More Z–Cyclic Room Squares

Y.S. Liaw*

Department of Mathematics
University of Glasgow
Glasgow G12 8QW
Scotland

ABSTRACT. This paper deals with the existence of Z–cyclic Room squares of order $2v$ (or of side $2v-1$) whenever $2v-1 = \Pi_{i=1}^{n} p_i^{\alpha_i}$, ($p_i = 2^{m_i} b_i + 1 \geq 7$ are distinct primes, b_i odd, $b_i > 1$, and α_i positive integers, $i = 1, 2, \cdots, n$), and includes some further results involving Fermat primes.

1 Introduction

A Room square of order $2v$ (or of side $2v-1$) is a $(2v-1) \times (2v-1)$ array based on $2v$ distinct symbols such that

(i) each cell is empty or contains an unordered pair of distinct symbols;

(ii) each row and each column contains each symbol exactly once;

(iii) each of the $v(2v-1)$ unordered pairs of distinct symbols occurs in precisely one cell of the array.

It is well-known (see [1] or [7]) that Room squares exist for all $v \geq 4$.

Definition 1.1. *A Room square of order $2v$ is Z–cyclic if its symbols are $\infty, 0, 1, \cdots, 2v-2$, and the top left diagonal cell contains $\{\infty, 0\}$, and whenever $\{a, b\}$ occurs in the (i,j)th cell, $\{a+1, b+1\}$ occurs in the (i+1, j+1)th cell, arithmetic being* $\pmod{2v-1}$, *with* $\infty + 1 = \infty$.

Phelps and Vanstone [8] constructed Z-cyclic Room squares of order $2v$, whenever $2v-1 = pq$ where p, q are primes and whenever $2v-1 = p^n$

*current address: Department of Applied Mathematics, Tatung Institute of Technology, Taipei, Taiwan, email: ysliaw@math.ttit.edu.tw

where p is a prime, n is any positive integer. I. Anderson and the author [2] constructed Z–cyclic Room squares of order $2v$, whenever $2v-1=p^\alpha$, (p prime, $p \equiv 3 \pmod 4$, $p \geq 7$) and whenever $2v-1=p^\alpha q$ (p,q primes, $p \equiv 3 \pmod 4$, $p \geq 7$, $q \geq 7$). In this paper, Z–cyclic Room squares of side $2v-1=\prod_{i=1}^{n} p_i^{\alpha_i}$, ($p_i$ not Fermat primes, $p_i \geq 7$) and $2v-1=p\cdot q$ (p, q distinct Fermat primes), are constructed. Furthermore, all the squares that are constructed will be skew, i.e. for all $i \neq j$, precisely one of the (i,j)th and (j,i)th cell contains an unordered pair, the other being empty.

2 The starter–adder constructions

If G is an additive Abelian group with identity element 0, and $G^\star = G \setminus \{0\}$, then a *starter* X for G is a partition of $G^\star$ into 2–sets such that $\{x-y; \{x,y\} \in X\} = G^\star$. An adder A for X is an injection $A : X \mapsto G^\star$ such that

$$\bigcup_{\{x,y\}\in X} \{x+\{x,y\}A, y+\{x,y\}A\} = G^\star.$$

For any starter X, we can define the map $A : X \mapsto G^\star$ by $\{x,y\}A = -(x+y)$. If A is an adder for X, then we say that X is a *strong* starter. For any strong starter X with adder A such that $\{x,y\}A \neq -\{x',y'\}A$ for all distinct $\{x,y\}$ and $\{x',y'\} \in X$, we say that X is a *skew* strong starter. In this paper we construct skew strong starters in Z_{2v-1}, thereby obtaining skew Z–cyclic Room squares.

Lemma 2.1. *If p is prime, $p \geq 7$, then there exists a skew strong starter in Z_p, and hence a skew Z–cyclic Room square of order $p+1$.*

Proof: See, for example, [1].

In the following, for a set A of positive integers and a positive integer a, aA means $\{ax : x \in A\}$.

Lemma 2.2. *Let $m = p^\alpha n$ where p is an odd prime, α and n are positive integers, and $(n,p)=1$. Then*

$$Z_m = pZ_{m/p} \cup \left\{ \bigcup_{d|n} d\{x \in Z_{m/d} : (x, m/d) = 1\} \right\}.$$

Furthermore, these sets are pairwise disjoint.

