# SOME CONSTRUCTIONS OF COMBINATORIAL DESIGNS

by
Yn Sheng Liaw

A thesis submitted to the Faculty of
Science, University of Glasgow, for the
degree of Doctor of Philosophy

Department of Mathematics
University of Glasgow
April,1994

ProQuest LLC.
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106 – 1346

# Contents

## Chapter 4 Z-cyclic triple whist tournaments

## Chapter 5 Z-cyclic Room squares

# Preface

This thesis is submitted to the University of Glasgow in accordance with the requirements for the degree of Doctor of Philosophy.

I would like to express my sincere gratitude to my superisor Dr. Ian Anderson for his advice, encouragement and guidance throughout the period of my research.

I would also like to record my thanks to Professor R. W. Ogden for providing me with the opportunity to study at Glasgow, and also to Professor P. F. Smith.

I should also like to thanks Dr. T. S. Lin, Professor, President of Tatung Institute of Technology, who is also Chairman of Tatung Company, for financial support, without which this thesis would not have been possible.

# Summary

In this thesis, we are concerned with some combinatorial designs — 1-rotational ($v$, 4, 1) designs, referee squares, triple whist tournaments and Room squares. Many of our constructions are Z-cyclic.

Chapter 2 is devoted to 1-rotational ($v$, 4, 1). The result is as follows.

**Theorem 2.3.2** If $v = 3\alpha\beta+1$ where $(3\alpha+1, 4, 1)$, $(3\beta+1, 4, 1)$ 1-rotational designs exist and $\beta \equiv \pm 1 \pmod 3$ then a 1-rotational $(v, 4, 1)$ design exists.

**Corollary 2.3.3** If $v = 3p_1^{\alpha_1} \cdots p_n^{\alpha_n} + 1$ where $p_i$ either are primes $\equiv 1 \pmod 4$ or $\frac{1}{3}(4^m - 1)$ and there is at most one $p_i$ such that $3p_i = 4^m - 1$ where $m \equiv 0 \pmod 3$ (and $\alpha_i = 1$ in this case), then a 1-rotational ($v$, 4, 1) design exists.

In Chapter 3, a method of constructing Z-cyclic referee squares is given, and we list Z-cyclic referee squares of side $2n - 1$ when $n < 17$ except 4 and 5. There are no Z-cyclic referee squares of side 7 and 9. We also show the following result:

**Corollary 3.4.4** If $m$ is an odd composite integer then there exists a referee square of side $m$.

Chapter 4 is devoted to triple whist tournaments. The results are as follow:

**Theorem 4.3.4** For all prime $p = 8t + 1$, $t$ odd, there exists Z-cyclic $TWh(p)$.

**Proposition 4.4.1** Let $p = 2^k t + 1$ be a prime where $t > 1$ is odd, $k \geq 2$ integer, $d = 2^k$, $m = 2^{k-1}$, $n = 2^{k-2}$ and let $\omega$ be a primitive root mod $p$. If $a_0, a_1, \cdots, a_{m-1}$ $c_0, c_1, \cdots, c_{n-1}$ are integers such that

1. $a_i + i \pmod d \in \{m, m+1, \cdots, d-1\}$ and are all distinct for

$i = 0, 1, \cdots, m-1$.

2. $\frac{\omega^{a_i}-1}{\omega^{a_0}-1} = \omega^{b_i}$, where $b_i + i$ are incongruent mod $m$ for $i = 0, 1, \cdots, m-1$.

3. $\omega^{dc_i+(2i+1)} - \omega^{2i} = \omega^{r_{4i+1}}, \omega^{dc_i+(2i+1)} - \omega^{2i+a_{2i}} = \omega^{r_{4i+2}}, \omega^{dc_i+(2i+1)+a_{2i+1}} - \omega^{2i+a_{2i}} = \omega^{r_{4i+3}}, \omega^{dc_i+(2i+1)+a_{2i+1}} - \omega^{2i} = \omega^{r_{4i+4}}$, for $i = 0, 1, \cdots, n-1$ where $\{r_i; i = 1, 2, \cdots, d\}$ is partitioned into two disjoint sets $\{r_{1,j}; j = 1, 2, \cdots, m\} \cup \{r_{2,j}; j = 1, 2, \cdots, m\}$ such that $r_{i,j}; j = 1, 2, \cdots, m$ are incongruent $\pmod{m}$ for $i = 1, 2$ respectively.

then the following table forms an initial round for a $Wh(p)$

$$(4.4.1) \qquad \{\{1, \omega^{a_0}; \omega^{dc_0+1}, \omega^{dc_0+1+a_1}\}, \{\omega^2, \omega^{2+a_2}; \omega^{dc_1+3}, \omega^{dc_1+3+a_3}\}, \cdots,$$
$$\{\omega^{2n-2}, \omega^{2n-2+a_{2n-2}}; \omega^{dc_n+2n-1}, \omega^{dc_n+2n-1+a_{2n-1}}\}\} \otimes \{1, \omega^d, \cdots, \omega^{d(t-1)}\}.$$

Furthermore, if in (3) the partition is restricted so that $\{r_i;\ i = 1, 2, \cdots, d\}$ $=\{r_{2i-1}; i = 1, 2, \cdots, m\} \cup \{r_{2i}; i = 1, 2, \cdots, m\}$ where, in both sets, the numbers are incongruent mod $(d)$, then the table (*4.4.1*) form an initial round for a $TWh(p)$

In particular, if we choose $a_{2i} = \frac{p+1}{2} = mt + 1$, $a_{2i+1} = a_1$ and $c_i = 0$ for $i = 0, 1, \cdots, n-1$ then the games becomes

$$\{\{1, -\omega; \omega, \omega^{1+a_1}\}, \{\omega^2, -\omega^3; \omega^3, \omega^{3+a_1}\}, \cdots,$$
$$\{\omega^{2n-2}, -\omega^{2n-1}; \omega^{2n-1}, \omega^{2n-1+a_1}\} \otimes \{1, \omega^d, \cdots, \omega^{d(t-1)}\}$$

Since $a_{2i} + 2i = mt + 2i + 1$ are odd, this forces $a_{2i+1} + 2i + 1 = a_1 + 2i + 1$ to be even, so $a_1 \equiv m - 1 \pmod{d}$. Therefore there are $t$ candidates for $a_1$, and a $TWh(p)$ exists provided that there exists $\omega$ and $a_1 \equiv 2^{k-1} - 1 \pmod{d}$ such that

$$(A) \qquad \begin{array}{ll} (i) & 2(\omega^{a_1+1} - 1) = \Box \\ (ii) & (\omega + 1)(\omega^{a_1} - 1) = \Box \\ (iii) & (\omega - 1)(\omega^{a_1} + 1) = \Box \end{array}$$

Using this we prove that a Z-cyclic $TWh(p)$ exits for all $p < 16097$ $(p \neq 257)$.

Using a similar method, we also show that the games

$$\{\{\omega^{2i}, \omega^{2i+a_0}; \omega^{m+2i}, -\omega^{m+2i+1}\}; i = 0, 1, \cdots, n-1\} \otimes \{1, \omega^d, \cdots, \omega^{d(t-1)}\}$$

latex form an initital round of a $TWh(p)$ provided that there exists $\omega$ and $a_0 \equiv 2^{k-1} + 1 \pmod{2^k}$ such that

$$(B) \qquad \begin{array}{ll} (i) & (\omega + 1)(\omega^{a_0} - 1) \neq \Box \\ (ii) & (\omega^{2^{k-1}} - 1)(\omega^{a_0} + \omega^{2^{k-1}+1}) \neq \Box \\ (iii & )(\omega^{2^{k-1}+1} + 1)(\omega^{a_0} - \omega^{2^{k-1}}) \neq \Box \end{array}$$

**Theorem 4.5.7** Let $p_i = 2^{m_i} t_i + 1$, $i = 1, 2, \cdots, r$ be primes, $m_i \geq 2$ be positive integers, $t_i$ be odd integers. If Z-cyclic $TWh(p_i)$ exist then a Z-cyclic $TWh(\prod_{i=1}^{r} p_i^{\alpha_i})$ exists for any positive integers $\alpha_i$.

**Theorem 4.6.1** Let $p_1 = 4t_1 + 3$, $p_i = 2^{m_i} t_i + 1$, $i = 2, 3, \cdots, r$ be primes, $m_i \geq 2$ be positive integers, $t_i$, $i = 1, 2, \cdots, n$ be odd integers. If Z-cyclic $TWh(p_1 + 1)$, $TWh(p_i)$ exist then a Z-cyclic $TWh(p_1 \cdot \prod_{i=2}^{r} p_i^{\alpha_i} + 1)$ exists for any positive integers $\alpha_i$ $i = 2, 3, \cdots, r$.

We also show that if $p = 8n + 5$ is prime, a Z-cyclic $Wh(8n + 5)$ exists with non-patterned initial round.

Finally, we construct Z-cyclic Room squares in Chapter 5. We show the following result:

**Theorem 5.3.5** If $p_i = 2^{n_i} a_i + 1$ are primes, $a_i$, are odd, $a_i > 1, \alpha_i$ are positive integers $i = 1, 2, \cdots, r$, then there exists a skew strong in $Z_{\prod_{i=1}^{r} p_i^{\alpha_i}}$, and hence a Z-cyclic Room square of order $\prod_{i=1}^{r} p_i^{\alpha_i} + 1$

Further, some results involving Fermat primes are obtained.

# Chapter 1

# Introduction

In this introduction, we give some basic definitions, establish standard notations, and present some fundamental results which we apply in this thesis.

## 1.1 Groups

Let $S$ be a set and let $S \times S$ denote the set of all ordered pairs $(s,\ t)$ with $s \in\ S,\ t \in\ S$. Then a mapping from $S \times S$ into $S$ will be called a (binary) operation on $S$.

A *group* $G$ is a nonempty set of elements together with a binary operation, which we denote by $\cdot$, such that the following three properties hold:

1. $\cdot$ is *associative*,

2. There is an *identity element* $e$ in $G$ such that for all $a \in G$

$$a \cdot e = e \cdot a = a$$

3. For each $a \in G$, there exists an *inverse element* $a^{-1} \in G$ such that

$$a \cdot a^{-1} = a^{-1} \cdot a = e.$$

If the group also satisfies

4. For all $a,\ b \in G$,

$$a \cdot b = b \cdot a,$$

then the group is called *Abelian* (or *commutative*).

Note: We usually omit the dot and write $ab$ for $a \cdot b$.

A group $G$ is called *finite* if $G$ is a finite set. In this case, the number of elements in $G$ is called the *order* of $G$ and is denoted by $|G|$. A nonempty subset $G'$ of a group $G$ which is itself a group, under the same operation, is called a *subgroup* of $G$.

If $a \in G$ we define $a^n$ for any integer $n$ by the following relations:

$$a^0 = e, \quad a^n = aa^{n-1}, \quad a^{-n} = (a^{-1})^n \text{ for } n > 0.$$

If $a^n = e$ for some positive integer $n$ there will be a smallest $n > 0$ with this property. The integer $n$ is called the *order of the element* $a$.

If $H$ is a subgroup of a finite group $G$, then for any element $a$ in $G$ there is an integer $n$ such that $a^n \in H$. If $a$ is already in $H$, we simply take $n = 1$. If $a \notin H$ we can take $n$ to be the order of $a$, since $a^n = e \in H$. However, there may be a smaller positive power of $a$ which lies in $H$. By the Well-ordering Principle, there is a smallest positive integer $n$ such that $a^n \in H$. We call this integer the *indicator* of $a$ in $H$.

**Theorem 1.1.1 ([12])** *Let $H$ be a subgroup of a finite Abelian group $G$, where $H \neq G$. Choose an element $a$ in $G$, $a \notin H$, and let $h$ be the indicator of $a$ in $H$. Then the set of products*

$$H_1 = \{a^i x;\ x \in H \quad and \quad 0 \leq i \leq h-1\}$$

*is a subgroup of $G$ which contains $H$. Moreover, the order of $H_1$ is $h$ times that of $H$. i.e. $|H_1| = h|H|$. We write $H_1 = \langle H, a\rangle$.*

**Corollary 1.1.2** *Let $H_0$ be a subgroup of a finite Abelian group $G$, where $H_0 \neq G$. Then there is a finite number of $x_i \in G \quad i = 1, 2, \cdots, n$ such that*

$$H_0 \subsetneqq H_1 = \langle H_0, x_1\rangle \subsetneqq H_2 = \langle H_1, x_2\rangle \subsetneqq \cdots \subsetneqq H_n = \langle H_{n-1}, x_n\rangle = G$$

*where the indicator of $x_i$ in $H_{i-1}$ is $h_i$ so that $x_i^{h_i} \in H_i$ but $x_i^j \notin H_i$ for $j < h_i$ and $h_1 h_2 \cdots h_n |H_0| = |G|$.*

## 1.2 Finite fields

It is well know [28] that for every prime $p$ and every positive integer $n$ there exists a finite field with $p^n = q$ elements (called the Galois field of order $q$). We shall denote this field by $F_q$.

For a finite field $F_q$ the multiplicative group $F_q^*$ of nonzero elements of $F_q$ is cyclic. A generator of the cyclic group $F_q^*$ is called a *primitive element* of $F_q$.

**Example 1.3.1** A finite field of 4 elements, take $0,\ 1,\ x,\ x+1$ as elements, whose addition and multiplication are carried out as follows.

| + | 0 | 1 | x | x+1 |
|---|---|---|---|---|
| 0 | 0 | 1 | x | x+1 |
| 1 | 1 | 0 | x+1 | x |
| x | x | x+1 | 0 | 1 |
| x+1 | x+1 | x | 1 | 0 |

| × | 0 | 1 | x | x+1 |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | x | x+1 |
| x | 0 | x | x+1 | 1 |
| x+1 | 0 | x+1 | 1 | x |

In this field $x$ is a primitive element.

**Theorem 1.2.1 (Cohen's theorem [18])** *Let $q$ be a prime power. If $g(x)$ is a quadratic polynomial over a finite field $F_q$ not of the form $a(x+b)^2$, where $a$ is a non-square in $F_q$, and $q > 211$, then $g(\omega)$ is a non-zero square in $F_q$ for some primitive element $\omega$ of $F_q$.*

**Theorem 1.2.2 (Mann's Lemma [29])** *Let $v = 4m+1$ be a power of a prime and let $\omega$ be a primitive element of $F_v$. Then there exist odd integers $c$, $d$ such that*

$$\frac{\omega^c + 1}{\omega^c - 1} = \omega^d$$

## 1.3 Primitive roots

Let $a$ and $m$ be relatively prime integers, with $m \geq 1$, and consider the positive powers of $a$

$$a,\ a^2,\ a^3, \cdots$$

We know, from the Euler-Fermat theorem, that $a^{\phi(m)} \equiv 1 \pmod{m}$. However, there may be an earlier power $a^f$ such that $a^f \equiv 1 \pmod{m}$. The smallest positive integer $f$ such that $a^f \equiv 1 \pmod{m}$ is called the *order* of $a$ mod $m$, and is denoted by writing $f = ord_m a$. If $ord_m a = \phi(m)$ then $a$ is called a *primitive root* mod $m$.

**Example 1.3.1** The table of primitive roots:

| $p$ | primitive roots | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 3 | 2 | | | | | | | | | | | | | | | |
| 5 | 2 | 3 | | | | | | | | | | | | | | |
| 7 | 3 | 5 | | | | | | | | | | | | | | |
| 11 | 2 | 6 | 7 | 8 | | | | | | | | | | | | |
| 13 | 2 | 6 | 7 | 11 | | | | | | | | | | | | |
| 17 | 3 | 5 | 6 | 7 | 10 | 11 | 12 | 14 | | | | | | | | |
| 19 | 2 | 3 | 10 | 13 | 14 | 15 | | | | | | | | | | |
| 23 | 5 | 7 | 10 | 11 | 14 | 15 | 17 | 19 | 20 | 21 | | | | | | |
| 29 | 2 | 3 | 8 | 10 | 11 | 14 | 15 | 18 | 19 | 21 | 26 | 27 | | | | |
| 31 | 3 | 11 | 12 | 13 | 17 | 21 | 22 | 24 | | | | | | | | |
| 37 | 2 | 5 | 13 | 15 | 17 | 18 | 19 | 20 | 22 | 24 | 32 | 35 | | | | |
| 41 | 6 | 7 | 11 | 12 | 13 | 15 | 17 | 19 | 22 | 24 | 26 | 28 | 29 | 30 | 34 | 35 |
| 43 | 3 | 5 | 12 | 18 | 19 | 20 | 26 | 28 | 29 | 30 | 33 | 34 | | | | |
| 47 | 5 | 10 | 11 | 13 | 15 | 19 | 20 | 22 | 23 | 26 | 29 | 30 | 31 | 33 | 35 | 38 |
| | 39 | 40 | 41 | 43 | 44 | 45 | | | | | | | | | | |
| 53 | 2 | 3 | 5 | 8 | 12 | 14 | 18 | 19 | 20 | 21 | 22 | 26 | 27 | 31 | 32 | 33 |
| | 34 | 35 | 39 | 41 | 45 | 48 | 50 | 51 | | | | | | | | |
| 59 | 2 | 6 | 8 | 10 | 11 | 13 | 14 | 18 | 23 | 24 | 30 | 31 | 32 | 33 | 34 | 37 |
| | 38 | 39 | 40 | 42 | 43 | 44 | 47 | 50 | 52 | 54 | 55 | 56 | | | | |
| 61 | 2 | 6 | 7 | 10 | 17 | 18 | 26 | 30 | 31 | 35 | 43 | 44 | 51 | 54 | 55 | 59 |
| 67 | 2 | 7 | 11 | 12 | 13 | 18 | 20 | 28 | 31 | 32 | 34 | 41 | 44 | 46 | 48 | 50 |
| | 51 | 57 | 61 | 63 | | | | | | | | | | | | |
| 71 | 7 | 11 | 13 | 21 | 22 | 28 | 31 | 33 | 35 | 42 | 44 | 47 | 52 | 53 | 55 | 56 |
| | 59 | 61 | 62 | 63 | 65 | 67 | 68 | 69 | | | | | | | | |
| 73 | 5 | 11 | 13 | 14 | 15 | 20 | 26 | 28 | 29 | 31 | 33 | 34 | 39 | 40 | 42 | 44 |
| | 45 | 47 | 53 | 58 | 59 | 60 | 62 | 68 | | | | | | | | |

**Theorem 1.3.1** *Let g.c.d$\{a, \ m\} = (a, \ m) = 1$. Then $a$ is a primitive root mod $m$ if and only if the numbers*

$$a, \ a^2, \ \cdots, a^{\phi(m)}$$

*form a reduced residue system mod $m$ which, under multiplication, is an Abelian group.*

Note: If $p$ is a prime then the finite field $F_p$ is isomorphic with $Z_p$. In this case the primitive element in $F_p$ is a primitive root mod $p$.

## 1.4 Balanced incomplete block designs

**Definition** A balanced incomplete block design (BIBD) with parameters $(v, \ b, \ r, \ k, \ \lambda)$ where $k < v$ (sometime abbreviated to a $(v, \ k, \ \lambda)$-*BIBD*) is a pair $(\mathcal{V}, \ \mathcal{B})$ that satisfies the following conditions:

1. $\mathcal{V}$ is a set of $v$ elements (called points).
2. $\mathcal{B}$ is a family of $b$ subsets of $\mathcal{V}$, each of cardinality $k$ (called blocks).
3. Every pair of distinct points occurs in exactly $\lambda$ blocks.

Let $(\mathcal{V}, \ \mathcal{B})$ be a $(v, \ k, \ \lambda)$-*BIBD* and let $s < 2$ be a non-negative integer. Let $\lambda_s$ denote the number of blocks containing a given $s$-subset $S$. Let

$H = \{(X, B); X$ is a $(2-s)$-subset of $\mathcal{V}, S \cap X = \Phi, B$ is a block with $S \cup X \subseteq B\}$.

Counting in two ways the cardinality of $H$, we get

$$\lambda_s \binom{k-s}{2-s} = \lambda \binom{v-s}{2-s}$$

This number $\lambda_s$ is therefore independent of the choice of $S$. Thus we have

1. A $(v, \ k, \ \lambda)$-*BIBD* has $b = \frac{\lambda v(v-1)}{k(k-1)}$ blocks.

2. Each element occurs in $r$ blocks where

$$r = \frac{\lambda(v-1)}{k-1}.$$

Therefore, a necessary condition for the existence of a $(v,\ k,\ \lambda)$ -*BIBD* is

$$\begin{aligned} \lambda(v-1) &\equiv 0 \pmod{k-1} \\ \lambda v(v-1) &\equiv 0 \pmod{k(k-1)} \end{aligned}$$

When $k = 4,\ \lambda = 3$, a necessary and sufficient condition for the existence of a $(v,\ k,\ \lambda)$-BIBD was proved by Hanani in 1961.

**Theorem 1.4.1 ([23])** *A necessary and sufficient condition for the existence of a* $(v, k, \lambda)$*-BIBD of* $v$ *elements with* $k = 4$ *and* $\lambda = 3$ *is that*

$$v \equiv 0 \quad or \quad 1 \pmod 4$$

A parallel class of blocks of a design $(\mathcal{V}, \mathcal{B})$ is a subfamily $\mathcal{B}_1 \subset \mathcal{B}$ of disjoint blocks which cover $\mathcal{V}$ with exception of at most one point. A parallel class of blocks of a $(v, k, \lambda)$-*BIBD* has exactly $\frac{v}{k}$ blocks if $v \equiv 0 \pmod k$ and $\frac{v-1}{k}$ if $v \equiv 1 \pmod k$.

A $(v, k, \lambda)$-*BIBD* is resolvable if its family $\mathcal{B}$ of blocks can be partitioned into parallel classes. The number of parallel classes of blocks is

$$\begin{array}{lll} \frac{\lambda(v-1)}{k-1} & \text{for} & v \equiv 0 \pmod k \\ \frac{\lambda v}{k-1} & \text{for} & v \equiv 1 \pmod k \end{array}$$

**Theorem 1.4.2 ([24])** *A necessary and sufficient condition for the existence of a resolvable* $(v, 4, 1)$*-BIBD is that* $v \equiv 4 \pmod{12}$.

In this thesis, we will discuss some special classes of $(v,\ 4,\ 3)$-*BIBD*, called whist tournaments of order $v$, denoted by $Wh(v)$, and Triple Whist tournaments of order $v$ where $v = 4n$ or $v = 4n + 1$, denoted by $TWh(v)$. We also deal with a special case of $(v, 4, 1)$-*BIBD*, called 1-rotational $(v, 4, 1)$-designs although these are not resolvable.

## 1.5 Difference systems

Let $G$ be an Abelian group of order $v$, $B$ be a subset (block) with $k$ elements $a_1, a_2, \cdots, a_k$ of $G$. The $k(k-1)$ differences $\pm(a_i - a_j)$, $i, \ j = 1, 2, \cdots, k, \ i \neq j$, arising from all distinct pairs of elements in the block $B$ are called the differences arising from the block $B$. From the block $B = \{a_1, a_2, \cdots, a_k\}$ we can form a set of $v$ blocks $\{a_1+\omega, a_2+\omega, \cdots a_k+\omega\}$, where $\omega$ runs over all the different elements of $G$. This set of $v$ blocks is said to be obtained by developing the initial block $B$.

Let $B_1, \ B_2, \ \cdots, \ B_t$ be blocks of size $k$ in an Abelian group $G$ of order $v$ such that the differences arising from the $B_i$ given each nonzero element of $G$ exactly $\lambda$ times. Then $B_1, \ B_2, \ \cdots, \ B_t$ are said to form a $(v, k, \lambda)$-difference system in $G$.

**Theorem 1.5.1** (**[15]**) *Let $G$ be an Abelian group of order $v$. If there exists a set of $t$ blocks $B_1, B_2, \cdots, B_t$ such that $B_1, B_2, \cdots, B_t$ form a $(v, k, \lambda)$-difference system in $G$, then we get a $(v, \ k, \ \lambda)$-BIBD design by developing the initial blocks $B_1, B_2, \cdots, B_t$.*

**Theorem 1.5.2** (**[15]**) *Let $G$ be an Abelian group of order $n$. To the elements of $G$ adjoin a new symbol $\infty$. If it is possible to find a set of $g + s$ blocks*

$$B_1, B_2, \cdots, \ B_g, \ B_1', \ B_2', \cdots, B_s' \tag{1.5.1}$$

*such that*

1. *Each of the blocks $B_1, \ B_2, \ \cdots, \ B_g$ contains $k$ distinct elements which are all different from $\infty$ while each of the blocks $B_1', \ B_2', \cdots, B_s'$ contains $\infty$ and $k-1$ other distinct elements.*

2. *The differences arising from the blocks $B_1, \ B_2, \cdots, B_g, B_1'', \ B_2'', \cdots, \ B_s''$, where the blocks $B_j''$ are obtained from $B_j'$ $\ j = 1, 2, \cdots, s$ by deleting the adjoined symbol $\infty$, gives each nonzero element of $G$ exactly $\lambda$ times.*

3. *$kg + \lambda = ns, \ \lambda = (k-1)s$.*

*then we get a BIBD with parameters*

$$v = n + 1, \ b = n(g + s), \ r = ns, \ k, \ \lambda$$

*by developing the blocks in (1.5.1), where $\infty$ remains unchanged during development.*

## 1.6 Starters and adders

If $G$ is an Abelian group of order $2n+1$ with identity 0 and $G^* = G - \{0\}$ then a *starter* $X$ for $G$ is a partition of $G^*$ into pairs such that $\{\pm(x_i - y_i); \{x_i, y_i\} \in X\} = G^*$. In fact, a starter $X$ for $G$ is a difference system, from which we can develop a resolvable $(2n+1,\ 2,\ 1)$-design. A starter is a *strong starter* if the sums $x_i + y_i$ of pairs $\{x_i,\ y_i\}$ are all distinct and non-zero. A *patterned starter* is a starter whose pairs are of the form $\{x_i,\ -x_i\}$. A starter $X = \{\{x_i, y_i\}; 1 \leq i \leq n\}$ is said to be *skew* if $\{\pm(x_i + y_i); 1 \leq i \leq n\} = G^*$. An *adder* $A = \{a_i; i = 1, 2, \cdots, n\}$ for a starter $X = \{\{x_i,\ y_i\}; i = 1, 2, \cdots, n\}$ in $G$ is a set of $n$ distinct non-zero elements $a_1, a_2, \cdots, a_n$ of $G$ such that $\{x_i + a_i, y_i + a_i; i = 1, 2, \cdots, n\} = G^*$.

**Lemma 1.6.1** *If* $X = \{\{x_i,\ y_i\};\ i = 1, 2, \cdots, n\}$ *is a strong starter in G, then the elements* $a_i = -(x_i + y_i)$ *form an adder.*

Note: If $A = \{a_i; i = 1, 2, \cdots, n\}$ is an adder for a starter $X = \{\{x_i, y_i\}; i = 1, 2, \cdots, n\}$ then $Y = \{\{x_i + a_i, y_i + a_i\}; i = 1, 2, \cdots, n\}$ is also a starter.

**Example 1.6.1** $X_1 = \{\{1,4\}, \{2,6\}, \{3,5\}, \{7,8\}\}$ is a starter in $Z_9$, since the differences between pairs are $\pm 3, \pm 4, \pm 2, \pm 1$. $A = \{7, 4, 2, 5\}$ is an adder for $X_1$, because the sums $1 + 7 = 8, 4 + 7 = 2, 2 + 4 = 6, 6 + 4 = 1, 3 + 2 = 5$, $5 + 2 = 7, 7 + 5 = 3, 8 + 5 = 4$ are all distinct and nonzero. However, $X_2 = \{\{1,2\}, \{5,7\}, \{3,6\}, \{4,8\}\}$ is a starter in $\mathbb{Z}_9$ but there is no adder for $X_2$.

**Example 1.6.2** $X_3 = \{\{8,9\}, \{4,6\}, \{2,5\}, \{10,3\}, \{1,7\}\}$ is a strong starter in $Z_{11}$. It forms a starter because the differences are $\pm 1, \pm 2$, $\pm 3$, $\pm 4$, $\pm 5$; and the starter $X_3$ is strong because the sums $8+9 = 6, 4+6 = 10, 2+5 = 7, 10+3 = 2, 1+7 = 8$ are all distinct and nonzero. Thus $A_1 = \{5, 1, 4, 9, 3\}$ is an adder for $X_3$. However, there is another adder for $X_3$, namely, $A_2 = \{8, 6, 2, 10, 7\}$.

**Notation:** $\{A, B, \cdots\} \otimes \{1, \omega^d, \cdots, \omega^{nd}\} = \{A, B, \cdots, \omega^d A,\ \omega^d B, \cdots\}$ where $A, B, \cdots$ are sets and $\omega, d, n$ are intgers.

We list all starters in $Z_7$, $Z_{11}$ and $Z_{13}$.

(A). For any primitive root $\omega$ of 7, the following three starters are all the starters in $Z_7$.

1. $\{\{1,\ \omega\},\{\omega^2,\ \omega^3\},\{\omega^4,\omega^5\}\}\otimes\{1,\ \omega\}$. Skew strong starters
2. $\{\{1,\ \omega^3\},\{\omega,\ \omega^4\},\{\omega^2,\omega^5\}\}$. patterned starter

(B) For any primitive root $\omega$ of 11 there exists a positive integer $a$ such that the following are all the 25 starters in $Z_{11}$. The possible pairs of $(\omega, a)$ are $(2,1),(6,9),(7,3),(8,7)$.

1. $\{\{1,\ \omega^a\},\{\omega^{2a},\ \omega^{3a}\},\{\omega^{4a},\omega^{5a}\},\{\omega^{6a},\ \omega^{7a}\},\{\omega^{8a},\ \omega^{9a}\}\}\otimes\{1,\ \omega\}$.
2. $\{\{1,\ \omega^{3a}\},\{\omega^{2a},\ \omega^{5a}\},\{\omega^{4a},\omega^{7a}\},\{\omega^{6a},\ \omega^{9a}\},\{\omega^{8a},\ \omega^a\}\}\otimes\{1,\ \omega\}$.
3. $\{\{1,\ \omega^{5a}\},\{\omega^{2a},\ \omega^{7a}\},\{\omega^{4a},\omega^{9a}\},\{\omega^{6a},\ \omega^a\},\{\omega^{8a},\ \omega^{3a}\}\}$.
4. $\{\{1,\ \omega^{3a}\},\{\omega^a,\ \omega^{2a}\},\{\omega^{4a},\omega^{9a}\},\{\omega^{5a},\ \omega^{7a}\},\{\omega^{6a},\ \omega^{8a}\}\}\otimes\{1,\ \omega,\cdots,\omega^9\}$.
5. $\{\{1,\ \omega^{4a}\},\{\omega^{2a},\ \omega^{6a}\},\{\omega^{3a},\omega^{9a}\},\{\omega^{5a},\ \omega^{7a}\},\{\omega^a,\ \omega^{8a}\}\}\otimes\{1,\ \omega,\cdots,\omega^9\}$.

(C) For any primitive root $\omega$ of 13 there exists a positive integer $a$ such that the following are all the 133 starters in $Z_{13}$. The possible pairs of $(\omega, a)$ are $(2,1),(6,5),(7,11),(11,7)$

1. $\{\{1,\omega^{2a}\},\{\omega^a,\omega^{3a}\},\{\omega^{4a},\omega^{6a}\},\{\omega^{5a},\omega^{7a}\},\{\omega^{8a},\omega^{10a}\},\{\omega^{9a},\omega^{11a}\}\}$
   $\otimes\{1,\omega,\omega^2,\omega^3\}$.
2. $\{\{1,\omega^a\},\{\omega^{4a},\omega^{5a}\},\{\omega^{8a},\omega^{9a}\},\{\omega^{2a},\omega^{7a}\},\{\omega^{6a},\omega^{11a}\},\{\omega^{10a},\omega^{3a}\}\}$
   $\otimes\{1,\omega,\omega^2,\omega^3\}$.
3. $\{\{1,\omega^{3a}\},\{\omega^{4a},\omega^{7a}\},\{\omega^{8a},\omega^{11a}\},\{\omega^a,\omega^{6a}\},\{\omega^{5a},\omega^{10a}\},\{\omega^{9a},\omega^{2a}\}\}$
   $\otimes\{1,\omega,\omega^2,\omega^3\}$.
4. $\{\{1,\omega^{6a}\},\{\omega^{2a},\omega^{8a}\},\{\omega^{4a},\omega^{10a}\},\{\omega^a,\omega^{7a}\},\{\omega^{3a},\omega^{9a}\},\{\omega^{5a},\omega^{11a}\}\}$.
5. $\{\{1,\omega^a\},\{\omega^{2a},\omega^{10a}\},\{\omega^{3a},\omega^{6a}\},\{\omega^{4a},\omega^{7a}\},\{\omega^{5a},\omega^{8a}\},\{\omega^{9a},\omega^{11a}\}\}$
   $\otimes\{1,\omega,\cdots,\omega^{11}\}$.
6. $\{\{1,\omega^a\},\{\omega^{2a},\omega^{6a}\},\{\omega^{3a},\omega^{7a}\},\{\omega^{4a},\omega^{8a}\},\{\omega^{5a},\omega^{10a}\},\{\omega^{9a},\omega^{11a}\}\}$
   $\otimes\{1,\omega,\cdots,\omega^{11}\}$.

7. $\{\{1,\omega^{a}\},\{\omega^{2a},\omega^{10a}\},\{\omega^{3a},\omega^{9a}\},\{\omega^{4a},\omega^{6a}\},\{\omega^{5a},\omega^{7a}\},\{\omega^{8a},\omega^{11a}\}\}$
   $\otimes\{1,\omega,\cdots,\omega^{11}\}$.
8. $\{\{1,\omega^{a}\},\{\omega^{2a},\omega^{6a}\},\{\omega^{3a},\omega^{10a}\},\{\omega^{4a},\omega^{11a}\},\{\omega^{5a},\omega^{8a}\},\{\omega^{9a},\omega^{7a}\}\}$
   $\otimes\{1,\omega,\cdots,\omega^{11}\}$.
9. $\{\{1,\omega^{a}\},\{\omega^{2a},\omega^{3a}\},\{\omega^{4a},\omega^{10a}\},\{\omega^{5a},\omega^{7a}\},\{\omega^{6a},\omega^{8a}\},\{\omega^{9a},\omega^{11a}\}\}$
   $\otimes\{1,\omega,\cdots,\omega^{11}\}$.
10. $\{\{1,\omega^{a}\},\{\omega^{2a},\omega^{5a}\},\{\omega^{3a},\omega^{7a}\},\{\omega^{4a},\omega^{10a}\},\{\omega^{6a},\omega^{11a}\},\{\omega^{8a},\omega^{9a}\}\}$
    $\otimes\{1,\omega,\cdots,\omega^{11}\}$.
11. $\{\{1,\omega^{a}\},\{\omega^{3a},\omega^{4a}\},\{\omega^{2a},\omega^{7a}\},\{\omega^{5a},\omega^{10a}\},\{\omega^{6a},\omega^{8a}\},\{\omega^{9a},\omega^{11a}\}\}$
    $\otimes\{1,\omega,\cdots,\omega^{11}\}$.
12. $\{\{1,\omega^{a}\},\{\omega^{3a},\omega^{4a}\},\{\omega^{2a},\omega^{11a}\},\{\omega^{5a},\omega^{10a}\},\}\{\omega^{6a},\omega^{9a}\},\{\omega^{7a},\omega^{8a}\}$
    $\otimes\{1,\omega,\cdots,\omega^{11}\}$.
13. $\{\{1,\omega^{2a}\},\{\omega^{a},\omega^{7a}\},\{\omega^{3a},\omega^{10a}\},\{\omega^{4a},\omega^{8a}\},\{\omega^{5a},\omega^{9a}\},\{\omega^{6a},\omega^{11a}\}\}$
    $\otimes\{1,\omega,\cdots,\omega^{11}\}$.
14. $\{\{1,\omega^{4a}\},\{\omega^{2a},\omega^{9a}\},\{\omega^{3a},\omega^{7a}\},\{\omega^{5a},\omega^{10a}\},\{\omega^{6a},\omega^{11a}\},\{\omega^{a},\omega^{8a}\}\}$
    $\otimes\{1,\omega,\cdots,\omega^{11}\}$.

We list all strong starters in $Z_{17}$.

For any primitive root $\omega$ of 17 there exists a positive integer $a$ such that the following are all the 224 strong starters in $Z_{17}$. The possible pairs of $(\omega,a)$ are (3,1),(5,13),(6,15),(7,3),(10,11),(11,7),(12,5),(14,9).

1. $\{\{1,\omega^{a}\},\{\omega^{3a},\omega^{4a}\},\{\omega^{13a},\omega^{15a}\},\{\omega^{8a},\omega^{10a}\},\{\omega^{2a},\omega^{5a}\},\{\omega^{6a},\omega^{9a}\},$
   $\{\omega^{11a},\omega^{14a}\},\{\omega^{7a},\omega^{12a}\}\}\otimes\{1,\omega,\cdots,\omega^{15}\}$.
2. $\{\{1,\omega^{2a}\},\{\omega^{3a},\omega^{6a}\},\{\omega^{7a},\omega^{11a}\},\{\omega^{9a},\omega^{13a}\},\{\omega^{5a},\omega^{10a}\},\{\omega^{12a},\omega^{a}\},$
   $\{\omega^{14a},\omega^{4a}\},\{\omega^{8a},\omega^{15a}\}\}\otimes\{1,\omega,\cdots,\omega^{15}\}$.
3. $\{\{1,\omega^{3a}\},\{\omega^{2a},\omega^{7a}\},\{\omega^{5a},\omega^{10a}\},\{\omega^{9a},\omega^{14a}\},\{\omega^{6a},\omega^{12a}\},\{\omega^{11a},\omega^{a}\},$
   $\{\omega^{4a},\omega^{13a}\},\{\omega^{8a},\omega^{15a}\}\}\otimes\{1,\omega,\cdots,\omega^{15}\}$.

4. $\{\{1,\omega^{3a}\},\{\omega^{2a},\omega^{5a}\},\{\omega^{4a},\omega^{8a}\},\{\omega^{9a},\omega^{13a}\},\{\omega^{10a},\omega^{14a}\},\{\omega^{11a},\omega^{15a}\},$ $\{\omega^{7a},\omega^{12a}\},\{\omega^{a},\omega^{6a}\}\}\otimes\{1,\omega,\cdots,\omega^{15}\}$.

5. $\{\{1,\omega^{a}\},\{\omega^{3a},\omega^{4a}\},\{\omega^{5a},\omega^{7a}\},\{\omega^{6a},\omega^{8a}\},\{\omega^{10a},\omega^{12a}\},\{\omega^{11a},\omega^{13a}\},$ $\{\omega^{2a},\omega^{14a}\},\{\omega^{9a},\omega^{15a}\}\}\otimes\{1,\omega,\cdots,\omega^{15}$.

6. $\{\{1,\omega^{2a}\},\{\omega^{10a},\omega^{12a}\},\{\omega^{9a},\omega^{13a}\},\{\omega^{3a},\omega^{7a}\},\{\omega^{a},\omega^{6a}\},\{\omega^{8a},\omega^{15a}\},$ $\{\omega^{4a},\omega^{11a}\},\{\omega^{5a},\omega^{14a}\}\}\otimes\{1,\omega,\cdots,\omega^{15}\}$.

7. $\{\{1,\omega^{2a}\},\{\omega^{3a},\omega^{6a}\},\{\omega^{9a},\omega^{12a}\},\{\omega^{10a},\omega^{15a}\},\{\omega^{7a},\omega^{13a}\},\{\omega^{4a},\omega^{11a}\},$ $\{\omega^{a},\omega^{8a}\},\{\omega^{14a},\omega^{5a}\}\}\otimes\{1,\omega,\cdots,\omega^{15}\}$.

8. $\{\{1,\omega^{2a}\},\{\omega^{3a},\omega^{6a}\},\{\omega^{7a},\omega^{11a}\},\{\omega^{9a},\omega^{13a}\},\{\omega^{5a},\omega^{10a}\},\{\omega^{12a},\omega^{a}\},$ $\{\omega^{4},\omega^{14a}\},\{\omega^{8a},\omega^{15a}\}\}\otimes\{1,\omega,\cdots,\omega^{15}\}$.

9. $\{\{1,\omega^{a}\},\{\omega^{5a},\omega^{6a}\},\{\omega^{11a},\omega^{13a}\},\{\omega^{10a},\omega^{12a}\},\{\omega^{2a},\omega^{15a}\},\{\omega^{3a},\omega^{8a}\},$ $\{\omega^{4a},\omega^{9a}\},\{\omega^{14a},\omega^{7a}\}\}\otimes\{1,\omega,\cdots,\omega^{15}\}$.

10. $\{\{1,\omega^{a}\},\{\omega^{3a},\omega^{4a}\},\{\omega^{13a},\omega^{15a}\},\{\omega^{8a},\omega^{10a}\},\{\omega^{2a},\omega^{5a}\},\{\omega^{6a},\omega^{9a}\},$ $\{\omega^{11a},\omega^{14a}\},\{\omega^{7a},\omega^{12a}\}\}\otimes\{1,\omega,\cdots,\omega^{15}\}$.

11. $\{\{1,\omega^{a}\},\{\omega^{3a},\omega^{4a}\},\{\omega^{6a},\omega^{7a}\},\{\omega^{10a},\omega^{11a}\},\{\omega^{13a},\omega^{15a}\},\{\omega^{2a},\omega^{14a}\},$ $\{\omega^{8a},\omega^{12a}\},\{\omega^{5a},\omega^{9a}\}\}\otimes\{1,\omega,\cdots,\omega^{15}\}$.

12. $\{\{1,\omega^{a}\},\{\omega^{7a},\omega^{11a}\},\{\omega^{6a},\omega^{10a}\},\{\omega^{3a},\omega^{8a}\},\{\omega^{9a},\omega^{15a}\},\{\omega^{12a},\omega^{2a}\},$ $\{\omega^{13a},\omega^{4a}\},\{\omega^{14a},\omega^{5a}\}\}\otimes\{1,\omega,\cdots,\omega^{15}\}$.

13. $\{\{1,\omega^{a}\},\{\omega^{7a},\omega^{11a}\},\{\omega^{3a},\omega^{14a}\},\{\omega^{5a},\omega^{10a}\},\{\omega^{6a},\omega^{12a}\},\{\omega^{2a},\omega^{9a}\},$ $\{\omega^{8a},\omega^{15a}\},\{\omega^{4a},\omega^{13a}\}\}\otimes\{1,\omega,\cdots,\omega^{15}\}$.

14. $\{\{1,\omega^{4a}\},\{\omega^{7a},\omega^{13a}\},\{\omega^{11a},\omega^{a}\},\{\omega^{2a},\omega^{8a}\},\{\omega^{6a},\omega^{12a}\},\{\omega^{9a},\omega^{15a}\},$ $\{\omega^{3a},\omega^{10a}\},\{\omega^{5a},\omega^{14a}\}\}\otimes\{1,\omega,\cdots,\omega^{15}\}$.

Finally, we list all skew strong starters in $Z_{19}$.

For any primitive root $\omega$ there exists a constant $a$ such that the following are all the 128 skew strong starters in $Z_{19}$. The possible pairs of $(\omega,a)$ are $(2,1),(3,7),(10,17),(13,11),(14,13),(15,5)$.

