# PERIODICITY MODULO $m$ AND DIVISIBILITY PROPERTIES OF THE PARTITION FUNCTION[1]

BY

MORRIS NEWMAN

**Introduction.** The subject matter of this paper arose in considering the distribution of the values of the unrestricted partition function $p(n)$ modulo $m$, $m$ an integer $\geqq 2$. Here $p(n)$ is defined by

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

The Ramanujan congruences

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

show that 5, 7, 11 divide $p(n)$ for infinitely many values of $n$, and Watson [9] has shown that the same is true for all powers of 5 and 7. In addition Lehner [3; 4] has shown that $11^2$ and $11^3$ also have this property. It is natural to conjecture therefore that $p(n)$ fills *all* residue classes modulo $m$ infinitely often; that is, that if $r$ is any integer such that $0 \leqq r \leqq m-1$, then the congruence

$$p(n) \equiv r \pmod{m}$$

has infinitely many solutions in non-negative integers $n$.

This conjecture seems difficult and I have only scattered results. In §2 of this paper it will be shown that the conjecture is true for $m=5$ and 13 by means of congruences derived from the elliptic modular functions, and similar theorems will be proved; for example that $p(5n+4)/5$ and $p(7n+5)/7$ fill all residue classes modulo 5 and 7 respectively, infinitely often. In §1 it will be shown in an elementary way that the conjecture is also true for $m=2$. Thus $p(n)$ is odd infinitely often and even infinitely often. In §1 we will also consider the question of the periodicity of a sequence modulo $m$ in some generality.

Received by the editors March 25, 1960.

(1) Some of the material of this paper was presented at the Number Theory Conference of the American Mathematical Society held in the summer of 1959 at the University of Colorado with the support of the National Science Foundation.

1. We first state and prove a theorem which leads immediately to a proof of the fact that $p(n)$ is odd infinitely often and even infinitely often.

THEOREM 1. *Let*

$$f(x) = \sum_{n=0}^{\infty} c_n x^{e_n}, \qquad 0 \leqq e_0 < e_1 < e_2 < \cdots,$$

*be a power series with integral coefficients and exponents such that*

$$e_{n+1} - e_n \to \infty \text{ as } n \to \infty, \tag{1}$$

$$(c_n, c_{n+1}, \cdots) = 1, \qquad n \geqq 0. \tag{2}$$

*Then there do not exist polynomials* $\alpha(x)$, $\beta(x)$ *with integral coefficients,* $\alpha(0) = 1$, *such that*

$$f(x) \equiv \beta(x)/\alpha(x) \pmod{m}. \tag{3}$$

In congruence (3) it is understood that the coefficients of corresponding powers of $x$ are congruent.

**Proof.** We note that if

$$\sum_{n=0}^{\infty} a_n x^n \sum_{n=0}^{\infty} c_n x^{e_n} = \sum_{n=0}^{\infty} b_n x^n$$

then

$$\sum_{e_k \leq n} c_k a_{n-e_k} = b_n, \qquad n \geqq 0.$$

Put

$$\alpha(x) = \sum_{n=0}^{r} a_n x^n, \qquad a_0 = 1,$$

$$\beta(x) = \sum_{n=0}^{s} b_n x^n.$$

Then

$$\alpha(x) f(x) \equiv \beta(x) \pmod{m}$$

implies that

$$\sum_{e_k \leq n} c_k a_{n-e_k} \equiv b_n \pmod{m};$$

and replacing $n$ by $e_n$,

$$\sum_{k=1}^{n} c_k a_{e_n - e_k} = c_n + \sum_{k=0}^{n-1} c_k a_{e_n - e_k} \equiv b_{e_n} \pmod{m}. \tag{4}$$

By (1) we can choose $n_0$ so large that for all $n \geqq n_0$, $e_n - e_{n-1} > r$, $e_n > s$. Then (4) implies that for all $n \geqq n_0$,

$$c_n \equiv 0 \pmod{m}.$$

But this contradicts (2), since $m > 1$. The theorem is thus proved.

