Memoirs of the College of Education
Akita University (Natural Science)
52, 1—10 (1997)

Computation of Modular Equation II

Hideji ITO

Abstract

This paper is a continuation of our previous paper [6], in which we treated modular equation $\Phi_n(X, j)$ in case n is a prime. Now we consider the case n is composite. By using resultant we can calculate them up to $n = 56$ and a few more. Also we include a detailed account of our computer program.

1 Modular equation $\Phi_n(X, j)$

Let z be a point in the upper half complex plane, and set $q = e^{2\pi iz}$. Then the basic elliptic modular function $j(z)$ is of the form

$$j(z) = 1/q + c_0 + c_1 q + c_2 q^2 + \cdots,$$

where $c_0 = 744$, $c_1 = 196884$, $c_2 = 21493760$, ... Classically, $j(z)$ plays a very important role in complex multplication theory. Even in recent years, $j(z)$ has been the object of intensive study. (See a survey article by M.Kaneko [9]). For example, the finite simple group called Monster has some mysterious connection with $j(z)$.

In my previous paper [6], we consider the problem of explicit computation of the modular equation $\Phi_p(X, j(z))$, which represents algebraic relation between $j(z)$ and $j(pz)$ (p is a prime) and discovered some curious congruences among coefficients of modular equation provided that the p are the Monster primes. Soon afterwards M.Kaneko [8] gives a theoretical explanation of that facts.

By now we have computed the prime case of $\Phi_p(X, j)$ up to $p = 73$ (for $59 \leq p \leq 73$ on machine NEC 4800/660, 596MIPS, with 512MB memory of Akita University Information Processing center).

2 The case n is composite

Now we consider $\Phi_n(X, j)$, n composite. Classically there is a formula given in Weber's book [12], p.242.

(1) If $(n_1, n_2) = 1$ then

$$\Phi_{n_1 n_2}(X, j) = \prod_{i=1}^{\psi(n_1)} \Phi_{n_2}(X, \xi_i),$$

where the ξ_i are the roots of $\Phi_{n_1}(X, j) = 0$.

(2) If $n = p^e$ (p is a prime, and $e > 2$) then

$$\Phi_{p^e}(X, j) = \frac{\prod_{i=1}^{\psi(p^{e-1})} \Phi_p(X, \xi_i)}{(\Phi_{p^{e-2}}(X, j))^p},$$

where the ξ_i are the roots of $\Phi_{p^{e-1}}(X, j) = 0$.

(3) If $n = p^2$ (p is a prime) then

$$\Phi_{p^2}(X, j) = \frac{\prod_{i=1}^{p+1} \Phi_p(X, \xi_i)}{(X - j)^{p+1}},$$

where the ξ_i are the roots of $\Phi_p(X, j) = 0$.

Here we set $\psi(n) = n\prod(1 + 1/p)$, p running over the prime divisors of n. Theoretically, this reduces the computation of modular equation to the case where n is a prime. But it seems that the above formula has been considered not appropriate for practical calculation. For example, Xiao-Tie She [13] calculated the case $n = 4$ by entirely different way, that is, by considering the behavior of q-expansion of $j(z)$ at the various cusps of $X_0(n)$ in the same way as in N.Yui [14]. But for larger n, his method becomes extremely complicated and was unable to get numerical results. On the other hand, our method in [6] applies to some degree but is difficult to do in general.

Recently by scrutinizing classical formulas (1) $\sim$ (3) above, we realize that the numerator of the formulas are nothing but a resultant of special kind. Let the resultant of two polynomials $f(X, Z)$, $g(Y, Z)$ in $\mathbf{C}[X, Y, Z]$ with respect to Z be denoted by $\mathrm{Resultant}_Z(f(X, Z), g(Y, Z))$. (Note that $f(X, Z)$ has no Y term, whereas $g(Y, Z)$ has no X term.)

