Mann's Lemma and Z-Cyclic Whist Tournaments

Ian Anderson
Department of Mathematics
University of Glasgow
Glasgow, Scotland G12 8QW

Norman J. Finizio
Department of Mathematics
University of Rhode Island
Kingston, RI 02881

Abstract. The main result of this study is that if q, p are primes such that $q \equiv 3 \pmod 4$, $q \geq 7$, $p \equiv 1 \pmod 4$, $\text{hcf}(q-1, p^{n-1}(p-1)) = 2$ and if there exists a Z-cyclic Wh$(q+1)$ then a Z-cyclic Wh(qp^n+1) exists for all $n \geq 0$. As an ingredient sufficient for this result we prove a version of Mann's Lemma in the ring Z_{qp^n}.

1. Introduction

The whist tournament problem for v players was introduced into the mathematical literature nearly 100 years ago by E.H. Moore [8]. Solutions to the whist tournament problem are known to exist [2], [6] for all $v \equiv 0, 1 \pmod 4$. For some history related to this problem see [2], [4]. In this paper we concentrate on $v \equiv 0 \pmod 4$.

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

(i) the games are arranged in $4n-1$ rounds, each of n games;
(ii) each player plays in one game in each round;
(iii) each player partners every other player exactly once;
(iv) each player opposes every other player exactly twice.

Games are denoted by 4-tuples (a, b, c, d) with a, c partners and b, d partners. Whenever the v-set is $Z_{4n-1} \cup \{\infty\}$ and each round can be obtained by adding $1 \pmod{4n-1}$ to each non-∞ element of the previous round we say that the Wh(v) is Z-cyclic.

Infinite classes of Z-cyclic Wh(v) are rare in the literature. G.L. Watson [9] establishes Z-cyclic Wh $\left(\prod_{i=1}^{m} p_i\right)$, where each prime p_i is of the form $p_i \equiv 1 \pmod 4$ and the present authors [3] establish Z-cyclic Wh$(3p^n+1)$ for all prime $p \equiv 1 \pmod 4$ and $n \geq 0$, and also Z-cyclic Wh(qp^n+1) for some specific primes q, p, $q \equiv 3 \pmod 4$, $p \equiv 1 \pmod 4$, $n \geq 0$. Here we prove that if p, q are primes, $q \equiv 3 \pmod 4$, $q \geq 7$, $p \equiv 1 \pmod 4$, $\text{hcf}(q-1, p^{n-1}(p-1)) = 2$ and if there exists a Z-cyclic Wh$(q+1)$ then there exists a Z-cyclic Wh(qp^n+1) for all $n \geq 0$. This is Theorem 2.1 of Section 2 which also contains several pertinent lemmas including a version of Mann's Lemma in the ring Z_{qp^n}. Several illustrations of Theorem 2.1 are presented in Section 3. Henceforth we assume that q, p are primes, $q \equiv 3 \pmod 4$, $q \geq 7$, $p \equiv 1 \pmod 4$.

For Z-cyclic Wh(v) it is enough to indicate the tables (games) for an initial round. Of course for such designs the set of rounds is a cyclic set and any round can be the initial round. We adhere to the convention that the initial round is that for which ∞ and 0 are partners. With each table (a, b, c, d) there are four (4) partner differences $\pm(a-c)$, $\pm(b-d)$ and eight (8) opponent differences $\pm(b-a), \pm(d-c), \pm(d-a), \pm(c-b)$. Any differences involving ∞ are to be ignored. A collection of n tables constitute an initial round of a Z-cyclic Wh($4n$) if and only if the n tables form a parallel class for $Z_{4n-1} \cup \{\infty\}$ and the partner differences cover each non-zero element of Z_{4n-1} exactly once and the opponent differences cover each non-zero element of Z_{4n-1} exactly twice [2].

