Introduction

The theorem which will ultimately be established in section 4 relies upon a fundamental theorem in number theory – in fact **the** fundamental theorem. The Fundamental Theorem of Arithmetic states that every positive integer, except 1, can be expressed uniquely as a product of primes.

Proof of this theorem can be found in [11, section 2.10].

The proof which established the existence of Room squares will rely upon various other theorems which collectively establish the existence of all Room squares with prime side, except 3 and 5. Then multiplication theorems will be developed to establish the existence of composite Room squares (those whose side is the product of two or more primes). Clearly if the prime Room squares can be proven to exist, and hence composite Room squares, the fundamental theorem will allow us to state that all Room squares exist with odd positive integer side. Apart from a few exceptional cases, this is basically what we wil be able to do.

Starters, Adders and Cyclic Room Squares

	0	1	2	3	4	5	6
0	∞0			25		16	34
1	45	∞1			36		20
2	31	56	∞2			40	
3		42	60	∞3			51
4	62		53	01	∞4		
5		03		64	12	∞5	
6			14		05	23	∞6

Figure 16 Cyclic Room square

The Room square in Figure 16 has a special property. The pairs in any element of the array are obtained by simply adding 1 (mod 7) to the pair in the element immediately above and to the left; along with the condition that

$$\infty + 1 = \infty$$

This special property means that the entire square can be determined by the pairs in the first row, with successive rows being developed in a cyclical manner according the simple addition rule. We call squares like the one in Figure 16 *cyclic* Room squares.

Also notice that $\{\infty, i\}$ occurs in position (i, i). A square with this property is said to be *standardised*. It is important to realise that any Room square can be standardised. As mentioned previously neither interchanging the rows or columns nor permuting the symbol-set on which the Room square is based has any effect of the "Room"-ness of that square.

The significance of cyclic Room squares is that the problem of constructing a Room square is (potentially) reduced to that of finding an appropriate first row. These rows cannot be chosen arbitrarily, both the pairs used and the positions in which they appear need to satisfy certain criteria, but when they do exist a corresponding Room square always exists. So proving the existence of this subclass of Room squares is a matter only of proving the existence of these special first rows.

Finding a starter

Suppose we wish to construct another Room square of the same size as Figure 16 based on the same symbols. This new square will also be standardized so we need only determine the three pairs that accompany $\{0, \infty\}$ in the first row (the starter), and the positions they occupy.

The set we will use to build our starter will be {1,2,...,6}.

Each member of this set must occur exactly once in the pairs of the starter − in order to satisfy the row condition for a Room square. Because of the cyclical construction the condition is automatically true for successive rows if true for the first.

Consider the existence in Figure 16 of an arbitrary pair $\{a,b\}$. We know one of the following must be true.

Either:

$$\{2+i,5+i\}=\{a,b\} \quad \text{or} \quad \{1+i,6+i\}=\{a,b\} \quad \text{or} \quad \{3+i,4+i\}=\{a,b\} \quad \text{for } i=0,1,2,...,6$$

Say $a-b=1$. Then $\{2+i,5+i\}=\{a,b\}$ could never be true because $(2+i)-(5+i)=-3$(mod \$ 7)=4\$ and $(5+i)-(2+i)=3$. Similarly, the differences in $\{1,6\}$ are ±5 so $\{a,b\}$ couldn't be generated from $\{1,6\}$.

However, $(4+i)-(3+i)=1$ so $\{a,b\}$ will inevitably be generated by $\{3,4\}$ for some value of $i=0,1,...,6$.
e.g. $\{2,3\}=\{3+6,4+6\}$

Because a and b separately take on all values from $\{0,1,2,...,6\}$, their differences will similarly take on all these values (except 0 because there are no pairs of the form $\{a,a\}$) and so an essential property for the starter must be that the six differences generated by its three pairs contain all of $\{1,2,...,6\}$.

When a starter satisfies this property, and the condition that the pairs contain in their union all of $\{1,2,...,6\}$, it is clear that it will inevitably generate the correct pairs which populate a 7x7 Room square. There are three pairs in the starter, each generates seven unique pairs under cyclical construction, which along with the seven pairs generated by $\{0,\infty\}$ counts for all the 28 unordered pairs from $\{\infty,0,1,...,6\}$.
A starter for larger Room squares of course has to obey the same criterion. We include a general definition based on [8]:
(1,0)450
Definition: If G is an additive Abelian group of order g, then a *starter* in G is a set of unordered pairs:

$$S=\{\{s_i,t_i\}:1\leq i\leq (g-1)/2\}$$

which satisfies these properties:

1. $\{s_i:1\leq i\leq (g-1)/2\}\cup\{t_i:1\leq i\leq (g-1)/2\}=G\backslash\{0\}$
2. $\{\pm(s_i-t_i):1\leq i\leq (g-1)/2\}=G\backslash\{0\}$

(1,0)450

Whenever we have any t sets $D_1,...,D_t$ each of size k in which each non-zero member of an additive abelian group can be represented as a difference between members of the $D_i\lambda$ times, we say those sets form a ***difference system***.
Much use will be made of difference systems throughout this work.
Notice that the definition of a starter presumes standardization, and therefore that $\{\infty,i\}$ is in position (i,i).
The following pairs form a starter in $G=\{0,1,2,...,6\}$ (an additive abelian group with order $g=7$.)

