

Pacific Journal of Mathematics

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

L. CARLITZ

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

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

where F is an arbitrary field, $f(x_1, \dots, x_r)$ 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

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

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

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

assume also

$$(3) \quad (m, m_i, q - 1) = 1 \quad (i = 1, \dots, r).$$

We consider the equation

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

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

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

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

Received August 8, 1953.

Pacific J. Math. 5 (1955), 177-181

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

$$(6) \quad y = \lambda^h, \quad x_{ij} = \lambda^{kM/m_i} z_{ij} \quad (M = m_1 m_2 \cdots m_r).$$

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

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

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

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

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

$$(9) \quad c_1 x_1^{a_1} + c_2 x_2^{a_2} + \cdots + c_s x_s^{a_s} = 0$$

subject to the conditions

$$c_1 c_2 \cdots c_s x_1 x_2 \cdots x_s \neq 0, \quad (a_i, q-1) = k_i, \quad (k_i, k_j) = 1 \text{ for } i \neq j,$$

is equal to

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

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

$$(11) \quad (k_i, k_j) = 1 \quad (i, j = 1, \dots, s; i \neq j),$$

then using (8) we get

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

Hence (if we take $N_0 = 1$)

$$\begin{aligned} (q-1)^s &= \sum_{r=1}^s (-1)^{s-r} \binom{s}{r} q \sum_{t=0}^r \binom{r}{t} N_t + (-1)^s \\ &= q \sum_{r=0}^s (-1)^{s-r} \binom{s}{r} \sum_{t=0}^r \binom{r}{t} N_t - (-1)^s (q-1) \\ &= q \sum_{t=0}^s \binom{s}{t} N_t \sum_{r=t}^s (-1)^{s-r} \binom{s-t}{s-r} - (-1)^s (q-1) \\ &= qN_s - (-1)^s (q-1), \end{aligned}$$

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

$$(12) \quad (k_1, k_2 k_3 \dots k_s) = 1,$$

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, \dots, x_s of

$$(13) \quad c_2 x_2^{a_2} + c_3 x_3^{a_3} + \dots + c_s x_s^{a_s} = 0.$$

Using (8) we now get

$$(14) \quad q^{s-1} = M_{s-1} + N_s + \binom{s-1}{1} N_{s-1} + \dots + \binom{s-1}{s-1} N_1,$$

which implies (with $M_0 = 1$)

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

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:

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

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

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

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

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

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

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

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

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

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

PACIFIC JOURNAL OF MATHEMATICS

EDITORS

H. L. ROYDEN
Stanford University
Stanford, California

R. P. DILWORTH
California Institute of Technology
Pasadena 4, California

E. HEWITT
University of Washington
Seattle 5, Washington

A. HORN*
University of California
Los Angeles 24, California

ASSOCIATE EDITORS

H. BUSEMANN	P. R. HALMOS	R. D. JAMES	GEORGE PÓLYA
HERBERT FEDERER	HEINZ HOPF	BORGE JESSEN	J. J. STOKER
MARSHALL HALL	ALFRED HORN	PAUL LÉVY	KOSAKU YOSIDA

SPONSORS

UNIVERSITY OF BRITISH COLUMBIA
CALIFORNIA INSTITUTE OF TECHNOLOGY
UNIVERSITY OF CALIFORNIA, BERKELEY
UNIVERSITY OF CALIFORNIA, DAVIS
UNIVERSITY OF CALIFORNIA, LOS ANGELES
UNIVERSITY OF CALIFORNIA, SANTA BARBARA
MONTANA STATE UNIVERSITY
UNIVERSITY OF NEVADA
OREGON STATE COLLEGE
UNIVERSITY OF OREGON
UNIVERSITY OF SOUTHERN CALIFORNIA

STANFORD RESEARCH INSTITUTE
STANFORD UNIVERSITY
UNIVERSITY OF UTAH
WASHINGTON STATE COLLEGE
UNIVERSITY OF WASHINGTON

* * *

AMERICAN MATHEMATICAL SOCIETY
HUGHES AIRCRAFT COMPANY
SHELL DEVELOPMENT COMPANY

Mathematical papers intended for publication in the *Pacific Journal of Mathematics* should be typewritten (double spaced), and the author should keep a complete copy. Manuscripts may be sent to any of the editors. Manuscripts intended for the outgoing editors should be sent to their successors. All other communications to the editors should be addressed to the managing editor, Alfred Horn at the University of California, Los Angeles 24, California.

50 reprints of each article are furnished free of charge; additional copies may be obtained at cost in multiples of 50.

The *Pacific Journal of Mathematics* is published quarterly, in March, June, September, and December. The price per volume (4 numbers) is \$12.00; single issues, \$3.50. Back numbers are available. Special price to individual faculty members of supporting institutions and to individual members of the American Mathematical Society: \$4.00 per volume; single issues, \$1.25.

Subscriptions, orders for back numbers, and changes of address should be sent to Pacific Journal of Mathematics, c/o University of California Press, Berkeley 4, California.

Printed at Kokusai Bunken Insatsusha (International Academic Printing Co., Ltd.), No. 10, 1-chome, Fujimi-cho, Chiyoda-ku, Tokyo, Japan.

* During the absence of E. G. Straus.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS, A NON-PROFIT CORPORATION
COPYRIGHT 1955 BY PACIFIC JOURNAL OF MATHEMATICS

Leonard M. Blumenthal, <i>An extension of a theorem of Jordan and von Neumann</i>	161
L. Carlitz, <i>Note on the multiplication formulas for the Jacobi elliptic functions</i>	169
L. Carlitz, <i>The number of solutions of certain types of equations in a finite field</i>	177
George Bernard Dantzig, Alexander Orden and Philip Wolfe, <i>The generalized simplex method for minimizing a linear form under linear inequality restraints</i>	183
Arthur Pentland Dempster and Seymour Schuster, <i>Constructions for poles and polars in n-dimensions</i>	197
Franklin Haimo, <i>Power-type endomorphisms of some class 2 groups</i>	201
Lloyd Kenneth Jackson, <i>On generalized subharmonic functions</i>	215
Samuel Karlin, <i>On the renewal equation</i>	229
Frank R. Olson, <i>Some determinants involving Bernoulli and Euler numbers of higher order</i>	259
R. S. Phillips, <i>The adjoint semi-group</i>	269
Alfred Tarski, <i>A lattice-theoretical fixpoint theorem and its applications</i>	285
Anne C. Davis, <i>A characterization of complete lattices</i>	311