Some new non-cyclic Latin squares that have cyclic and Youden properties

P.J. Owens
Department of Mathematical & Computing Sciences
University of Surrey, Guildford GU2 5XH, UK

D.A. Preece
Institute of Mathematics and Statistics, Cornwallis Building
The University, Canterbury, Kent CT2 7NF, UK

ABSTRACT. This note gives what is believed to be the first published example of a symmetric 11×11 Latin square which, although not cyclic, has the property that the permutation between any two rows is an 11-cycle. The square has the further property that two subsets of its rows constitute 5×11 Youden squares. The note shows how this 11×11 Latin square can be obtained by a general construction for $n \times n$ Latin squares where n is prime with $n \geq 11$. The permutation between any two rows of any Latin square obtained by the general construction is an n-cycle; two subsets of $(n-1)/2$ rows from the Latin square constitute Youden squares if $n \equiv 3 \pmod 8$.

1 Introduction

A *Latin square* of order n is an $n \times n$ array whose entries come from a set of n symbols, such that every symbol occurs once in each row and once in each column. We shall take the symbols to be $0, 1, 2, \ldots, n-1$ and also number the rows and columns from 0 to $n-1$. For general information on Latin squares see [1], the standard reference work.

A Latin square is said to be *based on a group* G if it becomes a Cayley table of G when suitable borders are added. A group is cyclic if a minimum set of generators consists of just one element and a Latin square based on a cyclic group is called a *cyclic* Latin square. In the simplest type of cyclic Latin square of order n the entry in cell (i,j) is equal to $i+j \pmod n$. This Latin square becomes the addition table modulo n when borders in natural order $0, 1, 2, \ldots, n-1$ are supplied.

ARS COMBINATORIA 44(1996), pp. 137-148

A *Youden square* of size $m \times n$, where $m < n$, is an array of m rows and n columns whose entries come from a set of n symbols with the following two properties:

(Y1) Every symbol occurs once in each row and at most once in each column.

(Y2) Every pair of symbols occurs in the same number of columns.

The sets of symbols in the columns of a Youden square constitute the blocks of a symmetric balanced incomplete block design. For a review of the literature on Youden squares, see Preece [7].

A permutation of n symbols is called *cyclic* if it is composed of a single n-cycle.

In this paper we are interested in Latin squares with the following property:

(P1) The permutation from row i_1 to row i_2 is cyclic, for all i_1 and all $i_2 \neq i_1$.

Every cyclic Latin square of prime order has property P1 and also has the corresponding property for columns. On the other hand, no Latin square of composite order based on a group has property P1.

Dénes and Keedwell [2] and Keedwell [3] show that, for all $n \geq 7$, there exists a non-cyclic Latin square of order n such that the permutations from column 0 to all other columns are cyclic. The transpose of such a Latin square has the corresponding property for rows. However, this property is much weaker than P1. The present note is believed to be the first publication to give Latin squares which, although not cyclic, have property P1.

From here onwards, except where otherwise stated, n is any prime not less than 11. Also, r denotes any primitive root (mod n) and $k = \frac{1}{2}(n-1)$. The entries in cell (i,j) of Latin squares L and M are denoted by $l(i,j)$ and $m(i,j)$, respectively. The n symbols will be treated as the elements of the Galois field $GF(n)$. Arithmetical operations may be performed on them so that, for instance, $n-1$ and $\frac{1}{2}(n+1)$ may be written as -1 and $\frac{1}{2}$ respectively. Moreover, equality will always be modulo n.

2 Construction and Proofs

Since n is prime and r is a primitive root (mod n), the symbols can be arranged in the order $0, 1, r, r^2, \ldots, r^{n-2}$, where $r^{n-1} = 1$. Take the addition table of $GF(n)$, with the borders arranged in this order, and let L be the

cyclic Latin square that remains when the borders are deleted. The entries of L are as follows:

$$l(0,0) = 0,$$
$$l(i,0) = l(0,i) = r^{i-1},$$
$$l(i,j) = r^{i-1} + r^{j-1},$$

for $1 \leq i \leq n-1$ and $1 \leq j \leq n-1$. Besides having property P1, L has properties P2, P3 as follows:

(P2) L is symmetric.