1. $\{\{\ 1,\omega^{a}\},\{\omega^{2a},\omega^{3a}\},\{\omega^{4a},\omega^{5a}\},\{\omega^{6a},\omega^{7a}\},\{\omega^{8a},\omega^{9a}\},\{\omega^{10a},\omega^{11a}\},$ $\{\omega^{12a},\omega^{13a}\},\{\omega^{14a},\omega^{15a}\},\{\omega^{16a},\omega^{17a}\}\}\otimes\{1,\omega\}.$
2. $\{\{1,\omega^{3a}\},\{\omega^{2a},\omega^{5a}\},\{\omega^{4a},\omega^{7a}\},\{\omega^{6a},\omega^{9a}\},\{\omega^{8a},\omega^{11a}\},\{\omega^{10a},\omega^{13a}\},$ $\{\omega^{12a},\omega^{15a}\},\{\omega^{14a},\omega^{17a}\},\{\omega^{16a},\omega^{a}\}\}\otimes\{1,\omega\}.$
3. $\{\{1,\omega^{5a}\},\{\omega^{2a},\omega^{7a}\},\{\omega^{4a},\omega^{9a}\},\{\omega^{6a},\omega^{11a}\},\{\omega^{8a},\omega^{13a}\},\{\omega^{10a},\omega^{15a}\},$ $\{\omega^{12a},\omega^{17a}\},\{\omega^{14a},\omega^{a}\},\{\omega^{16a},\omega^{3a}\}\}\otimes\{1,\omega\}.$
4. $\{\{1,\omega^{7a}\},\{\omega^{2a},\omega^{9a}\},\{\omega^{4a},\omega^{11a}\},\{\omega^{6a},\omega^{13a}\},\{\omega^{8a},\omega^{15a}\},\{\omega^{10a},\omega^{17a}\},$ $\{\omega^{12a},\omega^{a}\},\{\omega^{14a},\omega^{3a}\},\{\omega^{16a},\omega^{5a}\}\}\otimes\{1,\omega\}.$
5. $\{\{1,\omega^{3a}\},\{\omega^{a},\omega^{4a}\},\{\omega^{2a},\omega^{5a}\},\{\omega^{6a},\omega^{9a}\},\{\omega^{7a},\omega^{10a}\},\{\omega^{8a},\omega^{11a}\},$ $\{\omega^{12a},\omega^{15a}\},\{\omega^{13a},\omega^{16a}\},\{\omega^{14a},\omega^{17a}\}\}\otimes\{1,\omega,\cdots,\omega^{5}\}.$
6. $\{\{1,\omega^{7a}\},\{\omega^{2a},\omega^{4a}\},\{\omega^{3a},\omega^{5a}\},\{\omega^{6a},\omega^{13a}\},\{\omega^{8a},\omega^{10a}\},\{\omega^{9a},\omega^{11a}\},$ $\{\omega^{12a},\omega^{a}\},\{\omega^{14a},\omega^{16a}\},\{\omega^{15a},\omega^{17a}\}\}\otimes\{1,\omega,\cdots,\omega^{5}\}.$
7. $\{\{1,\omega^{a}\},\{\omega^{2a},\omega^{12a}\},\{\omega^{3a},\omega^{10a}\},\{\omega^{4a},\omega^{15a}\},\{\omega^{5a},\omega^{9a}\},\{\omega^{6a},\omega^{17a}\},$ $\{\omega^{8a},\omega^{11a}\},\{\omega^{7a},\omega^{14a}\}\{\omega^{13a},\omega^{16a}\}\}\otimes\{1,\omega,\cdots,\omega^{17}\}.$
8. $\{\{1,\omega^{a}\},\{\omega^{2a},\omega^{4a}\},\{\omega^{5a},\omega^{17a}\},\{\omega^{6a},\omega^{9a}\},\{\omega^{7a},\omega^{15a}\},\{\omega^{8a},\omega^{16a}\},$ $\{\omega^{10a},\omega^{12a}\},\{\omega^{11a},\omega^{14a}\}\{\omega^{3a},\omega^{13a}\}\}\otimes\{1,\omega,\cdots,\omega^{17}\}.$
9. $\{\{1,\omega^{a}\},\{\omega^{2a},\omega^{3a}\},\{\omega^{4a},\omega^{12a}\},\{\omega^{5a},\omega^{11a}\},\{\omega^{6a},\omega^{10a}\},\{\omega^{7a},\omega^{14a}\},$ $\{\omega^{8a},\omega^{15a}\},\{\omega^{9a},\omega^{16a}\},\{\omega^{13a},\omega^{17a}\}\}\otimes\{1,\omega,\cdots,\omega^{17}\}.$
10. $\{\{1,\omega^{a}\},\{\omega^{8a},\omega^{9a}\},\{\omega^{3a},\omega^{5a}\},\{\omega^{11a},\omega^{13a}\},\{\omega^{2a},\omega^{17a}\},\{\omega^{6a},\omega^{16a}\},$ $\{\omega^{4a},\omega^{15a}\},\{\omega^{7a},\omega^{12a}\},\{\omega^{10a},\omega^{14a}\}\}\otimes\{1,\omega,\cdots,\omega^{17}\}.$
11. $\{\{1,\omega^{2a}\},\{\omega^{10a},\omega^{12a}\},\{\omega^{3a},\omega^{6a}\},\{\omega^{a},\omega^{8a}\},\{\omega^{7a},\omega^{15a}\},\{\omega^{9a},\omega^{13a}\},$ $\{\omega^{11a},\omega^{17a}\},\{\omega^{4a},\omega^{14a}\},\{\omega^{16a},\omega^{5a}\}\}\otimes\{1,\omega,\cdots,\omega^{17}\}.$
12. $\{\{1,\omega^{2a}\},\{\omega^{3a},\omega^{5a}\},\{\omega^{13a},\omega^{15a}\},\{\omega^{6a},\omega^{9a}\},\{\omega^{7a},\omega^{11a}\},\{\omega^{8a},\omega^{12a}\},$ $\{\omega^{10a},\omega^{16a}\},\{\omega^{14a},\omega^{a}\},\{\omega^{4a},\omega^{17a}\}\}\otimes\{1,\omega,\cdots,\omega^{17}\}.$

## 1.7 Room squares

**Definition 1.7.1** A Room square of order $2n$ (or of side $2n-1$) is a $(2n-1) \times (2n-1)$ array based on $2n$ symbols $x_1, x_2, \cdots, x_{2n}$ such that

1. each cell either is empty or contains an unordered pair of symbols;
2. each symbol occurs once in each row and column;
3. each of the $n(2n-1)$ unordered pairs of distinct symbols occurs in exactly one cell of the array.

**Example 1.7.1** A Room square of order 10

$$\left(\begin{array}{ccccccccc}
\infty,0 & -- & 1,4 & -- & 7,8 & 2,6 & -- & 3,5 & -- \\
-- & \infty,1 & -- & 2,5 & -- & 8,0 & 3,7 & -- & 4,6 \\
5,7 & -- & \infty,2 & -- & 3,6 & -- & 0,1 & 4,8 & -- \\
-- & 6,8 & -- & \infty,3 & -- & 4,7 & -- & 1,2 & 5,0 \\
6,1 & -- & 7,0 & -- & \infty,4 & -- & 5,8 & -- & 2,3 \\
3,4 & 7,2 & -- & 8,1 & -- & \infty,5 & -- & 6,0 & -- \\
-- & 4,5 & 8,3 & -- & 0,2 & -- & \infty,6 & -- & 7,1 \\
8,2 & -- & 5,6 & 0,4 & -- & 1,3 & -- & \infty,7 & -- \\
-- & 0,3 & -- & 6,7 & 1,5 & -- & 2,4 & -- & \infty,8
\end{array}\right)$$

**Example 1.7.2** A Room square of order 12

$$\left(\begin{array}{ccccccccccc}
\infty,0 & X,3 & -- & 8,9 & 1,7 & 4,6 & -- & -- & -- & 2,5 & -- \\
-- & \infty,1 & 0,4 & -- & 9,X & 2,8 & 5,7 & -- & -- & -- & 3,6 \\
4,7 & -- & \infty,2 & 1,5 & -- & X,0 & 3,9 & 6,8 & -- & -- & -- \\
-- & 5,8 & -- & \infty,3 & 2,6 & -- & 0,1 & 4,X & 7,9 & -- & -- \\
-- & -- & 6,9 & -- & \infty,4 & 3,7 & -- & 1,2 & 5,0 & 8,X & -- \\
-- & -- & -- & 7,X & -- & \infty,5 & 4,8 & -- & 2,3 & 6,1 & 9,0 \\
X,1 & -- & -- & -- & 8,0 & -- & \infty,6 & 5,9 & -- & 3,4 & 7,2 \\
8,3 & 0,2 & -- & -- & -- & 9,1 & -- & \infty,7 & 6,X & -- & 4,5 \\
5,6 & 9,4 & 1,3 & -- & -- & -- & X,2 & -- & \infty,8 & 7,0 & -- \\
-- & 6,7 & X,5 & 2,4 & -- & -- & -- & 0,3 & -- & \infty,9 & 8,1 \\
9,2 & -- & 7,8 & 0,6 & 3,5 & -- & -- & -- & 1,4 & -- & \infty,X
\end{array}\right)$$

where $X = 10$.

Room squares were named after T. G. Room who published a paper [35] in 1955, in which he proved that Room squares of sides three and five do not exist and constructed a Room square of side seven. Room squares in fact had been discussed long before 1955. In 1850, Kirkman, while discussing the " 15 Schoolgirls Problem ", had exhibited a Room square of side seven.

A Room square of order $2n$ is $Z$-cyclic if its symbols are $\infty, 0, 1, \cdots, 2n-2$, 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 mod $(2n-1)$, with $\infty + a = \infty$ for all $a$. For example, Example 1.7.1. and 1.7.2 are $Z$-cyclic Room squares, obtained from starters $X_1$ and $X_3$.

It is now well known that Room squares exist for all odd sides except sides three and five. In this thesis, I will construct many $Z$-cyclic Room squares.

# Chapter 2

# 1-Rotational designs with block size 4

1-rotational $(v, 4, 1)$ designs are constructed for all $v$ of the form $v = 3p_1^{\alpha_1} \ldots p_n^{\alpha_n} + 1$, where $p_i$ either are primes $\equiv 1 \pmod 4$ or $\frac{1}{3}(4^m - 1)$ and there is at most one $p_i$ such that $3p_i = 4^m - 1$ where $9 \mid (4^m - 1)$ (and $\alpha_i = 1$ for this $p_i$). Further, for such $v$ a cyclic GDD$(v - 1, 4, 3)$ exists.

## 2.1 Introduction

A balanced incomplete $(v, k, \lambda)$ block design is a pair $\mathcal{D} = \{\mathcal{V}, \mathcal{B}\}$ where $\mathcal{V}$ is a $v$-set and $\mathcal{B}$ is a collection of $k$-subsets of $\mathcal{V}$ ( called blocks, $k < v$) such that each pair of elements of $\mathcal{V}$ occurs together in precisely $\lambda$ blocks. Such a design has $b = \frac{\lambda v(v-1)}{k(k-1)}$ blocks and every element of $\mathcal{V}$ belongs to $r = \frac{\lambda(v-1)}{k-1}$ blocks. The design is said to be resolvable if the set $\mathcal{B}$ of $b$ blocks can be partitioned into $r$ classes so that the blocks in each class form a partition of $\mathcal{V}$. In the particular case of $k = 4, \lambda = 1$, it was proved by Hanani, Ray-Chaudhuri and Wilson [24] that a resolvable $(v, 4, 1)$ design exists if and only if $v \equiv 4 \pmod{12}, v > 4$. Note that, for such designs, $v = 3r + 1$ where $r \equiv 1 \pmod 4$.

An automorphism of a $(v, k, \lambda)$ design $\mathcal{D} = \{\mathcal{V}, \mathcal{B}\}$ is a permutation of $\mathcal{V}$ which preserves $\mathcal{B}$. $\mathcal{D}$ is said to be 1-rotational if there is an automorphism of $\mathcal{D}$ which fixes one point (which we denote by $\infty$) and cycles the rest.

If $B = \{a, b, c, d\}$ is a block, we call the set $\{a + j, b + j, c + j, d + j\}$ the $j$-th translate of $B$. A $(v, 4, 1)$ design on $\mathcal{V} = Z_{v-1} \cup \{\infty\}$ is said to be Z-cyclically resolvable if the blocks of the $j$-th class are the $(j-1)$-th translates of the blocks of the base class $(\infty + j = \infty$ for all $j)$.

Phelps and Rosa [34] showed that a 1-rotational $(v, 3, 1)$ design exists if and only if $v \equiv 3$ or $9 \pmod{24}$

In this chapter, we will deal with 1-rotational $(v, 4, 1)$ designs. In 1896 [30] Moore presented a construction of resolvable $(v, 4, 1)$ designs whenever $v = 3p+1$, $p$ a prime, $p \equiv 1 \pmod 4$ and whenever $v = 4^m$; his examples were in fact all 1-rotational.

**Example 2.1.1** A resolvable $(16, 4, 1)$ design

$$\begin{array}{llll}
\{\infty,0,5,10\} & \{1,2,4,8\} & \{6,7,9,13\} & \{11,12,14,3\} \\
\{\infty,1,6,11\} & \{2,3,5,9\} & \{7,8,10,14\} & \{12,13,0,4\} \\
\{\infty,2,7,12\} & \{3,4,6,10\} & \{8,9,11,0\} & \{13,14,1,5\} \\
\{\infty,3,8,13\} & \{4,5,7,11\} & \{9,10,12,1\} & \{14,0,2,6\} \\
\{\infty,4,9,14\} & \{5,6,8,12\} & \{10,11,13,2\} & \{0,1,3,7\}.
\end{array}$$

It is also clearly Z-cyclically resolvable. Anderson and Finizio [7] constructed Z-cyclically resolvable $(v, 4, 1)$ designs for all $v$ of the form $3p_1^{\alpha_1} \cdots p_n^{\alpha_n} + 1$, where the $p_i$ are primes $\equiv 1 \pmod 4$, such that each $p_i - 1$ is divisible by the same power of 2. In the cases where $p_i - 1$ do not satisfy this condition, we show that (non-resolvable) 1-rotational designs exist.

## 2.2 Notation and basic lemmas

**Lemma 2.2.1 ([23])** *A $(v, 4, 1)$ design exists if and only if $v \equiv 1$ or 4 (mod 12).*

**Lemma 2.2.2** *A necessary condition for the existence of a 1-rotational $(v, 4, 1)$ design is $v \equiv 4 \pmod{12}$.*

**Proof.** Let $\mathcal{V} = Z_{v-1} \cup \{\infty\}$ and $\alpha = (\infty)(0, 1, \cdots, v-2)$ be an automorphism of a 1-rotational $(v, 4, 1)$ design. The pair $\{\infty, 0\}$ occurs in a block exactly once, say $\{\infty, 0, a_0, b_0\}$ where $a_0, b_0 \not\equiv 0 \pmod{v-1}$. We claim that

$a_0 = \frac{1}{3}(v-1)$, $b_0 = \frac{2}{3}(v-1)$. Since we want a 1-rotational $(v,4,1)$ design, if $\{\infty, 0, a_0, b_0\} \in \mathcal{B}$ then $\{\infty, y, 0, x\} \in \mathcal{B}$ where $y = -a_0$, $x = -a_0 + b_0$. Thus, since $0, \infty$ occur together exactly once, we must have $\{a_0, b_0\} = \{-a_0, -a_0 + b_0\}$. This implies $a_0 = \frac{1}{3}(v-1)$, $b_0 = \frac{2}{3}(v-1)$. Thus a 1-rotational $(v,4,1)$ design contains $\frac{v-1}{3}$ blocks of the form $\{\infty, i, i + \frac{v-1}{3}, i + \frac{2}{3}(v-1)\}$.

All the blocks of $\mathcal{B}$ not containing $\infty$ are partitioned into orbits under $\alpha$, all of which are of length $v-1$ except possibly a single orbit $Q_0$ of length $\frac{1}{4}(v-1)$ containing the 4-tuple $\{0, \frac{1}{4}(v-1), \frac{1}{2}(v-1), \frac{3}{4}(v-1)\}$. We claim no 1-rotational $(v,4,1)$ design contains 4-tuples of $Q_0$. If $Q_0$ were contained then this would require $v \equiv 1 \pmod 4$ and at the same time there would be need for further $\frac{1}{12}v(v-1) - \frac{1}{3}(v-1) - \frac{1}{4}(v-1) = \frac{1}{12}(v-1)(v-7)$ 4-tuples in $\mathcal{B}$ which would then necessarily have to be partitioned into $\frac{1}{12}(v-7)$ orbits of length $v-1$. This is obviously impossible as $\frac{1}{12}(v-7)$ is not an integer, since $v \equiv 1 \text{ or } 4 \pmod{12}$ by lemma 2.2.1.

If $\{a,b,c,d\}$ is a 4-tuple in one such orbit then clearly the twelve differences $\pm(a-b), \pm(a-c), \pm(a-d), \pm(b-c), \pm(b-d), \pm(c-d)$ are all distinct and if $\{a_1, b_1, c_1, d_1\}$ and $\{a_2, b_2, c_2, d_2\}$ are two 4-tuples from two distinct orbit in $\mathcal{B}$ then the corresponding 24 differences are all distinct. Since there are still $v-4$ non-zero differences "available", it follows that $\frac{1}{12}(v-4)$ must be integer and so we must have $v \equiv 4 \pmod{12}$.

**Definition 2.2.1** A group divisible design GDD$(v,k,m)$ consists of a collection of $m$-subsets, called groups, of a $v$-set $S$ and a collection of $k$-subsets, called blocks, such that

1. the groups form a partition of $S$,
2. each pair of elements from different groups occur together in exactly one block,
3. no block contains two elements from the same group.

**Example 2.2.1** The blocks $\{1,2,4\}, \{2,3,5\}$, $\{3,4,6\}$, $\{4,5,7\}$, $\{5,6,8\}$, $\{6,\ 7,1\}$, $\{7,8,2\}$, $\{8,1,3\}$ and the groups $\{1,5\}, \{2,6\}, \{3,7\}, \{4,8\}$ form a GDD(8,3,2).

**Definition 2.2.2** Let $D_1, \cdots, D_t$ be sets of size $k$ in $Z_v$ such that the differences arising from the $D_i$ give each element of $Z_v - \{\alpha, \beta, \gamma\}$ exactly $\lambda$ times. Then $D_1, \cdots, D_t$ are said to form a $(v, k, \lambda)$ difference system in $Z_v - \{\alpha, \beta, \gamma\}$.

Note that if $D_1, \cdots, D_t$ is a $(v, k, \lambda)$ difference system in $Z_v - \{\alpha, \beta, \gamma\}$ then so is $D_1 + a_1, \cdots D_t + a_t$ where $D_i + a_i = \{d_i^j + a_i; d_i^j \in D_i\}$.

**Example 2.2.2** $\{1,2,4,8\}$ is a $(15,4,1)$ difference system in $Z_{15} - \{0,5,10\}$ since the differences arising from $\{1,2,4,8\}$ are $\pm1, \pm3, \pm7, \pm2, \pm6, \pm4$. Similarly, $\{1,8,25,5\}$,$\{2,16,11,10\}$,$\{4,32,22,20\}$ is a difference system in $Z_{39} - \{0,13,26\}$ since the differences arising from them are $\pm7, \pm15, \pm4, \pm17, \pm3$, $\pm19, \pm14, \pm9$, $\pm8, \pm5, \pm6$, $\pm1, \pm11, \pm18, \pm16, \pm10, \pm12, \pm2$.

Note that if $D_1, \cdots, D_t$ is a $(3\beta, 4, 1)$ difference system in $Z_{3\beta} - \{0, \beta, 2\beta\}$ then the blocks $D_1, \cdots, D_t$ along with $\{\infty, 0, \beta, 2\beta\}$ will generate a 1-rotational $(3\beta + 1, 4, 1)$ design and so by Lemma 2.2.2 we must have $\beta \equiv 1 \pmod 4$.

**Lemma 2.2.3** *Let* $\alpha = 4t + 1$ *and* $D_i$, $i = 1, 2, \ldots, t$, *be a* $(3\alpha, 4, 1)$ *difference system in* $Z_{3\alpha} - \{0, \alpha, -\alpha\}$, $\beta = 4s + 1$ *and* $B_j$, $j = 1, 2, \ldots, s$, *be a* $(3\beta, 4, 1)$ *difference system in* $Z_{3\beta} - \{0, \beta, -\beta\}$. *If* $\beta \equiv \pm1 \pmod 3$ *then there is a* $(3\alpha\beta, 4, 1)$ *difference system in* $Z_{3\alpha\beta} - \{0, \alpha\beta, -\alpha\beta\}$.

**Proof.** Without loss of generality, let $D_i = \{0, d_1^i, d_2^i, d_3^i\}$ $i = 1, 2, \ldots, t$ and $B_j = \{0, b_1^j, b_2^j, b_3^j\}$ $j = 1, 2, \cdots, s$. We claim that the following 4-tuples form a difference system in $Z_{3\alpha\beta} - \{0, \alpha\beta, -\alpha\beta\}$:

$$\textit{(2.2.1)} \qquad \begin{array}{c} \{0, \alpha b_1^j, \alpha b_2^j, \alpha b_3^j\} \qquad j = 1, 2, \cdots, s \\ \{0, d_1^i + l \cdot 3\alpha, d_2^i + 2l \cdot 3\alpha, d_3^i + 3l \cdot 3\alpha\} \\ i = 1, 2, \cdots, t; \quad l = 0, 1, \cdots, \beta - 1. \end{array}$$

First consider the differences in $\{0, \alpha b_1^j, \alpha b_2^j, \alpha b_3^j\} \quad j = 1, 2, \cdots, s$. They are clearly $\alpha$ times the differences in $\{0, b_1^j, b_2^j, b_3^j\} \quad j = 1, 2, \cdots, s$, so the differences in $\{0, \alpha b_1^j,\ \alpha b_2^j, \alpha b_3^j\} \quad j = 1, 2, \cdots, s$ are the nonzero elements of $Z_{3\alpha\beta}$ which are multiples of $\alpha$ except $\alpha\beta, -\alpha\beta$.

Next consider the differences in $\{0, d_1^i + l \cdot 3\alpha, d_2^i + 2l \cdot 3\alpha, d_3^i + 3l \cdot 3\alpha\} \quad i = 1, 2, \cdots, t$; $l = 0, 1, \cdots, \beta - 1$. Let $a = 3\alpha$. For $i = 1, 2, \cdots, t$, the differences in $\{0, d_1^i + la, d_2^i + 2la, d_3^i + 3la\}$ are

$$\begin{array}{ll} & \pm(d_1^i + la), \pm(d_2^i - d_1^i + la), \\ (\mathit{2.2.2}) & \pm(d_3^i - d_2^i + la), \pm(d_2^i + 2la), \\ & \pm(d_3^i - d_1^i + 2la), \pm(d_3^i + 3la) \pmod{\beta a} \qquad l = 0, 1, 2, \cdots, \beta - 1. \end{array}$$

But since $2 \nmid \beta$ and $3 \nmid \beta$, we have $\{2l \pmod{\beta}; l \in Z_\beta\} = \{3l \pmod{\beta}; l \in Z_\beta\} = Z_\beta$, so (2.2.2) becomes

$$\begin{array}{l} \pm(d_1^i + la), \pm(d_2^i - d_1^i + la), \\ \pm(d_3^i - d_2^i + la), \pm(d_2^i + la), \\ \pm(d_3^i - d_1^i + la), \pm(d_3^i + la) \pmod{\beta a} \qquad l = 0, 1, \cdots, \beta - 1. \end{array}$$

Therefore (*2.2.1*) form a difference system in $Z_{\beta a} - \{0, \alpha\beta, -\alpha\beta\}$.

## 2.3 1-rotational $(v, 4, 1)$ designs

**Theorem 2.3.1 ([30])** *If $v = 3p+1$ or $4^m$ where $p$ is a prime $\equiv 1 \pmod{4}$, $m$ is a positive integer then a 1-rotational $(v, 4, 1)$ design exists.*

**Theorem 2.3.2** *If $v = 3\alpha\beta + 1$ where 1-rotational $(3\alpha + 1, 4, 1), (3\beta + 1, 4, 1)$ designs exist and $\beta \equiv \pm 1 \pmod{3}$ then a 1-rotational $(v, 4, 1)$ design exists.*

**Proof.** Suppose the initial blocks for 1-rotational $(3\alpha + 1, 4, 1)$ are $\{\infty, 0, \alpha, 2\alpha\}$, $D_i = \{d_0^i, d_1^i, d_2^i, d_3^i\}$ $i = 1, 2, \cdots, \alpha$ and those of $(3\beta + 1, 4, 1)$ are $\{\infty, 0, \beta, 2\beta\}$, $B_j$ $j = 1, 2, \cdots, \beta$. Then $D_i, B_j$ are difference systems in $Z_{3\alpha} - \{0, \alpha, 2\alpha\}$ and $Z_{3\beta} - \{0, \beta\ , 2\beta\}$ respectively. Thus, by Lemma 2.2.3, the following blocks form a difference system in $Z_{3\alpha\beta} - \{0, \alpha\beta,\ 2\alpha\beta\}$:

$$\begin{array}{ll} & \alpha B_j, \qquad j = 1, 2, \cdots, \beta; \\ (\mathit{2.3.1}) & \{d_0^i, d_1^i + l \cdot 3\alpha,{}_2^i + 2l \cdot 3\alpha, d_3^i + 3l \cdot 3\alpha\}, \\ & \qquad i = 1, 2, \cdots, \tfrac{1}{4}(\alpha - 1); \quad l = 0, 1, \cdots, \beta - 1. \end{array}$$

Therefore the block $\{\infty, 0, \alpha\beta, 2\alpha\beta\}$ and those in (2.3.1) are initial blocks for a 1-rotational $(3\alpha\beta+1, 4, 1)$ design.

**Corollary 2.3.3** *If* $v = 3p_1^{\alpha_1}\cdots p_n^{\alpha_n}+1$ *where* $p_i$ *either are primes* $\equiv 1 \pmod 4$ *or* $\frac{1}{3}(4^m-1)$ *and there is at most one* $p_i$ *such that* $3p_i = 4^m - 1$ *where* $m \equiv 0 \pmod 3$ *and* ($\alpha_i = 1$ *in this case), then a 1-rotational* $(v, 4, 1)$ *design exists.*

**Proof.** By induction with Theorem 2.3.2, since $4^m \equiv 1 \pmod 9$ precisely when $m \equiv 0 \pmod 3$.

**Example 2.3.1** Let $v = 3\cdot 13\cdot 17+1 = 664$. Since $52 = 3\cdot 17+1 = 12\cdot 4+4$ where 17 is a prime, so by Theorem 2.3.1 a 1-rotational $(52, 4, 1)$ design exists. Moore's example has initial blocks $\{\infty, 0, 17, 34\}, D_1 = \{1, 47, 16, 38\}, D_2 = \{5, 31, 29, 37\}, D_3 = \{25, 2, 43, 32\}, D_4 = \{23, 10, 11, 7\}$. Note that $D_1, D_2, D_3, D_4$ is a difference system in $Z_{51} - \{0, 17, 34\}$. Similarly, since $40 = 3\cdot 13+1 = 12\cdot 3+4$ where 13 is a prime, a 1-rotational $(40, 4, 1)$ design exists. Moore's example has initial blocks $\{\infty, 0, 13, 26\}, B_1 = \{1, 8, 25, 5\}$, $B_2 = \{2, 16, 11, 10\}, B_3 = \{4, 32, 22, 20\}$. Note that $B_1, B_2, B_3$ is a difference system in $Z_{39} - \{0, 13, 26\}$.

Therefore by Lemma 2.2.3, the following blocks form a difference system in $Z_{3\cdot 13\cdot 17} - \{0, 221, 442\}$.

$$\begin{aligned}
&\{17, 136, 425, 85\},\\
&\{34, 272, 187, 170\},\\
&\{68, 544, 374, 340\},\\
&\{1, 47 + l\cdot 51, 16 + 2l\cdot 51, 38 + 3l\cdot 51\},\\
&\{5, 31 + l\cdot 51, 29 + 2l\cdot 51, 37 + 3l\cdot 51\},\\
&\{25, 2 + l\cdot 51, 43 + 2l\cdot 51, 32 + 3l\cdot 51\},\\
&\{23, 10 + l\cdot 51, 11 + 2l\cdot 51, 7 + 3l\cdot 51\}; \qquad l = 0, 1, \cdots, 12.
\end{aligned} \tag{2.3.2}$$

Therefore the block $\{\infty, 0, 221, 442\}$ and those in (*2.3.2*) form the initial blocks for a 1-rotational $(664, 4, 1)$ design.

**Example 2.3.2** $v = 3 \cdot 5 \cdot 21 + 1 = 316$. Here we take $\alpha = 21$, $\beta = 5$. As in Example 2.1.1 a 1-rotational $(16, 4, 1)$ design exists and its initial blocks are $\{\infty, 0, 5, 10\}$, $D_1 = \{1, 2, 4, 8\}$. Further, since $64 = 4^3 = 3 \cdot 21 + 1 = 12 \cdot 5 + 4$, by Theorem 2.3.1 a 1-rotational $(64, 4, 1)$ design exists. Moore's example has initial blocks

$$\begin{aligned} &\{\infty, 0, 21, 42\},\\ B_1 &= \{1, 25, 56, 58\},\\ B_2 &= \{2, 50, 49, 53\},\\ B_3 &= \{3, 13, 20, 57\},\\ B_4 &= \{6, 26, 40, 51\},\\ B_5 &= \{12, 52, 17, 39\}. \end{aligned}$$

Note that $21 = 4 \cdot 5 + 1$ and $B_1, B_2, B_3, B_4, B_5$ is a difference system in $Z_{63} - \{0, 21, 42\}$.

So by Lemma 2.2.3 the following blocks form a difference system in $Z_{3 \cdot 5 \cdot 21} - \{0, 105, 210\}$.

$$\begin{aligned} &\{5, 125, 280, 290\},\\ &\{10, 250, 245, 265\},\\ &\{15, 65, 100, 285\},\\ &\{30, 130, 200, 255\},\\ &\{60, 260, 85, 195\}\\ &\{1, 2 + l \cdot 15, 4 + 2l \cdot 15, 8 + 3l \cdot 15\}. \qquad l = 0, 1, \cdots, 20. \end{aligned} \tag{2.3.3}$$

Therefore, the block $\{\infty, 0, 105, 210\}$ and those in (*2.3.3*) are the initial blocks for a 1-rotational $(316, 4, 1)$ design.

**Corollary 2.3.4** *If $v$ is as in Corollary 2.3.3 then a cyclic GDD$(v - 1, 4, 3)$ exists.*

**Proof** Take a 1-rotational $(v, 4, 1)$ design as above and delete $\infty$ from all blocks containing it to obtain a GDD$(v - 1, 4, 3)$, in which the resulting 3-element sets are the groups.

**Example 2.3.3** From Example 2.3.1 we know that the groups $\{i, i+221, i+442\}$ $i = 0, 1, \cdots, 220$ and the blocks

$$\begin{array}{l}
\{17+j, 136+j, 425+j, 85+j\},\\
\{34+j, 272+j, 187+j, 170+j\},\\
\{68+j, 544+j, 374+j, 340+j\},\\
\{1+j, 47+l\cdot 51+j, 16+2l\cdot 51+j, 38+3l\cdot 51+j\},\\
\{5+j, 31+l\cdot 51+j, 29+2l\cdot 51+j, 37+3l\cdot 51+j\},\\
\{25+j, 2+l\cdot 51+j, 43+2l\cdot 51+j, 32+3l\cdot 51+j\},\\
\{23+j, 10+l\cdot 51+j, 11+2l\cdot 51+j, 7+3l\cdot 51+j\},\\
\qquad\qquad j = 0, 1, \cdots, 562 \qquad l = 0, 1, \cdots, 12
\end{array}$$

with arithmetic mod 663 form a cyclic GDD$(663, 4, 3)$.

# Chapter 3

# Referee squares

In [11] Anderson, Hamilton and Hilton made a conjecture concerning the existence of a referee square for every odd integer $n \geq 3$ other than 5. In this paper the existence of a referee square of side $n$ is shown when $n$ is an odd composite integer.

## 3.1 Introduction

A referee square of side $n$ is an $n \times n$ array $R$ based on $\mathcal{V} = \{1, 2, \cdots, n\}$ such that

1. each cell either is empty or contains an unordered pair of distinct symbols on $\mathcal{V}$,
2. each $i \in \mathcal{V}$ occurs precisely once in each row (except the $i$-th) and in each column (except $i$-th column), and does not occur in the $i$-th row and $i$-th column,
3. each unordered pair of distinct elements of $\mathcal{V}$ occurs in exactly one cell of $R$,
4. the main diagonal cells are non-empty.

We give some examples in the following.

**Example 3.1.1** A referee square of side 7

$$\begin{pmatrix}
6,7 & 4,5 & -- & 2,3 & -- & -- & -- \\
3,5 & 7,1 & -- & -- & 4,6 & -- & -- \\
-- & -- & 5,6 & -- & 2,7 & 1,4 & -- \\
-- & 3,6 & 1,2 & 5,7 & -- & -- & -- \\
-- & -- & 4,7 & -- & 1,3 & -- & 2,6 \\
2,4 & -- & -- & -- & -- & 3,7 & 1,5 \\
-- & -- & -- & 1,6 & -- & 2,5 & 3,4
\end{pmatrix}$$

**Example 3.1.2** [11] A referee square of side 9

$$\begin{pmatrix}
8,9 & 6,7 & 4,5 & 2,3 & -- & -- & -- & -- & -- \\
5,7 & 4,9 & 6,8 & -- & 1,3 & -- & -- & -- & -- \\
2,6 & 1,5 & 7,9 & -- & 4,8 & -- & -- & -- & -- \\
-- & 3,8 & -- & 5,6 & -- & -- & 2,9 & 1,7 & -- \\
-- & -- & -- & -- & 6,9 & 3,7 & 1,4 & -- & 2,8 \\
3,4 & -- & 1,2 & 7,8 & -- & 5,9 & -- & -- & -- \\
-- & -- & -- & -- & -- & 2,4 & 5,8 & 3,9 & 1,6 \\
-- & -- & -- & 1,9 & 2,7 & -- & -- & 4,6 & 3,5 \\
-- & -- & -- & -- & -- & 1,8 & 3,6 & 2,5 & 4,7
\end{pmatrix}$$

**Example 3.1.3** A referee square of side 11

$$\left(\begin{array}{ccccccccccc}
2,3 & -- & 6,11 & 8,10 & -- & -- & -- & 4,7 & -- & -- & 5,9 \\
6,10 & 3,4 & -- & 7,1 & 9,11 & -- & -- & -- & 5,8 & -- & -- \\
-- & 7,11 & 4,5 & -- & 8,2 & 10,1 & -- & -- & -- & 6,9 & -- \\
-- & -- & 8,1 & 5,6 & -- & 9,3 & 11,2 & -- & -- & -- & 7,10 \\
8,11 & -- & -- & 9,2 & 6,7 & -- & 10,4 & 1,3 & -- & -- & -- \\
-- & 9,1 & -- & -- & 10,3 & 7,8 & -- & 11,5 & 2,4 & -- & -- \\
-- & -- & 10,2 & -- & -- & 11,4 & 8,9 & -- & 1,6 & 3,5 & -- \\
-- & -- & -- & 11,3 & -- & -- & 1,5 & 9,10 & -- & 2,7 & 4,6 \\
5,7 & -- & -- & -- & 1,4 & -- & -- & 2,6 & 10,11 & -- & 3,8 \\
4,9 & 6,8 & -- & -- & -- & 2,5 & -- & -- & 3,7 & 11,1 & -- \\
-- & 5,10 & 7,9 & -- & -- & -- & 3,6 & -- & -- & 4,8 & 1,2
\end{array}\right)$$

A referee square of side $n$ is Z-cyclic if, 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 mod $n$. Example 3.1.3 is Z-cyclic while examples 3.1.1 and 3.1.2 are not.

Anderson, Hamilton and Hilton [11] constructed Z-cyclic referee squares of side $n$ for $n = 3, 11, 13$. We begin by using the starter-adder method , successful in the construction of Room squares, to construct referee squares of side $n$ for a few value of $n$.

## 3.2 The starters construction

If G is an additive Abelian group with identity element 0, and $G^* = G - \{0\}$ then a starter X for G is a partition of $G^*$ into 2-sets such that $\{x_i - x_j; \{x_i, x_j\} \in X\} = G^*$. If X,Y are two starters for G and $\{x_{1i}, x_{2i}\} \in X, \{y_{1i}, y_{2i}\} \in Y$ with $x_{2i} - x_{1i} = y_{2i} - y_{1i}$ then the distance $d(\{x_{1i}, x_{2i},\}, \{y_{1i}, y_{2i}\})$ from $\{x_{1i}, x_{2i}\}$ to $\{y_{1i}, y_{2i}\}$ is defined by

$$d(\{x_{1i}, x_{2i}\}, \{y_{1i}, y_{2i}\}) = y_{1i} - x_{1i} \quad (= y_{2i} - x_{2i})\,.$$

**Theorem 3.2.1** *If there exist two starters $X, Y$ with distinct distances containing a zero distance in $Z_{2n+1}$ then a Z-cyclic referee square of side $2n+1$ exists.*

**Proof.** Let $X = \{\{x_{11}, x_{21}\}, \{x_{12}, x_{22}\}, \cdots, \{x_{1n}, x_{2n}\}\}$, $Y = \{\{y_{11}, y_{21}\}, \{y_{12}, y_{22}\}, \cdots, \{y_{1n}, y_{2n}\}\}$ (rearrange if necessary) be two starters with $x_{2i} - x_{1i} = y_{2i} - y_{1i}$ and all distance $d(\{x_{1i}, x_{2i}\}, \{y_{1i}, y_{2i}\})$ are distinct and containing a zero distance, say $d(\{x_{1j}, x_{2j}\}, \{y_{1j}, y_{2j}\}) = 0$. Let $a_i = d(\{x_{1i}, x_{2i}\}, \{y_{1i}, y_{2i}\})$ then $a_j = 0$ and $a_i \geq 1$ for $i \neq j$ and $a_k \neq a_h$ for $k \neq h$; thus if we place the pair $\{x_{1i} + 1, x_{2i} + 1\}$ in the first row and column $-a_i + 1 \pmod{2n+1}$ then $\{y_{1i} + 1, y_{2i} + 1\}$ will occur in the first column and row $a_i + 1 \pmod{2n+1}$ since the distance from $\{x_{1i}, x_{2i}\}$ to $\{y_{1i}, y_{2i}\}$ is $a_i$. Thus clearly 1 missing in first row and first column and so by the cyclic condition $i$ is missing from $i$-th row and $i$-th column, and a Z-cyclic referee square is constructed.

**Example 3.2.1** In $Z_{11}$

$$\begin{aligned} X &= \{\{1,2\}, \{7,9\}, \{3,6\}, \{4,8\}, \{5,10\}\} \\ Y &= \{\{1,2\}, \{4,6\}, \{7,10\}, \{5,9\}, \{3,8\}\} \end{aligned}$$

are two starters, with distances from X to Y given by

$$D = \{0, 8, 4, 1, 9\}.$$

so the first row of a Z-cyclic referee square is

$$\{2,3\}, --, \{6,11\}, \{8,10\}, --, --, --, \{4,7\}, --, --, \{5,9\}.$$

i.e Example 3.1.3.

**Examples 3.2.2**

(a) In $Z_{13}$

$$\begin{aligned} X &= \{\{9,10\},\{5,7\},\{1,4\},\{12,3\},\{6,11\},\{2,8\}\} \\ Y &= \{\{9,10\},\{12,1\},\{3,6\},\{4,8\},\{2,7\},\{5,11\}\} \\ D &= \{0,7,2,5,9,3\} \end{aligned}$$

so $\{10,11\}, --, --, --, \{7,12\}, --, \{6,8\}), --, \{13,4\}, --, \{3,9\}, \{2,5\}, --$ is the first row of a Z-cyclic referee square in $Z_{13}$.

(b)In $Z_{15}$,

$$\begin{aligned} X &= \{\{1,2\},\{3,5\},\{7,10\},\{9,13\},\{6,11\},\{8,14\},\{12,4\}\} \\ Y &= \{\{1,2\},\{6,8\},\{11,14\},\{5,9\},\{7,12\},\{13,4\},\{3,10\}\} \\ D &= \{0,3,4,11,1,5,6\} \end{aligned}$$

so $\{2,3\}, --, --, --, \{10,14\}, --, --, --, --, \{13,5\}, \{9,15\}, \{8,11\}$, $\{4,6\}, --, \{7,12\}$ is the first row of a Z-cyclic referee square in $Z_{15}$.

(c) In $Z_{17}$

$$\begin{aligned} X &= \{\{10,11\},\{12,14\},\{1,4\},\{5,9\},\{15,3\},\{2,8\},\{6,13\},\{16,7\}\} \\ Y &= \{\{10,11\},\{7,9\},\{5,8\},\{16,3\},\{13,1\},\{15,4\},\{12,2\},\{6,14\}\} \\ D &= \{0,12,4,11,15,13,6,7\} \end{aligned}$$

so $\{11,12\}, --, \{16,4\}, --, \{3,9\}, \{13,15\}, \{6,10\}, --, --, --, \{17,8\}$, $\{7,14\}, --, \{2,5\}, --, --, --$ is the first row of a Z-cyclic referee square in $Z_{17}$.

(d) In $Z_{19}$

$$\begin{aligned} X &= \{\{1,2\},\{15,17\},\{13,16\},\{4,8\},\{5,10\},\{6,12\},\{7,14\},\{3,11\},\{9,18\}\} \\ Y &= \{\{1,2\},\{3,5\},\{6,9\},\{13,17\},\{10,15\},\{8,14\},\{11,18\},\{4,12\},\{7,16\}\} \\ D &= \{0,7,12,9,5,2,4,1,17\} \end{aligned}$$

so $\{2,3\}, --, \{10,19\}, --, --, --, --, \{14,17\}, --, --, \{5,9\}, --,$ $\{16,18\}, --, \{8,15\}, --, \{7,13\}, \{4,12\}$ is the first row of a Z-cyclic referee square in $Z_{19}$

(e) In $Z_{21}$

$$\begin{aligned}
X &= \{\{1,2\},\{3,5\},\{4,7\},\{12,16\},\{10,15\},\{8,14\},\{13,20\},\{11,19\},\{9,18\},\\
&\quad \{17,6\}\}\\
Y &= \{\{1,2\},\{4,6\},\{13,16\},\{7,11\},\{15,20\},\{12,18\},\{3,10\},\{9,17\},\{5,14\},\\
&\quad \{19,8\}\}\\
D &= \{0,1,9,16,5,4,11,19,17,2\}
\end{aligned}$$

so $\{2,3\}, --, \{12,20\}, --, \{10,19\}, \{13,17\}, --, --, --, --, \{14,21\}, --,$ $\{5,8\}, --, --, --, \{11,16\}, \{9,15\}, --, \{18,7\}, \{4,6\}$ is the first row of a Z-cyclic referee square in $Z_{21}$.

(f) In $Z_{23}$

$$\begin{aligned}
X &= \{\{1,2\},\{3,5\},\{4,7\},\{13,17\},\{11,16\},\{8,14\},\{15,22\},\{10,18\},\\
&\quad \{12,21\},\{19,6\},\{9,20\}\}\\
Y &= \{\{1,2\},\{4,6\},\{8,11\},\{9,13\},\{14,19\},\{16,22\},\{10,17\},\{12,20\},\\
&\quad \{21,7\},\{18,5\},\{15,3\}\}\\
D &= \{0,1,4,19,3,8,18,2,9,22,6\}
\end{aligned}$$

(g) In $Z_{25}$

$$\begin{aligned}
X &= \{\{1,2\},\{4,6\},\{15,18\},\{8,12\}),\{16,21\},\{24,5\},\{10,17\},\{14,22\},\\
&\quad \{11,20\},\{3,13\},\{23,9\},\{7,19\}\}\\
Y &= \{\{1,2\},\{7,9\},\{10,13\},\{19,23\},\{3,8\},\{12,18\},\{15,22\},\{16,24\},\\
&\quad \{5,14\},\{11,21\},\{20,6\},\{17,4\}\}\\
D &= \{0,3,20,11,12,13,5,2,19,8,22,10\}
\end{aligned}$$

(h) In $Z_{27}$

$$\begin{aligned}
X &= \{\{1,2\},\{3,5\},\{6,9\},\{12,16\},\{10,15\},\{14,20\},\{17,24\},\{18,26\}\\
&\quad \{25,7\},\{13,23\},\{11,22\},\{19,4\},\{8,21\}\}\\
Y &= \{\{1,2\},\{4,6\},\{8,11\},\{20,24\},\{14,19\},\{17,23\},\{9,16\},\{7,15\},\\
&\quad \{21,3\},\{12,22\},\{26,10\},\{13,25\},\{5,18\}\}\\
D &= \{0,1,2,8,4,3,19,16,23,26,15,21,24\}
\end{aligned}$$

(i) In $Z_{29}$

$$\begin{aligned} X &= \{\{18,19\},\{20,22\},\{1,4\},\{11,15\},\{21,26\},\{2,8\},\{10,17\},\{28,7\},\\ &\quad \{3,12\},\{6,16\},\{23,5\},\{13,25\},\{14,27\},\{24,9\}\}\\ Y &= \{18,19\},\{1,3\},\{2,5\},\{23,27\},\{6,11\},\{8,14\},\{9,16\},\{13,21\},\\ &\quad \{24,4\},\{15,25\},\{17,28\},\{10,22\},\{7,20\},\{12,26\}\}\\ D &= \{0,10,1,12,14,6,28,14,21,9,23,26,22,17\} \end{aligned}$$

(j) In $Z_{31}$

$$\begin{aligned} X &= \{\{16,17\},\{1,3\},\{11,14\},\{2,6\},\{18,23\},\{22,28\},\{19,26\},\{4,12\},\\ &\quad \{20,29\},\{5,15\},\{30,10\},\{13,25\},\{27,9\},\{7,21\},\{24,8\}\}.\\ Y &= \{\{16,17\},\{2,4\},\{3,6\},\{9,13\},\{22,27\},\{20,26\},\{7,14\},\{10,18\},\\ &\quad \{23,1\},\{19,29\},\{25,5\},\{12,24\},\{8,21\},\{28,11\},\{15,30\}\}.\\ D &= \{0,1,23,7,4,29,19,6,3,14,26,30,12,21,22\}. \end{aligned}$$

(k) In $Z_{33}$

$$\begin{aligned} X &= \{\{1,2\},\{3,5\},\{4,7\},\{6,10\},\{19,24\},\{16,22\},\{20,27\},\{18,26\},\\ &\quad \{32,8\},\{11,21\},\{12,23\},\{13,25\},\{17,30\},\{28,9\},\{14,29\},\{15,31\}\}.\\ Y &= \{\{1,2\},\{10,12\},\{3,6\},\{4,8\},\{11,16\},\{22,28\},\{14,21\},\{19,27\},\\ &\quad \{29,5\},\{15,25\},\{20,31\},\{18,30\},\{13,26\},\{9,23\},\{17,32\},\{24,7\}\}.\\ D &= \{0,7,32,31,25,6,27,1,30,4,8,5,29,14,3,9\}. \end{aligned}$$

Conversely, if there exists a Z-cyclic referee square of side $2n+1$ in $Z_{2n+1}$ then the first row of this square contains $\{x_{11},x_{21}\},\{x_{12},x_{22}\},\cdots,\{x_{1n},x_{2n}\}$ where $x_{ij} \in Z_{2n+1} - \{1\}; i = 1,2, j = 1,2,\cdots,n$ and $X = \{\{x_{1i}-1, x_{2i}-1\}; 1 \leq i \leq n\}$ is a starter in $Z_{2n+1}$. Similarly, the first column of this square contains $\{y_{11},y_{21}\},\cdots,\{y_{1n},y_{2n}\}$, where $x_{11} = y_{11}$ and $x_{21} = y_{21}$ and $Y = \{\{y_{1i}-1, y_{2i}-1\}; 1 \leq i \leq n\}$ is a starter in $Z_{2n+1}$. Furthermore, the distances from X to Y ( or from Y to X ) are distinct and containing 0. Therefore there are no Z-cyclic referee squares in $Z_7$ and $Z_9$, since all starters in $Z_7$ are

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

and all starters in $Z_9$ are

$$\{\{1,2\},\{4,6\},\{5,8\},\{3,7\}\} \qquad \{\{1,2\},\{5,7\},\{3,6\},\{4,8\}\}$$

$$\{\{2,3\},\{6,8\},\{4,7\},\{1,5\}\} \qquad \{\{3,4\},\{5,7\},\{8,2\},\{6,1\}\}$$

$\{\{4,5\},\{8,1\},\{3,6\},\{7,2\}\}$ $\{\{5,6\},\{2,4\},\{7,1\},\{8,3\}\}$

$\{\{6,7\},\{1,3\},\{2,5\},\{4,8\}\}$ $\{\{7,8\},\{2,4\},\{3,6\},\{1,5\}\}$

$\{\{7,8\},\{3,5\},\{1,4\},\{2,6\}\}$

In both cases there are no pairs of starters satisfying the required conditions.

