CHAPTER IV

THE NUMBER OF SOLUTIONS OF A SYSTEM OF LINEAR AND QUADRATIC EQUATIONS OVER A FINITE FIELD

Let F denote a finite field of order q and characteristic p, and let a, b, a_i, b_i $(1 \leqslant i \leqslant t)$ denote elements of F such that $a_1 \cdots a_t \neq 0$ and such that exactly s of the elements b_i are $\neq 0$ where $1 \leqslant s \leqslant t$. In this chapter, we determine the number $N_{s,t}(a,b)$ of solutions in F of the system of equations,

$$(4\text{-}1) \qquad \begin{cases} a = a_1x_1^2 + \cdots + a_tx_t^2 \\ b = b_1x_1 + \cdots + b_tx_t \, . \end{cases}$$

The method of evaluating $N_{s,t}(a,b)$ is based upon an elementary application of exponential sums.

We introduce some notations and list some known results that are needed in the sequel. For an element a of F, let t(a) denote the <u>trace of a</u>, that is,

$$t(a) = a + a^p + \cdots + a^{p^{r-1}}, \qquad q = p^r,$$

and define

$$e(a) = \exp(2\pi i t(a)/p).$$

It follows at once that

$$(4\text{-}2) \qquad e(a+b) = e(a)e(b) \qquad \text{for some } a,\ b \in F.$$

In particular $e(0) = 1$. For arbitrary a, b, in F put

$$(4\text{-}3) \qquad S(a,b) = \sum_{x \in F} e(ax^2 + 2bx),$$

and let $\qquad G(a) = S(a,0)$.

4.1 Lemma. For $a, b \in F$,

$$(4\text{-}4) \qquad S(a,b) = \begin{cases} e(-b^2/a)G(a) & \text{if } a \neq 0 \neq b, \\ q & \text{if } a = 0 = b, \\ 0 & \text{if } a = 0 \neq b. \end{cases}$$

Proof. For $a = 0 = b$, the second of (4-4) is obvious. Assume $a \neq 0 \neq b$. We have

$$\begin{aligned} S(a,b) &= \sum_{x \in F} e(ax^2 + 2bx) \\ &= \sum_{x \in F} e(a(x^2 + \frac{2bx}{a} + \frac{b^2}{a^2} - \frac{b^2}{a^2})) \\ &= \sum_{x \in F} e(a(x + \frac{b}{a})^2)\, e(-\frac{b^2}{a}) \\ &= e(-\frac{b^2}{a}) \sum_{x \in F} e(a(x + \frac{b}{a})^2) \\ &= e(-b^2/a)\, G(a). \end{aligned}$$

Finally, we assume that $a = 0 \neq b$. Then there exists an element d in F such that $t(2bd) \neq 0$; for example we may take $d = 1/2b$, so that $t(2bd) = t(1) = r$. Hence for such d it is evident that $e(2bd) \neq 1$. Now by (4-2) we have

$$e(2bd) \sum_{x \in F} e(2bx) = \sum_{x \in F} e(2b(x+d)) = \sum_{x \in F} e(2bx),$$

or $$(e(2bd)-1) \sum_{x \in F} e(2bx) = 0.$$

Since $e(2bd) \neq 1$, $\sum_{x \in F}' e(2bx) = 0$. Hence by the definition (4-3), the third of (4-4) is proved.

4.2 Lemma. Let a be a non-zero element in F. Then

$$(4\text{-}5) \qquad G(a) = \Psi(a)\, G(1),$$

where $\Psi(a)$ denotes the Legendre symbol in F, that is, $\Psi(a) = +1, -1$ or 0 according as a is a square, a non-square or zero in F.

Proof. From (4-3), we get

$$G(a) = \sum_{x \in F} e(ax^2).$$

The sum

$$T_a = \sum_{x \in F}' \Psi(x) e(2ax) = \sum_{x_1} e(2ax_1) - \sum_{x_2} e(2ax_2),$$

where x_1 runs through the squares $\neq 0$ of F and x_2 runs through the non-squares. On the other hand, for $a \neq 0$, the third of (4-4) implies

$$1 + \sum_{x_1} e(2ax_1) + \sum_{x_2} e(2ax_2) = 0,$$

so that

$$T_a = 1 + 2\sum_{x_1} e(2ax_1) = G(a) ;$$

hence T_a and $G(a)$ are identical for $a \neq 0$.

