Exceptional congruences for powers of the partition function

by

MATTHEW BOYLAN (Urbana, IL)

1. Introduction. A partition of a positive integer n is any non-increasing sequence of positive integers whose sum is n. The partition function, denoted by p(n), enumerates the number of partitions of n. By convention, p(0) = 1 and p(n) = 0 if n < 0. As is well known by the work of Euler, the generating function for p(n) is given by

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

The study of the arithmetic properties of p(n) has a long history beginning with the fundamental work of Ramanujan [R1–R4]. When r is an integer, we denote by P_r the rth power of Euler's generating function. In this paper, we study arithmetic properties of the coefficients of P_r when r is positive. Therefore, we define the arithmetic functions $p_r(n)$, which we call the rth powers of the partition function, by

(1.1)
$$P_r(q) = \sum_{n=0}^{\infty} p_r(n) q^n := \prod_{n=1}^{\infty} (1-q^n)^{-r} = 1 + rq + \dots, \quad r \in \mathbb{Z}.$$

The functions $p_r(n)$ have been studied, for example, by Atkin, Gordon, Kiming, Newman, Olsson, Ramanujan, and Serre [A, G, K-O, N1–N7, S3].

If $\ell \geq 5$ is prime and $0 \leq a \leq \ell - 1$, then following Kiming and Olsson, we say that there is a *congruence for* p at (ℓ, r, a) if, for all integers n,

$$p_r(\ell n + a) \equiv 0 \pmod{\ell}.$$

Before presenting our results, we cite some facts from [K-O] concerning the classification of congruences of this type. In what follows, $\left(\frac{i}{\ell}\right)$ denotes the Legendre symbol modulo ℓ .

²⁰⁰⁰ Mathematics Subject Classification: Primary 11F33; Secondary 11P83.

The author thanks the National Science Foundation for its support through a VIGRE postdoctoral fellowship.

PROPOSITION 1.1 ([K-O, Lemma 1, Theorem 2]). Suppose that $\ell \geq 5$ is prime and $0 \leq a \leq \ell - 1$.

(1) There is a congruence for p at (ℓ, r, a) if and only if there is a congruence for p at $(\ell, r + \ell, a)$.

(2) If $r \equiv 0 \pmod{\ell}$, then there is a congruence for p at (ℓ, r, a) if and only if $a \neq 0$.

(3) There is a congruence for p at $(\ell, \ell - 1, a)$ if and only if

$$\left(\frac{24a+1}{\ell}\right) = -1.$$

(4) There is a congruence for p at $(\ell, \ell - 3, a)$ if and only if

$$\left(\frac{8a+1}{\ell}\right) \neq 1.$$

Items (3) and (4) of Proposition 1.1 follow from the following well known q-series identities of Euler and Jacobi together with item (1) of Proposition 1.1.

(1) (Euler)

$$\prod_{n=1}^{\infty} (1-q^n) = \sum_{n=-\infty}^{\infty} (-1)^n q^{n(3n+1)/2},$$

(2) (Jacobi)

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

Following the terminology of Kiming and Olsson, we say that a congruence for p at (ℓ, r, a) is *exceptional* if $1 \le r \le \ell - 1$ and $r \ne \ell - 1$, $\ell - 3$. The main result from [K-O] is the following.

THEOREM 1.2 ([K-O, Theorem 1]). If $\ell \geq 5$ is prime and if there is an exceptional congruence for p at (ℓ, r, a) , then r is odd and $24a \equiv r \pmod{\ell}$.

Therefore, we will say that ℓ is exceptional for r if there is an exceptional congruence in the distinguished class $24^{-1}r \pmod{\ell}$.

Now suppose that $\ell \geq 5$ is a fixed prime. One can classify all r for which ℓ is exceptional by a finite computation. In particular, by Proposition 1.1 and Theorem 1.2, it suffices to check whether ℓ is exceptional for all odd $r \leq \ell - 1$. Some details concerning computations of this type are included in Section 6.

In this paper we consider the problem of classifying all exceptional primes ℓ for a fixed r. This problem requires different methods; clearly, one cannot classify all exceptional primes for r by checking each prime $\ell \ge r+2$ individually. In [A-B], the author and Ahlgren use modular forms modulo ℓ to

reduce the problem for r = 1 to a finite computation. In particular, they show that the only congruences of the form $p(\ell n + a) \equiv 0 \pmod{\ell}$ are the celebrated Ramanujan congruences

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

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

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

In Section 2, we state the main theorem of this paper, Theorem 2.1, which is a generalization of the results in [A-B] to all odd r. In fact, for any odd r, we show (subject to a mild hypothesis) how to obtain the complete set of exceptional primes. We also state a related theorem, Theorem 2.3, which explains the existence of many exceptional congruences. As an example of Theorem 2.1, we completely classify all exceptional congruences for $r \leq 47$.

THEOREM 1.3. The following table gives the complete list of exceptional primes ℓ for $r \leq 47$.

r	ℓ	r	ℓ	r	l	r	l
1	5, 7, 11	13	17, 19, 23	25	29,31	37	41, 43, 47
3	11, 17	15	23, 29	27	31, 41	39	47, 53, 61
5	11, 23	17	23	29	none	41	47
7	11, 19	19	23	31	none	43	47
9	17, 19, 23	21	29, 31, 47	33	41, 43, 47, 59	45	53, 59, 71
11	none	23	none	35	none	47	none

The proofs of our results depend on a careful study of the reductions modulo primes of certain modular forms related to the functions $p_r(n)$. Section 3 gives the necessary facts on modular forms modulo primes. In Section 4, we prove Theorem 2.1, and in Section 5, we prove Theorem 2.3. In Section 6, we briefly describe how to computationally verify exceptional congruences.

2. Statement of results. Before we state our main result, we need to define our notation. If N and k are positive integers and χ is a Dirichlet character defined modulo N, then we denote by $M_k(\Gamma_0(N), \chi)$ the \mathbb{C} -vector space of holomorphic modular forms of weight k and character χ for $\Gamma_0(N)$. We denote by $S_k(\Gamma_0(N), \chi)$ the subspace of cusp forms in $M_k(\Gamma_0(N), \chi)$. We identify $f(z) \in M_k(\Gamma_0(N), \chi)$ with its Fourier series in the variable $q := e^{2\pi i z}$.

