SOME SPECIAL EQUATIONS IN A FINITE FIELD

L. Carlitz

1. The equation (1.1). Let $f_i(u)$, $i = 1, \cdots, r$ denote polynomials with coefficients in the finite field $GF(q)$, $q = p^n$. We consider the equation

$$(1.1) \qquad f_1(\xi_1) + \cdots + f_r(\xi_r) = \alpha \qquad (\xi_i, \alpha \in GF(q));$$

let N denote the number of solutions of (1.1).

For $\beta \in GF(q)$, put

$$e(\beta) = e^{2\pi i t(\beta)/p}, \quad t(\beta) = \beta + \beta^p + \cdots + \beta^{p^{n-1}}.$$

Then we may write

$$(1.2) \qquad qN = \sum_{\beta} e(-\alpha\beta) \sum_{\xi_1, \cdots, \xi_r} e(\beta f_1(\xi_1) + \cdots + \beta f_r(\xi_r)),$$

where the summation extends over all numbers β, ξ_i of $GF(q)$. Now put

$$(1.3) \qquad S(f) = \sum_{\xi} e(f(\xi)),$$

where f is any polynomial with coefficients in $GF(q)$. Then (1.2) becomes

$$qN = q^r + \sum_{\beta \neq 0} e(-\alpha\beta) \prod_{i=1}^{r} S(\beta f_i).$$

2. Estimate for N. If $\deg f \leq 2$, $S(f)$ can be evaluated explicitly. However, we are primarily interested in the case $\deg f > 2$. An estimate for $S(f)$ is given by the following:

THEOREM 1. *If $k = \deg f < p$, then*

$$(2.1) \qquad S(f) = O(q^{1-1/k}) \qquad (q \longrightarrow \infty).$$

Received March 19, 1952.

Pacific J. Math. 3 (1953), 13-24

Mordell [7] has proved (2.1) in the case $n = 1$, that is, $q = p$. However, examination of his proof shows that (2.1) holds for all $n \geq 1$ provided we have $\deg f < p$.

If we substitute from (2.1) in (1.4) we have at once:

THEOREM 2. *The number of solutions of* (1.1), *where* $\deg f_i = k_i < p$, *is given by*

$$N = q^{r-1} + O(q^{r-w}) \qquad \left(w = \frac{1}{k_1} + \cdots + \frac{1}{k_r}\right). \tag{2.2}$$

This result is trivial unless $w > 1$, which will evidently be satisfied for r sufficiently large.

Hua and Vandiver [5] and Weil [9] have discussed the number of solutions of (1.1) in the special case $f_i(x) = x^{k_i}$; their results are considerably better than (2.2).

If $g_i(u)$, $i = 1, \cdots, r$, denote a second set of polynomials with coefficients in $GF(q)$ and such that $\deg g_i < k_i$, then an estimate can be obtained for the weighted sum

$$S_g = \sum_{\xi_1, \cdots, \xi_r} e(g_1(\xi_1) + \cdots + g_r(\xi_r)),$$

where the summation is extended over all ξ_i satisfying (1.1). Indeed, we have

$$\begin{aligned} qS_g &= \sum_\beta e(-\alpha\beta) \sum_{\xi_1, \cdots, \xi_r} e\left\{\sum_{i=1}^r (\beta f_i(\xi_i) + g_i(\xi_i))\right\} \\ &= \sum_\beta e(-\alpha\beta) \prod_{i=1}^r S(\beta f_i + g_i), \end{aligned}$$

in the notation of (1.3); consequently if at least one $g_i(x)$ is of degree ≥ 1, it follows that

$$S_g = O(q^{r-w}) \qquad \left(w = \frac{1}{k_1} + \cdots + \frac{1}{k_r}\right).$$

If all $k_i = 2$ then an explicit formula can be obtained for S_g.