In the next place if $a = d^2$, $d \neq 0$, then we have

$$T_a = \sum_{x \in F} \Psi(x) e(2d^2x) = \sum_{x_1} e(2d^2x_1) - \sum_{x_2} e(2d^2x_2),$$

and

$$T_1 = \sum_{x \in F} \Psi(x)e(2x) = \sum_{x_1} e(2x_1) - \sum_{x_2} e(2x_2).$$

Thus we get $T_a = T_1$. If a is a non-square, then

$$T_a = \sum_{x \in F} \Psi(x)e(2ax) = \sum_{x_1} e(2ax_1) - \sum_{x_2} e(2ax_2),$$

where ax_1 is a non-square in F and ax_2 is a square in F. Hence we have $T_a = -T_1$. Now we have proved that $T_a = \Psi(a)T_1$. Since $T_a = G(a)$ and $T_1 = G(1)$, the lemma is now proved.

4.3 Theorem. Let $N_{s,t}(a,b)$ be the number of solutions in F of the system (4-1). Then for all $t \geqslant 1$,

$$N_{s,t}(a,b) = q^{-2} \sum_{u \in F} \sum_{v \in F} K(u,v)e(-au)e(-2bv), \tag{4-6}$$

where

$$K(u,v) = \sum_{\substack{x_i \in F \\ i=1,\dots,t}} e(u(a_1x_1^2 + \dots + a_tx_t^2))e(2v(b_1x_1 + \dots + b_tx_t)).$$

Proof. Consider the sum

$$\sum_{u \in F} \sum_{v \in F} \sum_{\substack{x_i \in F \\ i=1,\dots t}} e(u(a_1x_1^2 + \dots + a_tx_t^2))e(2v(b_1x_1 + \dots + b_tx_t))e(-au)e(-2bv).$$

For fixed point $(x_1, \dots, x_t) \in F^t$ where $F^t = F \times F \times \dots \times F$ (t times), we have

$$\sum_{u \in F} \sum_{v \in F} e(u(a_1x_1^2 + \dots + a_tx_t^2))e(2v(b_1x_1 + \dots + b_tx_t))e(-au)e(-2bv)$$

$$= \sum_{u \in F} \sum_{v \in F} e(u(a_1x_1^2 + \dots + a_tx_t^2 - a))e(2v(b_1x_1 + \dots + b_tx_t - b))$$

$$= \sum_{u \in F} e(u(a_1x_1^2+\dots+ a_tx_t^2- a)) \sum_{v \in F} e(2v(b_1x_1+\dots+ b_tx_t- b)).$$

Let $C = \sum_{u \in F} e(u(a_1x_1^2+\dots+ a_tx_t^2- a))$ and $D = \sum_{v \in F} e(2v(b_1x_1+\dots+ b_tx_t- b))$.

Then by Lemma 4.1, we have

$$C = \begin{cases} q & \text{if } (a_1x_1^2+\dots+ a_tx_t^2- a) = 0, \\ 0 & \text{if } (a_1x_1^2+\dots+ a_tx_t^2- a) \neq 0; \end{cases}$$

$$D = \begin{cases} q & \text{if } (b_1x_1+\dots+ b_tx_t- b) = 0, \\ 0 & \text{if } (b_1x_1+\dots+ b_tx_t- b) \neq 0. \end{cases}$$

We see that the product of C and D is q^2 if $(x_1,\dots, x_t)$ is a solution of the system (4-1). Otherwise it is zero. So we have

$$\sum_{\substack{x_i \in F \\ i=1,\dots,t}} CD = q^2 N_{s,t}(a,b).$$

Hence $N_{s,t}(a,b) = q^{-2} \sum_{u \in F} \sum_{v \in F} K(u,v)e(-au)e(-2bv),$

where

$$K(u,v) = \sum_{\substack{x_i \in F \\ i=1,\dots,t}} e(u(a_1x_1^2+\dots+ a_tx_t^2))e(2v(b_1x_1+\dots+ b_tx_t)).$$

