ON THE CONSTRUCTION OF SETS OF ORTHOGONAL LATIN SQUARES[1]

By H. B. Mann

Columbia University

1. Introduction.

An m-sided Latin square is an arrangement of m symbols into a square in such a way that no row and no column contains any symbol twice. Two Latin squares are called orthogonal if, when one is superimposed upon the other, every pair of symbols occurs only once. For instance the squares

$$\begin{matrix} A & B & C \\ B & C & A \\ C & A & B \end{matrix} \qquad\qquad \begin{matrix} \alpha & \beta & \gamma \\ \gamma & \alpha & \beta \\ \beta & \gamma & \alpha \end{matrix}$$

are orthogonal. The resulting square is

$$\begin{matrix} A\alpha & B\beta & C\gamma \\ B\gamma & C\alpha & A\beta \\ C\beta & A\gamma & B\alpha. \end{matrix}$$

A pair of orthogonal Latin squares is called a Graeco-Latin square. A method has not yet been found by which all possible sets of mutually orthogonal squares can be constructed. However, methods are available for constructing certain special sets, and although we cannot obtain all possible sets with these methods they yield a great variety of designs.

To understand these methods we shall have to use certain fundamental concepts of the theory of numbers. In the following we shall deal therefore only with integers and all symbols used will denote only integers.

Let a, b, m denote certain integers. We say

$$a \equiv b\ (m),$$

(in words a is congruent to b modulo m) if $a - b$ is divisible by m.

Such congruences can be treated like equations. For instance: If $a \equiv b\ (m)$, then $a \pm c \equiv b \pm c\ (m)$, $ac \equiv bc\ (m)$. The proofs of these statements are obvious from the definition of $a \equiv b\ (m)$.

If $a \equiv b\ (m)$, *and* $c \equiv d\ (m)$, *then* $ac \equiv bd\ (m)$, *and* $a \pm c \equiv b \pm d\ (m)$.

Proof: According to our definition we have

$$a - b = \lambda_1 m \qquad a = b + \lambda_1 m$$

$$c - d = \lambda_2 m \qquad c = d + \lambda_2 m$$

[1] An expository paper presented, at the invitation of the program committee, on September 12, 1943 at the Sixth Summer Meeting of the Institute, at the New Jersey College for Women, Rutgers University, New Brunswick, N. J.

$ac = bd + m(\lambda_2 b + \lambda_1 d + \lambda_1\lambda_2 m)$ and $a \pm c = b \pm d + m(\lambda_1 - \lambda_2)$. Hence $ac - bd$ and $(a \pm c) - (b \pm d)$ are divisible by m.

We have to be more careful with the division of congruences but we shall prove the following rule.

If a is prime to m and $ab \equiv ac\ (m)$ then $b \equiv c\ (m)$.

PROOF: $a(b - c) = \lambda_1 m$, by hypothesis. The left side of this equation is divisible by m. Since a is prime to m, $b - c$ must be divisible by m.

This rule means that we may cancel as in an ordinary equation as long as the cancelled factor is prime to the modulus.

Every number is congruent to one of the numbers $0, 1, 2, \cdots, m - 1$, because if a is any number we can find a number b such that $0 \leq a - bm = j < m$.

We shall now add, subtract and multiply mod m. That means we add, subtract and multiply in the ordinary way but shall always replace every number by its smallest positive remainder. Thus for instance

$$2 + 4 \equiv 1\ (5)$$

$$2 \cdot 4 \equiv 3\ (5).$$

2. Complete sets of m-sided orthogonal Latin squares, where m is prime.

Now let p be a prime number. We write down the following design

$$\begin{array}{cccc} 0 & 1 & \cdots & p-1 \\ j & 1+j & \cdots & p-1+j \\ 2j & 1+2j & \cdots & p-1+2j \\ \vdots & \vdots & \vdots & \vdots \\ (p-1)j & 1+(p-1)j & \cdots & p-1+(p-1)j \end{array} = L_j; \quad 0 < j \leq p - 1$$

where all expressions are to be taken mod p, that is we replace every number in this square by its smallest remainder mod p. We shall show that L_j is a Latin square. Here the rows and columns are numbered from 0 to $p - 1$. Assume that the kth row $(0 \leq k \leq p - 1)$ contains a number twice. Then we would have

$$a + kj \equiv b + kj\ (p) \qquad \text{with } a \not\equiv b\ (m).$$

But from this we obtain $a \equiv b\ (p)$, which is a contradiction. Now assume that a column contains a number twice. Then we would have

$$a + kj \equiv a + k'j\ (p), \qquad \text{with } k \not\equiv k'\ (m)$$

but from this we have

$$kj \equiv k'j\ (p),$$

and since j is prime to p

$$k \equiv k'\ (p),$$

which is again a contradiction.