**Conjecture 3.1** *For all odd integers $n \geq 11$, there are Z-cyclic referee squares of side $n$.*

## 3.3 The triplication and quintuplication theorems

**Theorem 3.3.1** *If a Room square of side $n$ exists then a referee square of side $3n$ exists.*

**Proof.** Suppose we have a Room square $R$ of side $n = 2s + 1$ with entries $\infty, 1, 2, \cdots, n$. By permuting rows and/or columns we may assume the square is standardized with the pairs $\{\infty, i\}$ occuring in order on the main diagonal. i.e $\{\infty, i\}$ in the position $(i, i)$. For each $i = 1, 2, 3$, let $x_i = x + n\,(i - 1)$ and define $R_{ij}$ to be the array obtaining from $R$ by deleting all main diagonal entries and replacing each remaining $\{x, y\}$ by $\{x_i, y_i\}$.

The arrays $R_{ij}, 1 \leq i, j \leq 3$, will contain among them all unordered pairs of numbers from 1 to $3n$ apart from the pairs $\{x_i, x_j\}$.

Suppose that we consider the following $3n \times 3n$ array $R'$

$$R' = \begin{pmatrix} R_{11} & R_{22} & R_{33} \\ R_{32} & R_{13} & R_{21} \\ R_{23} & R_{31} & R_{12} \end{pmatrix}.$$

Then each of the first $n$ rows contains each of $1, 2, \cdots, 3n$ exactly once, except that, in the $i$-th row , the number $i, i + n, i + 2n$ are missing. Similarly, these are missing from rows $i + n$ and $i + 2n$. A similar observation can be made about the columns. Note also that every unordered pair of numbers $x_i, y_j$ with $x \neq y$ occurs exactly once. Now we place pairs $\{i + n, i + 2n\}, \{i, i + 2n\}$ and $\{i, i + n\}$ in $(i, i)\,, (i + n, i + n)$ and $(i + 2n, i + 2n)$-th positions respectively. The resulting array is then a referee square of side $3n$.

**Example 3.3.1** Referee square of side 21. Let

$$R = \begin{pmatrix} \infty,1 & -- & -- & 3,6 & -- & 2,7 & 4,5 \\ 5,6 & \infty,2 & -- & -- & 4,7 & -- & 3,1 \\ 4,2 & 6,7 & \infty,3 & -- & -- & 5,1 & -- \\ -- & 5,3 & 7,1 & \infty,4 & -- & -- & 6,2 \\ 7,3 & -- & 6,4 & 1,2 & \infty,5 & -- & -- \\ -- & 1,4 & -- & 7,5 & 2,3 & \infty,6 & -- \\ -- & -- & 2,5 & -- & 1,6 & 3,4 & \infty,7 \end{pmatrix}$$

then, for example,

$$R_{12} = \begin{pmatrix} -- & -- & -- & 3,13 & -- & 2,14 & 4,12 \\ 5,13 & -- & -- & -- & 4,14 & -- & 3,8 \\ 4,9 & 6,14 & -- & -- & -- & 5,8 & -- \\ -- & 5,10 & 7,8 & -- & -- & -- & 6,9 \\ 7,10 & -- & 6,11 & 1,9 & -- & -- & -- \\ -- & 1,11 & -- & 7,12 & 2,10 & -- & -- \\ -- & -- & 2,12 & -- & 1,13 & 3,11 & -- \end{pmatrix}$$

and

$$R' = \begin{pmatrix}
-- & -- & -- & 3,6 & -- & 2,7 & 4,5 & -- & -- & -- & 10,13 & -- & 9,14 & 11,12 & -- & -- & -- & 17,20 & -- & 16,21 & 18,19 \\
5,6 & -- & -- & - & 4,7 & -- & 3,1 & 12,13 & -- & -- & -- & 11,14 & -- & 10,8 & 19,20 & -- & -- & -- & 18,21 & -- & 17,15 \\
4,2 & 6,7 & -- & -- & -- & 5,1 & -- & 11,9 & 13,14 & -- & -- & -- & 12,8 & -- & 18,16 & 20,21 & -- & -- & -- & 19,15 & -- \\
-- & 5,3 & 7,1 & -- & -- & -- & 6,2 & -- & 12,10 & 14,8 & -- & -- & -- & 13,9 & -- & 19,17 & 21,15 & -- & -- & -- & 20,16 \\
7,3 & -- & 6,4 & 1,2 & -- & -- & -- & 14,10 & -- & 13,11 & 8,9 & -- & -- & -- & 21,17 & -- & 20,18 & 15,16 & -- & -- & -- \\
-- & 1,4 & -- & 7,5 & 2,3 & -- & -- & -- & 8,11 & -- & 14,12 & 9,10 & -- & -- & -- & 15,18 & -- & 21,19 & 16,17 & -- & -- \\
-- & -- & 2,5 & -- & 1,6 & 3,4 & -- & -- & -- & 9,12 & -- & 8,13 & 10,11 & -- & -- & -- & 16,19 & -- & 15,20 & 17,18 & -- \\
-- & -- & -- & 17,13 & -- & 16,14 & 18,12 & -- & -- & -- & 3,20 & -- & 2,21 & 4,19 & -- & -- & -- & 10,6 & -- & 9,7 & 11,5 \\
19,13 & -- & -- & -- & 18,14 & -- & 17,8 & 5,20 & -- & -- & -- & 4,21 & -- & 3,15 & 12,6 & -- & -- & -- & 11,7 & -- & 10,1 \\
18,9 & 20,14 & -- & -- & -- & 19,8 & -- & 4,16 & 6,21 & -- & -- & -- & 5,15 & -- & 11,2 & 13,7 & -- & -- & -- & 12,1 & -- \\
-- & 19,10 & 21,8 & -- & -- & -- & 20,9 & -- & 5,17 & 7,15 & -- & -- & -- & 6,16 & -- & 12,3 & 14,1 & -- & -- & -- & 13,2 \\
21,10 & -- & 20,11 & 15,9 & -- & -- & -- & 7,17 & -- & 6,18 & 1,16 & -- & -- & -- & 14,3 & -- & 13,4 & 8,2 & -- & -- & -- \\
-- & 15,11 & -- & 21,12 & 16,10 & -- & -- & -- & 1,18 & -- & 7.19 & 2,17 & -- & -- & -- & 8,4 & -- & 14,5 & 9,3 & -- & -- \\
-- & -- & 16,12 & -- & 15,13 & 17,11 & -- & -- & -- & 2,19 & -- & 1,20 & 3,18 & -- & -- & -- & 9,5 & -- & 8,6 & 10,4 & -- \\
-- & -- & -- & 10,20 & -- & 9,21 & 11,19 & -- & -- & -- & 17,6 & -- & 16,7 & 18,5 & -- & -- & -- & 3,13 & -- & 2,14 & 4,12 \\
12,20 & -- & -- & -- & 11,21 & -- & 10,15 & 19,6 & -- & -- & -- & 18,7 & -- & 17,1 & 5,13 & -- & -- & -- & 4,14 & -- & 3,8 \\
11,16 & 13,21 & -- & -- & -- & 12,15 & -- & 18,2 & 20,7 & -- & -- & -- & 19,1 & -- & 4,9 & 6,14 & -- & -- & -- & 5,8 & -- \\
-- & 12,17 & 14,15 & -- & -- & -- & 13,16 & -- & 19,3 & 21,1 & -- & -- & -- & 20,2 & -- & 5,10 & 7,8 & -- & -- & -- & 6,9 \\
14,17 & -- & 13,18 & 8,16 & -- & -- & -- & 21,3 & -- & 20,4 & 15,2 & -- & -- & -- & 7,10 & -- & 6,11 & 1,9 & -- & -- & -- \\
-- & 8,18 & -- & 14,19 & 9,17 & -- & -- & -- & 15,4 & -- & 21,5 & 16,3 & -- & -- & -- & 1,11 & -- & 7,12 & 2,10 & -- & -- \\
-- & -- & 9,19 & -- & 8,20 & 10,18 & --, & -- & -- & 16,5 & -- & 15,6 & 17,4 & -- & -- & -- & 2,12 & -- & 1,13 & 3,11 & --
\end{pmatrix}
\quad
\begin{array}{ccc}
\multicolumn{3}{c}{\text{missing}} \\
\multicolumn{3}{c}{\text{numbers}} \\
1 & 8 & 15 \\
2 & 9 & 16 \\
3 & 10 & 17 \\
4 & 11 & 18 \\
5 & 12 & 19 \\
6 & 13 & 20 \\
7 & 11 & 21 \\
8 & 15 & 1 \\
9 & 16 & 2 \\
10 & 17 & 3 \\
11 & 18 & 4 \\
12 & 19 & 5 \\
13 & 20 & 6 \\
14 & 21 & 7 \\
15 & 1 & 8 \\
16 & 2 & 9 \\
17 & 3 & 10 \\
18 & 4 & 11 \\
19 & 5 & 12 \\
20 & 6 & 13 \\
21 & 7 & 11
\end{array}$$

$$\begin{array}{l|ccccccccccccccccccccc}
\text{missing} & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21 \\
 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\
\text{numbers} & 15 & 16 & 17 & 18 & 19 & 20 & 21 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 11
\end{array}$$

Thus the resulting array is a referee square of side 21.

$$\begin{pmatrix}
8,15 & -- & -- & 3,6 & -- & 2,7 & 4,5 & -- & -- & -- & 10,13 & -- & 9,14 & 11,12 & -- & -- & -- & 17,20 & -- & 16,21 & 18,19 \\
5,6 & 9,16 & -- & - & 4,7 & -- & 3,1 & 12,13 & -- & -- & -- & 11,14 & -- & 10,8 & 19,20 & -- & -- & -- & 18,21 & -- & 17,15 \\
4,2 & 6,7 & 10,17 & -- & -- & 5,1 & -- & 11,9 & 13,14 & -- & -- & -- & 12,8 & -- & 18,16 & 20,21 & -- & -- & -- & 19,15 & -- \\
-- & 5,3 & 7,1 & 11,18 & -- & -- & 6,2 & -- & 12,10 & 14,8 & -- & -- & -- & 13,9 & -- & 19,17 & 21,15 & -- & -- & -- & 20,16 \\
7,3 & -- & 6,4 & 1,2 & 12,19 & -- & -- & 14,10 & -- & 13,11 & 8,9 & -- & -- & -- & 21,17 & -- & 20,18 & 15,16 & -- & -- & -- \\
-- & 1,4 & -- & 7,5 & 2,3 & 13,20 & -- & -- & 8,11 & -- & 14,12 & 9,10 & -- & -- & -- & 15,18 & -- & 21,19 & 16,17 & -- & -- \\
-- & -- & 2,5 & -- & 1,6 & 3,4 & 14,21 & -- & -- & 9,12 & -- & 8,13 & 10,11 & -- & -- & -- & 16,19 & -- & 15,20 & 17,18 & -- \\
-- & -- & -- & 17,13 & -- & 16,14 & 18,12 & 15,1 & -- & -- & 3,20 & -- & 2,21 & 4,19 & -- & -- & -- & 10,6 & -- & 9,7 & 11,5 \\
19,13 & -- & -- & -- & 18,14 & -- & 17,8 & 5,20 & 16,2 & -- & -- & 4,21 & -- & 3,15 & 12,6 & -- & -- & -- & 11,7 & -- & 10,1 \\
18,9 & 20,14 & -- & -- & -- & 19,8 & -- & 4,16 & 6,21 & 17,3 & -- & -- & 5,15 & -- & 11,2 & 13,7 & -- & -- & -- & 12,1 & -- \\
-- & 19,10 & 21,8 & -- & -- & -- & 20,9 & -- & 5,17 & 7,15 & 18,4 & -- & -- & 6,16 & -- & 12,3 & 14,1 & -- & -- & -- & 13,2 \\
21,10 & -- & 20,11 & 15,9 & -- & -- & -- & 7,17 & -- & 6,18 & 1,16 & 19,5 & -- & -- & 14,3 & -- & 13,4 & 8,2 & -- & -- & -- \\
-- & 15,11 & -- & 21,12 & 16,10 & -- & -- & -- & 1,18 & -- & 7.19 & 2,17 & 20,6 & -- & -- & 8,4 & -- & 14,5 & 9,3 & -- & -- \\
-- & -- & 16,12 & -- & 15,13 & 17,11 & -- & -- & -- & 2,19 & -- & 1,20 & 3,18 & 21,7 & -- & -- & 9,5 & -- & 8,6 & 10,4 & -- \\
-- & -- & -- & 10,20 & -- & 9,21 & 11,19 & -- & -- & -- & 17,6 & -- & 16,7 & 18,5 & 1,8 & -- & -- & 3,13 & -- & 2,14 & 4,12 \\
12,20 & -- & -- & -- & 11,21 & -- & 10,15 & 19,6 & -- & -- & -- & 18,7 & -- & 17,1 & 5,13 & 2,9 & -- & -- & 4,14 & -- & 3,8 \\
11,16 & 13,21 & -- & -- & -- & 12,15 & -- & 18,2 & 20,7 & -- & -- & -- & 19,1 & -- & 4,9 & 6,14 & 3,10 & -- & -- & 5,8 & -- \\
-- & 12,17 & 14,15 & -- & -- & -- & 13,16 & -- & 19,3 & 21,1 & -- & -- & -- & 20,2 & -- & 5,10 & 7,8 & 4,11 & -- & -- & 6,9 \\
14,17 & -- & 13,18 & 8,16 & -- & -- & -- & 21,3 & -- & 20,4 & 15,2 & -- & -- & -- & 7,10 & -- & 6,11 & 1,9 & 5,12 & -- & -- \\
-- & 8,18 & -- & 14,19 & 9,17 & -- & -- & -- & 15,4 & -- & 21,5 & 16,3 & -- & -- & -- & 1,11 & -- & 7,12 & 2,10 & 6,13 & -- \\
-- & -- & 9,19 & -- & 8,20 & 10,18 & -- & -- & -- & 16,5 & -- & 15,6 & 17,4 & -- & -- & -- & 2,12 & -- & 1,13 & 3,11 & 14,7
\end{pmatrix}$$

Suppose we have a standardized Room square $R$ of side $n = 2s + 1$ with entries $\infty, 0, 1, \cdots, n-1$. Define the $n \times n$ $(0,1)$ matrix $M = (m_{ij})$ by

$$m_{ij} = \begin{cases} 1, & \text{if cell } (i,j) \text{ of } R \text{ is empty} \\ 0, & \text{otherwise.} \end{cases}$$

Then, since $n = 2s + 1$, $M$ has $s$ 1s in each row and each column, so that

$$(3.3.1) \qquad M = P_1 + P_2 + \cdots + P_s$$

where each $P_i$ is a permutation matrix,(see, for example,[**1**, Theorem 1.5.4]) Let $\phi$ be the permutation corresponding to $P_1$, i.e $\phi(\kappa) = \ell$ if and only if $P_1$ has entry 1 in the $(\kappa, \ell)$ position, and note that each cell $(\kappa, \phi(\kappa))$ in $R$ is empty. The following lemma is now clear.

**Lemma 3.3.2** ([**38**]) *Given a Room square $R$ of side $m$, where $m = 2r + 1$, there are $r$ permutations $\phi_1, \phi_2, \cdots, \phi_r$ of $\{1, 2, \cdots, m\}$ with the properties that $\phi_i(k) = \phi_j(k)$ never occurs unless $i = j$ and that cell $(k, \phi_i(k))$ is empty for $1 \le k \le m$, $1 \le i \le s$.*

**Theorem 3.3.3** *If a Room square of side $n$ exists then a referee square of side $5n$ exists.*

**Proof.** We proceed as in the triplication theorem, except this time we use the following

$$R = \begin{pmatrix} R_{11} & R_{22} & R_{33} & R_{44} & R_{55} \\ \phi R_{52} & R_{13} & \phi R_{24} & \phi R_{35} & R_{41} \\ R_{43} & \phi R_{54} & R_{15} & R_{21} & \phi R_{32} \\ R_{34} & \phi R_{45} & R_{51} & R_{12} & \phi R_{23} \\ \phi R_{25} & R_{31} & \phi R_{42} & \phi R_{53} & R_{14} \end{pmatrix}$$

where $\phi$ is the permutation associated with the permutation matrix $P_1$ which arises in the decomposition $M = P_1 + P_2 + \cdots + P_s$ in (*3.3.1*).

First consider the array $R'$ given by

$$R' = \begin{pmatrix} R_{11} & R_{22} & R_{33} & R_{44} & R_{55} \\ R_{52} & R_{13} & R_{24} & R_{35} & R_{41} \\ R_{43} & R_{54} & R_{15} & R_{21} & R_{32} \\ R_{34} & R_{45} & R_{51} & R_{12} & R_{23} \\ R_{25} & R_{31} & R_{42} & R_{53} & R_{14} \end{pmatrix}$$

Each of the first $n$ rows contains each $1, 2, \cdots, 5n$ exactly once, except that in the $i$-th row, the numbers $i, i+n, i+2n, i+3n, i+4n$ are missing. Similarly, these are missing from rows $i+n, i+2n, i+3n, i+4n$. A similar observation can be made about the columns. Unlike the triplication case, we find here that we cannot fit in the missing numbers as required. We get round this problem by replacing some of the $R_{ij}$ by $\phi R_{ij}$, where $\phi R_{ij}$ denotes the array obtained from $R_{ij}$ by permuting the columns of $R_{ij}$ by $\phi$. Because $R_{ij}$ is always in the same column of the array $R'$ as $R_{ji}$, and either both or neither have their columns permuted by $\phi$,the resulting array $R$ still has $i, i+n, i+2n, i+3n, i+4n$ missing from rows $i, i+n, \cdots, i+4n$, for each $i \leq n$, whereas $i$ is missing from columns $i, i+n, i+2n, i+3n, i+4n$; $i+n$ is missing from columns $\phi(i), i+n, \phi(i)+2n, i+3n, \phi(i)+4n$; $i+2n$ is missing from columns $i, i+n, i+2n, \phi(i)+3n, \phi(i)+4n$; $i+3n$ is missing from columns $i, \phi(i)+n, \phi(i)+2n, i+3n, i+4n$; $i+4n$ is missing from columns $\phi(i), \phi(i)+n, i+2n, \phi(i)+3n, i+4n$ . So we place

$\{i+2n, i+3n\}$ in cell $(i,i)$, $\{i+n, i+4n\}$ in cell $(i, \phi(i))$,
$\{i, i+2n\}$ in cell $(i+n, i+n)$, $\{i+3n, i+4n\}$ in cell $(i+n, n+\phi(i))$,
$\{i, i+4n\}$ in cell $(i+2n, i+2n)$, $\{i+n, i+3n\}$ in cell $(i+2n, 2n+\phi(i))$,
$\{i, i+n\}$ in cell $(i+3n, i+3n)$, $\{i+2n, i+4n\}$ in cell $(i+3n, 3n+\phi(i))$,
$\{i, i+3n\}$ in cell $(i+4n, i+4n)$, $\{i+n, i+2n\}$ in cell $(i+4n, 4n+\phi(i))$.

The resulting array is the required referee square of side $5n$.

The methods used in this section and the following section are based on the ideas used by Wallis [38].

## 3.4 Composition theorems for referee squares

**Theorem 3.4.1** *If a Room square of side $m$, a referee square of side $n$ and two MOLS of order $n$ exist, then a referee square of side $mn$ exists.*

**Proof.** Without lost of generality, suppose $M = \left(\{m_{ij}^1, m_{ij}^2\}\right)$ is a Room square on $\{\infty, 0, 1, \cdots, m-1\}$ with the pair $\{\infty, i-1\}$ in the position $(i,i)$, i.e $m_{ii}^1 = \infty$ and $m_{ii}^2 = i-1$. Let $N = \left(\{n_{ij}^1, n_{ij}^2\}\right)$ be a referee square on $\{1, 2, \cdots, n\}$. Then $n_{ij}^1, n_{ij}^2$ are either nil or belong to $\{1, 2, \cdots, n\} - \{i\}$ and are distinct for any fixed $i$, and each element of $\{1, 2, \cdots, n\} - \{i\}$ appears as $n_{ij}^1$ or $n_{ij}^2$ exactly once. Let

$A = (a_{ij}), B = (b_{ij})$ be two MOLS of order $n$, and let the join $(A, B)$ of $A$ and $B$ be $(\{a_{ij}, b_{ij}\})$. Alter $M$ by replacing each of its entries by an $n \times n$ array as follows.

(i) If cell $(i, j)$ of $M$ is empty, place an empty $n \times n$ array in it.

(ii) The cell $(i, i)$ of $M$ has $\{\infty, i-1\}$ in it. Place in that cell $N + n(i-1)$ which is obtained from $N$ by adding $n(i-1)$ to each non-nil entry.

(iii) If cell $(i, j)$ with $i \neq j$ of $M$ has $\{u, v\}$ with $0 < u < v$, add $un$ to each entry of $A$ and $vn$ to each entry of $B$ and place the join of the resulting MOLS in that cell, with ordered pairs replaced by unordered ones.

When this is done , clearly an $mn \times mn$ square array $R$ is obtained on the symbols $1, 2, \cdots, mn$; further , each cell of $R$ is either empty or contains a pair of symbols. We have to prove that each pair of symbols occurs exactly once in R. Certainly there are $m\frac{1}{2}n(n-1)$ pairs arising from (ii) and $\frac{1}{2}m(m-1)n^2$ pairs arising from (iii) i.e $\frac{1}{2}mn(mn-1)$ pairs altogether; so we only need to show that all pairs are distinct. Let $P(i, j)$ denote the collection of all pairs of $R$ arising from the $(i, j)$ cell of $M$. Then certainly all pairs in $P(i, j)$ are distinct; either they are all pairs in a Room square or they are all pairs in the join of two MOLS. Further if $(i, j) \neq (h, k)$ then $P(i, j)$ and $P(h, k)$ clearly have no pairs in common.

Finally, $i$ is missing in the $i$-th row and $i$-th column, since $R_{ii} = N_{i,i(modn)} + n[\frac{i-1}{n}]$ and $n^j_{ii(mod\ n)} \neq i\,(mod\ n)$ so $n^j_{ii(mod\ n)} + n[\frac{i-1}{n}] \neq i$ for $j = 1, 2$.

In fact, the procedures (i) (ii) (iii) in the above proof may be replaced by the following. Define the array $R$ by

$$R_{ij} = \begin{cases} \{n^1_{i,j} \pmod n + n[\frac{i-1}{n}], n^2_{i,j} \pmod n + n[\frac{j-1}{n}]\}, & \text{if } [\frac{i-1}{n}] = [\frac{j-1}{n}]; \\ \{a_{i,j} \pmod n + nm^1_{[\frac{i-1}{n}]+1,[\frac{j-1}{n}]+1}, b_{i,j} \pmod n + & \\ \qquad nm^2_{[\frac{i-1}{n}]+1,[\frac{j-1}{n}]+1}\}, & \text{if } [\frac{i-1}{n}] \neq [\frac{j-1}{n}]. \end{cases}$$

where $[x] = n-1$ if $n-1 \leq x < n$ and the arithmetical result will be nil if any one of $m^1_{ij}, m^2_{ij}, n^1_{ij}, n^2_{ij}$ is nil. i.e. nil+$a$ =nil.

**Example 3.4.1** We have a Room square of side 7

$$\begin{pmatrix} \infty,0 & -- & -- & 2,5 & -- & 1,6 & 3,4 \\ 4,5 & \infty,1 & -- & -- & 3,6 & -- & 2,0 \\ 3,1 & 5,6 & \infty,2 & -- & -- & 4,0 & -- \\ --, & 2,4 & 0,6 & \infty,3 & -- & 5,1 & \\ 6,2 & -- & 5,3 & 0,1 & \infty,4 & -- & -- \\ -- & 0,3 & -- & 6,4 & 1,2 & \infty,5 & -- \\ -- & -- & 1,4 & -- & 0,5 & 2,3 & \infty,6 \end{pmatrix}$$

a referee square $N$ of side 3 and MOLS of order 3

$$N = \begin{pmatrix} 2,3 & -- & -- \\ -- & 3,1 & -- \\ -- & -- & 1,2 \end{pmatrix} \qquad (A,B) = \begin{pmatrix} 1,1 & 2,2 & 3,3 \\ 3,2 & 1,3 & 2,1 \\ 2,3 & 3,1 & 1,2 \end{pmatrix}.$$

Thus a referee square R of side 21 exists. (We write $x_j$ for $x + nj$.)

$$R = \left(\begin{array}{ccccccccccccccccccccc}
2_0,3_0 & -- & -- & -- & -- & -- & -- & -- & -- & 1_2,1_5 & 2_2,2_5 & 3_2,3_5 & -- & -- & -- & 1_1,1_6 & 2_1,2_6 & 3_1,3_6 & 1_3,1_4 & 2_3,2_4 & 3_3,3_4 \\
-- & 3_0,1_0 & -- & -- & -- & -- & -- & -- & -- & 3_2,2_5 & 1_2,3_5 & 2_2,1_5 & -- & -- & -- & 3_1,2_6 & 1_1,3_6 & 2_1,1_6 & 3_3,2_4 & 1_3,3_4 & 2_3,1_4 \\
-- & -- & 1_0,2_0 & -- & -- & -- & -- & -- & -- & 2_2,3_5 & 3_2,1_5 & 1_2,2_5 & -- & -- & -- & 2_1,3_6 & 3_1,1_6 & 1_1,2_6 & 2_3,3_4 & 3_3,1_4 & 1_3,2_4 \\
1_4,1_5 & 2_4,2_5 & 3_4,3_5 & 2_1,3_1 & -- & -- & -- & -- & -- & -- & -- & -- & 1_3,1_6 & 2_3,2_6 & 3_3,3_6 & -- & -- & -- & 1_2,1_0 & 2_2,2_0 & 3_2,3_0 \\
3_4,2_5 & 1_4,3_5 & 2_4,1_5 & -- & 3_1,1_1 & -- & -- & -- & -- & -- & -- & -- & 3_3,2_6 & 1_3,3_6 & 2_3,1_6 & -- & -- & -- & 3_2,2_0 & 1_2,3_0 & 2_2,1_0 \\
2_4,3_5 & 3_4,1_5 & 1_4,2_5 & -- & -- & 1_1,2_1 & -- & -- & -- & -- & -- & -- & 2_3,3_6 & 3_3,1_6 & 1_3,1_6 & -- & -- & -- & 2_2,3_0 & 3_2,1_0 & 1_2,2_0 \\
1_3,1_1 & 2_3,2_1 & 3_3,3_1 & 1_5,1_6 & 2_5,2_6 & 3_5,3_6 & 2_2,3_2 & -- & -- & -- & -- & -- & -- & -- & -- & 1_4,1_0 & 2_4,2_0 & 3_4,3_0 & -- & -- & -- \\
3_3,2_1 & 1_3,3_1 & 2_3,1_1 & 3_5,2_6 & 1_5,3_6 & 2_5,1_6 & -- & 3_2,1_2 & -- & -- & -- & -- & -- & -- & -- & 3_4,2_0 & 1_4,3_0 & 2_4,1_0 & -- & -- & -- \\
2_3,3_1 & 3_3,1_1 & 1_3,2_1 & 2_5,3_6 & 3_5,1_6 & 1_5,2_6 & -- & -- & 1_2,2_2 & -- & -- & -- & -- & -- & -- & 2_4,3_0 & 3_4,1_0 & 1_4,2_0 & -- & -- & -- \\
-- & -- & -- & 1_4,1_2 & 2_4,2_2 & 3_4,3_2 & 1_6,1_0 & 2_6,2_0 & 3_6,3_0 & 2_3,3_3 & -- & -- & -- & -- & -- & -- & -- & -- & 1_5,1_1 & 2_5,2_1 & 3_5,3_1 \\
-- & -- & -- & 3_4,2_2 & 1_4,3_2 & 2_4,1_2 & 3_6,2_0 & 1_6,3_0 & 2_6,1_0 & -- & 3_3,1_3 & -- & -- & -- & -- & -- & -- & -- & 3_5,2_1 & 1_5,3_1 & 2_5,1_1 \\
-- & -- & -- & 2_4,3_2 & 3_4,1_2 & 1_4,2_2 & 2_6,3_0 & 3_6,1_0 & 1_6,2_0 & -- & -- & 1_3,2_3 & -- & -- & -- & -- & -- & -- & 2_5,3_1 & 3_5,1_1 & 1_5,2_1 \\
1_6,1_2 & 2_6,2_2 & 3_6,3_2 & -- & -- & -- & 1_5,1_3 & 2_5,2_3 & 3_5,3_3 & 1_0,1_1 & 2_0,2_1 & 3_0,3_1 & 2_4,3_4 & -- & -- & -- & -- & -- & -- & -- & -- \\
3_6,2_2 & 1_6,3_2 & 2_6,1_2 & -- & -- & -- & 3_5,2_3 & 1_5,3_3 & 2_5,1_3 & 3_0,2_1 & 1_0,3_1 & 2_0,1_1 & -- & 3_4,1_4 & -- & -- & -- & -- & -- & -- & -- \\
2_6,3_2 & 3_6,1_2 & 1_6,2_2 & -- & -- & -- & 2_5,3_3 & 3_5,1_3 & 1_5,2_3 & 2_0,3_1 & 3_0,1_1 & 1_0,2_1 & -- & -- & 1_4,2_4 & -- & -- & -- & -- & -- & -- \\
-- & -- & -- & 1_0,1_3 & 2_0,2_3 & 3_0,3_3 & -- & -- & -- & 1_6,1_4 & 2_6,2_4 & 3_6,3_4 & 1_1,1_2 & 2_1,2_2 & 3_1,3_2 & 2_5,3_5 & -- & -- & -- & -- & -- \\
-- & -- & -- & 3_0,2_3 & 1_0,3_3 & 2_0,1_3 & -- & -- & -- & 3_6,2_4 & 1_6,3_4 & 2_6,1_4 & 3_1,2_2 & 1_1,3_2 & 2_1,1_2 & -- & 3_5,1_5 & -- & -- & -- & -- \\
-- & -- & -- & 2_0,3_3 & 3_0,1_3 & 1_0,2_3 & -- & -- & -- & 2_6,3_4 & 3_6,1_4 & 1_6,2_4 & 2_1,3_2 & 3_1,1_2 & 1_1,2_2 & -- & -- & 1_5,2_5 & -- & -- & -- \\
-- & -- & -- & -- & -- & -- & 1_1,1_4 & 2_1,2_4 & 3_1,3_4 & -- & -- & -- & 1_0,1_5 & 2_0,2_5 & 3_0,3_5 & 1_2,1_3 & 2_2,2_3 & 3_2,3_3 & 2_6,3_6 & -- & -- \\
-- & -- & -- & -- & -- & -- & 3_1,2_4 & 1_1,3_4 & 2_1,1_4 & -- & -- & -- & 3_0,2_5 & 1_0,3_5 & 2_0,1_5 & 3_2,2_3 & 1_2,3_3 & 2_2,1_3 & -- & 3_6,1_6 & -- \\
-- & -- & -- & -- & -- & -- & 2_1,3_4 & 3_1,1_4 & 1_1,2_4 & -- & -- & -- & 2_0,3_5 & 3_0,1_5 & 1_0,2_5 & 2_2,3_3 & 3_2,1_3 & 1_2,2_3 & -- & -- & 1_6,2_6
\end{array}\right)$$

Our next theorem extends the results of section 3.

In [38] we have the following lemma. Suppose $n \geq 3$ is an odd integer; we denote by $\mathcal{A}_n$ the $n \times n$ array whose $(i,j)$-th entry is the ordered pair

$$(j - i + 1, i + j - 1)$$

where the elements $j - i + 1$ and $i + j - 1$ are taken modulo $n$ as members of the set $N = \{1, 2, \cdots, n\}$. For example, $\mathcal{A}_3$ and $\mathcal{A}_5$ are the arrays of suffixes in $R'$ in the proof of Theorem 3.3.1 and Theorem 3.3.3 respectively.

**Lemma 3.4.2** *The entries of $\mathcal{A}_n$ consist of the ordered pairs of members of $N$ taken once each. The entries in a given row or column of $\mathcal{A}_n$ contain between them every member of $N$ once as a left member and once as a right member. If the pair $(x, y)$ occurs in a given column then $(y, x)$ also occurs in that column.*

**Theorem 3.4.3** *If $m$ and $n$ are odd integers such that $m + 2 \geq n$ and if there is a Room square of side $m$ then there is a referee square of side $mn$.*

**Proof.** Let $m = 2r + 1, n = 2s + 1$; then $r \geq s - 1$. We want to construct a referee square of side $mn$ based on $\{1, 2, \cdots, mn\}$. It is convenient to write

$$x_j = x + m(j - 1) \quad \text{where } 1 \leq x \leq m,\ 1 \leq j \leq n$$

so that every integer from 1 to $mn$ has a unique representation. Given a standardized Room square $R$ and regarding the pairs in this Room square as ordered pairs, we write $R_{ij}$ for the array formed from $R$ in the following way:

(i) delete all diagonal entries,

(ii) replace the entry $\{x, y\}$ of $R$ by $\{x_i, y_j\}$.

The set of all arrays $R_{ij}$ with $1 \leq i \leq n$ and $1 \leq j \leq n$ will contain in them all ordered pairs of integers between 1 and $mn$ except for the pairs $\{x_i, x_j\}$.

If $n$ arrays $R_{ij}$ are placed in a row such that every member of $N = \{1, 2, \cdots, n\}$ occurs once as a left-hand index and once as a right-hand index of $R_{ij}$ then row $x$ of the resulting array will contain $1_j, 2_j, \cdots, m_j$; $j = 1, 2, \cdots, n$, precisely once except for each $x_j$. A similar remark applied to columns.

We construct a referee square by replacing every entry of $\mathcal{A}_n$ by a $m \times m$ block by the following rules. For a given $j$, select permutations $\phi_1^j, \phi_2^j, \cdots, \phi_n^j$ satisfying the following.

(i) $\phi_1^j$ and $\phi_j^j$ are the identity permutations.

(ii) $\phi_k^j = \phi_\ell^j$ if $(k, \ell)$ and $(\ell, k)$ occur in column $j$ of $\mathcal{A}_n$.

(iii) all the $\phi_k^j$ except the identity permutation are selected as distinct members of the set of $r$ permutations associated with the Room square $R$ as in (*3.3.1*) (exactly $s - 1$ such permutations are selected).

(iv) the remaining $\phi_k^j$ is chosen as the identity (by (i) this occurs only in case $j = 1$, say, $(k_1, \ell_1)$ ).

This will be possible since $m + 2 \geq n$ implies $r \geq s - 1$. Now replace the entry $(k, \ell)$ in column $j$ of $\mathcal{A}_n$ by the array $\phi_k^j R_{k\ell}$ which is obtained by performing the permutation $\phi_k^j$ on the columns of $R_{k\ell}$. The resulting array will contain every number from 1 to $mn$ in each row and each column except that every $x_k$, $k = 1, 2, \cdots, n$ is missing from every row $x_j, x = 1, 2, \cdots, m$; $j = 1, 2, \cdots, n$, and that when $j$ is such that $(k, \ell)$ is an entry in column $j$ of $\mathcal{A}_n$ then $x_k$ and $x_\ell$ are missing from column $\left(\phi_k^j(x)\right)_j$. Moreover, the array contains every unordered pair of numbers of $\{1, 2, \cdots, mn\}$ (in our construction the ordered pair are read unordered pair) except for the pairs of the form $(x_k, x_\ell)$ and contains each precisely once.

Now we insert $(i_{k_1}, i_{\ell_1})$ in cell $(i, i), (i, i_{2j-1})$ in cell $(i + jn, i + jn)$, $i = 1, 2, \cdots, m$; $j = 2, 3, \cdots, n$ and for each $k$, if $(k, \ell)$ with $k \neq \ell$ was an entry of column $j$ but not in $(j, j)$ of $\mathcal{A}_n$ (so $k \neq j$) we place $\{x_k, x_\ell\}$ in the $\left(x_j, \left(\phi_k^j(x)\right)_j\right)$ position of the new square. A referee square of side $mn$ is thus constructed.

**Corollary 3.4.4** *If $m$ is an odd composite integer then there exists a referee square of side $m$.*

**Proof.** Any such $m$ other than 9,15,25 can be expressed as a product $m = uv$ where $u \geq v > 1, u \geq 7$. By Theorem 3.4.3 and the existence of a Room square of order $u$, it follows that, for each such $m$, a referee square of side $m$ exists. Finally, referee squares of side 9,15,25 have already been exhibited in Examples 3.1.2 and 3.2.2 (b),(g).

# Chapter 4

# Z-cyclic triple whist tournaments

Let $p = 2^k t + 1$ be a prime where $t > 1$ is an odd integer, $k \geq 2$. Methods of constructing a Z-cyclic triple whist tournament $TWh(p)$ are given. By such methods we construct a Z-cyclic $TWh(p)$ for all primes $p$, $p \equiv 1 \pmod 4$, $29 \leq p \leq 16097$, except $p = 257$. Let $p_i = 2^{k_i} t_i + 1, q = 2^k t + 3$ be primes where $t, t_i; i = 1, 2, \cdots, r$ are odd $> 1$. We proved that if Z-cyclic $TWh(p_i)$ and $TWh(q+1)$ exist then Z-cyclic $TWh(\prod_{i=1}^r p_i^{\alpha_i})$ and $TWh(q \prod_{i=1}^r p_i^{\alpha_i} + 1)$ exist where $\alpha_i$ are positive integers. Further we show that whist tournaments of order $p \equiv 1 \pmod 4$ can be constructed in which the partner pairs form a non-patterned starter.

## 4.1 Introduction

If $G$ is an abelian group with identity element 0 and $G^* = G - \{0\}$ then a starter $X$ for $G$ is a partition of $G^*$ into pairs such that $\{x_i - y_i;\ \{x_i, y_i\} \in X\} = G^*$. A starter is a strong starter if the sums $x_i + y_i$ of pairs $\{x_i, y_i\}$ are all distinct and non-zero. A patterned starter is a starter whose pairs are of the form $\{x_i, -x_i\}$.

**Theorem 4.1.1** ([31]) *If $p$ is a prime and $p^n = 2^k t + 1$ where $t > 1$ is odd and $k > 0$, $d = 2^{k-1}$, and if $\theta$ is a primitive element in the Galois field $GF(p^n)$ then*

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

*is a strong starter.*

**Theorem 4.1.2** *If $p$ is a prime and $p = 2^k t + 1$ where $t > 1$ is odd, $d = 2^k$, $m = 2^{k-1}$, $n = 2^{k-2}$, if $\omega$ is a primitive root mod $p$, if $a_0, a_1, \cdots, a_{m-1}, c_0, c_1, \cdots, c_{n-1}$ are integers such that*

1. *$a_i+i \pmod d \in \{m, m+1, \cdots, d-1\}$ are all distinct, $i = 0, 1, \cdots, m-1$.*
2. *$\frac{\omega^{a_i}-1}{\omega^{a_0}-1} = \omega^{b_i}$ where $b_i+i$ are incongruent $\pmod m$, $i = 0, 1, \cdots, m-1$.*

*then the following pairs form a starter*

$$\{\{\omega^{2i}, \omega^{2i+a_{2i}}\}, \{\omega^{dc_i+(2i+1)}, \omega^{dc_i+(2i+1)+a_{2i+1}}\}\} \otimes \{1, \omega^d, \cdots, \omega^{d(t-1)}\}$$

*where $i = 0, 1. \cdots, n-1$.*

**Proof.** The differences between pairs are

(*0*). $(\omega^{a_0}-1) \cdot \{\pm 1, \pm\omega^d, \pm\omega^{2d}, \cdots, \pm\omega^{d(t-1)}\}$
(*1*). $(\omega^{a_1}-1) \cdot \{\pm\omega^{dc_0+1}, \pm\omega^{dc_0+1+d}, \pm\omega^{dc_0+1+2d}, \cdots, \pm\omega^{dc_0+1+d(t-1)}\}$
(*2*). $(\omega^{a_2}-1) \cdot \{\pm\omega^{2}, \pm\omega^{d+2}, \pm\omega^{2d+2}, \cdots, \pm\omega^{d(t-1)+2}\}$
(*3*). $(\omega^{a_3}-1) \cdot \{\pm\omega^{dc_1+3}, \pm\omega^{dc_1+3+d}, \pm\omega^{dc_1+3+2d}, \cdots, \pm\omega^{dc_1+3+d(t-1)}\}$
... ...............................................
(*m-1*). $(\omega^{a_{m-1}}-1) \cdot \{\pm\omega^{dc_n+m-1}, \pm\omega^{dc_n+m-1+d}, \cdots, \pm\omega^{dc_n+m-1+d(t-1)}\}$

If $\frac{\omega^{a_i}-1}{\omega^{a_0}-1} = \omega^{b_i}$ then $\omega^{a_i}-1 = (\omega^{a_0}-1)\omega^{b_i} \quad 0 \le i \le m-1$ and the differences (*0*)–(*m-1*) become

$$(A) \qquad \omega^{i+b_i}(\omega^{a_0}-1) \cdot \{\pm 1, \pm\omega^d, \cdots, \pm\omega^{d(t-1)}\}$$

Now $-1 = \omega^{\frac{d}{2}t}$ where $t$ is odd, so $-1 = \omega^{du+m}$ for some integer $u$, so $(A)$ become

$$\omega^{i+b_i}(\omega^{a_0}-1) \cdot \{1, \omega^m, \omega^{2m}, \omega^{3m}, \cdots, \omega^{d(t-1)}\}.$$

and these are just $1, \omega, \cdots, \omega^{dt-1}$. since $b_i+i$ are incongruent $\pmod m$. Therefore the differences are all distinct.

By the same argument, the following is true.

**Theorem 4.1.3** *If $p = 2^k t + 1$ is a prime where $t > 1$ is odd, $d = 2^k$, $m = 2^{k-1}$, $n = 2^{k-2}$, $\omega$ is a primitive root mod $p$, if $a_0, a_1, \cdots, a_{m-1}, c_0, c_1, \cdots, c_{n-1}$ are integers such that*

1. *$a_i+2i \pmod d \in \{1, 3, \cdots, d-1\}$ are all distinct, $i = 0, 1, \cdots, m-1$.*
2. *$\frac{\omega^{a_i}-1}{\omega^{a_0}-1} = \omega^{b_i}$ where $b_i+2i$ are incongruent mod $m$, $i = 0, 1, \cdots, m-1$.*

*then the following pairs form a starter*

$$\{\{\omega^{2i}, \omega^{2i+a_i}\}, \{\omega^{dc_i+m+2i}, \omega^{dc_i+m} + 2i + a_{(n+i)}\}\}\} \otimes \{1, \omega^d, \cdots, \omega^{d(t-1)}\}$$

*where $i = 0, 1. \cdots, n-1$.*

A whist tournament Wh($4n$) for $4n$ player is a schedule of games each involving two players $a, b$ playing against two other players $c, d$ such that

1. the games are arranged in $4n-1$ rounds each of $n$ games.
2. each player plays in exactly one game in each round.
3. each player partners each other player exactly once .
4. each player opposes every other player exactly twice.