3. Some special case. Let

$$f(x) = \alpha_1 x^{e_1} + \cdots + \alpha_k x^{e_k} \qquad (\alpha_i \in GF(q)); \tag{3.1}$$

Mordell has proved that

$$S(f) = O(q^{1-1/(2k)}) \qquad (q \longrightarrow \infty) \tag{3.2}$$

in the special case $q = p$. Negative values of e_i are permitted; however, in that case it is assumed that in the definition of $S(f)$, the summation is over $\xi \neq 0$. Clearly this does not affect the estimate (3.2). Here again we find that Mordell's proof applies to the general case. We state:

THEOREM 3. *If the integers e_i in* (3.1) *are incongruent* (mod $q-1$), *then* (3.2) *holds.*

(We remark that Min [6, p. 139, Lemma 1] states that (2.1) is valid, without mentioning the restriction $k < p$. However, his proof does not seem adequate. For example, for $k = p$, the system

$$\sum_{i=1}^{p} x_i^j = \sum_{i=1}^{p} y_i^j \qquad (j = 1, \cdots, p)$$

does not imply that the y's are a permutation of the x's.)

By means of Theorem 3 we obtain at once:

THEOREM 4. *Let $f_i(x)$, $i = 1, \cdots, r$, be polynomials of the type* (3.1), *with k replaced by k_i, and let no two exponents in $f_i(x)$ be congruent* (mod $q-1$). *Then the number of solutions of*

$$f_1(\xi_1) + \cdots + f_r(\xi_r) = \alpha \qquad (\xi_i \neq 0) \tag{3.3}$$

is given by

$$q^{r-1} + O(q^{r-w}) \qquad \left(w = \frac{1}{2k_1} + \cdots + \frac{1}{2k_r}\right). \tag{3.4}$$

Once again we have $w > 1$ for r sufficiently large.

The most interesting case of (3.1) is perhaps $f(x) = \alpha x + \beta x^{-1}$. The corresponding sum $S(f)$ is the Kloosterman sum

$$K(\alpha, \beta) = \sum_{\xi \neq 0} e(\alpha\xi + \beta\xi^{-1}). \tag{3.5}$$

Theorem 4 now implies:

THEOREM 5. *The number of solutions* $\xi_i \neq 0$ *of*

$$\alpha_1 \xi_1 + \frac{\beta_1}{\xi_1} + \cdots + \alpha_r \xi_r + \frac{\beta_r}{\xi_r} = \alpha \qquad (\alpha\alpha_i \beta_i \neq 0) \tag{3.6}$$

is given by

$$q^{r-1} + O(q^{3r/4}). \tag{3.7}$$

Indeed if we make use of Andre′ Weil's estimate [10] for (3.5)

$$|K(\alpha, \beta)| \leq 2q^{1/2},$$

then (3.7) can be replaced by

$$q^{r-1} + O(q^{r/2}), \tag{3.7$'$}$$

which is significant for $r \geq 3$.

4. Another special case. Let $p > 2$. Theorem 4 applies to $f(x) = x^2 + x^{-2}$, and indeed (3.7) furnishes on asymptotic formula for the number of solutions of

$$\alpha_1 \xi_1^2 + \frac{\beta_1}{\xi_1^2} + \cdots + \alpha_r \xi_r^2 + \frac{\beta_r}{\xi_r^2} = \alpha \qquad (\alpha\alpha_i \beta_i \neq 0). \tag{4.1}$$

However it is of interest to note that certain exact results can be obtained. Let N_1 and N_2 denote the number of solutions of (3.6) and (4.1), respectively. On the one hand

$$qN_1 = q^r + \sum_{\beta \neq 0} e(-\alpha\beta) \prod_{i=1}^{r} K(\beta\alpha_i, \beta\beta_i); \tag{4.2}$$

on the other hand

$$qN_2 = q^r + \sum_{\beta \neq 0} e(-\alpha\beta) \prod_{i=1}^{r} K_2(\beta\alpha_i, \beta\beta_i), \tag{4.3}$$

where

$$(4.4) \qquad K_2(\alpha, \beta) = \sum_{\xi \neq 0} e(\alpha \xi^2 + \beta \xi^{-2}).$$

