A REMARKABLE PROPERTY OF THE INTEGERS MOD N, AND ITS BEARING ON GROUP-THEORY.

BY R. VAIDYANATHASWAMY.

(From the University of Madras, Madras.)

Received December 14, 1936.

I. The Classification of the Elements of a Group into Conjugate Sets.

Let $S_1$, $S_2$, ..., $S_n$ be the elements of a group $G$ of order $n$, and let $S_1$ be the identity-element $E$ of the group. The elements which are permutable with an assigned element $S_i$ form a subgroup $H$ of $G$, of order $\frac{n}{d}$, say. The $n$ elements of $G$ fall into $d$ equinumerous subclasses with respect to $H$, namely $H$, $H_{S_\rho}$, $H_{S_\eta}$, ...

By definition of $H$, whatever element $S$ of $H$ we take, we have

$$S^{-1} S_i S = S_i;$$

and therefore also,

$$(S S_{\rho})^{-1} S_i S S_{\rho} = S_{\rho}^{-1} S^{-1} S_i S S_{\rho} = S_{\rho}^{-1} S_i S S_{\rho}. $$

Thus the value of the transform $T^{-1} S_i T$ depends solely on the subclass (1) to which $T$ belongs, so that there are exactly $d$ transforms of $S_i$ (including $S_i$ itself), $S_i$ and its transforms constitute a complete set of conjugate elements of $G$. Thus the $n$ elements of $G$ fall into a number (say $r$) of complete conjugate sets $C_1$, $C_2$, ..., $C_r$; where $C_i$ contains $h_i$ elements, $h_i$ being necessarily a divisor of $n$, and

$$h_1 + h_2 + \cdots + h_r = n.$$

The identity element $E$ constitutes by itself a complete conjugate set, and we can take $C_1 = E$, $h_1 = 1$.

The fundamental property of this division is that the classes $C$ combine among themselves by the group-operation. We mean by this that each element of $C_k$ occurs the same number $\gamma_{ij}^k$ of times among the $h_i h_j$ elements $C_i C_j$, obtained by multiplying each element of $C_i$ by each element of $C_j$. To prove this we have only to observe that if an element $c_k$ of $C_k$ occurs exactly $t$ times in the product-set $C_i C_j$, then $T^{-1} c_k T$ must also occur exactly $t$ times in the set $T^{-1} C_i C_j T = T^{-1} C_i T T^{-1} C_j T = C_i C_j$, and that by proper choice of $T$, $T^{-1} c_k T$ will coincide with any element of $C_k$. It follows that the classes $C$ can be taken as the elements of a linear algebra with the multiplication scheme

$$C_i C_j = \sum_k \gamma_{ij}^k C_k.$$
This is the 'algebra of conjugate sets' or the 'Frobenius algebra' associated with \( G \).

It is clear that there exist other divisions of the elements of \( G \) into classes which combine among themselves by the group-operation (in the sense explained). To begin with there is the trivial division into \( n \) classes, each class containing only a single element; there is also the equally trivial division in which there is only one class which contains all the elements. More generally it is easy to see that if \( G_1 \) is any subgroup of \( G \), there is a class-division of this kind determined by \( G_1 \); namely, an element \( S \) of \( G \) and all the elements which arise by transforming \( S \) by any element of \( G_1 \) are put into a class \( C_i \). The proof that the classes \( C_i \) thus arising combine among themselves by the group-operation, is word for word the same as before. For, if an element \( c_k \) of \( C_k \) occurs exactly \( t \) times in the product \( C_i C_j \), then if \( g \) is any element of \( G_1 \), \( g^{-1}c_kg \) should also occur exactly \( t \) times in the set \( g^{-1}C_i C_j g = g^{-1}C_i g^{-1}C_j g = C_i C_j \); and by definition of \( C_k \), \( g^{-1}c_kg \) can represent any element of \( C_k \) by suitable choice of \( g \).

If \( G_1 = E \), we have the trivial division into \( n \) classes, each containing a single element; if \( G_1 = G \) we have the Frobenius division into classes of conjugate sets. It is also clear that the classes corresponding to a general subgroup \( G_1 \) arise by a subdivision of the conjugate sets. We note also that if \( G \) is an Abelian group, then each element of \( G \) is a complete conjugate set by itself, and therefore the only division of \( G \) by this method into classes which combine among themselves by the group-operation, is the trivial division in which each class consists of a single element.

We proceed now to study a class-division of the integers mod \( N \), which apart from its intrinsic importance, will show that the above class-division of a group is not the most general one in which the classes combine by the group-operation. The property to be proved, of this class-division of the integers mod \( N \) does not seem to have been noticed before in mathematical literature; this is surprising in view of its fundamental character, and its importance in Additive Number-Theory.

We return in \( V \) to the question of class-division of a group.

