On Ito's Observation on Coefficients of the Modular Polynomial

By Masanobu KANEKO

Graduate School of Mathematics, Kyushu University

(Communicated by Shokichi IYANAGA, M. J. A., May 13, 1996)

1. Introduction. As a result of his extensive computation of the classical modular polynomial, Hideji Ito [5] found interesting congruence properties among coefficients of the polynomial modulo the squares of a certain finite number of primes, and remarked that these primes are precisely the prime factors of the order of the simple group "Monster".

In this note, we shall give an explanation for his observation by employing the well-known fact that the set of primes in question is identical with the set of p's with the property that all the j-invariants of supersingular elliptic curves in characteristic p belong to the prime field $\boldsymbol{F}_p$.

2. Statement and Proof. Let p be a prime number and let $\Phi_p(X, Y)$ denote the p -th modular polynomial, defined by the relation

$$\Phi_p(X, j(\tau)) = (X - j(p\tau)) \prod_{i=0}^{p-1} \left(X - j\left(\frac{\tau + i}{p}\right)\right),$$

where $j(\tau) = q^{-1} + 744 + 196884q + \cdots$ is, in the standard notation, the classical elliptic modular function. The polynomial $\Phi_p(X, Y)$ is symmetric in X and Y with integer coefficients of the form

$$\Phi_p(X, Y) = X^{p+1} + Y^{p+1} + \sum_{m,n=0}^{p} a_{mn} X^m Y^n \quad (a_{mn} \in \boldsymbol{Z}),$$

and satisfies the so-called Kronecker congruence relation:

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

From (1) we conclude

$$a_{11} \equiv a_{pp} \equiv -1 \pmod{p},$$

(in fact, $a_{pp} = -1$) and

$$a_{mn} \equiv 0 \pmod{p} \text{ for } (m, n) \neq (1,1), (p, p).$$

Ito computed $a_{mn} \bmod p^2$ and observed, among others, the following

Fact. *Let p be one of the primes in the set $M = \{p \mid \text{prime}, p \leq 31 \text{ or } p = 41, 47, 59, 71\}$. For $i = 1,2$, assume $0 < m_i, n_i < p$ and $(m_i, n_i) \neq (1, 1)$. If $m_1 + n_1 \equiv m_2 + n_2 \pmod{p-1}$, then*

$$\frac{a_{m_1 n_1}}{p} \equiv \frac{a_{m_2 n_2}}{p} \pmod{p}.$$

He also found that for other primes up to 2617 there always exist pairs (m_i, n_i) with $m_1 + n_1 \equiv m_2 + n_2 \pmod{p-1}$ for which the corresponding congruence for the coefficients does not hold. In the remainder of this paper we give a proof of this Fact, without relying on numerical computation.*)

Consider the following polynomial in one variable:

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

By the congruence relation (1), we have $R(X) \in \boldsymbol{Z}[X]$. Write $R(X) = \sum_{k=0}^{p^2+p} b_k X^k$. Let A be the set of pairs (m, n) satisfying the condition appearing in the statement of the Fact, i.e., $A = \{(m, n) \mid 0 < m, n < p, (m, n) \neq (1,1)\}$.

Lemma. *For $(m, n) \in A$, we have $\frac{a_{mn}}{p} = b_k$, with $k = m + np$. In this case the index k belongs to the set $B = \{k \mid p + 1 < k < p^2, p \nmid k\}$, and the map $(m, n) \mapsto m + np$ gives a bijection between the sets A and B.*

Proof. Note first that the image of the map $A \ni (m, n) \mapsto m + np$ is indeed in B, and if $k \in B$ and $k = m + np$ with $0 \leq m, n \leq p$, then $(m, n) \in A$. The map is injective because m is uniquely determined by $k \bmod p$, and thus $n = (k - m)/p$ is also unique. Since A and B have the same cardinality, $p^2 - 2p$, we obtain the lemma.

Since the congruence $m_1 + n_1 \equiv m_2 + n_2 \pmod{p-1}$ is equivalent to $m_1 + n_1 p \equiv m_2 + n_2 p \pmod{p-1}$, our proof of the Fact is reduced to show the following

Proposition. *Assume $p \in M$ and let $k_1, k_2 \in B$. If $k_1 \equiv k_2 \pmod{p-1}$, then $b_{k_1} \equiv b_{k_2} \pmod{p}$.*

Proof. Let $\bar{R}(X) = R(X) \bmod p \in \boldsymbol{F}_p[X]$. The degree of $\bar{R}(X)$ is at most (and exactly if

*) Note added in proof: Prof. T. Asai at Shizuoka informed the author that his student Hirohito Ninomiya independently obtained a similar proof.