(Memoirs of the Faculty of Education and Human Studies
Akita University (Natural Science)
55, 17－27 (2000))

On the Modular Equation of $j(z)^{1/3}$

Hideji ITO

(Received December 14, 1999)

In our previous papers [6], [7], we have studied the modular equation $\Phi_\ell(X,Y)$ of $j(z)$ where $j(z)$ is the most basic modular function with respect to $SL_2(\mathbf{Z})$. Now we study about the modular equation $\Phi_\ell^{(3)}(X,Y)$ of $j(z)^{1/3}$ which is a modular function for $\Gamma(3)$. Especially, we have otained the explicit form of $\Phi_\ell^{(3)}(X,Y)$ for all primes $\ell \leq 131$ and found that certain congruences of their coefficients (like those noted in [6]) hold for $\ell \in \mathcal{P} = \{2,5,7,13,19,31\}$. This is remarkable since if we include 3 in $\mathcal{P}$ then these primes in $\mathcal{P}$ coincide with those primes that arise in connection to the Monster simple group.

1 Introduction

Obeying the traditional notation, we put $\gamma_2(z) = j(z)^{1/3}$. As is classically known, $\gamma_2(z)$ is a modular function of level 3. That is, $\gamma_2(z)$ is a modular function with respect to $\Gamma(3) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z}) | \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod 3 \right\}$ (Lang [9] p.254). If ℓ is a rational prime ($\neq 3$) then we have an algebraic relation between $\gamma_2(z)$ and $\gamma_2(\ell z)$:

$$\Phi_\ell^{(3)}(\gamma_2(z), \gamma_2(\ell z)) = 0.$$

We call this formula the modular equation of $\gamma_2(z)(= j(z)^{1/3})$ and by abuse of language we call the polynomial $\Phi_\ell^{(3)}(X,Y)$ itself the modular equation of $\gamma_2(z)$.

Already Weber [11] p.248 gave the explicit form for $\ell = 2$:

$$\Phi_\ell^{(3)}(X,Y) = X^3 + Y^3 - X^2Y^2 + 5 \cdot 9 \cdot 11 \cdot XY - 2^4 \cdot 3^3 \cdot 5^3.$$

In a recent article [3], Elkies calls attention to $\Phi_\ell^{(3)}(X,Y)$ (after a suggestion of Atkin). He writes the above explicit formula and notes the smallness of the coefficients of $\Phi_\ell^{(3)}(X,Y)$ compared with those of $\Phi_\ell(X,Y)$ and states (without proof) the following two propositions:

(A) If we put $\Phi_\ell^{(3)}(X,Y) = X^{\ell+1} + Y^{\ell+1} + \Sigma_{a,b=0}^{\ell} f_{ab} X^a Y^b$, then we have $f_{ab} = 0$ unless $a + \ell b \equiv \ell + 1 \bmod 3$;

(B) We have $\Phi_\ell(X^3, Y^3) = \Phi_\ell^{(3)}(X,Y)\Phi_\ell^{(3)}(X,\zeta Y)\Phi_\ell^{(3)}(X,\zeta^2 Y)$ where ζ is a primitive 3-rd root of unity.

(We give proofs of (A) and (B) in the next section.)

Our purpose of this paper is to study about $\Phi_\ell^{(3)}(X,Y)$. As it seems there is few literature about it we give a rather detailed account of it.

Remark 1. The exact subgroup of $SL_2(\mathbf{Z})$ that leaves $\gamma_2(z)$ invariant is as follows:

$$\left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z}) | \quad a \equiv d \equiv 0 \bmod 3 \text{ or } b \equiv c \equiv 0 \bmod 3\right\}.$$

(See Cox [2] p.276.)

Remark 2. As for the computation of $\Phi_n(X,Y)$ (the modular equation of $j(z)$), we have obtained the explicit form of them for all $n \leq 100$ (including composite n) except for $n = 90$, 96 by March,1999.

2 The construction of $\Phi_\ell^{(3)}(X,Y)$

Let ℓ be a rational prime($\neq 3$). The construction(existence) of the modular equation $\Phi_\ell^{(3)}(X,Y)$ can be given along the same way as that of $\Phi_\ell(X,Y)$ but there are some delicate points to be considered (especially in step 6° below).

1° $\gamma_2(z)$ is a modular function with respect to

$$\Gamma(3) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z}) | \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod 3\right\}$$

(See Lang [9] p.254.)

