ARITHMETIC PROPERTIES OF THE PARTITION FUNCTION

Scott Ahlgren and Matthew Boylan

1. Introduction and statement of results

Let $p(n)$ denote the number of partitions of the positive integer n; $p(n)$ is the number of representations of n as a non-increasing sequence of positive integers (by convention, we agree that $p(0) = 1$ and that $p(n) = 0$ if $n < 0$). The study of the arithmetic properties of $p(n)$ has a long and rich history; see, for example, the works of Andrews, Atkin, Dyson, Garvan, Kim, Stanton, and Swinnerton-Dyer [An, An-G, At1, At-SwD, D, G-K-S]. These works have their origins in the groundbreaking observations of Ramanujan [R1, R2, R3, R4]. In Ramanujan's own words [R3],

> *I have proved a number of arithmetical properties of* $p(n)$ ... *in particular that*
>
> $$p(5n+4) \equiv 0 \pmod{5}, \tag{1.1}$$
>
> *and*
>
> $$p(7n+5) \equiv 0 \pmod{7}\dots. \tag{1.2}$$
>
> *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*
>
> $$p(11n+6) \equiv 0 \pmod{11}. \tag{1.3}$$
>
> *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.*

Recently (see [A], [O], [A-O]) it has been shown that in one sense, congruences like Ramanujan's original three examples are quite common. After these works, for example, it is now known that if M is any integer coprime to 6, then there exist integers a and b such that

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

The first author thanks the National Science Foundation for its support through grant DMS 01-34577. The second author thanks the National Science Foundation for its support through a VIGRE postdoctoral fellowship.

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

However, these congruences are much more complicated than (1.1)–(1.3); for example, one of the simplest congruences modulo 13 (which was first recorded by Atkin and O'Brien [At-Ob]) is

$$p(59^4 \cdot 13n + 111247) \equiv 0 \pmod{13}.$$

In general, if ℓ is a prime, then by a *Ramanujan congruence* modulo ℓ we will mean a congruence of the form

$$p(\ell n + \beta) \equiv 0 \pmod{\ell} \text{ for all } n$$

with some fixed $\beta \in \mathbb{Z}$.

A natural quantification of Ramanujan's statement is the assertion that the congruences (1.1)–(1.3) are the only ones of their kind. In other words,

Conjecture 1. *Suppose that ℓ is prime. If there is a Ramanujan congruence modulo ℓ, then the congruence must be one of* (1.1)*,* (1.2)*, or* (1.3)*.*

Here we prove

Theorem 1. *Conjecture 1 is true.*

We also consider another classical conjecture regarding the arithmetic of the partition function. In particular, we recall the conjecture of Newman [N1].

Conjecture 2. (Newman's Conjecture). *If M is a positive integer, then for every integer $0 \leq r < M$ there are infinitely many non-negative integers n such that $p(n) \equiv r \pmod{M}$.*

Atkin, Kolberg, Newman, and Kløve [At2, Ko, N1, Kl] proved the conjecture for $M = 2$, 5, 7, 13 17, 19, 29, and 31. In work of the first author [A] and Ono [O], conditions are obtained which (presumably) allow one to check the proof of the conjecture for any M coprime to 6. For prime values of M these conditions were recently simplified by Bruinier and Ono [B-O]. This allowed them to verify the truth of Newman's Conjecture for every prime $M < 2 \times 10^5$ with the possible exception of $M = 3$.

Combining a result of Bruinier and Ono [B-O] (see the end of Section 3 for a precise statement of the relevant theorem) with Theorem 1 yields the following as an immediate corollary.

Corollary 2. *Newman's Conjecture is true for every prime modulus M with the possible exception of $M = 3$. Moreover, if $\ell \geq 5$ is prime, then we have*

$$\#\{0 \leq n \leq X \quad : \quad p(n) \equiv r \pmod{\ell}\} \gg_{r,\ell} \begin{cases} \sqrt{X}/\log X & \text{if } 1 \leq r \leq \ell - 1, \\ X & \text{if } r = 0. \end{cases}$$

The proof of Theorem 1 depends on a careful study of the *filtration* of certain modular forms related to the partition function (this is the minimal weight at which the reductions of these forms can be realized as modular forms modulo ℓ; see Section 2 for details). In the second part of the paper we investigate a closely related topic; for every prime $\ell \geq 5$ and every $j \geq 1$ we determine the minimal weight k at which a natural generating function for partitions can be found as a modular form of weight k modulo ℓ^j. To state the result requires some notation.

If $\ell \geq 5$ is prime and $j \geq 1$ is an integer, then we define $1 \leq \beta_{\ell,j} \leq \ell^j - 1$ as the unique integer for which

$$24\beta_{\ell,j} \equiv 1 \pmod{\ell^j}.$$

Further, we define the even integer $k_{\ell,j}$ by

$$k_{\ell,j} := \begin{cases} \frac{\ell^{j-1}(\ell-1)}{2} - \frac{1}{2}\left(\frac{24\beta_{\ell,j}-1}{\ell^j} + 1\right) = \frac{(\ell^{j-1}+1)(\ell-1)}{2} - 12\left(\lfloor \ell/24 \rfloor + 1\right) & \text{if } j \text{ is odd,} \\ \ell^{j-1}(\ell-1) - \frac{1}{2}\left(\frac{24\beta_{\ell,j}-1}{\ell^j} + 1\right) = \ell^{j-1}(\ell-1) - 12 & \text{if } j \text{ is even.} \end{cases}$$

If k is an even integer, then we denote by M_k the space of holomorphic modular forms of weight k for $\mathrm{SL}_2(\mathbb{Z})$. We will prove the following.

