Memoirs of the Faculty of Education and Human Studies
Akita University (Natural Science)
63, 15 - 19 (2008)

Roots of One Parameter Modular Equations of $j(z)$

Hideji Ito*

We make experimental observation about one parameter modular equations $\Phi_p(X, X^p) = 0$ of the elliptic modular function $j(z)$, especially about their factorizations and behavior of their roots.

1 Introduction

The classical elliptic modular function $j(z)$ satisfies the so-called modular equation

$$\Phi_n(j(z), j(nz)) = 0,$$

for each natural number n, where the $\Phi_n(X, Y)$ are certain polynomials with gigantic coefficients (for large n) in $\mathbf{Z}[X, Y]$. An estimate of the magnitude of coefficients is given by P.Cohen [2]. Hereafter we consider the case $n = p$ (odd prime) exclusively unless othewise explicitly stated.

There is a long history of explicit calculation of modular polynomials $\Phi_p(X, Y)$. I myself computed them for all $p < 200$ around 2000. It seems the most extensive calculation was done by M.Rubinstein (with the aid from G.Seroussi) as far as $p < 360$. The result is on the web [11], although the method of calculation is apparently not published yet. More recently an entirely different method is given by Charles and Lauter [1]. They don't use q-expansions of $j(z)$ but rely on the grapf of supersigular elliptic curves over finite fields. (They even made their algorithm a US patent. [4])

Now putting $Y = X^p$ in $\Phi_p(X, Y)$, we get polynomials in one variable $\Phi_p(X, X^p)$. In this paper, we will call them one parameter modular polynomials and the equation $\Phi_p(X, X^p) = 0$ will be called one parameter modular equation. This is the object of study in this paper.

Explicitly, set $\Phi_p(X,Y) = X^{p+1} + Y^{p+1} + \sum a_{ik} X^i Y^k$, and $\Phi_p(X, X^p) = \sum d_k X^k$. Then we readly have

(i) $\deg \Phi_p(X, X^p) = p^2 + p - 1$,
$d_{p^2+p-1} = 744 \times p$

(ii) if $k = n + mp\,(m = 0$ or $0 < n, m < p$, $(n, m) \neq (1, 1))$, then we have $d_k = a_{nm}$; also we have $d_{p+1} = a_{11} + 1$, $d_{kp} = a_{p,k-1} + a_{0,k}$ $(1 \leq k \leq p)$.

They are used by Kaneko [10] to give a reduction of my observation [5] to yet another numerical facts. But he considered them solely in characteristic p. In contrast we consider them primarily over $\mathbf{C}$, the usual complex number field.

Our present study begins with the investigation of the magnitude of coefficients a_{nm}. Actually the biggest coefficient is usally a_{00} when it is not 0. When a_{00} is 0, the biggest one is a_{20} or $a_{1,1}$. See the table in the appendix 1. With our aim in mind, we are led to examine the solutions of $\Phi_p(X, X^p) = 0$, because the coefficients of a polynomial $f(X)$ in one variable are closely related with the solutions of the equation $f(X) = 0$ and the d_k and the a_{nm} are much the same as noted in (ii) above. By numerical and graphical calculation on computer we found that very striking patterns would emerge. As yet, we are unable to give proof of our observations. But I think it worthwhlie to record them here to allow everyone interested to examine our findings and pursue the investigation.

Most parts of the present paper were first reported in [8] which was written in Japanese. It contains the graphics of the distribution of roots of $\Phi_p(X, X^p) = 0$ for $p \leq 61$ and numerous tables of computed values relevant to our theme.

* The author was partially supported by Grant-in-Aid for Scientific Research (C)(2), No.1264007, Japan Society for the Promotion of Science.

2 Facterization of $\Phi_p(X, X^p)$

Let $\Phi_p^{(3)}(X, Y)$ be the modular polynomial of $j(z)^{1/3}$ which is a modular function with respect to $\Gamma(3)$ (see Ito [6]). Using it, we have a factorization of $\Phi_p(X, X^p)$ as follows.

