CHAPTER VI

ROOM SQUARES AND FERMAT NUMBERS

Definition 6.1 A number in the form $2^{2^k} + 1$ where k is a non-negative integer is called a Fermat number and we shall denote this number by F_k.

6.2 Existence of Room Square of side F_k except $k = 0,1,3$.

Lemma 6.2.1 If there exists a Room Square of side $2^d + 1$ and a Room Square of side $2^{a+d} + 1$ with a subsquare of side $2^a + 1$, then there is a Room Square of side $2^{a+md} + 1$ with a subsquare of side $2^{a+(m-1)d} + 1$ for $m = 1,2,,\ldots$

Proof. We proceed by induction on m. The case $m = 1$ follows immediately from the hypothesis of the lemma.

Suppose the case $m = k$ is true, so that there is a Room Square of side $2^{a+kd} + 1$ with a subsquare of side $2^{a+(k-1)d} + 1$.

Observe that

$$2^{a+(k+1)d} + 1 = (2^d+1)\left[(2^{a+kd} + 1) - (2^{a+(k-1)d} + 1)\right] + (2^{a+(k-1)d} + 1).$$

To apply theorem 4.1.2 we must show that $(2^{a+kd}) + 1) - (2^{a+(k-1)d} + 1) \neq 2$ or 6

Observe that $(2^{a+kd} + 1) - (2^{a+(k-1)d} + 1) = 2^{a+(k-1)d}.[2^d - 1]$.

Since the existence of Room Squares of sides $2^d + 1$ and $2^a + 1$ are assumed, hence $a, d \neq 0,1,2$. Therefore $2^d - 1 > 6$. Therefore

$$(2^{a+kd} + 1) - (2^{a+(k-1)d} + 1) \neq 2 \text{ or } 6 .$$

Therefore by theorem 4.1.2 , the case $m = k+1$ is true

Hence the lemma holds.

Q.E.D.

<u>Lemma 6.2.2</u> If there exist Room Squares of sides $x + 1$, $x - 1$ and $x^2 + 1$, then there exists a Room Square of side $x^{2n+3} + 1$ with a subsquare of side $x^2 + 1$ for $n = 1, 2, 3, \ldots\ldots$

<u>Proof.</u> Since Room Squares of sides $x + 1$ and $x - 1$ exist. Hence x must be even and $x + 1 \neq 3, 5$ and $x - 1 \neq 5$. Therefore $x \neq 2$ or 4 or 6 . Hence $x > 6$

For $n = 0, 1, 2, \ldots\ldots$ we define

$$S_o = x^2 - x + 1 ,$$

$$S_n = x^{2n+2} - x^{2n+1} + S_{n-1} , \quad n = 1, 2, \ldots .$$

We can shown by induction on n that

$$(x+1)S_n = x^{2n+3} + 1 \quad \text{and} \quad S_{n+1} - S_n > 6 \quad \text{for all} \quad n = 0,1,2,\ldots .$$

For each $n = 1, 2, \ldots$, let $S(n)$ be the statement that there exists a Room Square of side S_n with subsquares of sides S_{n-1} and $x^2 + 1$.

Observe that $S_o = (x-1)\left[(x+1) - 1\right] + 1$, and that [illegible]1, –

$(x+1) - 1 = x \neq 2$ or 6 .

Therefore by theorem 4.1.2, there is a Room Square of side

$(x-1)\left[(x+1) - 1\right] + 1 = S_o$.

Since a Room Square of side $x^2 + 1$ exists and a Room Square of side S_0 with a subsquare of side 1. exists. Furthermore

$S_o - 1 = x(x-1) > 6.(6-1)$, hence $S_o - 1 \neq 2$ or 6.

Therefore by theorem 4.1.2 there is a Room Square of side

$(x^2 + 1)(S_o - 1) + 1 = S_1$ with a subsquares of sides $x^2 + 1$ and S_o.

Therefore $S(1)$ holds.

Suppose that $S(k)$ is true, that is there exists a Room Square of side S_k with subsquares of sides S_{k-1} and $x^2 + 1$.

