Journal of the Mathematical Society of Japan Vol. 7, No. 3, June, 1955

# The number of solutions of some equations in a finite field.

By L. CARLITZ

(Received Dec. 25, 1953)

**1. Introduction.** The writer [1], [3] has determined the number of solutions of certain types of equations in a finite field. For example, making use of the well-known formulas for the number of solutions of $Q(\xi_1, \cdots, \xi_r)=\alpha$, where $Q$ denotes a quadratic form with coefficients in $GF(q)$, $q$ odd, such equations as

$$Q(\xi_1, \cdots, \xi_r)=\eta_1^{e_1} \cdots \eta_s^{e_s} \tag{1.1}$$

and

$$Q(\xi_1, \cdots, \xi_{2r})=f(\eta_1, \cdots, \eta_s), \tag{1.2}$$

where $f(\eta)$ donotes a polynomial that never vanishes, are readily handled. R. G. Pohrer [6] has found the number of solutions for a great many equations of this and other kinds.[1)]

In the present note we consider a few additional types. In general, when a quadratic form $Q(\xi_1, \cdots, \xi_r)$ occurs in an equation, the case $r$ odd is more difficult; this is illustrated for example by (1.2). However for an equation of the type

$$Q(\xi_1, \cdots, \xi_{2r+1})=g(\eta_1, \cdots, \eta_s), \tag{1.3}$$

it may be possible to find explicit formulas for the number of solutions when the polynomial $g(\eta)$ satisfies certain conditions. A particularly simple case is

$$g(\eta)=\prod_{i=1}^{s}(\eta_i^2+\beta_i\eta_i+\gamma_i); \tag{1.4}$$

1) To find the number of solutions of such simultaneous equations in a finite field is also of interest in connection with the algebraic geometry, as was pointed out by A. Weil: Bull. Amer. Math. Soc. 55 (1949) pp. 497-508.

thus if $q$ is odd and $\beta_i^2-2\gamma_i\neq 0$ for $i=1,\cdots,s$ then the number of solutions of (1.3) is given by

$$q^{2r+s}+(-1)^s q^r \psi((-1)^r\delta), \tag{1.5}$$

where $\delta$ is the discriminant of $Q(\xi)$. In the second place if

$$g(\eta)=\prod_{i=1}^{s}(\eta_i^3+\eta_i), \tag{1.6}$$

we may apply known results on Jacobsthal sums [5] to determine the number of solutions of (1.3). We find that the number is equal to

$$q^{2r+s}+q^r\psi((-1)^r\delta)J^s, \tag{1.7}$$

where $J=\sum_\xi \psi(\xi(\xi^2+1))$ is evaluated by (2.7), (2.8) and (2.9) below.

A somewhat different example is furnished by

$$g(\eta)=\prod_{i=1}^{s}(\eta_i^p-\eta_i+\alpha_i) \qquad (q=p^n). \tag{1.8}$$

For the number of solutions of this equation see Theorem 8. In particular if $n$ is odd and at least one $\alpha_i=0$ the number of solutions of (1.8) is simply $q^{2r+s}$.

In the next place we consider the equation

$$\alpha_1(\eta_1^p-\eta_1)+\cdots+\alpha_r(\eta_r^p-\eta_r)=\alpha, \tag{1.9}$$

and this in turn leads to such equations as

$$Q(\xi)=\alpha_1(\eta_1^p-\eta_1)+\cdots+\alpha_r(\eta_r^p-\eta_r)+\alpha. \tag{1.10}$$

For the results concerning (1.10) and (1.11) see Theorems 9 and 10 below.

Finally (§ 6) we discuss the equation

$$\xi^f=\eta^p-\eta+\alpha \qquad (f\,|\,q-1). \tag{1.11}$$

**2. Some preliminaries.** Let $q=p^n$, $p>2$, and put

$$Q(\xi)=Q(\xi_1,\cdots,\xi_t)=\sum_{i,j=1}^{t}\alpha_{ij}\xi_i\xi_j \quad (\alpha_{ij}\in GF(q)); \tag{2.1}$$

let $\delta=|\alpha_{ij}|$, the discriminant of $Q$. We assume $\delta\neq 0$. Now for $t=2r+1$, it is known that the number of solutions of $Q(\xi)=\alpha$, where

$\alpha \in GF(q)$ is given by

$$N_Q(\alpha)=q^{2r}+q^r\psi((-1)^r\alpha\delta), \tag{2.2}$$

where $\psi(\alpha)=0, +1, -1$ according as $\alpha$ is 0, a square or a nonsquare of $GF(q)$. For $t=2r$ the number of solutions is

$$N_Q(\alpha)=q^{2r-1}+q^{r-1}\psi((-1)^r\delta)k(\alpha), \tag{2.3}$$

where $k(\alpha)=q-1$ or $-1$ according as $\alpha=0$ or $\alpha\neq 0$.

