THE NUMBER OF SOLUTIONS OF CERTAIN TYPES OF EQUATIONS IN A FINITE FIELD

L. CARLITZ

1. Using a very simple principle, Morgan Ward [3] indicated how one can obtain all solutions of the equation

$$(1) \qquad y^m = f(x_1, \cdots, x_r) \qquad (y, x_i \in F),$$

where F is an arbitrary field, $f(x_1, \cdots, x_r)$ is a homogeneous polynomial of degree n with coefficients in F, and $(m, n) = 1$. The same principle had been applied earlier to a special equation by Hua and Vandiver [2]. If this principle is applied in the case of a finite field F we readily obtain the total number of solutions of equations of the type (1). Somewhat more generally, let

$$f_i(x_i) = f_i(x_{i1}, \cdots, x_{is_i}) \qquad (i = 1, \cdots, r)$$

denote r polynomials with coefficients in $GF(q)$, and assume

$$(2) \qquad f_i(\lambda x_1, \cdots, \lambda x_{s_i}) = \lambda^{m_i} f_i(x_1, \cdots, x_{s_i}) \qquad (\lambda \in GF(q));$$

assume also

$$(3) \qquad (m, m_i, q-1) = 1 \qquad (i = 1, \cdots, r).$$

We consider the equation

$$(4) \qquad y^m = f_1(x_{11}, \cdots, x_{1s_1}) + \cdots + f_r(x_{r1}, \cdots, x_{rs_r})$$

in $s_1 + \cdots + s_r + 1$ unknowns.

Suppose first we have a solution of (4) with $y \neq 0$. Select integers h, k, l such that

$$(5) \qquad hm + km_1 m_2 \cdots m_r + l(q-1) = 1, \qquad (h, q-1) = 1;$$

Received August 8, 1953.
Pacific J. Math. 5 (1955), 177-181

this can be done in view of (3). Next put

$$(6)\qquad y=\lambda^h,\ x_{ij}=\lambda^{kM/m_i}z_{ij}\qquad (M=m_1m_2\cdots m_r).$$

Substituting in (4) and using (2), we get

$$\lambda^{hm}=\lambda^{kM}\{f_1(z_1)+\cdots+f_r(z_r)\}.$$

Since $\lambda^{q-1}=1$, it is clear from (5) that

$$(7)\qquad \lambda=f_1(z_1)+\cdots+f_r(z_r).$$

Thus any solution (y, x_{ij}) of (4) with $y\neq 0$ can be obtained from (6) and (7) by assigning arbitrary values to z_{ij} such that the right member of (7) does not vanish. Let N denote the total number of solutions of (4) and let N_0 denote the number of solutions with $y=0$. Thus there are $N-N_0$ sets z_{ij} for which $\lambda\neq 0$. Since in all there are $q^{s_1+\cdots+s_r}$ sets z_{ij} it follows that

$$(8)\qquad N=q^{s_1+\cdots+s_r}.$$

This proves:

THEOREM. *Let the polynomials f_i satisfy* (2) *and* (3). *Then the total number of solutions of* (4) *is furnished by* (8).

2. In Theorem II of [2] Hua and Vandiver proved that the number of solutions of

$$(9)\qquad c_1x_1^{a_1}+c_2x_2^{a_2}+\cdots+c_sx_s^{a_s}=0$$

subject to the conditions

$$c_1c_2\cdots c_sx_1x_2\cdots x_s\neq 0,\ (a_i, q-1)=k_i,\ (k_i,k_j)=1\ \text{for}\ i\neq j,$$

is equal to

$$(10)\qquad \frac{q-1}{q}\{(q-1)^{s-1}+(-1)^s\}.$$

It is easy to show that (10) implies that the total number of solutions of (9) is equal to q^{s-1}, which agrees with (8). Conversely if N_s denotes the number of nonzero solutions of (9), and we assume that

$$(k_i, k_j) = 1 \qquad (i, j = 1, \cdots, s;\ i \neq j), \tag{11}$$

then using (8) we get

$$q^{s-1} = N_s + \binom{s}{1} N_{s-1} + \binom{s}{2} N_{s-2} + \cdots + \binom{s}{s-1} N_1 + 1.$$

