Congruences for the Coefficients of Modular Forms and for the Coefficients of $j(\tau)$

MORRIS NEWMAN

Congruence properties of the coefficients of the complete modular invariant

$$j(\tau) = 12^3 J(\tau) = \sum_{n=-1}^{\infty} c(n)x^n = \frac{1}{x} + 744 + 196884x + \cdots,$$

$x = \exp 2\pi i\tau$, $\text{im}\ \tau > 0$, have been given by D. H. Lehmer [1], J. Lehner [2; 3], and A. van Wijngaarden [4]. The moduli for which congruence properties have been determined are products of powers of $2, 3, 5, 7, 11$. Thus Lehner has shown that if $n > 1$ is divisible by $2^{a}3^{b}5^{c}7^{d}11^{e}$, where $a, b, c, d \geq 1$ and $e = 1, 2, 3$ then $c(n)$ is divisible by $2^{3a+8b+35c+11d}11^e$.

In this note we give several congruence properties modulo 13, derived from some general congruences for the coefficients of certain modular forms and an explicit formula for the coefficients $c(n)$. These general congruences are of interest in themselves and will be proved here as well.

If $n$ is a non-negative integer, define $p_r(n)$ as the coefficient of $x^n$ in $\prod(1-x^n)^r$; otherwise define $p_r(n)$ as zero.2 (Here and in what follows all products are extended from 1 to $\infty$ and all sums from 0 to $\infty$, unless otherwise stated.) Special cases of identities proved by the author in [5] and [6] follow:

Let $p$ be a prime $> 3$. Set $\delta = (p-1)/12$, $\Delta = (p^2-1)/12$. Then

(1) $p_2(np + \delta) = p_2(n)p_2(\delta) - p_2\left(\frac{n - \delta}{p}\right)$, $p \equiv 1 \pmod{12}$

(2) $p_2(np + \Delta) = (-1)^{(p+1)/2}p_2(n/p)$, $p \not\equiv 1 \pmod{12}$.

The coefficient $p_2(\delta)$ has been determined by the author in [7]. As a matter of fact, $p_2(\delta)$ is just $2(-1)^e$, where $e$ is the integer nearest to $(a+b)/6$ and $a, b$ are the uniquely determined positive integers such that $2p = a^2 + b^2$.

From these identities, we shall prove the following congruences:

Received by the editors March 7, 1958.

1 The preparation of this paper was supported (in part) by the Office of Naval Research.

2 The same convention applies to all the number-theoretical functions appearing subsequently.
Theorem. Let $Q$ be an integer and set $R = Qp + 2$. Then

(3) \[ p_R(np + \delta) \equiv p_2(\delta)p_{Q+2}(n) - p_{2p+Q}(n - \delta) \pmod{p}, \quad p \equiv 1 \pmod{12} \]

(4) \[ p_R(np + \Delta) \equiv (-1)^{(p+1)/2}p_{2p+Q}(n) \pmod{p}, \quad p \not\equiv 1 \pmod{12}. \]

Proof of the Theorem. We prove only congruence (3), the proof of congruence (4) being entirely similar. We have

\[ \prod (1 - x^n)^p = \prod (1 - x^n)^{Qp+2} \]
\[ = \prod (1 - x^{np})^Q(1 - x^n)^2 \pmod{p}. \]

Comparing coefficients, we find

\[ p_R(n) \equiv \sum_{0 \leq j < n/p} p_Q(j)p_2(n - pj) \pmod{p}. \]

Replace $n$ by $np + \delta$. Since $\delta/p < 1$, $j$ now runs from 0 to $n$ inclusive, and making use of (1) we find

\[ p_R(np + \delta) \equiv \sum_{j=0}^{n} p_Q(j)p_2((n - j)p + \delta) \]
\[ = \sum_{j=0}^{n} p_Q(j) \left\{ p_2(n - j)p_2(\delta) - p_2\left(\frac{n - j - \delta}{p}\right)\right\} \]
\[ = p_{Q+2}(n)p_2(\delta) - \sum_{j=0}^{n} p_Q(j)p_2\left(\frac{n - j - \delta}{p}\right) \pmod{p}. \]

Consider

\[ \sum_{j=0}^{n} p_Q(j)p_2\left(\frac{n - j - \delta}{p}\right) = \sum_{j=0}^{m} p_Q(m - j)p_2(j/p), \quad m = n - \delta. \]

We have

\[ \sum \left\{ \sum_{j=0}^{m} p_Q(m - j)p_2(j/p) \right\} x^m = \sum p_Q(m)x^m \cdot \sum p_2(m)x^{mp} \]
\[ = \prod (1 - x^m)^Q(1 - x^{mp})^2 \]
\[ = \prod (1 - x^m)^{Q+2p} \pmod{p}. \]

Thus

\[ \sum_{j=0}^{m} p_Q(m - j)p_2(j/p) \equiv p_{2p+Q}(m) \pmod{p}, \]

and the conclusion follows.

