ON THE NUMBER OF SOLUTIONS OF SOME GENERAL TYPES OF EQUATIONS IN A FINITE FIELD

OLIN B. FAIRCLOTH

1. **Introduction.** The conditional equation $f(x_1, \ldots, x_s) = 0$, where f is a polynomial in the x's with coefficients in a finite field $F(p^n)$, is connected with many well-known developments in number theory and algebra, such as: Waring's problem, the arithmetical theory of quadratic forms, the Riemann hypothesis for function fields, Fermat's Last Theorem, cyclotomy, and the theory of congruences in commutative rings.

In this paper we shall investigate *the number of distinct solutions, N_s, of equations of the type*

$$c_1x_1^{m_1} + c_2x_2^{m_2} + \ldots + c_sx_s^{m_s} = c, \tag{1.1}$$

$s \geqslant 2$, where the c's are given elements of a finite field $F(p^n)$, $c_1 \ldots c_s \neq 0$, p is an odd prime, and $p^n - 1 = q_im_i$ for each i. If $c \neq 0$, we shall for convenience consider the equation

$$g^{y_1m_1+r_1} + \ldots + g^{y_sm_s+r_s} = 1, \tag{1.2}$$

where g is a multiplicative generator of $F(p^n)$ aside from zero and

$$\frac{c_i}{c} = g^{hm_i+r_i}.$$

Let $(r_1, \ldots, r_s)$ *denote the number of distinct sets of y's* $(y_i = 0, 1, \ldots, q_i - 1)$ *that satisfy* (1.2); thus $(r_1, \ldots, r_s)\, m_1 \ldots m_s$ is the number of non-zero solutions of (1.1).

If α_i is a primitive m_i root of unity and ind a is defined such that $g^{\text{ind}\, a} = a$ for any non-zero a in $F(p^n)$, consider the generalized Jacobi-Cauchy cyclotomic sum

$$\psi(u_1, \ldots, u_s) = \sum_{a_1+\ldots+a_s=1} \prod_{i=1}^{s} \alpha_i^{u_i \,\text{ind}\, a_i}, \tag{1.3}$$

where the a's range over the non-zero elements of $F(p^n)$. Vandiver [7, p. 148] in a recent paper gave the following expression for the number of non-zero solutions of (1.1):

$$(r_1, \ldots, r_s) \prod_{i=1}^{s} m_i = \sum_{u_1,\ldots,u_s} \psi(u_1, \ldots, u_s) \prod_{i=1}^{s} \alpha_i^{-u_ir_i}, \tag{1.4}$$

where each u_i ranges independently over the set $0, 1, \ldots, m_i - 1$.

2. **Additive decomposition formulae for** $(r_1, \ldots, r_s)$. In order to apply these sums to the aforementioned equation, we shall first consider degenerate cases. If $u_i \equiv 0 \pmod{m_i}$ for each i, then

Received March 12, 1951; in revised form October 23, 1951.

https://doi.org/10.4153/CJM-1952-030-0 Published online by Cambridge University Press

$$\psi(0, \dots, 0) = \sum_{a_1+\dots+a_s=1} 1.$$

Our problem reduces to counting the sets of a's for which $a_1 + \dots + a_s = 1$. This number is easily obtained by induction and we have

LEMMA 2.1. *If* $u_i \equiv 0 \pmod{m_i}$ *for each* i, *then*

$$\psi(0, \dots, 0) = \{(p^n - 1)^s - (-1)^s\}/p^n.$$

This result was found independently by Whiteman [9].