4.4 <u>Theorem.</u> If $1 \leq s \leq t$, then for all $t \geq 1$,

$$(4\text{-}7) \qquad N_{s,t}(a,b) = q^{-2}\left\{q^t+ G^t(1)\Psi(A) \sum_{u \in F^*} \Psi^t(u)e(-au)S(-\tfrac{B}{u},-b)\right\},$$

where

$$(4\text{-}8) \qquad A = a_1\dots a_t \in F^* \quad \text{and} \quad B = \frac{b_1^2}{a_1}+\dots+ \frac{b_t^2}{a_t}.$$

Proof. There is no loss of generality in supposing $b_1, \ldots, b_s$ to be in F^* and $b_i = 0$ $(s < i \leq t)$. By Theorem 4.3, we have

$$N_{s,t}(a,b) = q^{-2} \sum_{u \in F} \sum_{v \in F} K(u,v) e(-au) e(-2bv),$$

where

$$K(u,v) = \sum_{\substack{x_i \in F \\ i=1,\ldots,t}} e(u(a_1x_1^2 + \ldots + a_tx_t^2)) e(2v(b_1x_1 + \ldots + b_tx_t)).$$

We write

$$N_{s,t}(a,b) = \sum_1 + \sum_2, \tag{4-9}$$

where $\sum_1$ consists of those terms in the expansion (4-6) for which $u = 0$ and $\sum_2$ those for which $u \neq 0$. We have

$$\begin{aligned} K(0,v) &= \sum_{\substack{x_i \in F \\ i=1,\ldots,t}} e(2v(b_1x_1 + \ldots + b_tx_t)) \\ &= \sum_{\substack{x_i \in F \\ i=1,\ldots,t}} \prod_{i=1}^{t} e(2vb_ix_i) \\ &= \prod_{i=1}^{t} \sum_{\substack{x_i \in F \\ i=1,\ldots,t}} e(2vb_ix_i) \\ &= \left[\prod_{i=1}^{s} S(0,b_iv) \right] \cdot q^{t-s} . \end{aligned}$$

Consequently, by Lemma 4.1, $K(0,v) = 0$ if $v \neq 0$ and q^t if $v = 0$; hence

$$\sum_1 = q^{t-2} . \tag{4-10}$$

Now we want to find the value of $\sum_2$ but we must first prove that $K(u,v) = \prod_{i=1}^{s} S(a_iu,b_iv) \prod_{i=s+1}^{t} G(a_iu)$. By using the formula (4-2), we can rewrite $K(u,v)$ to be

$$\begin{aligned}
K(u,v) &= \sum_{\substack{x_i \in F \\ i=1,\dots,t}} \prod_{i=1}^{t} e(ua_ix_i^2 + 2vb_ix_i) \\
&= \prod_{i=1}^{t} \sum_{\substack{x_i \in F \\ i=1,\dots,t}} e(a_iux_i^2 + 2b_ivx_i) \\
&= \prod_{i=1}^{t} S(a_iu,b_iv) \\
&= \prod_{i=1}^{s} S(a_iu,b_iv) \prod_{i=s+1}^{t} S(a_iu,0) \\
&= \prod_{i=1}^{s} S(a_iu,b_iv) \prod_{i=s+1}^{t} G(a_iu).
\end{aligned}$$

It follows that

$$\sum_2 = q^{-2} \sum_{\substack{u \in F^* \\ v \in F}} e(-(au+2bv)) \prod_{i=1}^{s} S(a_iu,b_iv) \prod_{i=s+1}^{t} G(a_iu).$$

By using (4-4) and (4-5), we have

$$\sum_2 = q^{-2} \sum_{\substack{u \in F^* \\ v \in F}} e(-(au+2bv)) \left(G^s(1)\Psi^s(u)\Psi(A_1)e(-v^2B/u)\right) \cdot \left(G^{t-s}(1)\Psi^{t-s}(u)\Psi(A_2)\right),$$

where $A_1 = a_1 \cdots a_s$, $A_2 = a_{s+1} \cdots a_t$ and $B = \frac{b_1^2}{a_1} + \cdots + \frac{b_t^2}{a_t}$. Let $A = A_1 A_2$.

Then we have, since $\Psi(A_1)\Psi(A_2) = \Psi(A_1 A_2) = \Psi(A)$,

$$(4\text{-}11) \qquad \sum_2 = q^{-2} G^t(1) \Psi(A) \sum_{u \in F^*} \Psi^t(u) e(-au)\, S(-\tfrac{B}{u}, -b) ,$$

and the theorem follows on combining (4-9), (4-10) and (4-11).

