CONGRUENCES FOR THE FOURIER COEFFICIENTS OF THE MODULAR INVARIANT $j(\tau)$

by D. B. LAHIRI, F.N.I., *Indian Statistical Institute, Calcutta*

(*Received April 14; after revision July 28, 1965*)

This paper deals with some new arithmetical properties of the Fourier coefficients $c(n)$ of the modular invariant $j(\tau)$. It establishes simple congruence relationships between $c(p^\lambda n)$ and $\sigma_k(n)$, with certain powers of p (= 2, 3, 5, 7) as moduli. It shows that if $n \equiv 0 \pmod{2^a\ 3^b\ 5^c\ 7^d}$ then $c(n) \equiv 0 \pmod{3^{3a+12}\ 3^{2b+5}\ 5^{c+2}\ 7^{d+1}}$ for almost all such values of n. Explicit expressions have been obtained for the least residues of $c(p^\lambda)$ to moduli which are some suitable powers of p. More general results are also given.

1. INTRODUCTION

The object of this paper is to develop in a connected manner some arithmetical properties of the integral coefficients $c(n)$ of the Fourier expansion of Klein's classical modular invariant,

$$j(\tau) = 1728\,J(\tau) = c(-\tau) + \sum_{n=0}^{\infty} c(n)e(n\tau),\ e(\tau) = \exp 2\pi i\tau.$$

Such properties have been studied previously by Lehmer (1942), Lehner (1949*a*, *b*), van Wijnggarden (1953), Newman (1958, 1960), and Kolberg (1961, 1962). The new results, Lahiri (1965), proved in this paper and their position in relation to some of the previously established properties are set forth in Section 3.

2. SOME SYMBOLS

The symbols λ and n stand for arbitrary positive integers unless otherwise specified; p represents any one of the primes 2, 3, 5 or 7. Occasionally p stands for the prime 13 also, and the text will explicitly state this whenever necessary. The symbols r_p, s_p, f_p, g_p, ρ_p, β_p, ν_p and $\mu_p(\lambda)$, or, simply r, s, f, g, ρ, β, ν and μ or $\mu(\lambda)$, are defined below. It will be noticed that $(p-1)r = 24$ and $\nu = \rho + r/2 - 1 = \mu(1)$.

p	r_p	s_p	f_p	g_p	ρ_p	β_p	ν_p	$\mu_p(\lambda)$
2	24	1	3	3	4	5	15	$3\lambda+12$
3	12	1	2	1	2	2	7	$2\lambda+5$
5	6	1	1	3	1	1	3	$\lambda+2$
7	4	3	1	5	1	1	2	$\lambda+1$
13	2	—	—	—	1	—	1	—

The symbol $d_q(\lambda)$ denotes a periodic function of λ of period M_q;
for $q = 2^5$, $d_q(\lambda) = 11, 1, 3, 9, 27, 17, 19, 25$ when $\lambda \equiv 0, 1, 2, \ldots . 7 \pmod 8$,
for $q = 2^4$, $d_q(\lambda) = 11, 1, 3, 9$ when $\lambda \equiv 0, 1, 2, 3 \pmod 4$,
for $q = 3^2$, $d_q(\lambda) = 1$ whatever be the value of λ,
for $q = 5$, $d_q(\lambda) = 2, 1, 3, 4$, when $\lambda \equiv 0, 1, 2, 3 \pmod 4$,
for $q = 7$, $d_q(\lambda) = 3, 1, 5, 4, 6, 2$ when $\lambda \equiv 0, 1, 2, \ldots . 5 \pmod 6$.
In fact $d_q(\lambda)$ is the least positive residue of $g^{\lambda-1}$ to modulus q, and $M_q = 8, 4, 1, 4, 6$ for $q = p^\alpha = 2^5, 2^4, 3^2, 5, 7$ respectively, is the order of $g \pmod q$, $g = g_p$.