2° For a rational prime $\ell(\neq 3)$, $\gamma_2(\ell z)$ is invariant under $\Gamma_0(\ell) \cap \Gamma(3)$, where $\Gamma_0(\ell) = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z}) | c \equiv 0 \bmod \ell\right\}$.

Proof. Let $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(\ell) \cap \Gamma(3)$. Then we have $\gamma_2(\ell\sigma z) = \gamma_2\left(\ell\dfrac{az+b}{cz+d}\right) = \gamma_2\left(\dfrac{a(\ell z)+\ell b}{(c/\ell)\ell z + d}\right)$. As $c \equiv 0 \bmod \ell$, we have $c/\ell \in \mathbf{Z}$. Also, the condition $c \equiv 0 \bmod 3$ means that c/ℓ is divisible by 3 (here we use $\ell \neq 3$). Hence $\sigma' = \begin{pmatrix} a & \ell b \\ c/\ell & d \end{pmatrix}$ is contained in $\Gamma(3)$. So we have $\gamma_2(\ell\sigma z) = \gamma_2(\sigma'\ell z) = \gamma_2(\ell z)$. (Q.E.D.)

3° The group index $[\Gamma(3) : \Gamma_0(\ell) \cap \Gamma(3)] = \ell + 1$ (for $\ell \neq 3$).

Proof. Since $\ell \neq 3$, we easily have $SL_2(\mathbf{Z}) = \Gamma(3) \cdot \Gamma_0(\ell)$. Also, as $SL_2(\mathbf{Z})/\Gamma(3) \cong SL_2(\mathbf{Z}/3\mathbf{Z})$, we know $[SL_2(\mathbf{Z}) : \Gamma(3)] = 12$. Therefore we have $\Gamma_0(\ell)/\Gamma_0(\ell) \cap \Gamma(3) \cong \Gamma_0(\ell) \cdot \Gamma(3)/\Gamma(3) = SL_2(\mathbf{Z})/\Gamma(3)$. On the other hand, we know $[SL_2(\mathbf{Z}) : \Gamma_0(\ell)] = \ell + 1$ ([10] p.24). Hence we have $[\Gamma(3) : \Gamma_0(3) \cap \Gamma(3)] = [SL_2(\mathbf{Z}) : \Gamma_0(\ell) \cap \Gamma(3)]/[SL_2(\mathbf{Z}) : \Gamma(3)] = [SL_2(\mathbf{Z}) : \Gamma_0(\ell) \cap \Gamma(3)]/[\Gamma_0(\ell) : \Gamma_0(\ell) \cap \Gamma(3)] = [SL_2(\mathbf{Z}) : \Gamma_0(\ell)] = \ell + 1$. (Q.E.D.)

4° Let $\{\sigma_i\}$ be the representatives of the coset decomposition of $\Gamma(3)$ by $\Gamma_0(\ell) \cap \Gamma(3)$:

$$\Gamma(3) = \bigcup_{i=1}^{\ell+1} (\Gamma_0(\ell) \cap \Gamma(3))\sigma_i.$$

We put

$$\Phi_\ell^{(3)}(X, \gamma_2(z)) = \prod_{i=1}^{\ell+1}(X - \gamma_2(\ell\sigma_i z)).$$

Then, as a polynomial of X, the coefficients of $\Phi_\ell^{(3)}(X, \gamma_2(z))$ are polynomials in $\gamma_2(z)$.

Proof. By construction, the coefficients of $\Phi_\ell^{(3)}(X, \gamma_2(z))$ are invariant under the action of $\Gamma(3)$. Let $\mathcal{H}$ be the complex upper half plane. We know $(\Gamma(3)\backslash\mathcal{H})^*$ is of genus 0 ($*$ means the compactification). (See Shimura [10] p.23.) And the field of $\Gamma(3)$-modular functions is generated by $\gamma_2(z)$. Especially, a holomorphic $\Gamma(3)$-modular function is a polynomial in $\gamma_2(z)$. (Q.E.D.)

5°. Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z})$, $\zeta = \exp((2/3)\pi\sqrt{-1})$. Then we have the following transformation formula of $\gamma_2(z)$:

$$\gamma_2\left(\frac{az+b}{cz+d}\right) = \zeta^{ac-ab+a^2cd-cd}\gamma_2(z)$$

(See Cox [2] p.251.)

