Bollettino
Unione Matematica Italiana

Stephan R. Cavior

On the least non-negative trace of a polynomial over a finite field.

Bollettino dell'Unione Matematica Italiana, Serie 3, Vol. **20** (1965), n.1, p. 120–121.

Zanichelli

<http://www.bdim.eu/item?id=BUMI_1965_3_20_1_120_0>

On the least non-negative trace of a polynomial over a finite field.

by STEPHAN R. CAVIOR

Summary. - *Generalizing a result due to Mordell, we find an estimate for the least non-negative trace of a polynomial over a finite field.*

Lel p be a prime and let $f(x)$ be a polynomial of degree n with integer coefficients. Let l denote the least non-negative residue of $f(x)$ (mod. p). In [1] MORDELL finds the estimate

$$l \leq n.p^{1/2} \log p. \tag{1}$$

The object of the present paper is to generalize (1) for a polynomial over an arbitrary finite field.

Accordingly, suppose that m is an integer, $m \geq 1$, and that F denotes the finite field of order $q = p^m$. Let $f(x)$ be a polynomial of degree n over F and let l denote the least non-negative trace of $f(x)$ as x ranges over F. In this paper we shall prove

$$l \leq n \cdot p^{1-m/2} \log p. \tag{2}$$

Following MORDELL, we define N_r to be the number of solutions of

$$t(f(x)) = r, \qquad (0 \leq r \leq p-1)$$

where $t(\alpha)$ denotes the trace of α for $\alpha \in F$. Then we have

$$p \cdot N_r = \sum_{u=0}^{p-1} \sum_{x \in F} e|u[t(f(x) - r]|. \tag{3}$$

If we sum (3) for $r = 0, 1, \ldots, s$ and isolate the term with $u = 0$, we obtain

$$\begin{aligned} p \cdot \sum_{r=0}^{s} N_r &= (s+1)q + \sum_{r=0}^{s} \sum_{u=1}^{p-1} \sum_{x \in F} e|u[t(f(x) - r)]| \\ &= (s+1)q + \sum_{u=1}^{p-1} \sum_{x \in F} e|u \cdot t(f(x))| \cdot \left\{ \frac{1 - e(-u(s+1))}{1 - e(-u)} \right\}. \end{aligned} \tag{4}$$

For $r \leq l-1$, $N_r = 0$. Setting $s = l-1$ yields

$$lq \leq \sum_{u=1}^{p-1} \left| \sum_{x \in F} e\{u \cdot t(f(x))\} \right| / \sin \pi u/p. \tag{5}$$

Now using the estimate

$$\left| \sum_{x \in F} e\{t(f(x))\} \right| \leq n \cdot q^{1/2}$$

due to CARLITZ and UCHIYAMA [2, p. 39], we obtain from (5)

$$lq \leq \sum_{u=1}^{p-1} n \cdot q^{1/2} / \sin \pi u/p$$

$$\leq pnq^{1/2} \log p.$$

Hence

$$l \leq np^{1-m/2} \log p.$$

It is interesting to note that for fixed p and n, $l \to 0$ as $m \to \infty$. In fact, $l = 0$ when

$$n \cdot p^{1-m/2} \cdot \log p < 1$$

or

$$m > \frac{2 \log (np \cdot \log p)}{\log p}.$$

To explain this fact, we recall that the traces of elements in F are integers (mod p) and that at most p^{m-1} of the numbers $\{f(x) : x \in F\}$ have a trace equal to $p-1$, $p-2$, ... and so forth. Thus, m is large enough, there exists some $x \in F$ such that $t(f(x)) = 0$.

REFERENCES

[1] L. J. MORDELL, *On the Least Residue and Non-Residue of a Polynomial*, «J. London Math. Sec.», vol. 38 (1963), pp. 451-453.

[2] L. CARLITZ and S. UCHIYAMA, *Bounds for Exponential Sums*, «Duke Math. J.», vol. 24 (1957, pp. 37-41.

Pervenuta alla Segreteria dell'U.M.I.
il 9 dicembre 1964