In particular, when k is even, we denote by M_k the \mathbb{C} -vector space of holomorphic modular forms of weight k with respect to $\Gamma_0(1) = \mathrm{SL}_2(\mathbb{Z})$. The usual Eisenstein series of weights 4 and 6 on $\mathrm{SL}_2(\mathbb{Z})$ are given by

$$E_4(z) := 1 + 240 \sum_{n=1}^{\infty} \sum_{\substack{d|n \\ d>0}} d^3 q^n \in M_4 \cap \mathbb{Z}[[q]],$$
$$E_6(z) := 1 - 504 \sum_{n=1}^{\infty} \sum_{\substack{d|n \\ d>0}} d^5 q^n \in M_6 \cap \mathbb{Z}[[q]].$$

For convenience, we define $E_k^*(z)$ by

$$E_k^*(z) := \begin{cases} 1 & \text{if } k \equiv 0 \pmod{12}, \\ E_4(z)^2 E_6(z) & \text{if } k \equiv 2 \pmod{12}, \\ E_4(z) & \text{if } k \equiv 4 \pmod{12}, \\ E_6(z) & \text{if } k \equiv 6 \pmod{12}, \\ E_4(z)^2 & \text{if } k \equiv 8 \pmod{12}, \\ E_4(z) E_6(z) & \text{if } k \equiv 10 \pmod{12}. \end{cases}$$

We recall that Dedekind's eta-function is given by

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

Then

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

is the unique normalized weight 12 cusp form on $SL_2(\mathbb{Z})$.

Throughout, we let r be a fixed odd positive integer, and we let

(2.2)
$$\alpha_r := \begin{cases} \left\lfloor \frac{r+3}{12} \right\rfloor & \text{if } r \not\equiv 11 \pmod{12}, \\ \left\lfloor \frac{r+3}{12} \right\rfloor - 1 & \text{if } r \equiv 11 \pmod{12}. \end{cases}$$

We define integers $a_{r,i}$ by

(2.3)
$$\sum_{n=i}^{\infty} a_{r,i}(n)q^n := P_r E_{r+3}^* E_4^{3(\alpha_r - 1)} \Delta^i = q^i + \dots, \quad 0 \le i \le \alpha_r.$$

We also let

$$A_r(0) := (-r)^{(r+3)/2},$$

and for each positive integer n, we define

$$A_r^{\pm}(n) := \pm (24n - r)^{(r+3)/2} p_r(n).$$

Next, we define the set

$$S := \{ (s(1), \dots, s(\alpha_r)) \mid s(j) \in \{+, -\}, 1 \le j \le \alpha_r \}.$$

190

For a fixed $\bar{s} = (s(1), \ldots, s(\alpha_r)) \in S$, we set

$$c_{r,0}(\bar{s}) := A_r(0),$$

$$c_{r,n}(\bar{s}) := A_r^{s(n)}(n) - \sum_{i=0}^{n-1} c_{r,i}(\bar{s}) a_{r,i}(n), \quad 1 \le n \le \alpha_r.$$

Finally, we define the set of integers $\mathfrak{B}_r(n)$ for each $n \ge \alpha_r + 1$ by

$$\mathfrak{B}_r(n) := \left\{ A_r^{\pm}(n) - \sum_{i=0}^{\alpha_r} c_{r,i}(\bar{s}) a_{r,i}(n) \right\}_{\bar{s} \in S}$$

We observe that each $\mathfrak{B}_r(n)$ contains 2^{α_r+1} integers. By Proposition 1.1, we need only consider $\ell \geq r$.

THEOREM 2.1. Let r be an odd positive integer.

(1) If $\ell = r + 2$ is prime, then ℓ is not exceptional for r.

(2) If $\ell = r + 4$ is prime, then ℓ is exceptional for r if and only if $\ell \equiv 2 \pmod{3}$.

(3) If $\ell \ge r+6$ is an exceptional prime for r, then for every $n \ge \alpha_r+1$, ℓ divides at least one integer in $\mathfrak{B}_r(n)$.

As an obvious corollary, we have

COROLLARY 2.2. If r is an odd positive integer and if there is some $n \ge \alpha_r + 1$ for which all of the integers in $\mathfrak{B}_r(n)$ are non-zero, then the set of exceptional primes for r is finite.

If the hypotheses of Corollary 2.2 are satisfied, then Theorem 2.1 may be used to show that all but finitely many primes are not exceptional for r. The remaining primes must be checked individually to determine whether they are exceptional, which may be done by applying Theorem 2.3 below or the methods of Section 6, as appropriate. In this way, the exceptional primes for r may be determined by a finite computation.

For example, to compute the exceptional primes for r = 37, we find that all of the integers in $\mathfrak{B}_{37}(4)$ and $\mathfrak{B}_{37}(5)$ are non-zero and that the only primes common to the prime divisors of the integers in both sets are $\ell = 41, 43$, and 47. These primes are exceptional for 37 by Theorem 2.3.

For completeness, we include Theorem 2.3, which is well known to experts. Its proof is included in Section 5. In contrast to Theorem 2.1 and Corollary 2.2, Theorem 2.3 explains the existence of many exceptional congruences.

THEOREM 2.3. Suppose that $\ell \geq 5$ is prime.

(1) Let i = 4, 8, or 14. If $\ell \equiv 2 \pmod{3}$ and $\ell - i > 0$, then ℓ is exceptional for $r = \ell - i$.

(2) Let i = 6 or 10. If $\ell \equiv 3 \pmod{4}$ and $\ell - i > 0$, then ℓ is exceptional for $r = \ell - i$.

(3) Let i = 26. If $\ell \equiv 11 \pmod{12}$ and $\ell - i > 0$, then ℓ is exceptional for $r = \ell - i$.

