GROUP PROPERTIES OF THE RESIDUE CLASSES OF CERTAIN KRONECKER MODULAR SYSTEMS AND SOME RELATED GENERALIZATIONS IN NUMBER THEORY*

BY

EDWARD KIRCHER

The object of this paper is to study the groups formed by the residue classes of a certain type of Kronecker modular system and some closely related generalizations of well-known theorems in number theory. The type of modular system to be studied is of the form $\mathfrak{M} = (\mathfrak{m}_n, \mathfrak{m}_{n-1}, \cdots, \mathfrak{m}_1, \mathfrak{m})$. Here $\mathfrak{m}$, defined by $(m_1, m_2, \cdots, m_k)$, is an ideal in the algebraic domain Ω of degree k. Each term $\mathfrak{m}_i$, $i = 1, 2, \cdots, n$, belongs to the domain of integrity of $\Omega_i = (\Omega, x_1, x_2, \cdots, x_i)$, and is defined by the fundamental system $(\psi_1^{(i)}, \psi_2^{(i)}, \cdots, \psi_{j_i}^{(i)})$. The various $\psi_j^{(i)}$, $j = 1, 2, \cdots, j_i$, are rational integral functions of x_i with coefficients that are in turn rational integral functions of $x_1, x_2, \cdots, x_{i-1}$, with coefficients that are algebraic integers in Ω. In every case the coefficient of the highest power of x_i in each of the $\psi_j^{(i)}$ shall be equal to 1. We shall see later that the developments of this paper also apply to modular systems where the last restriction here cited is omitted, being replaced by another admitting more systems, these new systems in every case being equivalent to a system in the standard form as here defined. Any expression that fulfills all of the conditions placed upon each $\psi_j^{(i)}$ with the possible exception of the last one, we shall call a *polynomial,* and no other expression shall be so designated. This definition includes all of the algebraic integers of Ω. Throughout this paper we shall deal exclusively with polynomials as here defined.

The first part of this paper will contain the introduction with the necessary definitions and a discussion concerning the factoring of the system $\mathfrak{M}$. The second section will then be devoted to setting up necessary and sufficient conditions that a set of residue classes belonging to $\mathfrak{M}$ form a group when taken modulo $\mathfrak{M}$. In the third section we shall study the structure of such a group with respect to groups belonging to certain modular factors of $\mathfrak{M}$, besides

* Preliminary report presented to the Society, Chicago, April 10, 1914.

deriving a few related theorems. Section four will then be devoted to a generalization of a number of well-known theorems in number theory by means of the definitions and results of the preceding sections. Several theorems of this last section have already been generalized by Hensel* and Landsberg† for the case that $n = 1$ and Ω is the rational realm. Other articles upon which this paper is based or to which it is closely related are due to the above, König,‡ and Hancock§ for the purely number theoretic point of view, while papers by Serret,|| G. A. Miller,¶ Georg Wolff,** and A. Ranum†† represent the application of group theory to the problem in question. G. A. Miller in particular has proved two theorems for the rational realm whose generalization for the realm Ω_n gives us the fundamental theorems of the second and third sections.

I. The modular system $\mathfrak{M}$ and its residue classes

Gauss, the founder of the theory of congruences, and Schoenemann carried on independent investigations‡‡ concerning the properties of congruences of the form $f_1(x) \equiv f_2(x)$, mod p, where $f_1(x)$ and $f_2(x)$ are rational integral functions of x with rational integral coefficients and p is a rational prime. Dedekind§§ extended some of these properties to the modular system (ψ, p), where ψ is a rational integral function of x with rational integral coefficients and p is a rational prime. Serret did considerable work along this line for the case where ψ is irreducible modulo p. Among other things he has shown that whenever this happens all the residue classes of (ψ, p), excepting the one containing 0, form a cyclic group modulo (ψ, p). Cauchy|||| had already studied some of the group properties of residues belonging to the rational integer m taken as modulus, but very little progress was made until Tanner¶¶ studied the group of totitives, or residues less than and prime to m. Besides

* Hensel, Crelle's Journal für Mathematik, vol. 119 (1898), pp. 175–185. See also vol. 118 (1897), pp. 234–250, and vol. 119 (1898), pp. 114–130.

† Landsberg, Göttinger Nachrichten, 1897, pp. 277ff.

‡ König, *Theorie der Algebraischen Grösszen*, pp. 351–361, 401ff.

§ H. Hancock, American Journal of Mathematics, vol. 24 (1901), pp. 39–60

|| Serret, *Cours d'Algèbre Supérieure*, third edition, vol. 2, § 345, § 363.

¶ G. A. Miller, Archiv der Mathematik und Physik, vol. 15 (1909), pp. 115–121; Annals of Mathematics, ser. 2, vol. 6 (1905), p. 49; American. Journal of Mathematics, vol. 27 (1905), pp. 315ff.

** Georg Wolff, *Gruppen der Reste eines beliebigen Moduls im algebraischen Zahlkörper*, Diss. Giessen, Göttingen, W. Kaestner, 1905.

†† A. Ranum, these Transactions, vol. 11 (1910), pp. 172–198.

‡‡ Gauss, *Werke*, Göttingen, 1876, vol. 2, pp. 21ff.; Schoenemann, Crelle's Journal für Mathematik, vol. 31 (1846), p. 269, vol. 32 (1846), p. 93.

§§ Dedekind, Crelle's Journal, vol. 54 (1857), pp. 1–13.

|||| Cauchy, *Exercices d'analyse et de physique mathématique*, vol. 3 (1844), p. 233.

¶¶ Tanner, Proceedings of the London Mathematical Society, vol. 20 (1888–89), pp. 63–83.

those mentioned in the preceding paragraph other papers giving extensive results from the standpoint of group theory have been published by Bachmann,* Weber,† and Zsigmondy.‡ Attention may also be called to a paper by E. H. Moore.§

We shall now give some necessary definitions. Let us write

$$\mathfrak{M}_i = (\mathfrak{m}_i, \mathfrak{m}_{i-1}, \cdots, \mathfrak{m}_1, \mathfrak{m}).$$

Hence $\mathfrak{M}_i = (\mathfrak{m}_i, \mathfrak{M}_{i-1})$, and in particular $\mathfrak{M}_n = \mathfrak{M}$, and $\mathfrak{M}_0 = \mathfrak{m}$. We know that in a given domain a Kronecker modular system defined by the polynomials $(M_1, M_2, \cdots, M_t)$ is composed of the totality of linear forms $T_1 M_1 + T_2 M_2 + \cdots + T_t M_t$, where the various T's range over all the polynomials of our domain. Hence it follows that if a polynomial f is congruent to zero, mod $\mathfrak{M}_i$, it can be expressed as a linear form $T_1 \psi_1^{(i)} + \cdots + T_j \psi_j^{(i)} + \cdots + T_{j_i} \psi_{j_i}^{(i)} +$ a polynomial congruent to zero modulo $\mathfrak{M}_{i-1}$. Such a polynomial f we shall often designate by $F(\mathfrak{M}_i)$. As all of the T's may be zero it follows that every $F(\mathfrak{m})$, $F(\mathfrak{M}_1)$, $\cdots$, $F(\mathfrak{M}_{i-1})$ is also a $F(\mathfrak{M}_i)$. A polynomial contained in the domain Ω_i but not in Ω_{i-1} shall always be considered as a rational integral function of x_i whose coefficients are contained in Ω_{i-1}. It is evident that while every $\psi_j^{(i)}$ is a $F(\mathfrak{M}_i)$, it is not a $F(\mathfrak{M}_{i-1})$ because the greatest common divisor of its coefficients is equal to 1, that being the coefficient of the highest power of x_i by definition. Two polynomials f_1 and f_2 shall be said to be *congruent* with respect to the modular system $\mathfrak{M}_i$, i. e., $f_1 \equiv f_2$ modulo $\mathfrak{M}_i$, if there exists an equation $f_1 = f_2 + F(\mathfrak{M}_i)$.

All polynomials that are congruent to one another when taken modulo $\mathfrak{M}_i$ form a *residue class* with respect to this modulus, and as any two differ from each other by some $F(\mathfrak{M}_i)$, it follows that in our group considerations and congruences we can represent a residue class by any one residue (i. e., polynomial) belonging to it and chosen to represent it. This *representative residue*, which we shall usually designate by f, shall always be chosen in such a manner that its degree in x_i is less than the degree in x_i of each of the ψ's that define $\mathfrak{m}_i$. The *norm* of $\mathfrak{M}_i$, written $N(\mathfrak{M}_i)$, shall be defined as being equal to the number of residue classes belonging to $\mathfrak{M}_i$. This norm is evidently a finite number. It may be mentioned that if none of the defining ψ's of $\mathfrak{m}_{i+1}$, $\mathfrak{m}_{i+2}$, $\cdots$, $\mathfrak{m}_n$ in $\mathfrak{M}$ are of a higher degree than the first in x_{i+1}, x_{i+2}, $\cdots$, x_n respectively, the corresponding residues must be of degree 0 in these unknowns

* Bachman, *Elemente der Zahlentheorie*, 1892, p. 57.

† Weber, *Algebra*, vol. 2, 1896, p. 60.

‡ Zsigmondy, Monatshefte für Mathematik und Physik, vol. 7 (1896), pp. 185 ff.

§ E. H. Moore, Bulletin of the American Mathematical Society, ser. 2, vol. 3 (1897), p. 372.

and belong to the system of residues of $\mathfrak{M}_i$. In particular, if every ψ used in defining the various $\mathfrak{m}_i$, $i = 1, 2, \cdots, n$, is of the first degree, our residue classes are identical with those of the ideal $\mathfrak{m}$.