We can obtain $p - 1$ such Latin squares corresponding to the $p - 1$ values which j can take.

We shall show that L_i is orthogonal to L_j if $i \neq j$. If this were not true we would have the same pair of numbers occurring in two different boxes of the square which results from the superimposition of L_i on L_j. Let mn be such a pair and assume that it occurs in the αth row and βth column and the γth row and δth column of the resulting square. Then m would occur in L_j in the αth row and βth column and in the γth row and δth column. Hence we would have

$$\text{(i)} \qquad \beta + \alpha j \equiv m \equiv \delta + \gamma j \ (p),$$

and similarly

$$\text{(i}'\text{)} \qquad \beta + \alpha i \equiv n \equiv \delta + \gamma i \ (p).$$

If we subtract the second congruence from the first we obtain

$$\alpha(j - i) \equiv \gamma(j - i) \ (p),$$

but $j < p$ and $i < p$ and $j \neq i$. Hence $j - i \not\equiv 0 \ (p)$ and we may therefore divide by $(j - i)$. This gives

$$\alpha \equiv \gamma \ (p).$$

Substituting this in (i) we obtain

$$\beta \equiv \delta \ (p).$$

Hence the two boxes must be the same. We have therefore the following theorem:

THEOREM 1: *If p is a prime number and*

$$L_j = \begin{array}{cccc} 0 & 1 & \cdots & p - 1 \\ j & 1 + j & \cdots & p - 1 + j \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ (p - 1)j & 1 + (p - 1)j & \cdots & p - 1 + (p - 1)j \end{array}$$

then $L_1, L_2, \cdots, L_{p-1}$ is a set of $p - 1$ orthogonal Latin squares.

As an application we can write down a set of 4 orthogonal Latin squares of side 5

$$\begin{array}{cccc} L_1 & L_2 & L_3 & L_4 \\ 0\,1\,2\,3\,4 & 0\,1\,2\,3\,4 & 0\,1\,2\,3\,4 & 0\,1\,2\,3\,4 \\ 1\,2\,3\,4\,0 & 2\,3\,4\,0\,1 & 3\,4\,0\,1\,2 & 4\,0\,1\,2\,3 \\ 2\,3\,4\,0\,1 & 4\,0\,1\,2\,3 & 1\,2\,3\,4\,0 & 3\,4\,0\,1\,2 \\ 3\,4\,0\,1\,2 & 1\,2\,3\,4\,0 & 4\,0\,1\,2\,3 & 2\,3\,4\,0\,1 \\ 4\,0\,1\,2\,3 & 3\,4\,0\,1\,2 & 2\,3\,4\,0\,1 & 1\,2\,3\,4\,0 \end{array}$$

A further simplification can be achieved if we know a primitive root mod p. A primitive root is a remainder a mod p such that every other remainder except 0 is equal to a power of a mod p. For example, 3 is a primitive root mod 7, for $3^0 \equiv 1\ (7), 3^1 \equiv 3(7), 3^2 \equiv 2(7), 3^3 \equiv 6(7), 3^4 \equiv 4(7), 3^5 \equiv 5(7)$.

For any number a we must have $a^{p-1} \equiv 1\ (p)$. We will prove this equation for primitive roots only, since we do not need the general case. Let a be a primitive root and assume that

$$a^{p-1} \equiv b \equiv a^q\ (p), \qquad \text{with } q < p - 1.$$

Then we would have

$$a^{p-1-q} \equiv a^{p'} \equiv 1\ (p), \qquad \text{with } p' < p - 1.$$

Hence we can obtain at most $p - 2$ different remainders $a^0a^1, \cdots, a^{p'-1}$ and a would not be a primitive root.

We now form

$$\bar{L}_i = \begin{array}{cccc} 0 & 1 & \cdots & p-1 \\ a^{0+i} & 1+a^{0+i} & \cdots & p-1+a^{0+i} \\ a^{1+i} & 1+a^{1+i} & \cdots & p-1+a^{1+i} \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ a^{p-2+i} & 1+a^{p-2+i} & \cdots & p-1+a^{p-2+i} \end{array} \cdot \quad (i = 0, 1, \cdots, p-2)$$

Exactly as in the case of the L_j of Theorem 1 it can be shown that $\bar{L}_i$ is orthogonal to $\bar{L}_j$ if $i \neq j$. For $k < p - 1$ the k-th row of $\bar{L}_i$ equals the $(k - 1)$st row of $\bar{L}_{i+1}$ and since $a^{p-1} \equiv 1\ (p)$ the last row of $\bar{L}_{i+1}$ equals the first row of $\bar{L}_i$. Hence $\bar{L}_{i+1}$ is obtained from $\bar{L}_i$ by a cyclical permutation of the $(p - 1)$ last rows. It is then only necessary to construct the first square. The others can be obtained by a cyclic permutation of the $(p - 1)$ last rows. We shall exemplify this by constructing a set of 6 seven-sided orthogonal squares.