We observe that Theorem 2.3 contains the Ramanujan congruences (1.2), (1.3), and (1.4) as special cases. In fact, Theorem 2.3 appears to explain most, but not all, exceptional congruences. Therefore, one might refer to congruences which are not explained by Theorem 2.3 as *superexceptional*. For example, Theorem 1.3 indicates that 19, 23 and 61 are superexceptional primes for 7, 5, and 39, respectively, and that these are the only superexceptional primes for $r \leq 47$.

Theorem 2.3 also shows that if $r \equiv 11 \pmod{12}$ and ℓ is exceptional for r, then ℓ must be superexceptional for r. This "explains" why no congruences of this specific type have been found (to our knowledge).

3. Modular forms modulo ℓ . We now record some relevant facts concerning modular forms modulo ℓ . Details may be found, for example, in [SwD] or [S1]. Throughout this section we will suppose that $\ell \geq 5$ is a fixed prime. If $f = \sum_{n=0}^{\infty} a(n)q^n \in M_k \cap \mathbb{Z}[[q]]$, then

$$f := f \pmod{\ell} \in \mathbb{F}_{\ell}[[q]].$$

We define the space of weight k modular forms modulo ℓ by

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

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 we have $\widetilde{f} \equiv \widetilde{g} \not\equiv 0 \pmod{\ell}$, then it must be that $k \equiv k' \pmod{\ell-1}$. It follows that if $f \in M_k \cap \mathbb{Z}[[q]]$ has $\widetilde{f} \not\equiv 0 \pmod{\ell}$, then

(3.1)
$$w(f) \equiv k \pmod{\ell - 1}.$$

Moreover, we see that $w(f) = -\infty$ if and only if $\tilde{f} \equiv 0 \pmod{\ell}$. We also recall the fact [S1, §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

$$(3.2) w(f^i) = iw(f).$$

We define the theta operator on formal power series by

(3.3)
$$\Theta\Big(\sum_{n=0}^{\infty} a(n)q^n\Big) := \sum_{n=1}^{\infty} na(n)q^n.$$

Lemma 3.1 is fundamentally important in what follows.

LEMMA 3.1 ([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 for some $\alpha \geq 0$, we have $w(\Theta f) = w(f) + \ell + 1 - \alpha(\ell - 1)$, with $\alpha > 0$ if and only if $w(f) \equiv 0 \pmod{\ell}$.

Next, we define the operator U_{ℓ} on formal power series by

(3.4)
$$\left(\sum_{n=0}^{\infty} a(n)q^n\right) \Big| U_{\ell} := \sum_{n=0}^{\infty} a(\ell n)q^n.$$

When N and k are positive integers and χ is a Dirichlet character defined modulo N, the Hecke operator $T_{\ell,k}$ acts on a modular form $f(z) = \sum_{n=0}^{\infty} a(n)q^n \in M_k(\Gamma_0(N), \chi)$ by the formula

(3.5)
$$\left(\sum_{n=0}^{\infty} a(n)q^n\right) \Big| T_{\ell,k} := \sum_{n=0}^{\infty} \left(a(\ell n) + \chi(\ell)\ell^{k-1}a\left(\frac{n}{\ell}\right)\right) q^n \\ \in M_k(\Gamma_0(N),\chi),$$

where $a\left(\frac{n}{\ell}\right) = 0$ if $\ell \nmid n$. Comparing (3.4) and (3.5), we see that for $k \geq 2$, the operators $T_{\ell,k}$ and U_{ℓ} agree modulo ℓ . It follows that $U_{\ell} : \widetilde{M}_k \to \widetilde{M}_k$. It is also well known that if $f(z) = \sum_{n=1}^{\infty} a(n)q^n$ is a normalized eigenform for all of the $T_{\ell,k}$, then

(3.6)
$$a(mn) = a(m)a(n)$$
 if $gcd(m, n) = 1$,

(3.7)
$$a(\ell^t) = a(\ell^{t-1})a(\ell) - \chi(\ell)\ell^{k-1}a(\ell^{t-2}) \quad \text{if } t \ge 1.$$

For all $f \in \mathbb{Z}[[q]]$, the relationship between the operators Θ and U_{ℓ} is given by

(3.8)
$$(f|U_{\ell})^{\ell} \equiv f - \Theta^{\ell-1} f \pmod{\ell}.$$

Using (3.8) and Lemma 3.1, we see that the operator U_{ℓ} contracts the space \widetilde{M}_k .

LEMMA 3.2 ([S1, §2.2, Lemme 2]). Suppose that $\ell \geq 5$ is prime and $f \in M_k \cap \mathbb{Z}[[q]]$.

(1) We have

$$w(f|U_{\ell}) \le \ell + \frac{w(f) - 1}{\ell}.$$

(2) If $w(f) = \ell - 1$, then

$$w(f|U_\ell) = \ell - 1.$$

We also require a suitable basis for the space \widetilde{M}_k . It is well known that

(3.9)
$$d_k := \operatorname{dimension}(M_k) = \begin{cases} \left\lfloor \frac{k}{12} \right\rfloor + 1 & \text{if } k \not\equiv 2 \pmod{12}, \\ \left\lfloor \frac{k}{12} \right\rfloor & \text{if } k \equiv 2 \pmod{12}. \end{cases}$$

Using the forms $E_k^*(z)$ defined in Section 2, we see that a basis for M_k may be given as

(3.10)
$$B_k = \{E_k^* E_4^{3(d_k - 1 - i)} \Delta^i = q^i + \dots\}_{i=0}^{d_k - 1}.$$

Therefore, a basis for M_k consists of the reductions modulo ℓ of the basis forms in B_k .

