\ell}$ with $m \equiv -1 \pmod{\ell}$, we have $a_{s,\ell}(n_{s,\ell}m^2) \not\equiv 0 \pmod{\ell}$.*

We defer the proof of Lemma 2.2 to Section 4. The next proposition highlights the significance of Lemma 2.2.

Proposition 2.3. *Lemma 2.2 implies Theorem 1.2.*

Proof. We first prove the proposition in the case $\ell = 3$. By Theorem 1.3, it suffices to show, for all integers r and s with $s \geq 1$ and $0 \leq r < 9^s$, that there is an integer $M_{s,r} \equiv r \pmod{9^s}$ for which $p(M_{s,r}) \not\equiv 0 \pmod{3}$. By Lemma 2.2, there is a positive integer $n_{s,3} \equiv 1 \pmod{3}$ such that for every prime $m \nmid n_{s,3}$ with $m \equiv -1 \pmod{3}$, we have $a_{s,3}(n_{s,3}m^2) \not\equiv 0 \pmod{3}$. Using Proposition 2.1, we see that

$$0 \not\equiv a_{s,3}(n_{s,3}m^2) \equiv \sum_{j=0}^{\infty} r_{s,3}(j)p \left(\frac{n_{s,3}m^2 - \frac{9^s-1}{8}}{3} - 9^s j \right) \pmod{3}.$$

Hence, it follows that there is an integer $j \geq 0$ for which

$$(2.5) \quad p \left(\frac{n_{s,3}m^2 - \frac{9^s-1}{8}}{3} - 9^s j \right) \not\equiv 0 \pmod{3}.$$

We emphasize that (2.5) holds for all primes $m \nmid n_{s,3}$ with $m \equiv -1 \pmod{3}$. Using Hensel's Lemma, one can show that the quadratic congruence in the variable x ,

$$(2.6) \quad \frac{n_{s,3}x^2 - \frac{9^s-1}{8}}{3} \equiv r \pmod{9^s},$$

has a unique solution $x \pmod{9^s}$ with $x \equiv -1 \pmod{3}$. By Dirichlet's Theorem, there are infinitely many primes $m \equiv x \pmod{9^s}$. In particular, there must be a prime $m_{s,r} \nmid n_{s,3}$ with $m_{s,r} \equiv -1 \pmod{3}$ satisfying (2.6). The result now follows with

$$M_{s,r} = \frac{n_{s,3}m_{s,r}^2 - \frac{9^s-1}{8}}{3}.$$

The $\ell = 5$ case differs slightly from the $\ell = 3$ case. Let $s \geq 1$ be an integer, and let $n_{s,5}$ be the integer whose existence is guaranteed by the $\ell = 5$ case of Lemma 2.2. By Theorem 1.3, it suffices to show, for all integers r with $r \equiv n_{s,5} - 1 \pmod{5}$ and $0 \leq r < 25^s$, that there is an integer $N_{s,r} \equiv r \pmod{25^s}$ for which $p(N_{s,r}) \not\equiv 0 \pmod{5}$. We note that $r \not\equiv 4 \pmod{5}$ since $n_{s,5} \not\equiv 0 \pmod{5}$.

To conclude the proof, we argue as in the case of $\ell = 3$, using the properties of $n_{s,5}$, Lemma 2.1, Hensel's Lemma, and Dirichlet's Theorem to produce an integer $N_{s,r}$ with the required properties. The $\ell = 7$ case is similar. □

3. MODULAR FORM COEFFICIENTS MODULO 3, 5, AND 7.

In view of Lemma 2.3, it suffices to prove Lemma 2.2. In this section, we use modular forms modulo primes ℓ , Hecke operators, and Galois representations to develop general techniques for studying the non-vanishing modulo $\ell \in \{3, 5, 7\}$ of ℓ -integral Fourier coefficients of modular forms on $\mathrm{SL}_2(\mathbb{Z})$.