We shall say that the modular system $\mathfrak{M}$ *contains* the modular system $\mathfrak{M}'$ whenever every $\psi_j^{(i)}$ used in defining $\mathfrak{m}, \mathfrak{m}_1, \cdots, \mathfrak{m}_n$, is a $F(\mathfrak{M}')$. If in addition there exists a third modular system $\mathfrak{M}''$ such that for any $F(\mathfrak{M}')$ and for any $F(\mathfrak{M}'')$ we always have $F(\mathfrak{M}')F(\mathfrak{M}'') = F(\mathfrak{M})$, $\mathfrak{M}$ is defined as equivalent to the *product* of $\mathfrak{M}'$ and $\mathfrak{M}''$, or $\mathfrak{M} = \mathfrak{M}'\mathfrak{M}''$. In general two modular systems are *equivalent* if every linear form of one system is also a linear form of the other. The equality sign shall be used to denote equivalence. Here $\mathfrak{M}'$ is a *modular factor* of $\mathfrak{M}$, and $\mathfrak{M}''$ is its *complementary modular factor*, while $\mathfrak{M}$ contains both $\mathfrak{M}'$ and $\mathfrak{M}''$. If there exists no modular factor of $\mathfrak{M}$ excepting $\mathfrak{M}$ itself and unity, $\mathfrak{M}$ is said to be an *irreducible modular system*. If $\mathfrak{M}$ contains no modular system besides itself and unity it is called an *absolute prime modular system*. Such a system we shall usually denote by $\mathfrak{P}$. Two modular systems $\mathfrak{M}'$ and $\mathfrak{M}''$ shall be defined as being *relatively prime* to another if the modular system $(\mathfrak{M}', \mathfrak{M}'')$ whose defining elements consist of the defining elements of $\mathfrak{M}'$ and $\mathfrak{M}''$ is equivalent to the unit system (1). Similarly a polynomial f is relatively prime to the system $\mathfrak{M}$ if the system $(f, \mathfrak{M})$ obtained by adjoining f to the defining elements of $\mathfrak{M}$ is equivalent to (1). Two polynomials f_1 and f_2 in the unknown x_i with coefficients that are polynomials in the domain Ω_{i-1} are said to be relatively prime modulo $\mathfrak{M}_{i-1}$ whenever the system defined by $(f_1, f_2, \mathfrak{M}_{i-1})$ is equivalent to (1). Since no defining element of $\mathfrak{M}_{i-1}$ contains the quantity x_i and it is assumed that $\mathfrak{M}_{i-1} \neq (1)$, it follows that this implies the relation $f'f_1 + f''f_2 \equiv 1$, mod $\mathfrak{M}_{i-1}$, where f' and f'' are two polynomials in the domain Ω_i. Making use of a well-known fact in the modular theory already proven by Kronecker* we have the following equivalence

$$\text{(I)} \quad (M, M_1, M_2, \cdots, M_t) = (M'M'', M_1, \cdots, M_t)$$
$$= (M', M_1, \cdots, M_t)(M'', M_1, \cdots, M_t)$$

whenever $M \equiv M'M''$, mod $(M_1, \cdots, M_t)$, and $(M', M'') \equiv 1$, modulo $(M_1, M_2, \cdots, M_t)$, i. e., the factors M' and M'' are relatively prime, mod $(M_1, M_2, \cdots, M_t)$. Hence the two factors on the right hand side of (I) are relatively prime, which condition can also be expressed by saying that they cannot both contain any absolute prime modular system in common. In the following paragraph we shall speak of breaking up

$$\mathfrak{M} = (\mathfrak{m}_n, \mathfrak{m}_{n-1}, \cdots, \mathfrak{m}_1, \mathfrak{m})$$

* Kronecker, *Festschrift*, Crelle, vol. 92 (1882), p. 78. König, *Algebraische Grösszen*, p. 356.

according to the principle (I), although each of the $\mathfrak{m}_i$ contains a number of defining elements, while in (I) each of the M's was merely a single polynomial. The two cases, however, are essentially the same, for each $\mathfrak{m}_i$ may be thought of as standing merely for the aggregate of its defining elements $\psi_j^{(i)}$. Then when $\mathfrak{m}_i$ is factored modulo some modular system as in the next paragraph we must think of the factoring as being applied to only one of these elements $\psi_j^{(i)}$, while each of the others will occur in both of the relatively prime factors on the right hand side.

If the ideal $\mathfrak{m}$ is equal to the product $\mathfrak{p}_1^{\alpha_1}\mathfrak{p}_2^{\alpha_2}\cdots\mathfrak{p}_j^{\alpha_j}\cdots\mathfrak{p}_r^{\alpha_r}$, where the various $\mathfrak{p}_j$ are distinct prime ideals, it follows from (I) that we have

$$\mathfrak{M} = \prod_{j=1}^{j=r}(\mathfrak{m}_n, \mathfrak{m}_{n-1}, \cdots, \mathfrak{m}_1, \mathfrak{p}_j^{\alpha_j}) = \prod\mathfrak{R},$$

i. e., $\mathfrak{M}$ is a product of modular systems of a type that we shall define by $\mathfrak{R}$ where any $\mathfrak{R}$ is a modular system whose last defining term $\mathfrak{m}$ is of the form $\mathfrak{p}^\alpha$. The factorization of $\mathfrak{m}_1$ in any one of the systems $\mathfrak{R}$ obtained above depends only upon the $\mathfrak{p}^\alpha$ term, since none of the $\mathfrak{m}_i$, $i = 2, 3, \cdots, n$, is contained in Ω_1. Let us suppose that the greatest possible number of factors, prime ea h to each, into which $\mathfrak{m}_1$ can be factored modulo $\mathfrak{p}^\alpha$, is equal to r_1 and that we have $\mathfrak{m}_1 \equiv \mathfrak{q}_{1,1}\mathfrak{q}_{1,2}\cdots\mathfrak{q}_{1,j}\cdots\mathfrak{q}_{1,r}$. Here each $\mathfrak{q}_{1,j}$ is defined by a set of defining elements $(\zeta_1, \zeta_2, \cdots, \zeta_j, \cdots, \zeta_{j_1})$, where ζ_j is a factor of $\psi_j^{(1)}$, mod $\mathfrak{p}^\alpha$. Moreover $\mathfrak{q}_{1,j}$ cannot be broken up into relatively prime factors, mod $\mathfrak{p}^\alpha$, by the principle of (I). By applying (I) to each of the systems $\mathfrak{R}$ obtained above we get in each case a decomposition of the form

$$\mathfrak{R} = \prod_{j=1}^{j=r_1}(\mathfrak{m}_n, \mathfrak{m}_{n-1}, \cdots, \mathfrak{m}_2, \mathfrak{q}_{1,j}, \mathfrak{p}^\alpha) = \prod\mathfrak{R}_1.$$

Continuing in a similar manner we have in general

$$\mathfrak{R}_{i-1} = \prod_{j=1}^{j=r_i}(\mathfrak{m}_n, \mathfrak{m}_{n-1}, \cdots, \mathfrak{m}_{i+1}, \mathfrak{q}_{i,j}, \mathfrak{q}_{i-1}, \cdots, \mathfrak{q}_1, \mathfrak{p}^\alpha) = \prod\mathfrak{R}_i.$$

It is evident that no two modular systems of the type $\mathfrak{R}_i$ obtained by factoring $\mathfrak{M}$ can have the same set of defining elements $(\mathfrak{q}_i, \mathfrak{q}_{i-1}, \cdots, \mathfrak{q}_1, \mathfrak{p}^\alpha)$, from which it follows that the various $\mathfrak{R}_i$ are all relatively prime to each other. We shall define $\Omega_i = (\mathfrak{q}_i, \mathfrak{q}_{i-1}, \cdots, \mathfrak{q}_1, \mathfrak{p}^\alpha)$, so that $\mathfrak{R}_i = (\mathfrak{m}_n, \cdots, \mathfrak{m}_{i+1}, \Omega_i)$. In $\mathfrak{R}_i$, Ω_i, $\mathfrak{m}_i$, $\mathfrak{q}_i$, etc., the subscript i simply indicates the type of the modular system or term. When we wish to distinguish between two systems of the same type a second subscript or an accent will be used. From what precedes we see that if we carry out the factoring of $\mathfrak{M}$ into modular factors as far as possible we shall in every case arrive at a product $\mathfrak{R}_{n-1} = \prod\mathfrak{R}_n$, where

$\mathfrak{Q}_n = \mathfrak{R}_n$. We shall always designate a system of type $\mathfrak{Q}_n$ by $\mathfrak{Q}$ and call it a *simple modular system* because it cannot be further decomposed into relatively prime factors by means of (I). This, however, does not prevent it from breaking up into the product of a number of modular systems no two of which can be relatively prime to each other. In fact a simple modular system is either an irreducible modular system, or it is equivalent to the product of a number of irreducible systems no two of which can be relatively prime. By combining the various steps we see that $\mathfrak{M} = \prod\mathfrak{Q}$, or $\mathfrak{M}$ can be factored into a product of simple modular systems all relatively prime to another, and this can be done in essentially only one way. This last statement will become evident if we reflect that in apparently different factorizations of $\mathfrak{M}$ into simple factors there must always exist a (1, 1) correspondence between the simple factors of the two sets, such that each pair of corresponding modular systems are equivalent. Hence we have the theorem:

THEOREM. *A modular system $\mathfrak{M}$ can be decomposed into a product of simple modular systems, all relatively prime to each other, in one and, essentially, only one way.*

We shall now prove that a simple modular system can contain only one absolute prime modular system $\mathfrak{P}$. In order to do this we shall first prove our proposition for an irreducible system $\mathfrak{Q}$, which we shall define by

$$\mathfrak{Q} = (\mathfrak{q}_n, \mathfrak{q}_{n-1}, \cdots, \mathfrak{q}_1, \mathfrak{p}^\alpha).$$

