CHARACTER SUMS AND PRIMITIVE ROOTS IN FINITE FIELDS

MATHEMATICS

1968

SovietRxiv

Abstract

Full Text

UDC 511.26

MATHEMATICS

A. A. KARATSUBA

CHARACTER SUMS AND PRIMITIVE ROOTS IN FINITE FIELDS

(Presented by Academician I. M. Vinogradov on 2 X 1967)

In the present article, using one example, a new approach is set forth to the problem of estimating character sums and the distribution of primitive roots in finite fields (see (1-6)). The corresponding estimate of the work (5) already holds for $H > p^{1/4+\varepsilon}$, $\varepsilon > 0$ an arbitrarily small number, and any fixed $n \geqslant 1$. The method of proof of the main theorem is also applicable to more general situations; the theorems of the article can be sharpened and generalized.

Let $n \geqslant 1$ be an integer, and let

$$F(x) = x^n + a_1 x^{n-1} + \cdots + a_n$$

be a polynomial with integer coefficients, irreducible mod p, where p is a prime number, $p \geqslant p_0 = p_0(F)$. Let, further, θ be a root of the equation

$$F(\theta) = 0$$

and let $G(p^n)$ be the Galois field with basis $\omega_1, \ldots, \omega_n$, where $\omega_0 = 1, \omega_1 = \theta, \ldots, \omega_n = \theta^{n-1}$. By χ we denote a nonprincipal Dirichlet character of the multiplicative group of the field $G(p^n)$.

If $x \in G(p^n)$, then $x = \omega_1 x_1 + \cdots + \omega_{nx} n$, where $0 \leq x_i \leq p-1$, $i = 1, 2, \ldots, n$. The set of $x \in G(p^n)$ for which $0 \leq \nu_i < x_i \leq \nu_i + H < p$, $i = 1, 2, \ldots, n$, will be denoted by $D_1(H) = D_1(H, \nu_1, \ldots, \nu_n)$. For $\nu_1 = \cdots = \nu_n = 0$, instead of $D_1(H)$ we shall write $D_0(H)$.

The constants in the sign $\ll$ of I. M. Vinogradov and in the symbol O depend, generally speaking, on F.

Theorem 1. For every $\varepsilon > 0$ there exist $\delta = \delta(\varepsilon) > 0$, $p_1 = p_1(\varepsilon)$, such that, for

$$H > p^{1/4+\varepsilon}, \qquad p > p_1,$$

the estimate

$$\left| \sum_{x \in D_1(H)} \chi(x) \right| < (Hp^{-\delta})^n$$

holds.

Theorem 2. Under the conditions of Theorem 1, the number of primitive roots lying in $D_1(H)$ is equal to

$$\frac{\varphi(p^n-1)}{p^n-1}\,H^n(1+O(p^{-n\delta})).$$

The proof of Theorem 2 follows from Theorem 1 in the usual way. For the proof of Theorem 1 we shall need the following two lemmas.

Lemma 1. Let r be an arbitrary positive integer and $0<h<p$. The following estimate holds:

$$\sum_{\lambda\in D_0(p)}\left|\sum_{z\in D_0(h)}\chi(\lambda+z)\right|^{2r}<(4r)^{r+1}p^nh^{nr}+2rp^{1/2}h^{2nr}.$$

Lemma 2. Let I be the number of solutions in $G(p^n)$ of the equation

$$xy=x'y',$$

where $x,x'\in D_1(H)$, $y,y'\in D_0(H_1)$, $1\le HH_1\ll p$.

Then for any $\varepsilon_1>0$ the estimate holds

$$I\ll(HH_1)^{n(1+\varepsilon_1)}.$$

Lemma 1 and its earlier analogues were proved by H. Davenport, P. Erdős ([7]), and D. Burgess ([3]). The proof makes essential use of A. Weil' s theorem ([8]) on zeros of special zeta-functions. Lemma 2 is a simple generalization of Yu. V. Linnik' s lemma (see ([9]), Lemma 6).

Proof of Theorem 1. We shall assume that

$$p^{1/4+\varepsilon}<H<p^{1/2+\varepsilon/8},$$

$0<\varepsilon<0.01$, since otherwise the theorem follows from ([5]). Define the quantities r,δ,H_1,H_2 by the equalities

$$r=\left[\frac{1}{\varepsilon}\right]+1,\quad \delta=\frac{\varepsilon}{4}\left(r+\frac{n}{2}\right)^{-1},\quad H_1=Hp^{-1/2r-n\delta},\quad H_2=p^{1/2r},$$

and let $y\in D_0(H_1)$, $z\in D_0(H_2)$. Then the following relation is valid (see ([10,11])):

$$\sum_{x\in D_1(H)}\chi(x)=\sum_{x\in D_1(H)}\chi(x+yz)+O((Hp^{-\delta})^n). \tag{1}$$

