[2] Hodge, W. V. D., (*a*) *J. Lond. Math. Soc.*, **36** (2), 257 (1933). (*b*) *Theory of Harmonic Integrals*, Cambridge, 1941.
[3] Lord Kelvin, *Papers*, **4**, 13, Cambridge University Press.
[4] Kodaira, *Ann. Math.*, **50**, 587 (1949).
[5] Lefschetz, S., *Topology*, New York, 1930.
[6] de Rham, G., *J. Math.*, 115–200 (1931).
[7] Tucker, A. W., *Bull. Am. Math. Soc.*, **47**, 714 (1941).

A SUMMARY OF NEW RESULTS CONCERNING THE SOLUTIONS OF EQUATIONS IN FINITE FIELDS

BY OLIN B. FAIRCLOTH

DEPARTMENT OF APPLIED MATHEMATICS, UNIVERSITY OF TEXAS

Communicated by H. S. Vandiver, July 9, 1951

In this paper we shall give a summary of several results we have obtained concerning the number of distinct sets of solutions of equations of the type

$$c_1x_1^{m_1} + c_2x_2^{m_2} + \ldots + c_sx_s^{m_s} + c_{s+1} = 0, \qquad (1)$$

$s \geqq 2$, where the c's are given elements of a finite field of order p^n, p an odd prime, which will be designated $F(p^n)$ and $p^n - 1 = q_im_i$, $i = 1, \ldots, s$, with $c_1 \ldots c_s \neq 0$ in $F(p^n)$. In the case $c_{s+1} \neq 0$ we shall consider the equation

$$g^{y_1m_1 + r_1} + g^{y_2m_2 + r_2} + \ldots + g^{y_sm_s + r_s} = 1 \qquad (2)$$

where g is a generator of $F(p^n)$ aside from zero and $-c_i/c_{s+1} = g^{h_im_i + r_i}$. Let $(r_1, \ldots, r_s)$ denote the number of distinct sets $y_1, \ldots, y_s$; $y_i = 0, 1, \ldots, q_i - 1$, that satisfy equation (2); thus $(r_1, \ldots, r_s)m_1 \ldots m_s$ is the number of distinct sets of non-zero solutions of (1).

H. S. Vandiver[1] gave an expression for the number of solutions of (2),

$$(r_1, \ldots, r_s) \prod_{i=1}^{s} m_i = \sum_{u_1, \ldots, u_s} \psi(\alpha_1^{u_1}, \ldots, \alpha_s^{u_s}) \prod_{i=1}^{s} \alpha_i^{-u_ir_i} \qquad (3)$$

where u_i ranges from 0 to $m_i - 1$, $i = 1, \ldots, s$. For $s > 1$,

$$\psi(\alpha_1^{u_1}, \ldots, \alpha_s^{u_s}) = \sum_{a_1, \ldots, a_{s-1}} \alpha_s^{u_s \operatorname{ind} A} \prod_{i=1}^{s-1} \alpha_i^{u_i \operatorname{ind} a_i}, \qquad (4)$$

$$\psi(\alpha_i^{u_i}) = 1 \qquad (4a)$$

where $\alpha_i = e^{2\pi i/m_i}$; $\operatorname{ind} a_i$ is defined $g^{\operatorname{ind} a_i} = a_i$ in $F(p^n)$ with g a generator of the cyclic group formed by the non-zero elements of $F(p^n)$ under multiplication; $\alpha_i^{u_i \operatorname{ind} 0} = 0$ for all u_i; and each a ranges independently over each non-zero element of $F(p^n)$ with $A = 1 - a_1 - \ldots - a_{s-1}$.