Theorem 2.1

(i) *If* $p \equiv 1 \pmod 6$, *then we have*

$$\Phi_p(X, X^p) = pX^2 F_p(X) G_p(X)$$

Here F_p, $G_p \in \mathbf{Z}[X]$ *are determined by*

$$\Phi_p^{(3)}(X, X^p) = pX^2 F_p(X^3),$$
$$\Phi_p^{(3)}(X, \zeta X^p)\Phi_p^{(3)}(X, \zeta^2 X^p) = X^4 G_p(X^3),$$

where ζ *is a third root of unity*($\neq 1$) *and we have*

$$\deg F_p(X) = (1/3)(p^2 + p - 5),$$
$$\deg G_p(X) = (2/3)(p^2 + p - 2).$$

(ii) *If* $p \not\equiv 1 \pmod 6$, *then we have*

$$\Phi_p(X, X^p) = p\tilde{F}_p(X)\tilde{G}_p(X)$$

Here $\tilde{F}_p$, $\tilde{G}_p \in \mathbf{Z}[X]$ *are determined by*

$$\Phi_p^{(3)}(X, X^p) = p\tilde{F}_p(X^3),$$
$$\Phi_p^{(3)}(X, \zeta X^p)\Phi_p^{(3)}(X, \zeta^2 X^p) = \tilde{G}_p(X^3),$$

and we have

$$\deg \tilde{F}_p(X) = (1/3)(p^2 + p - 3),$$
$$\deg \tilde{G}_p(X) = (2/3)(p^2 + p).$$

Proof. We first recall the relation

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

(See Elkies [3] or Ito [6].) Since the polynomial $\Phi_p^{(3)}(X, \zeta Y)\Phi_p^{(3)}(X, \zeta^2 Y)$ is invariant under the galois action of $\mathbf{Q}(\zeta) = \mathbf{Q}(\sqrt{-3})$ it is contained in $\mathbf{Z}[X, Y]$. Put $\Phi_p^{(3)}(X, Y) = X^{p+1} + Y^{p+1} + \sum_{a,b=0}^{p} f_{ab} X^a Y^b$. We know $f_{ab} = 0$ unless $a + pb \equiv p + 1 \pmod 3$. (See ibd.) So if we put $Y = X^p$, we have

$$\Phi_p^{(3)}(X, X^p) = X^{p+1} + X^{p(p+1)} + \sum_{a,b=0}^{p} f_{ab} X^{a+pb}$$

$$= X^{p+1} + \sum f_{ab} X^{a+pb}$$

Here in the sum the pair (a, b) runs through the range $0 \leq a, b \leq p$ with the condition $a + pb \equiv p + 1 \pmod 3$, $(a, b) \neq (0, 0)$. (Note that $f_{pp} = -1$.)

Suppose $p \equiv 1 \pmod 6$. Then we have $f_{00} = 0$ and $f_{1,0} = 0$. So we obtain

$$\Phi_p^{(3)}(X, X^p) = X^2(X^{p-1} + \sum f_{ab} X^{a+pb-2})$$

Since $p - 1 \equiv a + pb - 2 \equiv 0 \pmod 3$, we can write $\Phi_p^{(3)}(X, X^p) = X^2 S(X^3)$ for some polynomial $S(X) \in \mathbf{Z}[X]$. Also congruence relation $\Phi_p(X, Y) \equiv (X^p - Y)(X - Y^p) \pmod p$ gives us $\Phi_p^{(3)}(X, X^p) \equiv 0 \pmod p$. Hence we get the final form $\Phi_p^{(3)}(X, X^p) = pX^2 F_p(X^3)$ for some polynomial $F_p(X) \in \mathbf{Z}[X]$.

Also from this we easily see that we can write $\Phi_p^{(3)}(X, \zeta X^p)\Phi_p^{(3)}(X, \zeta^2 X^p) = X^4 G_p(X^3)$ for some $G_p(X) \in \mathbf{Z}[X]$. As for degrees of $F_p(X)$ and $G_p(X)$, note that $\Phi_p^{(3)}(X, X^p) = p^2 + p - 3$.

The case $p \not\equiv 1 \pmod 6$, that is, $p \equiv 2 \pmod 3$ can be dealt with similarly.

Computer calculation indicates that the polynomails $F_p(X)$, $G_p(X)$, $\tilde{F}_p(X)$ and $\tilde{G}_p(X)$ are always irreducible over $\mathbf{Z}$.

3 Distribution of the roots

Figure 1 shows the distribution of most roots of $\Phi_{37}(X, X^{37}) = 0$.