4. The proof of Theorem 2.1. The proof of Theorem 2.1 is an extension of the method of Ahlgren and Boylan [A-B] to all odd positive integers r. As in [A-B] and [K-O], we will consider the sequence of filtrations $\{w(f), w(\theta(f)), w(\theta^2(f)), \ldots\}$, where f is a suitable modular form. We remind the reader that ℓ is prime and $\ell \ge r + 2$. For the duration of the proof, we set

$$\delta_\ell := \frac{\ell^2 - 1}{24},$$

and observe that $24(-r\delta_{\ell}) \equiv r \pmod{\ell}$. From (1.1) and (2.1) we deduce that

$$\Delta^{r\delta_{\ell}} = q^{r\delta_{\ell}} \prod_{n=1}^{\infty} \frac{(1-q^n)^{r\ell^2}}{(1-q^n)^r} \equiv \prod_{n=1}^{\infty} (1-q^{\ell n})^{r\ell} \cdot \sum_{n=0}^{\infty} p_r(n-r\delta_{\ell})q^n \pmod{\ell},$$

which implies that

(4.1)
$$\Delta^{r\delta_{\ell}}|U_{\ell} \equiv \prod_{n=1}^{\infty} (1-q^n)^{r\ell} \cdot \sum_{n=0}^{\infty} p_r(\ell n - r\delta_{\ell})q^n \; (\mathrm{mod}\,\ell).$$

Hence, if ℓ is exceptional for r, (4.1) implies that $\Delta^{r\delta_{\ell}}|U_{\ell} \equiv 0 \pmod{\ell}$. That is, we must have $w(\Delta^{r\delta_{\ell}}|U_{\ell}) = -\infty$.

Furthermore, by (3.2), it is clear that

(4.2)
$$w(\Delta^{r\delta_{\ell}}) = r\delta_{\ell} \cdot w(\Delta) = \frac{r(\ell^2 - 1)}{2} \equiv \frac{\ell - r}{2} \pmod{\ell}.$$

By (3.9) and (3.10), a modular form $f \in M_k$ has $\operatorname{ord}_{\infty} f \leq k/12$. Therefore, we obtain the following.

LEMMA 4.1 (cf. [K-O, Lemma 2]). If m is a positive integer, then $w(\Theta^m \Delta^{r\delta_\ell}) \ge w(\Delta^{r\delta_\ell}).$

Using (4.2) and iterating Lemma 3.1 give

(4.3)
$$w(\Theta^{(\ell+r)/2}\Delta^{r\delta_{\ell}}) \equiv 0 \pmod{\ell},$$

where $j = (\ell + r)/2$ is the smallest positive integer for which $w(\Theta^j \Delta^{r\delta_\ell}) \equiv 0 \pmod{\ell}$. We turn to the proof of Theorem 2.1(1).

The proof of Theorem 2.1(1). Suppose that $\ell = r + 2$ is prime. If ℓ is exceptional for r, then using (3.2) and (3.8), we conclude that

$$w(\Delta^{r\delta_{\ell}}|U_{\ell}) = -\infty = \frac{1}{\ell} w(\Delta^{r\delta_{\ell}} - \Theta^{\ell-1}\Delta^{r\delta_{\ell}}).$$

It follows that $\Theta^{\ell-1}\Delta^{r\delta_{\ell}} \equiv \Delta^{r\delta_{\ell}} \pmod{\ell}$, and hence, that $w(\Theta^{\ell-1}\Delta^{r\delta_{\ell}}) = w(\Delta^{r\delta_{\ell}})$. By (4.3), we have $w(\Theta^{\ell-1}\Delta^{r\delta_{\ell}}) \equiv 0 \pmod{\ell}$, but by (4.2), we have $w(\Delta^{r\delta_{\ell}}) \not\equiv 0 \pmod{\ell}$. Therefore, the prime $\ell = r+2$ is not exceptional for r.

The proof of Theorem 2.1(2). To prove Theorem 2.1(2), we begin by defining, for every $n \ge 1$, integers $A_4(n)$ by

$$\sum_{n=1}^{\infty} A_4(n)q^n := \eta^4(6z) \in S_2(\Gamma_0(36)).$$

We need the following proposition.

PROPOSITION 4.2. If $\ell \geq 5$ is prime and $r = \ell - 4$, then ℓ is exceptional for r if and only if $A_4(\ell) \equiv 0 \pmod{\ell}$.

Proof. We observe that

$$\sum_{n=1}^{\infty} A_4(n)q^n = q \prod_{n=1}^{\infty} (1-q^{6n})^4 = q \prod_{n=1}^{\infty} \frac{(1-q^{6n})^\ell}{(1-q^{6n})^r}$$
$$\equiv \sum_{k=0}^{\infty} p_{-1}(k)q^{6k\ell} \cdot \sum_{j=0}^{\infty} p_r(j)q^{6j+1} \pmod{\ell}.$$

It follows that for all n, we have

(4.4)
$$A_4(6\ell n + \ell^2) \equiv \sum_{k=0}^{\infty} p_{-1}(k) p_r\left(\ell(n-k) + \frac{\ell^2 - 1}{6}\right) \pmod{\ell}$$

We note that $(\ell^2 - 1)/6 \equiv -r\delta_\ell \pmod{\ell}$. We let $6\ell n + \ell^2 = \ell^t s$ with $t \ge 1$ and $\ell \nmid s$. It is well known that the modular form $\eta^4(6z)$ is a normalized eigenform for all of the Hecke operators (since, for example, the space $S_2(\Gamma_0(36))$ is one-dimensional). By (3.6) and (3.7), we have the formulae

(4.5)
$$A_4(\ell^t s) = \begin{cases} A_4(\ell)A_4(s) & \text{if } t = 1, \\ (A_4(\ell^{t-1})A_4(\ell) - \ell A_4(\ell^{t-2}))A_4(s) \\ \equiv A_4(\ell^{t-1})A_4(\ell)A_4(s) \pmod{\ell} & \text{if } t > 1. \end{cases}$$

If $A_4(\ell) \equiv 0 \pmod{\ell}$, then by (4.5), we have

$$A_4(6\ell n + \ell^2) = A_4(\ell^t s) \equiv 0 \pmod{\ell} \quad \text{for all } n.$$

By induction on n using (4.4) and the fact that $p_{-1}(0) = 1$, we see that

$$p_r\left(\ell n + \frac{\ell^2 - 1}{6}\right) \equiv 0 \pmod{\ell} \quad \text{for all } n,$$

and hence, that ℓ is exceptional for r.

Conversely, if ℓ is exceptional for r, (4.4) shows that for all n, we must have $A_4(6n\ell + \ell^2) \equiv 0 \pmod{\ell}$. In particular, setting n = 0 and using (4.5) gives $A_4(\ell^2) \equiv A_4(\ell)^2 \equiv 0 \pmod{\ell}$. Hence $A_4(\ell) \equiv 0 \pmod{\ell}$.