II. The Algebra of Classes Mod \( N \).

Let \( t_1 = 1, t_2, t_3, \ldots, t_m = N \) be the distinct divisors of the integer \( N \). The \( N \) numbers \( 1, 2, \ldots, N \), considered as the representatives of the \( N \) distinct residue classes mod \( N \), may be divided into \( m \) classes, \( C_1, C_2, \ldots, C_m \), where \( C_i \) consists of the numbers whose greatest common divisor with \( N \) is \( t_i \). In particular, \( C_1 \) consists of the \( \phi(N) \) numbers less than and prime to \( N \); \( C_i \)
contains evidently \( \phi \left( \frac{N}{t_i} \right) \) numbers, and the fact that these classes exhaust the \( N \) numbers is expressed by the well-known relation:

\[
\Sigma \phi \left( \frac{N}{t_i} \right) = \Sigma \phi \left( t_i \right) = N.
\]

It is clear that the classes \( C \) combine among themselves by multiplication; for, if \( t_k \) be the g.c.d. (greatest common divisor) of \( N \) and \( t_i \), the \( \phi \left( \frac{N}{t_i} \right) \phi \left( \frac{N}{t_k} \right) \) numbers obtained by multiplying each number of \( C_i \) by each number of \( C_i \) are identical mod \( N \) with the \( \phi \left( \frac{N}{t_k} \right) \) numbers of \( C_k \) each repeated the same number of times. This is not however the remarkable property referred to in the title of this paper; the remarkable property is that the classes \( C \) combine among themselves by addition. The proof of this is on the same lines as in the case of the group. If \( c_k \), a number of the class \( C_k \), occurs exactly \( t \) times among the \( \phi \left( \frac{N}{t_i} \right) \phi \left( \frac{N}{t_k} \right) \) numbers \( C_i + C_j \) mod \( N \), then if \( h \) is any number prime to \( N \), \( hc_k \) must also occur exactly \( t \) times in the set:

\[
h (C_i + C_j) = hC_i + hC_j = C_i + C_j.
\]

By suitable choice of \( h \), \( hc_k \) can represent any number whatever of the class \( C_k \). Thus every number of the class \( C_k \) occurs the same number \( \gamma_{ij}^k \) of times among the numbers \( C_i + C_j \) mod \( N \).

To construct an algebra of the classes \( C \) analogous to the Frobenius algebra of a group, it will be convenient to change the notation, and let + denote logical addition (i.e., addition of aggregates), and indicate by \( C_i \times C_j = C_i \cap C_j \) the set of numbers obtained by adding each number of \( C_i \) to each number of \( C_j \). With this notation, our result takes the form:

\[
C_i C_j = \sum \gamma_{ij}^k C_k,
\]

where the \( \gamma_{ij}^k \)'s are positive integers or zero.

As an illustration, take \( N = 36 = 2^23^2 \). The divisors are:

\[
t_1 = 1 \quad t_2 = 2 \quad t_3 = 3 \quad t_4 = 4 \quad t_5 = 6 \quad t_6 = 9 \quad t_7 = 12 \quad t_8 = 18 \quad t_9 = 36.
\]

The classes are:

\[
C_1 = (1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35),
C_2 = (2, 10, 14, 22, 26, 34),
C_3 = (3, 15, 21, 33),
C_4 = (4, 8, 16, 20, 28, 32),
C_5 = (6, 30).
\]
\[ C_6 = (9, 27). \]
\[ C_7 = (12, 24). \]
\[ C_8 = (18). \]
\[ C_9 = (36). \]

Since \( C_9 \) is the zero residue-class \( C_6 C_9 = C_7 \). The multiplication scheme for the remaining eight classes is as follows:

\[
\begin{align*}
C_1^2 &= 6C_2 + 6C_4 + 12C_5 + 12C_7 + 12C_8 + 12C_9, \\
C_1 C_2 &= 3C_1 + 6C_2 + 6C_6.
\end{align*}
\]