Theorem 1 now implies

THEOREM 2. *The sequence $\{p(n)\}$ is never ultimately periodic modulo $m$ and consequently $p(n)$ fills at least two different residue classes modulo $m$ infinitely often. Thus $p(n)$ is odd infinitely often and even infinitely often.*

**Proof.** The Euler product

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

satisfies the requirements (1), (2). Thus $\phi(x)$ (and so $1/\phi(x)$) is never congruent modulo $m$ to a quotient $\beta(x)/\alpha(x)$. But it is easy to show that a sequence of integers $\{t_n\}$ is ultimately periodic modulo $m$ if and only if $\sum t_n x^n$ is congruent modulo $m$ to a quotient $\beta(x)/\alpha(x)$. (This is proved below.) Theorem 2 is therefore proved.

We now look at these questions somewhat more generally. Let $R_m$ be the totality of formal power series in $x$ which are congruent modulo $m$ to a quotient of polynomials with integral coefficients, the denominator having constant term 1; and let $S_m \subset R_m$ be defined by the additional requirement that the numerator have constant term 1 also. Then $R_m$ is closed with respect to addition, multiplication and differentiation, and $S_m$ is closed with respect to multiplication and division. Further, we have the theorem

THEOREM 3. *The sequence of integers $T = \{t_n\}$, $n \geqq 0$ is ultimately periodic modulo $m$ if and only if the formal power series*

$$f(x) = \sum_{n=0}^{\infty} t_n x^n$$

*is in $R_m$.*

**Proof.** If $T$ is ultimately periodic modulo $m$, then integral polynomials $\alpha(x)$, $\beta(x)$ and a positive integer $q$ exist such that

$$f(x) \equiv \alpha(x) + \beta(x) + x^q\beta(x) + x^{2q}\beta(x) + \cdots \pmod{m}$$

Hence

$$f(x) \equiv \frac{\alpha(x)(1 - x^q) + \beta(x)}{1 - x^q} \equiv \frac{\gamma(x)}{1 - x^q} \pmod{m},$$

where $\gamma(x)$ is an integral polynomial. Thus $f(x)$ is in $R_m$.

If $f(x)$ is in $R_m$, then integral polynomials $\alpha(x)$, $\beta(x)$ exist, $\alpha(0)=1$, such that

$$f(x) \equiv \beta(x)/\alpha(x) \pmod{m}.$$

This implies that fixed integers $a_1, a_2, \cdots, a_r$ exist such that for all $n \geqq n_0$,

$$t_n \equiv a_1 t_{n-1} + a_2 t_{n-2} + \cdots + a_r t_{n-r} \pmod{m}. \tag{5}$$

Now the total number of vectors

$$(t_{n-1}, t_{n-2}, \cdots, t_{n-r}) = \tau_n$$

is finite modulo $m$ ($m^r$ is an upper bound) and so there are integers $n_2 > n_1 \geqq n_0$ such that

$$\tau_{n_2} \equiv \tau_{n_1} \pmod{m}.$$

But then (5) implies that for all $k \geqq -r$,

$$t_{n_2+k} \equiv t_{n_1+k} \pmod{m},$$

and so $T$ is ultimately periodic modulo $m$, completing the proof of the theorem.

An easy deduction from the closure properties of the sets $R_m$, $S_m$ is

LEMMA 1. *If $r$ is a rational number in lowest terms whose numerator is prime to $m$ and $f(x)^r$ is in $S_m$, then $f'(x)/f(x)$ is in $R_m$.*

Using this lemma, we can prove

LEMMA 2. *Suppose that $T=\{t_n\}$, $Q=\{q_n\}$ are two sequences of integers defined for $n \geqq 0$ such that $t_0=0$, $q_0=1$ and*

$$nq_n = \sum_{k=1}^{n} t_k q_{n-k}, \qquad n \geqq 1. \tag{6}$$

*Then if $T$ is not ultimately periodic modulo $m$ neither is $Q$.*

**Proof.** Set $t(x)=\sum_{n=1}^{\infty} t_n x^n$, $q(x)=\sum_{n=0}^{\infty} q_n x^n$. Then (6) implies that

$$xq'(x)/q(x) = t(x).$$

Suppose $Q$ is ultimately periodic modulo $m$. Then $q(x)$ is in $R_m$ (Theorem 3) and since $q_0=1$, $q(x)$ is also in $S_m$. Thus $q'(x)/q(x)$ is in $R_m$ (Lemma 1), and therefore so is $t(x)$. Thus $T$ is also ultimately periodic modulo $m$ (Theorem 3) and the lemma is proved.