To conclude, it suffices to show that $A_4(\ell) \equiv 0 \pmod{\ell}$ if and only if $\ell \equiv 2 \pmod{3}$. This is a consequence of the following.

PROPOSITION 4.3 (cf. [M-O, Theorem 3]). If $\ell \geq 5$ is prime, then

(4.6)
$$A_4(\ell) = \begin{cases} 0 & \text{if } \ell \equiv 2 \pmod{3}, \\ 2n \cdot \binom{n}{3} & \text{if } \ell \equiv 1 \pmod{3}, \ \ell = n^2 + 3m^2. \end{cases}$$

One may deduce (4.6) by combining the following *q*-series identities of Gauss, Köhler, and Macdonald ([A-A-R, Corollary 10.4.2], [K], [M]).

(1) (Gauss)

$$\frac{\eta^2(z)}{\eta(2z)} = \prod_{n=1}^{\infty} \frac{(1-q^n)^2}{1-q^{2n}} = 1 + 2\sum_{n=1}^{\infty} (-1)^n q^{n^2},$$

(2) (Köhler–MacDonald)

$$\frac{\eta^5(6z)}{\eta^2(3z)} = q \prod_{n=1}^{\infty} \frac{(1-q^{6n})^5}{(1-q^{3n})^2} = \sum_{n=1}^{\infty} (-1)^{n-1} \left(\frac{n}{3}\right) n q^{n^2}.$$

We will revisit (4.6) in the context of Hecke newforms with complex multiplication in Section 5. \blacksquare

The proof of Theorem 2.1(3). We now consider primes $\ell \ge r+6$. In such cases, $(\ell + r)/2 < \ell - 2$, so by (4.3), (4.2), Lemmas 3.1 and 4.1, there is an integer $0 < \alpha < \ell - 1$ for which

(4.7)
$$w(\Theta^{(\ell+r)/2+1}\Delta^{r\delta_{\ell}}) = \frac{r(\ell^2-1)}{2} + \left(\frac{\ell+r}{2}+1\right)(\ell+1) - \alpha(\ell-1)$$

 $\ge w(\Delta^{r\delta_{\ell}}) = \frac{r(\ell^2-1)}{2}.$

From (4.7), we have

$$1 \le \alpha \le \left(\frac{\ell+r}{2}+1\right) \left(\frac{\ell+1}{\ell-1}\right)$$
$$= \left(\frac{\ell+r}{2}+1\right) \left(1+\frac{2}{\ell-1}\right) = \frac{\ell+r}{2}+2+\frac{r+3}{\ell-1}.$$

196

Hence, since $\ell \ge r+6$, we find that

(4.8)
$$1 \le \alpha \le (\ell + r)/2 + 2$$

We would like to obtain the exact value of α when ℓ is exceptional for r so that we may explicitly evaluate (4.7). If ℓ is exceptional for r, we recall that

$$w(\Delta^{r\delta_{\ell}}|U_{\ell}) = -\infty = \frac{1}{\ell} w(\Delta^{r\delta_{\ell}} - \Theta^{\ell-1}\Delta^{r\delta_{\ell}}).$$

Therefore, it is immediate that

(4.9)
$$w(\Theta^{\ell-1}\Delta^{r\delta_{\ell}}) = w(\Delta^{r\delta_{\ell}}) = r(\ell^2 - 1)/2.$$

If we suppose that $w(\Theta^{\ell-2}\Delta^{r\delta_{\ell}}) \not\equiv 0 \pmod{\ell}$, then Lemma 3.1 and (4.9) give

$$w(\Theta^{\ell-1}\Delta^{r\delta_\ell}) = w(\Theta^{\ell-2}\Delta^{r\delta_\ell}) + \ell + 1 = r(\ell^2 - 1)/2,$$

implying that

$$w(\Theta^{\ell-2}\Delta^{r\delta_{\ell}}) < w(\Delta^{r\delta_{\ell}}),$$

which contradicts Lemma 4.1. Thus, it must be that

(4.10)
$$w(\Theta^{\ell-2}\Delta^{r\delta_{\ell}}) \equiv 0 \pmod{\ell}.$$

From (4.3), (4.8), and (4.10), we see that there is a least positive integer $j \leq (\ell - r)/2 - 2$ for which

$$w(\Theta^{(\ell+r)/2+j}\Delta^{r\delta_{\ell}}) \equiv 0 \pmod{\ell}.$$

However, using (4.2), (4.3), and Lemma 3.1, we may also write

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

Since $\alpha_r \leq (\ell + r)/2 + 2$ and $j \leq (\ell - r)/2 - 2$, we conclude that $\alpha = (\ell + r)/2 + 2$.

Returning to the computation (4.7), we find that

$$w(\Theta^{(\ell+r)/2+1}\Delta^{r\delta_{\ell}}) = \frac{r(\ell^2 - 1)}{2} + \left(\frac{\ell + r}{2} + 1\right)(\ell + 1) + \left(\frac{\ell + r}{2} + 2\right)(\ell - 1)$$
$$= \frac{r(\ell^2 - 1)}{2} + r + 3 \equiv r + 3 \pmod{12},$$

which shows that the reduction modulo ℓ of

(4.11)
$$\Theta^{(\ell+r)/2+1} \Delta^{r\delta_{\ell}} = (r\delta_{\ell})^{(\ell+r)/2+1} q^{r\delta_{\ell}} + \dots \not\equiv 0 \pmod{\ell}$$

lies in the space $M_{(r(\ell^2-1))/2+r+3}$. By (3.10), a basis for $M_{(r(\ell^2-1))/2+r+3}$ may be given as

(4.12)
$$B_{r,\ell} := \{ E_{r+3}^* E_4^{3(r\delta_\ell + \alpha_r - i)} \Delta^i = q^i + \ldots \}_{i=0}^{r\delta_\ell + \alpha_r}.$$