To begin, let ℓ be prime, and let $f(z) = \sum a(n)q^n$ and $g(z) = \sum b(n)q^n \in M_k \cap \mathbb{Z}_{(\ell)}[[q]]$, where $\mathbb{Z}_{(\ell)}$ is the localization of the integers at (ℓ) . We say that $f(z) \equiv g(z) \pmod{\ell}$ if and only if for all integers $n \geq 0$, $a(n) \equiv b(n) \pmod{\ell}$.

For every prime p , there is a Hecke operator $T_{p,k} : S_k \mapsto S_k$ whose action is given by

$$(3.1) \quad \left(\sum_{n=0}^{\infty} a(n)q^n \right) | T_{p,k} = \sum_{n=0}^{\infty} \left(a(pn) + p^{k-1}a\left(\frac{n}{p}\right) \right) q^n.$$

We note that if $p \nmid n$, then $a\left(\frac{n}{p}\right) = 0$. We say that $f(z) \in S_k \cap \mathbb{Z}_{(\ell)}[[q]]$ is an eigenform for the Hecke operator $T_{p,k}$ modulo ℓ with eigenvalue $\lambda_p \in \mathbb{Z}/\ell\mathbb{Z}$ if

$$f(z) | T_{p,k} \equiv \lambda_p f(z) \pmod{\ell}.$$

The following lemma gives the key fact underlying the proof of Lemma 2.2.

Lemma 3.1. *Fix $\ell \in \{2, 3, 5, 7\}$. Suppose that for every prime $p \neq \ell$, $f(z) \in S_k \cap \mathbb{Z}_{(\ell)}[[q]]$ is an eigenform for $T_{p,k}$ modulo ℓ . If $p \equiv -1 \pmod{\ell}$, then we have*

$$f(z) | T_{p,k} \equiv 0 \pmod{\ell}.$$

Proof. Suppose, for primes $p \neq \ell$, that $f(z)$ has eigenvalues $\lambda_p \in \mathbb{Z}/\ell\mathbb{Z}$ for the Hecke operators $T_{p,k}$. A well-known theorem of Deligne [7, Théorème 6.7] states that there is a continuous semisimple Galois representation

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

unramified outside ℓ , such that for all primes $p \neq \ell$,

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

Now, let $\chi_\ell : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \mapsto (\mathbb{Z}/\ell\mathbb{Z})^*$ be the mod ℓ cyclotomic character. By a result of Atkin, Serre, and Tate [14, Theorem 3], there is an integer $i \geq 0$ such that $\rho_{\ell, f} \otimes \chi_\ell^i$ comes from an eigenform in M_k with $k \leq \ell + 1$. If $\ell \in \{2, 3, 5, 7\}$ and $k \leq \ell + 1$, then $S_k = \{0\}$, so $\rho_{\ell, f}$ must be reducible. For all primes $p \neq \ell$, we have $\chi_\ell(\mathrm{Frob}_p) \equiv p \pmod{\ell}$. Since $\rho_{\ell, f}$ is odd ($\mathrm{Det} \rho_{\ell, f}(c) \equiv -1 \pmod{\ell}$ when c is complex conjugation) and reducible, there are $m, n \in \mathbb{Z}/(\ell - 1)\mathbb{Z}$ with $m + n$ odd for which

$$\rho_{\ell, f} = \chi_\ell^m \oplus \chi_\ell^n.$$

Hence, observing that $n - m$ must be odd, if $p \equiv -1 \pmod{\ell}$ is prime, then we have

$$\lambda_p \equiv \mathrm{Tr} \rho_{\ell, f}(\mathrm{Frob}_p) \equiv p^m + p^n \equiv p^m(1 + p^{n-m}) \equiv 0 \pmod{\ell},$$

which proves the lemma. \square

Before giving the principal application of Lemma 3.1, we recall certain facts on modular forms modulo primes ℓ . Let $k \geq 4$ be an even integer. We require the normalized Eisenstein series of weight k on $\mathrm{SL}_2(\mathbb{Z})$ defined by

$$E_k(z) := 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sum_{d|n} d^{k-1} q^n \in M_k,$$

