POLYNOMIALS AND THEIR RESIDUE SYSTEMS*

BY

AUBREY J. KEMPNER

INTRODUCTION

The present paper develops an elementary theory of polynomials (with rational integral coefficients) with respect to a modulus m, where m is a given *composite rational integer*, and of residue systems of such polynomials with respect to a modulus m. Only isolated results have been previously established.

It is known that, for p a prime, and any set of integers α_i $(i = 0, 1, \cdots, p-1)$, there exist polynomials with integral coefficients of which the set form a complete residue system* modulo p such that $f(i) \equiv \alpha_i$. The simplest considerations show that this is not true for a composite modulus, m. In this case certain relations between the α_i $(i = 0, 1, \cdots, m-1)$ must be satisfied if they are to form a complete residue system modulo m of a polynomial with integral coefficients. The problem of establishing necessary and sufficient conditions for the α_i to be, for a given modulus m, such a residue system, and the examination of such systems, was the starting point for the present article. The existence of a certain type of isomorphism between the structure of the totality of reduced polynomials modulo m on one hand and the totality of complete residue systems modulo m on the other hand suggested an independent parallel development of the theory of the polynomials and the theory of the residue systems. This has been carried out in Part I (Residual congruences and completely reduced polynomials) and Part III (Residual congruences and residue systems).

After the article was written, I became acquainted with several papers on Kronecker modular systems which establish in a satisfactory manner relations between Part I and the well developed theory of modular systems. The short Part II, which was then inserted, is devoted to a brief discussion of this connection.

The classical methods of the theory of numbers may be said to have a

* Presented to the Society, Chicago, December, 1920.

* See, for example, Zsigmondy, Monatshefte für Mathematik und Physik, vol. 8 (1897), p. 20.

tendency to consider an investigation closed when the problem has been reduced to the treatment of a number of cases where the modulus is a prime or a power of a prime, leaving the synthesis of the general case from these special cases in descriptive form. The results and methods of the paper may make it possible to break down, in some fields of investigation, these barriers between the case of a prime modulus or a prime-power modulus, and the case of a general composite modulus.

It is certain that this cannot be accomplished unless the methods are general, lead without trials to clean-cut results, and are readily applicable to a given numerical case. The last demands will justify the inclusion of numerical examples throughout the work. They also made it desirable to treat in detail some of the simpler types (m a prime; m a product of distinct primes; m a power of a prime, with the sub-cases $m = p^\gamma, \gamma < p$; $m = p^\gamma, \gamma \geqq p$). This involves only a small increase in space, since the proof of the formulæ for the general case is naturally based on the simpler cases.

The methods employed tend to emphasize, for a given modulus, the totality of completely reduced polynomials modulo m rather than the individual polynomial, and the totality of complete residue systems modulo m rather than the individual residue system.*

Part III, however, also furnishes tools for the examination of the individual residue system. Some applications of the theory are reserved for another occasion.

The introduction of some new terms and symbols could not well be avoided.

A brief synopsis may be of assistance to the reader:

In Part I, for a given modulus, m, *a certain finite set of polynomials with integral coefficients is constructed such that the residue system modulo m of any polynomial with integral coefficients coincides with the residue system of exactly one polynomial of the set* (§§ 2–5). We shall call the polynomials of this set "completely reduced polynomials" modulo m (§ 5). Necessary and sufficient conditions, in terms of the coefficients, that a polynomial be completely reduced, and the number $N(m)$ of such polynomials, are established (§§ 5, 6) by means of the "chain of residual congruences" modulo m (§§ 3, 4), the "signature" $S(m)$ (§ 4), and the "characteristic" $C(m)$ (§ 5). The signature and the characteristic are symbols which depend only on the modulus m and which are readily found for a given m. The (for our purposes) essential properties of the chain of congruences are immediately determined from $S(m)$ and $C(m)$.

* One possible extension of this work, along group theoretic lines, would have points of contact with a long paper by Zsigmondy, Monatshefte für Mathematik und Physik, vol. 7 (1896), pp. 185–289, *Abelsche Gruppen und ihre Anwendung auf die Zahlentheorie;* with Weber, *Lehrbuch der Algebra*, II, 2d edition (1899), pp. 60–68 (Gruppe der Zahlklassen), and others.

The main link between Part I and Part III is established by the italicized passage above, which indicates the existence of a one-to-one correspondence between the completely reduced polynomials modulo m and the complete residue systems modulo m. In Part III, arithmetical sequences are made use of to establish for any given modulus a certain chain of congruences between the elements of a residue system (residual congruences of the second kind) (§§ 10, 11), by means of which necessary and sufficient conditions are derived that a given set of m integers may be the complete residue system, modulo m, of some polynomial with integral coefficients (§ 12). From the "chain of the second kind" are derived a "signature of m of the second kind," $S(m)$ (§ 11) and a "characteristic of m of the second kind," $C(m)$ (§ 12). It is shown that the new signature and characteristic may be denoted by the same symbols as the signature and characteristic introduced in Part I. The new signature and characteristic are therefore again derived directly from the modulus m, and completely determine the nature of the totality of complete residue systems modulo m (§ 13) in a manner entirely parallel to the determination of the totality of completely reduced polynomials in §§ 5, 6. The number of complete residue systems for a given m is again $N(m)$ (§ 13).

There exists a complete isomorphism between Part I and Part III, which permits us to translate a statement concerning either the system of completely reduced polynomials modulo m or the system of complete residue systems modulo m into a statement concerning the other system (§ 14). A résumé (§ 14) lists the main features of this isomorphism, as far as they are used in the present paper.

In checking the literature on the subject, Dickson's History*—particularly vol. 1, ch. 8 (Higher Congruences), and ch. 11 (Greatest Common Divisor)—has been of greatest value. I wish to express a sincere feeling of obligation to Professor Dickson for the assistance which his splendid book has rendered me in this respect.

I. Residual congruences and completely reduced polynomials

§ 1. The number $\mu(m)$

Definition 1: *We denote*† *by* $\mu(m)$, *or, when no ambiguity is possible, by* μ, *the smallest positive integer such that* $[\mu(m)]!$ *is divisible by* m.

We shall need only the following properties of $\mu(m)$:

* *History of the Theory of Numbers*, published by the Carnegie Institution of Washington, vol. 1 (1919), vol. 2 (1920).

† Compare Neuberg, Mathesis, vol. 27 (1887), p. 68; Nielsen, Nieuw Archief voor Wiskunde, (2), vol. 10 (1913), pp. 100–106; Kempner, American Mathematical Monthly, vol. 25 (1918), p. 204.

$m = 1$; $\mu(1)$ is arbitrarily defined to have the value 0,
$m = p$, p a prime; then $\mu(m) = p$,
$m = p_1 \cdot p_2 \cdots p_\lambda$, $p_1 < p_2 < \cdots < p_\lambda$ primes; then $\mu(m) = p_\lambda$,
$m = p^\gamma$, $\gamma < p$; then $\mu(m) = p \cdot \gamma$,

$m = p^\gamma$, $\gamma \geqq p$; in this case p^γ is no longer the highest power of p contained in $(p \cdot \gamma)!$ as a factor. Instead, $\mu(m)$ is now determined in the following manner. For any integer $k - 1$ let p^ρ be the highest power of p dividing $(k - 1)!$. The change in the exponent ρ caused by passing from $(k - 1)!$ to $k!$ will be as follows: ρ goes over into $\rho + \tau$ when $k \equiv 0 \bmod p^\tau$, but $k \not\equiv 0 \bmod p^{\tau+1}$; that is, for k not divisible by p, the exponent ρ does not change; for k divisible by p, but not by p^2, ρ increases by unity, etc., Therefore for any prime p and any positive integer k, the highest power of p dividing $k!$ can be found by the following simple scheme:*

Write in a horizontal line, as far as required, the multiples of p: $1 \cdot p$, $2 \cdot p, 3 \cdot p, \cdots$; for every positive integer t, write t under each one of these numbers containing as a factor p^t, but not containing p^{t+1}. For any number $k \cdot p$ in our first row, the exponent of the highest power of p contained as a factor in $(k \cdot p)!$ is obtained by adding all numbers written under $1 \cdot p$, $2 \cdot p, \cdots, k \cdot p$. This is indicated by the following schedule:

$1\cdot p$	$2\cdot p$	$\cdots$	p^2-p	p^2	p^2+p	$\cdots$	$2p^2-p$	$2p^2$	$2p^2+p$	$\cdots\cdots$	p^3-p	p^3	p^3+p	$\cdots$
1	1	$\cdots$	1	2	1	$\cdots$	1	2	1	$\cdots\cdots$	1	3	1	$\cdots$
1	2	$\cdots$	$p-1$	$p+1$	$p+2$	$\cdots$	$2p$	$2p+2$	$2p+3$	$\cdots\cdots$	p^2+p-2	p^2+p+1	p^2+p+2	$\cdots$.

Example: $p = 3$

1·3	2·3	3·3	4·3	5·3	6·3	7·3	8·3	9·3	10·3	11·3	12·3	13·3	14·3	15·3	$\cdots$
1	1	2	1	1	2	1	1	3	1	1	2	1	1	2	$\cdots$
1	2	4	5	6	8	9	10	13	14	15	17	18	19	21	$\cdots$,

so that, for example, $\mu(3^{10}) = 24$, since $8 \cdot 3$ is the smallest integer such that $24! \equiv 0 \bmod 3^{10}$. Also, $\mu(3^{11}) = \mu(3^{12}) = \mu(3^{13}) = 27$, etc. (For $\gamma < p$, only numbers 1 would occur in the second row.)

$m = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdots p_\lambda^{\gamma_\lambda}$, ($m$ any positive integer); in this case $\mu(m)$ is the largest (or one of the largest, in case several of the largest are equal) of the numbers $\mu(p_1^{\gamma_1}), \mu(p_2^{\gamma_2}), \cdots, \mu(p_\lambda^{\gamma_\lambda})$, that is,

$$\mu(m) = \text{Max.}\,(\mu(p_1^{\gamma_1}), \mu(p_2^{\gamma_2}), \cdots, \mu(p_\lambda^{\gamma_\lambda})).$$

From the last case, we derive immediately: *If m_1, m_2 are relatively prime,* $\mu(m_1 \cdot m_2) = \text{Max.}\,(\mu(m_1), \mu(m_2))$.

---

* In Kempner, loc. cit., a formula for $\mu(m)$ is given.

§ 2. Residual congruences modulo m

DEFINITION 2: *We call two polynomials $\phi(x)$, $\psi(x)$, with integral coefficients, residually congruent modulo m, and write*

$$\phi(x) \equiv\!\!\equiv \psi(x) \pmod{m},$$

when $\phi(x) \equiv \psi(x) \pmod{m}$ for all integers x.

We shall refer to such congruences as residual congruences. In particular, $\phi(x) \equiv\!\!\equiv 0 \pmod{m}$ is equivalent to the statement: $\phi(x)$ is a polynomial with integral coefficients which is divisible by m for all integral values of x.*

For convenience, the following facts, most of which are well known, are stated as lemmas.

LEMMA 1: (*a*) *For any positive integer d,*

$$\prod_{i=0}^{\mu(d)-1} (x - i) \equiv\!\!\equiv 0 \pmod{d};$$

(*b*) *For any positive integer d and any multiple m of d*

$$\frac{m}{d} \cdot \prod_{i=0}^{\mu(d)-1} (x - i) \equiv\!\!\equiv 0 \pmod{m}.$$

* An *identical* congruence $\phi(x) \equiv \psi(x) \pmod{m}$, which implies that corresponding coefficients in $\phi(x)$ and $\psi(x)$ are congruent modulo m, is always at the same time a *residual* congruence modulo m; but a *residual* congruence, which only implies that for any integral value of x the residues modulo m of $\phi(x)$ and of $\psi(x)$ have the same value, is not necessarily an *identical* congruence. The types of residual congruences best known are $\prod_{k=0}^{m-1}(x-k) \equiv\!\!\equiv 0 \pmod{m!}$, and the Fermat congruence $x^p \equiv x \pmod{p}$, p a prime. A partial examination of residual congruences has been made by Borel and Drach, *Introduction à l'étude de la théorie des nombres, etc.*, Paris, 1895, pp. 339–342, who use as a starting point Fermat's theorem, and by Nielsen, loc. cit. (§ 1), whose results are closely related to those of the present § 2, and which are derived by a similar method. Nielsen's object was the determination of the general type of "perfect polynomials," that is, of polynomials $f(x)$ with *rational* coefficients, not all of which are integers, and such that $f(x)$ is an integer for all integral values of x. Nielsen's paper has no connection with work following §§ 1, 2 of the present paper. The arrangement of his work and his notation are not well suited to our purposes, so that a simple reference to the article would not be a satisfactory substitute for this § 2.