$$\{1,3\} \qquad \{2,6\} \qquad \{4,5\}$$

Property 1 is satisfied because $\{1,3\}\cup\{2,6\}\cup\{4,5\}=G\backslash\{0\}$
Property 2 is also satisfied because

$$\{1-3=5,3-1=2,2-6=3,6-2=4,4-5=6,5-4=1\}=\{1,2,3,4,5,6\}=G\backslash\{0\}$$

Hence

$\infty 0$	13	26	45
$\infty 1$	24	30	56
$\infty 2$	35	41	60
$\infty 3$	46	52	01
$\infty 4$	50	63	12
$\infty 5$	61	04	23
$\infty 6$	02	15	34

Table 1

are all the unordered pairs from $\{\infty, 0, 1, ...6\}$ sorted into seven rows that contain each of $\{\infty, 0, 1, ..., 6\}$ exactly once. ALl that remains is to determine the columns.

Finding an adder

In constructing the starter we made use of the fact that each row has to contain each symbol exactly once and all unordered pairs from the symbol set have to occur exactly once in the whole array. The remaining condition – namely, that each symbol must occur once in each column – is now employed to finish the construction.

Again, because of the cyclical nature of Room squares generated from starters we can be sure that if one column contains each member of the symbol set, all columns will.

Also, because we have decided to construct a standardized Room Square we know that column i contains $\{\infty, i\}$. So the final column (column 6) contains $\{\infty, 6\}$, and depending on where we place the starter pairs it will also include:

$$\{1,3\} + x \qquad \{2,6\} + y \qquad \{4,5\} + z$$

For some distinct values of x, y and z (only one pair allowed per box).
Considering that the new pairs to form column 6 must contain in their union each of $\{0, 1, 2, ..., 5\}$ we build the following table.

x	$13 + x$	y	$26 + y$	z	$45 + z$
0	13	0	26	0	45
1	24	1	30	1	56
2	35	2	41	2	60
3	46	3	52	3	01
4	50	4	63	4	12
5	61	5	04	5	23

Table 2

Our task is simply to determine three unique values for x, y and z such that $13 + x, 26 + y$ and $45 + z$ contain in their union each of $\{0, 1, 2, ..., 5\}$. These values will then determine the positions to place 13, 26 and 45 in row 1.

Choosing 4 from the first column corresponds to having 50 appear in the final column of the Room Square and forces the selection of $y = 2$ from the next column of the table, (41 being the only pair not containing any of the already used 5,6 or 0). 23 is the only possible choice from the final column, accompanied by a value of $z = 5$. These three numbers are known as an *adder* corresponding to the starter 13,26,45. This is not necessarily the only adder.

If 50 is to be generated in the final column of the Room square by the pair 13 in the first row, then 13 must go in column $7-4=3$. Similarly 26 has to be put in column $7-2=5$ and 45 in $7-5=2$. We can now construct our cyclic room square.

∞0	45	13	-	26	-	-
-	∞1	56	24	-	30	-
-	-	∞2	60	35	-	41
52	-	-	∞3	01	46	-
-	63	-	-	∞4	12	50
61	-	04	-	-	∞5	23
34	02	-	15	-	-	∞6

Figure 17

In general, we define an adder by considering the elements which must accompany $\{\infty, 0\}$ in column 0. Therefore an adder is defined in the following way:
(1,0)450
An *adder* for a starter $S = \{\{s_i, t_i\} : 1 \leq i \leq (g-1)/2\}$ is a set of $(g-1)/2$ distinct non-zero elements $a_1, a_2, ..., a_{(g-1)/2}$ of G such that: $s_1 + a_1, t_1 + a_1, s_2 + a_2, ..., s_{(g-1)/2} + a_{(g-1)/2}, t_{(g-1)/2} + a_{(g-1)/2}$ are precisely all the non-zero elements of G.
(1,0)450
The *starter-adder* method employed in the above example was introduced in 1968[^4] by Stanton and Mullin [23], who used it to construct Room squares of side 11. They also went on to apply the method to larger squares and gave the first real suggestions that the number of Room squares is infinite.

Two simple Lemmas given by Stanton and Mullin demonstrated that the problem of finding starters for larger Room squares was straightforward. In fact they can be guaranteed always to exist, and the only difficulty comes from finding a corresponding adder, which is not guaranteed to exist.

Lemma 3.2.1 In an additive abelian group G of order $g = 2n-1$, then pairs

$$\{n-1, n\}, \{n-2, n+1\}, \{n-3, n+2\}, \{n-4, n+3\}, ...\{1, 2n-2\}$$

are a starter for a Room square of side $2n-1$.

Example 3.2
A Room square of side $2n-1 = 19$.
$n = 10, G = Z_{19}$

The set of pairs
$S_{19} = \{\{9,10\}, \{8,11\}, \{7,12\}, \{6,13\}, \{5,14\}, \{4,15\}, \{3,16\}, \{2,17\}, \{1,18\}\}$
is a starter.