where B_k is the k th Bernoulli number. We note the well-known fact that if ℓ is prime and $\ell - 1 \mid k$, then

$$(3.2) \quad E_k(z) \equiv 1 \pmod{\ell}.$$

If $j \geq 1$ is an integer, it is also well-known that S_{12j} has bases given by, for example,

$$(3.3) \quad \{E_4(z)^{3j-3} \Delta(z), \dots, E_4(z)^{3j-3t} \Delta(z)^t, \dots, \Delta(z)^j\},$$

$$(3.4) \quad \{E_6(z)^{2j-2} \Delta(z), \dots, E_6(z)^{2j-2s} \Delta(z)^s, \dots, \Delta(z)^j\}.$$

Now, fix $\ell \in \{3, 5, 7\}$, and let $f(z) \in S_{12j} \cap \mathbb{Z}_{(\ell)}[[q]]$. Using (3.2), (3.3), and (3.4), it follows that there are integers $a_{1,\ell}, \dots, a_{j,\ell} \in \mathbb{Z}/\ell\mathbb{Z}$ for which

$$(3.5) \quad f(z) \equiv \sum_{i=1}^j a_{i,\ell} \Delta(z)^i \pmod{\ell}.$$

In view of (3.5), for such primes ℓ , we also require information on $\Delta(z)^j \mid T_{\ell, 12j} \pmod{\ell}$.

Proposition 3.2. *Fix $\ell \in \{3, 5, 7\}$, and let $j \geq 1$ be an integer. There are integers $c_{j,\ell}$ and $d_{j,\ell}$ with $0 \leq d_{j,\ell} < j$ for which*

$$\Delta(z)^j \mid T_{\ell, 12j} \equiv c_{j,\ell} \Delta(z)^{d_{j,\ell}} \pmod{\ell}.$$

Remark. To illustrate, when $\ell = 3$, we have

$$\Delta(z)^j \mid T_{3, 12j} \equiv \begin{cases} \Delta(z)^{\frac{j}{3}} & \pmod{3} \text{ if } 3 \mid j \\ 0 & \pmod{3} \text{ if } 3 \nmid j. \end{cases}$$

This follows from formula (3.1), together with the easily verified facts that $\Delta(z) \mid T_{3, 12} \equiv 0 \pmod{3}$ and $\Delta(z)^2 \mid T_{3, 24} \equiv 0 \pmod{3}$.

We now turn to the principal application of Lemma 3.1.

Lemma 3.3. *Fix $\ell \in \{3, 5, 7\}$, let $j \geq 1$ be an integer, and let $f(z) \in S_{12j} \cap \mathbb{Z}_{(\ell)}[[q]]$ have $f(z) \not\equiv 0 \pmod{\ell}$. Then exactly one of the following must hold.*

(1) *For every prime p with $p \equiv -1 \pmod{\ell}$ or $p = \ell$, we have*

$$f(z) | T_{p,12j} \equiv 0 \pmod{\ell}.$$

(2) *There is an integer $i_{f,\ell} \geq 2$ for which the following are true:*

- *There are $i_{f,\ell} - 1$ distinct primes $p_1, \dots, p_{i_{f,\ell}-1} \equiv -1$ or $0 \pmod{\ell}$ such that*

$$f(z) | T_{p_1,12j} | \cdots | T_{p_{i_{f,\ell}-1},12j} \not\equiv 0 \pmod{\ell}.$$

- *For every collection of $i_{f,\ell}$ distinct primes $m_1, \dots, m_{i_{f,\ell}} \equiv -1$ or $0 \pmod{\ell}$, we have*

$$f(z) | T_{m_1,12j} | \cdots | T_{m_{i_{f,\ell}},12j} \equiv 0 \pmod{\ell}.$$

Remark. If $f(z)$ satisfies (1), we define $i_{f,\ell} := 1$.

Proof. We will prove the $\ell = 3$ case. The proofs of the other cases are similar. In view of (3.5), it suffices to prove the lemma with $f(z) = \Delta(z)^j$.

