

The number of solutions of a particular equation in a finite field.

Dedicated to the memory of Tibor Szele.

By L. CARLITZ in Durham, North Carolina.

1. INTRODUCTION. Let $q = p^n$ and $m|q+1$. Consider the equation

$$(1.1) \quad \xi_1^m + \cdots + \xi_s^m = 1.$$

FAIRCLOTH [1] has proved that N' , the number of non-zero solutions of (1.1) with $\xi_i \in GF(q^2)$, satisfies

$$(1.2) \quad q^2 N' = (q^2 - 1)^s \{ (mq - q - 1) + (m - 1)(-q - 1)^{s+1} \} / m.$$

The proof makes use of the generalized Jacobi—Kummer cyclotomic function and in particular of a theorem of MITCHELL [2].

If N denotes the *total* number of solutions of (1.1), then it is easily verified that (1.2) is equivalent to

$$(1.3) \quad q^2 N = q^{2s} - (-q)^s + ((m - 1)^s - (-1)^s)(q^m - q - 1) / m.$$

In the present note we determine the number of solutions of the more general equation

$$(1.4) \quad \alpha_1 \xi_1^m + \cdots + \alpha_s \xi_s^m = \alpha,$$

where $m|q+1$ and $\alpha_i, \alpha \in GF(q^2)$, $\alpha_i \neq 0$.

Let γ denote a generator of the multiplicative group of $GF(q^2)$ and let A_i consist of the numbers γ^{mj+i} , $j = 0, \dots, ((q^2 - 1)/m) - 1$; $i = 0, \dots, m - 1$. Also let s_i denote the number of coefficients $\alpha_k \in A_i$, so that $s_0 + \cdots + s_{m-1} = s$. Then we prove the following

Theorem 1. Let $N(\alpha)$ denote the number of solutions of (1.4). Then if $\alpha \in A_k$

$$(1.5) \quad q^2 N(\alpha) = q^{2s} + q^{s+1} (m - 1)^{s_k} (-1)^{s-s_k} - q^s (q + 1) / m \sum_{j=0}^{m-1} (m - 1)^{s_j} (-1)^{s-s_j},$$

while for $\alpha = 0$

$$(1.6) \quad q^2 N(0) = q^{2s} + q^s (q^2 - 1) / m \sum_{j=0}^{m-1} (m - 1)^{s_j} (-1)^{s-s_j}.$$

It is easily verified that when $\alpha_1 = \dots = \alpha_s = \alpha = 1$, (1.5) reduces to (1.3). For $s=2$ compare [3, Theorem 2].

2. Let $\chi(\alpha)$ denote a character of the multiplicative group of $GF(q^2)$ satisfying $\chi^m = \chi_0$, where χ_0 is the principal character. Put

$$(2.1) \quad e(\alpha) = e^{2\pi i t(\alpha)/p}, \quad t(\alpha) = \sum_{j=0}^{2n-1} \alpha^{p^j}$$

and define

$$(2.2) \quad \tau(\chi) = \sum_{\alpha} \chi(\alpha) e(\alpha),$$

the summation extending over all numbers of $GF(q^2)$.

Let $\theta \in GF(q^2)$, $\theta \notin GF(q)$. For $p > 2$ we may assume that $\theta^q = -\theta$. The following lemma holds.

Lemma.

$$(2.3) \quad \tau(\chi) = \begin{cases} q\chi(\theta) & (p > 2) \\ q & (p = 2). \end{cases}$$

This result is due to STICKELBERGER [4, p. 340]. For completeness we give the following simple proof.

(i) $p > 2$. Let $\alpha = a + b\theta$, where $a, b \in GF(q)$. Then by (2.1) $e(\alpha) = e(a)$. Thus $\tau(\chi) = \sum_{a,b} \chi(a + b\theta) e(a + b\theta) = \sum_{a,b} \chi(a + b\theta) e(a)$.

