POLYNOMIALS AND THEIR RESIDUE SYSTEMS

BY

AUBREY J. KEMPNER

(*Continued from page 266*)

III. Residual congruences and residue systems modulo m

§ 8. Reduced arithmetical sequences (modulo m)

We consider an arithmetical sequence of any order, $a_0, a_1, a_2, \cdots$, where all elements are integers, and reduce each term* modulo m (m a given positive integer), thus obtaining $\alpha_0, \alpha_1, \alpha_2, \cdots; 0 \leqq \alpha_i < m$. Similarly, the sequence of first differences is reduced modulo m, etc.—We introduce the following

Definition 7: *If the nth differences are all congruent to zero modulo m, but not all of the $n - 1$st differences are congruent to zero, we call the arithmetical sequence $a_0, a_1, a_2, \cdots$ an arithmetical sequence of order n modulo m; and we call the sequence $\alpha_0, \alpha_1, \alpha_2, \cdots, 0 \leqq \alpha_i < m$, a reduced arithmetical sequence of order n, modulo m.*—When there is no danger of ambiguity, abbreviated terms explaining themselves are used.

It is clear that a given arithmetical sequence leads to exactly one reduced arithmetical sequence modulo m, while a given arithmetical sequence modulo m may be derived from any one of an infinite number of arithmetical sequences.

Theorem VIII: *A reduced arithmetical sequence is periodic.*

Proof: The general term of an arithmetical sequence of order n of which all elements are integers may be represented by a polynomial $f(x)$ of degree n, with fractional (including integral) coefficients, the denominators of which are factors of $n!$ (including $n!$ itself). Assume then the polynomial to be written in the form $f(x) = (1/k) \cdot p(x)$, where $p(x)$ is a polynomial with integral coefficients and k a factor of $n!$. Then

$$\frac{1}{k} \cdot p(x + k \cdot m) \equiv \frac{1}{k} \cdot p(x) \pmod{m}$$

for all integral x; and $k \cdot m$, and all the more $n! \cdot m$, is either the length of the period or a multiple of the length of the period.

* R. D. Carmichael, *On sequences of integers defined by recurrence relations*, Quarterly Journal of Mathematics, vol. 48 (1920), pp. 343–372, has discussed, in an entirely different field, interesting applications of more general sequences obtained by reducing (modulo a given integer k) the elements $u_0, u_1, u_2, \cdots$ of a sequence satisfying a recurrence relation $u_{x+k} + \alpha_1 u_{x+k-1} + \cdots + \alpha_k u_x = \alpha$, in which $\alpha, \alpha_1, \cdots, \alpha_k$ are given integers.

Corollary: *In case $k = 1$, that is, in case the polynomial representing the general term of the arithmetical sequence of order n has integral coefficients, the length of the period is a factor of the modulus m, including m itself.*

Assume now

$$\begin{array}{llllllllll}
\alpha_{00} & \alpha_{01} & \alpha_{02} & \alpha_{03} & \cdots & & & & & \\
 & \alpha_{10} & \alpha_{11} & \alpha_{12} & \alpha_{13} & \cdots & & & & \\
 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & & \\
 & & \alpha_{n0} & \alpha_{n1} & \alpha_{n2} & \alpha_{n3} & \cdots, & & 0 \neq \alpha_{n0} = \alpha_{n1} = \alpha_{n2} = \cdots, &
\end{array}$$

to be a reduced arithmetical sequence modulo m of order n; then*

$$(8) \qquad \alpha_{0k} \equiv \sum_{\nu=0}^{\nu=n} \binom{k}{\nu} \alpha_{\nu 0} \pmod{m}, \qquad \text{where} \qquad \binom{k}{0} = 1;$$

$$(9) \qquad (-1)^k \cdot \alpha_{k0} \equiv \sum_{\nu=0}^{\nu=k} (-1)^\nu \binom{k}{\nu} \alpha_{0\nu} \pmod{m}.$$

Also, if $a_{00}, a_{01}, a_{02}, \cdots$ form an arithmetical sequence from which the reduced sequence in the α is obtained, and $a_{10}, a_{11}, a_{12}, \cdots$ the first differences, etc., then obviously

$$(8a) \qquad a_{0k} \equiv \sum \binom{k}{\nu} a_{\nu 0} \pmod{m},$$

$$(9a) \qquad (-1)^k \cdot a_{k0} \equiv \sum (-1)^\nu \binom{k}{\nu} a_{0\nu} \pmod{m}.$$

Theorem IX: *Assume $f(x)$ a polynomial with integral coefficients. The reduced arithmetical sequence modulo m derived from $\cdots f(-1), f(0), f(1), \cdots$ is of order lower than $\mu(m)$, where $\mu(m)$ is the number defined in § 1.*

Proof: The *reduced* sequence $\cdots \alpha_{-1}\, \alpha_0\, \alpha_1\, \alpha_2 \cdots$ is the same as if we had started, not from the polynomial $f(x)$, but from the corresponding, modulo m completely reduced, polynomial, which is of degree $< \mu(m)$.

* From the corresponding formulæ for arithmetical sequences of order n: $a_{00}, a_{01}, a_{02}, \cdots$. The second of these formulæ,

$$(-1)^k \cdot a_{k0} = \Sigma_{\nu=0}^{\nu=k} (-1)^\nu \cdot \binom{k}{\nu} a_{0\nu},$$

is obtained most directly by applying the first,

$$a_{0k} = \Sigma_{\nu=0}^{\nu=n} \binom{k}{\nu} a_{\nu 0},$$

to the arithmetical sequence obtained from the original sequence by replacing a_{ij} by $(-1)^{i+j} \cdot a_{ji}$, where now (on account of a_{ni} = constant), $a_{ji} = 0$ for $j > n$. (See § 10, end.)

COROLLARY: *Under the assumptions of the theorem, the* $\mu(m)$*th differences are all zero* ($\equiv 0 \pmod{m}$).

The theorem does *not* hold for arithmetical sequences whose elements are integers, but which are generated by polynomials with fractional, not integral, coefficients, as is shown by simple examples.

Example: $f(x) = 2 - \frac{5}{12}x + \frac{65}{24}x^2 - \frac{19}{12}x^3 + \frac{7}{24}x^4$ generates the arithmetical sequence of order four,

```
··· 2   3   4   6   17   52   133   ···
  ··· 1   1   2   11   35   81   156   ···
    ··· 0   1   9   24   46   75   111   ···
      ··· 1   8   15   22   29   36   43   ···
        ··· 7   7   7   7   7   7   7   ···
```

which reduces modulo 3 to a reduced sequence of order $4 > \mu(3)$ (but $\leqq n$):

```
··· 2   0   1   0   2   1   1   ···
  ··· 1   1   2   2   2   0   0   ···
    ··· 0   1   0   0   1   0   0   ···
      ··· 1   2   0   1   2   0   1   ···
        ··· 1   1   1   1   1   1   1   ···.
```

In order to avoid ambiguity, and to express our theorems in the simplest form, we define residue systems in the following way:

DEFINITION 8: *Let* $f(x)$ *be a polynomial with integral coefficients (admitting as a polynomial also a constant either different from, or equal to, zero) and* m *a given positive integer. Then the numbers* $\alpha_i \equiv f(i) \pmod{m}$, $0 \leqq \alpha_i < m$, $i = 0, 1, 2, \cdots$, *starting always with* $i = 0$, *form a complete residue system modulo* m *of* $f(x)$.

Important in this definition are the words: "starting always with $i = 0$." Thus, $0, 0, 2, 1, 2, 0, 0, 2, 1, \cdots$ is a residue system modulo 5 of $x^2 - x$; but $0, 2, 1, 2, 0, 0, 2, 1, 2, \cdots$ is not a residue system of $x^2 - x$, but of, for example, $x^2 + x$.

We can already state, as a consequence of Theorem IX, the

COROLLARY: *The first* $\mu(m)$ *elements of a residue system modulo* m *of a polynomial with integral coefficients completely determine the whole residue system.* Only an obvious modification is required, in case any $\mu(m)$ consecutive elements are given.

This does not hold for polynomials which assume integral values for all integral x, but with rational (not integral) coefficients. We shall also see later that, except for m a prime, the $\mu(m)$ elements are not independent of each other.

§ 9. Simple applications of reduced arithmetical sequences

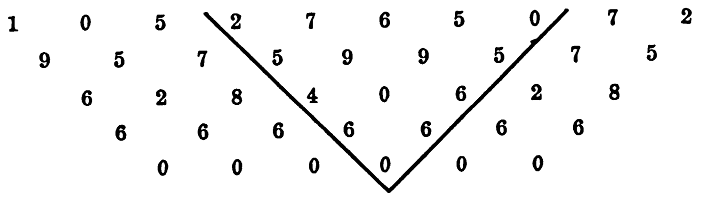
The preceding considerations permit a very simple treatment of the following problems.*

(*a*) Given a complete residue system modulo m; to determine the degree of the corresponding completely reduced polynomial.

Solution: We know that the degree is $< \mu(m)$. Determine $\mu(m)$. Form the sequence of first differences of the given residue system and reduce modulo m. If these differences are all zero, our function is a constant. If the ρth sequence of reduced differences (ρ necessarily $< \mu(m)$) is the first in which all elements vanish, the polynomial is of degree $\rho - 1$ exactly. In practice, one will make use of the fact that if in the $(\mu - 1)$st sequence of differences two consecutive elements are equal, then, since the (constant) μth difference is zero, all elements of the $(\mu - 1)$st sequence are equal; similarly, if there is a $k < \mu$ for which k consecutive elements of the sequence of differences of order $\mu - k + 1$ are equal, then all elements of this sequence vanish.