Theorem 3. *If $\ell \geq 5$ is prime and j is a positive integer, then there exists a modular form $F_{\ell,j}(z) \in M_{k_{\ell,j}} \cap \mathbb{Z}[[q]]$ such that*

$$\sum_{n=0}^{\infty} p(\ell^j n + \beta_{\ell,j}) q^n \equiv \prod_{n=1}^{\infty} (1-q^n)^{\frac{24\beta_{\ell,j}-1}{\ell^j}} \cdot F_{\ell,j}(z) \pmod{\ell^j}. \qquad (1.4)$$

Remark 1. We recall the fact (see, for example, Théorème 1 of [S]) that if $f \in M_k \cap \mathbb{Z}[[q]]$, $g \in M_{k'} \cap \mathbb{Z}[[q]]$ have $f \equiv g \pmod{\ell^j}$ and $f \not\equiv 0 \pmod{\ell}$, then $k \equiv k' \pmod{\ell^{j-1}(\ell-1)}$. Therefore, we see that the weight $k_{\ell,j}$ guaranteed by Theorem 3 is minimal in the sense that it can be reduced only in the case when $\sum_{n=0}^{\infty} p(\ell^j n + \beta_{\ell,j}) q^n \equiv 0 \pmod{\ell}$.

Remark 2. We also remark that $k_{\ell,j} < 0$ if and only if $j = 1$ and $\ell = 5, 7$, or 11. Therefore (1.1), (1.2), and (1.3) follow immediately from Theorem 3.

Remark 3. In the case when $j = 1$, this result has been obtained independently by K. S. Chua and H. H. Chan [C].

Theorem 3 is closely related to a claim made by Ramanujan in his Lost Notebook (see §15 of [Be-O]). In the case when $j = 1$, Ramanujan asserted that (1.4) holds for some modular form $F_{\ell,1} \in M_{\ell-13}$, which is indeed the case if $5 \leq \ell \leq 23$; in the general case, $\ell - 13$ should be replaced by $\ell - 13 - 12 \cdot \lfloor \ell/24 \rfloor$. For $\ell \leq 23$ Ramanujan computed the modular form $F_{\ell,1}$ explicitly; he obtained, for example,

$$\sum_{n=0}^{\infty} p(13n+6) q^n \equiv p(6) \cdot \prod_{n=1}^{\infty} (1-q^n)^{11} \pmod{13},$$

$$\sum_{n=0}^{\infty} p(17n+5) q^n \equiv p(5) \cdot \prod_{n=1}^{\infty} (1-q^n)^{7} \cdot E_4(z) \pmod{17}$$

(here E_4 denotes the usual normalized Eisenstein series of weight 4 on $\mathrm{SL}_2(\mathbb{Z})$).

In the next section we collect some facts which we shall need from the theory of modular forms. In Section 3, we prove Theorem 1 and Corollary 2, and in Sections 4 and 5 we prove Theorem 3.

2. Preliminaries on modular forms modulo ℓ.

In this section we recall some facts about modular forms modulo ℓ. One may consult, for example, [SwD] or [S] for details. Throughout we will suppose that ℓ is a fixed prime with $\ell \geq 5$. If k is an even integer, then we denote by M_k the complex vector space of holomorphic modular forms of weight k with respect to $\mathrm{SL}_2(\mathbb{Z})$. Each modular form f in such a space has a Fourier expansion

$$f(z) = \sum_{n=0}^{\infty} a(n)q^n \quad (q := e^{2\pi i z}).$$

If $f \in M_k \cap \mathbb{Z}[[q]]$, then $\widetilde{f} := f \pmod{\ell} \in \mathbb{F}_\ell[[q]]$. We define the space of weight k modular forms modulo ℓ by

$$\widetilde{M_k} := \left\{ \widetilde{f} \ : \ f \in M_k \cap \mathbb{Z}[[q]] \right\}.$$

The *filtration* of a modular form $f \in M_k \cap \mathbb{Z}[[q]]$ is defined by

$$w(f) := \inf\{k' \ : \ \widetilde{f} \in \widetilde{M_{k'}}\}.$$

If $f \in M_k \cap \mathbb{Z}[[q]]$ and $g \in M_{k'} \cap \mathbb{Z}[[q]]$ have $\widetilde{f} \equiv \widetilde{g} \not\equiv 0 \pmod{\ell}$, then we must have $k \equiv k' \pmod{\ell - 1}$. It follows that if $f \in M_k \cap \mathbb{Z}[[q]]$ has $\widetilde{f} \not\equiv 0 \pmod{\ell}$, then $w(f) \equiv k \pmod{\ell - 1}$. Moreover, we see that $w(f) = -\infty$ if and only if $\widetilde{f} \equiv 0 \pmod{\ell}$. We define the theta operator on formal power series by

$$\Theta\left(\sum_{n=0}^{\infty} a(n)q^n\right) := \sum_{n=1}^{\infty} na(n)q^n.$$

We have the following fundamental lemma.

Lemma 2.1 ([SwD, Lemmas 3, 5]). *The operator Θ maps $\widetilde{M_k}$ to $\widetilde{M_{k+\ell+1}}$. Moreover, if $f \in M_k \cap \mathbb{Z}[[q]]$ for some k, and $\widetilde{f} \not\equiv 0 \pmod{\ell}$, then $w(\Theta f) \leq w(f) + \ell + 1$, with equality if and only if $w(f) \not\equiv 0 \pmod{\ell}$.*

We define the operator U on formal power series by

$$\left(\sum_{n=0}^{\infty} a(n)q^n\right) \big| U := \sum_{n=0}^{\infty} a(\ell n)q^n.$$

We also recall that for each prime ℓ we have the Hecke operator $T_\ell \ : \ M_k \to M_k$ whose action on a form $f = \sum_{n=0}^{\infty} a(n)q^n \in M_k$ is given by

$$f\big|T_\ell = \sum_{n=0}^{\infty} \left(a(\ell n) + \ell^{k-1}a(n/\ell)\right) q^n.$$

