FUNCTIONS OVER THE RESIDUE FIELD MODULO A PRIME

DAVID LONDON and ZVI ZIEGLER

(Received 17 March 1966)

Introduction

Let F_p be the residue field modulo a prime number p. The mappings of F_p into itself are viewed as *functions in one variable over* F_p. When the mapping is onto, the function is a *permutation.*

In this paper we consider representations of functions over F_p as polynomials over F_p. Henceforth, we shall omit the domain and unless otherwise indicated, the domain is understood to be F_p. In section 1 we prove that every function in one variable admits of a unique representation as a polynomial of degree $\leqq p-1$ in one variable. Explicit expressions for the coefficients of a polynomial representing a given function are obtained. The main results of the paper are presented in section 2, where we obtain necessary and sufficient conditions for the coefficients of a polynomial in order that it should represent a permutation. From these conditions we derive some general conclusions about the nature of the coefficients of a polynomial representing a permutation. In section 3 we apply the foregoing analysis to the special circumstances F_3, F_5 and F_7.

This paper was written within the framework of a seminar in Algebra held in the Technion in 1959 under the guidance of Professor Dov Tamari. We are grateful to Professor Tamari for suggesting to us the topic of this research.

I. The representation of a function in one variable as a polynomial

Let a function $\phi(x)$ be given by the mapping

$$j \to i_j, \qquad j = 0, \cdots, p-1;\ i_j \in F_p.$$

We prove first that the function admits of a representation by a polynomial of degree $\leqq p-1$ and that such a representation is unique.

The polynomial

$$P(x) = \sum_{k=1}^{p} a_{p-k} x^{p-k}, \qquad a_{p-k} \in F_p$$

https://doi.org/10.1017/S1446788700004213 Published online by Cambridge University Press

represents the function $\phi(x)$ if, and only if

$$\phi(j) = P(j), \qquad j = 0, \cdots, p-1.$$

Hence, the necessary and sufficient conditions for such a representation are:

$$P(j) = \sum_{k=1}^{p} a_{p-k} j^{p-k} = i_j, \qquad j = 0, \cdots, p-1. \tag{1.1}$$

The determinant of this system is $\Delta =$

$$\begin{vmatrix} 0 & \cdots & 0 & 0 & 1 \\ 1^{p-1} & \cdots & 1^2 & 1 & 1 \\ 2^{p-1} & \cdots & 2^2 & 2 & 1 \\ \vdots & & \vdots & \vdots & \vdots \\ (p-1)^{p-1} & \cdots & (p-1)^2 & p-1 & 1 \end{vmatrix} = \begin{vmatrix} 1 & 1^{p-2} & \cdots & 1^2 & 1 \\ 1 & 2^{p-2} & \cdots & 2^2 & 2 \\ 1 & 3^{p-2} & \cdots & 3^2 & 3 \\ \vdots & \vdots & & \vdots & \vdots \\ 1 & (p-1)^{p-2} & \cdots & (p-1)^2 & (p-1) \end{vmatrix}.$$

The equality of the determinants follows by Fermat's Theorem [1, p. 48]. Since the right-hand side determinant is essentially the Van-der-Monde and p is a prime, we have $\Delta \neq 0$. This proves the existence and uniqueness of the representation.

We next obtain explicit expressions for the coefficients of the representing polynomial. It is well known [see 1, p. 122] that

$$\sum_{j=1}^{p-1} j^k = \begin{cases} 0 \text{ when } k \not\equiv 0 \pmod{p-1} \\ -1 \text{ when } k \equiv 0 \pmod{p-1}. \end{cases} \tag{1.2}$$

For each fixed k, $k = 1, \cdots, p-1$, we multiply the j-th equation of (1.1) by j^{k-1}, $j = 0, \cdots p-1$. We sum the equation thus obtained by columns and make use of (1.2). Thus we find

$$a_{p-k} = -\sum_{j=0}^{p-1} j^{k-1} i_j, \qquad k = 1, \cdots, p-1. \tag{1.3}$$

Clearly, we have also

$$a_0 = i_0. \tag{1.4}$$

This completes the proof of

THEOREM 1. *Let $\phi(x)$ be any function over F_p; it admits of a unique representation by a polynomial of degree $\leqq p-1$ over F_p. The coefficients of this polynomial are given explicitly by* (1.3) *and* (1.4).

II. The polynomial representation of a permutation

In this section we obtain necessary and sufficient conditions for the coefficients of a polynomial in order that it represents a permutation. We

https://doi.org/10.1017/S1446788700004213 Published online by Cambridge University Press

first obtain a system of necessary conditions for the coefficients. Later we show that these conditions are also sufficient.