We represent by the 4-tuple $(a, b; c, d)$ a whist game in which $a, b$ are partners as are $c, d$.

The whist tournament problem, namely the problem of constructing a $Wh(4n)$ for each $n \geq 1$, has its mathematical genesis in the classic paper of E.H Moore (1896) [30]. In that paper Moore refined the opponent relationships by defining $a$ and $c$ ( and also $b$ and $d$) to be opponents of the first kind and calling $a$ and $d$ (also $b$ and $c$) opponents of the second kind. Moore then defined a triple whist tournament $TWh(4m)$ to be a $Wh(4m)$ which satisfies the triple whist conditons:

5. every player is an opponent of the first kind with every other player exactly once, and consequently

6. every player is an opponent of the second kind with every other player exactly once.

A Wh($4n$) (resp. $TWh(4n)$) is called Z-cyclic if (1) the players are elements in $Z_{4n-1} \cup \{\infty\}$ and (2) there exists a round, called the initial round (alternatively round 1), such that for each $j = 1, 2, \cdots, 4n-2$, round $j+1$ is obtained by adding $j \pmod{4n-1}$ to each non-$\infty$ element of the initial round. Given a Z-cyclic $Wh(4n)$ (resp. $TWh(4n)$), any round can serve as the initial round. It is conventional to designate as initial round that in which $\infty$ and 0 are partners.

In 1970's the existence of $Wh(4n)$ was established for all $n$. The existence of Z-cyclic Wh($4n$) was established by Anderson and Finizio [9] when $4n-1$ is of the form $qp_1^{\alpha_1} \cdots p_n^{\alpha_n}$ where $q, p_1, \cdots p_n$ are primes. $q \equiv 3 \pmod 4$, $q \geq 7, p_i \equiv 1 \pmod 4$, $i = 1, 2, \cdots, n$ and $\alpha_i \geq 0, i = 1, 2, \cdots, n$ and a Z-cyclic $Wh(q+1)$ exists. They also established the existence of Z-cyclic $TWh(3p_1^{\alpha_1} \cdots p_n^{\alpha_n} + 1)$ whenever the $p_i$ are primes $\equiv 1 \pmod 4$ which are compatible. In this chapter we will show that Z-cyclic $TWh(q\prod_{i=1}^{n} p_i^{\alpha_i} + 1)$ exists when $p_i = 2^{n_i}t_i + 1$ are primes, $t_i \geq 1$ odd, $q \equiv 3 \pmod 4$, provided that Z-cyclic $TWh(p_i)$ and $TWh(q+1)$ exist.

A whist tournament $Wh(4n+1)$ for $4n+1$ players is a schedule of games each involving two players playing against two other players such that

1. the games are arranged in $4n+1$ rounds each of $n$ games.
2. each player plays in exactly one game in all but one of the rounds.
3. each player partners each other player exactly once .
4. each player opposes every other player exactly twice.

If condition 4 is replaced by the triple whist conditions 5 and 6 then it is called a triple whist tournament $TWh(4n+1)$.

If the players are the elements of $Z_{4n+1}$ and if each round is obtained by developing the initial round modulo $4n+1$, we say that the triple whist tournament is Z-cyclic. By convention we take the initial round to be the round in which player 0 does not play.

If $E$ is a subset of $Z_v$, we say that the games $\{a_i, b_i; c_i, d_i\}$ $i = 1, 2, \cdots, r$, satisfy the $Z$-cyclic triple whist tournament conditions on $E$ if

1. $\cup\{a_i, b_i, c_i, d_i\} = E$
2. $\{\pm(a_i - b_i), \pm(c_i - d_i); i = 1, 2, \cdots, r\} = E$
3. $\{\pm(a_i - c_i), \pm(b_i - d_i); i = 1, 2, \cdots, r\} = E$
4. $\{\pm(a_i - d_i), \pm(c_i - b_i); i = 1, 2, \cdots, r\} = E$

The games $\{a_i, b_i; c_i, d_i\}$, $i = 1, 2, \cdots, n$ form an initial round of a $Z$-cyclic $TWh(4n+1)$ if they satisfy the $Z$-cyclic triple whist tournament conditions on $Z_{4n+1} - \{0\}$.

In 1975 [14] Baker proved that if $p = 4n+1$ is prime, a Z- cyclic Wh($4n+1$) exists with patterned initial round. We will show that Z-cyclic Wh($4n+1$)

exists with non-patterned initial round. Recently Anderson, Cohen and Finizio [3] showed that Z-cyclic $TWh(v)$ exists when $v = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ where $p_i$ are $\equiv 5 \pmod 8), p_i \geq 29$. We will show that a Z-cyclic $TWh(v)$ exists when $v = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$, $p_i = 2^{n_i}t_i+1$ are primes and Z-cyclic $TWh(p_i)$ exist. Further methods of constructing $TWh(p_i)$ where $p_i$ are primes $\geq 29$ are given. We start with the special cases.

## 4.2 $TWh(p)$ when $p \equiv 5 \pmod 8$ is a prime

**Proposition 4.2.1** *Let $p = 4m+1$ be a prime, $m > 1$ odd and let $\omega$ be a primitive root $\pmod p$. If $a_0, a_1$ and $c_0$ are integers such that*

1. *$a_0, a_1+1 \pmod 4) \in \{2,3\}$ and are both distinct,*
2. *$\frac{\omega^{a_1}-1}{\omega^{a_0}-1}$ is a square.( i.e. $\frac{\omega^{a_1}-1}{\omega^{a_0}-1} = \omega^e$ where e is even),*
3. *exactly two of $\omega^{4c_0+1}-1, \omega^{4c_0+1}-\omega^{a_0}, \omega^{4c_0+a_1+1}-1, \omega^{4c_0+a_1+1}-\omega^{a_0}$ are squares,*

*then the following games form an initial round for a $Wh(p)$*

$$\{\omega^0, \omega^{a_0}; \omega^{4c_0+1}, \omega^{4c_0+1+a_1}\} \otimes \{1, \omega^4, \cdots, \omega^{4(m-1)}\}. \tag{4.2.1}$$

*Furthermore, if (3) is replaced by*

*3'. $(\omega^{4c_0+1}-1)(\omega^{4c_0+1+a_1}-\omega^{a_0})$ and $(\omega^{4c_0+1}-\omega^{a_0})(\omega^{4c_0+1+a_1}-1)$ are non-square.*

*then (4.2.1) form an initial round for a $TWh(p)$.*

**Proof.** Since $a_0, a_1+1 \pmod 4) \in \{2,3\}$ and are incongruent, so elements in (4.2.1) are non-zero element of $Z_p$ each occuring exactly once. By Theorem 4.1.2. the partner difference condition is satisfied.

The opponent differences are

$$\begin{array}{ll} (A) & (\omega^{4c_0+1}-1)\cdot\{\pm 1, \pm\omega^4, \cdots, \pm\omega^{4(m-1)}\} \\ (B) & (\omega^{4c_0+1+a_1}-\omega^{a_0})\cdot\{\pm 1, \pm\omega^4, \cdots, \pm\omega^{4(m-1)}\} \\ (C) & (\omega^{4c_0+1+a_1}-1)\cdot\{\pm 1, \pm\omega^4, \cdots, \pm\omega^{4(m-1)}\} \\ (D) & (\omega^{4c_0+1}-\omega^{a_0})\cdot\{\pm 1, \pm\omega^4, \cdots, \pm\omega^{4(m-1)}\}. \end{array}$$

By *3*, suppose for example that $\omega^{4c_0+1}-1$ and $\omega^{4c_0+1}-\omega^{a_0}$ are square and the other two are non-square; then $\frac{\omega^{4c_0+1+a_1}-1}{\omega^{4c_0+1}-1} = \omega^{r_1}$ and $\frac{\omega^{4c_0+1+a_1}-\omega^{a_0}}{\omega^{4c_0+1}-\omega^{a_0}} = \omega^{r_2}$ where $r_1, r_2$ are odd. So $(B)$ $(C)$ become

$$\begin{array}{ll} (B') & (\omega^{4c_0+1}-\omega^{a_0})\cdot\{\pm\omega^{r_2}, 4\pm\omega^{4+r_2},\cdots,\pm\omega^{r_2+4(m-1)}\} \\ (C') & (\omega^{4c_0+1}-1)\cdot\{\pm\omega^{r_1},\pm\omega^{r_1+4},\cdots,\pm\omega^{r_1+4(m-1)}\}. \end{array}$$

Now since $r_1$ is odd so $(A)\cup(C')$ is

$$\begin{aligned} &(\omega^{4c_0+1}-1)\cdot\{\pm 1,\pm\omega^4,\cdots,\pm\omega^{4(m-1)},\pm\omega^{r_1},\pm\omega^{4+r_1},\cdots,\pm\omega^{4(m-1)+r_1}\} \\ &=(\omega^{4c_0+1}-1)\cdot\{\omega^i; i=0,1,2,\cdots,4m-1\} \end{aligned}$$

This is the non-zero elements of $Z_p$, each occuring exactly once. Similarly, for (B′)∪ (D). Therefore the opponent differences give the non-zero elements of $Z_p$ each twice.

Finally, elements in (A)∪(B) are the opponent differences of 1st kind and these in (C)∪(D) are 2nd kind. If $(\omega^{4c_0+1}-1)$ $(\omega^{4c_0+1+a_1}-\omega^{a_0})$ and $(\omega^{4c_0+1}-\omega^{a_0})$ $(\omega^{4c_0+1+a_1}-1)$ are non-square then the same argument show that the required conditions are satisfied so $TWh(p)$ exists.

**Proposition 4.2.2** *Let* $p = 4m+1$ *be a prime,* $m > 1$ *odd and let* $\omega$ *be a primitive root mod* $p$*. If* $a_0$*,* $a_1$ *and* $c_0$ *are positive integers such that*

1. $a_0,\ a_1+1 \pmod 4 \in \{2,\ 3\}$ *and are both distinct;*
2. $\frac{\omega^{a_1}-1}{\omega^{a_0}-1} = \square$ *;*
3. $(\omega^{4c_0+1}-1)(\omega^{4c_0+1+a_1}-\omega^{a_0}) \neq \square$ *and* $(\omega^{4c_0+1}-\omega^{a_0})(\omega^{4c_0+1+a_1}-1) \neq \square$

*i.e. the quadruple* $(\omega,\ a_0,\ a_1,\ c_0)$ *satisfies conditions 1–3, then so does the quadruple* $(\omega^{p-2},\ a_0, a_1, c_0)$

**Proof.** Since $a_0,\ a_1+1 \pmod 4 \in \{2,\ 3\}$, so $a_0-a_1$ and $a_0+a_1$ are both even. So

$$\frac{(\omega^{p-2})^{a_1}-1}{(\omega^{p-2})^{a_0}-1} = \frac{(\omega^{p-1})^{a_1}(\omega^{-1})^{a_1}-1}{(\omega^{p-1})^{a_0}(\omega^{-1})^{a_0}-1} = \frac{\frac{1}{\omega^{a_1}}-1}{\frac{1}{\omega^{a_0}}-1} = \frac{\omega^{a_0-a_1}(\omega^{a_1}-1)}{\omega^{a_0}-1} = \square$$

$$\begin{aligned} &((\omega^{p-2})^{4c_0+1}-1)((\omega^{p-2})^{4c_0+1+a_1}-(\omega^{p-2})^{a_0}) = \\ &(\tfrac{1}{\omega^{4c_0+1}}-1)(\tfrac{1}{\omega^{4c_0+1+a_1}}-\tfrac{1}{\omega^{a_0}}) = \tfrac{(\omega^{4c_0+1}-1)(\omega^{4c_0+1+a_1}-\omega^{a_0})}{\omega^{8c_0+2+a_0+a_1}} \neq \square \\ &((\omega^{p-2})^{4c_0+1}-(\omega^{p-2})^{a_0})((\omega^{p-2})^{4c_0+1+a_1}-1) = \\ &(\tfrac{1}{\omega^{4c_0+1}}-\tfrac{1}{\omega^{a_0}})(\tfrac{1}{\omega^{4c_0+1+a_1}}-1) = \tfrac{(\omega^{4c_0+1}-\omega^{a_0})(\omega^{4c_0+1+a_1}-1)}{\omega^{8c_0+2+a_0+a_1}} \neq \square \end{aligned}$$

Therefore the quadruple $(\omega^{p-2},\ a_0,\ a_1,\ c_0)$ satisfies the conditions *1–3*.

**Example 4.2.1** (a) $TWh(29)$ with $\omega = 19$ or $26$

1. $a_0 = 2$, $a_1 = 6$, $c_0 = 0$. i.e. $\{1, \omega^2; \omega^1, \omega^7\} \otimes \{1, \omega^4, \cdots, \omega^{24}\}$.
2. $a_0 = 2$, $a_1 = 6$, $c_0 = 3$. i.e. $\{1, \omega^2; \omega^{13}, \omega^{19}\} \otimes \{1, \omega^4, \cdots, \omega^{24}\}$.
3. $a_0 = 2$, $a_1 = 14$, $c_0 = 3$. i.e. $\{1, \omega^2; \omega^{13}, \omega^{27}\} \otimes \{1, \omega^4, \cdots, \omega^{24}\}$.
4. $a_0 = 2$, $a_1 = 14$, $c_0 = 4$. i.e. $\{1, \omega^2; \omega^{17}, \omega^3\} \otimes \{1, \omega^4, \cdots, \omega^{24}\}$.
5. $a_0 = 2$, $a_1 = 22$, $c_0 = 0$. i.e. $\{1, \omega^2; \omega^1, \omega^{23}\} \otimes \{1, \omega^4, \cdots, \omega^{24}\}$.
6. $a_0 = 2$, $a_1 = 22$, $c_0 = 4$. i.e. $\{1, \omega^2; \omega^{17}, \omega^{11}\} \otimes \{1, \omega^4, \cdots, \omega^{24}\}$.
7. $a_0 = 3$, $a_1 = 13$, $c_0 = 0$. i.e. $\{1, \omega^3; \omega^1, \omega^{14}\} \otimes \{1, \omega^4, \cdots, \omega^{24}\}$.
8. $a_0 = 3$, $a_1 = 13$, $c_0 = 4$. i.e. $\{1, \omega^3; \omega^{17}, \omega^2\} \otimes \{1, \omega^4, \cdots, \omega^{24}\}$.
9. $a_0 = 6$, $a_1 = 2$, $c_0 = 1$. i.e. $\{1, \omega^6; \omega^5, \omega^7\} \otimes \{1, \omega^4, \cdots, \omega^{24}\}$.
10. $a_0 = 6$, $a_1 = 2$, $c_0 = 4$. i.e. $\{1, \omega^6; \omega^{17}, \omega^{19}\} \otimes \{1, \omega^4, \cdots, \omega^{24}\}$.

(b) $TWh(37)$ with $\omega = 19$ or $\omega = 2$

1. $a_0 = 2$, $a_1 = 6$, $c_0 = 0$. i.e. $\{1, \omega^2; \omega^1, \omega^7\} \otimes \{1, \omega^4, \cdots, \omega^{32}\}$.
2. $a_0 = 2$, $a_1 = 6$, $c_0 = 2$. i.e. $\{1, \omega^2; \omega^9, \omega^{15}\} \otimes \{1, \omega^4, \cdots, \omega^{32}\}$.
3. $a_0 = 2$, $a_1 = 6$, $c_0 = 4$. i.e. $\{1, \omega^2; \omega^{17}, \omega^{23}\} \otimes \{1, \omega^4, \cdots, \omega^{32}\}$.
4. $a_0 = 2$, $a_1 = 6$, $c_0 = 5$. i.e. $\{1, \omega^2; \omega^{21}, \omega^{27}\} \otimes \{1, \omega^4, \cdots, \omega^{32}\}$.
5. $a_0 = 2$, $a_1 = 30$, $c_0 = 0$. i.e. $\{1, \omega^2; \omega^1, \omega^{31}\} \otimes \{1, \omega^4, \cdots, \omega^{32}\}$.
6. $a_0 = 2$, $a_1 = 30$, $c_0 = 4$. i.e. $\{1, \omega^2; \omega^{17}, \omega^{11}\} \otimes \{1, \omega^4, \cdots, \omega^{32}\}$.
7. $a_0 = 2$, $a_1 = 30$, $c_0 = 5$. i.e. $\{1, \omega^2; \omega^{21}, \omega^{15}\} \otimes \{1, \omega^4, \cdots, \omega^{32}\}$.
8. $a_0 = 2$, $a_1 = 30$, $c_0 = 7$. i.e. $\{1, \omega^2; \omega^{29}, \omega^{23}\} \otimes \{1, \omega^4, \cdots, \omega^{32}\}$.
9. $a_0 = 3$, $a_1 = 1$, $c_0 = 4$. i.e. $\{1, \omega^3; \omega^{17}, \omega^{18}\} \otimes \{1, \omega^4, \cdots, \omega^{32}\}$.

10. $a_0 = 3, \quad a_1 = 1, \quad c_0 = 5.$ i.e. $\{1, \omega^3; \omega^{21}, \omega^{22}\} \otimes \{1, \omega^4, \cdots, \omega^{32}\}$.

**Existence of $Wh(p)$**

We consider three special cases of Proposition 4.2.1:

1. If $a_0 = a_1 = 2m$ then the condition (1), (2) are satisfied and condition (3), as in the proof, becomes

$$\omega^{2m}\frac{\omega^{4c_0+1}+1}{\omega^{4c_0+1}-1} = \omega^{r_1} \quad \text{and} \quad \omega^{2m}\frac{\omega^{4c_0+1}-1}{\omega^{4c_0+1}+1} = \omega^{r_2}$$

So if we can find $c_0$ such that $\frac{\omega^{4c_0+1}-1}{\omega^{4c_0+1}+1} = \omega^s$ where $s$ is odd then $Wh(p)$ exist. But by Mann's Lemma [29], there exist $\alpha, \beta$ odd such that $\frac{\omega^\alpha+1}{\omega^\alpha-1} = \omega^\beta$. If $\alpha = 4n+3$ we set $\alpha' = 4m - \alpha$ then $\alpha' \equiv 1 \pmod 4$ and $\frac{\omega^{\alpha'}+1}{\omega^{\alpha'}-1} = \omega^{2m+\beta}$ where $2m+\beta$ is odd. Therefore we can find $c_0$ such that $\frac{\omega^{4c_0+1}-1}{\omega^{4c_0+1}+1} = \omega^s$ where $s$ is odd. This is the Bose-Cameron type of tournament $\{1, -1; \omega^{4c+1}, -\omega^{4c+1}\} \otimes \{1, \omega^4, \cdots, \omega^{4(m-1)}\}$.

2. If $a_0 = a_1 = 2$ and $c_0 = 0$ then conditions (1), (2) are satisfied and condition (3) becomes $\omega^2 + \omega + 1$ is non-square. By Cohen's theorem for $p \geq 211$ there exists such $\omega$ and for $p \leq 211$ pairs $(p, \omega)$ are found $(13, 2), (29, 8), (37, 5)$, $(53, 5)$, $(61, 2)$, $(101, 2)$, $(109, 10)$, $(149, 3), (157, 6), 173, 2), (181, 2), (197, 3)$. Here the initial round is $\{1, \omega^2; \omega, \omega^3\} \otimes \{1, \omega^4, \cdots, \omega^{4(m-1)}\}$ in which the partner pairs are the Mullin-Nemeth starter pairs.

3. If $a_0 = a_1 = 2$ then the games are $\{1, \omega^2; \omega^{4c+1}, \omega^{4c+3}\} \otimes \{1, \omega^4, \cdots, \omega^{4(m-1)}\}$. Here again the partner pairs are the Mullin-Nemeth pairs. This construction will work if, for example, we can find $c$ such that $\omega^{4c+1} - 1$ is a square, $\omega^{4c-1} - 1$ and $\omega^{4c+3} - 1$ are non-squares. Many such examples exist. for example, when $c = 1$ we have

$$(p, \omega) = (29, 27), (37, 5), (53, 19), (101, 2), (149, 10), (173, 2), (182, 50),$$
$$(197, 8), (229, 23), (269, 12), (277, 31), (293, 2).$$

**Proposition 4.2.3** *Let $p = 4m + 1$ be a prime where $m > 1$ is odd and $\omega$ be a primitive root mod $p$. If $a_0, a_1, c_0$ are integers such that*

1. $\frac{\omega^{4a_1+1}-1}{\omega^{4a_0+1}-1}$ *is non-square,*
2. *exactly two of* $\omega^{4c_0+2}-1, \omega^{4c_0+2}-\omega^{4a_0+1}, \omega^{4(c_0+a_1)+3}-1, \omega^{4(c_0+a_1)+3}-\omega^{4a_0+1}$ *are square,*

*then the following forms an initial round for a Wh(p)*

$$\{\omega^0, \omega^{4a_0+1}; \omega^{4c_0+2}, \omega^{4(c_0+a_1)+3}\} \otimes \{1, \omega^4, \cdots, \omega^{4(m-1)}\} \tag{4.2.2}$$

*Furthermore, if (2) is replaced by (2′) then it is an initial round for a TWh(p)*

*2′* $(\omega^{4c_0+2}-1)(\omega^{4(c_0+a_1)+3}-\omega^{4a_0+1}), (\omega^{4c_0+2}-\omega^{4a_0+1})(\omega^{4(c_0+a_1)+3}-1)$
*are non-square*

**Proof.** Since $0,\ 4a_0+1,\ 4c_0+2,\ 4(c_0+a_1)+3$ are incongruent $\pmod 4$, so clearly elements in *4.2.2* are non-zero elements of $Z_{4m+1}$ each exactly once.

The partner differences are non-zero elements of $Z_{4m+1}$ each exactly once. This follows from Theorem 4.1.3.

The opponent diferences are dealt with as in the previous proof.

**Proposition 4.2.4** *Let* $p = 4m+1$ *be a prime,* $m > 1$ *odd and let* $\omega$ *be a primitive root mod p. If* $a_0,\ a_1$ *and* $c_0$ *are positive integers such that*

1. $\frac{\omega^{4a_1+1}-1}{\omega^{4a_0+1}-1} \neq \square$;
2. $(\omega^{4c_0+2}-1)(\omega^{4(c_0+a_1)+3}-\omega^{4a_0+1}) \neq \square$
3. $(\omega^{4c_0+2}-\omega^{4a_0+1})(\omega^{4(c_0+1+a_1)+3}-1) \neq \square$

*i.e. the quadruple* $(\omega,\ a_0,\ a_1,\ c_0)$ *satisfy conditions 1–3, then so does the quadruple* $(\omega^{p-2},\ a_0, a_1, c_0)$

**Proof.** The same argument as Proposition 4.2.2.

**Example 4.2.2**

(a) $TWh(29)$ with $\omega = 26$ or $\omega = 19$

1. $a_0 = 0,\quad a_1 = 1,\quad c_0 = 0.$ i.e. $\{1, \omega^1; \omega^2, \omega^7\} \otimes \{1, \omega^4, \cdots, \omega^{24}\}$.
2. $a_0 = 0,\quad a_1 = 1,\quad c_0 = 5.$ i.e. $\{1, \omega^1; \omega^{22}, \omega^{27}\} \otimes \{1, \omega^4, \cdots, \omega^{24}\}$.
3. $a_0 = 0,\quad a_1 = 4,\quad c_0 = 3.$ i.e. $\{1, \omega^1; \omega^{14}, \omega^3\} \otimes \{1, \omega^4, \cdots, \omega^{24}\}$.
4. $a_0 = 0,\quad a_1 = 4,\quad c_0 = 6.$ i.e. $\{1, \omega^1; \omega^{26}, \omega^{15}\} \otimes \{1, \omega^4, \cdots, \omega^{24}\}$.

5. $a_0 = 0, \quad a_1 = 5, \quad c_0 = 0.$ i.e. $\{1, \omega^1; \omega^2, \omega^{23}\} \otimes \{1, \omega^4, \cdots, \omega^{24}\}.$
6. $a_0 = 0, \quad a_1 = 5, \quad c_0 = 1.$ i.e. $\{1, \omega^1; \omega^6, \omega^{27}\} \otimes \{1, \omega^4, \cdots, \omega^{24}\}.$
7. $a_0 = 0, \quad a_1 = 5, \quad c_0 = 3.$ i.e. $\{1, \omega^1; \omega^{14}, \omega^7\} \otimes \{1, \omega^4, \cdots, \omega^{24}\}.$
8. $a_0 = 0, \quad a_1 = 5, \quad c_0 = 5.$ i.e. $\{1, \omega^1; \omega^{22}, \omega^{15}\} \otimes \{1, \omega^4, \cdots, \omega^{24}\}.$
9. $a_0 = 1, \quad a_1 = 0, \quad c_0 = 1.$ i.e. $\{1, \omega^5; \omega^6, \omega^7\} \otimes \{1, \omega^4, \cdots, \omega^{24}\}.$
10. $a_0 = 1, \quad a_1 = 0, \quad c_0 = 6.$ i.e. $\{1, \omega^5; \omega^{26}, \omega^{27}\} \otimes \{1, \omega^4, \cdots, \omega^{24}\}.$

(b) $TWh(37)$ with $\omega = 19$ or $\omega = 2$

1. $a_0 = 0, \quad a_1 = 1, \quad c_0 = 0.$ i.e. $\{1, \omega^1; \omega^2, \omega^7\} \otimes \{1, \omega^4, \cdots, \omega^{32}\}.$
2. $a_0 = 0, \quad a_1 = 1, \quad c_0 = 7.$ i.e. $\{1, \omega^1; \omega^{30}, \omega^{35}\} \otimes \{1, \omega^4, \cdots, \omega^{32}\}.$
3. $a_0 = 0, \quad a_1 = 3, \quad c_0 = 2.$ i.e. $\{1, \omega^1; \omega^{10}, \omega^{23}\} \otimes \{1, \omega^4, \cdots, \omega^{32}\}.$
4. $a_0 = 0, \quad a_1 = 3, \quad c_0 = 3.$ i.e. $\{1, \omega^1; \omega^{14}, \omega^{27}\} \otimes \{1, \omega^4, \cdots, \omega^{32}\}.$
5. $a_0 = 0, \quad a_1 = 6, \quad c_0 = 5.$ i.e. $\{1, \omega^1; \omega^{22}, \omega^{11}\} \otimes \{1, \omega^4, \cdots, \omega^{32}\}.$
6. $a_0 = 0, \quad a_1 = 6, \quad c_0 = 6.$ i.e. $\{1, \omega^1; \omega^{26}, \omega^{15}\} \otimes \{1, \omega^4, \cdots, \omega^{32}\}.$
7. $a_0 = 0, \quad a_1 = 7, \quad c_0 = 0.$ i.e. $\{1, \omega^1; \omega^2, \omega^{31}\} \otimes \{1, \omega^4, \cdots, \omega^{32}\}.$
8. $a_0 = 0, \quad a_1 = 7, \quad c_0 = 1.$ i.e. $\{1, \omega^1; \omega^6, \omega^{35}\} \otimes \{1, \omega^4, \cdots, \omega^{32}\}.$
9. $a_0 = 0, \quad a_1 = 8, \quad c_0 = 4.$ i.e. $\{1, \omega^1; \omega^{18}, \omega^{15}\} \otimes \{1, \omega^4, \cdots, \omega^{32}\}.$
10. $a_0 = 0, \quad a_1 = 8, \quad c_0 = 5.$ i.e. $\{1, \omega^1; \omega^{22}, \omega^{19}\} \otimes \{1, \omega^4, \cdots, \omega^{32}\}.$

In [3] Anderson, Cohen and Finizio proved that $TWh(v)$ exists where $v = \prod_{i=1}^{n} p_i^{\alpha_i}$ where the primes $p_i$ are $\equiv 5 \pmod 8$, $p_i \geq 29$. The method of the construction uses the existence of a primitive root $\omega$ of each $p_i (\neq 61)$ such that $\omega^2 \pm \omega + 1$ are both squares $\pmod{p_i}$. We show that their constructions $(A.2,\ B.1,\ C.1)$ are special cases of a more general family of construction arising from Theorem 4.2.1 and 4.2.3.

Construction A : If $\omega^2-1 \neq \square$ (non-square), $\omega^2+\omega+1=\square$ (square), $\omega^2-\omega+1=\square$ (square) then the following are an initial round for a $TWh(p)$

1. $\{1,\omega^2;-\omega^{-1},\omega^{-1}\} \otimes \{1,\omega^4,\cdots,\omega^{4(m-1)}\}$ by (2.1) : $a_0=2, a_1=2m, c_0=\frac{m-1}{2}$
2. $\{1,\omega^2;-\omega^3,\omega^3\} \otimes \{1,\omega^4,\cdots,\omega^{4(m-1)}\}$ by (2.1) : $a_0=2, a_1=2m, c_0=\frac{m+1}{2}$
3. $\{1.-\omega;-\omega^3,-1\} \otimes \{1,\omega^4,\cdots,\omega^{4(m-1)}\}$ by (2.1) : $a_0=2m+1, a_1=4m-3, c_0=\frac{m+1}{2}$
4. $\{1,\omega^{-3};\omega^{-2},-\omega^{-3}\} \otimes \{1,\omega^4,\cdots,\omega^{4(m-1)}\}$ by (2.2) : $a_0=-1, a_1=\frac{m-1}{2}, c_0=-1$

Construction B : If $\omega^2-1=\square$, $\omega^4+1=\square$, $\omega^4+\omega^2+1=\square$ then the following are an initial round for a $TWh(p)$

1. $\{1,\omega^3;\omega,-\omega^4\} \otimes \{1,\omega^4,\cdots,\omega^{4(m-1)}\}$ by (2.1) : $a_0=3, a_1=2m+3, c_0=0$
2. $\{1,\omega^3;-\omega^{-1},\omega^2\} \otimes \{1,\omega^4,\cdots,\omega^{4(m-1)}\}$ by (2.1) : $a_0=3, a_1=2m+3, c_0=\frac{m-1}{2}$
3. $\{1,\omega^{-1};-\omega^3,\omega^2\} \otimes \{1,\omega^4,\cdots,\omega^{4(m-1)}\}$ by (2.1) : $a_0=-1, a_1=2m-1, c_0=\frac{m+1}{2}$
4. $\{1,-\omega^3;\omega^2,\omega^{-1}\} \otimes \{1,\omega^4,\cdots,\omega^{4(m-1)}\}$ by (2.2) : $a_0=\frac{m+1}{2}, a_1=-1, c_0=0$

Construction C : If $\omega^4+1 \neq \square$, $\omega^2+\omega+1=\square$, $\omega^2-\omega+1=\square$ then the following are an initial round for a $TWh(p)$

1. $\{1,-\omega;\omega,-\omega^4\} \otimes \{1,\omega^4,\cdots,\omega^{4(m-1)}\}$ by (2.1) : $a_0=2m+1, a_1=2m+3, c_0=0$
2. $\{1,\omega^{-1};-\omega^{-1},-\omega^{-4}\} \otimes \{1,\omega^4,\cdots,\omega^{4(m-1)}\}$ by (2.1) : $a_0=-1, a_1=-3, c_0=\frac{m-1}{2}$

## 4.3 $TWh(p)$ where $p \equiv 9 \pmod{16}$ is a prime

**Proposition 4.3.1** *Let* $p=8t+1$ *be a prime where* $t>1$ *is odd and* $\omega$ *be a primitive root mod* $p$*. If* $a_0, a_1, a_2, a_3, c_0$ *and* $c_1$ *are integers such that*

1. $a_0, a_1+1, a_2+2, a_3+3 \pmod 8 \in \{4,5,6,7\}$ *and are all distinct,*
2. $\frac{\omega^{a_1}-1}{\omega^{a_0}-1}=\omega^{b_1}, \frac{\omega^{a_2}-1}{\omega^{a_0}-1}=\omega^{b_2}, \frac{\omega^{a_3}-1}{\omega^{a_0}-1}=\omega^{b_3}$, *where* $b_1+1, b_2+2, b_3+3 \pmod 4 \in \{1,2,3\}$ *and are all distinct,*

*3.* $\omega^{8c_0+1} - 1 = \omega^{r_1}$, $\omega^{8c_0+1} - \omega^{a_0} = \omega^{r_2}$, $\omega^{8c_0+1+a_1} - \omega^{a_0} = \omega^{r_3}$, $\omega^{8c_0+1+a_1} - 1 = \omega^{r_4}$, $\omega^{8c_1+3} - \omega^2 = \omega^{r_5}$, $\omega^{8c_1+3} - \omega^{2+a_2} = \omega^{r_6}$, $\omega^{8c_1+3+a_3} - \omega^{2+a_2} = \omega^{r_7}$, $\omega^{8c_1+3+a_3} - \omega^2 = \omega^{r_8}$ *where* $\{r_i; i = 1, 2, \cdots, 8\}$ *is partitioned into two disjoint sets* $\{r_{11}, r_{12}, r_{13}, r_{14}\} \cup \{r_{21}, r_{22}, r_{23}, r_{24}\}$ *such that* $r_{i1}, r_{i2}, r_{i3}, r_{i4}$ *are incongruent* $\pmod 4$ *for* $i = 1, 2$,

*then the following tables form an initial round for a* $Wh(p)$

$$\{\{1, \omega^{a_0}; \omega^{8c_0+1}, \omega^{8c_0+1+a_1}\}, \{\omega^2, \omega^{2+a_2}; \omega^{8c_1+3}, \omega^{8c_1+3+a_3}\}\}\otimes \{1, \omega^8, \cdots, \omega^{8(t-1)}\}. \tag{4.3.1}$$

*Furthermore, if in 3 we restrict* $r_1, r_3, r_5, r_7$ *and* $r_2, r_4, r_6, r_8$ *to be incongruent* mod(4) *respectively then the table (4.3.1) forms an initial round for a* $TWh(p)$

**Proof.** It follows from (1) that $0, a_0, 8c_0 + 1, 8c_0 + 1 + a_1, 2, 2 + a_2, 8c_1 + 3, 8c_1 + 3 + a_3$ are incongruent $\pmod 8$ so the elements in (*4.3.1*) are the non-zero elements of $Z_p$ each exactly once, and the partner difference condition is satisfied by Theorem 4.1.2. The opponent differences are

$$(A) \quad (\omega^{8c_0+1} - 1) \cdot \{\pm 1, \pm\omega^8, \cdots, \pm\omega^{8(t-1)}\}$$

$$(B) \quad (\omega^{8c_0+1+a_1} - \omega^{a_0}) \cdot \{\pm 1, \pm\omega^8, \cdots, \pm\omega^{8(t-1)}\}$$

$$(C) \quad (\omega^{8c_1+3} - \omega^2) \cdot \{\pm 1, \pm\omega^8, \cdots, \pm\omega^{8(t-1)}\}$$

$$(D) \quad (\omega^{8c_1+3+a_3} - \omega^{2+a_2}) \cdot \{\pm 1, \pm\omega^8, \cdots, \pm\omega^{8(t-1)}\}$$

$$(E) \quad (\omega^{8c_0+1} - \omega^{a_0}) \cdot \{\pm 1, \pm\omega^8, \cdots, \pm\omega^{8(t-1)}\}$$

$$(F) \quad (\omega^{8c_0+1+a_1} - 1) \cdot \{\pm 1, \pm\omega^8, \cdots, \pm\omega^{8(t-1)}\}$$

$$(G) \quad (\omega^{8c_1+3} - \omega^{2+a_2}) \cdot \{\pm 1, \pm\omega^8, \cdots, \pm\omega^{8(t-1)}\}$$

$$(H) \quad (\omega^{8c_1+3+a_3} - \omega^2) \cdot \{\pm 1, \pm\omega^8, \cdots, \pm\omega^{8(t-1)}\}$$

By the hypothesis $\omega^{8c_0+1} - 1 = \omega^{r_1}$, $\omega^{8c_0+1} - \omega^{a_0} = \omega^{r_2}$, $\omega^{8c_0+1+a_1} - \omega^{a_0} = \omega^{r_3}$, $\omega^{8c_0+1+a_1} - 1 = \omega^{r_4}$, $\omega^{8c_1+3} - \omega^2 = \omega^{r_5}$, $\omega^{8c_1+3} - \omega^{2+a_2} = \omega^{r_6}$, $\omega^{8c_1+3+a_3} - \omega^{2+a_2} = \omega^{r_7}$, $\omega^{8c_1+3+a_3} - \omega^2 = \omega^{r_8}$ where $\{r_i; i = 1, 2, \cdots, 8\}$ is partioned into two disjoint sets $\{r_{11}, r_{12}, r_{13}, r_{14}\} \cup \{r_{21}, r_{22}, r_{23}, r_{24}\}$ such that $r_{i1}, r_{i2}, r_{i3}, r_{i4}$ are incongruent $\pmod 4$ for $i = 1, 2$. Suppose for example that $r_1 \equiv r_2 \equiv 0, r_3 \equiv r_4 \equiv 1, r_5 \equiv r_6 \equiv 2, r_7 \equiv r_8 \equiv 3 \pmod 4$ then $(A), (B), (C), (D)$ become

$(A'), (B'), (C'), (D')$.

| | |
|---|---|
| (A′) | $\omega^{r_1} \cdot \{\pm 1, \pm\omega^8, \cdots, \pm\omega^{8(t-1)}\}$ |
| (B′) | $\omega^{r_3} \cdot \{\pm 1, \pm\omega^8, \cdots, \pm\omega^{8(t-1)}\}$ |
| (C′) | $\omega^{r_5} \cdot \{\pm 1, \pm\omega^8, \cdots, \pm\omega^{8(t-1)}\}$ |
| (D′) | $\omega^{r_7} \cdot \{\pm 1, \pm\omega^8, \cdots, \pm\omega^{8(t-1)}\}$ |

Since $r_1 \equiv 0, r_3 \equiv 1, r_5 \equiv 2, r_7 \equiv 3 \pmod 4$, so $(A) \cup (B) \cup (C) \cup (D)(= (A') \cup (B') \cup (C') \cup (D')) = \{\omega^i; i = 0, 1, \cdots, 8t-1\}$ i.e every non-zero elements of $Z_p$ each exactly once. Similarly, for $(E), (F), (G), (H)$. Therefore the opponent differences occur as non-zero elements of $Z_p$ each exactly twice.

In fact, the elements in $(A) \cup (B) \cup (C) \cup (D)$ are the opponent differences of 1st kind and these in $(E) \cup (F) \cup (G) \cup (H)$ are the opponent differences of 2nd kind. so it is an initial round for a $TWh(p)$.

**Example 4.3.1** (a) $TWh(41)$ with $\omega = 26$

1. $a_0 = 4,\ a_1 = 5,\ a_2 = 11,\ a_3 = 28,\ c_0 = 0,\ c_1 = 2.$
   i.e.$\{\{1, \omega^4; \omega^1, \omega^6\}, \{\omega^2, \omega^{13}; \omega^{19}, \omega^7\}\} \otimes \{1, \omega^8, \cdots, \omega^{32}\}$.

2. $a_0 = 4,\ a_1 = 6,\ a_2 = 27,\ a_3 = 11,\ c_0 = 0,\ c_1 = 1.$
   i.e.$\{\{1, \omega^4; \omega^1, \omega^7\}, \{\omega^2, \omega^{29}; \omega^{11}, \omega^{22}\}\} \otimes \{1, \omega^8, \cdots, \omega^{32}\}$.

3. $a_0 = 4,\ a_1 = 6,\ a_2 = 35,\ a_3 = 3,\ c_0 = 1,\ c_1 = 1.$
   i.e.$\{\{1, \omega^4; \omega^9, \omega^{15}\}, \{\omega^2, \omega^{37}; \omega^{11}, \omega^{14}\}\} \otimes \{1, \omega^8, \cdots, \omega^{32}\}$.

4. $a_0 = 4,\ a_1 = 12,\ a_2 = 4,\ a_3 = 12,\ c_0 = 2,\ c_1 = 2.$
   i.e.$\{\{1, \omega^4; \omega^{17}, \omega^{29}\}, \{\omega^2, \omega^6; \omega^{19}, \omega^{31}\}\} \otimes \{1, \omega^8, \cdots, \omega^{32}\}$.

5. $a_0 = 4,\ a_1 = 12,\ a_2 = 4,\ a_3 = 12,\ c_0 = 3,\ c_1 = 3.$
   i.e.$\{\{1, \omega^4; \omega^{25}, \omega^{37}\}, \{\omega^2, \omega^6; \omega^{27}, \omega^{39}\}\} \otimes \{1, \omega^8, \cdots, \omega^{32}\}$.

6. $a_0 = 4,\ a_1 = 12,\ a_2 = 36,\ a_3 = 28,\ c_0 = 2\ c_1 = 3.$
   i.e.$\{\{1, \omega^4; \omega^{17}, \omega^{29}\}, \{\omega^2, \omega^{38}; \omega^{27}, \omega^{15}\}\} \otimes \{1, \omega^8, \cdots, \omega^{32}\}$.

7. $a_0 = 4,\ a_1 = 12,\ a_2 = 36,\ a_3 = 28,\ c_0 = 3,\ c_1 = 4.$
   i.e.$\{\{1, \omega^4; \omega^{25}, \omega^{37}\}, \{\omega^2, \omega^{38}; \omega^{35}, \omega^{23}\}\} \otimes \{1, \omega^8, \cdots, \omega^{32}\}$.

8. $a_0 = 4,\ a_1 = 21,\ a_2 = 27,\ a_3 = 20,\ c_0 = 1,\ c_1 = 0.$
i.e.$\{\{1, \omega^4; \omega^9, \omega^{30}\}, \{\omega^2, \omega^{29}; \omega^3, \omega^{23}\}\} \otimes \{1, \omega^8, \cdots, \omega^{32}\}$.

9. $a_0 = 4,\ a_1 = 21,\ a_2 = 37,\ a_3 = 34,\ c_0 = 1,\ c_1 = 1.$
i.e.$\{\{1, \omega^4; \omega^9, \omega^{30}\}, \{\omega^2, \omega^{39}; \omega^{11}, \omega^5\}\} \otimes \{1, \omega^8, \cdots, \omega^{32}\}$.

10. $a_0 = 4,\ a_1 = 28,\ a_2 = 4,\ a_3 = 28,\ c_0 = 0,\ c_1 = 3.$
i.e.$\{\{1, \omega^4; \omega^1, \omega^{29}\}, \{\omega^2, \omega^6; \omega^{27}, \omega^{15}\}\} \otimes \{1, \omega^8, \cdots, \omega^{32}\}$.

(b) $TWh(73)$ with $\omega = 26, c_0 = c_1 = 0$

1. $a_0 = 4,\ a_1 = 13,\ a_2 = 13,\ a_3 = 18,\ c_0 = 0,\ c_1 = 0.$
i.e.$\{\{1, \omega^4; \omega^1, \omega^{14}\}, \{\omega^2, \omega^{15}; \omega^3, \omega^{21}\}\} \otimes \{1, \omega^8, \cdots, \omega^{64}\}$.

2. $a_0 = 4,\ a_1 = 29,\ a_2 = 13,\ a_3 = 10,\ c_0 = 0,\ c_1 = 0.$
i.e.$\{\{1, \omega^4; \omega^1, \omega^{30}\}, \{\omega^2, \omega^{15}; \omega^3, \omega^{13}\}\} \otimes \{1, \omega^8, \cdots, \omega^{64}\}$.

3. $a_0 = 4,\ a_1 = 38,\ a_2 = 3,\ a_3 = 11,\ c_0 = 0,\ c_1 = 0.$
i.e.$\{\{1, \omega^4; \omega^1, \omega^{39}\}, \{\omega^2, \omega^5; \omega^3, \omega^{14}\}\} \otimes \{1, \omega^8, \cdots, \omega^{64}\}$.

4. $a_0 = 4,\ a_1 = 38,\ a_2 = 28,\ a_3 = 26,\ c_0 = 0,\ c_1 = 0.$
i.e.$\{\{1, \omega^4; \omega^1, \omega^{39}\}, \{\omega^2, \omega^{30}; \omega^3, \omega^{29}\}\} \otimes \{1, \omega^8, \cdots, \omega^{64}\}$.

5. $a_0 = 4,\ a_1 = 38,\ a_2 = 43,\ a_3 = 59,\ c_0 = 0,\ c_1 = 0.$
i.e.$\{\{1, \omega^4; \omega^1, \omega^{39}\}, \{\omega^2, \omega^{45}; \omega^3, \omega^{62}\}\} \otimes \{1, \omega^8, \cdots, \omega^{64}\}$.

6. $a_0 = 4,\ a_1 = 38,\ a_2 = 44,\ a_3 = 26,\ c_0 = 0,\ c_1 = 0.$
i.e.$\{\{1, \omega^4; \omega^1, \omega^{39}\}, \{\omega^2, \omega^{46}; \omega^3, \omega^{29}\}\} \otimes \{1, \omega^8, \cdots, \omega^{64}\}$.

