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

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

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.