(*b*) Assume given consecutive residues modulo m, not necessarily starting from $f(0)$, but in sufficient number to determine the whole residue system. To complete the residue system and find the degree of the corresponding completely reduced polynomial.

Solution: The solution is obvious, by completing the sequence. For example, given modulo $10, f(3) \equiv 2, f(4) \equiv 7, f(5) \equiv 6, f(6) \equiv 5, f(7) \equiv 0$.



We construct first the part of the table wedged in between the slanting lines. From this we see that our polynomial is of degree three, exactly. By completing the arrangement as indicated, we find the complete residue system to be

1 0 5 2 7 6 5 0 7 2.

(*c*) Given a complete residue system modulo m, or at least enough to determine it by (*b*). To determine the corresponding completely reduced polynomial.

Solution: We assume in the residue system at least $\mu(m)$ consecutive elements known. If these are the first $\mu(m)$ elements, then

$$\alpha_{0k} \equiv \Sigma_{\nu=0}^{\mu(m)-1} \binom{k}{\nu} \alpha_{\nu 0} \quad (\text{mod } m)$$

determines a polynomial of the proper degree, and it remains to completely reduce this polynomial in case the coefficients do not satisfy the inequalities of § 5.

* In the treatment of these problems, the number $\mu(m)$ plays so natural a rôle that a method making systematic use of it may be expected to be somewhat simpler and shorter than methods where $\mu(m)$ is not explicitly employed. This is the justification for inserting these applications which are, on the whole, of the nature of simple interpolation problems.

Example: $f(4) \equiv 9, f(5) \equiv 16, f(6) \equiv 25, f(7) \equiv 6, f(8) \equiv 13, f(9) \equiv 4 \pmod{30}$. Since $\mu(30) = 5, f(x)$ is of degree $\mu - 1 = 4$ at most.

$$\begin{array}{ccccccccccc}
9 & & 16 & & 25 & & 6 & & 13 & & 4 \\
& 7 & & 9 & & 11 & & 7 & & 21 & \\
& & 2 & & 2 & & 26 & & 14 & & \\
& & & 0 & & 24 & & 18 & & & \\
& & & & 24 & & 24 & & & &
\end{array}$$

and

$$\phi(x) = 9 + 7\binom{x}{1} + 2\binom{x}{2} + 24\binom{x}{4} = 9 + 12x^2 - 6x^3 + x^4$$

is a polynomial for which, not as required, $f(4) \equiv 9, f(5) \equiv 16, \cdots \pmod{30}$, but instead $\phi(0) \equiv 9$, $\phi(1) \equiv 16$, $\cdots$ etc. To deduce the polynomial $f(x)$ from $\phi(x)$, we form first $g(x) = \phi(x - 4)$ and reduce the coefficients modulo 30, thus obtaining $g(x) \equiv 1 + 20 \cdot x + 0 \cdot x^2 + 8 \cdot x^3 + 1 \cdot x^4 \pmod{30}$, where now, as required, $g(4) = 9, g(5) = 16, \cdots$. However, $g(x)$ is not a completely reduced polynomial modulo 30, since each such polynomial must be of the form: $a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4, 0 \leqq a_0 < 30, 0 \leqq a_1 < 30, 0 \leqq a_2 < 15, 0 \leqq a_3 < 5, 0 \leqq a_4 < 5$, while in $g(x)$ we have $a_3 = 8$. In this case, where we need the individual completely reduced polynomial, it is necessary to reduce $g(x)$ by means of the explicit congruences $1 \cdot x(x-1)(x-2)(x-3)(x-4) \equiv 0, 5 \cdot x(x-1)(x-2) \equiv 0, 15 \cdot x(x-1) \equiv 0 \pmod{30}$. We find for our completely reduced polynomial $f(x) = 1 + 25x + 0x^2 + 3x^3 + 1x^4$, which satisfies the assumed conditions.

§ 10. Residual congruences modulo m of the second kind

We have seen that modulo m a residue system of a polynomial with integral coefficients is always completely determined by any $\mu(m)$ consecutive elements. By Definition 8, § 8, a residue system $\alpha_0, \alpha_1, \cdots, \alpha_{m-1}$ is distinct from $\alpha_1, \alpha_2, \cdots, \alpha_{m-1}, \alpha_0$ or from any other one obtained from it by cyclic interchange; (the passage from the generating polynomial of the one to the generating polynomial of the other is given by replacing, in $f(x)$, x by $x - c$, where c is a certain integer. See problem (*c*) of § 9). By definition, always $\alpha_i \equiv f(i) \pmod{m}$.

Unless m is a prime, there exist relations between these $\mu(m)$ residues, as will soon be seen from the fact that the number of distinct residue systems modulo m is, unless m is a prime, smaller than $m^{\mu(m)}$, the number which we should obtain if the $\mu(m)$ residues $\alpha_0, \alpha_1, \cdots, \alpha_{\mu(m)-1}$, which determine the whole residue system, were at liberty to range independently from 0 to $m - 1$. Our next problem is to establish these interrelations and generally to examine the structure of residue systems for a given modulus m.

We note first the obvious

LEMMA 9: *If p is any prime factor of the modulus m, and $\alpha_0, \alpha_1, \cdots, \alpha_{m-1}, \alpha_m = \alpha_0, \alpha_{m+1} = \alpha_1, \cdots$ the complete residue system modulo m of a polynomial with integral coefficients, then $\alpha_{k+p} \equiv \alpha_k \pmod{p}$ for all integral k.*

From this follows immediately

LEMMA 10: *If d is any divisor of m containing no square factors* (i.e., $d = p_1 \cdot p_2 \cdots p_\rho$, $p_1 \neq p_2 \neq \cdots \neq p_\rho$), *then $\alpha_{k+d} \equiv \alpha_k \pmod{d}$ for all integral k.*

We continue with the following assertion:

Let $\alpha_0, \alpha_1, \cdots, \alpha_{m-1}$, ($\alpha_i \equiv f(i) \pmod{m}$, $0 \leqq i < m$, $f(x)$ a polynomial with integral coefficients) be a complete residue system modulo m of $f(x)$, and let d be any divisor of m. Then

$$\alpha_{k+\mu(d)} - \binom{\mu(d)}{1} \cdot \alpha_{k+\mu(d)-1} + \binom{\mu(d)}{2} \cdot \alpha_{k+\mu(d)-2} - \cdots \pm \alpha_k \equiv 0 \pmod{d} \tag{10}$$

for $k = 0, 1, 2, \cdots, \mu(d) - 1$ and therefore for all integral k..

Proof: We reduce $\alpha_0, \alpha_1, \cdots, \alpha_{m-1}$, modulo d. Since d is a divisor of m, we shall obtain the same result as if we had reduced directly modulo d the arithmetical sequence $f(0), f(1), \cdots, f(m-1)$, that is, we shall obtain the complete residue system modulo d of $f(x)$, but repeated m/d times over. By Theorem IX, § 8, the differences of order $\mu(d)$ are all zero ($\equiv 0 \bmod d$). Applying formula (9) of § 8, writing α_i for α_{0i} and taking $k = \mu(d)$, the statement is proved. Therefore, for each divisor, d, of m (including $d = m$), any element $\alpha_{k+\mu(d)}$ of a residue system modulo m is, at least modulo d, determined by the $\mu(d)$ preceding elements $\alpha_k, \cdots, \alpha_{k+\mu(d)-1}$, of the residue system. In the same way, of course, each element is determined, modulo d, by the $\mu(d)$ succeeding elements of the residue system.

The following notation suggests itself immediately:

$$\alpha_{k+\mu(d)} \equiv l(\alpha_{k+\mu(d)-1}, \alpha_{k+\mu(d)-2}, \cdots, \alpha_k) \pmod{d} \quad (k = 0, 1, 2, \cdots),$$

or, in order to save space and in close analogy with Definition 3 of § 2,

$$\alpha_{k+\mu(d)} \equiv l \pmod{d} \qquad (k = 0, 1, 2, \cdots), \tag{11}$$

where $l(\alpha_{k+\mu(d)-1}, \cdots, \alpha_k)$ and l each stand for: any linear polynomial in $\alpha_{k+\mu(d)-1}, \cdots, \alpha_k$ with integral coefficients which satisfies for $k = 0, 1, 2, \cdots$ the congruence (11). If we think of k as a variable and replace it by x, we have a congruence satisfied by all integral values of x, that is, exactly the kind of congruence considered in § 2 (the fact that x now does not assume negative integral values being due to the notation only), and we therefore write, using again the symbol $\equiv$,

$$\alpha_{x+\mu(d)} \equiv l \pmod{d},$$

or, more conveniently for our purposes

$$\frac{m}{d} \cdot \alpha_{x+\mu(d)} \equiv l \pmod{m},$$

and call such congruences again residual congruences, or, if we wish to distinguish them from the residual congruences introduced in

Part I, residual congruences of the second kind (modulo m). Finally, in order to indicate still more clearly by the notation the intimate relationship existing between these new residual congruences and those of Part I, we denote

$$\frac{m}{d}\cdot\alpha_{x+\mu(d)}\equiv l \bmod m$$

also by

$$\Big\}\mu(d),\frac{m}{d}\Big\{\quad\text{or}\quad\Big\}\mu(d),\frac{m}{d}\Big\{_m\quad\text{or}\quad\Big\}\mu(d),\frac{m}{d}\Big\{\ (\bmod m).$$

We have thus proved

THEOREM X: *For any integer m and any factor d of m (including $d = m$, and, as a trivial case, $d = 1$), there exists a residual congruence of the second kind*

$$\alpha_{x+\mu(d)}-\binom{\mu(d)}{1}\cdot\alpha_{x+\mu(d)-1}+\binom{\mu(d)}{2}\cdot\alpha_{x+\mu(d)-2}-\cdots\pm\alpha_x\equiv 0\ (\bmod d),$$

or, using the notations introduced above,

(12) $\alpha_{x+\mu(d)}\equiv l\ (\bmod d)$, *or*[*] $\dfrac{m}{d}\cdot\alpha_{x+\mu(d)}\equiv l\ (\bmod m)$,

or

(12) $\Big\}\mu(d),\dfrac{m}{d}\Big\{$, *or* $\Big\}\mu(d),\dfrac{m}{d}\Big\{_m$.

