NOTE ON THE PERIOD OF A MARK IN A FINITE FIELD

BY MORGAN WARD

1. Introduction. If \( p \) is a fixed prime, and

\[ F(x) = x^k - c_1 x^{k-1} - \cdots - c_k, \]

where \( c_1, \ldots, c_k \) are rational integers, is a polynomial which is irreducible modulo \( p \), the period of a mark \( \alpha \) associated with the polynomial \( F(x) \) in the finite field \( \mathcal{F} \) 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 \( \tau \) denote the period of a mark \( \alpha \) associated with the irreducible polynomial \( F(x) \) modulo \( p \) in the finite field \( \mathcal{F} \) of order \( p^k \), and let \( \omega \) be the least positive value of \( n \) such that \( \alpha^n \) is congruent to a rational integer modulo \( p \).‡ Then \( \tau = \delta \theta \omega \), where \( \theta \) is the exponent to which norm \( \alpha \) belongs modulo \( p \), while \( \delta \) is an integer dividing the greatest common divisor of \( k \) and \( p - 1 \), and multiplying the greatest common divisor of \( \theta \) 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 \( \alpha \) 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 \( \alpha \) is also the rank of apparition of the prime \( p \) for the number \( \Delta_n = \pm \text{Res} \{ x^n - 1, F(x) \} \) studied recently by D. H. Lehmer and others. (Annals of Mathematics, (2), vol. 34 (1933), pp. 461–479.)
‡ In the case \( k = 2 \), \( \omega \) is the rank of apparition of the prime \( p \) for the Lucas function \( U_n \) associated with the polynomial \( x^2 - c_1 x - c_2 \) (D. H. Lehmer, Annals of Mathematics, (2), vol. 31 (1930), p. 422). In the general case, \( \omega \) has been termed the restricted period of \( F(x) \) modulo \( p \) (R. D. Carmichael, Quarterly Journal of Mathematics, vol. 48 (1920), p. 354).
2. Proof of the Theorem. We write as usual \( a \mid b \) for \( a \) divides \( b \), and \((a, b)\) for the greatest common divisor of \( a \) and \( b \). Denote the roots of \( F(x) = 0 \) in the finite field \( \mathcal{F} \) by \( \alpha, \alpha^p, \cdots, \alpha^{p(k-1)} \). Then

\[
\text{norm} \, \alpha \equiv \alpha^q \, (p),
\]

where \( q = 1 + p + p^2 + \cdots + p^{k-1} \).

As in the theorem, let \( \omega \) denote the least positive value of \( n \) such that \( \alpha^n \) is congruent to a rational integer modulo \( p \). Then every other such \( n \) is readily seen to be divisible by \( \omega \). In particular,

\[
\sigma = \frac{q}{\omega} = \frac{(p^k - 1)}{(\omega(p - 1))}
\]

is a rational integer, and

\[
\text{norm} \, \alpha \equiv M^\sigma \, (p),
\]

where \( \alpha^\sigma \equiv M \, (p), \, (1 \leq M \leq p-1) \).

Let \( \lambda \) be the exponent to which \( M \) belongs modulo \( p \), \( \theta \) the exponent to which \( \text{norm} \, \alpha \) belongs modulo \( p \), and \( \tau \) the period of \( \alpha \) in \( \mathcal{F} \). Then

\[
\tau = \delta \theta \omega,
\]

where \( \delta = (\lambda, \sigma) \).

For since \( \alpha^\lambda = M^\lambda \equiv 1 \, (p) \), \( \tau \mid \lambda \omega \), and since \( \alpha^\sigma \) is congruent to a rational integer modulo \( p \), \( \omega \mid \tau \). Therefore, \( \tau = \nu \omega \), where \( \nu \mid \lambda \). Then \( \alpha^\sigma = \alpha^\nu \equiv M^\nu \equiv 1 \, (p) \), so that \( \nu \mid \lambda \). Hence \( \nu = \lambda, \tau = \lambda \omega \).

