27. *On the Number of Distinct Values of a Polynomial with Coefficients in a Finite Field*

By Leonard CARLITZ
Department of Mathematics, Duke University, U.S.A.
(Comm. by Z. SUETUNA, M.J.A., March 12, 1955)

1. Let $GF(q)$ denote the finite field of order $q=p^\nu$ and put

$$f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x \qquad (a_j \in GF(q)), \tag{1.1}$$

where $1<n<p$. Let $V=V(f)$ denote the number of distinct values $f(x)$, $x \in GF(q)$. Uchiyama [2] has proved the following theorem: Suppose that

$$f^*(u, v)=\frac{f(u)-f(v)}{u-v} \tag{1.2}$$

is absolutely irreducible (that is, irreducible in every finite extension of $GF(q)$); then $V>q/2$ for all $n\geqq 4$. It is pointed out this conclusion cannot be asserted without the hypothesis concerning $f^*(u, v)$; moreover the proof of the theorem makes use of a deep theorem of A. Weil on the number of solutions of equations in two unknowns in a finite field.

In this note we wish to point out that it is easy to prove that $V>q/2$ *on the average*. More precisely we shall prove the following

Theorem. *The sum*

$$\sum_{a_1\in GF(q)} V(f)\geqq \frac{q^3}{2q-1}\geqq\frac{q^2}{2}, \tag{1.3}$$

where the summation is over the coefficient of the first degree term in $f(x)$.

We remark that this theorem is independent of any hypothesis on $f^*(u, v)$ and that the proof is quite elementary.

2. For $x \in GF(q)$, we define

$$e(x)=e^{2\pi i S(x)/p}, \qquad S(x)=x+x^p+\cdots+x^{p^{\nu-1}}. \tag{2.1}$$

Then $e(x+y)=e(x)e(y)$ and

$$\sum_x e(xy)=\begin{cases} q & (y=0) \\ 0 & (y\neq 0). \end{cases} \tag{2.2}$$

Following the notation of [2] we let M_r denote the number of $y \in GF(q)$ such that the equation $f(x)=y$ has precisely r distinct roots in $GF(q)$; then we have

$$V=\sum_{r=1}^{n} M_r, \qquad q=\sum_{r=1}^{n} rM_r. \tag{2.3}$$

Also if $N_1=N_1(f)$ is the number of solutions (x, y) of $f(x)-f(y)=0$, then

$$N_1=\sum_{r=1}^{n} r^2M_r. \tag{2.4}$$