Indeed, the differences are
$\{\pm(10-9), \pm(11-8), \pm(12-7), \pm(13-6), \pm(14-5), \pm(3-16), \pm(2-17), \pm(18-1)\}$
$= \{1, 18, 3, 16, 5, 14, 7, 12, 9, 10, 8, 11, 6, 13, 4, 15, 2, 17\} = G \backslash \{0\}$

Lemma 3.2.2 In the Galois field of order $k-1$, with primitive root a the following pairs form a starter for a Room square of side k.

$$\{a, a^n\}, \{a^2, a^{n+1}\}, \{a^3, a^{n+2}\}, ..., \{a^{n-1}, a^{2n-2}\}$$

Example 3.3
A Room square of side $2n-1 = 23$. $n = 12$. $a = 5$.
The set of pairs

$$S_{23} = \{\{5, 5^{12}\}, \{5^2, 5^{13}\}, \{5^3, 5^{14}\}, ..., \{5^{11}, 5^{22}\}\}$$

$$= \{\{5,18\},\{2,21\},\{10,13\},\{4,19\},\{20,3\},\{8,15\},\{17,6\},\{16,7\},\{11,12\},\{9,14\},\{22,1\}\}$$

is a starter.

On closer inspection the two types of starters are identical[^5] , with a general element being of the form

$$\{j,-j\}$$

Starters of this form are called *patterned* starters.

Stanton and Mullin went on to show that using the method outlined in Example 2.1 they could find adders corresponding to the patterned starters for $k = 7, 11, 13, 15, 17$. They had problems with 9 (but were able to construct one using a different method) and finding it too laborious for $k > 19$ they developed an algorithm which, when implemented in Fortran, was able to find patterned starters with adders for all odd k up to 49, with no further gaps. Suggesting the possibility (which they conjectured) that there are Room squares for all odd side greater than 5.

They also found an interesting result regarding the number of Room Squares which could be obtained from patterned starters, summarised in Table 3.

Value of k	Number of PRS
7	2
9	0
11	4
13	8
15	44
17	416
19	The programme was turned off after the production of 967 PRS

Table 3

Stanton & Mullin's results suggest that the number of PRS (patterned Room squares) increases very rapidly. Which, bearing in mind that the PRS are a sub-class of CRS (cyclic Room squares), which are in turn a sub-class of Room squares, implies that there are vast numbers of Room squares of large order.

Before introducing a class of starters for which the existence of a corresponding adder is guaranteed we quickly confirm that when a starter and adder exist then a Room square will always result. This seems obvious from the method outlined in the previous section, but now we prove it explicitly.

Theorem 3.2.1 [17]
If an Abelian group G of odd order $2n-1$ admits a starter and an adder, then there exists a Room square of order $2n$.

Proof
A square is constructed on the set $G \cup \{\infty\}$, where G is an additive Abelian group of order $2n-1$.

$$G = \{g_0 = 0, g_1, g_2, ..., g_{2n-2}\}$$

The columns and rows of the square are labelled as follows

	g_0	g_1	g_2	···	g_{2n-1}
g_0					
g_1					
g_2					

g_0

Figure 18

If a starter $\{\{s_1, t_1\}, \{s_2, t_2\}...\{s_{n-1}, t_{n-1}\}\}$ and an adder $\{a_1, a_2, ..., a_{n-1}\}$ can be ontained from G and if the square is populated by pairs of elements from G according to the following rules:

1. $\{\infty, g_i\}$ goes in (g_i, g_i)
2. While $\{s_i + g_i, t_i + g_i\}$ goes in $(g_i, g_i - a_i)$

for all $g_i \in G$. The remaining square will be a Room square on $G \cup \{\infty\}$.
Proof

1. Row $g_0 = 0$, contains the pairs $\{s_i, t_i\} : 1 \leq i \leq n - 1$, which are the elements of the starter, hence all of $G \backslash \{0\}$. These pairs are accompanied by $\{\infty, 0\}$, so row 0 contains all of $G \cup \{\infty\}$. Subsequent rows simple contain a permutation of the same elements, hence the *row property* of Room squares is satisfied for all rows.
2. As mentioned before, the starter forms a difference system in $G \backslash \{0\}$, so all unordered pairs of this set occur along with all unordered pairs of the form $\{\infty, g_i\} : 1 \leq i \leq n - 1$, hence *all unordered pairs from* $G \cup \{\infty\}$ *occur* in the square exactly once.
3. All pairs of the form $\{s_i + a_i, t_i + a_i\}$ go in $(a_i, 0)$, i.e. column 0. According to the definition of a starter these pairs are all of $G \backslash \{0\}$, and we know that $\{\infty, 0\}$ is also in column 0. So the first column, and hence all others, contains all of $G \cup \{\infty\}$, thus satisfying the *column property* of Room squares.

Strong Starters

The next state in proving the existence of Room squares came about, not by continuing to try to find adders for starters that were already known (the patterned starters, for example), but when Mullin & Nemeth in [17], discovered a class of starters that generated their own adders.

