NOTE ON THE PERIOD OF A MARK IN A FINITE FIELD

BY MORGAN WARD

1. *Introduction.* If p is a fixed prime, and

$$F(x) = x^k - c_1x^{k-1} - \cdots - c_k,$$

where $c_1, \cdots, c_k$ are rational integers, is a polynomial which is irreducible modulo p, the period of a mark α associated with the polynomial $F(x)$ in the finite field $\mathfrak{F}$ of order p^k is fundamental not only in the theory of finite fields,* but also in many allied arithmetical investigations involving recurring series.†

Our information about the actual value of this period is disappointingly meagre beyond the well known facts that it is a divisor of p^k-1 and that there actually exist polynomials $F(x)$ for which the period equals p^k-1. I prove here the following additional result.

THEOREM. *Let τ denote the period of a mark α associated with the irreducible polynomial $F(x)$ modulo p in the finite field $\mathfrak{F}$ of order p^k, and let ω be the least positive value of n such that α^n is congruent to a rational integer modulo p.‡ Then $\tau = \delta\theta\omega$, where θ is the exponent to which norm α belongs modulo p, while δ is an integer dividing the greatest common divisor of k and $p-1$, and multiplying the greatest common divisor of θ and the integer $\sigma = (p^k-1)/(\omega(p-1))$.*

---

* See, for example, Dickson, *Linear Groups*, 1901, Chapters 1–3.

† If $\Omega_{n+k} = c_1\Omega_{n+k-1} + \cdots + c_k\Omega_n$ is the difference equation associated with the polynomial $F(x)$, the period of α is the period modulo p of every sequence of rational integers satisfying the difference equation. (See Ward, Transactions of this Society, vol. 35 (1933), pp. 600–628, and the references given there.) The period of α is also the rank of apparition of the prime p for the number $\Delta_n = \pm\mathrm{Res}\{x^n-1, F(x)\}$ studied recently by D. H. Lehmer and others. (Annals of Mathematics, (2), vol. 34 (1933), pp. 461–479.)

‡ In the case $k=2$, ω is the rank of apparition of the prime p for the Lucas function U_n associated with the polynomial $x^2-c_1x-c_2$ (D. H. Lehmer, Annals of Mathematics, (2), vol. 31 (1930), p. 422). In the general case, ω has been termed the restricted period of $F(x)$ modulo p (R. D. Carmichael, Quarterly Journal of Mathematics, vol. 48 (1920), p. 354).