From this we see that, on each space $\widetilde{M_k}$, the operators U and T_ℓ agree modulo ℓ; in particular we conclude that U maps each space $\widetilde{M_k}$ into itself. Moreover, we have the relationship

$$\left(f\big|U\right)^\ell \equiv f - \Theta^{\ell-1}f \pmod{\ell} \tag{2.1}$$

for all $f \in \mathbb{Z}[[q]]$. Finally, we recall the fact [S, §2.2, Lemme 1] that if $f \in M_k \cap \mathbb{Z}[[q]]$ for some k, then for each $i \in \mathbb{N}$ we have

$$w(f^i) = iw(f). \tag{2.2}$$

3. Proof of Theorem 1.

That there are no Ramanujan congruences modulo 2 or 3 follows from the fact that $p(0) = 1$, $p(1) = 1$, and $p(2) = 2$. Now suppose that $\ell \geq 5$ is prime. Kiming and Olsson [K-Ol, Theorem 1] proved that if for some $\beta \in \mathbb{Z}$ there is a congruence

$$p(\ell n + \beta) \equiv 0 \pmod{\ell} \text{ for all } n,$$

then we must have $24\beta \equiv 1 \pmod{\ell}$. We define the positive integer δ_ℓ by

$$\delta_\ell := \frac{\ell^2 - 1}{24}. \tag{3.1}$$

In order to prove Theorem 1 it will, in view of this discussion, suffice to prove

Theorem 3.1. *If $\ell \geq 13$ is prime, then*

$$\sum_{n=0}^{\infty} p(\ell n - \delta_\ell) q^n \not\equiv 0 \pmod{\ell}.$$

The proof of Theorem 3.1 occupies most of this section. Let

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

be the unique normalized cusp form of weight 12 for $\mathrm{SL}_2(\mathbb{Z})$. For the duration we will suppose that

$$\ell \geq 13.$$

We now define

$$f_\ell(z) := \Delta^{\delta_\ell}(z).$$

Since

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

we have

$$f_\ell(z) = q^{\delta_\ell} \prod_{n=1}^{\infty} \frac{(1 - q^n)^{\ell^2}}{(1 - q^n)} \equiv \prod_{n=1}^{\infty} (1 - q^{\ell n})^\ell \cdot \sum_{n=0}^{\infty} p(n - \delta_\ell) q^n \pmod{\ell}.$$

Therefore

$$f_\ell \big| U \equiv \prod_{n=1}^{\infty} (1 - q^n)^\ell \cdot \sum_{n=0}^{\infty} p(\ell n - \delta_\ell) q^n \pmod{\ell}. \tag{3.2}$$

We conclude from (3.2) that if there is a Ramanujan congruence modulo ℓ, then $f_\ell \big| U \equiv 0 \pmod{\ell}$, or, in other words, $w(f_\ell \big| U) = -\infty$.

As in [K-Ol], we must study the filtration of the forms Θf_ℓ, $\Theta^2 f_\ell, \cdots$. We record two short lemmas for convenience.

Lemma 3.2. *(c.f. Lemma 2 of* [K-Ol]*). If $m \in \mathbb{N}$, and $\ell \geq 5$ is prime, then*

$$w(\Theta^m f_\ell) \geq w(f_\ell) = \tfrac{\ell^2-1}{2}.$$

Proof of Lemma 3.2. By (2.2) we have $w(f_\ell) = \delta_\ell w(\Delta) = \frac{\ell^2-1}{2}$. Now note that $f_\ell = q^{\delta_\ell} + \dots$, so that

$$\Theta^m f_\ell = \delta_\ell^m q^{\delta_\ell} + \cdots \not\equiv 0 \pmod{\ell}. \tag{3.3}$$

Suppose that $w(\Theta^m f_\ell) = k$ and set $d := \dim M_k > 0$. We recall the well known fact that M_k has a basis $\{g_0, \dots, g_{d-1}\}$ of forms with integral coefficients which have the form

$$g_0 = 1 + \dots\ ,\ g_1 = q + \dots\ ,\ g_2 = q^2 + \dots\ ,\ \dots\dots\ ,\ g_{d-1} = q^{d-1} + \dots$$

(such a basis can be constructed using $\Delta(z)$ and the Eisenstein series of weights 4 and 6 on $\mathrm{SL}_2(\mathbb{Z})$). Considering this fact, it is clear from (3.3) that $d \geq \frac{\ell^2-1}{24} + 1$. On the other hand, by classical dimension formulas we have $d \leq \frac{k}{12} + 1$. Therefore $k \geq \frac{\ell^2-1}{2}$, as claimed. □

Lemma 3.3. *Suppose that $\ell \geq 5$ is prime and let $f_\ell = \Delta^{\delta_\ell}$. Then either*

(1) $w(\Theta^{\ell-1} f_\ell) \equiv 0 \pmod{\ell}$, *or*
(2) $w(\Theta^{\ell-1} f_\ell) = w(f_\ell) = \frac{\ell^2-1}{2}$.

Moreover, in the first case we have $w(f_\ell|U) > 0$.

Remark. We note that, in view of Theorem 5.1 below, we always have $w(f_\ell|U) \leq \ell - 1$.

Proof of Lemma 3.3. We have $\Theta^\ell f \equiv \Theta f \pmod{\ell}$ for all $f \in \mathbb{Z}[[q]]$. Therefore, using Lemma 2.1, we see that $w(\Theta^\ell f_\ell) = w(\Theta f_\ell) = \frac{\ell^2-1}{2} + \ell + 1$. Using Lemma 2.1 again and the fact that $w(f_\ell) = \frac{\ell^2-1}{2}$, the assertion regarding the two possible values of $w(\Theta^{\ell-1} f_\ell)$ follows.

