MATH. SCAND. 10 (1962), 173–181

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

O. KOLBERG

1.

The modular invariant $j(\tau)$ is defined by

$$j(\tau) = x^{-1}\left(1+240\sum_{1}^{\infty}\sigma_3(n)x^n\right)^3\prod_{1}^{\infty}(1-x^n)^{-24}, \qquad x = \exp(2\pi i\tau),$$

where

$$\sigma_k(n) = \sum_{d|n} d^k .$$

The coefficients in the expansion

$$j(\tau) = \sum_{-1}^{\infty} c(n)x^n$$

have remarkable divisibility properties. Thus Lehner [5] [6] has shown that

$$c(2^a n) \equiv 0 \pmod{2^{3a+8}}, \tag{1.1}$$

$$c(3^a n) \equiv 0 \pmod{3^{2a+3}}, \tag{1.2}$$

$$c(5^a n) \equiv 0 \pmod{5^{a+1}}, \tag{1.3}$$

$$c(7^a n) \equiv 0 \pmod{7^{a}}, \tag{1.4}$$

for arbitrary positive integers a, n. He proved also that, if $a=1,2,3,$ and $n>0$, then

$$c(11^a n) \equiv 0 \pmod{11^{a}}. \tag{1.5}$$

It is not known whether (1.5) is valid for $a>3$. The congruence (1.1) has been somewhat improved by the author [2], we have, in fact

$$c(2^a n) \equiv -2^{3a+8}\,3^{a-1}\,\sigma_7(n) \pmod{2^{3a+13}}, \tag{1.6}$$

for $a>0$, n odd. It is probable that (1.2)–(1.4) can be sharpened in a similar way, but this will not be considered here. Especially, (1.6) proves Lehner's conjecture that 2^{3a+8} is the exact power of 2 dividing $c(2^a)$.

Received December 1, 1961.

Newman [10] has deduced an interesting congruence connecting $c(n)$ and Ramanujan's function $\tau(n)$, viz.

$$c(13n) \equiv -\tau(n) \pmod{13}, \qquad n>0 . \tag{1.7}$$

The function $\tau(n)$ is defined by

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

Now, if p is a prime we have (Mordell [7])

$$\tau(pn) = \tau(p)\tau(n)-p^{11}\tau(n/p) , \tag{1.8}$$

with $\tau(n/p)=0$ if $(n,p)=1$. By means of this, Newman obtains congruences involving $c(n)$ only, for example

$$c(91n) \equiv 0 \pmod{13} \quad \text{if} \quad (n,7) = 1 .$$

There also exist certain congruences for $c(n)$ $(\bmod p^a)$ with $(n,p)=1$. Thus, Lehmer [4] proved that

$$c(5n \pm 2) \equiv 0 \pmod{5} , \tag{1.9}$$

and for powers of 2 the author [2] has obtained the results (as usual, we write $\sigma(n)$ instead of $\sigma_1(n)$)

$$c(8n+1) \equiv 20\sigma_7(8n+1) \pmod{2^7} , \tag{1.10}$$

$$c(8n+3) \equiv \tfrac{1}{2}\sigma(8n+3) \pmod{2^3} , \tag{1.11}$$

$$c(8n+5) \equiv -12\sigma_7(8n+5) \pmod{2^8} . \tag{1.12}$$

In the following we shall deduce other congruences of this type, viz.

$$c(3n+1) \equiv 54\sigma(3n+1) \pmod{3^4} , \tag{1.13}$$

$$c(n) \equiv 10n\sigma(n) \pmod{5^2}, \qquad (n/5) = -1 , \tag{1.14}$$

$$c(n) \equiv 2n\sigma_3(n) \pmod{7}, \qquad (n/7) = 1 , \tag{1.15}$$

$$c(n) \equiv -2n^2\sigma_5(n)-3n^3\sigma_3(n) \pmod{11}, \qquad (n/11) = 1 , \tag{1.16}$$