(P3) Every left to right broken diagonal of L', except one, contains all the non-zero symbols in the cyclic order $1, r, r^2, \ldots, r^{n-2}$. The exceptional diagonal contains only zeros.

Here, L' denotes the array that remains when row 0 and column 0 are deleted from L. Property P3 follows from the identity $l(i+1,j+1) = rl(i,j)$ which holds for all non-zero i and j provided that $i+1$ (or $j+1$) is taken to be 1 when i (or j) is $n-1$, in accordance with the fact that $r^{n-1} = 1$.

Now convert L into a new $n \times n$ array M by means of the following transformation T. Take the three left to right broken diagonals of L' whose entries in its top row are 2, $\frac{1}{2}$, -1 and permute these diagonals so that these entries become $\frac{1}{2}$, -1, 2 respectively. Then M is a Latin square with properties P1, P2 and P3 but is not based on a group.

Table 1 shows M when $n = 11$ and $r = 2$. For these values of n and r, the entries -1 and $\frac{1}{2}$ are 10 and 6 respectively. The underlined entries are those that have been changed by T. It is easy to check that M has the properties stated above. For instance, the entries marked with asterisks show that M fails the quadrangle criterion [1, p.18] and therefore M is not based on a group.

0*	1*	2	4	8	5	10	9	7	3	6
1*	<u>6</u>*	3	5	9	<u>10</u>	0	<u>2</u>	8	4	7
2	3	<u>1</u>	6	10	7	<u>9</u>	0	<u>4</u>	5	8
4	5	6	<u>2</u>	1*	9	3	<u>7</u>	0*	<u>8</u>	10
8	9	10	1	<u>4</u>	2	7	6	<u>3</u>	0	<u>5</u>
5	<u>10</u>	7	9	2*	<u>8</u>	4	3	1*	<u>6</u>	0
10	0	<u>9</u>	3	7	4	<u>5</u>	8	6	2	<u>1</u>
9	<u>2</u>	0	<u>7</u>	6	3	8	<u>10</u>	5	1	4
7	8	<u>4</u>	0	<u>3</u>	1	6	5	<u>9</u>	10	2
3	4	5	<u>8</u>	0	<u>6</u>	2	1	10	<u>7</u>	9
6	7	8	10	<u>5</u>	0	<u>1</u>	4	2	9	<u>3</u>

Table 1

We now turn to the general proofs. First, it is trivial that property P3 of L is preserved in M. The other properties of M are proved in three theorems.

Theorem 1. *M is a Latin square and is symmetric.*

Proof: The effect of T is merely to permute three entries in each row of L except row 0, so M is row Latin [1, p.104].

To show that M is symmetric, consider first the entries in row 1 and column 1. Let v be the least positive integer such that $r^v = -\frac{1}{2}$. Then

$$l(1, v+1) = l(1,0) + l(0, v+1) = 1 + r^v = \frac{1}{2}$$

and hence, by the definition of T, $m(1, v+1) = -1$. By P3 it follows that

$$m(n-v, 1) = r^{n-v-1} m(1, v+1) = r^{-v}(-1) = 2.$$

Again,

$$l(1, n-v) = l(1,0) + l(0, n-v) = 1 + r^{n-v-1} = -1$$

so $m(1, n-v) = 2$. Hence

$$m(v+1, 1) = r^v m(1, n-v) = (-\frac{1}{2}) \cdot 2 = -1.$$

Thus $m(i,1) = m(1,i)$ for $i = v+1,\ n-v$. The same equality holds trivially for $i = 1$ and it holds for all other i since these entries of M are equal to the corresponding entries of L, which is symmetric. Hence row 1 and column 1 of M are identical. By P3 it follows that M is symmetric.