These residual congruences of the second kind are complete analoga of the residual congruences of § 2, and our considerations in Part III will go parallel with corresponding considerations of Part I, thus establishing a complete isomorphism between the structure of the totality of completely reduced polynomials modulo m and the totality of complete residue systems for the same modulus; such that every statement referring to the structure of the one totality leads immediately to a corresponding statement concerning the structure of the other.

The simple underlying reason for this parallelism may be indicated as follows: In an arithmetical sequence of order n,

$$\begin{array}{cccccccccc}
\cdots & a_{00} & a_{01} & a_{02} & \cdots & a_{0\lambda} & a_{0,\lambda+1} & \cdots & & \\
& \cdots & a_{10} & a_{11} & a_{12} & \cdots & a_{1\lambda} & a_{1,\lambda+1} & \cdots & \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
& & \cdots & a_{n0} & a_{n1} & a_{n2} & \cdots & a_{n\lambda} & a_{n,\lambda+1} & \cdots,
\end{array}$$

with $a_{\rho,\sigma+1}-a_{\rho,\sigma}=a_{\rho+1,\sigma}$, and $0\neq a_{n0}=a_{n1}=\cdots$, the formula (8):

[*] In the next congruence, all coefficients of l have m/d as a factor. This l is of course not identical with the l of the preceding congruence.

$a_{0k} = \sum_{\nu=0}^{\nu=n} \binom{k}{\nu} \cdot a_{\nu 0}$ expresses the values $a_{0i} = f(i)$ (and therefore also their residues modulo m, where m is a given integer), in terms of the coefficients of the expansion

$$f(x) = a_{00} + a_{10} \cdot \frac{x}{1} + a_{20} \cdot \frac{x(x-1)}{1 \cdot 2} + a_{30} \cdot \frac{x(x-1)(x-2)}{1 \cdot 2 \cdot 3} + \cdots,$$

that is, the residues of $f(x)$ modulo m are expressed in terms of the coefficients a_{i0}.

On the other hand, the formula (9): $(-1)^k \cdot a_{k0} = \sum_{\nu=0}^{\nu=k} (-1)^\nu \cdot \binom{k}{\nu} \cdot a_{0\nu}$, which gives the coefficients a_{k0} of $f(x) = \sum_{\nu=0}^{\nu=n} a_{\nu 0} \cdot \binom{x}{\nu}$ in terms of $f(i) = a_{0i}$, is nothing but (8) applied to the new arithmetical sequence

$$\begin{array}{ccccccccccccc}
\cdot\ \cdot\ \cdot & a_{00} & & -a_{10} & & a_{20} & & -a_{30} & & \cdot\ \cdot\ \cdot & & & \\
& \cdot\ \cdot\ \cdot & -a_{01} & & a_{11} & & -a_{21} & & a_{31} & & \cdot\ \cdot\ \cdot & & \\
& & \cdot\ \cdot\ \cdot & a_{02} & & -a_{12} & & a_{22} & & -a_{32} & & \cdot\ \cdot\ \cdot & \\
& & \cdot\ \cdot\ \cdot & \cdot & & \cdot & & \cdot & & \cdot\ \cdot\ \cdot & & \cdot\ , &
\end{array}$$

and we see that (8) and (9) are (essentially) the same formula, only with a_{i0} (the coefficients of $\sum a_{\nu 0} \cdot \binom{x}{\nu}$) and a_{0i} (the functional values $f(i)$) interchanged. (Compare § 8, second footnote, and § 2, end of long footnote.)

§ 11. Chain of residual congruences of the second kind; signature of the second kind

For any given modulus m we may derive a set of residual congruences of the second kind by choosing all factors of m, including m itself, and deriving for each factor the corresponding congruence (12) of § 10. However, in general these congruences will form subsets such that all congruences of any particular subset are implied by one congruence of this subset. These dependent congruences we shall reject, and the set of congruences retained we call a "a chain of residual congruences of the second kind, modulo m," or, a "chain of residual congruences," as in § 3, when the difference between the former type of chain and the present type does not have to be emphasized.

We shall have in detail:

(a) $m = p$, p a prime. Our chain consists of none but a trivial congruence. The p elements of a residue system modulo p may be chosen at random, so that no relation exists between them.* To the sole congruence $1 \cdot x^p \equiv \psi(x)$ $(\text{mod}\ p)$ or $\{p,\ 1\}$ of § 3 corresponds now the sole congruence $\alpha_{x+p} \mathrel{\bar{\equiv}} \alpha_x$ $(\text{mod}\ p)$ or $\}p,\ 1\{$. The "signature of the second kind," which we define under (b) below, is denoted for the case $m = p$ by $S(p) = \binom{p}{1}$, or $\binom{p\ \ 0}{1\ \ p}$, using the same notation which was introduced for the signature in § 4.

* See reference to Zsigmondy in Introduction.

(*b*) $m = p_1 \cdot p_2 \cdot p_3 \cdots p_\tau$, $p_1 < p_2 < \cdots < p_\tau$ prime numbers. Remembering that $\mu(p_1 \cdot p_2 \cdots p_i) = p_i$ $(i = 1, 2, \cdots, \tau)$ we obtain (from Theorem X, § 10) the set of residual congruences of the second kind

$$\alpha_{x+p_i} \equiv l \; (\operatorname{mod}\, (p_1 p_2 \cdots p_i)) \qquad (i = 1, 2, \cdots, \tau),$$

or

$$\}p_i,\, 1\{_{p_1 \cdot p_2 \cdots p_i}\,.$$

This chain may be written also in either one of the two forms

$$p_\tau \cdot p_{\tau-1} \cdots p_{i+1} \cdot \alpha_{x+p_i} \equiv l \; (\operatorname{mod}\, m) \quad (i = 1, 2, \cdots, \tau),$$ [*]

or

$$\}p_i,\, (p_\tau \cdot p_{\tau-1} \cdots p_{i+1})\{_m \qquad (i = 1, 2, \cdots, \tau).$$

These chains correspond exactly to the chains of §§ 3, 4. The (for our purposes unimportant) functions l may in case (*b*) be simplified by using Lemma 9 and 10. See Example, below.

We introduce a symbol, the signature of the second kind of m. Since we shall show that its properties are abstractly identical with the characteristic properties of the signature of m introduced in § 4, we shall denote it by the same symbol $S(m)$, or, if we wish to distinguish it from the other signature, by $S'(m)$. Likewise, we shall ordinarily omit the words "of the second kind," and call both simply "signature of m," when there is no risk of confusion. Then $S'(p_1 \cdot p_2 \cdots p_\tau)$ is read off from the chain of residual congruences above in the same way in which $S(p_1 p_2 \cdots p_\tau)$ was read off in § 4:

$$S'(p_1 p_2 \cdots p_\tau) = S(p_1 p_2 \cdots p_\tau)$$

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

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

Here the arbitrary entry 0, $(p_\tau p_{\tau-1} \cdots p_1)$ corresponds to the trivial congruence mentioned in the last footnote. As is clearly seen, our chain of residual congruences is completely determined by the signature of $p_1 p_2 \cdots p_\tau$. Each entry $(p_\tau \cdot p_{\tau-1} \cdots p_{i+1})$ in the second line of $S(p_1 p_2 \cdots p_\tau)$ gives the coefficient on the left side of one of the congruences, while the upper entry p_i gives us the number p_i of terms sufficient to insure that the product of any residue α by $p_\tau p_{\tau-1} \cdots p_{i+1}$ is completely determined by the following (or preceding) p_i residues.

[*] $i \equiv 0$ would correspond to the trivial congruenec $(m/1) \cdot \alpha_{x+1} \equiv 0 \bmod m$.

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

$$\begin{aligned} &\alpha_{x+5} - 5\alpha_{x+4} + 10\alpha_{x+3} - 10\alpha_{x+2} + 5\alpha_{x+1} - \alpha_x && \equiv 0 \pmod{30} \\ &5(\alpha_{x+3} - 3\alpha_{x+2} + 3\alpha_{x+1} - \alpha_x) && \equiv 0 \pmod{30} \\ &5 \cdot 3(\alpha_{x+2} - 2\alpha_{x+1} + \alpha_x) && \equiv 0 \pmod{30} \\ &5 \cdot 3 \cdot 2(\alpha_{x+1} - \alpha_x) && \equiv 0 \pmod{30}, \end{aligned}$$

of which the last congruence is trivial. These congruences are written

$$\begin{aligned} 1 \cdot \alpha_{x+5} &\equiv l \pmod{30} & & \}5, 1\{ \\ 5 \cdot \alpha_{x+3} &\equiv l \pmod{30} & \text{or} \quad & \}3, 5\{ \\ 5 \cdot 3\alpha_{x+2} &\equiv l \pmod{30} & & \}2, 5 \cdot 3\{, \end{aligned}$$

omitting the trivial congruence. The signature is

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

Besides, the congruences $\alpha_{x+5} \equiv \alpha_x \pmod 5$, $\alpha_{x+3} \equiv \alpha_x \pmod 3$, $\alpha_{x+2} \equiv \alpha_x \pmod 2$ of Lemma 9, § 10, tell us—as an obvious result—that in any residue system modulo 30 any element is congruent modulo 5 to its fifth succeeding or preceding element; is congruent modulo 3 to its third succeeding or preceding element, etc. Similarly modulo 6, 10, 15, from Lemma 10.

