SIMULTANEOUS PAIRS OF LINEAR AND QUADRATIC EQUATIONS IN A GALOIS FIELD

ECKFORD COHEN

1. Introduction. Let F denote the Galois field $GF(p^r)$ with p^r elements, where p is an *odd* prime and r is a positive integer. Suppose further that m and n are arbitrary elements of F and that α_i, β_i $(i = 1, \ldots, s)$ are *nonzero* elements of F. The purpose of this paper is to evaluate the function $N_s(m, n)$, defined, for an arbitrary positive integer s, to be the number of simultaneous solutions in F of the equations

$$\begin{cases} m = \alpha_1 x_1^2 + \ldots + \alpha_s x_s^2, \\ n = \beta_1 x_1 + \ldots + \beta_s x_s. \end{cases} \tag{1.1}$$

Explicit formulas for $N_s(m, n)$ are obtained in Theorem 1, and on the basis of this theorem, it is easy to establish the solvability criterion contained in Theorem 2. It follows from the latter criterion that the least value of s for which (1.1) is always solvable is the value $s = 4$. We mention that Theorem 1, in the special case $r = 1$ (that is, in the case of rational congruences (mod p)), reduces to a result of O'Connor and Pall **(3; 4)** proved by a different method.

It is of interest to compare Dickson's formulas **(2, §§64-67)** for the number of solutions $N_s(m)$ of the first equation in (1.1) alone, with the results for $N_s(m, n)$ obtained in this paper. As it might be expected, the results for the simultaneous problem are somewhat more involved. A significant difference between the results for the two problems arises from the fact that $N_s(m) > 0$ for all $s \geqslant 2$.

In this paper we use a direct method based on the trigonometric expansion of $N_s(m, n)$. The most that will be required is a double application of the generalized Cauchy-Gauss sum, (1.7) and (1.11) below.

Next we introduce some notation that will be needed in §2 and §3. Let $t(a)$ denote the trace of an element a in F,

$$t(a) = a + a^p + \ldots + a^{p^{r-1}}.$$

Then we place

$$e(a) = e^{2\pi i t(a)/p}, \tag{1.2}$$

from which it follows that $e(a + b) = e(a)\, e(b)$. The symbol $\sum_x$ will be used to indicate a sum over the totality of elements of F, while $\sum_{x \neq 0}$ will denote a sum over the nonzero elements of F. One will note the property,

$$\xi(a) = \sum_x e(ax) = \begin{cases} p^r, & a = 0, \\ 0, & a \neq 0, \end{cases} \tag{1.3}$$

Received June 4, 1956.

which may be restated in the form,

$$c(a) = \sum_{x \neq 0} e(ax) = \begin{cases} p^r - 1, & a = 0, \\ -1, & a \neq 0. \end{cases} \tag{1.4}$$

The symbol $\psi(a)$ will be used to denote the Legendre symbol in F, that is, $\psi(a) = 1, -1$, or 0 according as a is a nonzero square, a non-square, or is zero in F. We denote the quadratic Gauss sums in F by

$$G(a) = \sum_{x} e(ax^2), \tag{1.5}$$

$$G^*(a) = \sum_{x \neq 0} \psi(x)\, e(ax). \tag{1.6}$$

The less familiar Cauchy-Gauss sum is defined for F by

$$S(a, b) = \sum_{x} e(ax^2 + 2bx). \tag{1.7}$$

We mention the following well-known properties of $G(a)$ and $G^*(a)$:

$$G(a) = \psi(a)\, G(1), \qquad a \neq 0, \tag{1.8}$$

$$G^2(1) = \psi(-1)\, p^r, \tag{1.9}$$

$$G^*(a) = \begin{cases} G(a), & a \neq 0, \\ 0, & a = 0. \end{cases} \tag{1.10}$$

The sum $S(a, b)$ has the reduction property **(1, §6)**,

$$S(a, b) = \begin{cases} e(-b^2/a)\, G(a), & a \neq 0, \\ p^r, & a = b = 0, \\ 0, & a = 0, b \neq 0. \end{cases} \tag{1.11}$$

2. The evaluation of $N_s(m, n)$. We shall need the following additional notation,

$$\alpha = \alpha_1 \ldots \alpha_s, \tag{2.1}$$

$$\beta = \frac{\beta_1^{\,2}}{\alpha_1} + \ldots + \frac{\beta_s^{\,2}}{\alpha_s}, \tag{2.2}$$

$$\gamma = n^2 - \beta m. \tag{2.3}$$

The results of this section can be stated most conveniently in terms of the five following cases arising from conditions satisfied by m, n, β, and γ.