Example 1.1: (a) An initial round for a Z-cyclic Wh(8) is given by

$$(\infty,4,0,5), \quad (1,2,3,6).$$

(b) An initial round for a Z-cyclic Wh(12) is given by

$$(\infty,8,0,2), \quad (1,5,4,6), \quad (7,10,9,3).$$

2. Some Useful Lemmas and the Main Theorem

In the ring Z_{p^n}, p a prime, a primitive root of p^n is defined to be any non-zero element $W \in Z_{p^n}$ that satisfies the conditions $(W, p) = 1$ and $\text{ord}_{p^n} W = \varphi(p^n) = p^{n-1}(p-1)$. Primitive roots were found useful in [3] to establish infinite classes of Z-cyclic Wh(v). While we do not have a primitive root in the ring Z_{qp^n}, the following lemma demonstrates a maximum possible order.

Lemma 2.1. *If W is a primitive root of both q and p^n then*

$$\text{ord}_{qp^n} W = (q-1)p^{n-1}(p-1)/\text{hcf}(q-1, p^{n-1}(p-1)).$$

Proof:

$$\begin{aligned}\text{ord}_{qp^n} W &= \text{lcm}(\text{ord}_q W, \text{ord}_{p^n} W) = \text{lcm}(q-1, p^{n-1}(p-1)) \\ &= (q-1)p^{n-1}(p-1)/\text{hcf}(q-1, p^{n-1}(p-1))\end{aligned}$$

∎

It is well known [1] that if W is a primitive root of p^2 then W is a primitive root of p^n for all $n \geq 1$. Throughout the remainder of this paper we assume that $\text{hcf}(q-1, p^{n-1}(p-1)) = 2$ and that W is a primitive root of both q and p^2, (If a, b are primitive roots of p^n, q respectively, then by the Chinese remainder theorem, there exists W such that $W \equiv a \pmod{p^n}$ and $W \equiv b \pmod q$; this W is a common primitive root.) Define t and s by $4t = \frac{1}{2}(q-1)p^{n-1}(p-1)$ and $4s = p^{n-1}(p-1)$ respectively. Then $4t$ is the order of $W \pmod{qp^n}$.

Lemma 2.2. $W^i \not\equiv -1 \pmod{qp^n}$ *for all* $0 \leq i \leq 4t-1$.

Proof: Suppose that $W^i \equiv -1 \pmod{qp^n}$ for some i, $0 \leq i \leq 4t-1$; then $W^i \equiv -1 \pmod{q}$ and $W^i \equiv -1 \pmod{p^n}$. It follows that $i \equiv \frac{q-1}{2} \pmod{q-1}$ and $i \equiv \frac{1}{2}p^{n-1}(p-1) \pmod{p^n(p-1)}$. These give a contradiction since the first requires i to be odd, the second, i even. ∎

In Z_{qp^n}, P is to denote the set of all multiples of p (excluding 0), Q the set of all multiples of q (excluding 0), $Q^* = Q - (Q \cap P)$, and E is the set of all non-zero elements that are coprime to both p and q. Clearly $|P| = qp^{n-1} - 1$, $|Q^*| = p^{n-1}(p-1)$, and $|E| = 8t$. By Lemma 2.2 we can take E to be the union of two disjoint cyclic sets, $A = \{1, W, W^2, \ldots, W^{4t-1}\}$ and $B = \{-1, -W, -W^2, \ldots, -W^{4t-1}\}$.

Lemma 2.3. *The set* Q^* *is a cyclic set* $\{q_1, q_2, \ldots, q_{4s}\}$ *where*

(i) $q_{i+1} = Wq_i$ *for all* $1 \leq i \leq 4s-1$ *and* $W_{q_{4s}} = q_1$, *and*
(ii) $q_{i+2s} + q_i \equiv 0 \pmod{qp^n}$ *for all* $1 \leq i \leq 4s$.

Proof: Since W is coprime to p, $W^i q \in Q^*$ for all $0 \leq i \leq 4s-1$. Set $q_1 = q$ and $q_{i+1} = W_{q_i}$, $1 \leq i \leq 4s-1$. Since W is a primitive root of p^n we have

(a) $W^{4s} \equiv 1 \pmod{p^n}$ and
(b) $W^{2s} \equiv -1 \pmod{p^n}$.

