CHAPTER III

STARTERS, ADDERS AND ROOM SQUARES

3.1 Construction of Room Square of side p^n where p is an odd prime and p^n can be written in the form $p^n = 2^k t+1$; where t is an odd integer greater than 1.

Definition 3.1.1 Let G be a finite Abelian group of order $r = 2s + 1$, where s is a positive integer. By a starter in G we shall mean an s-tuple $X = (\{x_1, y_1\}, \{x_2, y_2\}, \ldots, \{x_s, y_s\})$ of unordered pairs of elements of G with the properties that:

(i) the elements $x_1, x_2, \ldots x_s, y_1, y_2, \ldots, y_s$ comprise all the non - zero elements of G ,

(ii) the differences $\pm (x_i - y_i)$; $i = 1, 2, \ldots, s$ comprise all the non - zero elements of G generating each precisely once.

A starter X is said to be strong if all sum $(x_i + y_i)$; $i = 1, 2, \ldots, s$, are distinct and are non zero elements of G

By an adder for a starter X, we shall mean an s-tuple $A_x = (a_1, a_2, \ldots, a_s)$ of non - zero elements of G such that the elements $x_i + a_i$, $y_i + a_i$; $i = 1, 2, \ldots, s$ are all distinct and comprise all the non - zero elements of G.

Theorem 3.1.2 If an abelian group of odd order r has a starter and an adder, then there is a Room Square of side r.

Proof Let $X = (\{x_1, y_1\}, \{x_2, y_2\}, \ldots\ldots, \{x_s, y_s\})$ and $A_x = (a_1, a_2, \ldots, a_s)$ be a starter and an adder of an abelian group G of odd order $r = 2s + 1$.

Let us label the group elements of G as $0 = g_1, g_2, \ldots, g_r$. Let $G^* = G \cup \{g_0\}$, where g_0 is not a member of G. Extend + to G^* by setting $g_0 + g = g + g_0 = g_0$ for all $g \in G^*$.

We first construct the first row of $\mathcal{R}$ as follow :

(1) place $\{g_0, g_1\}$ in the (1, 1) cell of $\mathcal{R}$,

(2) for $k \neq 1$, if $-g_k = a_i$ for some i, then we place $\{x_i, y_i\}$ in the (1, k) cell otherwise the (1, k) cell will be left empty.

The construction of other rows will be based on the first row as follows: For each j, k $1 < j \leq r$, $1 \leq k \leq r$, we have $g_k - g_j = g_l$ and $g_k + g_j = g_{l^*}$ for a unique l and l^*, $1 \leq l, l^* \leq r$.
We shall denote l and l^* by l_{jk} and l^*_{jk} respectively.
Now for $j > 1$, we construct row j as follow:
Put $\{g_0, g_j\}$ in the (j, j) cell. We leave the (j, k) cell empty when the $(1, l_{jk})$ cell is empty, however if $\{x_i, y_i\}$ is in the $(1, l_{jk})$, then we place $\{x_i + g_j, y_i + g_j\}$ in the (j, k) cell.

We shall show that the resulting array is a Room Square. By property (i) of a starter X, we observe that the elements appearing in row 1 will contain all elements of G^* exactly once. The elements appearing in row j are obtained from those in row 1 by adding g_j to the elements of row 1. So, by the group property we see that all elements of G^* will appear in row j precisely once.

Let $\{g_a, g_b\}$ be any unordered pair of elements of G. From the property (ii) of X, there will be $\{x_i, y_i\}$ in X such that

$$(\alpha) \qquad g_a - g_b = -(x_i - y_i),$$

$$(\beta) \qquad g_a - g_b = x_i - y_i .$$

$$\text{Let } g = \begin{cases} g_a - y_i & \text{if } (\alpha) \text{ holds} \\ g_b - y_i & \text{if } (\beta) \text{ holds .} \end{cases}$$

Then $\{x_i + g,\ y_i + g\} = \{g_a, g_b\}$. Therefore, every unordered pair $\{g_a, g_b\}$ of elements of G is a member of the set $\{\{x_i + \theta, y_i + \theta\} \mid i = 1, 2, \ldots, s ; \theta \in G\}$, so every unordered pair of elements of G appears some where in $\mathcal{R}$.