Using (1.1), (2.1), (2.3), (4.11), and (4.12), it follows that for $r\delta_{\ell} \leq i \leq r\delta_{\ell} + \alpha_r$, there are integers b_i which satisfy

$$(4.13) \quad \left(\frac{-6r}{\ell}\right) 24^{(r+3)/2} \Theta^{(\ell+r)/2+1} \Delta^{r\delta_{\ell}}$$

$$\equiv \left(\frac{-6r}{\ell}\right) 24^{(r+3)/2} \sum_{i=r\delta_{\ell}}^{r\delta_{\ell}+\alpha_{r}} b_{i} E_{r+3}^{*} E_{4}^{3(r\delta_{\ell}+\alpha_{r}-i)} \Delta^{i}$$

$$\equiv \Delta^{r\delta_{\ell}} \sum_{i=0}^{\alpha_{r}} \left(\frac{-6r}{\ell}\right) 24^{(r+3)/2} b_{i+r\delta_{\ell}} E_{r+3}^{*} E_{4}^{3(\alpha_{r}-i)} \Delta^{i}$$

$$\equiv q^{r\delta_{\ell}} \prod_{n=1}^{\infty} (1-q^{n})^{r\ell^{2}} \cdot \sum_{i=0}^{\alpha_{r}} c_{r,i} P_{r} E_{r+3}^{*} E_{4}^{3(\alpha_{r}-i)} \Delta^{i}$$

$$\equiv q^{r\delta_{\ell}} \prod_{n=1}^{\infty} (1-q^{n})^{r\ell^{2}} \cdot \sum_{i=0}^{\alpha_{r}} \sum_{n=i}^{\infty} c_{r,i} a_{r,i}(n) q^{n} \pmod{\ell},$$

where

$$c_{r,i} := \left(\frac{-6r}{\ell}\right) 24^{(r+3)/2} b_{i+r\delta_{\ell}}.$$

Next, we observe that

$$\Theta\left(\prod_{n=1}^{\infty} (1-q^n)^{r\ell^2}\right) \equiv 0 \; (\mathrm{mod}\,\ell).$$

Using this together with (1.1), (2.1), (3.3), and the fact that for all n, we have $n^{(\ell-1)/2} \equiv \left(\frac{n}{\ell}\right) \pmod{\ell}$, we compute

$$(4.14) \qquad \left(\frac{-6r}{\ell}\right) 24^{(r+3)/2} \Theta^{(\ell+r)/2+1} \Delta^{r\delta_{\ell}} = \left(\frac{-6r}{\ell}\right) 24^{(r+3)/2} \Theta^{(\ell+r)/2+1} \left(\prod_{n=1}^{\infty} (1-q^n)^{r\ell^2} \cdot \sum_{n=0}^{\infty} p_r(n)q^{n+r\delta_{\ell}}\right) \equiv \left(\frac{-6r}{\ell}\right) 24^{(r+3)/2} \prod_{n=1}^{\infty} (1-q^n)^{r\ell^2} \cdot \Theta^{(\ell+r)/2+1} \left(\sum_{n=0}^{\infty} p_r(n)q^{n+r\delta_{\ell}}\right) \equiv q^{r\delta_{\ell}} \prod_{n=1}^{\infty} (1-q^n)^{r\ell^2} \times \sum_{n=0}^{\infty} \left(\left(\frac{-6r}{\ell}\right) 24^{(r+3)/2} \left(n + \frac{r(\ell^2-1)}{24}\right)^{(\ell+r)/2+1} p_r(n)\right) q^n \equiv q^{r\delta_{\ell}} \prod_{n=1}^{\infty} (1-q^n)^{r\ell^2} \cdot \sum_{n=0}^{\infty} \left(\frac{r(r-24n)}{\ell}\right) (24n-r)^{(r+3)/2} p_r(n)q^n \pmod{\ell}.$$

Comparing coefficients in (4.13) and (4.14) yields

(4.15)
$$\sum_{i=0}^{\alpha_r} \sum_{n=i}^{\infty} c_{r,i} a_{r,i}(n) q^n$$
$$= \sum_{n=0}^{\alpha_r} \sum_{i=0}^n c_{r,i} a_{r,i}(n) q^n + \sum_{n=\alpha_r+1}^{\infty} \sum_{i=0}^{\alpha_r} c_{r,i} a_{r,i}(n) q^n$$
$$\equiv \sum_{n=0}^{\infty} \left(\frac{r(r-24n)}{\ell} \right) (24n-r)^{(r+3)/2} p_r(n) q^n \pmod{\ell}.$$

When $0 \le n \le \alpha_r$, we note that $a_{r,n}(n) = 1$. We also note that $p_r(0) = 1$ for all r. In particular, when n = 0, we see by (4.15) that

$$c_{r,0} \equiv \left(\frac{r^2}{\ell}\right) (-r)^{(r+3)/2} \pmod{\ell}.$$

Since $\ell \ge r + 6$, it follows that $\ell \nmid r$. Therefore, $\left(\frac{r^2}{\ell}\right) = 1$, which gives

(4.16)
$$c_{r,0} \equiv (-r)^{(r+3)/2} \pmod{\ell}.$$

Similarly, when $1 \leq n \leq \alpha_r$, we find that

$$c_{r,n} + \sum_{i=0}^{n-1} c_{r,i} a_{r,i}(n) \equiv \left(\frac{r(r-24n)}{\ell}\right) (24n-r)^{(r+3)/2} p_r(n) \pmod{\ell},$$

which implies that

(4.17)
$$c_{r,n} \equiv \left(\frac{r(r-24n)}{\ell}\right) (24n-r)^{(r+3)/2} p_r(n) - \sum_{i=0}^{n-1} c_{r,i} a_{r,i}(n) \pmod{\ell}.$$

When $r \not\equiv 9 \pmod{12}$, using (2.2), we observe that $24n - r < r + 6 \leq \ell$, so $\ell \nmid r - 24n$. Alternatively, when $r \equiv 9 \pmod{12}$, using (2.2), we see that $24n - r \leq r + 6 \leq \ell$. Hence, if $\ell \mid r - 24n$, then $\ell = 24n - r$. However, 24n - r is not prime when $r \equiv 9 \pmod{12}$, so $\ell \nmid r - 24n$. Therefore, when $1 \leq n \leq \alpha_r$ we must have $\left(\frac{r(r-24n)}{\ell}\right) = \pm 1$.