A very simple and elegant treatment of the related problem of determining the greatest common divisor d of all integers which can be represented by a *given* polynomial $f(x)$ with integral coefficients and for integral values of x, is due to Hensel, Journal für Mathematik, vol. 116 (1896), pp. 350–356. Hensel proves that d is the greatest common divisor of the $n+1$ numbers $f(0), f(1), \cdots, f(n)$, where n is the degree of the polynomial.

We also mention that, using the methods of Nielsen or of the present paper, it would be more natural to express, for example, necessary and sufficient conditions that a polynomial with integral coefficients be residually congruent to zero for a given modulus, in terms of the coefficients a_i of $f(x) = \Sigma a_i \cdot \binom{x}{i}$, that is, in terms of the coefficients of Newton's interpolation formula, rather than in terms of the coefficients c_i of the polynomial written in the form $f(x) = \Sigma c_i \cdot x^i$. For special purposes, McAtee, American Journal of Mathematics, vol. 41 (1919), pp. 225–242 (239), needed the necessary and sufficient conditions that $c_0 + c_1 x + c_2 x^2 + c_3 x^3 \equiv\!\!\equiv 0 \pmod{4}$, in terms of the c_i, and found them to be: $c_0 \equiv 0$, $2c_1 \equiv 2c_2 \equiv c_1 + c_2 + c_3 \equiv 0 \pmod{4}$. The present paper does not deal with this problem.

Proof: (*a*) follows from the definition of $\mu(d)$ (see § 1) and from the fact that $\binom{x}{\mu}$ is an integer. (*b*) is an immediate consequence of (*a*).

LEMMA 2: *Any polynomial* $f(x) = \sum_{k=0}^{k=n} c_k \cdot x^k$ *is uniquely representable in the form** $\sum_{k=0}^{k=n} a_k \cdot \binom{x}{k}$, *and* a_n, c_n *are both different from zero if one of them is different from zero.*

Proof: The actual transformation from one form to the other yields an immediate proof. (See, for example, Hensel, loc. cit. at the end of the first footnote of this section.)

LEMMA 3: *If* c_i $(i = 0, 1, \cdots, n)$ *are integers, then* $a_i/i!$ $(i = 0, 1, \cdots, n)$, *and therefore* a_i, *are integers.*

Proof: Compare coefficients of like powers of x in

$$\sum_{k=0}^{k=n} c_k \cdot x^k = \sum_{k=0}^{k=n} a_k \cdot \binom{x}{k}.$$

LEMMA 4: *If* $f(x) \equiv 0 \pmod{m}$, *then* $a_i \equiv 0 \pmod{m}$ $(i = 0, 1, \cdots, n)$.

Proof: Let successively $x = 0, 1, \cdots, n$, and consider the resulting recurrence formulæ for a_i.

By Lemma 4, if $f(x) \equiv 0 \pmod{m}$, and $f(x)$ a polynomial with integral coefficients, $f(x)$ must be of the form

$$(1) \qquad \sum_{k=0}^{k=n} m\alpha_k \cdot \binom{x}{k} = m\alpha_0 + \sum_{k=1}^{k=n} \left\{ \frac{m\alpha_k}{k!} \cdot \prod_{i=0}^{k-1} (x - i) \right\},$$

where α_k $(k = 0, 1, \cdots, n)$ are integers (positive, negative, or zero). We consider the coefficients $m\alpha_k/k!$. It follows from the definition of $\mu(m)$ that, considering u, v as unknown positive integers, the smallest value of v, for which $m \cdot u = v!$, is $v = \mu(m)$; and to this value of v corresponds

$$u = \mu(m)!/m.$$

Therefore the smallest value of k for which on the right side of (1) the coefficient $m\alpha_k/k!$ is unity, is $k = \mu(m)$.

We have thus derived:

LEMMA 5: *For a given modulus* m *the residual congruence*

$$(2) \qquad 1 \cdot \prod_{i=0}^{\mu(m)-1} (x - i) \equiv 0 \pmod{m}$$

is of lowest possible degree consistent with the condition that the coefficient of the highest power of x *shall be unity;* or, stating this result in a different form:

For any divisor d *of* m

$$(3) \qquad \frac{m}{d} \cdot \prod_{i=0}^{\mu(d)-1} (x - i) \equiv 0 \pmod{m}$$

* The fact that this is the expression for the sum of an arithmetical progression of order n is of importance in Part III and (implicitly) in Part I (compare § 10).

is a residual congruence modulo m of lowest possible degree consistent with the condition that the coefficient of the leading term shall have with m the greatest common divisor m/d.

From the preceding we abstract the following

THEOREM I: (*a*) *In any residual congruence modulo m, of degree exactly $\mu(d)$, where d is any divisor of m (including $d = m$ and the trivial case $d = 1$), the coefficient of the leading term* is either m/d or a multiple of m/d.*

(*b*) *In any residual congruence modulo m, of degree $< \mu(d)$, the coefficient of the leading term* has with m a greatest common divisor larger than m/d, and is therefore a multiple of m/d.*

For our purposes, the degree and the coefficient of the highest power of x in a residual congruence will be shown to be of particular importance. With this in mind, we introduce the following

DEFINITION 3: *We shall usually indicate a residual congruence e i t h e r by*

$$c \cdot x^n \equiv \psi(x) \pmod{m},$$

where $\psi(x)$ stands for the words† *"a n y p o l y n o m i a l i n x o f d e g r e e $< n$, w i t h i n t e g r a l c o e f f i c i e n t s, a n d w h i c h i s r e s i d u a l l y c o n g r u e n t t o $c \cdot x^n$, m o d u l o m," or, using a still more condensed notation, by $\{n, c\}$, or $\{n, c\}_m$, or $\{n, c\} \bmod m$, placing in evidence only the degree n, the coefficient c of the highest power of x, and, where advisable, the modulus m.*

In most cases, the properties just mentioned of $\psi(x)[= \psi_{n-1}(x)]$ are the only ones we shall make use of; consequently, we do not usually think of $\psi(x)$ as being any specific polynomial, but as any polynomial satisfying these conditions.

To illustrate by a simple example: $m = 30$; $1 \cdot x^5 \equiv x \pmod{30}$; but also $\prod_{i=0}^{i=4}(x - i) \equiv 0 \pmod{30}$; $5x(x-1)(x-2) \equiv 0 \pmod{30}$; $15 \cdot x(x-1) \equiv 0 \pmod{30}$. Therefore we may choose in $1 \cdot x^5 \equiv \psi(x) \pmod{30}$, $\psi(x) = x$, or $\psi(x) = x + \prod_{i=0}^{i=4}(x - i)$, or $\psi(x) = x + (ax + b) \cdot 5x(x-1)(x-2) + (dx^2 + ex + f) \cdot 15x(x-1)$, where a, b, d, e, f are any integers; etc. See also Part II.

§ 3. Construction and discussion of the chain of residual congruences modulo m

For a given modulus m we may derive a set of residual congruences by choosing all positive factors of m, including m (and unity, for reasons of convenience) and deriving the corresponding congruence (2), or (3), of § 2. We

* "Coefficient of the leading term" = "coefficient of the highest power of the variable which is not $\equiv 0 \pmod{m}$."

† Occasionally we shall indicate the fact that $\psi(x)$ is of degree not higher than $n - 1$, by writing $\psi_{n-1}(x)$.

shall show that these congruences will fall into subsets such that all congruences of any particular subset are implied by a single congruence of the subset. These dependent congruences we shall reject, and the set of congruences retained we shall call a "chain of residual congruences modulo m." We accomplish this by the following process, the discussion of which forms the object of the present and the following paragraph.

CONSTRUCTION OF CHAIN: **1.** Arrange the numbers $\mu(d)$, where d ranges over all positive factors of m (including $m = d_0$ and 1) in order of non-increasing magnitude of $\mu(d)$. Since the $\mu(d)$ are not necessarily all distinct, they will break up into subsets (some or all of which may contain a single element), such that in any subset all $\mu(d)$ are equal.

2. Arrange in each subset the $\mu(d)$ according to decreasing values of d, i.e., according to increasing values of m/d.

3. From each subset, select the first element. Let $\mu(d_i)$ be the element thus selected from the $(i+1)$th subset (where $d_0 = m$), then the numbers $\mu(d_0), \mu(d_1), \cdots, \mu(d_\tau), (d_\tau = 1, \mu(d_\tau) = 0)$, are seen to be arranged so that

$$(a) \quad \mu(d_i) > \mu(d_j), \qquad \text{for} \qquad i < j,$$

$$(b) \quad d_i > d_j, \qquad \frac{m}{d_i} < \frac{m}{d_j}, \qquad \text{for} \qquad i < j.$$

4. For each $\mu(d_i)$ $(i = 0, 1, \cdots, \tau)$ form the residual congruence

$$\frac{m}{d_i} \cdot x^{\mu(d_i)} \equiv \psi(x) \pmod{m}, \qquad \text{i.e.,} \qquad \left\{ \mu(d_i), \frac{m}{d_i} \right\}.$$

5. The set of residual congruences modulo m (of which the first is

$$1 \cdot x^{\mu(m)} \equiv \psi(x) \pmod{m},$$

and the last is the trivial congruence $m \cdot x^0 \equiv 0 \pmod{m}$)

$$\frac{m}{d_i} \cdot x^{\mu(d_i)} \equiv \psi(x) \bmod m, \qquad \text{i.e.,} \qquad \left\{ \mu(d_i), \frac{m}{d_i} \right\} \quad (i = 0, 1, \cdots, \tau),$$

is called the chain of residual congruences modulo m, or, the chain of congruences modulo m.

This process will be referred to as "Construction, § 3." From the Construction and from Theorem I we read off:

LEMMA 6: *In the chain of congruences as defined above, m/d_i is a proper factor of m/d_{i+1} $(i = 0, 1, \cdots, \tau - 1)$, (and consequently d_{i+1} a proper factor of d_i).*

For the further discussion of the chain we shall need a few facts concerning the types of relation which may exist between two residual congruences for the same modulus.

Let $\{\mu, g\}$ be a residual congruence modulo m, and $(g, m) = c$ the greatest common divisor of m, g. Then the existence of $\{\mu, g\}$ implies the existence of $\{\mu, c\}$, and conversely, as is seen by multiplying both sides of the first congruence by g', where $g \cdot g' \equiv c \pmod{m}$, and both sides of the second congruence by g/c, respectively. For this reason:

We always assume in a residual congruence that the coefficient of the highest power is a factor of the modulus: in $\{\mu, c\} \pmod{m}$, *c is always a factor of m (including* $c = 1$ *and the trivial case* $c = m$).

To the end of this paragraph, all residual congruences have the same modulus, m. In a system of two congruences $\{\mu_1, c_1\}$, $\{\mu_2, c_2\}$ we have nine possible combinations of $\mu_1 \gtreqless \mu_2$, $c_1 \gtreqless c_2$. By interchanging indices, these nine cases are reduced to the following five:

1. $c_1 = c_2$; $\mu_1 = \mu_2$. 2. $c_1 = c_2$; $\mu_1 < \mu_2$. 3. $c_1 < c_2$; $\mu_1 = \mu_2$.

4. $c_1 < c_2$; $\mu_1 < \mu_2$. 5. $c_1 < c_2$; $\mu_1 > \mu_2$, or $c_1 > c_2$; $\mu_1 < \mu_2$.

We introduce the following

DEFINITION 4: *Let* $I = \{\mu_1, c_1\}$, $II = \{\mu_2, c_2\}$; *we call I equivalent to II (or II equivalent to I), and write* $I = II$ *when both* $\mu_1 = \mu_2$, $c_1 = c_2$; *and call I stronger than II (or II weaker than I), and write* $I > II$ *(or* $II < I$*) when either* $c_1 = c_2$, $\mu_1 < \mu_2$; *or* $c_1 < c_2$, $\mu_1 = \mu_2$; *or* $c_1 < c_2$, $\mu_1 < \mu_2$. *In the cases not accounted for* ($c_1 < c_2$, $\mu_1 > \mu_2$; *and* $c_1 > c_2$, $\mu_1 < \mu_2$) *we do not consider I and II as standing to each other in any of the relations** $=, >, <$.

From Definition 4 follows immediately:

LEMMA 7: *If* $I = II$, *I and II are each one implied by the other, and therefore if either one is true, the other is also true.*

If $I > II$, $(II < I)$, *II is implied by I, and therefore if I, a stronger congruence, is true, II, a weaker congruence, is a fortiori true.*

While *any two congruences of the chain for a given m are not in any of the relations* $=, >, <$, *to each other,* we have

THEOREM II: *If we denote by II any residual congruence modulo m then either*

(α) *there is a congruence of the chain, I, such that* $I = II$; *or*

(β) *there is a congruence of the chain, I, such that* $I > II$:

In other words: Given any residual congruence modulo m, the chain contains a congruence not weaker than it.