L_1

0	1	2	3	4	5	6
1	2	3	4	5	6	0
3	4	5	6	0	1	2
2	3	4	5	6	0	1
6	0	1	2	3	4	5
4	5	6	0	1	2	3
5	6	0	1	2	3	4

L_2

0	1	2	3	4	5	6
3	4	5	6	0	1	2
2	3	4	5	6	0	1
6	0	1	2	3	4	5
4	5	6	0	1	2	3
5	6	0	1	2	3	4
1	2	3	4	5	6	0

L_3

0	1	2	3	4	5	6
2	3	4	5	6	0	1
6	0	1	2	3	4	5
4	5	6	0	1	2	3
5	6	0	1	2	3	4
1	2	3	4	5	6	0
3	4	5	6	0	1	2

L_4

0	1	2	3	4	5	6
6	0	1	2	3	4	5
4	5	6	0	1	2	3
5	6	0	1	2	3	4
1	2	3	4	5	6	0
3	4	5	6	0	1	2
2	3	4	5	6	0	1

L_5

0	1	2	3	4	5	6
4	5	6	0	1	2	3
5	6	0	1	2	3	4
1	2	3	4	5	6	0
3	4	5	6	0	1	2
2	3	4	5	6	0	1
6	0	1	2	3	4	5

L_6

0	1	2	3	4	5	6
5	6	0	1	2	3	4
1	2	3	4	5	6	0
3	4	5	6	0	1	2
2	3	4	5	6	0	1
6	0	1	2	3	4	5
4	5	6	0	1	2	3

In the theory of numbers it is shown that a primitive root exists for every prime number. If p is not too large a primitive root can easily be found by trial and error. We give a list of primitive roots for all primes under 30:

Prime number	Primitive root
3	2
5	2
7	3
11	2
13	2
17	3
19	2
23	5
29	2

In computing the first row of the first square it is not necessary to actually compute all powers of the primitive root. We can take advantage of the fact that a congruence may be multiplied by a number. Thus, for instance, for the first row of the 11-sided square we have $2^0 \equiv 1$ (11) $2^1 \equiv 2$ (11) $2^2 \equiv 4$ (11) $2^3 \equiv 8$ (11) $2^4 \equiv 5$ (11) $2^5 \equiv 2.5 \equiv 10$ (11) but $10 \equiv -1$ (11), hence we have without further computation $2^6 \equiv -2 \equiv 9$ (11) $2^7 \equiv -4 \equiv 7$ (11) $2^8 \equiv -8 \equiv 3$ (11) $2^9 \equiv -5 \equiv 6$ (11).

3. Complete sets of m-sided orthogonal Latin squares, where m is the power of a prime.

We have seen that we can always construct $m - 1$ orthogonal Latin squares if m is a prime number. We shall show how to construct $m - 1$ orthogonal Latin squares if m is the power of a prime. However, if we need only a Graeco-Latin square of side m and if m is odd, then we can use the following theorem:

THEOREM 2: *If m is odd, then the squares*

$$L_1 = \begin{array}{cccc} 0 & 1 & \cdots & m-1 \\ 1 & 1+1 & \cdots & m-1+1 \\ 2 & 1+2 & \cdots & m-1+2 \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ m-1 & 1+m-1 & \cdots & m-1+m-1 \end{array}$$

$$L_2 = \begin{array}{cccc} 0 & 1 & \cdots & m-1 \\ 2 & 1+2 & \cdots & m-1+2 \\ 2.2 & 1+2.2 & \cdots & m-1+2.2 \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ 2(m-1) & 1+2(m-1) & \cdots & m-1+2(m-1) \end{array}$$

are orthogonal.

The proof is similar to the proof of Theorem 1. We have to use the fact that 2 is prime to m.

We shall now prove the following statement: *For every remainder* $a \not\equiv 0(p)$ *there exists another remainder* a^{-1} *such that* $a \cdot a^{-1} \equiv 1(p)$.

PROOF: We form the sequence $a, a^2, \cdots, a^n, \cdots$. Since there is only a finite number of remainders, there must exist 2 values i and j such that

$$a^i \equiv a^j(p)$$

Let $i > j$. Then since a is prime to p we may divide by a^j. Putting $i - j = d$, we obtain

$$a^{i-j} = a^d \equiv 1(p).$$

Hence we may take $a^{-1} = a^{d-1}$ and our statement is proved. Thus we see that the system of remainders mod p with respect to addition as well as with respect to multiplication if 0 is excluded satisfies the following postulates:

(1) For every pair of elements A, B there is defined a product $A \cdot B$ within the system such that for any 3 elements A, B and C

$$A \cdot (B \cdot C) = (A \cdot B) \cdot C \qquad \text{(associative law)}$$

The "multiplication" may be any sort of composition. For example, either addition or multiplication of remainder classes.