Since M is symmetric and row Latin, it is also column Latin and therefore it is a Latin square. □

Theorem 2. *M is not based on a group.*

Proof: Consider the 2×2 subarrays of L that contain the entries

$$l(i_1, j_1) = 0, \quad l(i_1, j_2) = l(i_2, j_1) = 1, \quad l(i_2, j_2) = 2.$$

One of these is the leading subarray, specified by $i_1 = j_1 = 0$ and $i_2 = j_2 = 1$. Since L is based on a group and therefore satisfies the quadrangle criterion, there are n such subarrays. Under T, three occurrences of each non-zero symbol are moved to different cells but all zeros remain unmoved. Hence at most $3.3 = 9$ of the 2×2 subarrays of M that occupy the same cells as the above subarrays of L are altered and, since $n \geq 11$, at least two remain the same. The leading 2×2 subarray of M has three entries the same as in L but the entry 2 has been replaced by $\frac{1}{2}$. It follows that

M does not satisfy the quadrangle criterion and so M is not based on a group. □

Note that the proof of Theorem 2 requires that $n > 9$. Although M is still different from L when $n = 7$ or 5, it is cyclic. Thus 11 is the smallest prime for which Theorem 2 holds.

Theorem 3. *Every permutation between two rows of M is cyclic.*

Proof: Since M has the property P3 it is sufficient to consider the permutations (a) from row 0 to row 1 and (b) from row 1 to row i, $i > 1$. Let λ_i and μ_i denote the permutations from row 0 to row i in L and M respectively, $1 \leq i \leq n-1$.

(a) Now

$$\lambda_1 = (0, 1, 2, \ldots, -1),$$
$$\mu_1 = (0, 1, 2, \ldots, -1)(2, \frac{1}{2}, -1) = \lambda_1(2, \frac{1}{2}, -1),$$

where dots denote sequences rising in unit steps and, in any product of permutations, the leftmost permutation is applied first. The symbols in the 3-cycle $(2, \frac{1}{2}, -1)$ are actually $2, (n+1)/2, n-1$ so they are in the same cyclic order as in the n-cycle λ_1. Consequently μ_1 is cyclic; in fact

$$\mu_1 = (0, 1, \frac{1}{2}, \ldots, -2, 2, \ldots, -\frac{1}{2}, -1)$$

where dots again denote sequences rising in unit steps.

(b) The permutations from row 1 to row i in L and M are $\lambda_1^{-1}\lambda_i$ and $\mu_1^{-1}\mu_i$ respectively. By P3,

$$\mu_1^{-1}\mu_i = (-1, \frac{1}{2}, 2)\lambda_1^{-1}\lambda_i(2r^{i-1}, \frac{1}{2}r^{i-1}, -r^{i-1}).$$

Now λ_i is λ_1 raised to the power r^{i-1}, so $\lambda_1^{-1}\lambda_i$ is an n-cycle with successive entries rising in steps of $s \pmod n$, where $s = r^{i-1} - 1$.

It is convenient to change notation. Divide every symbol in $GF(n)$ by s and define

$$t = s^{-1}, \; u = s^{-1}r^{i-1} = t + 1.$$

Then $\mu_1^{-1}\mu_i$ is cyclic if and only if θ is cyclic, where

$$\theta = (-t, \frac{1}{2}t, 2t)\lambda_1(2u, \frac{1}{2}u, -u).$$

As an aid to the proof, we suppose that the n symbols are placed round a circle in clockwise ascending order $\pmod n$. Then the cyclic

permutation λ_1 causes a one step clockwise rotation. The order of the symbols $-t$, $\frac{1}{2}t$, $2t$ round the circle may be either (1) clockwise or (2) anticlockwise. In either case (see Figure 1) the positions of $2u$, $\frac{1}{2}u$, $-u$ relative to $-t$, $\frac{1}{2}t$, $2t$ are uniquely determined if these six symbols are all different. Indeed, $\frac{1}{2}t$ bisects one of the two arcs of the circle joining $-t$ to $2t$ because $2t-\frac{1}{2}t=\frac{1}{2}t-(-t)$, while $\frac{1}{2}u$ lies in the other arc because $\frac{1}{2}u-\frac{1}{2}t=\frac{1}{2}$, that is, $\frac{1}{2}(n+1)$; in addition, $-u=-t-1$ and $2u=2t+2$.