Proof: Consider $x \in Z_m$. If $p \mid x$ then $x \in pZ_{m/p}$. If $p \nmid x$ then $(x,m) = (x,n)$, so $x \in E_d = \{x \in Z_m; (x,m) = d\}$ for some $d \mid n$. These sets partition Z_m. Finally we note that E_d can be represented as $d\{x \in Z_{m/d}; (x, m/d) = 1\}$.

Example 2.1:

$$\begin{aligned}
Z_{2^3\cdot 3^2\cdot 5} &= 5Z_{2^3\cdot 3^2} \cup \{x \in Z_{2^3\cdot 3^2\cdot 5}; (x, 2^3\cdot 3^2\cdot 5) = 1\} \\
&\cup 2^3\{x \in Z_{3^2\cdot 5}; (x, 3^2\cdot 5) = 1\} \cup 2^2\{x \in Z_{2\cdot 3^2\cdot 5}; (x, 2\cdot 3^2\cdot 5) = 1\} \\
&\cup 2\{x \in Z_{2^2\cdot 3^2\cdot 5}; (x, 2^2\cdot 3^2\cdot 5) = 1\} \cup 3^2\{x \in Z_{2^3\cdot 5}; (x, 2^3\cdot 5) = 1\} \\
&\cup 3\{x \in Z_{2^3\cdot 3\cdot 5}; (x, 2^3\cdot 3\cdot 5) = 1\} \cup 2^3\cdot 3^2\{x \in Z_5; (x, 5) = 1\} \\
&\cup 2^3\cdot 3\{x \in Z_{3\cdot 5}; (x, 3\cdot 5) = 1\} \cup 2^2\cdot 3^2\{x \in Z_{2\cdot 5}; (x, 2\cdot 5) = 1\} \\
&\cup 2^2\cdot 3\{x \in Z_{2\cdot 3\cdot 5}; (x, 2\cdot 3\cdot 5) = 1\} \cup 2\cdot 3^2\{x \in Z_{2^2\cdot 5}; (z, 2^2\cdot 5) = 1\} \\
&\cup 2\cdot 3\{x \in Z_{2^2\cdot 3\cdot 5}; (x, 2^2\cdot 3\cdot 5) = 1\}
\end{aligned}$$

Theorem 2.1. *If $p = 2^m \cdot a + 1$, where $a > 1$ is odd, is a prime, $p \geq 7$, α is a positive integer, then there exists a skew strong starter in Z_{p^α}, and hence a skew Z-cyclic Room square of order $p^\alpha + 1$.*

Proof: The case $\alpha = 1$ follow from Lemma 2.1. To deal with the induction step, let $p^{\alpha-1}(p-1) = 2^m \cdot t$ where t is odd, and let ω be a primitive root of p^α and hence also of p. Let $d = 2^{m-1}$. Then $\omega, \omega^2, \cdots, \omega^{2dt} \equiv 1$ constitute a reduced set of residues $\pmod{p^\alpha}$, $\omega^{dt} \equiv -1 \pmod{p^\alpha}$. Further, we have $\omega^d \not\equiv \pm 1 \pmod{p}$; for otherwise $\omega^{2d} \equiv 1 \pmod{p}$, contradicting the fact that the order of $\omega \pmod{p}$ is $p - 1 = 2ad > 2d$ (since $a > 1$). Write down the elements of the reduced set of residues mod p^α in pairs as follows.

$$\{\omega^{2id+j}, \omega^{(2i+1)d+j}\}\ i = 0, 1, \cdots, t-1; j = 0, 1, \cdots, d-1. \quad (2.1.1)$$

The differences between each pair are $\pm\omega^{2id+j}(\omega^d - 1), 0 \leq i \leq t-1, 0 \leq j \leq d-1$. Now we can not have $\omega^{2id+j}(\omega^d - 1) \equiv \omega^{2Id+J}(\omega^d - 1)$ unless $i = I$ *and* $J = j$, for cancelling by $\omega^d - 1 \not\equiv 0 \pmod{p}$ gives $\omega^{2id+j} \equiv \omega^{2Id+J}$. i.e. $\omega^{2d(i-I)} \equiv \omega^{J-j}$, which due to the ranges of possible values of i, I, j, J can only occur if $i = I$ and $j = J$. Suppose next that $\omega^{2id+j}(\omega^d - 1) \equiv -\omega^{2Id+J}(\omega^d - 1)$. Then we would have $\omega^{2id+j} + \omega^{2Id+J} \equiv 0$. If $2id + j < 2Id + J$ then we would have $\omega^{2id+j}(1 + \omega^{(2I-2i)d+(J-j)}) \equiv 0$ so that $(2I - 2i)d + J - j = dt$. But $J - j$ lies in the interval $[-d+1, d-1]$ and so, being a multiple of d, must be 0. So $j = J$. Thus $2I - 2i = t$ contradicting the oddness of t. Also their sums are distinct, by the same argument with $1 + \omega^d$ in place of $\omega^d - 1$, where we note that $\omega^d + 1 \not\equiv 0 \pmod{p}$ as in the above and the skew property holds. Thus for a skew strong starter for Z_{p^α} we take the pairs in (2.1.1) together with the pairs $\{pa_i, pb_i\}$ where $\{a_i, b_i\}, i = 1, 2, \cdots, \frac{p^{\alpha-1}-1}{2}$, is a skew strong starter for $Z_{p^{\alpha-1}}$.