(2) There exists a unit element 1 such that

$$A \cdot 1 = 1 \cdot A = A.$$

(3) For every A in the system there exists an element A^{-1} such that

$$A \cdot A^{-1} = A^{-1} \cdot A = 1.$$

The unit element will be 0 if we consider the remainder classes with addition as composition. It will be 1 if multiplication is the composition. The inverse of a is $-a$ for the additive system, a^{-1} for the multiplicative system.

A system satisfying (1), (2) and (3) is called a group. The property $A \cdot B = B \cdot A$ is usually not postulated. If a group fulfills this condition, then it is called a commutative group or an Abelian group. A group can be defined by its generating elements. For example, let G be generated by the elements P, Q with the relations $P^2 = 1$, $Q^3 = 1$ and $PQ = Q^2P$. We then obtain the elements of G as $1, P, Q, PQ, PQ^2, Q^2$. The rules for the multiplication can be written down in the form of a table:

1	P	Q	PQ	PQ^2	Q^2
P	1	PQ	Q	Q^2	PQ^2
Q	PQ^2	Q^2	P	PQ	1
PQ	Q^2	PQ^2	1	Q	P
PQ^2	Q	P	Q^2	1	PQ
Q^2	PQ	1	PQ^2	P	Q

By inspection one can see that taking the elements of our group as symbols the multiplication table forms a Latin square. For instance, if we identify P with 2, Q with 3, etc. we obtain from the table above

1	2	3	4	5	6
2	1	4	3	6	5
3	5	6	2	4	1
4	6	5	1	3	2
5	3	2	6	1	4
6	4	1	5	2	3

We shall prove that this is generally true. Let the group G consist of the elements $A_1, \cdots, A_m$. We write down the multiplication table of the group:

$$\begin{array}{cccc}
A_1 & A_2 & \cdots & A_m \\
A_2 & A_2A_2 & \cdots & A_2A_m \\
\cdot & \cdot & \cdots & \cdot \\
\cdot & \cdot & \cdots & \cdot \\
\cdot & \cdot & \cdots & \cdot \\
A_m & A_mA_2 & \cdots & A_mA_m
\end{array}$$

Suppose this is not a Latin square. Then an element will occur twice in at least one row or at least one column, that is, we should have either

$$A_jA_i = A_jA_k, \qquad \text{for } i \neq k$$

or

$$A_jA_i = A_kA_i, \qquad \text{for } j \neq k.$$

Multiplying the first equation by A_j^{-1} on the left, we obtain $A_i = A_k$. Hence $i = k$. Similarly in the second case $j = k$, contrary to our assumption.

Two groups G and $\bar{G}$ are called isomorphic if we can map G into $\bar{G}$ in such a way that the mapping is not disturbed by multiplication. That is, if A is mapped on $\bar{A}$ and B on $\bar{B}$ and if $AB = C$ and $\bar{A}\bar{B} = \bar{C}$, then C must be mapped on $\bar{C}$. Such a mapping is called an isomorphism. If $G = \bar{G}$ then the mapping is called an automorphism. For instance, if we consider the remainder system mod m with addition as composition and j is any remainder, then the mapping $\bar{a} = ja$ is an automorphism. For if

$$a + b \equiv c(m)$$

then

$$aj + bj \equiv cj(m)$$

Some automorphisms establish a 1-to-1 correspondence between the elements of G. For instance, in the above example if j is prime to m the correspondence is bi-unique (that is only one element is mapped on any element of G) because if

$$aj \equiv bj(m),$$

and j is prime to m then

$$a \equiv b(m).$$

If j is not prime to m, the mapping would not be unique although it would still be an automorphism. From now on we shall consider only automorphisms which establish a 1-to-1 correspondence between the elements of G.

Let S be such an automorphism and denote by A^S the element into which A is mapped under the automorphism S. We put $(A^S)^S = A^{S^2}$, $(A^{S^2})^S = A^{S^3}$, etc. We also put $A^{S^0} = A$. We shall prove the following theorem:

Let S be an automorphism such that $S, S^2, \cdots, S^q$ map no element into itself except the element 1. *Then the Latin squares*

$$L_i = \begin{array}{cccc} 1 & A_2 & \cdots & A_m \\ A_2^{S^i} & A_2^{S^i}A_2 & \cdots & A_2^{S^i}A_m \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ A_m^{S^i} & A_m^{S^i}A_2 & \cdots & A_m^{S^i}A_m \end{array} \qquad (i = 0, 1, \cdots, q)$$

are orthogonal.