Hence (if we take $N_0 = 1$)

$$(q-1)^s = \sum_{r=1}^{s} (-1)^{s-r} \binom{s}{r} q \sum_{t=0}^{r} \binom{r}{t} N_t + (-1)^s$$

$$= q \sum_{r=0}^{s} (-1)^{s-r} \binom{s}{r} \sum_{t=0}^{r} \binom{r}{t} N_t - (-1)^s (q-1)$$

$$= q \sum_{t=0}^{s} \binom{s}{t} N_t \sum_{r=t}^{s} (-1)^{s-r} \binom{s-t}{s-r} - (-1)^s (q-1)$$

$$= qN_s - (-1)^s (q-1),$$

and (10) follows at once. Thus if we assume (11) then (8) and (10) are equivalent.

If in place of (11) we assume only that

$$(k_1, k_2 k_3 \cdots k_s) = 1, \tag{12}$$

the situation is somewhat different. As above let N_s denote the number of non-zero solutions of (9), and let M_{s-1} denote the total number of solutions $x_2, \cdots, x_s$ of

$$c_2 x_2^{a_2} + c_3 x_3^{a_3} + \cdots + c_s x_s^{a_s} = 0. \tag{13}$$

Using (8) we now get

$$q^{s-1} = M_{s-1} + N_s + \binom{s-1}{1} N_{s-1} + \cdots + \binom{s-1}{s-1} N_1, \tag{14}$$

which implies (with $M_0 = 1$)

$$(q-1)^{s-1} = \sum_{r=0}^{s-1} (-1)^{s-1-r} \binom{s-1}{r} M_r + N_s . \tag{15}$$

Thus making only the assumption (12) we see how the number of solutions of (13) can be expressed in terms of N_s and *vice versa*.

3. Returning to equation (4), we see that a similar result can be obtained if we allow f_i to contain additional unknowns:

$$f_i(x_i ; u_i) = f_i(x_{i1}, \cdots, x_{is_i}; u_{i1}, \cdots, u_{it_i}),$$

and assume that (2) holds only for the x's. Then the number of solutions (y, x_{ij}, u_{hk}) of (4) becomes

$$q^{s_1 + \cdots + s_r + t_1 + \cdots + t_r}.$$

Similarly we may replace the left member of (4) by

$$y_1^{a_1} y_2^{a_2} \cdots y_s^{a_s} \qquad (a_1, a_2, \cdots, a_s) = m.$$

Then assuming (3) we again find that the number of solutions of the modified equation is equal to

$$q^{s_1 + \cdots + s_r + s - 1}.$$

This kind of generalization lends itself well to equation (9). For example it is easy to show (see [**1**, Theorem 10]) that the total number of solutions of the equation

$$\sum_{i=1}^{t} c_i \prod_{j=1}^{k_i} x_{ij}^{a_{ij}} = 0,$$

subject to $(a_{i1}, \cdots, a_{ik_i}, q-1) = d_i$, $(d_i, d_j) = 1$ for $i \neq j$, is equal to

$$q^{k_1 + \cdots + k_t - 1}.$$

REFERENCE

1. L. Carlitz, *The number of solutions of certain equations in a finite field*, Proc. Nat. Acad. Sci. U.S.A. **38** (1952), 515-519.

2. L. K. Hua and H. S. Vandiver, *On the nature of the solutions of certain equations in a finite field*, Proc. Nat. Acad. Sci. U.S.A. **35** (1949), 481-487.

3. Morgan Ward, *A class of soluble diophantine equations*, Proc. Nat. Acad. Sci. U.S.A. **37** (1951), 113-114.

DUKE UNIVERSITY