SUMS OF PRIMITIVE ROOTS IN A FINITE FIELD

By L. Carlitz

1. In this paper we consider the following problem. Let α be an arbitrary number of the finite field $GF(p^n)$, and let $\beta_1, \cdots, \beta_r$ denote primitive roots of the field. Then we seek the number of solutions of

$$\alpha = \beta_1 + \cdots + \beta_r, \tag{1.1}$$

where r is a fixed integer ≥ 2. The problem can be generalized as follows. Let $e_i | p^n - 1$, $i = 1, \cdots, r$, and let β_i denote a number belonging to the exponent e_i; we then seek the number of solutions of (1.1) subject to these conditions. A further generalization is obtained by introducing non-zero coefficients $\alpha_1, \cdots, \alpha_r$; we then require the number of solutions $N_r(\alpha)$ of

$$\alpha = \alpha_1\beta_1 + \cdots + \alpha_r\beta_r. \tag{1.2}$$

We shall show that for $e_1 \leq \cdots \leq e_r$, $r \geq 3$,

$$N_r(\alpha) = \frac{\phi(e_1) \cdots \phi(e_r)}{p^n - 1} + O(p^{n(\frac{1}{2}+\epsilon)}\phi(e_3) \cdots \phi(e_r)) \qquad (p^n \to \infty), \tag{1.3}$$

while for $r = 2$, $\alpha \neq 0$,

$$N_2(\alpha) = \frac{\phi(e_1)\phi(e_2)}{p^n - 1} + O(p^{n(\frac{1}{2}+\epsilon)}).$$

In particular for $n = 1$, $e_1 = \cdots = e_r = p - 1$, (1.3) implies that the number of solutions of (1.2) in primitive roots (mod p), where now α, α_i are integers (mod p),

$$= \frac{\phi^r(p-1)}{p-1} + O(p^{r-\frac{3}{2}+\epsilon}). \tag{1.4}$$

In the next place we consider the equation

$$\alpha = \gamma_1\beta_1 + \cdots + \gamma_r\beta_r + \delta_1\xi_1^{k_1} + \cdots + \delta_s\xi_s^{k_s}, \tag{1.5}$$

where $\gamma_i\delta_i \neq 0$, $e_i | p^n - 1$, $k_i | p^n - 1$; as for the unknowns β_i, ξ_i, it is required that β_i belongs to the exponent e_i while ξ_i is arbitrary. If $N_{r,s}(\alpha)$ denotes the number of solutions of (1.5) subject to these conditions we show that

$$N_{r,s}(\alpha) = \phi(e_1) \cdots \phi(e_r)p^{n(s-1)} + O(p^{n(s-\frac{1}{2}+a+\epsilon)}\phi(e_2) \cdots \phi(e_r)), \tag{1.6}$$

provided $k_i = O(p^{na})$, $a < \frac{1}{2}$; (1.6) is valid for all α and $r \geq 1$, $s \geq 1$ (except $\alpha = 0$ when $r = s = 1$).

Received January 7, 1952.