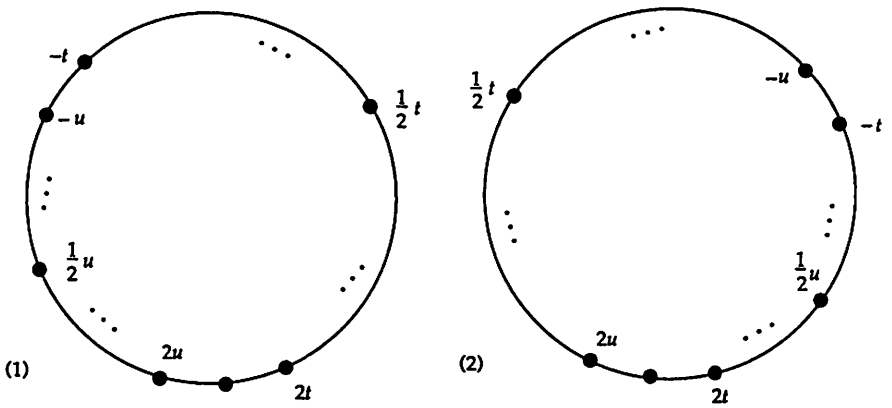

Figure 1

Groups of three dots in Figure 1 show where the symbols not specifically marked can lie. We use Figure 1 to evaluate the above expression for θ as a product of three cycles. In case (1),

$$\theta=(-t,\frac{1}{2}t+1,\ldots,2t,-t+1,\ldots,\frac{1}{2}t,2t+1,\\ \frac{1}{2}u,\ldots,-u-1,2u,\ldots,\frac{1}{2}u-1,-u)$$

and in case (2)

$$\theta=(-t,\frac{1}{2}t+1,\ldots,-u-1,2u,\ldots,\frac{1}{2}t,2t+1,\\ \frac{1}{2}u,\ldots,2t,-t+1,\ldots,\frac{1}{2}u-1,-u).$$

In both cases θ is cyclic.

It remains to consider the special subcases that arise when one of the symbols $2u$, $\frac{1}{2}u$, $-u$ coincides with one of the symbols $-t$, $\frac{1}{2}t$, $2t$.

Case (1), where $-t$, $\frac{1}{2}t$, $2t$ are in clockwise order, has only one special subcase (1a), given by $-u = 2t$ and $\frac{1}{2}u = -t$. This special subcase and the three special subcases of case (2) are shown in Figure 2. From Figure 2, diagrams (1a),