<table>
<thead>
<tr>
<th>Product</th>
<th>Class 1</th>
<th>Class 2</th>
<th>Class 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>( C_1 C_3 )</td>
<td>( 4C_2 + 4C_4 )</td>
<td>( C_2 C_8 = C_4 )</td>
<td>( C_3^2 = C_7 + 2C_9 )</td>
</tr>
<tr>
<td>( C_1 C_4 )</td>
<td>( 3C_1 + 6C_3 + 6C_6 )</td>
<td>( C_3 C_8 = C_3 )</td>
<td>( C_4 C_8 = C_4 )</td>
</tr>
<tr>
<td>( C_1 C_5 )</td>
<td>( 2C_1 )</td>
<td>( C_4 C_6 = 2C_1 )</td>
<td>( C_5 C_8 = C_5 + 2C_8 )</td>
</tr>
<tr>
<td>( C_1 C_6 )</td>
<td>( 2C_2 + 2C_4 )</td>
<td>( C_5 C_9 = C_3 + 2C_6 )</td>
<td>( C_6 C_8 = C_7 )</td>
</tr>
<tr>
<td>( C_1 C_7 )</td>
<td>( 2C_1 )</td>
<td>( C_6 C_6 = 2C_5 + 2C_7 )</td>
<td>( C_7 C_8 = C_7 )</td>
</tr>
<tr>
<td>( C_1 C_8 )</td>
<td>( C_1 )</td>
<td>( C_7 C_7 = C_3 + 2C_6 )</td>
<td>( C_8 C_8 = C_3 )</td>
</tr>
<tr>
<td>( C_1 C_9 )</td>
<td>( 2C_1 + 6C_7 + 6C_9 )</td>
<td>( C_8 C_8 = C_6 )</td>
<td>( C_9 C_9 = C_9 )</td>
</tr>
<tr>
<td>( C_2 C_3 )</td>
<td>( 2C_1 )</td>
<td>( C_4 C_3 = 3C_4 + 6C_7 + 6C_9 )</td>
<td>( C_1^2 = C_7 + 2C_9 )</td>
</tr>
<tr>
<td>( C_2 C_4 )</td>
<td>( 3C_2 + 6C_5 + 6C_8 )</td>
<td>( C_5 C_8 = C_5 )</td>
<td>( C_2 C_8 = C_4 )</td>
</tr>
<tr>
<td>( C_2 C_5 )</td>
<td>( 2C_4 )</td>
<td>( C_6 C_6 = C_1 )</td>
<td>( C_3 C_8 = C_9 )</td>
</tr>
<tr>
<td>( C_2 C_6 )</td>
<td>( C_1 )</td>
<td>( C_7 C_7 = 2C_4 )</td>
<td>( C_4 C_8 = C_4 )</td>
</tr>
<tr>
<td>( C_2 C_7 )</td>
<td>( 2C_2 )</td>
<td>( C_8 C_8 = C_4 )</td>
<td>( C_5 C_8 = C_9 )</td>
</tr>
</tbody>
</table>

### III. The Evaluation of \( \gamma_{\phi^k} \).

**Theorem I.** If \( t \) is a divisor of \( N \), the \( \phi(N) \) numbers prime to \( N \) fall into \( \phi(t) \) sets, each set consisting of \( \frac{\phi(N)}{\phi(t)} \) numbers equal to each other mod \( t \).

For, if \( M \) is prime to \( N \) (and therefore to \( t \)), the numbers

\[ M + t, \ M + 2t, \ldots, \ M + \frac{N}{t} \ t, \]

are distinct mod \( N \), and equal mod \( t \). To find the number of these numbers which are prime to \( N \), we note that none of these numbers are divisible by any prime factor of \( t \). Let \( p_1, p_2, \ldots \) be the prime factors of \( \frac{N}{t} \) which do not occur in \( t \). The condition,

\[ M + rt \neq 0 \mod p_1, p_2, \ldots, \]

gives

\[ r \neq -\frac{M}{t} \mod p_1, p_2, \ldots \]

Thus the required number is the number of residue classes-mod \( \binom{N}{t} \), which are not equal to \( -\frac{M}{t} \mod p_1 \) or \( p_2 \) or \ldots. By the familiar
argument which is used in evaluating Euler's function $\phi(N)$, this number is
\[
\frac{N}{t} \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots = \frac{\phi(N)}{\phi(t)}.
\]
Thus the $\phi(N)$ numbers prime to $N$ consist of sets of numbers equal to each other mod $t$. It is clear that there is one such set corresponding to each residue-class mod $t$, prime to $t$.

**Cor.** If $M$ is a given number prime to $N$, there are $\frac{\phi(N)}{\phi(t)}$ numbers.

$M'$ prime to $N$, such that $M + M' = 0 \mod t$. For $M'$ is one of the set of numbers equal to $-M$ mod $t$.

**THEOREM II.** \( \gamma_{11}^k = \phi(N) \cdot \Pi \left(1 - \frac{1}{\phi(t)} \right) \), where the product extends over all the prime factors of $N$ which do not occur in $t_k$.