For later reference, we denote the pairs in (2.1.1) by PIR_{p^α} (Pairs In Reduced set mod p^α).

Lemma 2.3. *For $i = 1, 2, \cdots, n$, let p_i be distinct primes, and α_i be positive integers. Let $p_i = 2^{m_i} \cdot u \cdot a_i + 1$ where u, a_i are odd and h.c.f $\{a_i; i = 1, 2, \cdots, n\} = 1$. Let $\ell = max\{m_i; i = 1, 2, \cdots, n\}$, $M = \prod_{i=1}^{n} p_i^{\alpha_i}$. Then there exists a common primitive root ω of $p_i^{\alpha_i}$, $i = 1, 2, \cdots, n$, and a positive integer t such that*

(1) $\omega^{2^\ell t} \equiv 1 \pmod M$, *and $H = \{\omega^i; i = 1, 2, \cdots, 2^\ell t\}$ is a multiplicative abelian group of order $2^\ell t$;*

(2) $\omega^{2^{\ell-1} \cdot t} \equiv -1 \pmod M$ *if $m_i = a \;\; \forall i = 1, 2, \cdots, n$;*

(3) $\omega^j \not\equiv -1 \pmod M \;\; \forall j$ *if $m_{i_1} \neq m_{i_2}$ for some $1 \leq i_1 \neq i_2 \leq n$;*

(4) *if $G = \{x \in Z_M; (x, M) = 1\}$ then G is a multiplicative abelian group of order $2^\ell \cdot t \cdot h$ for some positive integer h.*

Proof: (1) The existence of a common primitive root ω of $p_i^{\alpha_i}$ is assured by the Chinese Remainder Theorem and $(\omega, M) = 1$ since $(\omega, p_i) = 1$ for all $i = 1, 2, \cdots, n$. Now

$$\begin{aligned}
&l.c.m\{p_i^{\alpha_i - 1}(p_i - 1); i = 1, 2, \cdots, n\} \\
&= l.c.m\{(2^{m_i} \cdot u \cdot a_i + 1)^{\alpha_i - 1} \cdot 2^{m_i} \cdot u \cdot a_i; \;\; i = 1, 2, \cdots, n\} \\
&= 2^\ell \cdot t.
\end{aligned}$$

for some odd t. Thus since, if $\beta > \gamma$,

$$\begin{aligned}
&\omega^\beta \equiv \omega^\gamma \pmod M \\
\Longleftrightarrow\; &\omega^\gamma(\omega^{\beta-\gamma} - 1) \equiv 0 \pmod M \\
\Longleftrightarrow\; &\omega^{\beta-\gamma} - 1 \equiv 0 \pmod M \text{ since } (\omega, M) = 1) \\
\Longleftrightarrow\; &\omega^{\beta-\gamma} - 1 \equiv 0 \pmod{p_i^{\alpha_i}} \text{ for all } i = 1, 2, \cdots, n \\
\Longleftrightarrow\; &p_i^{\alpha_i - 1}(p_i - 1) \mid (\beta - \gamma) \text{ for all } i = 1, 2, \cdots, n \\
&\quad (\text{since } \omega \text{ is a primitive root modulo } p_i^{\alpha_i} \\
\Longleftrightarrow\; &l.c.m\{p_i^{\alpha_i - 1}(p_i - 1); i = 1, 2, \cdots, n\} \mid (\beta - \gamma)
\end{aligned}$$

therefore, the elements

$$\omega, \omega^2, \cdots, \omega^{2^\ell t}$$

are all distinct and $\omega^{2^\ell t} \equiv \omega^0 \equiv 1 \pmod M$ and $H = \{\omega^i; i = 1, 2, \cdots, 2^\ell t\}$ is a multiplicative abelian group of order $2^\ell t$.

