Akita University

Memoirs of the Faculty of Education and Human Studies
Akita University (Natural Science)
59, 1−9 (2004)

On Mod p^2 Periodicity of Coefficients of Modular Polynomials of Order p

Hideji ITO

We investigate periodic properties of the coefficients modulo p^2 of modular polynomials of order p of various modular functions which correspond to the conjugacy classes of the Monster simple group.

1 Introduction

Let $j(z)$ be the elliptic modular function and m a natural number. Then $j(z)$ and $j(mz)$ satisfy certain algebraic equation

$$\Phi_m(j(z), j(mz)) = 0.$$

The polynomial $\Phi_m(X,Y) \in \mathbf{Z}[X,Y]$ is called modular polynomial of $j(z)$ of order m and satisfies many properties. In particular, we have the Kronecker congruence relation for rational primes p:

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

We can put $\Phi_p(X,Y) = X^{p+1} + Y^{p+1} + \sum_{0\le n,m\le p} a_{nm}X^nY^m$ $(a_{nm} \in \mathbf{Z})$. In terms of their coefficients a_{nm}, above congruence means $a_{nm} \equiv 0 \pmod{p}$ except when $(n,m) = (1,1), (p,p)$.

In Ito [5], we computed explicit forms of $\Phi_p(X,Y)$ and as a by-product we discovered certain periodic properties of their coefficients when reducing them modulo p^2.

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* $a_{n_1m_1}/p \equiv a_{n_2m_2}/p \pmod{p}$ *for* $p \le 31$, $p = 41, 47, 59, 71$.

We also noted the famous fact that the set $\mathcal{P} = \{\text{primes } p \mid p \le 31,\ p = 41, 47, 59, 71\}$ is precisely the set of primes that divide the order of the Monster simple group $\mathcal{M}$.

Kaneko [8] gave a proof of our observation. Actually what he theoretically showed is to derive our numerical observation from a result of Ogg [10] : *all the supersingular j-invarinats modulo p are $\mathbf{F}_p$-rational if and only if p is contained in $\mathcal{P}$.*

In [6], we investigate the case of $j(z)^{1/3}$ (this has the same modular polynomial as that of $j(3z)^{1/3}$ which corresponds to the conjugacy class $3C$ of $\mathcal{M}$ in the notation of Conway-Norton [1]) and found the same type of periodic property holds for the primes in $\mathcal{P}'_{3C} = \{2, 5, 7, 13, 19, 31\}$. The set $\mathcal{P}_{3C}$ $(= \mathcal{P}'_{3C} \cup \{3\})$ precisely constitute the prime divisors of the order of the centralizer of $3C$.

The purpose of this paper is as follows.

(1) We give an explanation of the periodicity in the case of $j(z)^{1/3}$ just like the one given by Kaneko in the case of $j(z)$.

(2) We investigate (mainly numerically) the case of other modular functions which correspond to conjugacy classes $\mathcal{X}$ of $\mathcal{M}$. Especially we found another kind of periodicity− which we call of $(p+1)$-type − in some cases. (For example, $\mathcal{X} = 2B$ and $p = 7, 13$.)

Partial results and many detailed tables of a_{nm}/p (mod p) etc. can be found in Ito [7].

2 The case of $j(z)$

Our present study stems from the work of Kaneko [8]. So we review his method rather closely in the following four steps.

(1) Transform the polynomial $\Phi_p(X,Y)$ in two variables into the polynomial $R_p(X)$ in one variable :

$$R_p(X) = \frac{1}{p}\Phi_p(X, X^p).$$

By the Kronecker congruence relation, $R_p(X)$ is contained $\mathbf{Z}[X]$. Put $R_p(X) = \sum_{i=0}^{l} d_iX^i$. Then we have

Akita University

(i) $l = p^2 + p - 1$, $d_l = 744$,

(ii) if $k = m + np$ for $0 < m, n < p$, $(m, n) \neq (1, 1)$, then $d_k = a_{nm}$.

Here a_{nm}'s are the coefficients of $\Phi_p(X, Y)$ as in section 1.

(2) Consider the partial fraction expansion of $\frac{R_p(X)}{X^{p^2} - X}$ in $\mathbf{F}_p[X]$. The denominator $X^{p^2} - X$ factors into the product of irreducible polynomials $f(X)$ of $\mathbf{F}_p[X]$ of degree 1 or 2. If $f(X)$ also appears in the factorization of the numerator $R_p(X)$, then $f(X)$ can be cancelled out and $f(X)$ does not appear as one of the denominators in the partial fraction expansion. Now the crucial point is the following.

If the root α of $f(X)$ is not supersingular j-invariant in $\bar{\mathbf{F}}_p$ nor is equal to 0 nor is equal to 1728 (mod p), then we have $R_p(\alpha) = 0$. (That is, $f(X)$ appears in the factorization of $R_p(X)$.)

(An elementary proof of this is given by Kaneko-Zagier [9] p.124.)

So we have

$$\frac{R_p(X)}{X^{p^2} - X} \bmod p = F(X) + \sum_{\alpha \in S_0} \frac{\gamma_\alpha}{X - \alpha}.$$

Here we put $S_0 = \{\text{supersingular } j\text{-invariants } (\neq 0, 1728) \in \overline{\mathbf{F}_p}\}$ and $F(X)$ is a polynomial of degree $p-1$ and $\gamma_\alpha \in \mathbf{F}_p(\alpha)$. Also, we sometimes omit mod p when from the context there arise no misunderstanding.

