Memoirs of the College of Education
Akita University (Natural Science)
53, 17-23 (1998)

Values of Modular Polynomials modulo primes

Hideji ITO

(*Received December 15, 1997*)

Abstract

We gave an algorithm to compute the modular equation $\Phi_n(X, j)$ of $j(z)$ in [4]. Using the data accumulated we have found some congruences of values $\Phi_n(i, k)$ modulo a few primes. For example, $\Phi_n(-1, -1) \equiv 0 \bmod 7$ for all n and $\Phi_n(i, -1) \equiv 1 \bmod 7\,(0 \leq i \leq 5)$ for all n satisfying $\deg \Phi_n \equiv 0 \bmod 6$. Knowledge about supersingular elliptic curves enables us to give a proof of those facts. Some related problems are also discussed. In the Appendix, tables of values of $\Phi_n(i, k)$ mod 7 are given for several n.

1 Introduction.

Let $j(z)$ be the basic elliptic modular function, n a positive integer. Then $j(z)$ and $j(nz)$ satisfiy a certain equation (usually called a modular equation):

$$\Phi_n(X, Y) = 0 \qquad (X = j(z), Y = j(nz))$$

Explicitly the modular polynomial $\Phi_n(X, Y)$ is given by

$$\Phi_n(X, j(z)) = \prod_{\alpha \in M(n)} (X - j(\alpha z))$$

where $M(n) = \{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid ad - bc = n,\ d > 0, 0 \leq b < d,$ the common factor of rational integers a, b and d is $1\}$. So we can write

$$\Phi_n(X, Y) = X^m + Y^m + \sum_{i,k=0}^{m-1} a_{ik} X^i Y^k, \qquad m = \deg \Phi_n = n \prod_{p \mid n} (1 + p^{-1}).$$

We know $a_{ik} = a_{ki}$ (see [5], p.55). This gives us a method of checking the result of our computation of $\Phi_n(X, Y)$. Although that can be done easily on machine, we want to see the symmetry in our own eyes directly. So we make a table of $\Phi_n(i, k) \bmod p \quad (0 \leq i, k \leq p - 1)$. That is of course symmetrical in i and k and one can see it at a glance at least for small p even if n is large.

Looking into the tables obtained (see Appendix), you can see that there are some characteristic patterns of the values such as noted in the abstract. It is the purpose of this paper to investigate to what extent those patterns would hold in general.

2 The values of $\Phi_n(i,k)$ mod p.

Let p be a rational prime. We first note that the Kronecker congruence relation $\Phi_p(X,Y) \equiv (X^p - Y)(X - Y^p) \bmod p$ yields $\Phi_p(i,k) \equiv (i-k)^2 \bmod p$. This gives us a very typical table of values (see $\Phi_7(i,k)$ mod 7 in the Appendix).

Next we treat more general case. We need two facts.

(i) Let E and E' be elliptic curves over a field K with characteristic p (here $p = 0$ is permitted) and $j(E)$, $j(E')$ their j-invariants. Suppose $p \not| n$. If there is a cyclic n-isogeny between E and E', then we have $\Phi_n(j(E), j(E')) = 0$ and vice versa. (See [5] p.59.)

Remark. Suppose $n = p$, and j, $j' \in \mathbf{F}_p$. By the Kronecker congruence relation we have $\Phi_p(j,j') \equiv 0 \bmod p \iff j = j'$. On the other hand the supersingular elliptic curve defined over $\mathbf{F}_p$ has no subgroup of order p. So (i) cannot hold when $p|n$.

Hereafter we always assume $p \not| n$ unless otherwise explicitly stated.

(ii) Over $\overline{\mathbf{F}}_p$, the supersingular j-invariants are contained in $\mathbf{F}_{p^2}$ and can be explicitly calculated. We list them for several small primes. (See [1] p.257.)

p	supersingular j-invariants		
2	0	13	5
3	0	17	0, 8
5	0	19	7, 18
7	6	23	0, 3, 19

Theorem 1 *If there is only one supersingular elliptic curve E over $\overline{\mathbf{F}}_p$, then we have $\Phi_n(X, j(E)) \equiv (X - j(E))^{\deg \Phi_n} \bmod p$, for all n not divisible by p.*

Proof. We know $\Phi_n(X,j) = \prod_{j'}(X - j')$ where $j' = j(E')$ for some elliptic curve E' over $\overline{\mathbf{F}}_p$ and there is an n-cyclic isogeny between E and E'. If E is supersingular, so is E'. Hence our assumption means $j = j'$.