Let $\psi(\xi) = +1$ or -1 according as ξ is a square or a non-square of $GF(q)$. Then (4.4) implies

$$K_2(\alpha, \beta) = \sum_{\xi \neq 0} (1 + \psi(\xi))\, e(\alpha\xi + \beta\xi^{-1}) = K(\alpha, \beta) + L(\alpha, \beta),$$

where

$$(4.5) \qquad L(\alpha, \beta) = \sum_{\xi \neq 0} \psi(\xi)\, e(\alpha\xi + \beta\xi^{-1}).$$

Now it is not difficult to evaluate $L(\alpha, \beta)$ explicitly (compare [8, p.102]). We have

$$L(\alpha, \beta) = \begin{cases} 0 & (\psi(\alpha\beta) = -1) \\ G(1)\,(e(2\gamma) + e(-2\gamma)) & (\alpha\beta = \gamma^2). \end{cases}$$

As for the Gauss sum $G(1)$, we note [1, §3]

$$(4.7) \quad G(\alpha) = \sum_{\xi} e(\alpha\xi^2) = \psi(\alpha)\, G(1) \qquad (\alpha \neq 0;\ G^2(1) = q\psi(-1)).$$

Then by (4.3), (4.4), and (4.5),

$$(4.8) \qquad qN_2 = q^r + \sum_{\beta \neq 0} e(-\alpha\beta) \prod_{i=1}^{r} (K(\beta\alpha_i, \beta\beta_i) + L(\beta\alpha_i, \beta\beta_i)).$$

Comparison of (4.2) and (4.8) leads at once to:

THEOREM 6. *If $\psi(\alpha_i\beta_i) = -1$, $i = 1, \cdots, r$, then the number of solutions of (4.1) is equal to the number of solutions of (3.6).*

5. Quadratic forms. In the remainder of the paper we shall be concerned with a quadratic form

$$(5.1) \qquad Q(u_1, \cdots, u_r) = \sum_{i,j=1}^{r} \alpha_{ij} u_i u_j \quad (\alpha_{ij} \in GF(q),\ \delta = |\alpha_{ij}| \neq 0).$$

We recall that the number of solutions $N_Q(\alpha)$ of

$$(5.2) \qquad Q(\xi_1, \cdots, \xi_r) = \alpha$$

is given [4, pp. 47-48] by

$$(5.3) \qquad \begin{cases} q^{2s-1} + (q^s - q^{s-1})\, \psi((-1)^s \delta) & (\alpha = 0) \\ q^{2s-1} - q^{s-1}\, \psi((-1)^s \delta) & (\alpha \neq 0) \end{cases}$$

for $r = 2s$;

$$(5.4) \qquad q^{2s} + q^s\, \psi((-1)^s \alpha \delta)$$

for $r = 2s + 1$, where in (5.4) it is understood that $\psi(0) = 0$.

Now let $f(u_1, \cdots, u_t)$ denote an arbitrary polynomial with coefficients in $GF(q)$, and let $N_f(\alpha)$ denote the number of solutions ζ_1 of

$$(5.5) \qquad f(\zeta_1, \cdots, \zeta_t) = \alpha .$$

Clearly the number of solutions ξ_i, ζ_j of

$$(5.6) \qquad Q(\xi_1, \cdots, \xi_t) = f(\zeta_1, \cdots, \zeta_t)$$

is given by

$$(5.7) \qquad N = \sum_{\alpha} N_Q(\alpha)\, N_f(\alpha).$$

We shall now show that the right member of (5.7) can be evaluated in certain cases.