Hence we can write

$$R_p(X) \bmod p = (X^{p^2} - X)F(X) + (X^{p^2} - X) \sum_{\alpha \in S_0} \frac{\gamma_\alpha}{X - \alpha} \quad \cdots (*)$$

Note that at this stage α is only assumed to be in $\mathbf{F}_{p^2}$ not necessarily in $\mathbf{F}_p$. So if α does not contained in $\mathbf{F}_p$ then the term $\gamma_\alpha/(X - \alpha)$ together with its conjugate over $\mathbf{F}_p$ becomes a fraction whose denominator is some irreducible quadratic polynomial in $\mathbf{F}_p[X]$.

(3) Here enters the assumption: p is in $\mathcal{P} = \{\text{primes } p \mid p \leq 31, p = 41, 47, 59, 71\}$. It is well known that for p in $\mathcal{P}$ all the supersingular j-invariants in characteristic p are $\mathbf{F}_p$-rational and vice versa (Ogg [10] 7-07). Therefore for primes p in $\mathcal{P}$, α's in the formula $(*)$ are actually contained in $\mathbf{F}_p$. That is, $(*)$ holds as an equality in $\mathbf{F}_p(X)$.

(4) The periodic property of a_{nm}/p in the range $0 < n, m < p$, $(n, m) \neq (1, 1)$ is incorporated with that of d_k in the range $p + 1 < k \leq p^2 - 1$. So we can concentrate on the terms

$$(X^{p^2} - X) \sum_{\alpha \in S_0} \frac{\gamma_\alpha}{X - \alpha} \quad \cdots (**)$$

We have

$$\frac{X^{p^2} - X}{X - \alpha} = \frac{X^{p^2} - X}{X^p - X} \frac{X^p - X}{X - \alpha}$$

$$= (1 + X^{p-1} + X^{2(p-1)} + \cdots + X^{p(p-1)}) h_\alpha(X).$$

Here $h_\alpha(X)$ is a polynomial ($\in \mathbf{F}_p[X]$) of degree $\leq p - 1$ and has no constant term because $\alpha \neq 0$. Therefore it holds that

$$(**) = \left(\sum_{\alpha \in S_0} \gamma_\alpha h_\alpha(X)\right)(1 + X^{p-1} + X^{2(p-1)} + \cdots + X^{p(p-1)}).$$

Since $\sum_{\alpha \in S_0} \gamma_\alpha h_\alpha(X)$ is of degree $\leq p - 1$, the coefficients of $(**)$ repeat as those of $\sum_{\alpha \in S_0} \gamma_\alpha h_\alpha(X)$. This proves the periodicity of d_k and hence that of a_{nm}/p (mod p).

In Ito [5], we also make the following observation.

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:

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

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

As to this Kaneko [8] wrote "In conclusion, we remark that the other observation made in § 5 of Ito's paper can also be explained by using the above Key lemma," (this means the formula $(*)$ in (2)), and omitted any detail.

We think it worthwhile to treat these matters in some detail.

Write $\sum_{\alpha \in S_0} \gamma_\alpha h_\alpha(X) = b_1 X + b_2 X^2 + \cdots + b_{p-1} X^{p-1}$. The number $\{b_1, b_2, \ldots, b_{p-1}\}$ repeat itself in the sequence $\{d_k\}$ in the range $p + 1 < k \leq p^2 - 1$.

Akita University

Proposition 2.1. (i) *Let e_α be the order of α in $\mathbf{F}_p^*$. Then the period (=the length of periodic numbers) of $\{b_1, b_2, \ldots, b_{p-1}\}$ divides the least common multiple of e_α for all $\alpha \in S_0$.*

(ii) *We have $b_1 + b_2 + \cdots + b_{p-1} = 0$ in $\mathbf{F}_p$.*

Proof. Suppose first the set S_0 contains only one element α. Set $m = e_\alpha$. Then α satisfies $X^m - 1 = 0$. From $(X^m - 1)/(X - \alpha) = (X^m - \alpha^m)/(X - \alpha)$, we have

$$\frac{b}{X - \alpha} = \frac{b}{X^m - 1}(X^{m-1} + \alpha X^{m-2} + \alpha^2 X^{m-2} + \cdots + \alpha^{m-2} X + \alpha^{m-1}).$$

So, writing as

$$(X^{p^2} - X)\frac{b}{X - \alpha} = \frac{X^{p^2} - X}{X^p - X}\frac{X^p - X}{X^m - 1}\frac{X^m - 1}{X - \alpha} b,$$

we see that the sequence $\{b\alpha^{m-1}, b\alpha^{m-2}, \ldots, b\alpha, b\}$ repeats itself in $\{b_1, b_2, \ldots, b_{p-1}\}$.

When S_0 contains more than one element we add each periodic numbers coming from each $\alpha \in S_0$. This gives us the whole periodic sequence in $\{b_1, b_2, \ldots, b_{p-1}\}$

(2) As in (i) it suffices to treat the case $S_0 = \{\alpha\}$. So we must show that $1 + \alpha + \alpha^2 + \cdots + \alpha^{m-1} = 0$ in $\mathbf{F}_p$. But this is clear from $\alpha^m = 1$ and $\alpha \neq 1$. □

Example 2.2 $p = 13$. We have

$$\frac{R_{13}(X)}{X^{13^2} - X} = 5 + X + 8X^2 + 12X^3 + 5X^4 + X^5 + 8X^6 + 12X^7 + 5X^8 + 4X^9 + 5X^{10} + 10X^{11} + 3X^{12} + \frac{-1}{X - 5}.$$

In characteristic $p = 13$, there is only one supersingular j-invariant: $j = 5$. (See, for example, J.González [4] p.67.) Put $\alpha = 5$ in $\mathbf{F}_{13}^*$. Then we see that the order $e_\alpha = 4$ and $\{5^3, 5^2, 5^1, 1\} = \{8, 12, 5, 1\}$ (modulo 13). This explains the case $p = 13$.

