POLYNOMIALS OF SEVERAL VARIABLES AND THEIR RESIDUE SYSTEMS*

BY

AUBREY J. KEMPNER

INTRODUCTION

This paper gives an extension to polynomials of more than one variable of the theory of residue systems of a polynomial of a single variable.† The methods employed are similar to those of the earlier paper, which we shall therefore use freely and refer to as R. I.

All letters involved denote rational integers.

We recall the following definitions and facts.

A polynomial $f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n$ was called residually congruent zero modulo m, $f(x) \equiv 0 \pmod{m}$, when for all rational integral values of x we have $f(x) \equiv 0 \pmod{m}$. Similarly $f_1(x) \equiv f_2(x) \pmod{m}$, for two polynomials $f_1(x)$, $f_2(x)$, was defined.

For a positive integer m, $\mu(m)$ or μ_m denoted the smallest positive integer such that $\mu_m! \equiv 0 \pmod{m}$.

For a given modulus m we constructed, by a simple arithmetical process, the *signature* of m, $S(m)$ which depends on m alone,

$$S(m) = \begin{pmatrix} \mu(m) & \mu(d_1) & \cdots & \mu(d_i) & \cdots & \mu(d_{\tau-1}) & \mu(d_\tau) = 0 \\ m/d_0 = 1 & m/d_1 & \cdots & m/d_i & \cdots & m/d_{\tau-1} & m/d_\tau = m \end{pmatrix},$$

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

From $S(m)$ we could write down $C(m)$, the *characteristic* of m,

$$C(m) = \left(\begin{matrix} \mu(d_{\tau-1}) \\ m \end{matrix} \middle| \begin{matrix} \mu(d_{\tau-2}) - \mu(d_{\tau-1}) \\ m/d_{\tau-1} \end{matrix} \middle| \begin{matrix} \mu(d_{\tau-3}) - \mu(d_{\tau-2}) \\ m/d_{\tau-2} \end{matrix} \middle| \cdots \middle| \begin{matrix} \mu(m) - \mu(d_1) \\ m/d_1 \end{matrix}\right).$$

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

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

---

* Presented to the Society, December 26, 1924.

† Kempner, these Transactions, vol. 22 (1921), pp. 1-48.

‡ Or $(i = 0, 1, \cdots, \tau - 1)$, the congruence corresponding to $i = \tau$ being trivial.

that is, a set of congruences of the form

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

where $\psi(x)$ is a polynomial of degree $<\mu(d_i)$ with integral coefficients in more condensed notation, simply $\{\mu(d_i), m/d_i\}$. We also saw that it was sufficient, in considering residual congruences $a_0 x^k + a_1 x^{k-1} + \cdots + a_k \equiv 0 \pmod{m}$, to restrict a_0 to the divisors of m, including $a_0 = 1$ and $a_0 = m$.

Finally, this chain of congruences has the property that if there is any other residual congruence $cx^\nu \equiv \varphi(x) \pmod{m}$, where c is a divisor of m, then there is in our chain always a congruence for which either $c = m/d_i$, $\nu = \mu(d_i)$, or $c > m/d_i$, $\nu = \mu(d_i)$, or $c = m/d_i$, $\nu > \mu(d_i)$, or $c > m/d_i$, $\nu > \mu(d_i)$. We expressed this fact by saying that for every possible residual congruence modulo m there is in the chain a congruence which is not weaker than it. Its meaning is that every other residual congruence modulo m is a consequence of the congruences of the chain.

Reduced polynomials

1. **Definition.** *We call a polynomial $f(x_1, \cdots, x_k)$ residually congruent modulo m to another polynomial $\varphi(x_1, \cdots, x_k)$, $f \equiv \varphi \pmod{m}$, when for all sets of rational integral values of $x_1, \cdots, x_k$ we have $f \equiv \varphi \pmod{m}$.*

Lemma I. *For a given modulus m and any number k of variables, there exist polynomials $f(x_1, \cdots, x_k) \equiv 0 \pmod{m}$, f of the form $1 \cdot x_1^{\mu(m)} + \cdots + 1 \cdot x_k^{\mu(m)} + \varphi(x_1, \cdots, x_k)$, where φ is of degree $<\mu_m$ in each variable.*

Proof. For one variable, compare R. I, Lemma V. Let $f(x)$ be such a polynomial, then consider, for example, $f(x_1) + \cdots + f(x_k)$.