In the first place let $f = u^k$. Then (5.7) becomes

$$N = \sum_{\xi} N_Q(\xi^k) = N_Q(0) + \sum_{\xi \neq 0} N_Q(\xi^k).$$

Now apply (5.3) and we get, for $r = 2s$,

$$N = (q^{2s-1} + (q^s - q^{s-1})\, \psi((-1)^s \delta)) + (q-1)\,(q^{2s-1} - q^{s-1}\, \psi((-1)^s \delta)),$$

which is simply

$$(5.8) \qquad N = q^{2s} \qquad (r = 2s).$$

Similarly, application of (5.4) in the case $r = 2s + 1$ yields

$$(5.9) \qquad N = \begin{cases} q^{2s+1} & (k \text{ odd}) \\ q^{2s+1} + q^s(q-1)\,\psi((-1)^s\,\delta) & (k \text{ even}). \end{cases}$$

This proves:

THEOREM 7. *The number of solutions of*

$$Q(\xi_1, \cdots, \xi_r) = \zeta^k \qquad (k \geq 1)$$

is furnished by (5.8) *and* (5.9).

A slight generalization of Theorem 7 is contained in:

THEOREM 8. *The number of solutions of*

$$Q(\xi_1, \cdots, \xi_r) = \zeta_1^{k_1} \cdots \zeta_t^{k_t} \qquad (k_i \geq 1)$$

is given by

$$N = q^{t+2s-1} + \{(q^s - q^{s-1})\,q^t - q^s\,(q-1)^t\}\,\psi((-1)^s\delta)$$

for $r = 2s$;

$$N = \begin{cases} q^{t+2s} & ((k_1, \cdots, k_t) \text{ odd}) \\ q^{t+2s} + q^s\,(q-1)^t\,\psi((-1)^s\,\delta) & ((k_1, \cdots, k_t) \text{ even}) \end{cases}$$

for $r = 2s + 1$.

In the next place let f denote a polynomial such that $f(\zeta_2, \cdots, \zeta_t)$ never vanishes. Then since for $r = 2s$, $\alpha \neq 0$, $N_Q(\alpha)$ is independent of α, we see that the number of solutions of (5.6) is given by

$$(5.10) \qquad N = q^t\{q^{2s-1} - q^{s-2}\,\psi((-1)^s\,\delta)\}$$

for $r = 2s$. On the other hand, for $r = 2s + 1$ we get

$$(5.11) \qquad N = q^{t+3s} + q^s\,\psi((-1)^s\,\delta) \sum_{\zeta_1, \cdots, \zeta_t} \psi(f(\zeta_1, \cdots, \zeta_t)).$$

We state:

THEOREM 9. *Let f be a polynomial such that $f(\zeta_1, \cdots, \zeta_t)$ never vanishes. Then the number of solutions of* (5.6) *is furnished by* (5.10) *and* (5.11).

Note that the right member of (5.10) is independent of the polynomial f. It follows from (5.11) that the number of solutions of

$$Q(\xi_1, \cdots, \xi_{2s+1}) = f^{2m+1}(\zeta_1, \cdots, \zeta_t)$$

is the same for all values of m. Other special cases that lead to simple explicit results are contained in the following two theorems:

THEOREM 10. *Let f be a polynomial such that $f(\zeta_1, \cdots, \zeta_t)$ never vanishes. Then the number of solutions of*

$$Q(\xi_1, \cdots, \xi_{2s+1}) = f^2(\zeta_1, \cdots, \zeta_t)$$

is given by

$$q^{t+2s} + q^{t+s}\, \psi((-1)^s \delta).$$

THEOREM 11. *Let f be a polynomial such that $f(\zeta_1, \cdots, \zeta_t)$ never vanishes. Then the number of solutions ξ_i, η, ζ_j of*

$$Q(\xi_1, \cdots, \xi_r) = \eta^k f(\zeta_1, \cdots, \zeta_t) \qquad (k \geq 1)$$

is q^{t+2s} for $r = 2s$, while for $r = 2s + 1$ the number of solutions is given by

$$(5.12) \quad \begin{cases} q^{t+2s} & (k \text{ odd}) \\ q^{t+2s} + q^s(q-1)\, \psi((-1)^s \delta) \displaystyle\sum_{\zeta_1, \cdots, \zeta_t} \psi(f(\zeta_1, \cdots, \zeta_t)) & (k \text{ even}). \end{cases}$$