Example 2.3 $p = 17$. We have

$$\frac{R_{17}(X)}{X^{17^2} - X} = 9 + 16X + 2X^2 + 13X^3 + 8X^4 + X^5 + 15X^6 + 4X^7 + 9X^8 + 16X^9 + 2X^{10} + X^{11} + 9X^{12} + 3X^{13} + 16X^{14} + 15X^{15} + 13X^{16} + \frac{4}{X - 8}.$$

In characteristic $p = 17$, the set of supersingular j-invariants is $\{0, 8\}$. We have $e_8 = 8$ and $\{8^i | i = 7, 6, 5, \ldots, 1, 0\} = \{15, 4, 9, 16, 2, 13, 8, 1\}$ (mod 17). Multiplying them by 4 merely causes permutation among them. This explains the case $p = 17$.

Example 2.4 $p = 19$. We have

$$\frac{R_{19}(X)}{X^{19^2} - X} = 1 + 11X + 7X^2 + X^3 + 11X^4 + 7X^5 + X^6 + \cdots + 3X^{18} + \frac{7}{X - 7}.$$

In characteristic $p = 19$, the set of supersingular j-invariants is $\{7, 18\}$. But $18 \equiv 1728 \pmod{19}$. So $S_0 = \{7\}$ in the case $p = 19$. We have $e_7 = 3$ and $\{7^2, 7, 1\} = \{11, 7, 1\} \pmod{19}$.

Example 2.5 $p = 31$. We have

$$\frac{R_{31}(X)}{X^{31^2} - X} = 24 + 3X + 7X^2 + X^3 + 27X^4 + \cdots + 3X^{29} + \frac{20}{X - 4} + \frac{7}{X - 2}.$$

In characteristic $p = 31$, the set of supersingular j-invariants is $\{2, 4, 23\}$. But $23 \equiv 1728 \pmod{31}$. So $S_0 = \{2, 4\}$. We have $e_2 = e_4 = 5$. Hence the period is 5 and a little calculation gives the values of the case $p = 31$.

3 The Case of $j(z)^{1/3}$

Let $\Phi_p^{(3)}(X, Y)$ be the modular polynomial of $j(z)^{1/3}$. (See Ito [6].) Just like $\Phi_p(X, Y)$, $\Phi_p^{(3)}(X, Y)$ satisfies the Kronecker congruence relation. So if we put

$$R_p^{(3)}(X) = \frac{1}{p}\Phi_p^{(3)}(X, X^p),$$

then $R_p^{(3)}(X)$ is contained in $\mathbf{Z}[X]$. In [6] we observed that there is certain priodicity among the coefficients of $\Phi_p^{(3)}(X, Y)$ in some cases. Now we can explain these phenomenon as in the same way as in section 2. Recall that we denote by $\mathcal{P}$ the set of rational primes for which all the supersingular j-invariants in characteristic p are $\mathbf{F}_p$-rational and by S_0 the set {supersingular j-invariants ($\neq 0, 1728$) $\in \overline{\mathbf{F}_p}$}.

Theorem 3.1 *Suppose $p \in \mathcal{P}$ and all the third roots of $j \in S_0$ are $\mathbf{F}_p$-rational. Then the coefficients of $\Phi_p^{(3)}(X, Y)$ have periodic property just like that of $\Phi_p(X, Y)$.*

Proof. We repeat the same argument as in section 2. Suppose α satisfies $\alpha^3 = j \in \mathbf{F}_p$. What we have to do is to show that if j is not supersingular j-invariant

nor 0 nor 1728 (mod p) then we have $R_p^{(3)}(\alpha) = 0$. For that we use the following formula:

$$\Phi_p(X^3, Y^3) = \Phi_p^{(3)}(X, Y)\Phi_p^{(3)}(X, \zeta Y)\Phi_p^{(3)}(X, \zeta^2 Y)$$

where ζ is a primitive third root of 1. (See Elkies [3] p.37 or Ito [6].) By the assumption, we can assume that $p \equiv 1 \pmod 3$. Combining above formula with the next lemma we have the assertion of our theorem.

Lemma 3.2 *Suppose $p \equiv 1 \pmod 3$. Then we have the equality*

$$\Phi_p^{(3)}(X, \zeta X^p)\Phi_p(X, \zeta^2 X^p) = 9X^{2p+2}$$

as functions on $\mathbf{F}_{p^2}$. (In particular $\alpha \neq 0$ never annihilates $\Phi_p^{(3)}(X, \zeta X^p)\Phi_p^{(3)}(X, \zeta^2 X^p)$.)

Proof. Since $p \equiv 1 \pmod 3$ we have $\zeta^p = \zeta$. By the congruence relation

$$\Phi_p^{(3)}(X, Y) \equiv (X^p - Y)(X - Y^p) \pmod p,$$

we have

$$\begin{aligned}
&\Phi_p^{(3)}(X, \zeta X^p)\Phi_p^{(3)}(X, \zeta^2 X^p) \\
&\equiv (X^p - \zeta X^p)(X - \zeta^p X^{p^2})(X^p - \zeta^2 X^p) \\
&\qquad \times (X - \zeta^{2p} X^{p^2}) \pmod p \\
&\equiv X^p(1-\zeta)X(1 - \zeta X^{p^2-1})X^p(1-\zeta^2) \\
&\qquad \times X(1 - \zeta^2 X^{p^2-1}) \pmod p \\
&\equiv (1-\zeta)(1-\zeta^2)X^{2p+2}(1 - \zeta X^{p^2-1}) \\
&\qquad \times (1 - \zeta^2 X^{p^2-1}) \pmod p \\
&\equiv 3X^{2p+2} \\
&\qquad \times (1 - \zeta^2 X^{p^2-1} - \zeta X^{p^2-1} + X^{2p^2-2}) \pmod p \\
&\equiv 3X^{2p}(X^2 + X^{p^2+1} + X^{2p^2}) \pmod p \\
&= 3X^{2p}(X^2 + X^2 + X^2) \text{ (as functions on } \mathbf{F}_{p^2}) \\
&= 9X^{2p+2}
\end{aligned}$$