We turn to the other assertion. Combining (2.1) and (2.2), we see that

$$w(f_\ell|U) = \tfrac{1}{\ell} w(f_\ell - \Theta^{\ell-1} f_\ell). \tag{3.4}$$

If we are in the first case, then $w(\Theta^{\ell-1} f_\ell) \equiv 0 \pmod{\ell}$. Suppose by way of contradiction that $w(f_\ell|U) \leq 0$. Then (3.4) would imply that $f_\ell - \Theta^{\ell-1} f_\ell$ is constant modulo ℓ; it is then clear that this constant must be zero. In other words, we would be led to the conclusion that $f_\ell \equiv \Theta^{\ell-1} f_\ell \pmod{\ell}$, which is impossible since $w(f_\ell) = \frac{\ell^2-1}{2} \not\equiv 0 \pmod{\ell}$. □

We now turn to the proof of Theorem 3.1. Suppose by way of contradiction that $\ell \geq 13$ is a prime for which

$$\sum_{n=0}^{\infty} p(\ell n - \delta_\ell) q^n \equiv 0 \pmod{\ell}.$$

Then $w(f_\ell|U) = -\infty$, and so, by Lemma 3.3, we must have

$$w(\Theta^{\ell-1} f_\ell) = w(f_\ell) = \frac{\ell^2-1}{2}. \tag{3.5}$$

If it were the case that $w(\Theta^{\ell-2}f_\ell) \not\equiv 0 \pmod{\ell}$, then by Lemma 2.1 and (3.5) we would have

$$w(f_\ell) = w(\Theta^{\ell-1}f_\ell) = w(\Theta^{\ell-2}f_\ell) + \ell + 1,$$

which contradicts Lemma 3.2. Therefore we must have

$$w(\Theta^{\ell-2}f_\ell) \equiv 0 \pmod{\ell}. \tag{3.6}$$

Since $w(f_\ell) = \frac{\ell^2-1}{2}$, iterating Lemma 2.1 shows that $w(\Theta^{\frac{\ell+1}{2}}f_\ell) \equiv 0 \pmod{\ell}$. Then, again using Lemma 2.1, we see that there exists $\alpha \geq 1$ such that

$$w(\Theta^{\frac{\ell+3}{2}}f_\ell) = \frac{\ell^2-1}{2} + \frac{\ell+3}{2}\cdot(\ell+1) - \alpha(\ell-1). \tag{3.7}$$

Together, Lemma 3.2 and (3.7) imply that

$$\alpha \leq \frac{\ell+3}{2(\ell-1)}\cdot(\ell+1) = \frac{\ell+5}{2} + \frac{4}{\ell-1}.$$

Therefore, since $\ell > 5$, we conclude that $1 \leq \alpha \leq \frac{\ell+5}{2}$.

Suppose now that j is the least integer with $1 \leq j \leq \frac{\ell-5}{2}$ for which $w(\Theta^{\frac{\ell+1}{2}+j}f_\ell) \equiv 0 \pmod{\ell}$ (such a j exists by (3.6)). Then by Lemma 2.1 and (3.7) we have

$$w(\Theta^{\frac{\ell+1}{2}+j}f_\ell) = \frac{\ell^2-1}{2} + \left(\frac{\ell+1}{2}+j\right)(\ell+1) - \alpha(\ell-1) \equiv j + \alpha \equiv 0 \pmod{\ell}.$$

Since $1 \leq \alpha \leq \frac{\ell+5}{2}$ and $1 \leq j \leq \frac{\ell-5}{2}$, this implies that $\alpha = \frac{\ell+5}{2}$. Therefore (3.7) becomes

$$w(\Theta^{\frac{\ell+3}{2}}f_\ell) = \frac{\ell^2-1}{2} + \frac{\ell+3}{2}\cdot(\ell+1) - \frac{\ell+5}{2}\cdot(\ell-1) = \frac{\ell^2-1}{2} + 4. \tag{3.8}$$

To finish the proof of Theorem 3.1, note that

$$\Theta^{\frac{\ell+3}{2}}f_\ell = \delta_\ell^{\frac{\ell+3}{2}}q^{\delta_\ell} + \cdots = \delta_\ell^{\frac{\ell+3}{2}}q^{\frac{\ell^2-1}{24}} + \ldots. \tag{3.9}$$

Let

$$E_4(z) := 1 + 240\sum_{n=1}^{\infty}\sum_{d\mid n} d^3q^n = 1 + 240q + \ldots$$

be the usual Eisenstein series of weight 4 on $\mathrm{SL}_2(\mathbb{Z})$. Since $\frac{\ell^2-1}{2} \equiv 0 \pmod{12}$, a basis for $M_{\frac{\ell^2-1}{2}+4}$ is given by

$$\{E_4\cdot E_4^{\frac{\ell^2-1}{8}},\ E_4\cdot\Delta\cdot E_4^{\frac{\ell^2-1}{8}-3},\ \ldots,\ E_4\cdot\Delta^{\frac{\ell^2-1}{24}}\}. \tag{3.10}$$

In view of (3.8), (3.9), and (3.10) we must have

$$\Theta^{\frac{\ell+3}{2}} f_\ell \equiv \delta_\ell^{\frac{\ell+3}{2}} E_4 \cdot f_\ell \pmod{\ell}. \tag{3.11}$$

Now

$$f_\ell = q^{\delta_\ell}(1-q)^{\ell^2-1}\cdots \equiv q^{\delta_\ell} + q^{\delta_\ell+1} + \dots \pmod{\ell}.$$

Therefore

$$\Theta^{\frac{\ell+3}{2}} f_\ell \equiv \delta_\ell^{\frac{\ell+3}{2}} q^{\delta_\ell} + (\delta_\ell+1)^{\frac{\ell+3}{2}} q^{\delta_\ell+1} + \dots \pmod{\ell}. \tag{3.12}$$