Theorem 3.3.1 [17]
Suppose a starter $\{\{s_1, t_1\}, \{s_2, t_2\}, ..., \{s_{(g-1)/2}, t_{(g-1)/2}\}\}$ *exists, such that the sums of each pair* $(s_1 + t_1, s_2 + t_2, etc...)$ *are all distinct and non-zero, then that starter is said to be strong, and*

$$A(S) = \{a_i = -(s_i + t_i) : 1 \leq i \leq (g - 1)/2\}$$

is an adder for a starter.

Proof

(i) *The* a_i *are all distinct and non-zero*
All the $(s_i + t_i)$ are, by definition, distinct and non-zero. Therefore all the $a_i = -(s_i + t_i)$ are distinct and non-zero.

(ii) $s_1 + a_1, t_1 + a_1, s_2 + a_2, ..., s_{(g-1)/2}, t_{(g-1)/2} + a_{(g-1)/2}$ *are precisely all the non-zero elements of G.*

```
<span>l</span> $s_1+a_1=s_1-(s_1+t_1)=-t_1=t_{(g-1)/2}$\
$t_1+a_1=t_1-(s_1+t_1)=-s_1=s_{(g-1)/2}$\
\
$s_{(g-1)/2} + a_{(g-1)/2} = -t_{(g-1)/2} = t_1$\
$t_{(g-1)/2} + a_{(g-1)/2} = -s_{(g-1)/2} = s_1$\

Are all the non-zero elements of $G$ in reverse order.
```

(Notice that the patterned starter is not strong, on the contrary, the sums of its pairs are all identical.)

Example 3.3.1

The pairs $(5,7)(11,6)(2,8)(9,12)(10,1)(3,4)$, constitute a strong starter for a Room square of side 13, based on $G = Z_{13}$

Proof
Firstly, the pairs satisfy the conditions for being a starter, as the union of all pairs is equal to $G\backslash\{0\}$, and similarly the differences are all of $G\backslash\{0\}$.
Secondly the sums of the pairs, respectively 12,4,10,8,11,7, are all distinct and non-zero.
Therefore an adder is $\{-12,-4,-10,-8,-11,-7\} = \{1,9,3,5,2,6\}$
So the following is a legitimate first row for a cyclic Room square of order 14.

$\infty, 0$ – – – 11,6 – – 3,4 9,12 – 2,8 1,10 5,7 ———— — — — —— — — —— —— — —— —— ——

Mullin and Nemeth originally discovered strong starters for Room squares embedded within another type of combinatorial design, known as a Steiner triple system. With these they were able to prove that Room squares exist for all sides $v = 1$ mod 6. Rather than examine this approach we move on to a type of starter which provides its own adder.

The Mullin-Nemeth Starters

If x is a primitive element in $G = GF(p^n)$, then the elements $x^1, x^2, ..., x^{p^n-1} = 1$ are, by definition, all of $G\backslash\{0\}$. Alternatively, we can write $G\backslash\{0\} = \{x^0 = 1, x^1, ..., x^{p^n-2}\}$.

Example 3.4.1
The field $GF(23)$ has a primitive root $x = 5$, because
$5^0 = 1$, $5^1 = 5$, $5^2 = 2$, $5^3 = 10$, $5^4 = 4$, $5^5 = 20$, $5^6 = 8$, $5^7 = 17$, $5^8 = 16$, $5^9 = 11$, $5^{10} = 9$, $5^{11} = 22$, $5^{12} = 18$, $5^{13} = 21$, $5^{14} = 13$, $5^{15} = 19$, $5^{16} = 3$, $5^{17} = 15$, $5^{18} = 6$, $5^{19} = 7$, $5^{20} = 12$, $5^{21} = 14$ are all the non-zero elements of $GF(23)$.

Mullin & Nemeth in [17] used the theory of primitive elements to create strong starters in the additive group of (nearly) any Galois Field of prime power order. Which, because Theorems 3.2.1 and 3.3.1 were already known, was equivalent to proving the existence of Room squares for (nearly) all orders $p^n + 1$. Before introducing the general construction for these starters, we illustrate the basic method with a couple of examples of particular cases.

Example 3.4.2
We can create a strong starter from Example 2.5 simply by pairing the elements in the order in which they were generated.
i.e. $S = \{\{1,5\},\{2,10\},\{4,20\},\{8,17\},\{16,11\},\{9,22\},\{18,21\},\{13,19\},\{3,15\},\{6,7\},\{12,14\}\}$
is a strong starter.
Proof
Obviously each member of $GF(23)$ occurs once, because of the definition of a primitive root.
The differences

$$\{\pm4, \pm8, \pm7, \pm9, \pm10, \pm5, \pm3, \pm6, \pm11, \pm1, \pm2\}$$

are similarly all of $GF(23)$, so S is a starter. The sums

$$\{6, 12, 1, 2, 4, 8, 16, 9, 18, 13, 3\}$$

are all unique, and therefore S is strong and

$$A = \{17, 11, 22, 21, 19, 15, 7, 14, 5, 10, 20\}$$

is an adder for S.
So, the following row will generate a Room square of order 24 under cyclic construction.