By reducing the degenerate cases of (4), cases where $|\psi| \neq p^{(s-1)n/2}$, (see reference 2), we obtain

THEOREM I.

$$(r_1, \ldots, r_s) \prod_{i=1}^{s} m_i = p^{(s-1)n} - \sum_{t=1}^{s-1} S_t^s (r_1, \ldots, r_t) \prod_{i=1}^{t} m_i + B(r_1, \ldots, r_s) \quad (5)$$

where

$$B(r_1, \ldots, r_s) = \sum_{u_1, \ldots, u_s} \psi(\alpha_1^{u_1}, \ldots, \alpha_s^{u_s}) \prod_{i=1}^{s} \alpha_i^{-u_i r_i} \quad (6)$$

with u_i *ranging over the set* $1, 2, \ldots, m_i - 1$, *and*

$$S_t^s F(b_1, \ldots, b_t)$$

denotes the sum of the F's of the $\binom{s}{t}$ *distinct sets of b's taken t at a time.*

If we denote the number of solutions of (1) by

$$[r_1, \ldots, r_s], \quad (7)$$

we have from Theorem I,

COROLLARY.

$$[r_1, \ldots, r_s] = p^{(s-1)n} + B(r_1, \ldots, r_s) \quad (8)$$

where $B(r_1, \ldots, r_1)$ *is defined in* (6).

From (8) we obtain the following limits, (see reference 3),

$$\left|[r_1, \ldots, r_s] - p^{(s-1)n}\right| \leqq p^{(s-1)n/2} \left(\prod_{i=1}^{s} (m_i - 1) - K \right) + p^{(s-2)n/2} K \quad (9)$$

where K is the number of sets of u's in the sets $1, \ldots, m_i - 1$, $i = 1, \ldots, s$, such that $\alpha_1^{u_1} \ldots \alpha_s^{u_s} = 1$.

If M is the least common multiple of $m_1, \ldots, m_s$, we obtain from relation (3)

$$(r_1, \ldots, r_s) \prod_{i=1}^{s} m_i \leqq ((p^n - 1)^s - 1 + (-1)^{s+1})/p^n + ((p^{n/2}(M-1) + 1)^{s+1} + (M-1)(p^{n/2} + 1)^{s+1})/Mp^n. \quad (10)$$

From Corollary I

$$\sum_{r_1=0}^{m_i - 1} [r_1, \ldots, r_s] = p^{(s-1)n} m_i \quad (11)$$

follows easily.

Also from Corollary I we obtain, (see reference 4),

THEOREM II.

$$\sum_{r_1, \ldots, r_s} [r_1, \ldots, r_s]\,[r_1 + h_1, \ldots, r_s + h_s] = p^{2(s-1)n} \prod_{i=1}^{s} m_i +$$

$$\begin{cases} p^{(s-1)n} \prod_{i=1}^{s} m_i \prod_{i=1}^{t} (m_i - 1)(-1)^{s-t}, \begin{cases} h_i \equiv 0 \pmod{m_i}, & i \leq t \\ h_i \not\equiv 0 \pmod{m_i}, & i > t \end{cases} \\ p^{(s-1)n} \prod_{i=1}^{s} m_i (-1)^s, \; h_i \not\equiv 0 \pmod{m_i}, \; i = 1, \ldots, s \end{cases} +$$

$$(p^{(s-2)n} - p^{(s-1)n}) \prod_{i=1}^{s} m_i \sum_{u_1, \ldots, u_s} \alpha_1^{-u_1 h_1} \ldots \alpha_s^{-u_s h_s}$$

where the u's range over the sets 1, . . ., $m_i - 1$, $i = 1, \ldots, s$, such that $\alpha_1^{u_1} \ldots \alpha_s^{u_s} = 1$; and the r's range over the sets 0, 1, . . ., $m_i - 1$, $i = 1, \ldots, s$.

We obtain by direct addition from (3)

THEOREM III.

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

$$(-1)^t (r_1, \ldots, r_{s-t}) \prod_{i=1}^{s-t} m_i \quad (12)$$

where $s - t + 1 > 2$ and r_i range over the sets 0, 1, . . ., $m_i - 1$, $i = s - t + 1$, . . ., s. (13)

COROLLARY.

$$\sum_{r_2, \ldots, r_s} (r_1, \ldots, r_s) m_1 = (p^n - 1)\,((p^n - 1)^{s-1} - (-1)^{s-1})/p^n +$$

$$(-1)^{s-1} \begin{cases} 0, & r_1 \not\equiv 0 \pmod{m_1} \\ m_1, & r_1 \equiv 0 \pmod{m_1} \end{cases}$$

where r_i range over the sets 0, 1, . . ., $m_i - 1$, $i = 2, \ldots, s$.