6° Let $M_2(\mathbf{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbf{Z} \right\}$. Then we can write $\gamma_2(\ell\sigma_i z) = \gamma_2(\sigma z)$ for some σ in the set $M = \left\{ \begin{pmatrix} a & 3b \\ 0 & d \end{pmatrix} \in M_2(\mathbf{Z}) \mid a > 0,\ ad = \ell, 0 \le b \le d-1 \right\}$. The map $\sigma_i \mapsto \sigma$ gives a bijection from the right cosets of $\Gamma_0(\ell) \cap \Gamma(3)$ in $\Gamma(3)$ to the set M .

Proof. We rely on [10] chapter 3. First we need some notations. Fix N, a natural number (in our case $N = 3$), t a divisor of N (in our case $t = 3$), $\mathfrak{h}$ a subgroup of $(\mathbf{Z}/N\mathbf{Z})^\times$. As in [10] p.67, $\mathfrak{h}$ sometimes means the set of all integers whose residue class modulo N belong to $\mathfrak{h}$. Let Γ' ,Δ' and $\sigma_a \in SL_2(\mathbf{Z})$ be defined by the following way:

$$\Gamma' = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbf{Z}) \mid a \in \mathfrak{h}, b \equiv 0 \pmod{t}, c \equiv 0 \pmod{N} \right\};$$

$$\Delta' = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbf{Z}) \mid a \in \mathfrak{h}, b \equiv 0 \pmod{t}, c \equiv 0 \pmod{N}, ad - bc > 0 \right\};$$

$$\sigma_a \equiv \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix} \pmod{N}.$$

Then [10] Proposition 3.36 (p.72) asserts (for a natural number n) the following:

$$\{\alpha \in \Delta' \mid \det(\alpha) = n\} = \bigcup_a \bigcup_{b=0}^{d-1} \Gamma'\sigma_a \begin{pmatrix} a & bt \\ 0 & d \end{pmatrix} \qquad (a > 0,\ ad = n,\ (a, N) = 1).$$

Here the right hand side is of course disjoint union. Now we set $N = t = 3$ and $n = \ell$ (a rational prime $\neq 3$). Also we set $\mathfrak{h} = (\mathbf{Z}/3\mathbf{Z})^\times$. The double coset $\Gamma(3)\begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix}\Gamma(3)$ is certainly contained in the left hand side of the above formula (unlike $\Gamma' = SL_2(\mathbf{Z})$

they are not equal). Hence we have $\begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix} \sigma_i = \tilde{\sigma}_i \sigma_a \sigma$ for some $\tilde{\sigma}_i \in \Gamma'$, $a \in \mathfrak{h}$ and σ of the form $\begin{pmatrix} a & bt \\ 0 & d \end{pmatrix}$. By the transformation formula of $\gamma_2(z)$ in 5° the action of Γ' or σ_a leaves $\gamma_2(z)$ invariant. So we have $\gamma_2(\ell\sigma_i z) = \gamma_2(\tilde{\sigma}_i\sigma_a\sigma z) = \gamma_2(\sigma z)$.

Next we will show the injectivity of the correspondence between the set of cosets $\Gamma_0(\ell) \cap \Gamma(3) \backslash \Gamma(3)$ and the set M which is induced by the map $\sigma_i \mapsto \sigma$. We put $\sigma_0 = \begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix}$. If $\ell\sigma_i$ and $\ell\sigma_j$ (σ_i and σ_j are some coset representatives as in 3°) are contained in the same set $\Gamma'\sigma_a\sigma$ ($\sigma = \begin{pmatrix} a & bt \\ 0 & d \end{pmatrix}$), then we have $\sigma_0\sigma_i = \rho\sigma_a\sigma$, $\sigma_0\sigma_j = \rho'\sigma_a\sigma$ for some ρ, $\rho' \in \Gamma'$. From these relations we have $\sigma_0\sigma_i\sigma_j^{-1}\sigma_0^{-1} = \rho\sigma_a\sigma \cdot \sigma^{-1}\sigma_a^{-1}\rho'^{-1} = \rho\rho'^{-1}$. If we put $\pi = \rho\rho'^{-1}$, then we have $\pi \in \sigma_0\Gamma(3)\sigma_0^{-1} \cap \Gamma'$. Hence $\sigma_i\sigma_j^{-1} = \sigma_0^{-1}\pi\sigma_0 \in \Gamma(3) \cap \sigma_0^{-1}\Gamma'\sigma_0 \subset \Gamma(3) \cap \Gamma_0(\ell)$. (For the last inclusion, note that if $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma'$ then $\sigma_0^{-1}\begin{pmatrix} a & b \\ c & d \end{pmatrix}\sigma_0 = \begin{pmatrix} a & b/\ell \\ \ell c & d \end{pmatrix}$.) Hence σ_i and σ_j lie in the same coset, a contradiction. (Q.E.D.)