In particular if f is the square of a polynomial then the second of (5.12) reduces to

$$q^{t+2s} + q^{t+s}(q-1)\, \psi((-1)^s \delta).$$

It is clear how Theorem 11 can be generalized to give the number of solutions of

$$Q(\xi_1, \cdots, \xi_r) = \eta_1^{k_1} \cdots \eta_w^{k_w} f(\zeta_1, \cdots, \zeta_t).$$

A word may be added about a generalization of a different kind. Let Q_i denote quadratic forms in r_i indeterminates and of discriminant $\delta_i \neq 0$. Then we can treat such equations as

$$Q_1(\xi_1, \cdots, \xi_{r_1}) Q_2(\eta_1, \cdots, \eta_{r_2}) = \alpha. \tag{5.13}$$

For example, the number of solutions of (5.13) for $\alpha \neq 0$ is evidently

$$\sum_{\beta \neq 0} N_{Q_1}(\beta) N_{Q_2}(\alpha/\beta), \tag{5.14}$$

which can be evaluated by means of (5.3) and (5.4). In particular if r_1 and r_2 are both even, then (5.14) becomes

$$(q-1)(q^{2s_1-1} - q^{s_1-1}\psi((-1)^{s_1}\delta_1))(q^{2s_2-1} - q^{s_2-1}\psi((-1)^{s_2}\delta_2)),$$

where $r_i = 2s_i$. In similar fashion we can determine the number of solutions of, say,

$$Q_1 Q_2 + \cdots + Q_{2w-1} Q_{2w} = \alpha, \tag{5.15}$$

where no two Q's have any unknowns in common.

6. **Bounds** ($t = 1$). Returning to (5.11) and (5.12), we remark that since an exact formula for such sums as

$$\sum_{\zeta_1, \cdots, \zeta_t} \psi(f(\zeta_1, \cdots, \zeta_t)) \tag{6.1}$$

is usually not available, it is natural to look for a bound. We shall consider only the case $t = 1$. Then for the sum

$$T(f) = \sum_{\zeta} f(\zeta),$$

it follows from a theorem of Weil [10] that

$$T(f) = O(q^{1/2}); \tag{6.2}$$

by more elementary methods one can prove the weaker estimate [3]

$$T(f) = O(q^{1-\Theta_k}) \qquad (k = \deg f),$$

where $\Theta_3 = 1/4$, $\Theta_k = 3/2(k+4)$ for $k \geq 4$.

Thus applying (6.2) or (6.3) we obtain asymptotic results for (5.11) and (5.12) with $t = 1$.

7. **Extension of results of § 5.** The results of § 5 can be extended by making use of known results on the number of solutions of

$$(7.1) \qquad Q(U_1, \cdots, U_r) = \alpha$$

in polynomials $U_i \in GF[q, x]$ of degree $< m$; Q has its usual meaning. For simplicity we limit our attention to the case $r = 2s$. Cohen [2, p. 556, Cor. 3] has proved that the number of solutions of (7.1) with $r = 2s$ is

$$(7.2) \qquad \begin{cases} (q^s - \lambda)\, q^{(s-1)(2m-1)} & (\alpha \neq 0) \\ \lambda^m q^{ms} + (q^s - \lambda)\, q^{(s-1)(2m-1)} \sum_{z=0}^{m-1} \lambda^z q^{-z(s-2)} & (\alpha = 0), \end{cases}$$

where $\lambda = \psi((-1)^s \delta)$. Then we have:

