74. Note on the Mean Value of V(f). II

By Saburô UCHIYAMA

Mathematical Institute, Tokyo Metropolitan University, Tokyo

(Comm. by Z. SUETUNA, M.J.A., June 13, 1955)

1. Let $GF(q)$ denote a finite field of order $q=p^{\nu}$. In the following we shall consider polynomials of the form

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

where $1<n<p$, and the number $V(f)$ of distinct values $f(x)$, $x \in GF(q)$. L. Carlitz [1][1] has proved that we have

$$\sum_{a_1 \in GF(q)} V(f) \geqq \frac{q^3}{2q-1} > \frac{q^2}{2}, \tag{1.2}$$

where the summation is over the coefficient of the first degree term in $f(x)$. It is also known [2] that

$$\sum_{\deg f=n} V(f)=\sum_{r=1}^{n}(-1)^{r-1}\binom{q}{r}q^{n-r} \tag{1.3}$$

or

$$\sum_{\deg f=n} V(f)=c_nq^n+O(q^{n-1}), \tag{1.4}$$

where the summation on the left-hand side of (1.3) or (1.4) is over all polynomials of degree n of the form (1.1) and

$$c_n=1-\frac{1}{2!}+\frac{1}{3!}-\cdots+(-1)^{n-1}\frac{1}{n!}. \tag{1.5}$$

In fact, the sum on the left-hand side of (1.3) is equal to the number of distinct polynomials, of degree n,

$$f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0 \qquad (a_j \in GF(q))$$

having at least one linear polynomial factor in $GF[q,x]$. In this point of view the relation (1.3) is almost obvious.[2]

2. The purpose of this note is to prove the following

Theorem. *We have*

$$\sum_{(r)} V(f)=q^{-r}\sum_{\deg f=n} V(f)+R_{n,r} \qquad (1<n<p), \tag{2.1}$$

where the summation on the left-hand side is over the coefficients a_1, $a_2,\dots,a_{n-r-1}$ *in* $f(x)$ *and*

$$R_{n,r}=\begin{cases} 0 & \text{if } r=1, \\ O(q^{\theta n}) & \text{if } r\geqq 2, \end{cases}$$

with $\theta=1-\frac{1}{r}$. *In particular, if* $n\geqq r(r+1)$ *then*

$$\sum_{(r)} V(f)=c_nq^{n-r}+O(q^{n-r-1}), \tag{2.2}$$

where c_n *is the number given by* (1.5).

---

1) Numbers in brackets refer to the references at the end of this note.

2) Thus we may get a simple proof of (1.3). The idea was suggested to the author by K. Takeuchi.