We proceed by induction on j . To begin, we observe that for all primes p , $\Delta(z)$ is an eigenform for $T_{p,12}$ modulo 3. Therefore, by Lemma 3.1, if $p \equiv 2 \pmod{3}$, then $\Delta(z) | T_{p,12} \equiv 0 \pmod{3}$. As noted in the remark following Proposition 3.2, $\Delta(z) | T_{3,12} \equiv 0 \pmod{3}$. Hence, $\Delta(z)$ satisfies part (1) of the lemma.

Now, fix an integer $j \geq 2$. We assume, for every integer k with $1 \leq k \leq j - 1$, that there is an integer $i_k := i_{\Delta^k,3} \geq 1$ as in the proposition. Set $t := \max\{i_1, \dots, i_{j-1}\}$, and let primes $m_1, \dots, m_{t+1} \equiv -1$ or $0 \pmod{3}$ be given. We propose to show that

$$(3.6) \quad \Delta(z)^j | T_{m_1,12j} | \cdots | T_{m_{t+1},12j} \equiv 0 \pmod{3},$$

thereby proving the proposition with $1 \leq i_{\Delta^j,3} \leq t + 1$. For every integer $s \geq 1$, we define

$$G_s(z) := \Delta(z)^s | T_{m_1,12s} | \cdots | T_{m_t,12s} \in S_{12s} \cap \mathbb{Z}_{(3)}[[q]].$$

It suffices to show that $G_j(z) | T_{m_{t+1},12j} \equiv 0 \pmod{3}$. By the definition of t , we have

$$(3.7) \quad G_s(z) \equiv 0 \pmod{3} \text{ if } 1 \leq s \leq j - 1.$$

If we also have $G_j(z) \equiv 0 \pmod{3}$, then (3.6) holds. Thus, we assume that $G_j(z) \not\equiv 0 \pmod{3}$. We claim, for all primes p , that $G_j(z)$ is an eigenform for $T_{p,12j}$ modulo 3.

Let p be an arbitrary prime. By (3.5) it follows that there are integers $a_{1,p}, \dots, a_{j,p} \in \{0, 1, 2\}$ for which

$$(3.8) \quad \Delta(z)^j | T_{p,12j} \equiv a_{j,p} \Delta(z)^j + \sum_{i=1}^{j-1} a_{i,p} \Delta(z)^i \pmod{3}.$$

Using the commutativity of the Hecke operators, (3.7), and (3.8), we verify that $G_j(z) \not\equiv 0 \pmod{3}$ is an eigenform for $T_{p,12j}$ modulo 3:

$$\begin{aligned} G_j(z) | T_{p,12j} &= (\Delta(z)^j | T_{p,12j}) | T_{m_1,12j} | \cdots | T_{m_t,12j} \\ &\equiv a_{j,p} G_j(z) + \sum_{i=1}^{j-1} a_{i,p} G_i(z) \equiv a_{j,p} G_j(z) \pmod{3}. \end{aligned}$$

Lemma 3.1 now implies that if $m_{t+1} \equiv 2 \pmod{3}$, then $G_j(z) \mid T_{m_{t+1}, 12j} \equiv 0 \pmod{3}$.

It remains to show that $G_j(z) \mid T_{3, 12j} \equiv 0 \pmod{3}$. We compute as follows, using the commutativity of the Hecke operators and the remark after Proposition 3.2:

$$G_j(z) \mid T_{3, 12j} = (\Delta(z)^j \mid T_{3, 12j}) \mid T_{m_1, 12j} \mid \cdots \mid T_{m_t, 12j} \equiv \begin{cases} G_{\frac{j}{3}}(z) \pmod{3} & \text{if } 3 \mid j \\ 0 \pmod{3} & \text{if } 3 \nmid j. \end{cases}$$

If $3 \mid j$, then $\frac{j}{3} < j - 1$, so $G_{\frac{j}{3}}(z) \equiv 0 \pmod{3}$ by (3.7), proving the proposition. \square

