SANKHYĀ

THE INDIAN JOURNAL OF STATISTICS

Edited by : P. C. MAHALANOBIS

VOL. 3. PART 4. 1938.

ON THE APPLICATION OF THE PROPERTIES OF GALOIS FIELDS TO THE PROBLEM OF CONSTRUCTION OF HYPER-GRÆCO-LATIN SQUARES

BY RAJ CHANDRA BOSE

INTRODUCTION.

Two Latin squares may be said to be orthogonal to each other if, when they are superimposed, every letter of the one square occurs once and only once with every letter of the other. Such a pair of squares (one square being written with Greek letters) may be called a Græco-Latin square. When $p-1$ mutually orthogonal squares of side p exist, then by their superposition we get what may be called a completely orthogonalised or Hyper-Græco-Latin square.* The work of Fisher[1] and Yates[2] has shown that such squares are of fundamental importance in experimental design. It is easy to see that for a prime number p, a p-sided Hyper-Græco-Latin square exists Recently Yates has shown that Hyper Græco-Latin squares exist also for the cases $p=4$, 8, 9. Professor Fisher, during his recent visit to India, in a Seminar held under the auspices of the Indian Statistical Institute, made the surmise that it should be possible to construct a Hyper-Græco-Latin square for every value of p, which is a prime or a power of a prime. It is the object of this paper to prove that this surmise is correct, by using the properties of Galois Fields. It is hoped that the properties of Galois Fields, and the finite geometries connected with them, will prove useful in many problems of experimental design and the author hopes to pursue this matter in subsequent papers.

§1 ELEMENTARY PROPERTIES OF GALOIS FIELDS.

1. A set of elements $a, b, c, \ldots\ldots$, is said to form a *field* F when there exist two laws of composition, *viz.*, the addition denoted by + and the multiplication denoted by × or a dot, such that the following axioms are satisfied.

I (*i*) To any two elements a and b of F, there exists a unique element s belonging to F defined by

$$a+b=s$$

(*ii*) $a+b=b+a$

(*iii*) $a+(b+c)=(a+b)+c$

*The word Hyper-Græco-Latin square will throughout this paper be used to mean a completely orthogonalised Hyper-Græco-Latin square.

(*iv*) To any two elements a and b, there exists an element x belonging to F such that

$$a+x=b$$

On the basis of the axioms I (*i*)—(*iv*), regarding the first law of composition *viz.*, the addition, it can be shown that the element x in I (*iv*) is unique, and that there exists a unique element 0 in F with the property that c being any arbitrary element of F, $c+0=c$.

II (*i*) To any two elements a and b of F, there exists a unique element p belonging to F such that

$$a.b=p$$

(*ii*) $a.b=b.a$

(*iii*) $(a.b).c=a.(b.c)$

(*iv*) To any two elements a and b of F, ($b\neq0$), there exists an element y belonging to F, such that

$$y.a=b$$

It can be shown that the element y in II (*iv*) is unique, and F contains a unique element 1, with the property, that c being an arbitrary element of F, c.1 = c.

III $a(b+c)=ab+ac$

It also follows that $a.0=0$, where a is any arbitrary element of F, and that $1\neq0$.

The axioms I (*i*)—(*iv*), II (*i*)—(*iv*) and III, are obviously satisfied by the systems of all rational numbers, all real numbers, all complex numbers, so that these systems provide examples of fields. What interests us here is the existence of systems, containing only a finite number of elements, and yet satisfying all the above axioms. Such systems are called *Galois fields*. We shall briefly sketch their properties here.

2. The simplest example of a Galois field is provided by the field of the classes of residues modulo p, p being any prime positive integer. Let all integers congruent to one other modulo p, be considered to belong to the same class, and let the class to which the integer a belongs be denoted by (a). Then $(a)=(b)$ when and only when $a\equiv b \mod (p)$. Thus there exist only p different classes (0), (1), (2), ... $(p-1)$. The addition and multiplication of these classes are defined by

$$(a)+(b)=(a+b) \qquad \ldots \quad (1\cdot1)$$

$$(a).(b)=(ab) \qquad \ldots \quad (1\cdot15)$$

e.g. if $p=7$, there are seven classes (0), (1), (2), (3), (4), (5), (6).

$$(2)+(3)=(5) \qquad (3)+(5)=(8)=(1)$$

$$(2).(3)=(6) \qquad (3).(5)=(15)=(1)$$

It can be verified that all the axioms I (*i*)—(*iv*), II (*i*)—(*iv*) and III are satisfied. The field considered above is usually symbolised by GF_p. The integer a may be said to be a representative of the class (a). There is only one non-negative integer less than p, representative of (a). This may be called the standard representative of (a). For example if $p=7$, the standard representative of (17) is 3.

3. Sets of elements satisfying all the axioms I, II, III with the possible exception of II (*iv*), may be said to form a commutative ring.

The concept of a polynomial in ordinary algebra can be extended to any field, *viz.* if $a_0, a_1, a_2, \ldots, b_0, b_1, b_2, \ldots$ are elements of any field F, then new elements of the type

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots\ldots\ldots\ldots\ldots$$

constitute the set of polynomials belonging to what may be called the commutative ring F $[x]$, the addition and multiplication being defined in the ordinary way *viz.*

$$(a_0 + a_1 x + a_2 x^2 + \ldots\ldots\ldots) + (b_0 + b_1 x + b_2 x^2 + \ldots\ldots\ldots)$$
$$= (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \ldots\ldots\ldots \qquad \ldots \quad (1{\cdot}2)$$

$$(a_0 + a_1 x + a_2 x^2 + \ldots\ldots\ldots) \times (b_0 + b_1 x + b_2 x^2 + \ldots\ldots\ldots)$$
$$= a_0 b_0 + (a_1 b_0 + a_0 b_1)x + (a_2 b_0 + a_1 b_1 + a_0 b_2)x^2 + \ldots\ldots\ldots \qquad \ldots \quad (1{\cdot}25)$$

For polynomials belonging to $GF_p[x]$, a_0, a_1, etc. are residue classes mod (p).