Example 1. p=2. Since over $\mathbf{F}_2$ there is only one supersingular j-invariant (namely j=0), we have $\Phi_n(X,0) \equiv X^{\deg \Phi_n} \bmod 2$. Also we can explicitly give the values of $\Phi_n(X,1) \bmod p$ in case $n = \ell$ (a rational prime) as follows. Let a_p be the trace of Frobenius endomorphism of an elliptic curve over $\mathbf{F}_p$. As is well known $|a_p| \leq 2\sqrt{p}$. So if p =2, we have a_2=0, ±1, ±2. Only $a_2 = \pm1$ can give non-supersingular elliptic curves ($j = 1$). Let E be such an elliptic curve (i.e. $j(E) = 1$). Since in this case $a_p^2 - 4p = 1 - 4 \times 2 = -7$, the endomrphism ring End(E) is the maximal order of $\mathbf{Q}(\sqrt{-7})$. By Ito [3], if ℓ splits or ramifies in $\mathbf{Q}(\sqrt{-7})$ then there is at least one ℓ-isogeny $E \to E$, that is, $\Phi_\ell(1,1) = 0 \bmod 2$. While if ℓ remains prime in $\mathbf{Q}(\sqrt{-7})$ then there is no ℓ-isogeny $E \to E$, so $\Phi_\ell(1,1) \not\equiv 0 \bmod 2$, that is, $\Phi_\ell(1,1) \equiv 1 \bmod 2$. All in all we see that the table of the values of $\Phi_\ell(i,k) \bmod 2 \quad (0 \leq i,k \leq 1)$ is of type $\begin{matrix} 0 & 1 \\ 1 & 0 \end{matrix}$ in the first case and $\begin{matrix} 0 & 1 \\ 1 & 1 \end{matrix}$ in the second case. Here the first row means $\Phi_\ell(k,0) \bmod 2 \quad (k = 0,1)$, the second row $\Phi_\ell(k,1) \bmod 2 \quad (k = 0,1)$.

Example 2. p=3. $\Phi_n(X,0) \equiv X^{\deg \Phi_n} \bmod 3$. Similar reasoning as in Example 1 gives the values of $\Phi_\ell(i,i) \bmod 3\,(1 \le i \le 2)$ in some cases. Notations being the same as before, if $a_p = 1$ then $a_p^2 - 4p = -11$ and the corresponding j-invariant is $j = 1$. If $a_p = 2$, then $a_p^2 - 4p = -8$ and the corresponding j-invariant is j=2. So if ℓ splits or ramifies in $\mathbf{Q}(\sqrt{-11})$ ($\mathbf{Q}(\sqrt{-2})$, respectively), then $\Phi_\ell(1,1) \equiv 0 \bmod 3$ ($\Phi_\ell(2,2) \equiv 0 \bmod 3$, respectively).

Example 3. p=5. $\Phi_5(X,0) \equiv X^{\deg \Phi_n} \bmod 5$. So we have $\Phi_n(0,0) \equiv 0 \bmod 5$ for all n and $\Phi_n(k,0) \equiv 1 \bmod 5$ for $1 \le k \le 4$ provided $4 | \deg \Phi_n$.

Example 4. p=7. $\Phi_n(X,-1) \equiv (X+1)^{\deg \Phi_n} \bmod 7$. Especially, we have $\Phi_n(-1,-1) \equiv 0 \bmod 7$ for all n and $\Phi_n(i,-1) \equiv 1 \bmod 7\,(0 \le i \le 5)$ for all n satisfying $6 | \deg \Phi_n$. We note that if an odd prime $\ell \equiv 2 \bmod 3$ divides n then the last condition is satisfied.

Example 5. p=13. $\Phi_n(X,5) \equiv (X+8)^{\deg \Phi_n} \bmod 13$.

