FINITE GEOMETRIES AND CERTAIN DERIVED RESULTS IN THEORY OF NUMBERS.

By C. RADHAKRISHNA RAO.

(Communicated by Prof. P. C. Mahalanobis, O.B.E., F.R.S., F.N.I., I.E.S.)

(*Received December 8, 1944.*)

§0. INTRODUCTION.

(1) Singer (1938) proved the theorem that given an integer $m \geqslant 2$ of the form p^n (p being a prime) we can find $(m+1)$ integers

$$d_0, d_1, \ldots d_m \tag{0.10}$$

such that among the $m(m-1)$ differences $d_i - d_j$ ($i, j = 0, 1, 2 \ldots m$; $i \neq j$) reduced modulo m^2+m+1, the integers $1, 2, \ldots m^2+m$ occur exactly once. Bose (1942) gave the following theorem which he called 'the affine analogue of Singer's theorem'. Given an integer $m \geqslant 2$ of the form p^n (p being a prime) we can find m integers

$$d_1, d_2, \ldots d_m \tag{0.11}$$

such that among the $m(m-1)$ differences $d_i - d_j$ ($i, j = 1, 2 \ldots m$; $i \neq j$) reduced modulo m^2-1, all the positive integers less than m^2-1 and not divisible by $q = m+1$ occur exactly once.

(2) In this paper, I have derived a chain of theorems of the form, given an integer v, it is possible to find 's' sets of 'k' integers each—

$$\left.\begin{array}{l} d_{11}, d_{21}, \ldots d_{k1} \\ d_{12}, d_{22}, \ldots d_{k2} \\ \ldots\ldots\ldots\ldots \\ d_{1s}, d_{2s}, \ldots d_{ks} \end{array}\right\} \tag{0.20}$$

such that among the $sk(k-1)$ differences $d_{ir} - d_{jr}$ ($i, j = 1, 2 \ldots k$; $i \neq j$ and $r = 1, 2 \ldots s$) reduced modulo v, all integers less than v and not divisible by θ occur λ_1 times and those divisible by θ, λ_2 times. The value of v is either $(m^{t+1}-1)/(m-1)$ or (m^t-1) where $m = p^n$ (p being prime) and θ, either $(m^{t+1}-1)/(m^2-1)$ or $(m^t-1)/(m+1)$.

(3) These theorems are derived from a compact representation of d ($<t$) dimensional flats in a 't' dimensional finite space. If the points in a Projective or an Euclidean finite space of 't' dimensions are denoted by $1, 2 \ldots v$, then the compact representation consists in finding s ($<b$, the total number of d-dimensional flats in a t-space) d-dimensional flats, with points on it represented by integers, which generate the totality of the 'b' flats by the successive addition of

integers 1, 2 . . . v, and reduction to modulo v. The addition of the integers is carried on till the points of the flat are repeated in our process. The 's' flats which generate the totality are called the initial flats.

(4) The theorems of Singer and Bose come out from the compact representation of the lines in t-dimensional Projective geometry $PG(t, m)$ and the Euclidean geometry $EG(t, m)$.

(5) Incidentally, we arrive at cyclical solutions to combinatorial problems such as the Kirkman's school girl problem and Incomplete balanced designs derivable from finite geometries.

(6) It is, also, well known that the (m^t-1) degrees of freedom involved in the contrasts of m^t objects can be split into $(m^t-1)/(m-1)$ independent sets of $(m-1)$ degrees of freedom each; each set representing the comparisons arising out of m groups of m^{t-1} objects in each group. It has been shown that the existence of a difference set, possessing the properties mentioned in the present paper, is a sufficient condition for the splitting of the degrees of freedom.

(7) Various other theorems which are of interest in the theory of numbers and in the solution of combinatorial problems have been discussed at length and a variety of other problems, which have been partly solved, are reserved for a subsequent communication.

(8) Lastly, I wish to offer my thanks to Mr. R. C. Bose, Lecturer in the Department of Statistics in the Calcutta University, for his helpful guidance and criticism during the preparation of this paper.

§1. Finite Geometries.

(A) *Projective Space.*

(1) Veblen and Bussey have defined a finite projective geometry in the following way. It consists of a set of elements called points, for suggestiveness, which are subject to the following five conditions or postulates:—

(i) The set contains a finite number of points. It contains one or more subsets called lines, each of which contains at least three points.

(ii) If A and B are two distinct points, there is one and only one line that contains both A and B.

(iii) If A, B and C are non-collinear points and if a line 'm' contains a point D of the line AB and a point E of the line BC but does not contain A or B or C, then the line 'm' contains a point F of the line AC.

(iv_t) If 'k' is an integer less than t, not all the points considered are in the same k-space.

(v_t) If (iv_t) is satisfied, there exists in the set of points considered no $(t+1)$-space.

(2) The geometry, so defined, is said to be a geometry of the t-dimensional space. A point is called 0-space or flat and a line 1-space or flat. An m-space is inductively defined as follows. A 2-space which is called a plane consists of points which are collinear with a point not lying on a line and any point of the line. A 3-flat can be defined starting from a plane. In general, if $P_1, P_2, \ldots P_{m+1}$ are points not all in the same $(m-1)$-space, then the set of all points each of which is collinear with P_{m+1} and some point of the $(m-1)$-space formed by $P_1, P_2, \ldots P_m$ is the m-space formed by $P_1, P_2, \ldots P_{m+1}$.

(B) *Analytical Representation of the Projective Geometry.*

(3) With the help of the Galois field $GF(p^n)$, we can construct a finite projective geometry of 't' dimensions in the following manner. Any ordered set of $(t+1)$ elements

$$(x_0, x_1, \ldots x_t) \tag{1.30}$$

where the x's belong to $GF(p^n)$ and are not simultaneously zero, will be called a point. Two sets $(x_0, x_1, \ldots x_t)$ and $(y_0, y_1 \ldots y_t)$ represent the same point when and only when there exists an element $\sigma \neq 0$ of $GF(p^n)$ such that $y_i = \sigma x_i$ $(i = 0, 1, 2, \ldots t)$. We may call $x_0, x_1, \ldots x_t$ the co-ordinates of the point (1.30). All the points which satisfy a set of $(t-d)$ independent linear homogeneous equations

$$a_{i0}x_0 + a_{i1}x_1 + \ldots a_{it}x_t = 0 \tag{1.31}$$
$$i = 1, 2, \ldots, t-d.$$

may be said to form a 'd' dimensional subspace or a flat. The set of equations (1.31) may be said to represent this flat. The geometry, thus defined, is known to satisfy the postulates of Veblen and Bussey and is represented by $PG(t, p^n)$.

(4) We shall now take up another analytical representation which is fruitful for further work. In this case, a point of $PG(t,\ m = p^n)$ is represented by (ν) where ν is a non-zero element of $GF(m^{t+1})$. Two elements ν and $b\nu$, where b is an element of $GF(m)$, represent the same point which may be written as (ν) or $(b\nu)$. A d-flat is defined by the set of points

$$(a_0\nu_0+a_1\nu_1+\dots a_d\nu_d) \tag{1.40}$$

where a's run independently over the elements of $GF(m)$ and are not simultaneously zero and (ν_0), (ν_1), ... (ν_d) do not lie on a $(d-1)$-flat. Thus $(a_0\nu_0+a_1\nu_1)$ represents a line passing through the points (ν_0) and (ν_1) and $(a_0\nu_0+a_1\nu_1+a_2\nu_2)$, a plane through three non-collinear points (ν_0), (ν_1) and (ν_2). It is easy to verify that the geometry defined above satisfy the postulates of a finite projective geometry.

(5) The following considerations show the correspondence between the two types of representations given in paras (3) and (4) above. If x is a primitive element of $GF(m^{t+1})$, it satisfies an irreducible equation of the $(t+1)$th degree.

$$x^{t+1}-(a_tx^t+a_{t-1}x^{t-1}+\dots+a_0) = 0 \tag{1.50}$$

in $GF(m)$. The left-hand side expression is known as the minimum function. Since all the elements of $GF(m^{t+1})$ are residue classes mod $(x^{t+1}-a_tx^t-\dots a_0)$, it follows that any element of $GF(m^{t+1})$ can be represented either as a power of the primitive element x or a polynomial of degree less than $(t+1)$. If

$$x^k = b_tx^t+b_{t-1}x^{t-1}+\dots+b_0 \tag{1.51}$$

then the correspondence (x^k) as a point represented by an element of $GF(m^{t+1})$ and $(b_0, b_1, \dots b_t)$ as a point represented by an ordered set of the elements of $GF(m)$ is unique and connects up the two types of representations mentioned above.