We observe that

$$S_{k+1} = x^{2k+4} - x^{2k+3} + x^{2k+2} - x^{2k+1} + S_{k-1},$$

$$= (x^2 + 1)\left[S_k - S_{k-1} \right] + S_{k-1} .$$

So, by theorem 4.1.2, there exists a Room Square of side S_{k+1} with subsquares of sides S_k and $x^2 + 1$.

Hence $S(k+1)$ is true. Therefore the lemma holds.

Q.E.D.

<u>Lemma 6.2.3</u> If F_k is not prime, then there is a Room Square of side F_k. In particular there are Room Squares of sides F_5, F_6, F_7 and F_8.

<u>Proof</u>. It can be proved by induction on n that

$$(*) \qquad F_n = F_{n-1} \cdot F_{n-2} \cdots\cdots F_2 \cdot F_1 \cdot F_0 + 2, \quad \text{for all}$$

non-negative integers n. Assume that F_k is composite. Hence it has a factorization into primes :

$$F_k = p_1 p_2 \cdots\cdot p_t \, .$$

From a (*), we see that none of the prime factors p_i of F_k is of the form $p_i = 2^{2^q} + 1$. Hence by appendrix 1. all p_i must be of the form $p_i = 2^q t_i + 1$ where $t_i > 1$. By corollary 3.1.6, there is a Room Square of side p_i for all i. So, by theorem 4.1.4, there is a Room Square of side F_k .

According to [2] it is known that F_5, F_6, F_7 and F_8 are composite. Hence by Lemma 6.2.3 there are Room Square of sides F_5, F_6, F_7 and F_8.

Q.E.D.

Lemma 6.2.4 Room Square of side 17 exist.

Proof. We prove by displaying Room Square of side 17

0,1			12,7	10,9	16,3		17,2			6,13	11,8		4,15		4,15	
	0,2			13,8	11,10	17,4		1,3			7,14	12,9		5,16		15,
16,7		0,3			14,9	12,11	1,5		2,4			8,15	13,10		6,17	
	17,8		0,4			15,10		2,6		3,5				14,11		7,
8,2		1,9		0,5			16,11		3,7		4,6				15,12	
	9,3		2,10		0,6			17,12		4,8		5,7				16,
17,14		10,4		3,11		0,7			1,13		5,9		6,8			
	1,15		11,5		4,12		0,8			2,14		6,10		7,9		
		2,16		12,6		5,13		0,9			3,15		7,11		8,10	
			3,17		13,7		6,14		0,10			4,16		8,12		9,
10,12				4,1		14,8		7,15		0,11			5,17		9,13	
	11,13				5,2		15,9		8,15		0,12			8,1		10
11,15		12,14				6,3		16,10		9,17		0,13			7,2	
	12,16		13,15				7,4		17,11		10,1		0,14			8,
9,4		13,17		14,16				8,5		1,12		11,2		0,15		
	10,5		14,1		15,17				9,6		2,13		12,3		0,16	
		11,6		15,2		16,1				10,7		3,14		13,4		0,

Figure 6.1

This Room Square is found by R.C. Mullin by using computer search [10].

Lemma 6.2.5 There are Room Square of sides F_2, F_4 and $F_5 - 2$.

Proof. From Lemma 6.2.4 we see that Room Square of side $F_2 = 17$ exists,

Observe that the following identitys holds;

(1) $77 = 7.11$,

(2) $989 = 13(77 - 1) + 1$,

(3) $F_4 = 65537 = 67(989 - 11) + 11$.

By Corollary 3.1.6, there exist Room Square of side 7, 11, 13 and 67 .

From (1) and theorem 4.1.3, it follows that Room Square of side 77 with subsquare of side 11 exists .

From (2) and theorem 4.1.2, it follows that Room Square of side 989 with subsquare of side 77, which in turn has a subsquare of side 11, exists.

From (3) and theorem 4.1.2 , it follows that Room Square of side $F_4 = 65537$ exists.