If $n$ is a positive integer, let $\sigma(n)$ denote the sum of the divisors of $n$, and define $\sigma(n)$ as 0 otherwise. Then we have

LEMMA 3. *Let $r_1, e_1, r_2, e_2, \cdots, r_s, e_s$ be integers such that $0 < e_1 < e_2 < \cdots < e_s$. Set*

$$t_n = -\sum_{k=1}^{s} r_k e_k \sigma(n/e_k), \qquad n \geqq 1. \tag{7}$$

*Let $p$ be a prime such that $(r_1e_1, p) = 1$. Then the sequence $T = \{t_n\}$ is not ultimately periodic modulo $p$.*

**Proof.** Suppose the contrary. Then there is a positive integer $d$ such that for all $n \geqq n_0$ the numbers

$$t_{e_1(nd+1)}$$

are all in the same residue class modulo $p$. Choose $n_1 \geqq n_0$ so that $q = n_1 d + 1$ is prime and larger than $p$ and $e_s$ (Dirichlet's theorem). Since

$$q^2 = (n_1^2 d + 2n_1)d + 1 > n_1 d + 1$$

we have that $t_{e_1 q} \equiv t_{e_1 q^2} \pmod{p}$. Then (7) implies that

$$-r_1 e_1 \sigma(q) \equiv - r_1 e_1 \sigma(q^2) \pmod{p}$$

and since $(r_1e_1, p) = 1$ and $q$ is prime this implies that $q^2 \equiv 0 \pmod{p}$, a contradiction since $q \not\equiv p$. The lemma is therefore proved.

If we notice that with the values of $t_n$ as given in (7) the associated function $q(x)$ of Lemma 2 becomes

$$\phi(x^{e_1})^{r_1}\phi(x^{e_2})^{r_2} \cdots \phi(x^{e_s})^{r_s}, \tag{8}$$

where $\phi(x) = \prod_{n=1}^{\infty} (1 - x^n)$ is the Euler product, then we find from Lemmas 2 and 3

LEMMA 4. *Suppose that $m$ is divisible by a prime not dividing $r_1e_1$. Then the coefficients of the function* (8) *are not ultimately periodic modulo $m$.*

We remark that the restriction that $m$ be divisible by a prime not dividing $r_1e_1$ is sometimes necessary, since for example if $p$ is a prime

$$\phi(x)^p \phi(x^p)^{-1} \equiv 1 \pmod{p}.$$

Many of the functions common in analytic number theory are of the type (8). $\phi(x)^{-1}$ enumerates $p(n)$ and has already been discussed. Some others are

$\phi(x)^{-1}\phi(x^2)$, which enumerates $q(n)$, the number of partitions of $n$ into distinct parts (or into odd parts);

$\phi(x)^{-1}\phi(x^2)^2\phi(x^4)^{-1}$, which enumerates $q_0(n)$, the number of partitions of $n$ into distinct odd parts;

$\phi(x)^{-2s}\phi(x^2)^{5s}\phi(x^4)^{-2s}$, which enumerates $r_s(n)$, the number of representations of $n$ as the sum of $s$ squares.

Then Lemma 4 implies

THEOREM 4. *The sequences $\{q(n)\}$, $\{q_0(n)\}$ are not ultimately periodic* *modulo m. If m contains a prime factor not dividing* $2s$, *the sequence* $\{r_s(n)\}$ *is not ultimately periodic modulo m.*

We can draw a similar conclusion for the function $p_r(n)$ defined by

$$\sum_{n=0}^{\infty} p_r(n)x^n = \phi(x)^r = \prod_{n=1}^{\infty} (1 - x^n)^r;$$

but in this case a somewhat stronger result holds. We first prove the following strengthened version of Lemma 1:

LEMMA 5. *Let* $r \neq 0$ *be an integer and suppose that* $f(x)^r \in S_m$. *Then if* $p$ *is any prime dividing* $m$, $f'(x)/f(x) \in R_p$.