For, by Theorem I Cor. there occur among the \( \{\phi(N)\}^2 \) numbers of the set $C_{12}$, precisely $\frac{\phi(N)^2}{\phi(t_k)}$ which are divisible by $t_k$. In order that a number divisible by $t_k$ may belong to the class $C_k$, it is necessary and sufficient that it be not divisible by $t_k p_i$ for any prime factor $p_i$ of $\frac{N}{t_k}$. Hence the number of numbers of the set $C_{12}$ that belong to $C_k$ is:

\[
\left\{ \frac{1}{\phi(t_k)} - \sum_{k} \frac{1}{\phi(t_k p_i)} + \sum_{k} \frac{1}{\phi(t_k p_i p_j)} - \sum_{k} \frac{1}{\phi(t_k p_i p_j p_k)} + \cdots \right\}
\]

But by definition of $\gamma_{11}^k$, this number is $\gamma_{11}^k \cdot \phi(\frac{N}{t_k})$. Hence
\[
\gamma_{11}^k = \frac{\phi(N)^2}{\phi(t_k)} \cdot \left\{ \frac{1}{\phi(t_k)} - \sum_{k} \frac{1}{\phi(t_k p_i)} + \cdots \right\}.
\]

Now the prime factors of $\frac{N}{t_k}$ may be divided into two groups $(q_1, q_2, \cdots)$ and $(p_1, p_2, \cdots)$, where the $q$'s occur in $t_k$ and the $p$'s do not occur in $t_k$. It is clear that $\phi(t_k q_i) = q_i \phi(t_k)$ and $\phi(t_k p_i) = \phi(t_k) (p_i - 1)$. Hence:
\[
\gamma_{11}^k = \frac{\phi(N)^2}{\phi(t_k)} \cdot \phi(\frac{N}{t_k}) \cdot \Pi \left(1 - \frac{1}{q_i}\right) \cdot \Pi \left(1 - \frac{1}{p_i - 1}\right).
\]

Since $\phi(\frac{N}{t_k}) \phi(t_k) = \phi(N) \cdot \Pi \left(1 - \frac{1}{q_i}\right)$, we have finally
\[
\gamma_{11}^k = \phi(N) \cdot \Pi \left(1 - \frac{1}{p_i - 1}\right).
\]

**Cor.** $\gamma_{11}^k$ vanishes only when $N$ is even and $t_k$ odd. When $N$ is odd, $\gamma_{11}^k \neq 0$, and therefore all classes are represented in $C_{12}$. 
THEOREM III. If \( t_{ij} \) be the g.c.d. of \( t_i, t_j \), the \( \phi \left( \frac{N}{l_j} \right) \) numbers of \( C_i \) fall into \( \phi \left( \frac{t_j}{l_j} \right) \) equinumerous sets of numbers equal to each other mod \( t_j \). To each number of class \( (t_{ij}) \) mod \( t_j \), there corresponds one of these sets.

For if \( T_i \) be a number of \( C_i \), the numbers

\[
T_i + t_i, \quad T_i + 2t_i, \ldots, \quad T_i + \frac{N}{l_j} \cdot t_j,
\]

are distinct mod \( N \) and equal mod \( t_j \). We shall shew that exactly \( \phi \left( \frac{N}{l_i} \right) \) of these numbers belong to \( C_i \). The statements of the theorem follow then without difficulty.

Now if \( T_i + rt_i \) is to be divisible by \( t_i \), \( r \) must be divisible by \( \frac{t_i}{t_{ij}} \). Hence the numbers of the above series which are divisible by \( t_i \) are:

\[
T_i + \lambda \cdot \frac{t_i}{t_{ij}} \cdot t_j; \quad \lambda = 1, 2, \ldots, \frac{N}{l_j}.
\]

Out of these, the numbers that belong to \( C_i \) are those for which

\[
\frac{T_i}{t_i} + \lambda \frac{t_i}{t_{ij}} \text{ is prime to } \frac{N}{t_i}.
\]

By the reasoning of Theorem I, the number of values of \( \lambda \) for which this is the case is

\[
\phi \left( \frac{N}{l_i} \right) / \phi \left( \frac{t_j}{l_{ij}} \right).
\]

This proves the required result. Since this number is independent of the particular number \( T_i \) of \( C_i \), there follows the division of \( C_i \) into equinumerous subclasses mod \( t_j \), which are respectively equivalent to all the numbers mod \( t_j \) which have the g.c.d. \( t_{ij} \) with \( t_j \).

Cor. (1) If \( T \) is a given number of \( C_i \), the number of numbers \( T' \) of \( C_i \), for which \( T + T' = 0 \pmod{t_j} \) is by this theorem, the number belonging to a particular subclass of \( C_i \)—namely,

\[
\phi \left( \frac{N}{l_i} \right) / \phi \left( \frac{t_j}{l_{ij}} \right).
\]

Cor. (2) If \( c_i \) represents an arbitrary number of \( C_i \), the congruence

\[
c_i + c_j = 0 \pmod{t_k},
\]

has no solution, if the g.c.d. \( t_{ik} \) of \( t_i, t_k \) is not identical with \( t_{jk} \). If \( t = t_{ik} = t_{jk} \), the number of solutions of the congruence is:

\[
\phi \left( \frac{N}{l_i} \right) / \phi \left( \frac{t_k}{l_i} \right).
\]
The first part is a direct consequence of the theorem. To prove the second part, we have only to observe that to solve the congruence, we may choose for \( c_i \) any number of \( C_i \), and then \( c_i \) must belong to a particular subclass of \( C_i \) mod \( t_k \).

