AMM v. 75 (1968)

THE FACTORIZATION OF THE CYCLOTOMIC POLYNOMIALS MOD p

W. J. GUERRIER, University of Hawaii

Let n be a positive integer and denote by $F_n(X)$ the cyclotomic polynomial of order n. In teaching courses in algebraic number theory, I have found the theorem below on the factorization of $F_n(X)$ mod p very useful. I do not know, however, of any simple reference for this theorem. The object of this note is to provide such a reference.

THEOREM. *Let p be a prime and suppose that $p \nmid n$. Denote by ϕ the Euler ϕ-function.*

(i) *Set f = the (multiplicative) order of p* mod n. *Then $F_n(X)$ factors* mod p *into a product of $\phi(n)/f$ distinct irreducible polynomials each of degree f.*

(ii) *For any positive integer, r, $F_{p^r n}(X) = F_n(X)^{\phi(p^r)}$* (mod p).

Proof. (i): Denote by Z_p the field of p elements and let K be the splitting field over Z_p of the polynomial $X^{p^f} - X$. Since $n \mid p^f - 1$, K contains the nth roots of unity. Let ζ be a primitive nth root of unity. The map $x \rightarrow x^p$ is a generator for the Galois group of K/Z_p. Thus the minimal polynomial of ζ over Z_p is

$$(X - \zeta)(X - \zeta^p) \cdots (X - \zeta^{p^{f-1}})$$

and therefore $F_n(X)$ has an irreducible factor of degree f mod p.

Now choose another primitive nth root of unity η not among $\zeta, \zeta^p, \cdots, \zeta^{p^{f-1}}$. (Note that since $p \nmid n$, ξ^{p^i} is a primitive nth root of unity.) The polynomial

$$(X - \eta)(X - \eta^p) \cdots (X - \eta^{p^{f-1}})$$

is then a second irreducible factor of $F_n(X)$ of degree f. Continuing this process one arrives at the desired conclusion.

(ii): Let $\eta_1, \eta_2, \cdots, \eta_s$ ($s = \phi(n)$) be the primitive nth roots of unity and let ζ be a primitive $p^{r\text{th}}$ root of unity. Since $(n, p) = 1$ each of the elements $(\eta_i \zeta^j)^{p^r}$ $i = 1, \cdots, s$, $j = 1, \cdots, p^r$ is a primitive nth root. On the other hand for $(j, p) = 1$, $\eta_i \zeta^j$ is a primitive $p^r n$th root of unity and for $p \mid j$, $(\eta_i \zeta^j)^{p^{r-1}}$ is a primitive nth root. Thus one has

$$F_n(X^{p^r}) = \prod_{i,j} (X - \eta_i \zeta^j) = \prod_{\substack{i,j \\ (j,p)=1}} (X - \eta_i \zeta^j) \cdot \prod_{\substack{i,j \\ p \mid j}} (X - \eta_i \zeta^j)$$

$$= F_{p^r n}(X) \cdot F_n(X^{p^{r-1}}).$$

Therefore,

$$F_{p^r n}(X) = F_n(X^{p^r}) / F_n(X^{p^{r-1}}) \underset{(\text{mod } p)}{\equiv} F_n(X)^{p^r} / F_n(X)^{p^{r-1}}$$

$$= F_n(X)^{p^{r-1}(p-1)} = F_n(X)^{\phi(p^r)}.$$

This completes the proof of the theorem.