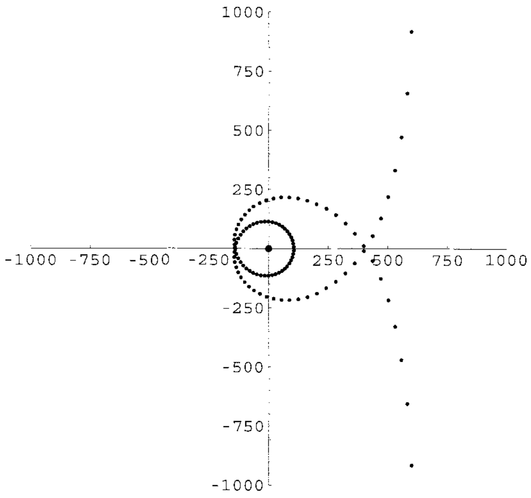

Figure 1: *Distribution of roots of* $\Phi_{37}(X, X^{37}) = 0$ (almost all)

The figure strongly suggests the existence of what we might call the "root curve" of $\Phi_{37}(X, X^{37}) = 0$. The roots not appearing in the figure are 6 in number and it seems they sit on the extension of the branch of the root curve.

Near the origin a lot of roots accumulate. Figure 2 shows their behavior.

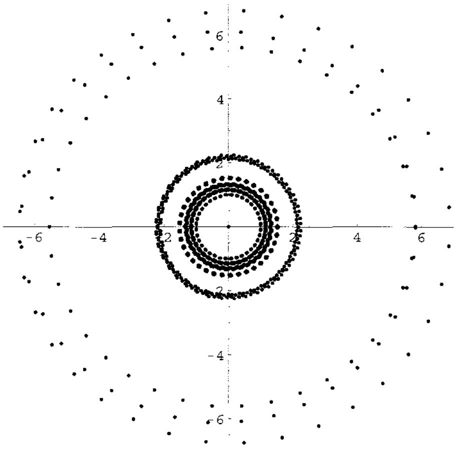

Figure 2: *Distribution of roots of* $\Phi_{37}(X, X^{37}) = 0$ $(-7 < \mathrm{Re(X)} < 7)$

To see more clearly we give the grapf in the range $|\mathrm{Re(X)}| < 2.5$ in Figure 3.

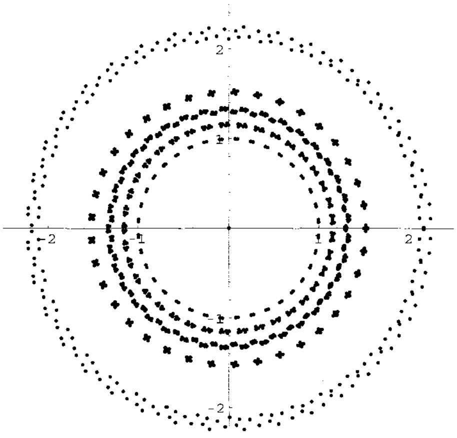

Figure 3: *Distribution of roots of* $\Phi_{37}(X, X^{37}) = 0$ $(-2.5 < \mathrm{Re(X)} < 2.5)$

In this paper we loosely use the term the root curve C_p of $\Phi_p(X, X^p) = 0$ to mean the hypothetical curve or the distribution of its roots itself. From experimental calculation such as the above we made several observations. They are summarized as follows.

(1) Except near the origin, there is quite a similarity among C_p's for different p. Indeed we suspect the existence of $\lim C_p$ as a specific curve.

(2) Near the origin, there are a number of "rings" (a kind of "spectrum"). The number becomes large as p becomes large. In the range $-2.5 < \mathrm{Re(X)} < 2.5$, the number is 1 for $p \leq 11$, 2 for $13 \leq p \leq 17$, 3 for $19 \leq p \leq 29$, 4 for $p = 31$, 5 for $p = 37$. For more bigger p, we are not sure about their number, because we cannot decide whether it is a single ring or two (or many more) rings that are too close to distiguish. (Compare Fig.2 and Fig.3.)

(3) The absolute values of the roots are always greater than 1 (except for the trivial one X= 0 in case $p \equiv 1 \pmod 6$). On the other hand, the maximal absolute value of the roots increase slowly. They are comparatively small. For example, for $p = 61$ the maximal value is approximately 7223.