---

*We develop the character of the relations between residual congruences only as far as they are needed for this paragraph. The use of the symbols $=, >, <$ in this connection is justified in view of the fact that (1) from $I > II$ follows $II < I$; (2) from $I = II$, $II = III$ follows $I = III$; (3) from $I > II$, $II > III$ follows $I > III$, and similarly for $<$; etc. The results of the remainder of this paragraph may perhaps also be expressed in the language of Kronecker modular systems.

Proof: Let $II = \{\gamma, c\}$ be the congruence to be examined, where c is a factor of m, say $c \cdot \delta = m$. If $\mu(d_0), \mu(d_1), \cdots, \mu(d_\tau)$ are the various values, in descending order of magnitude, which $\mu(d)$ assumes as d ranges over all divisors of m, then we know from "Construction" that our chain contains for each exponent $\mu(d_i)$ a congruence $I = \{\mu(d_i), m/d_i\}$. Therefore, for one of these factors, say for d_i, $\mu(d_i) = \mu(\delta)$. By Construction, either $d_i = \delta$, or $d_i = k \cdot \delta$, $k >$ 1 an integer. *Assume first* $\delta = d_i$: By Theorem I, § 2, I is the congruence of lowest possible degree with coefficient m/d_i. Hence, if $\gamma = \mu(d_i)$, $I = II$ by Definition 4; if $\gamma < \mu(d_i)$, II is impossible, by Theorem I; if $\gamma > \mu(d_i)$, $I > II$, by Definition 4. *Assume next* $d_i = k \cdot \delta$, $k > 1$, with $\mu(d_i) = \mu(\delta)$, as above. By Theorem I, $II' = \{\mu(\delta), c\}$ is the congruence of lowest possible degree with coefficient c. By Definition 4, $I > II'$. If $\gamma = \mu(\delta)$, $II = II'$, and hence $I > II$; if $\gamma < \mu(\delta)$, II is impossible; finally, if $\gamma > \mu(\delta)$, $II' > II$, and, since $I > II'$ (above), also $I > II$. Q.e.d.

We have thus established, by combining the Construction with the last theorem:

THEOREM II[a]: *For every modulus m the Construction of the present section establishes a completely determined chain of residual congruences*

$$\frac{m}{d_i} \cdot x^{\mu(d_i)} \equiv \psi(x) \pmod{m}, \quad \textit{i.e.,} \quad \left\{\mu(d_i), \frac{m}{d_i}\right\} \quad (i = 0, 1, \cdots, \tau),$$

and every residual congruence is either equivalent to, or weaker than, a congruence of the chain.

Compare Part II for the relation of the chain to Kronecker modular systems.

§ 4. The signature $S(m)$; continuation of the discussion of the chain

At the present stage of our investigation, we are handicapped by the length of the process described under the Construction of § 3. Our next step consists in showing how the chain may be obtained directly, for a given modulus m, by simple arithmetical operations. This is of importance if the method is to be applicable to a given numerical case.

From the chain $(m/d_i) \cdot x^{\mu(d_i)} \equiv \psi(x) \pmod{m}$, or $\{\mu(d_i), m/d_i\}$ $(i = 0, 1, \cdots, \tau)$, we derive a symbol which we call the "signature of m," $S(m)$, and which is obtained by placing together, for a given m, all the separate $\{\mu(d_i), m/d_i\}$ $(i = 0, 1, \cdots, \tau)$ in decreasing order of magnitude of d_i, but writing for convenience $\frac{\mu(d_i)}{m/d_i}$ for each i. This leads to

DEFINITION 5: *For a given modulus m, we define the signature $S(m)$ as follows:*

$$S(m) = \begin{bmatrix} \mu(m) & \mu(d_1) & \cdots & \mu(d_{\tau-1}) & \mu(d_\tau) = 0 \\ 1 & \dfrac{m}{d_1} & \cdots & \dfrac{m}{d_{\tau-1}} & \dfrac{m}{1} = m \end{bmatrix},$$

or (ignoring the trivial congruence),

$$S(m) = \begin{bmatrix} \mu(m) & \mu(d_1) & \cdots & \mu(d_{\tau-1}) \\ 1 & \frac{m}{d_1} & \cdots & \frac{m}{d_{\tau-1}} \end{bmatrix},$$

where $\{\mu(d_i), m/d_i\}$ $(i = 0, 1, \cdots, \tau)$ *is the chain of congruences modulo* m.

It follows that the chain of congruences is completely determined by the signature and conversely, so that our problem reduces to the determination of the signature for a given m. We consider successively the cases: $m = p$, a prime; $m = p_1 \cdot p_2 \cdots p_\tau$, $p_1 < p_2 < \cdots < p_\tau$, primes; $m = p^\gamma$, $\gamma < p$, p a prime; $m = p^\gamma$, $\gamma \geqq p$, p a prime; $m = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdots p_\nu^{\gamma_\nu}$, $p_1, \cdots, p_\nu$ distinct primes.

1. $m = p$: the construction of § 3 shows that the chain consists of the single congruence $\{p, 1\}$, besides the trivial $\{0, p\}$. Therefore

$$S(p) = \begin{pmatrix} p & 0 \\ 1 & p \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} p \\ 1 \end{pmatrix}.$$

Confusion with the binomial coefficient is not to be feared.

2. $m = p_1 \cdot p_2 \cdots p_\tau$, $p_1 < p_2 < \cdots < p_\tau$: from § 1, it follows that the factors $d_0, d_1, \cdots, d_\tau$ of step 4 of the Construction, and their respective μ values, are $d_i = p_1 \cdot p_2 \cdots p_{\tau-i}$, $\mu(d_i) = p_{\tau-i}$ $(i = 0, 1, \cdots, \tau)$, so that the residual congruences are $(m/d_i) \cdot x^{\mu(d_i)} \equiv \psi(x) \pmod m$, or,

$$\frac{m}{p_1 p_2 \cdots p_{\tau-i}} \cdot x^{p_{\tau-i}} \equiv \psi(x),$$

or $p_{\tau-i+1} \cdot p_{\tau-i+2} \cdots p_\tau \cdot x^{p_{\tau-i}} \equiv \psi(x)$, or $\{p_{\tau-i}, (p_{\tau-i+1} \cdots p_\tau)\}$.

$$S(p_1 p_2 \cdots p_\tau) = \begin{pmatrix} p_\tau & p_{\tau-1} & p_{\tau-2} & \cdots & p_1 & 0 \\ 1 & p_\tau & p_\tau \cdot p_{\tau-1} & \cdots & (p_\tau \cdot p_{\tau-1} \cdots p_2) & (p_\tau \cdot p_{\tau-1} \cdots p_1) \end{pmatrix}$$

$$= \begin{pmatrix} p_\tau & p_{\tau-1} & p_{\tau-2} & \cdots & p_1 \\ 1 & p_\tau & p_\tau \cdot p_{\tau-1} & \cdots & (p_\tau \cdot p_{\tau-1} \cdots p_2) \end{pmatrix}.$$

Example: $m = 2 \cdot 3 \cdot 5 \cdot 11$, $\mu(m) = 11$.

Chain of congruences: $\{11, 1\}$, $\{5, 11\}$, $\{3, 11 \cdot 5\}$, $\{2, 11 \cdot 5 \cdot 3\}$, $\{0, 11 \cdot 5 \cdot 3 \cdot 2\}$;

$$S(2 \cdot 3 \cdot 5 \cdot 11) = \begin{pmatrix} 11 & 5 & 3 & 2 \\ 1 & 11 & 11 \cdot 5 & 11 \cdot 5 \cdot 3 \end{pmatrix}.$$

Written out, the chain may be represented by either one of the systems: (all modulo $2 \cdot 3 \cdot 5 \cdot 11$)

$$\begin{aligned} 1 \cdot x^{11} &\equiv \psi(x) \\ 11 \cdot x^5 &\equiv \psi(x) \\ 11 \cdot 5 \cdot x^3 &\equiv \psi(x) \\ 11 \cdot 5 \cdot 3 \cdot x^2 &\equiv \psi(x) \end{aligned} \qquad \text{or} \qquad \begin{aligned} 1 \cdot \Pi_{i=0}^{i=10}(x - i) &\equiv 0 \\ 11 \cdot \Pi_{i=0}^{i=4}(x - i) &\equiv 0 \\ 11 \cdot 5 \cdot \Pi_{i=0}^{i=2}(x - i) &\equiv 0 \\ 11 \cdot 5 \cdot 3 \cdot \Pi_{i=0}^{i=1}(x - i) &\equiv 0. \end{aligned}$$

3. $m = p^\gamma$, $\gamma < p$. Now $d_i = p^{\gamma-i}$ $(i = 0, 1, \cdots, \gamma)$, and the chain of congruences is

$$p^i \cdot x^{p(\gamma-i)} \equiv \psi(x) \pmod{p^\gamma}, \qquad \text{or} \qquad \{p(\gamma - i), p^i\} \quad (i = 0, 1, \cdots, \gamma).$$

Hence

$$S(p^\gamma) = \begin{pmatrix} p\gamma & p(\gamma-1) & p(\gamma-2) & \cdots & p & 0 \\ 1 & p & p^2 & \cdots & p^{\gamma-1} & p^\gamma \end{pmatrix}$$

$$= \begin{pmatrix} p\gamma & p(\gamma-1) & p(\gamma-2) & \cdots & p \\ 1 & p & p^2 & \cdots & p^{\gamma-1} \end{pmatrix}.$$

Example: $m = 5^4$, $\mu(5^4) = 20$,

$$S(5^4) = \begin{pmatrix} 20 & 15 & 10 & 5 \\ 1 & 5 & 5^2 & 5^3 \end{pmatrix}.$$

Chain: $\{20, 1\}$, $\{15, 5\}$, $\{10, 5^2\}$, $\{5, 5^3\}$, i.e.,

$$\begin{aligned} &1 \cdot x^{20} \equiv \psi(x) && 1 \cdot \Pi_{i=0}^{i=19}(x - i) \equiv 0 \pmod{5^4} \\ &5 \cdot x^{15} \equiv \psi(x) && 5 \cdot \Pi_{i=0}^{i=14}(x - i) \equiv 0 \pmod{5^4} \\ &5^2 \cdot x^{10} \equiv \psi(x) \quad \text{or} && 5^2 \cdot \Pi_{i=0}^{i=9}(x - i) \equiv 0 \pmod{5^4} \\ &5^3 \cdot x^5 \equiv \psi(x) && 5^3 \cdot \Pi_{i=0}^{i=4}(x - i) \equiv 0 \pmod{5^4}. \end{aligned}$$

4. $m = p^\gamma$, $p \geqq \gamma$. Now, as in 3, the factors of m are exactly the numbers p^β, $\beta = 0, 1, \cdots, \gamma$; but to different values of β may now correspond the same value of μ (see § 1). From § 1, and from Construction, § 3, it is clear that the values of μ for all divisors of m are exactly the multiples of p up to $\mu(p^\gamma)$, which is itself a multiple of p. In our chain

$$(m/d_i) \cdot x^{\mu(d_i)} \equiv \psi(x), \qquad \text{or} \qquad \left\{\mu(d_i), \frac{m}{d_i}\right\} \quad (i = 0, 1, \cdots, \tau),$$

the degrees*

$$\mu(d_i) = \mu(p^\gamma) - i \cdot p \qquad (i = 0, 1, \cdots, \tau)$$

and the d_i are easily determined by the following schedule (compare § 1)

$$\begin{array}{cccccccc} \mu(d_{\tau-1}) & \mu(d_{\tau-2}) & \cdots & \mu(d_{\tau-i}) & \cdots & \mu(d_1) & \mu(d_0) \\ = 1 \cdot p & = 2 \cdot p & & = i \cdot p & & = \mu(p^\gamma) - p & = \mu(p^\gamma) \\ \delta_1 & \delta_2 & \cdots & \delta_i & \cdots & \delta_{\tau-1} & \delta_\tau \\ \delta_1 & \delta_1 + \delta_2 & \cdots & \sum_{j=1}^{j=i} \delta_j & \cdots & \sum_{j=1}^{j=\tau-1} \delta_j & \sum_{j=1}^{j=\tau} \delta_j. \end{array} \tag{4}$$

Here, for $i < \tau$, $\delta_i = t + 1$ when $i \equiv 0 \pmod{p^t}$ but $i \not\equiv 0 \pmod{p^{t+1}}$, that is, for $i < \tau$, δ_i is the exponent of the highest power of p dividing

* Where $d_\tau = 1$, $d_{\tau-1} = \mu(p) = p$.