We recall that the integers $A_r(0)$ and $A_r^{\pm}(n)$ are defined by

$$A_r(0) := (-r)^{(r+3)/2},$$

$$A_r^{\pm}(n) := \pm (24n - r)^{(r+3)/2} p_r(n), \quad n \ge 1.$$

Using (4.16) and (4.17), we find that there is an

$$\bar{s} \in S := \{\bar{s} = (s(1), \dots, s(\alpha_r)) \mid s(j) \in \{+, -\}, 1 \le j \le \alpha_r\}$$

for which

(4.18)
$$c_{r,0} \equiv c_{r,0}(\bar{s}) = A_r(0) \pmod{\ell}, \\c_{r,n} \equiv c_{r,n}(\bar{s}) \\= A_r^{s(n)}(n) - \sum_{i=0}^{n-1} c_{r,i}(\bar{s}) a_{r,i}(n) \pmod{\ell}, \quad 1 \le n \le \alpha_r.$$

Suppose now that $n \ge \alpha_r + 1$. By (4.15) and (4.18), we see that there is an $\bar{s} \in S$ for which

$$\left(\frac{r(r-24n)}{\ell}\right)(24n-r)^{(r+3)/2}p_r(n) - \sum_{i=0}^{\alpha_r} c_{r,i}(\bar{s})a_{r,i}(n) \equiv 0 \pmod{\ell}.$$

It follows that for every $n \ge \alpha_r + 1$, ℓ must divide one of the integers in the set

$$\left\{A_{r}^{\pm}(n) - \sum_{i=0}^{\alpha_{r}} c_{r,i}(\bar{s})a_{r,i}(n)\right\}_{\bar{s}\in S}.$$

This completes the proof of Theorem 2.1(3). \blacksquare

5. The proof of Theorem 2.3. A formal power series

$$F(q) = \sum_{n=0}^{\infty} a(n)q^n$$

is called *lacunary* if

$$\lim_{X \to \infty} \frac{\#\{n < X \mid a(n) = 0\}}{X} = 1.$$

Serre [S2, Théorème 17] proved that an integral weight modular form f(z) is lacunary if and only if it is a finite linear combination of modular forms with complex multiplication (see, for example, [Ri], for background on CM forms). In [S3], Serre classified all positive even powers of the Dedekind eta-function which are lacunary.

THEOREM 5.1 (Serre [S3, Théorème 1]). Suppose that r > 0 is an even integer. The function η^r is lacunary if and only if r is equal to 2, 4, 6, 8, 10, 14, or 26.

Moreover, in these seven cases, Serre gave an explicit decomposition of η^r as a linear combination of CM forms [S3, §2]. To see how Theorem 2.3 follows, we will prove (2) of that theorem for i = 10. We observe that Theorem 2.3(1) for i = 4 was proved in Section 4 as part of the proof of Theorem 2.1(2).

200

Following Serre $[S3, \S2.5]$, we write

$$\sum_{n=5}^{\infty} A(n)q^n = \eta^{10}(12z) = \frac{1}{96}(\phi_{K,c_+} - \phi_{K,c_-}),$$

where

$$\phi_{K,c_{\pm}} = E_4(12z)\eta^2(12z) \pm 48\eta^{10}(12z)$$
$$= \sum_{n=1}^{\infty} a_{\pm}(n)q^n \in S_5\left(\Gamma_0(2^4 \cdot 3^2), \left(\frac{-1}{\cdot}\right)\right)$$

are two CM newforms associated to certain Hecke characters c_{\pm} of the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-1})$. (For our purposes, the definition of these characters is not important.) Suppose that $\ell \geq 11$ is a fixed prime and that $\ell \equiv 3 \pmod{4}$. Suppose also that $r = \ell - 10$. Then

$$\sum_{n=5}^{\infty} A(n)q^n = \eta^{10}(12z) = q^5 \prod_{n=1}^{\infty} (1-q^{12n})^{10} = q^5 \prod_{n=1}^{\infty} \frac{(1-q^{12n})^{\ell}}{(1-q^{12n})^n}$$
$$\equiv \sum_{k=0}^{\infty} p_{-1}(k)q^{12\ell k} \cdot \sum_{j=0}^{\infty} p_r(j)q^{12j+5} \pmod{\ell}.$$

We deduce that

$$A(12\ell n + 5\ell^2) = \frac{1}{96} (a_+(12\ell n + 5\ell^2) - a_-(12\ell n + 5\ell^2))$$
$$\equiv \sum_{k=0}^{\infty} p_{-1}(k) p_r \left(\ell(n-k) + \frac{5(\ell^2 - 1)}{12}\right) \pmod{\ell},$$

and observe that $5(\ell^2 - 1)/12 \equiv -r\delta_{\ell} \pmod{\ell}$. Since the newforms $\phi_{K,c_{\pm}}$ arise from the field $K = \mathbb{Q}(\sqrt{-1})$, it must be that $a_{\pm}(\ell) = 0$ when $\ell \equiv 3 \pmod{4}$ is prime. Now we let $12\ell n + 5\ell^2 = \ell^t s$ with $t \geq 1$ and $\ell \nmid s$. The newforms $\phi_{k,c_{\pm}}$ are normalized eigenforms for the Hecke operators. By (3.6) and (3.7), it follows that when $\ell \equiv 3 \pmod{4}$, we obtain the formulae

$$a_{\pm}(\ell^{t}s) = \begin{cases} a_{\pm}(\ell)a_{\pm}(s) = 0 & \text{if } t = 1, \\ (a_{\pm}(\ell^{t-1})a_{\pm}(\ell) + \ell^{4}a_{\pm}(\ell^{t-2}))a(s) \equiv 0 \pmod{\ell} & \text{if } t > 1. \end{cases}$$

Therefore, for all $n \ge 0$, we see that

$$\sum_{k=0}^{\infty} p_{-1}(k) p_r\left(\ell(n-k) + \frac{5(\ell^2 - 1)}{12}\right) \equiv 0 \pmod{\ell}.$$

Theorem 2.3(2) with i = 10 now follows by induction on n since $p_{-1}(0) = 1$. The remaining parts of Theorem 2.3 have similar proofs, observing from [S3, §2, §3] that $\eta^6(4z)$ is a CM newform associated to the field $K = \mathbb{Q}(\sqrt{-1})$, that when r = 4, 8, or 14, η^r is a linear combination of CM newforms asso-

ciated to the field $K = \mathbb{Q}(\sqrt{-3})$, and that $\eta^{26}(12z)$ is a linear combination of CM newforms arising from the fields $K = \mathbb{Q}(\sqrt{-1})$ and $K' = \mathbb{Q}(\sqrt{-3})$.