Case I: $\beta = 0,\ n \neq 0,$

Case II: $\beta = n = 0,\quad m \neq 0,$

Case III: $\beta = m = n = 0,$

Case IV: $\beta \neq 0,\quad \gamma \neq 0,$

Case V: $\beta \neq 0,\quad \gamma = 0.$

We now prove

THEOREM 1. *The number of solutions $N_s(m, n)$ of (1.1) is given by*

https://doi.org/10.4153/CJM-1957-011-2 Published online by Cambridge University Press

$$(2.4)\quad N_s(m,n) = \begin{cases} p^{r(4k-2)} + p^{r(2k-1)}\,\psi(\alpha)\,\zeta, & s = 4k, \\ p^{r(4k-1)} + p^{r(2k-1)}\,\psi(\alpha)\,\eta, & s = 4k+1, \\ p^{4kr} + p^{2kr}\,\psi(-\alpha)\,\zeta, & s = 4k+2, \\ p^{r(4k+1)} + p^{2kr}\,\psi(-\alpha)\,\eta, & s = 4k+3, \end{cases}$$

where η *and* ζ *are defined by* $\eta = 0$, $\zeta = 0$ *in Case* I; $\eta = p^r\psi(m)$, $\zeta = -1$ *in Case* II; $\eta = 0$, $\zeta = p^r - 1$ *in Case* III; $\eta = -\psi(\beta)$, $\zeta = \psi(\gamma)$ *in Case* IV; $\eta = (p^r - 1)\,\psi(\beta)$, $\zeta = 0$ *in Case* V.

Remark. It is to be understood that $N_s(m,n)$ is undefined for any cases that may be incompatible.

Proof. The function $N_s(m,n)$ has the double Fourier expansion **(5)**,

$$(2.5)\quad N_s(m,n) = p^{-2r}\sum_u \sum_v A(u,v)\,e(-mu)\,e(-2nv),$$

$$A(u,v) = \sum_{x_1,\ldots,x_s} e\Big(u(\alpha_1 x_1^{\,2} + \ldots + \alpha_s x_s^{\,2})\Big)\,e\Big(2v(\beta_1 x_1 + \ldots + \beta_s x_s)\Big).$$

We break up this expansion into two parts according as $u = 0$ or $u \neq 0$, to get

$$(2.6)\qquad N_s(m,n) = \sum_1 + \sum_2,$$

where

$$(2.7)\qquad \sum_1 = p^{-2r}\sum_v e(-2nv)\prod_{i=1}^{s}\xi(2\beta_i v),$$

$$(2.8)\qquad \sum_2 = p^{-2r}\sum_{u\neq 0}\sum_v e(-mu)\,e(-2nv)\prod_{i=1}^{s} S(\alpha_i u, \beta_i v).$$

By (1.3) we have immediately

$$(2.9)\qquad \sum_1 = p^{r(s-2)}.$$

Now by (1.8) and (1.11) one obtains for $u \neq 0$,

$$S(\alpha_i u, \beta_i v) = e\left(\frac{-\beta_i^{\,2} v^2}{\alpha_i u}\right)\psi(\alpha_i u)\,G(1),$$

so that (2.8) becomes, using the definition of β,

$$(2.10)\qquad \sum_2 = G^s(1)\,p^{-2r}\,\psi(\alpha)\sum_{u\neq 0}\psi^s(u)\,e(-mu)\,S(-\beta/u, -n).$$

If $u \neq 0$, we have, again by (1.8) and (1.11),

$$(2.11)\qquad S(-\beta/u, -n) = \begin{cases} e(n^2u/\beta)\,\psi(-\beta u)\,G(1), & \beta \neq 0, \\ p^r, & \beta = n = 0, \\ 0, & \beta = 0,\ n \neq 0. \end{cases}$$

We now evaluate $\sum_2$ in the separate cases arising from (2.11). It follows immediately from (2.10) that

$$(2.12)\qquad \sum_2 = 0, \qquad \beta = 0,\ n \neq 0.$$

https://doi.org/10.4153/CJM-1957-011-2 Published online by Cambridge University Press

In case $\beta = n = 0$, we obtain from (2.10) and (2.11),

$$\sum_2 = \begin{cases} G^s(1)\, p^{-r}\, \psi(\alpha)\, c(-m), & \beta = n = 0,\ s \text{ even}, \\ G^s(1)\, p^{-r}\, \psi(\alpha)\, G^*(-m), & \beta = n = 0,\ s \text{ odd}. \end{cases} \tag{2.13}$$

Applying (1.4), (1.9), and (1.10) to (2.13), it follows, in case s is even, that

$$\sum_2 = \begin{cases} -\psi\left((-1)^{\frac{1}{2}s}\alpha\right) p^{\frac{1}{2}r(s-2)}, & \beta = n = 0,\ m \neq 0,\ s \text{ even}, \\ \psi\left((-1)^{\frac{1}{2}s}\alpha\right) p^{\frac{1}{2}r(s-2)}(p^r - 1), & \beta = m = n = 0,\ s \text{ even}, \end{cases} \tag{2.14}$$

and in case s is odd,

$$\sum_2 = \begin{cases} \psi\left((-1)^{\frac{1}{2}(s+3)}\alpha m\right) p^{\frac{1}{2}r(s-1)}, & \beta = n = 0,\ m \neq 0,\ s \text{ odd}, \\ 0, & \beta = m = n = 0,\ s \text{ odd}. \end{cases} \tag{2.15}$$