PROOF: Assume that L_i is not orthogonal to L_j. Let L_{ij} be the resulting square if L_j is superimposed on L_i. Then for some k and l and some r and s we should have the same pair of elements in the kth row and lth column and in the rth row and sth column. That is, we should have

$$A_k^{S^i}A_l = A_r^{S^i}A_s \tag{1}$$

$$A_k^{S^j}A_l = A_r^{S^j}A_s. \tag{2}$$

By taking the inverse elements it follows from (2) that

$$A_l^{-1}A_k^{-S^j} = A_s^{-1}A_r^{-S^j}. \tag{3}$$

Multiplying (1) and (3) we obtain

$$A_k^{S^i}A_k^{-S^j} = A_r^{S^i}A_r^{-S^j}.$$

Multiplying by $A_r^{-S^i}$ to the left, and by $A_k^{S^j}$ to the right, we obtain

$$A_r^{-S^i}A_k^{S^i} = A_r^{-S^j}A_k^{S^j}.$$

Since S^i and S^j are automorphisms we have

$$(A_r^{-1}A_k)^{S^i} = (A_r^{-1}A_k)^{S^j}.$$

Assuming $i > j$, then

$$[(A_r^{-1}A_k)^{S^j}]^{S^{i-j}} = (A_r^{-1}A_k)^{S^j}.$$

Because of $i \leq q, j \leq q$ we have $i - j \leq q$. By assumption therefore S^{i-j} can can leave only 1 fixed. Therefore

$$(A_r^{-1}A_k)^{S^j} = 1.$$

Hence

$$A_r^{-1}A_k = 1$$

$$A_r = A_k.$$

But then also

$$A_l = A_s.$$

Therefore $r = k$ and $l = s$. Hence the two compartments of L_{ij} cannot be different and our statement is proved.

We see therefore that we can construct a set of $q + 1$ orthogonal Latin squares if we can find a group G and an automorphism S of G such that

$$S, S^2, \cdots, S^q$$

maps no element into itself except the unit element. If $q = m - 2$ and we write

$$L_i = \begin{array}{ccccccc} 1 & A_2 & A_2^S & \cdot & \cdot & \cdot & A_2^{S^q} \\ A_2^{S^i} & A_2^{S^i}A_2 & \cdot & \cdot & \cdot & \cdot & A_2^{S^i}A_2^{S^q} \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ A_2^{S^{q+i}} & \cdot & \cdot & \cdot & \cdot & \cdot & A_2^{S^{q+i}}A_2^{S^q} \end{array}$$

then the $(k - 1)$st row of L_{i+1} equals the k-th row of L_i and all squares may be obtained from L_0 by a cyclical permutation of the rows.

We shall now consider commutative groups of prime power order p^n defined by the relations

$$P_1^p = P_2^p = \cdots = P_n^p = 1, \qquad P_iP_j = P_jP_i.$$

The elements of this group G have the form

$$P_1^{e_1} \cdots P_n^{e_n} \qquad e_1, \cdots, e_n = 0, 1, \cdots, p - 1.$$

We call $P_1 \cdots P_n$ a basis of G. We can easily change the basis. For instance if $P_1, \cdots, P_n$ is a basis then also $P_1, P_1P_2, \cdots, P_1P_n$ is a basis. For every expression we have

$$P_1^{e_1} \cdots P_n^{e_n} = P_1^{e_1 - e_2 \cdots - e_n}(P_1P_2)^{e_2} \cdots (P_1P_n)^{e_n},$$

since G is commutative. Such a change in the basis defines an automorphism of G at the same time. For let $P_1', \cdots, P_n'$ be the new basis. We can map

$$P_1^{e_1} \cdots P_n^{e_n}$$

into

$$P_1'^{e_1} \cdots P_n'^{e_n}.$$

On the other hand an automorphism is determined if we know on what elements the basis elements are mapped.

It can be shown that every such group admits an automorphism S such that $S, S^2, \cdots, S^{p^n-2}$ leaves no element fixed except 1. Hence we can always construct a set of $p^n - 1$ orthogonal squares of side p^n if p is a prime. We shall give these automorphisms explicitly for the groups of order 8, 9, 16, 25 and 27.