**Theorem IV.** If \( c_\lambda \) represents an arbitrary number of \( C_\lambda \), the equation

\[
c_i + c_j = c_k \quad (\text{mod } N)
\]

has no solution unless \( t_{ij} = t_{ik} = t_{jk} = t \) (where \( t_{ij} \) is the g.c.d. of \( t_i, t_j \)); if these conditions are satisfied the number of solutions is:

\[
\frac{\phi\left(\frac{N}{t_i}\right) \phi\left(\frac{N}{t_j}\right) \phi\left(\frac{N}{t_k}\right)}{\phi\left(\frac{N}{t}\right)} \cdot \prod_{q} \left(1 - \frac{1}{q} - 1\right)
\]

where the product extends over all those prime factors \( q \) of \( \frac{N}{t_k} \) which do not occur in \( \frac{t_k, t_i, t_j, t}{t_i, t_j, t} \).

For, by Theorem III Cor. (2), the number of solutions \( f(t_k) \) of \( c_i + c_j = 0 \) (mod \( t_k \)) is \( \frac{\phi\left(\frac{N}{t_i}\right) \phi\left(\frac{N}{t_j}\right) \phi\left(\frac{N}{t_k}\right)}{\phi\left(\frac{N}{t}\right)} \) if \( t_{ik} = t_{jk} = t \) (say) and zero otherwise.

Hence if \( t_{ik} = t_{jk} = t \), the number of cases in which \( c_i + c_j \) belongs to \( C_k \) is:

\[
f(t_k) = \sum f(t_k p_1) + \sum f(t_k p_1 p_2) - \ldots
\]

where the \( p \)'s are all the prime factors of \( \frac{N}{t_k} \).

Now \( f(t_k p_1 p_2, \ldots) \) is zero except when the two g.c.d.'s

\[
(t_k p_1 p_2, \ldots, t_i), \ (t_k p_1 p_2, \ldots, t_j)
\]

are identical; that is, unless the two g.c.d.'s

\[
\left(\frac{t_k}{t}, \frac{p_1 p_2 \ldots}{t}, \frac{t_j}{t}\right), \ \left(\frac{t_k}{t}, \frac{p_1 p_2 \ldots}{t}, \frac{t_i}{t}\right)
\]

are identical. Remembering that \( t_k/\ell \) is prime both to \( t_i/\ell \) and to \( t_j/\ell \), it is necessary for the identity of these two g.c.d.'s that each of the primes \( p_1, p_2 \ldots \) should occur either in both or in neither of \( t_i/\ell, t_j/\ell \). But if there are common factors of \( t_i/\ell, t_j/\ell \), it is easy to see that the series:

\[
f(t_k) = \sum f(t_k p_1) + \sum f(t_k p_1 p_2) - \ldots
\]

\[
= \phi\left(\frac{N}{t_i}\right) \phi\left(\frac{N}{t_j}\right) \left\{ \frac{1}{\phi\left(\frac{t_k}{t}\right)} - \sum \frac{1}{\phi\left\{\frac{t_k p_1}{(t_i, t_k p_1)}\right\}} + \sum \frac{1}{\phi\left\{\frac{t_k p_1 p_2}{(t_i, t_k p_1 p_2)}\right\}} \ldots \right\}
\]

[where the \( p \)'s are the prime factors which occur in both or in neither of \( t_i/\ell, t_j/\ell \), and \((a, b)\) denotes the g.c.d. of \( a \) and \( b \)] must be identically zero. Hence
the number of solutions required in the theorem is 0 unless \( t_{ij} = t = t_{ik} = t_{jk} \) [this is indeed directly evident from the equation \( c_i + c_j = c_k \pmod{N} \)].

Assuming then this condition satisfied, the \( p \)'s in the series (2) do not occur in \( t_i/t \) or \( t_j/t \), so that

\[
\phi \left( \frac{N}{i_k} \right) \phi \left( \frac{N}{i_j} \right) = \phi \left( \frac{t_k}{i} \right) \phi \left( \frac{t_j}{i} \right) \quad \text{(by 3)}
\]

Hence the series (2) reduces to:

\[
\frac{\phi \left( N/i_i \right) \phi \left( N/i_j \right)}{\phi \left( t_k/i \right)} \Pi \left( 1 - \frac{1}{p} \right) \Pi \left( 1 - \frac{1}{q - 1} \right)
\]

Now since the \( p \)'s are common prime factors of \( N/i_k \) and \( t_k/i \), we have

\[
\phi \left( \frac{N}{i} \right) \Pi \left( 1 - \frac{1}{p} \right) = \phi \left( \frac{N}{i_k} \right) \phi \left( \frac{t_k}{i} \right).
\]

Hence (4) reduces to:

\[
\frac{\phi \left( N/i_i \right) \phi \left( N/i_j \right) \phi \left( N/i_k \right)}{\phi \left( N/i \right)} \Pi \left( 1 - \frac{1}{q - 1} \right)
\]

which proves the theorem.