Further, we have

$$\delta_\ell^{\frac{\ell+3}{2}} E_4 \cdot f_\ell \equiv \delta_\ell^{\frac{\ell+3}{2}} (1+240q+\dots)(q^{\delta_\ell}+q^{\delta_\ell+1}+\dots) \equiv \delta_\ell^{\frac{\ell+3}{2}} q^{\delta_\ell} + 241\cdot\delta_\ell^{\frac{\ell+3}{2}} q^{\delta_\ell+1} + \dots \pmod{\ell}.$$

Together with (3.11) and (3.12), this shows that

$$(\delta_\ell+1)^{\frac{\ell+3}{2}} \equiv 241\cdot\delta_\ell^{\frac{\ell+3}{2}} \pmod{\ell}. \tag{3.13}$$

Since $1/\delta_\ell \equiv -24 \pmod{\ell}$, (3.13) yields

$$(-23)^2\cdot(-23)^{\frac{\ell-1}{2}} \equiv 241 \pmod{\ell},$$

which in turn (note that $\ell = 23$ is impossible) implies that

$$\pm 529 \equiv 241 \pmod{\ell}.$$

Theorem 3.1 follows since

$$529 + 241 = 770 = 2\cdot 5\cdot 7\cdot 11,$$

and

$$529 - 241 = 288 = 2^5\cdot 3^2.$$

This establishes Theorem 1. □

Proof of Corollary 2. For the primes $\ell \geq 13$, Corollary 2 follows immediately from Theorem 1 together with the following result of Bruinier and Ono [B-O].

Theorem ([B-O], Theorem 4). *If $\ell \geq 5$ is prime then at least one of the following is true:*

(1) *Newman's Conjecture is true for $M = \ell$ and*

$$\#\{0 \leq n \leq X \ : \ p(n) \equiv r \pmod{\ell}\} \gg_{r,\ell} \begin{cases} \sqrt{X}/\log X & \text{if } 1 \leq r < \ell, \\ X & \text{if } r = 0. \end{cases}$$

(2) *There is a Ramanujan congruence modulo ℓ.*

Although the density results stated in Corollary 2 for $\ell = 5$, 7, and 11 are not given explicitly in [B-O], a modification of the arguments in that paper shows that the results remain true for these primes. Therefore we include them in the statement of Corollary 2 for completeness. □

4. Modular forms on $\Gamma_0(\ell^j)$.

In this section we will suppose that $\ell \geq 5$ is prime and that $j \geq 1$. If χ is a Dirichlet character defined modulo ℓ^j and k is a positive integer, then we denote by $M_k(\Gamma_0(\ell^j), \chi)$ the usual space of holomorphic modular forms of weight k and character χ for $\Gamma_0(\ell^j)$.

If $f(z)$ is a function of the upper half-plane and $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2^+(\mathbb{Q})$, then we define the slash operator by

$$(f\big|_k\gamma)(z) := (\det\gamma)^{\frac{k}{2}}(cz+d)^{-k}f(\gamma z).$$

If m is a positive integer, then we define operators U_m and V_m on formal power series by

$$\left(\sum_{n=0}^{\infty} a(n)q^n\right) \mid U_m := \sum_{n=0}^{\infty} a(mn)q^n,$$
$$\left(\sum_{n=0}^{\infty} a(n)q^n\right) \mid V_m := \sum_{n=0}^{\infty} a(n)q^{mn}.$$

If $f(z) = \sum_{n=0}^{\infty} a(n)q^n$ and $k \in \mathbb{Z}$, then we have

$$f(z)\big|U_m = \frac{1}{m}\sum_{j=0}^{m-1} f\left(\frac{z+j}{m}\right) = m^{\frac{k}{2}-1}\sum_{j=0}^{m-1} f\big|_k \begin{pmatrix} 1 & j \\ 0 & m \end{pmatrix}. \tag{4.1}$$

If $j \geq 1$, then the map $f \mapsto f\big|U_\ell$ takes $M_k(\Gamma_0(\ell^j), \chi)$ into itself, while the map $f \mapsto f\big|V_\ell$ takes $M_k(\Gamma_0(\ell^j), \chi)$ into $M_k(\Gamma_0(\ell^{j+1}), \chi)$. We define W_ℓ by

$$W_\ell := \begin{pmatrix} 0 & -1 \\ \ell & 0 \end{pmatrix};$$

if χ is a real character, then the Fricke involution

$$f \mapsto f\big|_k W_\ell$$

maps $M_k(\Gamma_0(\ell), \chi)$ into itself.

If $f \in M_k(\Gamma_0(\ell))$ then we define the trace of f by

$$\mathrm{Tr}(f) := f + \ell^{1-\frac{k}{2}}(f\big|_k W_\ell)\big|U_\ell. \tag{4.2}$$

We recall two important properties of these operators.

Proposition 4.1 [At-L, Lemma 17]. *Suppose that ℓ is prime and that $f \in M_k(\Gamma_0(\ell^j))$.*

(1) *If $j \geq 2$, then $f\big|U_\ell \in M_k(\Gamma_0(\ell^{j-1}))$.*
(2) *If $j = 1$, then $\mathrm{Tr}(f) \in M_k$.*

Finally, we recall that Dedekind's eta-function is given by

$$\eta(z) := q^{\frac{1}{24}} \prod_{n=1}^{\infty} (1-q^n).$$

If $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, then we have the transformation formula

$$\eta\left(\frac{az+b}{cz+d}\right) = \epsilon_{a,b,c,d} \cdot (cz+d)^{\frac{1}{2}} \cdot \eta(z), \tag{4.3}$$

where $\epsilon_{a,b,c,d}$ is a 24-th root of unity (we always take the branch of the square root having non-negative real part). As a special case of this formula, we have

$$\eta(-1/z) = \sqrt{z/i} \cdot \eta(z). \tag{4.4}$$

5. The Proof of Theorem 3.

For the duration we will fix a prime $\ell \geq 5$ and a positive integer j. We define

$$f_{\ell,j}(z) = \frac{\eta^{\ell^j}(\ell^j z)}{\eta(z)}.$$

Using standard facts (see, for example, [G-H] or [N2]), we see that

$$f_{\ell,j}(z) \in M_{\frac{\ell^j-1}{2}}\left(\Gamma_0(\ell^j), \left(\tfrac{\bullet}{\ell}\right)^j\right). \tag{5.1}$$