We shall also require some results for the Jacobsthal sums [2, § 6]

$$J(f)=\sum_{\xi\in GF(q)}\psi(f(\xi)), \tag{2.4}$$

where $f(\alpha)$ is a polynomial in $\alpha$. In particular

$$J_2=\sum_{\xi}\psi(\xi^2-\delta)=k(\delta), \tag{2.5}$$

where $k(\delta)$ has the same meaning as in (2.3). Secondly for

$$J_3=J(\beta)=\sum_{\xi}\psi(\xi(\xi^2+\beta)) \tag{2.6}$$

we have $J(\alpha^2\beta)=\psi(\alpha)J(\beta)$. Now

$$J(\beta)=0 \qquad (q\equiv 3 \pmod 4), \tag{2.7}$$

while for $q\equiv 1 \pmod 4$ we have the following result. Let $\gamma$ be a number of $GF(q)$ such that $\psi(\gamma)=-1$. Put $u=\frac{1}{2}J(1)$, $v=\frac{1}{2}J(\gamma)$; then

$$u^2+v^2=q, \qquad u\equiv -1 \pmod 4. \tag{2.8}$$

Moreover

$$2u=J(1)\equiv -\binom{\frac{1}{2}(p-1)}{\frac{1}{4}(p-1)} \pmod p; \tag{2.9}$$

it is clear that $u$ is uniquely determined by (2.8) and (2.9).

Another useful formula is

$$\sum_{\xi}\psi((\xi-\beta_1)\cdots(\xi-\beta_4))=\psi\left(\frac{\beta_1-\beta_3}{\beta_1-\beta_4}\right)\sum_{\xi}\psi(\xi(\xi+1)(\xi+\rho)), \tag{2.10}$$

where

$$\rho=(\beta_1\beta_2, \beta_3\beta_4)=\frac{\beta_1-\beta_3}{\beta_1-\beta_4}\Big/\frac{\beta_2-\beta_3}{\beta_2-\beta_4}, \tag{2.11}$$

the cross ratio of $\beta_1, \beta_2, \beta_3, \beta_4$. In particular if $\rho=-1$, then (2.10) becomes

$$\begin{aligned}\sum_{\xi}\psi((\xi-\beta_1)\cdots(\xi-\beta_4))&=\psi\Big(\frac{\beta_1-\beta_3}{\beta_1-\beta_4}\Big)\sum_{\xi}\psi(\xi(\xi^2-1))\\&=(-1)^{\frac{1}{4}(q-1)}\psi\Big(\frac{\beta_1-\beta_3}{\beta_1-\beta_4}\Big)J(1)\end{aligned} \tag{2.12}$$

provided $q\equiv 1 \pmod 4$; if $q\equiv 3 \pmod 4$, it follows from (2.7) that the sum in the left member of (2.12) vanishes. For additional results on Jacobsthal sums see [7], [8].

In connection with (1.8) and (1.10) we allow a more general setting and consider the equation

$$\xi^q-\xi=\alpha \qquad (\alpha\in GF(q^m)). \tag{2.13}$$

It is familiar that (2.13) is solvable in the $GF(q^m)$ if and only if

$$\alpha+\alpha^q+\cdots+\alpha^{q^{m-1}}=0. \tag{2.14}$$

To apply the condition (2.14) below we define

$$E(\alpha)=\exp\{2\pi i\, t(\alpha)/p\}, \tag{2.15}$$

where

$$t(\alpha)=\sum_{i=0}^{mn-1}\alpha^{p^i}. \tag{2.16}$$

Then we have

$$\sum_{\beta\in GF(q)}E(\beta\alpha)=\begin{cases} q & (\sigma(\alpha)=0)\\ 0 & (\sigma(\alpha)\neq 0),\end{cases} \tag{2.17}$$

where $\sigma(\alpha)$ denotes the left member of (2.14). Thus (2.17) furnishes another criterion for the solvability of (2.13).