(2) If $m_i = a$ for all $i = 1, 2, \cdots, n$ then $\ell = a$. This implies $2^{\ell-1} t = \frac{1}{2} v_i \phi(p_i^{\alpha_i})$ where each v_i is odd. Since ω is a common primitive root of $p_i^{\alpha_i}$ for $i = 1, 2, \cdots, n$, we have $\omega^{\frac{1}{2}\phi(p_i^{\alpha_i})} \equiv -1 \pmod{p_i^{\alpha_i}}$. Thus $\omega^{2^{\ell-1} t} = (\omega^{\frac{1}{2}\phi(p_i^{\alpha_i})})^{v_i} \equiv -1 \pmod{p_i^{\alpha_i}}$ for each i. Therefore $\omega^{2^{\ell-1} t} \equiv -1 \pmod M$.

(3) If $m_{i_1} \neq m_{i_2}$ for some $1 \leq i_1 \neq i_2 \leq n$ we claim that $\omega^j \not\equiv -1 \pmod{M}$ for all j. Suppose that there exists some j_0 such that $\omega^{j_0} \equiv -1 \pmod{M}$. Then $\omega^{j_0} \equiv -1 \pmod{p_{i_1}}, \omega^{j_0} \equiv -1 \pmod{p_{i_2}}$, $\omega^{\frac{p_{i_1}-1}{2}} \equiv -1 \pmod{p_{i_1}}$ and $\omega^{\frac{p_{i_2}-1}{2}} \equiv -1 \pmod{p_{i_2}}$. Thus $j_0 \equiv \frac{p_{i_1}-1}{2} \pmod{p_{i_1}-1} \equiv \frac{p_{i_2}-1}{2} \pmod{p_{i_2}-1}$. It follows that $2^{m_{i_1}-m_{i_2}} a_{i_1}(2k+1) = a_{i_2}(2g+1)$ for some k and g, which is imposible, since a_{i_1}, a_{i_2}, $2k+1$, $2g+1$ are odd and $m_{i_1} \neq m_{i_2}$.

(4) Clearly G is a multiplicative Abelian group with order $\varphi(M)$ where

$$\varphi(M) = \prod_{i=1}^{n} p_i^{\alpha_i - 1}(p_i - 1) = 2^\ell th$$

for some positive integer h.

Lemma 2.4. *If $p_i \geq 5, i = 1, 2, \cdots, n$ and all symbols are as in Lemma 2.3 then the following holds.*

(1) *If $m_i = \ell$ and $u \cdot a_i > 1 \quad \forall\ i = 1, 2, \cdots, n$, set $d = 2^{\ell-1}$. Then H, having order $2^\ell t$, is a subgroup of G. G has $2^{(n-1)\ell}h$ disjoint cosets, say c_jH, $c_1 = 1$. In each coset c_jH, write down the elements of c_jH in pairs as follows:.*

$$\{c_j\omega^{2id+k}, c_j\omega^{(2i+1)d+k}\}\ i = 0, 1, \cdots, t-1;\ k = 0, 1, \cdots, d-1. \tag{2.4.1}$$

Their differences and sums satisfy the properties of a skew strong starter for G.

(2) *If $m_{i_1} \neq m_{i_2}$ for some $1 \leq i_1 \neq i_2 \leq n$, set $H_1 = \{\omega^i, -\omega^i,\ i = 0, 1, \cdots, 2^\ell t - 1\}$, so that H_1 has order $2^{\ell+1}t$ and is a subgroup of G. G has $2^{\sum m_i - \ell - 1}h$ disjoint cosets c_jH. In each coset, form the pairs*

$$\{c_j\omega^{2i}, c_j\omega^{2i+1}\}, \{-c_j\omega^{2i+1}, -c_j\omega^{2i+2}\};\ i = 0, 1, \cdots, 2^{\ell-1}t - 1. \tag{2.4.2}$$

Their differences and sums satisfy the properties of a skew strong starter for G.

Proof: (1) Use the same argument as in Theorem 2.1. Note $u \cdot a_i > 1\ \forall\ i = 1, 2, \cdots, n$.