The unordered pairs of the form $\{g_o, g_i\}$; $g_i \in G$ appears in the (i, i) cell. By counting we see that each row contains s unordered pairs from G and one unordered pair of the form $\{g_o, g_i\}$. Hence each row contains s + 1 unordered pairs. Hence the entired array contains r(s + 1) unordered pairs. Since G^* contains r + 1 elements, hence there are exactly $\frac{(r+1)(r)}{2} = r(s + 1)$ unordered pairs from G^*. Therefore every unordered pairs of elements of G^* appears precisely once in $\mathcal{R}$.

It remains to be shown that each elements of G^* appears in every column .

Let $\{u, v\}$ be any unordered pair of element of G^* in the k^{th} column of $\mathcal{R}$.

Assume that $\{u, v\}$ is in the (j, k) cell. By the construction of $\mathcal{R}$, we see that

$$u = x_p + g_j$$

$$v = y_p + g_j$$

for some p ; where the unordered pair $\{x_p, y_p\}$ appears in the $(1, l_{jk})$ cell.

The pair $\{x_p, y_p\}$ is in the $(1, l_{jk})$ cell if and only if the (l^*_{jt}, l^*_{kt}) cell contains $\{x_p + g_{l^*_{jt}}, y_p + g_{l^*_{jt}}\}$. Since $g_{l^*_{jt}} = g_j + g_t$.

Hence the (j, k) **ce**ll contains $\{x_p + g_j, y_p + g_j\}$ if and only if the (l^*_{jt}, l^*_{kt}) cell contains $\{x_p + g_j + g_t, y_p + g_j + g_t\}$.

Note that the $(l^*_{jt}, 1)$ cell is the (l^*_{jt}, l^*_{kt}) cell where $l^*_{kt} = 1$. Since $l^*_{kt} = 1$ if and only if $g_k + g_t = 0$, that is if and only if $-g_k = g_t$. For any t, $\{x_p + g_j + g_t, y_p + g_j + g_t\}$ appears in column 1.

Since $-g_k = g_t$, for some t . Hence $\{x_p + g_j - g_k, y_p + g_j - g_k\}$ appears in column 1. Choose $u' = x_p + g_j - g_k$; $v' = y_p + g_j - g_k$.

Then $u = u' + g_k$ and $v = v' + g_k$. So, we see that the elements in column k are obtained from the elements in column 1 by adding g_k to those in column 1 . Thus, if the elements of column 1 comprise all elements of G^* exactly once, then so do those every column .

For column 1, we observe that when $k > 1$, the (k, 1) cell contains $\{x_i + g_k, y_i + g_k\}$ if and only if $(1, l_{1k})$ cell contains $\{x_i, y_i\}$; that is if and only if $g_k = a_i$. So, the entries in the first column are $g_0, g_1, x_i + a_i, y_i + a_i, i = 1, 2, \ldots, s$. Since A_x is an adder, hence $x_i + a_i, y_i + a_i$; $i = 1, 2, \ldots, s$. comprise all the non - zero elements of G . Therefore the first column contains all the elements of G^* exactly once.

Q.E.D

<u>Theorem 3.1.3</u> If $X = (\{x_1, y_1\}, \{x_2, y_2\}, \ldots\ldots, \{x_s, y_s\})$ is a strong starter in an abelian group G of odd order $r = 2s + 1$. Then $A_x = (-(x_1 + y_1), -(x_2 + y_2)\ldots., -(x_s + y_s))$ is an adder for X.

<u>Proof</u> First we show that the components in A_x are distinct and non - zero elements from G .

Suppose that $-(x_i + y_i) = -(x_j + y_j)$ for $i \neq j$, then $x_i + y_i = x_j + y_j$ which contradicts to the assumption that X is strong starter.

Since each component in $((x_1 + y_1), (x_2 + y_2), \ldots\ldots, (x_s + y_s))$ is non - zero then each component in $(-(x_1 + y_1), -(x_2 + y_2), \ldots\ldots, -(x_s + y_s))$ is non - zero.

To show that A_x is an adder for X, we must show that the elements $x_i - (x_i + y_i)$, $y_i - (x_i + y_i)$; $i = 1, 2, \ldots, s$ are distinct and comprise all the non - zero elements of G.