-1.66cm

$\infty, 0$ 4,20 8,17 12,14 16,11 - 1,5 - 9,22 13,19 - - 2,10 6,7 - - 18,21 - 3,15 - - - - ——— —— —— ——- ——-
— —— — —— ——- — — —— —— — — ——- — —— — — — —

This is an example of the simplest case of the general theorem of Mullith & Nemeth, where the Galois field is Z_p (the integers mod p), with $p = 23 = 3(\mod 4)$ a prime.

Theorem 3.4.1 [1] *If $p = 4m + 3$ is prime, $m \geq 1$, then*

$$S = \{\{x^0, x^1\}, \{x^2, x^3\}, ..., \{x^{4m}, x^{4m+1}\}\}$$

is a strong starter in Z_p, and hence a Room square of order $p + 1$ exists.

Example 3.4.2 took $m = 5$ and $x = 5$.

A slightly more general version of Theorem 3.4.1, which we prove instead, involves any field of prime power order where $p^n = 2t + 1$, with $t > 1$ and odd. Of course, when p^n is not prime, the field will no longer be the integers mod p, instead the primitive element will be an irreducible polynomial whose coefficients belong to Z_p.

Theorem 3.4.2 [16] If $p^n = 2t + 1 = 3(\text{mod } 4)$ then

$$S = \{\{x^0, x^1\}, \{x^2, x^3\}, ..., \{x^{2t-2}, x^{2t-1}\}\}$$

is a strong starter in $GF(p^n), (p^n \neq 3)$

Proof
x is a primitive element, so the elements in the starter are all the non-zero members of $GF(P^n)$.
The differences are, respectively

$$\pm x^0(1 - x), \pm x^2(1 - x), ..., \pm x^{2t-2}(1 - x)$$

$(1 - x)$ is a non-zero ($x = 1$ is not primitive) member of $GF(p^n)$. So in order to show that these differences are all the $2t$ non-zero members of $GF(p^n)$ we merely need to prove that the $2t$ differences are all distinct and non-zero.
All the differences can be written $\pm x^{2i}(1 - x), 0 \leq i \leq t - 1$
$(1 - x) \neq 0$
$x^{2i}(1 - x) = x^{2j}(1 - x)$
$\Rightarrow x^{2i} = x^{2j} \Rightarrow i = j,$
because $0 \leq 2i, 2j \leq 2t - 2 < p^{n-1}$, and the primitive element, by definition, produces each element of $GF(p^n)$ exactly once as the indices range from 0 to p^{n-1}.
Similarly $-x^{2i}(1 - x) = -x^{2j}(1 - x)$ only when $i = j$.
So all the positive differences are unique, similarly the negative.
However, there remains a possibility for repetition when the signs are opposite:

$$x^{2i}(1 - x) = -x^{2j}(1 - x) \qquad ...(1)$$

Either $i = j$ or $i \neq j$
Let $i = j$, (1) becomes $x^{2i} + x^{2i} = 0, \Rightarrow 2x^{2i} = 0$, bit i takes values $0...t - 1$, so $x^2 = 0$ when $i = 1$, contradicting the order of the primitive element.
In the $i \neq j$ case, we assume (without loss of generality) that $i < j$ and write

$x^{2i} = -x^{2j}$
as $x^{2i}(1 + x^{2j-2i}) = 0$
$\Rightarrow x^{2j-2i} = -1$

but in $GF(2t + 1)$, $x^{\frac{1}{2}(q-1)} = x^t = -1$

$$2j - 2i = t$$

but this is a contradiction as we insisted that t be odd. So S is a starter.

To prove that S is strong we simply note that the sums can be written:

$x^0(1+x)$, $x^2(1+x)$, ..., $x^{2t-2}(1+x)$

$1+x=0 \Rightarrow x=-1$ is only true when $p^n=3$. So $(1+x)\neq 0$.
So $x^{2i}(1+x)=x^{2j}(1+x) \Rightarrow x^{2i}=x^{2j}$
We have already shown that

$$x^{2i}=x^{2j}$$

is only true for $i=j$. So all the sums are unique, and the starter is strong.

Hence, by theorems 2.1 and 2.2, Room squares exist for all $p^n = 3(\mathrm{mod}\ 4)$, and in the case when $p^n=3(\mathrm{mod}\ 4)$ is prime, these Room squares are based on Z_p.

The most generalised case of Mullin & Nemeth's theorem proves the existence of Room squares for all prime powers $p^n=2^kt+1$ where $k>1$ and $t>1$ is odd (k and t, both positive integers), and reduces to Theorem 3.4.2 when $k=1$.

Theorem 3.4.3 [16] A strong starter exists in $GF(p^n)$, where $p^n=2^kt+1$ (with $k>1$ and $t>1$ is odd).