A polynomial $f(x)$ of $F[x]$ is said to be irreducible, when it is impossible to find polynomials $\phi(x)$ and $\psi(x)$ of $F[x]$ of degrees m and n, $m \geq 1$, $n \geq 1$ satisfying

$$f(x) = \phi(x).\ \psi(x)$$

If however we can find $\phi(x)$ and $\psi(x)$ satisfying the above condition, then $f(x)$ is said to be reducible. $\phi(x)$ or $\psi(x)$ may be called a factor of $f(x)$. The polynomial $f(x)$ may be said to be divisible by $\phi(x)$ or $\psi(x)$.

Let $f(x)$be an irreducible polynomial of $F[x]$. Two polynomials $\phi_1(x)$ and $\phi_2(x)$, may be said to be congruent modulo $f(x)$ if $\phi_1(x) - \phi_2(x)$ is divisible by $f(x)$, and this may be written $\phi_1(x) \equiv \phi_2(x) \bmod f(x)$. The class of polynomials congruent to $\phi(x)$ modulo $f(x)$, being denoted by $[\phi(x)]$, we may define the addition and multiplication of these classes by

$$[\phi(x)] + [\psi(x)] = [\phi(x) + \psi(x)] \qquad \ldots \quad (1{\cdot}3)$$
$$[\phi(x)]\ .\ [\psi(x)] = [\phi(x).\ \psi(x)] \qquad \ldots \quad (1{\cdot}35)$$

It can be shown that these classes form a field. The polynomial $\phi(x)$ may be said to be a representative of the class $[\phi(x)]$. If n is the degree of $f(x)$, there is only one polynomial of degree less than n, representative of $[\phi(x)]$. This may be called the standard representative of $[\phi(x)]$.

4. It is known that the most general Galois field contains p^n elements, where p is a prime positive integer, and n any positive integer. Two Galois fields with the same number of elements, are isomorphic, *i.e.*, structurally identical, a (1,1) correspondence being possible between the elements, in such a way that the sum corresponds to the sum, and the product to the product. The Galois field with p^n elements is usually symbolised by GF_{p^n}.

Every element a other than 0 of GF_{p^n} satisfies the relation

$$a^{p^n - 1} - 1 = 0$$

Because of the isomorphism between any two Galois fields with the same number of elements, it is sufficient to write down the elements of any Galois field with a given number of elements, together with the addition and multiplication table. This may be done in the following manner:—

Consider the Binomial equation $x^{p^n-1}=1$, of ordinary algebra, and obtain in the usual manner the cyclotomic equation, *viz.*, the equation, which has for its roots, all the primitive roots of this equation. It is well known that the degree of this equation will be $m=\varphi(p^n-1)$ where $\varphi(p^n-1)$ denotes the number of integers less than p^n-1 and relatively prime to it. Let this equation be

$$x^m+a_{m-1}\,x^{m-1}+\ldots\ldots\ldots a_0=0 \qquad \ldots \quad (1\cdot5)$$

where $a_{m-1}\ldots a_0$ are integers. If in the left hand side we replace the integers a_i by their residue classes (a_i), modulo p, we get the polynomial

$$x^m+(a_{m-1})x^{m-1}+\ldots\ldots \quad (a_0) \qquad \ldots \quad (1\cdot6)$$

of $GF_p[x]$, which may be called the cyclotomic polynomial of order p^n-1 of $GF_p[x]$. Let $f(x)$ be an irreducible factor of (1·6). Consider the classes of polynomials of $GF_p[x]$ congruent modulo $f(x)$. Then these classes form the required Galois field with p^n elements, the addition and multiplication being carried out according to (1·1), (1·15), (1·2), (1·25), (1·3), (1·35). The degree of $f(x)$ is always n. $f(x)$ may be called the minimum function.

Instead of these classes, we may write down the polynomials which are their standard representatives, and the coefficients of these polynomials which are residue classes modulo p, may also be replaced by their standard representatives; provided we remember this fact at the time of forming sums and products. Then each element of the Galois field assumes the standard form

$$a_0+a_1x+a_2x^2+\ldots\ldots\,.\;+a_{n-1}x^{n-1}$$

where a_0, a_1 etc. are integers taking any value ranging from 0 to $p-1$. It is seen that there are exactly p^n such elements.

§2. CONNEXION OF FINITE GEOMETRIES WITH HYPER-GRÆCO-LATIN SQUARES.

1. We shall now discuss the connexion between a projective geometry with a finite number of points and lines, with Hyper-Græco-Latin Squares. We have to consider two kinds of elements 'points' and 'lines' A given point and a given line may or may not be 'incident'. We make the following axioms regarding points and lines, and the relation of incidence between them:—

(1) There is at least one line, incident with each of two distinct points.

(2) There is not more than one line incident with each of two distinct points.

(3) There is at least one point incident with each of two distinct lines.

(4) Not all points are incident with the same line.

(5) There are at least three points incident with every line.

(6) The number of points incident with at least one line is finite.

It can now be shown that there is not more than one point incident with two distinct lines and if the number of points incident with any one line is $s+1$, then

(*i*) there are precisely $s+1$ points incident with every line.