We shall also make use of some properties of the Gauss sum

$$G(\alpha)=\sum_{\xi\in GF(q^m)}\psi(\xi)E(\alpha\xi), \tag{2.18}$$

where now $\psi(\xi)=0$, $+1$ or $-1$ according as $\xi=0$, a square or non-square of $GF(q^m)$. We have

$$G(\alpha)=\psi(\alpha)G(1) \tag{2.19}$$

and

$$G^2(1)=\psi(-1)q^m\,. \tag{2.20}$$

For later use we also remark that if $E_1(\alpha)$ denotes the function (2.15) in the case $m=1$, then we have

$$E(\alpha)=E_1(\sigma(\alpha))\,, \tag{2.21}$$

where again $\sigma(\alpha)$ stands for the left member of (2.14). It will also be convenient to define $G_1(\alpha)$ as the sum (2.18) in the case $m=1$. The following formula holds [4]

$$G(1)=(-1)^{m-1}G_1(1)\,. \tag{2.22}$$

**3. Right members with quadratic and cubic factors.** Making use of (2.2) it is evident that the number of solutions of (1.3) is given by

$$\begin{aligned} N&=\sum_{\eta_1,\cdots,\eta_s\in GF(q)}\{q^{2r}+q^r\psi((-1)^r\delta g(\eta_1,\cdots,\eta_s)\}\\ &=q^{2r+s}+q^r\psi((-1)^r\delta)\sum_{\eta_1,\cdots,\eta_s}\psi(g(\eta_1,\cdots,\eta_s))\,. \end{aligned} \tag{3.1}$$

It is therefore necessary to evaluate

$$S_g=\sum_{\eta_1,\cdots,\eta_s}\psi(g(\eta_1,\cdots,\eta_s))\,. \tag{3.2}$$

Now if, changing the notation slightly,

$$g(\eta_1,\cdots,\eta_s,\zeta_1,\cdots,\zeta_t)=g_1(\eta_1,\cdots,\eta_s)g_2(\zeta_1,\cdots,\zeta_t)\,,$$

where $g_1, g_2$ are polynomials with coefficients in $GF(q)$, then (3.2) yields

$$S_g=\sum_{\eta_1,\cdots,\eta_s}\psi(g_1(\eta_1,\cdots,\eta_s)\sum_{\zeta_1,\cdots,\zeta_t}\psi(g_2(\zeta_1,\cdots,\zeta_t))=S_{g_1}S_{g_2}\,. \tag{3.3}$$

In particular assume

$$g(\eta_1,\cdots,\eta_s)=\prod_{k=1}^{s}(a_i\eta_i^2+b_i\eta_i+c_i)\qquad(a_i\neq 0)\,; \tag{3.4}$$

then (3.3) implies

$$S_g=\prod_{k=1}^{s}\psi(a_i(\eta_i^2-\delta_i)) \qquad (\delta_i=b_i^2-4a_ic_i)\,. \tag{3.5}$$

Using (2.5) this becomes

$$S_g=\psi(a_1\cdots a_s)k(\delta_1)\cdots k(\delta_s)\,. \tag{3.6}$$

Substituting from (3.6) in (3.1) and (3.2) we get

THEOREM 1. *The number of solutions $\xi_i$, $\eta_i$ of*

$$Q(\xi_1,\cdots,\xi_{2r+1})=\prod_{i=1}^{s}(\alpha_i\eta_i^2+\beta_i\eta_i+\gamma_i) \qquad (\alpha_i\neq 0)\,, \tag{3.7}$$

*is determined by*

$$N=q^{2r+s}+q^r\psi((-1)^r\delta\alpha_1\cdots\alpha_s)k(\delta_1)\cdots k(\delta_s)\,, \tag{3.8}$$

*where $\delta\neq 0$ is the discriminant of $Q(\xi)$ and $\delta_i=\beta_i^2-4\alpha_i\gamma_i$; the function $k(\alpha)$ has the same meaning as in* (2.3).

If one of the $\alpha_i=0$ the situation is simpler. Indeed it is easily seen that (3.1) implies the following (compare [3, Theorem 11])

THEOREM 2. *The number of solutions of*

$$Q(\xi_1,\cdots,\xi_{2r+1})=\eta f(\zeta_1,\cdots,\zeta_s)\,, \tag{3.9}$$

*where $f(\zeta)$ is an arbitrary polynomial, is equal to $q^{2r+s+1}$.*

While we are here primarily interested in quadratic forms with an odd number of indeterminates, it may be noted that (2.3) implies

THEOREM 3. *The number of solutions of*

$$Q(\xi_1,\cdots,\xi_{2r})=\prod_{i=1}^{s}(\alpha_i\eta_i^2+\beta_i\eta_i+\gamma_i) \qquad (\alpha_i\neq 0) \tag{3.10}$$

*is given by*

$$q^{2r+s-1}+q^{r-1}\psi((-1)^r\delta)((q-1)q^s-qA)\,, \tag{3.11}$$

*where*

$$A=\prod_{i=1}^{s}(q-1-\psi(\delta_i)) \qquad (\delta_i=\beta_i^2-4\alpha_i\gamma_i)\,. \tag{3.12}$$

To prove (3.11) it is only necessary to observe that (3.12) determines the number of times the right member of (3.10) does not vanish.