Cor. (1). Let \( g_1 = t \) be the g.c.d. of \( i_i, i_j, i_k \), \( g_2 \) the g.c.d. of their l.c.m.'s two at a time, and \( g_3 \) their l.c.m. The Theorem states that the number of solutions of \( c_i + c_j = c_k \pmod{N} \) is zero, unless \( g_2 = g_1 = t \). When this condition is satisfied the expression for the number of solutions given in the theorem, is equivalent to:

\[
\phi \left( \frac{N}{g_3} \right) \phi \left( \frac{N}{i} \right) \Pi \left( 1 - \frac{1}{q - 1} \right).
\]

where the product extends over the prime factors \( q \) of \( N/i \), which do not occur in \( g_3/t \). To prove this, write

\[
t_i = t_i T_i, \ t_j = t_j T_j, \ t_k = t_k T_k; \ g_3 = t_i T_i T_j T_k,
\]

where every two of \( T_i, T_j, T_k \) are relatively prime. It follows easily that

\[
\phi \left( \frac{N}{i_i} \right) \phi \left( \frac{N}{i_j} \right) \phi \left( \frac{N}{i_k} \right) = \phi \left( \frac{N}{g_3} \right) \left[ \phi \left( \frac{N}{i} \right) \right]^2.
\]
Further, the prime factors of \( N/t_k = N/t_{T_k} \) which do not occur in \( T_i, T_j, T_k \) are identical with the prime factors of \( N/t \) which do not occur in \( g_0/t \).

Hence the alternative form.

*Cor.* (2). It is clear that the number of solutions required in the theorem is equal to \( \gamma_{ij}^{*k} \phi(N/t_k) \). Hence

\[
\gamma_{ij}^{*k} = \frac{\phi\left(\frac{N}{t_i}\right) \phi\left(\frac{N}{t_j}\right)}{\phi\left(\frac{N}{t}\right)} \prod \left\{ 1 - \frac{1}{q-1} \right\} \text{ or } 0,
\]

according as the g.c.d. of every two of \( t_i, t_j, t_k \) is the same number \( t \) or not, the product extending over the prime factors \( q \) of \( \frac{N}{t} \) which do not occur in \( t, t' \) or \( t_k \).

**IV. Alternative Evaluation of \( \gamma_{ij}^{*k} \) by the Theory of Multiplicative Functions.**

The above direct evaluation of \( \gamma_{ij}^{*k} \) will now be confirmed by a less direct but more elegant method. The number of solutions of

\[ c_i + c_j = c_k \mod N, \]

is equal to \( \phi(N/t_k) \gamma_{ij}^{*k} \). Now, \( m \) and \( -m \) always belong to the same class \( \mod N \). Hence this number of solutions is also the number of solutions of

\[ c_i + c_j + c_k = 0 \mod N. \]

It is clear that this number \( v(N, t_i, t_j, t_k) \) (say) is a symmetric function of \( t_i, t_j, t_k \). More generally we may define the function \( v(N, M_1, M_2, M_3) \) as the number of solutions of

\[ c_1 + c_2 + c_3 = 0 \mod N, \]

with the condition that \( c_i \) is to belong to the same class \( \mod N \) as \( M_i \) \( (i = 1, 2, 3) \). It is clear that \( v(N, M_1, M_2, M_3) \) is a function symmetric in the arguments \( (M_1, M_2, M_3) \) and depending on \( M_1, M_2, M_3 \) only through the residue classes \( \mod N \), to which they belong.

**Theorem V.** The function \( v(N, M_1, M_2, M_3) \) is a multiplicative* function of its four arguments.

For the Chinese remainder theorem asserts that if \( N, N' \) be relatively prime, there is a unique number \( \mod NN' \) which is equal to two given numbers

\* A function \( f(M_1, M_2, \ldots) \) of positive integral arguments is said to be multiplicative if \( f(M_1 N_1, M_2 N_2, \ldots) = f(M_1, N_1, M_2, N_2, \ldots) f(N_1, N_2, \ldots) \) whenever \( (M_1 M_2 \ldots) \) is prime to \( (N_1 N_2 \ldots) \). For the properties of such functions, see R. Vaidyanathaswamy, "The Theory of Multiplicative Arithmetic Functions," Trans. Am. Math. Soc., 33, 2, pp. 579-662.
mod $N$ and $N'$ respectively. Further the unique number mod $NN'$ which is equal to a number of class $t$ (a divisor of $N$) mod $N$, and to a number of class $t'$ mod $N'$ must evidently belong to class $tt'$ mod $NN'$; and conversely.