(C) *The Euclidean Space.*

(6) The Euclidean geometry of 't' dimensions, denoted by $EG(t,\ m)$, is derivable from $PG(t,\ m)$ by cutting out one $(t-1)$-flat and all the points lying on it. The points of $EG(t,\ m)$ can be represented by ordered sets

$$(b_1, b_2, \dots b_t) \tag{1.60}$$

where the b's are elements of $GF(m)$. Two sets $(b_1, b_2, \dots b_t)$ and $(c_1, c_2, \dots c_t)$ represent the same point when and only when $b_i = c_i$ $(i = 1, 2, \dots t)$. All points which satisfy a set of $(t-d)$ consistent and independent linear equations

$$a_{i0}+a_{i1}b_1+\dots+a_{it}b_t = 0 \tag{1.61}$$
$$i = 1, 2, \dots t-d$$

may be said to form a d-flat.

(7) As in the case of the projective geometry, a similar representation is available in the case of $EG(t,\ m)$. A point is represented by (ν) where ν is an element of $GF(m^t)$, each element representing a unique point. A d-flat is defined by the totality of the points

$$(a_0\nu_0+a_1\nu_1+\dots+a_d\nu_d) \tag{1.70}$$

where the a's run through the elements of $GF(m)$ subject to the restriction $\Sigma a = 1$.

(8) If x is a primitive element of $GF(m^t)$ then the elements can be represented by the powers of x or their residue classes with respect to a minimum function of the t-th degree. If

$$x^k = b_tx^{t-1}+b_{t-1}x^{t-2}+\dots+b_1x^0 \tag{1.80}$$

then the correspondence

$$(x^k) \longrightarrow (b_1, b_2, \dots b_t) \tag{1.81}$$

brings out the identity of the representations of $EG(t,\ m)$ mentioned in paras. (6) and (7) above.

(9) It is easily derivable, from above, that the number of 'd' flats in $PG(t,\ m)$ and $EG(t,\ m)$ are $\phi(t, d, m)$ and $\phi(t, d, m)-\phi(t-1, d, m)$ respectively where

$$\phi(x, y, z) = \frac{(z^{x+1}-1)\dots(z^{x-y+1}-1)}{(z^{y+1}-1)\dots(z-1)} \tag{1.90}$$

§2. The Compact Representation of the d-flats.

(1) In this section it is proposed to enumerate the d-flats in $PG(t,\ m)$ and $EG(t,\ m)$ and consider the possibilities of representing them compactly.

(A) *General Considerations.*

(2) The d-flat in $PG(t, m)$, through the points $(x^{b_0}), (x^{b_1}), \ldots (x^{b_d})$ is given by

$$(\Sigma a_i x^{b_i}) \tag{2.20}$$

where a's are the elements of $GF(m)$, not all simultaneously zero. Let us consider the totality of the flats

$$(\Sigma a_i x^{b_i+\theta}) \tag{2.21}$$

for $\theta = 0, 1, 2, \ldots v-1$, where $v = (m^{t+1}-1)/(m-1)$. The flat corresponding to $\theta = \theta_i$ may be represented by (θ_i). We have the following results:

(i) *The flat (θ_i) is d-dimensional for all 'i'*, for, if not, there exist elements $c_0, c_1, \ldots c_{d-1}$ of $GF(m)$ such that

$$x^{b_d+\theta_i} = c_0 x^{b_0+\theta_i} + \ldots + c_{d-1} x^{b_{d-1}+\theta_i} \tag{2.22}$$

or

$$x^{b_d} = c_0 x^{b_0} + \ldots + c_{d-1} x^{b_{d-1}}$$

which shows that (2.20) is not d-dimensional contrary to our supposition.

(ii) If θ is the least value for which (θ) is identical with (0) or the initial flat, then θ may be called the cycle of the initial flat. In this case $(0), (\theta), (2\theta), \ldots (v)$ are all identical. Hence, it follows that θ, *the cycle of the initial flat is a divisor of v defined above.*

(iii) If (x^{c_i}) is a point on an initial flat with cycle θ, then $(x^{c_i+k\theta})$, where k is any integer, is also a point on the initial flat, for $(x^{c_i+k\theta})$ is a point on $(k\theta)$ which is identical with (0). Hence we get the result that *the points on an initial flat of cycle θ are given by (recording only powers of x's)*

$$\left.\begin{matrix} c_0, & c_0+\theta, \ldots & c_0+\overline{r-1}\,\theta \\ c_1, & c_1+\theta, \ldots & c_1+\overline{r-1}\,\theta \\ \cdots\cdot & \cdots & \cdots\cdot \\ c_p, & c_p+\theta, \ldots & c_p+\overline{r-1}\,\theta \end{matrix}\right\} \tag{2.23}$$

where $c_i-c_j \not\equiv 0 \bmod \theta$ and $v = r\theta$.

(iv) The number of points in (2.23) is evidently a multiple of r which gives the result that a necessary condition for a cycle $\theta<v$ for a d-flat is that *$\phi(t, 0, m)$, the number of points in a t-space and $\phi(d, 0, m)$, the number of points in a d-space are not relatively prime.*

(v) If $\theta<v$ is the cycle of an initial flat such as (2.23), then we can choose the flat with the points obtained by subtracting any c_i from all the powers of x's representing the points in (2.23), as an initial flat from which θ different flats can be generated.

(B) *Lines in $PG(t, m)$.*

(3) There are $v = (m^{t+1}-1)/(m-1)$ points, $b = \phi(t, 1, m)$ lines with $k = m+1$ points on each line. Through a point and a pair of points there pass $\phi(t-1, 0, m)$ lines and one line respectively.

(4) Since the points on an initial flat of cycle θ are of the form (2.23) with $c_0 = 0$, we can take its equation as

$$(a_0 x^0 + a_1 x^\theta) \tag{2.40}$$

If (x^c) is a point on it, then $(x^{c+\theta})$ is also a point and the line can be represented by

$$(a_0 x^{0+c} + a_1 x^{\theta+c}) \tag{2.41}$$

which shows that c must be a multiple of θ, the cycle of the initial flat, in which case all the points are of the form, recording only powers of x,

$$0, \theta, 2\theta, \ldots (r-1)\theta \tag{2.42}$$

where $r = (m+1)$. So, we get *the necessary condition for a partial cycle θ is that $\theta = v/(m+1)$ is integral. This is also sufficient,* for the line $(a_0 + a_1 x^\theta)$ where $\theta = v/(m+1)$ has the cycle θ.

(5) Hence we get the following theorems:

(i) *If $\theta = (m^{t+1}-1)/(m^2-1)$ is not integral, then every line has the cycle v and the totality of the lines can be generated from $\eta = (m^t-1)/(m^2-1)$ initial lines.*

Since the necessary and sufficient condition for a partial cycle to exist is not satisfied, every line has the cycle v. Since the total number of lines is $(m^{t+1}-1)(m^t-1)/(m^2-1)(m-1)$ the number of initial lines which generate the totality is $(m^t-1)/(m^2-1)$ which is necessarily integral if θ is not integral. Any pair of points occur in one and only one line.

(ii) *If* $\theta = (m^{t+1}-1)/(m^2-1)$ *is integral, the totality of the lines are generated from* $\eta = m(m^{t-1}-1)/(m^2-1)$ *initial lines of cycle* v *and the line* $(a_0+a_1x^\theta)$ *of cycle* θ.

As shown above only lines generated from $(a_0+a_1x^\theta)$ have the cycle θ and others v. Therefore, the other lines form into $\eta = (b-\theta)/v = m(m^{t-1}-1)/(m^2-1)$ groups *which is necessarily integral if* $(m^{t+1}-1)/(m^2-1)$ *is integral.* The pair of points (x^{c_i}) and (x^{c_j}) occur once in the lines generated from $(a_0+a_1x^\theta)$ when and only when $c_i-c_j \equiv 0 \pmod{\theta}$. Hence it follows that the pair (x^{c_i}) and (x^{c_j}) occur in one and only one of the lines generated from η initial lines of cycle v when and only when $c_i-c_j \not\equiv 0 \pmod{\theta}$.

(C) *Planes in PG(t, m).*

(6) There are $v = (m^{t+1}-1)/(m-1)$ points and $b = \phi(t, 2, m)$ planes with $k = (m^3-1)/(m-1)$ points on each plane. Through every point there pass $r = \phi(t-1, 1, m)$ planes and through a pair of points, $\lambda = \phi(t-2, 0, m)$ planes.