(*ii*) there are precisely $s+1$ lines incident with every point.

(*iii*) there are in all precisely s^2+s+1 points, and s^2+s+1 lines.

When a point and a line are incident with one another the point may be said to lie on the line, and the line may be said to pass through that point.

A projective geometry satisfying the above axioms (1)—(6), is not possible for every value s; when however such a geometry exists, its existence is exactly equivalent to the existence of an s-sided Hyper-Græco-Latin square. Given any prime number p, and a positive integer n, the Galois field always enables us to construct such a geometry with $s=p^n$, and hence an s-sided Hyper-Græco-Latin square. In the next section we shall discuss the actual procedure of construction, and in the final section consider the special cases $s=4$, 8, 9, 16, 25 and 27; the first three being already known. There of course exist other projective geometries not derivable from Galois fields. Hyper-Græco-Latin Squares belonging to such geometries, will be discussed in a later paper.

2. Take any one of the s^2+s+1 lines, and call it the line at infinity (l). Through each of the $s+1$ points on (l), there pass exactly s straight lines, other than (l) itself these $s(s+1)$ straight lines making up together with (l), the totality of s^2+s+1 straight lines. The s straight lines passing through a given point of (l), may be said to belong to the same parallel pencil. Choose any two points X and Y on (l). The intersections of the s lines forming the parallel pencil with vertex at X, with the s lines forming the parallel pencil with vertex at Y, yield s^2 points, which together with the $s+1$ points on (l), constitute the totality of s^2+s+1 points. The s^2 points not lying on (l) may be called finite points. The s^2+s lines other than (l) we may call finite lines. Let U_1, U_2,………U_{s-1} be the points other than X and Y on (l). The parallel pencils with vertices X, Y, U_i $(i=1, 2,………s-1)$ may be denoted by (X), (Y), (U_i). To the s lines of the pencil (X), we may attach the numbers 0, 1, 2,………$s-1$, one number being attached to each line. The same may be done to the lines of the pencil (Y). Consider now a finite point P. Let x be the number of the line of (X), and y the number of the line of (Y) passing through P. Then (x, y) may be called the coordinates of P. There are just s^2 ordered pairs (x, y) corresponding to the s^2 finite points. If we regard the x-coordinates as the row numbers, and y-coordinates as the column numbers, then the s^2 finite points correspond to the s^2 cells of an s-sided square [the i-th row or column being supposed to have the row or column number $(i-1)$]. The cell corresponding to the point (x, y), we may call the cell (x, y).

3. Now consider the pencil (U_1). We can as before attach in any manner the numbers 0, 1,………$s-1$ to the s lines of the pencil (U_1). Through every finite point there passes one and only one line of (U_1). Let u_1 be the number of the line of (U_1) passing through (x, y). In every cell (x, y) of our s-sided square we then put the corresponding number u_1. The arrangement that we thus get is a Latin square, for any row of our square corresponds to a certain line of the pencil (X), and through the s finite points of this line, there pass the s differnt lines of (U_1), one through each (a similar result holding for the columns). The numbering of the lines of the pencils (X), (Y) and (U_1), having once been fixed, this Latin square is uniquely determined. We shall call it the Latin square $[L_1]$. In the same way after having fixed the numbering of the lines in the pencils (U_2), (U_3), ………(U_{s-1}) we get the Latin squares $[L_2]$, $[L_3]$,……$[L_{s-1}]$. Finally it is clear that the $s-1$ Latin squares so obtained are mutually orthogonal. For if u_i denote the letter of (L_i) (here represented by one of the numbers 0, 1, 2,……$s-1$) in the cell (x, y), then to

any given value of u_i there corresponds a definite line of the pencil (U_i), and this line is met by the s different lines of (U_j), $i \neq j$ in the s finite points on it. Hence a given letter of $[L_i]$, occurs once and only once with every letter of $[L_j]$. The superimposition of the $s-1$ Latin squares we have obtained, gives us a Hyper-Græco-Latin square.

4. Conversely given an s-sided Hyper-Græco-Latin Square, we may call the component Latin squares $[L_1]$, $[L_2]$, ... $[L_{s-1}]$ and may identify their letters with the numbers 0, 1, 2, ... $s-1$. Let u_i denote as before the letter of $[L_i]$ in the cell (x, y). The s^2 cells may now be called finite points. The points corresponding to a fixed value of x, y, u_1, ... or u_{s-1}, may be considered to lie on the same finite line. We thus get s^2+s finite lines. The lines corresponding to the different constant values of (X), may be said to form the pencil (X). In the same way we define the pencils (Y), (U_1), ... (U_{s-1}). From the fact that $[L_1]$, $[L_2]$, ... $[L_{s-1}]$ are mutually orthogonal Latin squares, it is easy to deduce that any two finite points lie on one and only one line, and any two finite lines not belonging to the same pencil, intersect in one and only one finite point. If we now add new conceptual points X, Y, U_1, ... U_{s-1} considered to lie on a line viz. the line at infinity, X being incident with every line of (X), and no other finite line, (similar being the case for the other points Y, U_1, U_2, ... U_{s-1}), we get a plane projective geometry with s^2+s+1 points and as many lines, each line passing through $s+1$ points, and each point lying on $s+1$ lines. The geometry that we get by considering only finite points and finite lines, is the affine geometry of s^2 points and $s(s+1)$ lines. It should be noticed that these two geometries correspond exactly to the two types of orthogonal series of incomplete balanced blocks considered by Yates[3]; so that now it is possible to extend these series to any value of s, which is a prime or a power of a prime.