Proof
Let $d=2^{k-1}$
Then the strong starter in question looks like this: \$\$ S={

$$\begin{array}{ccccc}
(x^0,x^d) & (x^{2d},x^{3d}) & \$ \quad ... \quad \$ & (x^{(2t-2)d},x^{(2t-1)d}) \\
(x^1,x^{d+1}) & (x^{2d+1},x^{3d+1}) & \$ \quad ... \quad \$ & (x^{(2t-2)d+1},x^{(2t-1)d+1}) \\
 & & \$ \quad ... \quad \$ & \\
(x^{d-1},x^{2d-1}) & (x^{3d-1},x^{4d-1}) & \$ \quad ... \quad \$ & (x^{(2t-1)d-1},x^{2td-1}) \\
\hline
\end{array}$$

} \$\$ Where the pairs have been placed in an array to emphasise that, when read vertically, this is an exhaustive list of all the non-zero elements of $GH(p^n)$, ordered according to powers. Of course, in the $k=1, d=1$ case this starter reduces to the one quoted in Theorem 3.4.2.
To prove that S is a starter we need also to show, as usual, that the differences between pairs are all of $GF(p^n)$, and to show that the starter is strong we need to show that the sums of pairs are all distinct and non-zero.
The differences can be written in the following scheme:

$$\begin{array}{cccc}
x^0(1-x^d), & x^{2d}(1-x^d), & ..., & x^{(2t-2)d}(1-x^d), \\
x^1(1-x^d), & x^{2d+1}(1-x^d), & ..., & x^{(2t-2)d+1}(1-x^d), \\
 & & ... & \\
x^{d-1}(1-x^d), & x^{3d-1}(1-x^d), & ..., & x^{(2t-1)d-1}(1-x^d) \\
\hline
\end{array}$$

The order of x is $p^n-1=2^kt=2^{k-1}2t=2td>d$, (meaning $x^{2td}=1$ and $x^\alpha\neq 1$ when $1\leq\alpha<2dt$) and so $x^d\neq 1$, so $(1-x^d)\neq 0$.
We can write the differences in a general form:

$\pm x^{2id+j}(1-x^d) \qquad \text{where} \qquad 0\leq i\leq t-1, \quad 0\leq j\leq d-1$

: 1 :→ If there were repetition, either of the form $D=D$ or $-D=-D$, where $D=x^{2id+j}(1-x^d)$, then the following must hold:

Cancelling by $(1-x^d)$, legitimate because $(1-x^d)\neq 0$ gives:

dividing through by x^{2Id+j} leaves

But if $i \neq I$, then the LHS has an index which is an integer multiple of d. The index in the RHS, however, can never be an integer multiple of d because J and j range over the integers $0 ... d-1$. So the only possibility for equality is when both indices are zero, i.e. $i = I$ and $j = J$.

As in the previous proof we have to deal with the possibility of repetition for differences of opposite sign. For coincidence we require:

$$x^{2id+j} = -x^{2ID+J}$$

$$x^{2id+j} + x^{2Id+J} = 0$$

We assume that $2id + j < 2Id + J$ and rewrite this expression as:

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

Which implies that $x^{(2I-2i)d+(J-j)} = -1$
But in $GF(q), x^{\frac{1}{2}(q-1)} = -1$. Where, in this case $q - 1 = 2^k t$, so $\frac{1}{2}(q-1) = 2^{k-1}t = dt$.

$$\therefore x^{dt} = -1$$

$$\Rightarrow (2I - 2i)d + (J - j) = dt$$

$\Rightarrow (J - j)$ is an integer multiple of d or zero.

But J and j both take only the values $0 ... d-1$, so $(J - j)$ is in the interval $[1 - d, d - 1]$ and hence must be zero, leaving

$$(2I - 2i)d = dt$$

$$2I - 2i = t$$

But t is strictly odd, and so we have reached a contradiction, hence the differences are all unique, belong to $GF(p^n)$ and there are $2td$ of them, hence each member of $GF(p^n)$ occurs exactly once as a difference. So S is a starter.
To prove that the starter is strong we write the sums as

$$\begin{array}{cccc}
x^0(1-x^d), & x^{2d}(1-x^d), & ..., & x^{(2t-2)d}(1-x^d), \\
x^1(1-x^d), & x^{2d+1}(1-x^d), & ..., & x^{(2t-2)d+1}(1-x^d), \\
 & & ... & \\
x^{d-1}(1-x^d), & x^{3d-1}(1-x^d), & ..., & x^{(2t-1)d-1}(1-x^d) \\
\hline
\end{array}$$

and notice that $x^d = -1 \Rightarrow d = dt$ (because $x^{dt} = -1$) $\Rightarrow t = 1$, but instead we insisted that t be strictly greater than one (this being the reason why). So $(1 + x^d) \neq 0$ and the above argument (denoted by $\rightarrow$) involving $(1 - x^d)$ can be invoked, replacing $(1 - x^d)$ by $(1 + x^d)$. So S is a strong starter, and the general theorem of Mullin & Nemeth is proven, guaranteeing the existence of a vast class of Room Squares.

The Trouble with Fermat Numbers

Unfortunately, in establishing the Mullin & Nemeth starters we were forced to exclude a similarly vast, potentially infinite, class of Room squares by insisting that t be strictly greater than one. These exceptional Room squares have side $2^k + 1$.

Rectifying this problem is essential if we are to prove the existence of Room squares. As mentioned previously, the proof relies on a multiplication theorem, so proving that all the 'prime' Room squares exist is vital. Although the theorem of Mullin & Nemeth will take care of all squares with prime power side, the multiplication theorem is necessary for proving the existence of those whose side can be decomposed into prime factors different from each other. In fact, the multiplication theorem means that we can ignore the Mullin & Nemeth construction except in the prime case, resorting to multiplication to recover the prime power squares. Similarly we are only concerned with recovering the exceptional squares with side 2^k+1, when 2^k+1 is prime.