Theorem 2 *Let E is an elliptic curve ($\neq$supersingular) over $\mathbf{F}_p$ with j-invariant 0 and π_p its Frobenius endomorphism. Suppose* End(E) *is the maximal order of $\mathbf{Q}(\sqrt{-3})$ and the conductor of $\mathbf{Z}[\pi_p]$ is prime to ℓ(a rational prime $\neq p$). Then we have the following ($f(X)$ is some polynomial in X).*

(i) *If ℓ splits in $\mathbf{Q}(\sqrt{-3})$ (i.e. $\ell \equiv 1 \bmod 3$), then $\Phi_\ell(X,j) \equiv (X-j)^2 f(X)^3 \bmod p$.*

(ii) *If ℓ remains prime in $\mathbf{Q}(\sqrt{-3})$ (i.e. $\ell \equiv 2 \bmod 3$), then $\Phi_\ell(X,j) \equiv f(X)^3 \bmod p$.*

Proof. By Ito [3] Propsosition 2, the assumptions mean the number of $\mathbf{F}_p$-rational ℓ-isogenies from E is 2 or 0 corresponding to the cases (i) and (ii). Since the class number of $\mathbf{Q}(\sqrt{-3})$ is one, if there is an $\mathbf{F}_p$-rational ℓ-isogeny $E \to E'$, E' must be E itself. Also, as Aut(E) is isomorphic to the group of sixth roots of unity, multiplicity three occurs. Indeed, Aut(E) acts on the set $S = \{C \subset E \,|\, |C| = \ell\}$. Clearly $\{\pm 1\}$ fixes any C. Put $\zeta = (-1+\sqrt{-3})/2$. If $\zeta C = C$, then we easily see that $\pi_p C = C$, that is, C is $\mathbf{F}_p$-rational. If $\zeta C \neq C$, then we also have $\zeta^2 C \neq C$. But by [7] Proposition 3.7 we have $E/C \cong E/(\zeta C) \cong E/(\zeta^2 C)$. So their j-invariants must coincide.

Example 6. p=7. By the table in Ito [4] *II* p.5, our theorem applies for $\ell > 3$. By computation we have $\Phi_2(X,0) \equiv (X+5)^3 \bmod 7$, $\Phi_3(X,0) \equiv X(X+4)^3 \bmod 7$, $\Phi_5(X,0) \equiv (X^2+2X+5)^3 \bmod 7$, $\Phi_{11}(X,0) \equiv (X^4+3X^3+2X^2+X+3)^3 \bmod 7$, $\Phi_{13} \equiv X^2(X^4+X^3+3X^2+3X+1)^3 \bmod 7$, $\Phi_{17}(X,0) \equiv (X^6+4X^4+5X^3+2X^2+4X+4)^3 \bmod 7$, $\Phi_{19}(X,0) \equiv X^2(X^3+4X^2+3)^3(X^3+5X^2+2X+4)^3 \bmod 7$ etc.

In particular, we see that in case $\ell \equiv 2 \bmod 3$ the values of $\Phi_\ell(0,i) \bmod 7\,(0 \le i \le 6)$ must be 0 or ± 1.

3 Factorization of $\Phi_n(X,i) \bmod p$.

Theorems 1 and 2 suggest that we should investigate the factorization of $\Phi_n(X,i) \bmod p$ for each $0 \le i \le p-1$. The following theorem enables us to assert the coincidence of $\Phi_n(X,i) \bmod p$ for different i's ($0 \le i \le p-1$) for infinite number of n's.

Theorem 3 *Let ℓ be a rational prime and i, k two different integers* $(0 \leq i, k \leq p-1)$. *Suppose* $\Phi_\ell(X,i) \equiv \Phi_\ell(X,k) \bmod p$. *Then we have* $\Phi_{\ell m}(X,i) \equiv \Phi_{\ell m}(X,k) \bmod p$ *for all m not divisible by ℓ.*

Proof. We have $\Phi_{\ell m}(X,\xi) = \prod_\alpha \Phi_m(X,\alpha)$ where α runs through the solutions of $\Phi_\ell(X,\xi) = 0$ (see [8] p.242). This readily yields our assertion.

In the following examples, the numbers i and k are the supersingular j-invariants over the corresponding fields.

Examples. (1) Since we know $\Phi_3(X,0) \equiv \Phi_3(X,8) \equiv X(X-8)^3 \bmod 17$ by computation, we have $\Phi_{3m}(X,0) \equiv \Phi_{3m}(X,8) \bmod 17$ for all m $(3 \nmid m)$. (By the way, the facts $\Phi_9(X,0) \equiv (X+9)^{12} \bmod 17$ and $\Phi_9(X,8) \equiv X^4(X+9)^8$ mean we cannot drop the condition $\ell \nmid m$.) Also we know $\Phi_{11}(X,0) \equiv \Phi_{11}(X,8) \equiv X^3(X+9)^9 \bmod 17$ by computation, we have $\Phi_{11m}(X,0) \equiv \Phi_{11m}(X,8) \bmod 17$ for all m $(11 \nmid m)$.

