CHAPTER III

QUADRICS OVER A FINITE FIELD

In this chapter, we determine the number of solutions in a finite field F of the equation

$$a_1x_1^2+\dots+ a_tx_t^2 = a,$$

where $a_1,\dots, a_t$ are non-zero elements in F and $a \in F$. Every finite field considered from now on is of characteristic $p > 2$, where p is a prime number. The materials of this chapter are based on L.E.Dickson [5, §§ 61-66] .

3.1 Definition. A non-zero element x of the $GF[p^n]$ is called a square in $GF[p^n]$ if and only if there exists $y \in GF[p^n]$ satisfying $x = y^2$. Otherwise, x is called a non-square.

3.2 Theorem. Let $F = GF[p^n]$. Then the number of squares in F is $(p^n- 1)/2$ and the number of non-squares in F is also $(p^n- 1)/2$.

Proof. By Theorem 2.13, F^* is cyclic with $p^n- 1$ elements and say with generator u. Then $F^* = [u] = \{u, u^2,\dots, u^{p^n- 1} = 1\}$.
Since p is an odd prime, p^n is odd and thus $p^n- 1$ is even.
Hence $2 \mid p^n- 1$.
We claim that

$$(3\text{-}1) \qquad u^{\frac{p^n-1}{2}} = -1 .$$

Since $u^{\frac{p^n-1}{2}} \cdot u^{\frac{p^n-1}{2}} = u^{\frac{p^n-1}{2}+\frac{p^n-1}{2}} = u^{p^n-1} = 1$, we have

$$(u^{\frac{p^n-1}{2}})^2 - 1 = 0,$$

or

$$(u^{\frac{p^n-1}{2}} - 1)(u^{\frac{p^n-1}{2}} + 1) = 0.$$

Since each element in F^* is of the form u^k and if $k \neq r$, $u^k \neq u^r$, $1 \leqslant k, r \leqslant p^n - 1$, then $u^{\frac{p^n-1}{2}} \neq u^{p^n-1} = 1$ and hence $(u^{\frac{p^n-1}{2}} - 1) \neq 0$. Consequently, we have $(u^{\frac{p^n-1}{2}} + 1) = 0$, that is, $u^{\frac{p^n-1}{2}} = -1$ and the claim is proved.

If $x \in F$ is of the form u^{2h} for some h such that $1 \leqslant 2h \leqslant p^n - 1$, we have $x = (\pm u^h)^2$. Thus x is a square. Hence every element of F which is the even power of u is a square in F. Moreover, if x is an element of F which is the odd power of u, then x is a non-square. For if $u^{2h+1} = x^2$, then

$$\begin{aligned} u^{\frac{(2h+1)(p^n-1)}{2}} &= u^{h(p^n-1)} \cdot u^{\frac{p^n-1}{2}} \\ &= (u^{p^n-1})^h \cdot (-1) \\ &= 1 \cdot (-1) = -1, \end{aligned}$$

by virtue of (3-1). On the other hand,

$$\begin{aligned} u^{\frac{(2h+1)(p^n-1)}{2}} &= (u^{2h+1})^{\frac{p^n-1}{2}} \\ &= x^{p^n-1} \\ &= 1. \end{aligned}$$

Consequently, we have $1 = -1$ and thus $1 + 1 = 0$ which is not possible since characteristic of F is $p > 2$. Hence the odd powers of u are non-squares in F.

Therefore there are $(p^n-1)/2$ squares and as many non-squares in F.

3.3 Lemma. The sum of m odd positive integers is odd or even according as m is an odd or even positive integer.

Proof. Let s be the sum of m odd positive integers. Since each odd integer can be written as $2n_i + 1$, $i = 1,\ldots, m$, it follows that

$$s = (2n_1 + 1)+(2n_2 + 1)+\ldots+(2n_m + 1)$$

$$= 2(n_1 + n_2+\ldots+ n_m)+\underbrace{(1 + 1 +\ldots+ 1)}_{m \text{ times}}$$

$$= 2(n_1 + n_2+\ldots+ n_m)+ m.$$

But since the first term of s is even, s is therefore odd or even according as m is odd or even.

3.4 Theorem. The non-squares of any $GF[p^n]$ are non-squares or squares in the $GF[p^{nm}]$ according as m is odd or even.