As an example let us construct 7 orthogonal 8 sided squares. We shall use the group G generated by P, Q, R where $P^2 = Q^2 = R^2 = 1$. We use the automorphism S where

$$P^s = Q \qquad Q^s = R \qquad R^s = PQ.$$

We then have $P^s = Q$, $P^{s^2} = R$, $P^{s^3} = PQ$, $P^{s^4} = P^sQ^s = QR$, $P^{s^5} = Q^sR^s = PQR$, $P^{s^6} = P^sQ^sR^s = QRPQ = PR$, $P^{s^7} = P^sR^s = QPQ = P$. If we write the elements in the order $1, P, P^s, P^{s^2}, \cdots, P^{s^6}$ we obtain the following multiplication table:

1	P	Q	R	PQ	QR	PQR	PR
P	1	PQ	PR	Q	PQR	QR	R
Q	PQ	1	QR	P	R	PR	PQR
R	PR	QR	1	PQR	Q	PQ	P
PQ	Q	P	PQR	1	PR	R	QR
QR	PQR	R	Q	PR	1	P	PQ
PQR	QR	PR	PQ	R	P	1	Q
PR	R	PQR	P	QR	PQ	Q	1

The other squares are then obtained by a cyclical permutation of the rows of this square. We now write 2 instead of P, 3 instead of Q, etc. and obtain:

$$L_0 = \begin{array}{cccccccc} 1&2&3&4&5&6&7&8\\ 2&1&5&8&3&7&6&4\\ 3&5&1&6&2&4&8&7\\ 4&8&6&1&7&3&5&2\\ 5&3&2&7&1&8&4&6\\ 6&7&4&3&8&1&2&5\\ 7&6&8&5&4&2&1&3\\ 8&4&7&2&6&5&3&1 \end{array} \qquad L_1 = \begin{array}{cccccccc} 1&2&3&4&5&6&7&8\\ 3&5&1&6&2&4&8&7\\ 4&8&6&1&7&3&5&2\\ 5&3&2&7&1&8&4&6\\ 6&7&4&3&8&1&2&5\\ 7&6&8&5&4&2&1&3\\ 8&4&7&2&6&5&3&1\\ 2&1&5&8&3&7&6&4 \end{array}$$

and so forth.

For the group of order 9, generated by P, Q with the relations $P^3 = Q^3 = 1$ the automorphism $P^s = Q$, $Q^s = PQ$ has the property that $S, S^2, \cdots, S^7$ maps no element into itself. For the group of order 16 we have 4 basis elements P, Q, R, T with $P^2 = Q^2 = R^2 = T^2 = 1$ and S can be given by $P^s = Q$, $Q^s = R$, $R^s = T$, $T^s = PT$.

For the group of order 25 we have two basis elements P, Q with $P^5 = Q^5 = 1$ and the automorphism is given by $P^s = Q$, $Q^s = P^3Q$.

The group of order 27 is generated by P, Q, R and the defining relations are $P^3 = Q^3 = R^3 = 1$. The automorphism is given by $P^s = Q$, $Q^s = R$, $R^s = P^2Q$.

We have now shown

THEOREM 3: *Let $m = p^n$ and let G be the commutative group generated by $P_1, \cdots, P_n$ which satisfy the relations $P_1^p = P_2^p = \cdots = P_n^p = 1$. Let S be an* *automorphism such that* $P^{s^i} \neq P$ if $0 < i \leq m - 2$, $P \neq 1$. *Then the Latin squares*

$$L_i = \begin{array}{cccc} 1 & P & P^s \cdots & P^{s^{m-2}} \\ P^{s^i} & P^{s^i}P & \cdots\cdot & P^{s^i}P^{s^{m-2}} \\ P^{s^{1+i}} & P^{s^{1+i}}P & \cdots\cdot & P^{s^{1+i}}P^{s^{m-2}} \\ \cdot & \cdot & \cdots\cdot & \cdot \\ \cdot & \cdot & \cdots\cdot & \cdot \\ \cdot & \cdot & \cdots\cdot & \cdot \\ P^{s^{m-2+i}} & P^{s^{m-2+i}}P & \cdots\cdot & P^{s^{m-2+i}}P^{s^{m-2}} \end{array} \qquad (i = 0, 1, \cdots, m - 2),$$

are orthogonal. L_i *is obtained from* L_{i-1} *by a cyclical permutation of its last* $m - 1$ *rows.*

4. Remarks on the largest number of m-sided orthogonal Latin squares, for arbitrary m.

The general problem can be formulated as follows: Given a number m, what is the greatest number of orthogonal m-sided squares.

It is clear that this number cannot be larger than $m - 1$. For we can by renaming the numbers of the squares always transform them without changing their orthogonality in such a way that the first row is $1, 2, \cdots m$. Hence the pairs $1\ 1, 2\ 2, \cdots, m\, m$, occur for any two squares in the first row of the resulting square. Hence the numbers in the first column and second row of the squares must be different from 1 and different from each other. But we have only the numbers $2, \cdots, m$ at our disposal and these are only $m - 1$ numbers.