(2) Since we know $\Phi_2(X,7) \equiv \Phi_2(X,18) \equiv (X+1)(X+12)^2 \bmod 19$ by computation, we have $\Phi_{2m}(X,7) \equiv \Phi_{2m}(X,18) \bmod 19$ for all $m\,(2 \nmid m)$.

The problem is, of course, to find out which i and k satisfy the assumption in the first place. Also we note, in example (1), writing $\Phi_n(X,0) \equiv X^s(X-8)^t \bmod 17$ and $\Phi_n(X,8) \equiv X^u(X-8)^v \bmod 17$, we observe that $t = 3u$ always holds as far as our computation goes.

4 The number of zeros in the table $\{\Phi_n(i,k) \bmod p\}$.

We denote by $\mathrm{N}(n,p)$ the number of 0's in the table $\{\Phi_n(i,k) \bmod p\}$ $(0 \leq i, k \leq p-1)$. In this section, we investigate the case $n = \ell$ (a rational prime). In general it seems difficult to express $\mathrm{N}(\ell,p)$ in some explicit closed form. Here we give a certain estimate of it.

As is well known, the isogeny classes of elliptic curves defined over $\mathbf{F}_p$ correspond to the set $\{a_p \in \mathbf{Z} \,|\, |a_p| \leq 2\sqrt{p}\}$. Put $\pi_p = (a_p + \sqrt{a_p^2 - 4p})/2$. If the elliptic curve E over $\mathbf{F}_p$ corresponding to a_p is not supersingular, then $\mathrm{End}(E)$ is an order R (containning π_p) of the imaginary quadratic field $\mathbf{Q}(\pi_p)$. (Hereafter we call such an order R *admissible*.) And the number of the isomorphism classes of elliptic curves with the same endomorphism ring R is the class number $h(R)$ of R. (See Waterhouse [7] p.538-542.)

We denote by n_0, n_1, n_2 various sums of class numbers of admissible orders. Explicitly, $n_0 = \sum_{R_0} h(R_0)$ where R_0 runs through admissible orders in which ℓ ramifies. Also, $n_1 = \sum_{R_1} h(R_1)$ where R_1 runs through admissible orders in which ℓ splits and $h(R_1) = 1$, $n_2 = \sum_{R_2} h(R_2)$ where R_2 runs through admissible orders in which ℓ splits and $h(R_2) \geq 2$. Let m be the number of the supersingular j-invariants contained in $\mathbf{F}_p$.

Theorem 4 *Assume $\ell > 2\sqrt{p}$. Notations being the same as above, we have the following estimate :* $n_0 + n_1 + n_2 \leq \mathrm{N}(\ell,p) \leq m^2 + n_0 + n_1 + 2n_2$.

Proof. Since any elliptic curve isogenous to a supersingular elliptic curve is also supersingular, there are at most m^2 zeros of $\Phi_\ell(X,Y) \bmod p$ coming from the $\mathbf{F}_p$-rational supersingular j-invariants.

Suppose End(E) is of type R_0. Then by Ito [3], there is exactly one $\mathbf{F}_p$-rational ℓ-isogeny from E. (Here and in the following we need the assumption $\ell > 2\sqrt{p}$. This guarantees ℓ does not devide the conductor of End(E).) If End(E) is of type R_1, then there are two $\mathbf{F}_p$-rational ℓ-isogenies from E to some elliptic curve $E_i\,(i = 1, 2)$. Since the conductor of End(E_i) must be the same as that of End(E), we have $E_i = E\,(i = 1, 2)$. So in this case we get only one solution of $\Phi_\ell(X, Y) \equiv 0 \bmod p$, i.e., $\Phi_\ell(j(E), j(E)) \equiv 0 \bmod p$.

If End(E) is of type R_2, then E gives at least one solution and at most two solutions of $\Phi_\ell(X, Y) \equiv 0 \bmod p$. This completes our proof.