$\mu(d_{\tau-i}) = i \cdot p$ (so that $\delta_1 = \delta_2 = \cdots = \delta_{p-1} = 1$, $\delta_p = 2$, $\delta_{p+1} = \delta_{p+2} = \cdots = \delta_{2p-1} = 1$, $\delta_{2p} = 2$, $\delta_{2p+1} = 1$, $\cdots$, $\delta_{p^2} = 3$, $\delta_{p^2+1} = 1$, $\cdots$. In case 3, all $\delta = 1$; hence the greater complexity of case 4. For $i = \tau$, δ_τ is chosen so that $\sum_{j=1}^{j=\tau} \delta_j = \gamma$. In (4) therefore, for $i < \tau$, $\sum_{j=1}^{j=i} \delta_j$ is the exponent of the highest power of p dividing $[\mu(d_{\tau-i})]!$ so that, by Construction, § 3,

$$p^{\sum_{j=1}^{j=i}\delta_j} = d_{\tau-i} \qquad (i = 1, 2, \cdots, \tau - 1),$$

while

$$p^{\sum_{j=1}^{j=\tau}\delta_j} = p^\gamma = m$$

does not divide $[\mu(d_1)]!$, but does divide $[\mu(d_0)]! = [\mu(m)]!$, without, however, being necessarily the highest power of p dividing $[\mu(m)]!$. (See § 1, Example, and the example below.) Our chain of congruences modulo p^γ, $\{\mu(d_i), m/d_i\}$, therefore is

$$\begin{aligned}
1 \cdot x^{\mu(p^\gamma)} &\equiv \psi(x) \bmod p^\gamma, \\
p^{\delta_\tau} \cdot x^{\mu(p^\gamma)-p} &\equiv \psi(x) \bmod p^\gamma, \\
&\cdots\cdots\cdots \\
p^{\sum_{j=1}^{j=i}\delta_{\tau-j+1}} \cdot x^{\mu(p^\gamma)-ip} &\equiv \psi(x) \bmod p^\gamma, \\
&\cdots\cdots\cdots \\
p^{\gamma-1} \cdot x^p &\equiv \psi(x) \bmod p^\gamma,
\end{aligned}$$

or*, shorter,

$$\left\{\mu(p^\gamma) - i \cdot p,\ p^{\sum_{j=1}^{j=i}\delta_{\tau-j+1}}\right\} \qquad (i = 0, 1, \cdots, \tau),$$

where δ_i is determined from the schedule (4) above, and where $\sum_{j=1}^{j=i}\delta_{\tau-j+1}$ is defined to be zero for $i = 0$. Hence

$$S(p^\gamma) = \begin{pmatrix} \mu(p^\gamma) & \mu(p^\gamma)-p & \cdots & \mu(p^\gamma)-i\cdot p & \cdots & 2p & p & 0 \\ 1 & p^{\delta_\tau} & \cdots & p^{\delta_\tau+\delta_{\tau-1}+\cdots+\delta_{\tau-i+1}} & \cdots & p^{\delta_\tau+\delta_{\tau-1}+\cdots+\delta_2} & p^{\gamma-1} & p^\gamma \end{pmatrix}.$$

Case 3 is contained in 4 as a special case.

Example: $m = 3^{11}$.

	3	6	9	12	15	18	21	24	27
	1	1	2	1	1	2	1	1	1 †
	1	2	4	5	6	8	9	10	11
$11 - \Sigma\delta_i$:	10	9	7	6	5	3	2	1	0.

Therefore $\mu(3^{11}) = 27$, and

$$S(3^{11}) = \begin{pmatrix} 27 & 24 & 21 & 18 & 15 & 12 & 9 & 6 & 3 & 0 \\ 1 & 3^1 & 3^2 & 3^3 & 3^5 & 3^6 & 3^7 & 3^9 & 3^{10} & 3^{11} \end{pmatrix},$$

leading to the chain of congruences

---

* $p^{\delta_\tau+\delta_{\tau-1}+\cdots+\delta_2} = p^{\gamma-1}$, since $\delta_1 = 1$. The trivial congruence, corresponding to $i = \tau$, is here, and frequently elsewhere, suppressed.

† Under 27 we write 1, not 3, because $\Sigma\delta_i$ must be 11. Of course 27! is the smallest factorial of which 3^{11} is a factor, but also 3^{12} and 3^{13} are factors of 27!.

$$1 \cdot x^{27} \equiv \psi(x),\ 3 \cdot x^{24} \equiv \psi(x),\ \cdots,\ 3^{10} \cdot x^{3} \equiv \psi(x),\ \text{modulo } 3^{11},$$

or,

$$\{27, 1\},\ \{24, 3\},\ \{21, 3^2\},\ \{18, 3^3\},\ \{15, 3^5\},\ \{12, 3^6\},\ \{9, 3^7\},\ \{6, 3^9\},\ \{3, 3^{10}\}.$$

The influence of $\gamma \geqq p$ is reflected in the fact that the exponent in the leading coefficients of the congruences does not range over all values $0, 1, 2, \cdots, 10$, but only over $0, 1, 2, 3, 5, 6, 7, 9, 10$.

We proceed to the general case,

5. $m = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdots p_\nu^{\gamma_\nu}$, $p_1, p_2, \cdots, p_\nu$ distinct primes. We derive first a chain for $m = m_1 \cdot m_2$, $m_1 = p_1^{\gamma_1}$, $m_2 = p_2^{\gamma_2}$, and therefore $(m_1, m_2) = 1$ In the Construction of § 3, we have to consider $\mu(d)$ for all $d = p_1^{\rho_1} \cdot p_2^{\rho_2}$, $0 \leqq \rho_1 \leqq \gamma_1$, $0 \leqq \rho_2 \leqq \gamma_2$, and then to collect in separate sets all d for which $\mu(d)$ has the same value, and to retain for each μ only the largest d (in case there is one largest; otherwise, one of the largest). From the d so selected we should construct the chain in the following manner: For a $d = p_1^{\rho_1} \cdot p_2^{\rho_2}$ assume $\mu(p_1^{\rho_1}) > \mu(p_2^{\rho_2})$; then $\mu(p_1^{\rho_1} \cdot p_2^{\rho_2}) = \mu(p_1^{\rho_1})$, from § 1, end. Next consider $p_1^{\rho_1} \cdot p_2^{\rho_2+1}$; if $\mu(p_1^{\rho_1}) > \mu(p_2^{\rho_2+1})$, we have $\mu(p_1^{\rho_1} \cdot p_2^{\rho_2+1}) = \mu(p_1^{\rho_1})$, and the factor $p_1^{\rho_1} \cdot p_2^{\rho_2}$ of m is then disregarded. Letting ρ_2 increase in this way from $\rho_2, \rho_2 + 1, \cdots$ to γ_2, we shall either still have $\mu(p_1^{\rho_1}) > \mu(p_2^{\gamma_2})$, in which case all factors $p_1^{\rho_1} \cdot p_2^{\gamma_2-1}, p_1^{\rho_1} \cdot p_2^{\gamma_2-2}, \cdots, p_1^{\rho_1}$ are disregarded; or, $\mu(p_1^{\rho_1}) \leqq \mu(p_2^{\gamma_2})$, in which case there must be a largest exponent of p_2, (we designate it by $\rho_2 + \lambda - 1$), for which still $\mu(p_1^{\rho_1}) > \mu(p_2^{\rho_2+\lambda-1})$, but $\mu(p_1^{\rho_1}) \leqq \mu(p_2^{\rho_2+\lambda})$; then $\mu(p_1^{\rho_1} \cdot p_2^{\rho_2+\lambda}) = \mu(p_2^{\rho_2+\lambda})$. We consider in the same way the factors $p_2^{\rho_2+\lambda} \cdot p_1^{\rho_1}$, $p_2^{\rho_2+\lambda} \cdot p_1^{\rho_1+1}$, $p_2^{\rho_2+\lambda} \cdot p_1^{\rho_1+2}$, etc.: assume that $\mu(p_2^{\rho_2+\lambda}) > \mu(p_1^{\rho_1+\sigma-1})$, but $\mu(p_2^{\rho_2+\lambda}) \leqq \mu(p_1^{\rho_1+\sigma})$; then we disregard factors $p_2^{\rho_2+\lambda} \cdot p_1^{\rho_1}, \cdots, p_2^{\rho_2+\lambda} \cdot p^{\rho_1+\sigma-1}$, and retain as next factor $p_2^{\rho_2+\lambda} \cdot p_1^{\rho_1+\sigma}$; and so forth.

In this manner we systematically discover which factors d of m must be retained, and it is clear that they can be arranged in increasing order according to the schedule $\cdots p_1^{\rho_1} \cdot p_2^{\rho_2}, p_1^{\rho_1'} \cdot p_2^{\rho_2'}, \cdots$, where $\rho_1' \geqq \rho_1$, $\rho_2' \geqq \rho_2$, and the sign of equality holds in at most one of the two relations. It is also clear that the factors to be retained are uniquely determined by this process.

Example: $m = 5^4 \cdot 7^3$. $\mu(5^4 \cdot 7^3) = 3 \cdot 7$. In the following rectangular array for all divisors of m the factors which have to be retained for our chain are in heavy type:

	$\mu(7^1) = 7$,	$\mu(7^2) = 14$,	$\mu(7^3) = 21$,
$\mu(5^1) = 5$,	$\mu(5^1 \cdot 7^1) = 7$,	$\mu(5^1 \cdot 7^2) = 14$,	$\mu(5^1 \cdot 7^3) = 21$,
$\mu(5^2) = 10$,	$\mu(5^2 \cdot 7^1) = 10$,	$\mu(5^2 \cdot 7^2) = 14$,	$\mu(5^2 \cdot 7^3) = 21$,
$\mu(5^3) = 15$,	$\mu(5^3 \cdot 7^1) = 15$,	$\mu(5^3 \cdot 7^2) = 15$,	$\mu(5^3 \cdot 7^3) = 21$,
$\mu(5^4) = 20$,	$\mu(5^4 \cdot 7^1) = 20$,	$\mu(5^4 \cdot 7^2) = 20$,	$\mu(5^4 \cdot 7^3) = 21$.

We shall have the chain

$$\begin{aligned}
1 \cdot x^{3 \cdot 7} &\equiv \psi(x) \bmod 5^4 \cdot 7^3,\\
7 \cdot x^{4 \cdot 5} &\equiv \psi(x) \bmod 5^4 \cdot 7^3,\\
5 \cdot 7 \cdot x^{3 \cdot 5} &\equiv \psi(x) \bmod 5^4 \cdot 7^3,\\
5^2 \cdot 7 \cdot x^{2 \cdot 7} &\equiv \psi(x) \bmod 5^4 \cdot 7^3,\\
5^2 \cdot 7^2 \cdot x^{2 \cdot 5} &\equiv \psi(x) \bmod 5^4 \cdot 7^3,\\
5^3 \cdot 7^2 \cdot x^{1 \cdot 7} &\equiv \psi(x) \bmod 5^4 \cdot 7^3,\\
5^3 \cdot 7^3 \cdot x^{1 \cdot 5} &\equiv \psi(x) \bmod 5^4 \cdot 7^3,
\end{aligned}$$

or in condensed form: $\{21, 1\}$, $\{20, 7\}$, $\{15, 5 \cdot 7\}$, $\{14, 5^2 \cdot 7\}$, $\{10, 5^2 \cdot 7^2\}$, $\{7, 5^3 \cdot 7^2\}$, $\{5, 5^3 \cdot 7^3\}$. The corresponding signature is

$$S(5^4 \cdot 7^3) = \begin{pmatrix} 21 & 20 & 15 & 14 & 10 & 7 & 5 & 0 \\ 1 & 7 & 5 \cdot 7 & 5^2 \cdot 7 & 5^2 \cdot 7^2 & 5^3 \cdot 7^2 & 5^3 \cdot 7^3 & 5^4 \cdot 7^3 \end{pmatrix}.$$

For a modulus m with a large number of factors this method would be very tedious. We show (first without proof) how we may obtain for the example above $S(5^4 \cdot 7^3)$ by inspection from $S(5^4)$ and $S(7^3)$ and shall then prove that this method applies also to the (general) case $m = m_1 \cdot m_2$, $(m_1, m_2) = 1$.