(2) Since ω is a common primitive root of p_i $\forall i$ it follows that $\omega \pm 1 \not\equiv 0 \pmod{p_i}$ $\forall i$. The differences between the pairs in (2.4.2) are

$$\pm c_j\omega^{2i}(\omega - 1) \text{ and } \pm c_j\omega^{2i+1}(\omega - 1) \text{ where } i = 0, 1, \cdots, 2^{\ell-1}t - 1.$$

i.e. $c_j(\omega-1)$ times $\pm\omega^i,\ i=0,1,\cdots,2^{\ell-1}t-1$.

Since $c_j \in G,\ \omega-1 \not\equiv 0\ (mod\ p_i)\ \forall i$ and $\omega^j \not\equiv -1 (mod\ M)\ \forall\ j$, the $\pm\omega^i$ are all distinct and $c_j(\omega-1) \in G$, and so their differences are the elements of the coset $c_j(\omega-1)H$ each once. Similarly their sums are $c_j(\omega+1)$ times $\omega^{2i}, -\omega^{2i+1}$ where $i=0,1,\cdots,2^{\ell-1}t-1$. Since $\omega+1 \not\equiv 0\ (\text{mod } p_i)\ \forall i$, so $c_j(\omega+1) \in G$, and their sums are precisely half of the elements of the coset $c_j(\omega+1)H$. Finally, since $\omega^j \not\equiv -1\ (\text{mod } M)$, they have the skew property.

For later reference we denote the pairs in (2.4.1) and (2.4.2) by $PICH_M^{(1)}$ and $PICH_M^{(2)}$ (Pairs In Cosets of H) respectively. We also use the following notation

$$\chi(p_i; i=1,2,\cdots,n) = \begin{cases} 1, & \text{if } m_i = \ell \text{ for all } i=1,2,\cdots,n \\ 2, & \text{if } m_{i_1} \neq m_{i_2} \text{ for some } 1 \le i_1 \neq i_2 \le n. \end{cases}$$

Theorem 2.2. *If $p = 2^n \cdot a + 1 \ge 7$, $q = 2^m \cdot b + 1 \ge 7$, are distinct primes, and a, $b > 1$ are odd, $M = p^\alpha q^\beta$ where α, β are positive integers then there exists a skew strong starter in Z_M and hence a Z-cyclic Room square of order $M+1$.*

Proof: Let α be fixed and proceed by induction on β. For the case $\beta = 1$, we have

$$Z_{p^\alpha q} = qZ_{p^\alpha} \cup \left\{ \bigcup_{p^\alpha \neq d | p^\alpha} d\{x \in Z_{M/d}; (x, M/d) = 1\} \right\} \cup p^\alpha Z_q.$$

By Lemma 2.1 and Theorem 2.1 skew strong starters in Z_q, Z_{p^α} exist, say $\{c_i, d_i\}$, $\{a_i, b_i\}$ respectively. Use Lemma 2.4 for the set $\{x \in Z_{M/d};$ $(x, M/d) = 1\}$ for all $p^\alpha \neq d \mid p^\alpha$; the pairs $PICH_{M/d}^{\chi(p,q)}$ for all $p^\alpha \neq d \mid p^\alpha$, have the required properties. So the required pairs for a skew strong starter in $Z_{p^\alpha q}$ are

$$\{qa_i, qb_i\},\quad \{p^\alpha c_i, p^\alpha d_i\} \text{ and } dPICH_{M/d}^{\chi(p,q)} \text{ for all } p^\alpha \neq d \mid p^\alpha.$$

Now deal with the induction step. Suppose a skew strong starter in $Z_{p^\alpha q^{\beta-1}}$ exists, say $\{a_i, b_i\}$. Again by Lemma 2.2.

$$Z_{p^\alpha q^\beta} = qZ_{p^\alpha q^{\beta-1}} \cup \left\{ \bigcup_{d|p^\alpha} d\{x \in Z_{M/d}; (x, M/d) = 1\} \right\}$$

For the set $\{x \in Z_{M/d}; (x, m/d) = 1, d \neq p^\alpha\}$, by Lemma 2.4 the pairs $PICH_{M/d}^{\chi(p,q)}$ have the required properties; and for the set $\{x \in Z_{q^\beta}; (x, q^\beta) =$

1}, by Theorem 2.1 the pairs PIR_{q^β} have the required properties. Therefore the required pairs for a skew strong starter are

$$\{qa_i,\ qb_i\},\ dPICH_{M/d}^{\chi(p,q)} \text{ for all } p^\alpha \neq d \mid p^\alpha \text{ and } p^\alpha PIR_{q^\beta}.$$