By theorem 3.1.5 there exist Room Square of sides 47 and 83. Hence, by 4.1.2 there exists a Room Square of side $3855 = 47(83 - 1) + 1$.

Since $F_5 - 2 = 65537.17 . 3855$.

Hence by theorem 4.1.4 , there is a Room Square of side $F_5 - 2$.

Q.E.D.

<u>Theorem 6.2.6</u> There is a Room Square of side F_k unless $k = 0, 1, 3$.

<u>Proof</u> Lemma 6.2.3 and 6.2.5 garantee the existence of Room Square of sides F_2, F_4, F_5, F_6, F_7 and F_8.

Hence we need only to discuss the case $k > 8$.

Let $x = 2^{32}$, hence $F_k = x^{4(2^{k-7})} + 1$. The case $F_6 = x^2 + 1$, $F_5 = x + 1$. and $F_5 - 2 = x - 1$, so from lemma 6.2.3 and 6.2.5, there are Room Square of side $x^2 + 1$, $x + 1$ and $x - 1$. So by lemma 6.2.2 there is a Room Square of side $x^{2n+3} + 1$ with a subsequare of side $x^2 + 1$ for $n \geq 1$.

Letting $a = 64$ and $d = 64n + 32$, in lemma 6.2.1 we see that the existence of a Room Square of side $2^d + 1 = 2^{64n+32} + 1$ $= x^{2n+} + 1$ and a Room Square of side $2^{a+d} + 1 = 2^{96 + 64n} + 1$ $= x^{2n+3} + 1$ with a subsquare of side $2^a + 1 = 2^{64} + 1 = x^2 + 1$ implies the existence of Room Square of side

$2^{a+md} + 1 = 2^{64 + m(64n+32)} + 1 = x^{2 + (2n+1)m} + 1$ for $m \geq 0$.

In particular when $m = 2$, the Room Square of side $x^{4(n+\ )} + 1$ exists. Since there exists a Room Square of side $x^{2n+3} + 1$ with subsquare of side $x^2 + 1$ for every $n \geq 1$. Hence there exists a Room Square of side $x^{2(n-1)+3} + 1 = x^{2n+1} + 1$ with subsquare of side $x^2 + 1$ for every $n \geq 2$. So the existence of Room Square of side $x^{2n+1} + 1$ and a Room Square of side $x^{2n+3} + 1$ with a subsquare of side $x^2 + 1$

implies the existence of Room Square of side $x^{4(n+1)} + 1$ for $n \geq 2$.

Since $2^{k-7} = n+1$, hence $2^{k-7} \geq 3$, that is $k \geq 9$.

Therefore there is a Room Square of side F_k unless $k = 0, 1, 3$.

Q.E.D.

6.3 Existence of Room Square of side $F_3 = 257$.

Theorem 6.3.1 Suppose there is a Room Square of side r with a subsquare of side s; where $r - s \neq 2, 4,$ or 12. Then there is a Room Square of side $5(r-s) + s$ with subsquares of sides r and s.

Proof. Observe that if $r = s$, we have $5(r-s) + s = s$. In this case the theorem is trivial. Hence we assume $s < r$.

Let $\mathcal{R}^{(1)}$ be a Room Square of side r with a subsquare $\bar{\mathcal{R}}$ of side s. Since r and s are odd integers, hence $r - s$ is even. Let us write $r - s = 2n$, where n is a positive integer.

We may assume that $\mathcal{R}^{(1)}$ is standardized and based on $\{0,1,2,\ldots\ldots, 2n, 2n+1, \ldots\ldots, 2n+s\}$ and $\bar{\mathcal{R}}$ is based on $\{0, 2n+1,\ldots\ldots, 2n+s\}$, whence $\bar{\mathcal{R}}$ occupied the last s rows and the last s columns of $\mathcal{R}^{(1)}$, hence we may represent $\mathcal{R}^{(1)}$ as follows :

$$\mathcal{R}^{(1)} = \begin{array}{|c|c|} \hline A^{(1)} & A^{(2)} \\ \hline A^{(3)} & \bar{\mathcal{R}} \\ \hline \end{array}$$

Figure 6.2

where $A^{(1)}$, $A^{(2)}$, $A^{(3)}$ are some arrays.