If $\alpha = 1$ and for every value of i each defining element $\zeta_j^{(i)}$ of $\mathfrak{q}_i$ is an irreducible rational integral function of x_i when taken modulo $(\mathfrak{q}_{i-1}, \mathfrak{q}_{i-2}, \cdots, \mathfrak{p})$, our irreducible system is seen to be an absolute prime system. To prove our statement for any irreducible system $\mathfrak{Q}$ it will be necessary to give a generalized version of a proof due to Schoenemann.* Let $\mathfrak{Q}_{i-1}$ be the irreducible modular system formed by the defining elements $\mathfrak{q}_{i-1}, \mathfrak{q}_{i-2}, \cdots, \mathfrak{p}^\alpha$ of $\mathfrak{Q}$. Also let $\mathfrak{P}_{i-1}$ be one of the absolute prime systems contained in $\mathfrak{Q}_{i-1}$. Let us consider the totality of polynomials of degree s in x_i whose coefficients belong to Ω_{i-1} and are taken modulo $\mathfrak{Q}_{i-1}$, the coefficient of the highest power of x_i always being 1. From this total pick out all of those that reduce to the same given polynomial f when taken modulo $\mathfrak{P}_{i-1}$. It is evident that the number of values of a coefficient of such a polynomial that are incongruent each to each, mod $\mathfrak{Q}_{i-1}$, but reduce to the same value, mod $\mathfrak{P}_{i-1}$, is the same no matter to what value, mod $\mathfrak{P}_{i-1}$, they reduce. Let K represent this number. It follows at once that the number of polynomials, incongruent each to each modulo $\mathfrak{Q}_{i-1}$, that reduce to f modulo $\mathfrak{P}_{i-1}$ is equal to K^s. Let f break up into r distinct factors, mod $\mathfrak{P}_{i-1}$, any two of which are relatively prime to

* Schoenemann, Crelle's Journal für Mathematik, vol. 32 (1846), pp. 93ff.

each other with respect to $\mathfrak{P}_{i-1}$. Suppose that these different factors are of degrees $s_1, s_2, \cdots, s_r$, respectively, where $s_1 + s_2 + \cdots + s_r = s$. Since the highest power of x_i in each of them has the coefficient 1, it follows that there are K^{s_1} polynomials of degree s_1 incongruent modulo $\mathfrak{Q}_{i-1}$, with the coefficient of $x_i^{s_1}$ equal to 1 that reduce to the first of the factors of f, mod $\mathfrak{P}_{i-1}$. Similarly there are K^{s_2} for the second, etc., so that there are $K^s = K^{s_1}K^{s_2}\cdots K^{s_r}$ product combinations of these polynomials, incongruent each to each modulo $\mathfrak{Q}_{i-1}$, that reduce to f modulo $\mathfrak{P}_{i-1}$. Since no more than K^s incongruent residues of $\mathfrak{Q}_{i-1}$ can reduce to f modulo $\mathfrak{P}_{i-1}$ these product combinations evidently include all of the incongruent residues of $\mathfrak{Q}_{i-1}$ that reduce to f, modulo $\mathfrak{P}_{i-1}$. Hence we have shown that any polynomial considered as having coefficients belonging to the residue system of $\mathfrak{Q}_{i-1}$ that factors into r relatively prime factors modulo $\mathfrak{P}_{i-1}$ must also factor into r relatively prime factors modulo $\mathfrak{Q}_{i-1}$. Hence any polynomial that is irreducible modulo $\mathfrak{Q}_{i-1}$ either is irreducible or is a power of an irreducible polynomial modulo $\mathfrak{P}_{i-1}$. Let us now study the nature of the defining elements of $\mathfrak{P}$. As it is an absolute prime modular system it follows at once that it must include $\mathfrak{p}$ among its defining elements. As for the elements $\zeta_1^{(1)}, \zeta_2^{(1)}, \cdots, \zeta_{j_1}^{(1)}$, of $\mathfrak{q}_1$, we know that none of them can factor into factors that are relatively prime, mod $\mathfrak{p}^a$, for then it would follow by (I) that $\mathfrak{Q}$ could not be irreducible. Hence it follows from the preceding arguments that each $\zeta_j^{(1)}$ must, mod $\mathfrak{p}$, reduce to some power of an irreducible polynomial $\xi_j^{(1)}$. The system $\mathfrak{P}$ can contain only the first power of such a $\xi_j^{(1)}$ as a defining element. With respect to an absolute prime modular system two irreducible factors are either relatively prime or identical, hence it follows that for each $\xi_j^{(1)}, j = 2, 3, \cdots, j_1$, we either have $(\xi_j^{(1)}, \xi_1^{(1)}, \mathfrak{p}) = (1)$, or $\xi_j^{(1)} \equiv 0$, mod $(\xi_1^{(1)}, \mathfrak{p})$. If the former case occurs for any one of the $\xi_j^{(1)}$ our system $\mathfrak{P}$ is equivalent to the unit system, if this is not the case the polynomials $\xi_j^{(1)}, j = 2, 3, \cdots, j_1$, may simply be omitted from the list of defining elements. If the system thus obtained from $\mathfrak{p}$ and $\zeta_j^{(1)}$ is not equivalent to unity a similar method of reasoning may be applied to the elements $\zeta_j^{(2)}, j = 1, 2, \cdots, j_2$, of $\mathfrak{q}_2$ in $\mathfrak{Q}$, these elements being reduced modulo the absolute prime modular system $(\xi_1^{(1)}, \mathfrak{p})$. Hereafter we shall write $\xi_1^{(1)}$ as ξ_1 when there is only one distinct polynomial of this type in the unknown x_1. It is seen that $\mathfrak{P}$ either contains one irreducible polynomial ξ_2 as a defining element in the unknown x_2, or $\mathfrak{P} = (1)$. Continuing in this manner we can show that either

$$\mathfrak{P} = (\xi_n, \xi_{n-1}, \cdots, \xi_i, \cdots, \xi_1, \mathfrak{p})$$

or $\mathfrak{P} = (1)$. In either case we see that $\mathfrak{Q}$ can contain one and only one absolute prime modular system if (1) is counted as such a system. But if

$\mathfrak{P} = (1)$ it easily follows that $\mathfrak{Q} = (1)$. We omit the proof. Moreover, it follows that all of these conclusions hold true for all simple systems, for a simple system $\mathfrak{Q}$ can at most be equal to the product of a number of irreducible modular systems no two of which are relatively prime. Since each of these irreducible systems can contain but one absolute prime system $\mathfrak{P}$ it follows that all must contain the same system $\mathfrak{P}$, and therefore the simple system $\mathfrak{Q}$ can contain only this one system $\mathfrak{P}$. Hence we have proven the theorem:

THEOREM. *A simple modular system* $\mathfrak{Q}$, *not equivalent to* (1), *contains one and only one absolute prime modular system* $\mathfrak{P}$.

From the preceding we see that when we break up a modular system $\mathfrak{M}$ into its simple factors, a number of the systems $\mathfrak{Q}$ obtained may be equivalent to (1). These are not to be looked upon as modular factors of $\mathfrak{Q}$ in the ordinary sense, their purpose merely being to enable us to build up $\mathfrak{M}$ in its standard form as the product of simple systems $\mathfrak{Q}$ of standard form.

Let us suppose that the polynomial f belonging to the residue system of $\mathfrak{M}$ can be written as a $F(\mathfrak{M}'')$. If $\mathfrak{M}''$ is a modular factor of $\mathfrak{M}$ we shall define it as a *common factor* of f and $\mathfrak{M}$. If in addition we have $\mathfrak{M} = \mathfrak{M}'\mathfrak{M}''$ and $(f, \mathfrak{M}') = (1)$, we shall define $\mathfrak{M}''$ as the *greatest common divisor* of f and $\mathfrak{M}$. It may be noticed that the word factor when used in connection with f simply means that f is a polynomial congruent to zero with respect to the modular system used in this connection. Moreover every modular factor of $\mathfrak{M}$ is equivalent to the product of some of the irreducible modular factors of $\mathfrak{M}$. We have defined f as being prime to $\mathfrak{M}$ whenever $(f, \mathfrak{M}) = (1)$. We shall define the total number of residue classes of the modular system $\mathfrak{M}$ whose residues are prime to $\mathfrak{M}$ as the *totient* of $\mathfrak{M}$, and designate it by $\phi(\mathfrak{M})$. There also exist modular systems $\mathfrak{M}''$ that either are not factors of $\mathfrak{M}$ at all, or in case they are, $(\mathfrak{M}', \mathfrak{M}'') \neq (1)$. If such a system $\mathfrak{M}''$ includes f among the polynomials $F(\mathfrak{M}'')$, where f in turn is not congruent to 0 with respect to any modular system $\mathfrak{M}_1$ that contains $\mathfrak{M}''$ and is itself contained in $\mathfrak{M}$, it follows that while $(f, \mathfrak{M})$ may be taken as being equal to $\mathfrak{M}''$, this system is not to be considered as a greatest common divisor according to the definition given above. Whenever this happens we shall say that f and $\mathfrak{M}$ have a *hidden factor* in common, where it may happen that the hidden factor is not at all a modular factor of $\mathfrak{M}$. Here $\mathfrak{M}''$ is equal to the product of those simple modular factors of $\mathfrak{M}$ with respect to which f is congruent to 0, and of a number of simple and often irreducible systems each of which is contained in $\mathfrak{M}$, but none of them equivalent to a simple modular factor of $\mathfrak{M}$. It is this latter set of modular factors that comprise the " hidden " part of the common factor of f and $\mathfrak{M}$. The whole question may be summed up by saying that

whenever f and $\mathfrak{M}$ have a hidden factor in common and $(f, \mathfrak{M}) = \mathfrak{M}''$, there does not exist a modular system $\mathfrak{M}'$ such that $\mathfrak{M} = \mathfrak{M}'\mathfrak{M}''$ and $(\mathfrak{M}', \mathfrak{M}'') = (1)$. As an illustration we may cite the following example. Let $\mathfrak{M} = (x^4 + 5x^3 + 2x^2 + 7x, 9) = (x^2 + 4x + 7, 9)(x + 1, 9)(x, 9)$, and $f = x^3 + 4x^2 + x$. Here f is prime to $(x + 1, 9)$, has the factor $(x, 9)$ in common with $\mathfrak{M}$, and while it is not a polynomial $F(x^2 + 4x + 7, 9)$, it is a $F(x^2 + x + 1, 3)$, where $(x^2 + x + 1, 3)$ is the absolute prime system contained in $(x^2 + 4x + 7, 9)$. Hence the hidden factor is $(x^2 + x + 1, 3)$, while $\mathfrak{M}'' = (x, 9)(x^2 + x + 1, 3) = (x^3 + x^2 + x, 3x, 9)$. If $\mathfrak{M}$ is irreducible it follows that $\mathfrak{M}''$ is either equal to $\mathfrak{M}$, to (1), or contains a hidden factor.

