Computation of the Modular Equation

By Hideji ITO*)

Department of Mathematics, College of Education, Akita University

(Communicated by Shokichi IYANAGA, M. J. A., March 13, 1995)

1. Introduction. To each rational prime p, the basic elliptic modular function $j(z)$ gives rise to the modular equation

$$\Phi_p(X, j) = 0.$$

To be more explicit, the p-th modular polynomial $\Phi_p(X, j)$ is defined by

$$\Phi_p(X, j) = (X - j(pz)) \prod_{i=0}^{p-1} \left(X - j\left(\frac{z+i}{p}\right)\right).$$

It is a polynomial in X and $j(z)$ with rational integer coefficients. These coefficients are, in general, gigantic numbers for larger p and the explicit values of them are hard to determine. Classically, H. J. S. Smith computed them for $p = 2, 3$ (1878, 1879), Berwick [2] for $p = 5$ (1916). In recent years, Herrmann [4] published the results up to $p = 7$ (1975), and Kaltofen-Yui [5] gave the results for $p = 11$ (1984). In a letter to the author dated December 3, 1992, Professor Yui informed us that the explicit forms of $\Phi_p(X, j)$ are known up to $p = 31$.

The purpose of this note is to give a simple new algorithm to compute $\Phi_p(X, j)$. By using it, we have obtained explicit forms of them up to $p = 53$. Also, we have discovered some remarkable properties of the coefficients of $\Phi_p(X, j)$, which may have some clues in the investigation of the so called Moonshine phenomenon of the Monster simple group.

We use *Mathematica* ver. 2 on Sony NEWS 3860 (a work station; 20 MIPS with 16 MB RAM memory).

2. Preliminaries. Our approach begins with the following well-known proposition:

Let $f(z)$ be a $SL_2(\boldsymbol{Z})$-modular function that is holomorhic on the upper half plane and let its q-expansion be

$$f(z) = a_{-n}q^{-n} + a_{-(n-1)}q^{-(n-1)} + \cdots \quad (a_i \in \boldsymbol{Z},\ q = e^{2\pi\sqrt{-1}z}).$$

Then $f(z)$ is a polynomial $F(j(z))$ in $j(z)$ with coefficients in $\boldsymbol{Z}$.

It is easy to give an algorithm to get $F(j(z))$ by recursive procedure. (See Lang [9], p. 54.)

We can rewrite the modular polynomial as follows:

$$\Phi_p(X, j) = X^{p+1} + \sum_{i=1}^{p+1} (-1)^i s_i(j) X^{p-i+1}$$
$$= X^{p+1} + j^{p+1} + \sum_{n,m=0}^{p} a_{nm} X^n j^m \quad (a_{nm} \in \boldsymbol{Z}).$$

Here we mean by $s_i(j)$ the i-th fundamental symmetric function in

$$j(pz),\ j\left(\frac{z}{p}\right),\ j\left(\frac{z+1}{p}\right), \ldots,\ j\left(\frac{z+p-1}{p}\right),$$

which is evidently $SL_2(\boldsymbol{Z})$-modular and holomorphic on the upper half plane. So we have

$$s_i(j) = S_i(j)$$

for some polynomial $S_i(j)$ in $j(z)$ (with coefficients in $\boldsymbol{Z}$). We have to obtain the explicit forms of the $S_i(j)$. These matters are, of course, well known. But, in general, it is quite difficult to get the q-expansions of the $s_i(j)$ explicitly. (Except for $i = 1$. In this case $s_1(j) = j(pz) + j(z/p) + \cdots + j((z+p-1)/p) = q^{-p} + 744(p+1) + \cdots$.)

Herrmann [4] took the way of reducing q-expansions of the s_k modulo various primes and using an estimate of the coefficients plus the Chinese remainder theorem he recovered the values.

Kaltofen-Yui [5] took a different view point. They started with the equation $\Phi_p(j(pz), j(z)) = 0$. Substituting the q-expansions of $j(z)$ and $j(pz)$, they got a system of linear equations in the a_{nm}, which has some special features suitable for solving.

3. Our method. The key point of our method lies in the use of power sums and the Newton formula applying for $j(z/p), j((z+1)/p), \ldots, j((z+p-1)/p)$ (note that we treat $j(pz)$ separately).

*) Partially supported by Grant-in-Aid for Scientific Research (No. 05640245), The Ministry of Education, Science and Culture, Japan.