In

$$S(5^4) = \begin{pmatrix} 20 & 15 & 10 & 5 & 0 \\ 5^0 & 5^1 & 5^2 & 5^3 & 5^4 \end{pmatrix}, \qquad S(7^3) = \begin{pmatrix} 21 & 14 & 7 & 0 \\ 7^0 & 7^1 & 7^2 & 7^3 \end{pmatrix},$$

combine the two sets as follows, arranging the exponents in decreasing order of magnitude:

$$\begin{array}{cccccccc} 21 & 20 & 15 & 14 & 10 & 7 & 5 & 0 \\ 1 = 7^0 & 1 = 5^0 & 5^1 & 7^1 & 5^2 & 7^2 & 5^3 & 5^4, 7^3. \end{array}$$

In the second row every 7^k (except 7^0 and 7^3) is spaced between two powers of 5, say 5^γ, 5^δ, $\gamma < \delta$; thus 7^1 between 5^1 and 5^2, 7^2 between 5^2 and 5^3. We multiply 7^k by 5^δ, and replace 7^k by $7^k \cdot 5^\delta$. Similarly, every 5^l (except 5^4) is spaced between two powers of $7, 7^\epsilon, 7^\xi$, $\epsilon < \xi$. This 5^l is multiplied by 7^ξ, so that 5^l is replaced by $5^l \cdot 7^\xi$. We obtain

$$\begin{array}{cccccccc} 3 \cdot 7 & 4 \cdot 5 & 3 \cdot 5 & 2 \cdot 7 & 2 \cdot 5 & 1 \cdot 7 & 1 \cdot 5 & 0 \\ 1 = 7^0 & 1 = 5^0 & 5^1 & 7^1 & 5^2 & 7^2 & 5^3 & 7^3, 5^4 \\ 1 = 7^0 & 5^0 \cdot 7^1 & 5^1 \cdot 7^1 & 5^2 \cdot 7^1 & 5^2 \cdot 7^2 & 5^3 \cdot 7^2 & 5^3 \cdot 7^3 & 5^4 \cdot 7^3, \end{array}$$

and the first and third lines represent $S(5^4 \cdot 7^3)$.

There is one more point to consider. It may (and frequently will) happen that one of the congruences in the chain for m_1 and one of the congruences in the chain for m_2 will have the same degree.

For example, in $m = 2^7 \cdot 3^4$, $\mu(2^4) = \mu(3^2) = 6$. We have, for this case:

$$S(2^7) = \begin{pmatrix} 8 & 6 & 4 & 2 & 0 \\ 2^0 & 2^3 & 2^4 & 2^6 & 2^7 \end{pmatrix}, \qquad S(3^4) = \begin{pmatrix} 9 & 6 & 3 & 0 \\ 3^0 & 3^2 & 3^3 & 3^4 \end{pmatrix},$$

and, combining (and writing the coefficients in two separate lines),

$$\begin{array}{ccccccc} 9 & 8 & 6 & 4 & 3 & 2 & 0 \\ 3^0 & & 3^2 & & 3^3 & & 3^4 \\ & 2^0 & 2^3 & 2^4 & & 2^6 & 2^7 \\ \hline 3^0 \cdot 2^0 & 2^0 \cdot 3^2 & 3^2 \cdot 2^3 & 2^4 \cdot 3^3 & 3^3 \cdot 2^6 & 2^6 \cdot 3^4 & 3^4 \cdot 2^7; \end{array}$$

hence

$$S(2^7 \cdot 3^4) = \begin{pmatrix} 9 & 8 & 6 & 4 & 3 & 2 & 0 \\ 1 & 3^2 & 2^3 \cdot 3^2 & 2^4 \cdot 3^3 & 2^6 \cdot 3^3 & 2^6 \cdot 3^4 & 2^7 \cdot 3^4 \end{pmatrix},$$

leading to the chain $\{9, 1\}$, $\{8, 3^2\}$, $\{6, 2^3 \cdot 3^2\}$, $\cdots$, $\{2, 2^6 \cdot 3^4\}$.

We show that the method used in these two examples applies without change to the general case $m = n \cdot n'$, n, n' any factors of m, which we assume to b

relatively prime, as we may do without causing loss of generality, since the case $m = p^\nu$ has already been treated.

For this, we prove

LEMMA 8: *Let*

$$S(n) = \begin{bmatrix} \mu(n) & \mu(d_1) & \cdots & \mu(d_\lambda) \\ 1 = \dfrac{n}{n} & \dfrac{n}{d_1} & \cdots & \dfrac{n}{d_\lambda} \end{bmatrix},$$

$$S(n') = \begin{bmatrix} \mu(n') & \mu(d_1') & \cdots & \mu(d_\tau') \\ 1 = \dfrac{n'}{n'} & \dfrac{n'}{d_1'} & \cdots & \dfrac{n'}{d_\tau'} \end{bmatrix},$$

so that the d_i $(d_i > d_{i+1})$ are certain factors of n, and the d_j' $(d_j' > d_{j+1}')$, certain factors of n'; assume also that, after all exponents in both signatures have been arranged in decreasing order of magnitude, a part of the combination is as follows:

$$\begin{matrix} \cdots\ \mu(d_\alpha)\ \mu(d_{\alpha+1}) & \cdots\ \mu(d_{\alpha'})\ \mu(d_\beta')\ \mu(d_{\beta+1}') & \cdots\ \mu(d_{\beta'}')\ \mu(d_\gamma)\ \mu(d_{\gamma+1}) & \cdots \\ \cdots\ \dfrac{n}{d_\alpha}\quad \dfrac{n}{d_{\alpha+1}} & \cdots\ \dfrac{n}{d_{\alpha'}}\quad \dfrac{n'}{d_\beta'}\quad \dfrac{n'}{d_{\beta+1}'} & \cdots\ \dfrac{n'}{d_{\beta'}'}\quad \dfrac{n}{d_\gamma}\quad \dfrac{n}{d_{\gamma+1}} & \cdots, \end{matrix}$$

then the corresponding part of $S(n \cdot n')$ is:

$$\begin{bmatrix} \cdots\ \mu(d_\alpha \cdot d_\beta') & \mu(d_{\alpha+1} \cdot d_\beta') & \cdots\ \mu(d_{\alpha'} \cdot d_\beta') & \mu(d_\beta' \cdot d_\gamma) & \mu(d_{\beta+1}' \cdot d_\gamma) & \cdots \\ \cdots\ \dfrac{n}{d_\alpha} \cdot \dfrac{n'}{d_\beta'} & \dfrac{n}{d_{\alpha+1}} \cdot \dfrac{n'}{d_\beta'} & \cdots\ \dfrac{n}{d_{\alpha'}} \cdot \dfrac{n'}{d_\beta'} & \dfrac{n'}{d_\beta'} \cdot \dfrac{n}{d_\gamma} & \dfrac{n'}{d_{\beta+1}'} \cdot \dfrac{n}{d_\gamma} & \cdots \end{bmatrix}$$

$$\begin{bmatrix} \mu(d_{\beta'}' \cdot d_\gamma) & \mu(d_\gamma \cdot d_\delta') & \mu(d_{\gamma+1} \cdot d_\delta') & \cdots \\ \dfrac{n'}{d_{\beta'}'} \cdot \dfrac{n}{d_\gamma} & \dfrac{n}{d_\gamma} \cdot \dfrac{n'}{d_\delta'} & \dfrac{n}{d_{\gamma+1}} \cdot \dfrac{n'}{d_\delta'} & \cdots \end{bmatrix}.$$

Proof: For any $\mu(d_i)$ the signature $S(n)$ yields a residual congruence $\{\mu(d_i), n/d_i\}_n$, and for any $\mu(d_j')$ we get from $S(n')$ a congruence $\{\mu(d_j'), n'/d_j'\}_{n'}$. After combining the signatures in decreasing order of the μ, as assumed in the lemma, we select any one of the $\mu(d)$, for example $\mu(d_i)$. This $\mu(d_i)$ will be followed* by some $\mu(d')$, say $\mu(d_j')$, and therefore $\mu(d_i) \geqslant \mu(d_j')$, and, since d_i and d_j' are relatively prime, $\mu(d_i) = \mu(d_i d_j')$ (see § 1, end), where $d_i d_j'$ is some divisor of $n \cdot n'$. Therefore (§ 2), there exists a congruence $\{\mu(d_i d_j'), nn'/d_i d_j'\}_{nn'}$. The possibility of a $\mu(d)$ equaling a $\mu(d')$ offers no difficulty. (See Example $S(2^7 \cdot 3^4)$ above.) It is seen that all residual congruences modulo nn' which the construction of § 3 calls for, actually are obtained in this way. The lemma is thus proved.

* Unless $\mu(d_i)$ is smaller than any $\mu(d')$, which will always happen for the smallest $\mu(d)$, except when the smallest $\mu(d')$ is smaller than any $\mu(d)$. This does not give rise to any difficulty. See Example $S(5^4 \cdot 7^3)$, above.

Since, by assumption, $\mu(d_\alpha) > \mu(d'_\beta)$, $\mu(d_{\alpha+1}) > \mu(d'_\beta)$, $\cdots$, $\mu(d_{\alpha'}) > \mu(d'_\beta)$, we shall have $\mu(d_\alpha \cdot d'_\beta) = \mu(d_\alpha)$, $\mu(d_{\alpha+1} \cdot d'_\beta) = \mu(d_{\alpha+1})$, $\cdots$, $\mu(d_{\alpha'} \cdot d'_\beta) = \mu(d_{\alpha'})$; similarly, $\mu(d'_\beta \cdot d_\gamma) = \mu(d'_\beta)$, $\mu(d'_{\beta+1} \cdot d_\gamma) = \mu(d'_{\beta+1})$, $\cdots$, $\mu(d'_{\beta'} \cdot d_\gamma) = \mu(d'_{\beta'})$; and $\mu(d_\gamma \cdot d'_\delta) = \mu(d_\gamma)$, $\mu(d_{\gamma+1} \cdot d'_\delta) = \mu(d_{\gamma+1})$, $\cdots$. Then part of our signature $S(n \cdot n')$ is given by

$$\begin{array}{c} \cdots \mu(d_\alpha)\ \mu(d_{\alpha+1}) \cdots \mu(d_{\alpha'})\ \mu(d'_\beta)\ \mu(d'_{\beta+1}) \cdots \mu(d'_{\beta'})\ \mu(d_\gamma)\ \mu(d_{\gamma+1}) \cdots \\ \cdots \quad \dfrac{nn'}{d_\alpha d'_\beta} \quad \dfrac{nn'}{d_{\alpha+1} d'_\beta} \quad \cdots \quad \dfrac{nn'}{d_{\alpha'} d'_\beta} \quad \dfrac{nn'}{d'_\beta d_\gamma} \quad \dfrac{nn'}{d'_{\beta+1} d_\gamma} \quad \cdots \quad \dfrac{nn'}{d'_{\beta'} d_\gamma} \quad \dfrac{nn'}{d_\gamma d'_\delta} \quad \dfrac{nn'}{d_{\gamma+1} d'_\delta} \quad \cdots . \end{array}$$

But this represents exactly the law indicated in the special examples $m = 5^4 \cdot 7^3$, $m = 2^7 \cdot 3^4$ above. To make this perfectly clear, we rewrite a few lines from these problems, with only obvious modifications:

$$n = 5^4, \qquad n' = 7^3. \qquad S(5^4) = \begin{pmatrix} \mu(5^4) & \mu(5^3) & \mu(5^2) & \mu(5^1) & \mu(1) \\ =20 & =15 & =10 & =5 & =0 \\ 5^0 & 5^1 & 5^2 & 5^3 & 5^4 \end{pmatrix};$$

$$S(7^3) = \begin{pmatrix} \mu(7^3) & \mu(7^2) & \mu(7^1) & \mu(1) \\ =21 & =14 & =7 & =0 \\ 7^0 & 7^1 & 7^2 & 7^3 \end{pmatrix}.$$

From these, by Lemma 8 and taking the last remarks into account,

$$S(5^4 \cdot 7^3) = \begin{pmatrix} \mu(7^3 \cdot 5^4) & \mu(5^4 \cdot 7^2) & \mu(5^3 \cdot 7^3) & \mu(7^2 \cdot 5^2) & \mu(5^2 \cdot 7^1) & \mu(7^1 \cdot 5^1) & \mu(5^1 \cdot 7^0) \\ =\mu(7^3) & =\mu(5^4) & =\mu(5^3) & =\mu(7^2) & =\mu(5^2) & =\mu(7^1) & =\mu(5^1) \\ 7^0 \cdot 5^0 & 5^0 \cdot 7^1 & 5^1 \cdot 7^1 & 7^1 \cdot 5^2 & 5^2 \cdot 7^2 & 7^2 \cdot 5^3 & 5^3 \cdot 7^3 \end{pmatrix},$$

in agreement with the example.