Turning next to the equation

$$Q(\xi_1,\cdots,\xi_{2r+1})=\prod_{i=1}^{s}(\eta_i^3+\beta_i\eta_i) \tag{3.13}$$

we get at once by means of (3.1) the following result.

THEOREM 4. *The number of solutions of* (3.13) *is furnished by*

$$q^{2r+s}+q^r\psi((-1)^r\delta)\prod_{i=1}^{s}J(\beta_i)\,, \tag{3.14}$$

*where*

$$J(\beta)=\sum_{\xi}\psi(\xi(\xi^2+\beta))\,. \tag{3.15}$$

*The value of* $J(\beta)$ *is determined by* (2.7), (2.8) *and* (2.9).

In particular for $q\equiv 3 \pmod 4$, (2.7) yields

THEOREM 5. *If* $q\equiv 3 \pmod 4$, *the number of solutions of*

$$Q(\xi_1,\cdots,\xi_{2r+1})=(\eta^3+\beta\eta)f(\zeta_1,\cdots,\zeta_s)\,, \tag{3.16}$$

*where* $f(\zeta)$ *is an arbitrary polynomial, is equal to*

$$q^{2r+s+1}. \tag{3.17}$$

Making use of the transformation formulas (2.10) and (2.12) we get

THEOREM 6. *The number of solutions of*

$$Q(\xi_1,\cdots,\xi_{2r+1})=\prod_{i=1}^{s}\prod_{j=1}^{4}(\eta_i-\beta_{ij})\,, \tag{3.18}$$

*where for each* $i$ *the* $\beta_{ij}$ *are distinct, is equal to*

$$q^{2r+s}+q^r\psi((-1)^r\delta)\prod_{i=1}^{s}\psi\left(\frac{\beta_{i1}-\beta_{i3}}{\beta_{i1}-\beta_{i4}}\right)K(\rho_i)\,, \tag{3.19}$$

*where* $\rho_i$ *is the cross ratio of* $\beta_{i1}, \beta_{i2}, \beta_{i3}, \beta_{i4}$ *and*

$$K(\rho)=\sum_{\xi}\psi(\xi(\xi+1)(\xi+\rho))\,. \tag{3.20}$$

*In particular if all* $\rho_i=-1$, *then* (3.19) *becomes*

$$q^{2r+s}+q^r(-1)^{s(q-1)/4}\psi((-1)^s\delta)J^s(1)\prod_{i=1}^{s}\psi\left(\frac{\beta_{i1}-\beta_{i3}}{\beta_{i1}-\beta_{i4}}\right). \tag{3.21}$$

*for* $q\equiv 1 \pmod 4$, *while for* $q\equiv 3 \pmod 4$ *the number of solutions of* (3.18) *is* $q^{2r+s}$.

It is clear how to obtain the number of solutions of the equation

$$Q(\xi_1,\cdots,\xi_{2r+1})=g(\eta_1,\cdots,\eta_s) \tag{3.22}$$

where $g(\eta)$ is a product of quadratics and of cubics and quartics of the type treated above. We shall not take the space to state such results explicitly. It may be remarked that the number of solutions of

$$Q(\xi_1, \cdots, \xi_{2r+1}) = \eta + \frac{\alpha}{\eta} \qquad (\eta \neq 0) \tag{3.23}$$

is evidently

$$q^{2r+1} + q^r \psi((-1)^r \delta) \sum_{\eta \neq 0} \psi\Big(\eta + \frac{\alpha}{\eta}\Big).$$

Since

$$\sum_{\eta \neq 0} \psi\Big(\eta + \frac{\alpha}{\eta}\Big) = \sum_{\eta} \psi(\eta(\eta^2 + \alpha)) = J(\alpha),$$

we see that the number of solutions of (3.23) is

$$q^{2r+1} + q^r \psi((-1)^r \delta) J(\alpha). \tag{3.24}$$

In the same way the number of solutions of

$$Q(\xi_1, \cdots, \xi_{2r+1}) = \prod_{i=1}^{s} \Big(\eta_i + \frac{\alpha_i}{\eta_i}\Big) \qquad (\eta_i \neq 0) \tag{3.25}$$

is readily expressed in terms of $J(\alpha_i)$. Thus the range of (3.22) can be extended. Also by making use of some of the results of [7] and [8], other equations of the type (3.22) can be treated.