(4) The most remarkable phenomenon we found is this: except in the trivial case, there is only one real root of $\Phi_p(X, X^p) = 0$, and if p becomes large those values approach quite fast to $-5.54590087936085183481444190913227054114 00\cdots$ monotonously from below. (This fact somewhat supports our conjecture made in (1) even near the origin in some modified way.)

(5) What is the value z for which $j(z)$ is the above mentioned unique root? Evidently z is on the line $\mathrm{Re}(z) = \frac{-1}{2}$ close to $\zeta = (-1 + \sqrt{-3})/2$. We found an approximate value of $z = -1/2 + 0.916953958i$, where $i = \sqrt{-1}$.

(6) If $j(z)$ satisfies $\Phi_p(j(z), j(z)^p) = 0$, then $j(z)^p$ must be of the form $j(\sigma z)$ for some σ in the set

$$\{\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & k \\ 0 & p \end{pmatrix} \ (0 \leq k \leq p-1)\}.$$

Numerically we found for the value z in (5),

$$\sigma = \begin{pmatrix} 1 & c \\ 0 & p \end{pmatrix} \text{ for } c = (p+1)/2.$$

(7) The theorem 2.1 says that the polynomial $\Phi_p(X, X^p)$ has two factors (except for the trivial one). But the root curve C_p does not split into two parts in any obvious way. Indeed both factors have similar root curves, naturaly with fewer points than C_p. See Figure 4 for the first factor of $\Phi_{37}(X, X^{37})$. Also we note that the unique real root mentined in (4) always belongs to the first factor.

Remark 3.1 We obtain other root curves corresponding to some modular functions such as t_{2A} or t_{2B}, the notation being the same as in [9]. See appendix 2 for their graphics.

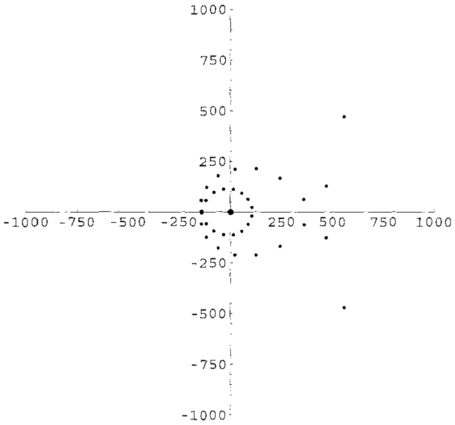

Figure 4: *Distribution of roots of the first factor of* $\Phi_{37}(X, X^{37}) = 0$ (almsost all)

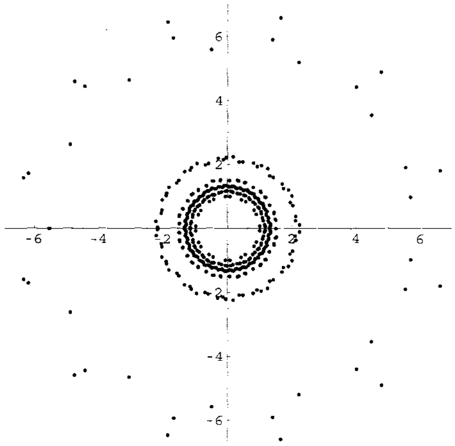

Figure 5: *Distribution of roots of the first factor of* $\Phi_{37}(X, X^{37}) = 0$ ($-7 <$ Re(X)< 7)

Appendix 1. Maximal values of the absolute values of the coefficients of $\Phi_p(X, Y)$

In the range $p \leq 199$, if $p \equiv 5 \bmod 6$ then $|a_{00}|$ is maximal, while if $p \equiv 1 \bmod 6$ then as is well known $a_{00} = 0$ (in fact, in this case we have $a_{00} = a_{10} = 0$ (see Ito [7]) and $|a_{20}|$ or $|a_{11}|$ is maximal. We denote by M the maximal value of the $|a_{ij}|$ in the following table.