Theorem 1 *Corresponding to the above formulas* (1) $\sim$ (3), *we have the following.*

(1) *If* $n = n_1 n_2$, $(n_1, n_2) = 1$, *then*

$$\Phi_n(X, Y) = \mathrm{Resultant}_Z(\Phi_{n_1}(X, Z), \Phi_{n_2}(Y, Z)).$$

(2) *If* $n = p^e$, (p *is a prime,* $e > 2$), *then*

$$\Phi_{p^e}(X, Y) = \frac{\mathrm{Resultant}_Z(\Phi_{p^{e-1}}(X, Z), \Phi_p(Y, Z))}{(\Phi_{p^{e-2}}(X, Y))^p}$$

(3) *If* $n = p^2$ (p *is a prime*) *then*

$$\Phi_{p^2}(X, Y) = \frac{\mathrm{Resultant}_Z(\Phi_p(X, Z), \Phi_p(Y, Z))}{(X - Y)^{p+1}}$$

Proof. First recall some properties of resultant. Let A be a ring and two polynomials $F(Z)$, $G(Z)$ be in $A[Z]$. The resultant of $F(Z)$ and $G(Z)$ satisfies

$$\mathrm{Resultant}_Z(F, G) = \prod_{i=1}^{m} F(\xi_i) \cdots (*),$$

where m is the degree of G and the ξ_i are the roots of $G(Z) = 0$.

Now set $A = \mathbf{Q}[X, Y]$, $F(Z) = \Phi_{n_1}(X, Z)$, $G(Z) = \Phi_{n_2}(Y, Z)$ and consider F, G as elements of $A[Z]$. Then the roots ξ_i of $G(Z) = 0$ are the roots of $\Phi_{n_2}(Y, Z) = 0$. Hence by $(*)$ we obtain

$$\prod_{i=1}^{\psi(n_2)} \Phi_{n_1}(X,\xi_i) = \prod_{i=1}^{\psi(n_2)} F(\xi_i) = \mathrm{Resultant}_Z(F(X,Z),G(Y,Z)). \qquad \text{Q.E.D.}$$

Since we already have explicit forms of $\Phi_p(X,Y)$ (up to $p \leq 73$ at present) and resultant is a built-in function (in *Mathematica*), this theorem enables us to compute $\Phi_n(X,Y)$ for n composite. At present (March '97) we have computed up to $n \leq 56$ and a few more ($n = 65, 77$). (Complexity is better measured by $\psi(n)$, not by n itself.) For larger n, it requires huge memory and cannot be done easily (at least on our machine).

Though it little eases our computation, the formula (2) and (3) in theorem 1 above can be generalized as follows.

Theorem 2 *Suppose $n = s + t$. We have the following formula:*

$$\Phi_{p^n}(X,Y) = \frac{\mathrm{Resultant}_Z(\Phi_{p^s}(X,Z),\Phi_{p^t}(Y,Z))}{D_p(s,t)}.$$

The denominator is a polynomial in X and Y and can be given explicitly as follows.

$$(1) \quad If\ s > t,\ then\ D_p(s,t) = \Big(\prod_{i=1}^{t-1} \Phi_{p^{n-2i}}(X,Y)\Big)^{\varphi(p^i)} \cdot (\Phi_{p^{n-2t}}(X,Y))^{p^t}.$$

$$(2) \quad If\ s = t,\ then\ D_p(s,s) = \Big(\prod_{i=1}^{t-1} \Phi_{p^{n-2i}}(X,Y)\Big)^{\varphi(p^i)} \cdot (X-Y)^{\varphi(p^s)}$$

Proof. Suppose two elliptic curves E and E' have j-invariants j, j' respectively. As is well known, if j, $j' \in \mathbf{C}$ satisfy $\Phi_m(j,j') = 0$, then there is a cyclic m-isogeny $E \longrightarrow E'$ (or by its dual $E' \longrightarrow E$) and vice-versa. So for a given j, if j' runs over such values ($m = p^n$) then we have $\Phi_{p^n}(j,j') = \prod(j - j')$. Also we know that a p^n-cyclic isogeny $E \longrightarrow E'$ factors as $g \circ f : E \longrightarrow E'' \longrightarrow E'$ where $f : E \longrightarrow E''$ is a cyclic p^s-isogeny and $g : E'' \longrightarrow E'$ is a cyclic p^t-isogeny.