Now let $t_i$ be the g.c.d. $(N, M_i)$ and $t_i'$ the g.c.d. $(N', M_i')$. If $NM_1M_2M_3$ be prime to $N'M_1'M_2'M_3'$, then $v(NN', M_1M_1', M_2M_2', M_3M_3')$ is the number of solutions of the equation:

$$k_1 + k_2 + k_3 = 0 \pmod{NN'},$$

where $k_i$ belongs to the class $t_i t_i'$ mod $NN'$. This implies each of the equations

$$k_1 + k_2 + k_3 = 0 \pmod{N},$$

$$k_1 + k_2 + k_3 = 0 \pmod{N_1'},$$

where $k_i$ is a number of class $t_i$ in (2) and a number of class $t_i'$ in (3). Thus each solution of (1) yields a unique solution of (2) and a unique solution of (3). Conversely, since there is, by the Chinese remainder theorem, a unique number of class $t t_i'$ mod $(NN')$ which is equal mod $N$ to a given number of class $t_i$ and mod $N'$ to a given number of class $t_i'$, it follows that any solution of (2) can be combined with any solution of (3) so as to produce a unique solution of (1). Hence the number of solutions of (1) is the product of the numbers of solutions of (2) and (3); or:

$$v(NN', M_1M_1', M_2M_2', M_3M_3') = v(N, M_1, M_2, M_3) v(N', M_1', M_2', M_3')$$

if $NM_1M_2M_3$ is prime to $N'M_1'M_2'M_3'$. This proves the multiplicative property of the function $v(N, M_1, M_2, M_3)$.

A similar proof holds for the corresponding function defined in the same way for more than three arguments $M$.

**Theorem VI.** The function $v(N, M_1, M_2, \ldots, M_r)$ defined as the number of solutions of the equation

$$c_1 + c_2 + \ldots + c_r = 0 \pmod{N},$$

where $c_i$ belongs to the same class mod $N$ as $M_i$, is equal to

$$v(N, g_1, g_2, \ldots, g_r),$$

where $g_1$ is the g.c.d. and $g_r$ the l.c.m. of $M_1, M_2, \ldots, M_r$ and $g_i$ the g.c.d. of their l.c.m.'s $i$ at a time.$\dagger$

For since the function $v$ is multiplicative, it is sufficient to prove the result when all the arguments are powers of a prime $p$; i.e., it is sufficient to prove the theorem for $v(p^n, p^{k_1}, p^{k_2}, \ldots, p^{k_r})$. Since however $v$ is symmetric in

$\dagger$ $g_1, g_2, \ldots, g_r$ were called the successive g.c.d.'s of $M_1, M_2, \ldots, M_r$ in my paper "on the Arithmetico-logical symmetric functions of $n$ Attributes", *Proc. of the Ind. Acad. of Sciences*. The index of any prime $p$ in $g_i$ is the $i$th in ascending order of its indices in $M_1, M_2, \ldots, M_r$. 

the arguments $M_1, M_2, \ldots, M_r$, we can rearrange $p_1^k, p_2^k, \ldots, p_r^k$ in the ascending order of indices without affecting the value of the function. This rearrangement is equivalent to replacing $p_1^k, p_2^k, \ldots, p_r^k$ by their successive g.c.d.'s. Thus the theorem is proved when the arguments are powers of a prime, and therefore for the general case.

Cor. If $g'_i$ is the g.c.d. of $g_i$ and $N$,

$$v(N, M_1, M_2, \ldots) = v(N, g_1, g_2, \ldots) = v(N, g'_1, g'_2, \ldots).$$

For the values of $g_1, g_2, \ldots$ are relevant to the value of $v$, only through the classes mod $N$ to which they belong.

**Theorem VII.** $v(N, M_1, M_2, M_3) = \phi \left( \frac{N}{g_2} \right) \phi \left( \frac{N}{g_1} \right) \Pi \left( 1 - \frac{1}{q - 1} \right)$ or zero,

according as $g_1 = \pm g_2$, where $g_1, g_2, g_3$ are the g.c.d.'s with $N$ of the successive g.c.d.'s of $M_1, M_2, M_3$ and the product extends over the prime factors $q$ of $N$ which do not occur in $g_3$.