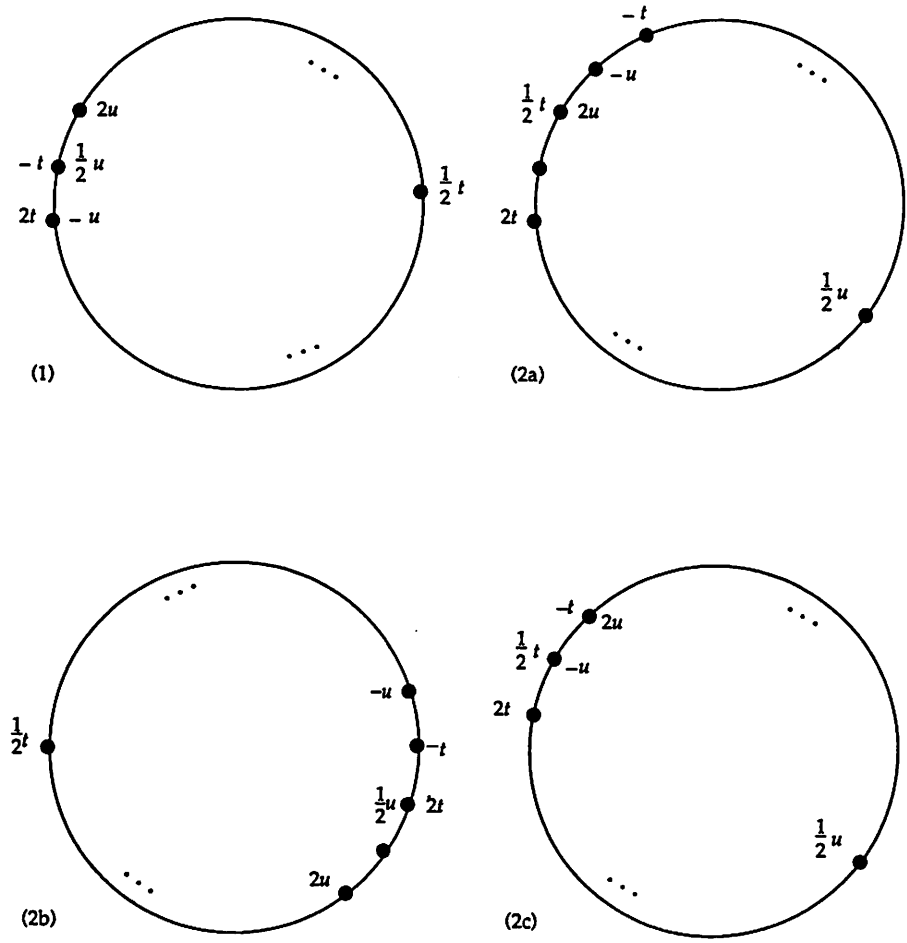

Figure 2

(2a), (2b), (2c), we obtain

$$\theta = (-t, \frac{1}{2}t+1, \ldots, 2t-1, 2u, \ldots, \frac{1}{2}t, 2t),$$

$$\theta = (-t, 2u, 2t+1, \frac{1}{2}u, \ldots, 2t, -t+1, \ldots, \frac{1}{2}u-1, -u),$$

$$\theta = (-t, \frac{1}{2}t+1, \ldots, -u-1, 2u, \ldots, \frac{1}{2}t, 2t+1, \frac{1}{2}u, -u),$$

$$\theta = (-t, \frac{1}{2}u, \ldots, 2t, -t+1, \ldots, \frac{1}{2}u-1, -u),$$

respectively. In all four special subcases θ is cyclic.

□

Because M is symmetric, Theorem 3 implies that every permutation between two columns of M is also cyclic.

Another property that M shares with L is given in Theorem 4.

Theorem 4. *The species to which M belongs consists of only one transformation set.*

Proof: We must show that every permutation of the three constraints of M (rows, columns and symbols) leads to a Latin square from the same transformation set. Since M is symmetric it is sufficient to consider only the interchange of columns and symbols. Let M_0 denote the Latin square obtained from M by permuting its columns to bring row 0 into natural order. Since M_0 is in the same transformation set as M we may start with M_0 instead of M.

In M_0, the permutations from column labels to row entries are ϵ, the identity permutation, for row 0 and $\mu_i = \lambda_i(2r^{i-1}, \frac{1}{2}r^{i-1}, -r^{i-1})$ for row i, $1 \leq i \leq n-1$. (The notation is as in Theorem 3.) To interchange columns and symbols, the permutations μ_i must be replaced by their inverses. Now

$$\mu_i^{-1} = (-r^{i-1}, \frac{1}{2}r^{i-1}, 2r^{i-1})\lambda_i^{-1},$$

where λ_i^{-1} is λ_1 raised to the power $-r^{i-1}$. The identity $(a,b,c)\lambda_1 = \lambda_1(a+1, b+1, c+1)$ holds for every 3-cycle (a,b,c). By applying it $-r^{i-1}$ times we get

$$\mu_i^{-1} = \lambda_i^{-1}(-r^{i-1} - r^{i-1}, \frac{1}{2}r^{i-1} - r^{i-1}, 2r^{i-1} - r^{i-1})$$

$$= \lambda_i^{-1}(-2r^{i-1}, -\frac{1}{2}r^{i-1}, r^{i-1}).$$

But $r^k = -1$, so $-r^{i-1} = r^{k+i-1}$ and $\lambda_i^{-1} = \lambda_{k+i}$. (The suffix $k+i$ is taken modulo $2k$ in the range 1 to $2k$.) Hence

$$\mu_i^{-1} = \lambda_{k+i}(2r^{k+i-1}, \frac{1}{2}r^{k+i-1}, -r^{k+i-1}) = \mu_{k+i}.$$

It follows that the new Latin square can be converted back into M_0 by merely interchanging rows $1, 2, \ldots, k$ with rows $k+1, k+2, \ldots, 2k$ respectively. Thus there has been no change of transformation set. □

3 The Youden property

In this section n is prime, $n \geq 11$ and also $n \equiv 3 \pmod 8$.