On the other hand, $\mathrm{Resultant}_Z(\Phi_{p^s}(X,Z),\Phi_{p^t}(Y,Z)) = \prod_{i=1}^{\psi(p^t)} \Phi_{p^s}(X,\xi_i)$ (the ξ_i are the roots of $G(Z) = 0$ where $G(Z) = \Phi_{p^t}(Y,Z)$) embodies all compositions of cyclic p^s-isogenies and cyclic p^t-isogenies of above type. But they are not necessarilly cyclic. One must exclude the case where g is involved with ${}^t f$ (the dual of f). Classifying to what extent $\ker(g)$ and $\mathrm{Ker}({}^t f)$ intersect,we get our results. Q.E.D.

Examples. The case p=2. For brevity we abbreviate $\mathrm{Resultant}_Z(F(X,Z),G(Y,Z))$ as $\mathrm{Res}(F,G)$ and $\Phi_m(X,Y)$ etc. as Φ_m.

$\Phi_{16} = \mathrm{Res}(\Phi_4,\Phi_4)/(X-Y)^6$

$\Phi_{32} = \mathrm{Res}(\Phi_8,\Phi_4)/\Phi_8\Phi_2^4$

$\Phi_{64} = \mathrm{Res}(\Phi_{32},\Phi_2)/\Phi_{16}^2 = \mathrm{Res}(\Phi_{16},\Phi_4)/\Phi_4^4\Phi_{16} = \mathrm{Res}(\Phi_8,\Phi_8)/(X-Y)^{12}\Phi_4^2\Phi_{16}$

3 Some verification

After you perform some calculation, you had better to make a check on your results. Below we list up several methods of verification in our case.

(i) Coincidence with past results.

For p=2, 3, 5, 7, see Herrmann [4]. For p=11, see Kaltofen-Yui [7]. For $n = 4$, see Xiao-Tie She [13].

(ii) Symmetric property of coefficients.

If we set $\Phi_n(X,Y) = X^{\psi(n)} + Y^{\psi(n)} + \sum a_{ik}X^iY^k$, then we must have $a_{ik} = a_{ki}$. (See, for example, Lang [10] p.55.)

(iii) The Kronecker congruence relation.

If p is a prime then we have $\Phi_p(X,Y) \equiv (X^p - Y)(X - Y^p) \pmod{p}$. This means $a_{ik} \equiv 0 \pmod{p}$ except for $a_{11} \equiv a_{pp} \equiv -1 \pmod{p}$. (See Lang [10] p.57.)

(iv) Isogenous pair of elliptic curves over $\mathbf{Q}$.

If there is a cyclic n-isogeny $E \longrightarrow E'$, then their j-invariants j, j' satisfies $\Phi_n(j,j') = 0$. (See Lang [10] p.59, Theorem 5.) By Birch-Kuyk [1] or Cremona [2], we can find such pairs in a few cases. We denote the j-invariant of NA (in the notation of above books) by $j(NA)$.

For $n = 2$, 3, 4, 5, 6, 8 and 9, there are plenty of them. For n=7, $j(26D)$ and $j(26E)$. For $n = 16$, $j(15A)$=−1/15, $j(15H)$=1114544804970241/405. For n=25, $j(11A)$=−4096/11, $j(11C)$=−52893159101157376/11. For $n = 27$, $j(27C)$=$j(27D)$=−12288000, etc.

For $n = 11$, 17, 19, 37, 43, 67 and 163, see for example Cremona [2] p.78.

Of course, by Mazur's theorem there are only finitely many of them. More precisely they are $n = 1 \sim 19$, 21, 25, 27, 37, 43, 67 and 163.

(v) Isogenous pair of elliptic curves over finite fields.

Let ℓ be a rational prime. If ℓ is not a divisor of n, then $\Phi_n(j,j') = 0$ in $\mathbf{F}_\ell(=\mathbf{Z}/\ell\mathbf{Z})$ is equivalent with the existence of a cyclic n-isogeny $E_j \longrightarrow E_{j'}$, where E_j, $E_{j'}$ are the elliptic curves over $\mathbf{F}_\ell$ with j-invariants j, j' respectively. On the other hand, we can find $\mathbf{F}_\ell$-rational cyclic n-isogenies as follows(cf. Ito [5], §5.) Let $a_\ell \in \mathbf{Z}$ be $|a_\ell| \leq 2\sqrt{\ell}$. Then to each value of a_ℓ, there corresponds an isogeney class of elliptic curves whose Frobenius endomorphism can be identified with $\pi_\ell = (-a_\ell + \sqrt{a_\ell^2 - 4\ell})/2$. We know the following.