For convenience, we define

$$r_{\ell,j} := \frac{24\beta_{\ell,j}-1}{\ell^j} = \begin{cases} 24 \cdot (\lfloor \ell/24 \rfloor + 1) - \ell & \text{if } j \text{ is odd,} \\ 23 & \text{if } j \text{ is even,} \end{cases}$$

and

$$\lambda_{\ell,j} := \begin{cases} \frac{\ell^j-1}{2} + \frac{\ell^{j-1}(\ell-1)}{2} & \text{if } j \text{ is odd,} \\ \frac{\ell^j-1}{2} + \ell^{j-1}(\ell-1) & \text{if } j \text{ is even.} \end{cases}$$

We will show that Theorem 3 is a consequence of the following result.

Theorem 5.1. *If $\ell \geq 5$ is prime, and $j \geq 1$ is an integer, then there is a modular form $G_{\ell,j}(z) \in M_{\lambda_{\ell,j}} \cap \mathbb{Z}[[q]]$ such that $f_{\ell,j}(z) \big| U_{\ell^j} \equiv G_{\ell,j}(z) \pmod{\ell^j}$.*

To show that Theorem 5.1 implies Theorem 3, we begin by observing that

$$f_{\ell,j} \big| U_{\ell^j} = \prod_{n=1}^{\infty} (1-q^n)^{\ell^j} \cdot \sum_{n=0}^{\infty} p(\ell^j n + \beta_{\ell,j}) q^{n+\frac{r_{\ell,j}+\ell^j}{24}} = p(\beta_{\ell,j}) q^{\frac{r_{\ell,j}+\ell^j}{24}} + \cdots. \tag{5.2}$$

By Theorem 5.1, there exists $G_{\ell,j} \in M_{\lambda_{\ell,j}} \cap \mathbb{Z}[[q]]$ such that $f_{\ell,j}\big|U_{\ell^j} \equiv G_{\ell,j} \pmod{\ell^j}$. We may clearly suppose that $G_{\ell,j}$ vanishes to order at least $\frac{r_{\ell,j}+\ell^j}{24}$ at ∞. Using the fact that $\lambda_{\ell,j} = k_{\ell,j} + \frac{r_{\ell,j}+\ell^j}{2}$, we conclude that

$$G_{\ell,j}(z) = \Delta(z)^{\frac{r_{\ell,j}+\ell^j}{24}} \cdot F_{\ell,j}(z),$$

where $F_{\ell,j}(z) \in M_{k_{\ell,j}}$. By (5.2) we then have

$$\prod_{n=1}^{\infty}(1-q^n)^{\ell^j} \cdot \sum_{n=0}^{\infty} p(\ell^j n + \beta_{\ell,j}) q^{n+\frac{r_{\ell,j}+\ell^j}{24}} \equiv \Delta^{\frac{r_{\ell,j}+\ell^j}{24}}(z) \cdot F_{\ell,j}(z) \pmod{\ell^j},$$

from which Theorem 3 follows immediately.

We turn, therefore, to the proof of Theorem 5.1. We define

$$h_{\ell,j}(z) := \left(\frac{\eta^{\ell}(z)}{\eta(\ell z)}\right)^{\ell^{j-1}}.$$

We begin by recording some basic properties of this modular form.

Lemma 5.2. *Suppose that $\ell \geq 5$ is prime and that $j \geq 1$. Then*

(1) $h_{\ell,j}(z) \in M_{\frac{\ell^{j-1}(\ell-1)}{2}}\left(\Gamma_0(\ell), \left(\frac{\bullet}{\ell}\right)\right)$.

(2) $h_{\ell,j}(z) \equiv 1 \pmod{\ell^j}$.

(3) $h_{\ell,j}(z)\big|_{\frac{\ell^{j-1}(\ell-1)}{2}} W_\ell = \ell^{\frac{\ell^j+\ell^{j-1}}{4}} \cdot (-i)^{\frac{\ell^j-\ell^{j-1}}{2}} \cdot \left(\frac{\eta^{\ell}(\ell z)}{\eta(z)}\right)^{\ell^{j-1}}$.

Proof of Lemma 5.2. The first assertion follows from standard facts [G-H, N2], and the second is clear from the fact that

$$\prod_{n=1}^{\infty} \frac{(1-q^n)^{\ell}}{(1-q^{\ell n})} \equiv 1 \pmod{\ell}.$$

The third follows from a computation using (4.4). □

Now define

$$\rho_{\ell,j} := \begin{cases} 1 & \text{if } j \text{ is odd,} \\ 2 & \text{if } j \text{ is even.} \end{cases}$$

Then define

$$g_{\ell,j} := \left\{ f_{\ell,j} \cdot (h_{\ell,j}^{\rho_{\ell,j}} \big| V_{\ell^{j-1}}) \right\} \big| U_{\ell^{j-1}}.$$

Using (5.1), Lemma 5.2, and Proposition 4.1, we see that

$$g_{\ell,j} \in M_{\lambda_{\ell,j}}(\Gamma_0(\ell));$$

moreover it is clear that $g_{\ell,j}$ has integral coefficients. A straightforward argument shows that

$$g_{\ell,j} = f_{\ell,j} \big| U_{\ell^{j-1}} \cdot h_{\ell,j}^{\rho_{\ell,j}}.$$