Since for $a \in GF(q)$, $a \neq 0$,

$$a^{(q^2-1)/m} = a^{(q-1)(q+1)/m} = 1,$$

it follows that $\chi(a) = 1$. Consequently

$$\begin{aligned} \tau(\chi) &= \sum_b \chi(b\theta) + \sum_{a \neq 0} \chi(a + b\theta) e(a) = (q-1)\chi(\theta) \sum_b \chi(1 + b\theta) \sum_{a \neq 0} e(a) = \\ &= (q-1)\chi(\theta) - \frac{1}{q-1} \sum_{\substack{a,b \\ a \neq 0}} \chi(a + b\theta) = (q-1)\chi(\theta) + \frac{1}{q-1} \sum_b \chi(b\theta) = q\chi(\theta). \end{aligned}$$

(ii) $p = 2$. Let $\theta^q + \theta = c \neq 0$; also let $e_0(a)$ denote the function (2, 1) for the $GF(q)$. Then for $\alpha = a + b\theta$, $\alpha^q + \alpha = bc$ so that $e(\alpha) = e_0(bc)$. Thus

$$\begin{aligned} \tau(\chi) &= \sum_{a,b} \chi(a + b\theta) e_0(bc) = \sum_a \chi(a) + \sum_{b \neq 0} \chi(a + b\theta) e_0(bc) = \\ &= q-1 + \sum_a \chi(a + \theta) \sum_{b \neq 0} e_0(bc) = q-1 - \frac{1}{q-1} \sum_{\substack{a,b \\ b \neq 0}} \chi(a + b\theta) = \\ &= q-1 + \frac{1}{q-1} \sum_a \chi(a) = q. \end{aligned}$$

This completes the proof of the Lemma.

3. Put

$$(3.1) \quad S(\alpha) = \sum_{\xi} e(\alpha \xi^m).$$

Then it is familiar that

$$(3.2) \quad S(\alpha) = \sum_{\chi \neq \chi_0} \chi(\alpha) \tau(\bar{\chi}) \quad (\alpha \neq 0).$$

Then by (2.3)

$$(3.3) \quad S(\alpha) = q \sum_{\chi \neq \chi_0} \chi(\alpha) \bar{\chi}(\theta) = q \sum_{\chi \neq \chi_0} \chi(\alpha \theta^{-1}) \quad (p \neq 2).$$

Since

$$(3.4) \quad \sum_{\chi} \chi(\alpha) = \begin{cases} m & (\alpha \in A_0) \\ 0 & (\text{otherwise}), \end{cases}$$

it is clear that for $p = 2$

$$(3.5) \quad S(\alpha) = \begin{cases} q(m-1) & (\alpha \theta^{-1} \in A_0) \\ -q & (\text{otherwise}). \end{cases}$$

Similarly for $p \neq 2$ we get

$$(3.6) \quad S(\alpha) = \begin{cases} q(m-1) & (\alpha \in A_0) \\ -q & (\text{otherwise}). \end{cases}$$

4. Since

$$(4.1) \quad \sum_{\beta \in GF(q^2)} e(\alpha \beta) = \begin{cases} q^2 & (\alpha = 0) \\ 0 & (\alpha \neq 0) \end{cases}$$

it follows that $N(\alpha)$, the number of solutions of (1.4) satisfies

$$\begin{aligned} q^2 N(\alpha) &= \sum_{\beta} \sum_{\xi_1, \dots, \xi_s} e\{\beta(\alpha_1 \xi_1^m + \dots + \alpha_s \xi_s^m - \alpha)\} = \\ &= \sum_{\beta} e(-\alpha \beta) \sum_{\xi_1, \dots, \xi_s} e\{\beta(\alpha_1 \xi_1^m + \dots + \alpha_s \xi_s^m)\} = \sum_{\beta} e(-\alpha \beta) \prod_{i=1}^s S(\alpha_i \beta) = \\ &= q^{2s} + \sum_{\beta \neq 0} e(-\alpha \beta^{-1}) \prod_{i=1}^s S(\alpha_i \beta^{-1}). \end{aligned}$$

Now assume first that $p \neq 2$ and let s_i denote the number of $\alpha_j \in A_i$. Then by (3.3) and (3.4) we get

$$\begin{aligned} (4.2) \quad q^2 N(\alpha) &= q^{2s} + q^s \sum_{\beta \neq 0} e(-\alpha \beta^{-1}) \prod_{i=1}^s \sum_{\chi \neq \chi_0} \chi(\alpha_i \beta^{-1} \theta) = \\ &= q^{2s} + q^s \sum_{\beta \neq 0} e(-\alpha \beta^{-1} \theta^{-1}) \prod_{i=1}^s \sum_{\chi \neq \chi_0} \chi(\alpha_i \beta^{-1}) = \\ &= q^{2s} + q^s \sum_{j=0}^{m-1} \sum_{\beta \in A_j} e(-\alpha \beta^{-1} \theta^{-1}) (m-1)^{s_j} (-1)^{s-s_j}. \end{aligned}$$