(We use the relation $X^{p^2} = X$ when we consider both sides as functions on $\mathbf{F}_{p^2}$ in the last but one line.) □

The primes in $\{13, 19, 31\}$ satisfy the assumption of the theorem as the following table shows.

p	supersingular j-invariant	$j^{1/3} \pmod p$
13	5	7, 8, 11
19	7	4, 6, 9
	18($\equiv 1728 \bmod 19$)	8, 12, 18
31	2	4, 7, 20
	4	16, 18, 28
	23($\equiv 1728 \bmod 31$)	12, 21, 29

Explicit forms of $R_p^{(3)}(X)/(X^{p^2} - X) \mod p$ are given as follows.

$p = 13$.

$$10X + 6X^4 + 12X^7 + X^{10} + \frac{12}{X+2} + \frac{10}{X+5} + \frac{4}{X+6}$$

$p = 19$.

$$3X + 10X^4 + 16X^7 + 12X^{10} + 13X^{13} + X^{16} + \frac{4}{X+10} + \frac{6}{X+13} + \frac{9}{X+15}$$

$p = 31$.

$$30X + 2X^4 + 24X^7 + 14X^{10} + 15X^{16} + 22X^{19} + X^{22} + X^{25} + \frac{2}{X+11} + \frac{19}{X+24} + \frac{10}{X+27} + \frac{8}{X+15} + \frac{9}{X+3} + \frac{14}{X+13}$$

4 The case of $t_{\ell B}$ $(\ell = 2, 3, 5)$

We use the notation of Conway-Norton [1]. The conjugacy classes of ℓB $(\ell = 2, 3, 5, 7, 13)$ correspond to modular functions $t_{\ell B}$. Explicitly they are given as

$$t_{\ell B}(z) = \left(\frac{\eta(z)}{\eta(\ell z)}\right)^{\frac{24}{(24, \ell-1)}}$$

where $\eta(z)$ is the Dedekind eta function. For above values of ℓ, ℓB corresponds to $\Gamma_0(\ell)$ and $X_0(\ell)$ is of genus 0 (notations being the standard one). So $j(z)$ can be written by $t_{\ell B}$. Explicit forms of them can be gotten, for example, as follows. Taking into consideration of poles and degrees ($[\mathrm{SL}_2(\mathbf{Z}) : \Gamma_0(\ell)] = \ell + 1$), we can write $j(z) = (t_{\ell B}^{\ell+1} + a t_{\ell B}^{\ell} + \cdots + b)/(t_{\ell B})^{\ell}$. Substitute q-expansions of $j(z)$ and $t_{\ell B}$ and compare their coefficients. (The explicit forms of them are given in appendix.)

Rewriting above formula we obtain the defining equation of $t_{\ell B}$ over $\mathbf{Q}(j(z))$, which we denote by $f_{\ell B}(X, j) = 0$. For example,

$$f_{2B}(X, j) = X^3 + (2^8 3 - j)X^2 + 2^{16} 3X + 2^{24}.$$

One may notice that the constant term of $f_{\ell B}$ is of the form ℓ^m and the exponent m is a multiple of ℓ. This is true in general and is proved by J.González [4] (Theorem 2.1) in more precise form.

Now $t_{\ell B}$ has modular equations (Cummins-Gannon [2]) which we denote as

$$\Phi_p^{(\ell B)}(X, Y) = 0.$$

As the cases of $j(z)$ and $j(z)^{1/3}$ suggest, we are led to consider whether coefficients of $\Phi_p^{(\ell B)}(X,Y)$ have periodic property modulo p^2 or not for those values of p which divide the order of centralizer of the conjugacy classe ℓB in $\mathcal{M}$.

By computing their explicit forms we have several observations. As before S_0 is the set of supersingular j-invariant ($\neq 0, 1728$) in characteristic in p. Put $R_p^{(\ell B)}(X) = \frac{1}{p}\Phi_p^{(\ell B)}(X, X^p)$.

Observation 1. *Coefficients of* $R_p^{(\ell B)}(X) \bmod p$ *have periodic property if all the following assumptions hold*:

(i) *all the supersingular* j*-invariants in* S_0 *are* $\mathbf{F}_p$*-rational,*

(ii) *if* $j \in S_0$, *then* $f_{\ell B}(X, j) \bmod p$ *factors as*

$$f_{\ell B}(X,j) \equiv (X-\alpha)(X-\beta)(X-\gamma) \pmod p \quad (\alpha,\beta,\gamma \in \mathbf{F}_p),$$

(iii) *if* $j = 0$ *or* $j \equiv 1728 \bmod p$ *is supersingular* j*-invariant in characteristic* p, *then* $f(X,0) \bmod p$ *or* $f(X,1728) \bmod p$ *havs a multiple factor* $X-\delta$ *of degree one* ($\delta \in \mathbf{F}_p$).

To express it more explicitly, under these assumptions, numerial examples show that we have partial fraction expansion of the following form:

$$\frac{R_p^{(\ell B)}(X)}{X^{p^2}-X} \bmod p$$
$$= F(X) + \frac{s_\alpha}{X-\alpha} + \frac{s_\beta}{X-\beta} + \frac{s_\gamma}{X-\gamma} + \frac{s_\delta}{X-\delta} + \cdots.$$

Here $F(X)$ is a polynomial $\in \mathbf{F}_p[X]$ of degree $p-1$ and s_α etc. are contained in $\mathbf{F}_p$.