To show that, here again, the method requires no real modification when a $\mu(d_i)$ equals a $\mu(d_j)$, we indicate in the same manner the work for the other example, $m = 2^7 \cdot 3^4$.

$$n = 2^7, \qquad n' = 3^4. \qquad S(2^7) = \begin{pmatrix} \mu(2^7) & \mu(2^6) & \mu(2^5) & \mu(2^4) & \mu(2^3) & \mu(2^2) & \mu(2^1) & \mu(2^0) \\ =8 & =6 & =4 & =2 & =0 \\ 2^0 & 2^1 & 2^2 & 2^3 & 2^4 & 2^5 & 2^6 & 2^7 \end{pmatrix},$$

$$\mu(3^4) = \begin{pmatrix} \mu(3^4) & \mu(3^3) & \mu(3^2) & \mu(3^1) & \mu(3^0) \\ =9 & =6 & =3 & =0 \\ 3^0 & 3^1 & 3^2 & 3^3 & 3^4 \end{pmatrix}.$$

Then

$$S(2^7 \cdot 3^4) = \begin{pmatrix} \mu(3^4 \cdot 2^7) & \mu(2^7 \cdot 3^2) & \mu(2^4 \cdot 3^2) & \mu(3^2 \cdot 2^3) & \mu(2^3 \cdot 3^1) & \mu(3^1 \cdot 2^2) & \mu(2^2 \cdot 3^0) \\ =\mu(3^4) & =\mu(2^7) & =\mu(2^4)=\mu(3^2) & =\mu(3^2) & =\mu(2^3) & =\mu(3^1) & =\mu(2^1) \\ 3^0 \cdot 2^0 & 2^0 \cdot 3^2 & 3^2 \cdot 2^3 & 3^2 \cdot 2^4 & 2^4 \cdot 3^3 & 3^3 \cdot 2^5 & 2^5 \cdot 3^4 \end{pmatrix},$$

i.e.,

$$\begin{pmatrix} 9 & 8 & 6 & 6 & 4 & 3 & 2 \\ 1 & 3^2 & 2^3 \cdot 3^2 & 3^2 \cdot 2^4 & 2^4 \cdot 3^3 & 3^3 \cdot 2^5 & 2^5 \cdot 3^4 \end{pmatrix},$$

in agreement with the example, since $\{6, 3^2 \cdot 2^4\}_{27 \cdot 34} < \{6, 3^2 \cdot 2^3\}_{27 \cdot 34}$, and may therefore be omitted.

The general case, $m = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdots p_\nu^{\gamma_\nu}$, can always be treated by successive applications of the lemma last proved. However, it would be a very simple matter to display a schematic arrangement by means of which $S(p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdots p_\nu^{\gamma_\nu})$ is obtained in one step from $S(p_i^{\gamma_i})$ $(i = 1, 2, \cdots, \nu)$, if this were worth while. One example, below, is worked out in this way, and this will suffice to make clear the general process.

Example: $m = 2^7 \cdot 3^4 \cdot 7^2$. $\mu(7^2) = 14$, $\mu(3^4) = 9$, $\mu(2^7) = 8$; $\mu(2^7 \cdot 3^4 \cdot 5^3) = 14$.

$$S(2^7) = \begin{pmatrix} 8 & 6 & 4 & 2 & 0 \\ 2^0 & 2^1 & 2^2 & 2^6 & 2^7 \end{pmatrix}; \qquad S(3^4) = \begin{pmatrix} 9 & 6 & 3 & 0 \\ 3^0 & 3^2 & 3^3 & 3^4 \end{pmatrix} \quad \text{(see above)},$$

$$S(7^2) = \begin{pmatrix} 14 & 7 & 0 \\ 7^0 & 7^1 & 7^2 \end{pmatrix}.$$

14	9	8	7	6	4	3	2	0
7^0			7^1					7^2
	3^0			3^2		3^3		3^4
		2^0		2^3	2^4		2^6	2^7
7^0;	$3^0 \cdot 7^1$;	$7^1 \cdot 3^2$;	$7^1 3^2 2^3$;	$2^3 3^2 7^2$;	$2^4 3^3 7^2$;	$3^3 2^6 7^2$;	$2^6 3^4 7^2$;	$2^7 3^4 7^2$;

$S(2^7 \cdot 3^4 \cdot 7^2)$

$$= \begin{pmatrix} 11 & 9 & 8 & 7 & 6 & 4 & 3 & 2 & 0 \\ 1 & 7 & 3^2 \cdot 7 & 2^3 \cdot 3^2 \cdot 7 & 2^5 \cdot 3^2 \cdot 7^2 & 2^4 \cdot 3^3 \cdot 7^2 & 2^6 \cdot 3^3 \cdot 7^2 & 2^6 \cdot 3^4 \cdot 7^2 & 2^7 \cdot 3^4 \cdot 7^2 \end{pmatrix}$$

Chain: $\{14, 1\}$, $\{9, 7\}$, $\{8, 3^2 \cdot 7\}$, $\{7, 2^3 \cdot 3^2 \cdot 7\}$, $\cdots$, $\{2, 2^6 \cdot 3^4 \cdot 7^2\}$.

We combine the results of §§ 3, 4 in the following theorem.

THEOREM III: *To any positive integer m (the modulus)—which we assume given in factored form—we can determine by a definite and very simple arithmetical process the signature*

$$S(m) = \begin{bmatrix} \mu(m) & \mu(d_1) & \cdots & \mu(d_i) & \mu(d_{i+1}) & \cdots & \mu(d_{\tau-1}) & \mu(d_\tau) = 0 \\ \dfrac{m}{d_0} = 1 & \dfrac{m}{d_1} & \cdots & \dfrac{m}{d_i} & \dfrac{m}{d_{i+1}} & \cdots & \dfrac{m}{d_{\tau-1}} & \dfrac{m}{d_\tau} = m \end{bmatrix}$$

where each d_i is a proper factor of all d_j, $j > i$, and consequently a divisor of m, and $d_0 = m$, $d_\tau = 1$.

$S(m)$ completely determines the chain of residual congruences modulo m,

$$\frac{m}{d_i} \prod_{i=0}^{\mu(d_i)-1} (x - i) \equiv 0 \pmod{m} \qquad (i = 0, 1, \cdots, \tau - 1) \text{ or } (i = 0, 1, \cdots, \tau)$$

or,

$$\frac{m}{d_i} \cdot x^{\mu(d_i)} \equiv \psi(x) \pmod{m} \qquad (i = 0, 1, \cdots, \tau),$$

*or, as we also write,**

$$\left\{ \mu(d_i), \frac{m}{d_i} \right\} \qquad (i = 0, 1, \cdots, \tau).$$

Every residual congruence modulo m is either equivalent to, or weaker than, a congruence of the chain.

If $m = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdots p_\nu^{\gamma_\nu}$, then the number of congruences in the chain modulo m is $\leqq \gamma_1 + \gamma_2 + \cdots + \gamma_\gamma$ (besides the trivial congruence).

* When the modulus m is to be explicitly stated,

$$\left\{ \mu(d_i), \frac{m}{d_i} \right\}_m \quad \text{or} \quad \left\{ \mu(d_i), \frac{m}{d_i} \right\} \pmod{m}.$$

§ 5. Completely reduced polynomials modulo m; the characteristic $C(m)$

We make use of the chain of congruences of §§ 3, 4 to reduce any polynomial with integral coefficients to a normal form which is to be, modulo m, residually congruent to the given polynomial. First we may, by repeated application of the first congruence $\{\mu(m), 1\}$, reduce a polynomial of any degree to one of degree at most $\mu(m) - 1$; then repeated application of the second congruence, $\{\mu(d_1), m/d_1\}$, permits us to reduce in the new polynomial the coefficients of $x^{\mu(m)-1}, x^{\mu(m)-2}, \cdots, x^{\mu(d_1)}$ to numbers of the set $0, 1, \cdots, (m/d_1) - 1$. In the same way, $\{\mu(d_2), m/d_2\}$ reduces, without affecting coefficients already reduced, the coefficients of $x^{\mu(d_1)-1}, \cdots, x^{\mu(d_2)}$ to numbers of the set $0, 1, \cdots, (m/d_2) - 1$. Continuing in this manner, we find that finally the coefficients of $x^{\mu(d_{\tau-2})-1}, x^{\mu(d_{\tau-2})-2}, \cdots, x^{\mu(d_{\tau-1})}$ are restricted to the numbers $0, 1, \cdots, (m/d_{\tau-1}) - 1$, while the coefficients of $x^{\mu(d_{\tau-1})-1}, x^{\mu(d_{\tau-1})-2}, \cdots, x^1, x^0$ are not restricted at all beyond the obvious limitation that they shall belong to the set $0, 1, \cdots, m - 1$.

We are thus led to an arrangement of the following type: any polynomial is reducible by the chain of residual congruences modulo m to a normal form in which the degree is $\mu(m) - 1$* and in which

the terms with exponents:	$\mu(1) = 0, \cdots, \mu(d_{\tau-1}) - 1$	$\mu(d_{\tau-1}) \cdots \mu(d_{\tau-2}) - 1$	
have their coefficients restricted to the numbers	$0 \cdots m - 1$	$0 \cdots (m/d_{\tau-1}) - 1$	
	$\cdots\cdots$	$\mu(d_2) \cdots \mu(d_1) - 1$	$\mu(d_1) \cdots \mu(m) - 1$
	$\cdots\cdots$	$0 \cdots (m/d_2) - 1$	$0 \cdots (m/d_1) - 1$.

We have then: counting the degree of the reduced polynomial as exactly $\mu(m) - 1$, and assuming it written in the form $a_0 + a_1 x + a_2 x^2 + \cdots + a_{\mu(m)-1} \cdot x^{\mu(m)-1}$,

the $\mu(d_{\tau-1})$ lowest coefficients† $a_0, \cdots, a_{\mu(d_{\tau-1})-1}$ are each one of the m numbers $0, 1, \cdots, m - 1$;

. . . . . .

the $\mu(d_{i-1}) - \mu(d_i)$ coefficients $a_{\mu(d_i)}, \cdots, a_{\mu(d_{i-1})-1}$ are each one of the m/d_i numbers $0, 1, \cdots, (m/d_i) - 1$;

. . . . . .

the $\mu(d_1) - \mu(d_2)$ coefficients $a_{\mu(d_2)}, \cdots, a_{\mu(d_1)-1}$ are each one of the m/d_2 numbers $0, 1, \cdots, (m/d_2) - 1$; and, finally,

the $\mu(m) - \mu(d_1)$ highest coefficients $a_{\mu(d_1)}, \cdots, a_{\mu(m)-1}$ are each one of the m/d_1 numbers $0, 1, \cdots, (m/d_1) - 1$.

---

* Admitting that one, or more, of the highest powers of x may have a coefficient 0; or all coefficients may be zero, including the constant term.

† For conformity with what follows, we should write: "the $\mu(d_{\tau-1}) - \mu(d_\tau)$ lowest coefficients," but $d_\tau = 1$, $\mu(d_\tau) = 0$ (§ 1, beginning).

This is indicated by the following symbol which we call the characteristic of m, and denote by $C(m)$.

DEFINITION 6: *We define the characteristic of m, $C(m)$, by writing in a first line the number of coefficients in each subset and in a second line the number of values over which the coefficients in each subset may range, and arranging so that going from left to right corresponds to increasing degrees of the terms:*

$$C(m) = \left(\begin{array}{c|c|c|c|c} \mu(d_{\tau-1}) & \mu(d_{\tau-2}) - \mu(d_{\tau-1}) & \cdots & \mu(d_{i-1}) - \mu(d_i) & \cdots \\ m & \frac{m}{d_{\tau-1}} & \cdots & \frac{m}{d_i} & \cdots \end{array} \right. \left. \begin{array}{c|c} \mu(d_1) - \mu(d_2) & \mu(m) - \mu(d_1) \\ \frac{m}{d_2} & \frac{m}{d_1} \end{array} \right).$$

We call a polynomial of degree $\leqq \mu(m) - 1$, and of which the coefficients are restricted as indicated, a completely reduced polynomial modulo m, or simply a completely reduced polynomial.

Two completely reduced polynomials modulo m cannot be residually congruent modulo m without being identical; that is, if $f_1(x) \equiv f_2(x) \bmod m$, and $f_1(x)$, $f_2(x)$ are both completely reduced modulo m, then $f_1(x)$ and $f_2(x)$ have corresponding coefficients equal to each other. For, if this were not so, we should have $\phi(x) = f_1(x) - f_2(x) \equiv 0 \bmod m$; and in the polynomial $\phi(x)$ at least one coefficient would be different from zero. Assume that in $\phi(x)$ the highest term whose coefficient does not vanish is $c \cdot x^\gamma$, $\mu(d_i) \leqq \gamma < \mu(d_{i-1})$. Since both in $f_1(x)$ and in $f_2(x)$ the coefficient of x^γ lies between 0 (incl.) and m/d_i (excl.), we shall have $0 \leqq c < m/d_i$, thus contradicting Theorem 1, § 2. In particular, a completely reduced polynomial is residually congruent to zero when and only when all coefficients and the constant term are zero.