We finally arrive at the following formula:

$$\Phi_\ell^{(3)}(X, \gamma_2(z)) = \prod_{\substack{ad=\ell, a>0 \\ 0 \le b \le d-1}} (X - \gamma_2((az+3b)/d))$$

Put $q = \exp(2\pi\sqrt{-1}z)$. In the next section we see that the q-expansion of $\gamma_2(z)$ is of the form

$$\gamma_2(z) = q^{-1/3}(1 + a_1 q + a_2 q^2 + a_3 q^3 + \cdots) \quad (a_i \in \mathbf{Z}).$$

Now we give proofs of (A) and (B) mentioned in section 1.

Proof of (A). By the modular equation, we have the relation

$$\Phi_\ell^{(3)}(\gamma_2(z), \gamma_2(\ell z)) = 0.$$

Substituting the q-expansions of $\gamma_2(z)$ and $\gamma_2(\ell z)$ into it, we get

$$q^{-(\ell+1)/3}(1 + a_1 q + a_2 q^2 + \cdots)^{\ell+1} + q^{-\ell(\ell+1)/3}(1 + a_1 q^\ell + a_2 q^{2\ell} + \cdots)^{\ell+1}$$
$$+ \sum_{a,b=0}^{\ell} f_{ab} q^{-a/3}(1 + a_1 q + a_2 q^2 + \cdots)^a q^{-b\ell/3}(1 + a_1 q^\ell + a_2 q^{2\ell} + \cdots)^b = 0.$$

Equating the coefficients of the q^n-term, we get relations among the a_i. In particular, if certain terms of the same power of q appear only once then its coefficient f_{ab} must be 0. From the q-expansions of $\gamma_2(z)^{\ell+1}$ and $\gamma_2(\ell z)^{\ell+1}$ we know that their exponents of q are always of the form $A/3$ where $A \equiv -(\ell+1) \pmod 3$. We next look at the sum over a, b ($0 \le a, b \le \ell$). We consider f_{ab} downward, that is, we first consider $f_{\ell,\ell}$, next $f_{\ell-1,\ell}$ etc. We easily see that $f_{\ell,\ell} = -1$ for any ℓ. The term $f_{\ell-1,\ell}q^{-(\ell-1)/3}q^{-\ell^2/3} = f_{\ell-1,\ell}q^{-(\ell-1+\ell^2)/3}$ is the only term of that power of q. Since $\ell - 1 + \ell^2 \not\equiv \ell + 1 \bmod 3$, we

have $f_{\ell-1,\ell} = 0$. This also leads that we have $f_{\ell-1-3m,\ell} = 0$ $m = 1, 2, \ldots$, inductively. By similar reasoning, we know $f_{ab} = 0$ unless $a + b\ell \equiv \ell + 1 \pmod 3$. (Q.E.D.)

Proof of (B). We know

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

So we have

$$\begin{aligned}\Phi_\ell(X^3, j(z)) &= (X^3 - j(\ell z)) \prod_{i=0}^{\ell-1} \left(X^3 - j\left(\frac{z+i}{\ell}\right)\right) \\ &= (X - j^{1/3}(\ell z))(X - \zeta j^{1/3}(\ell z))(X - \zeta^2 j^{1/3}(\ell z)) \times \\ &\quad \prod_{i=0}^{\ell-1} \left(X - j^{1/3}\left(\frac{z+i}{\ell}\right)\right)\left(X - \zeta j^{1/3}\left(\frac{z+i}{\ell}\right)\right)\left(X - \zeta^2 j^{1/3}\left(\frac{z+i}{\ell}\right)\right) \cdots (*)\end{aligned}$$

On the other hand, by the transformation formula in 5°, we have

$$j^{1/3}\left(\frac{z+3s}{\ell}\right) = \zeta^a j^{1/3}\left(\frac{z+i}{\ell}\right)$$

Here we put $3s = i + \ell a$. As ℓ is not divisible by 3, the map $s \mapsto i$ gives a bijection $\mathbf{Z}/\ell\mathbf{Z} \longrightarrow \mathbf{Z}/\ell\mathbf{Z}$. Hence the above $(*)$ is equal to the following form:

$$\begin{aligned}&(X - \gamma_2(\ell z)) \prod_{s=0}^{\ell-1} \left(X - \gamma_2\left(\frac{z+3s}{\ell}\right)\right) \times (X - \zeta\gamma_2(\ell z)) \prod_{s=0}^{\ell-1} \left(X - \zeta\gamma_2\left(\frac{z+3s}{\ell}\right)\right) \\ &\times (X - \zeta^2\gamma_2(\ell z)) \prod_{s=0}^{\ell-1} \left(X - \zeta^2\gamma_2\left(\frac{z+3s}{\ell}\right)\right)\end{aligned}$$

Thus we get

$$\Phi_\ell(X^3, Y^3) = \Phi_\ell^{(3)}(X, Y)\Phi_\ell^{(3)}(X, \zeta Y)\Phi_\ell^{(3)}(X, \zeta^2 Y).$$

(Q.E.D.)