Some interesting consequences of this theorem are obtained by
choosing \( Q = \pm 2, \ Q = -2p \). Setting \( \alpha = 2p + 2, \ \beta = 2p - 2, \ and \ \gamma = 2p^2 - 2 \) we find

\begin{align}
(5) \quad & p_\alpha(np + \delta) \equiv p_\delta(np + p) - p_\alpha(n - \delta) \pmod{p}, \quad p \equiv 1 \pmod{12} \\
(6) \quad & p_\beta(np + \delta) \equiv - p_\delta(n - \delta) \pmod{p}, \quad n \geq 1, \ p \equiv 1 \pmod{12} \\
(7) \quad & p_\gamma(np + \delta) \equiv p_\delta(p_{-\delta}(np)) \pmod{p}, \quad n \geq 1, \ p \equiv 1 \pmod{12} \\
(8) \quad & p_\alpha(np + \Delta) \equiv (-1)^{(p+1)/2}p_\alpha(n) \pmod{p}, \quad p \neq 1 \pmod{12} \\
(9) \quad & p_{-\gamma}(np + \Delta) \equiv 0 \pmod{p}, \quad n \geq 1, \ p \neq 1 \pmod{12}.
\end{align}

For \( p = 13 \), (6) implies that

\begin{align}
(10) \quad & p_{-\gamma}(13n + 1) \equiv - p_{24}(n - 1) \equiv - \tau(n) \pmod{13}, \quad n \geq 1.
\end{align}

We now wish to employ these congruences to determine a congruence for \( j(\tau) \) modulo 13. It is known that if

\[ G_k = \sum_{n=1}^{\infty} (n\tau + n)^{-2k} = \frac{B_k}{k} \sum_{n=1}^{\infty} \sigma_{2k-1}(n)x^n \]

is the Eisenstein modular form,

\[ \Delta = \prod_{n=1}^{\infty} (1 - x^n)^2 = \sum_{n=1}^{\infty} \tau(n)x^n, \]

and \( r, s \) are integers such that \( rk = 6s \), then \( G_k/\Delta^s \) is an entire modular function on the full modular group \( \Gamma \) having a pole of order \( s \) in the uniformizing variable \( x \) at \( \tau = i\infty \), and so is a polynomial in \( J \) of degree \( s \). For \( k = 6, r = s = 1 \), we find that \( G_6/\Delta \) is linear in \( J \). Comparing coefficients we find that

\begin{align}
(11) \quad & c(n) = p_{-24}(n + 1) + \frac{24 \cdot 2730}{691} \sum_{j=0}^{n} \sigma_{11}(j + 1)p_{-24}(n - j), \quad n \geq 1
\end{align}

and since \( 13 \mid 2730 \), this implies that

\begin{align}
(12) \quad & c(n) \equiv p_{-24}(n + 1) \pmod{13}, \quad n \geq 1.
\end{align}

Thus making use of (10) we obtain the interesting congruence

\begin{align}
(13) \quad & c(13n) \equiv - \tau(n) \pmod{13}, \quad n \geq 1.
\end{align}

It is known that \( \tau(n) \) is multiplicative. In fact if \( p \) is a prime, Mordell has shown that

\begin{align}
(14) \quad & \tau(np) = \tau(n)\tau(p) - p^{11}\tau(n/p).
\end{align}

We thus obtain the following congruence, using (13) and (14):

\begin{align}
(15) \quad & c(13np) + c(13n)c(13p) + p^{11}c(13n/p) \equiv 0 \pmod{13}.
\end{align}
From (15) we find easily that if $p$ is a prime such that $13 \mid \tau(p)$, and if $(n, p) = 1$, then

\[(16) \quad c(13n p^{a-1}) \equiv 0 \pmod{13}.
\]

For $p < 200$, this happens for $p = 7, 11, 157, 179$. Thus we can say for example that $c(91n)$ is divisible by 13 if $(n, 7) = 1$ and that $c(143n)$ is divisible by 13 if $(n, 11) = 1$. The least value which is an instance of (16) is 91. In his paper [4] van Wijngaarden gives $c(91)$, and this is indeed divisible by 13.

Several instances of (15) follow:

\[(17) \quad c(26n) \equiv 2c(13n) + 6c(13n/2) \pmod{13},
\]

\[(18) \quad c(39n) \equiv 5c(13n) + 4c(13n/3) \pmod{13},
\]

\[(19) \quad c(169n) \equiv 8c(13n) \pmod{13}.
\]

References