(7) Let us consider a plane with cycle $\theta<v$. If the point $(x^{2\theta})$ lies on the line joining (x^0) and (x^θ) then the points $(x^{i\theta})$ for all i lie on it; hence the integer $s = v/\theta$ must divide $(m+1)$. But the necessary condition demands that $(m^3-1)/(m-1)$ is divisible by s which is not possible since $(m+1)$ and $(m^3-1)/(m-1)$ do not have a common factor. Therefore (x^0), (x^θ) and $(x^{2\theta})$ are not collinear, and so constitute a plane. If (x^c) is any point on this, then (x^{0+c}), $(x^{\theta+c})$ and $(x^{2\theta+c})$ are also points on this which shows that the planes $(a_0x^0+a_1x^\theta+a_2x^{2\theta})$ and $(a_0x^{0+c}+a_1x^{\theta+c}+a_2x^{2\theta+c})$ are identical. This leads to the result that c is a multiple of θ, hence all points are of the form $(x^{i\theta})$ where $\theta = v/k$. Hence we get *the necessary condition for the existence of a partial cycle* θ *is that* $\theta = (m^{t+1}-1)/(m^3-1)$ *is integral. This is also sufficient,* for the plane $(a_0x^0+a_1x^\theta+a_2x^{2\theta})$ has the cycle θ.

(8) Hence we get the following theorems:

(i) *If* $\theta = (m^{t+1}-1)/(m^3-1)$ *is not integral, then all the planes have the cycle* v *and the totality of the planes can be generated from* $\eta = (m^t-1)(m^{t-1}-1)/(m^3-1)(m^2-1)$ *initial planes.*

The total number of planes is $\phi(t, 2, m)$ which form into $b/v = (m^t-1)(m^{t-1}-1)/(m^3-1)(m^2-1)$ groups *which is necessarily integral if* θ *is not integral.* Any given pair of points occur in $\lambda = (m^{t-1}-1)/(m-1)$ planes in the totality of the generated planes.

(ii) *If* $\theta = (m^{t+1}-1)/(m^3-1)$ *is an integer, then the totality of the planes can be generated from* $\eta = (m-1)[(m^t-1)(m^{t-1}-1)/(m^2-1)(m-1)-1]/(m^3-1)$ *initial planes of cycle* v *and the plane* $(a_0+a_1x^\theta+a_2x^{2\theta})$ *of cycle* θ.

The proof is similar to that given in theorem (ii) of para. (5).

(9) As a corollary to this theorem we get since η is necessarily integral

$$\frac{(m^t-1)(m^{t-1}-1)}{(m^3-1)(m^2-1)} \equiv 1 \left(\operatorname{mod} \frac{m^3-1}{m-1}\right) \text{ if } (t+1) \equiv 0 \pmod{3}.$$

(10) The pair of points (x^{c_i}) and (x^{c_j}) occur once in the planes generated from $(a_0+a_1x^\theta+a_2x^{2\theta})$ if and only if $c_i-c_j \equiv 0 \pmod{\theta}$. Hence the pair (x^{c_i}), (x^{c_j}) occurs in λ or $\lambda-1$ times in the planes generated from η initial planes of theorem (ii) according as $c_i-c_j \not\equiv$ or $\equiv 0 \pmod{\theta}$.

(D) *3-flats in PG(t, m).*

(11) There are $v = (m^{t+1}-1)/(m-1)$ points, $b = \phi(t, 3, m)$, 3-flats, with $(m^4-1)/(m-1)$ points on each. Through a point and a pair of points there pass $r = \phi(t-1, 2, m)$ and $\lambda = \phi(t-2, 1, m)$, 3-flats respectively.

(12) Let us consider the 3-flats with cycle $\theta<v$. If $(x^{2\theta})$ is collinear with (x^0) and (x^θ), then $(x^{i\theta})$ for all i lies on the line formed by (x^0) and (x^θ). Also, if (x^c) is a point on it, because of the relation

$$a_0x^{0+c}+a_1x^{\theta+c} = x^{2c} \tag{2.12,0}$$

obtained by multiplying $a_0x^0+a_1x^\theta = x^c$ by x^c, it follows that (x^{2c}) and hence (x^{ic}) for all i are points on the line. If (x^b) is any point on the initial 3-flat with cycle θ, then (x^{b+jc}) for all j are points on it, for multiplying

$$a_0x^0+a_1x^\theta = x^{jc} \tag{2.12,1}$$

by x^b

we get
$$a_0x^{0+b}+a_1x^{\theta+b}x = x^{b+jc} \tag{2.12,2}$$

Hence we get that the 3-flats $(a_0x^0+a_1x^\theta+a_2x^b)$ and $(a_0x^{0+c}+a_1x^{\theta+c}+a_2x^{b+c})$ are identical which leads to the result that c is a multiple θ and $\theta = v/(m+1)$ is an integer. Thus we get that a 3-space with cycle θ consists of the following (m^2+1) lines defined by the points on them as (recording only powers of x)

$$\left.\begin{array}{lll} 0, & \theta, & \ldots m\theta \\ c_1, & c_1+\theta, & \ldots c_1+m\theta \\ \ldots & \ldots & \ldots \\ c_{m^2}, & c_{m^2}+\theta, & \ldots c_{m^2}+m\theta \end{array}\right\} \tag{2.12,3}$$

From the representation of lines in $PG(t, m)$ we find that the lines of the form (2.12,3) are θ in number generated from the initial line (recording only powers of x)

$$0, \theta, \ldots m\theta \tag{2.12,4}$$

All the 3-flats of cycle θ are built up by taking any two lines from the θ lines generated from (2.12,4).

(13) Let us consider the initial flats of cycle $\theta_1<v$ where θ_1 is such that the points (x^0), (x^{θ_1}), $(x^{2\theta_1})$ are not collinear. Evidently $(x^{3\theta_1})$ cannot lie on the plane formed by (x^0), (x^{θ_1}) and $(x^{2\theta_1})$, for in this case $(m^3-1)/(m-1)$ and $(m^4-1)/(m-1)$ have a common factor which is not possible. Hence the 3-flat with cycle θ_1 is determined by the four points (x^0), (x^{θ_1}), $(x^{2\theta_1})$ and $(x^{3\theta_1})$ and only points of the form $(x^{i\theta})$ for any i lie on it. Hence it follows that $\theta_1 = v(m-1)/(m^4-1) = (m^{t+1}-1)/(m^4-1)$ is integral and also $\theta/\theta_1 = (m^2+1)$ which is an integer. These 3-flats are also built out of the lines (2.12,3).

(14) Hence we get the following theorems:

(i) *If* $\theta = (m^{t+1}-1)/(m^2-1)$ *is not integral, the totality of the* 3-*spaces can be generated from* $\eta = \phi(t, 3, m)/\phi(t, 0, m)$ *initial* 3-*spaces of cycle* v.

Any pair of points occur in λ of the total 3-spaces.

(ii) *If* $\theta = (m^{t+1}-1)/(m^2-1)$ *is integral and* $\theta_1 = (m^{t+1}-1)/(m^4-1)$ *is not integral, the totality of the* 3-*spaces can be generated from* $y = (m^{t-1}-1)/(m^4-1)$ *initial* 3-*spaces of cycle* θ *and* $\eta = (b-\theta y)/v$ *initial* 3-*spaces of cycle* v.

The point pair (x^{c_i}) and (x^{c_j}) appear $(\lambda-1)$ times and once in the totality of 3-spaces of cycles v and θ respectively when and only when $c_i-c_j \not\equiv 0 \pmod{\theta}$ and $\lambda-(m^{t-1}-1)/(m^2-1)$ and $(m^{t-1}-1)/(m^2-1)$ times when $c_i-c_j \equiv 0 \pmod{\theta}$.

(iii) *If* $\theta_1 = (m^{t+1}-1)/(m^4-1)$ *is integral in which case* $\theta = (m^{t+1}-1)/(m^2-1)$ *is necessarily integral, the totality of the* 3-*spaces can be generated from the same number of initial* 3-*spaces of cycle* v *as in theorem* (ii), *and* $y = m^2(m^{t-3}-1)/(m^4-1)$ *initial* 3-*spaces of cycle* θ *and the initial* 3-*spaces* $(a_0x^0+a_1x^{\theta_1}+a_2x^{2\theta_1}+a_3x^{3\theta_1})$ *of cycle* θ_1.