If
$$x_i - (x_i + y_i) = x_j - (x_j + y_j), \text{ or}$$
$$y_i - (x_i + y_i) = y_i - (x_j + y_j), \text{ or}$$
$$x_i - (x_i + y_i) = y_j - (x_j + y_j) \quad \text{for } i \neq j, \text{ then}$$
we would have $y_i = y_j$, or $x_i = x_j$, or $y_i = x_j$ respectively. In any case, the conclusion is contrary to the assumption that X is a starter.

Now, if $x_i - (x_i + y_i) = 0$ for some i, then $y_i = 0$ which is a contradiction. Similary if $y_i - (x_i + y_i) = 0$ for some i, then $x_i = 0$ which is a contradiction.

By counting the elements $x_i - (x_i + y_i)$, $y_i - (x_i + y_i)$, $i = 1,2,\ldots, s$, we see that there are 2s elements.

So $x_i - (x_i + y_i)$, $y_i - (x_i + y_i)$ $i = 1, 2, \ldots, s$ comprise all the non - zero elements of G precisely once.

Hence A_x is an adder for X.

Q.E.D.

Theorem 3.1.4 There exists a strong starter for $G = GF(p^n)$; where p is a prime and $p^n = 2^k t+1$ for k a positive integer and t an integer greater than 1.

Proof. Let $2^{k-1} = d$ and x be a primitive elements in $GF(2^k t+1)$.

$$X_o = (\{x^o, x^d\}, \{x, x^{d+1}\}, \ldots\ldots, \{x^{d-1}, x^{2d-1}\}),$$

$$X_{2d} = (\{x^{2d}, x^{3d}\}, \{x^{2d+1}, x^{3d+1}\}, \ldots\ldots, \{x^{3d-1}, x^{4d-1}\}),$$

$$\vdots$$

$$X_{(2t-2)d} = (\{x^{(2t-2)d}, x^{(2t-1)d}\}, \{x^{(2t-2)d+1}, x^{(2t-1)d+1}\}, \ldots\ldots, \{x^{(2t-1)d-1}, x^{2td-1}\}).$$

We shall show that

$X = (X_o, X_{2d}, \ldots, X_{(2t-2)d})$ is a strong starter for $G = GF(2^k t + 1)$. The elements $x^o, x^1, \ldots\ldots, x^{2td-1} = x^{p^n-2}$ comprises $G - \{0\}$.

The differences between elements in the components of $X_0, X_{2d}, \ldots\ldots, X_{(2t-2)d}$ are

$$\pm\ x^{0}(1 - x^{d}),\ \pm\ x(1 - x^{d}),\ \ldots\ldots\ldots,\ \pm\ x^{d-1}(1 - x^{d}),$$

$$\pm\ x^{2d}(1 - x^{d}),\ \pm\ x^{2d+1}(1 - x^{d}),\ \ldots\ldots\ldots,\ \pm\ x^{3d-1}(1 - x^{d}),$$

$$\vdots$$

$$\pm\ x^{(2t-2)d}(1 - x^{d}),\ \pm\ x^{(2t-2)d+1}(1 - x^{d}),\ \ldots\ldots\ldots\ldots,$$

$$\pm\ x^{(2t-1)d-1}(1 - x^{d})$$ respectively.

Note that $(1 - x^{d})$ is non - zero element of G, since the order of x is by hypothes is $2td > d$.

We claim that all the differences are distinct and comprise the non-zero elements of G .

<u>case 1</u> If $x^{2id+j}(1 - x^{d}) = x^{2i'd+j'}(1 - x^{d})$ or

$$- x^{2id+j}(1 - x^{d}) = -x^{2i'd+j'}(1 - x^{d}) .$$

Then $x^{2id+j} = x^{2i'd+j'}$; where $0 \leq i, i' \leq t - 1$ and $0 \leq j, j' \leq d - 1$.

Therefore $x^{2id+j} - x^{2i'd+j'} = 0$, that is $x^{2id+j}(1 - x^{2i'd+j' - 2id-j}) = 0$.

Hence $x^{2i'd+j' - 2id-j} = 1$. Since x is of order $2td$.

Hence $2i'd + j' - 2id - j \equiv 0 \pmod{2td}$.