(c) $m = p^\gamma$. We assume first

(c_1) $\gamma < p$. In this case we may again conveniently replace in the congruences of Theorem 10 the functions l by a simpler set. We show this by proving

LEMMA 11: *For* $m = p^\gamma$, $\gamma < p$, *the residual congruences*

$$(13) \qquad \begin{aligned} &\alpha_{x+k\cdot p} - \binom{k}{1}\alpha_{x+(k-1)\cdot p} + \binom{k}{2}\alpha_{x+(k-2)\cdot p} - \\ &\qquad\qquad + \cdots \pm \binom{k}{1}\alpha_{x+p} \mp \alpha_x \equiv 0 \pmod{p^k} \end{aligned}$$

hold for $k = 1, 2, \cdots, \gamma$.

Proof: For $k = 1$, obviously $\alpha_{x+p} \equiv \alpha_x \pmod p$; for $k = 2$, we shall have $\alpha_{x+2p} - 2\alpha_{x+p} + \alpha_x \equiv 0 \pmod{p^2}$, since, if $f(x)$ is a polynomial with integral coefficients (of degree n), then $F(x) = (1/p)\{f(x+p) - f(x)\}$, $F(x+p) = (1/p)\{f(x+2p) - f(x+p)\}$ are again polynomials (of degree $n-1$) with integral coefficients, and therefore

$$F(x+p) - F(x) = (1/p)\{f(x+2p) - 2f(x+p) + f(x)\} \equiv 0 \pmod p.$$

Similarly, the lemma is proved for the kth differences of $f(x)$, $k = 1, 2, \cdots, \gamma$.

DEFINITION 9: *We denote the congruence* (13) *by* $\alpha_{x+k\cdot p} \equiv l' \pmod{p^k}$, *in case we wish to emphasize the special character of* (13).

Here the l' are certain l (see Theorem X), but the accent is introduced to remind us that of the $k \cdot p$ elements of the residue system preceding (or

[*] Compare the examples of § 11 with those of § 4.

succeeding) any element $\alpha_{x+k\cdot p}$, only the k equidistant elements $\alpha_{x+(k-1)\cdot p}$, $\alpha_{x+(k-2)\cdot p}$, $\cdots$, α_{x+p}, α_x are involved in the congruence.

We thus obtain for $m = p^\gamma$, $\gamma < p$, the chain of residual congruences

$$p^i \cdot \alpha_{x+(\gamma-i)\cdot p} \equiv l' \pmod{p^\gamma} \qquad (i = 0, 1, \cdots, \gamma - 1).^*$$

This is again completely analogous to § 4. The signature, introduced as in case (b), coincides again with $S(m)$ of § 4:

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

Example: $m = 5^4$; $\mu(5^4) = 20$. The chain of congruences is, written out in full:

$$\alpha_{x+20} - 4 \cdot \alpha_{x+15} + 6 \cdot \alpha_{x+10} - 4 \cdot \alpha_{x+5} + \alpha_x \equiv 0 \pmod{5^4}$$
$$5(\alpha_{x+15} - 3 \cdot \alpha_{x+10} + 3 \cdot \alpha_{x+5} - \alpha_x) \equiv 0 \pmod{5^4}$$
$$5^2(\alpha_{x+10} - 2 \cdot \alpha_{x+5} + \alpha_x) \equiv 0 \pmod{5^4}$$
$$5^3(\alpha_{x+5} - \alpha_x) \equiv 0 \pmod{5^4},$$

or,

$$5^i \cdot \alpha_{x+5(4-i)} \equiv l', \qquad \text{resp.} \qquad 5^i \cdot \alpha_{x+5(4-i)} \equiv l \pmod{5^4}, \qquad (i=0, 1, 2, 3)$$

or

$$\}\, 5(4 - i),\ 5^i\, \{ \pmod{5^4} \qquad (i=0, 1, 2, 3).$$

The signature is again

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

Each of the congruences yields a number of distinct relations between the elements of any residue system modulo 5^4 (of a polynomial with integral coefficients). For example, the first congruence written out yields

$$\alpha_{20} - 4 \cdot \alpha_{15} + 6 \cdot \alpha_{10} - 4 \cdot \alpha_5 + \alpha_0 \equiv 0 \pmod{5^4},$$
$$\alpha_{21} - 4 \cdot \alpha_{16} + 6 \cdot \alpha_{11} - 4 \cdot x_6 + \alpha_1 \equiv 0 \pmod{5^4}, \qquad \text{etc.},$$

where the elements of the residue system may be thought of as repeated periodically indefinitely in either direction.

In this example, and similarly in other cases, the full congruences may be chosen instead of the set (13), that is

$$\alpha_{x+20} - \binom{20}{1}\alpha_{x+19} + \binom{20}{2}\alpha_{x+18} - + \cdots - \binom{20}{1}\alpha_{x+1} + \alpha_x \equiv 0 \pmod{5^4}$$
$$5\left(\alpha_{x+15} - \binom{15}{1}\alpha_{x+14} + \binom{15}{2}\alpha_{x+13} - + \cdots + \binom{15}{1}\alpha_{x+1} - \alpha_x\right) \equiv 0 \pmod{5^4}$$
$$5^2\left(\alpha_{x+10} - \binom{10}{1}\alpha_{x+9} + \binom{10}{2}\alpha_{x+8} - + \cdots - \binom{10}{1}\alpha_{x+1} + \alpha_x\right) \equiv 0 \pmod{5^4}$$
$$5^3\left(\alpha_{x+5} - \binom{5}{1}\alpha_{x+4} + \binom{5}{2}\alpha_{x+3} - \binom{5}{2}\alpha_{x+2} + \binom{5}{1}\alpha_{x+1} - \alpha_x\right) \equiv 0 \pmod{5^4}.$$

This set has the same signature as (13), and will therefore lead to the same reductions for all purposes for which we shall use the system.

(c_2) $m = p^\gamma$, $\gamma \geqq p$. By making use of the properties of $\mu(m)$ derived in § 1, the considerations applied in (c_1) will now lead to the chain

[*] $i = \gamma$ corresponding to the trivial congruence.

$$\begin{array}{ll}
\alpha_{x+p} \equiv \alpha_x \pmod{p}, & \text{or} \\
\alpha_{x+p} \equiv l' \pmod{p},^{*} & \text{and similarly} \\
\alpha_{x+2p} \equiv l' \pmod{p^2}, & \\
\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot & \\
\alpha_{x+ip} \equiv l' \pmod{p^i}, & i < p, \\
\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot & \\
\alpha_{x+p^2} \equiv l' \pmod{p^{p+1}}, \text{ not only modulo } p^p, \text{ since } \mu(p^p) = \mu(p^{p+1}) = p^2; & \\
\alpha_{x+p^2+p} \equiv l' \pmod{p^{p+2}}, & \\
\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot & \\
\alpha_{x+p^2+i\cdot p} \equiv l' \pmod{p^{p+i+1}}, & i < p, \\
\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot & \\
\alpha_{x+2p^2} \equiv l' \pmod{p^{2p+2}}, \text{ not only modulo } p^{2p+1}; & \\
\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot & \\
\alpha_{x+\rho p^2} \equiv l' \pmod{p^{\rho(p+1)}}, & \rho < p, \\
\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot & \\
\alpha_{x+p^3} \equiv l' \pmod{p^{p^2+p+1}}, \text{ not only mod } p^{p(p+1)}; & \\
\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\,. &
\end{array}$$

Making all moduli equal to p^γ, we shall have $\}\mu(p^\gamma),\ 1\{;\ \}\mu(p^{\gamma_1}),\ p^{\gamma-\gamma_1}\{;\ \cdots;\ \}\mu(p^{\gamma_i}),\ p^{\gamma-\gamma_i}\{;\ \cdots;\ \{\mu(p),\ p^{\gamma-1}\{$, all modulo p^γ, where $\gamma_1, \gamma_2, \cdots$ are determined as the largest integers for which, resp., $\mu(p^{\gamma_1}) = \mu(p^\gamma) - p$, $\cdots, \mu(p^{\gamma_i}) = \mu(p^\gamma) - ip, \cdots$. (Compare the parallel work in § 4, case 4.) Introducing the symbol for the signature as in (*b*) of this section, we obtain the expression which we had found in § 4:

$$S(p^\gamma) = \begin{pmatrix} \mu(p^\gamma) & \mu(p^\gamma) - 1 \cdot p & \cdots & \mu(p^\gamma) - ip & \cdots & 0 \\ 1 & p^\gamma/p^{\gamma_1} & \cdots & p^\gamma/p^{\gamma_i} & \cdots & p^\gamma \end{pmatrix}.$$

From this formula, $S(p^\gamma)$, $\gamma < p$, is obtained as a special case.

Example: $m = 3^{11}$; $S(3^{11})$ as in § 4, leading to the chain: $1 \cdot \alpha_{x+27} \equiv l'$; $3 \cdot \alpha_{x+24} \equiv l'$; $3^2 \cdot \alpha_{x+21} \equiv l'$; $\cdots$; all modulo 3^{11}. Each congruence establishes, as in the last example, a large number of interrelations between the elements of the residue system modulo 3^{11} of any polynomial with integral coefficients.