7. $a_0 = 5,\ a_1 = 6,\ a_2 = 50,\ a_3 = 67,\ c_0 = 0,\ c_1 = 0.$
i.e.$\{\{1, \omega^5; \omega^1, \omega^7\}, \{\omega^2, \omega^{52}; \omega^3, \omega^{70}\}\} \otimes \{1, \omega^8, \cdots, \omega^{64}\}$.

8. $a_0 = 5,\ a_1 = 43,\ a_2 = 5,\ a_3 = 43,\ c_0 = 0,\ c_1 = 0.$
i.e.$\{\{1, \omega^5; \omega^1, \omega^{44}\}, \{\omega^2, \omega^7; \omega^3, \omega^{46}\}\} \otimes \{1, \omega^8, \cdots, \omega^{64}\}$.

9. $a_0 = 5,\ a_1 = 43,\ a_2 = 29,\ a_3 = 67,\ c_0 = 0,\ c_1 = 0.$
i.e.$\{\{1, \omega^5; \omega^1, \omega^{44}\}, \{\omega^2, \omega^{31}; \omega^3, \omega^{70}\}\} \otimes \{1, \omega^8, \cdots, \omega^{64}\}$.

10. $a_0 = 5,\ a_1 = 46,\ a_2 = 68,\ a_3 = 49,\ c_0 = 0,\ c_1 = 0.$
i.e.$\{\{1, \omega^5; \omega^1, \omega^{47}\}, \{\omega^2, \omega^{70}; \omega^3, \omega^{52}\}\} \otimes \{1, \omega^8, \cdots, \omega^{64}\}.$

(c) $TWh(89)$ with $\omega = 6$ and $c_0 = 0,\ c_1 = 0$

1. $a_0 = 4,\ a_1 = 38,\ a_2 = 68,\ a_3 = 18,\ c_0 = 0,\ c_1 = 0.$
i.e. $\{\{1, \omega^4; \omega^1, \omega^{39}\}, \{\omega^2, \omega^{70}; \omega^3, \omega^{21}\}\} \otimes \{1, \omega^8, \cdots, \omega^{80}\}.$

2. $a_0 = 4,\ a_1 = 44,\ a_2 = 4,\ a_3 = 44,\ c_0 = 0,\ c_1 = 0.$
i.e.$\{\{1, \omega^4; \omega^1, \omega^{45}\}, \{\omega^2, \omega^6; \omega^3, \omega^{47}\}\} \otimes \{1, \omega^8, \cdots, \omega^{80}\}.$

3. $a_0 = 4,\ a_1 = 44,\ a_2 = 68,\ a_3 = 44,\ c_0 = 0,\ c_1 = 0.$
i.e.$\{\{1, \omega^4; \omega^1, \omega^{45}\}, \{\omega^2, \omega^{70}; \omega^3, \omega^{47}\}\} \otimes \{1, \omega^8, \cdots, \omega^{80}\}.$

4. $a_0 = 4,\ a_1 = 68,\ a_2 = 53,\ a_3 = 11,\ c_0 = 0,\ c_1 = 0.$
i.e.$\{\{1, \omega^4; \omega^1, \omega^{69}\}, \{\omega^2, \omega^{55}; \omega^3, \omega^{14}\}\} \otimes \{1, \omega^8, \cdots, \omega^{80}\}.$

5. $a_0 = 4,\ a_1 = 68,\ a_2 = 69,\ a_3 = 27,\ c_0 = 0,\ c_1 = 0.$
i.e.$\{\{1, \omega^4; \omega^1, \omega^{69}\}, \{\omega^2, \omega^{71}; \omega^3, \omega^{30}\}\} \otimes \{1, \omega^8, \cdots, \omega^{80}\}.$

6. $a_0 = 4,\ a_1 = 69,\ a_2 = 11,\ a_3 = 36,\ c_0 = 0,\ c_1 = 0.$
i.e.$\{\{1, \omega^4; \omega^1, \omega^{70}\}, \{\omega^2, \omega^{13}; \omega^3, \omega^{39}\}\} \otimes \{1, \omega^8, \cdots, \omega^{80}\}.$

7. $a_0 = 4,\ a_1 = 69,\ a_2 = 53,\ a_3 = 34,\ c_0 = 0,\ c_1 = 0.$
i.e.$\{\{1, \omega^4; \omega^1, \omega^{70}\}, \{\omega^2, \omega^{55}; \omega^3, \omega^{37}\}\} \otimes \{1, \omega^8, \cdots, \omega^{80}\}.$

8. $a_0 = 4,\ a_1 = 70,\ a_2 = 59,\ a_3 = 27,\ c_0 = 0,\ c_1 = 0.$
i.e.$\{\{1, \omega^4; \omega^1, \omega^{71}\}, \{\omega^2, \omega^{61}; \omega^3, \omega^{30}\}\} \otimes \{1, \omega^8, \cdots, \omega^{80}\}.$

9. $a_0 = 5,\ a_1 = 38,\ a_2 = 74,\ a_3 = 67,\ c_0 = 0,\ c_1 = 0.$
i.e.$\{\{1, \omega^5; \omega^1, \omega^{39}\}, \{\omega^2, \omega^{76}; \omega^3, \omega^{70}\}\} \otimes \{1, \omega^8, \cdots, \omega^{80}\}.$

10. $a_0 = 5,\ a_1 = 51,\ a_2 = 5,\ a_3 = 51,\ c_0 = 0,\ c_1 = 0.$
i.e.$\{\{1, \omega^5; \omega^1, \omega^{52}\}, \{\omega^2, \omega^7; \omega^3, \omega^{54}\}\} \otimes \{1, \omega^8, \cdots, \omega^{80}\}.$

### Particular cases of proposition 4.3.1

**Corollary 4.3.2** *If* $a_0 = a_2 = 4$, $a_1 = a_3 = 4t$ *and* $c_0 = c_1 = 0$ *then the following games form an initial round for a* $TWh(p)$ *provided that* $\omega^4 - 1 = \Box$, $(\omega - 1)(\omega^3 + 1) = \Box$, $(\omega + 1)(\omega^3 - 1) = \Box$*:*

$$(4.3.2) \qquad \{\{1, \omega^4; \omega, -\omega\}, \{\omega^2, \omega^6; \omega^3, -\omega^3\}\} \otimes \{1, \omega^8, \cdots, \omega^{8(t-1)}\}$$

**Proof.** If $a_0 = a_2 = 4$, $a_1 = a_3 = 4t$ and $c_0 = c_1 = 0$ then $a_0 \equiv 4$, $a_1 + 1 \equiv 5$, $a_2 + 2 \equiv 6$, $a_3 + 3 \equiv 7 \pmod 8$. so the elements in (*4.3.2*) are non-zero elements of $Z_p$ each exactly once.

For the partner condition, since $\omega^{b_1} = \frac{-2}{\omega^4 - 1}$, $\omega^{b_2} = 1$, $\omega^{b_3} = \frac{-2}{\omega^4 - 1}$ so $b_1 = b_3$ and $b_2 \equiv 0 \pmod 4$. Therefore the condition $b_1 + 1$, $b_2 + 2$, $b_3 + 3 \not\equiv 0 \pmod 4$ and are incongruent force $b_1$ to be even. But $2 = \Box$, so $b_1$ is even if $\omega^4 - 1 = \Box$.

For the opponent differences of 1st kind, since $\omega^{r_1} = \omega - 1$, $\omega^{r_3} = \omega^{4t+1} - \omega^4 = \omega^{4t+1}(\omega^3 + 1)$, $\omega^{r_5} = \omega^2(\omega - 1)$, $\omega^{r_7} = \omega^{4t+3} - \omega^6 = \omega^{4t+3}(\omega^3 + 1)$, so $r_1$, $r_3$, $r_5$, $r_7$ are incongruent mod 4 if $(\omega - 1)(\omega^3 + 1) = \Box$.

For the opponent differences of 2nd kind, since $\omega^{r_2} = \omega^{4t+1}(\omega^3 - 1)$, $\omega^{r_4} = \omega^{4t+1} - 1 = \omega^{4t}(\omega + 1)$, $\omega^{r_6} = \omega^3 - \omega^6 = \omega^{4t+3}(\omega^3 - 1)$ $\omega^{r_8} = \omega^{4t+3} - \omega^2 = \omega^{4t+2}(\omega + 1)$, so $r_2$, $r_4$, $r_6$, $r_8$ are incongruent mod 4 if $(\omega + 1)(\omega^3 - 1) = \Box$.

**Corollary 4.3.3** *If* $a_0 = a_2 = 4t + 1$, $a_1 = a_3 = 3$, $c_0 = c_1 = 0$ *then the games*

$$(4.3.3) \qquad \{\{1, -\omega; \omega, \omega^4\}, \{\omega^2, -\omega^3; \omega^3, \omega^6\} \otimes \{1, \omega^8, \cdots, \omega^{8(t-1)}\}$$

*form an initial round for a* $TWh(p)$ *provided that*

$$\omega^4 - 1 = \Box, \ (\omega - 1)(\omega^3 + 1) = \Box, \ (\omega + 1)(\omega^3 - 1) = \Box.$$

**Remark.** The constructions in (*4.3.2*) and (*4.3.3*) are essentially the same in the sense that $a, b, c$ and $d$ occur in a table with different order. Therefore one can be obtained from the other.

It follows from an unpublished result of G. McNay that the conditions

$$\omega^4 - 1 = \Box, \ (\omega - 1)(\omega^3 + 1) = \Box, \ (\omega + 1)(\omega^3 - 1) = \Box$$

which we require for the construction (*4.3.2*) hold for some primitive root $\omega$ of $p$, provied $p > 2^{24}$. Using PARI.GP, we have checked all $p = 8t + 1, (t \text{ odd}), p < 2^{24}$, and have confirmed that such $\omega$ always exists provided $p \geq 89$. We thus have

**Theorem 4.3.4** *For all prime $p = 8t + 1$, $t$ odd, there exists Z-cyclic $TWh(p)$.*

We tabulate appropriate $\omega$ for each such prime $p < 5000$.

$$\begin{array}{llllll}
(p,\omega) = & (41, no), & (73, no), & (89, 6), & (137, 5), & (233, 27), \\
(281, 19), & (313, 41), & (409, 35), & (457, 52), & (521, 85), & (569, 3), \\
(601, 11), & (617, 42), & (809, 3), & (857, 11), & (937, 69), & (953, 38), \\
(1033, 60), & (1049, 39), & (1097, 11), & (1129, 68), & (1289, 12), & (1321, 13), \\
(1433, 6), & (1481, 3), & (1609, 35), & (1657, 11), & (1721, 12), & (1801, 87), \\
(1913, 5), & (2089, 62), & (2137, 47), & (2153, 10), & (2281, 56), & (2297, 31), \\
(2377, 31), & (2393, 20), & (2441, 99), & (2473, 35), & (2521, 34), & (2617, 14), \\
(2633, 5), & (2713, 5), & (2729, 27), & (2777, 13), & (2857, 29), & (2950, 60), \\
(2969, 22), & (3001, 107), & (3049, 62), & (3209, 11), & (3257, 26), & (3433, 14), \\
(3449, 44), & (3529, 115), & (3593, 17), & (3673, 43), & (3769, 44), & (3833, 12), \\
(3881, 23), & (3929, 3), & (4057, 17), & (4073, 28), & (4153, 51), & (4201, 218), \\
(4217, 19), & (4297, 56), & (4409, 37), & (4441, 44), & (4457, 14), & (4649, 22), \\
(4729, 47), & (4793, 14), & (4889, 24), & (4937, 21), & (4969, 38). &
\end{array}$$

**Proposition 4.3.5** *Let $p = 8t + 1$ be a prime where $t > 1$ is odd and $\omega$ be a primitive root mod $p$. If $a_0, a_1, a_2, a_3, c_0$ and $c_1$ are integers such that*

1. $a_0, a_1 + 1, a_2 + 2, a_3 + 3 \pmod 8 \in \{4, 5, 6, 7\}$ *and are all distinct.*
2. $\frac{\omega^{a_1}-1}{\omega^{a_0}-1} = \omega^{b_1}, \frac{\omega^{a_2}-1}{\omega^{a_0}-1} = \omega^{b_2}, \frac{\omega^{a_3}-1}{\omega^{a_0}-1} = \omega^{b_3}$, *where* $b_1+1, b_2+2, b_3+3 \pmod 4 \in \{1, 2, 3\}$ *and are all distinct.*
3. $\omega^{8c_1+3} - 1 = \omega^{r_1}, \omega^{8c_1+3} - \omega^{a_0} = \omega^{r_2}$, $\omega^{8c_1+3+a_3} - \omega^{a_0} = \omega^{r_3}$, $\omega^{8c_1+3+a_3} - 1 = \omega^{r_4}$, $\omega^{8c_0+1} - \omega^2 = \omega^{r_5}$, $\omega^{8c_0+1} - \omega^{2+a_2} = \omega^{r_6}$, $\omega^{8c_0+1+a_1} - \omega^{2+a_2} = \omega^{r_7}$, $\omega^{8c_0+1+a_1} - \omega^2 = \omega^{r_8}$ *where* $\{r_i; i = 1, 2, \cdots, 8\}$ *is partitioned into two disjoint sets* $\{r_{11}, r_{12}, r_{13}, r_{14}\} \cup \{r_{21}, r_{22}, r_{23}, r_{24}\}$ *such that* $r_{i1}, r_{i2}, r_{i3}, r_{i4}$ *are incongruent* $\pmod 4$ *for* $i = 1, 2$

*then the following table forms an initial round for a $Wh(p)$*

$$\{\{1, \omega^{a_0}; \omega^{8c_1+3}, \omega^{8c_1+3+a_3}\}, \{\omega^2, \omega^{2+a_2}; \omega^{8c_0+1}, \omega^{8c_0+1+a_1}\}\} \otimes \{1, \omega^8, \cdots, \omega^{8(t-1)}\}. \tag{4.3.4}$$

*Furthermore, if in (3) we restrict $r_1, r_3, r_5, r_7$ and $r_2, r_4, r_6, r_8$ to be incongruent mod(4) respectively then the table (4.3.4) forms an initial round for a $TWh(p)$*

**Example 4.3.2** $TWh(41)$ with $\omega = 19$

1. $a_0 = 4,\ a_1 = 5,\ a_2 = 5,\ a_3 = 18,\ c_0 = 3,\ c_1 = 0.$

   i.e.$\{\{1, \omega^4; \omega^3, \omega^{21}\}, \{\omega^2, \omega^7; \omega^{25}, \omega^{30}\}\} \otimes \{1, \omega^8, \cdots, \omega^{32}\}$.

2. $a_0 = 4,\ a_1 = 5,\ a_2 = 13,\ a_3 = 26,\ c_0 = 4,\ c_1 = 2.$
   i.e.$\{\{1, \omega^4; \omega^{19}, \omega^5\}, \{\omega^2, \omega^{15}; \omega^{33}, \omega^{38}\}\} \otimes \{1, \omega^8, \cdots, \omega^{32}\}.$

3. $a_0 = 4,\ a_1 = 12,\ a_2 = 36,\ a_3 = 12,\ c_0 = 0,\ c_1 = 0.$
   i.e.$\{\{1, \omega^4; \omega^3, \omega^{15}\}, \{\omega^2, \omega^{38}; \omega^1, \omega^{13}\}\} \otimes \{1, \omega^8, \cdots, \omega^{32}\}.$

4. $a_0 = 4,\ a_1 = 13,\ a_2 = 5,\ a_3 = 26,\ c_0 = 4,\ c_1 = 2.$
   i.e.$\{\{1, \omega^4; \omega^{19}, \omega^5\}, \{\omega^2, \omega^7; \omega^{33}, \omega^6\}\} \otimes \{1, \omega^8, \cdots, \omega^{32}\}.$

5. $a_0 = 4,\ a_1 = 13,\ a_2 = 13,\ a_3 = 18,\ c_0 = 0,\ c_1 = 0.$
   i.e.$\{\{1, \omega^4; \omega^3, \omega^{21}\}, \{\omega^2, \omega^{15}; \omega^1, \omega^{14}\}\} \otimes \{1, \omega^8, \cdots, \omega^{32}\}.$

6. $a_0 = 4,\ a_1 = 21,\ a_2 = 37,\ a_3 = 18,\ c_0 = 0,\ c_1 = 0.$
   i.e.$\{\{1, \omega^4; \omega^3, \omega^{21}, \{\omega^2, \omega^{39}; \omega^1, \omega^{22}\}\} \otimes \{1, \omega^8, \cdots, \omega^{32}\}.$

7. $a_0 = 4,\ a_1 = 28,\ a_2 = 4,\ a_3 = 12,\ c_0 = 2,\ c_1 = 0.$
   i.e.$\{\{1, \omega^4; \omega^3, \omega^{15}\}, \{\omega^2, \omega^6; \omega^{17}, \omega^5\}\} \otimes \{1, \omega^8, \cdots, \omega^{32}\}.$

8. $a_0 = 4,\ a_1 = 30,\ a_2 = 27,\ a_3 = 19,\ c_0 = 0,\ c_1 = 3.$
   i.e.$\{\{1, \omega^4; \omega^{27}, \omega^6\}, \{\omega^2, \omega^{29}; \omega^1, \omega^{31}\}\} \otimes \{1, \omega^8, \cdots, \omega^{32}\}.$

9. $a_0 = 4,\ a_1 = 36,\ a_2 = 13,\ a_3 = 19,\ c_0 = 2,\ c_1 = 1.$
   i.e.$\{\{1, \omega^4; \omega^{11}, \omega^{30}\}, \{\omega^2, \omega^{15}; \omega^{17}, \omega^{13}\}\} \otimes \{1, \omega^8, \cdots, \omega^{32}\}.$

10. $a_0 = 5,\ a_1 = 3,\ a_2 = 37,\ a_3 = 27,\ c_0 = 3,\ c_1 = 0.$
    i.e.$\{\{1, \omega^5; \omega^3, \omega^{30}\}, \{\omega^2, \omega^{39}; \omega^{25}, \omega^{28}\}\} \otimes \{1, \omega^8, \cdots, \omega^{32}\}.$

**Proposition 4.3.6** *Let $p = 8t + 1$ be a prime where $t > 1$ is odd and $\omega$ be a primitive root mod $p$. if $a_0, a_1, a_2, a_3, c_0$ and $c_1$ are integers such that*

1. $a_0, a_1 + 1, a_2 + 2, a_3 + 3 \pmod 8 \in \{4, 5, 6, 7\}$ *and are all distinct.*
2. $\frac{\omega^{a_1}-1}{\omega^{a_0}-1} = \omega^{b_1}, \frac{\omega^{a_2}-1}{\omega^{a_0}-1} = \omega^{b_2}, \frac{\omega^{a_3}-1}{\omega^{a_0}-1} = \omega^{b_3}$, *where* $b_1+1, b_2+2, b_3+3 \pmod 4 \in \{1, 2, 3\}$ *and are all distinct.*
3. $\omega^2 - 1 = \omega^{r_1},\ \omega^2 - \omega^{a_0} = \omega^{r_2},\ \omega^{2+a_2} - \omega^{a_0} = \omega^{r_3},\ \omega^{2+a_2} - 1 = \omega^{r_4},\ \omega^{8c_1+3} - \omega^{8c_1+1} = \omega^{r_5},\ \omega^{8c_1+3} - \omega^{8c_1+1+a_1} = \omega^{r_6},\ \omega^{8c_1+3+a_3} - \omega^{8c_1+1+a_1} = \omega^{r_7},\ \omega^{8c_1+3+a_3} - \omega^{8c_1+1} = \omega^{r_8}$ *where* $\{r_i; i = 1, 2, \cdots, 8\}$ *is partitioned into two disjoint sets* $\{r_{11}, r_{12}, r_{13}, r_{14}\} \cup \{r_{21}, r_{22}, r_{23}, r_{24}\}$ *such that* $r_{i1}, r_{i2}, r_{i3}, r_{i4}$ *are incongruent* $\pmod 4$ *for* $i = 1, 2$

*then the following table forms an initial round for a* $Wh(p)$

$$\{\{1,\omega^{a_0};\omega^2,\omega^{2+a_2}\},\{\omega^{8c_0+1},\omega^{8c_0+1+a_1};\omega^{8c_1+3},\omega^{8c_1+3+a_3}\}\}\otimes \{1,\omega^8,\cdots,\omega^{8(t-1)}\}. \tag{4.3.5}$$

*Furthermore, if in (3) we restrict* $r_1, r_3, r_5, r_7$ *and* $r_2, r_4, r_6, r_8$ *to be incongruent mod*(4) *respectively then the table (4.3.5) forms an initial round for a* $TWh(p)$.

**Example 4.3.3** $TWh(41)$ with $\omega = 26$

1. $a_0 = 4,\ a_1 = 12,\ a_2 = 20,\ a_3 = 20,\ c_0 = 0,\ c_1 = 3.$
   i.e.$\{\{1,\omega^4;\omega^2,\omega^{22}\},\{\omega^1,\omega^{13};\omega^{27},\omega^7\}\}\otimes\{1,\omega^8,\cdots,\omega^{32}\}.$
2. $a_0 = 4,\ a_1 = 12,\ a_2 = 20,\ a_3 = 20,\ c_0 = 1,\ c_1 = 4.$
   i.e.$\{\{1,\omega^4;\omega^2,\omega^{22}\},\{\omega^9,\omega^{21};\omega^{35},\omega^{15}\}\}\otimes\{1,\omega^8,\cdots,\omega^{32}\}.$
3. $a_0 = 4,\ a_1 = 12,\ a_2 = 20,\ a_3 = 20,\ c_0 = 2,\ c_1 = 0.$
   i.e.$\{\{1,\omega^4;\omega^2,\omega^{22}\},\{\omega^{17},\omega^{29};\omega^3,\omega^{23}\}\}\otimes\{1,\omega^8,\cdots,\omega^{32}\}.$
4. $a_0 = 4,\ a_1 = 12,\ a_2 = 20,\ a_3 = 20,\ c_0 = 3,\ c_1 = 1.$
   i.e.$\{\{1,\omega^4;\omega^2,\omega^{22}\},\{\omega^{25},\omega^{37};\omega^{11},\omega^{31}\}\}\otimes\{1,\omega^{38},\cdots,\omega^{32}\}.$
5. $a_0 = 4,\ a_1 = 12,\ a_2 = 20,\ a_3 = 20,\ c_0 = 4,\ c_1 = 2.$
   i.e.$\{\{1,\omega^4;\omega^2,\omega^{22}\},\{\omega^{33},\omega^5;\omega^{19},\omega^{39}\}\}\otimes\{1,\omega^8,\cdots,\omega^{32}\}.$
6. $a_0 = 4,\ a_1 = 28,\ a_2 = 20,\ a_3 = 20,\ c_0 = 0,\ c_1 = 4.$
   i.e.$\{\{1,\omega^4;\omega^2,\omega^{22}\},\{\omega^1,\omega^{29};\omega^{35},\omega^{15}\}\}\otimes\{1,\omega^{38},\cdots,\omega^{32}\}.$
7. $a_0 = 4,\ a_1 = 28,\ a_2 = 20,\ a_3 = 20,\ c_0 = 1,\ c_1 = 0.$
   i.e.$\{\{1,\omega^4;\omega^2,\omega^{22}\},\{\omega^9,\omega^{37};\omega^3,\omega^{23}\}\}\otimes\{1,\omega^8,\cdots,\omega^{32}\}.$
8. $a_0 = 4,\ a_1 = 28,\ a_2 = 20,\ a_3 = 20,\ c_0 = 2,\ c_1 = 1.$
   i.e.$\{\{1,\omega^4;\omega^2,\omega^{22}\},\{\omega^{17},\omega^5;\omega^{11},\omega^{31}\}\}\otimes\{1,\omega^{38},\cdots,\omega^{32}\}.$
9. $a_0 = 4,\ a_1 = 28,\ a_2 = 20,\ a_3 = 20,\ c_0 = 3,\ c_1 = 2.$
   i.e.$\{\{1,\omega^4;\omega^2,\omega^{22}\},\{\omega^{25},\omega^{13};\omega^{19},\omega^{39}\}\}\otimes\{1,\omega^8,\cdots,\omega^{32}\}.$
10. $a_0 = 4,\ a_1 = 28,\ a_2 = 20,\ a_3 = 20,\ c_0 = 4,\ c_1 = 3.$
    i.e.$\{\{1,\omega^4;\omega^2,\omega^{22}\},\{\omega^{33},\omega^{21};\omega^{27},\omega^7\}\}\otimes\{1,\omega^{38},\cdots,\omega^{32}\}.$

**Proposition 4.3.7** *Let $p = 8t + 1$ be a prime where $t > 1$ is odd and $\omega$ be a primitive root mod $p$. If $a_0, a_1, a_2, a_3, c_0$ and $c_1$ are integers such that*

1. $a_0, a_1 + 2, a_2 + 4, a_3 + 6 \pmod 8 \in \{1,3,5,7\}$ *and are all distinct.*
2. $\frac{\omega^{a_1}-1}{\omega^{a_0}-1} = \omega^{b_1}, \frac{\omega^{a_2}-1}{\omega^{a_0}-1} = \omega^{b_2}, \frac{\omega^{a_3}-1}{\omega^{a_0}-1} = \omega^{b_3}$, *where* $b_1+1, b_2+2, b_3+3 \pmod 4 \in \{1,2,3\}$ *and are all distinct.*
3. $\omega^{8c_0+4} - 1 = \omega^{r_1}$, $\omega^{8c_0+4} - \omega^{a_0} = \omega^{r_2}$, $\omega^{8c_0+4+a_2} - \omega^{a_0} = \omega^{r_3}$, $\omega^{8c_0+4+a_2} - 1 = \omega^{r_4}$, $\omega^{8c_1+6} - \omega^2 = \omega^{r_5}$, $\omega^{8c_1+6} - \omega^{2+a_1} = \omega^{r_6}$, $\omega^{8c_1+6+a_3} - \omega^{2+a_1} = \omega^{r_7}$, $\omega^{8c_1+6+a_3} - \omega^2 = \omega^{r_8}$ *where* $\{r_i; i = 1, 2, \cdots 8\}$ *is partitioned into two disjoint sets* $\{r_{11}, r_{12}, r_{13}, r_{14}\} \cup \{r_{21}, r_{22}, r_{23}, r_{24}\}$ *such that* $r_{i1}, r_{i2}r_{i3}, r_{i4}$ *are incongruent* $\pmod 4$ *for* $i = 1, 2$

*then the following table forms an initial round for a $Wh(p)$*

$$(4.3.6) \qquad \{\{1, \omega^{a_0}; \omega^{8c_0+4}, \omega^{8c_0+4+a_2}\}, \{\omega^2, \omega^{2+a_1}; \omega^{8c_1+6}, \omega^{8c_1+6+a_3}\}\}\otimes \{1, \omega^8, \cdots, \omega^{8(t-1)}\}.$$

*Furthermore, if in (3) we restrict $r_1, r_3, r_5, r_7$ and $r_2, r_4, r_6, r_8$ to be incongruent mod(4) respectively then the table (4.3.6) forms an initial round for a $TWh(p)$*

**Example 4.3.4** $TWh(41)$ with $\omega = 26$

1. $a_0 = 5,\ a_1 = 5,\ a_2 = 15,\ a_3 = 27,\ c_0 = 2,\ c_1 = 0.$
   i.e.$\{\{1, \omega^5; \omega^{20}, \omega^{35}\}, \{\omega^2, \omega^7; \omega^6, \omega^{33}\}\} \otimes \{1, \omega^8, \cdots, \omega^{32}\}.$
2. $a_0 = 5,\ a_1 = 15,\ a_2 = 27,\ a_3 = 5,\ c_0 = 0,\ c_1 = 2.$
   i.e.$\{\{1, \omega^5; \omega^4, \omega^{31}\}, \{\omega^2, \omega^{17}; \omega^{22}, \omega^{27}\}\} \otimes \{1, \omega^8, \cdots, \omega^{32}\}.$
3. $a_0 = 5,\ a_1 = 17,\ a_2 = 13,\ a_3 = 33,\ c_0 = 1,\ c_1 = 2.$
   i.e.$\{\{1, \omega^5; \omega^{12}, \omega^{25}\}, \{\omega^2, \omega^{19}; \omega^{22}, \omega^{15}\}\} \otimes \{1, \omega^8, \cdots, \omega^{32}\}.$
4. $a_0 = 5,\ a_1 = 33,\ a_2 = 13,\ a_3 = 17,\ c_0 = 1,\ c_1 = 2.$
   i.e.$\{\{1, \omega^5; \omega^{12}, \omega^{25}\}, \{\omega^2, \omega^{35}; \omega^{22}, \omega^{39}\}\} \otimes \{1, \omega^8, \cdots, \omega^{32}\}.$
5. $a_0 = 5,\ a_1 = 37,\ a_2 = 23,\ a_3 = 19,\ c_0 = 2,\ c_1 = 4.$
   i.e.$\{\{1, \omega^5; \omega^{20}, \omega^3\}, \{\omega^2, \omega^{39}; \omega^{38}, \omega^{17}\}\} \otimes \{1, \omega^8, \cdots, \omega^{32}\}.$
6. $a_0 = 7,\ a_1 = 7,\ a_2 = 15,\ a_3 = 15,\ c_0 = 0,\ c_1 = 0.$
   i.e.$\{\{1, \omega^7; \omega^4, \omega^{19}\}, \{\omega^2, \omega^9; \omega^6, \omega^{21}\}\} \otimes \{1, \omega^8, \cdots, \omega^{32}\}.$

7. $a_0 = 7,\ a_1 = 7,\ a_2 = 15,\ a_3 = 15,\ c_0 = 3,\ c_1 = 3.$
   i.e.$\{\{1, \omega^7; \omega^{28}, \omega^3\}, \{\omega^2, \omega^9; \omega^{30}, \omega^5\}\} \otimes \{1, \omega^8, \cdots, \omega^{32}\}.$

8. $a_0 = 7,\ a_1 = 9,\ a_2 = 25,\ a_3 = 27,\ c_0 = 0,\ c_1 = 2.$
   i.e.$\{\{1, \omega^7; \omega^4, \omega^{29}\}, \{\omega^2, \omega^{11}; \omega^{22}, \omega^9\}\} \otimes \{1, \omega^8, \cdots, \omega^{32}\}.$

9. $a_0 = 7,\ a_1 = 15,\ a_2 = 15,\ a_3 = 7,\ c_0 = 0,\ c_1 = 4.$
   i.e.$\{\{1, \omega^7; \omega^4, \omega^{19}\}, \{\omega^2, \omega^{17}; \omega^{38}, \omega^5\}\} \otimes \{1, \omega^8, \cdots, \omega^{32}\}.$

10. $a_0 = 7,\ a_1 = 15,\ a_2 = 15,\ a_3 = 7,\ c_0 = 3,\ c_1 = 1.$
    i.e.$\{\{1, \omega^7; \omega^{28}, \omega^3\}, \{\omega^2, \omega^{17}; \omega^{14}, \omega^{21}\}\} \otimes \{1, \omega^8, \cdots, \omega^{32}\}.$

**Corollary 4.3.8** *If* $a_0 = a_1 = 5,\ a_2 = a_3 = 4t + 1,\ c_0 = c_1 = 0$ *then the games*

$$\{\{1, \omega^5; \omega^4, -\omega^5\}, \{\omega^2, \omega^7; \omega^6, -\omega^7\}\} \otimes \{1, \omega^8 \cdots, \omega^{8(t-1)}\}$$

*form an initial round for a* $TWh(p)$ *provided that*

$$\omega^4 - 1 = \square, \quad (\omega + 1)(\omega^5 - 1) \neq \square, \quad (\omega - 1)(\omega^5 + 1) \neq \square.$$

**Proof.** The same argument as Corollary 4.3.2

We tabulate appropriate $\omega$ for each such prime $p < 5000$.

$(p, \omega) =$ $(41, no)$, $(73, 31)$, $(89, no)$, $(137, no)$, $(233, 20)$,
$(281, 24)$, $(313, 31)$, $(409, 140)$, $(457, no)$, $(521, 28)$, $(569, 12)$,
$(601, 55)$, $(617, 17)$, $(809, 31)$, $(857, 11)$, $(937, 45)$, $(953, 20)$,
$(1033, 69)$, $(1049, 68)$, $(1097, 11)$, $(1129, 174)$, $(1289, 13)$, $(1321, 85)$,
$(1433, 17)$, $(1481, 42)$, $(1609, 43)$, $(1657, 45)$, $(1721, 12)$, $(1801, 19)$,
$(1913, 13)$, $(2089, 11)$, $(2137, 10)$, $(2153, 5)$, $(2281, 68)$, $(2297, 35)$,
$(2377, 13)$, $(2393, 6)$, $(2441, 17)$, $(2473, 5)$, $(2521, 19)$, $(2617, 14)$,
$(2633, 5)$, $(2713, 5)$, $(2729, 30)$, $(2777, 34)$, $(2857, 22)$, $(2950, 63)$,
$(2969, 15)$, $(3001, 26)$, $(3049, 47)$, $(3209, 24)$, $(3257, 12)$, $(3433, 31)$,
$(3449, 6)$, $(3529, 37)$, $(3593, 12)$, $(3673, 43)$, $(3769, 11)$, $(3833, 6)$,
$(3881, 23)$, $(3929, 12)$, $(4057, 10)$, $(4073, 10)$, $(4153, 31)$, $(4201, 23)$,
$(4217, 14)$, $(4297, 74)$, $(4409, 127)$, $(4441, 21)$, $(4457, 5)$, $(4649, 44)$,
$(4729, 55)$, $(4793, 24)$, $(4889, 31)$, $(4937, 53)$, $(4969, 73)$.

**Proposition 4.3.9** *Let* $p = 8t + 1$ *be a prime where* $t > 1$ *is odd and* $\omega$ *be a primitive root mod* $p$. *If* $a_0, a_1, a_2, a_3, c_0$ *and* $c_1$ *are integers such that*

*1.* $a_0, a_1+2, a_2+4, a_3+6 \pmod 8 \in \{1,3,5,7\}$ *and are all distinct.*

*2.* $\frac{\omega^{a_1}-1}{\omega^{a_0}-1} = \omega^{b_1}, \frac{\omega^{a_2}-1}{\omega^{a_0}-1} = \omega^{b_2}, \frac{\omega^{a_3}-1}{\omega^{a_0}-1} = \omega^{b_3}$, *where* $b_1+1, b_2+2, b_3+3 \pmod 4 \in \{1,2,3\}$ *and are all distinct.*

*3.* $\omega^2-1=\omega^{r_1}$, $\omega^2-\omega^{a_0}=\omega^{r_2}$, $\omega^{2+a_1}-\omega^{a_0}=\omega^{r_3}$, $\omega^{2+a_1}-1=\omega^{r_4}$, $\omega^{8c_1+6}-\omega^{8c_0+4}=\omega^{r_5}$, $\omega^{8c_1+6}-\omega^{8c_0+4+a_2}=\omega^{r_6}$, $\omega^{8c_1+6+a_3}-\omega^{8c_0+4+a_2}=\omega^{r_7}$, $\omega^{8c_1+6+a_3}-\omega^{8c_0+4}=\omega^{r_8}$ *where* $\{r_i; i=1,2,\cdots,8\}$ *is partitioned into two disjoint sets* $\{r_{11},r_{12},r_{13},r_{14}\}\cup\{r_{21},r_{22},r_{23},r_{24}\}$ *such that* $r_{i1},r_{i2},r_{i3},r_{i4}$ *are incongruent* $\pmod 4$ *for* $i=1,2$

*then the following table forms an initial round for a* $Wh(p)$

$$\{\{1,\omega^{a_0};\omega^2,\omega^{2+a_1}\},\{\omega^{8c_0+4},\omega^{8c_0+4+a_2};\omega^{8c_1+6},\omega^{8c_1+6+a_3}\}\}\otimes \{1,\omega^8,\cdots,\omega^{8(t-1)}\}. \tag{4.3.7}$$

*Furthermore, if in (3) we restrict* $r_1,r_3,r_5,r_7$ *and* $r_2,r_4,r_6,r_8$ *to be incongruent mod*(4) *respectively then the table (4.3.7) forms an initial round for a* $TWh(p)$

**Example 4.3.5** $TWh(41)$ with $\omega=26$

1. $a_0=5,\ a_1=15,\ a_2=39,\ a_3=1,\ c_0=1,\ c_1=0.$
   i.e.$\{\{1,\omega^5;\omega^{10},\omega^{25}\},\{\omega^4,\omega^3;\omega^6,\omega^7\}\}\otimes\{1,\omega^8,\cdots,\omega^{32}\}.$

2. $a_0=5,\ a_1=15,\ a_2=39,\ a_3=9,\ c_0=1,\ c_1=3.$
   i.e.$\{\{1,\omega^5;\omega^{10},\omega^{25}\},\{\omega^4,\omega^3;\omega^{30},\omega^{39}\}\}\otimes\{1,\omega^8,\cdots,\omega^{32}\}.$

3. $a_0=5,\ a_1=17,\ a_2=11,\ a_3=27,\ c_0=0,\ c_1=4.$
   i.e.$\{\{1,\omega^5;\omega^2,\omega^{19}\},\{\omega^4,\omega^{15};\omega^{38},\omega^{25}\}\}\otimes\{1,\omega^8,\cdots,\omega^{32}\}.$

4. $a_0=5,\ a_1=17,\ a_2=19,\ a_3=3,\ c_0=0,\ c_1=4.$
   i.e.$\{\{1,\omega^5;\omega^2,\omega^{19}\},\{\omega^4,\omega^{23};\omega^{38},\omega^1\}\}\otimes\{1,\omega^8,\cdots,\omega^{32}\}.$

5. $a_0=5,\ a_1=29,\ a_2=31,\ a_3=27,\ c_0=1,\ c_1=4.$
   i.e.$\{\{1,\omega^5;\omega^{10},\omega^{39}\},\{\omega^4,\omega^{35};\omega^{38},\omega^{25}\}\}\otimes\{1,\omega^8,\cdots,\omega^{32}\}.$

6. $a_0=5,\ a_1=33,\ a_2=13,\ a_3=9,\ c_0=2\ c_1=4.$
   i.e.$\{\{1,\omega^5;\omega^{18},\omega^{11}\},\{\omega^4,\omega^{17};\omega^{38},\omega^7\}\}\otimes\{1,\omega^8,\cdots,\omega^{32}\}.$

7. $a_0=5,\ a_1=33,\ a_2=13,\ a_3=9,\ c_0=4,\ c_1=1.$
   i.e.$\{\{1,\omega^5;\omega^{34},\omega^{27}\},\{\omega^4,\omega^{17};\omega^{14},\omega^{23}\}\}\otimes\{1,\omega^8,\cdots,\omega^{32}\}.$

8. $a_0 = 7,\ a_1 = 9,\ a_2 = 17,\ a_3 = 3,\ c_0 = 3,\ c_1 = 4.$
   i.e.$\{\{1, \omega^7; \omega^{26}, \omega^{35}\}, \{\omega^4, \omega^{21}; \omega^{38}, \omega^1\}\} \otimes \{1, \omega^8, \cdots, \omega^{32}\}.$

9. $a_0 = 7,\ a_1 = 17,\ a_2 = 17,\ a_3 = 3,\ c_0 = 0,\ c_1 = 4.$
   i.e.$\{\{1, \omega^7; \omega^2, \omega^{19}\}, \{\omega^4, \omega^{21}; \omega^{38}, \omega^1\}\} \otimes \{1, \omega^8, \cdots, \omega^{32}\}.$

10. $a_0 = 7,\ a_1 = 35,\ a_2 = 31,\ a_3 = 27,\ c_0 = 2,\ c_1 = 4.$
    i.e.$\{\{1, \omega^7; \omega^{18}, \omega^{13}\}, \{\omega^4, \omega^{35}; \omega^{38}, \omega^{25}\}\} \otimes \{1, \omega^8, \cdots, \omega^{32}\}.$

**Proposition 4.3.10** *Let $p = 8t + 1$ be a prime where $t > 1$ is odd and $\omega$ be a primitive root mod $p$. If $a_0, a_1, a_2, a_3, c_0$ and $c_1$ are integers such that*

1. $a_0, a_1 + 2, a_2 + 4, a_3 + 6 \pmod{8} \in \{1, 3, 5, 7\}$ *and are all distinct.*

2. $\frac{\omega^{a_1}-1}{\omega^{a_0}-1} = \omega^{b_1}, \frac{\omega^{a_2}-1}{\omega^{a_0}-1} = \omega^{b_2}, \frac{\omega^{a_3}-1}{\omega^{a_0}-1} = \omega^{b_3}$, *where* $b_1+1, b_2+2, b_3+3 \pmod{4} \in \{1, 2, 3\}$ *and are all distinct.*

3. $\omega^{8c_1+6} - 1 = \omega^{r_1}, \omega^{8c_1+6} - \omega^{a_0} = \omega^{r_2},\ \omega^{8c_1+6+a_3} - \omega^{a_0} = \omega^{r_3},\ \omega^{8c_1+6+a_3} - 1 = \omega^{r_4},\ \omega^{8c_0+4} - \omega^2 = \omega^{r_5},\ \omega^{8c_0+4} - \omega^{2+a_1} = \omega^{r_6},\ \omega^{8c_0+4+a_2} - \omega^{2+a_1} = \omega^{r_7},\ \omega^{8c_0+4+a_2} - \omega^2 = \omega^{r_8}$ *where* $\{r_i; i = 1, 2, \cdots 8\}$ *is partitioned into two disjoint sets* $\{r_{11}, r_{12}, r_{13}, r_{14}\} \cup \{r_{21}, r_{22}, r_{23}, r_{24}\}$ *such that* $r_{i1}, r_{i2} r_{i3}, r_{i4}$ *are incongruent* $\pmod{4}$ *for* $i = 1, 2$

*then the following table forms an initial round for a $Wh(p)$*

$$\{\{1, \omega^{a_0}; \omega^{8c_1+6}, \omega^{8c_1+6+a_3}\}, \{\omega^2, \omega^{2+a_1}; \omega^{8c_0+4}, \omega^{8c_0+4+a_2}\}\} \otimes \{1, \omega^8, \cdots, \omega^{8(t-1)}\}. \tag{4.3.8}$$

*Furthermore, if in (3) we restrict $r_1, r_3, r_5, r_4$ and $r_2, r_4, r_6, r_8$ are incongruent mod(4) respectively then the table (4.3.8) forms an initial for a $TWh(p)$*

**Example 4.3.6** $TWh(41)$ with $\omega = 26$

1. $a_0 = 5,\ a_1 = 9,\ a_2 = 11,\ a_3 = 27,\ c_0 = 1,\ c_1 = 2.$
   i.e.$\{\{1, \omega^5; \omega^{14}, \omega^1\}, \{\omega^2, \omega^{11}; \omega^{20}, \omega^{31}\}\} \otimes \{1, \omega^8, \cdots, \omega^{32}\}.$

2. $a_0 = 5,\ a_1 = 15,\ a_2 = 31,\ a_3 = 17,\ c_0 = 0,\ c_1 = 3.$
   i.e.$\{\{1, \omega^5; \omega^6, \omega^{23}\}, \{\omega^2, \omega^{17}; \omega^{28}, \omega^{19}\}\} \otimes \{1, \omega^8, \cdots, \omega^{32}\}.$

3. $a_0 = 5,\ a_1 = 17,\ a_2 = 11,\ a_3 = 27,\ c_0 = 0,\ c_1 = 3.$
   i.e.$\{\{1, \omega^5; \omega^6, \omega^{33}\}, \{\omega^2, \omega^{19}; \omega^{28}, \omega^{39}\}\} \otimes \{1, \omega^8, \cdots, \omega^{32}\}.$

4. $a_0 = 5,\ a_1 = 29,\ a_2 = 29,\ a_3 = 21,\ c_0 = 3,\ c_1 = 0.$
   i.e.$\{\{1, \omega^5; \omega^{30}, \omega^{11}\}, \{\omega^2, \omega^{31}; \omega^4, \omega^{33}\}\} \otimes \{1, \omega^8, \cdots, \omega^{32}\}.$

5. $a_0 = 5,\ a_1 = 29,\ a_2 = 31,\ a_3 = 27,\ c_0 = 1,\ c_1 = 2.$
   i.e.$\{\{1, \omega^5; \omega^{14}, \omega^1\}, \{\omega^2, \omega^{31}; \omega^{20}, \omega^{11}\}\} \otimes \{1, \omega^8, \cdots, \omega^{32}\}.$

6. $a_0 = 5,\ a_1 = 37,\ a_2 = 23,\ a_3 = 19,\ c_0 = 4,\ c_1 = 4.$
   i.e.$\{\{1, \omega^5; \omega^{38}, \omega^{17}\}, \{\omega^2, \omega^{39}; \omega^{36}, \omega^{19}\}\} \otimes \{1, \omega^8, \cdots, \omega^{32}\}.$

7. $a_0 = 5,\ a_1 = 37,\ a_2 = 23,\ a_3 = 35,\ c_0 = 3,\ c_1 = 4.$
   i.e.$\{\{1, \omega^5; \omega^{30}, \omega^{25}\}, \{\omega^2, \omega^{39}; \omega^{36}, \omega^{19}\}\} \otimes \{1, \omega^8, \cdots, \omega^{32}\}.$

8. $a_0 = 5,\ a_1 = 37,\ a_2 = 31,\ a_3 = 19,\ c_0 = 2,\ c_1 = 3.$
   i.e.$\{\{1, \omega^5; \omega^{22}, \omega^1\}, \{\omega^2, \omega^{39}; \omega^{28}, \omega^{19}\}\} \otimes \{1, \omega^8, \cdots, \omega^{32}\}.$

9. $a_0 = 5,\ a_1 = 37,\ a_2 = 39,\ a_3 = 19,\ c_0 = 0,\ c_1 = 2.$
   i.e.$\{\{1, \omega^5; \omega^6, \omega^{25}\}, \{\omega^2, \omega^{39}; \omega^{20}, \omega^{19}\}\} \otimes \{1, \omega^8, \cdots, \omega^{32}\}.$

10. $a_0 = 7,\ a_1 = 19,\ a_2 = 31,\ a_3 = 27,\ c_0 = 3,\ c_1 = 4.$
    i.e.$\{\{1, \omega^7; \omega^{30}, \omega^{17}\}, \{\omega^2, \omega^{21}; \omega^{36}, \omega^{27}\}\} \otimes \{1, \omega^8, \cdots, \omega^{32}\}.$

## 4.4 $TWh(p)$ where $p = 2^k t + 1,\ t > 1,\ k > 1$

Finally to deal with the general case, we give two examples of the constructions for $TWh(p)$ where $p = 2^k t + 1,\ t > 1,\ k > 1$ where $t$ is odd integer.