Proof. Let $F = GF[p^n]$ and $L = GF[p^{nm}]$. Let u be a generator of L^*. Then $L^* = [u]$ with $u^{p^{nm}-1} = 1$. Since $|F^*| = p^n - 1$, where $|F^*|$ denotes the number of elements in F^*, and F^* is a subgroup of L^*, $(p^n-1)\,|\,(p^{nm}-1)$. Let $r = (p^{nm}-1)/(p^n-1)$. Then $v = u^r$ is a generator of F^*. Hence the non-zero elements of F^* are given by the formula

$$v^s = u^{rs},$$

where $s = 1, \ldots, p^n - 1$. Let v^k be a non-square in F, so that k is odd. It will be a non-square or a square in L according as kr is odd or even, that is, according as r is odd or even. But

$$r = \frac{p^{nm} - 1}{p^n - 1}$$

$$= \frac{1 - (p^n)^m}{1 - p^n}$$

$$= \frac{(1 - p^n)(1 + p^n + \ldots + (p^n)^{m-1})}{1 - p^n}$$

$$= 1 + p^n + \ldots + p^{(m-1)n} .$$

Thus r is the sum of m odd positive integers. Hence by Lemma 3.3 r is odd or even according as m is odd or even.

The theorem is now proved.

3.5 Theorem. Let a_1, a_2 be non-zero elements of $GF[p^n]$ and let $a \in GF[p^n]$. Then the number of solutions of the equation

$$a_1x_1^2 + a_2x_2^2 = a \qquad (3\text{-}2)$$

is $p^n - \theta$ or $p^n + (p^n - 1)\theta$ according as $a \neq 0$ or $a = 0$, where $\theta = +1$ or -1 according as $-a_1a_2$ is a square or a non-square in $GF[p^n]$.

Proof. Consider the equation (3-2)

$$a_1x_1^2 + a_2x_2^2 = a.$$

Setting $a_1x_1 = y$ and multiplying a_1 to (3-2), the equation becomes

(3-3) $$y^2 + a_1a_2x_2^2 = a_1a.$$

We divide into two cases according as $-a_1a_2$ is a square or a non-square.

Case 1. If $-a_1a_2$ is a square in $GF[p^n]$, say $-a_1a_2 = b^2$, then we have

(3-4) $$y^2 - b^2x_2^2 = a_1a.$$

We set $y + bx_2 = z_1$, $y - bx_2 = z_2$, then

$$y = \frac{1}{2}(z_1 + z_2) \quad \text{and} \quad x_2 = \frac{1}{2b}(z_1 - z_2).$$

Substitute y and x_2 in (3-4), the equation becomes

$$\left[\frac{1}{2}(z_1 + z_2)\right]^2 - b^2\left[\frac{1}{2b}(z_1 - z_2)\right]^2 = a_1a,$$

multiply the equation out we obtain

$$\frac{1}{4}(z_1^2 + 2z_1z_2 + z_2^2) - \frac{1}{4}(z_1^2 - 2z_1z_2 + z_2^2) = a_1a,$$

or

(3-5) $$z_1z_2 = a_1a.$$

If $a \neq 0$, we can assign to z_2 any one of the $p^n - 1$ non-zero elements in $GF[p^n]$, and the corresponding value of z_1 is determined by equation (3-5). There are in this case $p^n - 1$ sets of solutions x_1, x_2 in the field of the given equation.

If $a = 0$, then we get $z_1z_2 = 0$. Thus $z_1 = 0$ or $z_2 = 0$. For $z_1 = 0$, we have $y + bx_2 = 0$ and since $y = a_1x_1$, we have $a_1x_1 = -bx_2$. There are in this case $p^n - 1$ sets of solutions x_1, x_2.

For $z_2 = 0$, we have $y - bx_2 = 0$ and then $a_1x_1 = bx_2$. There are also $p^n - 1$ sets of solutions x_1, x_2. Another solution of the equation $z_1z_2 = 0$ is $z_1 = 0$ and $z_2 = 0$, that is $(x_1,x_2) = (0,0)$ is one of the solutions of (3-2). Hence all together there are $1 + (p^n - 1)+(p^n - 1) = 1 + 2(p^n - 1)$ sets of solutions of the equation (3-2) in this case.

Case 2. If $-a_1a_2$ is a non-square in the $GF[p^n]$, then the equation

(3-6) $$x^2 = -a_1a_2$$

is irreducible in the field ; for if $x^2 + a_1a_2 = 0$ is reducible, then we can write $x^2 + a_1a_2 = x^2 - (-a_1a_2) = (x-d)(x+d) = x^2 - d^2$ for some $d \in GF[p^n]$, and therefore $-a_1a_2 = d^2$, this is impossible since $-a_1a_2$ is a non-square in $GF[p^n]$. Now $f(x) = x^2 + a_1a_2$ is irreducible polynomial over $F = GF[p^n]$. Let F' be the splitting field of $f(x)$ over F. Let i be a root of $f(x)$. Then $i \in F'$. Let $E = F(i)$. Consequently, $E = GF[p^{2n}]$ by Theorem 2.19 . Now $\pm i$ are roots of (3-6) and by Corollary 2.24 , $i^{p^n} = -i$. We therefore have the identity