Observation 2. *Let* a_{nm} *be the coefficients of* X^nY^m *in* $\Phi_p^{(\ell B)}(X,Y)$. *In some cases there is another type of periodicity among* a_{nm} :

$$\text{if } n_1 - m_1 = n_2 - m_2 \text{ then } \frac{a_{n_1 m_1}}{p} \equiv \frac{a_{n_2 m_2}}{p} \pmod p$$

for $0 < n_i, m_i < p$, $(n_i, m_i) \neq (1,1)$ $(i = 1,2)$.

Later we give an explanation of the origin of this phenomenon. Considering that we call this type of periodicity of $(p+1)$-type, while the previous one is to be called normal type or $(p-1)$-type.

In the following we denote by $\mathcal{P}_{\ell B}$ the set of prime divisors of the order of $C_{\mathcal{M}}(\ell B)$ (the centralizer of ℓB in $\mathcal{M}$).

Example 4.1 $t_{2B} = \eta(z)^{24}/\eta(2z)^{24}$, $\mathcal{P}_{2B} = \{2,3,5,7,11,13,23\}$.

$\boldsymbol{p=7}$. $j = 6(\equiv 1728 \pmod 7)$ is the only supersingular j-invariant in characteristic $p = 7$.

$$f_{2B}(X,6) \equiv (X+1)(X+6)^2 \pmod 7$$
$$R_7^{(2B)}(X)/(X^{7^2}-X) \equiv 4+4X+4X^2+4X^3+4X^4+4X^5+4X^6+\frac{4}{X+6} \pmod 7$$

$\boldsymbol{p=11}$. $j = 0$ and $j = 1(\equiv 1728 \bmod 11)$ are the supersingular j-invariants in characteristic $p = 11$.

$$f_{2B}(X,0) \equiv (X+3)^3 \pmod{11}$$
$$f_{2B}(X,1) \equiv (X+9)(X+5)^2 \pmod{11}$$
$$R_{11}^{(2B)}(X)/(X^{11^2}-X) \equiv 9+6X+5X^2+5X^3+8X^4+2X^5+5X^6+6X^7+6X^8+3X^9+9X^{10}+\frac{5}{X+3}+\frac{9}{X+5} \pmod{11}$$

$\boldsymbol{p=23}$. $j = 0$ and $j = 3(\equiv 1728 \pmod{23})$ and $j = 19$ are the supersingular j-invariants in characteristic $p = 23$.

$$f_{2B}(X,0) \equiv (X+3)^3 \pmod{23}$$
$$f_{2B}(X,3) \equiv (X+18)(X+17)^2 \pmod{23}$$
$$f_{2B}(X,19) \equiv (X+5)(X+15)(X+16) \pmod{23}$$
$$R_{23}^{(2B)}(X)/(X^{23^2}-X) \equiv 22+3X+11X^2+3X^3+19X^4+15X^5+10X^6+\cdots+22X^{22}+\frac{18}{X+3}+\frac{8}{X+5}+\frac{1}{X+15}+\frac{2}{X+17}+\frac{6}{X+16} \pmod{23}$$

Example 4.2 (periodic of $(p+1)$-type) t_{2B}, $p = 13$.

$j = 5(\not\equiv 1728 \pmod{13})$ is the only supersingular j-invariant in characteristic $p = 13$.

$$f_{2B}(X,5) \equiv (X+1)(X^2+8X+1) \pmod{13}$$
$$R_{13}^{(2B)}(X)/(X^{13^2}-X) \equiv 2+5X+12X^2+X^3+8X^4+11X^5+10X^6+11X^7+8X^8+X^9+12X^{10}+5X^{11}+2X^{12}+\frac{9}{X+1}+\frac{7X+2}{X^2+8X+1} \pmod{13}$$

From this we see that $R_{13}^{(2B)}(X)$ has no periodicity of normal type among its coefficients. But by direct calculation, one knows they have periodicity of $(p+1)$-type. We can give an explanation as in the next proposition.

Like before ($\mathcal{X} = 2B$), for a conjugacy class of $\mathcal{X}$ of $\mathcal{M}$, we denote by $\Phi_p^{(\mathcal{X})}(X,Y)$ corresponding modular polynomial and by e_α the order of α in $\overline{\mathbf{F}}_p^*$.

Proposition 4.3 *Suppose the partial fraction expansion of* $\frac{1}{p}\Phi_p^{(\mathcal{X})}(X, X^p)/(X^{p^2} - X) \mod p$ *has a term whose denominator* $g(X)$ *is an irreducible polynomial of degree* 1 *or* 2 *in* $\mathbf{F}_p[X]$. *Let* $\alpha(g)$ *be a root of* $g(X) = 0$. *If the* $e_{\alpha(g)}$ *for all* $g(X)$*'s divide* $p+1$, *then the coefficients* (mod p^2) *of* $\Phi_p^{(\mathcal{X})}(X, Y)$ *have periodic property of* $(p+1)$*-type.*

Proof. Recall the argument in section 2. We have only to deal with the case of $\deg g(X) = 2$. So we have $X^{p+1} - 1 = g(X)h(X)$ for some polynomial $h(X)$ in $\mathbf{F}_p[X]$ of degree $p-1$. Write as follows:

$$\frac{X^{p^2} - X}{g(X)} = \frac{X^{p^2} - X}{X^{p+1} - 1} \cdot \frac{X^{p+1} - 1}{g(X)}$$
$$= X(1 + X^{p+1} + X^{2(p+1)} + \cdots + X^{(p-2)(p+1)}) \cdot h(X).$$

From this we have periodicity modulo $p+1$ among coefficients of $\frac{1}{p}\Phi_p^{(\mathcal{X})}(X, X^p)$ just like in section 2. Also note that if $k = m + np$ then $k = m + n((p+1) - 1) \equiv m - n \pmod{(p+1)}$. Hence we have our assertion. □

Example 4.2 (Continued.) The case of $\mathcal{X} = 2B$ and $p = 13$. $j = 5$ is the only supersingular j-invariant in characteristic $p = 13$. Suppose α satisfies $\alpha^2 + 8\alpha + 1 \equiv 0 \pmod{13}$. Then $\alpha^2 = -8\alpha - 1$ in $\mathbf{F}_{13}^*$. We compute $\alpha^7 \equiv -1 \pmod{13}$. So $e_\alpha = 14$ in accordance with proposition 4.3.

