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 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

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

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
$a_{mn} \equiv 0 \pmod{p}$ 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 $R(X) \in \mathbf{Z}[X]$. 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 $\dfrac{a_{mn}}{p} = b_k$, 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 $\bar{R}(X) = R(X) \bmod p \in F_p[X]$. The degree of $\bar{R}(X)$ is at most (and exactly if

$p \nmid 744) p^2 + p - 1$, since $a_{pp} = -1$. The key ingredient of our proof is the following lemma, which is essentially contained in Prop. 1 in Koike [6].

Key Lemma. *We can write $\bar{R}(X)$ as*
$$\bar{R}(X) = (X^{p^2} - X)\Phi(X)$$
$$+ (X^{p^2} - X)\sum_{j_0 \in S}\frac{r_{j_0}}{X - j_0},$$
where $\phi(X) \in \mathbf{F}_p[X]$ is a polynomial of degree no greater than $p - 1$, S is the set of supersingular j-invariants in $\mathbf{F}_{p^2}$ other than 0 and 1728, and $r_{j_0} \in \mathbf{F}_p(j_0) \subset \mathbf{F}_{p^2}$.

For the reader's convenience, we briefly sketch the proof of this lemma (see [6] for the details). Taking into account the degree of $\bar{R}(X)$, the assertion is equivalent to the following fact:

(*) *Suppose $\alpha \in \mathbf{F}_{p^2}$. If $\alpha = 0$, 1728, or an j-invariant of an ordinary elliptic curve, then $\bar{R}(\alpha) = 0$.*

Write $j(p\tau) \equiv j(\tau)^p + p \cdot \gamma \pmod{p^2}$ with suitable element $\gamma \in \mathbf{Q}(j(\tau))$. By the Taylor expansion
$$(0 \equiv)\Phi_p(j(\tau), j(\tau)^p + p\cdot\gamma) \equiv \Phi_p(j(\tau), j(\tau)^p)$$
$$+ p\cdot\gamma\cdot\frac{\partial}{\partial Y}\Phi_p(j(\tau), j(\tau)^p) \mod p^2,$$
we have
$$\bar{R}(X) \equiv -\gamma\cdot\frac{\partial}{\partial Y}\Phi_p(X, X^p) \mod p$$
$$(\gamma = \gamma(X), X = j(\tau)).$$
Since the congruence relation (1) implies
$$\frac{\partial}{\partial Y}\Phi_p(X, X^p) \equiv X^{p^2} - X \mod p,$$
we see that (*) is then equivalent to γ being regular at 0, 1728, and ordinary j-invariants in $\mathbf{F}_{p^2}$. This is well-known, and seems to originate in the work of Igusa [3, p. 472 footnote]. (See also e. g. de Shalit [1], Dwork [2], and Ihara [4] for this and various intimately related subjects.) Returning to the proof of the proposition, recall that $p \in M$ if and only if all the supersingular

j-invariants (which are *a priori* in $\mathbf{F}_{p^2}$) belong to $\mathbf{F}_p$ (Ogg [7]). For $j_0 \in \mathbf{F}_p$, $j_0 \neq 0$, set $h_{j_0}(X) = (X^p - X)/(X - j_0)$. This is a polynomial of degree $p - 1$ having no constant term. (Note that 0 is excluded from the set S in the Key Lemma.) With this we have
$$\frac{X^{p^2} - X}{X - j_0} = h_{j_0}(X)(1 + X^{p-1} + X^{2(p-1)} + \cdots + X^{p(p-1)}).$$

This expression, together with the vanishing of the coefficients of X^k ($p < k < p^2$) in $(X^{p^2} - X) \times \phi(X)$, immediately yields the proposition and hence completes the proof of Ito's observation.

In conclusion, we remark that the other observations made in § 5 of Ito's paper can also be explained by using the above Key Lemma.

References

[1] E. de Shalit: Kronecker's polynomial, supersingular elliptic curves, and p-adic periods of modular curves. Contemporary Math., **165**, 135–148 (1994).

[2] B. Dwork: p-adic Cycles. Publ. Math. IHES, **37**, 27–115 (1969).

[3] J-I. Igusa: Fibre systems of Jacobian varieties III. Amer. J. Math. , **81**, 453–476 (1959).

[4] Y. Ihara: On the differentials associated to congruence relations and the Schwarzian equations defining uniformizations. J. Fac. Sci. Univ. Tokyo, **21**, 309–332 (1974).

[5] H. Ito: Computation of the modular equation. Proc. Japan Acad. , **71A**, 48–50 (1995).

[6] M. Koike: Congruences between modular forms and functions and applications to the conjecture of Atkin. J. Fac. Sci. Univ. Tokyo, **20**, 129–169 (1973).

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