$$c(n) \equiv -5\tau(n)-3n^3\sigma_5(n)-2n^4\sigma_3(n) \pmod{13}, \qquad (n/13) = -1 , \tag{1.17}$$

where (n/p) is Legendre's symbol. Especially, for the respective moduli we can find constants a, b such that $c(an+b)\equiv 0$. Thus, (1.17) implies

$$c(2^4\cdot 3^3\cdot 7^2\cdot 13n+2^3\cdot 3^2\cdot 5\cdot 7) \equiv 0 \pmod{13} ,$$

since $\tau(n)$ and $\sigma_k(n)$ are multiplicative, and $\tau(7)\equiv\sigma_3(8)\equiv\sigma_5(9)\equiv 0$ $(\bmod 13)$.

For prime moduli >13 there seem to be no congruences similar to (1.9)–(1.17). However, it is possible to deduce certain results akin to Newman's formula (1.7): Let

$$\sum_{k}^{\infty} \tau_k(n)x^n = x^k \prod_{1}^{\infty} (1-x^n)^{24k},$$

so that $\tau_1(n)=\tau(n)$. Then for $n>0$ we have

$$c(17n) \equiv 7\tau_4(17n) \pmod{17}, \tag{1.18}$$

$$c(19n) \equiv 4\tau_3(19n) \pmod{19}, \tag{1.19}$$

$$c(23n) \equiv 13\tau_{11}(23n) \pmod{23}. \tag{1.20}$$

These congruences are special cases of a more general result which can be stated as follows:

THEOREM 1. *Let p be a prime $\geqq 13$, and put*

$$r = \left[\frac{p}{12}\right], \qquad t = \frac{p-1}{(p-1,12)}.$$

Then there exist constants a_k not all $\equiv 0 \pmod{p}$, such that

$$a_0 c(pn) \equiv \sum_{k=1}^{r} a_k \tau_{kt}(pn) \pmod{p}, \qquad n>0. \tag{1.21}$$

Now consider the determinant

$$d = |\tau_{kt}(pn)|, \qquad k,n = 1,2,\ldots r.$$

Obviously, by Theorem 1 we get:

COROLLARY. *If $d \not\equiv 0 \pmod{p}$, then there is a unique congruence of the form*

$$c(pn) \equiv \sum_{k=1}^{r} b_k \tau_{kt}(pn) \pmod{p}, \qquad n>0. \tag{1.22}$$

Putting $p=17$, 19, 23 and evaluating, we easily obtain (1.18)–(1.20). Newman's congruence (1.7) also follows from the corollary, since $\tau(13n) = \tau(13)\tau(n) \pmod{13}$, cf. (1.8). The numerical values necessary for the computation can be found in tables given by Newman [9], Watson [12], and van Wijngaarden [13].

According to a theorem of Newman [8] the functions $\tau_k(n)$, $k=2,3,\ldots$, satisfy identities similar to (1.8), but with a greater number of terms. Therefore, by (1.18)–(1.20) and corresponding results for $p>23$, it should be possible to deduce new congruence properties of $c(n)$; but the required identities are not yet explicitly known.

It is an open question whether a congruence of the form (1.22) exists for arbitrary p. There may be values of p such that $a_0 \equiv 0 \pmod{p}$ for any set of numbers a_k satisfying (1.21). A result akin to theorem 1, involving the partition function instead of $c(n)$, was proved in [3], and in that case such "exceptional" primes do actually occur, the first one being $p=23$.

2.