Suppose (a) $\mathbf{Z}[\pi_\ell]$ is the maximal order of $\mathbf{Q}(\pi_\ell)$,(b) p splits in $\mathbf{Z}[\pi_\ell]$, (c) the class number of $\mathbf{Z}[\pi_\ell]$ is 1, then there is a unique elliptic curve E defined over $\mathbf{F}_\ell$ corresponding to a_ℓ and E has a cyclic p-isogeny $E \longrightarrow E$. So in this case we have $\Phi_p(j(E),j(E)) = 0$ in $\mathbf{F}_\ell$. (Note that the converse dose not necessarily holds. The reason is, $Y_0(n)$ in the standard notation is not the plane curve $C_n : \Phi_n(X,Y) = 0$ itself. $Y_0(n)$ is the desingularisation of C_n.)

Example. p=7. First we enumerate all isogeny classes of elliptic curves over $\mathbf{F}_\ell$ (cf. Waterhouse [11] p.542 except the values of j-invarians. We calculate them in reverse way, that is, from the Weierstrass equation corresponding to the value j we calculate the value of a_ℓ. And as for the exact correspondence of endomorphism rings and the j-invariants, we use Ito [5] and the knowledge of $\mathbf{F}_\ell$-rational points of each curves.)

a_ℓ	π_ℓ	Endomrphism ring	j–invariants
0	$\sqrt{-7}$	maximal order	6
		index 2	6
± 1	$(1 \pm 3\sqrt{-3})/2$	maximal order	0
		index 3	3
± 2	$1 \pm \sqrt{-6}$	maximal order	4, 5
± 3	$(3 \pm \sqrt{-19})/2$	maximal order	1
± 4	$2 \pm \sqrt{-3}$	maximal order	0
		index 2	2
± 5	$(5 \pm \sqrt{-3})/2$	maximal order	0

Since $\left(\frac{-19}{5}\right) = 1$, we have $\Phi_5(1,1) \equiv 0 \pmod 7$. Also $\left(\frac{-19}{17}\right) = 1$, (or $\left(\frac{-19}{23}\right) = 1$ etc.) implies $\Phi_{17}(1,1) \equiv 0 \pmod 7$ (or $\Phi_{23}(1,1) \equiv 0 \pmod 7$ etc.)

Incidentally we suspect that $\Phi_n(-1,-1) \equiv 0 \pmod 7$ for all n. At any rate, it seems there are many things to be cleared.

(vi) Fricke's parametrisation.

In case $X_0(n)$ is of genus 0, then $j(z)$ and $j(nz)$ can be parametrized by an uniformizing function. Fricke [3] enumerates such parametrization. For example, when $n = 9$, we have $j(z) = 12^3 J(\tau)$ and $j(9z) = 12^3 J(3/\tau)$, where $J(\tau) = (9\tau^4 + 36\tau^3 + 54\tau^2 + 28\tau + 1)/64\tau(\tau^2 + 3\tau + 3)$ (Fricke [3] p.387). So substituting them into $\Phi_9(X,Y)$ $(X = j(z), Y = j(9z))$, we must have value 0. And indeed such is the case.

Appendix.

In this appendix, we explain our actual way of calculation in detail. We use *Mathematica* version 2 . First we define several functions. (In parenthesis, we indicate the name of the file that contains it.)

(1) $c_n = c[n]$. **(jcoef.m)**

The $c[n]$ are the coefficients of q-expansion of $j(z) = \sum_{-1}^{\infty} c[n]q^n$. We rely on the Lehmer formula.

```
% Computation of the q-coefficients of j(z) %

tau[n_]:=tau[n]=RamanujanTau[n]
c[-1]=1
c[0]=744
c[1]=196884
c[n_]:=c[n]=65520*(DivisorSigma[11,n+1]-tau[n+1])/691-tau[n+2]-
          24*tau[n+1]-Sum[c[k]*tau[n+1-k],{k,n-1}]
```

Remark: The calculation of Ramanujan's tau .