Primes of this form are known as **Fermat Numbers** or **Fermat Primes**, after Pierre de Fermat who, 360 years ago conjectured that numbers of the form $2^k + 1$ are always prime when k is a power of two.

$$\begin{array}{l} F_m = 2^{2^m} + 1 \\ F_0 = 2^1 + 1 = 3 \\ F_1 = 2^2 + 1 = 5 \\ F_2 = 2^4 + 1 = 17 \\ F_3 = 2^8 + 1 = 257 \\ \underline{F_4 = 2^{16} + 1 = 65537} \end{array}$$

After the first four of Fermat's numbers, all of which were known to him to be prime. Nearly one hundred years later Euler calculated the following,

$$F_5 = 2^{32} + 1 = 4294967297 = 641 \times 6700417$$

and in doing so disproved Fermat's conjecture.

Since Euler's time, F_6, F_7 and F_8 have all been factorised[^6] . It is also known, although most of the factorisations remain unknown, that F_m is composite for $m = [9...23]$. F_{24}, a number with over 5 million digits, remains in doubt.

Whether there be an infinite number of Fermat primes or whether, as empirically seems to be the case, there are only finitely many (possibly just five) such primes, in order for the proof of the existence of Room squares for all odd side greater than 7 to be complete these Fermat prime Room squares must be included.

When the problem of Fermat Room squares was tackled first in the early 1970s, W.D.Wallis used a Theorem of J.D.Horton's which adapted a famous result of E.H.Moore's from the theory of Steiner triple systems.

Moore, in 1893, was able to prove that if Steiner triple systems of orders v_1, v_2 and v_3 exist, where the v_2 system is a sub-system of the v_3 system, then an STS of order $v_1(v_2 - v_3) + v_3$ also exists. Horton[12] adapted this result to other combinatorial objects including Room squares and Wallis[25] was able to use this Moore-type construction method to include all of the Fermat primes, except $F_3 = 257$[^7] .

Example 3.5.1
If Room squares with side v_1, v_2 and v_3 exist, where the square of side v_2 is a subsquare of the square with side v_3, then a Room square of side $F_4 = 65537$ exists. Room squares of side 7 and 11 exist, according to the theory of Mullin & Nemeth. Applying Horton's theorem once, with $v_3 = 0$ gives a new square of side $v_1 v_2 = 77$ (note that Horton's theorem reduces to the multiplication theorem when $v_3 = 0$).

The trivial Room square of side one exists, and the Mullin & Nemeth starters will provide a Room square of size 13. So we can apply Horton's theorem once again to gain a Room square of side 989 because:

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

Finally we can use Mullin & Nemeth to produce a Room square of side 67, and a final application of Horton's theorem gives:

$$65537 = 67(989 - 11) + 11$$

The proof of Horton's theorem and also an explanation of Wallis's application of that theorem to solving the Fermat prime problem is excluded because another solution was subsequently found. A year after Wallis had published his solution to the Fermat problem, Chong and Chan published their (independent) discovery of the strong starters which are known as the Mullin & Nemeth starters. Also included in their paper was an alternative solution to the same problem, but their solution continued to involve the starter-adder method. This theorem we prove instead.

Theorem 3.5.1 [6] For every Galois field of order $(2^{2^m}+1)$, where $m \geq 2$, there exists a Room square of order $(2^{2^m}+2)$.

Proof
The following pairs in Z_p (where $p = 2^{2^d}+1$ and $d = 2^{m-1}$) constitute a strong starter.

1. $\{i+(r-1)2^d, i2^d-(r-1\}$
2. $\{(2^d-i)2^d+r, (2^{d-1}-r)2^d+2^{d-1}-i+1\}$
3. $\{2^{d-1}+r-1)2^d+2^{d-1}+i, (2^{d-1}+i-1)2^d+2^{d-1}-(r-1)\}$
4. $\{(2^{d-1}-i)2^d+2^{d-1}+r, (2^d-r+1)2^d-i+1\}$

Where $1 \leq r \leq 2^{d-2}$ and $1 \leq i \leq 2^{d-1}$, so rather than just 4 pairs there are $4 \cdot 2^{d-2} \cdot 2^{d-1} = 2^{2d-1}$ pairs arranged in four different classes. Before completing the proof we pause for an example just to illustrate the real simplicity of these apparently complicated pairs.

Example 3.5.2
Suppose $p = 2^{2 \cdot 2}+1 = 17 = F_2$, then $d = 2^1 \Rightarrow m = 2$
$r = 1, 1 \leq i \leq 2$ and the following pairs should be a strong starter.