Suppose $u_1 \equiv 0 \pmod{m_1}$ and $u_s \not\equiv 0 \pmod{m_s}$; we then have

$$\psi(0, u_2, \dots, u_s) = \sum_{a_1+\dots+a_s=1} \prod_{i=2}^{s} \alpha_i^{u_i \operatorname{ind} a_i}.$$

In the above sum $a_2, \dots, a_s$ range independently over all the non-zero elements of $F(p^n)$ except those for which $a_2 + \dots + a_s = 1$; thus $\psi(0, u_2, \dots, u_s) = -\psi(u_2, \dots, u_s)$. By continually applying this result we obtain

LEMMA 2.2. *If* $u_i \equiv 0 \pmod{m_i}$, $i = 1, \dots, t$, $t < s$, *and* $u_s \not\equiv 0 \pmod{m_s}$, *then*

$$\psi(0, \dots, 0, u_{t+1}, \dots, u_s) = (-1)^t \psi(u_{t+1}, \dots, u_s).$$

As our last degenerate case suppose

$$\prod_{i=1}^{s} \alpha_i^{u_i} = 1, \qquad u_s \not\equiv 0 \pmod{m_s}.$$

Under this assumption (1.3) may be written

$$\psi(u_1, \dots, u_s) = \sum_{a_1+\dots+a_s=1} \prod_{i=2}^{s} \alpha_i^{u_i \operatorname{ind} a_i/a_1}. \tag{2.1}$$

Let $a_i = -b_i a_1$, $i > 1$; the right-hand side of (2.1) becomes

$$\sum_{a_1(1-b_2-\dots-b_s)=1} \prod_{i=2}^{s} \alpha_i^{u_i \operatorname{ind} b_i} \alpha_1^{u_1 \operatorname{ind} (-1)}.$$

In the above sum $b_2, \dots, b_s$ range independently over the non-zero elements of $F(p^n)$ except those for which $1 - b_2 - \dots - b_s = 0$. Thus we have

LEMMA 2.3. *If*

$$\prod_{i=1} \alpha_i^{u_i} = 1, \qquad u_s \not\equiv 0 \pmod{m_s},$$

then

$$\psi(u_1, \dots, u_s) = -\psi(u_2, \dots, u_s)\alpha_1^{u_1 \operatorname{ind} (-1)}.$$

Lemma 2.1 and Lemma 2.2 enable us to write the right-hand side of (1.4) as sums of ψ's where none of the u's are zero. Let

$$\Phi(r_1, \dots, r_t) = \sum_{u_1, \dots, u_t} \psi(u_1, \dots, u_t) \prod_{i=1}^{t} \alpha_i^{-u_i r_i}, \tag{2.2}$$

where each u_i ranges independently over the set $1, \dots, m_i - 1$. From Lemma 2.3 we have, in the case $t \geqslant 2$,

https://doi.org/10.4153/CJM-1952-030-0 Published online by Cambridge University Press

$$\Phi(r_1, \ldots, r_t) = \sum \psi(u_1, \ldots, u_t) \prod_{i=1}^{t} a_i^{-u_i r_i} \tag{2.3}$$
$$- \sum \psi(u_2, \ldots, u_t) a_1^{u_1 \text{ ind } (-1)} \prod_{i=1}^{t} a_i^{-u_i r_i},$$

where in the first sum each u_i ranges over the set $1, \ldots, m_i - 1$ such that

$$\prod_{i=1}^{t} a_i^{u_i} \neq 1,$$

and in the second sum each u_i ranges over the set $1, \ldots, m_i - 1$ such that

$$\prod_{i=1}^{t} a_i^{u_i} = 1.$$

If F is an arbitrary function of the b's then denote by

$$\mathop{\mathrm{S}}_{t}^{s} F(b_1, \ldots, b_t) \tag{2.4}$$

the sum of the F's of the $\binom{s}{t}$ distinct sets of b's taken t at a time. If we expand the right-hand side of (1.4) and reduce the degenerate terms by Lemmas 2.1 and 2.2, we have

THEOREM 2.1.

$$(r_1, \ldots, r_s) \prod_{i=1}^{s} m_i = \{(p^n - 1)^s - (-1)^s\}/p^n + \sum_{t=1}^{s} (-1)^{s-t} \mathop{\mathrm{S}}_{t}^{s} \Phi(r_1, \ldots, r_t),$$

where $\Phi(r_1, \ldots, r_t)$ *is defined by* (2.3).