In our paper [6], we wrote that $\tau(n)$ is a built-in function in *Mathematica*. Strictly speaking, it is in the standard package : NumberTheory`Ramanujan`. Later, we realized that it is more efficient to use Ramanujan's recursive formula as is explained in the following paper.

D.H.Lehmer, "Ramanujan's Function $\tau(n)$" , Duke Math. J.(1943) 483-492.

The formula (14) in this paper is as follows:

$$(n-1)\tau(n) = \sum_{m=1}^{b_n}(-1)^{m+1}(2m+1)\times\{n-1-9m(m+1)/2\}\tau\{n-m(m+1)/2\}$$

where, $b_n = \frac{1}{2}((1+8m)^{\frac{1}{2}}-1)$ (its integer part).)

(This is not incorporated in this version, but if you want $\tau(n)$ for bigger n (≥ 5000), you should use it.)

(2) times1[A,B,m] **(jpower.m)**

The list of the coefficients of the expansion of the product of two polynomials $\sum_{i=0}^{m-1} a_i X^i$ and $\sum_{i=0}^{m-1} b_i X^i$ (from the 0-th term to the (m−1)-th power term). We make two lists A=$\{a_0, a_1, \ldots, a_{m-1}\}$, B=$\{b_0, b_1, \ldots, b_{m-1}\}$. We ignore n-th power terms ($n \geq m$). That's because in our application A and B are the lists of coefficients of some finite terms in infinite series. So after taking the product, n-th power terms ($n \geq m$) are not correct values.

```
times1[A_List,B_List,m_]:=
            Module[{A1=A, B1=Table[0,{m}], C1={}},
            Do[{A1, B1}= {Drop[A1,-1], B1+B[[i]]*A1};
              C1=AppendTo[C1,B1[[1]]];
              B1=Drop[B1,1],
              {i,1,m}]
            ;C1]
```

(3) LQJ[n] **(LQJ.m)**

```
(* LQJ[n] is the list of the lists of the coefficients of
   the q-expansion of j(q)^m,
   (1<=m<=n), up to the constant term.  *)

L1[n_]:=Table[c[i],{i,-1,n-1}]
LQJ[n_]:=Module[{A={},B=L1[n]},
  Do[{A,B}={Append[A,Take[B,i+1]],times1[B,L1[n],n+1]},{i,1,n}];A]
```

(4) Jcqn[p_,k_] **(jpower.m)**

The list of the coefficients of q^0, q^p, q^{2p},..., q^{p^2} in the q-expansion of $j(z)^k$. To get them, we must first calculate q-expansions of $j(z)^k$. jqp[1] is the list of the coefficients of the q-expansion of $j(z)$ (up to the n-th term; if you want $\Phi_p(X,j)$, then $n = q^{p^2+p}$.) Suppose we want Φ_p as far as p=31. Then n=1000 will suffice. So, in the following example, we take up to q^{1000} . (Why 1002, in the second line? That's because when we take up to q^n we must take into account the constant term and the (−1)-th power term.) jqp[i] is the list of the coefficients of the q-expansion of $j(z)^i$ up to q^{1000}.

```
jqp[1]=Table[c[i],{i,-1,1000}]
jqp[i_]:=jqp[i]=times1[jqp[1],jqp[i-1],1002]
jqpn[k_,n_]:=jqp[k][[n+1+k]]
Jcqn[p_,k_]:=Table[jqpn[k,i],{i,0,p^2,p}]
```

Warning: For bigger $p > 31$ (or smaller $p < 31$), you must change the values 1000 and 1002 for appropriate values.

(5) `jpol[{d_0,d_1,...,d_k}]` **(jpol.m)**

Loosely speaking, this is the list of the coefficients of j-polynomial expression of $\frac{d_0}{q^k} + \frac{d_1}{q^{k-1}} + \cdots + \frac{d_{k-1}}{q} + d_k + \cdots$ (the ordering is from the highest to the constant term).

```
(* jpol[List] gives the j-polynomial expression of the given list
    of numbers *)

LQJ[0]={1}
jpol[F_]:=Module[{C={},A=F,n=Length[F]-1},
   Do[{C,A}={Append[C,First[A]],
            Rest[A-A[[1]]*LQJ[50][[n+1-i]]]},{i,1,n+1}];C]

(* For p>50, you must modify the above value 50 in LQJ[ ] *)
```