4.5 Corrollary. The value of $N_{s,t}(a,b)$ is independent of the value of s, subject to the condition, $1 \leqslant s \leqslant t$; more precisely, the value of $N_{s,t}(a,b)$ is not changed if the b_i in (4-1) are replaced by any set of t elements of F, not all zero, such that the value of B is left invariant.

In addition to Corollary 4.5, we shall need the following well-known result for the number of representations $N_t(a)$ of an element a of F in the form,

$$(4\text{-}12) \qquad a_1 x_1^2 + \cdots + a_t x_t^2 = a , \qquad A = a_1 \cdots a_t \neq 0,$$

for fixed elements $a_1, \ldots, a_t$ of F.

We combine the results in Theorem 3.6 and 3.7 to obtain the following theorem.

4.6 Theorem. Let $t = 2k$ or $2k+1$ according as t is even or odd.

(i) For $a \neq 0$,

$$(4\text{-}13) \qquad N_t(a) = \begin{cases} q^{t-1} - q^{k-1}\Psi((-1)^k A) & \text{if } t = 2k, \\ q^{t-1} + q^k \Psi((-1)^k a A) & \text{if } t = 2k+1 ; \end{cases}$$

(ii) if $a = 0$,

$$(4\text{-}14) \qquad N_t(a) = \begin{cases} q^{t-1} + q^{k-1}(q-1)\Psi((-1)^k A) & \text{if } t = 2k, \\ q^{t-1} & \text{if } t = 2k+1. \end{cases}$$

We are now ready to prove our main result.

4.7 <u>Theorem</u>. (E.Cohen [3, Theorem 2]). Let $N_{s,t}(a,b)$, s, A and B be defined as in Theorem 4.4 and let $D = b^2 - aB$. Then we have :

(i) In case $B \neq 0$, $D = 0$,

$$(4\text{-}15) \qquad N_{s,t}(a,b) = \begin{cases} q^{t-2} + q^{k-1}(q-1)\Psi((-1)^k AB) & \text{if } t = 2k+1, \\ q^{t-2} & \text{if } t = 2k\ ; \end{cases}$$

(ii) in case $B \neq 0$, $D \neq 0$,

$$(4\text{-}16) \qquad N_{s,t}(a,b) = \begin{cases} q^{t-2} - q^{k-1}\Psi((-1)^k AB) & \text{if } t = 2k+1, \\ q^{t-2} + q^{k-1}\Psi((-1)^k AD) & \text{if } t = 2k\ ; \end{cases}$$

(iii) in case $B = 0$, $D = 0$, $a = 0$,

$$(4\text{-}17) \qquad N_{s,t}(a,b) = \begin{cases} q^{t-2} + q^{k-1}(q-1)\Psi((-1)^k A) & \text{if } t = 2k, \\ q^{t-2} & \text{if } t = 2k+1\ ; \end{cases}$$

(iv) in case $B = 0$, $D = 0$, $a \neq 0$,

$$(4\text{-}18) \qquad N_{s,t}(a,b) = \begin{cases} q^{t-2} - q^{k-1}\Psi((-1)^k A) & \text{if } t = 2k, \\ q^{t-2} + q^{k}\Psi((-1)^k aA) & \text{if } t = 2k+1\ ; \end{cases}$$

(v) in case $B = 0$, $D \neq 0$, $N_{s,t}(a,b) = q^{t-2}$.

Proof. We divide the proof into four parts, corresponding to special cases arising from the application of the Corollary 4.5.