Theorem 2.1 enables us in special cases to find the exact values of

$$(r_1, \ldots, r_s) \prod_{i=1}^{s} m_i$$

in terms of p, n, and m's explicitly. As an example, suppose $m_1 = \ldots = m_s = m$, n even and $p^{\frac{1}{2}n} + 1 \equiv 0 \pmod{m}$. If $u_i \not\equiv 0 \pmod{m}$ for any i and

$$\psi_{j,t} = \psi(u_1 + \ldots + u_j, u_{j+1}, \ldots, u_t),$$

then

$$\psi_{1,t} = p^{kn} \psi_{1,2} \psi_{2,3} \ldots \psi_{t-1,t}, \tag{2.5}$$

where k is the number of j's for which $u_1 + \ldots + u_j \equiv 0 \pmod{m}$, $j < t$. (For proof see [1, p. 265].) If $u_1 + \ldots + u_j \equiv 0 \pmod{m}$, we have from Lemmas 2.2 and 2.3,

$$\psi_{j-1,j} = \psi_{j,j+1} = -1.$$

If $u_1 + \ldots + u_j \not\equiv 0 \pmod{m}$, Mitchell [5, p. 177] proved $\psi_{j-1,j} = p^{\frac{1}{2}n}$. Among the first $t - 2$ elements in the right-hand side of (2.5), $2k$ have the value -1 and the remaining have the value $p^{\frac{1}{2}n}$; thus

$$\psi_{1,t} = \begin{cases} p^{\frac{1}{2}n(t-1)}, & u_1 + \ldots + u_t \not\equiv 0 \pmod{m}, \\ -p^{\frac{1}{2}n(t-2)}, & u_1 + \ldots + u_t \equiv 0 \pmod{m}. \end{cases}$$

https://doi.org/10.4153/CJM-1952-030-0 Published online by Cambridge University Press

As the u's range independently over the set $1, 2, \ldots, m - 1$, we have, by an easy induction, $u_1 + \ldots + u_t \not\equiv 0 \pmod{m}$ for $(m - 1\{(\mathrm{m} - 1)^t - (-1)^t\}/m$ sets of u's, and $u_1 + \ldots + u_t \equiv 0 \pmod{m}$ for $(m - 1)\{(m - 1)^{t-1} - (-1)^{t-1}\}/m$ sets of u's. Thus if $r_1 \equiv \ldots \equiv r_s \equiv 0 \pmod{m}$,

$$\Phi(r_1, \ldots, r_t) = p^{\frac{1}{2}n(t-1)}(m - 1)\{(m - 1)^t - (-1)^t \\ - p^{-\frac{1}{2}n}((m - 1)^{t-1} + (-1)^t)\}/m.$$

If we substitute this value in Theorem 2.1 and reduce the resulting sum, we obtain

$$(2.6) \qquad N = (p^n - 1)^s/p^n + \{(mp^{\frac{1}{2}n} - p^{\frac{1}{2}n} - 1)^{s+1} \\ + (m - 1)(-p^{\frac{1}{2}n} - 1)^{s+1}\}/mp^n.$$

In the above formula N denotes the number of non-zero solutions in $F(p^n)$ (n even and $p^{\frac{1}{2}n} + 1 \equiv 0 \pmod{m}$) of

$$x_1^{\ m} + \ldots + x_s^{\ m} = 1.$$

We shall now obtain another additive decomposition formula for $(r_1, \ldots, r_s)$. Suppose for any $t \leqslant k \geqslant 2$,

$$(2.7) \quad (r_1, \ldots, r_t)\prod_{i=1}^{t} m_i = p^{(t-1)n} - \sum_{j=1}^{t-1} \mathop{\mathsf{S}}_{j}^{t} (r_1, \ldots, r_j)\prod_{i=1}^{j} m_i + \Phi(r_1, \ldots, r_t).$$