Theorem 2.3. *If $p = 2^n \cdot a + 1 \geq 7$, $q = 2^m \cdot b + 1 \geq 7$, $m \neq n$ are primes, a, b are odd, then there exists a skew strong starter in Z_{pq} and hence a Z-cyclic Room square of order $pq + 1$.*

Proof: By Lemma 2.2, $Z_{pq} = qZ_p \cup \{x \in Z_{pq}; p \nmid x,\ q \nmid x\} \cup pZ_q$. Since $m \neq n$, it follows by Lemma 2.4(2) that the pairs $PICH_{pq}^{(2)}$ have the required properties, so the required pairs for a skew strong starter are the following:

$$qSST_p,\ PICH_{pq}^{(2)} \text{ and } pSST_q.$$

where SST_p, SST_q are skew strong starters in Z_p, Z_q given in Lemma 2.2.

Corollary 2.3.1. *Let $p = 2^n a + 1$ be a prime, where $a > 1$ odd, and $n \neq 2$. If there exists a skew strong starter in Z_{5p} then there is also one in Z_{5p^α}.*

Proof: By hypothesis a skew strong starter exists in Z_{5p} so the case $\alpha = 1$ is true. Deal with the induction step. By Lemma 2.2

$$Z_{5p^\alpha} = pZ_{5p^{\alpha-1}} \cup \{x \in Z_{5p^\alpha}; (x, 5p^\alpha) = 1\} \cup 5\{x \in Z_{p^\alpha}; (x, p^\alpha) = 1\}.$$

By (2.1.1) and Lemma 2.4(2) the pairs PIR_{p^α} and $PICH_{5p^\alpha}^{(2)}$ have the required properties and by the induction hypothesis a skew strong starter in $Z_{5p^{\alpha-1}}$ exists, say $\{a_i,\ b_i\}$. Then for the required pairs for a skew strong starter we take

$$\{pa_i,\ pb_i\},\quad PICH_{5p^\alpha}^{(2)},\quad 5PIR_{p^\alpha}.$$

Example 2.2: There exists a skew strong starter in $Z_{5\cdot 7^2}$, since $\{1,2\}$, $\{3,5\}, \{4,7\}, \{6,10\}, \{12,17\}, \{21,27\}, \{15,22\}, \{24,32\}, \{19,28\}, \{20,30\}$, $\{33,9\}, \{14,26\}, \{16,29\}, \{11,25\}, \{8,23\}, \{18,34\}, \{31,13\}$ is a skew strong starter in Z_{35}.

Corollary 2.3.2. *Let p, q be primes, $p = 2^n a + 1 \geq 7, a > 1$ odd, $q = 2^m + 1 \geq 7$, $m \neq n$, α be a positive integer. Then there exists a skew strong starter in $Z_{p^\alpha q}$ and hence a Z-cyclic Room square of order $p^\alpha q + 1$.*

Proof: Same as Corollary 2.3.1 with 5 replaced by q.

Example 2.3: There exists a skew strong starter in $Z_{7^2\cdot 17}$ and $Z_{11^2\cdot 17}$.

Theorem 2.4. *If, for $i = 1, 2, \cdots, n$, $p_i = 2^{n_i} u a_i + 1$ are distinct primes, u, a_i, are odd, $ua_i > 1, \alpha_i$ are positive integers, $M = \prod_{i=1}^{n} p_i^{\alpha_i}$, then there* *exists a skew strong starter in Z_M, and hence a Z-cyclic Room square of order $M+1$.*

Proof: Proceed by induction on n. The case $n=1$ follows from Theorem 2.1 and the case $n=2$ follows from Theorem 2.2. Now deal with the induction step, suppose that there exists a skew strong starter in Z_N where $N=\prod_{i=1}^{n-1} p_i^{\alpha_i}$. We want to show that there exists a skew strong starter in Z_M. We deal with this by induction on α_n. For the case $\alpha_n=1$, let ω be a common primitive root of $p_i^{\alpha_i}$ $i=1,2,\cdots,n-1$ and p_n. By Lemma 2.2

$$Z_{Np_n}=p_nZ_N\cup\left\{\bigcup_{N\neq d|N} d\{x\in Z_{M/d};(x,M/d)=1\}\right\}\cup NZ_{p_n}$$