**Proof.** If $(p, r) = 1$ the conclusion is evident from Lemma 1. Suppose $p \mid r$, and put $r = pr_0$. Let $\alpha(x)$ be the polynomial of least degree with integral coefficients and constant term 1 such that

$$f(x)^r \equiv \beta(x)/\alpha(x) \pmod{p}$$

where $\beta(x)$ is also a polynomial with integral coefficients and constant term 1. Then

$$\alpha(x)f(x)^r \equiv \beta(x) \pmod{p}$$

and differentiating both sides,

$$\alpha'(x)f(x)^r \equiv \beta'(x) \pmod{p}$$

since $p \mid r$. But this implies that

$$\alpha'(x) \equiv 0 \pmod{p} \tag{9}$$

(since $\alpha(x)$ was of least degree) and so also

$$\beta'(x) \equiv 0 \pmod{p}. \tag{10}$$

But (9) and (10) now imply that

$$\alpha(x) \equiv \alpha_0(x^p) \pmod{p},$$
$$\beta(x) \equiv \beta_0(x^p) \pmod{p},$$

where $\alpha_0(u)$, $\beta_0(u)$ are again integral polynomials with constant terms 1. Since

$$f(x)^r = f(x)^{pr_0} \equiv f(x^p)^{r_0} \pmod{p},$$

it follows that

$$f(x)^{r_0} \equiv \beta_0(x)/\alpha_0(x) \pmod{p}$$

and the argument can be repeated until an exponent $r_1$ is reached such that $f(x)^{r_1} \in S_p$ and $(r_1, p) = 1$. The conclusion then follows from Lemma 1.

We now obtain from Lemma 5

THEOREM 5. *The sequence* $\{p_r(n)\}$, *where r is a nonzero integer, is not ultimately periodic modulo m.*

2. In this section we leave the elementary(²) and make use of some deep identities and congruences from the theory of the elliptic modular functions. We first prove the following lemma which will be needed later:

LEMMA 6. *Let p be a prime not dividing the positive integer c. Let e be the exponent of c modulo p. Then if a is not divisible by p the solutions of*

$$xc^x \equiv a \pmod{p} \tag{11}$$

*fall into e classes modulo p which are given by*

$$x = (ey + r)p - ac^{e-r}(p - 1), \qquad 0 \leqq r \leqq e - 1. \tag{12}$$

*If* $p|a$ *then* (11) *has just one class of solutions modulo p given by*

$$x = yp.$$

*In either case* (11) *is satisfied by infinitely many positive integers x.*

**Proof.** We can assume that $(a, p) = 1$, the latter part of the lemma being trivial. Set $x = et + r$, $0 \leqq r \leqq e - 1$. Then (11) becomes

$$(et + r)c^r \equiv a \pmod{p}$$

so that

$$t \equiv \frac{p-1}{e}(r - ac^{e-r}) \pmod{p}.$$

Thus $t = yp + ((p-1)/e)(r - ac^{e-r})$ and so $x$ is of the form given in (12).

Two solutions with different $r$'s are in different classes modulo $p$, since for

$$x_1 = (ey_1 + r_1)p - ac^{e-r_1}(p - 1),$$

$$x_2 = (ey_2 + r_2)p - ac^{e-r_2}(p - 1),$$

we have $x_1 \equiv ac^{e-r_1} \pmod{p}$, $x_2 \equiv ac^{e-r_2} \pmod{p}$, so that $x_1 \equiv x_2 \pmod{p}$ if and only if $c^{r_1 - r_2} \equiv 1 \pmod{p}$, which implies that $r_1 = r_2$.

We now collect together some congruences for easy reference.

LEMMA 7. *The following congruences are valid*:

$$p(5n + 1) \equiv p_{23}(5n) \pmod{5} \quad (\textit{Kolberg } [2]), \tag{13}$$

(²) It might be argued that Euler's pentagonal number theorem $\prod_{n=1}^{\infty}(1 - x^n) = \sum_{n=-\infty}^{\infty}(-1)^n x^{(3n^2+n)/2}$ used in §1, Theorem 2 is not elementary, but the fact that a combinatorial proof of this result has been given by F. Franklin (see [1, pp. 83–85]) justifies its occurrence in §1. Of course it is possible that the same fate awaits some of the identities used in §2 which are presently not considered elementary.