For, $v(N, M_1, M_2, M_3) = v(N, g_1, g_2, g_3)$ is the number of solutions of

$$c_1 + c_2 + c_3 = 0 \pmod{N},$$

where $c_i$ belongs to the class $g_i$ ($i = 1, 2, 3$); that is, of

$$k_1 + k_2 + k_3 = 0 \pmod{\frac{N}{g_1}},$$

where $k_1$ is prime to $\frac{N}{g_1}$ and $k_2, k_3$ belong to the respective classes $\frac{g_2}{g_1}, \frac{g_3}{g_1}$ mod $\frac{N}{g_1}$.

This congruence has evidently no solution if $g_2 \neq g_1$; if $g_2 = g_1$,

by Theorem II, the number of solutions is $\phi \left( \frac{N}{g_2} \right) \phi \left( \frac{N}{g_1} \right) \Pi \left( 1 - \frac{1}{q - 1} \right)$

as stated.

Cor. If $M_1, M_2, M_3$ belong to the classes $C_i, C_j, C_k$ respectively mod $N$,

then $v(N, M_1, M_2, M_3) = \phi \left( \frac{N}{t_k} \right) \gamma_{ij}^k$. Hence

$$\gamma_{ij}^k = \frac{1}{\phi(N/t_k)} \cdot \frac{\phi(N/g_3) \cdot \phi(N/g_1)}{\phi(N/g_2)} \Pi \left( 1 - \frac{1}{q - 1} \right).$$

**Theorem VIII.**

$$v(N, M_1, M_2, \ldots, M_r) = \sum \frac{v(N, M_1, M_2, \ldots, M_r, t) \cdot v(N, M_1, M_2, \ldots, M_r, t)}{\phi \left( \frac{N}{t} \right)}$$

where the sum extends over all divisors $t$ of $N$.

For, the solutions enumerated in $v(N, M_1, M_2, \ldots, M_r)$ are also the solutions of the simultaneous equations.
\[ c_1 + c_2 + \ldots + c_k = m \pmod{N} \]
\[ c_{k+1} + c_{k+2} + \ldots + c_r = -m \pmod{N} \quad (m = 1, 2, \ldots, N), \]

where \( c_i \) belongs to the same class as \( M_i \). When \( m \) is a given number belonging to the same class as the divisor \( t \) of \( N \), the number of solutions of these two equations is:

\[ \nu \left( N, M_1, M_2, \ldots, M_k, t \right) \cdot \frac{\phi \left( \frac{N}{t} \right)}{\phi \left( \frac{N}{t} \right)} \]

Hence, when \( m \) varies over the \( \phi \left( \frac{N}{t} \right) \) numbers of class \( (t) \), the number of solutions obtained is \( \phi \left( \frac{N}{t} \right) \) times this number. By summing over all the divisors \( t \), we get the result of the theorem.

### V. The Class-Division of a Group

**Theorem IX.** There exists a division of the elements of a group \( G \), into classes which combine among themselves by the group operation, corresponding to every group \( G_1 \) of automorphisms of \( G \).

For, let each element of \( G \) with all the elements into which it is transformed by the automorphisms in \( G_1 \) be put into a class; the classes thus formed combine among themselves by the group-operation. For if \( c_k \) an element of the class \( C_k \) occurs precisely \( t \) times in the set \( C_i C_j \), then if \( g \) is any automorphism comprised in \( G_1 \), the element \( g(c_k) \) must occur precisely \( t \) times in the set \( g(C_i C_j) = g(C_i)g(C_j) \); that is to say, in the set \( C_i C_j \). By proper choice of \( g \), \( g(c_k) \) can represent any element of the class \( C_k \), which proves the theorem.

If \( G_2 \) is any subgroup of \( G_1 \), it is clear that the class-division corresponding to \( G_2 \) is obtained by a subdivision of the classes \( C \) corresponding to \( G_1 \). If \( G_1 \) is the group of inner automorphisms we obtain the class-division into conjugate sets and the associated Frobenius algebra of the group. If \( G_1 \) is the total group of automorphisms of \( G \), the corresponding class-division is a maximal one, in the sense that every other class-division (e.g., the division into conjugate sets of elements) arises by a subdivision of the classes corresponding to the maximal division. Thus the maximal division arises by grouping together certain conjugate sets of elements into classes. In certain cases, the maximal classes consist of all elements of the same order of the group. It will be seen presently that this is the case in Abelian groups. Whether this is the case in other classes of groups (for example, in groups of odd order) I am unable to say definitely.
An Abelian group has no inner automorphisms other than the identical automorphism. A cyclic group of order N is abstractly identical with the additive group of residue-classes mod N. The (outer) automorphisms of the cyclic group correspond to the multiplication of the residue-classes by a number prime to N. The class-division of the numbers mod N which we have discussed is precisely the maximal class-division which corresponds to the total group of automorphisms of the cyclic group. It is clear that in this division the elements of a class are all the elements of the group of a given order. This division can be obviously extended to any Abelian group.