-1.15cm

	$i=1, r=1$	$i=2, r=1$
1	$\{1+0\cdot 2^2, 1\cdot 2^2-0\} = \{1,4\}$	$\{2+0\cdot 2^2, 2\cdot 2^2-0\} = \{2,8\}$
2	$\{(2^2-1)2^2+1, (2^1-1)2^2+2^1-1+1\} = \{13,6\}$	$\{(2^2-2)2^2+1, (2^1-1)2^2+2^1-2+1\} = \{9,5\}$
3	$\{(2^1+1-1)2^2+2^1+1, (2^1+1-1)2^2+2^1-(1-1)\}$ $= \{11,10\}$	$\{(2^1+1-1)2^2+2^1+2, (2^1+2-1)2^2+2^1-(1-1)\}$ $= \{12,14\}$
4	$\{(2^1-1)2^2+2^1+1, (2^2-1+1)2^2-1+1\}$ $= \{7,16\}$	$\{(2^1-2)2^2+2^1+1, (2^2-1+1)2^2-2+1\}$ $= \{3,15\}$

Table 4

The pairs generated by this method contain each non-zero member of Z_{17} exactly once in their union satisfying the first property of a starter.
The differences are $\{\pm 3, \pm 7, \pm 1, \pm 8, \pm 6, \pm 4, \pm 2, \pm 5\} = Z_{17} \backslash \{0\}$, satisfying the other necessary property of a starter.
The sums 5,2,4,6,10,14,9,1 are all unique, hence the starter is strong and the set
$\{-5,-2,-4,-6,-10,-14,-9,-1\} = \{12,15,13,11,3,8,16\}$ is an adder. So the following first row will generate a Room square under cyclic construction:

$\infty, 0$ 3,15 13,6 - 11,10 1,4 7,16 - - 12,14 2,8 - - - 9,5 - - ———— —— —— — ——- —— —— — — ——- —— — — — —— — —

In order to prove that the pairs 1...4 are a strong starter from any Z_p we need to prove the following:

1. The union of all the pairs contains each non-zero member of Z_p exactly once.
2. The differences are all the non-zero members of Z_p exactly once.

3. The sums are all distinct and non-zero.

This is a formidable task, one that would take many pages to prove in full detail. So instead we sketch an outline of the proof, explicitly proving a few specific cases.

First we prove (a) completely.
The non-zero members of Z_P, namely $\{1...2^{2d}\}$, can be represented uniquely by:

$$C(u,v) = u2^d + v \quad \text{where} \quad 1 \leq v \leq 2^d \ \text{ and } \ 0 \leq u \leq 2^d - 1$$

Proof
Indeed if

$$u_1 2^d + v_1 = u_2 2^d + v_2$$

then

$$(u_1 - u_2)2^d = (v_2 - v_1)$$

The RHS takes integer values in the interval $[-(2^d - 1), 2^d - 1]$, which is symmetric about the origin and smaller than 2^d on both sides. Whereas the LHS takes integer multiple steps of size 2^d, so the equality can only hold in the case when both sides equal zero. Which implies $u_1 = u_2$, $v_1 = v_2$ and $C(u,v)$ is unique representation the non-zero members of Z_p. u takes 2^d values and v takes 2^d values so there are 2^{2d} unique non-zero members of Z_p represented in this way, so each member of Z_p is represented.
The left and right hand members of each pair can be characterised by a range of values of u and v in the following manner.
Take, for instance, the left hand member of pair 1.

$$i + (r-1)2^d$$

Here $v = i$ and so $1 \leq v \leq 2^{d-1}$, while $u = (r-1)$, so $0 \leq u \leq 2^{d-2} - 1$. The full list of intervals for each member of each pair is tabulated below.

Pair	Member	u	V
1.	L	$[0, 2^{d-2} - 1]$	$[1, 2^{d-1}]$
	R	$[0, 2^{d-1} - 1]$	$[3 \cdot 2^{d-2} + 1, 2^d]$
2.	L	$[2^{d-1}, 2^d - 1]$	$[1, 2^{d-2}]$
	R	$[2^{d-2}, 2^{d-1} - 1]$	$[1, 2^{d-1}]$
3.	L	$[2^{d-1}, 3 \cdot 2^{d-2} - 1]$	$[1 + 2^{d-1}, 2^d]$
	R	$[2^{d-1}, 2^d - 1]$	$[1 + 2^{d-2}, 2^{d-1}]$
4.	L	$[0, 2^{d-1} - 1]$	$[1 + 2^{d-1}, 3 \cdot 2^{d-2}]$
	R	$[3 \cdot 2^{d-2}, 2^d - 1]$	$[1 + 2^{d-1}, 2^d]$

Table 5

It was mentioned earlier that there were 2^{2d-1} pairs, each of which has two members, so there are 2^{2d} elements altogether in the pairs of the starter, which is the same as the number of elements in Z_p. Because $C(u,v)$ is a unique representation for each member of Z_p, for an element of Z_p to occur more than once in the starter requires repetition of both u and v. This cannot happen because when two intervals overlap (as they do in the values of v for 1L and 2R).

To prove (b) we need to show that the differences between two pairs of type 1 are all unique, similarly between two pairs of types 2,3 and 4. Moreover we need to show that there can be no repetition in differences between a pair of type 1 and a pair of type 2, also type 1 with types 3 in 4. Similarly for 2,3 and 4. All together there are ten cases to prove, tabulated below, where a pair of numbers represents the two types of pairs from the starter.

Table 6