In particular $j' - j \equiv 0 \pmod{2d}$, and since $0 \leq j, j' \leq d - 1$, we must have $j' - j = 0$. Therefore $2(i' - i)d \equiv 0 \pmod{2td}$. That is $(i' - i) \equiv 0 \pmod{t}$, and since $0 \leq i, i' \leq t - 1$, hence $i' - i = 0$.

<u>case 2.</u> If $x^{2id+j}(1 - x^d) = - x^{2i'd+j'}(1 - x^d)$ for $0 \leq i, i' \leq t -$ and $0 \leq j, j' \leq d - 1$, then $x^{2id+j} + x^{2i'd+j'} = 0$. Suppose that $2id+j = 2i'd+j'$. Then we have $2x^{2id+j} = 0$. Therefore the field $GF(p^n)$ would have characteristic 2, an impossibility since p^n is odd. Therefore $2id + j \neq 2i'd + j'$.

Assuming that $2id + j < 2i'd + j'$, we write

$$x^{2id+j}(1 + x^{2i'd+j' - 2id-j}) = 0,$$

then $$x^{2i'd+j' - 2id - j} = -1,$$ and squaring

$$x^{2(j'-j) + 4d(i'-i)} = 1.$$

This must mean

$$2(j'- j) + 4d(i'- i) \equiv 0 \pmod{2\,dt},$$ since 2 dt is the order of x. In particular

$$2(j' - j) \equiv 0 \pmod{2d}$$

and since $0 \leq j \leq d - 1$ and $0 \leq j' \leq d - 1$ we must have $j' - j = 0$.

Therefore

$$4d(i' - i) \equiv 0 (\mathrm{mod}\ 2dt) . \quad \text{That is}$$

$$2(i' - i) \equiv 0 (\mathrm{mod}\ t) .$$

Since $-t+1 \leq i' - i \leq t - 1$, so $i' = i$ or $2(i' - i) = \pm t$.

If $i' = i$, then we have $2x^{2id+j}(1 - x^d) = 0$ which is impossible since 2, x and $1 - x^d$ are non - zero in $GF(p^n)$.

If $2(i' - i') = \pm t$, then it contradicts the fact that t is an odd integer.

Therefore differences between elements is the component of $X_o, X_{2d}, \ldots, X_{(2t-2)d}$ are distinct and non-zero. By counting the elements in the components of $X_o, X_{2d}, \ldots, X_{(2t-2)d}$, we see that there are $p^n - 1$ elements, hence they comprise all elements of $G \sim \{0\}$.

The fact they that starter X is strong can be seen by noting that the sums of elements in the pairs in the components of $X_o, X_{2d}, \ldots,$ $X_{(2t-2)d}$ are the same as differences with the factor $(1+x^d)$ rather than $(1 - x^d)$. But $(1 + x^d)$ is non-zero, since X is of order 2td. Then the sums of elements in the pairs in the components $X_o, X_{2d}, \ldots, X_{(2t-2)d}$ are non-zero.

Suppose that $x^{2id+j}(1+x^d) = x^{2i'd+j'}(1 + x^d)$; where $0 \leq i, i' \leq t - 1$ and $0 \leq j, j' \leq d - 1$. By similar argument that we have shown in case 1. we shall have $i = i'$ and $j = j'$.

Therefore the theorem follows.

Q.E.D.

Theorem 3.1.5 If p is an odd prime such that $p^n = 2^k t + 1$, where t is an odd integer greater than 1 and k is a positive integer, then there is a Room Square of side p^n .

Proof. This theorem follows from theorems 3.1.2, 3.1.3, 3.1.4.

Q.E.D.

Corollary 3.1.6 There is a Room Square of side p, where p is an odd prime and $p = 2^k t + 1$; where k is a positive integer, t is an odd integer greater than 1.

Proof. This corollary is just a special case (n = 1) of theorem 3.1.5 .

Q.E.D.

3.2 Construction of Room Square of side $5p^n$ where p is an odd prime and p^n can be written in the form $p^n = 2^k t + 1$, where t is an odd integer greater than 1.

Theorem 3.2.1 If G is a finite abelian group of order relatively prime to 6, which admits a strong starter, then there is a strong starter in the direct sum of G with the cyclic group of order 5.