Part 1. Suppose $B \neq 0$ and that at least one a_i is such that Ba_i is a square ; without loss of generality suppose that Ba_1 is a non-zero square of F. By Corollary 4.5, $N_{s,t}(a,b)$ is in this case equal to the number of solutions of

$$(4\text{-}19) \qquad \begin{cases} a = a_1x_1^2+\dots+ a_tx_t^2 , \\ b = B_1x_1, \end{cases}$$

where B_1 is determined so that $B = B_1^2/ a_1$. We eliminate x_1 between the equations of (4-19), then we have

$$a = a_1\frac{b^2}{B_1^2} + a_2x_2^2+\dots+ a_tx_t^2 ,$$

or equivalently,

$$a - \frac{b^2}{B} = a_2x_2^2+\dots+ a_tx_t^2 .$$

That is

$$(4\text{-}20) \qquad -\frac{D}{B} = a_2x_2^2+\dots+ a_tx_t^2 \qquad (t \geqslant 2).$$

The number of solutions of (4-19) is the same as that of (4-20). Applying Theorem 4.6 with t replaced by t-1, a by $-D/B$, and A by $a_2\dots a_t$ (let we place $A' = a_2\dots a_t$), and using the fact that $\Psi(a_1B) = 1$, we have for $D = 0$,

$$(4\text{-}21)\qquad N_{t-1}(-D/B) = \begin{cases} q^{t-2} + q^{k-1}(q-1)\Psi((-1)^k A') & \text{if } t-1 = 2k, \\ q^{t-2} & \text{if } t-1 = 2k+1. \end{cases}$$

Since $A' = A/a_1$ and $\Psi(a_1 B) = 1$, we have

$$\Psi((-1)^k A') = \Psi((-1)^k \frac{A}{a_1})\Psi(a_1 B) = \Psi((-1)^k AB).$$

Then equation (4-21) becomes

$$N_{t-1}(-D/B) = \begin{cases} q^{t-2} + q^{k-1}(q-1)\Psi((-1)^k AB) & \text{if } t = 2k+1, \\ q^{t-2} & \text{if } t = 2k. \end{cases}$$

For $D \neq 0$,

$$(4\text{-}22)\qquad N_{t-1}(-D/B) = \begin{cases} q^{t-2} - q^{k-1}\Psi((-1)^k A') & \text{if } t-1 = 2k, \\ q^{t-2} + q^{k}\Psi((-1)^{k+1}\frac{D}{B} A') & \text{if } t-1 = 2k+1. \end{cases}$$

Since $\Psi(\frac{D}{B} A') = \Psi(\frac{D}{B} A')\,\Psi(a_1 B) = \Psi(DA)$, the equation (4-22) becomes

$$N_{t-1}(-D/B) = \begin{cases} q^{t-2} - q^{k-1}\Psi((-1)^k AB) & \text{if } t = 2k+1, \\ q^{t-2} + q^{k-1}\Psi((-1)^k DA) & \text{if } t = 2k. \end{cases}$$

Hence the formulas (4-15) and (4-16) result in this case provided $t \neq 1$. In the special case $t = 1$, we have equations $a = a_1 x_1^2$ and $b = B_1 x_1$. Since $A = a_1$ and $B = B_1^2/a_1$, $AB = a_1 \cdot \frac{B_1^2}{a_1} = B_1^2$ which is a square in F. Therefore the formulas (4-15) and (4-16) with $s = t = 1$, $k = 0$, agree with the obvious result,

$$N_{1,1}(a,b) = \begin{cases} 1 & \text{if } B \neq 0,\ D = 0, \\ 0 & \text{if } B \neq 0,\ D \neq 0. \end{cases}$$

Part 2. Suppose $B \neq 0$ and $a_i B$ is a non-square in F for every $i \leqslant t$. These conditions imply that $t > 1$ and that $a_1 a_2$ is a square in F; for if $t = 1$, we have $s = 1$ and so $a_1 B$ is a square which is not possible; moreover if $a_1 a_2$ is a non-square, then $a_1 B \cdot a_2 B = a_1 a_2 B^2$ is a non-square which contradicts the fact that $a_1 B$ and $a_2 B$ are both non-square, thus $a_1 a_2$ must be a square in F. By Theorem 3.5, there exists a pair of elements B_1, B_2 of F such that $B = B_1^2/a_1 + B_2^2/a_2$ and $B_1 \neq 0 \neq B_2$. Choosing a fixed pair of such elements B_1, B_2, it results from Corollary 4.5 that $N_{s,t}(a,b)$ is in the present case equal to the number of solutions of

$$\text{(4-23)} \qquad \begin{cases} a = a_1 x_1^2 + \dots + a_t x_t^2 , \\ b = B_1 x_1 + B_2 x_2 . \end{cases}$$