The point pair (x^{c_i}), (x^{c_j}) occur in $\lambda-1$, 1, 0, 3-spaces or $\lambda-1$, 0, 1, 3-spaces of cycles v, θ and θ_1 respectively according as $c_i-c_j \not\equiv 0 \pmod{\theta_1}$ or is $\equiv 0 \pmod{\theta_1}$ and $\not\equiv 0 \pmod{\theta}$. They occur in $\lambda-(m^{t-1}-1)/(m^2-1)$, $(m^{t-1}-1)/(m^2-1)-1$ and 1, 3-spaces of cycles v, θ and θ_1 respectively when $c_i-c_j \equiv 0 \pmod{\theta}$.

(E) *d-spaces in PG(t, m).*

(15) We can now generalise the theorems mentioned to the case of d-flats in $PG(t, m)$. There are $v = (m^{t+1}-1)/(m-1)$ points, and $b = \phi(t, d, m)$, d-flats with $k = (m^{d+1}-1)/(m-1)$ points on each d-flat. Through a point and a pair of points there pass $r = \phi(t-1, d-1, m)$ and $\lambda = \phi(t-2, d-2, m)$ d-flats respectively.

(16) We have the following theorems:

(i) *If* $(m^{t+1}-1)/(m-1)$ *and* $(m^{d+1}-1)/(m-1)$ *do not have a common factor of the form* $(m^{s+1}-1)/(m-1)$, *then all the d-spaces have the cycle v and can be generated from* $\eta = \phi(t, d, m)/\phi(t, 0, m)$ *initial d-flats.*

As a consequence of this we get that $(t-1)$-spaces in a t-space are of cycle v for $\phi(t, 0, m)$ and $\phi(t-1, 0, m)$ do not have a common factor of the form $\phi(s, 0, m)$.

(ii) *If* $r_1, r_2, \ldots r_p$ *are integers such that*

(*a*) $0 < r_1 < r_2 < \ldots\ldots r_p < t$

(*b*) $(m^{d+1}-1)/(m^{r_i+1}-1) = s_i$ integral for all i

(*c*) $(d+1)/(r_i+1) \quad = t_i$,,

(*d*) $(r_{i+1}+1)/(r_i+1) \quad = l_i$,,

(*e*) $(m^{t+1}-1)/(m^{r_i+1}-1) = \theta_i$,,

then there are

$$y_i = (n_i - n_{i+1})/\theta_i \text{ where } n_i = {}_{\theta_i}c_{t_i}/{}_{s_i}c_{t_i}$$

initial spaces of cycle θ_i $(i = 1, 2, \ldots p)$ *and*

$$\eta = (b-n_1)/v$$

initial spaces of cycle v from which the totality of the d-spaces can be generated.

The proof can be built up on lines suggested in particular cases. The pair of points (x^{c_i}) and (x^{c_j}) occur in $(\lambda-\lambda_1)$ and λ_1, d-spaces of cycles v and less than v respectively when $c_i - c_j \equiv 0 \pmod{\theta_1}$ and $(\lambda - \lambda_2)$ and λ_2, d-spaces of cycle v and less than v when $(c_i - c_j) \not\equiv 0 \pmod{\theta_1}$. The values of λ_1 and λ_2 are respectively

$$_{\theta_1}c_{t_1-1}/_{s_1-1}c_{t_1-1} \text{ and } _{\theta_1}c_{t_1-2}/_{s_1-2}c_{t_1-2}.$$

(F) *d-spaces in EG(t, m).*

(17) The m^t points in $EG(t, m)$ are represented by (0), $(x^0), \ldots (x^{m^t-2})$ where x is a primitive element of $GF(m^t)$. If b is the total number of d-flats in $EG(t,m)$, then there are $b-\phi(t-1, d-1, m)$ d-flats passing through (0). *Any flat not passing through the point* (0) *has the cycle* $v = (m^t-1)$, for, if not, it follows that (m^t-1) and m^d have a common factor, which is impossible.

(18) Let us consider a d-flat passing through (0),

$$(a_0 0 + a_1 x^{b_1} + \ldots a_d x^{b_d}) \tag{2.18,0}$$

where $a_1, a_2, \ldots a_d$ are elements of $GF(m)$ and the restriction $(a_0 + a_1 + \ldots + a_d = 1)$ need not be imposed for the coefficient of a_0 is 0. Since

$$0, x^0, x^\theta, \ldots\ldots x^{(m-2)\theta} \tag{2.18,1}$$

where $\theta = (m^t-1)/(m-1)$ are the elements of $GF(m)$, it follows that if (x^c) is a point on (2.18,0) then $(x^{c+i\theta})$ for any i lies on it. From this we, at once, get the lines through (0) as

$$(0), (x^i), (x^{i+\theta}) \ldots \tag{2.18,2}$$
$$i = 0, 1, \ldots (\theta-1)$$

and any d-space is built out of d suitably chosen lines from (2.18,2). All these d-flats, passing through (0), have their cycle as θ or some integer less than θ.

(19) It can be easily shown that a pair of points (x^{c_i}) and (x^{c_j}) can occur together only in flats through (0) when $c_i - c_j \equiv 0 \pmod{\theta}$. Hence any such point pair occur together $\lambda = \phi(t-2, d-2, m)$ and 0 times in the d-flats passing through the (0) and not passing through (0) respectively. Also the triplet (0), (x^{c_i}), (x^{c_j}) where $c_i - c_j \not\equiv 0 \pmod{\theta}$ lie on $\lambda_1 = \phi(t-3, d-3, m)$ d-flats. Hence we get, *that the pair of points* (x^{c_i}) *and* (x^{c_j}) *occur together in* λ_1 *and* $\lambda-\lambda_1$, *d-flats passing through the origin and not passing through the origin respectively if* $c_i - c_j \not\equiv 0 \pmod{\theta}$.

(20) Not all d-flats through (0) have the cycle θ. If $\theta_1 < \theta$ is a cycle then $\theta = r_1\theta_1$, in which case the d-flats of cycle θ_1 are built out of the r_1-dimensional spaces defined by

$$\left.\begin{array}{l} 0,\ (x^i),\ (x^{i+\theta})\ldots \\ \quad (x^{i+\theta_1}),\ (x^{i+\theta_1+\theta})\ldots \\ \quad \ldots\ldots\ldots\ldots\ldots \\ \quad (x^{i+\overline{r_1-1}\,\theta_1}),\ (x^{i+\overline{r_1-1}\,\theta_1+\theta})\ldots \end{array}\right\} \qquad (2.20,0)$$
$$i = 0,\ 1,\ \ldots.(\theta_1-1).$$

From this it follows that (m^d-1) is divisible by $(m^{r_1}-1)$ and the number of d-flats that can be built out of (2.20,0) is ${}_{\theta_1}c_{t_1}/{}_{s_1}c_{t_1}$ where $s_1 = (m^d-1)/(m^{r_1}-1)$ and $t_1 = d/r_1$. Out of these we have to search for flats of cycle $\theta_2 < \theta_1$ and so on.

(21) Hence we get the following theorems:

(i) *All the d-flats* $b_1 = \phi(t, d, m) - 2\phi(t-1, d-1, m)$ *in number not passing through* (0) *have* $v = (m^t-1)$ *as their cycle and hence can be generated from* $\eta = b_1/v$ *initial d-flats. The point pair* $(x^{c_i}), (x^{c_j})$ *occur in* $\phi(t-2, d-2, m) - \phi(t-3, d-3, m)$ *or* 0 *of these flats according as* $c_i - c_j \not\equiv 0$ *or* $\equiv 0\left(\bmod \dfrac{m^t-1}{m-1}\right)$.

(ii) *Any d-flat through* (0) *is built out of the* θ *lines*

$$0,\ (x^i),\ (x^{i+\theta})\ldots. \qquad (2.21,0)$$
$$i = 0,\ 1,\ \ldots\ (\theta-1)$$

and if (m^d-1) *and* (m^t-1) *do not have any common factor of the form* (m^r-1) *other than* $(m-1)$, *then all the d-flats through* (0) *have the cycle* θ *and hence can be generated from* $y = \phi(t-1, d-1, m)/\theta$ *initial d-flats. The pair of points* (x^{c_i}) *and* (x^{c_j}) *occur in* $\phi(t-2, m-2, m)$ *or* $\phi(t-3, d-3, m)$ *of these flats according as* $c_i - c_j \equiv 0$ *or* $\not\equiv 0$ *(mod* θ*).*

(iii) *In general if* $h = p_0 p_1^{i_1} p_2^{i_2}\ldots$ *(where* $p_0 = 1$ *and p's are primes such that* $p_i < p_{i+1}$*) is the H.C.F. of d and t, then the d-flats through the* (0) *will have cycles of the form* $\theta_{js} = (m^t-1)/(m^{r_{js}}-1)$ *where* $r_{js} = p_1^{i_1} p_2^{i_2}\ldots p_j^{s}$ $(j = 0, 1, \ldots;\ s = 0, 1, \ldots i_j)$. *The number of initial flats from which all flats of cycle* θ_{js} *can be generated is given by*

$$(n_{js} - n_{j+1,\,s+1})/\theta_{js} \qquad (2.21,1)$$

where n_{js} *is the number of d-flats that can be generated from* θ_{js}*-flats of* r_{js}*-dimensions having only* (0) *in common which comes out as*

$$n_{js} = {}_{\theta_{js}}c_{d/r_{js}}/{}_{q_{js}}c_{d/r_{js}} \qquad (2.21,2)$$

where $q_{js} = (m^d-1)/(m^{r_{js}}-1)$.