By the induction hypothesis there exists a skew strong starter in Z_N, say $\{a_i,b_i\}$, by hypothesis of p_n there exists a skew strong starter in Z_{p_n} say $\{c_j,d_j\}$, and by Lemma 2.4 the pairs $PICH_{M/d}^{\chi(p_i)}$, where $N\neq d\mid N$, have the required properties, so the required pairs for a skew strong starter in Z_M are

$$\{p_na_i,p_nb_i\},\ N\{c_j,d_j\}\text{ and }dPICH_{M/d}^{\chi(p_i)}\text{ where }N\neq d\mid N.$$

Now deal with the induction step. Suppose there is a skew strong starter in $Z_{Np_n^{\alpha_n-1}}$. Then by Lemma 2.2 again,

$$Z_M=p_nZ_{M/p_n}\cup\left\{\bigcup_{d|N} d\{x\in Z_{M/d};(x,M/d)=1\}\right\}$$

and by the same argument, the required pairs for a skew strong starter in Z_M are

$$\{p_na_i,p_nb_i\},\ NPIR_{p_n^{\alpha_n}}\text{ and }dPICH_{M/d}^{\chi(p_i)}\text{ where }N\neq d\mid N,$$

where $\{a_i,b_i\}$ is a skew strong starter for $Z_{Np_n^{\alpha_n-1}}$.

Corollary 2.4.1. *Let $p_1,\cdots,p_n$ be distinct primes. Let $p_i=2^{m_i}a_i+1\geq 7$, where a_i are odd, α_i are positive integers satisfying the following two conditions;*

(1) $\alpha_j=1$ *whenever* $a_j=1$

(2) $a_{i_j}\geq 3\ \ \forall\, j=1,2,\cdots,k$; *whenever* $m_{i_1}=m_{i_2}=\cdots=m_{i_k}$

then there exists a skew strong starter in $Z_{\prod_{i=1}^n p_i^{\alpha_i}}$ and hence a Z-cyclic Room square of order $(\prod_{i=1}^n p_i^{\alpha_i})+1$.

Example 2.4: There exists a skew strong starter in $Z_{7^2\cdot 11\cdot 17\cdot 257}$. Since

$$\begin{aligned} Z_{7^2\cdot 11\cdot 17\cdot 257} = {} & 257Z_{7^2\cdot 11\cdot 17} \cup \{x \in Z_{7^2\cdot 11\cdot 17\cdot 257}; (x, 7^2\cdot 11\cdot 17\cdot 257) = 1\} \\ & \cup 17\{x \in Z_{7^2\cdot 11\cdot 257}; (x, 7^2\cdot 11\cdot 257) = 1\} \\ & \cup 11\{x \in Z_{7^2\cdot 17\cdot 257}; (x, 7^2\cdot 17\cdot 257) = 1\} \\ & \cup 7\{x \in Z_{7\cdot 11\cdot 17\cdot 257}; (x, 7\cdot 11\cdot 17\cdot 257) = 1\} \\ & \cup 7^2\{x \in Z_{11\cdot 17\cdot 257}; (x, 11\cdot 17\cdot 257) = 1\} \\ & \cup 11\cdot 17\{x \in Z_{7^2\cdot 257}; (x, 7^2\cdot 257) = 1\} \\ & \cup 7\cdot 11\{x \in Z_{7\cdot 17\cdot 257}; (x, 7\cdot 17\cdot 257) = 1\} \\ & \cup 7^2\cdot 11\{x \in Z_{17\cdot 257}; (x, 17\cdot 257) = 1\} \\ & \cup 7\cdot 17\{x \in Z_{7\cdot 11\cdot 257}; (x, 7\cdot 11\cdot 257) = 1\} \\ & \cup 7^2\cdot 17\{x \in Z_{11\cdot 257}; (x, 11\cdot 257) = 1\} \\ & \cup 7\cdot 11\cdot 17\{x \in Z_{7\cdot 257}; (x, 7\cdot 257) = 1\} \cup 7^2\cdot 11\cdot 17 Z_{257}. \end{aligned}$$

Here $7 = 2\cdot 3+1$, $11 = 2\cdot 5+1$, $17 = 2^4+1$, $257 = 2^8+1$.