§3. The method of Construction of the Hyper-Græco-Latin Square.

1. Let $\alpha_0=0, \alpha_1, \alpha_2, \ldots. \alpha_{s-1}$, be the elements of the Galois field GF_{p^n}, $(s=p^n)$. The s^2 ordered pairs (x, y) where x and y are elements of GF_{p^n}, may be regarded as forming the finite points of the geometry discussed in §2. All points (x, y) satisfying a linear equation of the form

$$ax+by+c=0 \qquad \ldots \quad (3\cdot1)$$

where a, b, c, are elements of GF_{p^n}, a and b not being simultaneously 0, may be said to lie on a finite line with the equation (3·1)*. The line whose equation is

$$a'x+b'y+c'=0 \qquad \ldots \quad (3\cdot11)$$

is identical with the line whose equation is (3·1) when and only when

$$bc'-b'c=ca'-c'a=ab'-a'b=0 \qquad \ldots \quad (3\cdot12)$$

Hence the linear equations can be reduced to one of the standard forms

$$x=\alpha_j \qquad (j=0, 1, \ldots\ldots\ldots s-1) \qquad \ldots \quad (3\cdot2)$$

$$y=\alpha_j \qquad (j=0, 1, \ldots\ldots\ldots s-1) \qquad \ldots \quad (3\cdot3)$$

$$x+\alpha_i y=\alpha_j \qquad (i=1, \ldots\ldots s-1, j=0, 1, \ldots s-1) \qquad \ldots \quad (3\cdot4)$$

*It should be remembered that all ordinary algebraic operations are possible, in view of the fact that GF_{p^n} is a field.

Hence there are in all $s+s+s(s-1)=s^2+s$ finite lines.

On any line with equation of the form (3·2), there are exactly s finite points, corresponding to the s different values of y. Similarly on every line with equation of the form (3·3), there are exactly s finite points corresponding to the s different values of x. Finally consider a line with equation of the form (3·4). Given any fixed value of x say a_p, y is uniquely determined (cf§1). Hence there are exactly s points on a line with equation of this form also. Hence every finite line has s points on it.

The lines $x=a_j$ form the parallel pencil (X), the lines $y=a_j$ form the parallel pencil (Y), the lines $x+a_iy=a_j$ (i being fixed), form the parallel pencil (U$_i$). It is easy to see that any two lines not belonging to the same parallel pencil intersect in a unique finite point. It can also be verified that through every finite point, there passes exactly one line of each of the $s+1$ parallel pencils, and that any two finite points are joined by one and only one finite line. We have thus obtained the affine geometry with s^2 points and s^2+s lines. Adding the conceptual points X, Y, U$_1$, ... U$_{s-1}$ regarded as the vertices of the pencils (X), (Y), (U$_1$), ... (U$_{s-1}$) lying on a conceptual line, *viz.* the line at infinity, we get a projective geometry with s^2+s+1 points and s^2+s+1 lines. With this the proof of the existence of an s-sided Hyper-Græco-Latin square when s is a prime or a power of a prime is complete.

2. The simplest way of numbering the lines of the $s+1$ parallel pencils is to associate the number j to any line whose equation is expressed in one of the standard forms (3·2), (3·3), (3·4). Considering as before our Hyper-Græco-Latin square as formed of superimposed Latin squares [L$_1$], [L$_2$], ... [L$_{s-1}$] to find the letter of [L$_i$] in the cell (p,q), we have to find the number of the line belonging to (U$_i$), which passes through the intersection of the line nugber p of (X) and the line number q of (Y). To do this we determine a_j from (3·4), after putting $x=a_p$, $y=a_q$. Then j is the required number. The crux of our whole discussion may now be stated in the form of the following theorem.

THEOREM I. Let $a_0=0$; $a_1, a_2, \ldots\ldots a_{s-1}$ be the elements of the Galois field GF$_{p^n}$, $(s=p^n)$, p being a prime, and n any +ve integer. Consider an s-sided square, and number the rows and columns 0, 1, 2, ... $s-1$, the cell (p, q)* denoting the intersection of the row number p, and the column number q. If now in every cell (p, q) we put the number j determined by

$$a_j=a_p+a_ia_q \text{ (i fixed and non-zero)} \tag{3·5}$$

we get a Latin square [L$_i$]. The s−1 Latin squares [L$_1$], [L$_2$] .... [L$_{s-1}$] are all mutually orthogonal and their superimposition leads to a Hyper-Græco-Latin square.

3. It is clear from the general theorem proved above that the actual form in which we get the Hyper-Græco-Latin square will depend on how the identification between $a_1, a_2, \ldots\ldots a_{s-1}$ and the elements of GF$_{p^n}$ (other than the null element), when expressed in the standard form, is made. In the case $n=1$, *i.e.* when s is a prime number p, the simplest way of identification is to set a_i equal to the residue class (i), modulo p. Our theorem then leads to the standard method of construction of a p-sided Hyper-Græco-Latin square when p is a prime.

*The 'p' of (p, q) numbering the cell should not be confused with the 'p' of $s=p^n$.