Now write \( \lambda = \delta \lambda', \sigma = \delta \sigma', \) where \( (\lambda, \sigma) = \delta, \, (\lambda', \sigma') = 1 \). Then

\[
(\text{norm} \, \alpha)^{\lambda'} = M^{\lambda' \nu} = M^{\lambda' \sigma'} \equiv 1 \, (p),
\]

so that \( \theta \mid \lambda' \). Moreover, we have \( M^{\theta \nu} = (\text{norm} \, \alpha)^{\theta} \equiv 1 \, (p) \), so that \( \lambda \mid \theta \sigma, \lambda' \mid \theta \sigma', \lambda' \mid \theta \sigma', \lambda' \mid \theta \). Therefore \( \lambda' = \theta \) and \( \lambda = \delta \lambda' = \delta \theta, \tau = \lambda \omega = \delta \theta \omega \). Finally,

\[
(1) \quad \tau = \delta \theta \omega,
\]

(2) \quad \delta \mid (k, p - 1).

For since \( \theta \mid \lambda, \, (\theta, \sigma) \mid (\lambda, \sigma) = \delta, \) and since

\[
q = ((p - 1 + 1)^k - 1)/(p - 1) \equiv k \, (p - 1),
\]

we have \( (q, p - 1) = (k, p - 1) \). Therefore, since \( \delta \mid \lambda \mid p - 1 \) and \( \delta \mid \sigma \mid q, \delta \mid (q, p - 1) \), it follows that \( \delta \mid (k, p - 1) \). Equations (1) and (2) give us our theorem.

3. Conclusion. To illustrate the theorem, consider the Fibo-
nacci series $0, 1, 1, 2, 3, 5, 8, 13, \cdots$ giving the values of the Lucas function $U_n$ associated with the polynomial $x^2 - x - 1$. This polynomial is irreducible modulo 13, so that the period of the Fibonacci series modulo 13 gives the period of the mark $\alpha$ associated with $x^2 - x - 1$ in the finite field of order $13^2$. We have $\omega = 7$, norm $\alpha = -1$, $\theta = 2$, $k = 2$, $\sigma = 2$, $p - 1 = 12$. Hence (2) becomes $(2, 2) \mid \delta \mid (2, 12)$, so that $\delta = 2$. Hence the period is 28, which is easily verified directly. It seems quite difficult to determine the exact value of $\delta$ in all cases.*

California Institute of Technology

---

ON A PROBLEM OF KNASTER AND ZARANKIEWICZ†

BY J. H. ROBERTS

Knaster and Zarankiewicz have proposed the following problem:‡ "Does every continuum $A$ contain a subcontinuum $B$ such that $A - B$ is connected?" Knaster has shown,§ by an example in 3-space, that the answer is in the negative. In the present paper an example is given of a plane continuum $M$ such that every non-degenerate proper subcontinuum of $M$ disconnects $M$.

The point sets considered in this paper all lie in a plane.

Definition of $F(C; X, Y; \varepsilon)$. Let $C$ be any simple closed curve, $X$ and $Y$ distinct points of $C$, and $\varepsilon$ any positive number. There exists a finite set of points $A_1, A_2, \cdots, A_n$, $(n > 2)$, such that (a) $A_1 + A_2 + \cdots + A_n$ contains $X + Y$, (b) $A_1, A_2, \cdots, A_n$ lie on $C$ in the order $A_1A_2 \cdots A_nA_1$, and (c) $A_\ell$ and $A_{\ell+1}$ (subscripts are to be reduced modulo $n$) are the end points of an arc $t_\ell$ of diameter $< \varepsilon$ which is a subset of $C$ not containing $A_{\ell+2}$. There exists a set of mutually exclusive arc segments $v_1, v_2, \cdots, v_n$ lying within $C$ such that $v_i + t_i$ is a simple closed curve $w_i$ of diameter $< \varepsilon$. Let $J$ denote the simple closed curve

* See the discussion at the close of my paper, Transactions of this Society, vol. 33 (1931), p. 165.
† Presented to the Society, December 1, 1933.
‡ Fundamenta Mathematicae, vol. 8 (1926), Problem 42, p. 376.