81. On the Cardinality of Value Set of Polynomials with Coefficients in a Finite Field

By Javier GOMEZ-CALDERON

The Pennsylvania State University

(Communicated by Shokichi, IYANAGA, M. J. A., Dec. 14, 1992)

1. Introduction. Let F_q denote the finite field of order q where q is a prime power. If $f(x)$ is a polynomial of positive degree d over F_q, let $V_f=\{f(x): x\in F_q\}$ denote the image or value set of $f(x)$ and $|V_f|$ denote the cardinality of V_f. Since $f(x)$ cannot assume a given value more than d times, it is clear that

$$\left[\frac{q-1}{d}\right]+1\leq |V_f|\leq q,$$

where $[x]$ denotes the greatest integer $\leq x$. Uchiyama [3] has proved that if F_q is of sufficiently large characteristic and

$$\frac{f(x)-f(y)}{x-y}$$

is absolutely irreducible, then $|V_f|>\frac{q}{2}$ for all $d\geq 4$. Carlitz [1] has also proved that $|V_f|>\frac{q}{2}$ "on the average." More precisely, Carlitz proved that

$$\sum_{a_1\in F_q}|V_f|\geq \frac{q^2}{2},$$

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

In this note we determine a lower bound for $|V_f|$ when $(d,q)=1$, $d^4<q$ and the multiplicative order of q modulo $p_i^{a_i}$ is $p_i^{a_i}-p_i^{a_i-1}$ for all prime power $p_i^{a_i}\,\|\,d$. We prove that

$$|V_f|\geq \frac{q}{1+\sum_{D|d} \emptyset(D)/\operatorname{lcm}(\emptyset(p_1^{b_1}),\ldots,\emptyset(p_r^{b_r}))},$$

where $D=p_1^{b_1}p_2^{b_2}\cdots p_r^{b_r}$ and $\emptyset(D)$ denotes the Euler Phi Function.

2. Theorem and proof. We will need the following two lemmas.

Lemma 1. *Let $f(x)$ be a monic polynomial over F_q of degree $d<q$. Let $\#f^*(x,y)$ denote the number of solutions (x,y) in $F_q\times F_q$ of the equation $f^*(x,y)=f(x)-f(y)=0$. Assume*

$$\#f^*(x,y)\leq cq$$

for some constant c, $1<c<d$. Then

$$\frac{q}{c}\leq |V_f|.$$

Proof. Let R_i denote the number of images of $f(x)$ that occur exactly i times as x ranges over F_q, not counting multiplicities. Then

$$\sum_{i=1}^{d} iR_i=q,\quad |V_f|=\sum_{i=1}^{d}R_i,\ \text{and}\ \#f^*(x,y)=\sum_{i=1}^{d}i^2R_i.$$