4. When however n is not equal to 1, *i.e.* s is a power (other than the first) of a prime, the simplest procedure seems to be as follows:—

Let $f(x)$ be the minimum function, *i.e.* an irreducible factor of the cyclotomic polyniminal of the order p^n-1 of $GF_p[x]$. Then the elements of GF_{p^n} can be represented uniquely by the residue classes modulo $f(x)$ of the polynomials

$$0,\ x^0=1,\ x,\ x^2,\ x^3,\ldots\ldots\ldots x^{s-1} \quad (s=p^n) \qquad \ldots (3\cdot6)$$

We can then identify a_0 with 0, and a_i with the class represented by the x^{i-1}. Since $x^{s-1}=1$, we then get the following rule for the multiplication of the elements of the Galois field.

$$\left.\begin{array}{l} \alpha_i\alpha_j=\alpha_0 \text{ if either } i=0 \text{ or } j=0, \\ \alpha_i\alpha_j=\alpha_l \text{ where } l\equiv(i+j-1) \bmod (s-1),\ 1\leqq l\leqq s-1 \\ \qquad \text{if } i\neq o,\ j\neq o. \end{array}\right| \qquad \ldots (3\cdot7)$$

To apply the fundamental theorem to the construction of Hyper-Græco-Latin squares, it is now only necessary to form the addition table of the elements of GF_{p^n}. To do this we have to express the elements, when given in the form (3·6), in the standard form, and then get the sum. The actual procedure will become clearer by the special cases considered in the next section.

§4. Discussion of Special Cases.

1. Let us apply our method to the construction of a 4-sided Hyper-Græco-Latin Square. Here we have to consider the Galois Field GF_{2^2}. The characteristic of the field is 2, and every element other than 0, satisfies

$$x^3-1=0$$

In GF_2 there are only two elements, having the standard representatives 0 and 1. The ordinary cyclotomic polynomial of order 3, is

$$x^2+x+1$$

and this may be regarded also as the cyclotomic polynomial of $GF_2[x]$, provided we now regard 1 as the standard representative of (1). Since x^2+x+1 is irreducible in $GF_2[x]$, the minimum function $f(x)$ is given by

$$f(x)=x^2+x+1$$

Since our field is of characteristic 2 addition is identical with subtraction. The four elements written in the form (3·6) are the classes represented by 0, 1, x, x^2. When expressed in the standard form they become 0, 1, x, $1+x$. Hence we have

$$\alpha_0=0; \qquad \alpha_1=1; \qquad \alpha_2=x; \qquad \alpha_3=1+x.$$

Since our field is of characteristic 2, in calculating with $\alpha_0, \alpha_1, \alpha_2, \alpha_3$ we must always make $2=0$ since 2 and 0 now stand for (2) and (0) which are identical.

$$\begin{array}{rclcll} \alpha_0+\alpha_i &=& 0+\alpha_i &=& \alpha_i & (i=1,2,3) \\ \alpha_i+\alpha_i &=& 2\alpha_i &=& 0 & (i=1,2,3) \\ \alpha_1+\alpha_2 &=& 1+x &=& \alpha_3 & \\ \alpha_1+\alpha_3 &=& 2+x &=& \alpha_2 & \\ \alpha_2+\alpha_3 &=& 1+2x &=& \alpha_1 & \end{array}$$

Hence we have the following addition table, where to find the sum of α_i and α_j, we look up the element which is common to the row headed by α_i and the column headed by α_j.

α_0	α_1	α_2	α_3
α_1	0	α_3	α_2
α_2	α_3	0	α_1
α_3	α_2	α_1	0

Forming now the Latin square $[L_1]$, $[L_2]$, $[L_3]$ according to our general Theorem 1, using the formula (3·7) for multiplication, and writing their elements in the first, second and third places respectively as in the following scheme, we get the required Hyper-Græco-Latin square.

0 0 0	1 2 3	2 3 1	3 1 2
1 1 1	0 3 2	3 2 0	2 0 3
2 2 2	3 0 1	0 1 3	1 3 0
3 3 3	2 1 0	1 0 2	0 2 1

Considering only the suffixes in the addition table we get the Latin square

0	1	2	3
1	0	3	2
2	3	0	1
3	2	1	0

which we may call the key Latin square. It is then easy to see that the Latin square $[L_1]$ is the same as the key Latin square, while $[L_2]$ and $[L_3]$ have been derived from it by keeping the column number 0 fixed, and cyclically interchanging the columns number 1, 2, 3.

We shall now prove that this result is general for the method of identification adopted by us. Since α_0 is 0, it is clear from Theorem I, that the column number 0, of any one of the Latin squares $[L_i]$, has the numbers

$$0, 1, 2, \ldots\ldots\ldots\ldots s-1$$

so that it remains fixed.

Let now i have any fixed value satisfying $1 \leqq i \leqq s-2$. Let j be the number in the cell (p, q) of $[L_i]$, and j' be the number in the cell $(p, q-1)$ of $[L_{i+1}]$, $p \neq 0$, $q \neq 0$. Then

$$\alpha_j = \alpha_p + \alpha_i \, \alpha_q \qquad\qquad \alpha_{j'} = \alpha_p + \alpha_{i+1} \, \alpha_{q-1}$$

When $q \neq 1$, the formula (3·7) shows that $j = j'$. Hence for $q \neq 1$, the column number $q-1$ of $[L_{i+1}]$ is identical with the column number q of $[L_i]$. In the same way it is seen that the number in the cell $(p, 1)$ of $[L_i]$ is identical with the number in the cell $(p, s-1)$ of $[L_{i+1}]$ so that the column number $s-1$ of $[L_{i+1}]$ is identical with the column number 1 of $[L_i]$. Hence we have

Theorem II. If we make the identification of the elements of the Galois field, in the way considered in the last paragraph of §3, and form the key Latin square $[L_1]$ by taking only the suffixes in the addition table; and form other Latin squares $[L_2]$, $[L_3]$, ... $[L_{s-1}]$ from it by cyclically interchanging the columns number 1, 2, ... $s-1$ of $[L_1]$,* then these $s-1$ Latin squares are mutually orthogonal and their superposition leads to a Hyper-Græco-Latin square.