If ℓ is prime and $f(z)$ is as in the hypothesis of Lemma 3.3, we define the *nilpotency degree* of $f(z)$ modulo ℓ by

$$\text{nil}_\ell(f) := i_{f, \ell} \geq 1.$$

For example, one can show that $\text{nil}_3(\Delta^7) = 5$. Moreover, for $\ell \in \{3, 5, 7\}$, the proof of Lemma 3.3 shows that if $j \geq 1$ is an integer and $f(z) \in S_{12j} \cap \mathbb{Z}_{(\ell)}[[q]]$, then $\text{nil}_\ell(f) \leq j$.

We now describe how to use $\text{nil}_\ell(f)$ to deduce information about coefficients of $f(z)$ which do not vanish modulo ℓ .

Proposition 3.4. *Fix $\ell \in \{3, 5, 7\}$, let $j \geq 1$ be an integer, and let $f(z) = \sum a(n)q^n \in S_{12j} \cap \mathbb{Z}_{(\ell)}[[q]]$ have $\text{nil}_\ell(f) = i_{f, \ell} \geq 1$.*

- (1) *Suppose that $i_{f, \ell} = 1$. Then there is an integer $r_{f, \ell} \geq 1$ such that $a(r_{f, \ell}) \not\equiv 0 \pmod{\ell}$ and $r_{f, \ell}$ is divisible neither by ℓ nor by primes $p \equiv -1 \pmod{\ell}$.*
- (2) *Suppose that $i_{f, \ell} \geq 2$. Then there is an integer $t_{f, \ell} \geq 1$ and distinct primes $p_1, \dots, p_{i_{f, \ell}-1} \equiv -1 \pmod{\ell}$ or $0 \pmod{\ell}$ such that $a(t_{f, \ell} p_1 \cdots p_{i_{f, \ell}-1}) \not\equiv 0 \pmod{\ell}$ and $t_{f, \ell}$ is divisible neither by ℓ nor by primes $p \equiv -1 \pmod{\ell}$.*

Proof. We prove the proposition for $\ell = 3$. The proofs of the other cases are similar. Using (3.1), $\text{nil}_3(f) = 1$ implies that

$$f(z) \mid T_{3, 12j} = \sum_{n=1}^{\infty} \left(a(3n) + 3^{12j-1} a\left(\frac{n}{3}\right) \right) q^n \equiv \sum_{n=1}^{\infty} a(3n) q^n \equiv 0 \pmod{3},$$

from which it follows that

$$(3.9) \quad a(3n) \equiv 0 \pmod{3}.$$

Now, let $p \equiv -1 \pmod{3}$ be prime. By the same reasoning, we have

$$f(z) \mid T_{p, 12j} = \sum_{n=1}^{\infty} \left(a(np) + p^{12j-1} a\left(\frac{n}{p}\right) \right) q^n \equiv 0 \pmod{3},$$

which gives

$$(3.10) \quad a(np) \equiv a\left(\frac{n}{p}\right) \pmod{3}.$$

Suppose that $k \geq 1$ is an integer with $p \mid k$. Then there are positive integers r and m with $p \nmid m$ for which $k = mp^r$. If r is even, then repeated application of (3.10) (with n replaced by mp^b for suitable integers b) yields

$$(3.11) \quad a(k) = a(mp^r) \equiv a(mp^{r-2}) \equiv \cdots \equiv a(m) \pmod{3}.$$

If r is odd, then by the same argument, we have

$$(3.12) \quad a(k) = a(mp^r) \equiv a(mp^{r-2}) \equiv \cdots \equiv a(mp) \equiv a\left(\frac{m}{p}\right) \equiv 0 \pmod{3}.$$

Hence, (3.9), (3.11), and (3.12) show that there must be an integer $r_{f,3}$ with the properties stated in part (1) of the proposition.