Since $n \equiv 3 \pmod 4$, the element -1 is a quadratic non-residue modulo n [4, p.66] so we can arrange all the symbols in the order

$$0, 1, r^2, r^4, \ldots, r^{n-3}, -1, -r^2, -r^4, \ldots, -r^{n-3}.$$

Here, zero is followed by the k quadratic residues and then the k quadratic non-residues. Let σ be the permutation from the arrangement of the symbols used in constructing L to the new arrangement.

Take the addition table of $GF(n)$, with the borders arranged as above, and then delete the borders. The Latin square L^* that remains can be obtained from L by applying the permutation σ to its rows and to its columns. Let M^* be the Latin square obtained in the same way from M and let T^* be the transformation from L^* to M^*. To investigate M^* we consider first L^*.

The part of L^* excluding row 0 and column 0 splits into four natural $k \times k$ subarrays, corresponding to the separation of quadratic residues from quadratic non-residues in the new arrangement of symbols. The entries in these subarrays are as follows:

$$l^*(i,j) = r^{2i-2} + r^{2j-2} = -l^*(k+i, k+j),$$
$$l^*(i,k+j) = r^{2i-2} - r^{2j-2} = -l^*(k+i, j),$$

for $1 \leq i \leq k$ and $1 \leq j \leq k$. Properties P1 and P2 hold for L^* because it is cyclic and by construction. In place of P3, L^* has the following property P3*:

(P3*) In the four natural $k \times k$ subarrays, every left to right broken diagonal, unless it contains only zeros, contains either all the quadratic residues or all the quadratic non-residues and they occur in the same cyclic order as in row 0 and column 0.

For later reference we state one further property P4 that follows trivially from the above expressions for the entries of L^*.

(P4) The sums of entries in cells (i,j), $(k+i, k+j)$ and in cells $(i, k+j)$, $(k+i, j)$ are zero $\pmod n$, for $1 \leq i \leq k$ and $1 \leq j \leq k$.

Rows 1 to k of L^* are easily seen to constitute a Youden square of size $k \times n$. The property Y1 is immediate. Also, the quadratic residues (mod n), which fill column 0 of this subarray, form a difference set (mod n) because n is prime and $n \equiv 3 \pmod 4$ [9, p.192]. Moreover, L^* was defined by means of an addition table (mod n), so if $l^*(i_2, 0) - l^*(i_1, 0) = d$ then $l^*(i_2, j) - l^*(i_1, j) = d$ for $0 \leq j \leq n-1$. By Y1, the n pairs $(l^*(i_1, j), l^*(i_2, j))$ are (in some order) all the pairs $(x, x+d)$, $0 \leq x \leq n-1$. Hence property Y2 holds.

By P4, rows $k+1$ to $2k$ of L^* form a second Youden square. It can be obtained from the one in rows 1 to k by interchanging columns $1, 2, \ldots, k$ with columns $k+1, k+2, \ldots, 2k$ respectively and replacing each symbol x by $-x$. The complementary sets of rows of L^*, namely rows $k+1$ to $2k$ together with row 0 and rows 0 to k, form Youden squares of size $(k+1) \times n$.

As an illustration, Table 2 gives L^* for $n = 11$, $k = 5$ and $r = 2$. Gaps are used to show the four natural $k \times k$ subarrays; entries that are altered by T^* are underlined.