**Proposition 4.4.1** *Let $p = 2^k t + 1$ be a prime where $t > 1$ be odd, $k \geq 2$ integer, $d = 2^k$, $m = 2^{k-1}$, $n = 2^{k-2}$ and $\omega$ be a primitive root mod $p$. If $a_0, a_1, \cdots, a_{m-1}$ $c_0, c_1, \cdots, c_{n-1}$ are integers such that*

1. $a_i + i \pmod{d} \in \{m, m+1, \cdots, d-1\}$ *and are all distinct for* $i = 0, 1, \cdots, m-1$.
2. $\frac{\omega^{a_i} - 1}{\omega^{a_0} - 1} = \omega^{b_i}$, *where $b_i + i$ are incongruent mod $m$ for $i = 0, 1, \cdots, m-1$.*
3. $\omega^{dc_i + (2i+1)} - \omega^{2i} = \omega^{r_{4i+1}}, \omega^{dc_i+(2i+1)} - \omega^{2i+a_{2i}} = \omega^{r_{4i+2}}, \omega^{dc_i+(2i+1)+a_{2i+1}} - \omega^{2i+a_{2i}} = \omega^{r_{4i+3}}, \omega^{dc_i+(2i+1)+a_{2i+1}} - \omega^{2i} = \omega^{r_{4i+4}}$, *for $i = 0, 1, \cdots, n-1$ where $\{r_i; i = 1, 2, \cdots, d\}$ is partitioned into two disjoint sets $\{r_{1,j}; j =$*

*$1, 2, \cdots, m\} \cup \{r_{2,j}; j = 1, 2, \cdots, m\}$ such that $r_{i,j}; j = 1, 2, \cdots, m$ are incongruent $\pmod m$ for $i = 1, 2$ respectively.*

*then the following table forms an initial round for a $Wh(p)$*

$$\{\{1, \omega^{a_0}; \omega^{dc_0+1}, \omega^{dc_0+1+a_1}\}, \{\omega^2, \omega^{2+a_2}; \omega^{dc_1+3}, \omega^{dc_1+3+a_3}\}, \cdots, \\ \{\omega^{2n-2}, \omega^{2n-2+a_{2n-2}}; \omega^{dc_n+2n-1}, \omega^{dc_n+2n-1+a_{2n-1}}\}\} \otimes \{1, \omega^d, \cdots, \omega^{d(t-1)}\}. \tag{4.4.1}$$

*Furthermore, if in (3) the partition is restricted so that $\{r_i;\ i = 1, 2, \cdots, d\}$ $=\{r_{2i-1}; i = 1, 2, \cdots, m\} \cup \{r_{2i}; i = 1, 2, \cdots, m\}$ where, in both sets, the numbers are incongruent mod $(m)$, then the table (4.4.1) form an initial round for a $TWh(p)$*

In particular, if we choose $a_{2i} = \frac{p+1}{2} = mt + 1$, $a_{2i+1} = a_1$ and $c_i = 0$ for $i = 0, 1, \cdots, n-1$ then the games becomes

$$\{\{1, -\omega; \omega, \omega^{1+a_1}\}, \{\omega^2, -\omega^3; \omega^3, \omega^{3+a_1}\}, \cdots, \\ \{\omega^{2n-2}, -\omega^{2n-1}; \omega^{2n-1}, \omega^{2n-1+a_1}\} \otimes \{1, \omega^d, \cdots, \omega^{d(t-1)}\}$$

Since $a_{2i} + 2i = mt + 2i + 1$ are odd, this forces $a_{2i+1} + 2i + 1 = a_1 + 2i + 1$ to be even, so $a_1 \equiv m - 1 \pmod d$. Therefore there are $t$ candidates for $a_1$.

The partner differences are

$$(\omega + 1) \cdot \{\pm 1, \pm\omega^2, \cdots, \pm\omega^{2n-2}\} \otimes \{1, \omega^d, \cdots, \omega^{d(t-1)}\} \\ (\omega^{a_1} - 1) \cdot \{\pm\omega, \pm\omega^3, \cdots, \pm\omega^{2n-1}\} \otimes \{1, \omega^d, \cdots, \omega^{d(t-1)}\}$$

The opponent differences of 1st kind are

$$(\omega - 1) \cdot \{\pm 1, \pm\omega^2, \cdots, \pm\omega^{2n-2}\} \otimes \{1, \omega^d, \cdots, \omega^{d(t-1)}\} \\ (\omega^{a_1} + 1) \cdot \{\pm\omega, \pm\omega^3, \cdots, \pm\omega^{2n-1}\} \otimes \{1, \omega^d, \cdots, \omega^{d(t-1)}\}$$

The opponent differences of 2nd kind are

$$(2\omega) \cdot \{\pm 1, \pm\omega^2, \cdots, \pm\omega^{2n-2}\} \otimes \{1, \omega^d, \cdots, \omega^{d(t-1)}\} \\ (\omega^{a_1+1} - 1) \cdot \{\pm\omega, \pm\omega^3, \cdots, \pm\omega^{2n-1}\} \otimes \{1, \omega^d, \cdots, \omega^{d(t-1)}\}$$

Therefore a $TWh(p)$ exists provided that there exists $\omega$ and $a_1 \equiv 2^{k-1} - 1 \pmod d$ such that

$$(A) \qquad \begin{array}{rl} (i) & 2(\omega^{a_1+1} - 1) = \square \\ (ii) & (\omega + 1)(\omega^{a_1} - 1) = \square \\ (iii) & (\omega - 1)(\omega^{a_1} + 1) = \square \end{array}$$

**Remark:** 1. If $k = 3$ and $a_1 = 3$ then it is Corollary 4.3.2

2. If $k \geq 3$ then $(i)$ is replaced by $\omega^{a_1+1} - 1 = \square$, since $2 = \square$.

**Example 4.4.1** We list some examples of $p$,$a_1$ and $\omega$ which satisfy the above three conditions in (A); where * denotes $a_1 \neq 2^{k-1} - 1$ but $a_1 \equiv 2^{k-1} - 1 \pmod{d}$.

$$\begin{array}{llll}
(p, a_1, \omega) = & (41, no) & (73, *11, 31) & (89, 3, 6) \\
(97, *79, 5) & (113, 7, 21) & (137, 3, 5) & (193, 31, 5) \\
(241, 7, 7) & (337, *199, 10) & (353, 15, 3) & (401, 7, 3) \\
(433, 7, 7) & (449, 31, 17) & (457, 3, 52) & (521, 3, 85) \\
(577, 31, 21) & (593, 7, 41) & (641, no) & (673, 15, 11) \\
(769, 127, 14) & (881, 79, 14) & (927, 15, 35) & (977, 7, 24) \\
(1009, 7, 11) & (1153, 63, 76) & (1201, 7, 71) & (1217, 31, 3) \\
(1249, 271, 7) & (1297, 7, 15) & (1361, 7, 3) & (1409, 63, 27) \\
(1489, 7, 21) & (1553, 7, 5) & (1601, 31, 853) & (1697, 15, 13) \\
(1777, 7, 20) & (1873, 7, 10) & (1889, 15, 6) & (2017, 15, 19) \\
(2081, 15, 6) & (2113, 31, 5) & (2129, 7, 75) & (2161, 7, 53) \\
(2273, 15, 5) & (2417, 7, 6) & (2593, 15, 7) & (2609, 7, 27) \\
(2657, 15, 17) & (2687, 63, 39) & (2753, 31, 10) & (2801, 7, 13) \\
(2833, 7, 51) & (2897, 7, 13) & (3041, 15, 46) & (3089, 7, 15) \\
(3121, 7, 7) & (3137, 31, 62) & (3217, 7, 23) & (3313, 7, 85) \\
(3329, 127, 22) & (3361, 15, 119) & (3617, 15, 12) & (3697, 7, 5) \\
(3761, 7, 22) & (3793, 7, 7) & (3889, 7, 38) & (4001, 15, 17) \\
(4129, 15, 53) & (4177, 7, 31) & (4241, 7, 28) & (4273, 7, 97) \\
(4289, 31, 6) & (4337, 7, 21) & (4481, 63, 3) & (4513, 15, 82) \\
(4561, 7, 67) & (4657, 7, 30) & (4673, 31, 3) & (4721, 7, 6) \\
(4801, 31, 71) & (4817, 7, 29) & (4993, 63, 35) & (5009, 343, 3) \\
(5081, 59, 3) & (5113, 75, 19) & (5153, 79, 5) & (5209, 59, 17) \\
(5233, 119, 10) & (5273, 27, 3) & (5281, 175, 5) & (5297, 23, 3) \\
(5393, 87, 3) & (5417, 67, 3) & (5441, 95, 3) & (5449, 43, 7) \\
(5521, 359, 11) & (5569, 1695, 13) & (5641, 67, 14) & (5657, 11, 3) \\
(5689, 3, 11) & (5737, 3, 5) & (5801, 139, 10) & (5849, 3, 3) \\
(5857, 47, 7) & (5881, 139, 31) & (5897, 123, 3) & (5953, 95, 7) \\
(6073, 59, 17) & (6089, 83, 3) & (6113, 47, 3) & (6121, 43, 7) \\
(6217, 43, 5) & (6257, 39, 3) & (6329, 99, 3) & (6337, 287, 10) \\
(6353, 135, 3) & (6361, 59, 19) & (6449, 55, 3) & (6473, 11, 3) \\
(6481, 135, 7) & (6521, 43, 6) & (6529, 63, 7) & (6553, 115, 10) \\
(6569, 75, 3) & (6577, 23, 5) & (6673, 39, 5) & (6689, 79, 3)
\end{array}$$

We have extended this list by computer up to $p = 160997$.

**Proposition 4.4.2** *Let $p = 2^k t + 1$ be a prime where $t > 1$ odd, $k \geq 2$ integer, $d = 2^k$, $m = 2^{k-1}$, $n = 2^{k-2}$ and $\omega$ be a primitive root mod $p$. If $a_0, a_1, \cdots, a_{m-1}$, $c_0, c_1, \cdots, c_{n-1}$ are integers such that*

1. *$a_i + 2i \pmod d \in \{1, 3, \cdots, d-1\}$ and are all distinct for $i = 0, 1, \cdots, m-1$.*

2. *$\frac{\omega^{a_i}-1}{\omega^{a_0}-1} = \omega^{b_i}$, where $b_i + 2i \not\equiv 0 \pmod m$ and are all distinct for $i = 1, 2, \cdots, m-1$.*

3. *$\omega^{dc_i+m+2i} - \omega^{2i} = \omega^{r_{4i+1}}$, $\omega^{dc_i+m+2i+a_{n+i}} - \omega^{2i+a_i} = \omega^{r_{4i+3}}$, $\omega^{dc_i+m+2i} - \omega^{2i+a_i} = \omega^{r_{4i+2}}$, $\omega^{dc_i+m+2i+a_{n+i})} - \omega^{2i} = \omega^{r_{4i+4}}$, for $i = 0, 1, \cdots, n-1$ where $\{r_i; i = 1, 2, \cdots, d\}$ is partitioned into two disjoint sets $\{r_{1,j}; j = 1, 2, \cdots, m\} \cup \{r_{2,j}; j = 1, 2, \cdots, m\}$ such that the $r_{i,j}$; $j = 1, 2, \cdots, m$ are incongruent $\pmod m$ for $i = 1, 2$ respectively.*

*then the following table forms an initial round for a $Wh(p)$*

$$\{\{\omega^{2i}, \omega^{2i+a_i}; \omega^{dc_i+m+2i}, \omega^{dc_i+m+2i+a_{n+i}}\}\} \otimes \{1, \omega^d, \cdots, \omega^{d(t-1)}\}. \tag{4.4.2}$$

*where $i = 0, 1, \cdots, n-1$.*

*Furthermore, if in (3) the partition is restricted so that*

$$\{r_i; i = 1, 2, \cdots, d\} = \{r_{2i-1}; i = 1, 2, \cdots, m\} \cup \{r_{2i}; i = 1, 2, \cdots, m\}$$

*where, in both sets, the numbers are incongruent (mod d), then the table (4.4.2) form an initial round for a $TWh(p)$*

In particular, if we choose $a_{n+i} = \frac{p+1}{2}$, $a_i = a_0$, for $i = 0, 1, \cdots, n-1$ then since $\omega^{m+2i+a_{n+i}} = \omega^{m+2i+mt+1} = -\omega^{m+2i+1}$, the games become

$$\{\{\omega^{2i}, \omega^{2i+a_0}; \omega^{m+2i}, -\omega^{m+2i+1}\}; i = 0, 1, \cdots, n-1\}\} \otimes \{1, \omega^d, \cdots, \omega^{d(t-1)}\}$$

Furthermore,since $a_{n+i} + 2(n+i) = 2^{k-1}t + 1 + 2n + 2i \equiv 2i + 1 \pmod d$ for $i = 0.1, \cdots, n-1$. Condition (1) forces $a_i + 2i \pmod d \in \{m+1, m+2, \cdots, d-1\}$ for $i = 0, 1, \cdots, n-1$. Thus $a_0 = a_i$ $i = 1, 2, \cdots, n-1$ implies $a_0 \equiv m + 1 \pmod d$.

The partner differences are

$$\begin{array}{l} (\omega^{a_0} - 1) \cdot \{1, \omega^2, \cdots, \omega^{2n-2}\} \otimes \{\pm 1, \pm\omega^d, \cdots, \pm\omega^{d(t-1)}\} \\ (\omega + 1)\omega^m \cdot \{1, \omega^2, \cdots, \omega^{2(n-2)}\} \otimes \{\pm 1, \pm\omega^d, \cdots, \pm\omega^{d(t-1)}\} \end{array}$$

So we need $(\omega^{a_0} - 1)(\omega + 1) \neq \Box$.

The opponent differences of 1st kind are

$$\begin{array}{l}(\omega^m - 1)\cdot\{1,\omega^2,\cdots,\omega^{2n-2}\}\otimes\{\pm 1,\pm\omega^d,\cdots,\pm\omega^{d(t-1)}\}\\(\omega^{m+1} + \omega^{a_0})\cdot\{1,\omega^2,\cdots,\omega^{2n-2}\}\otimes\{\pm 1,\pm\omega^d,\cdots,\pm\omega^{d(t-1)}\}\end{array}$$

So we need $(\omega^m - 1)(\omega^{a_0} + \omega^{m+1}) \neq \square$.

The opponent differences of 2nd kind are

$$\begin{array}{l}(\omega^{m+1} + 1)\cdot\{1,\omega^2,\cdots,\omega^{2n-2}\}\otimes\{\pm 1,\pm\omega^d,\cdots,\pm\omega^{d(t-1)}\}\\(\omega^{a_0} - \omega^m)\cdot\{1,\omega^2,\cdots,\omega^{2n-2}\}\}\otimes\{\pm 1,\pm\omega^d,\cdots,\pm\omega^{d(t-1)}\}\end{array}$$

So we need $(\omega^{m+1} + 1)(\omega^{a_0} - \omega^m) \neq \square$

Therefore a $TWh(p)$ exists provided that there exists $\omega$ and $a_0 \equiv 2^{k-1} + 1 \pmod{2^k}$ such that

$$(B) \qquad \begin{array}{ll}(i) & (\omega + 1)(\omega^{a_0} - 1) \neq \square\\(ii) & (\omega^{2^{k-1}} - 1)(\omega^{a_0} + \omega^{2^{k-1}+1}) \neq \square\\(iii & )(\omega^{2^{k-1}+1} + 1)(\omega^{a_0} - \omega^{2^{k-1}}) \neq \square\end{array}$$

**Example 4.4.2** We list some examples of $p$, $a_0$ and $\omega$ which satisfy the three conditions in $B$:

$(p, a_1, \omega) =$ $(41, *13, 6)$, $(73, 5, 31)$, $(89, *13, 14)$, $(97, 17, 5)$,
$(113, 9, 29)$, $(137, *13, 5)$, $(193, 33, 5)$, $(241, 9, 7)$, $(337, 9, 19)$,
$(353, 17, 3)$, $(401, 9, 17)$, $(433, 9, 7)$, $(449, 33, 6)$, $(457, *13, 15)$,
$(521, 5, 28)$, $(577, 33, 45)$, $(593, 9, 5)$, $(641, *193, 12)$, $(673, 17, 30)$,
$(769, 129, 42)$, $(881, 9, 3)$, $(927, 17, 13)$, $(977, 9, 13)$, $(1009, 9, 11)$,
$(1153, 65, 166)$, $(1201, 9, 37)$, $(1217, 33, 7)$, $(1249, 17, 33)$, $(1297, 9, 62)$,
$(1361, 9, 16)$, $(1409, 65, 67)$, $(1489, 9, 52)$, $(1553, 9, 6)$, $(1601, 33, 14)$,
$(1697, 17, 7)$, $(1777, 9, 33)$, $(1873, 9, 10)$, $(1889, 17, 67)$, $(2017, 17, 35)$,
$(2081, 17, 6)$, $(2113, 33, 55)$, $(2129, 9, 24)$, $(2161, 9, 38)$, $(2273, 17, 14)$,
$(2417, 9, 10)$, $(2593, 17, 45)$, $(2609, 9, 12)$, $(2657, 17, 17)$, $(2687, 65, 57)$,
$(2753, 33, 5)$, $(2801, 9, 12)$, $(2833, 9, 10)$, $(2897, 9, 3)$, $(3041, 17, 46)$,
$(3089, 9, 26)$, $(3121, 9, 17)$, $(3137, 33, 19)$, $(3217, 9, 69)$, $(3313, 9, 30)$,
$(3329, 129, 12)$, $(3361, 17, 86)$, $(3617, 17, 5)$, $(3697, 9, 5)$, $(3761, 9, 6)$,
$(3793, 9, 31)$, $(3889, 9, 33)$, $(4001, 17, 22)$, $(4129, 17, 65)$, $(4177, 9, 31)$,
$(4241, 9, 39)$, $(4273, 9, 68)$, $(4289, 33, 7)$, $(4337, 9, 21)$, $(4481, 65, 17)$,
$(4513, 17, 29)$, $(4561, 9, 85)$, $(4657, 9, 41)$, $(4673, 33, 5)$, $(4721, 9, 54)$,
$(4801, 33, 19)$, $(4817, 9, 11)$, $(4993, 65, 19)$.

## 4.5 Composition theorem for $TWh(4n+1)$

In this section we show how to construct some $TWh(4n+1)$ where $4n+1$ is a composite integer.

**Theorem 4.5.1** *Let $p = 2^m t + 1$ be a prime where $t$ is odd. Suppose that a Z-cyclic $TWh(p)$ exists. Then a Z-cyclic $TWh(p^n)$ exists for any positive integer $n \geq 2$*

**proof.** We prove it by induction. Let $\omega$ be a primitive root mod $p^2$ then it is a primitive root mod $p^n$ for all $n$. Suppose that a Z-cyclic $TWh(p)$ exists with an initial round games

$$\{\{\omega^{a_j},\ \omega^{b_j};\ \omega^{c_j},\ \omega^{d_j}\};\ j = 1, 2, \cdots, 2^{m-2}t\}$$

where $a_j,\ b_j,\ c_j,\ d_j \quad j = 1, 2, \cdots, 2^{m-2}t$ are incongruent mod $(p-1)$. Suppose that a Z-cyclic $TWh(p^{n-1})$ exists with initial round games $I(p^{n-1})$. We decompose $Z_{p^n}$ as follows

$$Z_{p^n} = P \cup E \cup \{0\}$$

where $P = \{x \in Z_{p^n}; p \mid x, x \neq 0\}$, $E = \{x \in Z_{p^n}; p \nmid x\}$. Then $|P| = p^{n-1} - 1$ and $|E| = \phi(p^n) = 2^m t p^{n-1} = 2^m u$, say.

Observe that $E$ can be written as a cyclic set

$$E = \{1,\ \omega,\ \omega^2, \cdots, \omega^{2^m u - 1}\}.$$

Let $E$ be decomposed as $E_1 \cup E_2 \cup E_3, \cdots, E_{p^{n-1}}$ where

$$\begin{array}{ll}
E_1 & = \{1, \omega, \omega^2, \cdots, \omega^{p-2}\} \\
E_2 & = \{\omega^{p-1}, \omega^p, \omega^{p+1}, \cdots, \omega^{2p-3}\} = \omega^{p-1}E_1 \\
E_3 & = \{\omega^{2(p-1)}, \omega^{2(p-1)+1}, \omega^{2(p-1)+2}, \cdots, \omega^{3(p-1)-1}\} = \omega^{2(p-1)}E_1 \\
 & \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
E_{p^{n-1}} & = \{\omega^{(p^{n-1}-1)(p-1)}, \omega^{(p^{n-1}-1)(p-1)+1}, \cdots, \omega^{p^{n-1}(p-1)-1}\} = \omega^{(p^{n-1}-1)(p-1)}E_1.
\end{array}$$

If each $E_j \quad (j = 1, 2, \cdots, p^{n-1})$ is considered as mod $p$, it is in fact the power sequence $1,\ \omega,\ \omega^2, \cdots, \omega^{p-2} \pmod{p}$. We claim that the games

$$(A) \quad \{\{\omega^{a_j}, \omega^{b_j}; \omega^{c_j}, \omega^{d_j}\};\ j = 1, 2, \cdots\ 2^{m-2}t\} \otimes \{1, \omega^{p-1}, \cdots, \omega^{(p^{n-1}-1)(p-1)}\}$$

satisfy the conditions to be an initial round for a Z-cyclic $TWh(p^n)$ on $E$.

Since $\{\{\omega^{a_j},\omega^{b_j};\omega^{c_j},\omega^{d_j}\};\ j=1,2,\cdots\ 2^{m-2}t\}$ are games of an initial round for a $TWh(p)$ so

1. $a_j,\ b_j,\ c_j,\ d_j\quad (j=1,2,\cdots,2^{m-2}t)$ are incongruent mod $(p-1)$.
2. the partner (resp. 1st, 2nd opponent) differences arising from $\{\{\omega^{a_j},\omega^{b_j};\omega^{c_j},\omega^{d_j}\};\ j=1,2,\cdots\ 2^{m-2}t\}$ occupy incongruent positions mod $(p-1)$.

It follows that

1. the elements in (A) are the elements of $E$ each occurring exactly once,
2. the partner(resp. 1st, 2nd opponent) differences arising from $\omega^{j(p-1)}E_1$ $j=1,2,\cdots,p^{n-1}$, occupy incongruent positions mod $p^{n-1}(p-1)$.

Therefore the partner and triple-whist tournament conditions are satisfied, and for an initial round of a $TWh(p^n)$ we take games in (A) union $p\cdot IR(p^{n-1})$.

**Examples 4.5.1**

(a) If $p=29,\ \omega=19$ then as showed in Example 4.2.1.(a).(1) the following games form an initial round for a $TWh(29)$,

$$\{1,\omega^2;\ \omega,\omega^7\}\otimes\{1,\omega^4,\cdots,\omega^{24}\}$$

and $\omega=19$ is also a primitive root mod $29^2$, Therefore

$$29\cdot\{\{1,\omega^2;\ \omega,\omega^7\}\otimes\{1,\omega^4,\cdots,\omega^{24}\}\quad(\text{mod } 29)\}\cup$$
$$\{\{1,\omega^2;\ \omega,\omega^7\}\otimes\{1,\omega^4,\cdots,\omega^{808}\}\quad(\text{mod } 841)\}$$

is an initial round for a $TWh(841)$.

(b) If $p=41,\ \omega=26$ then as shown in Example 4.3.1.(a).(1) the following games form an initial round for a $TWh(41)$,

$$\{\{\{1,\omega^4;\omega,\omega^6\},\{\omega^2,\omega^{13};\omega^{19},\omega^7\}\}\otimes\{1,\omega^8,\cdots,\omega^{32}\}$$

and $\omega=26$ is a primitive root (mod 1681) also. Therefore

$$41\cdot\{\{\{1,\omega^4;\omega,\omega^6\},\{\omega^2,\omega^{13};\omega^{19},\omega^7\}\}\otimes\{1,\omega^8,\cdots,\omega^{32}\}\quad(\text{mod } 41)\}$$
$$\cup\{\{\{1,\omega^4;\omega,\omega^6\},\{\omega^2,\omega^{13};\omega^{19},\omega^7\}\}\otimes\{1,\omega^8,\cdots,\omega^{1632}\}\quad(\text{mod } 1681)\}$$

is an initial round for a $TWh(1681)$.

**Lemma 4.5.2** *Let* $p = 2^{m_1}t_1 + 1$, $q = 2^{m_2}t_2 + 1$ *be primes where* $t_1$, $t_2$ *are odd integers,* $m_1$, $m_2$ *are integers* $\geq 1$. *Let* $v = p^{n_1}q^{n_2}$ *where* $n_1$, $n_2$ *are integers,* $\omega$ *be a primitive root of both* $p^2$ *and* $q^2$, *g.c.d* $\{p^{n_1-1}(p-1),\ q^{n_2-1}(q-1)\} = 2e$ *and* $p^{n_1-1}(p-1)q^{n_2-1}(q-1) = 2de$. *Then there exists an integer* $x \equiv 1 \pmod p$ *such that*

1. *the* $2de$ *integers* $\omega^s x^i \quad (s = 0, 1, \cdots, d-1; i = 0, 1, \cdots, 2e-1)$ *constitute a reduced residue system mod* $(v)$ .
2. $x^{2e} \equiv \omega^u \pmod v$ *for some integer* $u \quad 0 \leq u \leq d-1$ *and* $2^{m_1}t_1 \mid u$.
3. *If* $m_1 = m_2$ *then* $\omega^{\frac{d}{2}} \equiv -1 \pmod v$.
4. *If* $m_1 \neq m_2$ *then* $x^e \equiv -\omega^k \pmod v$ *where* $k$ *is even and* $\omega^s \not\equiv -1 \pmod v$ *for all* $s$.
5. *If* $m_1 \neq m_2$ *and* $m_2 = 1$ *then we may choose* $y$ *such that* $y^e \equiv -\omega^h \pmod v$ *where* $h$ *is odd.*

**Proof** Let $x$, $y$ be a pair of integers satisfying the simultaneous congruences

$$(A) \qquad \left\{\begin{array}{ll} x & \equiv 1 \pmod{p^{n_1}} \\ x & \equiv \omega \pmod{q^{n_2}} \end{array}\right. \qquad \left\{\begin{array}{ll} y & \equiv \omega \pmod{p^{n_1}} \\ y & \equiv 1 \pmod{q^{n_2}} \end{array}\right.$$

That integers $x$, $y$ exist is assured by the Chinese Remainder Theorem.

Since $p$ and $q$ are primes, we have $xy \equiv \omega \pmod{pq}$. Since $\omega$ is a common primitive root of $p^2$ and $q^2$, so it is of $p^{n_1}$ and $q^{n_2}$. The order of $\omega \pmod v$ is l.c.m $\{p^{n_1-1}(p-1), q^{n_2-1}(q-1)\} = d$. We shall prove that the integers $x$, $y$ defined by (A) satisfy the assertion. For this purpose we first show that no power $\omega^s \quad (s = 0, 1, \cdots, d-1)$ of $\omega$ is congruent modulo $v$ to a power $x^i \quad i = 0, 1, \cdots, 2e-1$ of $x$ except $s = i = 0$. Suppose that $\omega^s \equiv x^i \pmod v$ then $\omega^s \equiv x^i \pmod{p^{n_1}}$, and $\omega^s \equiv x^i \pmod{q^{n_2}}$. Thus $\omega^s \equiv 1 \pmod{p^{n_1}}$ and $\omega^s \equiv \omega^i \pmod{q^{n_2}}$; so $p^{n_1-1}(p-1) \mid s$ and $q^{n_2-1}(q-1) \mid s-i$. Hence $2e \mid i$ and so $i \geq 2e$ unless $i = 0$ which implies $\omega^s \equiv 1 \pmod v$. Thus $s = 0$. It follows that $\omega^s x^i \equiv \omega^t x^j \pmod v \quad (s, t = 0, 1. \cdots, d-1; i,\ j = 0, 1, \cdots, 2e-1)$ is not possible unless $s = t$ and $i = j$. Therefore the proof of (1) is complete.

For the proof (2), since g.c.d $\{x^{2e}, v\} = 1$, so $x^{2e} \equiv \omega^u x^i \pmod v$ for some $0 \leq i \leq 2e-1$ and $0 \leq u \leq d-1$. If $i > 0$ then $x^{2e-i} \equiv \omega^u \pmod v$ a contradiction, so $x^{2e} \equiv \omega^u \pmod v$, and since $x \equiv 1 \pmod p$ so $x^{2e} \equiv \omega^u \pmod v$ implies $1 \equiv \omega^u \pmod p$, it follows that $2^{m}{}_1t_1 = p-1 \mid u$. Similarly, for $y^{2e} \equiv \omega^u \pmod v$.

If $m_1 = m_2$ then since $\omega$ is a common primitive root of $p^2$ and $q^2$ so it is of $p^{n_1}$ and $q^{n_2}$. Therefore

$$\omega^{p^{n_1-1}(p-1)} = 1 \pmod{p^{n_1}} \qquad \text{and} \qquad \omega^{\frac{p^{n_1-1}(p-1)}{2}} = -1 \pmod{p^{n_1}}$$

$$\omega^{q^{n_2-1}(q-1)} = 1 \pmod{q^{n_2}} \qquad \text{and} \qquad \omega^{\frac{q^{n_2-1}(q-1)}{2}} = -1 \pmod{q^{n_2}}$$

Thus for any integer $k_1,\ k_2$ we have

$$\omega^{k_1 p^{n_1-1}(p-1)} = p^{n_1}c_1 + 1 \qquad \text{and} \qquad \omega^{k_2 q^{n_2-1}(q-1)} = q^{n_2}d_1 + 1 \qquad \text{for some } c_1,\ d_1.$$

In particular, we take

$$k_1 = \frac{\frac{q^{n_2-1}(q-1)}{2e} - 1}{2} \qquad \text{and} \qquad k_2 = \frac{\frac{p^{n_1-1}(p-1)}{2e} - 1}{2}$$

where $k_1$ and $k_2$ are integers, since $m_1 = m_2$. We have

$$\omega^{(\frac{\frac{q^{n_2-1}(q-1)}{2e}-1}{2})p^{n_1-1}(p-1)} = p^{n_1}c_1 + 1 \quad \text{and} \quad \omega^{(\frac{\frac{p^{n_1-1}(p-1)}{2e}-1}{2})k_2 q^{n_2-1}(q-1)} = q^{n_2}d_1 + 1$$

for some integers $c_1,\ d_1$.

*i.e.* $\omega^{\frac{d}{2}-\frac{p^{n_1-1}(p-1)}{2}} = p^{n_1}c_1 + 1$ and $\omega^{\frac{d}{2}-\frac{q^{n_2-1}(q-1)}{2}} = q^{n_2}d_1 + 1$ for some $c_1,\ d_1$

But

$$\omega^{\frac{p^{n_1-1}(p-1)}{2}} = p^{n_1}c_2 - 1 \quad \text{and} \quad \omega^{\frac{q^{n_2-1}(q-1)}{2}} = q^{n_2}d_2 - 1 \quad \text{for some } c_2,\ d_2.$$

It follows that $\omega^{\frac{d}{2}} + 1 = p^{n_1}c_3$ and $\omega^{\frac{d}{2}} + 1 = q^{n_2}d_3$ and since $p,\ q$ are coprime. Therefore, $\omega^{\frac{d}{2}} \equiv -1 \pmod v$.

If $m_1 \neq m_2$ then we claim that $x^e \equiv -\omega^k \pmod v$ where $k$ is even. Let us put $p^{n_1-1}(p-1) = 2ef$, $q^{n_2-1}(q-1) = 2ef'$ then $d = 2eff'$. Since $m_1 \neq m_2$ , $ff'$ is even and *g.c.d* $\{f,\ f'\} = 1$. Without loss of generality, suppose that $m_1 > m_2$ then $f$ is even and $f'$ is odd. Set $f = 2^\ell f_1$, where $f_1 \geq 1$ is odd. Then $p^{n_1-1}(p-1) = 2^{\ell+1}ef_1$ where $f_1$ is odd. First we show there is no $s$ such that $\omega^s \equiv -1 \pmod{v}$. On the contrary , suppose that there exists $s$ such that $\omega^s \equiv -1 \pmod{v}$; then $\omega^s \equiv -1 \pmod{p^{n_1}}$ and $\omega^s \equiv -1 \pmod{q^{n_2}}$. But $\omega^{\frac{p^{n_1-1}(p-1)}{2}} \equiv -1 \pmod{p^{n_1}}$ and $\omega^{\frac{q^{n_2-1}(q-1)}{2}} \equiv -1 \pmod{q^{n_2}}$ so

$$s \equiv \frac{p^{n_1-1}(p-1)}{2} \pmod{p^{n_1-1}(p-1)} \text{ and } s \equiv \frac{q^{n_2-1}(q-1)}{2} \pmod{q^{n_2-1}(q-1)}$$

$$i.e. \quad s = mp^{n_1-1}(p-1) + \frac{p^{n_1-1}(p-1)}{2} = nq^{n_2-1}(q-1) + \frac{q^{n_2-1}(q-1)}{2}$$

so

$$2^\ell f_1(2m+1) = f'(2n+1)$$

This is impossible since $\ell \geq 1$ and $f_1,\ f',\ 2m+1,\ 2n+1$ are odd. There are no value of $s$ such that $-1 \equiv \omega^s \pmod{v}$. We therefore put $-1 \equiv \omega^s x^i \pmod{v}$ with $0 < i \leq 2e-1,\ 0 \leq s \leq d-1$. Squaring both members of this congruence we have

$$1 \equiv \omega^{2s} x^{2i} \pmod{v}$$

Since $\omega^d \equiv 1 \pmod{v}$ so $1 \equiv \omega^{s_1} x^{2i}$ where $0 \leq s_1 \leq d-1$ and $0 < i \leq 2e-1$. If $0 < i < e$ then $1 \equiv \omega^{s_1} x^{2i}$ where $0 \leq s_1 \leq d-1$ and $0 < 2i < 2e$. This implies $s = 0$ and $i = 0$, a contradiction. If $e < i < 2e$ then $2e < 2i < 4e$. Since $x^{2e} \equiv \omega^{u_1} \pmod{v}$, where $0 \leq u_1 \leq d-1$, thus $1 \equiv \omega^{s_1+u_1} x^{2i-2e} \pmod{v}$ where $0 < 2i-2e < 2e,\ 0 \leq s_1 \leq d-1,\ 0 \leq u_1 \leq d-1$. If $0 \leq s_1+u_1 \leq d-1$ then $2i-2e = 0$ implies $i = e < i$ , a contradiction. If $d \leq s_1+u_1 \leq 2d-2$ then $1 \equiv \omega^{s_1+u_1} x^{2i-2e} \pmod{v}$ implies $1 \equiv \omega^{s_1+u_1-d} x^{2i-2e} \pmod{v}$ which implies $2i-2e = 0$ and $i = e < i$ a contradiction. Therefore the two assumptions $0 < i < e$ and $e < i < 2e$ both lead to contradictions. The only remainding possiblity is $e = i$, so $-1 \equiv \omega^{s_1} x^e \pmod{v}$ where $0 \leq s_1 \leq d-1$. Thus $x^e \equiv -\omega^{-s_1} \pmod{v} \equiv -\omega^k \pmod{v}$ where $0 \leq k \leq d-1$. Similarly, $y^e \equiv -\omega^h \pmod{v}$.

By definition of $x$ we have $x \equiv 1 \pmod{p}$ so $-x^e \equiv -1 \equiv \omega^{\frac{p-1}{2}} \pmod{p}$. But $x^e \equiv -\omega^k \pmod{v}$ implies $-x^e \equiv \omega^k \pmod{p}$. Thus $\omega^k \equiv \omega^{\frac{p-1}{2}} \pmod{p}$, Therefore $k \equiv \frac{p-1}{2} \pmod{(p-1)}$ which is even since $m_1 > m_2 \geq 1$.

Finally, by the same argument we have $h \equiv \frac{q-1}{2} \pmod{q-1}$, so if $m_2 = 1$ then $\frac{q-1}{2} = t_2$ which is odd, therefore $h$ is odd.

**Lemma 4.5.3** *Let* $p_1 = 2^{m_1}t_1 + 1$, $p_2 = 2^{m_2}t_2 + 1$ *be primes where* $m_1, m_2 \geq 2$, $m_1 \neq m_2$ *are positive integers,* $t_1$, $t_2$ *are odd integers. Then there exist games which satisfy the Z-cyclic triple whist tournament conditions on the reduced residue system mod* $v$ *where* $v = p_1^{\alpha_1}p_2^{\alpha_2}$ *for any positive integers* $\alpha_1$, $\alpha_2$.

**Proof.** Let $\omega$ be a common primitive root $\pmod{p_1^2}$ and $\pmod{p_2^2}$; then it is a primitive root $\pmod{p_1^{\alpha_1}}$ and $\pmod{p_2^{\alpha_2}}$. Assume that $m_1 > m_2$ and $g.c.d\{p_1^{\alpha_1-1}(p_1-1),\ p_2^{\alpha_2-1}(p_2-1)\} = 2^{m_2}e$ where $e$ is an odd integer and $l.c.m\{p_1^{\alpha_1-1}(p_1-1), p_2^{\alpha_2-1}(p_2-1)\} = \ell$; then $p_1^{\alpha_1-1}(p_1-1)p_2^{\alpha_2-1}(p_2-1) = 2^{m_2}e\ell$. Therefore by Lemma 4.5.2 there exists an integer $x \equiv 1 \pmod{p_1}$ such that

1. the $2^{m_2}e\ell$ integers $\omega^s x^i$ $(s = 0, 1, \cdots, \ell-1; i = 0, 1, \cdots, 2^{m_2}e-1)$ constitute the reduced residue system $\pmod{v}$.
2. $x^{2^{m_2}e} \equiv \omega^u \pmod{v}$ for some even $u$, $0 \leq u \leq \ell - 1$.
3. $x^{2^{m_2-1}e} \equiv -\omega^k \pmod{v}$ for some even $k$, $0 \leq k \leq \ell - 1$.
4. $\omega^s \not\equiv -1 \pmod{v}$ for any $s$.

Let $H = \{\omega^s; 0 \leq s \leq \ell - 1\}$. Then the $2^{m_2}e\ell$ integers of the reduced residue system mod $v$ are partitioned into pairwise disjoint sets $H$, $xH, \cdots x^{2^{m_2}e-1}H$ and since $x^{2^{m_2-1}e} = -\omega^k \pmod{v}$, so $x^{2^{m_2-1}e}H = -H$, $x^{2^{m_2-1}e+1}H = -xH, \cdots$, $x^{2^{m_2}e-1}H = -x^{2^{m_2-1}e}H$.

Take games

$$(A) \qquad x^i\{1, \omega; -\omega, -\omega^2\} \otimes \{1, \omega^2, \cdots, \omega^{\ell-2}\} \qquad i = 0, 1, \cdots, 2^{m_2-1}e - 1.$$

The partner differences are

$$\{\pm x^i(\omega - 1), \pm x^i(\omega^2 - \omega)\} \otimes \{1, \omega^2, \cdots, \omega^{\ell-2}\} \qquad i = 0, 1, \cdots, 2^{m_2-1}e - 1.$$

$$i.e. \qquad (\omega - 1)(\pm x^i) \cdot \{1, \omega, \cdots, \omega^{\ell-1}\} \qquad i = 0, 1, \cdots, 2^{m_2-1}e - 1.$$

The opponent differences of the 1st kind are

$$\{\pm x^i(\omega + 1), \pm x^i(\omega^2 + \omega)\} \otimes \{1, \omega^2, \cdots, \omega^{\ell-2}\} \qquad i = 0, 1, \cdots, 2^{m_2-1}e - 1.$$

$$i.e. \qquad (\omega + 1)(\pm x^i) \cdot \{1, \omega, \cdots, \omega^{\ell-1}\} \qquad i = 0, 1, \cdots, 2^{m_2-1}e - 1.$$

In both cases, the differences give the elements of the reduced residue system mod $v$ exactly once.

The opponent differences of the 2nd kind are

$$\{\pm 2x^i\omega, \pm x^i(\omega^2+1)\} \otimes \{1, \omega^2, \cdots, \omega^{\ell-2}\} \qquad i = 0, 1, \cdots, 2^{m_2-1}e-1.$$

Suppose that $\frac{\omega^2+1}{2} \in x^j H$ then $\frac{\omega^2+1}{2} = x^{j_0}\omega^b$ or $-x^{j_0}\omega^b$ for some $0 \leq b \leq \ell - 1$ and $0 \leq j_0 \leq 2^{m_2-1}e-1$, Thus if we choose $\omega$ so that $\frac{\omega^2+1}{2} \equiv \omega^a \pmod{p_1}$ where $a$ is even then $b$ is also even. (Such a $\omega$ exists by Cohen's lemma.)

The opponent differences of 2nd kind are

$$\{\pm 2\omega x^i, \pm 2x^{j_0+i}\omega^b\} \otimes \{1, \omega^2, \cdots \omega^{\ell-2}\} \qquad i = 0, 1, \cdots, 2^{m_2-1}e-1.$$

$$i.e. \quad (\pm 2x^i) \cdot \{\omega, \omega^3, \cdots, \omega^{\ell-1}\} \cup (\pm 2x^{j_0+i}) \cdot \{\omega^b, \omega^{b+2}, \cdots, \omega^{b+\ell-2}\}$$
$$i = 0, 1, \cdots, 2^{m_2-1}e-1.$$

Since $b$ is even so they are

$$(\pm 2x^i) \cdot \{\omega, \omega^3, \cdots, \omega^{\ell-1}\} \cup (\pm 2x^{j_0+i}) \cdot \{1, \omega^2, \cdots, \omega^{\ell-2}\}$$
$$i = 0, 1, \cdots, 2^{m_2-1}e-1.$$

Since $0 \leq i \leq 2^{m_2-1}e-1$ so $j_0 \leq j_0 + i \leq j_0 + 2^{m_2-1}e-1$ where $0 \leq j_0 \leq 2^{m_2-1}e-1$. Further, since $x^{2^{m_2-1}e} = -\omega^k \pmod{v}$where $k$ is even so as $i$ runs from 0 to $2^{m_2-1}e-1$ the set $\{\pm 2x^{j_0+i}\} \otimes \{1, \omega^2, \cdots, \omega^{\ell-2}\}$ is the same set $\{\pm 2x^i\} \otimes \{1, \omega^2, \cdots, \omega^{\ell-2}\}$ where $0 \leq i \leq 2^{m_2-1}e-1$. Therefore the opponent differences of 2nd kind are

$$(\pm 2x^i) \cdot \{1, \omega, \cdots, \omega^{\ell-1}\} \qquad i = 0, 1, \cdots, 2^{m_2-1}e-1.$$

as required.