Whenever we shall speak of a necessary and sufficient condition that a set of residue classes belonging to $\mathfrak{M}$ form a group, we shall always mean a *maximal set*, i. e. a set such that there exist no other residue classes belonging to $\mathfrak{M}$ which when added to the set will cause the augmented set also to form a group modulo $\mathfrak{M}$. Such a group we shall for convenience sake designate as a *maximal group*. Certain subsets of a maximal set will form subgroups of the corresponding maximal groups.

II. Determination of conditions that a set of residue classes form a group

We shall proceed to derive some theorems concerning necessary and sufficient conditions under which a set of residue classes may form a group. Represent each residue class of the modular system $\mathfrak{M}$ by some representative residue. Let us exclude all residues with hidden factors. As we shall soon prove that these cannot belong to a group this exclusion does not affect the generality of the following arguments. It is at once evident that all residues belonging to any one group must have the same greatest common divisor with $\mathfrak{M}$. For let us suppose that f_1 and f_2 are any two residues belonging to the same group. From the definition of a group we know that there exists a residue X in such a group such that $f_1 X \equiv f_2$, mod $\mathfrak{M}$. If $\mathfrak{Q}$ is a simple modular factor of $(f_1, \mathfrak{M})$ that is not contained by $(f_2, \mathfrak{M})$, the above congruence does not hold modulo $\mathfrak{Q}$, one side reducing to zero while the other does not. Since this cannot be, $(f_1, \mathfrak{M})$ and $(f_2, \mathfrak{M})$ cannot differ. Hence the condition is necessary.

Let us take the totality of representative residues f that have the same greatest common divisor with $\mathfrak{M}$, and designate this divisor by $\mathfrak{M}''$. From previous definitions it follows that there must exist a system $\mathfrak{M}'$ such that $\mathfrak{M}'\mathfrak{M}'' = \mathfrak{M}$ and $(\mathfrak{M}', \mathfrak{M}'') = 1$. The product of any two residues of our set gives a third one of the set. For if

$$f_1 f_2 \equiv f_3, \quad \text{mod } \mathfrak{M},$$

be such a product, it follows that

$$f_1 f_2 \equiv f_3, \mod \mathfrak{M}''.$$

and as $f_1 f_2 \equiv 0$, mod $\mathfrak{M}''$, we have

$$f_3 \equiv 0, \mod \mathfrak{M}''.$$

Moreover, f_3 has no other modular factor in common with $\mathfrak{M}$ since it would then follow in a similar manner that either f_1 or f_2 would have to contain this factor, a fact contrary to hypothesis. In the second place the product of one residue of the set by all of the set gives back all, for otherwise there would exist at least one congruence of the form

$$f_1 f_2 \equiv f_1 f_3, \mod \mathfrak{M},$$

from which follows

(A) $$f_1 (f_2 - f_3) \equiv 0, \mod \mathfrak{M}.$$

Since f_2 and f_3 both contain $\mathfrak{M}''$ and $\mathfrak{M} = \mathfrak{M}' \mathfrak{M}''$ it follows that

$$f_2 - f_3 \equiv 0, \mod \mathfrak{M}''.$$

As f_1 is prime to $\mathfrak{M}'$ it follows from (A) that we must have

$$f_2 - f_3 \equiv 0, \mod \mathfrak{M}',$$

and therefore

$$f_2 \equiv f_3, \mod \mathfrak{M},$$

which is contrary to assumptions. Hence we must get back the whole set of residues. Since the associative and commutative laws of multiplication hold our residues form an abelian group of finite order. Our group is maximal because it contains all residue classes whose residues have the greatest common divisor $\mathfrak{M}''$ with $\mathfrak{M}$.

We shall now prove that representative residues with hidden factors do not belong to groups. If f were such a residue and belonged to such a group, it would have to repeat itself if raised to a sufficiently high power, mod $\mathfrak{M}$, and therefore also modulo every simple modular divisor of $\mathfrak{M}$. Let $\mathfrak{Q}$ be one of those simple modular factors of $\mathfrak{M}$ that contains a system $\mathfrak{Q}'$ that is a hidden factor of f. If $\mathfrak{Q}$ is defined by $(\mathfrak{q}_n, \mathfrak{q}_{n-1}, \cdots, \mathfrak{q}_1, \mathfrak{p}^\alpha)$ we can write the following *descending sequence* of modular systems contained in $\mathfrak{Q}$:

$$\mathfrak{Q} = \mathfrak{Q}_1 = (\mathfrak{q}_n, \mathfrak{q}_{n-1}, \cdots, \mathfrak{q}_2, \mathfrak{q}_1, \mathfrak{p}^\alpha),$$

$$\mathfrak{Q}_2 = (\mathfrak{q}_n, \mathfrak{q}_{n-1}, \cdots, \mathfrak{q}_2, \mathfrak{q}_1, \mathfrak{p}^{\alpha-1}),$$

$$\mathfrak{Q}_3 = (\mathfrak{q}_n, \mathfrak{q}_{n-1}, \cdots, \mathfrak{q}_2, \mathfrak{q}_1, \mathfrak{p}^{\alpha-2}),$$

. . . . . .

$$\mathfrak{Q}_{a-1} = (\mathfrak{q}_n, \mathfrak{q}_{n-1}, \cdots, \mathfrak{q}_2, \mathfrak{q}_1, \mathfrak{p}^2),$$

$$\mathfrak{Q}_a = (\mathfrak{q}_n, \mathfrak{q}_{n-1}, \cdots, \mathfrak{q}_2, \mathfrak{q}_1, \mathfrak{p})$$

$$= (\mathfrak{q}_n, \mathfrak{q}_{n-1}, \cdots, \mathfrak{q}_2, \xi_1^{\epsilon_1}, \mathfrak{p}),$$

where $\xi_1^{\epsilon_1}$ is the highest common divisor, mod $\mathfrak{p}$, of all the defining elements of $\mathfrak{q}_1$.

$$\mathfrak{Q}_{a+1} = (\mathfrak{q}_n, \mathfrak{q}_{n-1}, \cdots, \mathfrak{q}_2, \xi_1^{\epsilon_1-1}, \mathfrak{p}),$$

. . . . . .

$$\mathfrak{Q}_{a+\epsilon_1-1} = (\mathfrak{q}_n, \mathfrak{q}_{n-1}, \cdots, \mathfrak{q}_2, \xi_1, \mathfrak{p}),$$

$$= (\mathfrak{q}_n, \mathfrak{q}_{n-1}, \cdots, \xi_2^{\epsilon_2}, \xi_1, \mathfrak{p}),$$

. . . . . .

. . . . . .

$$\mathfrak{Q}_{k-1} = (\mathfrak{q}_n, \xi_{n-1}^2, \xi_{n-2}, \cdots, \xi_1, \mathfrak{p}),$$

$$\mathfrak{Q}_k = (\mathfrak{q}_n, \xi_{n-1}, \cdots, \xi_1, \mathfrak{p}),$$

$$= (\xi_n^{\epsilon_n}, \xi_{n-1}, \cdots, \xi_1, \mathfrak{p}),$$

. . . . . .

$$\mathfrak{Q}_{\rho-1} = (\xi_n^2, \xi_{n-1}, \cdots, \xi_1, \mathfrak{p}),$$

$$\mathfrak{Q}_\rho = \mathfrak{P} = (\xi_n, \xi_{n-1}, \cdots, \xi_1, \mathfrak{p}).$$

Let $\mathfrak{Q}_\tau$ designate the first modular system in this sequence that is contained in $\mathfrak{Q}'$, and let us write

$$\mathfrak{Q}_\tau = (\mathfrak{q}_n, \cdots, \mathfrak{q}_{s+1}, \xi_s^r, \xi_{s-1}, \cdots, \xi_1, \mathfrak{p}).$$

By our assumptions $f \equiv 0$, mod $\mathfrak{Q}_\tau$, and $f \not\equiv 0$, mod $\mathfrak{Q}_{\tau-\sigma}$, $\sigma = 1, 2, \cdots, \tau - 1$, the existence of these congruences being based upon the fact that f is a $F(\mathfrak{P})$, but not a $F(\mathfrak{Q})$. From the nature of the above sequence it is at once evident that $f^2 \equiv 0$, mod $\mathfrak{Q}_{\tau-1}$. In a similar manner we see that $f^4 = (f^2)^2 \equiv 0$, mod $\mathfrak{Q}_{\tau-2}$, etc., so that there must exist some power of f, either f^{2^σ} or a lower power, that is congruent to 0, mod $\mathfrak{Q}_{\tau-\sigma}$. Let f^ω be this power of f. It follows that all higher powers of f, beginning with f^ω, are congruent to 0, mod $\mathfrak{Q}_{\tau-\sigma}$. Since this was not true for f itself, we see that f cannot repeat itself when raised to powers modulo $\mathfrak{Q}_{\tau-\sigma}$ in general and modulo $\mathfrak{Q}$ in particular. Hence f cannot belong to a group and we have proven the theorem:

THEOREM. *A necessary and sufficient condition that a set of residue classes belonging to the modular system $\mathfrak{M}$ form a maximal group is that* (1) *these residue classes contain all polynomials having the greatest common divisor $\mathfrak{M}''$ with $\mathfrak{M}$;* (2) *there exists a modular system $\mathfrak{M}'$, relatively prime to $\mathfrak{M}''$, such that $\mathfrak{M} = \mathfrak{M}'\mathfrak{M}''$.*

When $\mathfrak{M}'' = (1)$ we have the residues prime to $\mathfrak{M}$. This group we designate as the $\mathfrak{M}$ *group of totitives.*