Let d be an element of F such that $d^2 = a_1 a_2$. We eliminate x_1 between the equations of (4-23) by substituting $x_1 = \dfrac{b - B_2 x_2}{B_1}$ from the second equation of (4-23) into the first one, then we have

$$a = a_1 \left[\frac{b - B_2 x_2}{B_1} \right]^2 + a_2 x_2^2 + \dots + a_t x_t^2$$

$$= \frac{1}{B_1^2} \left[a_1 b^2 - 2 b a_1 B_2 x_2 + (a_1 B_2^2 + a_2 B_1^2) x_2^2 \right] + a_3 x_3^2 + \dots + a_t x_t^2$$

$$= \frac{1}{B_1^2} \left[a_1 b^2 - 2 b a_1 B_2 x_2 + a_1 a_2 B x_2^2 \right] + a_3 x_3^2 + \dots + a_t x_t^2$$

$$= \frac{B}{B_1^2}\left[a_1a_2x_2^2 - \frac{2ba_1B_2}{B}x_2 + \frac{b^2a_1^2B_2^2}{B^2a_1a_2} - \frac{b^2a_1B_2^2}{B^2a_2} + \frac{a_1b^2}{B}\right]$$

$$+ a_3x_3^2 + \dots + a_tx_t^2$$

$$= \frac{B}{B_1^2}\left[\left(\sqrt{a_1a_2}\,x_2 - \frac{ba_1B_2}{B\sqrt{a_1a_2}}\right)^2 + \frac{a_1b^2}{B} - \frac{a_1b^2}{B^2}\frac{(B-B_1^2)}{a_1}\right]$$

$$+ a_3x_3^2 + \dots + a_tx_t^2$$

$$= \frac{B}{B_1^2}\left[\left(\sqrt{a_1a_2}\,x_2 - \frac{ba_1B_2}{B\sqrt{a_1a_2}}\right)^2 + \frac{b^2B_1^2}{B^2}\right] + a_3x_3^2 + \dots + a_tx_t^2\,,$$

or equivalently,

$$a - \frac{b^2}{B} = \frac{B}{B_1^2}\left(\sqrt{a_1a_2}\,x_2 - \frac{ba_1B_2}{B\sqrt{a_1a_2}}\right)^2 + a_3x_3^2 + \dots + a_tx_t^2.$$

Thus by involving completing a square, the equations (4-23) lead to the single equation,

$$(4\text{-}24) \qquad -\frac{D}{B} = BZ^2 + a_3x_3^2 + \dots + a_tx_t^2\,,$$

where $Z = \frac{1}{B_1}\left(dx_2 - \frac{ba_1B_2}{Bd}\right)$. Therefore, the number of solutions of (4-24) is given by $N_{s,t}(a,b)$. Application of Theorem 4.6 with t replaced by t-1, a by -D/B and A by $Ba_3 \dots a_t$ (by B if t = 2), in connection with the observation, $\Psi(a_1a_2) = 1$, leads to the formulas (4-15) and (4-16). Notice that the equation (4-24) and equation (4-20) have the same type, so the number of solutions of

(4-24) is the same as that of solutions of (4-20), that is, the formulas (4-15) and (4-16).

Cases(i) and (ii) of the theorem are now completely established; that is, the theorem is now proved in the case $B \neq 0$. In the remainder of the proof, B has the value 0 and $t > 1$.

Part 3. Let us suppose now that $B = 0$ and that integers i,j exist, $i \neq j$, $1 \leqslant i, j \leqslant t$, such that $-a_i a_j$ is a square of F. Without loss of generality suppose that $-a_1 a_2$ is a square. It follows that we can pick non-zero elements B_1, B_2 of F such that $0 = B_1^2/a_1 + B_2^2/a_2$; for any such pair B_1, B_2, $N_{s,t}(a,b)$ is in this case equal to the number of solutions of (4-23). Eliminate of x_1 from (4-23) yields the equation,

$$(4\text{-}25) \qquad \frac{B_1^2 a - a_1 b^2}{B_1^2} = \frac{-2ba_1 B_2}{B_1^2} x_2 + a_3 x_3^2 + \dots + a_t x_t^2 ,$$