Corollary. The constant term of $\Phi_\ell(X, Y)$ is always cube.

Examples

$$\begin{aligned}\Phi_2(0,0) &= -2^{12}3^9 5^9, & \Phi_3(0,0) &= 0 \\ \Phi_5(0,0) &= 2^{90}3^{18}5^3 11^9, & \Phi_7(0,0) &= 0 \\ \Phi_{11}(0,0) &= 2^{189}3^{36}5^{36}11^3 17^9 29^9, & \Phi_{13}(0,0) &= 0\end{aligned}$$

Note that in case $\ell \equiv 1 \bmod 3$ we always have $\Phi_\ell(0,0) = 0$. By Gross-Zagier [4] p.195, we know that the primes p dividing $\Phi_\ell(0,0)$ are very small: $p \leq (9\ell^2)/4$.

Following assertions can be proven by similar reasoning as in [9].
(1) $\Phi_\ell^{(3)}(X, Y)$ is irreducible in $\mathbf{C}[X, Y]$.
(2) $\Phi_\ell^{(3)}(X, Y) = \Phi_\ell^{(3)}(Y, X)$.
(3) $\Phi_\ell^{(3)}(X, Y) \equiv (X^\ell - Y)(X - Y^\ell) \pmod \ell$.

3 The computation of $\Phi_\ell^{(3)}(X,Y)$

We make several modifications to the procedure of the computation of $\Phi_\ell(X,Y)$ given in [6].

1° Coefficients of the q-expansion of $\gamma_2(z)$.

We know $j(z) = 2^6 3^3 \dfrac{g_2(z)^3}{\Delta(z)}$. Here

$$\begin{aligned} g_2(z) &= \frac{1}{2^2 3}(1 + 240\sum_{n=1}^{\infty}\sigma_3(n)q^n) \qquad (\sigma_3(n) = \sum_{d|n} d^3), \\ \Delta(z) &= (2\pi)^{12} q \prod_{n=1}^{\infty}(1-q^n)^{24}. \end{aligned}$$

We have (recall we put $\gamma_2(z) = j(z)^{1/3}$)

$$\gamma_2(z) q^{1/3} \prod_{n=1}^{\infty}(1-q^n)^8 = 1 + 240\sum_{n=1}^{\infty}\sigma_3(n)q^n.$$

So the q-expansion of $\gamma_2(z)$ is of the form $\gamma_2(z) = q^{-1/3}(1 + a_1 q + a_2 q^2 + \cdots)$ $(a_i \in \mathbf{Z})$. On the other hand, we have Jacobi formulas:

$$\begin{aligned} \prod_{n=1}^{\infty}(1-q^n) &= \sum_{n=-\infty}^{\infty}(-1)^n q^{(1/2)n(3n+1)} \\ \prod_{n=1}^{\infty}(1-q^n)^3 &= \sum_{n=0}^{\infty}(-1)^n(2n+1)q^{(1/2)n(n+1)} \end{aligned}$$

(See [5] p.284-285.) So by repeated applications of `times1` of [6] II p.6 and simple inversion, we get coefficients a_i.

But we prefer another method. We already have coefficients of the q-expansion of $j(z)$ (we accumulated them up to $n = 20000$). The following theorem enables us to compute the coefficients of the q-expansion of $j(z)^M$ (M is a natural number or a fraction $1/m$ $(m \in \mathrm{N})$) from those of $j(z)$.