It is therefore only necessary to construct the key Latin square in any given case. A further simplification will be introduced at a later stage.

2. Let us now consider the case $s=8$. The cyclotomic polynomial of order 7 is

$$x^6+x^5+x^4+x^3+x^2+x+1$$

when regarded as a polynomial of $GF_2[x]$ it can be factorised as $(x^3+x^2+1)\,(x^3+x+1)$. We shall take our minimum function $f(x)$ to be x^3+x^2+1. Then

$$\begin{array}{ll}
\alpha_0 = 0 & \alpha_1 = 1 \\
\alpha_2 = x & \alpha_3 = x^2 \\
\alpha_4 = x^3 = x^2+1 & \alpha^5 = x^4 = x^3+x = x^2+x+1 \\
\alpha_6 = x^5 = x^3+x^2+x = x+1 & \alpha_7 = x^6 = x^2+x
\end{array}$$

* $[L_{i+1}]$ is derived from $[L_i]$ by displacing the columns number 2, 3,......... $s-1$ one step to the left, and carrying the column number 1 to the last column

where we have to remember that since we are considering a field of characteristic 2, addition is the same as subtraction. To form the addition table we have now to find the sum of every two elements, *e.g.*

$$\alpha_4+\alpha_6= (x^2+1)+(x+1)= x^2+x=\alpha_7$$

$$\alpha_5+\alpha_7= (x^2+x+1)+(x^2+x) =1=\alpha_1$$

Forming the addition table and taking only the suffixes, we now have our key Latin square.

0	1	2	3	4	5	6	7
1	0	6	4	3	7	2	5
2	6	0	7	5	4	1	3
3	4	7	0	1	6	5	2
4	3	5	1	0	2	7	6
5	7	4	6	2	0	3	1
6	2	1	5	7	3	0	4
7	5	3	2	6	1	4	0

When the six other Latin squares obtained from it by a cyclic interchange of the columns headed by 1, 2, 3, 4, 5, 6, 7, are superimposed on it, we get an 8-sided Hyper-Græco-Latin square.

3. We shall now consider the case $s=9$. The cyclotomic polynomial of order 8 is x^4+1, and this when regarded as a polynomial of $GF_3[x]$ is factorisable as $(x^2+x+2)(x^2+2x+2)$. Let us then take the minimum function $f(x)$ to be x^2+x+2. Here we are dealing with a field of characteristic 3, so that $3=0$ remembering of course that now our integers are standard representatives of classes of residues mod 3.

$\alpha_0=0$ $\qquad\qquad$ $\alpha_1=1$

$\alpha_2=x$ $\qquad\qquad$ $\alpha_3=x^2=2x+1$

$\alpha_4=x^3=2x^2+x=2x+2$ $\qquad\qquad$ $\alpha_5=2x^2+2x=2$

$\alpha_6=2x$ $\qquad\qquad$ $\alpha_7=2x^2=x+2$

$\alpha_8=x^2+2x=x+1$

Hence forming our addition table and taking only the suffixes we obtain our Key Latin square in the form

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

Superposing on this the seven other Latin squares derivable from it by a cyclic interchange of the columns headed by 1, 2, 3, ... 8, we get a 9-sided Hyper-Græco-Latin square.

4. If we now carefully observe the form of the Key Latin square for the cases $s=4, 8, 9$; then denoting by $j\ (p, q)$ the number in the cell (p, q), we find:

If p and q have any values such that $1 \leq p \leq s-2$, $1 \leq q \leq s-2$ then

$$\left.\begin{array}{lll} \text{(i)} & j\ (p+1,\ q+1)=0 & \text{when } j\ (p,\ q)=0 \\ \text{(ii)} & j\ (p+1,\ q+1)=1+j\ (p,\ q) & \text{when } j\ (p,\ q)=1,\ 2, \ldots\ldots s-2 \\ \text{(iii)} & j\ (p+1,\ q+1)=1 & \text{when } j\ (p,\ q)=s-1 \end{array}\right\} \quad \ldots (4{\cdot}5)$$

We shall now prove these results to be general.

If $\alpha_p+\alpha_q=\alpha_r$ and $\alpha_{p+1}+\alpha_{q+1}=\alpha'_r$ then $j\ (p,\ q)=r$, and $j\ (p+1,\ q+1)=r'$

Now from (3·7) we find, since $1 \leq p \leq s-2$, $1 \leq q \leq s-2$,

$$\alpha_{p+1}=a_1\,\alpha_p, \qquad \alpha_{q+1}=\alpha_1\,\alpha_q$$

$$\alpha'_r \ =\alpha_{p+1}+\alpha_{q+1}=\alpha_1\,(\alpha_p+\alpha_q)=\alpha_1\,\alpha_r$$

When $j\ (p,q)=0$ $r=0$. Hence $\alpha_r=\alpha_0=0$. Thus $\alpha'_r=0$, *ie*, $r'=0$ or $j(p+1,\ q+1)=0$.