We shall proceed to restate this condition in another form. It is evident that if we have a maximal set forming a group modulo $\mathfrak{M}$, that this set must also form a group with respect to every modular factor of $\mathfrak{M}$. On the other hand, if we pick out any largest possible set of residues, mod $\mathfrak{M}$, such that the residues of the set form a group with respect to every simple modular factor of $\mathfrak{M}$, this set must also form a maximal group modulo $\mathfrak{M}$. For if f_1 and f_2 are any two of the set, their product, which we may denote by f_3, must also be in the set, for in the contrary case there would exist at least one modular factor of $\mathfrak{M}$ with respect to which our set does not form a group, which is contrary to assumptions. Again the product of one residue of the set into all the residues of the set gives back the whole set, mod $\mathfrak{M}$. If this were not the case at least one product would have to be repeated, let us say

$$f_1 f_2 \equiv f_1 f_3, \mod \mathfrak{M}.$$

This congruence must also hold for every simple modular factor $\mathfrak{Q}$ of $\mathfrak{M}$. Since, however, our set forms a group with respect to each of these factors, it follows from the definition of a group that for all values of $\mathfrak{Q}$ we have

$$f_2 \equiv f_3, \mod \mathfrak{Q}.$$

But a congruence that holds for every simple modular factor of $\mathfrak{M}$ also holds modulo $\mathfrak{M}$.* As this contradicts our assumption it follows that no product can be repeated. Hence our statement is proven and we have the theorem:

THEOREM. *A necessary and sufficient condition that a set of residue classes form a group modulo* $\mathfrak{M}$ *is that they form a group with respect to every simple modular factor of* $\mathfrak{M}$. This theorem does not state quite as much as the preceding one, but will be found useful later on.

Let us now consider the total number of possible maximal groups. By the first theorem of this section no two maximal groups can have the same unit operator. As a group can have but one unit operator it follows that the number of maximal groups belonging to $\mathfrak{M}$ is equal to the number of unit or idempotent operators found in a complete set of representative residues. This number is evidently equal to the number of possible values of $\mathfrak{M}''$, where $\mathfrak{M} = \mathfrak{M}'\mathfrak{M}''$ and $(\mathfrak{M}', \mathfrak{M}'') = (1)$. Since $\mathfrak{M}''$ is equal to the product of a number of simple modular factors $\mathfrak{Q}$ of $\mathfrak{M}$, this is equal to the number of possible combinations of the different simple modular factors of $\mathfrak{M}$, first taken one at a time, then two at a time, etc., until finally all are taken at once, besides the case when $\mathfrak{M}'' = (1)$. This number we know to be 2^λ, where λ is equal to the number of simple modular factors in $\mathfrak{M}$. Hence we have the theorem:

* König, *Algebraische Grösszen*, p. 355.

THEOREM. *The residue classes of the modular system* $\mathfrak{M}$ *contain* 2^λ *maximal groups, where* λ *is equal to the number of distinct simple modular factors of* $\mathfrak{M}$.

We shall now see that the restrictions we imposed upon our modular system in the opening paragraph of this paper are not as great as it may seem. Let us consider the defining elements $\psi_1^{(i)}, \psi_2^{(i)}, \cdots, \psi_{j_i}^{(i)}$ of $\mathfrak{m}_i$. As long as only one of these ψ's, say $\psi_1^{(i)}$, has the coefficient of the highest power of x_i equal to 1 our developments evidently hold, for any defining element $\psi_j^{(i)}$ of which this is not true can be replaced by the defining element $\psi_j^{(i)} + \psi_1^{(i)}$ whenever the degree of $\psi_1^{(i)}$ is greater than that of $\psi_j^{(i)}$, and by $x_i^\kappa \psi_1^{(i)} + \psi_j^{(i)}$ when the degree of $\psi_j^{(i)}$ is greater than that of $\psi_1^{(i)}$, the κ being so chosen that the degree of $x_i^\kappa \psi_1^{(i)}$ in x_i is greater than that of $\psi_j^{(i)}$. The question now arises what conditions must the various $\psi_j^{(i)}$ fulfil so that we can always, if necessary, replace the defining elements of $\mathfrak{m}_i$ by an equivalent set with at least one defining element $\psi_j^{(i)}$ whose highest power of x_i has the coefficient 1. By the first theorem of this section we saw that all residues of $\mathfrak{M}_{i-1}$ that are prime to this system form a group modulo $\mathfrak{M}_{i-1}$. We may now consider the coefficients of the various $\psi_j^{(i)}$ of $\mathfrak{m}_i$ as being taken modulo $\mathfrak{M}_{i-1}$. If the coefficient of the highest power of x_i of one of these defining ψ's, say $\psi_1^{(i)}$, is relatively prime to $\mathfrak{M}_{i-1}$, there exists a residue modulo $\mathfrak{M}_{i-1}$ that when multiplied into this coefficient gives 1, mod $\mathfrak{M}_{i-1}$. Let us multiply $\psi_1^{(i)}$ by this inverse to the highest coefficient of $\psi_1^{(i)}$. Modulo $\mathfrak{M}_{i-1}$ we now have a $\psi_j^{(i)}$ that has the coefficient of the highest power of x_i equal to 1. But it is also evident that if we replace our old defining element of $\mathfrak{m}_i$ by this new one, the $\mathfrak{m}_i$ is not changed and the same is true of $\mathfrak{M}$. Hence we have proven the following:

THEOREM. *Any modular system fulfilling the conditions laid down in the first paragraph of this paper with the exception of the one concerning the coefficients of the highest powers of the various* x_i *in each of the different* $\psi_j^{(i)}$ *being equal to* 1, *is equivalent to a system* $\mathfrak{M}$ *of standard form as there defined if every one of the various* $\mathfrak{m}_i$ *in the system under consideration contains at least one defining element* $\psi_j^{(i)}$ *such that the coefficient of the highest power of* x_i *in this* $\psi_j^{(i)}$ *is relatively prime to the modular system* $(\mathfrak{m}_{i-1}, \mathfrak{m}_{i-2}, \cdots, \mathfrak{m}_1, \mathfrak{m})$ *contained in the system under consideration.*

It is evident that all of the developments of this paper hold for all systems fulfilling the conditions just stated. Since each of these systems is equivalent to a system in the standard form we shall always replace each system by a system equivalent to it and in the standard form.

III. COMPOSITION OF A MAXIMAL GROUP BELONGING TO $\mathfrak{M}$

We shall now proceed to study the structure of any maximal group belonging to $\mathfrak{M}$. Let us take the group G whose operators f have with $\mathfrak{M}$ the greatest

common divisor $(f, \mathfrak{M}) = \mathfrak{M}''$, where $\mathfrak{M} = \mathfrak{M}'\mathfrak{M}''$ and $(\mathfrak{M}', \mathfrak{M}'') = (1)$. Also let us suppose that we can factor $\mathfrak{M}$ in some other way, let us say $\mathfrak{M} = \mathfrak{M}_1\mathfrak{M}_2$, where $(\mathfrak{M}_1, \mathfrak{M}_2) = (1)$. Let us write $\mathfrak{M}' = \mathfrak{M}_1'\mathfrak{M}_2'$ and $\mathfrak{M}'' = \mathfrak{M}_1''\mathfrak{M}_2''$, where $\mathfrak{M}_1 = \mathfrak{M}_1'\mathfrak{M}_1''$ and $\mathfrak{M}_2 = \mathfrak{M}_2'\mathfrak{M}_2''$. Let f_τ', $\tau = 1, 2, \cdots, N(\mathfrak{M}_1)$, be a complete set of representative residues of $\mathfrak{M}_1$. Similarly let f_τ'', $\tau = 1, 2, \cdots, N(\mathfrak{M}_2)$, be a complete set of representative residues of $\mathfrak{M}_2$. Since $(\mathfrak{M}_1, \mathfrak{M}_2) = (1)$, it follows that there is at least one defining element ζ' of $\mathfrak{M}_1$ that is relatively prime to $\mathfrak{M}_2$, and similarly at least one defining element ζ'' of $\mathfrak{M}_2$ that is relatively prime to $\mathfrak{M}_1$. Let us write down the $N(\mathfrak{M}_1)$ polynomials of the form $\zeta'' f_\tau' + 1$, $\tau = 1, 2, \cdots, N(\mathfrak{M}_1)$. These are all incongruent modulo $\mathfrak{M}_1$, for if two were congruent it would follow from this congruence which we shall denote by

$$\zeta'' f_1' + 1 \equiv \zeta'' f_2' + 1, \mod \mathfrak{M}_1,$$

that we have

$$\zeta''(f_1' - f_2') \equiv 0, \mod \mathfrak{M}_1,$$

and since ζ'' is relatively prime to $\mathfrak{M}_1$ it follows that

$$f_1' \equiv f_2', \mod \mathfrak{M}_1,$$

which is contrary to assumptions. Hence the polynomials $\zeta'' f_\tau' + 1$, $\tau = 1, 2, \cdots, N(\mathfrak{M}_1)$, constitute a complete set of representative residues modulo $\mathfrak{M}_1$. Similarly we can represent a complete set of residues of $\mathfrak{M}_2$ in the form $\zeta' f_\tau'' + 1$, $\tau = 1, 2, \cdots, N(\mathfrak{M}_2)$. If we multiply each polynomial of the complete set of the $\zeta'' f_\tau' + 1$ into each one of the set $\zeta' f_\tau'' + 1$ the resulting products are all incongruent modulo $\mathfrak{M}$. For suppose that two of these products are congruent, let us say

$$(\zeta'' f_1' + 1)(\zeta' f_1'' + 1) \equiv (\zeta'' f_2' + 1)(\zeta' f_2'' + 1), \mod \mathfrak{M}.$$

Since this congruence also holds modulo $\mathfrak{M}_1$ and $\zeta' \equiv 0$, mod $\mathfrak{M}_1$, it follows that

$$\zeta'' f_1' + 1 \equiv \zeta'' f_2' + 1, \mod \mathfrak{M}_1,$$

and therefore

$$f_1' \equiv f_2', \mod \mathfrak{M}_1.$$

In a similar way we see that our congruence reduces to $f_1'' \equiv f_2''$, mod $\mathfrak{M}_2$. Since our two products are not composed of the same factors we see that they cannot be congruent modulo $\mathfrak{M}$. Since every residue of $\mathfrak{M}$ must be congruent to some $\xi'' f_\tau' + 1$ modulo $\mathfrak{M}_1$ and to some $\zeta' f_\tau'' + 1$ modulo $\mathfrak{M}_2$, it follows that it must be congruent to their product modulo $\mathfrak{M}$, and we see that this set of products gives us a complete set of residues modulo $\mathfrak{M}$. We shall make use of this fact later on.