the number of whose solutions is $N_{s,t}(a,b)$. If $b \neq 0$, x_2 in (4-25) is determined on assigning arbitrary values to $x_3, \dots, x_t$; hence in case $D \neq 0$ (because $D = b^2 - aB$, and $b \neq 0$, $B = 0$), $N_{s,t}(a,b) = q^{t-2}$ (Case (v)). If $b = 0$, x_2 can be chosen arbitrarily in (4-25) provided $t > 2$, so that $N_{s,t}(a,0) = q\, L(a)$, where L(a) is the number of solutions of $a = a_3 x_3^2 + \dots + a_t x_t^2$. Applying Theorem 4.6 with t replaced by t-2 and the fact that $\Psi(-a_1 a_2) = 1$, $A' = a_3 \dots a_t = A/a_1 a_2$, we have L(a) as follows :

$$\text{if } a = 0, \quad L(a) = \begin{cases} q^{t-3} + q^{k-1}(q-1)\Psi((-1)^k A') & \text{if } t-2 = 2k, \\ q^{t-3} & \text{if } t-2 = 2k+1 \ ; \end{cases}$$

$$\text{if } a \neq 0, \quad L(a) = \begin{cases} q^{t-3} - q^{k-1}\Psi((-1)^k A') & \text{if } t-2 = 2k, \\ q^{t-3} + q^{k}\Psi((-1)^k aA') & \text{if } t-2 = 2k+1. \end{cases}$$

Put $k+1 = k'$, we have

$$\text{if } a = 0, \quad L(a) = \begin{cases} q^{t-3} + q^{k'-2}(q-1)\Psi((-1)^{k'} A) & \text{if } t = 2k', \\ q^{t-3} & \text{if } t = 2k'+1 \ ; \end{cases}$$

$$\text{if } a \neq 0, \quad L(a) = \begin{cases} q^{t-3} - q^{k'-2}\Psi((-1)^{k'} A) & \text{if } t = 2k', \\ q^{t-3} + q^{k'-1}\Psi((-1)^{k'} aA) & \text{if } t = 2k'+1. \end{cases}$$

Therefore if $a = 0$,

$$N_{s,t}(a,0) = qL(a) = \begin{cases} q^{t-2} + q^{k'-1}(q-1)\Psi((-1)^{k'} A) & \text{if } t = 2k', \\ q^{t-2} & \text{if } t = 2k'+1 \ ; \end{cases}$$

if $a \neq 0$,

$$N_{s,t}(a,0) = qL(a) = \begin{cases} q^{t-2} - q^{k'-1}\Psi((-1)^{k'} A) & \text{if } t = 2k', \\ q^{t-2} + q^{k'}\Psi((-1)^{k'} aA) & \text{if } t = 2k'+1. \end{cases}$$

Hence we get (4-17) and (4-18) provided $t \neq 2$. In case $b = 0$, $t = 2$, (4-25) reduces to $a = 0 \cdot x_2$, so that

$$N_{s,2}(a,0) = \begin{cases} q & \text{if } a = 0, \\ 0 & \text{if } a \neq 0. \end{cases}$$

This agrees with (4-17) and (4-18), in case $t = 2$, $k = 1$. Cases(iii) and (iv), for which $D = 0$, are therefore completed from this part of the proof.

Part 4. There remains to consider the case in which $B = 0$ and $-a_i a_j$ is a non-square of F for all $i \neq j$, $1 \leq i, j \leq t$. These conditions imply that $t \geq 3$. For if $t = 2$, then there exists a pair of elements B_1, B_2 of F such that

$$\frac{B_1^2}{a_1} + \frac{B_2^2}{a_2} = 0.$$

Then

$$B_1^2 = -\frac{a_1}{a_2} B_2^2 = -a_1 a_2 \frac{B_2^2}{a_2^2}.$$

Therefore

$$-a_1 a_2 = \left(\frac{B_1 a_2}{B_2}\right)^2.$$

This is impossible since $-a_1 a_2$ is a non-square of F by the assumption, if $t = 1$, then $i = 1 = j$. Thus it is not in the case. Let us choose non-zero elements B_1, B_2, B_3 of F such that $B_1^2/a_1 + B_2^2/a_2 + B_3^2/a_3 = 0$; this is possible by an argument used in Part 2. It follows then as before that $N_{s,t}(a,b)$ is in the present case the same as the number of solutions of

$$(4\text{-}26)\qquad \begin{cases} a = a_1x_1^2+\dots+a_tx_t^2 , \\ b = B_1x_1+B_2x_2+B_3x_3 . \end{cases}$$