We put

$$t_1 = j\left(\frac{z}{p}\right) + j\left(\frac{z+1}{p}\right) + \cdots + j\left(\frac{z+p-1}{p}\right)$$

$$t_2 = \sum_{0 \le n < m \le p-1} j\left(\frac{z+n}{p}\right) j\left(\frac{z+m}{p}\right)$$

$$\vdots$$

t_k = the k-th fundamental symmetric function of

$$j\left(\frac{z}{p}\right),\ j\left(\frac{z+1}{p}\right), \ldots, j\left(\frac{z+p-1}{p}\right)$$

$$\vdots$$

$$t_p = j\left(\frac{z}{p}\right) j\left(\frac{z+1}{p}\right) \cdots j\left(\frac{z+p-1}{p}\right)$$

Also we put $t_0 = 1$, $t_{p+1} = 0$. Then we have

$$s_k = j(pz)t_{k-1} + t_k \quad (1 \le k \le p+1).$$

Let the q-expansion of $j(z)$ be as follows:

$$j(z) = \frac{1}{q} + c_0 + c_1 q + c_2 q^2 + \cdots \quad (c_i \in \boldsymbol{Z}).$$

Then we have

$$j(pz) = \frac{1}{q^p} + c_0 + c_1 q^p + c_2 q^{2p} + \cdots$$

$$j\left(\frac{z+i}{p}\right) = \frac{1}{\zeta^i q^{1/p}} + c_0 + c_1 \zeta^i q^{1/p} + c_2 \zeta^{2i} q^{2/p} + \cdots \quad (\zeta = e^{(2\pi\sqrt{-1})/p}).$$

To get $S_k(j)$ (= the polynomial expression of $s_k(j)$ in j), we need the q-expansions of the $s_k(j)$ up to the constant term. So we must have the q-expansions of the $t_k(j)$ up to the p-th power of q. To compute them, we introduce the k-th power sum u_k of $j(z/p), \ldots, j((z+p-1)/p)$:

$$u_k = j\left(\frac{z}{p}\right)^k + j\left(\frac{z+1}{p}\right)^k + \cdots + j\left(\frac{z+p-1}{p}\right)^k \quad (1 \le k \le p).$$

Their q-expansions can be obtained from that of $j(z)^k$. In fact, let

$$j(z)^k = \sum_{n=-k}^{\infty} c_k(n) q^n.$$

Then we have the following proposition.

Proposition 1.

$$u_k = p \sum_{n=0}^{\infty} c_k(pn) q^n \quad (1 \le k \le p-1)$$

$$u_p = p\left(\frac{1}{q} + \sum_{n=0}^{\infty} c_p(pn) q^n\right) \quad (k = p)$$

Proof. See, for example, Lehner [7], p. 138.

The Newton formula enables us to get recursively the q-expansions of the t_k:

$$t_1 = u_1$$

$$t_2 = \frac{-1}{2}(u_2 - u_1 t_1)$$

$$t_3 = \frac{1}{3}(u_3 - t_1 u_2 + t_2 u_1)$$

$$\cdots$$

Since the t_k and the $u_k (k < p)$ have no polar term and we need the q-expansions only up to the p-the power of q, above calculations are in effect polynomial calculations. Only t_p has polar term $1/q$.

In this way, we obtain the q-expansions of the s_k up to the constant term and by the well-known method explained in section 2 we get the $S_k(j)$.

Although in a different context, power sums and the Newton formula already appeared in modular function theory (Watson [10], Lehner [7, 8]).

4. Two remarks. We make two remarks concerning the actual programming.

1. *The values of* c_n.

We use the following formula of D. H. Lehmer (Lehmer [6], Apostol [1], p. 93):

$$\frac{65520}{691}\{\sigma_{11}(n) - \tau(n)\} = \tau(n+1) + 24\tau(n) + \sum_{k=1}^{n-1} c_k \tau(n-k)$$

Here $\tau(n)$ is Ramanujan's tau function and $\sigma_{11}(n) = \sum_{d|n} d^{11}$. As $\tau(n)$ is a built-in function in *Mathematica*, this seems the easiest way for us.

2. *The computation of* $c_k(n)$.

The computation of $c_k(n)$ (= the coefficient of q^n in the q-expansion of $j(z)^k$) up to $n = p^2$ took most of our computer time. As we need $j(z)^k$ for whole $1 \le k \le p$, we proceed in an iterative way. Multiplying $j(z)$ by q, we can treat it as a polynomial in q. Let

$$f(q) = \sum_{i=0}^{n} a_i q^i,\ g(q) = \sum_{i=0}^{n} b_i q^i \quad (a_i, b_i \in \boldsymbol{Z}).$$

We want to compute $f(q)g(q) \bmod q^{n+1}$ efficiently. Since the polynomial multiplication takes much time and need considerable memory, we actually did it as a list operation.

5. Some properties of $a_{nm}/p \pmod{p}$. Recall the Kronecker congruence relation:

$$\Phi_p(X, j) \equiv (X^p - j)(X - j^p) \pmod{p}$$

In terms of the coefficients a_{nm}, this means

$$a_{nm} \equiv 0 \pmod{p}$$

except for $a_{11} \equiv a_{pp} \equiv -1 \pmod{p}$.

In this section, we consider $a_{nm} \pmod{p^2}$.