In case $\beta \neq 0$, it follows from (2.10) and (2.11) that

$$\sum_2 = \begin{cases} G^{s+1}(1)\, p^{-2r}\, \psi(-\alpha\beta)\, G^*(\gamma/\beta), & \beta \neq 0,\ s \text{ even}, \\ G^{s+1}(1)\, p^{-2r}\, \psi(-\alpha\beta)\, c(\gamma/\beta), & \beta \neq 0,\ s \text{ odd}. \end{cases} \tag{2.16}$$

Applying (1.4), (1.9), and (1.10) to (2.16), we obtain, in case s is even,

$$\sum_2 = \begin{cases} \psi\left((-1)^{\frac{1}{2}(s+4)}\alpha\gamma\right) p^{\frac{1}{2}r(s-2)}, & \beta \neq 0,\ \gamma \neq 0,\ s \text{ even}, \\ 0, & \beta \neq 0,\ \gamma = 0,\ s \text{ even}, \end{cases} \tag{2.17}$$

and in case s is odd,

$$\sum_2 = \begin{cases} -\psi\left((-1)^{\frac{1}{2}(s+3)}\alpha\beta\right) p^{\frac{1}{2}r(s-3)}, & \beta \neq 0,\ \gamma \neq 0,\ s \text{ odd}, \\ \psi\left((-1)^{\frac{1}{2}(s+3)}\alpha\beta\right) p^{\frac{1}{2}r(s-3)}\,(p^r - 1), & \beta \neq 0,\ \gamma = 0,\ s \text{ odd}. \end{cases} \tag{2.18}$$

Combining (2.6), (2.9), (2.12), (2.14), (2.15), (2.17), and (2.18) the theorem follows.

3. Solvability criterion. We now apply Theorem 1 to the cases $s \leqslant 4$ to obtain the following explicit results.

$$N_1(m, n) = \begin{cases} 1, & \text{Case V}, \\ 0, & \text{Case IV}; \end{cases} \tag{3.1}$$

$$N_2(m, n) = \begin{cases} 1, & \text{Cases I, V}, \\ 0, & \text{Case II}, \\ p^r, & \text{Case III}, \\ 1 + \psi(-\alpha\gamma), & \text{Case IV}; \end{cases} \tag{3.2}$$

https://doi.org/10.4153/CJM-1957-011-2 Published online by Cambridge University Press

$$N_3(m, n) = \begin{cases} p^r, & \text{Cases I, III,} \\ p^r + p^r\psi(-\alpha m), & \text{Case II,} \\ p^r - \psi(-\alpha\beta), & \text{Case IV,} \\ p^r + (p^r - 1)\,\psi(-\alpha\beta), & \text{Case V;} \end{cases} \tag{3.3}$$

$$N_4(m, n) = \begin{cases} p^{2r}, & \text{Cases I, V,} \\ p^{2r} - p^r\,\psi(\alpha), & \text{Case II,} \\ p^{2r} + p^r(p^r - 1)\,\psi(\alpha), & \text{Case III,} \\ p^{2r} + p^r\,\psi(\alpha\gamma), & \text{Case IV.} \end{cases} \tag{3.4}$$

It is noted that Cases I, II, and III do not arise if $s = 1$ or if $s = 2$ and $\psi(-\alpha) = -1$.

On the basis of (3.1), (3.2), (3.3), and (3.4) we obtain immediately the following solvability criterion.

THEOREM 2. *Subject to the restrictions stated in the Introduction,* (1.1) *is always solvable* ($N_s(m, n) > 0$) *provided* $s \geqslant 4$. *The only cases in which* (1.1) *is insolvable, that is when* $N_s(m, n) = 0$, *are the following:*

(1) $s = 1, \quad \gamma \neq 0,$
(2) $s = 2, \quad \beta \neq 0, \quad \gamma \neq 0, \quad \psi(-\alpha\gamma) = -1,$
(3) $s = 2, \quad \beta = n = 0, \quad m \neq 0,$
(4) $s = 3, \quad \beta = n = 0, \quad m \neq 0, \quad \psi(-\alpha m) = -1,$

where α, β, *and* γ *are defined as in* §2.

REFERENCES

1. Leonard Carlitz, *Weighted quadratic partitions over a finite field*, Can. J. Math., *5* (1953), 317–323.
2. L. E. Dickson, *Linear Groups* (Leipzig, 1901).
3. R. E. O'Connor, *Quadratic and linear congruence*, Bull. Amer. Math. Soc., *45* (1939), 792–798.
4. R. E. O'Connor and Gordon Pall, *The quaternion congruence* $\bar{t}at \equiv b \pmod{g}$, Amer. J. Math., *61* (1939), 487–508.
5. A. L. Whiteman, *Finite Fourier series and equations in finite fields*, Trans. Amer. Math. Soc., *54* (1953), 78–98.

University of Tennessee