(*d*) $m = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdots p_\nu^{\gamma_\nu}$. We define for general m the chain of congruences of the second kind in such manner as to make it also for this case clear that the signature of the second kind is represented by the same symbol as the signature introduced in § 4. We know from Theorem X, § 10, that for every divisor d of m exists a congruence

$$\frac{m}{d} \cdot \alpha_{x+\mu(d)} \equiv l \pmod{m}, \qquad \text{or} \qquad \Big\}\mu(d),\ \frac{m}{d}\Big\{_m,$$

corresponding to a congruence

[*] Here, as in the following congruences, it is only for special purposes sometimes of advantage to use the l' instead of the l. The accent may be omitted throughout. (See (c_1)).

$$\frac{m}{d}\cdot x^{\mu(d)} \equiv \psi(x) \pmod{m}, \qquad \text{or} \qquad \left\{\mu(d),\, \frac{m}{d}\right\}_m .$$

We define, always in analogy with §§ 3, 4, a "chain of residual congruences of the second kind," or, simply, a "chain" for m by the following

CONSTRUCTION: *For all divisors of* m, *namely* $d_0 = m, d_1, d_2, \cdots, d_r = 1$, *find the corresponding* $\mu(d)$ *and consider the couples of numbers* $\mu(d), m/d$. *Each of these couples leads to a residual congruence,* $\}\mu(d),\, m/d\{_m$. *If for two divisors,* d_ρ, d_σ *of* m, *we have* $\mu(d_\rho) = \mu(d_\sigma)$, *we retain only the larger of the divisors* d_ρ, d_σ, *ignoring the other. We finally obtain in this manner a set of congruences, one for each of the distinct values* $\mu(d_1), \mu(d_2), \cdots$, *and these, arranged in decreasing order of magnitude of the* μ, *are defined to form the "chain of residual congruences of the second kind modulo* m."

The operations which we have thus performed on the number m are identical with those of "Construction" § 3. We next define (as already indicated in (*b*), (*c*), (*d*), above) the signature of m of the second kind by the same symbol

$$S(m) = \begin{bmatrix} \mu(m) & \mu(d_1) & \cdots & \mu(d_i) & \cdots & \mu(d_r) \\ 1 & \dfrac{m}{d_1} & \cdots & \dfrac{m}{d_i} & \cdots & \dfrac{m}{d_r} \end{bmatrix}$$

used for the signature in § 4, and call the signature of the second kind again simply the "signature of m."

We are now in a position to state the result derived in the present section as follows:

THEOREM XI: *For any given modulus* m *we determine*

$$S(m) = \begin{bmatrix} \mu(m) & \mu(d_1) & \cdots & \mu(d_i) & \cdots & \mu(d_r) \\ 1 & \dfrac{m}{d_1} & \cdots & \dfrac{m}{d_i} & \cdots & \dfrac{m}{d_r} \end{bmatrix}$$

as explained in § 4. *The signature determines a chain of congruences, modulo* m,

$$1\cdot\left(\alpha_{x+\mu(m)} - \binom{\mu(m)}{1}\cdot\alpha_{x+\mu(m)-1} + \binom{\mu(m)}{2}\cdot\alpha_{x+\mu(m)-2} - + \cdots \pm \alpha_x\right) \equiv 0,$$

$$\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot$$

$$\frac{m}{d_i}\cdot\left(\alpha_{x+\mu(d_i)} - \binom{\mu(d_i)}{1}\cdot\alpha_{x+\mu(d_i)-1} + \binom{\mu(d_i)}{2}\cdot\alpha_{x+\mu(d_i)-2} - + \cdots \pm \alpha_x\right) \equiv 0,$$

$$\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot$$

$$\frac{m}{1}\cdot(\alpha_{x+1} - \alpha_x) \equiv 0,$$

*or, using the notation** *of Theorem X,* § 10,

* For many purposes, only the quantities $\mu(d_i)$ and m/d_i taken from our congruences are required, that is, exactly the information furnished by the signature. We also remember that in some cases the full congruences of Theorem XI may be simplified, as in (*b*), (*c*) of this section.

$$\frac{m}{d_i} \cdot \alpha_{x+\mu(d_i)} \equiv l \pmod{m} \qquad \textit{or} \qquad \Big\}\mu(d_i), \frac{m}{d_i}\Big\{_m \qquad (i = 0, 1, \cdots, \tau).$$

We have now proved that, while the signature of the second kind has an entirely different meaning from the signature as defined in Part I, yet they may be represented by the same symbol $S(m)$. Moreover, this symbol governs certain operations, notably the formation of the " chains of residual congruences " of Part I and of the " chains of residual congruences of the second kind," and, while these two kinds of chains have different meanings and deal with entirely different objects, yet the operations in the two cases are formally identical.

Example: $m = 5^4 \cdot 7^3$. $\mu(5^4 \cdot 7^3) = 21$,

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

$1 \cdot \alpha_{x+21} \equiv l$; $7 \cdot \alpha_{x+20} \equiv l$; $5 \cdot 7 \cdot \alpha_{x+15} \equiv l$; $5^2 \cdot 7 \cdot \alpha_{x+14} \equiv l$; $5^2 \cdot 7^2 \cdot \alpha_{x+10} \equiv l$; $5^3 \cdot 7^2 \cdot \alpha_{x+7} \equiv l$; $5^3 \cdot 7^3 \cdot \alpha_{x+5} \equiv l$, all modulo $5^4 \cdot 7^3$; or $\}21, 1\{$; $\}20, 7\{$; $\}15, 5 \cdot 7\{$; $\}14, 5^2 \cdot 7\{$; $\}10, 5^2 \cdot 7^2\{$; $\}7, 5^3 \cdot 7^2\{$; $\}5, 5^3 \cdot 7^3\{$ mod $5^4 \cdot 7^3$.

Similarly, the chain of congruences of the second kind for $m = 2^7 \cdot 3^4 \cdot 7^2$ may be read off immediately from $S(2^7 \cdot 3^4 \cdot 7^2)$, as given in § 4.

§ 12. Complete residue systems modulo m; the characteristic $C(m)$

We make use of the " chain of congruences " of the preceding paragraph in the following manner. For a given m let $\alpha_0, \alpha_1, \alpha_2, \cdots, \alpha_{m-1}$ be a residue system (that is $0 \leqq \alpha_i < m$, $f(i) \equiv \alpha_i \pmod{m}$, $f(x)$ a polynomial with integral coefficients). We divide by vertical bars our system into subsets containing respectively $\mu(d_\tau)$, $\mu(d_{\tau-1}) - \mu(d_\tau)$, $\mu(d_{\tau-2}) - \mu(d_{\tau-1})$, $\cdots$, $\mu(m) - \mu(d_1)$, $m - \mu(m)$ terms, starting from, and including, α_0:

$$\left|\begin{matrix} \alpha_0, \alpha_1 \cdots \alpha_{\mu(d_{\tau-1})-1} \\ \mu(d_{\tau-1}) \end{matrix}\right|\begin{matrix} \alpha_{\mu(d_{\tau-1})} \cdots \alpha_{\mu(d_{\tau-2})-1} \\ \mu(d_{\tau-2}) - \mu(d_{\tau-1}) \end{matrix}\Bigg| \cdots \Bigg|\begin{matrix} \alpha_{\mu(d_i)} \cdots \alpha_{\mu(d_{i-1})-1} \\ \mu(d_{i-1}) - \mu(d_i) \end{matrix}\Bigg|$$

$$\cdots \left|\begin{matrix} \alpha_{\mu(d1)} \cdots \alpha_{\mu(m)-1} \\ \mu(m) - \mu(d_1) \end{matrix}\right|\begin{matrix} \alpha_{\mu(m)} \cdots \alpha_{m-1} \\ m - \mu(m) \end{matrix}\Bigg|,$$

where the second line indicates the number of elements contained in each subset.

By the first congruence of our chain, $1 \cdot \alpha_{x+\mu(m)} \equiv l \pmod{m}$, every element after the $\mu(m)$th, that is, all elements $\alpha_{\mu(m)}, \alpha_{\mu(m)+1}, \cdots, \alpha_{m-1}$ are completely determined by the first $\mu(m)$ elements $\alpha_0, \cdots, \alpha_{\mu(m)-1}$, since, by assigning to x the value 0, we obtain from $\alpha_0, \cdots, \alpha_{\mu(m)-1}$ the value of $\alpha_{\mu(m)}$; then, from the same congruence, for $x = 1$, we obtain from $\alpha_1, \cdots, \alpha_{\mu(m)}$ the value of $\alpha_{\mu(m)+1}$, etc., such that any $\mu(m)$ consecutive elements determine all of the rest. By the second congruence $(m/d_1) \cdot \alpha_{x+\mu(d_1)} \equiv l \pmod{m}$, each of the $\mu(m) - \mu(d_1)$ elements $\alpha_{\mu(d_1)} \cdots \alpha_{\mu(m)-1}$ is *partly* determined by the $\mu(d_1)$ first elements, namely modulo d_1, so that, if the $\mu(d_1)$ first elements are fixed, each of the $\mu(m) - \mu(d_1)$ next elements have only m/d_1 among the values $0 \cdots m-1$ to range over. Similarly, by the third congruence, each of the $\mu(d_1) - \mu(d_2)$ elements $\alpha_{\mu(d_2)}, \cdots, \alpha_{\mu(d_1)-1}$ is determined modulo d_2, so that each has but m/d_2 of the values $0 \cdots m-1$ to range over. Finally, using each congruence in this way, the last one,* $(m/d_{\tau-1}) \cdot \alpha_{x+\mu(d_{\tau-1})} \equiv l$ mod m, tells us that, if the $\mu(d_{\tau-1})$ first elements $\alpha_0, \cdots, \alpha_{\mu(d_{\tau-1})}$ are known, then the next $\mu(d_{\tau-2}) - \mu(d_{\tau-1})$ elements, $\alpha_{\mu(d_{\tau-1})}, \cdots, \alpha_{\mu(d_{\tau-2})-1}$, are determined modulo $d_{\tau-1}$, leaving each one of these elements $m/d_{\tau-1}$ of the values $0, \cdots, m-1$ to range over.