Indeed, if

$$y=\sum_{i=1}^{n}\omega_iy_i,\quad z=\sum_{j=1}^{n}\omega_jz_j,\quad \omega_i\omega_j=\sum_{k=1}^{n}\omega_kd_{ijk},$$

then

$$yz = \sum_{k=1}^{n} \omega_k t_k, \tag{2}$$

where

$$t_k = \sum_{i,j=1}^{n} y_i z_j d_{ijk} \ll H_1 H_2 = H p^{-n\delta}.$$

Therefore we have

$$\sum_{x \in D_1(H)} \chi(x) = \sum_{\nu_1 < x_1 \le \nu_1 + H} \cdots \sum_{\nu_n < x_n \le \nu_n + H} \chi(\omega_1 x_1 + \cdots + \omega_{nx} n) =$$

$$= \sum_{\nu_1 < x_1 \le \nu_1 + H} \cdots \sum_{\nu_{n-1} < x_{n-1} \le \nu_{n-1} + H} \left(\sum_{\nu_n + t_n < x_n \le \nu_n + t_n + H} \chi(\omega_1 x_1 + \cdots + \omega_{nx} n) \right.$$

$$\left. + \sum_{\nu_n < x_n \le \nu_n + t_n} \chi(\omega_1 x_1 + \cdots + \omega_{nx} n) - \sum_{\nu_n + H < x_n \le \nu_n + t_n + H} \chi(\omega_1 x_1 + \cdots + \omega_{nx} n) \right) =$$

$$= \sum_{\nu_1 < x_1 \le \nu_1 + H} \cdots \sum_{\nu_n < x_n \le \nu_n + H} \chi(\omega_1 x_1 + \cdots + \omega_n (x_n + t_n)) + 2\theta_n H^{n-1} t_n = \cdots =$$

$$= \sum_{\nu_1 < x_1 \le \nu_1 + H} \cdots \sum_{\nu_n < x_n \le \nu_n + H} \chi(\omega_1 (x_1 + t_1) + \cdots + \omega_n (x_n + t_n)) + 2\theta_1 H^{n-1} t_1 + \cdots + 2\theta_{nH}^{n-1} t_n,$$

where $|\theta_1| \le 1, \ldots, |\theta_n| \le 1$. Hence, from (2), (1) follows.

Summing (1) over all $y \in D_0(H_1)$, $z \in D_0(H_2)$, we obtain

$$\sum_{x \in D_1(H)} \chi(x) = W + O((Hp^{-\delta})^n), \tag{3}$$

where

$$W = (H_1 H_2)^{-n} \sum_{x \in D_1(H)} \sum_{y \in D_0(H_1)} \sum_{z \in D_0(H_2)} \chi(x + yz).$$

Let us consider the sum W. Using the multiplicativity of χ, we obtain

$$|W| \ll (H_1 H_2)^{-n} \sum_{\lambda} I(\lambda) \left| \sum_{z \in D_2(H_2)} \chi(\lambda + z) \right|, \tag{4}$$

where $I(\lambda)$ is the number of solutions of the equation $xy^{-1} = \lambda$, $x \in D_1(H)$, $y \in D_0(H_1)$. Since

$$\sum_{\lambda} I(\lambda) = (HH_1)^n, \qquad \sum_{\lambda} I^2(\lambda) = I,$$

raising (4) to the power $2r$ and successively applying Hölder' s and Cauchy' s inequalities gives

$$|W|^{2r} \ll (H_1H_2)^{-2nr}\left(\sum_{\lambda} I(\lambda)\right)^{2(r-1)} \sum_{\lambda} I^2(\lambda) \sum_{\lambda}\left|\sum_{x\in D_0(H_2)} \chi(\lambda+z)\right|^{2r} \ll$$

$$\ll (H_1H_2)^{-2nr}(HH_1)^{2n(r-1)}(HH_1)^{n(1+\varepsilon_1)} \sum_{\lambda\in D_0(p)}\left|\sum_{z\in D_0(H_2)} \chi(\lambda+z)\right|^{2r}.$$

Applying the estimate of Lemma 1 to the last double sum, after simple computations we arrive at the estimate

$$|W| \ll (Hp^{-\delta})^n.$$

The assertion of the theorem follows from this inequality and (3).

Mathematical Institute named after V. A. Steklov
Academy of Sciences of the USSR

Received
20 IX 1967

REFERENCES

[1] I. M. Vinogradov, Zhurn. Fiz.-matem. obshch. univ., Perm, **1**, 94 (1918).
[2] G. Pólya, Göttinger Nachr., **21** (1918).
[3] D. A. Burgess, Proc. London Math. Soc. (3), **12**, 179 (1962).
[4] D. A. Burgess, Proc. London Math. Soc. (1), **17**, 11 (1967).
[5] H. Davenport, D. J. Lewis, Rend. Circ. Mat. Palermo (2), **12**, 129 (1963).
[6] J. H. Jordan, Proc. London Math. Soc. (1), **17**, 1 (1967).
[7] H. Davenport, P. Erdős, Publ. Math. Debrecen, **2**, 252 (1952).
[8] A. Weil, Actualités math. sci., Paris, No. 1041 (1948).
[9] Yu. V. Linnik, Matem. sborn., **12** (54), 225 (1943).
[10] I. M. Vinogradov, Izv. AN SSSR, ser. matem., **22**, 2, 161 (1958).
[11] A. A. Karatsuba, Izv. AN SSSR, ser. matem., **28**, 1, 237 (1964).

Note: Figure translations are in progress. See original paper for figures.