The following problem involving sums may be mentioned. The number of solutions of

$$Q(\xi_1, \cdots, \xi_{2r+1}) = \eta^3 + \alpha\eta + \zeta^3 + \alpha\zeta \tag{3.26}$$

is evidently equal to

$$q^{2r+2} + q^r \psi((-1)^r \delta) S, \tag{3.27}$$

where

$$S = \sum_{\eta, \zeta} \psi(\eta^3 + \alpha\eta + \zeta^3 + \alpha\zeta) = \sum_{\tau, \zeta} \psi(\tau(\tau^2 - 3\tau\zeta + 3\zeta^2 + \alpha)).$$

For $p \neq 3$ we put

$$S = \sum_{\tau} \psi(\tau) S_\tau, \qquad S_\tau = \sum_{\zeta} \psi(\tau^2 - 3\tau\zeta + 3\zeta^2 + \alpha).$$

The sum $S_\tau$ is easily evaluated by means of (2.5). We find that

$$S_\tau=\psi(3)k(\tau^2+4\alpha)\,. \tag{3.28}$$

Thus if $\psi(-4\alpha)=-1$ or 0 we get

$$S=-\psi(3)\sum_\tau \psi(\tau)=0\,, \tag{3.29}$$

while if $-4\alpha=\beta^2$ then

$$S=q(\psi(\beta)+\psi(-\beta))\psi(3)=q\psi(3\beta)(1+\psi(-1))\,. \tag{3.30}$$

This proves

THEOREM 7. ($p\neq 3$). *The number of solutions of* (3.26) *is furnished by* (3.27) *together with* (3.29) *and* (3.30).

The equation (3.26) can be generalized in the obvious way by alllowing products in the right member.

**4. Number of solutions of (1.8).** In order to find the number of solutions of (1.8) we first consider the sum

$$T=T(\alpha)=\sum_{\eta\in GF(q^m)}\psi(\eta^q-\eta+\alpha)\qquad(\alpha\in GF(q^m))\,, \tag{4.1}$$

where now $\psi(\alpha)=0$, $+1$ or $-1$ according as $\alpha$ is 0, a square or non-square of $GF(q^m)$.

Making use of (2.15) and (2.17) we get

$$qT=\sum_{\xi\in GF(q^m)}\psi(\xi+\alpha)\sum_{\beta\in GF(q)}E(\beta\xi)\,. \tag{4.2}$$

Replacing $\xi+\alpha$ by $\eta$, (4.2) becomes

$$qT=\sum_{\beta\in GF(q)}E(-\beta\alpha)\sum_{\eta\in GF(q^m)}\psi(\eta)E(\beta\eta)\,. \tag{4.3}$$

Now using (2.18) and (2.19) we see that

$$qT=\sum_{\beta\in GF(q)}E(-\beta\alpha)G(\beta)=G(1)\sum_{\beta\in GF(q)}\psi(\beta)E(-\beta\alpha)\,. \tag{4.4}$$

For $m$ even every number of $GF(q)$ is a square of $GF(q^m)$; thus again using (2.17), (4.4) implies

$$T=q^{-1}G(1)\sum_{\beta\neq 0}E(-\beta\alpha)=q^{-1}G(1)k(\sigma(\alpha))\qquad(m\text{ even})\,. \tag{4.5}$$

On the other hand when $m$ is odd, it follows from (2.21) that

$$\sum_{\beta\in GF(q)}\psi(\beta)E(-\beta\alpha)=\sum_{\beta\in GF(q)}\psi(\beta)E_1(-\beta s(\alpha))=G_1(-\sigma(\alpha))\,,$$

where $G_1(-\sigma(\alpha))$ is the Gauss sum for $GF(q)$. Thus (4.4) yields

$$qT=G(1)G_1(-\sigma(\alpha))=\psi(\sigma(\alpha))G(1)G_1(-1)\,. \tag{4.6}$$

Hence by (2.22) and (2.20), (4.6) becomes

$$T=\psi\big((-1)^{\frac{1}{2}(m-1)}\sigma(\alpha)\big)q^{\frac{1}{2}(m-1)} \qquad (m \text{ odd})\,. \tag{4.7}$$

Thus by means of (4.5) and (4.7) the sum (4.1) is evaluated in all cases (including $\alpha=0$).