(6) u[k,p],t[k,p],s[k,p] **(jmod.m)**

In our paper [6], these are denoted as u_k, t_k, s_k. That is

$u[k,p] = j(\frac{z}{p})^k + j(\frac{z+1}{p})^k + \cdots + j(\frac{z+p-1}{p})^k$,

$t[k,p]$ = the k-th elementary symmetric polynomial in $j(\frac{z}{p}), j(\frac{z+1}{p}), \ldots, j(\frac{z+p-1}{p})$,

$s[k,p]$ = the k-th elementary symmetric polynomial in $j(pz), j(\frac{z}{p}), j(\frac{z+1}{p})$, $\ldots, j(\frac{z+p-1}{p})$.

```
(* u[k,p] = k-th power sum of j(z/p),j((z+1)/p),...,j((z+p-1)/p)
    (except u[p,p], see below)
   t[k,p] = k-th elementary symmetric function
                        in j(z/p),...,j((z+p-1)/p)
   s[k,p] =k-th elementary symmetric function
                      in j(pz),j(z/p),...,j((z+p-1)/p)
   We have s[k,p]=j(pz)*t[k-1,p]+t[k,p]       *)


u[k_,p_]:=u[k,p]=p*Jcqn[p,k]

(*  At first we define u[k_,p_]:=p*Join[{1},Jcqn[p,k]]/;k==p. But
it causes inconvienience in t[p,p]. So the above u[p,p] is actually
 u[p,p]-p*(1/q).The definition of t[p,p] takes care of this point
 correctly. *)

t[0,p_]:=Flatten[{{1},Table[0,{p}]}]
t[1,p_]:=u[1,p]
tt[k_,p_]:=tt[k,p]=
((-1)^(k-1))*(1/k)*Sum[(-1)^i*times1[u[k-i,p],t[i,p],p+1],{i,0,k-1}]

t[k_,p_]:=tt[k,p]/;1<=k<=p-1
t[k_,p_]:=Flatten[{{(-1)^(k-1)},tt[p,p]}]/;k==p
t[k_,p_]:=Table[0,{p+1}]/;k==p+1

s[k_,p_]:=t[k-1,p]+Flatten[{Table[0,{p-1}],(-1)^(p-1)*Floor[k/p],
```

```
                        744*t[k-1,p][[1]]+tt[k,p][[1]]}]/;1<=k<=p
s[k_,p_]:=t[k-1,p]+Flatten[{Table[0,{p}],(-1)^(p-1)*744,
                    744*tt[k-1,p][[1]]}]                /;k==p+1
```

(7) cmodj[n,p] (**jmod.m**)

This is $(-1)^{p-n+1}S_{p-n+1}(j)$ in our paper [6], that is, the coefficient of X^n in $\Phi_p(X,j)$. Not as a polynomial in j, but as a list of the coefficients. (The ordering is from the highest power of j .) The index of S is not naturally correlated to the argument of cmodj. That's because, in the computation of the modular equation $\Phi_p(X,j)$, we get first the coefficient of X^p, next the coefficient of X^{p-1} and so on.

```
cmodj[k_,p_]:=jpol[(-1)^k s[k,p]]
```

Steps of calculation

Once you get $\Phi_p(X,j)$ and $\Phi_q(X,j)$ (p and q are different primes) as polynomials, it is easy to get $\Phi_{pq}(X,j)$, at least for p and/or q of small size. That is, simply type

Resultant[$\Phi_p(X,Z), \Phi_q(j,Z), Z$].

To get $\Phi_{p^2}(X,j)$, you type

Simplify[Factor[Resultant[$\Phi_p(X,Z), \Phi_p(j,Z), Z$]]/(($X-j$)$^{p+1}$)],

and so forth. So in the sequel, we concentrate on the case n is a prime p.

Suppose we want Φ_2, Φ_3,..., Φ_{31} at a time. Among the coefficients of the q-expansion of $j(z)^k$, we need up to the (31^2+31)-th power term in q. But as it makes little difference, we calculate them up to the term q^{1000}.