THEOREM 12. *The number of solutions of*

$$(7.3) \qquad Q(U_1, \cdots, U_{2s}) = \zeta_1^{k_1} \cdots \zeta_t^{k_t} \qquad (k_1 \geq 1)$$

in polynomials U_i of degree $< m$ is

$$(q^t - (q-1)^t)\left\{\lambda^m q^{ms} + (q^s - \lambda)\, q^{(s-1)(2m-1)} \sum_{z=0}^{m-1} \lambda^z q^{-z(s-2)}\right\}$$
$$+ (q-1)^t (q^s - \lambda)\, q^{(s-1)(2m-1)},$$

where $\lambda = \psi((-1)^s \delta)$.

The proof is like that of Theorem 7.

THEOREM 13. *Let f be a polynomial such that $f(\zeta_1, \cdots, \zeta_t)$ never vanishes. Then the number of solutions of*

$$Q(U_1, \cdots, U_{2s}) = f(\zeta_1, \cdots, \zeta_t)$$

in polynomials U_i *of degree* $< m$ *and* $\zeta_j \in GF(q)$ *is*

$$q^{t+(s-1)(2k-1)}(q^s - \lambda).$$

THEOREM 14. *Let* f *be a polynomial such that* $f(\zeta_1, \cdots, \zeta_t)$ *never vanishes. Then the number of solutions of*

$$Q(U_1, \cdots, U_{2s}) = \eta_1^{k_1} \cdots \eta_t^{k_t} f(\zeta_1, \cdots, \zeta_w) \qquad (k_i \geq 1),$$

with $\deg U_i < m$, *is* q^w *times the number of solutions of* (7.3).

The proof of these theorems is immediate.

Finally we mention problems like (5.13) and (5.15) in which the unknowns are polynomials. Thus for example the number of solutions of

$$Q_1(U_1, \cdots, U_{2s_i}) U_2(V_1, \cdots, V_{2s_2}) = f(\zeta_1, \cdots, \zeta_t),$$

with $\deg U_i < m_i$, $\deg U_2 < m_2$, where f never vanishes, is equal to

$$q^{t+(s_1-1)(2m_1-1)+(s_2-1)(2m_2-1)}(q^{s_1} - \lambda_1)(q^{s_2} - \lambda_2)(q-1),$$

where $\lambda_i = \psi((-1)^{s_i}\delta_i)$, and δ_i is the discriminant of Q_i.

It may also be mentioned that in a problem like (7.3) we may restrict some of the U_i to be primary of degree m; the final formula is similar to that obtained in Theorem 12. The same remark applies to the other theorems of this section.

REFERENCES

1. L. Carlitz, *The singular series for sums of squares of polynomials*, Duke Math. J. 14 (1947), 1105-1120.

2. Eckford Cohen, *Sums of an even number of squares in* $GF[p^n, x]$ II, Duke Math. J. 14 (1947), 545-557.

3. H. Davenport, *On character sums in finite fields*, Acta Math. 71 (1939), 99-121.

4. L. E. Dickson, *Linear groups*, Leipzig, 1901.

5. L. K. Hua and H. S. Vandiver, *Characters over certain types of rings with applications to the theory of equations in a finite field*, Proc. Nat. Acad. Sci., U.S.A. 35 (1949), 94-99.

6. S. H. Min, *On systems of algebraic equations and certain multiple exponential sums*, Quart. J. Math. Oxford Ser. 18 (1947), 133-142.

7. L. J. Mordell, *On a sum analogous to a Gauss's sum,* Quart. J. Math. Oxford Ser. 3 (1932), 161-167.

8. H. Salié, *Über die Kloostermanschen Summen $S(u, v; q)$*, Math. Z. 34 (1932), 91-109.

9. André Weil, *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc. 55 (1949), 497-508.

10. André Weil, *On some exponential sums*, Proc. Nat. Acad. Sci. U.S.A. 34 (1948), 204-207.

DUKE UNIVERSITY