If we eliminate x_1 and simplify the resulting equation by completion of squares, (4-26) is replaced by the single equation,

$$(4\text{-}27)\qquad a - \frac{a_1a_2b^2}{P} = PZ^2 - \frac{(2ba_1a_2B_3)}{P}x_3 + a_4x_4^2+\dots+a_tx_t^2 ,$$

where $P = B_1^2a_2+B_2^2a_1 = -a_1a_2a_3^{-1}B_3^2 \neq 0$ and $Z = (x_2+a_1B_2B_3P^{-1}x_3-ba_1B_2P^{-1})/B_1$. If $b = 0$, that is, in case $D = 0$, $N_{s,t}(a,0) = qL'(a)$, where $L'(a)$ is the number of solutions of $a = PZ_1^2+a_4x_4^2+\dots+a_tx_t^2$,
where $Z_1 = (x_2+a_1B_2B_3P^{-1}x_3)/B_1$. By Theorem 4.6 on replacing A by $Pa_4\dots a_t$ (let $A' = Pa_4\dots a_t$) and t by t-2 and noting that $\Psi(P) = \Psi(-a_1a_2a_3)$, then we have

$$\text{if } a = 0,\quad L'(a) = \begin{cases} q^{t-3}+q^{k-1}(q-1)\,\Psi((-1)^kA') & \text{if } t-2 = 2k, \\ q^{t-3} & \text{if } t-2 = 2k+1 ; \end{cases}$$

$$\text{if } a \neq 0,\quad L'(a) = \begin{cases} q^{t-3}-q^{k-1}\,\Psi((-1)^kA') & \text{if } t-2 = 2k, \\ q^{t-3}+q^k\,\Psi((-1)^kaA') & \text{if } t-2 = 2k+1 . \end{cases}$$

Since $A' = Pa_4\dots a_t$, $\Psi((-1)^kA') = \Psi((-1)^kPa_4\dots a_t)$
$= \Psi((-1)^ka_4\dots a_t)\,\Psi(P) = \Psi((-1)^ka_4\dots a_t)\,\Psi(-a_1a_2a_3)$
$= \Psi((-1)^{k+1}a_1a_2a_3a_4\dots a_t) = \Psi((-1)^{k+1}A)$. Put $k+1 = k'$,
then we have

$$\text{if } a = 0, \quad L'(a) = \begin{cases} q^{t-3} + q^{k'-2}(q-1)\,\Psi((-1)^{k'}A) & \text{if } t = 2k', \\ q^{t-3} & \text{if } t = 2k'+1\ ; \end{cases}$$

$$\text{if } a \neq 0, \quad L'(a) = \begin{cases} q^{t-3} - q^{k'-2}\,\Psi((-1)^{k'}A) & \text{if } t = 2k', \\ q^{t-3} + q^{k'-1}\,\Psi((-1)^{k'}aA) & \text{if } t = 2k'+1. \end{cases}$$

Using the fact that $N_{s,t}(a,0) = q\,L'(a)$, cases (iii) and (iv) are therefore completed. If $b \neq 0$ (or equivalently, $D \neq 0$), Z, $x_4, \ldots, x_t$ in (4-27) can be assigned arbitrarily from which case (v) results. This completes the proof of the theorem.

Examination of Theorem 4.7 leads almost immediately to the following.

4.8 <u>Corollary</u>. $N_{s,t}(a,b) > 0$ for all $t \geqslant 4$, and $N_{s,3}(a,b) = 0$ if and only if $a \neq 0$, $b = B = 0$ and $\Psi(-aA) = -1$; moreover, $N_{s,t}(0,0) > 1$ for all $t \geqslant 4$, while $N_{s,3}(0,0) = 1$ if and only if $B \neq 0$ and $\Psi(-AB) = -1$.

4.9 <u>Corollary</u>. The formula, $N_{s,t}(a,b) = q^{t-2}$, holds if and only if one of the following sets of conditions is satisfied :

(i) $B \neq 0$, $D = 0$, t is even,

(ii) $B = D = a = 0$, t is odd,

(iii) $B = 0$, $D \neq 0$.