This is obviously true for $k = 2$. If we solve for $\Phi(r_1, \ldots, r_t)$ in (2.7) and substitute in Theorem 2.1, $s = k + 1$, we have

$$(r_1, \ldots, r_{k+1})\prod_{i=1}^{k+1} = \{(p^n - 1)^{k+1} - (-1)^{k+1}\}/p^n \\ + \sum_{t=1}^{k}(-1)^{k+1-t} \mathop{\mathsf{S}}_{t}^{k+1} \{-p^{(t-1)n} + \sum_{j=1}^{t} \mathop{\mathsf{S}}_{j}^{t} (r_1, \ldots, r_j)\prod_{i=1}^{j} m_i\} + \Phi(r_1, \ldots, r_{k+1}).$$

For any $t \geqslant j$ we note that the term $(r_1, \ldots, r_j)$ will be contained in the remaining $k + 1 - j$ sets taken $t - j$ at a time; thus the coefficient of

$$(r_1, \ldots, r_j)\prod_{i=1}^{j} m_i$$

is

$$\sum_{t=j}^{k} (-1)^{k+1-t}\binom{k + 1 - j}{t - j},$$

which can be reduced to minus one. The constant terms, when collected, are

$$\frac{(p^n - 1)^{k+1} - (-1)^{k+1}}{p^n} - \sum_{t=1}^{k} (-1)^{k+1-t}\binom{k+1}{t}p^{(t-1)n},$$

which can be reduced, in a similar manner, to p^{kn}. Thus we have established by induction

THEOREM 2.2. *If* $s \geqslant 2$,

$$(r_1, \ldots, r_s)\prod_{i=1}^{s} m_i = p^{(s-1)n} - \sum_{t=1}^{s-1} \mathop{S}_{t}^{s} (r_1, \ldots, r_t)\prod_{i=1}^{t} m_i + \Phi(r_1, \ldots, r_s),$$

where Φ *is defined in* (2.3).

If $c \neq 0$ in equation (1.1),

$$N_s = \sum_{t=1}^{s} \mathop{S}_{t}^{s} (r_1, \ldots, r_t)\prod_{i=1}^{t} m_i;$$

thus we immediately obtain from Theorem 2.2 the

COROLLARY. $N_s = p^{(s-1)n} + \Phi(r_1, \ldots, r_s).$

Weil [**8**, p. 502] has a more complicated expression for N_s in terms of characters.

If $u_i \not\equiv 0 \pmod{m_i}$ for any i,

$$|\psi(u_1, \ldots, u_s)| = \begin{cases} p^{\frac{1}{2}n(s-1)}, & \prod_{i=1}^{s} a_i^{u_i} \neq 1, \\ p^{\frac{1}{2}n(s-2)}, & \prod_{i=1}^{s} a_i^{u_i} = 1. \end{cases}$$

(For proof see [**1**, p. 263].) From the Corollary we then obtain

$$|N_s - p^{(s-1)n}| \leqslant p^{\frac{1}{2}n(s-1)}\left(\prod_{i=1}^{s} (m_i - 1) - K_s\right) + p^{\frac{1}{2}n(s-2)}K_s,$$

where K_s is the number of sets of u's for which

$$\prod_{i=1}^{s} a_i^{u_i} = 1.$$

This limit is better than that given by Hua and Vandiver [**2**, p. 99] or Weil [**8**, p. 502]. Whiteman [**9**, p. 378] found that

$$K_s = \sum_{t=2}^{s} (-1)^{s-t} \mathop{S}_{t}^{s} \frac{m_1 \ldots m_t}{[m_1, \ldots, m_t]} + (-1)^{s-1}(s-1),$$

where $[m_1, \ldots, m_t]$ is the least common multiple of $m_1, \ldots, m_t$.

We can again give the exact values of N_s in certain special cases.