The number of d-flats of cycle θ_{js} through a given point pair can be easily ascertained in particular cases.

§3. Generalisation of the Difference Theorems of Bose.

(1) In this section, certain theorems known as difference theorems of Bose (1939) have been generalised to obtain a further simplification in the presentation of the geometry and to derive the theorems of the next article.

(A) *The First Theorem of Differences.*

(2) Let m be a modul or an Abelian group satisfying the additive postulates of a field containing the v elements

$$x^{(0)},\ x^{(1)},\ \ldots\ x^{(v-1)} \qquad (3.20)$$

To these we add an element ∞ which remains invariant for any addition of the elements of m to it. Thus

$$\infty + x^{(i)} = x^{(i)} \text{ for all } i \qquad (3.21)$$

The totality of the $(v+1)$ elements of m and ∞ may be denoted by M. Let $B_1, B_2, \ldots B_h$ represent sets of $k_1, k_2, \ldots k_h$ distinct elements of M respectively. By the successive addition of the elements of m to the set B_i containing k_i elements, m sets of k_i elements are formed. By repeating this process on $B_1, B_2, \ldots B_h$ we get mh sets in which there are m sets of $k_1, k_2, \ldots k_h$ elements. The sets $B_1, B_2, \ldots B_h$ from which the totality of the sets is generated are called the initial sets. We get the following results:

(i) If ∞ occurs r_∞ times in all the initial sets, then it occurs mr_∞ times in the totality of the generated sets and *vice versa*, for ∞ remains invariant for the addition of the elements of m.

(ii) Any element of m occurs $(k_1+k_2+\ldots k_h-r_\infty)$ times in the totality of the sets, for any element of m in any initial set generates all the elements of m by successive addition of the elements of m.

(iii) If ∞ and $x^{(i)}$ occur together in $\lambda_{\infty i}$ of the totality of mh sets then the total number of elements of m that occur in the initial sets in which ∞ occurs is $\lambda_{\infty i}$, for if ∞ and $x^{(j)}$ any element of m occur in any initial set then the set obtained by the addition of $\theta = x^{(i)}-x^{(j)}$ contains ∞ and $x^{(i)}$.

(iv) If $x^{(i)}$ and $x^{(j)}$ $(i \neq j)$ occur λ_{ij} times in all the sets, then it is possible to find λ_{ij} ordered pairs $(x^{(i')}, y^{(j')})$ in the initial sets such that for each pair

$$x^{(i')}-y^{(j')} = x^{(i)}-x^{(j)} \tag{3.22}$$

the above relation holds and conversely, for if a pair $x^{(i)}$ and $x^{(j)}$ occur in a set obtained from the addition of θ to an initial set then the pair of elements $x^{(i')}$ and $x^{(j')}$ from which $x^{(i)}$ and $x^{(j)}$ are obtained are such that

$$x^{(i')}+\theta = x^{(i)} \text{ and } x^{(j')}+\theta = x^{(j)} \tag{3.23}$$

and hence the result. Conversely, if a pair of elements $x^{(i')}$ and $x^{(j')}$ are found in any initial set satisfying the condition (3.22), then $x^{(i)}$ and $x^{(j)}$ appear in the set obtained by the addition of θ given by any equation in (3.23).

(3) Hence we get the following theorem:

If in the totality of the sets generated from the initial sets $B_1, B_2, \ldots B_h$ containing $k_1, k_2, \ldots k_h$ distinct elements of M,

(i) ∞ *and* $x^{(i)}$ *occur in* $\lambda_{\infty i}$ *sets,*
(ii) $x^{(i)}$ and $x^{(j)}$ $(i \neq j)$ *occur in* λ_{ij} *sets,*
(iii) ∞ *occurs* mr_∞ *times*;

then in the totality of the sets

(*a*) $\lambda_{\infty 0} = \lambda_{\infty 1} = \lambda_{\infty 2} = \ldots \lambda_{\infty\, m-1} = \lambda_\infty$
(*b*) *Every element of* m *is repeated* $\Sigma k - r_\infty$ *times;*

and in the initial sets the following hold good:

(α) ∞ *occurs* r_∞ *times.*
(β) *The number of elements of* m *that occur in the initial sets in which* ∞ *occurs is* λ_∞.
(γ) *From an initial set* B_i *with* k_i *elements, we can form* $k_i(k_i-1)$ *ordered pairs of elements* (x, y) *which supply* $k_i(k_i-1)$ *values of differences* $(x-y)$. *Under the conditions of this theorem the* $\Sigma k_i(k_i-1)$ *differences arising from all the initial sets contain the elements* $(x^{(i)}-x^{(j)})$, λ_{ij} *times for all* i *and* j *such that* $i \neq j$.

Conversely, if (α), (β) *and* (γ) *hold with the initial sets then* (i), (ii), (iii) *and* (*a*) *and* (*b*) *are true.*

(B) *The Second Theorem of Differences.*

(4) Let us consider the modul of residue classes (mod m) where m is an integer, so that the elements may be represented by $0, 1, 2 \ldots, (m-1)$. If θ is the least value for which an initial set is reproduced, then the initial set is said to have a cycle θ. Since the addition of m is equivalent to addition of 0 in which case the set remains the same, it follows that $m/\theta = p$ is an integer. The initial set with k elements is then composed of the elements

$$e_i,\ e_i+\theta,\ \ldots\ e_i+(p-1)\theta \tag{3.40}$$
$$i = 1, 2, \ldots n$$

such that $e_i - e_j \not\equiv 0 \pmod{\theta}$. Hence $k = np$ where n is integral.

As a necessary condition for an initial set with k elements other than ∞ to have a cycle less than m is that the H.C.F. of m and k is not unity. The following results hold for such sets:

(i) In the θ sets generated all pairs of elements of m with differences as multiples of θ occur n times each.

(ii) Given the set of elements (3.40) we can by a suitable adjustment write it as

$$g_i,\ g_i+\theta,\ \ldots\ g_i+(p-1)\theta \qquad i = 1, 2, \ldots n \tag{3.41}$$

such that $g_i<\theta$ for all i and $(g_i-g_j) \not\equiv 0 \pmod{\theta}$. The set can be compactly represented in this case by

$$(g_1, g_2, \ldots g_n)_\theta \tag{3.42}$$

If a pair of elements (x, y), such that $x-y \not\equiv 0 \pmod{\theta}$, occur in the totality of the sets generated from (3.41), then there exists a pair of elements $g_r+p_1\theta$ and $g_s+p_2\theta$ in an initial set together with an element $g_t<\theta$ such that

$$g_r+p_1\theta+g_t = x,\ g_s+p_2\theta+g_t = y \tag{3.43}$$

from which we get

$$x-y \equiv \overline{g_r-g_s} \pmod{\theta} \tag{3.44}$$

(iii) Hence we get the result that if a pair of elements (x, y, $x-y \not\equiv 0 \bmod \theta$) appear in λ_{xy} of the generated sets it is possible to find a pair of g's in (3.42) such that the condition (3.44) holds.