Our process of reduction of polynomials of more than one variable is carried out in the following manner.

For a given m, and k variables, we shall obviously have the following residual congruences, at least: For x_1, the τ congruences

$$\frac{m}{d_i} \cdot \prod_{j=0}^{\mu(d_i)-1} (x_1 - j) \equiv 0 \pmod{m} \quad (i = 0, 1, \cdots, \tau - 1)$$

or, as we also write, $\{\mu(d_i), m/d_i\}$ or $\{\mu(d_i), m/d_i\}_{x_1}$. Similarly, for each x_ν, $\{\mu(d_i), m/d_i\}_{x_\nu}$.

We first show how far a given polynomial in $x_1, \cdots, x_k$ may be reduced by these congruences; then we shall show that no further reduction is

possible, thus proving that all other conceivable residual congruences modulo m are implied by—that is, are consequences of—the congruences

$$\text{I} \qquad \{\mu(d_i),\ m/d_i\}_{x_\nu} \qquad (i = 0, 1, \cdots, \tau - 1;\ \nu = 1, \cdots, k).$$

For this reason we shall call the $k \cdot \tau$ congruences I a chain of residual congruences modulo m for k variables.

Assume first in our polynomial a term of type $cx_1^{\alpha_1} \cdots x_k^{\alpha_k}$, where at least one of the exponents $\alpha_1, \cdots, \alpha_k \geqq \mu(m)$. Assume, for example, α_1 to be the largest of these exponents, in case there is a largest one, or one of the largest, if two or more are equal. We then depress $cx_1^{\alpha_1} \cdots x_k^{\alpha_k}$ by applying $\{\mu(m),\ m/m = 1\}_{x_1}$, and similarly for each exponent which is $\geqq \mu(m)$.

We thereby obtain as a first step the following reduction.

LEMMA II. *For any given polynomial $f(x_1, \cdots, x_k)$ there exists at least one polynomial $g(x_1, \cdots, x_k)$ satisfying the conditions*

(1) $f \equiv g \pmod m$;

(2) *g is of degree at most $\mu_m - 1$ in each variable separately, and consequently of total degree at most $k \cdot \mu_m - k$;*

(3) *each coefficient of g has one of the values $0, 1, \cdots, m-1$.*

This is accomplished by the sole use of the congruences $\{\mu(m), 1\}$, written for $x_1, \cdots, x_k$ separately. We examine next the influence of the remaining congruences $\{\mu(d_i),\ m/d_i\}_{x_j}$, $i > 0$.

Our polynomial has now no term with exponents $\geqq \mu(m)$. We select a term, if there be any such, in which there is at least one exponent λ, $\mu(m) > \lambda \geqq \mu(d_1)$. Assume for example β_1 in $ex_1^{\beta_1} \cdots x_k^{\beta_k}$ to be such an exponent. Using $\{\mu(d_1),\ m/d_1\}_{x_1}$, we reduce all such powers of x_1 to the power $x_1^{\mu(d_1)}$ and lower powers, and the coefficient e to one of the values $0, 1, \cdots, m/d_1 - 1$. Similarly we reduce all powers of $x_2, \cdots, x_k$ which have exponents between $\mu(m)$ (exclusive) and $\mu(d_1)$ (inclusive). We continue in the same manner for all exponents between $\mu(d_1)$ (exclusive) and $\mu(d_2)$ (inclusive), using the congruence $\{\mu(d_2),\ m/d_2\}_{x_j}$; etc. We shall finally reach the following result (compare R. I, § 5):

THEOREM I. *Assume any polynomial $f(x_1, \cdots, x_k)$. Then there exists at least one polynomial*

$$g(x_1, \cdots, x_k) = \sum_{i_k=0}^{\lambda_k} \cdots \sum_{i_1=0}^{\lambda_1} a_{i_1 i_2 \cdots i_k} x_1^{i_1} \cdots x_k^{i_k}$$

for which

(1) $f \equiv g \pmod m$,

(2) $\lambda_j \leqq \mu(m) - 1 \quad (j = 1, \cdots, k)$,

(3) $a_{i_1 \cdots i_k}$ $(i_1 = 0, 1, \cdots, \mu(d_{\tau-1}) - 1; \cdots; i_k = 0, 1, \cdots, \mu(d_{\tau-1}) - 1)$

has a value $0, 1, \cdots, m-1$,

(4) $a_{i_1 \cdots i_k}$ $(i_1, \cdots, i_k = \mu(d_{\tau-1}), \cdots, \mu(d_{\tau-2}) - 1)$

has a value $0, 1, \cdots, m/d_{\tau-1} - 1$,

. . . . . .