3. Linear relations involving $(r_1, \ldots, r_s)$. If in relation (1.4) we let r_i range over the set $0, 1, \ldots, m_i - 1$ $(i = 1, \ldots, t)$, we have for $t < s$,

$$\text{(3.1)} \quad \sum_{r_1, \ldots, r_t} (r_1, \ldots, r_s)\prod_{i=1}^{s} m_i$$

$$= \sum_{u_1, \ldots, u_s} \psi(u_1, \ldots, u_s) \prod_{i=t+1}^{s} a_i^{-u_i r_i} \sum_{r_1, \ldots, r_t} \prod_{i=1}^{t} a_i^{-u_i r_i}.$$

We see that each term equals zero unless $u_i = 0$ for each i $(i = 1, \ldots, t)$; thus the right-hand side of (3.1) becomes

$$\prod_{i=1}^{t} m_i \sum_{u_{t+1}, \ldots, u_s} \psi(0, \ldots, 0, u_{t+1}, \ldots, u_s) \prod_{i=t+1}^{s} a_i^{-u_i r_i}.$$

https://doi.org/10.4153/CJM-1952-030-0 Published online by Cambridge University Press

$\psi(0, \dots, 0, u_{t+1}, \dots, u_s)$ can be reduced by Lemma 2.2 if $u_i \neq 0$ for some i. If we add and subtract $\psi(u_{t+1}, \dots, u_s)$, $u_{t+1} = \dots = u_s = 0$, we obtain

$$\sum_{r_1, \dots, r_t} (r_1, \dots, r_s) \prod_{i=t+1}^{s} m_i = \{(p^n - 1)^s - (-1)^s\}/p^n$$
$$- (-1)^t\{(p^n - 1)^{s-t} - (-1)^{s-t}\}/p^n + (-1)^t \sum \psi(u_{t+1}, \dots, u_s) \prod_{i=t+1}^{s} a_i^{-u_i r_i},$$

where each u_i ranges independently over the set $0, 1, \dots, m_i - 1$; thus we have, in view of (1.4),

THEOREM 3.1.

$$\sum_{r_1, \dots, r_t} (r_1, \dots, r_s) \prod_{i=t+1}^{s} m_i = (p^n - 1)^{s-t}\{(p^n - 1)^t - (-1)^t\}/p^n$$
$$+ (-1)^t (r_{t+1}, \dots, r_s) \prod_{i=t+1}^{s} m_i,$$

where for $i = 1, \dots, t$ $(t < s)$, each r_i ranges independently over the set $0, 1, \dots, m_i - 1$.

4. On equation (1.1) **with** $c = 0$. In this section we shall investigate the number of distinct non-zero solutions of equation (1.1) with $c = 0$. With a slight modification of the function defined in (1.3) we can establish relations analogous to those given in Theorem 2.1 and Theorem 2.2 for this case. Owing to the special character of this problem we are able to find by elementary methods a recursion formula that expresses the number of solutions of (1.1) in terms of the number of solutions of equations containing fewer terms. The methods employed here first appeared in a paper by Hua and Vandiver [**4**, p. 486].

If the m's in (1.1) are grouped into k sets which are prime each to each, we have an equation of the form

$$(4.1) \qquad \sum_{i=1}^{s_1} c_{1,i} x_{1,i}^{m_{1,i}} + \dots + \sum_{i=1}^{s_k} c_{k,i} x_{k,i}^{m_{k,i}} = 0.$$

Let m_j be the least common multiple of $m_{j,i}$ for each j and $i = 1, \dots, s_j$; thus $(m_h, m_t) = 1, h \neq t$. Also impose the condition that $m_j = m_{j,1}$ for each j less than k. *Denote by $N_{t,k}$ the number of non-zero solutions of*

$$(4.2) \qquad \sum_{i=1}^{s_t} c_{t,i} x_{t,i}^{m_{t,i}} + \dots + \sum_{i=1}^{s_k} c_{k,i} x_{k,i}^{m_{k,i}} = 0.$$

Also denote by H_t and G_t the number of distinct non-zero solutions of

$$(4.3) \qquad h_t \equiv \sum_{i=1}^{s_t} c_{t,i} x_{t,i}^{m_{t,i}} = 0$$

and

$$(4.4) \qquad g_t \equiv c_{t,1} + \sum_{i=2}^{s_t} c_{t,i} x_{t,i}^{m_{t,i}} = 0,$$

respectively.