**Theorem 4.5.4** *Let $p_1 = 2^{m_1}t_1 + 1$, $p_2 = 2^{m_2}t_2 + 1$ be primes where $m_1$, $m_2 \geq 2$, $m_1 \neq m_2$ are positive integers, $t_1$, $t_2$ are odd integers. Suppose that Z-cyclic $TWh(p_1)$ and Z-cyclic $TWh(p_2)$ exist. Then a Z-cyclic $TWh(p_1^{\alpha_1}p_2^{\alpha_2})$ exists.*

**Proof.** For a fixed integer $\alpha_2$ we proceed by induction on $\alpha_1$. First we show that for $\alpha_1 = 1$ the statement is true. Let $\omega$ be a common primitive root mod $p_i^2$ $i = 1, 2$ and let $v_1 = p_1p_2^{\alpha_2}$. Decompose $Z_{v_1}$ as following:

$$Z_{v_1} = P_1 \cup \{I_{(0,1)} \cup I_{(0,2)} \cup \cdots \cup I_{(0,\alpha_2-1)} \cup p_2^{\alpha_2}(Z_{p_1} - \{0\}) \cup E$$

where

$$\begin{aligned}
P_1 &= \{x \in Z_{v_1}; p_1 \mid x\} = p_1 Z_{p_2^{\alpha_2}} \\
I_{(0,1)} &= \{x \in Z_{v_1}; p_1 \nmid x, p_2 \mid x, p_2^2 \nmid x\} = p_2\{x \in Z_{p_1p_2^{\alpha_2-1}}; p_1 \nmid x, p_2 \nmid x\} \\
&= p_2 Z_{(1,\alpha_2-1)}, \text{ say,} \\
I_{(0,2)} &= \{x \in Z_{v_1}; p_1 \nmid x, p_2^2 \mid x, p_2^3 \nmid x\} = p_2^2\{x \in Z_{p_1p_2^{\alpha_2-2}}; p_1 \nmid x, p_2 \nmid x\} \\
&= p_2^2 Z_{(1,\alpha_2-2)} \\
\cdots & \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
I_{(0,\alpha_2-1)} &= \{x \in Z_{v_1}; p_1 \nmid x, p_2^{\alpha_2-1} \mid x, p_2^{\alpha_2} \nmid x\} = p_2^{\alpha_2-1}\{x \in Z_{p_1p_2}; p_1 \nmid x, p_2 \nmid x\} \\
&= p_2^{\alpha_2-1} Z_{(1,1)} \\
E &= \{x \in Z_{v_1}; p_1 \nmid x, p_2 \nmid x\}
\end{aligned}$$

Suppose that Z-cyclic $TWh(p_1)$, $TWh(p_2)$ exists. By Theorem 4.5.1 a Z-cyclic $TWh(p_2^{\alpha_2})$ exists, so associated with $TWh(p_1)$ and $TWh(p_2^{\alpha_2})$ there are initial rounds, say, IR($p_1$) and IR($p_2^{\alpha_2}$) respectively, Also by Lemma 4.5.3, in each set $Z_{(1,\alpha_2-1)}$, $Z_{(1,\alpha_2-2)}, \cdots$, $Z_{(1,1)}$, $E$ there exist games which satisfy the triple whist conditions, say $G(Z_{(1,\alpha_2-i)})$ $i = 1, 2, \cdots, \alpha_2 - 1$ and $G(E)$ respectively, Thus for an initial round for a $TWh(v_1)$ we take games

$$p_1 IR(p_2^{\alpha_2}) \cup_{i=1}^{\alpha_2-1} p_2^i G(Z_{(1,\alpha_2-i)}) \cup p_2^{\alpha_2} \cdot IR(p_1) \cup G(E).$$

For the induction step, suppose that $TWh(p_1^{\alpha_1-1}p_2^{\alpha_2})$ exists with an initial round $IR(p_1^{\alpha_1-1}p_2^{\alpha_2})$. Let $v = p_1^{\alpha_1}p_2^{\alpha_2}$ and decompose $Z_v$ as following:

$$Z_v = P_1 \cup \{I_{(0,1)} \cup I_{(0,2)} \cup \cdots \cup I_{(0,\alpha_2-1)}\} \cup I_{(0,\alpha_2)} \cup E.$$

where

$$\begin{aligned}
P_1 = &\quad \{x \in Z_v; p_1 \mid x\} = p_1 Z_{p_1{}^{\alpha_1-1} p_2^{\alpha_2}} \\
I_{(0,1)} = &\quad \{x \in Z_v; p_1 \nmid x, p_2 \mid x, p_2^2 \nmid x\} = p_2\{x \in Z_{p_1^{\alpha_1} p_2^{\alpha_2-1}}; p_1 \nmid x, p_2 \nmid x\} \\
= &\quad p_2 Z_{(\alpha_1,\alpha_2-1)} \\
I_{(0,2)} = &\quad \{x \in Z_v; p_1 \nmid x, p_2^2 \mid x, p_2^3 \nmid x\} = p_2^2\{x \in Z_{p_1 p_2^{\alpha_2-2}}; p_1 \nmid x, p_2 \nmid x\} \\
= &\quad p_2^2 Z_{(\alpha_1,\alpha_2-2)} \\
&\quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
I_{(0,\alpha_2-1)} = &\quad \{x \in Z_v; p_1 \nmid x, p_2^{\alpha_2-1} \mid x, p_2^{\alpha_2} \nmid x\} = p_2^{\alpha_2-1}\{x \in Z_{p_1 p_2}; p_1 \nmid x, p_2 \nmid x\} \\
= &\quad p_2^{\alpha_2-1} Z_{(\alpha_1,1)} \\
I_{(0,\alpha_2)} = &\quad \{x \in Z_v; p_1 \nmid x, p_2^{\alpha_2} \mid x\} = p_2^{\alpha_2}\{Z_{p_1}^{\alpha_1}; p_1 \nmid x\} \\
= &\quad p_2^{\alpha_2} Z_{(\alpha_1,0)} \\
E = &\quad \{x \in Z_v; p_1 \nmid x, p_2 \nmid x\}
\end{aligned}$$

Suppose that $Z$-cyclic $TWh(p_1)$, $TWh(p_2)$ exist. By the proof of Theorem 4.5.1, there exist games, say $(IR(p_1^{\alpha_1}))$, which satisfies the triple whist conditions for $Z_{(\alpha_1,0)}$, and by Lemma 4.5.3 in each set $Z_{(\alpha_1,\alpha_2-i)}$, $i = 1, 2, \cdots, \alpha_2 - 1$ and $E$ there exist games which satisfy the triple whist conditions, say $G(Z_{(\alpha_1,\alpha_2-i)})$ $i = 1, 2, \cdots, \alpha_2 - 1$ and $G(E)$ respectively, Thus for an initial round for a $TWh(v)$ we take games

$$p_1 IR(p_1^{\alpha_1-1} p_2^{\alpha_2}) \cup_{i=1}^{\alpha_2-1} p_2^i G(Z_{(\alpha_1,\alpha_2-i)}) \cup p_2^{\alpha_2} \cdot IR(p_1^{\alpha_1}) \cup G(E).$$

**Example 4.5.2** (a) Find a $TWh(29 \cdot 41)$.

(1) From Example 4.2.1(a)(1), the following games with $\omega = 19$ from an initial round for a $TWh(29)$, and $\frac{\omega^2+1}{2} = 7 = \omega^{20} \pmod{29}$.

$$\{1, \omega^2; \omega, \omega^7\} \otimes \{1, \omega^4, \cdots, \omega^{24}\}$$

From Example 4.3.2.(1), the following games with $\omega = 19$ from an initial round for a $TWh(41)$.

$$\{\{1, \omega^4; \omega^3, \omega^{21}\}, \{\omega^2, \omega^7; \omega^{25}, \omega^{30}\}, \otimes\{1, \omega^8, \cdots, \omega^{32}\}$$

Decompose $Z_{29 \cdot 41}$ as the following

$$Z_{29 \cdot 41} = P_1 \cup P_2 \cup E \cup \{0\}$$

where

$$\begin{aligned}
P_1 &= \{x \in Z_{29 \cdot 41}; 29 \mid x, x \neq 0\} = 29 \cdot (Z_{41} - \{0\}) \\
P_2 &= \{x \in Z_{29 \cdot 41}; 41 \mid x, x \neq 0\} = 41 \cdot (Z_{29} - \{0\}) \\
E &= \{x \in Z_{29 \cdot 41}; 29 \nmid x,\ 41 \nmid x\}
\end{aligned}$$

Since $\omega = 19$ is a common primitive root mod 29 and mod 41, $ord_{mod 29\cdot 41}\omega = l.c.m.\{28, 40\} = 280$, $g.c.d.\{28, 40\} = 4$, and $x = 552$ satisfies

$$\begin{cases} x & \equiv 1 \pmod{29} \\ x & \equiv 19 \pmod{41}. \end{cases}$$

Thus the games

$$\{x^i \cdot \{1, \omega; -\omega, -\omega^2\} \otimes \{1, \omega^2, \cdots, \omega^{278}\} \qquad i = 0, 1$$

satisfy the required conditions in $E$. Therefore, the following games form an initial round for a $TWh(1189)$.

$$\begin{array}{l} 29 \cdot \{\{\{1, \omega^4; \omega^3, \omega^{21}\}, \{\omega^2, \omega^7; \omega^{25}, \omega^{30}\}\} \otimes \{1, \omega^8, \cdots, \omega^{32}\} (\text{mod } 41)\} \cup \\ 41 \cdot \{\{1, \omega^2; \omega, \omega^7\} \otimes \{1, \omega^4, \cdots, \omega^{24}\} (\text{mod } 29)\} \cup \\ \{x^i \cdot \{1, \omega; -\omega, -\omega^2\} \otimes \{1, \omega^2, \cdots, \omega^{278}\} (\text{mod } 1189); i = 0, 1\}. \end{array}$$

(2) If $\omega = 26$ then $\frac{\omega^2+1}{2} = 5 = \omega^{10} \pmod{29}$, and from 3.1(a)(1) the following games form an initial round for a $TWh(41)$.

$$\{\{1, \omega^4; \omega, \omega^6\}, \{\omega^2, \omega^{13}; \omega^{19}, \omega^7\}, \otimes \{1, \omega^8, \cdots, \omega^{32}\}$$

and $x = 436$ satisfies

$$\begin{cases} x & \equiv 1 \pmod{29} \\ x & \equiv 26 \pmod{41}. \end{cases}$$

Thus the following games form an initial round for a $TWh(1189)$.

$$\begin{array}{l} 29 \cdot \{\{\{1, \omega^4; \omega, \omega^6\}, \{\omega^2, \omega^{13}; \omega^{19}, \omega^7\}\} \otimes \{1, \omega^8, \cdots, \omega^{32}\} \quad (\text{mod } 41)\} \cup \\ 41 \cdot \{\{1, \omega^2; \omega, \omega^7\} \otimes \{1, \omega^8, \cdots, \omega^{24}\} \quad (\text{mod } 29)\} \cup \\ \{x^i \cdot \{1, \omega; -\omega, -\omega^2\} \otimes \{1, \omega^2, \cdots, \omega^{278}\} \quad (\text{mod } 1189); i = 0, 1\}. \end{array}$$

(b) Find a $TWh(37 \cdot 41)$.

From Example 4.2.2(b)(1), the following games with $\omega = 19$ from an initial round for a $TWh(37)$, and $\frac{\omega^2+1}{2} = 33 = \omega^{16} \pmod{37}$.

$$\{1, \omega; \omega^2, \omega^7\} \otimes \{1, \omega^4, \cdots, \omega^{32}\}$$

From Example 4.3.2(1), the following games with $\omega = 19$ from an initial round for a $TWh(41)$.

$$\{\{1, \omega^4; \omega^3, \omega^{21}\}, \{\omega^2, \omega^7; \omega^{25}, \omega^{30}\}\} \otimes \{1, \omega^8, \cdots, \omega^{32}\}$$

Decompose $Z_{37\cdot 41}$ as the following

$$Z_{37\cdot 41} = P_1 \cup P_2 \cup E \cup \{0\}$$

where

$$\begin{aligned} P_1 &= \{x \in Z_{37\cdot 41}; 37 \mid x, x \neq 0\} = 37 \cdot (Z_{41} - \{0\}) \\ P_2 &= \{x \in Z_{37\cdot 41}; 41 \mid x, x \neq 0\} = 41 \cdot (Z_{37} - \{0\}) \\ E &= \{x \in Z_{29\cdot 41}; 37 \nmid x,\ 41 \nmid x\} \end{aligned}$$

Since $\omega = 19$ is a common primitive root mod 37 and mod 41. $ord_{mod 29\cdot 41}\omega = l.c.m.\{36, 40\} = 360$, $g.c.d.\{36, 40\} = 4$ and $x = 593$ satisfies

$$\begin{cases} x & \equiv 1 \pmod{37} \\ x & \equiv 19 \pmod{41} \end{cases}$$

Thus the games

$$\{x^i \cdot \{1, \omega; -\omega, -\omega^2\} \otimes \{1, \omega^2, \cdots, \omega^{358}\} \qquad i = 0, 1$$

satisfy the required conditions in $E$. Therefore, the following games form an initial round for a $TWh(1517)$.

$$\begin{aligned} &37 \cdot \{\{\{1, \omega^4; \omega^3, \omega^{21}\}, \{\omega^2, \omega^7; \omega^{25}, \omega^{30}\}\} \otimes \{1, \omega^8, \cdots, \omega^{32}\} \pmod{41}\} \cup \\ &41 \cdot \{\{1, \omega; \omega^2, \omega^7\} \otimes \{1, \omega^4, \cdots, \omega^{32}\} \pmod{37}\} \cup \\ &\{x^i \cdot \{1, \omega; -\omega, -\omega^2\} \otimes \{1, \omega^2, \cdots, \omega^{358}\} \pmod{1517}; i = 0, 1\}. \end{aligned}$$

(c) Find a $TWh(41 \cdot 29^2)$

Let $v = 41 \cdot 29^2$, since $\omega = 26$ is a common primitive root (mod 41) and $mod 29^2$. Note $\frac{\omega^2+1}{2} = 31 = \omega^4$ mod 41. Decompose $Z_v$ as the following,

$$Z_v = P_1 \cup I_{(0,1)} \cup I_{(0,2)} \cup E$$

where

$$\begin{aligned} P_1 &= \{x \in Z_v; 41 \mid x\} = 41 \cdot Z_{29^2}, \\ I_{(0,1)} &= \{x \in Z_v; 41 \nmid x,\ 29 \mid x,\ 29^2 \nmid x\} = 29 \cdot Z_{(1,1)}, \\ I_{(0,2)} &= \{x \in Z_v; 41 \nmid x, 29^2 \mid x\} = 29^2 \cdot (Z_{41} - \{0\}), \\ E &= \{x \in Z_v; 29 \nmid x,\ 41 \nmid x\} \end{aligned}$$

$ord_{mod 41\cdot 29^2}\omega = l.c.m.\{40, 29 \cdot 28\} = 8120$, $g.c.d.\ \{40, 29 \cdot 28\} = 4$. $x = 26938$ satisfies

$$\begin{cases} x & \equiv 1 \pmod{41} \\ x & \equiv 26 \pmod{29^2} \end{cases}$$

Therefore the games

$$\{x^i \cdot \{1, \omega; -\omega, -\omega^2\} \otimes \{1, \omega^2, \cdots, \omega^{8118}\} \quad i = 0, 1; x = 26938\}$$

satisfy the required conditions for a $TWh(41 \cdot 29^2)$ on $E$.

From Example 4.5.1.(a) we have an initial round for $TWh(29^2)$, from Example 4.5.2.(a)(2) we have games for $Z_{(1,1)}$. Therfore, the following games form an initial round for a $TWh(41 \cdot 29^2)$

$$\begin{array}{l}
41 \cdot 29 \cdot \{\{1, \omega^2; \omega, \omega^7\} \otimes \{1, \omega^4, \cdots, \omega^{24}\} \pmod{29}\} \cup \\
41 \cdot \{\{1, \omega^2; \omega, \omega^7\} \otimes \{1, \omega^4, \cdots, \omega^{808}\} \pmod{841}\} \cup \\
29 \cdot \{x^i\{1, \omega; -\omega, -\omega^2\} \otimes \{1, \omega^2, \cdots, \omega^{278}\} \pmod{1189}; i = 0, 1, x = 436\} \cup \\
29^2 \cdot \{\{\{1, \omega^4; \omega, \omega^6\}, \{\omega^2, \omega^{13}; \omega^{19}, \omega^7\}\} \otimes \{1, \omega^8 \cdots, \omega^{32}\} \pmod{41}\} \cup \\
\{x^i \cdot \{1, \omega; -\omega, -\omega^2\} \otimes \{1, \omega^2, \cdots, \omega^{8118}\} (\bmod\ 41 \cdot 29^2);\ i = 0, 1,\ x = 26938\}.
\end{array}$$

**Lemma 4.5.5** *Let* $p_1 = 2^m t_1 + 1$, $p_2 = 2^m t_2 + 1$ *are primes where* $m \geq 1$ *are positive integers,* $t_1$, $t_2$ *odd integers. If Z-cyclic* $TWh(p_1)$ *exists then there exists games which satisfy the Z-cyclic triple whist tournament conditions on the reduced residue system (mod* $v$*) where* $v = p_1^{\alpha_1} p_2^{\alpha_2}$ *for any positive integers* $\alpha_1$, $\alpha_2$.

**Proof.** Let $\omega$ be a common primitive root of $p_1^2$ and $p_2^2$, $g.c.d\ \{p_1^{\alpha_1 - 1}(p_1 - 1),\ p_2^{\alpha_2 - 1}(p_2 - 1)\} = 2^m e$ where e is odd and $l.c.m\{p_1^{\alpha_1 - 1}(p_1 - 1),\ p_2^{\alpha_2 - 1}(p_2 - 1)\} = \ell$; then $p_1^{\alpha_1 - 1}(p_1 - 1) p_2^{\alpha_2 - 1}(p_2 - 1) = 2^m \ell e$. By Lemma 4.5.2 there exists an integer $x \equiv 1 \pmod{p_1}$ such that the $2^m e \ell$ integers $x^i \omega^s$ $(s = 0, 1, \cdots, \ell - 1;\ i = 0, 1, \cdots, 2^m e - 1)$ constitute the reduced residue system mod $v$ with $x^{2^m e} \equiv \omega^u \pmod{v}$ for some integer $0 \leq u \leq \ell - 1$. Note that $2^m e \mid u$ and $x \equiv 1 \pmod{p_1}$

Let $H = \{\omega^s; 0 \leq s \leq \ell - 1\}$ then the $2^m e \ell$ integers are decomposed into cosets $H$, $xH$, $x^2 H, \cdots, x^{2^m e - 1} H$, note also $-1 \in H$.

Suppose that $TWh(p_1)$ exists with the following games as an initial round

$$\{\omega^{a_1},\ \omega^{b_1};\ \omega^{c_1},\ \omega^{d_1}\}, \{\omega^{a_2}, \omega^{b_2};\ \omega^{c_2},\ \omega^{d_2}\}, \cdots, \{\omega^{a_h}, \omega^{b_h};\ \omega^{c_h},\ \omega^{d_h}\}$$

where $h = 2^{m-2} t_1 = \frac{p_1 - 1}{4}$.

Let $\frac{\ell}{p_1-1} = \frac{p_1^{\alpha_1-1}p_2^{\alpha_2-1}t_2}{e} = n$ and $H$ be decomposed as $H = H_0 \cup H_1 \cup \cdots \cup H_{n-1}$ where

$$\begin{aligned} H_0 &= \{1, \omega, \omega^2, \cdots, \omega^{(p_1-1)-1}\} \\ H_1 &= \{\omega^{p_1-1}, \omega^{p_1}, \omega^{p_1+1}, \cdots, \omega^{2(p_1-1)-1}\} \\ H_2 &= \{\omega^{2(p_1-1)}, \omega^{2p_1-1}, \omega^{2p_1}, \cdots, \omega^{3(p_1-1)-1}\} \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ H_{n-1} &= \{\omega^{(n-1)(p_1-1)}, \omega^{(n-1)(p_1-1)+1}, \cdots, \omega^{n(p_1-1)-1}\} \end{aligned}$$

If each $H_j$ $(j = 0, 1, \cdots, n-1)$ is considered mod $p_1$, it is in fact the power sequence $1, \omega, \cdots, \omega^{p_1-2}$ (mod $p_1$). We claim the games

$$(A) \quad \{x^i\omega^{k(p_1-1)}\{\omega^{a_j}, \omega^{b_j}; \omega^{c_j}, \omega^{d_j}\}; 0 \leq i \leq 2^m e - 1, 0 \leq k \leq n-1, 0 \leq j \leq h\}$$

satisfy the required conditions in the reduced residue system mod $v$

Since $\{\{\omega^{a_j}, \omega^{b_j}; \omega^{c_j}, \omega^{d_j}\}; j = 1, 2, \cdots, h\}$ is an initial round for a $TWh(p_1)$ so

1. $a_j,\ b_j,\ c_j,\ d_j \quad j = 1, 2, \cdots, h$ are incongruent mod $2^m t_1$,
2. the partner (resp. first opponent, second opponent) arising from $\{\omega^{a_j}, \omega^{b_j}; \omega^{c_j}, \omega^{d_j}\}$ occupy incongruent positions mod $2^m t_1$.

It follows that

1. the elements in (A) are elements in the reduced residue system each occuring exactly once;
2. the partner (resp. first opponent, second opponent) differences arising from $\{x^i\{\omega^{a_j}, \omega^{b_j}; \omega^{c_j}, \omega^{d_j}\}\}$ occupy incongruent positions (mod $2^m t_1$) in $x^i H$

Therefore the triple-whist conditions satisfied.

**Theorem 4.5.6** *Let $p_1 = 2^m t_1 + 1,\ p_2 = 2^m t_2 + 1$ be primes where $m \geq 1$ and $t_1,\ t_2$ are odd integers. If Z-cyclic $TWh(p_1)$ and Z-cyclic $TWh(p_2)$ exist then Z-cyclic $TWh(v)$ exists where $v = p_1^{\alpha_1}p_2^{\alpha_2}$ for any positive integers $\alpha_1,\ \alpha_2$.*

**Proof.** The proof is as for Theorem 4.5.4 except that Lemma 4.5.5 is used in place Lemma 4.5.3.

**Example 4.5.3** (a) Find a $TWh(29 \cdot 37)$.

Let $\omega = 19$ then $ord_{mod\ 29 \cdot 37}\omega = 252$, $g.c.d.\{28,\ 36\} = 4$, and $x = 204$ satisfies

$$\begin{cases} x & \equiv 1 \pmod{29} \\ x & \equiv 19 \pmod{37}. \end{cases}$$

Let $H = \{1, \omega, \omega^2, \cdots, \omega^{251}\}$; then the reduced residue system mod $29 \cdot 37$ of 1008 integers is decomposed into 4 cosets

$$H,\ xH\ , x^2H,\ x^3H.$$

The set $H$ is decomposed as

$$H = H_0 \cup H_1 \cup \cdots \cup H_8$$

where $H_0 = \{1, \omega, \cdots, \omega^{27}\}$ and $H_i = \omega^{28(i-1)}H_0 \quad i = 1, 2, \cdots, 8$.

By Example 2.1.(a),(1) $TWh(29)$ exists with an initial round

$$\{1, \omega^2; \omega, \omega^7\} \otimes \{1, \omega^4, \cdots, \omega^{24}\}.$$

Thus the games

$$x^i \cdot \omega^{28k} \cdot \{1, \omega^2; \omega, \omega^7\} \otimes \{1, \omega^4, \cdots, \omega^{24}\} \quad i = 0, 1, 2, 3;\ k = 0, 1, \cdots, 8.$$

satisfy the required conditions for a $TWh(29 \cdot 37)$ on the set $E$.

Therefore the following games form an initial round for a $TWh(29 \cdot 37)$.

$$\begin{array}{l} 29 \cdot \{\{1, \omega; \omega^2, \omega^7\} \otimes \{1, \omega^4, \cdots, \omega^{32}\} (\text{mod } 37)\} \cup \\ 37 \cdot \{\{1, \omega^2; \omega, \omega^7\} \otimes \{1, \omega^4, \cdots, \omega^{24}\} (\text{mod } 29)\} \cup \\ \{x^i \cdot \omega^{28k} \cdot \{1, \omega^2; \omega, \omega^7\} \otimes \{1, \omega^4, \cdots, \omega^{24}\} (\text{mod } 29 \cdot 37)\}. \end{array}$$

form an initial round for a $TWh(29 \cdot 37)$.

(b) Find a $TWh(41 \cdot 73)$

Since $\omega = 26$ is a common primitive root of 41 and 73 $ord_{41 \cdot 73}\omega = 360$, $g.c.d.\{40, 72\} = 8$, $x = 1559$ satisfies

$$\begin{cases} x & \equiv 1 \pmod{41} \\ x & \equiv 26 \pmod{73}. \end{cases}$$

Let $H = \{1, \omega, \cdots, \omega^{359}\}$; then the 2880 integers in the reduced residue system mod $41 \cdot 73$ are placed into eight cosets

$$H, xH, x^2H, \cdots, x^7H$$

The set $H$ is decomposed as

$$H = H_0 \cup H_2 \cup \cdots \cup H_8$$

where

$$\begin{array}{l} H_0 = \{1, \omega, \cdots, \omega^{39}\} \\ H_k = \omega^{40(k-1)} H_0 \qquad k = 1, 2, \cdots, 8. \end{array}$$

$TWh(41)$ exists with an initial round

$$\{\{1, \omega^4; \omega, \omega^6\}, \{\omega^2, \omega^{13}; \omega^{19}, \omega^7\} \otimes \{1, \omega, \cdots, \omega^{32}\}$$

Therefore, the games

$$x^i \cdot \omega^{40k} \cdot \{\{1, \omega^4; \omega, \omega^6\}, \{\omega^2, \omega^{13}; \omega^{19}, \omega^7\} \otimes \{1, \omega, \cdots, \omega^{32}\}$$
$$i = 0, 1, \cdots, 7; \;\; k = 0, 1, 2, \cdots, 8.$$

satisfy the required conditions to be an initial round on the reduced residue system mod $(41 \cdot 73)$.

Let $Z_{41\cdot 73}$ be decomposed as $Z_{41\cdot 73} = P_1 \cup P_2 \cup E$ where

$$\begin{array}{l} P_1 = \{x \in Z_{41\cdot 73}; 41 \mid x, \} = 41 \cdot Z_{73}, \\ P_2 = \{x \in Z_{41\cdot 73}; 73 \mid x\} = 73 \cdot \{Z_{41} - \{0\}\} \\ E = \{x \in Z_{41\cdot 73}; 73 \nmid x, 41 \nmid x\} \end{array}$$

Therefore the following games form an initial round for a $TWh(41 \cdot 73)$

$$\begin{array}{l} 73 \cdot \{\{\{1, \omega^4; \omega, \omega^6\}, \{\omega^2, \omega^{13}; \omega^{19}, \omega^7\} \otimes \{1, \omega^8 \cdots, \omega^{32}\} (\text{mod } 41)\} \cup \\ 41 \cdot \{\{\{1, \omega^4; \omega, \omega^{14}\}, \{\omega^2, \omega^{15}; \omega^3, \omega^{21}\}\} \otimes \{1, \omega^8, \cdot, \omega^{64}\} (\text{mod } 73)\} \cup \\ \{x^i \cdot \omega^{40k} \cdot \{\{1, \omega^4; \omega, \omega^6\}, \{\omega^2, \omega^{13}; \omega^{19}, \omega^7\}\} \otimes \{1, \omega^8 \cdots, \omega^{32}\} (\text{mod } 41 \cdot 73)\}. \end{array}$$

**Theorem 4.5.7** *Let $p_i = 2^{m_i} t_i + 1$, $i = 1, 2, \cdots, r$ be primes, $m_i \geq 2$ be positive integers, $t_i$ be odd integers. If Z-cyclic $TWh(p_i)$ exist then a Z-cyclic $TWh(\prod_{i=1}^{r} p_i^{\alpha_i})$ exists for any positive integers $\alpha_i$.*

**Proof.** We prove by induction on $r$; the cases $r = 1, 2$ were proved in Theorem 4.5.1, 4.5.2 and 4.5.3. Suppose that the statement is true for $r-1$. i.e. $TWh(\prod_{i=2}^{r} p_i^{\alpha_i})$ exists; we want to show that $TWh(\prod_{i=1}^{r} p_i^{\alpha_i})$ exists. We first show that $TWh\ (p_1 \prod_{i=2}^{r} p_i^{\alpha_i})$ exists.

Let $\omega$ be a common primitive root of mod $p_i^2$ $\ i = 1, 2, \cdots, r$ and let $v_1 = \prod_{i=1}^{r} p_i^{\alpha_i}$, where $\alpha_1 = 1$. We decompose $Z_{v_1}$ as the following "layers": one is $P_1 = \{x \in Z_{v_1}; p_1 \mid x\}$ and the others are

$$I_{(0,\beta_2,\cdots,\beta_r)} = \{x \in Z_{v_1}; p_1 \nmid x,\ p_i^{\beta_i} \mid x,\ p_i^{\beta_i+1} \nmid x \text{ if } \beta_i < \alpha_i\}$$

for each $r$-tuple $(0, \beta_2, \cdots, \beta_r)$ where $0 \le \beta_i \le \alpha_i$ $i = 2, 3, \cdots, r$. We first show how to construct initial round games on a given $I_{(0,\beta_2,\cdots,\beta_r)}$. Set $\pi_{(\beta_1,\cdots,\beta_r)} = \prod_{i=1}^{r} p_i^{\beta_i}$. where we put $\beta_1 = 0$. Then

$$I_{(\beta_1,\cdots,\beta_r)} = \pi_{(\beta_1,\cdots,\beta_r)} \cdot Z_{(\gamma_1,\cdots,\gamma_r)}$$

where $Z_{(\gamma_1,\cdots,\gamma_r)} = \{x \in Z_{\pi_{(\gamma_1,\cdots,\gamma_r)}}; p_i \nmid x \text{ if } \gamma_i \ne 0\}$ and $\alpha_i = \beta_i + \gamma_i$, $i = 1, 2, \cdots, r$

Let $\tau = ord_{\pi_{(\gamma_1,\cdots,\gamma_r)}}\omega = l.c.m\ \{p_i^{\gamma_i - 1}(p_i - 1); \gamma_i > 0\} = 4t_0$, since $\gamma_1 = 1 \ne 0$.

**Lemma A** $|Z_{(\gamma_1,\cdots,\gamma_r)}| = \phi(\pi_{(\gamma_1,\cdots,\gamma_r)}) = \prod_{\gamma_i \ne 0} p_i^{\gamma_i - 1}(p_i - 1) = 4t_0 n_0$

**Lemma B** $\omega^\ell \not\equiv -1 \pmod{\pi_{(\gamma_1,\cdots,\gamma_r)}}$ if there are $\gamma_i \ne 0$, $\gamma_j \ne 0$, $i \ne j$ with $m_i \ne m_j$.

**Lemma C** $\omega^{\frac{\tau}{2}} \equiv -1 \pmod{\pi_{(\gamma_1,\cdots,\gamma_r)}}$ if $m_i = a$ for all $i$ such that $\gamma_i \ne 0$.

**Lemma D** If $x \in Z_{(\gamma_1,\cdots,\gamma_r)}$ then the minimum value of $\tau$ such that $x\omega^\tau \equiv x \pmod{\pi_{(\gamma_1,\cdots,\gamma_r)}}$ is $\tau = ord_{\pi_{(\gamma_1,\cdots,\gamma_r)}}\omega$

**Proof** Full details can be found in [9].

**Case 1.** If there exists $\gamma_i \ne 0$, $\gamma_j \ne 0$ $i \ne j$ with $m_i \ne m_j$ then $\omega^\ell \not\equiv -1 \pmod{\pi_{(\gamma_1,\cdots,\gamma_r)}}$ for all $\ell$ and $|Z_{(\gamma_1,\cdots,\gamma_r)}| = 4t_0 n_0$ where $n_0$ is even, say, $n_0 = 2n$. Thus $x\omega^\ell \not\equiv -x \pmod{\pi_{(\gamma_1,\cdots,\gamma_r)}}$ for all $x \in Z_{(\gamma_1,\cdots,\gamma_r)}$ $\forall \ell$. We define

$$C_x = \{x, x\omega, x\omega^2, \cdots, x\omega^{4t_0 - 1}\}$$

then $C_x \cap C_{-x} = \emptyset$ and we can find successively $x_1, x_2, \cdots, x_n \in Z_{(\gamma_1,\cdots,\gamma_r)}$ such that $x_i \not\equiv \pm\omega^\ell x_j \pmod{\pi_{(\gamma_1,\cdots,\gamma_r)}}$ $\forall \ell$ and all $i \ne j$ and $Z_{(\gamma_1,\cdots,\gamma_r)} = (C_{x_1} \cup C_{-x_1}) \cup$

$\cdots(C_{x_n}\cup C_{-x_n})$. Since any $C_x$ can be represented by any of $x, x\omega,\cdots,x\omega^{4t_0-1}$ and since $4t_0\geq p_k-1$ for any $k$ with $\gamma_k\neq 0$, we can always choose $x_i$ so that $x_i\equiv 1 \pmod{p_1}$.

**Lemma E** The games

$$\{x_i, x_i\omega; -x_i\omega, -x_i\omega^2\}\otimes\{1,\omega^2,\cdots,\omega^{4t_0-2}\} \qquad i=1,2,\cdots,n$$

satisfy the initial round triple whist conditions for $Z_{(\gamma_1,\cdots,\gamma_r)}$ provided we choose $\omega$ so that $\frac{\omega^2+1}{2}=\Box \pmod{p_1}$.

**Proof.** The partner differences are

$$\begin{aligned}&\{\pm x_i(\omega-1),\pm x_i(\omega^2-\omega)\}\otimes\{1,\omega^2,\cdots,\omega^{4t_0-2}\}\\=&\pm x_i(\omega-1)\}\cdot\{1,\ \omega,\cdots,\omega^{4t_0-1}\}.\end{aligned}$$

The opponent differences the of 1st kind are

$$\begin{aligned}&\{\pm x_i(\omega+1),\pm x_i(\omega^2+\omega)\}\otimes\{1,\omega^2,\cdots,\omega^{4t_0-2}\}\\=&\pm x^i(\omega+1)\cdot\{1,\ \omega,\cdots,\omega^{4t_0-1}\}.\end{aligned}$$

The opponent differences of the 2nd kind are

$$\begin{aligned}&\{\pm 2x_i\omega,\pm x_i(\omega^2+1)\}\otimes\{1,\omega^2,\cdots,\omega^{4t_0-2}\}\\=&(\pm 2x_i\omega)\cdot\{1,\ \omega^2,\cdots,\omega^{4t_0-2}\}\cup(\pm x_i(\omega^2+1))\cdot\{1,\ \omega^2,\cdots,\omega^{4t_0-2}\}.\end{aligned}$$

Clearly $\pm 2x_i\omega^{2u+1}$, $i=1,2,\cdots,n; u=0,1,\cdots,2t_0-1$ are all distinct, as are all $\pm x_i(\omega^2+1)\omega^{2u}$. It remains to show that no one of $\pm 2x_i\omega^{2u+1}$ is the same as $\pm x_j(\omega^2+1)\omega^{2v}$ for any $i,\ j,\ u,\ v$. Assume to the contrary that $\pm 2x_i\omega^{2u+1}\equiv\pm x_j(\omega^2+1)\omega^{2v} \pmod{\pi_{(\gamma_1,\cdots,\gamma_r)}}$ for some $i,\ j,\ u,\ v$. Then $\pm 2x_i\omega^{2u+1}\equiv\pm x_j(\omega^2+1)\omega^{2v} \pmod{p_k}$ $\forall k$ which implies $2\omega^{2(u-v)+1}\equiv\pm(\omega^2+1) \pmod{p_1}$. This cannot be take place by our choice of $\omega$ such that $2\omega(\omega^2+1)$ is quadratic non-residue mod $p_1$.

Therefore each kind of differences occurs in $Z_{(\gamma_1,\cdots,\gamma_r)}$ each exactly once as required. Thus an initial round in $I_{(\beta_1,\cdots,\beta_r)}$ is $\pi_{(\beta_1\cdots\beta_r)}\cdot\{x_i,x_i\omega;-x_i\omega,-x_i\omega^2\}\otimes\{1,\omega^2,\cdots,\omega^{4t_0-1}\} \pmod{\pi_{(\gamma_1,\cdots,\gamma_r)}}\}$

**Case 2.** If whenever $\gamma_i\neq 0$ we have $m_i=a$ then $\omega^{2t_0}\equiv -1 \bmod(\pi_{(\gamma_1,\cdots,\gamma_r)})$. Note that $\gamma_1=1$.

Let $x\in Z_{(\gamma_1,\cdots,\gamma_r)}$. By Lemma D, put $C_x=\{x,x\omega,\cdots,x\omega^{4t_0-1}\}$. Then because $x\omega^{2t_0}\equiv -x \pmod{\pi_{(\gamma_1,\cdots,\gamma_r)}}$, $-x\in C_x$, We can write $Z_{(\gamma_1,\cdots,\gamma_r)}=\cup_{i=1}^{no}C_{x_i}$

where $|Z_{(\gamma_1,\cdots,\gamma_r)}| = 4t_0n_0$ and we can choose the representive element $x_i$ so that $x_i \equiv 1 \pmod{p_1}$ and $x_i \notin \cup_{j=1}^{i-1} C_{x_j}$ for each $i$.

Let $d = 2^a t_1$ then $d \mid 4t_0$. Set $4t_0 = dm$. Since $TWh(p_1)$ exists, suppose that an initial round for $TWh(p_1)$ is

$$\{\omega^{a_1}, \omega^{b_1}; \omega^{c_1}, \omega^{d_1}\}, \{\omega^{a_2}, \omega^{b_2}; \omega^{c_2}, \omega^{d_2}\}, \cdots, \{\omega^{a_h}, \omega^{b_h}; \omega^{c_h}, \omega^{d_h}\}$$

where $h = 2^{a-2}t_1 = \frac{d}{4}$.

We claim the games

$$(A) \qquad x_i\{\{\omega^{a_1}, \omega^{b_1}; \omega^{c_1}, \omega^{d_1}\}, \{\omega^{a_2}, \omega^{b_2}; \omega^{c_2}, \omega^{d_2}\}, \cdots, \{\omega^{a_h}, \omega^{b_h}; \omega^{c_h}, \omega^{d_h}\}\}\otimes$$
$$\{1, \omega^d, \omega^{2d}, \cdots, \omega^{(m-1)d}\} \quad i = 1, 2, \cdots, n_0.$$

satisfy the required conditions in $Z_{(\gamma_1,\cdots,\gamma_r)}$.

First note that the elements that occur in $(A)$ are precisely all elements of $Z_{(\gamma_1,\cdots,\gamma_r)}$ each exactly once, since $a_i, b_i, c_i$ and $d_i$ $i = 1, 2, \cdots, h$ are incongruent mod $d$. What we need to show is that the partner (resp. 1st and 2nd opponent) differences are distinct, and are all in $Z_{(\gamma_1,\cdots,\gamma_r)}$.

The partner differences are

$$\{\pm x_i(\omega^{b_j} - \omega^{a_j}), \pm x_i(\omega^{d_j} - \omega^{c_j}).$$

No $\omega^{b_j} - \omega^{a_j}$ can be divisible by any $p_i$ if we have ordered the $p_i$ so that $p_1 < p_2 < \cdots < p_r$, for $|b_j - a_j| < p_1 - 1 < p_i - 1$ for each $i$. So the partner differences are indeed all in $Z_{(\gamma_1,\cdots,\gamma_r)}$.

Suppose, for example, $x_i(\omega^{b_{j_0}} - \omega^{a_{j_0}}) = \pm x_\ell(\omega^{d_{j_1}} - \omega^{c_{j_1}})\omega^{dk_1} \pmod{\pi_{(\gamma_1,\cdots,\gamma_r)}}$ for some $i$, $j_0$, $j_1$, $k_1$. Considering these mod $p_1$ gives

$$(B) \qquad (\omega^{b_{j_0}} - \omega^{a_{j_0}}) \equiv \pm(\omega^{d_{j_1}} - \omega^{c_{j_1}}) \pmod{p_1}$$

But since

$$\{\omega^{a_j}, \omega^{b_j}; \omega^{c_j}, \omega^{d_j}\} \qquad j = 1, 2, \cdots, h.$$

is an initial round for $TWh(p_1)$ so the partner differences arise from them are

$$\pm(\omega^{b_j} - \omega^{a_j}), \pm(\omega^{d_j} - \omega^{c_j}) \qquad j = 1, 2, \cdots, h.$$

and these are incongruent (mod $p_1$).

A similar argument holds for opponent differences. So the games (A) with each multiplied by $\pi_{(\beta_1,\cdots,\beta_r)}$ gives initial round games $G(I_{(0,\beta_2,\cdots,\beta_r)})$.

Suppose that $TWh(\prod_{i=2}^r p_i^{\alpha_i})$ exists with initial round games $IR(\prod_{i=2}^r p_i^{\alpha_i})$. Therefore for an initial round for a $TWh(p_1\prod_{i=2}^r p_i^{\alpha_i})$ we take games

$$p_1 \cdot IR(\prod_{i=2}^r p_i^{\alpha_i}) \cup_{i=2}^r G(I_{(0,\beta_2,\cdots\beta_r)}).$$

Finally, we prove that $TWh(\prod_{i=1}^r p_i^{\alpha_i})$ exists by induction on $\alpha_1$. The argument is the same as above, except this time $P_1 = \{x \in Z_v; p_1 \mid x\} = p_1 \cdot Z_{p_1^{\alpha_1-1}\prod_{i=2}^r p_i^{\alpha_i}}$ and others are $I_{(\beta_1,\cdots\beta_r)} = \{x \in Z_v; p_1 \nmid x,\ p_i^{\beta_i} \mid x,\ p_i^{\beta+1} \nmid x \text{ if } \beta_i < \alpha_i\}$ for any r-tuple $(\beta_1,\cdots,\beta_r)$ with $0 \le \beta_i \le \alpha_i \quad i = 2,\ldots,r$. Thus the following games form an initial round for a Z-cyclic $TWh(\prod_{i=1}^r p_i^{\alpha_i}$

$$p_1 \cdot IR(p_1^{\alpha_1-1}\prod_{i=2}^r p_i^{\alpha_i}) \cup G(I_{(\beta_1,\cdots,\beta_r)})$$

Note: There is no need to use the same $\omega$ in each $I_{(\beta_1,\beta_2,\cdots,\beta_r)}$. However, it simplifies matter if we can; This happen in the following examples.

**Example 4.5.4** Find a $TWh(29 \cdot 37 \cdot 41)$

Let $v = 29 \cdot 37 \cdot 41$ then $\omega = 19$ is a common primitive root of 29, 37 and 41, where $\frac{\omega^2+1}{2} = \omega^{20}(\text{mod}29)$ and $\frac{\omega^2+1}{2} = \omega^{16}$ (mod37). We decompose $Z_v$ as follows:

$$Z_v = P_1 \cup I_{(0,0,0)} \cup I_{(0,0,1)} \cup I_{(0,1,0)} \cup I_{(0,1,1)}$$

where

$$P_1 = \{x \in Z_v; 29 \mid x\} = 29 \cdot Z_{37\cdot 41},$$

$$I_{(0,0,0)} = \{x \in Z_v; 29 \nmid x, 37 \nmid x, 41 \nmid x\} = Z_{(1,1,1)},$$

$$I_{(0,0,1)} = \{x \in Z_v; 29 \nmid x, 37 \nmid x, 41 \mid x\} = 41 \cdot \{x \in Z_{29\cdot 37}; 29 \nmid x, 37 \nmid x\}$$
$$= 41 \cdot Z_{(1,1,0)},$$

$$I_{(0,1,0)} = \{x \in Z_v; 29 \nmid x, 37 \mid x, 41 \nmid x\} = 37 \cdot \{x \in Z_{29\cdot 41}; 29 \nmid x, 41 \nmid x\}$$
$$= 37 \cdot Z_{(1,0,1)},$$

$$I_{(0,1,1)} = \{x \in Z_v; 29 \nmid x, 37 \mid x, 37^2 \nmid x, 41 \mid x, 41^2 \nmid x\} = 37 \cdot 41\{x \in Z_{29}; 29 \nmid x\}$$

It is only the set $Z_{(1,1,1)} = \{x \in Z_v; 29 \nmid x, 37 \nmid x, 41 \nmid x\}$ that needs to have further details of construction. Note that $ord_{29\cdot37\cdot41} = 2520$. Let $G = \{x; (x,v) = 1\}$, $H = \{\omega^s; 0 \leq s \leq 2519\}$ then $H$ is a subgroup of $G$ and $[G:H] = 16$. By Lemma 5.1 $-1 \notin H$. Solve the following system of congruences

$$\begin{cases} x \equiv 1 \pmod{29} \\ x \equiv 19 \pmod{37} \\ x \equiv 1 \pmod{41} \end{cases} \qquad \begin{cases} y \equiv 1 \pmod{29} \\ y \equiv 1 \pmod{37} \\ y \equiv 19 \pmod{41} \end{cases}$$

We have $x = 13080$, $y = 27899$, and $x \notin H$, $x^2 \equiv 41616 \notin H$, $x^3 \equiv 11891 \notin H$, $x^4 \equiv 19025 \in H$, so the indicator of $x$ in $H$ is 4. Thus by Theorem 1.1.1, the set $H_1 = \{x^i\omega^s; 0 \leq i \leq 3, 0 \leq s \leq 2519\}$ is a subgroup of $G$ and $|H_1| = 4|G|$, so $[G:H_1] = 4$. Further, $y \notin H_1$, $y^2 \equiv 30045 \notin H_1$, $y^3 \equiv 26826 \notin H_1$, $y^4 \equiv 9658 \in H_1$. By Theorem 1.1.1 again $H_2 = \{y^jx^i\omega^s : 0 \leq i,j \leq 3,\ 0 \leq s \leq 2519\} = G$. Therefore the reduced residue system mod $v$ was decomposed as

$$\cup_{j=0}^{3} \cup_{i=0}^{3} y^jx^iH \qquad \text{where} \qquad x^iy^j \equiv 1 \pmod{29}$$

Thus the games

$$y^jx^i \cdot \{1,\omega; -\omega, -\omega^2\} \otimes \{1, \omega^2, \cdots, \omega^{2518}\}$$

satisfy the required conditions to be the part of an initial round for $TWh(29 \cdot 37 \cdot 41)$ in the set $Z_{(1,1,1)}$.