We now turn to the proofs of (1.13)–(1.17). Let

$$\Phi_{r,s} = \sum_1^\infty n^r \sigma_{s-r}(n) x^n ,$$

$$P = 1-24\Phi_{0,1}, \qquad Q = 1+240\Phi_{0,3}, \qquad R = 1-504\Phi_{0,5} . \tag{2.1}$$

It is well known, cf. Ramanujan [11], that if r and s are non-negative integers of opposite parity, then $\Phi_{r,s}$ can be expressed as a polynomial in P, Q, R. Especially

$$1+480\Phi_{0,7} = Q^2 , \tag{2.2}$$

$$1-264\Phi_{0,9} = QR , \tag{2.3}$$

$$691+65520\Phi_{0,11} = 441Q^3+250R^2 , \tag{2.4}$$

$$1-24\Phi_{0,13} = Q^2R . \tag{2.5}$$

Also, putting $\delta = xd/dx$ we have

$$\delta P = (P^2-Q)/12, \qquad \delta Q = (PQ-R)/3, \qquad \delta R = (PR-Q^2)/2 . \tag{2.6}$$

We shall not write down the expressions for $\Phi_{r,s}$, $r>0$, needed in the following. In fact, since $\delta\Phi_{r,s} = \Phi_{r+1,s+1}$, these formulae are easily deduced from (2.1)–(2.6).

Further, we define

$$F = x \prod_1^\infty (1-x^n)^{24} .$$

It is known (cf. [11]) that

$$Q^3-R^2 = 1728F . \tag{2.7}$$

We also notice the simple result $\delta F = PF$, which follows directly from (2.6) and (2.7). Finally, we remark that in this notation $j(\tau)$ can be written

$$j = j(\tau) = Q^3F^{-1} = R^2F^{-1}+1728 . \tag{2.8}$$

Now, to prove (1.13) we proceed as follows: From the definition of R we get $R^2 \equiv 2R-1 \pmod{3^4}$, and hence, by (2.8)

$$j-27 \equiv (2R-1)F^{-1} \pmod{3^4}.$$

The congruences refer to the coefficients of the power series in x. Further, by straightforward computation it is easily verified that

$$\begin{aligned} 2R-1 &= 2P^3+864P\Phi_{1,2}-1728\Phi_{2,3}-1\,, \\ \delta^3F^{-1} &= (-P^3-72P\Phi_{1,2}+24\Phi_{2,3})F^{-1}\,. \end{aligned}$$

Combining, we obtain

$$j-27+(2\delta^3+1)F^{-1} \equiv 3(7\Phi_{2,3}-3P\Phi_{1,2})F^{-1} \pmod{3^4}. \tag{2.9}$$

Since $\sigma(3n+2) \equiv 0 \pmod 3$ we have

$$\Phi_{1,2} \equiv \Phi_{2,3} \pmod 3. \tag{2.10}$$

We also need the congruence

$$F \equiv \Phi_{1,2} \pmod 3, \tag{2.11}$$

which follows from the well-known result $F \equiv \Phi_{2,3} \pmod{3^2}$ due to Bambah and Chowla [1]. Using now (2.9)–(2.11) together with the obvious congruence $P \equiv 1 \pmod 3$, we obtain

$$\begin{aligned} &\delta(\delta+1)j+\delta(\delta+1)(2\delta^3+1)F^{-1} \\ &\quad\equiv 3^2(\delta+1)\{P(P\Phi_{1,2}-\Phi_{2,3})F^{-1}\} \pmod{3^4} \\ &\quad\equiv 3^2(\delta+1)\{(P\Phi_{1,2}-\Phi_{2,3})F^{-1}\} \pmod{3^4} \\ &\quad\equiv 3^2\{3\Phi_{1,2}{}^2-(P-1)(P\Phi_{1,2}-\Phi_{2,3})\}F^{-1} \pmod{3^4} \\ &\quad\equiv 3^3\Phi_{1,2} \pmod{3^4}, \end{aligned}$$

and hence

$$c(3n+1) \equiv 54\sigma(3n+1)-\{2(3n+1)^3+1\}\tau_{-1}(3n+1) \pmod{3^4}.$$

Thus, it remains only to prove that $\tau_{-1}(3n+1) \equiv 0 \pmod{3^3}$. In fact, since $(1-x^n)^{27} \equiv (1-x^{3n})^9 \pmod{3^3}$, we have by a well-known identity of Jacobi

$$\begin{aligned} \sum_{-1}^{\infty} \tau_{-1}(n)x^n &\equiv x^{-1}\prod_{1}^{\infty}(1-x^{3n})^{-9}(1-x^n)^3 \pmod{3^3} \\ &\equiv \sum_{0}^{\infty}(-1)^n(2n+1)x^{\frac{1}{2}(n-1)(n+2)}\prod_{1}^{\infty}(1-x^{3n})^{-9} \pmod{3^3}. \end{aligned}$$