From (a) we obtain $W^{4s}q \equiv q \pmod{qp^n}$ and from (b) we have $W^{2s}q \equiv -q \pmod{qp^n}$. ∎

In Lemmas 2.4 and 2.5 liberal use is made of the fact that $\operatorname{ord}_p W = p-1$ and $\operatorname{ord}_q W = q-1$.

Lemma 2.4. *If* α *is odd then*

(i) $W^\alpha - 1$ *is coprtme to both* p *and* q, *and*
(ii) $W^\alpha + 1$ *is coprime to* p *and is a multiple of* q *if and only if* α *is an odd multiple of* $\frac{q-1}{2}$.

Proof:

(i) $W^\alpha\lambda - 1 \equiv 0 \pmod{p} \Leftrightarrow \alpha = k(p-1)$, a contradiction since α is odd, $p-1$ is even. $W^\alpha - 1 \equiv 0 \pmod{q} \Leftrightarrow \alpha = k(q-1)$, a similar contradiction.
(ii) $W^\alpha + 1 \equiv 0 \pmod{p} \Leftrightarrow \alpha = k(\frac{p-1}{2})$, k odd $\Rightarrow \alpha$ even; contradiction. $W^\alpha + 1 \equiv 0 \pmod{q} \Leftrightarrow \alpha = k(\frac{q-1}{2})$, k odd. ∎

Lemma 2.5. *If* α *is even then*

(i) $W^\alpha - 1$ *is a multiple of* p *if and only if* α *is a multiple of* $p-1$,
(ii) $W^\alpha - 1$ *is a multiple of* q *if and only if* α *is a multiple of* $q-1$,
(iii) $W^\alpha + 1$ *is a multiple of* p *if and only if* α *is an odd multiple of* $\frac{p-1}{2}$, *and*
(iv) $W^\alpha + 1$ *is coprime to* q.

Proof:

(i) "only if": $\alpha \equiv 0 \pmod{p-1} \Rightarrow \alpha = k(p-1) \Rightarrow W^\alpha - 1 = (W^{p-1})^k - 1 \equiv 1^k - 1 \pmod{p} \equiv 0 \pmod{p}$. "if": $W^\alpha - 1 \equiv 0 \pmod{p} \Rightarrow \alpha = k(p-1)$.

(ii) $W^\alpha - 1 \equiv 0 \pmod{q} \Leftrightarrow \alpha = k(q-1)$.

(iii) $W^\alpha + 1 \equiv 0 \pmod{p} \Leftrightarrow \alpha = k(\frac{p-1}{2})$, k odd.

(iv) $W^\alpha + 1 \equiv 0 \pmod{q} \Leftrightarrow \alpha = k(\frac{q-1}{2})$, k odd $\Rightarrow \alpha$ odd; contradiction. ∎

Consider the following subsets of Z_{4t}.

$$W_1 = \left\{x\colon x \text{ is a multiple of } \frac{p-1}{2}\right\} \backslash \{0\},$$
$$W_2 = \left\{x\colon x \text{ is a multiple of } \frac{q-1}{2}\right\} \backslash \{0\}.$$

Note that $|W_1 \cup W_2 \cup \{0\}| = (q-1)p^{n-1} + (p-1)p^{n-1} - 2p^{n-1}$. Set

$$Z^* = Z_{4t} - (W_1 \cup W_2 \cup \{0\}),$$

then $|Z^*| = \frac{1}{2}p^{n-1}(p-3)(q-3) \geq 4$. Further note that W_1 contains only even integers, W_2 contains one more odd integer than even integers and $|W_1 - (W_1 \cap W_2)| = p^{n-1}(q-3) \geq 4$. We conclude that Z^* contains at least four (4) more odd integers than even integers.

The following lemma appears in [7] and has come to be known as Mann's Lemma.

Lemma. *Let $4u + 1$ be a power of a prime and let x be a primitive element of $GF(4u+1)$. Then there exist odd integers c, d such that*

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

Combining the material commencing with Lemma 2.2 we can prove the following version of Mann's Lemma for the set E.