Suppose now that $\alpha \in A_k$. Let ν be a fixed number of A_j so that

$$\begin{aligned} \sum_{\beta \in A_j} e(-\alpha \beta^{-1} \theta^{-1}) &= \sum_{\beta \in A_0} e(-\alpha \beta^{-1} \nu^{-1} \theta^{-1}), \\ 1 + m \sum_{\beta \in A_j} e(-\alpha \beta^{-1} \theta^{-1}) &= S(-\alpha \nu^{-1} \theta^{-1}) = \\ &= \begin{cases} q(m-1) & (\alpha \nu^{-1} \in A_0) \\ -q & (\text{otherwise}), \end{cases} \end{aligned}$$

by (3.5). Thus (4.2) becomes

$$\begin{aligned} q^2 N(\alpha) &= q^{2s} - q^s(q+1)/m \sum_{\substack{j=0 \\ j \neq k}}^{m-1} (m-1)^{s_j} (-1)^{s-s_j} + \\ &+ q^s \left(q - \frac{q+1}{m} \right) (m-1)^{s_k} (-1)^{s-s_k} = q^{2s} + q^{s+1} (m-1)^{s_k} (-1)^{s-s_k} - \\ &- q^s(q+1)/m \sum_{j=0}^{m-1} (m-1)^{s_j} (-1)^{s-s_j}. \end{aligned}$$

This completes the proof of (1.5).

When $\alpha = 0$, (4.2) becomes

$$\begin{aligned} q^2 N(0) &= q^{2s} + q^s \sum_{j=0}^{m-1} \sum_{\beta \in A_j} (m-1)^{s_j} (-1)^{s-s_j} = \\ &= q^{2s} + q^s(q^2-1)/m \sum_{j=0}^{m-1} (m-1)^{s_j} (-1)^{s-s_j}, \end{aligned}$$

which proves (1.6).

5. If we use the fuller notation

$$(5.1) \quad N(\alpha, s_0, \dots, s_{m-1})$$

for the number of solutions of (1.4), then it is evident that

$$(5.2) \quad \sum_{\xi + \eta = \alpha} N(\xi, s_0, \dots, s_{m-1}) N(\eta, t_0, \dots, t_{m-1}) = N(\alpha, s_0 + t_0, \dots, s_{m-1} + t_{m-1})$$

for arbitrary non-negative s_i, t_j such that $s_0 + \dots + s_{m-1} \geq 1$, $t_0 + \dots + t_{m-1} \geq 1$.

When $s_0 = \dots = s_{m-1} = 0$, we may define

$$N(\alpha; 0, \dots, 0) = 0 \quad (\alpha \neq 0), \quad N(0; 0, \dots, 0) = 1,$$

which is in agreement with (1.5) and (1.6). We then find that (5.2) holds for all non-negative integral values of s_i, t_j . Indeed a further generalization is possible. If we define $N(\alpha; s_0, \dots, s_{m-1})$ by means of (1.5) and (1.6) for arbitrary integral values of $s_0, \dots, s_{m-1}$ then we can assert that (5.2) holds for all s_i, t_j ; in fact if we use (1.5) and (1.6) for complex values of the parameters (with $q^s = e^{s \log q}$, $(-1)^s = e^{\pi i s}$, etc.) then (5.2) holds in this case also. A direct proof is rather complicated. However the formula can be

proved rapidly in the following way. Exactly as in the proof of Theorem 1, we may show that

$$q^2 N(\alpha; s_0, \dots, s_{m-1}) = \sum_{\beta} e(-\alpha\beta) \prod_{i=0}^{m-1} S^{s_i}(\delta_i\beta),$$

where $\delta_i \in A_i$ but is otherwise arbitrary. Now employing (4. 1), (5. 2) follows immediately. This proves

Theorem 2. *The function $N(\alpha; s_0, \dots, s_{m-1})$ satisfies (5. 2) for arbitrary complex values of s_i, t_j .*

Bibliography.

- [1] O. B. FAIRCLOTH, On the number of solutions of some general types of equations in a finite field, *Canad. J. Math.* **4** (1952), 343—351.
- [2] H. H. MITCHELL, On the generalized Jacobi—Kummer cyclotomic function, *Trans. Amer. Math. Soc.* **17** (1916), 165—177.
- [3] H. H. MITCHELL, On the congruence $cx^\lambda + 1 = dy^\lambda$ in a Galois field, *Ann. of Math.* (2) **18** (1916—17), 120—131.
- [4] L. STICKELBERGER, Über eine Verallgemeinerung der Kreisteilung, *Math. Ann.* **37** (1890), 321—367.

(Received October 17, 1955.)