$$(14)\qquad p(5n+2) \equiv p_{23}(5n+1) \pmod 5 \ (\textit{Kolberg } [2]),$$

$$(15)\qquad \frac{1}{5}\, p(5n+4) \equiv p_{19}(n) \pmod 5 \ (\textit{Ramanujan } [1, \text{pp. } 89\text{–}90]),$$

$$(16)\qquad \frac{1}{25}\, p(25n+24) \equiv 3p_{23}(n) \pmod 5 \ (\textit{Zuckerman } [10]),$$

$$(17)\qquad \frac{1}{7}\, p(7n+5) \equiv p_{17}(n) \pmod 7 \ (\textit{Ramanujan } [1, \text{pp. } 89\text{–}90]),$$

$$(18)\qquad \frac{1}{49}\, p(49n+47) \equiv 5p_{23}(n) \pmod 7 \ (\textit{Zuckerman } [10]),$$

$$(19)\qquad p\left(84n^2 - \frac{1}{24}(n^2-1)\right) \equiv 0 \pmod{13},\ (n, 6) = 1 \ (\textit{Newman } [6]),$$

$$(20)\qquad p((24t+11)\Delta_n + 13t + 6) \equiv 6^n p(13t+6) \pmod{13},$$

$$\Delta_n = \frac{13}{24}(13^{2n} - 1) \ (\textit{Newman } [8]),$$

$$(21)\qquad c(13n) \equiv -\, p_{24}(n-1) \equiv -\, \tau(n) \pmod{13},$$

*where*

$$\sum_{n=-1}^{\infty} c(n)x^n = j(\tau) = 12^3 J(\tau), \qquad x = \exp 2\pi i\tau,$$

*$J(\tau)$ the complete modular invariant* (*Newman* [1]).

The author has shown in [5] that if $r$ is even, $0 \leqq r \leqq 24$, and $p$ is a prime such that $\delta = r(p-1)/24 \equiv 0 \pmod 1$ then for all integral $n$

$$(22)\qquad p_r(np+\delta) = p_r(n)p_r(\delta) - p^{(r/2)-1}p_r\left(\frac{n-\delta}{p}\right).$$

Set $a_n = r(p^n - 1)/24$, $p_r(a_n) = t_n$. Then $t_0 = 1$, $t_1 = p_r(\delta)$, and replacing $n$ by $a_n$ in (22),

$$(23)\qquad t_{n+1} = p_r(\delta)t_n - p^{(r/2)-1}t_{n-1}, \qquad n \geqq 1.$$

Define

$$\Delta = p_r(\delta)^2 - 4p^{(r/2)-1}.$$

Then it is easy to prove from (23) that

$$(24)\qquad t_n = 2^{-n} \sum_{0 \leq k \leq n/2} \binom{n+1}{2k+1} p_r(\delta)^{n-2k}\Delta^k.$$

Thus if $q$ is any odd prime divisor of $\Delta$,

$$t_n \equiv (n+1)\left(\frac{p_r(\delta)}{2}\right)^n \pmod{q}. \tag{25}$$

Lemma 6 and (25) together now imply

THEOREM 6. *Suppose that $r$ is even, $0 \leqq r \leqq 24$, and $p$ is a prime such that $\delta = r(p-1)/24$ is an integer. Let $q$ be any odd prime divisor of $\Delta = p_r(\delta)^2 - 4p^{(r/2)-1}$ which is different from $p$. Then the sequence $\{p_r(n)\}$ fills all residue classes modulo $q$ infinitely often.*

An interesting application arises by choosing $r = 24$, $p = 79$ or $163$. These primes are the only ones $<200$ such that

$$\tau(p)^2 = p_{24}(p-1)^2 \equiv 4p^{11} \pmod{13}.$$

Then Theorem 6 and (21) imply

THEOREM 7. *The sequence $\{c(13n)\}$ fills all residue classes modulo 13 infinitely often.*

The author has shown in [6] that if $r$ is odd, $1 \leqq r \leqq 23$, and $p$ is a prime such that $r\nu = r(p^2-1)/24 \equiv 0 \pmod 1$ then for all integral $n$,

$$p_r(np^2 + r\nu) - \gamma_n p_r(n) + p^{r-2} p_r\left(\frac{n - r\nu}{p^2}\right) = 0, \tag{26}$$

where

$$\gamma_n = c - \left(\frac{r\nu - n}{p}\right) p^{(r-3)/2} a, \qquad c = p_r(r\nu) + \left(\frac{r\nu}{p}\right) p^{(r-3)/2} a.$$