(5) Hence we get the following theorem:

If in the totality of the sets generated from the initial sets B_1, B_2 ... B_h with k_1, k_2 ... k_h elements and having a cycle θ,

(i) *∞ occurs θr_∞ times,*
(ii) *∞ and i occur in $\lambda_{\infty i}$ sets,*
(iii) *i and j such that $i-j \not\equiv 0 \pmod{\theta}$ occur in λ_{ij} sets,*

then

(I) $\lambda_{\infty 0} = \lambda_{\infty 1} = \lambda_{\infty 2} = \ldots \lambda_{\infty (m-1)} = \lambda_\infty$

(II) *k_i or k_i-1 in the case in which ∞ occurs in the set B_i is divisible by $p = m/\theta$ and the quotient may be denoted by q_i,*

and in the totality of the sets

(*a*) *every element of m is repeated Σq_i times,*
(*b*) *a pair of elements i and j such that $i-j \equiv 0 \pmod{\theta}$ appear in Σq_i sets,*

and in the initial sets

(α) *∞ occurs r_∞ times,*
(β) *the initial blocks can be compactly represented by reducing the elements to modulo θ and omitting the repeated elements and among the differences arising from the reduced sets λ_{ij} differences are congruent to $(i-j) \pmod{\theta}$,*
(γ) *$\lambda_\infty = \Sigma' q_i$ where Σ' denotes summation over the initial sets in which ∞ occurs.*

Conversely if (α) *and* (β) *hold in the initial sets, then* (i), (ii), (iii) *and* (I), (II) *and* (*a*) *and* (*b*) *are true.*

(6) By combining the theorems (A) and (B) and also introducing sets with different cycles we can build up a comprehensive theorem. Only the λ's which give the number of times a pair of elements occur in the totality are to be built up by the addition of λ's from the various groups.

§4. Theorems of the Number Theory.

(1) With the help of theorems of §3 we can translate the theorems of §2 giving the compact representation of the finite geometries into theorems of the form mentioned in §0. We have already seen that the points on any flat can, as well, be represented by powers of x, the primitive element of $GF(m^{t+1})$ or $GF(m^t)$, reduced modulo v and the flat (c) obtained by multiplication of the equation to the initial flat by x^c can be represented by the powers of x's obtained by

adding c to the corresponding powers in the initial flat and reduction to modulo v. The point (0) in the Euclidean geometry will then correspond to ∞ mentioned in §3.

(A) *General Theorems.*

(2) Corresponding to the theorem of the form, that in the totality of the flats generated from η initial flats of cycle v, the number of points in the geometry, the points (x^{c_i}) and (x^{c_j}) occur in λ_1 or λ_2 flats according as $c_i-c_j \not\equiv 0$ or $\equiv 0 \pmod{\theta}$ we get the following theorem. Given an integer $m = p^n$ (p being a prime) it is possible to find η sets of k integers each

$$\left.\begin{array}{l} d_{11},\ d_{12},\ \ldots\ d_{1k} \\ d_{21},\ d_{22},\ \ldots\ d_{2k} \\ \ldots\ \ldots\ \ldots \\ d_{\eta 1},\ d_{\eta 2},\ \ldots\ d_{\eta k} \end{array}\right\} \tag{4.20}$$

such that the differences $d_{ir}-d_{is}$ ($r, s = 1, 2, \ldots k$, $r \neq s$; $i = 1, 2, \ldots \eta$) reduced modulo v (which we may call the differences arising from the difference set 4.20) contain all integers less than v and not divisible by θ, λ_1 times and those divisible by θ, λ_2 times. The η sets (4.20) are called initial sets of cycle v which, in this theorem, is of the form $(m^{t+1}-1)/(m-1)$ or (m^t-1) and θ is of the form $(m^{t+1}-1)/(m^2-1)$ or $(m^t-1)/(m-1)$ and k is of the form $(m^{d+1}-1)/(m-1)$ or m^d. The method of obtaining the difference set (4.20) is to replace the points on the η initial flats of any finite geometry by the powers of x's, reduced modulo v. It is easily seen that the set (4.20) can be replaced by any set obtained by the addition of an integer b and reduction to mod v without destroying its property given above. We may say that two sets are identical if one can be derived from the other by the addition of an integer and reduction to (mod v). If $(a_0x^{c_0}+a_1x^{c_1}+a_2x^{c_2}+ \ldots)$ is the equation of a flat with a given cycle, then $(a_0x^{c_0}+a_1x^{c_1}+a_2x^{c_2}+ \ldots)^{p^q}$, where p is the prime of the above theorems, represents a flat of the same dimensions and with same cycle for

$$(a_0x^{c_0}+a_1x^{c_1}+\ldots)^{p^q} = a_0x^{c_0p^q}+a_1x^{c_1p^q}+\ldots.$$

This leads us to the result that the difference set (4.20) is identical with the set obtained by the transformation

$$d_{rs}p^q+b \equiv d'_{rs} \pmod{v}.$$

(3) Corresponding to the theorem of the form that in the totality of the d-flats containing k elements each generated from y initial flats of cycle θ, the pair of points (x^{c_i}) and (x^{c_j}) occur in $y\mu_1$ or μ_2 flats according as $c_i-c_j \equiv 0$ or $\not\equiv 0 \pmod{\theta}$ we get the following theorem:

Given an integer $m = p^n$ (p being a prime) it is possible to find y sets of μ_1 integers

$$\begin{array}{l} g_{11},\ g_{12}\ \cdots\ g_{1\mu_1} \\ g_{21},\ g_{22}\ \cdots\ g_{2\mu_1} \\ \cdots\ \ \ \cdots\ \cdots \\ g_{y1},\ g_{y2}\ \cdots\ g_{y\mu_1} \end{array} \tag{4.30}$$

such that the differences arising from them (mod θ) contain every integer less than θ, μ_2 times.

(B) *Some Special Theorems and Examples.*

(4) Considering the lines in $PG(t, m)$ we get the following theorems when m is an integer of the form p^n (p being a prime).

(i) *If $\theta = (m^{t+1}-1)/(m^2-1)$ is not integral, it is possible to find $y = (m^t-1)/(m^2-1)$ sets*

$$\begin{array}{c} d_{0j},\ d_{1j},\ \ldots\ d_{mj} \\ j = 1, 2, \ldots y \end{array} \tag{4.40}$$

such that the differences arising (mod v) contain the integers less than v once and once only.

Example (i). Consider $PG(4, 2)$ with 31 points and 155 lines. We choose the line (a_0+a_1x). In the choice of the next line we need only see that the powers of the base points do not have a difference congruent (mod 31) to any difference arising out of the powers of the points in the first line. Similarly a third line is chosen, etc. as the initial lines. In this case

$$(a_0+a_1x), \quad (a_0+a_1x^2)$$
$$(a_0+a_1x^4), \quad (a_0+a_1x^7)$$
$$(a_0+a_1x^8)$$

are suitably chosen lines with the points

$$[(x^0), (x^1), (x^{18})] \quad [(x^0), (x^2), (x^5)]$$
$$[(x^0), (x^4), (x^{10})] \quad [(x^0), (x^7), (x^{22})]$$
$$[(x^0), (x^8), (x^{20})]$$

from which we immediately write down the difference set as

$$(0, 1, 18) \quad (0, 2, 5)$$
$$(0, 4, 10) \quad (0, 7, 22)$$
$$(0, 8, 20)$$

with the property that the differences arising from them (mod 31) contain all integers less than 31, 7 times each. The 155 lines of the geometry can also be compactly represented by these 5 initial lines from which the totality can be generated.

(ii) *If* $\theta = (m^{t+1}-1)/(m^2-1)$ *is integral, it is possible to find* $\eta = m(m^{t-1}-1)/(m^2-1)$ *sets*

$$d_{0j}, d_{1j}, \ldots d_{mj}$$
$$j = 1, 2, \ldots y$$

such that the differences arising from them [*mod* $(m^{t+1}-1)/(m-1)$] *contain all integers less than* v *and not divisible by* θ *once and those divisible by* θ, *zero times.*

The lines of the geometry $PG(t, m)$ can be generated from the above difference set with cycle v and the set $(0, \theta, 2\theta, \ldots m\theta)$ with cycle θ.

Example (ii). Consider $PG(3, 2)$ with 15 points and 35 lines. The geometry can be represented by the initial lines

$$(a_0+a_1x^8) \ (a_0+a_1x^{11})$$

of cycle 15 and the line $(a_0+a_1x^5)$ of cycle 5. By taking powers of x's we get the difference sets

$$(0, 6, 8), \quad (0, 11, 14)$$

of cycle 15 and (0, 5, 10) of cycle 5.

(5) Consider the lines in $EG(t, m)$, we get the following theorem for a given integer $m = p$ (p being a prime).

It is possible to find $\eta = (m^{t-1}-1)/(m-1)$ *sets of integers*

$$d_{i1}, d_{i2}, \ldots d_{im}$$
$$i = 1, 2, \ldots \eta$$

such that the differences arising from them (*mod* $v = (m^t-1)$) *contain all integers less than* v *and not divisible by* $\theta = v/(m-1)$ *once and those divisible by* θ *zero times.*

The geometry is represented by $v\eta$ lines developed from the above difference set and the θ lines generated from

$$\infty, 0, \theta, \ldots \overline{m-2}\theta$$

with cycle θ. The choice of lines is as before.