(5) $a_{i_1 \cdots i_k}$ $(i_1, \cdots, i_k = \mu(d_1), \cdots, \mu(m) - 1)$

has a value $0, 1, \cdots, m/d_1 - 1$.

2. **Definition.** *Polynomials satisfying* (2), (3), (4), (5) *of Theorem* I *we call completely reduced modulo* m.

We wish to show that our reduction is complete in this sense:

THEOREM II. *Every polynomial is residually congruent modulo* m *to exactly one completely reduced polynomial.*

Before entering upon the proof, we recall that we have in the proof of Theorem I exactly exhausted the force of the congruences I. Therefore in agreement with our definition in R. I (§ 3, and § 4, Theorem III) the uniqueness theorem just stated is equivalent to

THEOREM III. *The congruences* I *form a chain of residual congruences modulo* m *for* k *variables.*

Proof. Our theorem is obviously of the same content as the following statement: If $g_1 = \sum \cdots \sum a_{i_1 \cdots i_k} x_1^{i_1} \cdots x_k^{i_k}$ and $g_2 = \sum \cdots \sum b_{i_1 \cdots i_k} x_1^{i_1} \cdots x_k^{i_k}$ are two completely reduced polynomials modulo m, then $g_1 \equiv g_2$ when and only when $a_{i_1 \cdots i_k} = b_{i_1 \cdots i_k}$ for all $i_1, \cdots, i_k$, that is, $g = g_1 - g_2$ is $\equiv 0$ only when all coefficients vanish.

If there should exist any additional residual congruence modulo m which is not implied by the congruences I, then the application of these congruences to it will show that it may be reduced to the form $f(x_1, \cdots, x_k) \equiv 0 \pmod{m}$, where

(1) the highest degree of any x_j which occurs is exactly one of the $\mu(d_i)$,

(2) each term containing this $x_j^{\mu(d_i)}$ will have its coefficient $= 0, 1, \cdots, m/d_i - 1$.

These properties are suffiicient to enable us to argue precisely as in R. I for polynomials of a single variable. Pages 9, 10 of the former paper carry over with only natural modifications, and need not be reprinted. Theorem II and III are thus proved.

3. For the case of two variables, x_1, x_2, a geometrical scheme for exhibiting the character of the completely reduced polynomials is easily devised:

We arrange the coefficients of any completely reduced polynomial modulo m, $f = \sum \sum a_{ij} x_1^i x_2^j$ in a rectangular array

$$\begin{array}{cccc} a_{00} & a_{10} & \cdots & a_{\mu(m)-1,\,0} \\ a_{01} & a_{11} & \cdots & a_{\mu(m)-1,\,1} \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ a_{0,\,\mu(m)-1} & a_{1,\,\mu(m)-1} & \cdots & a_{\mu(m)-1,\,\mu(m)-1}. \end{array}$$