$$\begin{aligned} y^2 + a_1a_2x_2^2 &= (y + ix_2)(y + i^{p^n}x_2) \\ &= (y + ix_2)(y^{p^n} + i^{p^n}x_2^{p^n}) \quad \text{[by Lemma 2.3]} \\ &= (y + ix_2)(y + ix_2)^{p^n} \quad \text{[by Theorem 2.9]} \\ &= (y + ix_2)^{p^n+1} . \end{aligned}$$

Then the equation (3-3) becomes

$$(3\text{-}7) \qquad (y + ix_2)^{p^n+1} = a_1 a .$$

Let $Z = y + ix_2$, then the equation (3-7) becomes

$$(3\text{-}8) \qquad Z^{p^n+1} = a_1 a .$$

If $a = 0$, then $Z = 0$ and therefore a single set of solutions is ($x_1 = 0$, $x_2 = 0$).

If $a \neq 0$, let R be a generator of the $GF[p^{2n}]$ and set $a_1 a = R^k$, where k is an integer, then

$$R^{k(p^n-1)} = (a_1 a)^{p^n-1} = 1.$$

So $k(p^n-1)$ is divisible by $p^{2n}-1$. We may therefore set $k = r(p^n+1)$, where r is a suitable positive integer. Since $Z = y + ix_2 \in GF[p^{2n}]$, we may set $Z = R^t$. The equation (3-8) becomes

$$R^{t(p^n+1)} = R^{r(p^n+1)} .$$

Hence $\quad t(p^n+1) \equiv r(p^n+1) \quad (\text{mod } (p^{2n}-1))$. This congruence has p^n+1 distinct solutions for t, namely,

$$t = r,\ r + p^n-1,\ r + 2(p^n-1), \ldots,\ r + p^n(p^n-1).$$

The corresponding values of $R^t = Z = y + ix_2$ give p^n+1 distinct sets of solutions x_1, x_2 of the given equation.

3.6 <u>Theorem</u>. The number of solutions $(x_1, \ldots, x_{2m})$ in the $GF[p^n]$ of the equation

(3-9) $$a_1x_1^2+\dots+a_{2m}x_{2m}^2 = a,$$

where every a_j is a non-zero element in the field, is

$$p^{n(2m-1)} - \theta\, p^{n(m-1)} \qquad \text{if } a \neq 0$$

$$p^{n(2m-1)} + \theta\,(p^{nm} - p^{n(m-1)}) \qquad \text{if } a = 0,$$

where θ is +1 or −1 according as $(-1)^m a_1\dots a_{2m}$ is a square or a non-square in the field.

Proof. By Theorem 3.5, the theorem is true if $m = 1$. To prove the theorem by induction, we suppose it true for equations in $2(m-1)$ variables. The equation (3-9) is equivalent to the system of two equations

(3-10) $$a_1x_1^2+a_2x_2^2 = \eta,$$

(3-11) $$a_3x_3^2+\dots+a_{2m}x_{2m}^2 = a-\eta.$$

Case 1. Let $a \neq 0$. For each of the p^n-2 values of η different from a and 0, the equation (3-10) has $p^n-\beta$ sets of solutions, while by hypothesis the equation (3-11) has $p^{n(2m-3)} - \mu p^{n(m-2)}$, where $\beta = \pm 1$ according as $-a_1a_2$ is a square or a non-square and $\mu = \pm 1$ according as $(-1)^{m-1}a_3\dots a_{2m}$ is a square or a non-square. For $\eta = 0$, the equations become

$$a_1x_1^2+a_2x_2^2 = 0 \qquad \text{and} \qquad a_3x_3^2+\dots+a_{2m}x_{2m}^2 = a.$$

They have respectively, by Theorem 3.5 and hypothesis, $p^n+(p^n-1)\beta$

and $p^{n(2m-3)} - \mu p^{n(m-2)}$ sets of solutions. Finally, for $\eta = a$, we have

$$a_1x_1^2 + a_2x_2^2 = a \quad \text{and} \quad a_3x_3^2 + \dots + a_{2m}x_{2m}^2 = 0.$$