Since $m_t = m_{t,1}(t < k)$ we can transform (4.4) into (4.3) by multiplying through by $x_{t,1}^{m_t}$; thus there are $(p^n - 1)$ distinct solutions of (4.3) for each solution of (4.4). For each solution of (4.3) we obtain a solution of (4.4) by dividing through by the same quantity, hence we have

LEMMA 4.1. *If H_t and G_t are the number of distinct non-zero solutions of* (4.3) *and* (4.4) *respectively and $m_{t,1} \equiv 0 \pmod{m_{t,i}}$ $(i = 2, \ldots, s_t)$, then*

$$H_t = (p^n - 1)G_t.$$

Let $M = m_2 \ldots m_k$, $k \geqslant 2$; since $(m_1, M) = 1$, it is known that there exist numbers a and b such that

$$am_1 + bM = 1, \qquad (a, p^n - 1) = 1. \tag{4.5}$$

Since $(a, p^n - 1) = 1$, we can determine $y_{t,i}$, in $F(p^n)$, such that

$$x_{1,1} = y_{1,1}^{a},$$

$$x_{1,i} = y_{1,i}y_{1,1}^{am_1/m_{1,i}}, \qquad i > 1,$$

$$x_{t,i} = y_{t,i}y_{1,1}^{-bM/m_{t,i}}, \qquad t > 1, \text{ for any } i.$$

If we substitute the above relations in (4.1) and reduce by (4.5), we have

$$y_{1,1}\left(c_{1,1} + \sum_{i=2}^{s_1} c_{1,1}y_{1,i}^{m_{1,i}}\right) + \sum_{t=2}^{k}\sum_{i=1}^{s_t} c_{t,i}y_{t,i}^{m_{t,i}} = 0. \tag{4.6}$$

For the

$$(p^n - 1)^{s_2+\ldots+s_k} - N_{2,k}$$

values of $y_{t,i}$ $(t > 1)$ for which

$$\sum_{t=2}^{k} h_t \neq 0,$$

and the

$$(p^n - 1)^{s_1-1} - G_1$$

values of $y_{1,i}$ $(i > 1)$ for which $g_1 \neq 0$, there exists a unique $y_{1,1}$. For the $N_{2,k}$ values of $y_{t,i}$ $(t > 1)$ for which

$$\sum_{t=2}^{k} h_t = 0,$$

and the G_1 values of $y_{1,i}$ $(i > 1)$ for which $g_1 = 0$, there are $p^n - 1$ values of $y_{1,1}$. Consequently we have

$$N_{1,k} = \{(p^n - 1)^{s_2+\ldots+s_k} - N_{2,k}\}\{(p^n - 1)^{s_1-1} - G_1\} + (p^n - 1)N_{2,k}G_1.$$

In view of Lemma 4.1 we write

$$N_{1,k} = p^{-n}(p^n - 1)^{s_1+\ldots+s_k}$$
$$+ \{(p^n - 1)^{s_1} - p^nH_1\}\{(p^n - 1)^{s_2+\ldots+s_k} - p^nN_{2,k}\}/p^n(p^n - 1).$$

We obtain by induction,

https://doi.org/10.4153/CJM-1952-030-0 Published online by Cambridge University Press

THEOREM 4.1. *If $N_{1,k}$ and H_t denote the number of distinct non-zero solutions in $F(p^n)$ of* (4.1) *and* (4.3) *respectively, if m_t is the least common multiple of $m_{t,i}$ with $(m_t, m_r) = 1 (t \neq r)$, and if $m_t = m_{t,1}$ $(t < k)$, then*

$$N_{1,k} = p^{-n}(p^n - 1)^{s_1 + \ldots + s_k} + \frac{(-1)^k}{p^n(p^n - 1)^{k-1}} \prod_{t=1}^{k} \{(p^n - 1)^{s_t} - p^n H_t\}.$$

This recursion formula has a distinct advantage in that H_t is the number of solutions of an equation whose coefficients are in the original equation. It enables us to give the exact values of the number of solutions in a great variety of special cases; we shall give two of these here.