3. The Results

Newman (1958) proved that $c(13n) \equiv -\tau(n) \pmod{13}$, where $\tau(n)$ is Ramanujan's function, defined by

$$x\left\{\prod_{m=1}^{\infty}(1-x^m)\right\}^{24} = \sum_{n=1}^{\infty}\tau(n)x^n.$$

We shall re-establish Newman's result by a different method; and establish similar congruences given below for other primes, p, *viz.* 2, 3, 5, 7.

Theorem 1. If p stands for any of the primes 2, 3, 5, 7, 13, then

$$c(pn) \equiv -p^{\nu/2-1}\tau(n) \pmod{p^\nu}.$$

A generalization for all the above primes excepting 13 follows.

Theorem 2.

$$c(p^\lambda n) \equiv c(p^\lambda)\tau(n) \pmod{p^\mu}.$$

The next theorem helps the replacement of the $c(p^\lambda)$ in Theorem 2 by suitable multiples of certain powers of the primes.

Theorem 3. The numerically least negative residue of $c(p^\lambda)$ to the modulus $p^{\mu-\rho+\beta}$ is $-d_q(\lambda)p^{\mu-\rho}$, where $q = p^\beta$.

It is easy to deduce from this theorem the undernoted result.

Corollary 1. The highest power of p dividing $c(p^\lambda)$ is $p^{\mu-\rho}$.

Lehner (1964) showed, as is also evident from the next theorem, that

$$c(p^\lambda n) \equiv 0 \pmod{p^{\mu-\rho}}. \tag{1}$$

Thus $c(p^\lambda)$ is divisible by $p^{\mu-\rho}$ which, as proved by Kolberg, is the highest power dividing $c(p^\lambda)$ for $p = 2, 3$. Corollary 1 shows this to be true for $p = 5, 7$ also.

Congruence relations between $c(p^\lambda n)$ and $\sigma_s(n)$, the sum of the s-th powers of the divisors of n, are given below.

Theorem 4.

$$c(p^\lambda n) \equiv -d_q(\lambda)p^{\mu-\rho}n^s\sigma_s(n) \pmod{p^\mu}, \quad q = p^\rho.$$

Calculation of residues of $c(p^\lambda n)$ to the modulus p^μ is simplified by the use of the above theorem as $\sigma_s(n)$ is more amenable to residue determination. Kolberg obtained the residues of $c(2^\lambda n)$ and $c(3^\lambda n)$ for the moduli $2^{3\lambda+13}$ and $3^{2\lambda+6}$ respectively; his results are therefore stronger, for the primes 2 and 3, than those obtainable from Theorem 4, where the corresponding moduli are of lower powers being $2^{3\lambda+12}$ and $3^{2\lambda+5}$.

It is possible to specify the n's for which p^δ is the highest power dividing $c(p^\lambda n)$, provided $\mu-\rho \leqslant \delta < \mu$. The case $\delta = \mu-\rho$, which gives a generalization of Kolberg type of divisibility property like Corollary 1, follows.

COROLLARY 2. The highest power of the prime p dividing $c(p^\lambda n)$ would be $p^{\mu-\rho}$, if and only if $\alpha_0 = 0, \alpha_1 \not\equiv -1 \pmod p$, $\alpha_{p-1} \not\equiv 1 \pmod 2$ for $p = 2, 3$; and the additional conditions for $p = 5$ are $\alpha_2, \alpha_3 \not\equiv 3 \pmod 5$, and for $p = 7$, $\alpha_2, \alpha_4 \not\equiv -1 \pmod 7$ and $\alpha_3, \alpha_5 \not\equiv 1 \pmod 2$, where p_i stands for any prime falling in the residue class $i \pmod p$, and α_i's are the exponents of such primes in the standard form of n.

The sets of n's for which $c(p^\lambda n)$ has p^δ as a divisor require similar elaborate specifications when $\mu-\rho < \delta \leqslant \mu$. We concentrate on their more interesting subsets, simply specifiable as arithmetic progressions.