Turning now to the equation

$$Q(\xi_1,\cdots,\xi_{2r+1})=\prod_{i=1}^{s}(\eta_i^q-q_i+\alpha_i)\,, \tag{4.8}$$

it is clear that the number of solutions of (4.8) is equal to

$$q^{m(2r+s)}+q^{mr}\psi((-1)^r\delta)\prod_{i=1}^{s}T(\alpha_i)\,, \tag{4.9}$$

where $T(\alpha)$ is defined by (4.1). Now if $m$ is even it is evident that (4.5) implies

$$\prod_{i=1}^{s}T(\alpha_i)=q^{-s}G^s(1)\prod_{i=1}^{s}k(\sigma(\alpha_i))\,. \tag{4.10}$$

For $m$ odd, (4.7) yields

$$\prod_{i=1}^{s}T(\alpha_i)=\psi\Big\{(-1)^{\frac{1}{2}s(m-1)}\prod_{i=1}^{s}\sigma(\alpha_i)\Big\}q^{\frac{1}{2}s(m-1)}\,. \tag{4.11}$$

Combining (4.9), (4.10), (4.11) we get

THEOREM 8. *The number of solutions $\xi_i, \eta_i G\in F(q^m)$ of the equations* (4.8) *is equal to*

$$q^{m(2r+s)}+q^{mr-s}G^s(1)\psi((-1)^r\delta)\prod_{i=1}^{s}k\sigma(\alpha_i) \tag{4.12}$$

*for $m$ even, and to*

$$q^{m(2r+s)}+q^{ml}\psi\{(-1)^l\delta\prod_{i=1}^{s}\sigma(\alpha_i)\} \qquad \Big(l=r+\frac{1}{2}s(m-1)\Big) \tag{4.13}$$

*for $m$ odd.*

**5. Number of solutions of (1.9) and (1.10).** We consider now the equation

$$\alpha_1(\eta_1^q-\eta_1)+\cdots+\alpha_s(\eta_s^q-\eta_s)=\alpha \qquad (m, r\geq 2)\,, \tag{5.1}$$

where $\alpha, \alpha_i, \eta_i\in GF(q^m)$. The case in which the $\alpha_i$ are proportional to

numbers of $GF(q)$ is of little interest and will be excluded. Now when $\eta^q-\eta=\alpha$ is solvable for $\eta$ it has exactly $q$ solutions; hence by (2.17) the number of solutions of (5.1) is equal to

$$q^s \sum_{\alpha_1\zeta_1+\cdots+\alpha_s\zeta_s=\alpha} q^{-s} \sum_{\beta_1,\cdots,\beta_s\in GF(q)} E(\beta_1\zeta_1+\cdots+\beta_s\zeta_s), \tag{5.2}$$

where the outer sum in (5.2) is over $\zeta_i\in GF(q^m)$. We may assume $\alpha_r\neq 0$; then we have

$$\sum_{\alpha_1\zeta_1+\cdots+\alpha_s\zeta_s=\alpha} E(\beta_1\zeta_1+\cdots+\beta_s\zeta_s)=\sum_{\zeta_1,\cdots,\zeta_{s-1}} E\left\{\sum_{i=1}^{s-1}(\beta_i-\alpha_s^{-1}\beta_s\alpha_i)\zeta_i+\alpha_s^{-1}\beta_s\alpha\right\}. \tag{5.3}$$

But in view of the hypothesis that the $\alpha_i$ are not proportional to numbers of $GF(q)$ it is clear from (2.17) that the right member of (5.3) vanishes unless $\beta_1=\cdots=\beta_s=0$, in which case the sum reduces to $q^{m(r-1)}$. Hence (5.2) becomes

$$q^{m(s-1)}. \tag{5.4}$$

This proves the following

THEOREM 9. *If the numbers $\alpha_1,\cdots,\alpha_s\in GF(q^m)$ are not proportional to numbers of $GF(q)$, then the number of solutions $\eta_i\in GF(q^m)$ of the equation* (5.1) *is furnished by* (5.4) *for all $\alpha\in GF(q^m)$.*

We remark that this result does not hold when $r=1$. The equation $\eta^q-\eta=\alpha$ is solvable only when (2.14) holds, in which case there are precisely $q$ solutions. It is also necessary that $m>1$ in (5.1); when $m=1$ it is evident that the equation is solvable only for $\alpha=0$, in which case there are exactly $q^s$ solutions.