Corollary 2.4.2. *Let $p_1, \cdots, p_n$ are distinct primes. Let $p_i = 2^{m_i}\cdot a_i + 1 \geq 7$, a_i odd, α_i positive integers satisfying the following conditions.*

(1) *$\alpha_j = 1$ whenever $a_j = 1$,*

(2) *$a_{i_j} > 1$ for $j = 1, 2$ whenever $m_{i_1} = m_{i_2}$ where $i_1 \neq i_2$,*

(3) *$m_i \neq 2$ $(i = 1, 2, \cdots, n)$,*

(4) *there exists a (skew) strong starter in $Z_{5\cdot p_i}$ for all $i = 1, 2, \cdots, n$.*

Then there exists a (skew) strong starter in $Z_{5\cdot \prod_{i=1}^n p_i^{\alpha_i}}$ and hence a Z-cyclic Room square of order $5\cdot(\prod_{i=1}^n p_i^{\alpha_i}) + 1$.

Example 2.5: There exists a skew strong starter in $Z_{5\cdot 7^2\cdot 11}$, since

$$\begin{aligned} Z_{5\cdot 7^2\cdot 11} = {} & 11Z_{5\cdot 7^2} \cup 7\{x \in Z_{5\cdot 7\cdot 11}; (x, 5\cdot 7\cdot 11) = 1\} \cup \\ & 7^2\{x \in Z_{5\cdot 11}; (x, 5\cdot 11) = 1\} \cup 5\{x \in Z_{7^2\cdot 11}; (x, 7^2\cdot 11) = 1\} \cup \\ & 5\cdot 7\{x \in Z_{7\cdot 11}; (x, 7\cdot 11) = 1\} \cup 5\cdot 7^2 Z_{11} \end{aligned}$$

and

$$Z_{5\cdot 7^2} = 7Z_{5\cdot 7} \cup \{x \in Z_{5\cdot 7^2}; (x, 5\cdot 7^2) = 1\} \cup 5\{x \in Z_{7^2}; (x, 7^2) = 1\}.$$

3 Patterned starters

Let G be an additive abelian group of order $2v+1$. The set $P = \{\{x_i, -x_i\}; i = 1, 2, \cdots, v\}$ is a starter, called a patterned starter. Let $S = \{\{x_i, y_i\}; i = 1, 2, \cdots, v\}$ and $T = \{\{u_i, v_i\}; i = 1, 2, \cdots, v\}$ be two starters, then, for each i, there is a unique j such that $x_i - y_i = \pm(u_j - v_j)$. Without loss of generality, we can suppose that $x_i - y_i = u_j - v_j$. Let $d_i = u_j - x_i = v_j - y_i$. Then if the d_i are all distinct and nonzero we say that S and T are orthogonal starters.

Theorem 3.1. [5] *If there exists a strong starter S in an additive abelian group of odd order $2v+1$, then the starters S, $-S$ and P are pairwise orthogonal.*

We therefore have the following theorem.

Theorem 3.2. *There exists a patterned skew Z-cyclic Room square of order $2v$ whenever $2v - 1 = \prod_{i=1}^{n} p_i^{\alpha_i}$ (where p_i are as in Corollary 2.4.1 or 2.4.2).*

Acknowledgements. I would like to thank my supervisor, Dr. Ian Anderson, for his advice and the Tatung Institute of Technology for its financial support. I would also like to thank the referee for his valued suggestions on the representation of this paper.

References

[1] I. Anderson, *Combinatorial designs*, Ellis Horwood, Chichester, 1990.

[2] I. Anderson and Y.S. Liaw, Z-cyclic Room squares, *Bull. Inst. Combinatorics and Applications* 5 (1992), 51–57.

[3] K. Byleen, On Stanton and Mullin's construction of Room squares, *Ann. Math. Statist.* **11** (1970), 1122–1125.

[4] J.H. Dinitz and D.R. Stinson, *Contemporary design theory: A collection of surveys*, John Wiley and Sons, 1992.

[5] J.D. Horton, Room designs and one-factorizations, *Aeq. Math.* **22** (1981), 56–63.

[6] F.K. Hwang, Strong starters, balanced starters and partitionable starters, *Bull. Inst. Math. Academia Sinica* **11** (1983), 561–572.

[7] R.C. Mullin and W.D. Wallis, The existence of Room squares, *Aeq. Math.* **13** (1975), 1–7.

[8] K.T. Phelps and S.A. Vanstone, Isomorphism of strong starters in cyclic groups, *J. Combinatorial Theory, Series A* **57** (1991), 287–293.

[9] R.C. Mullin and E. Nemeth, An existence theorem for Room squares, *Canad. Math. Bull.* **12** (1969), 493–497.

[10] R.G. Stanton and R.C. Mullin, Construction of Room squares, *Ann. Math. Statist.* **39** (1968), 1540–1548.