SOLUTIONS OF SOME SYSTEMS OF EQUATIONS OVER A FINITE FIELD WITH APPLICATIONS TO GEOMETRY

FUANGLADA R. JUNG

1. Introduction. Let F denote a finite field of order q and of odd characteristic p and let $a, b, c, a_i, b_i, c_i, 1 \leq i \leq t$, denote elements of F such that $a_1 \cdots a_t \neq 0$ and not all the b_i's and c_i's are zero. In this paper we determine the number $N_t(a, b, c)$ of solutions in F of the system of equations

$$\begin{aligned} a_1x_1^2 + \cdots + a_tx_t^2 &= a \\ b_1x_1 + \cdots + b_tx_t &= b \\ c_1x_1 + \cdots + c_tx_t &= c. \end{aligned} \tag{1.1}$$

We note that if the last two equations in (1.1) have no common solution, then $N_t(a, b, c) = 0$ and if the last two equations in (1.1) are equivalent, then $N_t(a, b, c) = N_t(a, b)$, where $N_t(a, b)$ is the number of common solutions of the first two equations in (1.1). Since $N_t(a, b)$ is known [4; Theorem 2], we may exclude the above two cases, that is, if r and s denote the numbers of nonzero b_i's and c_i's respectively, $1 \leq r, s \leq t$, then we may exclude the case (*) given by the following condition.

$$(*) \quad \begin{cases} b_i \text{ and } c_i \text{ are both zero or both nonzero, } 1 \leq i \leq t, \text{ (and therefore } r = s) \\ b_j/c_j = b_k/c_k \text{ for all } k, j \in \{1, \cdots, t\} \text{ such that } c_k \neq 0 \neq c_j . \end{cases}$$

Excluding the case (*) explicit formulas of $N_t(a, b, c)$ in accordance with various cases are obtained in Theorem 1. As a consequence of a complete evaluation of $N_t(a, b, c)$ we obtain a solvability criterion for the system (1.1) in Theorem 2.

We note that the case when all the b_i's and c_i's are nonzero had been considered by E. Cohen [3] and that some of our results correct a mistake which arose from an omission in his argument. Furthermore, the method of evaluating $N_t(a, b, c)$ is based upon an elementary application of finite Fourier series and Gaussian sums. The treatment is somewhat more direct than that of Cohen in the analogous problem concerned with a single linear equation [4]. Moreover, our main results (Theorems 1 and 2) are independent of those of Dickson [5; §§65–66] and of Cohen [4].

Received November 8, 1971. This paper is a part of the author's Ph.D. dissertation written at Kansas State University under the supervision of Professor Eckford Cohen. This work was supported in part by NSF grant GP-8742.