p	M	$\log_{10} M$	p	M	$\log_{10} M$
2	$-a_{00}$	14.1972	89	a_{00}	1495.47
3	a_{01}	21.2684	97	a_{20}	1648.14
5	a_{00}	47.1503	101	a_{00}	1730.99
7	a_{20}	66.1658	103	$-a_{11}$	1770.24
11	a_{00}	126.594	107	a_{00}	1853.68
13	a_{20}	149.168	109	a_{11}	1890.91
17	a_{00}	212.202	113	a_{00}	1974.96
19	a_{11}	239.505	127	a_{11}	2257.42
23	a_{00}	308.441	131	a_{00}	2342.90
29	a_{00}	405.549	137	a_{00}	2463.06
31	$-a_{11}$	433.413	139	a_{20}	2503.78
37	a_{11}	531.844	149	a_{00}	2711.69
41	a_{00}	605.604	151	a_{11}	2752.83
43	$-a_{11}$	638.621	157	$-a_{11}$	2878.1
47	a_{00}	714.979	163	a_{20}	3003.9
53	a_{00}	824.389	167	a_{00}	3092.09
59	a_{00}	934.341	173	a_{00}	3217.89
61	a_{11}	967.128	179	a_{00}	3344.72
67	a_{20}	1077.78	181	a_{20}	3382.71
71	a_{00}	1156.12	191	a_{00}	3597.38
73	$-a_{11}$	1189.65	193	a_{11}	3597.38
79	a_{20}	1302.59	197	a_{00}	3723.41
83	a_{00}	1382.02	199	$-a_{11}$	3765.3

(When a_{**} is negative we write $-a_{**}$ in the above table.)

Appendix 2.

Modular polynomials of order p of t_{2A} (t_{2B}, respectively) are denoted by $\Phi_p^{(t_{2A})}$ ($\Phi_p^{(t_{2B})}$, respectively).

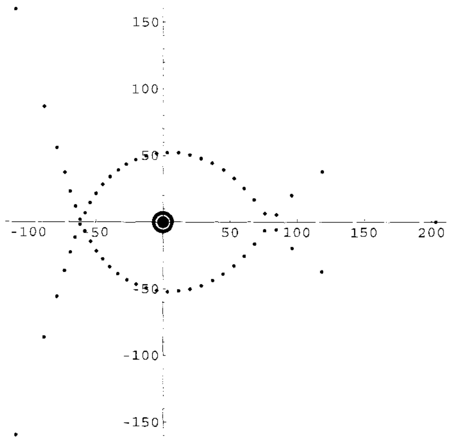

Figure 6: *Distribution of roots of* $\Phi_{31}^{(t_{2A})}(X, X^{31}) = 0$ (all)

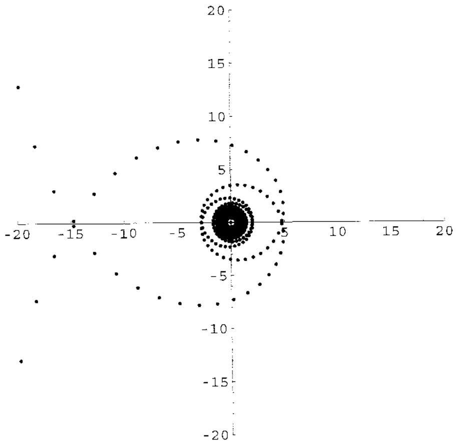

Figure 7: *Distribution of roots of* $\Phi_{31}^{(t_{2B})}(X, X^{31}) = 0$
$(-20 < \mathrm{Re(X)} < 20)$

References

[1] D.Charles and K.Lauter,Computing Modular Polynomials, LMS J. Comput. Math. **8** (2005), 195-204.

[2] P.Cohen, On the coefficients of the transformation polynomials for the elliptic modular function, Math. Proc. Camb. Philos. Soc. **95** (1984), 389-402.

[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] http://www.freepatentsonline.com/20060206554.html

[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) **55** (2000), 17-27.

[7] Hideji Ito, Two remarks on the Modular Polynomials of $j(z)$, Memoirs of the Faculty of Education and Human Studies, Akita Univ. (Natural Sciences) **56** (2001), 35-42.

[8] Hideji Ito, Report on modular equations and elliptic curves(*in Japanese*)(2002), pp.101.

[9] Hideji Ito, On Mod p^2 Periodicity of Coefficients of Modular Polynomials, Memoirs of the Faculty of Education and Human Studies, Akita Univ. (Natural Sciences) **59** (2004), 1-9.

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

[11] M.Rubinstein, http://www.math.uwaterloo.ca/~mrubinst/modularpolynomials/phi_l.html

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

E-mail : itoh@math.akita-u.ac.jp