26. *On Certain Numerical Invariants of Mappings over Finite Fields. V*

By Takashi ONO

Department of Mathematics, Johns Hopkins University

(Communicated by Shokichi IYANAGA, M. J. A., Jan. 12, 1981)

Introduction. This is a continuation of our paper [2] which will be referred to as (I) in this paper.[1] Let k be a finite field with q elements: $k=\boldsymbol{F}_q$, χ be a non-trivial character of the multiplicative group $k^\times$ (extended by $\chi(0)=0$) and f be a function $k\to k$. We shall put

$$S_f(\chi)=\sum_{x\in k}\chi(f(x)).$$

Consider the polynomial

$$f(x)=x^m+Ax+B,\quad A,\ B\in k,\quad m\geqq 3. \tag{0.1}$$

Denote by $\Delta(A, B)$ the discriminant of $f(x)$, i.e.

$$\Delta(A, B)=(-1)^{m-1}(m-1)^{m-1}A^m+m^mB^{m-1}. \tag{0.2}$$

We assume that $(q, m)=(q, m-1)=1$. The purpose of the paper is to prove the following

Theorem. *Let d be an integer $\geqq 2$ such that $(q, d)=(d, m)=(d, m-2)=1$ and let χ be a non-trivial character of $k^\times$ of exponent d. Then, there is a polynomial $f(x)=x^m+Ax+B$ with $A\neq 0$, $B\neq 0$, $\Delta(A, B)\neq 0$ such that*

$$|S_f(\chi)|<\kappa\sqrt{q}, \tag{0.3}$$

where $\kappa=\sqrt{3}$ if $m=3$ and $\kappa=\sqrt{2(m-1)}$ if $m\geqq 4$.

Remark 1. By the well-known theorem[2] we know that

$$|S_f(\chi)|\leqq(m-1)\sqrt{q} \tag{0.4}$$

for any polynomial f of degree m with $(d, m)=1$.

Remark 2. When $d=2$, m can be any odd integer $\geqq 3$ and since there is only one quadratic character χ we have the relation

$$N=q+S_f(\chi),$$

where N denotes the number of solutions $(x, y)\in k^2$ of the equation

$$y^2=x^m+Ax+B. \tag{0.5}$$

Therefore, our Theorem means that among hyperelliptic curves of type (0.5) with $A\neq 0$, $B\neq 0$, $\Delta(A, B)\neq 0$, there is a curve which satisfies the inequality

$$|N-q|<\kappa\sqrt{q} \tag{0.6}$$

where $\kappa=\sqrt{3}$ if $m=3$ and $\kappa=\sqrt{2(m-1)}$ if $m\geqq 5$ (m: odd). A similar remark can be made for the case $d=3$.

---

1) For example, we mean by (I.2.3) the item (2.3) in (I).

2) See Theorem 2C on p. 43 of [1].