Lemma 2.6. *There exists at least one pair of odd integers (α, β) such that $\alpha, \beta \in Z^*$ and either*

$$W^\alpha + 1 \equiv W^\beta(W^\alpha - 1) \pmod{qp^n}, \tag{2.1}$$

or

$$W^\alpha - 1 \equiv -W^\beta(W^\alpha + 1) \pmod{qp^n}. \tag{2.2}$$

Proof: Let $\alpha \in Z^*$ then both $W^\alpha + 1$, $W^\alpha - 1$ belong to E. We consider two cases.

Case 1. $W^\alpha+1, W^\alpha-1$ both belong to A or both belong to B. In either situation there exists a unique $\beta \neq 0$ such that $W^\alpha + 1 \equiv W^\beta(W^\alpha - 1) \pmod{qp^n}$. Hence $W^\beta + 1 \equiv W^\alpha(W^\beta - 1) \pmod{qp^n}$. Now $W^\beta - 1$ must belong to either P, Q^*, or E and likewise for $W^\beta + 1$. If $W^\beta - 1 \in P$ then so is $W^\alpha\,(W^\beta - 1)$ and hence so is $W^\beta + 1$ which leads to the contradiction that two multiples of p differ by 2. If $W^\beta - 1 \in Q^*$ then by Lemma 2.3, $W^\alpha(W^\beta - 1) \in Q^*$ and we are led to a similar contradiction. Thus both $W^\beta - 1, W^\beta + 1$ belong to E (in fact both belong to the same set A or B) and $\beta \in Z^*$.

Case 2. $W^\alpha + 1, W^\alpha - 1$ belong to opposite sets, say $W^\alpha + 1 \in A, W^\alpha - 1 \in B$. Then there exists a unique $\beta \neq 0$ such that $W^\alpha - 1 \equiv -W^\beta(W^\alpha + 1) \pmod{qp^n}$. Hence $W^\beta - 1 \equiv -W^\alpha(W^\beta + 1) \pmod{qp^n}$ and we can argue as in Case 1 to conclude that $\beta \in Z^*$.

Thus there is a unique pairing (α, β) of elements in Z^* and since Z^* contains at least four (4) more odd integers than even integers, there must be at least two (2) pairs (α, β) for which both are odd integers. ∎

Lemma 2.7. $s \in Z^*$.

Proof: By definition s is an odd multiple of $\frac{p-1}{4}$ and therefore cannot belong to W_1. If $s \in W_2$ there must exist an integer k such that $s = k(\frac{q-1}{2})$. Thus $p^{n-1}(p-1) = 2k(q-1)$ and we conclude that $q-1$ must divide $p^{n-1}(p-1)$ which is a contradiction since $q \geq 7$ and $\mathrm{hcf}(q-1, p^{n-1}(p-1)) = 2$. ∎

Lemma 2.8. $q(W^s - 1) \equiv W^s q(W^s + 1) \pmod{qp^n}$.

Proof: From Lemma 2.7 we conclude that $q(W^s + 1), q(W^s - 1) \in Q^*$. The congruence follows by applying Lemma 2.3(ii). ∎

We are now in a position to prove the main result of this paper.

Theorem 2.1. *If* $p \equiv 1 \pmod 4$ *and* $q \equiv 3 \pmod 4$ *are primes such that* $q \geq 7$ *and* $\mathrm{hcf}(q-1, p^{n-1}(p-1)) = 2$ *and if a* Z*-cyclic* $\mathrm{Wh}(q+1)$ *exists, then a* Z*-cyclic* $\mathrm{Wh}(qp^n+1)$ *exists for all* $n \geq 0$.