THEOREM 5. The only p primes for which there exist at least one positive integer λ and another positive integer $k < p$ such that

$$c(p^\lambda(pn+k)) \equiv 0 \pmod{p^{\mu-\rho+1}},$$

for every non-negative value of n, are 3 and 7. In these cases every positive integer is an admissible value of λ, and the admissible values of k are independent of λ, being always the quadratic non-residues of p.

Relaxation of the form of the argument to $p^\lambda(p^\epsilon n+k)$ enables inclusion of the case $p = 2$ also, the moduli being even higher than $p^{\mu-\rho+1}$. Further relaxation to $p^\lambda(an+b)$ where a and b are no longer co-prime gives congruences to still higher modulus. Illustrations follow.

THEOREM 6.

$c(2^\lambda(2^\epsilon n-1)) \equiv 0 \pmod{2^{\mu-\rho+\epsilon}}$, $\epsilon = 2, 3$;

$c(p^\lambda(p^\epsilon u^2 n-u)) \equiv 0 \pmod{p^\mu}$ if $u \equiv -1 \pmod{p^\epsilon}$, $\epsilon = 4-\mu$, $p = 2, 3$;

$c(p^\lambda(u^2 n-ud)) \equiv 0 \pmod{p^\mu}$ if $\sigma_s(u) \equiv 0 \pmod{p^\rho}$, $(u, d) = 1$.

Non-existence of roots of $c(p^\lambda n) \equiv d \pmod{p^\mu}$ when $p^{\mu-\rho}$ is not a divisor of d is obvious from Theorem 4. It is therefore sufficient to consider the following congruence for studying the number of roots.

THEOREM 7. The congruence $c(p^\lambda n) \equiv dp^{\mu-\rho} \pmod{p^\mu}$, $0 \leqslant d < p^\rho$, has an infinity of solutions for any given λ and d. If $d = 0$, then the same set of values of n, constituting almost all positive integers, satisfies the congruence whatever λ may be. But if n is given any of the rare values for which

$c(p^\lambda n)$ is not divisible by p^μ, then for 7 non-zero values of d for $p = 3$, and 11, 13 or 14 values (depending upon n) for $p = 2$, the congruence is not satisfied even by a single value of λ; λ's exist in all other cases.

The case $\lambda = 1$ of the first part of the theorem shows that $p^{-\nu+\rho}c(pn)$ falls in all residue classes modulo p^ρ infinitely often, where p is understood to be 2, 3, 5 or 7. That this holds for $p = 13$ also is seen from Newman's (1960) result for that prime.

COROLLARY 3.

$$c(2^a3^b5^c7^dn) \equiv 0 \pmod{2^{3a+12}\,3^{2b+5}\,5^{c+2}\,7^{d+1}}$$

for almost all values of n where $a, b, c, d > 0$.

This may be compared with Lehner's result,

$$c(2^a3^b5^c7^dn) \equiv 0 \pmod{2^{3a+8}\,3^{2b+3}\,5^{c+1}\,7^d},$$

for all values of n. If a, b, c or d vanishes, then the corresponding prime powers are to be totally removed from the moduli in the two congruences for $c(n)$.

4. LEHNER'S IDENTITIES

We require some identities due to Lehner (1964). For $p = 2, 3, 5, 7, 13$ he proved that

$$\sum_{n=0}^{\infty} c(pn)e(n\tau) = C + p^{r/2-1}\sum_{h=1}^{\rho z} C_h p^{r(h-1)/2}\Phi_p(\tau)^h, \tag{2}$$