Example 4.4 The case of $\mathcal{X} = 3B$. $\mathcal{P}_{3B} = \{2, 3, 5, 7, 11, 13\}$.

$p = 5$. (periodic of normal type)

$f_{3B}(X, 0) \equiv (X+2)(X+3)^2 \pmod 5$.

$R_5^{(3B)}(X)/(X^{5^2} - X) \equiv 3 + 4X + 2X^2 + X^3 + 3X^4 + \frac{1}{X+3} \pmod 5$.

$p = 7$.

$f_{3B}(X, 6) \equiv (1 + 4X + X^2)^2 \pmod 7$.

$R_7^{(3B)}(X)/(X^{7^2} - X) \equiv 2 + 5X^2 + X^3 + 5X^4 + 2X^6 + \frac{5+6X}{1+4X+X^2} \pmod 7$.

If α is a root of $1 + 4X + X^2 \equiv 0 \pmod 7$ then by calculation we see $e_\alpha = 8$. So in this case we have periodicity of $(p+1)$-type.

$p = 11$.

$f_{3B}(X, 0) \equiv (X+1)^3(X+5) \pmod{11}$.

$f_{3B}(X, 1) \equiv (X+3)^2(X+6)^2 \pmod{11}$.

$R_{11}^{(3B)}(X)/(X^{11^2} - X) \equiv 10 + 7X^2 + 3X^3 + \cdots + 10X^{10} + \frac{4}{X+1} + \frac{3}{X+3} + \frac{9}{X+6} \pmod{11}$.

So in this case we have periodicity of normal type.

$p = 13$.

$f_{3B}(X, 5) \equiv (1 + 3X + X^2)(1 + 7X + X^2) \pmod{13}$.

$R_{13}^{(3B)}(X)/(X^{13^2} - X) \equiv 1 + 9X + 2X^2 + \cdots + X^{12} + \frac{4+3X}{1+7X+X^2} + \frac{8+X}{1+3X+X^2} \pmod{13}$.

If α is a root of $1 + 7X + X^2 \equiv 0 \pmod{13}$ then by calculation we see $e_\alpha = 14$. Also if β is a root of $1 + 3X + X^2 \equiv 0 \pmod{13}$ then we see $e_\beta = 7$. So in this case we have periodicity of $(p+1)$-type.

$p = 17$. (We include this case to contrast against above examples.)

$f_{3B}(X, 0) \equiv (5+X)^3(10+X) \pmod{17}$.

$f_{3B}(X, 8) \equiv (3+X)(7+X)(15+7X+X^2) \pmod{17}$.

$R_{17}^{(3B)}(X)/(X^{17^2} - X) \equiv 5 + X + 7X^2 + \cdots + 5X^{16} + \frac{8}{7+X} + \frac{1}{5+X} + \frac{-1}{3+X} + \frac{7+2X}{15+7X+X^2} \pmod{17}$.

If α is a root of $15 + 7X + X^2 \equiv 0 \pmod{17}$ then by calculation we see $e_\alpha = 48$ and 48 is not a divisor of $p+1 = 18$. So in this case we have no periodicity (neither normal nor $(p+1)$-type). Indeed, we can see that by direct calculation of $\Phi_{17}^{(3B)}(X, Y)$.

Example 4.5 The case of $\mathcal{X} = 5B$. $\mathcal{P}_{5B} = \{2, 3, 5, 7\}$.

When $p = 7$, there is no periodicity, while when $p = 11 (\notin \mathcal{P}_{5B})$ we have periodicity of normal type. This means strict analogy with the case of $j(z)$ or $j(z)^{1/3}$ cannot hold in general.

$R_7^{(5B)}(X)/(X^{7^2} - X) \equiv 1 + X + 5X^2 + 5X^4 + 6X^5 + X^6 + \frac{1+4X}{6+4X+X^2} \pmod 7$.

$f_{5B}(X, 6) \equiv (6 + X + X^2)(6 + 4X + X^2)^2 \pmod 7$.

$R_{11}^{(5B)}(X)/((X^{11^2} - X) \equiv 5 + X + 4X^2 + X^3 + 8X^4 + \cdots + 5X^{10} + \frac{9}{X+2} + \frac{9}{X+6} + \frac{3}{X+8} + \frac{4}{X+9} \pmod{11}$.

$f_{5B}(X, 0) \equiv (X+2)^3(X+6)^3 \pmod{11}$.

$f_{5B}(X, 1) \equiv (X+8)^2(X+9)^2(X^2+4) \pmod{11}$.

5 The Case of $t_{\ell A}$ $(\ell = 2, 3, 5, 7)$

By explicit calculation, we observe that the coefficients of $\Phi_p^{(\ell A)}(X, Y)$ have periodic property of normal type for all $p \neq \ell$ in $\mathcal{P}_{\ell A}$. (Well, for $p = 2, 3$, periodic property is trivial matter. So we disregard them here and in fact we already do so.)