Let N be the number of distinct non-zero solutions in $F(p^n)$ of

$$\sum_{t=1}^{k} \sum_{i=1}^{s_t} x_{t,i}^{m_t} = 0,$$

where n is even, $p^{\frac{1}{2}n} + 1 \equiv 0 \pmod{m_t}$ $(t = 1, \ldots, k)$, and $(m_t, m_r) = 1$ $(t \neq r)$. Then we have, by (2.6),

$$H_t = (p^n - 1)\{(p^n - 1)^{s_t - 1} m_t + (p^{\frac{1}{2}n} m_t - p^{\frac{1}{2}n} - 1)^{s_t}$$
$$+ (m_t - 1)(-p^{\frac{1}{2}n} - 1)^{s_t}\}/m_t p^n$$

in Theorem 4.1.

In order to apply this theorem to a second special case we shall first find the number of solutions of

$$(4.7) \qquad x_1^{c_1 m} - x_2^{c_2 m} = 0$$

in $F(p^n)$, where $(c_1, c_2) = 1$ and $p^n - 1 \equiv 0 \pmod{c_i m}$ for each i. Since $(c_1, c_2) = 1$, there exist integers a and b such that $ac_1 + bc_2 = 1$, where $(a, p^n - 1) = 1$. We can determine y_1 and y_2 such that $x_1 = y_1^a$ and $x_2 = y_2 y_1^{-b}$; if we substitute these values in (4.7), we then have

$$y_1^m = y_2^{c_2 m}.$$

For the $p^n - 1$ distinct values of y_2 there are m values of y_1. Thus if H is the number of distinct non-zero solutions of (4.7), then

$$(4.8) \qquad H = (p^n - 1)m.$$

If N denotes the number of distinct non-zero solutions in $F(p^n)$ of

$$\sum_{i=1}^{k} (x_{i,1}^{a_i m_i} - x_{i,2}^{m_i}) = 0,$$

with $(a_r m_r, a_t m_t) = 1$ $(r \neq t)$, then from Theorem 4.1 and (4.8) we obtain

$$N = (1/p^n)(p^n - 1)^{2k} + (-1)^k (p^n - 1)(1/p^n) \prod_{t=1}^{k} (p^n - 1 - p^n m_t).$$

This method is extremely useful in investigating trinomial equations of the type (1.1) with $c = 0$. We can give explicit formulae for the number of non-zero solutions in the case $(m_1, m_2 m_3) = 1$ and in general reduce the exponents, except in the case where one exponent is divisible by the other two.

https://doi.org/10.4153/CJM-1952-030-0 Published online by Cambridge University Press

References

1. O. B. Faircloth and H. S. Vandiver, *On the multiplicative properties of a generalized Jacobi-Cauchy cyclotomic sum*, Proc. Nat. Acad. Sci., vol. 36 (1950), 260-267.
2. L. K. Hua and H. S. Vandiver, *Characters over certain types of rings with application to the theory of equations in a finite field*, Proc. Nat. Acad. Sci., vol. 35 (1949), 94-99.
3. ———, *On the number of solutions of some trinomial equations in a finite field*, Proc. Nat. Acad. Sci., vol. 35 (1949), 477-481.
4. ———, *On the nature of the solutions of certain equations in a finite field*, Proc. Nat. Acad. Sci., vol. 35 (1949), 481-487.
5. H. H. Mitchell, *On the generalized Jacobi-Kummer cyclotomic function*, Trans. Amer. Math. Soc., vol. 17 (1916), 165-177.
6. H. S. Vandiver, *On the number of solutions of some general types of equations in a finite field*, Proc. Nat. Acad. Sci., vol. 32 (1946), 47-52.
7. ———, *On a generalization of a Jacobi exponential sum associated with cyclotomy*, Proc. Nat. Acad. Sci., vol. 36 (1950), 144-151.
8. A. Weil, *Number of solutions of equations in a finite field*, Bull. Amer. Math. Soc., vol. 55 (1949), 497-508.
9. A. L. Whiteman, *Finite Fourier series and cyclotomy*, Proc. Nat. Acad. Sci., vol. 37 (1951), 375-378.

The University of Texas

https://doi.org/10.4153/CJM-1952-030-0 Published online by Cambridge University Press