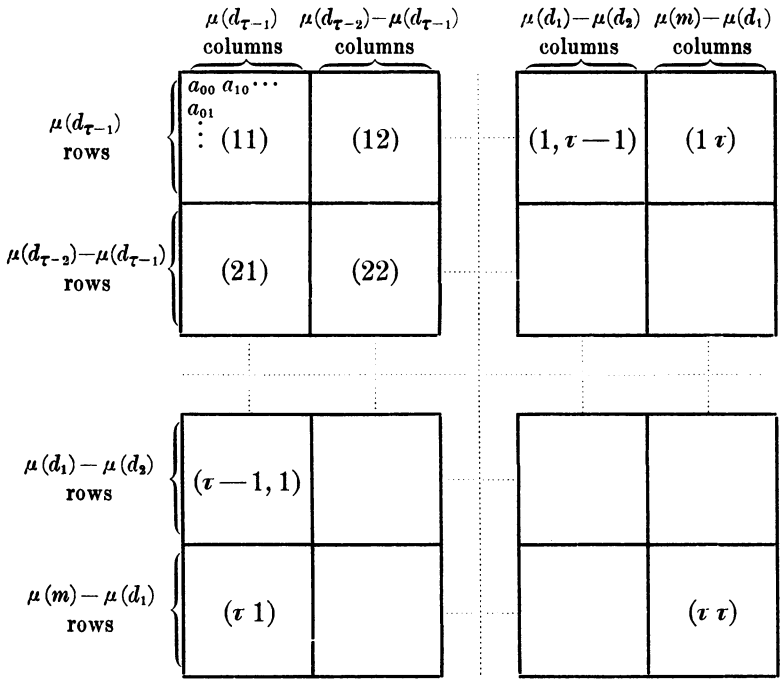

Fig. 1

If we denote by (s, t) the sth horizontal and tth vertical of the rectangular blocks into which our array is broken up, then each of the $[\mu(d_{\tau-1})]^2$ coefficients a_{ij} lying in $(1, 1)$ has one of the m values $0, 1, \cdots, m-1$; each of the $\mu^2 d_{\tau-2} - \mu^2 d_{\tau-1}$* coefficients in $(1, 2)+(2, 2)+(2, 1)$ has one of the $m/d_{\tau-1}$ values $0, 1, \cdots, m/d_{\tau-1}-1$; each of the $\mu^2 d_{\tau-3} - \mu^2 d_{\tau-2}$ coefficients in $(1, 3)+(2, 3)+(3, 3)+(3, 2)+(3, 1)$ has one of the $m/d_{\tau-2}$ values $0, 1, \cdots, m/d_{\tau-2}-1$, etc.; finally, each of the $\mu^2 m - \mu^2 d_1$ coefficients in $(1, \tau)+(2, \tau)+\cdots+(\tau, \tau)+(\tau, \tau-1)+\cdots+(\tau, 1)$ has one of the values $0, 1, \cdots, m/d_1-1$.

The array of Fig. 1 is clearly determined by the characteristic $C(m)$.

This geometrical representation extends in an obvious manner to a space of k dimensions for the case of k variables.

* Writing $\mu^2 d_{\tau-1}$ for $[\mu(d_{\tau-1})]^2$, etc.

We illustrate the definition of a completely reduced polynomial by a very simple example.

EXAMPLE. $m = 2^2 \cdot 3$, $\mu(12) = 4$; $S(12) = \begin{pmatrix} 4 & 3 & 2 \\ 1 & 2 & 6 \end{pmatrix}$; $C(12) = \left(\begin{array}{c|c|c} 2 & 1 & 1 \\ 12 & 6 & 2 \end{array}\right)$;

$$\left(\begin{array}{cc|c|c} a_{00} & a_{10} & a_{20} & a_{30} \\ a_{01} & a_{11} & a_{21} & a_{31} \\ \hline a_{02} & a_{12} & a_{22} & a_{32} \\ \hline a_{03} & a_{13} & a_{23} & a_{33} \end{array}\right),$$

where $a_{00}, a_{10}, a_{01}, a_{11}$ may have any value $0, 1, \cdots, 11$; $a_{20}, a_{21}, a_{22}, a_{12}, a_{02}$ may have any value $0, 1, \cdots, 5$; $a_{30}, a_{31}, a_{32}, a_{33}, a_{23}, a_{13}, a_{03}$ may have either of the values $0, 1$.

For a simple numerical case the reduction of a given polynomial to a completely reduced polynomial is carried out as follows:

EXAMPLE. $f(x_1, x_2) = 29x_1^6 x_2^5 + 7x_1^5 + 10x_1^2 x_2$, $m = 12$.