Now let us pick out of the total set $\zeta'' f''_\tau + 1$ all of those residues that have the greatest common divisor $\mathfrak{M}_1''$ with $\mathfrak{M}_1$. Similarly pick out all those of the set $\zeta' f''_\tau + 1$ whose greatest common divisor with $\mathfrak{M}_2$ is $\mathfrak{M}_2''$. The first of these selected sets forms a group modulo $\mathfrak{M}_1$ by the first theorem of the preceding section, while modulo $\mathfrak{M}_2$ it forms a group of order one because all of its operators reduce to 1. Hence this selected set must also form a group modulo $\mathfrak{M}$ by the second theorem of the preceding section. A similar argument holds for the second selected set. The products obtained by multiplying the elements of one group into the elements of the other group modulo $\mathfrak{M}$ must all have with $\mathfrak{M}$ the greatest common divisor $\mathfrak{M}''$, for $(\mathfrak{M}_1'', \mathfrak{M}_2'') = (1)$. Moreover it is evident that no product can be formed such that it has the greatest common divisor $\mathfrak{M}''$ with $\mathfrak{M}$ unless it is formed by the product of two elements belonging to those two groups. Hence it is seen that we can represent a group G of residues belonging to $\mathfrak{M}$ and such that its operators all satisfy the condition $(f, \mathfrak{M}) = \mathfrak{M}''$, where $\mathfrak{M} = \mathfrak{M}'\mathfrak{M}''$ and

$$(\mathfrak{M}', (\mathfrak{M}'' = (1),$$

as the direct product of two groups of residues simply isomorphic to the groups to which the residues of G reduce modulo the systems $\mathfrak{M}_1$ and $\mathfrak{M}_2$ respectively, where $\mathfrak{M} = \mathfrak{M}_1\mathfrak{M}_2$ and $(\mathfrak{M}_1, \mathfrak{M}_2) = (1)$. Hence we have the theorem:

THEOREM. *Any maximal group G of residues belonging to the modular system $\mathfrak{M} = \mathfrak{M}_1\mathfrak{M}_2$, where $(\mathfrak{M}_1, \mathfrak{M}_2) = (1)$, is the direct product of two groups simply isomorphic to the groups obtained modulo $\mathfrak{M}_1$ and $\mathfrak{M}_2$ when the operators of G are taken modulo these two systems.*

Each of the two systems $\mathfrak{M}_1$ and $\mathfrak{M}_2$ may again be broken up into two factors that are relatively prime to another, and it may be shown that our group G taken modulo $\mathfrak{M}$ is the direct product of four groups simply isomorphic to the groups obtained by taking the operators of G modulo these factors of $\mathfrak{M}_1$ and $\mathfrak{M}_2$, which is necessarily true because G depends upon the groups to which its operators reduce modulo $\mathfrak{M}_1$ and $\mathfrak{M}_2$, and these groups in turn depend upon the four groups mentioned. Continuing to divide up the factors of $\mathfrak{M}$ in this manner until we reach the simple modular factors Ω we see that we have shown the following theorem to hold:

THEOREM. *A maximal group G belonging to the modular system $\mathfrak{M}$ is the direct product of groups simply isomorphic to the groups obtained when the operators of G are taken modulo the various simple modular factors of $\mathfrak{M}$.*

Let us suppose that the operators of G all have the greatest common divisor $\mathfrak{M}''$ with $\mathfrak{M}$, where $\mathfrak{M} = \mathfrak{M}'\mathfrak{M}''$, and $(\mathfrak{M}', \mathfrak{M}'') = 1$. Every simple modular factor of $\mathfrak{M}$ is necessarily a factor of $\mathfrak{M}'$ or of $\mathfrak{M}''$. If it is a factor of $\mathfrak{M}''$ the residues of G give only an operator congruent to zero, i. e., a group of order

one, modulo this simple factor. If it is a factor of $\mathfrak{M}'$ we have the group of totitives of this factor when taking the operators of G modulo this factor, for otherwise by retracing our steps we could show that whenever this is not the case our group G is not maximal modulo $\mathfrak{M}$. Hence G is the direct product of groups simply isomorphic to the product of the groups of totitives of the various simple modular factors of $\mathfrak{M}'$ and groups of order 1 corresponding to the simple factors of $\mathfrak{M}''$. Since these latter groups can exercise no influence upon the structure of the abstract group formed by the product of the groups of totitives mentioned, it follows that we have proven the theorem:

THEOREM. *The maximal group G formed by the residue classes of the modular system $\mathfrak{M}$ whose representative residues have with $\mathfrak{M}$ the greatest common divisor $\mathfrak{M}''$, where $\mathfrak{M} = \mathfrak{M}'\mathfrak{M}''$ and $(\mathfrak{M}', \mathfrak{M}'') = (1)$, is the direct product of groups simply isomorphic to the groups of totitives of the various simple modular factors of $\mathfrak{M}'$.*

Since the group of totitives of $\mathfrak{M}'$ is also the direct product of groups simply isomorphic to the groups of totitives of the various simple modular factors of $\mathfrak{M}'$ we have at once the following theorem:

THEOREM. *Any maximal group belonging to the modular system $\mathfrak{M}$ is simply isomorphic to the group of totitives of some modular factor of $\mathfrak{M}$.*

We shall now state a theorem whose proof is based upon the following two facts. In the first place any modular system contained in $\mathfrak{M}$ is equal to the product of simple modular systems each of which is in turn contained in one of the simple modular factors of $\mathfrak{M}$. Secondly the group of totitives of a simple modular system $\mathfrak{Q}$ contains as a subgroup a group simply isomorphic with the group of totitives of any modular system contained in $\mathfrak{Q}$. The former of these statements is self-evident, while the latter follows from the fact that every quotient group of an abelian group is simply isomorphic to a subgroup of the same group. From this there follows the theorem:

THEOREM. *The group of totitives belonging to the modular system $\mathfrak{M}$ contains as a subgroup a group simply isomorphic to any group of residue classes belonging to $\mathfrak{M}$ or to any modular system contained in $\mathfrak{M}$.*

Our problem has now been reduced to one dealing with the groups belonging to a simple modular system $\mathfrak{Q}$. Such a system can have but two maximal groups. One of these is of order 1 and contains the 0 as its only operator, while the other one is the $\mathfrak{Q}$ group of totitives of order $\phi(\mathfrak{Q})$, where $\phi(\mathfrak{Q})$ represents the number of residue classes whose representative residues are prime to $\mathfrak{Q}$. The question of determining the structure of this group is rather difficult and will not be solved. We shall, however, determine its order $\phi(\mathfrak{Q})$ and some of its properties.

Let us first confine ourselves to the case where $\mathfrak{Q}$ is an absolute prime

modular system $\mathfrak{P}$. We know that the congruence

$$A_0 X^n + A_1 X^{n-1} + \cdots + A_n \equiv 0, \mod \mathfrak{P},$$

where $A_0 \not\equiv 0$, the A's being polynomials, cannot be satisfied by more than n polynomials.* All the representative residues belonging to $\mathfrak{P}$ are relatively prime to $\mathfrak{P}$, excepting the 0. Let f be any one of these. Since it belongs to the $\mathfrak{P}$ group of totitives it must repeat itself when raised to powers. Let τ designate its order. The polynomials $f, f^2, \cdots, f^\tau = 1$ are all incongruent. Let σ represent any one of the numbers $1, 2, \cdots, \tau$. Then

$$(f^\sigma)^\tau - 1 \equiv 0, \mod \mathfrak{P}.$$

This congruence is of the form

$$X^n - 1 \equiv 0, \mod \mathfrak{P},$$

and cannot have more than n solutions. Since $f, f^2, \cdots, f^\tau$ satisfy this congruence it is evident that no other representative residue of $\mathfrak{P}$ can do so. Let δ be the order of f^σ, $\sigma = 1, 2, \cdots, \tau$. Now $\delta\sigma$ necessarily is a multiple of τ. If τ is prime to σ we have $\delta = \tau$, otherwise if ω is the greatest common divisor of τ and σ,

$$(f^\sigma)^{\tau/\omega} \equiv (f^{\sigma/\omega})^\tau \equiv 1, \mod \mathfrak{P},$$

so that f^σ is of lower order than f. As there are but $\phi(\tau)$ integers of the set $1, 2, \cdots, \tau$, that are prime to τ it follows that there are but $\phi(\tau)$ residues belonging to our representative set modulo $\mathfrak{P}$ that are of order τ. Hence the $\mathfrak{P}$ group of totitives can have but one subgroup of order τ, where τ is the order of any operator in the group. Hence it follows at once that our group is cyclic. Since 0 is the only representative residue of $\mathfrak{P}$ that does not belong to this group we have its order equal to $\phi(\mathfrak{P}) = N(\mathfrak{P}) - 1$. But the value of $N(\mathfrak{P})$ is equal to $[N(\mathfrak{p})]^{\epsilon_1\epsilon_2\cdots\epsilon_n}$, where $\mathfrak{P} = (\xi_n, \xi_{n-1}, \cdots, \xi_1, \mathfrak{p})$, and ξ_i is of degree ϵ_i.† Hence it follows that $N(\mathfrak{P})$ is of the form $p^{\epsilon_0\epsilon_1\cdots\epsilon_n}$, where p is the rational prime divisible by $\mathfrak{p}$, and $N(\mathfrak{p}) = p^{\epsilon_0}$. Therefore we have proven the following theorem first given by Serret for the case that $\mathfrak{P} = (\xi_1, p)$, and Ω is the rational realm:

All the residue classes of an absolute prime modular system $\mathfrak{P}$ with the exception of the one containing the 0, form a cyclic group of order

$$\phi(\mathfrak{P}) = N(\mathfrak{P}) - 1 = p^{\epsilon_0\epsilon_1\cdots\epsilon_n} - 1.$$

Let us again as in section II write a descending sequence of modular systems beginning with Ω and ending with $\mathfrak{P}$, the absolute prime system contained

* König, *Algebraische Gröszen*, p. 413.