Suppose that the polynomial $P(x)=\sum_{k=1}^{p} a_{p-k}x^{p-k}$ represents a permutation. Then the values $P(j)=i_j$, $j=0,\cdots,p-1$, run over the full residue class mod p, so that

$$\sum_{j=0}^{p-1} i_j = 0. \tag{2.1}$$

Combining (2.1) with (1.3) for $k=1$, we find the first necessary condition,

$$a_{p-1} = 0. \tag{A.1}$$

We rewrite now the system (1.1) in the form

$$\sum_{k=2}^{p} a_{p-k} j^{p-k} = i_j - i_0 = i'_j, \qquad j = 1,\cdots,p-1. \tag{2.2}$$

Since the numbers i_j, $j=0,\cdots,p-1$, cover the full residue class mod p, the numbers i'_j, $j=1,\cdots,p-1$, cover the residue class without the zero. We square each equation of (2.2) and sum the resulting $p-1$ equations by columns. Since the numbers i'_j run over the residue class without the zero, we see, by (1.2), that the coefficient of the $(p-1)$-th power has to vanish. This yields

$$a^2_{(p-1)/2}+2a_{p-2}a_1+\cdots+2a_{(p+1)/2}a_{(p-3)/2}=0. \tag{A.2}$$

Similarly, by raising each of the equations in (2.2) to the $3,\cdots,(p-1)$-th powers, we obtain the rest of the conditions.

The k-th condition, $k=2,\cdots,p-2$, has the form

$$\sum \frac{k!}{i_1!\cdots i_{p-1}!}\, a_1^{i_1}\cdots a_{p-1}^{i_{p-1}} = 0, \qquad k=2,\cdots,p-2, \tag{A. k}$$

where the summation extends over the $(p-1)$-tuples $(i_1,\cdots,i_{p-1})$, $0 \leqq i_1,\cdots,i_{p-1} \leqq k$, which satisfy the conditions

$$\begin{aligned} &i_1+\cdots+i_{p-1}=k \\ &i_1+2i_2+\cdots+(p-1)i_{p-1} \equiv 0 \pmod{p-1}. \end{aligned} \tag{2.3}$$

The last condition has the form

$$\sum \frac{(p-1)!}{i_1!\cdots i_{p-1}!}\, a_1^{i_1}\cdots a_{p-1}^{i_{p-1}} = +1 \tag{A. $p-1$}$$

where $(i_1,\cdots,i_{p-1})$ satisfy (2.3) with k replaced by $p-1$.

REMARKS. a) Taking into consideration condition (A.1), we can put $i_{p-1}=0$ in the conditions (A.2)$-$(A. $p-1$).

b) None of the $(p-1)$ conditions involves a_0.

c) Condition (A. $p-1$) is satisfied for every polynomial which attains the value i_0 exactly once.

We now prove that the conditions (A.1)—(A. $p-1$) are sufficient conditions for the corresponding polynomial to represent a permutation. Let $P(x)$ be a polynomial whose coefficients satisfy (A.1)—(A. $p-1$). Denoting by l_j the values

$$l_j = P(j)-P(0), \qquad j = 1, \cdots, p-1,$$

we find that they satisfy:

$$(2.4) \qquad \begin{cases} \sum_{j=1}^{p-1} l_j^k = 0, & k = 1, \cdots, p-2, \\ \sum_{j=1}^{p-1} l_j^{p-1} = -1. \end{cases}$$

We construct the Van-der-Monde built on $l_1, \cdots, l_{p-1}$,

$$V = \begin{vmatrix} 1 & \cdots & 1 \\ l_1 & \cdots & l_{p-1} \\ \vdots & & \vdots \\ l_1^{p-2} & \cdots & l_{p-1}^{p-2} \end{vmatrix}.$$

Equations (2.4) imply that

$$V^2 = \begin{vmatrix} -1 & 0 & \cdots & & 0 \\ 0 & 0 & \cdots & 0 & -1 \\ 0 & 0 & \cdots & -1 & 0 \\ \vdots & \vdots & & & \vdots \\ 0 & -1 & 0 & \cdots & 0 \end{vmatrix} = \pm 1.$$

Hence,

$$(2.5) \qquad V = \prod_{j>k} (l_j - l_k) \neq 0$$

so that l_j, $j = 1, \cdots, p-1$ have to be distinct. Therefore, they take all the values of the residue class mod p except the zero. Thus, $P(0)$ and $P(j) = P(0)+l_j$, $j = 1, \cdots, p-1$, run over the entire residue class. We have thus proved

THEOREM 2. *Necessary and sufficient conditions for the polynomial* $P(x) = \sum_{k=1}^{p} a_{p-k} x^{p-k}$ *to represent a permutation are that its coefficients satisfy* (A.1)—(A. $p-1$).