Turning next to the equation

$$Q(\xi_1,\cdots,\xi_{2r+1})=\sum_{i=1}^{s}\alpha_i(\eta_i^q-\eta_i)+\alpha \qquad (s\geq 2), \tag{5.5}$$

where $Q$ is of discriminant $\delta\neq 0$, we can determine the number of solutions repidly by means of the last theorem, provided the $\alpha_i$ satisfy the hypothesis of the theorem. For if $\beta$ denotes the right member of (5.5) we consider the equation

$$Q(\xi_1,\cdots,\xi_{2r+1})=\beta. \tag{5.6}$$

By (2.2), (5.6) has

$$q^{2rm}+q^{rm}\psi((-1)^r\beta\delta) \tag{5.7}$$

solutions for fixed $\beta$. But by Theorem 9, for each $\beta$ there are $q^{m(s-1)}$ sets $\eta_1, \cdots, \eta_s$. Consequently it follows from (5.7) that the total number of solutions of (5.5) is given by

$$q^{m(2r+s-1)}+q^{m(r+s-1)}\psi((-1)^r\beta\delta). \tag{5.8}$$

We may state

THEOREM 10. *If the hypothesis of Theorem* 9 *is satisfied and* $Q(\xi)$ *is of discriminant* $\delta\neq 0$ *then the number of solutions* $\xi_i, \eta_i \in GF(q^m)$ *of* (5.5) *is furnished by* (5.8).

The hypothesis $s\geq 2$ is indeed necessary; the case $s=1$ is covered by Theorem 8.

It may be noted that the number of solutions of

$$Q(\xi_1, \cdots, \xi_{2r})=\sum_{i=1}^{s}\alpha_i(\eta_i^q-\eta_i)+\alpha \qquad (s\geq 2), \tag{5.9}$$

subject to the hypothesis of Theorem 10, is given by

$$q^{m(2r-s-2)}. \tag{5.10}$$

The proof of (5.10) is an immediate consequence of (2.3) and Theorem 9. Similarly it is easily seen that the number of solutions of

$$Q(\xi_1, \cdots, \xi_{2r})=\prod_{i=1}^{s}(\eta_i^q-\eta_i+\alpha_i) \tag{5.11}$$

is equal to

$$\begin{cases} q^{ms}\{q^{m(2r-1)}-q^{m(r-1)}\psi((-1)^r\delta\} & (t(\alpha_i)\neq 0,\ i=1, \cdots, s) \\ q^{m(s-l)+l}\{q^{m(2r-1)}+q^{m(r-1)}(q^m-1)\psi((-1)^r\delta) & \text{(otherwise)}, \end{cases} \tag{5.12}$$

where in the latter case $t(\alpha_i)=0$ for precisely $l$ values of $i$. This result may be compared with (4.12).

**6. The equation (1.11).** Let $f\mid q^m-1$ and consider the equation

$$\xi^f=\eta^q-\eta+\alpha. \tag{6.1}$$

We let $\chi(\alpha)$ denote a character of the multiplicative group of $GF(q^m)$ such that $\chi^f=\chi_0$, the principal character. Then as is familiar

$$\sum_{\chi}\chi(\alpha)=\begin{cases} f & (\alpha=\beta^f) \\ 0 & \text{(otherwise)}, \end{cases} \tag{6.2}$$

where the summation is over all $\chi$ such that $\chi^f=\chi_0$ and $\alpha$, $\beta$ denote non-zero numbers of $GF(q^m)$. We shall also require

$$\tau=\tau(\chi)=\sum_{\alpha\in GF(q^m)}\chi(\alpha)E(\alpha), \tag{6.3}$$

where $E(\alpha)$ is defined by (2.15). It is well known that

$$|\tau(\chi)|=q^{\frac{1}{2}m} \quad (\chi\neq\chi_0), \qquad \tau(\chi_0)=-1. \tag{6.4}$$

Moreover if $f\mid q^m-1$ and $m\equiv 1 \pmod f$ and

$$\tau_1(\chi)=\sum_{\alpha\in GF(q)}\chi(\alpha)E_1(\alpha), \tag{6.5}$$

where $E_1(\alpha)$ has the same meaning as in (2.21), then we have [4]

$$\tau(\chi)=(-1)^{m-1}(\tau_1(\chi))^m. \tag{6.6}$$

Using (6.2) it is evident that the number of solutions of (6.1) with $\xi\neq 0$ is

$$N=\sum_{\chi}\sum_{\eta\in GF(q^m)}\chi(\eta^q-\eta+\alpha); \tag{6.7}$$

therefore, by (2.17), (6.7) becomes

$$N=\sum_{\chi}\sum_{\zeta\in GF(q^m)}\sum_{\beta\in GF(q)}\chi(\zeta+\alpha)E(\beta\zeta)=\sum_{\chi}\sum_{\beta}E(-\beta\alpha)\sum_{\zeta}\chi(\zeta)E(\beta\zeta). \tag{6.8}$$