If $m_1 = m_2 = \ldots = m_s$, n even and $p^{n/2} + 1 \equiv 0 \pmod{m_1}$, then we have obtained the exact values of $(0, \ldots, 0)m_1^s$ and $[0, \ldots, 0]$ in terms of s, p, n and m_1 explicitly.

If the m's in (1) are grouped into k sets which are prime each to each with $c_{s+1} = 0$, we have an equation of the form

$$\sum_{i=1}^{s_1} c_{1,i} x_{1,i} u^{m_{1,i}} + \sum_{i=1}^{s_2} c_{2,i}\, x_{2,i}^{m_{2,i}} + \ldots + \sum_{i=1}^{s_k} c_{k,1}\, x_{k,i}^{m_{k,i}} = 0 \quad (14)$$

Let m_t be the least common multiple of $m_{t,i}$ for each t and $i = 1, \ldots, s_t$; thus $(m_h, m_j) = 1$, $h \neq j$. Also impose the condition that $m_t = m_{t,1}$, $t < k$. Let H_t denote the number of distinct non-zero solutions of

$$\sum_{i=1}^{s_t} c_{t,i}\, x_{t,i}^{m_{t,i}} = 0.$$

THEOREM IV. *If N_k denotes the number of distinct sets of non-zero solutions in $F(p^n)$ of (14) then*

$$N_k = (1/p^n)(p^n - 1)^{s_1 + \ldots + s_k} + (-1)^k \prod_{i=1}^{k} ((p^n - 1)^{s_t} - p^n H_t)/p^n(p^n - 1)^{k-1}.$$

From Theorem IV we may in a great variety of cases find the exact values of N_k; such as trinomial equations of type (1) with $c_{s+1} = 0$ and one exponent prime to the other two.

[1] Vandiver, H. S., "On a Generalization of a Jacobi Exponential Sum Associated with Cyclotomy," these PROCEEDINGS, **36**, 144–151 (1950).

[2] Faircloth, O. B., and Vandiver, H. S., "On Multiplicative Properties of a Generalized Jacobi-Cauchy Cyclotomic Sum," *Ibid.*, **36**, 260–267 (1950).

[3] Weil, A., "Numbers of Solutions of Equations in Finite Fields," *Bull. Am. Math. Soc.*, **55**, 497–508 (1949). This limit is an improvement over that given by Weil, p. 502.

[4] Whiteman, A. L., "Finite Fourier Series and Cyclotomy," these PROCEEDINGS, **37**, 373–378 (1951). In this paper Whiteman gives analogous quadratic relations involving the parentheses symbols.

COMPACT SUBGROUPS

BY A. M. GLEASON

HARVARD UNIVERSITY

Communicated by J. L. Walsh, July 6, 1951

THEOREM: *Every connected compact subgroup of a locally compact group is contained in a maximal connected compact subgroup.*

For connected (L)-groups (locally compact groups which are projective limits of Lie groups) Iwasawa[1] has shown the existence of maximal compact subgroups and that all of these are conjugate. His proof relies on analytic investigation of the approximating Lie groups. Our proof uses only methods of group theory and topology and leads to a much weaker result, which, however, strengthens the standing conjecture that all connected locally compact groups are (L)-groups.

LEMMA 1. *Let* $\{H_\alpha\}$ *be an increasing collection of connected closed subgroups of a locally compact group* G. *Let* U *be a neighborhood of* e *in* G. *Then there exists an index* β *such that* $H_\alpha \subset H_\beta U$ *for all* α.

Proof: Without loss of generality we assume U compact. If the conclusion is false, then we can choose from $\{H_\alpha\}$ an infinite sequence (which we reindex) $H_0 \subset H_1$ non-$\subset H_2 \subset \ldots$ such that H_i non-$\subset H_{i-1}U$ for $i = 1, 2, \ldots$ Assuming such a sequence we shall deduce a contradiction.

Let V be another neighborhood of e such that $V^2 \subset U$. For each $i = 1, 2, \ldots$ we shall find an element h_i such that $h_i \in U \cap H_i$ and h_i non-$\in H_{i-1}V$. Let φ be the natural mapping of H_i onto the right coset space H_i/H_{i-1}. Now $\varphi(U \cap H_i)$ does not cover H_i/H_{i-1}, for if it did we should have