Theorem *Let* $f(x) = b_0 + b_1 x + b_2 x^2 + b_3 x^3 + \cdots$ $(b_0 = 1)$ *and* $f(x)^M = B_0 + B_1 x + B_2 x^2 + B_3 x^3 + \cdots$ $(B_0 = 1)$ $(M \in \mathrm{N}$ *or* $M = 1/m\,(m \in \mathrm{N}))$. *Define* p_k *recursively by*

$$\begin{aligned} p_1 &= b_1, \\ p_k &= \sum_{i=1}^{k-1}(-1)^{i-1} b_i p_{k-i} + (-1)^{k-1} k b_k \quad (k \geq 2). \end{aligned}$$

Then we have

$$B_k = (-1)^{k-1}\frac{M}{k}\left(\sum_{i=0}^{k-1}(-1)^i B_i p_{k-i}\right).$$

Proof. Fix n and put

$$\begin{aligned} f_n(x) &= 1 + b_1 x + b_2 x^2 + \cdots + b_n x^n \\ F_n(x) &= f_n(x)^M. \end{aligned}$$

Then we have $F_n(x) \equiv f(x)^M \bmod x^{n+1}$, that is, they are equal up to the term x^n. Let $g_n(x) = x^n + b_1 x^{n-1} + \cdots + b_{n-1}x + b_n$ and $\{\alpha_i\}$ be the roots of $g_n(x) = 0$. We have

$$g_n(x) = \prod_{i=1}^{n}(x - \alpha_i)$$

and b_i is the i-th elementary symmetric function of $\{\alpha_i\}$. By the Newton formula we get the k-th power sum of the roots $p_k = \sum \alpha_i^k$ recursively as in the statement of our theorem. Put

$$g_n(x)^M = \prod_{i=1}^{n}(x - \alpha_i)^M = \sum_{i=1}^{nM} \tilde{B}_{nM-i} x^i.$$

Here $\tilde{B}_{nM-i}$ is the i-th elementary symmetric function in $\alpha_1, \ldots, \alpha_1, \alpha_2, \ldots, \alpha_2, \ldots, \alpha_n, \ldots, \alpha_n$ (each repeated M times). Then the kth power sums of the roots of $g_n(x)^M = 0$ (which we put P_k) are simply given by

$$P_k = M p_k \qquad (*).$$

So the Newton formula again (this time using backwards) gives us the $\tilde{B}_i$. And we have $B_i = \tilde{B}_i$ $(1 \le i \le n)$. As n is arbitrary, we have B_i for all i in this way.

When $M = 1/m$, the above relation $(*)$ becomes $mP_k = p_k$ and the rest is the same as before. (Q.E.D.)

2° $\gamma_2(z)^m$

To compute $\Phi_\ell^{(3)}(X, Y)$, we need $\gamma_2(z)^m$ up to $m = \ell$. Put $g = q^{1/3} = \exp(2\pi\sqrt{-1}z/3)$. We use g-expansion of $\gamma_2(z)$:

$$\gamma_2(z) = g^{-1} + a_1 g^2 + a_2 g^5 + a_3 g^8 + \cdots.$$

Let $\gamma_2(z)^m = \sum_{n=-m}^{\infty} a_m(n) g^n$. Like [6] Proposition 1, we have the following lemma.

Lemma

$$\sum_{i=0}^{\ell-1} \gamma_2((z+3i)/\ell)^m = \begin{cases} \ell \sum_{n=0}^{\infty} a_m(\ell n) g^n & \text{if } 1 \le m \le \ell - 1 \\ \ell(1/g + \sum_{n=0}^{\infty} a_\ell(\ell n) g^n) & \text{if } m = \ell. \end{cases}$$

From this and our procedure (see next 3°), we need g-expansion of $\gamma_2(z)$ up to the term $g^{\ell^2+\ell-1}$. (Note that $\gamma_2(z)^\ell = \gamma_2(z)\gamma_2(z)^{\ell-1} = (g^{-1} + \cdots)(g^{-(\ell-1)} + \cdots)$.)

3° The computation of the k-th elementary symmetric function s_k of $\gamma_2(\ell z)$, $\gamma_2(z/\ell)$, $\gamma_2((z + 3\cdot 1)/\ell)$,$\cdots$, $\gamma_2((z + 3(\ell - 1))/\ell)$.

Like the case of $\Phi_\ell(X,Y)$ [4], we first compute the k-th elementary symmetric functions t_k of $\gamma_2(z/\ell)$, $\gamma_2((z+3\cdot 1)/\ell)$, $\cdots$, $\gamma_2((z+3(\ell-1))/\ell)$, then we use the formula

$$s_k = \gamma_2(\ell z)t_{k-1} + t_k.$$

The procedure goes like [6] II p.7. Since $\gamma_2(z)$ has many 0 coefficients in its g-expansion, it becomes simpler than [6]. In the notation of [6] II p.7, we have

```
s2[k,p]/;1<=k<=p:=t2[k-1,p]+
                  Flatten[{Table[0,{p-1}],(-1)^(p-1)*Floor[k/p],0}]
s2[k,p]/;k==p+1 :=t2[k-1,p]
```

(Here we use p in place of ℓ.)