Obviously, in the power series expansion of the last expression the coefficient of x^{3n+1} vanishes, and this completes the proof of (1.13).

Similarly, we see that $Q \equiv 1 \pmod 5$, and hence $Q^2 \equiv 2Q-1 \pmod{5^2}$, $Q^3 \equiv 3Q-2 \pmod{5^2}$. Using this, we find

$$j \equiv (3Q-2)F^{-1} \pmod{5^2},$$

$$\begin{aligned} 96F(\delta^4+2\delta^2+5)F^{-1} \\ &= 55P^4+30P^2Q+8PR+3Q^2+176P^2+16Q+480 \\ &\equiv -4(P-R)^2+4R^2+10P^2(3P^2+1)-3Q+2 \pmod{5^2}. \end{aligned}$$

Further, since $d^5 \equiv d \pmod 5$ we have $\Phi_{0,5} \equiv \Phi_{0,1} \pmod 5$, and therefore $P-R \equiv 0 \pmod 5$, $R^2 = Q^3-1728F \equiv 3Q-3F-2 \pmod{5^2}$, $P^2 \equiv R^2 \equiv 2F+1 \pmod 5$. It follows that

$$(\delta^4+2\delta^2+5)F^{-1} \equiv (-Q+9)F^{-1}-5F-7 \pmod{5^2}.$$

Noticing that $\Phi_{1,2} = (Q-P^2)/288 \equiv 2-2P^2 \equiv F \pmod 5$ we thus obtain

$$j-4 \equiv 10\Phi_{1,2}-3(\delta^4+2\delta^2+5)F^{-1} \pmod{5^2},$$

which yields

$$c(n) \equiv 10n\sigma(n)-3(n^4+2n^2+5)\tau_{-1}(n) \pmod{5^2}, \qquad n>0.$$

Finally, by means of Euler's "pentagonal theorem" we get

$$\begin{aligned} \sum_{-1}^{\infty} \tau_{-1}(n)x^n &\equiv x^{-1}\prod_{1}^{\infty}(1-x^{5n})^{-5}(1-x^n) \pmod{5^2} \\ &\equiv \sum_{-\infty}^{\infty}(-1)^n x^{(n+1)(3n-2)/2}\prod_{1}^{\infty}(1-x^{5n})^{-5} \pmod{5^2}, \end{aligned}$$

and (1.14) follows.

The proofs of (1.15)–(1.17) are simpler, because of the prime moduli. In the first case, from (2.1) and (2.2) we obtain $R \equiv 1$, $Q^2 \equiv P$, $F = (Q^3-R^2)/1728 \equiv 1-PQ$, $P^3 \equiv P^2Q^2 \equiv F^2-2F+1 \pmod 7$. By means of this it is easily verified that

$$j+3 \equiv 2\Phi_{1,4}+3(\delta^3-1)F^{-1} \pmod 7,$$

which implies (1.15).