Here $((r\nu - n)/p)$ is the Legendre-Jacobi symbol of quadratic reciprocity and

$$a = (-1)^{(p-1)(p-1-2r)/8}.$$

Let $a_0$ be arbitrary, and set

$$a_n = p^{2n} a_0 + r(p^{2n} - 1)/24,$$
$$t_n = p_r(a_n).$$

Then $a_n$ satisfies

$$a_{n+1} = p^2 a_n + r\nu$$

and replacing $n$ by $a_n$ in (26) we find that $t_0 = p_r(a_0)$, $t_1 = p_r(p^2 a_0 + r\nu)$,

$$t_{n+1} - c t_n + p^{r-2} t_{n-1} = 0, \qquad n \geqq 1. \tag{27}$$

We are going to apply Lemma 7 to the recurrence (27). The general procedure is to find values of $r$ and $p$ which make the desired divisibility properties of the sequences under consideration evident. This entails much numerical work and involves a knowledge of the coefficients $p_r(n)$, some of which are tabulated in [6].

We notice first that congruences (19) and (20) settle the conjecture mentioned in the introduction for $m=13$. Thus (19) shows that the zero class occurs infinitely often; and if we notice in (20) that 6 is a primitive root of 13 and $t$ may be chosen so that $(p(13t+6), 13)=1$ then also all other classes must occur infinitely often. Thus

THEOREM 8. *The sequence* $\{p(n)\}$ *fills all residue classes modulo* 13 *infinitely often.*

We now consider congruences (13) and (14). For this purpose we choose $r=23$, and $p\equiv \pm 1 \pmod 5$. Then $a_n \equiv a_0 \pmod 5$ and we will choose $a_0$ so that either $a_0\equiv 0 \pmod 5$ or $a_0 \equiv 1 \pmod 5$. Then (13) and (14) imply that

$$p(1 + a_n) \equiv t_n \pmod 5.$$

Since $p^2\equiv 1 \pmod 5$ (27) implies that

$$p(1 + a_{n+1}) - cp(1 + a_n) + p\cdot p(1 + a_{n-1}) \equiv 0 \pmod 5, \qquad n \geqq 1. \tag{28}$$

Here $c$ satisfies

$$c \equiv p_{23}(23\nu) + \left(\frac{-69}{p}\right) \pmod 5.$$

We make the choice $p=11$. Then from the tables given in [6] we find that $c\equiv 2 \pmod 5$, and (28) becomes

$$p(1 + a_{n+1}) - 2p(1 + a_n) + p(1 + a_{n-1}) = 0 \pmod 5$$

which implies that

$$p(1 + a_n) \equiv (t_1 - t_0)n + t_0 \pmod 5. \tag{29}$$

Everything depends on the initial values $t_0$, $t_1$. We have for $r=23$, $p=11$ from (26) that

$$\begin{gathered} p_{23}(121a_0 + 115) - \gamma_{a_0}p_{23}(a_0) + 11^{21}p_{23}\left(\frac{a_0 - 115}{121}\right) = 0, \\ \gamma_{a_0} = c - \left(\frac{115 - a_0}{11}\right)11^{10}. \end{gathered} \tag{30}$$

Choose $a_0$ so that

$$a_0 \not\equiv 115 \pmod{121}.$$

Then (30) implies that

$$t_1 - t_0 \equiv \left(1 + \left(\frac{5 - a_0}{11}\right)\right)t_0 \pmod 5.$$

Since we do not want $t_1 - t_0 \equiv 0 \pmod 5$, we choose $a_0$ so that

$$\left(\frac{5 - a_0}{11}\right) \not\equiv -1.$$

Then

$$a_0 \equiv 0, 1, 2, 4, 5, 7 \pmod{11}.$$

Thus $a_0$ must satisfy

$$\begin{aligned} &a_0 \equiv 0, 1 \pmod 5, \\ &a_0 \equiv 0, 1, 2, 4, 5, 7 \pmod{11}, \\ &a_0 \not\equiv 115 \pmod{121}. \end{aligned} \tag{31}$$

After $a_0$ is chosen to satisfy (31), we must still verify that $t_0 \not\equiv 0 \pmod 5$. The first few $a_0$'s satisfying (31) and the associated $t_0$'s and $t_1 - t_0$'s follow:

