A THEOREM ON PERMUTATIONS IN A FINITE FIELD

L. CARLITZ

Let F_q denote the finite field of order q, where $q=p^n$ is odd. Put $\psi(a)=+1$, -1 or 0 according as a is a nonzero square, a non-square or 0 in F_q. Then we have

$$\psi(a) = a^m, \tag{1}$$

where $q=2m+1$. A polynomial $f(x)$ with coefficients in F_q is called a permutation polynomial if the numbers $f(a)$, $a\in F_q$, are distinct. For references see [**1**, Chapter 18; **2**, Chapter 5].

The following theorem answers a question raised by W. A. Pierce in a letter to the writer.

THEOREM. *Let $f(x)$ be a permutation polynomial such that*

$$f(0) = 0, \qquad f(1) = 1 \tag{2}$$

and

$$\psi(f(a) - f(b)) = \psi(a - b) \tag{3}$$

for all a, $b\in F_q$. Then we have

$$f(x) = x^{p^j} \tag{4}$$

for some j in the range $0\leqq j<n$.

PROOF. For fixed $c\in F_q$ put

$$y = f(c + x) - f(c). \tag{5}$$

It follows from the hypothesis that when x runs through the nonzero squares of F_q the same is true of y; a like result holds for the nonsquares. Thus, if u is an indeterminate, we have

$$\prod_{\psi(x)=1} \{u - f(c + x)\} = \prod_{\psi(y)=1} \{u - f(c) - y\}.$$

Now it is familiar that

$$\prod_{\psi(x)=1} (u - x) = u^m - 1.$$

Consequently

Received by the editors April 15, 1959 and, in revised form, August 1, 1959.

$$\prod_{\psi(x)=1} \{u - f(c+x)\} = (u - f(c))^m - 1. \tag{6}$$

Similarly we have

$$\prod_{\psi(x)=-1} \{u - f(c+x)\} = (u - f(c))^m + 1. \tag{7}$$

Combining (6) and (7) we get

$$\prod_{x \in F_q} \{u - f(c+x)\}^{\psi(x)} = \frac{(u - f(c))^m - 1}{(u - f(c))^m + 1}, \tag{8}$$

the product in the left member extending over all x in F_q. From (8) we get

$$\begin{aligned} \sum_{x \in F_q} \frac{\psi(x)}{u - f(c+x)} &= \frac{m(u - f(c))^{m-1}}{(u - f(c))^m - 1} - \frac{m(u - f(c))^{m-1}}{(u - f(c))^m + 1} \\ &= -\frac{(u - f(c))^{m-1}}{(u - f(c))^{2m} - 1} \\ &= -\frac{(u - f(c))^m}{u^{2m+1} - u}, \end{aligned}$$

so that

$$\sum_{x \in F_q} \psi(x) \frac{u^q - u}{u - f(c+x)} = -(u - f(c))^m.$$

Since $u^q - u = [u - f(x+c)]^q - [u - f(x+c)]$, the left member becomes

$$\begin{aligned} \sum_{x \in F_q} \psi(x)\{(u - f(c+x))^{2m} - 1\} &= \sum_{x \in F_q} \psi(x)(u - f(c+x))^{2m} \\ &= \sum_{x \in F_q} \psi(x - c)(u - f(x))^{2m} \end{aligned}$$

and therefore

$$\sum_{x \in F_q} \psi(x - c)(u - f(x))^{2m} = -(u - f(c))^m. \tag{9}$$

Expanding each side of (9) we evidently obtain

$$\sum_{x \in F_q} (x - c)^m f^r(x) = 0 \qquad (1 \leqq r < m), \tag{10}$$

$$C_{2m,m-r} \sum_{x \in F_q} (x - c)^m f^{m+r}(x) = (-1)^{m+1} C_{m,r} f^r(c) \qquad (0 \leqq r \leqq m). \tag{11}$$

Since, by (3), $f^m(x) = x^m$, (11) may be written as

$$C_{2m,m-r}\sum_{x\in F_q}(x-c)^m x^m f^r(x) = (-1)^{m+1}C_{m,r}f^r(c) \qquad (0 \leqq r \leqq m). \tag{12}$$