We have thus proved

THEOREM IV: *Every polynomial with integral coefficients is modulo m residually congruent to one and only one completely reduced polynomial. In greater detail:*

If the signature of m is

$$S(m) = \begin{pmatrix} \mu(m) & \mu(d_1) & \mu(d_2) & \cdots & \mu(d_{\tau-1}) & \mu(d_\tau) = 0 \\ 1 & m/d_1 & m/d_2 & \cdots & m/d_{\tau-1} & m/d_\tau = m \end{pmatrix},$$

then the characteristic is

$$C(m) = \left(\begin{array}{c|c|c|c|c} \mu(d_{\tau-1}) & \mu(d_{\tau-2}) - \mu(d_{\tau-1}) & \cdots & \mu(d_1) - \mu(d_2) & \mu(m) - \mu(d_1) \\ m & m/d_{\tau-1} & \cdots & m/d_2 & m/d_1 \end{array} \right),$$

and every polynomial with integral coefficients is modulo m residually congruent to exactly one polynomial $a_0 + a_1 x + \cdots + a_{\mu(d_i)-1} \cdot x^{\mu(d_i)-1} + a_{\mu(d_i)} \cdot x^{\mu(d_i)}$

$+ \cdots + a_{\mu(d_{i-1})-1} \cdot x^{\mu(d_{i-1})-1} + a_{\mu(d_{i-1})} \cdot x^{\mu(d_{i-1})} + \cdots + a_{\mu(d_1)-1} \cdot x^{\mu(d_1)-1}$ $+ a_{\mu(d_1)} \cdot x^{\mu(d_1)} + \cdots + a_{\mu(m)-1} \cdot x^{\mu(m)-1}$, *in which each of the coefficients* $a_0, \cdots, a_{\mu(d_{\tau-1})-1}$ *has a value* $0, 1, \cdots, m-1$; *each of the coefficients* $a_{\mu(d_i)}, \cdots, a_{\mu(d_{i-1})-1}$ *has a value* $0, 1, \cdots, (m/d_i) - 1$.

For any m, *the characteristic may be immediately read off from the signature.*

When m contains only distinct prime factors, or when m is of the form p^γ, $\gamma < p$, the characteristic is expressible in terms of the prime factors and the exponent, without making explicit use of the μ function:

(*a*) $m = p$; $\quad S(p) = \begin{pmatrix} p & 0 \\ 1 & p \end{pmatrix}$; $\quad C(p) = \begin{pmatrix} \left|\begin{matrix} p \\ p \end{matrix}\right| \end{pmatrix}$.

(*b*) $m = p_1 \cdot p_2 \cdots p_\rho$, $\quad p_1 < p_2 < \cdots < p_\rho$;

$$S(p_1 p_2 \cdots p_\rho) = \begin{pmatrix} p_\rho & p_{\rho-1} & p_{\rho-2} & \cdots & p_2 & p_1 & 0 \\ 1 & p_\rho & p_\rho \cdot p_{\rho-1} & \cdots & p_\rho \cdot p_{\rho-1} \cdots p_3 & p_\rho \cdot p_{\rho-1} \cdots p_2 & p_\rho \cdot p_{\rho-1} \cdots p_1 \end{pmatrix};$$

$$C(p_1 p_2 \cdots p_\rho) = \left(\begin{array}{c|c|c|c|c|c} p_1 & p_2 - p_1 & p_3 - p_2 & \cdots & p_{\rho-1} - p_{\rho-2} & p_\rho - p_{\rho-1} \\ p_\rho p_{\rho-1} \cdots p_1 & p_\rho \cdot p_{\rho-1} \cdots p_2 & p_\rho p_{\rho-1} \cdots p_3 & \cdots & p_\rho p_{\rho-1} & p_\rho \end{array}\right).$$

(c_1) $m = p^\gamma$, $\quad \gamma < p$

$$S(p^\gamma) = \begin{pmatrix} p\gamma & \rho(\gamma-1) & p(\gamma-2) & \cdots & p^2 & p & 0 \\ 1 & p & p^2 & \cdots & p^{\gamma-2} & p^{\gamma-1} & p^\gamma \end{pmatrix};$$

$$C(p^\gamma) = \left(\begin{array}{c|c|c|c|c|c} p & p & p & \cdots & p & p \\ p^\gamma & p^{\gamma-1} & p^{\gamma-2} & \cdots & p^2 & p \end{array}\right).$$

But whatever the type of m, the characteristic, and thereby the set of completely reduced polynomials modulo m, are in all cases easily determined. Examples are given in § 6.

We see that the chain of residual congruences modulo m, and likewise, the characteristic $C(m)$ or the signature $S(m)$, determine:

1. The structure of the system of completely reduced polynomials modulo m;
2. The structure of the individual completely reduced polynomial modulo m.

§ 6. The number $N(m)$ of completely reduced polynomials modulo m. Classes of polynomials

From the characteristic $C(m)$ it is easily possible to determine the number $N(m)$ of distinct completely reduced polynomials modulo m, since the characteristic gives the degree $\mu(m) - 1$ of the polynomial as well as the range of values for each coefficient. We obtain,* since there are $\mu(m) - \mu(d_1)$ coef-

* Counting as a completely reduced polynomial also the polynomial all of whose coefficients are zero, as well as the constants $1, 2, \cdots, m-1$.

ficients which may independently assume any of the values $0, 1, \cdots, (m/d_1) - 1$, etc.,

THEOREM* V:

$$N(m) = \left(\frac{m}{d_1}\right)^{\mu(m)-\mu(d_1)} \cdot \left(\frac{m}{d_2}\right)^{\mu(d_1)-\mu(d_2)} \cdots \left(\frac{m}{d_{\tau-1}}\right)^{\mu(d_{\tau-2})-\mu(d_{\tau-1})} \cdot m^{\mu(d_{\tau-1})}$$

$$= m^{\mu(m)} \cdot d_1^{\mu(d_1)-\mu(m)} \cdot d_2^{\mu(d_2)-\mu(d_1)} \cdots d_{\tau-1}^{\mu(d_{\tau-1})-\mu(d_{\tau-2})} \tag{5}$$

$$= \left(\frac{m}{d_1}\right)^{\mu(m)} \cdot \left(\frac{d_1}{d_2}\right)^{\mu(d_1)} \cdots \left(\frac{d_{\tau-2}}{d_{\tau-1}}\right)^{\mu(d_{\tau-2})} \cdot \left(\frac{d_{\tau-1}}{1}\right)^{\mu(d_{\tau-1})}$$

Special cases are:

(*a*) $m = p$; $\quad N(p) = p^p$.

(*b*) $m = p_1 \cdot p_2 \cdots p_\gamma$, $p_1, \cdots, p_\gamma$ distinct primes:

$$N(p_1 \cdot p_2 \cdots p_\gamma) = p_1^{p_1} \cdot p_2^{p_2} \cdots p_\gamma^{p_\gamma}.$$

(c_1) $m = p^\gamma$, $\gamma < p$; $N(p^\gamma) = p^{p(1+2+\cdots+\gamma)} = p^{p\gamma(\gamma+1)/2}$.

From the manner in which in § 4 the signature of $m_1 \cdot m_2$ was derived from $S(m_1)$ and $S(m_2)$, it follows that, for m_1, m_2 relatively prime, we shall have $N(m_1 \cdot m_2) = N(m_1) \cdot N(m_2)$. However, since we have explained a direct and simple method for determining $N(m)$ for any given m, we shall not discuss the functional properties of $N(m)$.

Our work suggests a division of all polynomials with integral coefficients into $N(m)$ *classes modulo* m *by grouping always into one class the infinitude of polynomials which are residually congruent modulo* m *to the same completely reduced polynomial.* All polynomials belonging to the same class will be residually congruent to each other, modulo m, and we may select the completely reduced polynomial as representative of the entire class. The main property of the classes, for our present purposes, is expressed in the (now obvious)

THEOREM VI: *There are exactly* $N(m)$ *classes of polynomials modulo* m; *every polynomial belongs to exactly one class; all polynomials belonging to the same class have the same complete residue system modulo* m; *no two polynomials belonging to distinct classes have the same complete residue system.*

From this follows a result, which, from its character, belongs to the third part of the present paper, and which may be briefly stated as follows:

Of the m^m *possible sets of* m *numbers which may be chosen from the elements* $0, 1, 2, \cdots, m-1$ (*with repetition*), *exactly* $N(m)$ *are complete residue systems modulo* m *of some polynomial with integral coefficients.*

---

* Compare Part II, end.

Example* 1: $m = 7$. $\mu(m) = 7$; $S(7) = \begin{pmatrix} 7 & 0 \\ 1 & 7 \end{pmatrix}$; $C(7) = \begin{pmatrix} \left|\begin{matrix} 7 \\ 7 \end{matrix}\right| \end{pmatrix}$; $N(7) = 7^7$.

The completely reduced polynomials modulo 7 are the polynomials $a_0 + a_1 x + \cdots + a_6 x^6$, where each coefficient independently assumes all values $0, 1, \cdots, 6$.

Example 2: $m = 2 \cdot 3 \cdot 5 \cdot 11$. $\mu(m) = 11$;

$$S(m) = \begin{pmatrix} 11 & 5 & 3 & 2 & 0 \\ 1 & 11 & 11 \cdot 5 & 11 \cdot 5 \cdot 3 & 11 \cdot 5 \cdot 3 \cdot 2 \end{pmatrix};$$

$$C(m) = \left(\begin{array}{c|c|c|c} 2 & 1 & 2 & 6 \\ 11 \cdot 5 \cdot 3 \cdot 2 & 11 \cdot 5 \cdot 3 & 11 \cdot 5 & 11 \end{array}\right);$$

$$N(m) = 11^6 \cdot (11 \cdot 5)^2 \cdot (11 \cdot 5 \cdot 3)^1 \cdot (11 \cdot 5 \cdot 3 \cdot 2)^2 = 2^2 \cdot 3^3 \cdot 5^5 \cdot 11^{11}.$$

The completely reduced polynomials modulo $2 \cdot 3 \cdot 5 \cdot 11$ are the following: $a_0 + a_1 x + a_2 x^2 + \cdots + a_{10} x^{10}$, where $0 \leqq a_0, a_1 < 11 \cdot 5 \cdot 3 \cdot 2$; $0 \leqq a_2 < 11 \cdot 5 \cdot 3$; $0 \leqq a_3, a_4 < 11 \cdot 5$; $0 \leqq a_5, a_6, a_7, a_8, a_9, a_{10} < 11$.

Example 3: $m = 3^{11}$. $\mu(3^{11}) = 27$,

$$S(3^{11}) = \begin{pmatrix} 27 & 24 & 21 & 18 & 15 & 12 & 9 & 6 & 3 & 0 \\ 3^0 & 3^1 & 3^2 & 3^3 & 3^5 & 3^6 & 3^7 & 3^9 & 3^{10} & 3^{11} \end{pmatrix},$$

$$C(3^{11}) = \left(\begin{array}{c|c|c|c|c|c|c|c|c|c} 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 \\ 3^{11} & 3^{10} & 3^9 & 3^7 & 3^6 & 3^5 & 3^3 & 3^2 & 3^1 \end{array}\right),$$

$$N(3^{11}) = 3^{3(11+10+9+7+6+5+3+2+1)} = 3^{3 \cdot 54}.$$

The completely reduced polynomials modulo 3^{11} are $a_0 + a_1 x + a_2 x^2 + \cdots + a_{26} x^{26}$, where $0 \leqq a_{0,1,2} < 3^{11}$; $0 \leqq a_{3,4,5} < 3^{10}$; $0 \leqq a_{6,7,8} < 3^9$; $0 \leqq a_{9,10,11} < 3^7$; $0 \leqq a_{12,13,14} < 3^6$; $0 \leqq a_{15,16,17} < 3^5$; $0 \leqq a_{18,19,20} < 3^3$; $0 \leqq a_{21,22,23} < 3^2$; $0 \leqq a_{24,25,26} < 3$.

Example 4: $m = 2^7 \cdot 3^4 \cdot 7^2$. $\mu(2^7 \cdot 3^4 \cdot 7^2) = 14$,

$$S(m) = \begin{pmatrix} 14 & 9 & 8 & 7 & 6 & 4 & 3 & 2 & 0 \\ 1 & 7 & 3^2 \cdot 7 & 2^3 \cdot 3^2 \cdot 7 & 2^4 \cdot 3^3 \cdot 7^2 & 2^4 \cdot 3^3 \cdot 7^2 & 2^5 \cdot 3^3 \cdot 7^2 & 2^6 \cdot 3^4 \cdot 7^2 & 2^7 \cdot 3^4 \cdot 7^2 \end{pmatrix};$$

$$C(m) = \left(\begin{array}{c|c|c|c|c|c|c|c|c} 2 & 1 & 1 & 2 & 1 & 1 & 1 & 1 & 5 \\ 2^7 \cdot 3^4 \cdot 7^2 & 2^6 \cdot 3^4 \cdot 7^2 & 2^5 \cdot 3^3 \cdot 7^2 & 2^4 \cdot 3^3 \cdot 7^2 & 2^3 \cdot 3^3 \cdot 7^2 & 2^3 \cdot 3^2 \cdot 7 & 3^2 \cdot 7 & 7 \end{array}\right);$$

$N(m)$† $= 2^{40} \cdot 3^{27} \cdot 7^{21}$.