We have shown that if m is the power of a prime $m - 1$ orthogonal squares can always be constructed by the use of groups. Hence our problem is solved if m is the power of a prime. Very little is known about numbers which are not prime powers. Tarry (*Compte Rendu*, 1900) has shown that no 6 sided Graeco-Latin square exists. It is conjectured but not yet proved that no Graeco-Latin square of side $4n + 2$ exists. We shall, however, show the following: If $m = p_1^{e_1} \cdots p_n^{e_n}$ where p_i is a prime number ($p_i \neq p_j$ for $i \neq j$) and if $r =$ minimum $p_i^{e_i} - 1$ then r orthogonal Latin squares can be constructed from commutative groups of order m.

We take the group G of order m generated by e_1 elements of order p_1, e_2 element of order p_2, $\cdots$, e_n elements of order p_n. We determine the automorphisms T_i of the subgroup generated by the elements of order p_i such that T_i, $T_i^2, \cdots, T_i^{p_i^{e_i}-2}$ leave no element of order p_i fixed. We define then an automorphism $\overline{T}_i$ of G generated by changing the basis elements of order p_i in the same way as they are changed by T_i and leaving the other basis elements fixed. Then

$$T = \overline{T}_1\overline{T}_2 \cdots \overline{T}_n$$

is an automorphism whose first $r - 1$ powers leave no element fixed. Hence the r Latin squares

$$L_i = \begin{matrix} 1 & A_2 & \cdots & A_m \\ A_2^{T^i} & A_2^{T^i}A_2 & \cdots & A_2^{T^i}A_m \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ A_m^{T^i} & A_m^{T^i}A_2 & \cdots & A_m^{T^i}A_m \end{matrix} \qquad (i = 0, 1, \cdots, r - 1)$$

are orthogonal.

TABLE I

1	P	Q	PQ	PR	QR²	PQR⁴	PR³	QR	PQR²	PR⁴	QR³	PQR	PR²	QR⁴	PQR³	R	R²	R⁴	R³
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
2	1	4	3	17	10	15	20	13	6	19	16	9	18	7	12	5	14	11	8
3	4	1	2	13	18	11	16	17	14	7	20	5	10	19	8	9	6	15	12
4	3	2	1	9	14	19	12	5	18	15	8	17	6	11	20	13	10	7	16
5	17	13	9	18	16	3	19	10	12	1	7	6	20	4	15	14	8	2	11
6	10	18	14	16	19	5	4	20	11	13	1	8	7	17	2	12	15	9	3
7	15	11	19	3	5	20	6	2	17	12	14	1	9	8	18	4	13	16	10
8	20	16	12	19	4	6	17	7	3	18	13	15	1	10	9	11	2	14	5
9	13	17	5	10	20	2	7	18	8	4	19	14	16	1	11	6	12	3	15
10	6	14	18	12	11	17	3	8	19	9	2	20	15	5	1	16	7	13	4
11	19	7	15	1	13	12	18	4	9	20	10	3	17	16	6	2	5	8	14
12	16	20	8	7	1	14	13	19	2	10	17	11	4	18	5	15	3	6	9
13	9	5	17	6	8	1	15	14	20	3	11	18	12	2	19	10	16	4	7
14	18	10	6	20	7	9	1	16	15	17	4	12	19	13	3	8	11	5	2
15	7	19	11	4	17	8	10	1	5	16	18	2	13	20	14	3	9	12	6
16	12	8	20	15	2	18	9	11	1	6	5	19	3	14	17	7	4	10	13
17	5	9	13	14	12	4	11	6	16	2	15	10	8	3	7	18	20	1	19
18	14	6	10	8	15	13	2	12	7	5	3	16	11	9	4	20	19	17	1
19	11	15	7	2	9	16	14	3	13	8	6	4	5	12	10	1	17	20	18
20	8	12	16	11	3	10	5	15	4	14	9	7	2	6	13	19	1	18	17

We shall exemplify this by constructing 3 orthogonal squares of side 20. We use the group G generated by P, Q, R with the defining relations: $P^2 = Q^2 = 1$; $R^5 = 1$. The automorphisms are given by: $P^{\bar{T}_1} = Q$, $Q^{\bar{T}_1} = PQ$, $R^{\bar{T}_1} = R$, $P^{\bar{T}_2} = P$, $Q^{\bar{T}_2} = Q$, $R^{\bar{T}_2} = R$. Hence $T = \bar{T}_1\bar{T}_2$ is given by: $P^T = Q$, $Q^T = TQ$, $R^T = R^2$. Therefore we have: $P^T = Q$, $P^{T^2} = PQ$, $P^{T^3} = P^TQ^T = P$, $(PR)^T = QR^2$, $(PR)^{T^2} = PQR^4$, $(PR)^{T^3} = PR^3$, $(PR)^{T^4} = QR$, $(PR)^{T^5} = PQR^2$, $(PR)^{T^6} = PR^4$, $(PR)^{T^7} = QR^3$, $(PR)^{T^8} = PQR$, $(PR)^{T^9} = PR^2$, $(PR)^{T^{10}} = QR^4$, $(PR)^{T^{11}} = PQR^3$, $(PR)^{T^{12}} = PR$, $R^T = R^2$, $R^{T^2} = R^4$, $R^{T^3} = R^3$, $R^{T^4} = R$.