0	1	4	5	9	3	10	7	6	2	8
1	2	5	6	10	4	0	8	7	3	9
4	5	8	9	2	7	3	0	10	6	1
5	6	9	10	3	8	4	1	0	7	2
9	10	2	3	7	1	8	5	4	0	6
3	4	7	8	1	6	2	10	9	5	0
10	0	3	4	8	2	9	6	5	1	7
7	8	0	1	5	10	6	3	2	9	4
6	7	10	0	4	9	5	2	1	8	3
2	3	6	7	0	5	1	9	8	4	10
8	9	1	2	6	0	7	4	3	10	5

Table 2

Now consider M^*. The permutation σ applied both to rows and to columns of M converts it into M^*, so properties P1 and P2 of M are preserved in M^*. Each broken diagonal of L' becomes, in L^*, a pair of broken diagonals in two of the natural $k \times k$ subarrays, either those at the top left and bottom right or the other two. Since T permutes three broken diagonals of L', the transformation T^* permutes three pairs of broken diagonals in $k \times k$ subarrays. Properties P3* and P4 of L^* are preserved in M^*.

In each column of L^*, except column 0, the transformation T^* permutes three entries. In column 1 the permuted entries are 2, $\frac{1}{2}$, -1 and they lie in rows whose entries in column 0 are 1, $-\frac{1}{2}$, -2, respectively. Now 1 is a quadratic residue modulo any integer and -2 is a quadratic residue

(mod n) since $n \equiv 3 \pmod 8$ [4, pp. 66, 68]. It follows that $-\frac{1}{2}$ is also a quadratic residue (mod n). Hence the three pairs of broken diagonals permuted by T^* are all in the top left and bottom right $k \times k$ subarrays. Hence the effect of T^* on the subarray composed of rows 1 to k of L^* is merely to permute three entries in each of columns 1 to k. Because the set of entries in each column of the subarray is not altered by T^*, the property of L^* that rows 1 to k form a Youden square is preserved in M^*. Similarly, M^* contains three other Youden squares in the same positions as those in L^*. When $n = 11$, the 5×11 Youden squares in M^* are readily recognized as coming from species 2 of Preece [6, Table 1].

Since M^* is obtainable from M by merely permuting rows and columns it belongs to the same species with only one transformation set.

Remarks

The total enumeration of 7×7 Latin squares by Norton [5] and Sade [8] shows that there is no non-cyclic 7×7 Latin square that has both property P1 and the corresponding property for columns. No non-cyclic 5×5 Latin square has property P1.

When n is even, an n-cycle is an odd permutation but the product of two n-cycles is even and therefore not cyclic. Since the permutation from row 0 of a Latin square to row 2 is the product of the permutations from row 0 to row 1 and row 1 to row 2, no Latin square of even order $n > 2$ has the property P1.

It is an open question whether there is a Latin square of composite odd order with the property P1. If there is, it cannot be based on a group.

References

[1] J. Dénes and A.D. Keedwell, *Latin squares and their applications*, Akadémiai Kiadó, Budapest; English Universities Press, London; Academic Press, New York, 1974.

[2] J. Dénes and A.D. Keedwell, Latin squares and one-factorizations of complete graphs: (II) Enumerating one-factorizations of the complete directed graph K_n^* using MacMahon's double partition idea, *Utilitas Math.* **34** (1988), 73–83.

[3] A.D. Keedwell, Proper loops of order n in which each non-identity element has left order n, *Demonstratio Math.* **24** (1991), 27–33.

[4] W.J. LeVeque, *Topics in number theory, Vol. I*, Addison-Wesley, Reading, MA, 1956.

[5] H.W. Norton, The 7×7 squares, *Annals of Eugenics* **9** (1939), 269–307.

[6] D.A. Preece, Some designs based on 11 × 5 Youden 'squares', *Utilitas Math.* **9** (1976), 139–146.

[7] D.A. Preece, Fifty years of Youden squares: a review, *Bull. Inst. Math. Appl.* **26** (1990), 65–75.

[8] A. Sade, An omission in Norton's list of 7 × 7 squares, *Ann. Math. Statist.* **22** (1951), 306–307.

[9] A.P. Street and W.D. Wallis, *Combinatorial theory: an introduction*, the Charles Babbage Research Centre, Box 370, St. Pierre, Manitoba, Canada, 1977.