Therefore the following games form an initial round for a $TWh(29 \cdot 37 \cdot 41)$:

$$\begin{array}{l}
29 \cdot 37 \cdot \{\{\{1,\omega^4;\omega^3,\omega^{21}\},\{\omega^2,\omega^7;\omega^{25},\omega^{30}\}\} \otimes \{1,\omega^8,\cdots,\omega^{32}\}(\mathrm{mod}\ 41);\}\cup \\
29 \cdot 41 \cdot \{\{1,\omega;\omega^2,\omega^7\} \otimes \{1,\omega^4,\cdots,\omega^{32}\}(\mathrm{mod}\ 37);\}\cup \\
29 \cdot \{x_1^i\{1,\omega;-\omega,-\omega^2\} \otimes \{1,\omega^2,\cdots,\omega^{358}\}(\mathrm{mod}\ 1517); x_1 = 593, i = 0,1\}\}\cup \\
\{y^jx^i \cdot \{1,\omega;-\omega,-\omega^2\} \otimes \{1,\omega^2,\cdots,\omega^{2518}\}(\mathrm{mod}\ v); y = 27899,\ x = 13080\}\cup \\
41 \cdot \{x^i\omega^{28k}\{1,\omega^2;\omega,\omega^7\} \otimes \{1,\omega^4,\cdots,\omega^{24}\}(\mathrm{mod}\ 29\cdot37); 0 \leq i \leq 3, 0 \leq k \leq 8\} \\
\cup 37 \cdot \{x^i\{1,\omega;-\omega,-\omega^2\} \otimes \{1,\omega^2,\cdots,\omega^{278}\}(\mathrm{mod}\ 1189);\ i = 0,1,\ x = 436\}\}\cup \\
37 \cdot 41 \cdot \{\{1,\omega^2;\omega,\omega^7\} \otimes \{1,\omega^4,\cdots,\omega^{24}\} \quad (\mathrm{mod}\ 29)\}
\end{array}$$

## 4.6 Composition theorem for $TWh(4n)$

In this last section, we deal with the Triple Whist Tournament of order $4n$ using the same method as in section 4.5.

**Theorem 4.6.1** *Let $p_1 = 4t_1+3$, $p_i = 2^{m_i}t_i+1$, $i = 2, 3, \cdots, r$ be primes, $m_i \geq 2$ be positive integers, $t_i$, $i = 1, 2, \cdots, r$ be odd integers. If Z-cyclic $TWh(p_1 + 1)$, Z-cyclic $TWh(p_i)$ exist then a Z-cyclic $TWh(p_1 \cdot \prod_{i=2}^{r} p_i^{\alpha_i} + 1)$ exists for any positive integers $\alpha_i \quad i = 2, 3, \cdots, r$.*

**Proof.** Let $v = p_1 \prod_{i=2}^{r} p_i^{\alpha_i}, \pi_{(\beta_1,\cdots,\beta_r)} = \prod_{i=1}^{r} p_i^{\beta_i}, \quad \alpha_1 = 1, \ \beta_1 = 0$, and let $\omega$ be a common primitive root of $p_i^2 \quad i = 1, 2, \cdots, r$. We decompose $Z_v$ into the following "layers"; one is $P_1 = \{x \in Z_{v_1}; p_1 \mid x\}$ and the others are

$$I_{(0,\beta_2,\cdots,\beta_r)} = \{x \in Z_{v_1}; p_1 \nmid x, \ p_i^{\beta_i} \mid x, \ p_i^{\beta_i+1} \nmid x \text{ if } \ \beta_i < \alpha_i\}$$

for each $r$-tuple $(0, \beta_2, \cdots, \beta_r)$ where $0 \leq \beta_i \leq \alpha_i \quad i = 2, 3, \cdots, r$. We first show how to construct initial round games on a given $I_{(0,\beta_2,\cdots,\beta_r)}$. Note that

$$I_{(\beta_1,\cdots,\beta_r)} = \pi_{(\beta_1,\cdots,\beta_r)} \cdot Z_{(\gamma_1,\cdots,\gamma_r)}$$

where $Z_{(\gamma_1,\gamma_2,\cdots,\gamma_r)} = \{x \in Z_{\pi_{(\gamma_1,\cdots,\gamma_r)}}; p_i \nmid x \text{ if } \gamma_i \neq 0\}$ and $\alpha_i = \beta_i + \gamma_i$, $i = 1, 2, \cdots, r$.

Let $\tau = ord_{\pi_{(\gamma_1,\cdots,\gamma_r)}}\omega = l.c.m \ \{p_i^{\gamma_i-1}(p_i - 1); \gamma_i > 0\}$. Then $\tau = 4t_0$ for all $Z_{(\gamma_1,\cdots,\gamma_r)}$ except $Z_{(\gamma_1,\cdots,\gamma_r)}$ with $\gamma_2 = \cdots = \gamma_r = 0$ which we will deal with separately.

We now deal with the initial games in $Z_{(\gamma_1,\cdots,\gamma_r)}$ where not all $\gamma_i \quad i = 2, 3, \cdots, r$ are zero. Since $\gamma_1 = 1$ and there are some $\gamma_i \neq 0 \quad 2 \leq i \leq r$, so we proceed as in case 1 in the proof of Theorem 4.5.4 and we take $\pi_{(\beta_1,\cdots,\beta_r)} \{\{x_i, x_i\omega; -x_i\omega, -x_i\omega^2\} \otimes \{1, \omega^2, \cdots, \omega^{4t_0-1}\} \pmod{\pi_{(\gamma_1,\cdots,\gamma_r)}}\}$ as initial games in $I_{(\beta_1,\cdots,\beta_r)}$

For $I_{(0,\alpha_2,\cdots,\alpha_r)} = \pi_{(0,\alpha_2,\cdots,\alpha_r)} \cdot Z_{(1,0,\cdots,0)} = \prod_{i=2}^{r} p_i^{\alpha_i} \cdot Z_{p_1}$. By the hypothesis $TWh(p_1 + 1)$ exists.

Therefore for the initial round of a $TWh(p_1 \prod_{i=2}^{r} p_i^{\alpha_i} + 1)$ we take games of the initial round of $TWh(\prod_{i=2}^{r} p_i^{\alpha_i})$ with each entry multiplied by $p_1$ and the games in $I_{(\beta_1,\cdots,\beta_r)}$ constructed above along with the initial round games in $TWh(p_1 + 1)$ with every non-$\infty$ element multiplied by $p_2^{\alpha_2} \cdots p_r^{\alpha_r}$.

**Example 4.6.1** Find a $TWh(7 \cdot 29 \cdot 41 + 1)$

Let $v = 7 \cdot 29 \cdot 41 + 1$, since $\omega = 26$ is a common primitive root of mod 7, mod 29 and mod 41, where $\frac{\omega^2+1}{2} = \omega^{10} \pmod{29}$ and $\frac{\omega^2+1}{2} = \omega^{46} \pmod{41}$. We decompose $Z_v$ as follows:

$$Z_v = P_1 \cup I_{(0,0,0)} \cup I_{(0,0,1)} \cup I_{(0,1,0)} \cup I_{(0,1,1)}$$

where

$$\begin{aligned}
P_1 &= \{x \in Z_v; 7 \mid x\} = 7 \cdot Z_{29 \cdot 41}, \\
I_{(0,0,0)} &= \{x \in Z_v; 7 \nmid x, 29 \nmid x, 41 \nmid x\} = Z_{(1,1,1)}, \\
I_{(0,0,1)} &= \{x \in Z_v; 7 \nmid x, 29 \nmid x, 41 \mid x\} = 41 \cdot \{x \in Z_{7 \cdot 29}; 7 \nmid x, 29 \nmid x\} \\
&= 41 \cdot Z_{(1,1,0)}, \\
I_{(0,1,0)} &= \{x \in Z_v; 7 \nmid x, 29 \mid x, 41 \nmid x\} = 29 \cdot \{x \in Z_{7 \cdot 41}; 7 \nmid x, 41 \nmid x\} \\
&= 37 \cdot Z_{(1,0,1)}, \\
I_{(0,1,1)} &= \{x \in Z_v; 7 \nmid x, 29 \mid x, 41 \mid x\} = 29 \cdot 41 \cdot \{x \in Z_7; 7 \nmid x\}
\end{aligned}$$

First we deal with $Z_{(1,1,1)} = \{x \in Z_v; 7 \nmid x, 29 \nmid x, 41 \nmid x\}$. $ord_{7 \cdot 29 \cdot 41}\omega = 840$. Let $G = \{x; (x,v) = 1\}$, $H = \{\omega^s; 0 \le s \le 839\}$ then $H$ is a subgroup of $G$ and $[G : H] = 8$. By Lemma 4.5.1 $-1 \notin H$. Solve the following two systems of congruences

$$\begin{cases} x \equiv 1 \pmod{41} \\ x \equiv 26 \pmod{29} \\ x \equiv 1 \pmod{7} \end{cases} \qquad \begin{cases} y \equiv 1 \pmod{41} \\ y \equiv 1 \pmod{29} \\ y \equiv 26 \pmod{7} \end{cases}$$

We have $x = 3158$, $y = 3568$, and $x \notin H$, $x^2 \equiv 2010 \notin H$, $x^3 \equiv 5454 \notin H$, $x^4 \equiv 3445 \in H$, so the indicator of $x$ in $H$ is 4. Thus by Theorem 1.1.1, the set $H_1 = \{x^i\omega^s; 0 \le i \le 3, 0 \le s \le 839\}$ is a subgroup of $G$ and $|H_1| = 4|H|$, so $[G : H_1] = 2$. Further, $y \notin H_1$, $y^2 \equiv 4757 \in H_1$. By Lemma 1.1.1 again $H_2 = \{y^j x^i \omega^s : 0 \le j \le 1,\ 0 \le i \le 3,\ 0 \le s \le 839\} = G$. Therefore the reduced residue system mod $v$ was decomposed as

$$\cup_{j=0}^{1} \cup_{i=0}^{3} y^j x^i H \qquad \text{where} \qquad x^i y^j \equiv 1 \pmod{41}$$

Thus the games

$$(A)\quad y^j x^i \cdot \{1, \omega; -\omega, -\omega^2\} \otimes \{1, \omega^2, \cdots, \omega^{838}\} \qquad \text{where} \quad 0 \le i \le 3,\ 0 \le j \le 1$$

satisfy the required conditions to be the part of an initial round for $TWh(7{\cdot}29{\cdot}41)$ in the set $Z_{(1,1,1)}$.

For the set $I_{(0,0,1)} = 41{\cdot}\{x \in Z_{7\cdot 29}; 7 \nmid x,\ 29 \nmid x\}$. $ord_{7\cdot 29} = 84$, $g.c.d.\ \{6,\ 28\} = 2$. Solve the following equations

$$\begin{cases} z \equiv 1 \pmod{29} \\ z \equiv 26 \pmod{7} \end{cases}$$

We have $z = 117$. Let $H_3 = \{\omega^s; 0 \le s \le 83\}$. Then the 168 integers in the reduced residue system mod(203) are decomposed into two cosets

$$z^i H \quad i = 0, 1, \qquad \text{where} \quad z = 117 = -\omega^{70},\ z^2 = \omega^{56}$$

Thus the following games satisfy the required conditions on $I_{(0,0,1)}$.

$$(B) \qquad 29 \cdot \{1, \omega; -\omega, -\omega^2\} \otimes \{1, \omega^2, \cdots, \omega^{82}\}$$

For the set $I_{(0,1,0)} = 29\{x \in Z_{7\cdot 41}; 7 \nmid x,\ 41 \nmid x\}$. $ord_{7\cdot 41} = 120$, $g.c.d.\{6,\ 40\} = 2$. Solve the following system of congruences

$$\begin{cases} u \equiv 1 \pmod{41} \\ u \equiv 26 \pmod{7} \end{cases}$$

We have $u = 124$. Let $H_4 = \{\omega^s; 0 \le s \le 119\}$, then the reduced residue system of 240 integers mod(287) was decomposed into two cosets

$$u^i H \quad i = 0, 1 \qquad \text{where} \quad u = 124 = -\omega^{100},\ u^2 = \omega^{80}$$

Thus the following games satisfy the required conditions on $I_{(0,1,0)}$.

$$(C) \qquad 29 \cdot \{1, \omega; -\omega, -\omega^2\} \otimes \{1, \omega^2, \cdots, \omega^{118}\}$$

From an initial round $\{\infty, 0; 4, 5\}, \{1, 3; 2, 6\}$ of $TWh(8)$. We have the following games for the set $I_{(0,1,1)}$

$$(D) \qquad 29 \cdot 41 \cdot \{\{\infty, 0; 4, 5\}, \{1, 3; 2, 6\}\} \qquad \text{where } a \cdot \infty = \infty.$$

From Example 4.5.2.$(a)$, we construct the following games for $P_1$, where $\omega = 26$.

$(E)$

$$7 \cdot 29 \cdot \{\{\{1, \omega^4; \omega, \omega^6\}, \{\omega^2, \omega^{13}; \omega^{19}, \omega^7\}\} \otimes \{1, \omega^8, \cdots, \omega^{32}\} (\text{mod } 41)\} \cup$$
$$7 \cdot 41 \cdot \{\{1, \omega^2; \omega, \omega^7\} \otimes \{1, \omega^8, \cdots, \omega^{24}\} \quad (\text{mod } 29)\} \cup$$
$$7 \cdot \{x^i \cdot \{1, \omega; -\omega, -\omega^2\} \otimes \{1, \omega^2, \cdots, \omega^{278}\} (\text{mod } 1189); i = 0, 1, x = 436\}.$$

Therefore, $A \cup B \cup C \cup D \cup E$ form an initial round for a $TWh(7 \cdot 29 \cdot 41)$.

# Chapter 5

# Z-cyclic Room squares

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

## 5.1 Introduction

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

1. each cell is empty or contains an unordered pair of distinct symbols;
2. each row and each column contains each symbol exactly once;
3. each of the $n(2n-1)$ unordered pairs of distinct symbols occurs in precisely one cell of the array.

A Room square is $Z$-cyclic if $S = \{\infty, 0, 1, \cdots, 2n-2\}$, if the top left cell contains the pair $\{\infty, 0\}$, and if, 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 modulo $2n-1$, $\infty + 1 = \infty$.

It was proved in the 1970's that a Room square of order $2n$ exists for all $n \geq 4$. We now show that many of the ideas of the previous chapter can be used to construct $Z$-cyclic Room squares; this simplifies work of Gross and Leonard

[21] on this subject. The squares constructed will all be skew as well as $Z$-cyclic; recall that, to construct such squares it is sufficient to construct skew starters in $Z_{2n-1}$. i.e. a partition $X = \{\{a_1,\ b_1\}, \{a_2,\ b_2\}, \cdots, \{a_{n-1},\ b_{n-1}\}\}$ of $Z_{2n-1} - \{0\}$ such that both

$$\{\pm(a_i - b_i);\ 1 \leq i \leq n-1\} = Z_{2n-1} - \{0\}$$

and

$$\{\pm(a_i + b_i);\ 1 \leq i \leq n-1\} = Z_{2n-1} - \{0\}$$

are satisfied.

## 5.2 Basic constructions

**Lemma 5.2.1** *Let $p_i$ be distinct primes, $\alpha_i$ be positive integers, $i = 1,\ 2, \cdots, n$. Let $p_i = 2^{m_i} \cdot u \cdot a_i + 1$ where $u$, $a_i$ are odd and h.c.f $\{a_i; i = 1, 2, \cdots, n\} = 1$ , $\ell = max\{m_i; i = 1, 2, \cdots, n\}$, $m = \sum m_i$, and let $\omega$ be a common primitive root of $p_i^{\alpha_i}$, $i = 1, 2, \cdots, n$. Then there exists $t$ such that*

1. $\omega^{2^\ell t} \equiv 1 \pmod{\prod_{i=1}^n p_i^{\alpha_i}}$;
2. $\omega^{2^{\ell-1} \cdot t} \equiv -1 \pmod{\prod_{i=1}^n p_i^{\alpha_i}}$, *if $m_i = k$ $\forall i = 1, 2, \cdots, n$ for some positive integer $k$;*
3. $\omega^j \not\equiv -1 \pmod{\prod_{i=1}^n p_i^{\alpha_i}}$ $\forall j$ *if $m_{i_1} \neq m_{i_2}$ for some $1 \leq i_1 \neq i_2 \leq n$;*
4. *if $G = \{x \in Z_{\prod_{i=1}^n p_i^{\alpha_i}}; (x, \prod_{i=1}^n p_i^{\alpha_i}) = 1\}$ then $G$ is an Abelian group of order $2^m \cdot t \cdot h$ for some $h$.*

**Proof.** *1.* Let $p_i = 2^{m_i} \cdot u \cdot a_i + 1$ where $u$, $a_i$ are odd and $h.c.f\{a_i; i = 1, 2, \cdots, n\} = 1$, Then

$$\begin{aligned} &h.c.f\{p_i^{\alpha_i - 1}(p_i - 1); i = 1, 2, \cdots, n\} \\ &= h.c.f\{(2^{m_i} \cdot u \cdot a_i + 1)^{\alpha_i - 1} \cdot 2^{m_i} \cdot u \cdot a_i;\quad i = 1, 2, \cdots, n\} \\ &= 2^\sigma \cdot u \cdot v \end{aligned}$$

where $\sigma = min\{m_i; i = 1, 2, \cdots, n\}, v = h.c.f\{(2^{m_i} \cdot u \cdot a_i + 1)^{\alpha_i - 1} \cdot a_i;\quad i = 1, 2, \cdots, n\}$;

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

where $w = l.c.m\{(2^{m_i}ua_i+1)^{\alpha_i-1}\cdot a_i/v;\ i=1,2,\cdots,n\}$ and $t = u\cdot v\cdot w$.

Let $\omega$ be a common primitive root of $p_i^{\alpha_i}$. Then the order of $\omega$ (mod $\prod_{i=1}^{n} p_i^{\alpha_i}$) is $l.c.m\{p_i^{\alpha_i-1}(p_i-1); i = 1,2,\cdots,n\} = 2^{\ell}\cdot t$, so $\omega^{2^{\ell}\cdot t} \equiv 1$ (mod $\prod_{i=1}^{n} p_i^{\alpha_i}$).

*2.* If $m_i = k\ \forall\ i = 1,2,\cdots,n$ for some positive integer $k$ then $\ell = k$ and we claim $\omega^{2^{\ell-1}\cdot t} \equiv -1 \pmod{\prod_{i=1}^{n} p_i^{\alpha_i}}$. Since $\omega$ is a common primitive root of $p_i^{\alpha_i}; i = 1,2,\cdots,n$ so

$$\omega^{p_i^{\alpha_i-1}(p_i-1)} \equiv 1 \pmod{p_i^{\alpha_i}} \qquad \text{and} \qquad \omega^{p_i^{\alpha_i-1}(p_i-1)/2} \equiv -1 \pmod{p_i^{\alpha_i}}$$

for all $i = 1,2,\cdots,n$. i.e.

$$\omega^{p_i^{\alpha_i-1}(p_i-1)} = p_i^{\alpha_i}A_i^{(1)}+1 \qquad \text{and} \qquad \omega^{p_i^{\alpha_i-1}(p_i-1)/2} = p_i^{\alpha_i}A_i^{(2)}-1$$

for some $A_i^{(1)}, A_i^{(2)};\ \ \forall i = 1,2,\cdots,n$.

So for any integer $k_i$ we have

$$\omega^{k_i p_i^{\alpha_i-1}(p_i-1)} = p_i^{\alpha_i}B_i^{(1)}+1 \qquad \text{for some} \quad B_i^{(1)}$$

In particular, we take $k_i = \frac{\frac{t}{p_i^{\alpha_i-1}ua_i}-1}{2}$ (integers) $i = 1,2,\cdots,n$. Then we have

$$\omega^{2^{\ell-1}t-\frac{p_i^{\alpha_i-1}(p_i-1)}{2}} = p_i^{\alpha_i}\cdot B_i^{(1)}+1$$

and

$$\omega^{\frac{p_i^{\alpha_i-1}(p_i-1)}{2}} = p_i^{\alpha_i}A_i^{(2)}-1 \quad i=1,2,\cdots,n$$

Therefore

$$\begin{aligned} \omega^{2^{\ell-1}\cdot t} &= (p_i^{\alpha_i}B_i^{(1)}+1)(p_i^{\alpha_i}A_i^{(2)}-1) \\ &= p_i^{\alpha_i}A_i^{(3)}-1 \qquad \text{for some} \qquad A_i^{(3)} \qquad i=1,2,\cdots,n \end{aligned}$$

$$i.e.\ \ \omega^{2^{\ell-1}\cdot t}+1=p_i^{\alpha_i}A_i^{(3)} \qquad \forall\, i=1,2,\cdots,n$$

Thus, since $p_i$, $i=1,2,\cdots,n$ are distinct primes,

$$\omega^{2^{\ell-1}\cdot t}+1=\prod_{i=1}^{n}p_i^{\alpha_i}\cdot A \qquad \text{for some } A.$$

*3.* If $m_{i_1}\neq m_{i_2}$ for some $1\leq i_1\neq i_2\leq n$ we claim that $\omega^j\not\equiv -1 \pmod{\prod_{i=1}^{n}p_i^{\alpha_i}}$ for all $j$. Suppose that there exists some $j_0$ such that $\omega^{j_0}\equiv -1 \pmod{\prod_{i=1}^{n}p_i^{\alpha_i}}$. Then $\omega^{j_0}\equiv -1 \pmod{p_{i_1}}$, $\omega^{j_0}\equiv -1 \pmod{p_{i_2}}$. But $\omega^{\frac{p_{i_1}-1}{2}}\equiv -1 \pmod{p_{i_1}}$ and $\omega^{\frac{p_{i_2}-1}{2}}\equiv -1 \pmod{p_{i_2}}$. Thus $j_0\equiv\frac{p_{i_1}-1}{2}(\mathrm{mod}(\ p_{i_1}-1))\equiv\frac{p_{i_2}-1}{2}(\mathrm{mod}(\ p_{i_2}-1))$. 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 an Abelian group with order $\varphi(\prod_{i=1}^{n}p_i^{\alpha_i})$ where

$$\begin{aligned}\varphi(\textstyle\prod_{i=1}^{n}p_i^{\alpha_i}) &= \textstyle\prod_{i=1}^{n}p_i^{\alpha_i-1}(p_i-1)\\ &= \textstyle\prod_{i=1}^{n}(2^{m_i}\cdot u\cdot a_i+1)^{\alpha_i-1}\cdot 2^{m_i}\cdot u\cdot a_i\\ &= 2^m\cdot u^n\cdot v^n\cdot\textstyle\prod_{i=1}^{n}b_i\\ &= 2^m\cdot u\cdot v\cdot w\cdot u^{n-1}\cdot v^{n-1}\cdot[\textstyle\prod_{i=1}^{n}b_i]/w\\ &= 2^m\cdot t\cdot h.\end{aligned}$$

where $h=[u^{n-1}\cdot v^{n-1}\cdot\prod_{i=1}^{n}b_i]/w$ and $b_i=(2^{m_i}\cdot u\cdot a_i+1)^{\alpha_i-1}\cdot a_i/v$ for all $i=1,2,\cdots,n$.

**Lemma 5.2.2** *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]

**Theorem 5.2.3** *If $p=2^k\cdot t+1$, where $t>1$ is odd, is a prime, $p\geq 7$, then there exists a skew strong starter in $Z_{p^\alpha}$ for $\alpha\geq 1$, and hence a skew Z-cyclic Room square of order $p^\alpha+1$.*

**Proof.** The case $\alpha=1$ follows from Lemma 5.2.2. For the induction step, let $E$ denote the reduced residue system mod $p^\alpha$, and let $\omega$ be a primitive root of $p^2$ (and hence of $p^\alpha$ for each $\alpha$), Let $d=2^{k-1}$. Then, mod $p^\alpha$, $\omega$ has order

$p^{\alpha-1}(p-1) = 2^k m = 2dm$, say, where $m$ is odd, and $\omega^{dm} \equiv -1 \pmod{p^\alpha}$. We claim that the pairs

$$(5.2.1) \qquad \{\{\omega^{i+2jd}, \omega^{i+(2j+1)d}\}; 0 \le i \le d-1,\ 0 \le j \le m-1\}$$

form a skew starter for $E$.

The differences between each pair are $\pm\omega^{2jd+i}(\omega^d - 1), 0 \le i \le d-1, 0 \le j \le m-1$ where $\omega^d \not\equiv 1 \text{mod } p$. Clearly $\omega^{2jd+i} \equiv \omega^{2Jd+I}$ if and only if $i = I$ and $j = J$. So now suppose $\omega^{2jd+i} \equiv -\omega^{2Jd+I}$. If $2jd + i < 2Jd + I$ we would have $\omega^{2jd+i}(1+\omega^{2(J-j)d+(I-i)}) \equiv 0$ so that $2(J-j)d+(I-i) = dm \pmod{2dm}$. Since $0 < 2(J-j)d + (I-i) < 2dm$, this requires $2(J-j)d + (I-i) < dm$, whence $I = i$. Thus $2(J-j) = m$ contradicting the oddness of $m$. So all the differences are distinct. The sums and their negatives are similarly distinct; the argument is the same, with $\omega^d - 1$ replaced by $\omega^d + 1$. Since $t > 1$, $\omega^d + 1 \not\equiv 0 \pmod{p}$.

Thus, for $Z_{p^\alpha}$, we take the starter in $E$ along with the pairs $\{pc_i,\ pd_i\}$ where the pairs $\{c_i,\ d_i\}$ form a starter for $Z_{p^{\alpha-1}}$.

For later reference, we denote the pairs in (*5.2.1*) by $PIR_{p^\alpha}$ (Pairs In Reduced set mod $p^\alpha$).

## 5.3 Composition Theorem

We now consider the products of primes. Let $E$ denote the reduced residue system mod $p_1^{\alpha_2} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}$. Then $|E| = \Pi_{i=1}^{i=r} p_i^{\alpha_i - 1}(p_i - 1)$. If $\omega$ is a common primitive root of $p_i^2, p_2^2, \cdots, p_r^2$, and $v = p_i^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$.

$$ord_v\omega = l.c.m\{p_i^{\alpha_i - 1}(p_i - 1); i = 1, 2, \cdots, r\} = 2^\ell t.,$$

where $t$ is odd, $\ell = max\{k_i; 1 \le i \le r\}$, and $p_i = 2^{k_i} t_i + 1$ ($t_i$ odd, $t_i > 1$).

By Lemma 5.2.1. $\omega^{2^{\ell-1}t} \equiv -1 \pmod{v}$, if $m_i = \ell \quad \forall \quad i = 1, 2, \cdots, n$, whereas if the $m_i$ are not all equal, then $\omega^j \not\equiv -1 \pmod{v}$ for each $j$.

**Case 1.** If $m_i = \ell$ for each $i$, let

$$H = \{1, \omega, \omega^2, \cdots, \omega^{2^\ell t - 1}\};$$

then $E$ has coset decomposition

$$E = c_1H \cup c_2H \cup \cdots \cup c_kH.$$

where $c_1 = 1$ and $|E| = k|H|$, and it is easy to check that the pairs

$$(5.3.1) \qquad \{\{c_h\omega^{i+2jd}, c_h\omega^{i+(2j+1)d}\}; 0 \leq i \leq d-1, 0 \leq j \leq t-1, 1 \leq h \leq k\}$$

form a skew strong starter for $E$. The proof is as for Theorem 5.2.3; again we need primes to be non-Fermat.

**Case 2.** If the $m_i$ are not all equal, take

$$H = \{\pm 1, \pm\omega, \pm\omega^2, \cdots, \pm\omega^{2^\ell t-1}\}.$$

Then $E$ has coset decomposition

$$E = c_1H \cup c_2H \cup \cdots \cup c_fH$$

where $c_1 = 1$, $|E| = f|H|$, and the pairs

$$(5.3.2) \qquad \{c_h\omega^{2i},\ c_h\omega^{2i+1}\}, \{-c_h\omega^{2i+1}, -c_h\omega^{2i+2}\}$$

are easily checked to satisfy the condition for a skew strong starter. So in either case, we obtain a skew strong starter in the reduced residue system $E$.

For later reference we denote the pairs in (5.3.1) and (5.3.2) by $PICH^{(1)}_{p_i^{\alpha_1}\cdots p_n^{\alpha_n}}$ and $PICH^{(2)}_{p_i^{\alpha_1}\cdots p_n^{\alpha_n}}$ (Pairs In Cosets of H) respectively. We also use the following notation

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

**Theorem 5.3.1** *If $p = 2^n \cdot a + 1 \geq 7$, $q = 2^m \cdot b + 1 \geq 7$, are distinct primes, and $a$, $b > 1$ are odd then there exists a skew strong starter in $Z_{p^\alpha q^\beta}$ $(\alpha, \beta \geq 1)$ and hence a Z-cyclic Room square of order $p^\alpha q^\beta + 1$.*

**Proof.** Let $\alpha$ be fixed and use induction on $\beta$. For $\beta = 1$, we have

$$Z_{p^\alpha q} = qZ_{p^\alpha} \cup \cup_{i=0}^{\alpha-1} p^i Z_{(\alpha-i,1)} \cup p^\alpha Z_q.$$

By Lemma 5.2.1 and Lemma 5.2.2 skew strong starters in $Z_q$, $Z_{p^\alpha}$ exist, say $\{c_i, d_i\}$, $\{a_i, b_i\}$ respectively. For the set $Z_{(\alpha-i,1)}$ $i = 0, 1, \cdots, \alpha-1$; the pairs $PICH_{p^{\alpha-i}}^{\chi(p,q)}$ $i = 0, 1, \cdots, \alpha-1$, have the required properties. So the required pairs for a skew strong starter in $Z_{p^\alpha q}$ are

$$\{qa_i, qb_i\}, \qquad \{p^\alpha c_i, p^\alpha d_i\} \text{ and } \quad p^i PICH_{p^{\alpha-i}}^{\chi(p,q)} \qquad i = 0, 1, \cdots, \alpha-1.$$

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

$$Z_{p^\alpha q^\beta} = qZ_{p^\alpha q^{\beta-1}} \cup \cup_{i=0}^{\alpha-1} p^i Z_{(\alpha-i,\beta)} \cup p^\alpha Z_{(0,\beta)}.$$

For the set $Z_{(\alpha-i,\beta)}$, the pairs $PICH_{p^{\alpha-i}q^\beta}^{\chi(p,q)}$ for all $i = 0, 1, \cdots, \alpha-1$ have the required properties; and for the set $Z_{(0,\beta)}$, the pairs $PIR_{q^\beta}$ have the required properties. Therefore the required pairs for a skew strong starter are

$$\{qa_i,\ qb_i\}, \quad p^i PICH_{p^{\alpha-i}q^\beta}^{\chi(p,q)} \text{ for all } \quad i = 0, 1, \cdots, \alpha-1 \quad \text{and} \quad p^\alpha PIR_{q^\beta}.$$

**Theorem 5.3.2** *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.** $Z_{pq} = qZ_p \cup Z_{(1,1)} \cup pZ_q$. Since $m \neq n$ the pairs $PICH_{pq}^{(2)}$ have the required properties, so the required pairs for a skew strong starter are the following :

$$q \cdot SST_p, \quad PICH_{pq}^{(2)} \ \textit{and} \ \ p \cdot SST_q.$$

where $SST_p, SST_q$ are skew strong starters in $Z_p, Z_q$ respectively given in Lemma 5.2.2.

**Theorem 5.3.3** *Let* $p = 2^n + 1$ *be a prime, where* $a > 1$ *odd,* $n \neq 2$. *If there exists a skew strong starter in* $Z_{5p}$ *then there is also one in* $Z_{5p^\alpha}$.

**Proof.** By hypothesis a skew strong starter exists in $Z_{5p}$ so the case $\alpha = 1$ is true. Deal with the induction step; let $p_1 = 5$, $p_2 = p$ and let the set $Z_{5p^\alpha}$ be decomposed as following:

$$\begin{aligned} Z_{5p^\alpha} &= \{x \in Z_{5p^\alpha}; p \mid x\} \cup \{x \in Z_{5p^\alpha}; 5 \nmid x, p \nmid x\} \cup 5\{x \in Z_{p^\alpha}; p \nmid x\} \\ &= pZ_{5p^{\alpha-1}} \cup Z_{(1,\alpha)} \cup 5Z_{(0,\alpha)} \end{aligned}$$

Therefore the pairs $PIR_{p^\alpha}$ and $PICH^{(2)}_{5p^\alpha}$ have the required properties and by 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

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

.

**Example 5.3.1** 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 $Z_{35}$.

**Theorem 5.3.4** *Let $p,q$ be primes where $p = 2^n a + 1 \geq 7, a > 1$ odd, $q = 2^m + 1 \geq 7$, $m \neq n$, $\alpha$ is 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 Theorem 5.3.3 with 5 replaced by $q$.

**Example 5.3.2** There exists a skew strong starter in $Z_{7^2 \cdot 17}$ and $Z_{11^2 \cdot 17}$.

**Theorem 5.3.5** *If $p_i = 2^{n_i} a_i + 1$ are primes, $a_i$, are odd, $a_i > 1, \alpha_i$ are positive integers $i = 1, 2, \cdots, r$, then there exists a skew strong in $Z_{\prod_{i=1}^r p_i^{\alpha_i}}$, and hence a Z-cyclic Room square of order $\prod_{i=1}^r p_i^{\alpha_i} + 1$*

**Proof.** Proceed by induction on $r$. The case $r = 1$ follows from Theorem 5.2.3 and the case $r = 2$ follows from Theorem 5.3.1. Now deal with the induction step; suppose that there exists a skew strong starter in $Z_{\prod_{i=1}^{r-1} p_i^{\alpha_i}}$. We want to show that there exists a skew strong starter in $Z_{\prod_{i=1}^r p_i^{\alpha_i}}$.

First consider $Z_{(\prod_{i=1}^{r-1} p_i^{\alpha_i})p_r}$, we have

$$Z_{(\prod_{i=1}^{r-1} p_i^{\alpha_i})p_r} = p_r Z_{\prod_{i=1}^{r-1} p_i^{\alpha_i}} \cup \bigcup_{(\beta_1,\beta_2,\cdots,\beta_{r-1},0)} I_{(\beta_1,\beta_2,\cdots,\beta_{r-1},0)}$$

where $I_{(\beta_1,\beta_2,\cdots,\beta_{r-1},0)} = \pi_{(\beta_1,\beta_2,\cdots,\beta_{r-1},0)} Z_{(\alpha_1-\beta_1,\cdots,\alpha_{r-1}-\ \beta_{r-1},1)}$, the union running over all $r$-tuple $(\beta_1, \beta_2, \cdots, \beta_r)$ with $0 \leq \beta_i \leq \alpha_i$ for each $1 \leq i \leq r-1$ and $\alpha_r = 1$, $\beta_r = 0$. For each $I$ we have a skew strong starter and along with them we take a starter for $Z_{\prod_{i=1}^{r-1} p_i^{\alpha_i}}$ with each element multiplied by $p_r$.

For the induction step, we consider $\alpha_r \geq 2$ and write

$$\prod_{i=1}^{r} p_i^{\alpha_i} = p_r Z_{(\prod_{i=1}^{r-1} p_i^{\alpha_i}) p_r^{\alpha_r - 1}} \cup \cup_{(\beta_1, \cdots, \beta_{r-1}, 0)} I_{(\beta_1, \cdots, \beta_{r-1}, 0)}$$

and proceed as before.

**Corollary 5.3.6** *Let* $p_i = 2^{m_i} a_i + 1 \geq 7, a_i$ *are odd,* $\alpha_i$ *are positive integers* $i = 1, 2, \cdots, n$ *and*

1. *if* $a_\ell = 1$ *then* $\alpha_\ell = 1$
2. *if* $m_{i_1} = m_{i_2} = \cdots = m_{i_k}$ *then* $a_{i_\ell} > 1 \;\; \forall \; \ell = 1, 2, \cdots, k;$

*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 5.3.3** There exists a skew strong starter in $Z_{7^2 \cdot 11 \cdot 17 \cdot 257}$. We use

$$\begin{array}{ll}
Z_{7^2 \cdot 11 \cdot 17 \cdot 257} & = 257 Z_{7^2 \cdot 11 \cdot 17} \cup \{x \in Z_{7^2 \cdot 11 \cdot 17 \cdot 257}; 7 \nmid x, 11 \nmid x, 17 \nmid x, 257 \nmid x\} \\
& \cup 17\{x \in Z_{7^2 \cdot 11 \cdot 257}; 7 \nmid x, 11 \nmid x, 257 \nmid x\} \\
& \cup 11\{x \in Z_{7^2 \cdot 17 \cdot 257}; 7 \nmid x, 17 \nmid x, 257 \nmid x\} \\
& \cup 7\{x \in Z_{7 \cdot 11 i 7 \cdot 257}; 7 \nmid x, 11 \nmid x, 17 \nmid x, 257 \nmid x\} \\
& \cup 7^2\{x \in Z_{11 i 7 \cdot 257}; 11 \nmid x, 17 \nmid x, 257 \nmid x\} \\
& \cup 11 \cdot 17\{x \in Z_{7^2 \cdot 257}; 7 \nmid x, 257 \nmid x\} \\
& \cup 7 \cdot 11\{x \in Z_{7 \cdot 17 \cdot 257}; 7 \nmid x, 17 \nmid x, 257 \nmid x\} \\
& \cup 7^2 \cdot 11\{x \in Z_{17 \cdot 257}; 17 \nmid x, 257 \nmid x\} \\
& \cup 7 \cdot 17\{x \in Z_{7 \cdot 11 \cdot 257}; 7 \nmid x, 11 \nmid x, 157 \nmid x\} \\
& \cup 7^2 \cdot 17\{x \in Z_{11 \cdot 257}; 11 \nmid x, 257 \nmid x\} \\
& \cup 7 \cdot 11 \cdot 17\{x \in Z_{7 \cdot 257}; 7 \nmid x, 257 \nmid x\} \\
& \cup 7^2 \cdot 11 \cdot 17 Z_{257}.
\end{array}$$

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

**Corollary 5.3.7** *Let* $p_i = 2^{m_i} \cdot a_i + 1 \geq 7$, $a_i$ *odd,* $\alpha_i$ *positive integers* $i = 1, 2, \cdots, n$ *satisfying the following conditions*

1. *If* $a_\ell = 1$ *for some* $\ell \in \{1, 2, \cdots, n\}$ *then* $\alpha_\ell = 1$.
2. *If* $m_{i_1} = m_{i_2} = \cdots = m_{i_k} \quad i_j \in \{1, 2, \cdots, n\}$ *then* $a_{i_j} > 1 \;\; \forall j = 1, 2, \cdots, k$.
3. *Suppose* $m_i \neq 2 \quad (i = 1, 2, \cdots, n)$.
4. *Suppose there exists a (skew) strong starter in* $Z_{5 \cdot p_i}$ *for all* $i = 1, 2, \cdots, n-1$.

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

$$\begin{aligned} Z_{5\cdot 7^2\cdot 11} &= 11Z_{5\cdot 7^2} \cup 7\{x \in Z_{5\cdot 7\cdot 11}; 5 \nmid x, 7 \nmid x, 11 \nmid x\} \cup \\ & \quad 7^2\{x \in Z_{5\cdot 11}; 5 \nmid x, 11 \nmid x\} \cup 5\{x \in Z_{7_2\cdot 11}; 7 \nmid x, 11 \nmid x\} \cup \\ & \quad 5 \cdot 7\{x \in Z_{7\cdot 11}; 7 \nmid x, 11 \nmid x\} \cup 5 \cdot 7^2 Z_{11}. \end{aligned}$$

and

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

# Bibliography

[1] I. Anderson. *Combinatorial designs.* Ellis Horwood, Chichester (1991)

[2] I. Anderson and N. J. Finizio. Cyclic whist tournaments. *Discrete Math.*. **125** (1994): 5–10.

[3] I. Anderson, S. D. Cohen and N. J. Finizio. An existence theorem for cyclic triple whist tournaments. *Discrete Math.* to appear.

[4] I. Anderson and N. J. Finizio. A generelization of a construction of E. H. Moore. *Bulletin I. C. A.*. **6** (1992):39–46.

[5] I. Anderson and N. J. Finizio. An infinite class of cyclic whist tournaments. *Congressus Numeratium.* **91** (1992):7–18.

[6] I. Anderson and Y. S. Liaw. Z-cyclic Room squares. *Bulletin I. C. A.*. **5** (1992): 51–57

[7] I. Anderson and N. J. Finizio. Cyclically resolvable designs and triple whist tournaments. *J. Combinatorial Designs.* **1** (1993): 347–358.

[8] I. Anderson and N. J. Finizio. Cohen's theorem and Z-cyclic whist tournaments. *Ars Combinatoria.* to appear

[9] I. Anderson and N. J. Finizio. Many more Z-cyclic whist tournaments. *Congressus Numeratium.* **94** (1993):123–129.

[10] I. Anderson and N. J. Finizio. Mann's lemma and Z-cyclic whist tournaments. *Ars Combinatoria.* to appear.

[11] I. Anderson, G. W. Hamilton and A. J. W. Hilton. Referee squares, preprint.

[12] T. M. Apostol. *Introduction to analytic number theory.* Springer (1976)

[13] T. D. Beth, D. Jungnickel and H. Lenz. *Design Theory.* Cambridge University Press, Cambridge (1985).

[14] R. D. Baker, Whist tournaments. Proc. 6th S. E. Coference on Combinatorics, Graph theory and Computing. *Congressus Numeratium.* **14** (1975): 89–100.

[15] R. C. Bose. On the construction of balanced incomplete block designs. *Ann. Eugenics.* **9** (1939): 353–399.

[16] R. C. Bose and J. M. Cameron. The bridge tournament problem and calibration designs for comparing pairs of objects. *J. Res. Nat. Bureau Standards.* **69** B (1965): 323–332.

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

[18] S. D. Cohen. Primitive roots and powers among values of polynomials over finite fields. *Journal für die reine und angewandte Math.* (Crelle's Journal)**350** (1984):137–151.

[19] J. H. Dinitz and D. R. Stinson. *Contemporary Design Theory.* Wiley (1992).

[20] K. B. Gross. Some new classes of strong starters. *Discrete Math..* **12** (1975):225–243.

[21] K. B. Gross and P. A. Leonard. The existence of strong starters in cyclic groups *Utilitas Mathematica* **7** (1975): 187–195.

[22] M. Hall. *Combinatorial theory (2nd edition).* Wiley (1986).

[23] H. Hanani, The existence and construction of balanced incomplete block designs. *Ann. Math. Stat..* **32** (1961): 361–386.

[24] H. Hanani, D. K, Ray-Chaudhuri and R. M. Wilson. On resolvable designs. *Discrete Math.* **3** (1972): 343–357.

[25] J. D. Horton. Quintuplication of Room squares. *Aequat. Math.* **7** (1971):243–245.

[26] T. P. Kirkman. Note on an unanswered prize question. *Cambridge and Dublin Math. J..* **5** (1850):255–262.

[27] W. L. Kocay, D. R. Stinson and S. A. Vanstone. On strong starters in cyclic groups. *Discrete Math.* **56**, (1985):45–60.

[28] R. Lidl and H. Niederreiter. *Finite fields.* Encyclopaedia of mathematics Vol. 20, Cambridge University Press. .

[29] H. B. Mann *Analysis and designs of experiments* Dover 1949.

[30] E. H. Moore Tactical memoranda I-III. *American J. Math.* **18** (1896): 264–303.

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

[32] R. C. Mullin and E. Nemeth, On furnishing room squares, *J. Combinatorial Theory* **7** (1969):266–272.

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

[34] K. T. Phelps and A. Rosa. Steiner triple systems with rotational automorphisms. *Discrete Math..* **33** (1981): 57–66.

[35] T. G. Room, A new type of magic square. *Math. Gaz.* **39** (1955): 307.

[36] T. Storer, Cyclotomy in G. D. $(p^{\alpha}q^{\beta}r^{\gamma})$. *Portugaliae Mathematica.* **26** (1967). 83–91.

[37] W. D. Wallis. *Combinatorial Designs.* Marcel Dekker, (1988).

[38] W. D. Wallis, A. P. Street and J. S. Wallis. *Combinatorics: Room squares, Sum-free sets, Hadamard matrices.* Lecture Notes in Math. **292** Springer.

[39] G. L. Watson. Bridge problem. *Math. Gazette.* **38** (1954):129–130.

[40] A. L. Whiteman. A family of difference sets. *Illinois J. Math..* **6** (1962): 107–121.