As chain of congruences we choose $x_1(x_1 - 1)(x_1 - 2)(x_1 - 3) \equiv 0$, $2x_1(x_1 - 1)(x_1 - 2) \equiv 0$, $6x_1(x_1 - 1) \equiv 0 \pmod{12}$, and similar congruences for x_2. We find easily

$$29x_1^6 x_2^5 \equiv x_1^2 x_2^3 - 2x_1^2 x_2 - 6x_1 x_2; \; 7x_1^5 \equiv x_1^3 + 6x_1; \; 10x_1^2 x_2 \equiv 4x_1^2 x_2 + 6x_1 x_2;$$

and thus $f(x_1, x_2) \equiv x_1^2 x_2^3 + 2x_1^2 x_2 + x_1^3 + 6x_1$, with the arrangement of coefficients

$$\left(\begin{array}{ccc|c} 0 & 6 & 0 & 1 \\ 0 & 0 & 2 & 0 \\ \hline 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 1 & 0 \end{array}\right)$$

which agrees with our definition of completely reduced polynomials.

4. Collecting results, we have

THEOREM IV. *For a given modulus m, and k variables $x_1, \cdots, x_k$, the signature $S(m)$ determines a chain of residual congruences* I, $\{\mu(d_i), m/d_i\}_{x_j}$. *These congruences reduce any polynomial $f(x_1, \cdots, x_k)$ to a completely reduced polynomial $g(x_1, \cdots, x_k)$. The structure of this polynomial is completely determined by the characteristic $C(m)$. The reduction is unique.*

In particular, from $S(p) = \begin{pmatrix} p \\ 1 \end{pmatrix}$ and $C(p) = \left(\left|\begin{matrix} p \\ p \end{matrix}\right|\right)$ for p a prime, it follows that for this case there is no restriction on the completely reduced polynomial beyond the obvious one that the degree of each variable is $\leq p - 1$. The coefficients range independently over $0, 1, \cdots, p - 1$. In all other cases we have restrictions of a very strong character.

5. It is now a simple matter to read off, for a given m, from the schedule of coefficients of the completely reduced polynomials, or from $C(m)$, the total number, $N = N(m)$, of such polynomials.

For two variables, we have $\mu^2 d_{\tau-1}$ coefficients which may assume independently each of m values, then $\mu^2 d_{\tau-1} - \mu^2 d_{\tau-2}$ coefficients which assume each $m/d_{\tau-1}$ values, etc., down to $\mu^2 d_1 - \mu^2 d_2$ coefficients each assuming m/d_2 values, and, finally, $\mu^2 m - \mu^2 d_1$ coefficients, each assuming m/d_1 values. We find, altogether (compare R. I, Theorem V),

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

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

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

For polynomials of k variables, we obtain in the same manner

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

The following are special cases.

COROLLARY. (a) *for* $m = p$, *a prime, there are no relations between the coefficients, and* $N = p^{(p^k)}$;

(b) *for* $m = p_1 \cdot p_2 \cdots p_s$, $N = p_1^{p_1^k} \cdots p_s^{p_s^k}$;

(c) *for* $m = p^\lambda$, $\lambda < p$,*

$$N = p^{p^k[1^k \cdot \lambda + (2^k - 1^k)(\lambda - 1) + (3^k - 2^k)(\lambda - 2) + \cdots + (\lambda^k - (\lambda-1)^k) \cdot 1]}.$$

RESIDUE SYSTEMS

6. We turn our attention to the individual residue systems modulo m of polynomials of more than one variable. We shall again find the rather remarkable isomorphism between the structure of the totality of the residue systems and the totality of the completely reduced polynomials which we encountered in R. I. We recall the main argument used in this connection in R. I. Defining a residue system of $f(x)$, modulo m, as the set of smallest non negative residues of $f(0)$, $f(1)$, $\cdots$, $f(m-1)$, taken in the order indicated, we saw that certain congruential relations exist between these m numbers; it was then easy to show that these relations are just sufficient to cut down the number m^m of sets which we should have if each residue assumed unrestrictedly all values $0, 1, \cdots, m-1$, to the number $N(m)$ of

* For the restriction $\lambda < p$, compare R. I, Theorem V.

completely reduced polynomials. From this followed that the set of all residue systems modulo m is obtained by taking into account exactly the congruential relations mentioned above.*