Similarly, we have $QR \equiv 1$, $5Q^3-4R^2 \equiv P$, $PQ \equiv Q(R^2+5F) \equiv R+5QF$, $PR \equiv R(Q^3+4F) \equiv Q^2+4RF \pmod{11}$; and a simple calculation yields

$$j+4 \equiv 4\Phi_{1,8}-2\Phi_{2,7}+4\Phi_{3,6}-5\delta(\delta^5-1)F^{-1} \pmod{11}.$$

This proves (1.16) because

$$\sigma_7(n) = n^7\sigma_{-7}(n) \equiv n^2\sigma_3(n) \pmod{11}, \qquad (n/11) = 1.$$

For the modulus 13 we shall give some more details: First, by (2.4) and (2.5) we get $6Q^3-5R^2 \equiv 1$, $Q^2R \equiv P$. It follows that $Q^3 \equiv 5F+1$,

$R^2 \equiv 6F+1$, $P^2 \equiv Q^4R^2 \equiv Q(4F^2-2F+1)$, $PQ \equiv Q^3R \equiv R(5F+1)$, $PR \equiv Q^2R^2 \equiv Q^2(6F+1)$.

Further we find, using the congruence for P^2

$$\delta^2(F^{-1}+5F) \equiv (2P^2-Q)F^{-1}+5QF \equiv QF^{-1}-4Q\,.$$

Applying the operator δ, inserting for PQ, and replacing δQ by $6\Phi_{1,4}$ we get

$$\delta^3(F^{-1}+5F) \equiv -RF^{-1}+R+2\Phi_{1,4}\,.$$

Continuing in this way, and noticing that $j=Q^3F^{-1} \equiv F^{-1}+5$, we obtain the congruence

$$j-4 \equiv -5F+\Phi_{1,10}-5\Phi_{2,9}+5\Phi_{3,8}-\Phi_{4,7}-6(\delta^6+1)(F^{-1}+5F) \pmod{13}\,,$$

and (1.17) follows in the same way as (1.16).

3.

It remains to prove theorem 1. For this purpose we use a somewhat different technique. First, we need a well-known recursion formula for $\Phi_{0,2k+1}$. In fact, putting

$$S_k = -(2k+2)^{-1}B_{k+1}+\Phi_{0,k}$$

where $B_2=1/6$, $B_4=-1/30, \ldots$ denote Bernoulli numbers, we have (cf. Ramanujan [11]) for k even and $\geqq 4$

$$\frac{(k-2)(k+5)}{12(k+1)(k+2)}S_{k+3} = \binom{k}{2}S_3S_{k-1}+\binom{k}{4}S_5S_{k-3}+\ldots+\binom{k}{k-2}S_{k-1}S_3\,.$$

It follows that

$$pS_{p-2} = \sum_{4\mu+6\nu=p-1} \alpha_{\mu\nu}Q^\mu R^\nu\,,$$

where $\alpha_{\mu\nu}$ are rational numbers not containing p in the denominator. On the other hand we have (all congruences are modulo p)

$$pS_{p-2} = -p(2p-2)^{-1}B_{p-1}+p\Phi_{0,p-2} \equiv \tfrac{1}{2}pB_{p-1} \equiv -\tfrac{1}{2}\,,$$

cf. the well known formula

$$\sum_{\nu=0}^{k-1}\binom{k}{\nu}B_\nu = 0\,.$$

Comparing the two expressions for pS_{p-2} we get a congruence involving only Q and R. Inserting for Q^3 and R^2 from (2.8), we see that the result can be written in the form

$$F^{-r} \equiv \begin{cases} f(j) & p = 12r+1 \\ Qf(j) & p = 12r+5 \\ Rf(j) & p = 12r+7 \\ QRf(j) & p = 12r+11, \end{cases} \tag{3.1}$$

where $f(j) = f_p(j)$ is a polynomial in j of degree r with integral coefficients. Remembering the definition of t, we obtain

$$F^{-t} \equiv \begin{cases} f(j) \\ jf(j)^3 \\ (j-1728)f(j)^2 \\ j^2(j-1728)^3 f(j)^6 . \end{cases} \tag{3.2}$$

From (2.6) and (2.8) we get $\delta j = -Q^2RF^{-1}$, and hence

$$Q = \frac{(\delta j)^2}{j(j-1728)}, \qquad R = -\frac{(\delta j)^3}{j^2(j-1728)}, \qquad F = \frac{(\delta j)^6}{j^4(j-1728)^3}.$$