We have so far subjected each element of the residue system following the first $\mu(d_{\tau-1})$ elements, that is, we have subjected each of the elements $\alpha_{\mu(d_{\tau-1})}$, $\alpha_{\mu(d_{\tau-1})+1}, \cdots, \alpha_{m-1}$, to *one* of the congruences of the chain. Thus, $\alpha_{\mu(d_{\tau-1})}$, $\cdots, \alpha_{\mu(d_{\tau-2})-1}$ have been subjected *only* to $\}\mu(d_{\tau-1}), m/d_{\tau-1}\{_m$; while similarly $\alpha_{\mu(d_{\tau-2})}, \cdots, \alpha_{\mu(d_{\tau-3})-1}$ have been subjected *only* to $\}\mu(d_{\tau-2}, m/d_{\tau-2}\{$; $\alpha_{\mu(d_{\tau-3})}, \cdots, \alpha_{\mu(d_{\tau-4})-1}$ only to $\}\mu(d_{\tau-3}), m/d_{\tau-3}\{$; and so forth. In reality, however, $\alpha_{\mu(d_{\tau-2})}, \cdots, \alpha_{\mu(d_{\tau-3})-1}$ are affected not only by $\}\mu(d_{\tau-2}), m/d_{\tau-2}\{$, but also by $\}\mu(d_{\tau-1}), m/d_{\tau-1}\{$; $\alpha_{\mu(d_{\tau-3})}, \cdots, \alpha_{\mu(d_{\tau-4})-1}$ are affected not only by $\}\mu(d_{\tau-3}), m/d_{\tau-3}\{$, but also by $\}\mu(d_{\tau-2}), m/d_{\tau-2}\{$ and $\}\mu(d_{\tau-1}), m/d_{\tau-1}\{$, etc. *We shall show*† *in* § 13 *that the* α_i *are not any farther restricted by these additional considerations*, so that:

the number of values among the numbers $0, 1, \cdots, m-1$ left available for each of $\alpha_{\mu(d_{\tau-1})}, \cdots, \alpha_{\mu(d_{\tau-2})-1}$, after $\alpha_0, \cdots, \alpha_{\mu(d_{\tau-1})-1}$ have been arbitrarily chosen (from $0, 1, \cdots, m-1$), is *exactly* $m/d_{\tau-1}$;

the number of values available for each of $\alpha_{\mu(d_{\tau-2})}, \cdots, \alpha_{\mu(d_{\tau-3})-1}$, after the $\alpha_0, \cdots, \alpha_{\mu(d_{\tau-1})-1}$ have been arbitrarily chosen and the $\alpha_{\mu(d_{\tau-1})}, \cdots$, $\alpha_{\mu(d_{\tau-2})-1}$ have been chosen subject to (1), is *exactly* $m/d_{\tau-2}$; etc.; generally:

the number of values available for $\alpha_{\mu(d_i)}, \cdots, \alpha_{\mu(d_{i-1})-1}$, after $\alpha_0, \cdots, \alpha_{\mu(d_{\tau-1})-1}$ have been arbitrarily chosen, after $\alpha_{\mu(d_{\tau-1})}, \cdots, \alpha_{\mu(d_{\tau-2})-1}$ have been chosen subject to (1), $\alpha_{\mu(d_{\tau-2})}, \cdots, \alpha_{\mu(d_{\tau-3})-1}$ subject to (2), etc., is *exactly* m/d_i.

We continue our discussion under the assumption of this at present not completely proved statement.

We are thus led, for any modulus m, to an arrangement of the following type, where in the first line the range of the index ν of the elements α_ν is given

* Omitting the trivial one $\}1, m/d_\tau\{$, $d_\tau = 1$.

† By proving that the present restrictions on the α_i are already sufficient to reduce the possible number of residue systems modulo m to its true number (see § 13, Theorem XIII, proof).

for each subset of the alpha's, while in the second line is entered for each subset the number of values over which each alpha of the subset is allowed to range:

$$\begin{array}{c|c|c|c|}
0\cdots\mu(d_{r-1})-1 & \mu(d_{r-1})\cdots\mu(d_{r-2})-1 & \cdots & \mu(d_i)\cdots\mu(d_{i-1})-1 \\
m & m/d_{r-1} & & m/d_i
\end{array}$$

$$\begin{array}{c|c|c}
\cdots & \mu(d_1)\cdots\mu(m)-1 & \mu(m)\cdots\cdot m-1 \\
 & m/d_1 & 1
\end{array}$$

We replace in the first line $0\cdots\mu(d_{r-1})-1$ by the number of elements contained in this subset, that is, by $\mu(d_{r-1})$, and similarly for the other subsets, and are led to the

Definition 10: *To every positive integer m corresponds a symbol $C(m)$, which we call the characteristic of m of the second kind, or, since it is represented by the same symbol which was introduced for the characteristic of* § 5, *simply the characteristic of m. $C(m)$ is defined as*

$$C(m)=\left(\begin{array}{c|c|c|c|}
\mu(d_{r-1}) & \mu(d_{r-2})-\mu(d_{r-1}) & \cdots & \mu(d_{i-1})-\mu(d_i) \\
m & m/d_{r-1} & & m/d_i
\end{array}\right.\cdot$$

$$\left.\begin{array}{c|c|c}
\cdots & \mu(d_1)-\mu(d_2) & \mu(m)-\mu(d_1) \\
 & m/d_2 & m/d_1
\end{array}\right).$$

In this symbol the first line gives the number of those elements of the residue system modulo m of any polynomial with integral coefficients which are contained in the successive subsets described above, while the lower line gives the number of numbers of the set $0, 1, 2, \cdots, m-1$ over which each element of the respective subset may range.

We know that $C(m)$ of Part I, and therefore also $C(m)$ of the present part, can be written down in all cases directly from $S(m)$, which, in turn, is derived from m by a simple and direct process.

§ 13. The number $N(m)$ of complete residue systems modulo m. Discussion of the totality of residue systems modulo m

Theorem XII: *For a given modulus m the number of residue systems $\alpha_0, \alpha_1, \cdots, \alpha_{m-1}$, $0 \leqq \alpha_i < m$, is $N(m)$.* (For definition of $N(m)$, see § 6.)

Proof: To every polynomial (with integral coefficients) corresponds *one* residue system $\alpha_0, \alpha_1, \cdots, \alpha_{m-1}$, and to no two *completely reduced* polynomials corresponds the same residue system unless corresponding coefficients be equal (or their difference would be a polynomial congruent to zero modulo m for all integral values of the argument, thus leading to a contradiction of Theorem IV of § 5 and the lines preceding the theorem. Therefore the number of residue systems modulo m is $N(m)$, the number of completely reduced polynomials.

THEOREM XIII: *A set of m integers* $\alpha_0, \cdots, \alpha_{m-1}$, $0 \leqq \alpha_i < m$, *forms a residue system modulo m of a polynomial with integral coefficients when and only when the chain of congruences of* § 11 *is satisfied.*

Proof: We know from § 12 that the condition is *necessary*. To show that it is also *sufficient*, we argue as follows:

(*a*) The true number of residue systems modulo m is $N(m)$ (Theorem XII).

(In particular, therefore, the formulæ of § 6 for $N(m)$ (for the general case as well as for the special cases) hold for the number of residue systems. We have thus a simple direct method of determining this number for any given modulus m.)

(*b*) We know that in the discussion of § 12 we have possibly left too large a range of values for the α_i, since we are not certain that we have exhausted the force of the chain of congruences $\}\mu(d_i), m/d_i\{$; therefore the number,—say $N'(m)$,—which we obtain by considering only the restrictions indicated in § 12, satisfies $N'(m) \geqq N(m)$ (the true number).

(*c*) It is easily shown that we obtain the right number $N(m)$ of residue systems by admitting just the congruential restrictions considered in § 12. We conclude this from the parallelism between the characteristic $C(m)$ of the first kind and the characteristic $C'(m)$ of the second kind. Both are denoted by

$$\left(\begin{array}{c|c|c|c|c|c} \mu(d_{r-1}) & \mu(d_{r-2}) - \mu(d_{r-1}) & \cdots & \mu(d_{i-1}) - \mu(d_i) & \cdots & \mu(m) - \mu(d_1) \\ m & m/d_{r-1} & & m/d_i & & m/d_1 \end{array}\right).$$

For the completely reduced polynomials we recall that $C(m)$ informs us that there are (certain) $\mu(d_{i-1}) - \mu(d_i)$ coefficients which range independently over m/d_i values $0, \cdots, (m/d_i) - 1$, thus leading to the expressions for $N(m)$ given in Theorem V. For the residue systems, $C(m)$ informs us that there are (certain) $\mu(d_{i-1}) - \mu(d_i)$ elements α which may each assume m/d_i values from among the numbers $0, \cdots, m-1$. These values are determined by the congruences of the chain. By referring to § 12, beginning, it is clear that we thus obtain exactly the expression obtained in § 6 for $N(m)$. Therefore $N'(m) = N(m)$.