The following property, which we illustrate only by considering the special case $m = 2^7 \cdot 3^4 \cdot 7^2$, also holds for all m, as is immediately seen. For complicated moduli, it may be used as a convenient check.—On the same linear scale measure off, starting always from the same point, 0, the lengths 2, 4, 6, 8 $= \mu(2^7)$; 3, 6, 9 $= \mu(3^4)$; 7, 14 $= \mu(7^2)$. We obtain in this manner the following marks on our scale: 0 2 3 4 6 7 8 9 14, that is, the first line of $S(2^7 \cdot 3^4 \cdot 7^2)$, in reversed order; and the set of intervals between successive points, 2, 1, 1, 2, 1, 1, 1, 5 gives the first line of the characteristic, in proper order. The analogy with the method of the "Sieve of Eratosthenes" is obvious.

---

* Compare examples of § 4.

† The fact that each exponent is divisible by the corresponding base, is the expression of a simple theorem which holds for all values of m.

The completely reduced polynomials modulo $2^7 \cdot 3^4 \cdot 7^2$ are $a_0 + a_1 x + \cdots + a_{13} x^{13}$, where $0 \leqq a_0, a_1 < 2^7 \cdot 3^4 \cdot 7^2$; $\cdots$; $0 \leqq a_8 < 3^2 \cdot 7$; $0 \leqq a_{9,10,11,12,13} < 7$.

II. Residual congruences and Kronecker modular systems

§ 7. Residual congruences and Kronecker* modular systems

From Part I, §§ 2, 3, 4, it follows that the existence of a residual congruence $f(x) \equiv \phi(x) \pmod{m}$ is equivalent to the existence of an ordinary identity† in x of the following kind, in which $c_0(x)$, $c_1(x)$, $\cdots$ denote polynomials in x with integral coefficients (which may reduce to constants, including 0):

$$f(x) = \phi(x) + c_0(x) \cdot g_0(x) + c_1(x) \cdot g_1(x) + \cdots + c_{\tau-1}(x) \cdot g_{\tau-1}(x), \tag{6}$$

where

$$g_k(x) = \frac{m}{d_k} \cdot \prod_{i=0}^{\mu(d_k)-1} (x - i) \qquad \text{for } k > 0; \qquad g_0(x) = m.$$

This identity is, in Kronecker's notation, equivalent to

$$f(x) \equiv \phi(x) \operatorname{modd}\left[m; \frac{m}{d_1} \prod_{i=0}^{\mu(d_1)-1} (x - i); \frac{m}{d_2} \prod_{i=0}^{\mu(d_2)-1} (x - i); \cdots; \frac{m}{d_{\tau-1}} \prod_{i=0}^{\mu(d_{\tau-1})-1} (x - i) \right], \tag{7}$$

and, if we write for shortness $[m; \cdots; (m/d_{\tau-1}) \cdot \prod_{i=0}^{\mu(d_{\tau-1})-1}(x - i)] = M$, then M is a Kronecker modular system or a Kronecker modulus.

The congruence has this peculiarity, that all functions $g_k(x)$ of the modulus are themselves residually congruent to zero modulo m. The fact that the functions of the modulus determine the complete chain of congruences modulo m, as explained in Part I, corresponds to the combined statements:‡

(*a*) if $f(x)$, $\phi(x)$ are any two polynomials (with integral coefficients) such that $f(x) \equiv \phi(x) \bmod m$, then $c_0(x)$, $c_1(x)$, $\cdots$, $c_{\tau-1}(x)$ can be determined so that (6) is satisfied;

(*b*) if any function $g_k(x)$ is omitted from the modulus M, then there exist residual congruences $f(x) \equiv \phi(x) \pmod{m}$ for which the identity (6) cannot be satisfied.

In other words: every polynomial with integral coefficients, and whose value is divisible by m for all integral values of x, is representable in the

* Instead of using, as in the text, *one* Kronecker modulus, I had originally employed a *set* of congruences with double moduli $(c, \phi(x))$. L. E. Dickson, in conversation, suggested the use of a single Kronecker modulus.

† The sign of equality, $=$, is used, to avoid confusion with the sign for "congruent to."

‡ On account of the properties (*a*), (*b*), the modular system M may be called a "reduced fundamental" modular system. For a related "fundamental system," introduced for a different purpose, and consequently not reduced, see Hensel, *Ueber die Zahlenteiler ganzzahliger Funktionen*, Journal für Mathematik, vol. 116 (1896), pp. 350–356.

form $\sum_{k=0}^{r-1} c_k \cdot g_k(x)$, and if any of the $g_k(x)$ are omitted, there will be such polynomials $\phi(x)$ which can no longer be represented in the form (6).

Many authors have continued along various lines the work on modular systems inaugurated by Kronecker. One problem, in particular, is the examination of the "equivalence" of two such modular systems, and the reduction of a modular system to a canonical form. This subject is treated, for example, in several papers by Hensel* and Landsberg.* The necessary and sufficient conditions that a modular system shall be in canonical form may, according to these authors, be stated as follows (see 5 of last footnote, p. 365):

A modular system, M, is in canonical form when it is of the form

$$M = [g_1, k_1 \cdot g_2, k_2 \cdot g_3, \cdots, k_{r-1} \cdot g_r, k_r],$$

where

I. g_i $(i = 1, \cdots, r)$ are polynomials (in x) with integral coefficients and with the coefficient of the highest power of x each equal to unity;

II. The degrees γ_i of g_i $(i = 1, \cdots, r)$ are decreasing integers, $\gamma_i > \gamma_{i+1}$;

III. k_i $(i = 1, \cdots, r)$ are integers and each k_i is a proper factor of the next k_{i+1} (and therefore of all succeeding k);

IV. For $\sigma = 1, 2, \cdots, r-1$, $r > 1$, the polynomial g_σ is divisible by the modular system

$$\left[g_{\sigma+1}, \frac{k_{\sigma+1}}{k_\sigma} \cdot g_{\sigma+2}, \cdots, \frac{k_{r-1}}{k_\sigma} \cdot g_r, \frac{k_r}{k_\sigma}\right],$$

(and this new system is then, as a consequence of I–IV, again in canonical form).

After these preliminary remarks, we may state the relation between Part I of the present work and the theory of Kronecker modular systems as follows:

THEOREM VII: *For a given m the Kronecker modular system*

$$M = \left[1 \cdot \prod^{\mu(m)-1}(x-i); \frac{m}{d_{r-1}} \cdot \prod^{\mu(d_{r-1})-1}(x-i); \cdots; \frac{m}{d_2} \cdot \prod^{\mu(d_2)-1}(x-i); \right.$$
$$\left. \frac{m}{d_1} \cdot \prod^{\mu(d_1)-1}(x-i); m\right],$$

---

*1, 2. Hensel: *Zurückführung der Divisorensysteme auf eine reducierte Form*, I, Journal für Mathematik, vol. 118 (1897), pp. 234–251; II, vol. 119 (1898), pp. 114–130;

3. Hensel: *Ueber die elementaren arithmetischen Eigenschaften der reinen Modulsysteme*, ibid., vol. 119 (1898), pp. 175–185;

4. Landsberg, *Ueber Modulsysteme zweiter Stufe und Zahlenringe*, Nachrichten der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse, (1897), pp. 277–303 (277–286).

5. Encyclopédie des sciences mathématiques, Tome I, vol. 2, Landsberg-Hadamard-Kürschák, *Propriétés générales des corps et des variétés algébriques*, pp. 342–366.

See also Hancock, *Canonical forms for the unique representation of Kronecker's modular systems*, Journal für Mathematik, vol. 119 (1898), pp. 148–170.

which is uniquely determined by the signature

$$S(m) = \begin{bmatrix} \mu(m) & \mu(d_1) & \mu(d_2) & \cdots & \mu(d_{\tau-1}) & \mu(d_\tau) = 0 \\ 1 & \frac{m}{d_1} & \frac{m}{d_2} & \cdots & \frac{m}{d_{\tau-1}} & \frac{m}{1} = m \end{bmatrix},$$

is in canonical form.

Proof: Conditions I, II, III are obviously satisfied. To show that IV is also satisfied, it is only necessary to translate condition IV into language not involving the special notation of modular systems:

IV. For $\sigma = 1, 2, \cdots, r-1, r > 1$, the polynomial g_σ can be expressed (identically in x) in the form

$$g_\sigma = \psi_{\sigma+1} \cdot g_{\sigma+1} + \frac{k_{\sigma+1}}{k_\sigma} \cdot \psi_{\sigma+2} \cdot g_{\sigma+2} + \cdots + \frac{k_{r-1}}{k_\sigma} \cdot \psi_r \cdot g_\nu + \frac{k_r}{k_\sigma} \cdot \psi_{\sigma+1},$$

where $\psi_{\sigma+1}, \cdots, \psi_{r+1}$, and (as we know), $g_{\sigma+1}, \cdots, g_r$ are polynomials in x with integral coefficients, and (as we know), $k_{\sigma+1}/k_\sigma, \cdots, k_{r-1}/k_\sigma, k_r/k_\sigma$ are integers.

Applying this condition to our modular system M, we obtain for IV:

"We have to show that it is possible to determine, for σ equal to any of the values $1, 2, \cdots, r-1$, a set of polynomials in x, $\psi_\sigma, \psi_{\sigma+1}, \cdots, \psi_r$, with integral coefficients, such that the following equation is satisfied identically in x:

$$\prod_{i=0}^{\mu(d_{r-\sigma+1})-1} (x-i) = \prod_{i=0}^{\mu(d_{r-\sigma})-1} (x-i)\cdot\psi_\sigma + \frac{d_{r-\sigma}}{d_{r-\sigma-1}} \cdot \prod_{i=0}^{\mu(d_{r-\sigma-1})-1} (x-i)\cdot\psi_{\sigma+1}$$

$$+ \frac{d_{r-\sigma}}{d_{r-\sigma-2}} \cdot \prod_{i=0}^{\mu(d_{r-\sigma-2})-1} (x-i)\cdot\psi_{\sigma+2} + \cdots + \frac{d_{r-\sigma}}{d_1} \cdot \prod_{i=0}^{\mu(d_1)-1} (x-i)\cdot\psi_{r-1} + d_{r-\sigma}\cdot\psi_r."$$

Inspection shows that this happens for

$$\psi_\sigma = \prod_{i=\mu(d_{r-\sigma})}^{\mu(d_{r-\sigma+1})-1} (x-i); \qquad \psi_k = 0, \quad (k = \sigma+1, \cdots, r).$$

Example: $m = 2 \cdot 3 \cdot 5$.

$$S(2\cdot 3\cdot 5) = \begin{pmatrix} 5 & 3 & 2 \\ 1 & 5 & 3\cdot 5 \end{pmatrix};$$

$$M = [1 \cdot \Pi_{i=0}^{i=4}(x-i);\ 5 \cdot \Pi_{i=0}^{i=2}(x-i);\ 3\cdot 5 \cdot \Pi_{i=0}^{i=1}(x-i);\ 2\cdot 3\cdot 5].$$

Then

$$\Pi_{i=0}^{i=4}(x-i) = \frac{5}{5} \cdot \Pi_{i=0}^{i=2}(x-i)\cdot\psi_1 + \frac{3\cdot 5}{5} \cdot \Pi_{i=0}^{i=1}(x-i)\cdot\psi_2 + \frac{2\cdot 3\cdot 5}{5}\cdot\psi_3$$

for $\psi_1 = (x-3)(x-4)$, $\psi_2 = 0$, $\psi_3 = 0$; similarly

$$\Pi_{i=0}^{i=2}(x-i) = \frac{3\cdot 5}{3\cdot 5} \cdot \Pi_{i=0}^{i=1}(x-i)\cdot\psi_4 + \frac{2\cdot 3\cdot 5}{3\cdot 5}\cdot\psi_5$$

for $\psi_4 = x - 2$, $\psi_5 = 0$; and

$$\Pi_{i=0}^{i=1}(x - i) = \frac{2 \cdot 3 \cdot 5}{2 \cdot 3 \cdot 5}\psi_6,$$

for $\psi_6 = x(x - 1)$.

The problem of determining $N(m)$ for a given modulus (see § 6) has its exact counterpart in the case of a general modular system in canonical form, and is treated by Hensel, loc. cit. 3, and Landsberg, loc. cit. 4. In Landsberg's terminology, $N(m)$ is the Norm of the modular system.

(*To be continued.*)