with C a constant and C_h integral (depending upon p), and where

$$\Phi_p(\tau) = (\eta(p\tau)/\eta(\tau))^r,$$

$$\eta(\tau) = e(\tau/24)\prod_{m=1}^{\infty}(1-e(m\tau)),\ Im\,\tau > 0.$$

He derives the further identities which (with some notational changes) are

$$\sum_{n=0}^{\infty} c(2^\lambda n)e(n\tau) = A + 2^{3\lambda+8}\sum_{h=1}^{v} A_h 2^{3(h-1)}\Phi_2(\tau)^h, \tag{3}$$

$$\sum_{n=0}^{\infty} c(3^\lambda n)e(n\tau) = A + 3^{2\lambda+3}\sum_{h=1}^{v} A_h 3^{4(h-1)}\Phi_3(\tau)^h, \tag{4}$$

$$\sum_{n=0}^{\infty} c(5^\lambda n)e(n\tau) = A + 5^{\lambda+1}A_1\Phi_5(\tau) + 5^{\lambda+1}\sum_{h=2}^{v} A_h 5^h\Phi_5(\tau)^h, \tag{5}$$

$$\sum_{n=0}^{\infty} c(7^\lambda n)e(n\tau) = A + 7^\lambda A_1\Phi_7(\tau) + 7^\lambda\sum_{h=2}^{v} A_h 7^h\Phi_7(\tau)^h, \tag{6}$$

where the A_h's are integers. The A_h's and v depend upon λ and also on the prime p appearing in the subscript of $\Phi_p(\tau)$.

5. A Lemma

It is easily seen that with $p = 2, 3, 5, 7, 13$

$$\Phi_p(\tau) = e(\tau)\left\{\prod_{m=1}^{\infty}(1-e(mp\tau))/\prod_{m=1}^{\infty}(1-e(m\tau))\right\}^r = x(f(x^p)/f(x))^r,$$

where $x = e(\tau)$ and $f(x) = \prod_{m=1}^{\infty}(1-x^m)$.

Now it is easy to derive by elementary means that $f(x^p) = \{f(x)\}^p + pI$, where I is a power series in x with integral coefficients; and therefore we get $f(x^p)/f(x) = \{f(x)\}^{p-1} + pI$; ($I$ possibly different in different cases). Thus

$$\Phi_p(\tau) = x(\{f(x)\}^{p-1} + pI)^r = x\{f(x)\}^{(p-1)r} + pI = x\{f(x)\}^{24} + pI.$$

But for the primes 2 and 3 we obtain the following more general relations:

$$\Phi_2(\tau) = x(f(x)+2I)^{24}$$
$$= x(\{f(x)\}^{24} + 24\,.\,2I\{f(x)\}^{23} + 12\,.\,23\,.\,2^2I\{f(x)\}^{22} + 4\,.\,23\,.\,22\,.\,2^3I\{f(x)\}^{21} + 2^4I)$$
$$= x\{f(x)\}^{24} + 2^4I.$$

$$\Phi_3(\tau) = x(\{f(x)\}^2 + 3I)^{12} = x(\{f(x)\}^{24} + 12\,.\,3I\{f(x)\}^{22} + 3^2I),$$
$$= x\{f(x)\}^{24} + 3^2I.$$

By combining the above results we arrive at the following lemma:

Lemma. $\Phi_p(\tau) = x(f(x^p)/f(x))^r = x\{f(x)\}^{24} + p^pI.$

6. Proof of Theorem 1

The identity (2) can be written as

$$\sum_{n=0}^{\infty} c(pn)x^n = C + p^{r/2-1}\sum_{h=1}^{p^2} C_h p^{r(h-1)/2} x^h (f(x^p)/f(x))^{rh}. \tag{7}$$

Clubbing together the terms corresponding to $h > 2$ as $p^{r-1}I$, we have

$$\sum_{n=0}^{\infty} c(pn)x^n = C + C_1 p^{r/2-1}\,.\,x(f(x^p)/f(x))^r + p^{r-1}I,$$
$$= C + C_1 p^{r/2-1}\,.\,(x\{f(x)\}^{24} + p^pI) + p^{r-1}I,$$
$$= C + C_1 p^{r/2-1}\,.\,x\{f(x)\}^{24} + p^\nu I,$$
$$= C + C_1 p^{r/2-1}\sum_{n=1}^{\infty}\tau(n)x^n + p^\nu I.$$