(*d*) Therefore every one of the $N(m)$ sets $\alpha_0, \cdots, \alpha_{m-1}$ which are selected by our chain of congruences from among the m^m possible ways of selecting m elements each ranging over $0, 1, \cdots, m-1$, must be a residue system; that is, the congruences of the chain constitute also a *sufficient* condition for $\alpha_0, \cdots, \alpha_{m-1}$ to be a residue system, q.e.d.

This proof settles the desideratum of § 12, since, if the chain of congruences should imply any more restrictions on the α than we have admitted, the number of possible residue systems would be smaller than $N(m)$.

The preceding work also proves

THEOREM XIV: *A residue system modulo m is completely determined by its first $\mu(m)$ elements (or by any $\mu(m)$ consecutive elements (see § 8, end)); but these $\mu(m)$ elements are not independent of each other; they are related in the manner explained in § 12. A complete description of these interrelations is given by the characteristic $C(m)$.*

This method of constructing the totality of residue systems for a given modulus m is unsymmetrical in that it does not deal with all elements in the same fashion. But it should be kept in mind that no one element is qualitatively distinguished above the others, since, by replacing in the corresponding polynomial x by $x - a$, any element may be brought to any other position, through a cyclic interchange. In particular, if all residue systems modulo m were written one under another,

$$\begin{array}{cccc} \alpha_0 & \alpha_1 & \cdots & \alpha_{m-1} \\ \alpha_0' & \alpha_1' & \cdots & \alpha_{m-1}' \\ \cdot & \cdot & \cdot & \cdot \\ \alpha_0^{(N(m)-1)} & \alpha_1^{(N(m)-1)} & \cdots & \alpha_{m-1}^{(N(m)-1)}, \end{array}$$

there would be in each vertical column $N(m)/m$ zero's, $N(m)/m$ one's, $N(m)/m$ two's, etc., as is easily seen.

We insert a few simple remarks:

1. Assume $m = p_1 \cdot p_2 \cdots p_r$. We consider the congruences (Lemma 9, § 10)

$$\alpha_{x+p_i} \equiv \alpha_x \pmod{p_i} \qquad (i = 1, 2, \cdots, r).$$

By counting the number of systems $\alpha_0, \alpha_1, \cdots, \alpha_{m-1}$ which satisfy these congruences, we are led again to the number $N(m)$, so that we may add to Theorem XIII:

COROLLARY: *For $m = p_1 \cdot p_2 \cdots p_r$, the set $\alpha_0, \alpha_1, \cdots, \alpha_{m-1}$ form a residue system modulo m when and only when*

$$\alpha_k \equiv \alpha_{k+p_i} \equiv \alpha_{k+2p_i} \equiv \alpha_{k+3p_i} \equiv \cdots \pmod{p_i} \begin{pmatrix} k = 0, 1, \cdots, p_i - 1 \\ i = 1, 2, \cdots, r \end{pmatrix}.$$

Similarly, we may make use of Definition 9, § 11, for $m = p^\gamma$.

2. Assume $m = p$. In this case we have no problem. $N(p) = p^p$, and therefore every set $\alpha_0, \alpha_1, \cdots, \alpha_{p-1}, 0 \leqq \alpha_i < p$, is the residue system of exactly one completely reduced polynomial modulo p. (See § 11 (*a*)).

In all other cases (m npt a prime), we may not select the elements of our set at random from the numbers $0, 1, \cdots, m - 1$, and expect to have a residue system modulo m of a polynomial with integral coefficients, since $N(m) < m^m$ for m not prime* (§ 6).

3. For polynomials with *fractional* (including integral) *coefficients, but which give integral values for all integral x*—we denote for the moment such polynomials by $u(x)$—the following is obvious when one makes use of arithmetical progressions:

Given any set of m integers $\beta_0, \beta_1, \cdots, \beta_{m-1}$, there always exists a polynomial $u(x)$ of degree $\leqq m$ for which $u(i) = \beta_i$.

It is therefore, a fortiori, always possible to determine a polynomial $u(x)$ which has an assigned residue system for a modulus m.

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

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

$N(m) = 2^2 \cdot 3^3 \cdot 5^5 \cdot 11^{11}$. For the totality of residue systems modulo $2 \cdot 3 \cdot 5 \cdot 11$ we read off from $C(m)$:

Each of the first two elements α_0, α_1 (or any two consecutive elements) may have any one of the m values $0, 1, \cdots, m - 1$;

the one element α_2 may have any one of $11 \cdot 5 \cdot 3$ values which are determined from α_0, α_1 by a congruence of the chain;

each of the two elements α_3, α_4 may have any one of the $11 \cdot 5$ values which are determined from α_0, α_1, α_2 by a congruence of the chain;

each of the six elements α_5, α_6, α_7, α_8, α_9, α_{10} may have any one of the 11 values determined from α_0, α_1, α_2, α_3, α_4 by a congruence of the chain;

each of the remaining $330 - 11 = 319$ elements $\alpha_{11}, \cdots, \alpha_{329}$ is completely determined by the first eleven, $\alpha_0, \cdots, \alpha_{10}$.

Chain of congruences: }11, 1{; }5, 11{; }3, 11 · 5{; }2, 11 · 5 · 3{, all modulo $2 \cdot 3 \cdot 5 \cdot 11$; or (see Corollary above) $\alpha_{x+11} \equiv \alpha_x \bmod 11$; $\alpha_{x+5} \equiv \alpha_x \bmod 5$; $\alpha_{x+3} \equiv \alpha_x \bmod 3$; $\alpha_{x+2} \equiv \alpha_x \bmod 2$.

For the practical determination of the complete residue system modulo m, when a sufficient number of consecutive elements are given to uniquely characterize it, compare § 9.

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

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

$N(3^{11}) = 3^{162}$ (as compared with $(3^{11})^{3^{11}} = 3^{1948617}$ possible sets of 3^{11} elements chosen independently from $0, \cdots, 3^{11} - 1$).

The chain of congruences is (from $S(3^{11})$, see § 4) }27, 1{; }24, 3{; }21, 3^2{; ⋯; }6, 3^9{; }3, 3^{10}{, all modulo 3^{11}

Each of the first three elements of a residue system moduio 3^{11} may be arbitrarily chosen from the 3^{11} numbers $0, \cdots, 3^{11} - 1$; and, similarly, each element of the jth group of three elements may have any of the t_j values determined by the $(11 - j)$th congruence of the chain (not counting the trivial congruence), where $j = 1, 2, \cdots, 9$; $t_1 = 3^{11}$, $t_2 = 3^{10}$, $t_3 = 3^9$, $t_4 = 3^7$, $t_5 = 3^6$, $t_6 = 3^5$, $t_7 = 3^3$, $t_8 = 3^2$, $t_9 = 3^1$. The remaining $3^{11} - 27$ elements are then uniquely determined.

* For example, for $m = 5$, the set $0, 3, 1, 4, 2$, chosen at random, are the residue system of $0 \cdot x^4 + 0 \cdot x^3 + 0 \cdot x^2 + 3x + 0$, etc. But, modulo 4, there is no polynomial with integral coefficients of which, for example, $1, 0, 0, 2$ is the residue system.

† Compare examples in §§ 4, 6, 11.

Example. $m = 5^4 \cdot 7^3$:

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

$N(5^4 \cdot 7^3) = 5^{50} \cdot 7^{42}$ (as compared with $5^{857500} \cdot 7^{643125}$ possible combinations).

The first five elements may be assumed chosen at random; for the next two we may still choose from $5^3 \cdot 7^3$ numbers lying between $0,\ 5^4 \cdot 7^3 - 1$, etc.; in the set comprising the sixteenth to twentieth elements each element may be chosen from among $5 \cdot 7$ numbers; the twenty-first element may be chosen from 7 numbers; all the others ($5^4 \cdot 7^3 - 21$ in number) are then determined.

The chain of congruences may be written, from $S(5^4 \cdot 7^3)$ (compare § 4): $1 \cdot \alpha_{x+21} \equiv l$; $7 \cdot \alpha_{x+20} \equiv l$; $5 \cdot 7 \cdot \alpha_{x+15} \equiv l$; $5^2 \cdot 7 \cdot \alpha_{x+14} \equiv l$; $5^2 \cdot 7^2 \cdot \alpha_{x+10} \equiv l$; $5^3 \cdot 7^2 \cdot \alpha_{x+7} \equiv l$; $5^3 \cdot 7^3 \cdot \alpha_{x+5} \equiv l$, all modulo $5^4 \cdot 7^3$; or, in full:

$$1 \cdot \left(\alpha_{x+21} - \tbinom{21}{1} \cdot \alpha_{x+20} + \tbinom{21}{2} \cdot \alpha_{x+19} - \cdots - \alpha_x\right) \equiv 0,$$

$$7 \cdot \left(\alpha_{x+20} - \tbinom{20}{1} \cdot \alpha_{x+19} + \tbinom{20}{2} \cdot \alpha_{x+18} - \cdots + \alpha_x\right) \equiv 0,$$

$$\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot$$

$$5^3 \cdot 7^3 \cdot \left(\alpha_{x+5} - \tbinom{5}{1} \cdot \alpha_{x+4} + \tbinom{5}{2} \cdot \alpha_{x+3} - \cdots - \alpha_x\right) \equiv 0, \text{ all modulo } 5^4 \cdot 7^3.$$

As a last example, we select a number containing more than two distinct prime factors:

Example. $m = 2^7 \cdot 3^4 \cdot 7^2$: referring to § 6 for $C(2^7 \cdot 3^4 \cdot 7^2)$ and $S(2^7 \cdot 3^4 \cdot 7^2)$, we find $N(m) = 2^{40} \cdot 3^{27} \cdot 7^{21}$, and see that:

$\alpha_{0,1}$ may be assigned any values $0, \cdots, m-1$;
α_2 may be assigned any one of $2^6 \cdot 3^4 \cdot 7^2$ values;
α_3 " " " " " " $2^6 \cdot 3^3 \cdot 7^2$ " ;
$\alpha_{4,5}$ may each be assigned any of $2^4 \cdot 3^3 \cdot 7^2$ values;
α_6 may be assigned any one of $2^3 \cdot 3^2 \cdot 7^2$ values;
α_7 " " " " " " $2^3 \cdot 3^2 \cdot 7$ " ;
α_8 " " " " " " $3^2 \cdot 7$ " ;
$\alpha_{9,10,11,12,13}$ may each be assigned any of 7 values.