When $j(p, q) = r$ $(1 \leq r \leq s-2)$, then $\alpha_{r'} = \alpha_{r+1}$ so that $r' = r+1$. Hence $j(p+1, q+1) = 1 + j(p, q)$

When $j(p, q) = s-1$, $\alpha_{r'} = \alpha_s$ $\alpha_{s-1} = \alpha_1$, so that $r' = 1$. Hence $j(p+1, q+1) = 1$

The rules symbolised by (4·5), introduce a great simplification in the work of constructing the Key Latin square. The row number 0 is always composed of the numbers 0, 1, 2, ... $s-1$, in this order. We now form only the row number 1 of the addition table, and from it the row number 1 of the Key Latin square by taking only the suffixes in the addition table. The remainder of the Key Latin square can now be very quickly filled up. We begin from any number of the row number 1, and proceed by single steps in the direction of the leading diagonal. If the initial number in the row number 1 is 0, then we fill each successive cell we get by 0. If however the initial number is other than 0, then in each successive cell we put a number one greater than the number in the preceding cell; remembering however that when the number $s-1$ is reached in a cell, the succeeding cell must be filled up by the number 1. The unfilled portion of the Key Latin square may now be easily filled up, on account of the symmetry of Key Latin square about the leading diagonal.

Henceforward therefore it is only necessary to specify the numbers, in the row number 1 of the Key Latin square. We shall do this for the cases $s = 16$, 25 and 27.

5. We now consider the case $s = 16$. We have now to deal with the field GF_{2^4} of characteristic 2.

The ordinary cyclotomic polynomial of order 15 is

$$x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$$

Hence the cyclotomic polynomial of $GF_2[x]$ of order 15 is

$$x^8 + x^7 + x^5 + x^4 + x^3 + x + 1$$

which is factorisable as

$$(x^4 + x^3 + 1)\ (x^4 + x + 1)$$

We can therefore take our minimum function $f(x)$ as

$$f(x) = x^4 + x^3 + 1$$

$\alpha_0 = 0$	$\alpha_1 = 1$
$\alpha_2 = x$	$\alpha_3 = x^2$
$\alpha_4 = x^3$	$\alpha^5 = x^4 = x^3 + 1$
$\alpha_6 = x^5 = x^4 + x = x^3 + x + 1$	$\alpha_7 = x^6 = x^4 + x^2 + x = x^3 + x^2 + x + 1$
$\alpha_8 = x^7 = x^4 + x^3 + x^2 + x = x^2 + x + 1$	$\alpha_9 = x^8 = x^3 + x^2 + x$
$\alpha_{10} = x^9 = x^4 + x^3 + x^2 = x^2 + 1$	$\alpha_{11} = x^{10} = x^3 + x$
$\alpha_{12} = x^{11} = x^4 + x^2 = x^3 + x^2 + 1$	$\alpha_{13} = x^{12} = x^4 + x^3 + x = x + 1$
$\alpha_{14} = x^{13} = x^2 + x$	$\alpha_{15} = x^{14} = x^3 + x^2$

Now $\alpha_1+\alpha_0=\alpha_1$, $\alpha_1+\alpha_1=0$, $\alpha_1+\alpha_2=\alpha_{13}$, $\alpha_1+\alpha_3=\alpha_{10}$

$\alpha_1+\alpha_4=\alpha_5$, $\alpha_1+\alpha_5=\alpha_4$, $\alpha_1+\alpha_6=\alpha_{11}$, $\alpha_1+\alpha_7=\alpha_9$

$\alpha_1+\alpha_8=\alpha_{14}$, $\alpha_1+\alpha_9=\alpha_7$, $\alpha_1+\alpha_{10}=\alpha_3$, $\alpha_1+\alpha_{11}=\alpha_6$

$\alpha_1+\alpha_{12}=\alpha_{15}$, $\alpha_1+\alpha_{13}=\alpha_2$, $\alpha_1+\alpha_{14}=\alpha_8$, $\alpha_1+\alpha_{15}=\alpha_{12}$.

Hence the row number one of the Key Latin square is

1, 0, 13, 10, 5, 4, 11, 9, 14, 7, 3, 6, 15, 2, 8, 12

From this the Key Latin square can be formed according to the process explained before. Now by a cyclic interchange of the columns number 1—15, we get 14 other Latin squares, which superimposed on the Key Latin square give us the 16-sided Hyper-Græco-Latin square.

6. Let us now consider the case $s=25$. We have now to deal with the field GF_5, of characteristic 5.

The ordinary cyclotomic polynomial of order 24 is

$$x^8-x^4+1$$

hence the corresponding cyclotomic polynomial of $GF_5[x]$ is

$$x^8+4x^4+1$$

where the integers are now standard representatives of classes of residues modulo 5. This can be factorised as

$$(x^2+2x+3)\ (x^2+x+2)\ (x^2+4x+2)\ (x^2+3x+3)$$

so that we can take our minimum function $f(x)$ as

$$f\ (x)=\quad x^2+2x+3$$

$\alpha_0=0$ $\alpha_1=1$

$\alpha_2=x$ $\alpha_3=x^2=3x+2$

$\alpha_4=x^3=3x^2+2x=x+1$ $\alpha_5=x^4=x^2+x=4x+2$

$\alpha_6=x^5=4x^2+2x=4x+3$ $\alpha_7=x^6=4x^2+3x=3$

$\alpha_8=x^7=3x$ $\alpha_9=x^8=3x^2=4x+1$

$\alpha_{10}=x^9=4x^2+x=3x+3$ $\alpha_{11}=x^{10}=3x^2+3x=2x+1$

$\alpha_{12}=x^{11}=2x^2+x=2x+4$ $\alpha_{13}=x^{12}=2x^2+4x=4$

$\alpha_{14}=x^{13}=4x$ $\alpha_{15}=x^{14}=4x^2=2x+3$

$\alpha_{16}=x^{15}=2x^2+3x=4x+4$ $\alpha_{17}=x^{16}=4x^2+4x=x+3$

$\alpha_{18}=x^{17}=x^2+3x=x+2$ $\alpha_{19}=x^{18}=x^2+2x=2$

$\alpha_{20}=x^{19}=2x$ $\alpha_{21}=x^{20}=2x^2=x+4$

$\alpha_{22}=x^{21}=x^2+4x=2x+2$ $\alpha_{23}=x^{22}=2x^2+2x=3x+4$

$\alpha_{24}=x^{23}=3x^2+4x=3x+1$

Forming now the row number 1 of our addition table, and taking only the suffixes, we get the row number 1, of the Key Latin square as

1, 19, 4, 10, 18, 6, 16, 13, 24, 5, 23, 22, 20, 0, 9, 12, 14, 21, 17, 7, 11, 2, 15, 8, 3.