Comparing coefficients of x^n, $n > 0$, we get $c(pn) \equiv C_1 p^{r/2-1}\tau(n) \pmod{p^\nu}$; and in particular, $c(p) \equiv C_1 p^{r/2-1}\tau(1) = C_1 p^{r/2-1} \pmod{p^\nu}$. Hence $c(pn) \equiv c(p)\tau(n) \pmod{p^\nu}$, p being 2, 3, 5, 7, 13 as in identity (2).

Theorem 1 follows by considering the values of $c(p)$ given in Section 8.

7. Proof of Theorem 2

Expressing the identities (3)–(6) in terms of x, and noting that $p^{\mu+\rho}$ is a common factor of the coefficients of the terms involving $\Phi_p(\tau)^h$, with $h \geqslant 2$, we easily obtain

$$\sum_{n=0}^{\infty} c(p^\lambda n)x^n = A + p^{\mu-\rho}A_1 x(f(x^p)/f(x))^r + p^{\mu+\rho}I. \tag{8}$$

Now making use of the lemma it is a simple deduction that

$$\sum_{n=0}^{\infty} c(p^\lambda n)x^n = A + p^{\mu-\rho}A_1 x\{f(x)\}^{24} + p^\mu I. \tag{9}$$

By equating the coefficients of x^n, $n > 0$, on both sides, and using the particular case $n = 1$ for replacing A_1, as in the proof of Theorem 1, we get Theorem 2. Using the weaker form of Theorem 3 given near the end of the next section, the right-hand side may be freed from the Fourier coefficient $c(p^\lambda)$ as follows:

Theorem 2′.

$$c(p^\lambda n) \equiv -d_q(\lambda)p^{\mu-\rho}\tau(n) \pmod{p^\mu},\ q = p^\rho.$$

8. Proof of Theorem 3

Comparing the coefficients on both sides of (8) we get, for $n > 0$, $c(p^\lambda n) \equiv p^{\mu-\rho}A_1 b_p(n) \pmod{p^{\mu+\rho}}$, where

$$\Phi_p(\tau) = x(f(x^p)/f(x))^r = \sum_{n=1}^{\infty} b_p(n)x^n.$$

Using the case $n = 1$, this congruence leads to the interesting result,

$$c(p^\lambda n) \equiv c(p^\lambda)b_p(n) \pmod{p^{\mu+\rho}}. \tag{10}$$

Now this congruence with $n = p^\gamma$ gives

$$p^{\mu(\lambda+\gamma)-\mu(\lambda)}l(p^{\lambda+\gamma}) \equiv b_p(p^\gamma)l(p^\lambda) \pmod{p^{2\rho}}, \tag{11}$$

where $l(p^\lambda) = p^{-\mu(\lambda)+\rho}c(p^\lambda)$ is integral in virtue of (1).

The following expansions give the first few values of $b_p(n)$:

$$\Phi_2(\tau) = x + 24x^2 + \ldots,$$
$$\Phi_3(\tau) = x + 12x^2 + 90x^3 + \ldots,$$
$$\Phi_5(\tau) = x + 6x^2 + 27x^3 + 98x^4 + 315x^5 + \ldots,$$
$$\Phi_7(\tau) = x + 4x^2 + 14x^3 + 40x^4 + 105x^5 + 252x^6 + 574x^7 + \ldots$$