For $\beta=0$ we get

$$\sum_{\chi}\sum_{\zeta}\chi(\zeta)=\sum_{\zeta}\chi_0(\zeta)+\sum_{\chi\neq\chi_0}\sum_{\zeta}\chi(\zeta)=q^m-1;$$

thus substitution in (6.8) yields

$$N=q^m-1+\sum_{\chi}\sum_{\beta}\bar{\chi}(\beta)E(-\beta\alpha)\sum_{\zeta}\chi(\zeta)E(\zeta). \tag{6.9}$$

If $f\mid m$, then $\beta=\gamma^f$, $\gamma\in GF(q^m)$ and therefore $\bar{\chi}(\beta)=1$; thus (6.9) becomes

$$N=q^m-1+\sum_{\beta\neq 0}E(-\beta\alpha)\sum_{\chi}\tau(\chi).$$

Using (2.17) and (6.2) this becomes

$$N=q^m-1+k(\sigma(\alpha))\sum_{\xi\neq 0}E(\xi^f) \qquad (f\mid m), \tag{6.10}$$

where $\sigma(\alpha)=\alpha+\alpha^q+\cdots+\alpha^{q^{m-1}}$ and $k(\xi)$ has the same meaning as in (2.3).

In the next place we note that (6.9) can be written in the form

$$N=q^m-1+\sum_{\chi}\sum_{\beta}\bar{\chi}(\beta)E_1(-\beta\sigma(\alpha))\tau(\chi), \tag{6.11}$$

where we have used (2.21). Thus in particular we get

$$N=q^m-1+\sum_{\chi}\sum_{\beta}\bar{\chi}(\beta)\tau(\chi) \qquad (\sigma(\alpha)=0). \tag{6.12}$$

Now let us suppose that $f\mid q-1$, so that $\beta\in GF(q)$, $\chi(\beta)$ is a multiplicative character of $GF(q)$ that satisfies $\chi^f=\chi_0$. Then (6.12) reduces to

$$N=q^m-q \qquad (\sigma(\alpha)=0). \tag{6.13}$$

When $\sigma(\alpha)\neq 0$, (6.11) becomes

$$N=q^m-1+\sum_{\chi}\chi(-\sigma(\alpha))\tau_1(\bar{\chi})\tau(\chi) \qquad (\sigma(\alpha)\neq 0), \tag{6.14}$$

where $\tau_1(\bar{\chi})$ is defined by (6.5). If we make the additional assumption that $m\equiv 1 \pmod f$ then (6.6) applies and we get

$$N=q^m+(-1)^{m-1}q\sum_{\chi\neq\chi_0}\chi(-\sigma(\alpha))(\tau_1(\chi))^{m-1} \qquad (\sigma(\alpha)\neq 0). \tag{6.15}$$

In particular (6.15) implies

$$|N-q^m|\leq(f-1)q^{\frac{1}{2}(m+1)}. \tag{6.16}$$

We may state

THEOREM 11. *The number of solutions of* (6.1) *with* $\xi\neq 0$ *satisfies* (6.9). *If* $f\mid m$ *then* (6.10) *holds. If* $f\mid q-1$ *and* $\sigma(\alpha)=0$ *then* (6.13) *holds. If* $\sigma(\alpha)\neq 0$ *and* $q\equiv m\equiv 1 \pmod f$ *then* (6.15) *and* (6.16) *hold. There are* $q$ *additional solutions with* $\xi=0$ *only when* $\sigma(\alpha)=0$.

Duke University

## References

[1] L. Carlitz, The number of solutions of some special equations in a finite field, Pacific Journal of Mathematics, vol. 4 (1954), pp. 207-217

[2] L. Carlitz, Pairs of quadratic equations in a finite field, American Journal of Mathematics, vol. 76 (1954), pp. 137-154.

[3] L. Carlitz, Some special equations in a finite field, Pacific Journal of Mathemtics, vol. 3 (1953), pp. 13-24.
[4] H. Davenport and H. Hasse, Die Nullstellen der Kongruenzzetafunktionen in gewißen zyklischen Fällen, Journal für die reine und angewandte Mathematik, vol. 172 (1935), pp. 151-182.
[5] E. Jacobsthal, Über die Darstellung der Primzahlen der Form $4n+1$ als Summe zweier Quadrate, Journal für die reine und angewandte Mathematik, vol. 132 (1907). pp. 238-245.
[6] R. G. Pohrer, On the solution of equations in a finite field, not yet published.
[7] A. L. Whiteman. Cyclotomy and Jacobsthal sums, American Journal of Mathematics, vol. 74 (1952), pp. 89-99.
[8] A. L. Whiteman, Theorems analogous to Jacobsthal's theorem, Duke Mathematical Journal, vol. 16 (1949), pp. 619-626.