Proposition 2. *Suppose* $p \le 11$. *If* $nm \ne 0 \pmod{p}$ and $(n, m) \ne (1,1)$, *then we have*

$$a_{nm} \equiv 0 \pmod{p^2}.$$

Proof. By Lehner's theorem [7, 8], we have

$$c_k(pn) \equiv 0 \pmod{p}, \ (p \leq 11)$$

for every integer n. Hence the algorithm explained in section 3 together with Proposition 1 gives the assertion.

When $13 \leq p \leq 23$, we observe $a_{nm} \not\equiv 0 \pmod{p^2}$ for all n, m. When $p \geq 29$, there are cases where p^2 divides a_{nm}. For example, when $p = 29$, we have $a_{1,26} \equiv 0 \pmod{29^2}$.

At any rate, since we have $a_{nm} \equiv 0 \pmod{p}$ (except for $(n, m) = (1,1), (p, p)$), we are led to consider the behavior of $a_{nm}/p \pmod{p}$, and found some remarkable phenomenon.

Fact 1. *Suppose* $0 < n_i, m_i < p$, $(n_i, m_i) \neq (1,1)$ $(i = 1,2)$. *If* $n_1 + m_1 \equiv n_2 + m_2 \pmod{p-1}$, *then we have*

$$a_{n_1 m_1}/p \equiv a_{n_2 m_2}/p \pmod{p},$$

for $p \leq 31$ *or* $p = 41,47,59,71$. *And for other* $p \leq 2617$, *these congruences don't hold* (*at least for some pair of indices*).

Though we have gotten exact values of the a_{nm} only up to $p = 53$, what we need to verify the above fact is their values modulo p^2. So it becomes possible to check for $p = 59, 71$. For other p, what we actually checked is $a_{p-1,p-3} \not\equiv a_{p-2,p-2} \pmod{p^2}$. When this doesn't hold, then we next checked whether $a_{p-1,p-4} \not\equiv a_{p-2,p-3} \pmod{p^2}$. (This requires only the q-expansion of $j(z)^2 \pmod{p^2}$ up to the term q^{3p}.)

Fact 2. *Suppose* $p = 13, 17, 19$ *or* 31. *Then to each* $n (2 \leq n \leq p-1)$, *the* $a_{nm}/p \pmod{p}$ $(1 \leq m \leq p-1)$ *repeat themselves the following values*:

$\{8,12,5,1\}$	$\cdots$	*if* $p = 13$,
$\{2,13,8,1,15,4,9,16\}$	$\cdots$	*if* $p = 17$,
$\{7,1,11\}$	$\cdots$	*if* $p = 19$,
$\{7,1,27,24,3\}$	$\cdots$	*if* $p = 31$.

When $n = 1$, *then the same thing occurs but the range of* m *has to be changed to* $2 \leq m \leq p$.

This seems to show that there is certain period f with the values of $a_{nm}/p \pmod{p}$. As f divides $p-1$ in the above four cases, one might expect $f = p-1$ for other values of $p (p = 23,29,41,47,59,71)$. Also above examples suggest various relations among the values (such as $8+5 = 12+1 = 13$ in case $p = 13$, etc.)

The primes $p \leq 31, p = 41,47,59,71$ are exactly the primes that divide the order of the Monster simple group (cf. Conway-Norton [3]), which are at the same time equal to the primes for which the function field determined by the normalizer of $\Gamma_0(p)$ has genus 0. Up to present, the modular equation has played no part in the investigation of the Moonshine phenomenon. It seems to the author that it will deserve further study.

References

[1] T. M. Apostol: Modular Functions and Dirichlet Series in Number Theory. Springer (1976).

[2] W. E. H. Berwick: An invariant modular equation of the fifth order. Quart. J. Math., **47**, 94–103 (1916).

[3] J. H. Conway and S. P. Norton: Monstrous moonshine. Bull. London Math. Soc., **11**, 308–339 (1979).

[4] O. Herrmann: Über die Berechung der Fourier-coefficienten der Funktion $j(\tau)$. J. Riene Angew. Math., **274**, 187–195 (1975).

[5] E. Kaltofen and N. Yui: On the modular equation of order 11. Proc. of the 1984 MACSYMA User's Conference, 472–485 (1984).

[6] D. H. Lehmer: Properties of the coefficients of the modular invariant $J(\tau)$. Amer. J. Math., **64**, 488–502 (1942).

[7] J. Lehner: Divisibility properties of the Fourier coefficients of the modular invariant $j(\tau)$. Amer. J. Math., **71**, 136–148 (1949).

[8] J. Lehner: Further congruence properties of the Fourier coefficients of the modular invariant $j(\tau)$. Amer. J. Math., **71**, 373–386 (1949).

[9] S. Lang: Elliptic Functions. Addison-Wesley (1973).

[10] G. N. Watson: Ramanujans Vermutung über Zerfällungsanzahlen. J. Riene Angew. Math., **179**, 97–128 (1938).