We shall build a Room Square $\mathcal{R}^*$ of side $5(r-s) + s = 10n + s$ based on $S = \{0, 1_0, 2_0, \ldots (2n)_0, 1_1, 2_1, \ldots, (2n)_1, \ldots\ldots 1_4, 2_4, \ldots (2n)_4, 2n+1, \ldots, 2n+s\}$.

Let $\mathcal{L} = \{0, 2n+1, \ldots, 2n+s\}$, let $R^{**} = \{1, 2, \ldots, 2n\}$ and for $i = 0,1,2,3,4$ let $R_i = \{1_i, 2_i, \ldots, (2n)_i\}$.

For each $j = 1,2,3$, let us construct arrays $A_i^{(j)}$; $i = 0,1,2,3,4$, of the same size as that of $A^{(j)}$ as follows :-

Let
$$g_i(x) = \begin{cases} x_i & \text{if } 0 < x \leq 2n \\ x & \text{otherwise.} \end{cases}$$

For each $j = 1,2,3$, whenever $\{x, y\}$ occurs in $A^{(j)}$ we place $\{g_i(x), g_i(y)\}$ in the same position in $A_i^{(j)}$.

Since $r - s = 2n \neq 2, 4$, or 12. Hence $n \neq 1, 2$ or 6. Therefore there exists a pair of orthogonal Latin Square of order n.

Let P and Q be a orthogonal Latin Squares of order n based on $\{1, 2, \ldots, n\}$.

$$\text{Let} \qquad h_i(x) = \begin{cases} x_i & \text{if } 1 \leq i \leq 4 \\ (x+n)_{i-5} & \text{if } 5 \leq i \leq 9 . \end{cases}$$

For each i ; $1 \leq i \leq 9$, let P_i be obtained from P by replacing every entry x by $h_i(x)$. Similary for Q_i be obtained from Q as the same fashion.

For $i, j = 1, \ldots, 9$, let L_{ij} be an n x n array obtained by replacing each entry (x, y) of (P_i, Q_j) by $\{x, y\}$.

We now arrange all the arrays $A_i^{(j)}$ ' s L_{ij} ' s into a new array $\mathcal{K}^*$ as follows :

$\mathcal{R}^* =$

<table>
<tr><td colspan="2" rowspan="2">$A_0^{(1)}$</td><td>L_{24}</td><td></td><td>L_{39}</td><td></td><td>L_{67}</td><td></td><td>L_{18}</td><td></td><td rowspan="2">$A_0^{(2)}$</td></tr>
<tr><td></td><td>L_{79}</td><td></td><td>L_{34}</td><td></td><td>L_{12}</td><td></td><td>L_{68}</td></tr>
<tr><td>L_{47}</td><td></td><td colspan="2" rowspan="2">$A_1^{(1)}$</td><td></td><td>L_{08}</td><td></td><td>L_{59}</td><td></td><td>L_{23}</td><td rowspan="2">$A_1^{(2)}$</td></tr>
<tr><td></td><td>L_{29}</td><td>L_{58}</td><td></td><td>L_{04}</td><td></td><td>L_{37}</td><td></td></tr>
<tr><td></td><td>L_{48}</td><td></td><td>L_{03}</td><td colspan="2" rowspan="2">$A_2^{(1)}$</td><td>L_{19}</td><td></td><td>L_{56}</td><td></td><td rowspan="2">$A_2^{(2)}$</td></tr>
<tr><td>L_{89}</td><td></td><td>L_{35}</td><td></td><td></td><td>L_{46}</td><td></td><td>L_{01}</td></tr>
<tr><td>L_{26}</td><td></td><td>L_{09}</td><td></td><td>L_{14}</td><td></td><td colspan="2" rowspan="2">$A_3^{(1)}$</td><td></td><td>L_{57}</td><td rowspan="2">$A_3^{(2)}$</td></tr>
<tr><td></td><td>L_{17}</td><td></td><td>L_{45}</td><td></td><td>L_{69}</td><td>L_{02}</td><td></td></tr>
<tr><td>L_{13}</td><td></td><td>L_{78}</td><td></td><td>L_{06}</td><td></td><td>L_{25}</td><td></td><td colspan="2" rowspan="2">$A_4^{(1)}$</td><td rowspan="2">$A_4^{(2)}$</td></tr>
<tr><td></td><td>L_{36}</td><td></td><td>L_{28}</td><td></td><td>L_{15}</td><td></td><td>L_{07}</td></tr>
<tr><td colspan="2">$A_0^{(3)}$</td><td colspan="2">$A_1^{(3)}$</td><td colspan="2">$A_2^{(3)}$</td><td colspan="2">$A_3^{(3)}$</td><td colspan="2">$A_4^{(3)}$</td><td>$\bar{\mathcal{R}}$</td></tr>
</table>