Therefore, we see by (4.2) that

$$\operatorname{Tr}(g_{\ell,j}\big|_{\lambda_{\ell,j}} W_\ell) = \left\{ f_{\ell,j} \big| U_{\ell^{j-1}} \cdot h_{\ell,j}^{\rho_{\ell,j}} \right\} \big|_{\lambda_{\ell,j}} W_\ell + \ell^{1-\frac{\lambda_{\ell,j}}{2}} \cdot \left\{ f_{\ell,j} \big| U_{\ell^{j-1}} \cdot h_{\ell,j}^{\rho_{\ell,j}} \right\} \big| U_\ell. \tag{5.3}$$

Since the map $f \mapsto f\big|_k W_\ell$ preserves the field of rationality of a modular form $f \in M_k(\Gamma_0(\ell))$, each of the three summands in (5.3) has rational coefficients. Moreover, we have

$$\left\{ f_{\ell,j} \big| U_{\ell^{j-1}} \cdot h_{\ell,j}^{\rho_{\ell,j}} \right\} \big| U_\ell \equiv f_{\ell,j} \big| U_{\ell^j} \pmod{\ell^j}. \tag{5.4}$$

We will prove the following.

Lemma 5.3. *If $\ell \geq 5$ is prime and $j \geq 1$, then we have*

$$\ell^{\frac{\lambda_{\ell,j}}{2}-1} \cdot \left\{ f_{\ell,j} \big| U_{\ell^{j-1}} \cdot h_{\ell,j}^{\rho_{\ell,j}} \right\} \big|_{\lambda_{\ell,j}} W_\ell \equiv 0 \pmod{\ell^j}.$$

Theorem 5.1 follows immediately from Lemma 5.3, (5.3), and (5.4). Indeed, defining

$$G_{\ell,j} := \ell^{\frac{\lambda_{\ell,j}}{2}-1} \cdot \operatorname{Tr}(g_{\ell,j}\big|_{\lambda_{\ell,j}} W_\ell) \in M_{\lambda_{\ell,j}},$$

we see from these facts that $G_{\ell,j}$ has rational, ℓ-integral coefficients and that

$$G_{\ell,j} \equiv f_{\ell,j} \big| U_{\ell^j} \pmod{\ell^j}.$$

Theorem 5.1 follows (since $G_{\ell,j}$ has bounded denominators we may, if necessary, replace $G_{\ell,j}$ by $N \cdot G_{\ell,j}$ with a suitable integer $N \equiv 1 \pmod{\ell^j}$).

It remains only to prove Lemma 5.3. For the duration, let $\zeta := \exp(2\pi i/24\ell^j)$, and define

$$q_{\ell^j} := q^{\frac{1}{\ell^j}}.$$

We will consider power series in the ring $(\mathbb{Z}[\zeta])[[q_{\ell^j}]]$. In view of the third part of Lemma 5.2, it will suffice to show that, in this ring, we have

$$\ell^{\frac{(2\rho_{\ell,j}+1)\ell^j-5}{4}} \cdot \left\{ f_{\ell,j} \big| U_{\ell^{j-1}} \right\} \big|_{\frac{\ell^j-1}{2}} W_\ell \equiv 0 \pmod{\ell^j}.$$

By (4.1) and (4.3) we have

$$\begin{aligned} \ell^{\frac{(2\rho_{\ell,j}+1)\ell^j-5}{4}} \cdot \left\{ f_{\ell,j} \big| U_{\ell^{j-1}} \right\} \big|_{\frac{\ell^j-1}{2}} W_\ell &= \ell^{\frac{(2\rho_{\ell,j}+j)\ell^j-5j}{4}} \cdot \sum_{m=0}^{\ell^{j-1}-1} f_{\ell,j} \big|_{\frac{\ell^j-1}{2}} \begin{pmatrix} 1 & m \\ 0 & \ell^{j-1} \end{pmatrix} \big|_{\frac{\ell^j-1}{2}} \begin{pmatrix} 0 & -1 \\ \ell & 0 \end{pmatrix} \\ &= \ell^{\frac{\rho_{\ell,j}\ell^j-2j}{2}} \cdot z^{-\frac{\ell^j-1}{2}} \cdot \sum_{m=0}^{\ell^{j-1}-1} \frac{\eta^{\ell^j}\left(m\ell - \frac{1}{z}\right)}{\eta\left(\frac{m\ell z-1}{\ell^j z}\right)} \\ &= \ell^{\frac{\rho_{\ell,j}\ell^j-2j}{2}} \cdot z^{\frac{1}{2}} \cdot \eta^{\ell^j}(z) \cdot \sum_{m=0}^{\ell^{j-1}-1} \frac{\alpha_m}{\eta\left(\frac{m\ell z-1}{\ell^j z}\right)}, \end{aligned} \tag{5.5}$$

where α_m is some 24-th root of unity.

Fix m with $1 \leq m \leq \ell^{j-1} - 1$, and write $m = \ell^r t$ with $\ell \nmid t$ and $0 \leq r \leq j-2$. Then there are integers b, d for which $bt + d\ell^{j-r-1} = -1$. Hence,

$$\begin{pmatrix} m\ell & -1 \\ \ell^j & 0 \end{pmatrix} = \begin{pmatrix} t & d \\ \ell^{j-r-1} & -b \end{pmatrix} \cdot \begin{pmatrix} \ell^{r+1} & b \\ 0 & \ell^{j-r-1} \end{pmatrix},$$

where the first matrix on the right is in $\mathrm{SL}_2(\mathbb{Z})$. We conclude by (4.3) that

$$\eta\left(\frac{m\ell z - 1}{\ell^j z}\right) = \beta_m \cdot \ell^{\frac{r+1}{2}} \cdot z^{\frac{1}{2}} \cdot \eta\left(\frac{\ell^{r+1} z + b}{\ell^{j-r-1}}\right), \tag{5.6}$$

where β_m is a 24-th root of unity. It follows from (5.6) that if $m \geq 1$, then the term corresponding to m in (5.5) is given by

$$T_m := \frac{\alpha_m}{\zeta^{\ell^{r+1}b}\beta_m} \cdot \ell^{\frac{\rho_{\ell,j}\ell^j - 2j - r - 1}{2}} \cdot q_{\ell^j}^{\frac{\ell^{2j} - \ell^{2r+2}}{24}} \cdot \prod_{n=1}^{\infty} \frac{(1-q^n)^{\ell^j}}{(1 - \zeta^{24\ell^{r+1}bn} q_{\ell^j}^{\ell^{2r+2}n})}. \tag{5.7}$$