They have respectively $p^n - \beta$ and $p^{n(2m-3)} + \mu(p^{n(m-1)} - p^{n(m-2)})$ sets of solutions. The total number of sets of solutions is therefore

$$(p^n-2)(p^n-\beta)(p^{n(2m-3)}-\mu p^{n(m-2)}) + \{p^n+(p^n-1)\beta\}\{p^{n(2m-3)}-\mu p^{n(m-2)}\}$$
$$+(p^n-\beta)\{p^{n(2m-3)}+\mu(p^{n(m-1)}-p^{n(m-2)})\}$$
$$= p^{n(2m-3)}\{(p^n-2)(p^n-\beta)+(p^n+(p^n-1)\beta)+p^n-\beta\}+p^{n(m-1)}\{\mu(p^n-\beta)\}$$
$$+p^{n(m-2)}\{-\mu(p^n-2)(p^n-\beta)-\mu(p^n+(p^n-1)\beta)-\mu(p^n-\beta)\}$$
$$= p^{n(2m-1)}-\beta\mu p^{n(m-1)}.$$

Since the product of two squares or of two non-squares is again a square; but the product of a square by a non-square is a non-square. $\beta\mu = \theta$. Hence the induction is complete.

<u>Case 2</u>. Let $a = 0$. For each of the p^n-1 values of $\eta \neq 0$, the equation (3-10) has $p^n - \beta$ sets of solutions, while the equation (3-11) has $p^{n(2m-3)}-\mu p^{n(m-2)}$, where $\beta = \pm 1$ according as $-a_1a_2$ is a square or a non-square and $\mu = \pm 1$ according as $(-1)^{m-1} a_3 \dots a_{2m}$ is a square or a non-square. For $\eta = 0$, the equations become

$$a_1x_1^2 + a_2x_2^2 = 0 \quad \text{and} \quad a_3x_3^2 + \dots + a_{2m}x_{2m}^2 = 0.$$

Thus they have respectively $p^n+(p^n-1)\beta$ and $p^{n(2m-3)}+\mu(p^{n(m-1)}-p^{n(m-2)})$ sets of solutions. We find the total number of solutions to be

$$(p^n-1)(p^n-\beta)\{p^{n(2m-3)}-\mu p^{n(m-2)}\}+\{p^n+(p^n-1)\beta\}\{p^{n(2m-3)}+\mu(p^{n(m-1)}-p^{n(m-2)})\}$$

$$= p^{n(2m-3)}\{(p^n-1)(p^n-\beta)+(p^n+(p^n-1)\beta)\}+p^{n(m-2)}\{-\mu(p^n-1)(p^n-\beta)$$

$$-\mu(p^n+(p^n-1)\beta)\}+p^{n(m-1)}\{\mu(p^n+(p^n-1)\beta)\}$$

$$= p^{n(2m-1)}+\beta\mu(p^{nm}-p^{n(m-1)})$$

$$= p^{n(2m-1)}+\theta(p^{nm}-p^{n(m-1)}).$$

Hence the theorem is proved.

3.7 <u>Theorem</u>. The number of solutions in the $GF[p^n]$ of the equation

$$(3\text{-}12) \qquad a_1x_1^2+\dots+a_{2m+1}x_{2m+1}^2 = a,$$

where each a_j is a non-zero element in the field and a belongs to the field, is $p^{2nm}+\omega p^{nm}$, where $\omega = +1$, -1 or 0 according as $(-1)^m aa_1\dots a_{2m+1}$ is a square, a non-square or zero in the field.

<u>Proof</u>. Consider the equivalent system of equations

$$(3\text{-}13) \qquad a_1x_1^2 = \eta,$$

$$(3\text{-}14) \qquad a_2x_2^2+\dots+a_{2m+1}x_{2m+1}^2 = a-\eta.$$

If $\eta = 0$, then (3-13) has only one solution $x_1 = 0$. If $\eta \neq 0$, we have $x_1^2 = \eta/a_1$ and then (3-13) has two or no solutions according as η/a_1 is a square or a non-square, that is, according as $a_1^2\eta/a_1 = a_1\eta$ is a square or a non-square. Let

$$\mu = \begin{cases} +1 & \text{if } a_1 a \text{ is a square,} \\ -1 & \text{if } a_1 a \text{ is a non-square,} \\ 0 & \text{if } a = 0. \end{cases}$$

We may express the number of solutions of the equation (3-14) by Theorem 3.6, if we set $\theta = \pm 1$ according as $(-1)^m a_2 \ldots a_{2m+1}$ is a square or a non-square. Evidently we have $\mu\theta = \omega$, that is, $\omega = +1, -1$ or 0 according as $(-1)^m aa_1 \ldots a_{2m+1}$ is a square, a non-square or zero in the field.