Example. p=11. The next table on the left enumerates the isomorphism classes of elliptic curves over $\mathbf{F}_{11}$. Here R means endomorphism ring, h the class number of R and j the corresponding j-invariant. On the right we give the table of the values $\Phi_7(i, k)$ mod $11\,(0 \le i, k \le 10)$. (If $\Phi_7(X, Y)$ is suitably defined, in the language of *Mathematica*, this is Table[$\Phi_7(i, k)$ mod $11, \{i, 0, 10\}, \{k, 0, 10\}$]//TableForm. Namely, the i-th row is the list of the values of $\Phi_7(i-1, k)$ mod $11\,(0 \le k \le 10)$.)

a_p	π_p	R	h	j
0	$\sqrt{-11}$	maximal	1	1
		conductor 2	3	0,(1?)
±1	$(1 \pm \sqrt{-43})/2$	maximal	1	6
±2	$1 \pm \sqrt{-10}$	maximal	2	7, 9
$\pm$ 3	$(3 \pm \sqrt{-35})/2$	maximal	2	4, 10
$\pm$ 4	$2 \pm \sqrt{-7}$	maximal	1	2
		conductor 2	1	8
$\pm$ 5	$(5 \pm \sqrt{-19})/2$	maximal	1	5
$\pm$ 6	$3 \pm \sqrt{-2}$	maximal	1	3

$\Phi_7(i, k)$ mod 11

0	0	4	4	4	1	4	3	3	1	9
0	0	5	9	1	5	4	5	1	9	5
4	5	0	8	10	1	9	1	8	3	6
4	9	8	1	9	5	4	6	8	9	3
4	1	10	9	8	5	3	7	2	6	0
1	5	1	5	5	0	2	2	5	2	5
4	4	9	4	3	2	8	5	9	6	1
3	5	1	6	7	2	5	5	4	0	6
3	1	8	8	2	5	9	4	0	9	6
1	9	3	9	6	2	6	0	9	9	1
9	5	6	3	0	5	1	6	6	1	2

Suppose $\ell = 7$. The case a_{11}=3 gives a ramified case. So each j=4, 10 gives one $\mathbf{F}_p$-solution of $\Phi_7(X, j) \equiv$ mod11. (At this stage we can't decide whether $\Phi_7(4, 4) \equiv \Phi_7(10, 10) \equiv 0 \bmod 7$ or $\Phi_7(4, 10) \equiv \Phi_7(10, 4) \equiv 0 \bmod 7$. The table above on the right shows that the latter occurs.) The case a_{11}=4 also gives a ramified case. Since h=1 and the conductor is prime to 7, we must have $\Phi_7(2, 2) \equiv \Phi_7(8, 8) \equiv 0 \bmod 11$. The case a_{11}=2 gives the splitting case with class number 2. So in this case we have at least 2, at most 4 solutions of $\Phi_7(i, k) \equiv 0 \bmod 11$. (Actually, the table above on the right shows there are two of them.) The case $a_{11} = 5$ gives the splitting case with class number 1. So in this case we have exactly one solution, that is, $\Phi_7(5, 5) \equiv 0 \bmod 11$. Hence, finally, we get an estimate $2 + 2 + 2 + 1 \le \mathrm{N}(7, 11) \le 2^2 + 2 + 2 + 2 \cdot 2 + 1$, that is, $7 \le \mathrm{N}(7,11) \le 13$. The true value of N(7,11) is 11, by the table above on the right. (As for the value of j corresponding to each a_{11}, we use values of j-invariants of elliptic curves of *CM*-type defined over $\mathbf{Q}$ given for example in [6] p.483. Also we use the value $j(\sqrt{-10}) = 2^6 3^3 5\sqrt{5}(2 + \sqrt{5})^2(4 + 3\sqrt{5})^3$ given in [2] p.408. From this we have $j(\sqrt{-10}) \equiv 7, 9 \bmod 11$. About the case a_p=0 with the conductor 2, we cannot as yet determine whether j=1 really occurs.)

Remark. We give a correction to our previous paper [4] "Computation of the Modular Equation II ". When p=2, the left hand side of Theorem 1 (3) should have the minus sign. This mistake comes from the imprecise formula (*). The right hand side of this formula should have $(-1)^{mm'}$ before $\prod$. Here m' is the degree of F. When n or n' is odd then the sign is plus. So nothing affects in theorem 1 of [4] *II*. But in the case $n=n'=2$ the sign is minus, because $m=m'=3$.

Appendix. $\Phi_n(i,k)$ mod 7 $\quad (0 \le i,k \le p-1)$

The i-th row of each table is the list of $\Phi_n(i-1,k)$ mod 7 $(0 \le k \le 6)$.