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | $a_0$ | 0 | 1 | 5 | 11 | 15 | 16 | 26 | 35 | 40 | 45 | 46 | 51 | 55 | 56 | 60 |
| (32) | $t_0 \pmod 5$ | 1 | 2 | 1 | 2 | 1 | 2 | 0 | 2 | 3 | 3 | 4 | 4 | 3 | 4 | 0 |
| | $t_1 - t_0 \pmod 5$ | 2 | 4 | 1 | 4 | 2 | 2 | 0 | 4 | 1 | 1 | 3 | 3 | 1 | 3 | 0 |

Summarizing, we have proved

THEOREM 9. *Let* $a_n = 121^n a_0 + (23/24)(121^n - 1)$. *Then for all* $n \geqq 0$,

$$p(1 + a_n) \equiv \begin{cases} 2n + 1 \pmod 5, & a_0 = 0, 15, \cdots \\ 4n + 2 \pmod 5, & a_0 = 1, 11, 35, \cdots \\ n + 1 \pmod 5, & a_0 = 5, \cdots \\ 2n + 2 \pmod 5, & a_0 = 16, \cdots \\ n + 3 \pmod 5, & a_0 = 40, 45, 55, \cdots \\ 3n + 4 \pmod 5, & a_0 = 46, 51, 56, \cdots \end{cases} \tag{33}$$

*Thus the sequence* $\{p(n)\}$ *fills all residue classes modulo* 5 *infinitely often.*

We make the remark that the choice $p = 11$ was one of expediency only. Other primes would do as well.

Since $p(125n+24)/25 \equiv 3p(5n+1) \pmod 5$ (by (13) and (16)) Theorem 9 implies

THEOREM 10. *The sequence* $\{p(125n+24)/25\}$ *fills all residue classes modulo* 5 *infinitely often.*

Precisely the same procedure can be applied to the remaining congruences of Lemma 7. Some typical results are

$$\frac{1}{5}\, p\left(\frac{95 \cdot 13^{2n} + 1}{24}\right) \equiv 2^n \pmod 5, \tag{34}$$

$$\frac{1}{7}\, p\left(\frac{119\cdot 11^{2n}+1}{24}\right) \equiv (-1)^n(4n+1) \pmod 7, \tag{35}$$

$$\frac{1}{49}\, p\left(\frac{1127\cdot 11^{2n}+1}{24}\right) \equiv (-1)^{n-1}(n+2) \pmod 7. \tag{36}$$

Since $p(5n+4)/5$ certainly fills the zero class modulo 5 infinitely often, and 2 is a primitive root of 5, we can conclude with the aid of Lemma 6.

THEOREM 11. *The sequences* $\{p(5n+4)/5\}$, $\{p(7n+5)/7\}$, $\{p(49n+47)/49\}$ *fill all residue classes infinitely often modulo* 5, 7, 7 *respectively.*

We mention in conclusion that similar results modulo 10, 26, 65 may be derived.

## REFERENCES


1. G. H. Hardy, *Ramanujan*, Cambridge University Press, 1940.
2. O. Kolberg, *Some identities involving the partition function*, Math. Scand. vol. 5 (1957) pp. 77–92.
3. J. Lehner, *Ramanujan identities involving the partition function for the moduli* $11^\alpha$, Amer. J. Math. vol. 65 (1943) pp. 492–520.
4. ———, *Proof of Ramanujan's partition congruence for the modulus* $11^3$, Proc. Amer. Math. Soc. vol. 1 (1950) pp. 172–181.
5. M. Newman, *Remarks on some modular identities*, Trans. Amer. Math. Soc. vol. 73 (1952) pp. 313–320.
6. ———, *Further identities and congruences for the coefficients of modular forms*, Canad. J. Math. vol. 10 (1958) pp. 577–586.
7. ———, *Congruences for the coefficients of modular forms and for the coefficients of* $j(\tau)$, Proc. Amer. Math. Soc. vol. 9 (1958) pp. 609–612.
8. ———, *Congruences for the coefficients of modular forms and some new congruences for the partition function*, Canad. J. Math. vol. 9 (1957) pp. 549–552.
9. G. N. Watson, *Ramanujan's Vermutung über Zerfällungsanzahlen*, J. Reine Angew. Math. vol. 179 (1938) pp. 97–128.
10. H. Zuckerman, *Identities analogous to Ramanujan's identities involving the partition function*, Duke Math. J. vol. 5 (1939) pp. 88–110.



NATIONAL BUREAU OF STANDARDS,
WASHINGTON, D. C.