<u>Case 1</u>. $(\mu = 0)$. For $\eta = 0$, we get

$$a_1 x_1^2 = 0 \quad \text{and} \quad a_2 x_2^2 + \ldots + a_{2m+1} x_{2m+1}^2 = 0.$$

The first equation has one solution while the second has $p^{n(2m-1)} + \theta(p^{nm} - p^{n(m-1)})$. For $\eta \neq 0$, the equations become

$$a_1 x_1^2 = \eta \quad \text{and} \quad a_2 x_2^2 + \ldots + a_{2m+1} x_{2m+1}^2 = -\eta .$$

The first equation has solution only when $a_1 \eta$ is a square and there are $(p^n - 1)/2$ values of such η since the number of squares in $GF[p^n]$ is $(p^n - 1)/2$ by Theorem 3.2. Thus for each of the $(p^n - 1)/2$ values of η, the first equation has two solutions while the second has $p^{n(2m-1)} - \theta p^{n(m-1)}$. Hence according as $\mu = 0$, the total number of solutions of the pair of equations is

$$1 \cdot \{p^{n(2m-1)} + \theta(p^{nm} - p^{n(m-1)})\} + 2 \cdot \frac{(p^n - 1)}{2} \{p^{n(2m-1)} - \theta p^{n(m-1)}\}$$

$$= p^{n(2m-1)}\{1 + p^n - 1\} + \theta p^{nm} - p^{n(m-1)}\{\theta + \theta(p^n - 1)\}$$

$$= p^{2nm}.$$

Case 2. ($\mu = +1$). For $\eta = 0$, the equation (3-13) has only one solution while the equation (3-14) has $p^{n(2m-1)} - \theta p^{n(m-1)}$. For $\eta = a$, we get

$$a_1 x_1^2 = a \quad \text{and} \quad a_2 x_2^2 + \dots + a_{2m+1} x_{2m+1}^2 = 0.$$

Since $a_1 a$ is a square, the first equation has two solutions. At the same time, there are $p^{n(2m-1)} + \theta(p^{nm} - p^{n(m-1)})$ sets of solutions for the second equation. For each of the $[(p^n-1)/2] - 1 = (p^n-3)/2$ values of η different from 0 and a, the equation (3-13) has two solutions while the equation (3-14) has $p^{n(2m-1)} - \theta p^{n(m-1)}$. Hence according as $\mu = +1$, the total number of solutions of the pair of equations is

$$1 \cdot \{p^{n(2m-1)} - \theta p^{n(m-1)}\} + 2 \cdot \{p^{n(2m-1)} + \theta(p^{nm} - p^{n(m-1)})\} + 2 \cdot \left(\frac{p^n-3}{2}\right)\{p^{n(2m-1)} - \theta p^{n(m-1)}\}$$

$$= p^{n(2m-1)}\{1+2+p^n-3\} + p^{n(m-1)}\{-\theta-2\theta-\theta p^n+3\theta\} + 2\theta p^{nm}$$

$$= p^{2nm} + \theta p^{nm}.$$

Case 3. ($\mu = -1$). For $\eta = 0$, the equation (3-13) has only one solution while the equation (3-14) has $p^{n(2m-1)} - \theta p^{n(m-1)}$. For $\eta = a$, we have $a_1 x_1^2 = a$. This equation has solution only when a/a_1 is a square, that is, a and a_1 are both square or non-square, but this is not possible since $a_1 a$ is non-square. Thus for $\eta = a$, the equation (3-13) has no solution. For $\eta \neq 0$, the equation (3-13) is $a_1 x_1^2 = \eta \neq 0$. Then for each of the $(p^n-1)/2$ values of η, it has two solutions according as $a_1\eta$ is a square. Since $a_1 a$ is a non-square and $a_1\eta$ is a square, $a \neq \eta$, that is, $a-\eta \neq 0$. Therefore the equation (3-14) has $p^{n(2m-1)}-\theta p^{n(m-1)}$ sets of solutions. Hence the total number of solutions of the pair of equations for $\mu = -1$ is

$$1\cdot\{p^{n(2m-1)}-\theta p^{n(m-1)}\} + 2\cdot\left(\frac{p^n-1}{2}\right)\{p^{n(2m-1)}-\theta p^{n(m-1)}\}$$

$$= p^{n(2m-1)}\{1+p^n-1\} + p^{n(m-1)}\{-\theta-\theta p^n+\theta\}$$

$$= p^{2nm}-\theta p^{nm}.$$

Therefore there are $p^{2nm}+\omega p^{nm}$ sets of solutions of (3-12) where $\omega = +1, -1$ or 0 according as $(-1)^m a a_1 \ldots a_{2m+1}$ is a square, a non-square or zero in the $GF[p^n]$.