Φ_2

6	6	0	1	1	6	1
6	5	4	2	5	5	1
0	4	3	3	3	2	6
1	2	3	3	1	3	1
1	5	3	1	5	0	6
6	5	2	3	0	6	6
1	1	6	1	6	6	0

Φ_3

0	6	5	0	4	5	1
6	2	5	5	2	6	2
5	5	0	3	2	2	4
0	5	3	2	6	1	4
4	2	2	6	5	0	2
5	6	2	1	0	6	1
1	2	4	4	2	1	0

Φ_4

6	1	6	1	6	6	1
1	3	1	6	3	5	1
6	1	0	5	3	4	1
1	6	5	6	3	5	1
6	3	3	3	2	2	1
6	5	4	5	2	4	1
1	1	1	1	1	1	0

Φ_5

6	1	6	6	1	6	1
1	0	6	1	5	6	1
6	6	1	6	4	3	1
6	1	6	3	5	5	1
1	5	4	5	4	0	1
6	6	3	5	0	6	1
1	1	1	1	1	1	0

Φ_6

6	6	0	6	1	1	1
6	5	4	3	6	4	1
0	4	6	0	2	3	1
6	3	0	2	4	1	1
1	6	2	4	0	6	1
1	4	3	1	6	0	1
1	1	1	1	1	1	0

Φ_7

0	1	4	2	2	4	1
1	0	1	4	2	2	4
4	1	0	1	4	2	2
2	4	1	0	1	4	2
2	2	4	1	0	1	4
4	2	2	4	1	0	1
1	4	2	2	4	1	0

Φ_8

6	1	6	6	6	1	1
1	6	5	5	4	4	1
6	5	5	4	1	2	1
6	5	4	5	3	3	1
6	4	1	3	5	4	1
1	4	2	3	4	5	1
1	1	1	1	1	1	0

Φ_9

1	1	1	0	6	6	1
1	1	1	6	4	2	1
1	1	1	6	4	4	1
0	6	6	0	1	2	1
6	4	4	1	1	2	1
6	2	4	2	2	4	1
1	1	1	1	1	1	0

Φ_{10}

6	6	1	6	1	6	1
6	6	1	4	4	3	1
1	1	1	1	2	1	1
6	4	1	6	4	6	1
1	4	2	4	0	2	1
6	3	1	6	2	0	1
1	1	1	1	1	1	0

Φ_{11}

6	6	1	1	1	1	1
6	0	6	2	4	5	1
1	6	3	3	3	5	1
1	2	3	6	3	6	1
1	4	3	3	6	0	1
1	5	5	6	0	6	1
1	1	1	1	1	1	0

Φ_{13}

0	1	4	5	5	4	1
1	5	6	6	2	2	4
4	6	0	2	4	4	2
5	6	2	0	2	2	2
5	2	4	2	2	3	4
4	2	4	2	3	6	1
1	4	2	2	4	1	0

Φ_{17}

1	6	6	1	1	1	1
6	0	1	3	4	6	1
6	1	5	3	1	5	1
1	3	3	5	4	2	1
1	4	1	4	2	5	1
1	6	5	2	5	1	1
1	1	1	1	1	1	0

Φ_{19}

0	6	3	2	5	3	1
6	0	6	5	4	5	4
3	6	0	6	5	2	2
2	5	6	0	3	5	2
5	4	5	3	6	5	4
3	5	2	5	5	1	1
1	4	2	2	4	1	0

Φ_{23}

6	1	1	6	1	6	1
1	0	1	6	4	1	1
1	1	5	2	6	3	1
6	6	2	5	2	6	1
1	4	6	2	5	6	1
6	1	3	6	6	6	1
1	1	1	1	1	1	0

Φ_{29}

6	1	1	6	1	1	1
1	5	3	2	1	1	1
1	3	5	4	6	6	1
6	2	4	6	6	1	1
1	1	6	6	3	0	1
1	1	6	1	0	5	1
1	1	1	1	1	1	0

References

[1] M.Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, Abh. Math. Sem. Univ. Hamburg **14** (1941), 197–272.

[2] R.Fricke, Lehrbuch der Algebra III, Friedr. Vieweg & Sohn, 1928.

[3] 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.

[4] Hideji Ito, 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 Science) **52** (1997), 1–10.

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

[6] J.H.Silverman, Advanced Topics in the Arithmetic of Elliptic Curves, Springer, 1994.

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

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

Department of Mathematics
College of Education, Akita University
Akita 010-8502, Japan