Figure 6.3

We shall show that $\mathcal{R}^*$ is a Room Square of side $10n + s$ based on S. It is clear from the construction of $\mathcal{R}^*$ that each cell of $\mathcal{R}^*$ that each cell of $\mathcal{R}^*$ may be empty or contain two distinct elements of S.

Next, we shall show that each row of $\mathcal{R}^*$ contains all elements of S precisely once.

Let $1 \leq i \leq 10n + s$. Let a be any element of S. We claim that a appears in row i precisely once.

First, we consider the case $1 \leq i \leq n$. Assume that $a \in R_0 \cup \mathcal{L}$

We first observe that the array $K = \boxed{A^{(1)} \mid A^{(2)}}$ is the first 2n rows of $\mathcal{R}$. Therefore row i of K contains all elements of $R^{**} \cup \mathcal{L} = \{0, 1, 2, \ldots, 2n, 2n+1, \ldots, 2n+s\}$ precisely once. Using this fact together with the definition of $A_0^{(1)}$, $A_0^{(2)}$, we see that row i of the array $K^* = \boxed{A_0^{(1)} \mid A_0^{(2)}}$ contains all elements of $R_0 \cup \mathcal{L} = \{0, 1_0, 2_0, \ldots, (2n)_0, 2n+1, \ldots, 2n+s\}$ precisely once. Therefore each element of $R_0 \cup \mathcal{L} = \{0, 1_0, 2_0, \ldots, (2n)_0\ 2n+1, \ldots, 2n+s\}$ appears precisely once in the row i of $\mathcal{R}^*$. Hence a appears in row i of $\mathcal{R}^*$. Now, if $a \notin R_0 \cup \mathcal{L}$, then $a \in R_1 \cup R_2 \cup R_3 \cup R_4$.

Assume that $a \in R_1$. Therefore $a = x_1$; where $1 \leq x \leq 2n$. By the construction of L_{18} from (P_1, Q_8) we see that row i of L_{18} contains $a = x_1$, where $1 \leq x \leq n$ precisely once. By the same reason, we see that row i of L_{67} contains $a = x_1$ where $n < x \leq 2n$ precisely once. Hence row i of the array $\boxed{L_{67} \mid L_{18}}$ contains all elements of R_1 precisely once.

We observe that $a = x_1$ can not appear in L_{24} and L_{39} because the entries in L_{24} and L_{39} are of the form $\{x_2, y_4\}$ and $\{x_3, (y+n)_4\}$ respectively.

Therefore $a = x_1$ appears precisely once in row i of $\mathcal{R}^*$. By the same arguments we shall show that if $a = x_2$ or $a = x_3$ or $a = x_4$ a will appear precisely once in row i of $\mathcal{R}^*$. Therefore $a \in S$ appears precisely once in row i of $\mathcal{R}^*$. By similar argument, it can be seen that what we claim holds for the case $n < i \leq 10n$.