If $i_f := i_{f,3} \geq 2$, then there are distinct primes $p_1, \dots, p_{i_f-1} \equiv -1$ or $0 \pmod{3}$ such that

$$f(z) \mid T_{p_1,12j} \mid \cdots \mid T_{p_{i_f-1},12j} \not\equiv 0 \pmod{3}.$$

For convenience, we define $g(z) \in S_{12j} \cap \mathbb{Z}_{(3)}[[q]]$ by

$$g(z) := f(z) \mid T_{p_1,12j} \mid \cdots \mid T_{p_{i_f-1},12j}.$$

Therefore, the condition that $\text{nil}_3(f) = i_f$ implies that $\text{nil}_3(g) = 1$.

Now, for all integers n and j with $n \geq 0$ and $1 \leq j \leq i_f - 1$, we define $b_j(n) \in \mathbb{Z}_{(3)}$ by

$$\begin{aligned} \sum b_1(n)q^n &= f(z) \mid T_{p_1,12j} \\ \sum b_2(n)q^n &= f(z) \mid T_{p_1,12j} \mid T_{p_2,12j} \\ &\vdots \\ \sum b_{i_f-1}(n)q^n &= f(z) \mid T_{p_1,12j} \mid \cdots \mid T_{p_{i_f-1}} = g(z). \end{aligned}$$

Since $\text{nil}_3(g) = 1$, it follows by part (1) of the proposition that there is an integer $t_f \geq 1$ which is divisible neither by 3 nor by primes $p \equiv -1 \pmod{3}$ and which has $b_{i_f-1}(t_f) \not\equiv 0 \pmod{3}$. Furthermore, since $p_1, \dots, p_{i_f-1} \equiv -1$ or $0 \pmod{3}$, we see that

$$(3.13) \quad \gcd(t_f, p_1 \cdots p_{i_f-1}) = 1.$$

Repeatedly using formula (3.1) together with (3.13), we obtain

$$\begin{aligned} 0 \not\equiv b_{i_f-1}(t_f) &\equiv b_{i_f-2}(t_f p_{i_f-1}) - b_{i_f-2}\left(\frac{t_f}{p_{i_f-1}}\right) &&\equiv b_{i_f-2}(t_f p_{i_f-1}) \\ &\equiv b_{i_f-3}(t_f p_{i_f-2} p_{i_f-1}) - b_{i_f-3}\left(\frac{t_f p_{i_f-1}}{p_{i_f-2}}\right) &&\equiv b_{i_f-3}(t_f p_{i_f-2} p_{i_f-1}) \\ &\vdots &&\vdots \\ &\equiv b_1(t_f p_1 \cdots p_{i_f-1}) - b_1\left(\frac{t_f p_3 \cdots p_{i_f-1}}{p_2}\right) &&\equiv b_1(t_f p_2 \cdots p_{i_f-1}) \\ &\equiv a(t_f p_1 \cdots p_{i_f-1}) - a\left(\frac{t_f p_2 \cdots p_{i_f-1}}{p_1}\right) &&\equiv a(t_f p_1 \cdots p_{i_f-1}) \pmod{3}. \end{aligned}$$

The lemma follows with $t_{f,3} = t_f$. □

4. THE PROOF OF LEMMA 2.2.

In this section we prove Lemma 2.2, whose truth implies our theorems on the non-vanishing of partition values modulo $\ell \in \{3, 5, 7\}$. Recall that the lemma gives a uniform description of infinitely many integers n for which $a_{s,\ell}(n) \not\equiv 0 \pmod{\ell}$, where the $a_{s,\ell}(n)$ are integers defined by

$$\sum_{n=1}^{\infty} a_{s,\ell}(n)q^n := \begin{cases} \Delta(z)^{\frac{\ell^{2s}-1}{8}} & \text{if } \ell = 3 \\ \Delta(z)^{\frac{\ell^{2s}-1}{24}} & \text{if } \ell \in \{5, 7\}. \end{cases}$$