Taking $\gamma = 1$ in (11) and substituting the values of $b_p(p)$ we obtain

$$l(p^{\lambda+1}) \equiv gl(p^\lambda) \pmod{p^\beta}.$$

By a process of iteration one can derive easily the relation,

$$l(p^\lambda) \equiv g^{\lambda-1}l(p) \pmod{p^\beta}. \tag{12}$$

The values of $l(p)$ are derivable from Zuckerman's (1939) table of $c(n)$. The values of $c(p)$ including that of $c(13)$ used in Theorem 1 for re-establishing

Newman's congruence are given below.

$$c(2) = 21493760 = 2^{11}(2^8 \cdot 41 - 1) \equiv 2^{11}t(2),$$
$$c(3) = 864299970 = 3^6(3^6 \cdot 4879 - 1) \equiv 3^6 t(3),$$
$$c(5) = 33320264060\,0 = 5^2(5^4 \cdot 21324969 - 1) \equiv 5^2 t(5),$$
$$c(7) = 44656994071935 = 7(7^4 \cdot 2657047306 - 1) \equiv 7t(7),$$
$$c(13) = 4872010111798142520 = 13 \cdot 374770008599857117 - 1.$$

It is now easily seen that the $t(p)$ appearing on the right-hand side of (12) can be replaced by -1. Then it is also easily seen that $-d_q(\lambda)$, with $q = p^\beta$, is the (numerically) least negative residue of the right-hand side of (12) to the modulus p^β. Thus

$$t(p^\lambda) \equiv -d_q(\lambda) \pmod{p^\beta},\ q = p^\beta. \tag{13}$$

Now we revert to the function $c(p^\lambda)$ instead of $t(p^\lambda)$, obtaining

$$c(p^\lambda) \equiv -d_q(\lambda)p^{\mu-\rho} \pmod{p^{\mu-\rho+\beta}}. \tag{14}$$

Theorem 3 follows from the inequality $d_q(\lambda)p^{\mu-\rho} < p^{\mu-\rho+\beta}$. Corollary 1 is an obvious deduction from the theorem, or its slightly weaker version, *viz.* the numerically least negative residue of $c(p^\lambda)$ to the modulus p^μ is $-d_q(\lambda)p^{\mu-\rho}$, where $q = p^\rho$.

It might be of interest to note that with $\lambda = 1$, (11) gives

$$b_p(p^\gamma) \equiv 0 \pmod{p^{2\rho}} \tag{15}$$

if $\gamma > 2$ when $p = 2$, and if $\gamma \geqslant 2$ when $p = 3, 5, 7$. This follows from the facts that $t(p)$ is not divisible by p, and that $\mu(1+\gamma)-\mu(1) \geqslant 2\rho$ for $\gamma > 2$ when $p = 2$, and for $\gamma \geqslant 2$ when $p = 3, 5, 7$.

9. Proof of Theorem 4

Making use of the congruence, Lahiri (1947),

$$\tau(n) \equiv 5(3n^4-7n^3)\sigma_3(n)-7(2n^5-5n^4)\sigma(n) \pmod{2^4 \cdot 3^2 \cdot 5 \cdot 7}, \tag{16}$$

and remembering Lehner's divisibility property, (1), it is not difficult to establish from Theorem 2′ that, with $q = p^\rho$,

$$c(p^\lambda n) \equiv -d_q(\lambda)(5(3n^4-7n^3)\sigma_3(n)-7(2n^5-5n^4)\sigma(n))p^{\mu-\rho} \pmod{p^\mu}. \tag{17}$$

The neater form (but involving symbols f and s) given in Theorem 4 is obtained by using the Ramanujan congruences listed by Rushforth (1952). These congruences, also derivable from (16), are

$$\tau(n) \equiv n^f\sigma_s(n) \pmod{p^\rho}. \tag{18}$$

The validity of Corollary 2 and the subsequent observation is easily established by considering the divisibility properties of $\sigma_s(p_i^{\alpha_i})$.