(1) **RamanujanTau[n]**

First you load the necessary package:

<< NumberTheory`Ramanujan`

Then

Table[RamanujanTau[i],{i,1,2000}]>> rama2000.d

Now you write

"RamanujanTau[i_]:=rama2000[[i]]/;1 <= i <= 2000

rama2000="

at the top of the file rama2000.d.

The values of $\tau(n)$ are important for themselves. So, in the sequel, we actually use values of them stored beforehand.

(2) **c[n]**

First you load

<<rama2000.d;

<<jcoef.m

Then you type in as follows:

Table[c[i],{i,-1,1000}] >> jcoef1000.d

After that, you must make appropriate editing in the file jcoef1000.d. For example, at the top of the file you insert

c[i_]:=jcoef1000[[i+2]]/; -1<=i<=1000

jcoef1000=

The numerical values of c[n] are very important. So, again, these are to be stored separatedly.

(3) **LQJ[n]**

Although we want Φ_n up to $n = 31$, we compute $j(q)^n$ as far as $n = 50$, since it takes no more time and memory. (Note that here we need only up to the constant term.)

```
<< jcoef1000.d;
<< LQJ.m
<< jpower.m
```

Then

```
LQJ[50]>> LQJ50.d
```

(At the top of the file LQJ50.d, you must write "LQJ[50]:=".)

(These list of values can be used for different $p < 50$. So you should store them).

(4) $\boldsymbol{j(z)^m}$ $(1 \leq m \leq 31)$ up to the term q^{1000}

(If you want Φ_p, then you need up to $m = p$.) This part of the computation takes the most of the time. In case of Φ_{31}, the result of computation takes about 6MB disk space. (So it causes no problem. But for larger p, it requires huge memory and disk space. Since what we need in the final step is Jcqn$[p, m]$, not $j(z)^m$, so, it is better to compute step by step. Note that to compute $j(z)^m$ you only need $j(z)$ and $j(z)^{m-1}$. So you can discard $j(z)^k (2 \leq k \leq m-2)$, once you get Jcqn[$p$,$m-1$].)

Load

```
<< jcoef1000.d;
<< jpower.m
```

Type in

```
Table[jqp[i],{i,1,31}];
```

(5) $\boldsymbol{\Phi_p(X, j)}$

After the computation in (4) is done, you load some more files:

```
<<jmod.m
<<jpol.m
<<LQJ50.d
```

Then type in

```
Table[cmodj[i,2],{i,1,3}]
```

This gives the list of the coefficients of $\Phi_2(X, j)$. In the same way you get the list of the coefficients of Φ_p up to $p = 31$.

References

[1] B.J.Birch and W.Kuyk (eds.), Modular Functions of One Variable IV, Lecture Notes in Mathematics **476**, Springer, 1975.

[2] J.E.Cremona, Algorithms for modular elliptic curves, Cambridge University Press, 1992.

[3] R.Fricke, Die Elliptischen Funktionen und ihre Anwendungen II, Teubner, 1922.

[4] O.Herrmann, Über die Berechnung der Fourierkoeffizienten der Funktion $j(\tau)$, J. Reine Angew. Math., **274** (1975), 187–195.

[5] Hideji Ito, On the Number of Rational Cyclic Subgroups of Elliptic Curves over Finite Fields, Memoirs of the College of Education, Akita Univ. (Natural Science) **41** (1990), 33–42.

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

[7] E.Kaltofen and N.Yui, On the modular equation of order 11, Proc. of the 1984 MACSYMA USERS CONFERENCE, General Electric (1984), 472–485.

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

[9] M.Kaneko, 楕円曲線の j 不変量に関する話題, 第 41 回代数学シンポジウム報告集 (1996), 96–112.

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

[11] W.C.Waterhouse, Abelian Varieties over finite fields, Ann. scient. Éc. Norm.Sup.,4^e serie, t.2 (1969), 521–560.

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

[13] Xiao-Tie She, Explicit Formulas For The Modular Equations, pp.28, (Brown Univ. Unpublished?) (1991).

[14] N.Yui, Explicit Form of Modular Equation, J. Reine Angew. Math. **299-300** (1978), 185–200.

Department of Mathematics
College of Education, Akita University
Akita 010, Japan