† König, *Algebraische Gröszen*, pp. 403–404.

in $\mathfrak{Q}$. Since $\mathfrak{Q}$ is simple it follows that every operator in the $\mathfrak{Q}$ group of totitives is relatively prime to every modular system in the sequence. Write down the group of totitives of each of the modular systems in our sequence. Set off in each of them, excepting the case of $\mathfrak{P}$, the subgroup composed of all the operators that reduce to 1 when taken modulo the next system in the sequence. For $\mathfrak{P}$ take the whole group of totitives. It now easily follows that the operators of the $\mathfrak{Q}_\tau$ group of totitives can be obtained by multiplying together, mod $\mathfrak{Q}_\tau$, the operators of the $\mathfrak{Q}_{\tau+1}$ group of totitives and the subgroup of the $\mathfrak{Q}_\tau$ group composed of those operators that reduce to 1, mod $\mathfrak{Q}_{\tau+1}$. For in the first place no two such products are congruent, mod $\mathfrak{Q}_\tau$, for if this were the case and we had

$$a_1 b_1 \equiv a_2 b_2, \mod \mathfrak{Q}_\tau,$$

where a_1 and a_2 are operators of the $\mathfrak{Q}_{\tau+1}$ group of totitives, and b_1 and b_2 are operators of the $\mathfrak{Q}_\tau$ group that reduce to 1, mod $\mathfrak{Q}_{\tau+1}$, it would follow that the above congruence would reduce to $a_1 \equiv a_2$, mod $\mathfrak{Q}_{\tau+1}$, so that $a_1 = a_2$. Hence we have $a_1 b_1 \equiv a_1 b_2$, mod $\mathfrak{Q}_\tau$, and therefore $b_1 \equiv b_2$, mod $\mathfrak{Q}_\tau$, for a_1, b_1, and b_2 are all relatively prime to $\mathfrak{Q}_\tau$, and therefore operators in the $\mathfrak{Q}_\tau$ group of totitives. Hence $b_1 = b_2$, and we see that to be congruent modulo $\mathfrak{Q}_\tau$ such products must be identical. The entire $\mathfrak{Q}_\tau$ group of totitives reduces to the $\mathfrak{Q}_{\tau+1}$ group of totitives when its operators are taken modulo $\mathfrak{Q}_{\tau+1}$. The number of operators that reduce to any given operator of the $\mathfrak{Q}_{\tau+1}$ group is evidently the same in all cases, and is equal to the order of the subgroup of the $\mathfrak{Q}_\tau$ group used in forming these products. Hence the order of the $\mathfrak{Q}_\tau$ group of totitives is equal to the product of the order of the $\mathfrak{Q}_{\tau+1}$ group of totitives and the order of the subgroup of the $\mathfrak{Q}_\tau$ group composed of the operators that reduce to 1, mod $\mathfrak{Q}_{\tau+1}$. This holds for all systems in the sequence, beginning with $\mathfrak{Q}$, excepting $\mathfrak{P}$, the latter case having been considered in the last theorem. Hence the order of the $\mathfrak{Q}$ group of totitives is equal to the product of the orders of the various subgroups in the different $\mathfrak{Q}_\tau$ groups composed of operators reducing to 1 modulo the next lower system, multiplied into the order of the $\mathfrak{P}$ group of totitives. We have already determined the order of the latter group, and shall now proceed to determine the orders of the subgroups in question.

By assumption we have for any operator f in the subgroup chosen from $\mathfrak{Q}_\tau$ that $f = 1 + F(\mathfrak{Q}_{\tau+1})$. Raising f to powers we can write

$$f^\sigma = (1 + F(\mathfrak{Q}_{\tau+1}))^\sigma = 1 + \sigma \cdot F(\mathfrak{Q}_{\tau+1}) + F'(\mathfrak{Q}_\tau).$$

The order of f, mod $\mathfrak{Q}_\tau$, is determined by seeing when $\sigma \cdot F(\mathfrak{Q}_{\tau+1})$ is an $F(\mathfrak{Q}_\tau)$. We know that $\mathfrak{Q}_{\tau+1}$ and $\mathfrak{Q}_\tau$ differ only in that the former has a

defining element ξ_s^r, while the latter has ξ_s^{r+1}, and so it follows that $\sigma \cdot F(\mathfrak{Q}_{\tau+1})$ is an $F(\mathfrak{Q}_\tau)$ only when σ is divisible by $\mathfrak{p}$, the ideal included among the defining elements of $\mathfrak{Q}_\tau$. Obviously the lowest integer divisible by $\mathfrak{p}$ is the rational prime p contained in $N(\mathfrak{p})$. Hence f is of order p, mod $\mathfrak{Q}_\tau$. Since f was any operator of this subgroup except the identity, it follows that all operators of this subgroup, with that exception, are of order p and that the order of the subgroup is a power of p. A few subgroups at the head of the sequence may have to be considered separately, namely in case a power of $\mathfrak{p}$ higher than the first is the last defining element of the modular system in question. It is evident, however, that if a power of $\mathfrak{p}$ is not a factor of p, then the lowest rational integer of which a power of $\mathfrak{p}$ is a factor is a power of p. Hence the order of the subgroups belonging to the first systems in the sequence must also be a power of p. Hence all of our subgroups have orders that are powers of p. Since the $\mathfrak{P}$ group of totitives is of order $p^\lambda - 1$, where $\lambda = \epsilon_0 \epsilon_1 \cdots \epsilon_n$, it follows that we have the theorem:

THEOREM. *The order $\phi(\mathfrak{Q})$ of the group of totitives of a simple modular system $\mathfrak{Q}$ is of the form $p^\kappa(p^\lambda - 1)$. The subgroup of order $p^\lambda - 1$ is a cyclic group.*

Another expression for this order will be given in the next section.

The question of determining the basis and invariants of the subgroup of order p^κ will not be taken up, being considerably more difficult, as has already been stated. It has been partially solved by Georg Wolff when a Weber "funktional" is taken as modulus, while A. Ranum has solved it completely for the case in which $\mathfrak{Q}$ is an ideal in a quadratic realm.

IV. SOME GENERALIZATIONS IN NUMBER THEORY

The results obtained in the preceding sections give rise at once to a number of generalizations of some very well-known theorems in number theory. To begin with, the fact that the representative residues prime to any modular system $\mathfrak{M}$ form a group of order $\phi(\mathfrak{M})$ gives us at once the following generalization of Fermat's theorem:

THEOREM. *Whenever f is a residue of the modular system $\mathfrak{M}$ that is prime to $\mathfrak{M}$, then we have $f^{\phi(\mathfrak{M})} \equiv 1$, mod $\mathfrak{M}$.*

When we multiply a complete set of representative residues of the modular system $\mathfrak{M}$ into a residue prime to that system we must get back a complete system. For suppose that f_1 is prime to $\mathfrak{M}$, and that the two products $f_1 f_2$ and $f_1 f_3$ are congruent, mod $\mathfrak{M}$. From this we have $f_1(f_2 - f_3) \equiv 0$, mod $\mathfrak{M}$, and as $(f_1, \mathfrak{M}) = (1)$ it follows that $f_2 - f_3 \equiv 0$, mod $\mathfrak{M}$, which cannot be if f_2 and f_3 are distinct representative residues of $\mathfrak{M}$. Hence we have:

THEOREM. *When a complete residue system of the modular system $\mathfrak{M}$ is*

multiplied by a residue prime to this modular system we get back the whole system.

The corollary of this theorem concerning the reduced residue system follows at once from the group property of the residue classes prime to $\mathfrak{M}$.

From a theorem of the preceding section we have that the order $\phi(\mathfrak{P})$ of the $\mathfrak{P}$ group of totitives is of the form $p^\lambda - 1$, where p divides $N(\mathfrak{p})$, $\mathfrak{p}$ being a defining element of $\mathfrak{P}$. If $p = 2$, $\phi(\mathfrak{P})$ is odd, and as the product of all the operators of a cyclic group of odd order gives us the identity, it follows that if $p = 2$ the product of all the operators of the $\mathfrak{P}$ group of totitives is congruent to 1, mod $\mathfrak{P}$, and therefore also congruent to -1, for $-1 \equiv 1$ modulo 2, and therefore modulo $\mathfrak{p}$ or $\mathfrak{P}$. If $p > 2$, $\phi(\mathfrak{P})$ is even. From group theory we have that the product of all the operators of a cyclic group of even order gives the operator of order 2. Since -1 is the operator of order 2 for any group of totitives of $\mathfrak{P}$ where $N(\mathfrak{p})$ is not a power of 2, it follows that our product is again congruent to -1 modulo $\mathfrak{P}$. Hence we have the following generalization of Wilson's theorem:

THEOREM. *If $\mathfrak{P}$ be an absolute prime modular system, and $f_1, f_2, \cdots, f_{\phi(\mathfrak{P})}$ is a complete system of residues prime to this modular system, then*

$$f_1 f_2 \cdots f_{\phi(\mathfrak{P})} + 1 \equiv 0, \quad \text{mod } \mathfrak{P}.$$

This theorem has already been proven by H. Hancock for the system $\mathfrak{P}$ as here defined.