But we are unable to give a theoretical explanation nor give a formulation like before. Nonetheless it seems some relation exists between periodicity and supersingular j-invariants. Next example is a typical one.

Example 5.1 The case of $t_{2A} = t_{2B} + 4096/t_{2B}$. $\mathcal{P}_{2A} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 31, 47\}$.

The class $2A$ corresponds to $X_0(2)^+ = X_0(2)/w_2$, where w_2 is the Fricke involution coming from the linear fractional transformation $\begin{pmatrix} 0 & -1 \\ 2 & 0 \end{pmatrix}$ on the upper half plane. The elliptic modular function $j(z)$ cannot be expressed in t_{2A} alone but we have

$$j + j|w_2 = (t_{2A})^2 + 49t_{2A} - 2^9 13.$$

Now $j|w_2 = j(2z)$. We know $j(z)$ and $j(2z)$ satisfy the modular equation $\Phi_2(X, Y) = 0$. Put $g_{2A}(X, j) = \Phi_2(j, X^2 + 49X - 2^9 13 - j)$. This is contained in $\mathbf{Z}[X, j]$. Also we put $R_p^{(2A)}(X) = \frac{1}{p}\Phi_p^{(2A)}(X, X^p)$. When $p = 5, 7$ we have $a_{nm}/p \equiv 0 \pmod{p}$ for n, m in the usual range.

$(R_p^{(2A)}(X)/(X^{p^2} - X) \bmod p$ is a polynomial for $p = 5, 7$.)

$p = 11$.

$$R_{11}^{(2A)}(X)/(X^{11^2} - X) \equiv 10 + 8X + X^2 + \cdots + 9X^{10} + \frac{1}{8 + X} \pmod{11}$$

$$g_{2A}(X, 0) \equiv (X + 8)^6 \pmod{11}$$

$$g_{2A}(X, 1) \equiv (X + 7)(X + 8)^4(X + 9) \pmod{11}$$

$p = 13$.

$$R_{13}^{(2A)}(X)/(X^{13^2} - X) \equiv 9 + 11X + X^2 + \cdots + 2X^{12} + \frac{11}{8 + X} \pmod{13}$$

$$g_{2A}(X, 5) \equiv (X + 2)^3(X + 8)^3 \pmod{13}$$

$p = 17$.

$$R_{17}^{(2A)}(X)/(X^{17^2} - X) \equiv 2 + 6X + 3X^2 + \cdots + 10X^{16} + \frac{1}{X} + \frac{1}{13 + X} \pmod{17}$$

$$g_{2A}(X, 0) \equiv X^3(X + 15)^3 \pmod{17}$$

$$g_{2A}(X, 8) \equiv X(X + 2)^2(X + 13)^2(X + 15) \pmod{17}$$

$p = 19$.

$$R_{19}^{(2A)}(X)/(X^{19^2} - X) \equiv 4 + 8X + 17X^2 + \cdots + 14X^{18} + \frac{15}{9 + X} + \frac{6}{12 + X} \pmod{19}$$

$$g_{2A}(X, 18) \equiv (X + 12)^2(X + 14)(X + 16)(X + 18)^2 \pmod{19}$$

$$g_{2A}(X, 7) \equiv (X + 2)^2(X + 9)^2(X + 12)^2(X + 18)^2 \pmod{19}$$

So it seems some relation exists between the denominators of the partial fraction expansion of $R_p^{(2A)}(X)/(X^{p^2} - X) \bmod p$ and the factorizations of $g_{2A}(X, j) \bmod p$ where j is a supersingular j-invariant. (In cases $p = 23, 31, 47$, we have similar phenomena.) Why those particular factors appear in the denominator is a problem we must solve.

We also note that in case $\mathcal{X} = 5A$, $p = 13$, there occurs periodicity of normal type even though $p = 13$ is not contained in $\mathcal{P}_{5A}$. Taking the Example 4.5 also into account, we realize that things are not so simple as we first imagined them to be.

References

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

[2] C.J.Cummins and T.Gannon, Modular equations and the genus zero properties of moonshine functions, Invent.math. **129** (1997), 413-443.

[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] J.González, On the j-invariants of the quadratic $\mathbf{Q}$-curves, J.London Math.Soc. (2) **63** (2001), 52-68.

[5] Hideji Ito, Computation of the Modular Equation, Proc. Japan Acad. **71**, Series (A) No.3 (1995), 48-50.

[6] Hideji Ito, On the Modular Equation of $j(z)^{1/3}$, Memoirs of the Faculty of Education and Human Studies, Akita Univ. (Natural Sciences) **56** (2001), 36-42.

Akita University

[7] Hideji Ito, モジュラー方程式と楕円曲線の研究 (Report on modular equations and elliptic curves), 科学研究費補助金基盤研究 C(2) 研究成果報告書 (2002), pp.101. (*In Japanese.*)

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

[9] M.Kaneko and Zagier, Supersingular j-invariants, hypergeometric series, and Atkin's orthogonal polynomials, AMS/IP Studies in Advanced Mathematics **7** (1998), 97-126.

[10] A.P.Ogg, Automorphismes de Courbes Modulaires, Sém. Delange-Pisot-Poitou, 16e année. **7** (1975), 1-8.

Appendix 1. Two examples of periodicity of coefficients of modular polynomials

(1) The case of $j(z)$ $(p = 13)$ (normal type)
The values of $(a_{ik}/13) \pmod{13}$ of $\Phi_{13}(X, Y)$.