Proof. We prove the $\ell = 3$ case of the lemma; the proofs of the other cases are similar. We first note that for all integers $s \geq 1$, $\Delta(z)^{\frac{9^s-1}{8}} \not\equiv 0 \pmod{3}$, so there is an integer

$$i_s := \text{nil}_3(\Delta^{\frac{9^s-1}{8}}) \geq 1.$$

If $i_s = 1$, then by part (1) of Proposition 3.4, there is an integer $r_{s,3} \geq 1$ with $a_{s,3}(r_{s,3}) \not\equiv 0 \pmod{3}$ and such that $r_{s,3}$ is divisible neither by 3 nor by primes $p \equiv -1 \pmod{3}$. Now, let $m \nmid r_{s,3}$ be prime with $m \equiv -1 \pmod{3}$, and for convenience, denote by

$$k_s := \frac{3(9^s - 1)}{2}$$

the weight of the cusp form $\Delta(z)^{\frac{9^s-1}{8}}$. Since $\text{nil}_3(\Delta^{\frac{9^s-1}{8}}) = 1$, we obtain

$$\Delta(z)^{\frac{9^s-1}{8}} \mid T_{m,k_s} = \sum_{n=1}^{\infty} \left(a_{s,3}(mn) - m^{k_s-1} \binom{n}{m} \right) q^n \equiv 0 \pmod{3},$$

which implies, for all integers $n \geq 1$, that

$$(4.1) \quad a_{s,3}(nm) \equiv a_{s,3} \left(\frac{n}{m} \right) \pmod{3}.$$

Replacing n by $r_{s,3}m$ in (4.1) yields

$$a_{s,3}(r_{s,3}m^2) \equiv a_{s,3}(r_{s,3}) \not\equiv 0 \pmod{3},$$

which gives the lemma in this case with $n_{s,3} = r_{s,3}$.

Now, suppose that $i_s \geq 2$. By part (2) of Proposition 3.4, there is an integer $t_{s,3} \geq 1$ which is divisible neither by 3 nor by primes $p \equiv -1 \pmod{3}$ and a collection of $i_s - 1$ distinct primes $p_1, \dots, p_{i_s-1} \equiv -1$ or $0 \pmod{3}$ such that $a_{s,3}(t_{s,3}p_1 \cdots p_{i_s-1}) \not\equiv 0 \pmod{3}$. Part (2) of Proposition 2.1 implies that $t_{s,3}p_1 \cdots p_{i_s-1} \not\equiv 0 \pmod{3}$, so we must have $p_1, \dots, p_{i_s-1} \equiv -1 \pmod{3}$.

Next, we let $m \nmid t_{s,3}p_1 \cdots p_{i_s-1}$ be prime with $m \equiv -1 \pmod{3}$. For all integers n and j with $n \geq 1$ and $0 \leq j \leq i_s - 1$, we define integers $c_j(n)$ by

$$\begin{aligned} \sum c_0(n)q^n &= \Delta(z)^{\frac{9^s-1}{8}} \mid T_{m,k_s} \\ \sum c_1(n)q^n &= \Delta(z)^{\frac{9^s-1}{8}} \mid T_{m,k_s} \mid T_{p_1,k_s} \\ &\vdots \\ \sum c_{i_s-1}(n)q^n &= \Delta(z)^{\frac{9^s-1}{8}} \mid T_{m,k_s} \mid T_{p_1,k_s} \mid \cdots \mid T_{p_{i_s-1},k_s}. \end{aligned}$$

Since $\text{nil}_3(\Delta^{\frac{9^s-1}{8}}) = i_s$, it follows that for all integers $n \geq 1$,

$$(4.2) \quad c_{i_s-1}(n) \equiv 0 \pmod{3}.$$

In particular, setting $n = t_{s,3}m$ in (4.2), we obtain

$$c_{i_s-1}(t_{s,3}m) \equiv 0 \pmod{3}.$$

By the same argument as in the proof of Proposition 3.4, using formula (3.1) and the fact that $\text{gcd}(t_{s,3}, p_1 \cdots p_{i_s-1}) = 1$, we obtain