We now make some general observations concerning the coefficients of a polynomial $P(x)$ representing a permutation. Let $(p-1)/k$ be a natural number larger than 1. By considering the necessary condition (A. k) we

https://doi.org/10.1017/S1446788700004213 Published online by Cambridge University Press

find that in this condition a_j^k appears as a summand if, and only if j has one of the values

$$\frac{i(p-1)}{k}, \qquad i = 1, \cdots, k.$$

Furthermore, if $k_1, \cdots, k_l$ satisfy

$$\frac{i_0(p-1)}{k} < k_j < \frac{(i_0+1)(p-1)}{k}, \qquad j = 1, \cdots, l,$$

for some i_0, $0 \leqq i_0 \leqq k-1$, then there is no summand of the form $a_{k_1}^{ik_1} \cdots a_{k_l}^{ik_l}$. These considerations yield

Corollary 2.1. *Let $P(x) = \sum_{k=1}^{p} a_{p-k} x^{p-k}$ be a polynomial representing a permutation; let k be a divisor of $p-1$ (different from $p-1$), and let i_0 be some integer, $0 \leqq i_0 \leqq k-1$. If $a_j = 0$ for every j satisfying one of the inequalities*

$$\frac{(i_0+1)(p-1)}{k} < j \tag{2.6}$$

or

$$\frac{i_0(p-1)}{k} \geqq j, \tag{2.7}$$

then

$$a_{(i_0+1)(p-1)/k} = 0. \tag{2.8}$$

For $i_0 \neq 0$, we also have:

If $a_j = 0$ for every j satisfying one of the inequalities

$$\frac{(i_0+1)(p-1)}{k} \leqq j \tag{2.6'}$$

or

$$\frac{i_0(p-1)}{k} > j, \tag{2.7'}$$

then

$$a_{i_0(p-1)/k} = 0. \tag{2.8'}$$

Since we may choose $a_0 = 0$ without loss of generality, the result formulated in (2.6), (2.7) and (2.8) for $i_0 = 0$, yields

Corollary 2.2 *The actual degree of a polynomial representing a permutation can never be $(p-1)/k$.*

Since $a_{p-1} = 0$ is always satisfied, the result formulated in (2.6'), (2.7') and (2.8') for $i_0 = k-1$, yields

Corollary 2.3. *The exponent of the lowest power appearing in a polynomial representing a permutation cannot be equal to* $((k-1)(p-1))/k$, $k > 1$.

Since the number $p-1$ is always divisible by 1, 2, $(p-1)/2$, we have

Corollary 2.4. *a) The actual degree of a polynomial representing a permutation cannot be* $p-1$. *(This amounts to a rephrasing of condition* (A.1).*)*

b) The actual degree of a polynomial representing a permutation can never be $(p-1)/2$; *the exponent of the lowest power appearing in a polynomial representing a permutation is never* $(p-1)/2$.

c) A polynomial of actual degree 2 cannot represent a permutation; if the lowest power appearing in a polynomial is $p-3$, *it cannot represent a permutation.*

A similar analysis yields

Corollary 2.5. *The polynomial* $P(x) = x^k$ *represents a permutation if, and only if* $(k, p-1) = 1$.

This last corollary can also be derived directly by using the fact that the multiplicative group is cyclic.

It is clear that if $P(x)$ is a polynomial representing a permutation, then $aP(x)+b$, $a \neq 0$, is also, such a polynomial. In particular:

All the linear polynomials $P(x) = ax+b$, $a \neq 0$ represent permutations.

III. A detailed discussion of F_3, F_5 and F_7

a) Let $p = 3$. There are $3! = 6$ permutations. The number of linear polynomials is $3\times 2 = 6$. Since every linear polynomial represents a permutation, we see that in this case the linear polynomials are the only polynomials representing permutations.

b) Let $p = 5$. In this case, the number of permutations is $5! = 120$, while the number of linear polynomials is only $5\times 4 = 20$. Hence, there exist 100 non-linear polynomials representing permutations. Corollary 2.4 implies that neither second degree polynomials nor fourth degree polynomials can represent permutations. The system of necessary and sufficient conditions for this case is

$$a_4 = 0 \tag{3.1}$$

$$a_2^2+2a_1a_3 = 0 \tag{3.2}$$

$$a_2(a_1^2+a_3^2) = 0 \tag{3.3}$$

$$a_3^4+a_2^4+a_1^4+6a_3^2a_1^2+12a_3a_2^2a_1 = 1. \tag{3.4}$$

It can be easily verified that there exist $(4\times 5+5)\times 5$ distinct polynomials satisfying (3.1) and (3.2). Five of these are constants (not satisfying (3.4)) and the remaining 120 are theefore the polynomials representing per-

https://doi.org/10.1017/S1446788700004213 Published online by Cambridge University Press

mutations. Hence, (3.1), (3.2) and (3.4) are the necessary and sufficient conditions. This is an example demonstrating that the system of conditions (A.1)—(A. $p-1$) is ***not independent*** in general. We do not know how to find an independent system for general p.

c) Let $p = 7$. The number of permutations is $7! = 5040$, while the number of linear polynomials is only $7 \times 6 = 42$. Corollary 2.4 rules out polynomials of degrees 2, 3 and 6 thus leaving 4998 fifth and fourth degree polynomial representing permutations (e.g., $P(x) = x^5$ or, $P(x) = 3x^4 + 4x^3 + 2x^2$). Analysis of the system (A.1)—(A. $p-1$) is complicated in this case, and therefore will not be discussed in detail.

Reference

[1] I. M. Vinogradov, *Elements of Number Theory* (Dover, 1949).

Technion, Haifa