Now, assume that $10n < i \leq 10n + s$. Row i is one of the last s - rows of $\mathcal{R}^*$. We first observe that the array $S^* = \boxed{A^{(3)}} \boxed{\bar{\mathcal{R}}}$ consists of the last s - row of $\mathcal{R}^{(1)}$. Therefore each row of S contains all elements of $\bar{R}^{**} \cup \mathcal{L} = \{0, 1, 2, \dots, 2n, 2n+1, \dots, 2n+s\}$ precisely once. Using this fact together with the definition of $A_i^{(3)}$, $i = 0,1,2,3,4$, we see that row i of the array

$$S^{**} = \boxed{A_0^{(3)}}\boxed{A_1^{(3)}}\boxed{A_2^{(3)}}\boxed{A_3^{(3)}}\boxed{A_4^{(3)}}\boxed{\bar{\mathcal{R}}}$$

contains all elements of S precisely once.

Therefore row i of $\mathcal{R}^*$ contains all elements of S precisely once.

Similar proof is appied to columns.

It remains to be shown that every unordered pair of elements of S appears precisely once in $\mathcal{R}^*$.

Let u, t be any two distinct elements of S . We shall show that $\{u, t\}$ must appear in some cell of $\mathcal{R}^*$.

If one of the element of $\{u, t\}$ is 0, say $u = 0$, then $t = x_i$ where $1 \leq x \leq 2n$; $0 \leq i \leq 4$ or $t = 2n + z$ for $0 < z \leq s$.

If $t = x_i$, then $\{u, t\} = \{0, x_i\}$ appears in some cell of $A_i^{(1)}$ which is a subarray of $\mathcal{R}^*$. Therefore $\{u, t\} = \{0, x_i\}$ appears in some cell of $\mathcal{R}^*$.

If $t = 2n+z$, then $\{u, t\} = \{0, 2n+z\}$ appears in some cell of $\overline{\mathcal{R}}$ which is a subarray of $\mathcal{R}^*$. Therefore $\{u, t\} = \{0, 2n+z\}$ appears in some cell of $\mathcal{R}^*$.

If none of the element of $\{u, t\}$ is 0, then $u = x_i$ or $2n + z_1$ and $t = y_j$ or $2n + z_2$ where $0 \leq i, j \leq 4$; $1 \leq x, y \leq 2n$ and $0 < z_1 , z_2 \leq s$.

If $u = x_i$ and $t = y_j$; where $1 \leq x, y \leq n$, then $\{s, t\} = \{x_i, y_j\}$ appears in L_{ij} which is a subarray of $\mathcal{R}^*$. Therefore $\{u, t\} = \{x_i, y_j\}$ appears in some cell of $\mathcal{R}^*$.

If $u = x_i$ and $t = y_j$; where $n < x, y \leq 2n$ then $\{u, t\} = \{x_i, y_j\}$ appears in $L_{i+5\ j+5}$ which is a subarray of $\mathcal{R}^*$. Therefore $\{u, t\} = \{x_i, y_j\}$ appears in some cell of $\mathcal{R}^*$.

If $u = x_i$ and $t = y_j$; where $1 \leq x \leq n$ and $n < y \leq 2n$ then $\{u, t\} = \{x_i, y_j\}$ appears in L_{ij+5} which is a subarray of $\mathcal{R}^*$.