Example. Consider $EG(3, 3)$ with 117 lines and 27 points choosing the initial lines

$$(a_0+a_1x^i) \quad i = 1, 2, 3, 7$$

of cycle 26, we get the difference set

$$(0, 1, 22); \ (0, 2, 8); \ (0, 3, 14); \ (0, 7, 17)$$

where the differences arising from them (mod 26) contain all integers except 13 once. The lines of the geometry are generated from the four sets above of cycle 26 and the set $(\infty, 0, 13)$ of cycle 13.

(6) We give here two general theorems for $m = p^n$ (p being prime):

(i) Considering d-flats in $PG(t, m)$ we get

(*a*) *If* $v = (m^{t+1}-1)/(m-1)$ *and* $k = (m^{d+1}-1)/(m-1)$ *do not have a common factor of the form* $(m^{s+1}-1)/(m-1)$, *then it is possible to find* $y = \phi(t, d, m)/\phi(t, 0, m)$ *sets of integers*

$$d_{i1}, d_{i2}, \ldots d_{ik}; \quad i = 1, 2, \ldots y$$

such that the differences arising from them (mod v*) contain all integers less than* v, $\lambda = \phi(t-2, d-2, m)$ *times.*

(*b*) *If* r_1 *is the integer for which* $(m^{r_1+1}-1)/(m-1)$ *divides both* $(m^{t+1}-1)/(m-1)$ *and* $(m^{d+1}-1)/(m-1)$, *it is possible to find*

$$\eta = [\phi(t, d, m) - {}_{\theta_1}c_{t_1}/{}_{s_1}c_{t_1}]/v$$

sets of integers such that the differences arising from them (mod v*) contain all integers less than* v *and not divisible by* $\boldsymbol{\theta_1}$, $\lambda-\lambda_2$ *times and those divisible by* $\boldsymbol{\theta_1}$, $\lambda-\lambda_1$ *times where*

$$\theta_1 = (m^{t+1}-1)/(m^{r_1+1}-1); \; s_1 = (m^{d+1}-1)/(m-1); \; t_1 = (d+1)/(r_1+1)$$

$$\lambda_1 = {}_{\theta_1}c_{t_1-1}/{}_{s_1-1}c_{t_1-1}$$

$$\lambda_2 = {}_{\theta_1}c_{t_1-2}/{}_{s_1-2}c_{t_1-2}$$

which are the constants discussed in §2, *para.* (16).

(ii) *Considering the d-flats in* $EG(t,m)$ *we get that it is possible to find*

$$y = [\phi(t, d, m) - 2\phi(t-1, d-1, m)]/(m^t-1)$$

sets of m^d *integers such that the differences arising from them mod* $v = (m^t-1)$ *contain all integers less than* $\boldsymbol{v}$ ***and not divisible by*** $\theta = (m^t-1)/(m-1)$, $\phi(t-2, d-2, m) - \phi(t-3, d-3, m)$ *times and rest zero times.*

(C) *Splitting into Orthogonal Groups.*

(7) Considering the $(t-1)$-flats in $EG(t, m)$ we get the set of $k = m^d$ integers

$$d_1, d_2, \ldots d_k \tag{4.70}$$

such that the differences arising from them mod $v = (m^t-1)$ contain all integers less than v and not divisible by θ, m^{t-2} times each and those divisible by θ, zero times. A method of constructing such difference sets was discussed in (Rao: 1944*a*).

If we represent the sets obtained by the addition of an integer c to (4.70) and reduction to mod v, by (c), we get the result that the elements common to (c_1) and (c_2) is m^{t-2} or 0 according as $c_1-c_2 \not\equiv 0$ or $\equiv 0$ (mod θ). For if x is an element common to (c_1) and (c_2) then there exist integers y_1 and y_2 in (4.70) such that

$$y_1+c_1 \equiv x \equiv y_2+c_2 \tag{4.71}$$

or

$$y_1-y_2 \equiv c_2-c_1 \tag{4.72}$$

and conversely, there exists a common element to (c_1) and (c_2) if there exist a pair of numbers y_1 and y_2 such that (4.72) is satisfied. Hence the result stated above.

(8) We consider the θ groups of sets

$$(i), \; (i+\theta), \ldots (i+\overline{m-2}\,\theta), \; (r_i) \tag{4.80}$$
$$i = 0, 1, 2, \ldots (\theta-1)$$

where (r_i) is the set of integers less than v other than those contained in the sets (i), $(i+\theta)$, ... $(i+\overline{m-2}\,\theta)$. They possess the following properties:—

(*a*) No two sets in a group can have an integer in common by the above result.

(*b*) The groups $(i+r\theta)$ and $(j+s\theta)$ have m^{t-2} integers in common if $i \neq j$.

(*c*) $(i+s\theta)$ and (r_j) $(i \neq j)$ have m^{t-2} integers in common.

(*d*) (r_i) and (r_j), $(i \neq j)$ also have m^{t-2} integers in common.

The θ groups have, then, the property that any set of a group is built out of m^{t-2} integers chosen from each set of any other group. Such groups may be called orthogonal groups. Thus we get the result that $(m^t-1)/(m-1)$ orthogonal groups consisting of m sets of m^{t-1} objects each can be formed with m^t objects when m is prime or a prime power. This result is very important in splitting of degrees of freedom in the design of experiments in statistics and also in reduction of quadratic forms. A fuller treatment of these topics is reserved for a subsequent communication.

§5. Further Problems.

(1) By the use of the theorems developed in this paper some cyclic solutions have been obtained for combinatorial problems involved in the classical example of Kirkman's school girl problem and in the construction of incomplete block designs (Rao: 1944*b*).

(2) It has been shown that the existence of a difference set need not, always, imply the existence of a finite geometry.

(3) The problem as to the existence of these difference sets when m is not a prime or a prime power is under consideration.

(4) New methods for the quick derivation of the difference sets have been investigated.

(5) Some of the results already arrived at will form the topic of another communication.

Bibliography.

Bose, R. C. (1939). On the Construction of Balanced Incomplete Block Designs. *Ann. Eugen.*, **9**, 353–399.
——— (1942). The Affine Analogue of Singer's Theorem. *Proc. Ind. Sci. Cong.* (1942).
Rao, C. R. (1944*a*). Extension of the Difference Theorems of Singer and Bose. *Science and Culture*, **10**, 57.
——— (1944*b*). Some new Cyclic Solutions of Incomplete Block Designs. *Proc. Ind. Sci. Cong.* (1945).
Singer, J. (1938). A Theorem in Finite Projective Geometry and some Applications to the Number Theory. *Trans. Am. Math. Soc.*, **43**, 377–85.

ON FOSSIL FISH-TEETH FROM THE NICOBAR ISLANDS.[1]

By K. Krishnan Nair, *M.Sc., Gallery Assistant, Zoological Survey of India.*

(Communicated by Rai Bahadur S. L Hora, D.Sc., F.R.S.E., F.N.I.)

(*Received January 10, 1945.*)

The fossil fish-teeth described below were sent by the Geological Survey of India to Dr. S. L. Hora for identification. After a preliminary study, he handed over the material to me for a detailed report. I am very grateful to him for affording me an opportunity to study these interesting fossils.

The history of these specimens is very meagre. They were collected along with specimens of celts and rocks on the Trincat Island, Nicobars, and presented to the Geological Survey of India in March 1941 by Mr. R. H. Scott, K.I.H., Assistant Commissioner, Nicobars, the Andamans. No further information regarding the localities, etc. from which the material was collected is available.

Class **Elasmobranchii.**

Genus *Carcharodon* M. and H.

This is an imperfect tooth of a shark. The base towards the sides is broken off and the enamel coating near the tip of the crown on its outer surface is also chipped off in certain

[1] Published with permission of the Director, Zoological Survey of India. This paper had been accepted in 1942 for publication in the *Rec. Geo. Surv. Ind.*, but due to the cessation of publication of the journal, it could not be published. My grateful thanks are due to the Director, Geological Survey of India, for permitting me to publish this article in the *Proc. National Inst. Sci. India.*—K. K. Nair, Supdt. of Fisheries, Bengal.

areas. The tooth had presumably been used as an implement of some kind and as a result the lateral serrations which are of importance for specific identification have disappeared while the outer surface is polished to a considerable degree. However, enough traces of serration are left in some places (Pl. IV, fig. 3) for the identification of the tooth.