We also mention that one may deduce Theorem 2.3 from the perspective of modular functions using the work of Newman [N2, Theorem 1].

6. Remarks on computation. Suppose that $\ell \geq 5$ is prime and that r is an odd integer with $1 \leq r \leq \ell - 1$. Suppose also that ℓ is exceptional for r, but not superexceptional for r. The exceptionality of ℓ may then be verified by Theorem 2.3. On the other hand, to verify that ℓ is superexceptional for r requires a finite computation.

There are a variety of ways to computationally verify an alleged superexceptional congruence. Suppose $f = \sum_{n=0}^{\infty} a(n)q^n \cap \mathbb{Z}[[q]]$ has $\tilde{f} \in \tilde{M}_k$. By (3.9), if $a(n) \equiv 0 \pmod{\ell}$ for all $n \leq \lfloor \frac{k}{12} \rfloor$, then $f \equiv 0 \pmod{\ell}$. Furthermore, by (4.1), ℓ is exceptional for r if and only if $\Delta^{r\delta_\ell} | U_\ell \equiv 0 \pmod{\ell}$. Applying Lemma 3.2 together with (3.1) shows that $w(\Delta^{r\delta_\ell} | U_\ell) \leq r(\ell-1)$. Hence, to verify the alleged exceptionality of ℓ for r, it suffices to check that the first $\lfloor \frac{r(\ell-1)}{12} \rfloor$ coefficients of $\Delta^{r\delta_\ell} | U_\ell$ vanish modulo ℓ .

Other computational methods may also be used. For example, using methods different than ours, Kiming and Olsson [K-O, Theorem 4] determined all r for which $\ell \leq 19$ is exceptional. We also note that, in recent work, Stanger [St, Theorem 1] used modular functions to develop a different computational criteria. He used this criteria to classify all r for which a fixed $\ell \leq 71$ is exceptional.

References

- [A-B] S. Ahlgren and M. Boylan, Arithmetic properties of the partition function, Invent. Math., to appear.
- [A-A-R] G. Andrews, R. Askey, and R. Roy, Special Functions, Cambridge Univ. Press, 1999.
- [A] A. O. L. Atkin, Ramanujan congruences for $p_{-k}(n)$, Canad. J. Math. 20 (1968), 67–78.
- [G] B. Gordon, Ramanujan congruences for $p_{-k} \pmod{11^r}$, Glasgow Math. J. 24 (1983), 107–123.
- [K-O] I. Kiming and J. Olsson, Congruences like Ramanujan's for powers of the partition function, Arch. Math. (Basel) 59 (1992), 348–360.
- [K] G. Köhler, Theta series on the theta group, Abh. Math. Sem. Univ. Hamburg 58 (1988), 15–45.
- [M] I. G. MacDonald, Affine root systems of Dedekind's η-function, Invent. Math. 15 (1972), 91–143.
- [M-O] Y. Martin and K. Ono, *Eta-quotients and elliptic curves*, Proc. Amer. Math. Soc. 125 (1997), 3169–3176.
- [N1] M. Newman, Remarks on some modular identities, Trans. Amer. Math. Soc. 73 (1952), 313–320.

- [N2] M. Newman, The coefficients of certain infinite products, Proc. Amer. Math. Soc. 4 (1953), 435–439.
- [N3] —, An identity for the coefficients of certain modular forms, J. London Math. Soc. 30 (1955), 488–493.
- [N4] —, On the existence of identities for the coefficients of certain modular forms, ibid. 31 (1956), 350–359.
- [N5] —, Some theorems about $p_r(n)$, Canad. J. Math. 9 (1957), 68–70.
- [N6] —, Congruences for the coefficients of modular forms and some new congruences for the partition function, ibid. 9 (1957), 549–552.
- [N7] —, Further identities and congruences for the coefficients of modular forms, ibid. 10 (1958), 577–586.
- [R1] S. Ramanujan, On certain arithmetical functions, Trans. Cambridge Philos. Soc. 22 (1916), 159–184.
- [R2] —, Some properties of p(n), the number of partitions of n, Proc. Cambridge Philos. Soc. 19 (1919), 207–210.
- [R3] —, Congruence properties of partitions, Proc. London Math. Soc. 18 (1920), xix.
- [R4] —, Congruence properties of partitions, Math. Z. 9 (1921), 147–153.
- [Ri] K. Ribet, Galois representations attached to eigenforms with Nebentypus, in: Lecture Notes in Math. 601, Springer, 1977, 17–51.
- [S1] J.-P. Serre, Formes modulaires et fonctions zêta p-adiques, in: Lecture Notes in Math. 350, Springer, 1973, 191–268.
- [S2] —, Quelques applications du théorème de densité de Chebotarev, Inst. Hautes Études Sci. Publ. Math. 54 (1981), 323–401.
- [S3] —, Sur la lacunarité des puissances de η , Glasgow Math. J. 27 (1985), 203–221.
- [St] A. D. Stanger, *Exceptional congruences for powers of the partition function*, Ramanujan J., to appear.
- [SwD] H. P. F. Swinnerton-Dyer, On l-adic representations and congruences for coefficients of modular forms, in: Lecture Notes in Math. 350, Springer, 1973, 1–55.

Department of Mathematics University of Illinois Urbana, IL 61801, U.S.A. E-mail: boylan@math.uiuc.edu

Received on 17.2.2003

(4466)