10. Proof of Theorem 5

If for any particular value of λ, $c(p^\lambda(pn+k))$ is divisible by $p^{\mu-\rho+1}$ for every $n \geqslant 0$, then from Theorem 4 it is easily seen that $\sigma_s(pn+k)$ must be divisible by p for all such n's. But it can be easily checked that for $p = 2$

and 5 there are always some values of n for which $\sigma(pn+k)$ is not divisible by p, for every fixed positive value of $k < p$. For $p = 3$ and 7 similar illustrations are easily available when k is a quadratic residue of p. We are thus left only with the cases $p = 3$ and 7 with k a quadratic non-residue. To demonstrate that for these cases $c(p^\lambda(pn+k))$ is divisible by $p^{\mu-\rho+1}$ we require the result,

$$\sigma_l(n) \equiv 0 \pmod{p}, \quad l = \tfrac{1}{2}(p-1), \tag{19}$$

when n is a quadratic non-residue of any odd prime p; reference may be made to Ramanathan (1945) and also to Lahiri (1946). Now by Theorem 4 we have

$$c(3^\lambda(3n+2)) \equiv -3^{2\lambda+3}(3n+2)^2\sigma(3n+2) \pmod{3^{2\lambda+5}}, \; n > 0;$$

and, further, by Ramanathan's result (19), $\sigma(3n+2) \equiv 0 \pmod 3$. Thus,

$$c(3^\lambda(3n+2)) \equiv 0 \pmod{3^{2\lambda+4}}. \tag{20}$$

Similarly, by using Ramanathan's result for $p = 7$ we have

$$c(7^\lambda(7n+k)) \equiv 0 \pmod{7^{\lambda+1}}, \tag{21}$$

where k is any quadratic non-residue of 7. This congruence is also directly derivable from Theorem 2′ and Ramanujan's congruence, Hardy (1940), $\tau(7n+k) \equiv 0 \pmod 7$ for the same values of k. The result (20) for the prime 3 is also derivable from the same theorem provided it is backed by the easily established fact that $\tau(3n+2) \equiv 0 \pmod 3$.

11. Proof of Theorem 6

By considering the expression for $8n-1$ in the form $\Pi p_1^{\alpha_1}\Pi p_2^{\alpha_2}\Pi p_3^{\alpha_3}\Pi p_4^{\alpha_4}$, where p_i stands for any prime falling in the residue class $i \pmod{2^3}$, it is possible to establish from first principles that $\sigma(8n-1) \equiv 0 \pmod{2^3}$. Also, $\sigma(4n-1) \equiv 0 \pmod{2^2}$ is similarly but more simply obtainable. These results were proved by Ramanathan (1943). The first congruence of Theorem 6 is now obtained by an application of these results to the case $p = 2$ of Theorem 4.

For the second congruence we note that $\sigma(p^\epsilon u^2 n-u) = \sigma(u)\sigma(p^\epsilon un-1)$. But as $\sigma(4n-1) \equiv 0 \pmod{2^2}$ and $\sigma(3n-1) \equiv 0 \pmod 3$, the two right-hand factors are both multiples of p^ϵ, and therefore $\sigma(p^\epsilon u^2 n-u) \equiv 0 \pmod{p^{2\epsilon}}$. The required result now follows from Theorem 4. Multiplicative properties of $\sigma_s(n)$ may be similarly exploited to establish the last and other congruences.

12. Proof of Theorem 7

If $n = w^{\theta-1}$: where $w = 17, 19, 11, 29$ for $p = 2, 3, 5, 7$, then Theorem 4 gives $c(p^\lambda n) \equiv -d_q(\lambda)p^{\mu-\rho}.\theta \pmod{p^\mu}$. And as θ runs over all positive integers, $-d_q(\lambda)\theta$, for any given λ, runs over each of the residues modulo p^ρ infinitely often. Hence the first part of the theorem.