$\frac{168}{13}$	3	10	5	4	5	12	8	1	5	12	8	1	2
3	12	8	1	5	12	8	1	5	12	8	1	5	2
10	8	1	5	12	8	1	5	12	8	1	5	12	3
5	1	5	12	8	1	5	12	8	1	5	12	8	10
4	5	12	8	1	5	12	8	1	5	12	8	1	0
5	12	8	1	5	12	8	1	5	12	8	1	5	0
12	8	1	5	12	8	1	5	12	8	1	5	12	0
8	1	5	12	8	1	5	12	8	1	5	12	8	0
1	5	12	8	1	5	12	8	1	5	12	8	1	0
5	12	8	1	5	12	8	1	5	12	8	1	5	0
12	8	1	5	12	8	1	5	12	8	1	5	12	0
8	1	5	12	8	1	5	12	8	1	5	12	8	0
1	5	12	8	1	5	12	8	1	5	12	8	$\frac{12}{13}$	0
2	2	3	10	0	0	0	0	0	0	0	0	0	0

The value of $(a_{ik}/13) \pmod{13}$ lies at the intersection of the $(14-i)$-th row and the $(14-k)$-th column.

(2) The case of t_{2B} $(p = 13)$ $((p+1)$-type)
The values of $(b_{ik}/13) \pmod{13}$ of $\Phi_{13}^{(t_{2B})}(X, Y)$.

$\frac{168}{13}$	2	5	12	1	8	11	10	11	8	1	12	5	0
2	3	2	5	12	1	8	11	10	11	8	1	12	0
5	2	3	2	5	12	1	8	11	10	11	8	1	0
12	5	2	3	2	5	12	1	8	11	10	11	8	0
1	12	5	2	3	2	5	12	1	8	11	10	11	0
8	1	12	5	2	3	2	5	12	1	8	11	10	0
11	8	1	12	5	2	3	2	5	12	1	8	11	0
10	11	8	1	12	5	2	3	2	5	12	1	8	0
11	10	11	8	1	12	5	2	3	2	5	12	1	0
8	11	10	11	8	1	12	5	2	3	2	5	12	0
1	8	11	10	11	8	1	12	5	2	3	2	5	0
12	1	8	11	10	11	8	1	12	5	2	3	2	0
5	12	1	8	11	10	11	8	1	12	5	2	$\frac{38}{13}$	0
0	0	0	0	0	0	0	0	0	0	0	0	0	0

The value of $(b_{ik}/13) \pmod{13}$ lies at the intersection of the $(14-i)$-th row and the $(14-k)$-th column. (Here b_{nm} is the coefficient of $X^n Y^m$ in $\Phi_{13}^{(2B)}(X, Y)$.)

Appendix 2. Explicit forms of $j(z)$ in $t_{\ell B}$

In the following we write t_ℓ in place of $t_{\ell B}$ for short.

$$
\begin{aligned}
j(z) &= \frac{t_2^3 + 2^8 3 t_2^2 + 2^{16} 3 t_2 + 2^{24}}{(t_2)^2} \\
&= \frac{(t_2 + 2^8)^3}{(t_2)^2} \\
&= \frac{t_3^4 + 2^2 3^3 7 t_3^3 + 2 \cdot 3^9 5 t_3^2 + 2^2 3^{14} t_3 + 3^{18}}{(t_3)^3} \\
&= \frac{(t_3 + 3^3)(t_3 + 3^5)^3}{(t_3)^3} \\
&= \frac{h_5(t_5)}{(t_5)^5} \\
&= \frac{h_7(t_7)}{(t_7)^7} \\
&= \frac{h_{13}(t_{13})}{(t_{13})^{13}}
\end{aligned}
$$

$$
\begin{aligned}
h_5(t) &= t^6 + 2\cdot 3\cdot 5^3 t^5 + 3^2 5^5\, 7t^4 + 2^2 5^8 13 t^3 \\
&\quad + 3^2 5^{10} 7 t^2 + 2\cdot 3\cdot 5^{13} t + 5^{15} \\
&= (t^2 + 2\cdot 5^3 t + 5^5)^3
\end{aligned}
$$

$$
\begin{aligned}
h_7(t) &= t^8 + 2^2 11\cdot 17 t^7 + 2\cdot 7^4 41 t^6 + 2^4 7^6 11 t^5 \\
&\quad + 5\cdot 7^7 13^2 t^4 + 2^4 7^9 17 t^3 + 2\cdot 7^{11} 23 t^2 \\
&\quad + 2^2 7^{13} t + 7^{14} \\
&= (t^2 + 13t + 7^2)(t^2 + 5\cdot 7^2 t + 7^4)^3
\end{aligned}
$$

$$
\begin{aligned}
h_{13}(t) &= t^{14} + 2\cdot 373 t^{13} + 5\cdot 13^2 233 t^{12} + 2^2 7^4 13^3 t^{11} \\
&\quad + 2^3 7\cdot 13^4 487 t^{10} + 2^2 5\cdot 11^2 13^5 17 t^9 \\
&\quad + 2\cdot 11\cdot 13^7 137 t^8 + 2^2 5\cdot 13^7 1283 t^7 \\
&\quad + 2\cdot 13^8 6043 t^6 + 2^2 5\cdot 11\cdot 13^9 19 t^5 \\
&\quad + 2^3 7\cdot 13^{10} 19 t^4 + 2^2 7^2 13^{11} t^3 \\
&\quad + 5^2 13^{12} t^2 + 2\cdot 13^{13} t + 13^{13} \\
&= (t^2 + 5t + 13) \\
&\quad \times (t^4 + 13\cdot 19 t^3 + 2^2 5\cdot 13^2 t^2 + 7\cdot 13^3 t + 13^4)^3
\end{aligned}
$$

DEPARTMENT OF MATHEMATICS
FACULTY OF EDUCATION AND HUMAN STUDIES
AKITA UNIVERSITY
AKITA 010-8502, JAPAN
E-mail : itoh@math.akita-u.ac.jp