We need only construct one key square if we write down the elements in the way in which they are written above. Then we have only to mark the end of each cycle. Thus in our present case we have:

$$1 \mid P, Q, PQ \mid PR, QR^2, PQR^4, PR^3, QR, PQR^2, PR^4, QR^3, PQR, PR^2, QR^4, PQR^3 \mid R, R^2, R^4, R^3 \mid$$

The vertical lines mark the cycles in which the elements are permuted by the automorphisms. We then write down the key square in Table I. From this key square we can easily obtain a set of 3 orthogonal squares by permuting the rows within the cycles indicated. Because of space difficulties we give only the first half of the square in Table II.

TABLE II

1,1	2,2	3,3	4,4	5,5	6,6	7,7	8,8	9,9	10,10
1	2	3	4	5	6	7	8	9	10
2,3	1,4	4,1	3,2	17,13	10,18	15,11	20,16	13,17	6,14
4	3	2	1	9	14	19	12	5	18
3,4	4,3	1,2	2,1	13,9	18,14	11,19	16,12	17,5	14,18
2	1	4	3	17	10	15	20	13	6
4,2	3,1	2,4	1,3	9,17	14,10	19,15	12,20	5,13	18,6
3	4	1	2	13	18	11	16	17	14
5,6	17,10	13,18	9,14	18,16	16,19	3,5	19,4	10,20	12,11
7	15	11	19	3	5	20	6	2	17
6,7	10,15	18,11	14,19	16,3	19,5	5,20	4,6	20,2	11,17
8	20	16	12	19	4	6	17	7	3
7,8	15,20	11,16	19,12	3,19	5,4	20,6	6,17	2,7	17,3
9	13	17	5	10	20	2	7	18	8
8,9	20,13	16,17	12,5	19,10	4,20	6,2	17,7	7,18	3,8
10	6	14	18	12	11	17	3	8	19
9,10	13,6	7,14	5,18	10,12	20,11	2,17	7,3	18,8	8,19
11	19	7	15	1	13	12	18	4	9
10,11	6,19	14,7	18,15	12,1	11,13	17,12	3,18	8,4	19,9
12	16	20	8	7	1	14	13	19	2
11,12	19,16	7,20	15,8	1,7	13,1	12,14	18,13	4,19	9,2
13	9	5	17	6	8	1	15	14	20
12,13	16,9	20,5	8,17	7,6	1,8	14,1	13,15	19,14	2,20
14	18	10	6	20	7	9	1	16	15
13,14	9,18	5,10	17,6	6,20	8,7	1,9	15,1	14,16	20,15
15	7	19	11	4	17	8	10	1	5
14,15	18,7	10,19	6,11	20,4	7,17	9,8	1,10	16,1	15,5
16	12	8	20	15	2	18	9	11	1
15,16	7,12	19,8	11,20	4,15	17,2	8,18	10,9	1,11	5,1
5	17	13	9	18	16	3	19	10	12
16,5	12,17	8,13	20,9	15,18	2,16	18,3	9,19	11,10	1,12
6	10	18	14	16	19	5	4	20	11
17,18	5,14	9,6	13,10	14,8	12,15	4,13	11,2	6,12	16,7
19	11	15	7	2	9	16	14	3	13
18,19	14,11	6,15	10,7	8,2	15,9	13,16	2,14	12,3	7,13
20	8	12	16	11	3	10	5	15	4
19,20	11,8	15,12	7,16	2,11	9,3	16,10	14,5	3,15	13,4
17	5	9	13	14	12	4	11	6	16
20,17	8,5	12,9	16,13	11,14	3,12	10,4	5,11	15,6	4,16
18	14	6	10	8	15	13	2	12	7

One might hope that with other groups more than r = minimum $p_i^{e_i} - 1$ orthogonal squares might be obtained. It has been shown however that using any group and its automorphisms at most r orthogonal squares can be obtained.

A more general method based on groups is given in a recent paper (H. B. Mann, "The construction of sets of orthogonal Latin squares," *Annals of Math. Stat.*, Vol. 13 (1942)). It can be shown that also with this more general method no $4n + 2$ sided Graeco-Latin square can be constructed.

ADDITIONAL LITERATURE

R. C. Bose: "On the application of the properties of Galois-fields to the construction of completely orthogonalized Latin squares," *Sankhyā*, 1939.

"On completely orthogonalized sets of Latin squares," *Sankhyā*, 1941.