Therefore $\{u, t\} = \{x_i , y_j\}$ appears in some cell of $\mathcal{R}^*$.
If $u = x_i$ and $t = y_j$; where $n < x \leq 2n$ and $1 \leq y \leq n$, then $\{u , t\} = \{x_i, y_j\}$ appears in $L_{i+5\ j}$ which is a subarray of $\mathcal{R}^*$.
Therefore $\{u, t\} = \{x_i, y_j\}$ appears in some cell of $\mathcal{R}^*$.
If $u = x_i$ and $t = 2n + z_2$ where $1 \leq x \leq 2n$ and $z_2 > 0$, then $\{u, t\} = \{x_i, 2n+z_2\}$ appears in $A_i^{(1)}$ or $A_i^{(2)}$ which are subarrays of $\mathcal{R}^*$. Therefore $\{u , t\} = \{x_i , 2n+z_2\}$ appears in some cell of $\mathcal{R}^*$.
If $u = 2n+z_1$ and $t = y_j$ where $1 \leq y \leq n$ and $z_1 > 0$, then $\{u , t\} = \{2n+z_1 , y_j\}$ appears in $A_j^{(1)}$ or $A_j^{(2)}$ which are subarrays of $\mathcal{R}^*$. Therefore $\{u , t\} = \{2n+z_1 , y_j\}$ appears insome cell of $\mathcal{R}^*$.
If $u = 2n+ z_1$ and $t = 2n+z_2$ where $z_1 , z_2 > 0$, then $\{u , t\} = \{2n + z_1 , 2n + z_2\}$ appears in $\bar{\mathcal{R}}$ which is a subarray of $\mathcal{R}^*$.
Therefore $\{u , t\} = \{2n + z_1 , 2n + z_2\}$ appears in some cell of $\mathcal{R}^*$.
Therefore every unordered pair of elements of S appears in $\mathcal{R}^*$ at least once Now, we shall that each unordered pair of elements of S appears at most once in $\mathcal{R}^*$.

Since each $A^{(1)}$ and $A^{(2)}$ together contains $\frac{1}{2}(2n + s + 1)$ pairs per row. Hence $A_i^{(1)}$ and $A_i^{(2)}$ together contains $\frac{1}{2}(2n + s + 1)$ pairs per row. Each row of L_{ij} contains n pairs. Each row of $A_i^{(3)}$ contains $\frac{1}{2}(2n)$ pairs and $\bar{\mathcal{R}}$ contains $\frac{1}{2}(s + 1)$ pair per row.
So, the number of pairs in $\mathcal{R}^*$ is

$$10n \left[\frac{1}{2}(2n + s + 1) + 4n \right] + s \left[\frac{1}{2}(s + 1) + \frac{5}{2}(2n) \right]$$
$$= \frac{1}{2}\left[20n^2 + 10ns + 10n + 80n^2 \right] + \frac{1}{2}\left[s^2 + s + 10ns \right]$$
$$= \frac{1}{2}\left[10n + s \right] . \left[10n + s + 1 \right] .$$

This is precisly the number of unordered pair which can be formed from S,

so each unordered pair of elements of S appears at most once in $\mathcal{R}^*$.
Therefore $\mathcal{R}^*$ is a Room Square of side $10n+s$ and based on S.

Finally, observe that subarray

$A_4^{(1)}$	$A_4^{(2)}$
$A_4^{(3)}$	$\bar{\mathcal{R}}$

and $\bar{\mathcal{R}}$ are the requires subsquares of sides r and s.
Therefore the theorem follows.

Q.E.D

Lemma 6.3.2 Room Square of side 9 exists.

Proof We prove by displaying Room Square of side 9.

0,1	6,9	4,8					5,7	2,3
3,4	0,2	7,1	5,9					6,8
7,9	4,5	0,3	8,2	6,1				
	8,1	5,6	0,4	9,3	7,2			
		9,2	6,7	0,5	1,4	8,3		
			1,3	7,8	0,6	2,5	9,4	
				2,4	8,9	0,7	3,6	1,5
2,6					3,5	9,1	0,8	4,7
5,8	3,7					4,6	1,2	0,9

Figure 6.4

This Room Square is found by R.C. Mullin by using computer search[10].

Corollary 6.3.3 There exists a Room Square of side 257.

Proof. By lemma 6.3.2, there is a Room Square of side 9 with subsquare of side 1. By Corollary 3.1.6, there is a Room Square of side 7. Hence by theorem 4.1.2 there is a Room Square of side $7(9 - 1) + 1 = 57$, with subsquare of side 7. Therefore by theorem 6.3.1 there is a Room Square of side $5(57 - 7) + 7 = 257$.

Therefore the Corollary follows.

Q.E.D