Put

$$f^r(x) = \sum_{j=1}^{2m-1} b_j^{(r)} x^j \qquad (1 \leqq r < 2m); \tag{13}$$

where the right member denotes the reduced form of $f^r(x)$, that is, the residue of $f^r(x)$ (mod $x^q - x$); by a known property of permutation polynomials [2, p. 59] the degree is indeed less than $2m$. We now substitute from (13) in (10) and (12) and recall that [2, p. 54] for all $s \geqq 1$

$$\sum_{x\in F_q} x^s = \begin{cases} -1 & (q-1 \mid s), \\ 0 & (\text{otherwise}). \end{cases}$$

It follows from (10) that

$$C_{m,s}b_{m+s}^{(r)} = 0 \qquad (1 \leqq r < m;\ 0 \leqq s \leqq m), \tag{14}$$

and from (12) that

$$(-1)^s C_{2m,m-r}b_s^{(r)} = (-1)^m C_{m,r}b_s^{(r)} \qquad (0 \leqq r \leqq m;\ 0 \leqq s \leqq 2m). \tag{15}$$

If q is a prime, the binomial coefficients $C_{m,s}$ are all prime to q and (14) implies $\deg f^r(x) < m$ for $1 \leqq r < m$. But if $\deg f(x) = k > 1$, there is a least positive integer $r < m$ such that $\deg f^r(x) = rk \geqq m$. Hence $\deg f(x) = 1$, so that by (2) $f(x) = x$ and the theorem is proved for this case.

The general case is more troublesome. Let M denote the set of integers of the form

$$a_0 + a_1 p + \cdots + a_{n-1}p^{n-1} \qquad (0 \leqq a_j \leqq (p-1)/2),$$

where $q = p^n$. It is familiar that the binomial coefficient $C_{m,t}$ is prime to p if and only if $t \in M$ (for proof see [5, p. 52]). If $r \in M$, $r < m$, it is evident from (15) that $\deg f^r(x) < m$; if also $s \notin M$ then (15) implies $b_s^{(r)} = 0$. Therefore, when $r \in M$, $r < m$, the only nonzero terms in the right member of (13) are those for which $j \in M$.

Since

$$f(x)f^{m-1}(x) = f^m(x) = x^m, \tag{16}$$

and since $f(x)$ and $f^{m-1}(x)$—in reduced form—are of degree $< m$, it follows from (16) that $f(x) = x^k$ for some $k \in M$, $k < m$. Put

$$k = k_0 + k_1 p + \cdots + k_{n-1}p^{n-1} \qquad (0 \leqq k_j < (p-1)/2).$$

Then, in the first place, if the largest $k_i \geqq 2$, take the least r such that $rk_i > p/2$; this implies $kr \notin M$, but $r \in M$ so that we have a contradiction. In the second place, if all $k_i \leqq 1$, but $k \neq p^i$, then

$$k = p^s + \cdots + p^t \qquad (0 \leqq s < t < n).$$

It follows that the residue (mod $q-1$) of

$$(1 + (p - 1)p^{n-t}/2)k$$

is not in M, while

$$1 + (p - 1)p^{n-t}/2 \in M.$$

Hence if

$$1 + (p - 1)p^{n-t}/2 < m, \tag{17}$$

we again have a contradiction. It is easily verified that (17) holds except for $q=3$ or 9. The case $q=3$ has already been disposed of. As for $q=9$, it is clear that $k=4$ cannot occur. Consequently $k=p^i$ and the theorem is proved.

The referee has kindly called the writer's attention to papers by Järnefelt [4] and Kustaanheimo [5] which are related to the subject matter of the present note.

The writer is indebted to Professor Pierce for many helpful comments.

References

1. L. E. Dickson, *History of the theory of numbers*, vol. 3, Washington, 1923.

2. ———, *Linear groups*, Leipzig, 1901.

3. G. Järnefelt, *Reflections on a finite approximation to Euclidean geometry. Physical and astronomical prospects*. Ann. Acad. Sci. Fenn. Ser. A. I. no. 96 (1951).

4. P. Kustaanheimo, *On the relation of order in geometries over a Galois field*, Soc. Sci. Fenn. Comment Phys.-Math. vol. 20 no. 8 (1957).

5. E. Lucas, *Sur les congruences des nombres eulériennes et des coefficients différentiels des fonctions trigonométriques, suivant un module premier*, Bull. Soc. Math. France vol. 6 (1878) pp. 49–54.

Duke University