In proving one of the theorems in section three we saw that it is possible to obtain a complete system of representative residues of the modular system $\mathfrak{M}$ by multiplying together the complete systems of representative residues of two systems $\mathfrak{M}'$ and $\mathfrak{M}''$, provided that $\mathfrak{M} = \mathfrak{M}'\mathfrak{M}''$, and $(\mathfrak{M}', \mathfrak{M}'') = (1)$, whenever the last two sets of representative residues were properly chosen. From this we have at once the theorem:

THEOREM. *If $\mathfrak{M} = \mathfrak{M}'\mathfrak{M}''$, where $(\mathfrak{M}', \mathfrak{M}'') = (1)$, we have*

$$N(\mathfrak{M}') = N(\mathfrak{M}')N(\mathfrak{M}'').$$

By breaking up both $\mathfrak{M}'$ and $\mathfrak{M}''$ into relatively prime factors and continuing until simple modular factors of $\mathfrak{M}$ are reached we can prove the following theorem:

THEOREM. *The norm of the modular system $\mathfrak{M}$ is equal to the product of the norms of its simple modular factors.*

Now suppose that we have $\mathfrak{M} = \mathfrak{M}'\mathfrak{M}''\mathfrak{M}'''\cdots\mathfrak{M}^{(s)}$, where all of the different factors of $\mathfrak{M}$ are relatively prime to another. Then there always exists one, and only one residue class, mod $\mathfrak{M}$, all of whose polynomials will reduce to a given set $f^{(i)}$ of residues modulo $\mathfrak{M}^{(i)}$, $i = 1, 2, \cdots, s$. This gives us the theorem:

THEOREM. *If the modular system* $\mathfrak{M}$ *is equal to the product of the modular systems* $\mathfrak{M}', \mathfrak{M}'', \cdots, \mathfrak{M}^{(i)}, \cdots, \mathfrak{M}^{(s)}$, *all of them relatively prime to each other, and if* $f', f'', \cdots, f^{(i)}, \cdots, f^{(s)}$ *be any polynomials, there exist polynomials,* f, *such that* $f \equiv f^{(i)}$, *mod* $\mathfrak{M}^{(i)}$, *and all of these polynomials are congruent each to each, mod* $\mathfrak{M}$.

From this it follows that if $\mathfrak{M} = \mathfrak{M}'\mathfrak{M}''$, $(\mathfrak{M}', \mathfrak{M}'') = (1)$, that there are exactly $N(\mathfrak{M}')$ residues of a complete residue system, mod $\mathfrak{M}$, that reduce to 0, mod $\mathfrak{M}''$, while they are incongruent each to each, mod $\mathfrak{M}'$, forming a complete residue system with respect to this modular system. Hence we have at once:

THEOREM. *If* $\mathfrak{M} = \mathfrak{M}'\mathfrak{M}''$, *where* $(\mathfrak{M}', \mathfrak{M}'') = (1)$, *there are exactly* $N(\mathfrak{M}')$ *residues in a complete residue system, mod* $\mathfrak{M}$, *that are divisible by the modular factor* $\mathfrak{M}''$.

Since the $\mathfrak{M}$ group of totitives is the direct product of groups simply isomorphic to the various groups of totitives of the simple modular factors of $\mathfrak{M}$, it follows that $\phi(\mathfrak{M}) = \phi(\mathfrak{Q}_1)\phi(\mathfrak{Q}_2)\cdots\phi(\mathfrak{Q}_t)$, where

$$\mathfrak{M} = \mathfrak{Q}_1\mathfrak{Q}_2\cdots\mathfrak{Q}_j\cdots\mathfrak{Q}_t.$$

If $\mathfrak{M} = \mathfrak{M}'\mathfrak{M}''$, $(\mathfrak{M}', \mathfrak{M}'') = (1)$, it follows that $\phi(\mathfrak{M}')$ is equal to the product of a certain number of these $\phi(\mathfrak{Q}_j)$, while $\phi(\mathfrak{M}'')$ is equal to the product of the remaining ones. Hence we have proved:

THEOREM. *If* $\mathfrak{M} = \mathfrak{M}'\mathfrak{M}''$, *where* $(\mathfrak{M}', \mathfrak{M}'') = (1)$, *it follows that*

$$\phi(\mathfrak{M}) = \phi(\mathfrak{M}')\phi(\mathfrak{M}'').$$

Let us repeat the reasoning employed in connection with the theorem preceding the last one, but let us restrict ourselves to the residues prime to $\mathfrak{M}'$. We see at once that there are $\phi(\mathfrak{M}')$ of these residues that are congruent to 0, mod $\mathfrak{M}''$. Hence we get the theorem:

THEOREM. *If* $\mathfrak{M} = \mathfrak{M}'\mathfrak{M}''$, *where* $(\mathfrak{M}', \mathfrak{M}'') = (1)$, *then there are exactly* $\phi(\mathfrak{M}')$ *incongruent residues* f, *mod* $\mathfrak{M}$, *such that* $(f, \mathfrak{M}) = \mathfrak{M}''$.

This also represents the order of a maximal group belonging to the system $\mathfrak{M}$.

Let us now proceed to the solution of the congruence $f_1 X \equiv f_2$, mod $\mathfrak{M}$, where f_2 is any representative residue belonging to $\mathfrak{M}$, while with respect to f_1 we shall limit ourselves to such residues of the modular system $\mathfrak{M}$ as fulfil the conditions $(f_1, \mathfrak{M}) = \mathfrak{M}''$, where $\mathfrak{M} = \mathfrak{M}'\mathfrak{M}''$ and $(\mathfrak{M}', \mathfrak{M}'') = (1)$. Two cases can then occur with respect to any simple modular factor $\mathfrak{Q}$ of $\mathfrak{M}$. Either f_1 is congruent to zero, mod $\mathfrak{Q}$, or $(f_1, \mathfrak{Q}) = (1)$. In the latter case the congruence $f_1 X \equiv f_2$, mod $\mathfrak{Q}$, can have but one solution by the second theorem of this section. In the other case $f_1 X \equiv f_2$, mod $\mathfrak{Q}$, reduces to $0 \cdot X \equiv 0$, mod $\mathfrak{Q}$, since it is evident that the right hand side must vanish

when this is true of the left-hand side. Here X can take any one of the $N(\mathfrak{Q})$ values of the different residues in the complete residue system of $\mathfrak{Q}$. By determining the number of solutions of $f_1 X \equiv f_2$, with respect to each of the simple modular factors of $\mathfrak{M}$ taken as modulus, we find by repeated application of the fifth theorem of this section that the number of solutions, mod $\mathfrak{M}$, is equal to $N(\mathfrak{M}'')$. In case that f_1 does not fulfil the restrictions imposed the congruence may or may not have a solution. Consider for instance the modular system $(x^2+2, 4)$. Here the residues $x+1$ and $3x+1$ fulfil the restrictions while $x+2$, $3x$, and $2x+2$ do not. The congruence $(x+2)\cdot X \equiv 3x$, mod $(x^2+2, 4)$, is satisfied by $x+1$ and $3x+1$, while the congruence $(2x+2)\cdot X \equiv 3x$, mod $(x^2+2, 4)$, has no solution. Hence we have proved the theorem:

THEOREM. *A necessary and sufficient condition that the congruence $f_1 X \equiv f_2$, mod $\mathfrak{M}$, be solvable, where f_1 and f_2 are any two residues of $\mathfrak{M}$ excepting that if $(\mathfrak{M}, f_1) = \mathfrak{M}''$ and $\mathfrak{M} = \mathfrak{M}'\mathfrak{M}''$ we have $(f_1, \mathfrak{M}') = (1)$, is that f_2 contains as a modular factor $(\mathfrak{M}, f_1) = \mathfrak{M}''$. The number of solutions is equal to $N(\mathfrak{M}'')$. If f_1 does not satisfy these restrictions the congruence may or may not have solutions.*

It is evident that every residue belonging to the modular system $\mathfrak{Q}$ is either prime to $\mathfrak{Q}$ or is a $F(\mathfrak{P})$, where $\mathfrak{P}$ is the absolute prime modular system contained in $\mathfrak{Q}$. Hence all residues not prime to $\mathfrak{Q}$ reduce to 0, mod $\mathfrak{P}$, while the $\phi(\mathfrak{Q})$ others reduce to one of the other residues of $\mathfrak{P}$. Since it is easily shown that the number of residues of $\mathfrak{Q}$ reducing to any given residue of $\mathfrak{P}$ when taken modulo $\mathfrak{P}$ is always the same, it follows that of the $N(\mathfrak{Q})$ residues belonging to $\mathfrak{Q}$ there are $N(\mathfrak{Q})/N(\mathfrak{P})$ that are not prime to $\mathfrak{P}$. Hence we have proved the theorem:

THEOREM. *If a simple modular system $\mathfrak{Q}$ contains the absolute prime modular system $\mathfrak{P}$, the order of the group of totitives of $\mathfrak{Q}$ is equal to*

$$\phi(\mathfrak{Q}) = N(\mathfrak{Q})\left(1 - \frac{1}{N(\mathfrak{P})}\right).$$

We have proved in a preceding theorem that $\phi(\mathfrak{M}) = \phi(\mathfrak{M}')\phi(\mathfrak{M}'')$, if $(\mathfrak{M}', \mathfrak{M}'') = (1)$ and $\mathfrak{M} = \mathfrak{M}'\mathfrak{M}''$. Since all the simple modular factors of $\mathfrak{M}$ are relatively prime it follows at once that we have

THEOREM. *The value of the totient $\phi(\mathfrak{M})$ is given by the expression*

$$\phi(\mathfrak{M}) = N(\mathfrak{M}) \prod_{j=1}^{j=t} \left(1 - \frac{1}{N(\mathfrak{P}_j)}\right),$$

where $\mathfrak{M} = \prod_{j=1}^{j=t} \mathfrak{Q}_j$, and the simple modular system $\mathfrak{Q}_j$ contains the absolute prime system $\mathfrak{P}_j$.

MASSACHUSETTS INSTITUTE OF TECHNOLOGY,
December 31, 1914.