Furthermore, applying (4.4) we find that the term corresponding to $m = 0$ in (5.5) is given by

$$T_0 := \gamma \cdot \ell^{\frac{\rho_{\ell,j}\ell^j - 3j}{2}} \cdot \frac{\eta^{\ell^j}(z)}{\eta(\ell^j z)}, \tag{5.8}$$

where γ is a root of unity. Since $\ell \geq 5$ and $j \geq 1$ we have

$$\frac{\rho_{\ell,j}\ell^j - 2j - r - 1}{2} > \frac{\rho_{\ell,j}\ell^j - 3j}{2} \geq j. \tag{5.9}$$

By (5.7), (5.8), and (5.9) we have $T_m \equiv 0 \pmod{\ell^j}$ in $(\mathbb{Z}[\zeta])[[q_{\ell^j}]]$ for all m. This proves Lemma 5.3, and with it Theorem 5.1. □

Acknowledgements. The authors thank B. Berndt, H.H. Chan, and K. Ono for their valuable comments and suggestions.

References

[A] S. Ahlgren, *The partition function modulo composite integers M*, Math. Ann. **318** (2000), 795–803.

[A-O] S. Ahlgren and K. Ono, *Congruence properties for the partition function*, Proc. Nat. Acad. Sci., U.S.A. **98** (2001), no. 23, 12882-12884.

[An] G. E. Andrews, *The theory of partitions*, Cambridge Univ. Press, 1998.

[An-G] G. E. Andrews and F. Garvan, *Dyson's crank of a partition*, Bull. Amer. Math. Soc. (N.S.) **18** (1988), 167-171.

[At1] A. O. L. Atkin, *Proof of a conjecture of Ramanujan*, Glasgow Math. J. **8** (1967), 14-32.

[At2] A. O. L. Atkin, *Multiplicative congruence properties and density problems for $p(n)$*, Proc. London Math. Soc. (3) **18** (1968), 563–576.

[At-L] A. O. L. Atkin and J. Lehner, *Hecke operators on $\Gamma_0(N)$*, Math. Ann. **185** (1970), 134-160.

[At-Ob] A .O. L. Atkin and J. N. O'Brien, *Some properties of $p(n)$ and $c(n)$ modulo powers of* 13, Trans. Amer. Math. Soc. **126** (1967), 442-459.

[At-SwD] A. O. L. Atkin and H. P. F. Swinnerton-Dyer, *Some properties of partitions*, Proc. London Math. Soc. (3) **4** (1954), 84-106.

[Be-O] B. C. Berndt and K. Ono, *Ramanujan's unpublished manuscript on the partition and tau functions with commentary*, Seminaire Lotharingien de Combinatoire **42** (1999), Art. B42.

[B-O] J. H. Bruinier and K. Ono, *Coefficients of half-integral weight modular forms*, J. Number Theory **99** (2003), 164-179.

[C] H. H. Chan, *private communication.*

[D] F. J. Dyson, *Some guesses in the theory of partitions*, Eureka (Cambridge) **8** (1944), 10-15.

[G-K-S] F. Garvan, D. Kim and D. Stanton, *Cranks and t-cores*, Invent. Math. **101** (1990), 1-17.

[G-H] B. Gordon and K. Hughes, *Multiplicative properties of eta-products, II*, Cont. Math. **143** (1993), 415–430.

[K-Ol] I. Kiming and J. Olsson, *Congruences like Ramanujan's for powers of the partition function*, Arch. Math. **59** (1992), 348–360.

[Kl] T. Kløve, *Recurrence formulae for the coefficients of modular forms and congruences for the partition function and for the coefficients of $j(\tau)$, $(j(\tau)-1728)^{1/2}$, and $j(\tau)^{1/3}$*, Math. Scand. **23** (1969), 133-159.

[Ko] O. Kolberg, *Note on the parity of the partition function*, Math. Scand. **7** (1959), 377–378.

[N1] M. Newman, *Periodicity modulo m and divisibility properties of the partition function*, Trans. Amer. Math. Soc. **97** (1960), 225–236.

[N2] M. Newman, *Construction and application of a certain class of modular functions*, Proc. London Math. Soc. (3) **7** (1957), 334-350.

[O] K. Ono, *Distribution of the partition function modulo m*, Annals of Math. **151** (2000), 293–307.

[R1] S. Ramanujan, *On certain arithmetical functions*, Trans. Cambridge Philos. Soc. **22** (1916), 159–184.

[R2] S. Ramanujan, *Some properties of $p(n)$, the number of partitions of n*, Proc. Cambridge Philos. Soc. **19** (1919), 207–210.

[R3] S. Ramanujan, *Congruence properties of partitions*, Proc. London Math. Soc. **18** (1920), xix.

[R4] S. Ramanujan, *Congruence properties of partitions*, Math. Z. **9** (1921), 147–153.

[S] J.-P. Serre, *Formes modulaires et fonctions zêta p-adiques*, Springer Lect. Notes in Math. **350** (1973), 191–268.

[SwD] H. P. F. Swinnerton-Dyer, *On ℓ-adic representations and congruences for coefficients of modular forms*, Springer Lect. Notes in Math. **350** (1973), 1–55.

Department of Mathematics, University of Illinois, Urbana, Illinois 61801
E-mail address: ahlgren@math.uiuc.edu

Department of Mathematics, University of Illinois, Urbana, Illinois 61801
E-mail address: boylan@math.uiuc.edu