From this now the Key Latin square can be written down and hence the complete Hyper-Græco-Latin square.

7. Finally let us consider the case $s=27$.

The ordinary cyclotomic polynomial of order 26 is

$$x^{12}-x^{11}+x^{10}-x^{9}+x^{8}-x^{7}+x^{6}-x^{5}+x^{4}-x^{3}+x^{2}-x+1$$

Hence the corresponding cyclotomic polynomial of $GF_3[x]$ is

$$x^{12}+2x^{11}+x^{10}+2x^{9}+x^{8}+2x^{7}+x^{6}+2x^{5}+x^{4}+2x^{3}+x^{2}+2x+1$$

where the integers are now standard representatives of classes of residues modulo 3. This can be factorised as

$$(x^3+2x+1)\ (x^3+2x^2+1)\ (x^3+x^2+2x+1)\ (x^3+2x^2+x+1)$$

We can therefore take our minimum function $f(x)$ as

$$f(x)=x^3+2x+1$$

$$\begin{array}{ll}
\alpha_0=0 & \alpha_1=1 \\
\alpha_2=x & \alpha_3=x^2 \\
\alpha_4=x^3=x+2 & \alpha_5=x^4=x^2+2x \\
\alpha_6=x^5=x^3+2x^2=2x^2+x+2 & \alpha_7=x^6=2x^3+x^2+2x=x^2+x+1 \\
\alpha_8=x^7=x^3+x^2+x=x^2+2x+2 & \alpha_9=x^8=x^3+2x^2+2x=2x^2+2 \\
\alpha_{10}=x^9=2x^3+2x=x+1 & \alpha_{11}=x^{10}=x^2+x \\
\alpha_{12}=x^{11}=x^3+x^2=x^2+x+2 & \alpha_{13}=x^{12}=x^3+x^2+2x=x^2+2 \\
\alpha_{14}=x^{13}=x^3+2x=2 & \alpha_{15}=x^{14}=2x \\
\alpha_{16}=x^{15}=2x^2 & \alpha_{17}=x^{16}=2x^3=2x+1 \\
\alpha_{18}=x^{17}=2x^2+x & \alpha_{19}=x^{18}=2x^3+x^2=x^2+2x+1 \\
\alpha_{20}=x^{19}=x^3+2x^2+x=2x^2+2x+2 & \alpha_{21}=x^{20}=2x^3+2x^2+2x=2x^2+x+1 \\
\alpha_{22}=x^{21}=2x^3+x^2+x=x^2+1 & \alpha_{23}=x^{22}=x^3+x=2x+2 \\
\alpha_{24}=x^{23}=2x^2+2x & \alpha_{25}=x^{24}=2x^3+2x^2=2x^2+2x+1 \\
\alpha_{26}=x^{25}=2x^3+2x^2+x=2x^2+1 &
\end{array}$$

We can now form the row number 1 of the addition table and from this by taking only the suffixes, the row number 1 of the Key Latin square comes out as

1, 14, 10, 22, 2, 19, 18, 12, 5, 16, 4, 7,11, 3, 0, 17, 26, 23, 21, 8, 24, 6, 13, 15, 25, 20, 9.

From this the Key Latin square, and the complete Hyper-Græco-Latin square can be generated, as explained before.

Summary.

By using the properties of the Galois Field GF_{p^n}, it is possible to build up a projective geometry with s^2+s+1 points, and s^2+s+1 lines, where $s=p^n$, p being a prime integer, and n any positive integer. It has been shown that the existence of such a geometry is exactly equivalent to the existence of an s-sided completely orthogonalised Hyper-Græco-Latin square. This completes the proof of the existence of such a square when the number of elements in each row is a prime or a power of a prime. The actual form in which the Hyper-Græco-Latin square will be obtained depends on the manner of identification of the lines forming the pencils defining the coordinates of the points of our geometry, and the elements of the Galois-field. When $n=1$, *i.e.* s is a prime, a certain simple mode of identification is shown to lead to the usual method of construction of Hyper-Græco-Latin square of this special type. When however $n>1$, so that s is a power (other than 1) of a prime, it is shown that there exists a certain method of identification, for which the component Latin squares, of the completely orthogonalised Hyper-Græco-Latin square, are all derivable from one of them, called the Key Latin square, by a simple system of cyclic interchanges. Further it is shown that the Key Latin square itself can be generated from the row number one, according to simple rules. Thus the actual labour of construction is considerably simplified. Actual cases in which $s=4$, 8, 9, 16, 25 or 27 have been discussed.

References.

1. Fisher, R. A.: *The Design of Experiments, Edinburgh*, 2nd Edition, 1937.

2. Yates, F.: *The Design and Analysis of Factorial Experiments Imperial Bureau of Soil Science*, Technical Communication, No. 35, 1937.

3. Yates, F.: Incomplete Randomised Blocks. *Annals of Eugenics*, Vol. VII, part 2, pp. 121—140.

[*Paper received 17 August, 1938*]