Inserting this into (3.1) and combining with (3.2) we find

$$F^{kt}(\delta j)^{p-1} \equiv \begin{cases} j^{8r}(j-1728)^{6r} f(j)^{-k-2} \\ j^{8r-k+2}(j-1728)^{6r+2} f(j)^{-3k-2} \\ j^{8r+4}(j-1728)^{6r-k+2} f(j)^{-2k-2} \\ j^{8r-2k+6}(j-1728)^{6r-3k+4} f(j)^{-6k-2} \end{cases}$$

for an arbitrary integer k. Now let k take the values $0,1,\ldots r$. It follows that

$$F^{kt} \equiv (f(j)\delta j)^{-p} g_k(j)\delta j ,$$

where $g_k(j)$ is a polynomial in j of degree $(r+1)p-kt-1$. Further, putting $k=0$ and multiplying by j we get

$$j \equiv (f(j)\delta j)^{-p} g_{-1}(j)\delta j ,$$

where $g_{-1}(j)$ is a polynomial of degree $(r+1)p$. Now, if $(m,p)=1$ we have $j^{m-1}\delta j \equiv \delta(m^{p-2}j^m)$. We conclude that, for $k = -1,0,\ldots r$

$$g_k(j)\delta j \equiv \delta h_k(j) + \sum_{m=1}^{r+1} A_{km} j^{mp-1}\delta j ,$$

$h_k(j)$ being a polynomial with integral coefficients. Hence, by suitable choice of a_k we obtain a congruence of the form

$$a_{-1}j + \sum_{k=0}^{r} a_k F^{kt} \equiv (f(j)\delta j)^{-p}\,\delta h(j) .$$

Considering now the power series expansion of the right-hand side, we see that the coefficient of x^{pn} is $\equiv 0$, and this proves the theorem.

REFERENCES

1. R. P. Bambah and S. Chowla, *A new congruence property of Ramanujan's function* $\tau(n)$, Bull. Amer. Math. Soc. 53 (1947), 768–769.
2. O. Kolberg, *Congruences for the coefficients of the modular invariant* $j(\tau)$ *modulo powers of 2*, Univ. Bergen Årb. naturv. r. 1961.
3. O. Kolberg, *Some remarks on a class of partition congruences*, Univ. Bergen Årb. naturv. r. 1961.
4. D. H. Lehmer, *Properties of the coefficients of the modular invariant* $J(\tau)$, Amer. J. Math. 64 (1942), 488–502.
5. J. Lehner, *Divisibility properties of the Fourier coefficients of the modular invariant* $j(\tau)$, Amer. J. Math. 71 (1949), 136–148.
6. J. Lehner, *Further congruence properties of the Fourier coefficients of the modular invariant* $j(\tau)$, Amer. J. Math. 71 (1949), 373–386.
7. L. J. Mordell, *On Mr. Ramanujan's empirical expansions of modular functions*, Proc. Cambridge Philos. Soc. 19 (1919), 117–124.
8. M. Newman, *On the existence of identities for the coefficients of certain modular forms*, J. London Math. Soc. 31 (1956), 350–359.
9. M. Newman, *A table of the coefficients of the powers of* $\eta(\tau)$, Nederl. Akad. Wetensch. Proc. Ser. A 59 (1956), 204–216.
10. M. Newman, *Congruences for the coefficients of modular forms and for the coefficients of* $j(\tau)$, Proc. Amer. Math. Soc. 9 (1958), 609–612.
11. S. Ramanujan, *On certain arithmetical functions*, Trans. Cambridge Philos. Soc. 22 (1916), 159–184.
12. G. N. Watson, *A table of Ramanujan's function* $\tau(n)$, Proc. London Math. Soc. (2) 51 (1950), 1–13.
13. A. van Wijngaarden, *On the coefficients of the modular invariant* $J(\tau)$, Nederl. Akad. Wetensch. Proc. Ser. A 56 (1953), 389–400.

UNIVERSITY OF BERGEN, NORWAY