$$\begin{aligned} 0 &\equiv c_{i_s-1}(t_{s,3}m) \\ &\equiv c_{i_s-2}(t_{s,3}p_{i_s-1}m) \\ &\equiv c_{i_s-3}(t_{s,3}p_{i_s-2}p_{i_s-1}m) \\ &\quad \vdots \\ &\equiv c_0(t_{s,3}p_1 \cdots p_{i_s-1}m) \\ &\equiv a_{s,3}(t_{s,3}p_1 \cdots p_{i_s-1}m^2) - a_{s,3}(t_{s,3}p_1 \cdots p_{i_s-1}) \pmod{3}. \end{aligned}$$

Therefore, we have

$$a_{s,3}(t_{s,3}p_1 \cdots p_{i_s-1}m^2) \equiv a_{s,3}(t_{s,3}p_1 \cdots p_{i_s-1}) \pmod{3},$$

which proves the lemma when $i_s \geq 2$ with $n_{s,3} = t_{s,3}p_1 \cdots p_{i_s-1}$. \square

REFERENCES

- [1] S. Ahlgren, *Distribution of the parity of the partition function in arithmetic progressions*, Indag. Math. **10** (1999), no. 2, 173-181.
- [2] S. Ahlgren, *Non-vanishing of the partition function modulo odd primes ℓ* , Mathematika **46** (1999), no. 1, 185-192.
- [3] S. Ahlgren, *Distribution of the partition function modulo positive integers M* , Math. Ann. **318** (2000), no. 4, 795-803.
- [4] S. Ahlgren and K. Ono, *Congruences and conjectures for the partition function, q -series with applications to combinatorics, number theory, and physics* (Urbana, IL, 2000), 1-10, Contemp. Math., 291, Amer. Math. Soc., Providence, RI, 2001.
- [5] S. Ahlgren and K. Ono, *Congruence properties of the partition function*, Proc. Natl. Acad. Sci. USA **98** (2001), no. 23, 12882-12884.
- [6] M. Boylan and K. Ono, *Parity of the partition function in arithmetic progressions, II*, Bull. London Math. Soc. **33** (2001), no. 5, 558-564.
- [7] P. Deligne and J.-P. Serre, *Formes modulaires de poids 1*, Ann. Sci. École Norm. Sup. (4) **7** (1974), 507-530.
- [8] N. Koblitz, *Introduction to elliptic curves and modular forms*, Second edition, Graduate Texts in Mathematics, 97, Springer-Verlag, New York, 1993.
- [9] J.-L. Nicolas, I. Z. Rusza, and A. Sárközy, *On the parity of additive representation functions*, (with an appendix by J.-P. Serre), J. Number Theory **73** (1998), no. 2, 292-317.
- [10] K. Ono, *Parity of the partition function in arithmetic progressions*, J. Reine Angew. Math. **472** (1996), 1-15.
- [11] K. Ono, *Distribution of the partition function modulo m* , Ann. of Math. (2) **151** (2000), no. 1, 293-307.
- [12] K. Ono, *The web of modularity: Arithmetic of the coefficients of modular forms and q -series*, Conference Board of the Math. Sciences, Regional Conference Series in Mathematics, 102, Amer. Math. Soc., Providence, RI, 2004.
- [13] K. Ono and C. Skinner, *Fourier coefficients of half-integral weight modular forms modulo ℓ* , Ann. of Math. (2) **147** (1998), no. 2, 453-470.
- [14] J.-P. Serre, *Valeurs propres des opérateurs de Hecke modulo ℓ* , Astérisque **24-25** (1975), 109-117.

- [15] M. V. Subbarao, *Some remarks on the partition function*, Amer. Math. Monthly **73** (1966), 851-854.
- [16] H. P. F. Swinnerton-Dyer, *On ℓ -adic representations and congruences for coefficients of modular forms*, Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, 1972), 1-55. Lecture Notes in Math., Vol. 350, Springer, Berlin, 1973.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF SOUTH CAROLINA, COLUMBIA, SC 29208
E-mail address: boylan@math.sc.edu