A joint consideration of Theorem 4 and Watson's (1935) theorem that $\sigma_l(n)$ is divisible by any prescribed number for 'almost all' values of n, for

any odd l shows that $c(p^\lambda n)$ is divisible by p^μ for 'almost all' values of n, *viz.* the roots of $n^l\sigma_s(n) \equiv 0 \pmod{p^\mu}$. More specifically, if $\psi(N)$ is the number of n's $< N$ for which $c(p^\lambda n)$ is divisible by p^μ, then $\psi(N)/N \to 1$ as $N \to \infty$.

If $c(p^\lambda n) \not\equiv 0 \pmod{p^\mu}$ then $n^l\sigma_s(n) \not\equiv 0 \pmod{p^\mu}$ and as $d_q(\lambda)$ has M_q values $-d_q(\lambda)n^l\sigma_s(n)$ has $< M_q$ (non-zero) values incongruent modulo q, for variations in λ. Closer scrutiny yields the exact number. And the last part follows.

Corollary 3 follows immediately from the second part of the theorem.

Acknowledgement

Compared to the original paper submitted for publication, this revised one takes up much less space. This improvement has been occasioned by the referee's useful suggestion to reduce the size of the paper.

References

Hardy, G. H. (1940). Ramanujan, Cambridge.

Kolberg, O. (1961). Congruences for the coefficients of the modular invariant $j(\tau)$ modulo powers of 2. *Acta Univ. Bergen*, No. 16, 3–9.

——— (1962). The coefficients of $j(\tau)$ modulo powers of 3. *Acta Univ. Bergen*, No. 16, 1–7.

Lahiri, D. B. (1946). On Ramanujan's function $\tau(n)$ and the divisor function $\sigma_k(n)$. Part I. *Bull. Calcutta math. Soc.*, 38, 193–206.

——— (1947). On Ramanujan's function $\tau(n)$ and the divisor function $\sigma_k(n)$, Part II. *Bull. Calcutta math. Soc.*, 39, 33–52.

——— (1965). Some arithmetical properties of the Fourier coefficients of the modular invariant $j(\tau)$. *Curr. Sci.*, 34, 208.

Lehmer, D. H. (1942). Properties of the coefficients of the modular invariant $j(\tau)$. *Am. J. Math.*, 64, 488–502.

Lehner, J. (1949a). Divisibility properties of the Fourier coefficients of the modular invariant $j(\tau)$. *Am. J. Math.*, 71, 136–148.

——— (1949b). Further congruence properties of the Fourier coefficients of the modular invariant $j(\tau)$. *Am. J. Math.*, 71, 373–386.

——— (1964). Discontinuous groups and automorphic functions. *Am. Math. Soc. Math. Surv.*, No. VIII.

Newman, M. (1958). Congruences for the coefficients of modular forms and for the coefficients of $j(\tau)$. *Proc. Am. math. Soc.*, 9, 609–612.

——— (1960). Periodicity modulo m and divisibility properties of the partition function. *Trans. Am. Math. Soc.*, 97, 225–236.

Ramanathan, K. G. (1943). Congruence properties of $\sigma(n)$, the sum of divisors of n. *Maths. Stud.*, 11, 33–35.

——— (1945). Congruence properties of Ramanujan's function $\tau(n)$ II. *J. Indian math. Soc.*, 9, 55–59.

Rushforth, M. (1952). Congruence properties of the partition function $p(n)$ and associated functions. *Proc. Camb. phil. Soc.*, 48, 402–413.

van Wijnggarden, A. (1953). On the coefficients of the modular invariant $j(\tau)$. *Proc. K. ned. Akad. Wet.*, A 56 = *Indagationes Math.*, 15, 380–400.

Watson, G. N. (1936). Über Ramanujansche Kongruenzeigenschaften der Zerfällungsanzahlen. *Math. Z.*, 39, 712–731.

Zuckerman, H. S. (1939). The computation of the smaller coefficients of $j(\tau)$. *Bull. Am. math. Soc.*, 45, 917–919.