Proof: The proof is by induction on n. The case $n = 0$ yields to the Z-cyclic $\mathrm{Wh}(q+1)$. In the general case we provide separate constructions for the sets $P \cup \{0, \infty\}$, Q^*, and E. Let W be a primitive root of both q and p^2. For the set E take $\alpha \in Z^*$ such that (α, β) form a pair of odd integers guaranteed by Lemma 2.6. As initial round for the elements of E form the $2t$ tables $(1, W^\alpha, -1, -W^\alpha)$ times $1, W^2, W^4, \ldots, W^{4t-2}$. The partnership differences are $\pm 2, \pm 2W^\alpha$ times $1, W^2, W^4, \ldots, W^{4t-2}$. Now $2, 2W^\alpha$ belong to the same set, say A, and -2, $-2W^\alpha$ belong to the other set, B. Since α is odd the parity of $2W^\alpha$ as an element in A is opposite to the parity of 2 as an element in A. Consequently the differences $2, 2W^2, 2W^4, \ldots, 2W^{4t-2}$ cover all elements of A of one parity and the differences $2W^\alpha, 2W^{\alpha+2}, 2W^{\alpha+4}, \ldots, 2W^{\alpha+4t-2}$ cover all elements of A of opposite parity. Similarly for -2, $-2W^\alpha$ in the set B. Thus the partnership difference condition is satisfied for the set E. Opponent differences are $\pm(W^\alpha - 1)$ times $1, W^2, W^4, \ldots, W^{4t-2}$ (twice) and $\pm(W^\alpha + 1)$ times $1, W^2, W^4, \ldots, W^{4t-2}$ (twice). From Lemma 2.6 one of (2.1), (2.2) must hold and either one indicates that as elements in A, B the parity of $W^\alpha + 1$ is opposite to that of $W^\alpha - 1$ since β is odd. Thus we can argue just as in the partnership case to conclude that the opponent difference condition is satisfied for the set E. As initial round for the set Q^* take the s tables $(q, qW^s, qW^{2s}, qW^{3s})$ times $1, W^2, \ldots, W^{s-1}$. By Lemma 2.3 the basic table has the structure $(q, qW^s, -q, -qW^s)$. The partnership differences are $\pm 2q$, $\pm 2qW^s$ times $1, W^2, \ldots, W^{s-1}$. Thus the partnership difference condition is satisfied since if $2q = q_i$ then $2qW^s = q_{i+s}$, $-2q = q_{i+2s}$, and $-2qW^s = q_{i+3s}$. Opponent differences are $\pm q(W^s - 1)$ times $1, W, W^2, \ldots, W^{s-1}$ (twice) and $\pm q(W^s + 1)$ times $1, W, W^2, \ldots, W^{s-1}$ (twice). Invoking Lemma 2.8 we can verify the opponent difference condition just as in the partnership case. As initial round for the set $P \cup \{0, \infty\}$ we take the initial round of a Z-cyclic Wh$(qp^{n-1} + 1)$ and multiply each non-∞ element by p. As initial round for the Z-cyclic Wh$(qp^n + 1)$ form the union of the initial rounds for E, Q^*, and $P \cup \{0, \infty\}$. ∎

3. Specific Wh(v)

If one wishes to construct a specific Wh(v) using Theorem 2.1 there are two major drawbacks. One drawback is the paucity of known Z-cyclic Wh$(q+1)$. At present solutions are known only for $q = 7, 11, 19, 23,$ and 31. Secondly there are two obvious computational complexities, namely the determination of a common primitive root of q and p^2 and the determination of a pair (α, β) needed for the construction. v must be very small in order for these tasks to be amenable to hand calculation. On the other hand, for reasonable v both tasks are routine with the use of a computer.

The Wh(v) produced by Constructions 1 and 2 in [5] can all be obtained from Theorem 2.1. Indeed Construction 1 is associated with $\alpha = 1$. For the cases covered by Construction 2 and some additional cases consult the table below.

Example 3.1: The simplest case which serves to illustrate Theorem 2.1 is that of $q = 7, p = 5$ with $W = 3$. In the case $n = 1$ there are four solutions corresponding to $(\alpha, \beta) = (1,7), (5,11), (7,1), (11,5)$. Note that although as a pairing in Z^*, $(\alpha, \beta) = (\beta, \alpha)$, (α, β) yields a different Wh(v) than does (β, α) whenever $\alpha \neq \beta$. Listed below are solutions for $n = 1, 2, 3, 4$. In cases $n = 2, 3, 4$ we provide only the initial tables (in condensed form) for the sets Q^* and E. For the set $P \cup \{0, \infty\}$ we take the Wh(v) for the previous value of n and multiply each non-∞ element by p.