The crown of the tooth is fairly large and triangular. Its outer surface is highly convex while the inner is more or less flat, with the apex of the crown gently bending inwards. The base of the tooth is concave. Both the outer and inner surfaces of the crown are ornamented with vertical striae which are more in number on the outer convex surface than on the inner flat surface. The lateral edges and the tip are thin and sharp, but this may be due to the grinding which the tooth had been subjected to while in use as an implement. The lateral edges are definitely serrated, though in the specimen, they are not easily made out. The greatest thickness of the tooth, 18 mm., is in the centre of the crown towards the base. The whole tooth is grey coloured.

This tooth is apparently of a shark of the genus *Carcharodon* Müller and Henle, species of which, according to Zittel possess large teeth and are abundantly represented in the Tertiary and later formations of nearly all parts of the world, and also on the beds of existing oceans. They are mostly Tertiary but one species is reported from the Upper Cretaceous and one recent species is also known.

With the kind permission of Mr. V. P. Sondhi, Assistant Director, Geological Survey of India, I was able to study and compare some of the type specimens of *Carcharodon* fossil teeth in the collections of the Geological Survey of India with the above specimen. This tooth exhibits striking resemblance to some teeth of *Carcharodon megalodon* Agassiz. The lateral edges are bent since the tooth itself is slightly arched inwards, as in the case of the type-specimen, No. 7780 of the Geological Survey of India, which was identified and described as a lateral tooth of *C. megalodon* Ag. by Noetling. Presumably the unequal lateral sides might have influenced the author to assign to it a lateral position. Noetling was not sure of the horizon from which his material came, but Stuart (1910) in a later article says that the specimen was collected by Noetling from the Pegu shales at Padaukpin. The age of the Pegu shales is believed to be Middle Tertiary. The sides of the fossil tooth described above are symmetrical, and its general shape is exactly like that of an imperfect tooth described and identified by Martin as of *Carcharodon megalodon* Ag. from the Tertiary of Europe. In the absence of the marginal serrations referred to above it is not possible to definitely assign the tooth to any species of *Carcharodon.*

Genus *Oxyrhina* Agassiz (Pl. IV, figs. 4-5.)

The crown and the base of this tooth are fully exposed. The inner surface of the crown is convex while the outer surface is flattened. The convex surface, just above the base, is slightly constricted in the middle region. The tip of the crown is slightly hooked laterally and as a result the sharp lateral edges of the tooth are unequal. The convex surface bears a number of vertical striae more or less confined to the middle region. The enamel of the crown descends lower at the sides than at the centre so that the boundary line is in the shape of an obtuse angle. Lateral denticles are absent in this specimen. The whole crown is highly polished, of an ivory white colour resembling somewhat the claw of a tiger.

This tooth does not possess any crenulations or longitudinal ridges on the crown near the base, as in some of the type-specimens of *Oxyrhina triangularis* Egerton or *O.* (*Meristodon*) sp., preserved in the collections of the Geological Survey of India. But its general shape, absence of lateral denticles and serrations along the lateral edges would justify its reference to the genus *Oxyrhina* Agassiz, species of which are distributed from the Cretaceous to the recent times.

Class **Teleostei.**

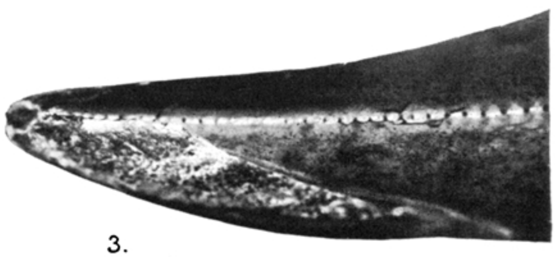
Genus *Diodon* Linn (Pl. IV, figs. 6, 7 and 8).

The three available pieces, *a*, *b*, and *c* are the inner dental plates of a species of the genus *Diodon* Linn. These plates are situated immediately behind the modified jaws, both the upper and the lower. The pieces (*a*) and (*b*) appear to belong to the same plate (Pl. IV, figs. 7 and 8), while piece (*c*) (Pl. IV, fig. 6) belongs to a different species.

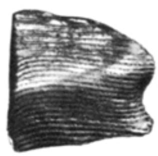
The dental plates are formed by more or less oblique piles of lamellae with crenulated edges closely pressed together. The lamellae are unequal in size; the biggest lamellae lie near

1.

2.

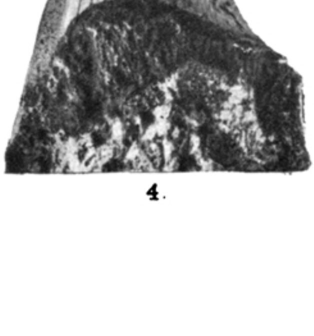


3.



6.

7.



4.

5.

8.

the middle and the smallest are at the apex. These lamellae are divided into symmetrical halves by a vertical line. On the exposed face, there is a sort of rough parallelogram, with its longest axis transversely placed, slightly raised from the rest of the face. The parallelogram in its turn shows a gradual concavity in the centre. There are about twenty-seven closely packed lamellae in this plate (Pl. IV, figs. 7 and 8).

This dental plate differs from that of *Diodon scillae* Agassiz (Woodward, pp. 572-573) in not possessing a constricted waist, while it differs from *D. foleyi* from Ramri Island, off the Arakan Coast (Lydekker, 1880, pp. 59, 60), in not having a pronounced concavity on the exposed face. In *D. ventus* (Leidy, pp. 255-256) the number of lamellae is very small, about ten. The apex of the dental plate of *D. sigma* (Martin, pp. 726-727; Rothpletz and Simonelli, Pl. xxxvi, figs. 1, 1*a*) is rather truncate and not slightly tapering as in the present specimen; further there are only about eighteen lamellae in it. The dental plate of *D. sinhaleyus* (Deraniyagala, pp. 365-366) also does not agree fully with the tooth in question, for the apex is more or less ovate and there is a much smaller number of lamellae in it. Out of the two common recent species, only one, *Diodon histrix* Linn., possesses an inner dental plate. This plate, while it is similar in shape to the fossil plate in question, has a smaller number of lamellae. Hence this plate has to be left as belonging to species of the genus *Diodon* which according to Zittel occurs in the Eocene, Oligocene and Miocene.

The specimen *c* (Pl. IV, fig. 6) is one-half of the inner dental plate of a species of *Diodon*. It differs from the two halves described above in having a sort of constricted waist and resembles closely the inner dental plate of *Diodon scillae* Ag., as figured by Woodward in his 'Catalogue of Fossil Fishes in the British Museum'. *Diodon scillae*, according to Woodward, has been reported from the Miocene of Italy, Sicily and Malta.

List of References.

Deraniyagala, P. E. P. (1937). Miocene Fishes from Ceylon. *Spol. Zeylanica*, **20**, 365-366.

Leidy, Jos. (1842). *Journ. Acad. Nat. Sci. Philadelphia*, **8**, 255-256, pl. xxxiv, figs. 15-16.

Lydekker, R. (1880). Teeth of Fossil Fishes from Ramri Island and the Punjab. *Rec. G.S.I.*, **13**, 59-60.

——— (1886). Indian Tertiary and Post-Tertiary Vertebrata. *Pal. Indica*, Ser. X, **3**, 257, pl. xxxv, figs. 10 and 10*a*.

Martin, K. Palaeontologische Ergebnisse von Tiefbohrungen Aoy Java. *Sammlungen des Geologischen Reichs Mus. Leiden*, **3**, 23-24, pl. 1, figs. 12 and 12*a*.

Noetling, Fritz (1901). Fauna of the Miocene Beds of Burma. *Pal. Indica*, New Series I, pt. 3, 374, pl. xxv, fig. 8.

Rothpletz, A. and Simonelli, V. (1890). *Zeitschr. d. Deutsch. geol. Ges.*, **42**, 726-727, pl. xxxvi, figs. 1 and 1*a*.

Stuart, Murray (1910). Fossil Fish Teeth from the Pegu System. *Rec. G.S.I.*, **38**, 292-301.

Von Zittel, K. A. (1902). *Text Book of Palaeontology*, **2**.

Woodward, A. S. (1901). *Catal. Fossil Fish. Brit. Mus.*, **4**, 572-573.

Explanation of Plate IV.

Fig. 1.—Outer surface of an imperfect tooth of *Carcharodon* Müller and Henle.
Fig. 2.—Inner surface of the same.
Fig. 3.—Side view of the same.
Fig. 4.—Inner surface of a tooth of *Oxyrhina* Agassiz.
Fig. 5.—Outer surface of the same.
Fig. 6.—Front view of one-half of the inner dental plate of *Diodon* Linn.
Fig. 7.—Back view of a dental plate of *Diodon* Linn.
Fig. 8.—Front view of the same.