Proof. Let us write n = 2s + 1 for the order of G. Since G is finite abelian group, then it is a direct sum of cyclic group, we can interpret any cyclic group of order m as the ring of integer modulo m under addition, and consider G as the additive group of the direct sum of these rings. In this way we endow G with a multiplication. This multiplication will have an identity element, 1 say ;. We write 1 + 1 as 2 and 1 + 1 + 1 as 3 and 2^{-1} and 3^{-1} will exist since $(n,6) = 1$.

Let the strong starter in G be

$$X = (\{x_1, y_1\}, \{x_2, y_2\}, \ldots\ldots, \{x_s, y_s\}).$$

Choose two non-zero elements a and b of G such that neither a nor b equals $x_i + y_i$ for any i . This can be done as there are s elements in the set of sums of X, while there are 2s - non - zero elements of G and $s \geqslant 3$.

$$\text{Write} \quad h = 2^{-2}(b-a) \quad \text{and} \quad g = 2^{-1}a .$$

Finally, partition the set of non-zero elements of G into two classes P and N, in such a way that $h \in P$, $-3^{-1}h \in P$ and $x \in P$ if and only if $-x \in N$.

For convenience, we assume that $P = \{h, x_{11}, x_{12}, \ldots, x_{1l}\}$; $N = \{x_{21}, x_{22}, \ldots\ldots, x_{2m}\}$. We shall denote the elements of Z_5 by 0, 1, 2, 3, 4 and denote the elements of $G \oplus Z_5$ by (x, i), where $x \in G$ and $i \in Z_5$.

Now setting

$$A = (\{(x_1,0), (y_1,0)\}, \{(x_2,0), (y_2,0)\}, \ldots\ldots, \{(x_s,0), (y_s,0)\}),$$

$$B = (\{(x_{11}+g,1), (2x_{11}+g,2)\}, \{(x_{12}+g,1), (2x_{12}+g,2)\}, \ldots\ldots, \{(x_{1l}+g,1), (2x_{1l}+g,2)\}),$$

$$C = \Big(\{(x_{11}+g,4),\ (2x_{11}+g,3)\},\ \{(x_{12}+g,4),\ (2x_{12}+g,\ 3)\}, \ldots\ldots,$$
$$\{(x_{11}+g,4),\ (2x_{11}+g,3)\} \Big),$$

$$D = \Big(\{(x_{21}+g,1),\ (2x_{21}+g,3)\},\ \{(x_{22}+g,1), (2x_{22}+g,3)\}, \ldots\ldots,$$
$$\{(x_{2m}+g,1),\ (2x_{2m}+g,3)\} \Big),$$

$$E = \Big(\{(x_{21}+g,4),\ (2x_{21}+g,2)\},\ \{(x_{22}+g,4),\ (2x_{22}+g,2)\}, \ldots\ldots,$$
$$\{(x_{2m}+g,4),\ (2x_{2m}+g,2)\} \Big),$$

$$F = \Big(\{(h+g,1),\ (g,2)\},\ \{(h+g,4),\ (g,3)\},\ \{(g,1),\ (g,4)\},$$
$$\{(2h+g,2),\ (2h+g,3)\} \Big).$$

We claim that $X^* = (A, B, C, D, E, F)$ is a strong starter for $G \oplus Z_5$. To prove that X^* is a starter, we must show that every non-zero elements of $G \oplus Z_5$ occurs in one component of X^* and that the set of all differences between elements of pairs in the components of X^* also consists of non-zero elements of $G \oplus Z_5$.

Since X is a starter, we see that each non-zero element of $G \oplus Z_5$ of the form $(x,0)$ appears precisely once in some pair in the components of A.

Since $x + g$ will run over G as x runs over G, hence each element of the form $(x,1)$ appears precisely once in one of B, D or F.

Since $2x + g$ will run over G as x runs over G, hence each element of the form $(x,2)$ appears exactly once in B, D or F. Similarly all elements of the form $(x, 3)$, and $(x,4)$ appear exactly once.

Next we shall that all non-zero elements also occur as the difference of pairs in the components of X^*.

Again, since X is a starter, it follows that all elements of the form (x,0) occur as differences of pairs in the components of A.