4° $\Phi_\ell^{(3)}(X,Y)$

Once you have non-positive terms of g-expansions of s_k $(1 \le k \le \ell+1)$, then by using recursive method like before ([6] or [9] p.54), you can express s_k as a polynomial in $\gamma_2(z)$ (actually as a list of their coefficients). Collecting them we finally obtain $\Phi_\ell^{(3)}(X,Y)$.

4 A mysterious coincidence

Put $\Phi_\ell(X,Y) = X^{\ell+1} + Y^{\ell+1} + \sum_{n,m=0}^{\ell} a_{nm}X^nY^m$. In [6] we make some observations about values of $a_{nm}/\ell \bmod \ell$. Especially we note the following:

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

$$\frac{a_{n_1 m_1}}{\ell} \equiv \frac{a_{n_2 m_2}}{\ell} \bmod \ell$$

for $\ell \le 31$ *or* $\ell = 41, 47, 59, 71$.

Naturally we are led to consider the matter in our $j(z)^{1/3}$ case. And we find the following:

We have the same congruences precisely when $\ell = 2, 5, 7, 13, 19, 31$ *in the range* $\ell \le 131$.

In appendix 2, we give the table of $f_{ab}/\ell \bmod \ell$ for $\ell = 13$.

Now we consider about the meaning of the values of ℓ satisfying such the congruences. In case of $j(z)$, the primes $\ell \le 31, \ell = 41, 47, 59, 71$ are precisely those primes that divide the order of the Monster group $\mathcal{M}$. In our present case of $j(z)^{1/3}$, the primes $\ell = 2, 5, 7, 11, 19, 31$ and 3 are precisely those primes that divide the order of the centralizer of the conjugacy class 3C of $\mathcal{M}$ which corresponds to $j(3z)^{1/3}$ (see Conway-Norton [1] p.327). (The order of $\mathcal{M}$ is the order of the centralizer of the identity and $j(z)$ corresponds to the identity.)

This is a remarkable coincidence. Kaneko [8] gave a proof of our previous observation, but it seems that it is not easy to apply his method to our present case of $j(z)^{1/3}$.

Appendix 1 The explicit form of $\Phi_\ell^{(3)}(X,Y)$ $(\ell = 2,5,7,11)$

$$\Phi_2^{(3)}(X,Y) = -54000 + X^3 + 495XY - X^2Y^2 + Y^3$$

$$\Phi_5^{(3)}(X,Y) = 5209253090426880 + 654403829760X^3 + X^6 - 82577379557376XY + 66211200X^4Y + 229282790400X^2Y^2 + 1240X^5Y^2 + 654403829760Y^3 - 125915650X^3Y^3 + 66211200XY^4 + 20620X^4Y^4 + 1240X^2Y^5 - X^5Y^5 + Y^6$$

$$\Phi_7^{(3)}(X,Y) = 113568003894804480000000X^2 + 3484850555289600X^5 + X^8 + 21091200723320832000000XY + 1050026597609472000X^4Y - 401660X^7Y + 113568003894804480000000Y^2 + 5452915936075776000X^3Y^2 + 24762303370X^6Y^2 + 5452915936075776000X^2Y^3 - 10422120833264X^5Y^3 + 1050026597609472000XY^4 + 49402229030035X^4Y^4 + 1736X^7Y^4 + 3484850555289600Y^5 - 10422120833264X^3Y^5 + 7402528X^6Y^5 + 24762303370X^2Y^6 + 7402528X^5Y^6 - 401660XY^7 + 1736X^4Y^7 - X^7Y^7 + Y^8$$