$n = 1$ $(\alpha, \beta) = (1,7)$ {Congruence 2.2 holds}, $(t, s) = (3.1)$.

$$E: (1,3,34,32), \quad (9,27,26,8), \quad (11,33,24,2),$$
$$(29,17,6,18), \quad (16,13,19,22), \quad (4,12,31,23).$$
$$Q^*: (7,21,28,14).$$
$$P \cup \{0,\infty\}: \quad (\infty,20,0,25), \quad (5,10,15,30)$$

{see Example 1.1(a)}.

$n = 2$ $(\alpha, \beta) = (1,7)$ {Congruence 2.2 holds}, $(t, s) = (15,5)$.

$$E: \ (1,3,174,172) \quad \text{times} \quad 1, W^2, W^4, \ldots, W^{58}$$
$$Q: (7,126,168,49) \quad \text{times} \quad 1, W, W^2, W^3, W^4.$$

$n = 3$ $(\alpha, \beta) = (1,7)$ {Congruence 2.2 holds}, $(t, s) = (75,25)$.

$$E: \ (1,3,874,872) \quad \text{times} \quad 1, W^2, W^4, \ldots, W^{298}.$$
$$Q: (7,476,868,399) \quad \text{times} \quad 1, W, W^2, \ldots, W^{24}.$$

$n = 4$ $(\alpha, \beta) = (1,7)$ {Congruence 2.2 holds}, $(t, s) = (375,125)$.

$$E: \ (1,3,4374,4372) \quad \text{times} \quad 1, W^2, W^4, \ldots, W^{1498}$$
$$Q: (7,3101,4386,1274) \quad \text{times} \quad 1, W, W^2, \ldots, W^{124}.$$

Example 3.2: For the case $q = 11, p = 5$, $\text{hcf}(q-1, p^{n-1}(p-1)) = 2$ if and only if $n = 1$. Hence for this choice of (q, p) we cannot obtain an infinite class of solutions via the construction of Theorem 2.1. Nevertheless this construction can be employed with $W = 2$, to obtain a Z-cyclic Wh(56).

$n = 1$ $(\alpha, \beta) = (3,9)$ {Congruence 2.1 holds}, $(t, s) = (5,1)$.

$$E: (1,8,54,47) \quad \text{times} \quad 1, W^2, W^4, \ldots, W^{18}$$
$$Q^*: (11,22,44,33)$$
$$P \cup \{0,\infty\}: \quad (\infty,40,0,10), \quad (5,25,20,30), \quad (35,50,45,15)$$

{see Example 1.1(b)}.

v	q	p	n	W	α	β	Congruence
624	7	89	1	3	5	5	2.1
792	7	113	1	3	7	97	2.2
804	11	73	1	5	7	261	2.2
852	23	37	1	2	5	7	2.2
960	7	137	1	3	7	331	2.2
980	11	89	1	3	7	339	2.1
1860	11	13	2	2	3	609	2.1
2024	7	17	2	3	5	131	2.1
3888	23	13	2	7	3	453	2.2
5492	19	17	2	3	3	1075	2.2
5888	7	29	2	3	1	781	2.2
6648	23	17	2	5	1	1713	2.2
8960	31	17	2	3	3	1781	2.1

Table 3.1

References

1. Allenby, R.B.J.T. and E.J. Redfern, "Introduction to Number Theory with Computing", Edward Arnold, 1989.
2. Anderson, I., "Combinatorial Designs", Prentice-Hall, Englewood Cliffs, NJ, 1990.
3. Anderson, I. and N.J. Finizio, *Cyclic whist tournaments*, Discrete Math.. (to appear).
4. Baker, R., *Whist tournaments*, Proc. Sixth Southeastern Conference on Combinatorics, Graph Theory, and Computing, Florida Atlantic University (1975), 89–100.
5. Finizio, N.J., *Cyclic whist tournaments—Part 1*. (submitted).
6. Hartman, A., *Resolvable designs*, M.Sc. Thesis, Technion, Israel (1978).
7. Mann, H.B., "Analysis and Design of Experiments", Dover Publications Inc., New York, 1949.
8. Moore, E.H., *Tactical memoranda I–III*, Amer. J. Math. **18** (1896), 264–303.
9. Watson, G.L., *Bridge problem*, Math. Gazette **38** (1954), 129–130.