Observe that from B and C we can obtain the difference

$$(x_{1i},1) = (2x_{1i}+g,2) - (x_{1i}+g,1), \text{ and}$$

$$-(x_{1i},1) = (x_{1i}+g,1) - (2x_{1i}+g,2) .$$

Since $x_{1i} \in P$, hence $-x_{1i} \in N$. The only elements of $G \oplus Z_5$ of the form (x,1) which are not among the $(x_{1i},1)$ and $-(x_{1i},1)$ are (0,1),(h,1) and (-h,1). However, these elements can be seen to be the differences of pairs in F

$$(0,1) = (2h+g,3) - (2h+g,2) ,$$

$$(h,1) = (h+g,4) - (g,3) ,$$

$$(-h,1) = (g,2) - (h+g,1) .$$

The remaining non-zero elements of $G \oplus Z_5$ can be seen to be differences of elements in the pair in X^* in the same way as those of the form (x,1). It can be seen that all the elements of the form (x,2) can be written as differences of elements in the pairs of B, E, and F .

All the elements of the form (x,3) can be written as difference of elements in the pair of D, E and F.

All the elements of the form (x,4) can be written as differences of elements in the pair of B, C and F.

So X^* is a starter of $G \oplus Z_5$.

We complete the proof by showing that the starter X^* is strong.

We shall show that the sums of elements in pairs in the components of X^* are all distinct and non-zero elements of $G \oplus Z_5$. The sums of elements in the pairs in A have the form $(x_i + y_i, 0)$. Since X is a strong starter. Hence $x_i + y_i$; $i = 1, 2, \ldots, s$ are non-zero and distinct.

Hence the sums of elements in the pair in the components of A are non-zero and distinct.

The sums of elements in the pairs in the components of B are of the form $(3x + 2g, 3)$ where $x \in P$ and $x \neq h$. Similarly the sums of elements in the pairs in the components C are of the form $(3x + 2g, 2)$ where $x \in P$ and $x \neq h$.

Similarly the sums of elements in the pairs in the components D, and F are of the form $(3x + 2g, 4)$ and $(3x + 2g, 1)$ for $x \in N$.

Clearly all the elements of the forms $(3x + 2g, 3), (3x + 2g, 2)$, $(3x + 2g, 4)$ and $(3x + 2g, 1)$ are non-zero.

Suppose that $3x + 2g = 3x_1 + 2g$ where $x_1 \neq x$. Then we have $3x = 3x_1$. Since 3^{-1} exists. Hence $x_1 = x$.

Therefore all elements of the form $(3x + 2g, 3), (3x + 2g, 2), (3x + 2g, 4)$ and $(3x + 2g, 1)$ are distinct and non-zero.

Finally the sums of the pair from F are $(h + 2g, 3), (h + 2g, 2) (2g, 0)$ and $(4h + 2g, 0)$. These are distinct from the other sums. Suppose that $(h + 2g, 3)$ is among the above sums.

Hence $(h + 2g, 3) = (3x + 2g, 3)$ for some $x \in P$, and $x \neq h$.

Therefore we have must
$$h + 2g = 3x + 2g,$$
$$h = 3x,$$
$$3^{-1}h = x .$$

This shows that $3^{-1}h \in P$, which is a contradiction. Hence $(h + 2g, 3)$ is distinct from the other sums. The same argument shows that $(h + 2g, 2)$ are distinct from the other sums.

Suppose that $(2g, 0)$ is among the above sums.

Hence $(2g, 0) = (x_i + y_i, 0)$ for some $\{x_i, y_i\}$ in X.

Therefore $a = 2g = x_i + y_i$, which is contrary to the choice of a.

Hence $(2g, 0)$ is not among the above sums. Similarly we can show that $(4h + 2g, 0)$ is distinct from the other sums.

Therefore $X^* = (A, B, C, D, E, F)$ is a strong starter for $G \oplus Z_5$.

Q.E.D.

<u>Theorem 3.2.2</u> If p is an odd prime such that $p^n = 2^k t + 1$; where k is a positive integer, and t is an odd integer greater than 1, then there is a Room Square of side $5p^n$.

<u>Proof</u>. This theorem follows from theorems 3.2.1, 3.1.2, 3.1.3 and 3.1.4 .

Q.E.D.

<u>Corollary 3.2.3</u>. If p is an odd prime and such that $p = 2^k t + 1$, where k is a positive integer and t is an odd integer greater than 1, then there is a Room Square of side $5p$.

<u>Proff.</u> This Corollary is just a special case $n = 1$ of theorem 3.2.2 .

Q.E.D.