The remaining 508018 elements of the residue system are then uniquely determined.

In view of the results derived in §§ 8–13, we may say:

THEOREM XV: *The chain of residual congruences of the second kind, and likewise the symbols $S(m)$ and $C(m)$, are obtainable by means of simple rational operations and determine*

1. *the structure of the totality of complete residue systems modulo m of polynomials with integral coefficients;*
2. *the structure of the individual residue system modulo m of a polynomial with integral coefficients.*

IV. OUTLINE OF THE ISOMORPHISM BETWEEN POLYNOMIALS AND RESIDUE SYSTEMS

§ 14. Correspondence between completely reduced polynomials and complete residue systems.—Résumé

Our work up to the present point has established a close analogy between completely reduced polynomials on the one hand and complete residue systems on the other hand. The following definitions serve to emphasize this correspondence.

DEFINITION 11: *A completely reduced polynomial modulo* m, $c_0 + c_1 \cdot x + \cdots + c_{\mu(m)-1} \cdot x^{\mu(m)-1}$, *is denoted by its coefficients* $(c_0, c_1, \cdots, c_{\mu(m)-1})_m$, *where the coefficients of missing terms (also of the highest powers of* x, *if missing) are denoted by* 0.

A complete residue system modulo m, $\alpha_0, \alpha_1, \cdots, \alpha_{m-1}$, *is denoted by the* $\mu(m)$ *first elements* $[\alpha_0, \alpha_1, \cdots, \alpha_{\mu(m)-1}]_m$.

We know that to each $(c_0, c_1, \cdots, c_{\mu(m)-1})_m$ corresponds one and only one $[\alpha_0, \alpha_1, \cdots, \alpha_{\mu(m)-1}]_m$, in such manner that $\alpha_0, \alpha_1, \alpha_2, \cdots, \alpha_{m-1}$ form the residue system modulo m of $c_0 + c_1 x + c_2 x^2 + \cdots + c_{\mu(m)-1} \cdot x^{\mu(m)-1}$; and this polynomial is the only completely reduced polynomial modulo m to which belongs the residue system $\alpha_0, \alpha_1, \alpha_2, \cdots, \alpha_{m-1}$. This leads to

DEFINITION 12: *If* $[\alpha_0, \alpha_1, \alpha_2, \cdots, \alpha_{\mu(m)-1}]_m$ *is the residue system modulo* m *of the polynomial* $(c_0, c_1, c_2, \cdots, c_{\mu(m)-1})_m$, *we write*

$$(c_0, c_1, c_2, \cdots, c_{\mu(m)-1})_m \sim [\alpha_0, \alpha_1, \alpha_2, \cdots, \alpha_{\mu(m)-1}]_m,$$

or

$$[\alpha_0, \alpha_1, \alpha_2, \cdots, \alpha_{\mu(m)-1}]_m \sim (c_0, c_1, c_2, \cdots, c_{\mu(m)-1})_m,$$

and call the residue system and the polynomial equivalent (each to the other).

If we consider for a given m the totality of the $(c_0, c_1, c_2, \cdots, c_{\mu(m)-1})_m$ and the totality of the $[\alpha_0, \alpha_1, \alpha_2, \cdots, \alpha_{\mu(m)-1}]_m$, we see from our preceding work that the relations between the various $(c_0, c_1, c_2, \cdots, c_{\mu(m)-1})_m$ and the various $[\alpha_0, \alpha_1, \alpha_2, \cdots, \alpha_{\mu(m)-1}]_m$ are abstractly identical. To recapitulate (with the notation used throughout):

The first $\mu(d_{\tau-1})$ coefficients $c_0, c_1, \cdots, c_{\mu(d_{\tau-1})-1}$ may be selected at random from the numbers $0, 1, \cdots, m-1$, permitting repetition; similarly the first $\mu(d_{\tau-1})$ residues $\alpha_0, \alpha_1, \cdots, \alpha_{\mu(d_{\tau-1})-1}$ may be selected at random from the numbers $0, 1, \cdots, m-1$, permitting repetition;

and in the same manner:

any subset of $\mu(d_{i-1}) - \mu(d_i)$ coefficients $c_{\mu(d_i)}, \cdots, c_{\mu(d_{i-1})-1}$ may be selected at random from m/d_i numbers, namely from

$$0, 1, \cdots, (m/d_i) - 1 \qquad (i = 1, 2, \cdots, \tau);$$

any subset of $\mu(d_{i-1}) - \mu(d_i)$ residues $\alpha_{\mu(d_i)}, \cdots, \alpha_{\ (d_{i-1})-1}$ may be selected at random from m/d_i numbers, namely from the numbers of the set $0, 1, \cdots, m$ determined by the congruence $\alpha_{x+\mu(d_i)} \equiv l \bmod d_i$.

This isomorphism holds true to the last set of $\mu(m) - \mu(d_1)$ coefficients $c_{\mu(d_1)}, \cdots, c_{\mu(m)-1}$ and the set of $\mu(m) - \mu(d_1)$ elements of the residue system $\alpha_{\mu(d_1)}, \cdots, \alpha_{\mu(m)-1}$. All coefficients of the completely reduced polynomial are thereby determined, while the residue system is also determined because the $m - \mu(m)$ elements $\alpha_{\mu(m)}, \cdots, \alpha_{m-1}$ which are not represented in the symbol $[\alpha_0, \cdots, \alpha_{\mu(m)-1}]_m$ are uniquely determined by $\alpha_0, \cdots, \alpha_{\mu(m)-1}$.

RÉSUMÉ

MODULUS m

POLYNOMIALS — **RESIDUE SYSTEMS**

For every divisor d of m exists a congruence:

Residual congruence: § 2

$$\frac{m}{d} \cdot \Pi_{k=0}^{\mu(d)-1} (x - k) \equiv 0 \pmod{m},$$

or

$$\frac{m}{d} \cdot x^{\mu(d)} \equiv \psi(x) \pmod{m}$$

or

$$\left\{ \mu(d), \frac{m}{d} \right\}_m.$$

Residual congruence (second kind): § 10

$$\frac{m}{d} \cdot \sum_{i=0}^{\mu(d)} \binom{\mu(d)}{i} \cdot \alpha_{x+\mu(d)-i} \equiv 0 \pmod{m},$$

or

$$\frac{m}{d} \cdot \alpha_{x+\mu(d)} \equiv l \pmod{m}$$

or

$$\Big\} \mu(d), \frac{m}{d} \Big\{_m.$$

Signature of m: § 4

$$S(m) = \begin{pmatrix} \mu(m) & \cdots & \mu(d_i) & \cdots & \mu(d_\tau) \\ 1 & \cdots & m/d_i & \cdots & m/d_\tau \end{pmatrix}.$$

Signature of m (second kind): § 11

$$S(m) = \begin{pmatrix} \mu(m) & \cdots & \mu(d_i) & \cdots & \mu(d_\tau) \\ 1 & \cdots & m/d_i & \cdots & m/d_\tau \end{pmatrix}.$$

Chain of residual congruences: § 3

$$\frac{m}{d_i} \cdot x^{\mu(d_i)} \equiv \psi(x) \pmod{m};$$

or

$$\left\{ \mu(d_i), \frac{m}{d_i} \right\}_m \quad (i=0, 1, 2, \cdots, \tau).$$

Chain of residual congruences (second kind): § 11

$$\frac{m}{d_i} \cdot \alpha_{x+\mu(d_i)} \equiv l \pmod{m};$$

or

$$\Big\} \mu(d_i), \frac{m}{d_i} \Big\{_m \quad (i=0, 1, 2, \cdots, \tau).$$

Characteristic of m: § 5 — *Characteristic of m (second kind):* § 12

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

Completely reduced polynomial: §§ 5, 14

$$c_0 + c_1 \cdot x + \cdots + c_{\mu(m)-1} \cdot x^{\mu(m)-1} = (c_0, c_1, \cdots, c_{\mu(m)-1})_m$$

Complete residue system: §§ 12, 14

$$\alpha_0, \alpha_1, \cdots, \alpha_{\mu(m)-1}, \alpha_{\mu(m)}, \cdots, \alpha_{m-1} = [\alpha_0, \alpha_1, \cdots, \alpha_{\mu(m)-1}]_m$$

$$(c_0, c_1, \cdots, c_{\mu(m)-1})_m \quad \backsim \quad [\alpha_0, \alpha_1, \cdots, \alpha_{\mu(m)-1}]_m$$

Number of completely reduced polynomials: § 6

$$N(m).$$

Number of complete residue systems: § 13

$$N(m).$$

UNIVERSITY OF ILLINOIS,
URBANA, ILLINOIS