$$\Phi_{11}^{(3)}(X,Y) = 157731443735844291334094035353600000000000000 - 4968642685537287745410642739200000000000X^3 + 4568814367232227043086172160000000X^6 + 9882363411841352509440000X^9 + X^{12} - 3611862990088230006609527439360000000000000XY + 434802578620080779104459161600000000X^4Y - 380540316399841352835189964800000X^7Y + 413077590081446400X^{10}Y + 400796701349895944471082486988800000000X^2Y^2 - 7389159768252291652798906368000000X^5Y^2 + 607058665139184599465625600 0X^8Y^2 + 302197280X^{11}Y^2 - 4968642685537287745410642739200000000000Y^3 - 22464991805058247431285846835200000000X^3Y^3 - 1144692425423600993725378560000 0X^6Y^3 - 4974463399905062614720 4X^9Y^3 + 434802578620080779104459161600000000XY^4 + 53162188387540857929234527027200000X^4Y^4 + 14180598822887453449928793600X^7Y^4 + 3140098322119440X^{10}Y^4 - 7389159768252291652798906368000000X^2Y^5 - 46935639980826194752956426240000X^5Y^5 + 64506524322802023105072 0X^8Y^5 - 1984268X^{11}Y^5 + 4568814367232227043086172160000000000Y^6 - 1144692425423600993725378560000 0X^3Y^6 + 131829888420874420227434880 6X^6Y^6 + 2599709219284278200X^9Y^6 - 3805403163998413528351899648000 0XY^7 + 14180598822887453449928793600X^4Y^7 - 5628290007831270614736 0X^7Y^7 + 901748705440X^{10}Y^7 + 607058665139184599465625600 0X^2Y^8 + 64506524322802023105072 0X^5Y^8 + 555944624302357752X^8Y^8 + 2728X^{11}Y^8 + 9882363411841352509440000 0Y^9 - 4974463399905062614720 4X^3Y^9 + 2599709219284278200X^6Y^9 - 1840508903585X^9Y^9 + 413077590081446400XY^{10} + 3140098322119440X^4Y^{10} + 901748705440X^7Y^{10} + 2344386X^{10}Y^{10} + 302197280X^2Y^{11} - 1984268X^5Y^{11} + 2728X^8Y^{11} - X^{11}Y^{11} + Y^{12}$$

Appendix 2 The table of $f_{nm}/\ell \bmod \ell$ for $\ell = 13$.

0	0	12	0	0	1	0	0	5	0	0	5	0	0
0	a	0	0	7	0	0	4	0	0	6	0	0	10
12	0	0	7	0	0	4	0	0	6	0	0	9	0
0	0	7	0	0	4	0	0	6	0	0	9	0	0
0	7	0	0	4	0	0	6	0	0	9	0	0	6
1	0	0	4	0	0	6	0	0	9	0	0	7	0
0	0	4	0	0	6	0	0	9	0	0	7	0	0
0	4	0	0	6	0	0	9	0	0	7	0	0	12
5	0	0	6	0	0	9	0	0	7	0	0	4	0
0	0	6	0	0	9	0	0	7	0	0	4	0	0
0	6	0	0	9	0	0	7	0	0	4	0	0	1
5	0	0	9	0	0	7	0	0	4	0	0	6	0
0	0	9	0	0	7	0	0	4	0	0	6	0	0
0	10	0	0	6	0	0	12	0	0	1	0	0	b

$(a = 116/13, \quad b = 168/13)$

The value $f_{nm}/\ell \bmod \ell$ lies at the intersection of the $(n+1)$-th row and the $(m+1)$-th column.

References

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

[2] D.Cox, Primes of the Form $x^2 + ny^2$, John Wiley & Sons, New York, 1989.

[3] N.D.Elkies, Elliptic and modular curves over finite fields and related computational issues, AMS/IP Studies in Advanced Mathematics **7**, (1998), 21-76.

[4] B.Gross and D.Zagier, On singular moduli, J. Reine Angew. Math. **355** (1985), 191-220.

[5] G.H.Hardy-E.M.Wright, An introduction to the theory of numbers, *Fourth edition*, Oxford Univ. Press, 1960.

[6] Hideji Ito, The Computation of the Modular Equation, Proc. Japan Acad. **71**, Series (**A**) No.3 (1995), 48-50. *II*, Memoirs of the College of Education, Akita Univ. (Natural Sciences) **52** (1997), 1-10.

[7] Hideji Ito, Values of Modular Polynomials modulo primes, Memoirs of the College of Education, Akita Univ. (Natural Sciences) **53** (1998), 17-23.

[8] M.Kaneko, On Ito's observation on coefficients of the modular polynomial, Proc. Japan Acad. **72**, Series (A) (1996), 95-96.

[9] S.Lang, Elliptic Functions, Addison-Wesley, Reading, 1973.

[10] G.Shimura, Introduction to the Arithmetic Theory of Automorphic Forms, Princeton Univ. Press, Princeton, NJ, 1971.

[11] H.Weber, Lehrbuch der Algebra III, Zweite Auflage, Friedr. Vieweg & Sohn, 1908.

Department of Mathematics
Faculty of Education and Humann Studies
Akita University
Akita 010-8502, Japan