7. For

$$C(m) = \left(\begin{matrix}\mu(d_{\tau-1}) \\ m\end{matrix}\middle|\begin{matrix}\mu(d_{\tau-2})-\mu(d_{\tau-1}) \\ m/d_{\tau-1}\end{matrix}\middle|\cdots\middle|\begin{matrix}\mu(m)-\mu(d_1) \\ m/d_1\end{matrix}\right)$$

and one variable the residue system possesses the following structure (writing c_i for the smallest non-negative residue of $f(i)$):

$$c_0 \cdots c_{\mu(d_{\tau-1})-1} \mid c_{\mu(d_{\tau-1})} \cdots c_{\mu(d_{\tau-2})-1} \mid \cdots \mid c_{\mu(d_2)} \cdots c_{\mu(d_1)-1} \mid c_{\mu(d_1)} \cdots c_{\mu(m)-1} \mid c_{\mu(m)} \cdots c_{m-1}.$$

The first group of $\mu(d_{\tau-1})$ residues may be chosen arbitrarily, i. e., each one may range independently over the values $0, 1, \cdots, m-1$. The second set, of $\mu(d_{\tau-2}) - \mu(d_{\tau-1})$ residues, are then no longer quite unrestricted; as a result of the congruential relations between the elements of the residue system, each one of this set may assume independently any value among certain $m/d_{\tau-1}$ of the numbers $0, 1, \cdots, m-1$; the elements of the third set, of $\mu(d_{\tau-3}) - \mu(d_{\tau-2})$ residues, are then more strongly restricted: each of these may assume independently any among certain $m/d_{\tau-2}$ of the numbers $0, 1, \cdots, m-1$, etc. Each of the $\mu(m) - \mu(d_1)$ elements of the last set but one may still assume independently any among certain m/d_1 of the numbers $0, 1, \cdots, m-1$, and, finally, all the $m - \mu(m)$ residues of the last set are uniquely determined. On account of the fact mentioned last, it is, in any symbolic notation for a residue system, unnecessary to consider more than the first $\mu(m)$ elements.

The congruential relations between the elements of the residue system, which determine the structure of the system, are of the following type (R. I, Theorem X):

For any modulus m and any factor d of m (including $d = m$ and $d = 1$) there exists a "*residual congruence*"

$$\frac{m}{d}\left[c_{x+\mu(d)} - \binom{\mu(d)}{1} c_{x+\mu(d)-1} + \binom{\mu(d)}{2} c_{x+\mu(d)-2} - \cdots \pm c_x\right] \equiv 0 \pmod{m},$$

which we also denote by $\}\mu(d),\ m/d\{$, or $(m/d)\cdot c_{x+\mu(d)} \equiv l \pmod{m}$, where l indicates some linear function of $c_{x+\mu(d)-1}, \cdots, c_x$, with integral coefficients in which we are not interested.

* Compare R. I, §§ 10-13.

From the signature $S(m)$ we read off a chain of residual congruences, all modulo m,

$$(m/d_i)\cdot c_{x+\mu(d_i)} \equiv l \pmod m, \quad \text{or} \quad \}\,\mu(d_i),\ m/d_i\,\{ \qquad (i=0,1,\cdots,\tau-1).$$

The congruences of this chain just exhaust the relations which exist between the elements of a residue system.

8. **Two variables,** $k=2$. We define our residue system to be the system of integers

$$\begin{array}{cccc} c_{00} & c_{10} & \cdots & c_{m-1,0} \\ c_{01} & c_{11} & \cdots & c_{m-1,1} \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ c_{0,m-1} & c_{1,m-1} & \cdots & c_{m-1,m-1}, \end{array}$$

where c_{ij} is the smallest non-negative residue modulo m of $f(i,j)$. We shall then have in the jth row the residues of a polynomial in x alone, $f(x,j)$, and similarly in the ith column the residues of a polynomial in y alone, $f(i,y)$. Therefore we shall certainly have in each row and each column separately the same structure as for a polynomial in one variable.

Thinking of $f(x,y)$ as a polynomial in x alone, we shall have for our residue system a structure which will be sufficiently clearly indicated by Fig. 2 (where only a first index i has been inserted instead of c_{ij}), but thinking of $f(x,y)$ as a polynomial in y alone, we shall have a structure as represented by Fig. 3 (with second index j inserted instead of c_{ij}). Treating next x, y as varying independently of each other, the two structures will be in a certain sense superimposed, and we shall have an arrangement as in Fig. 4.

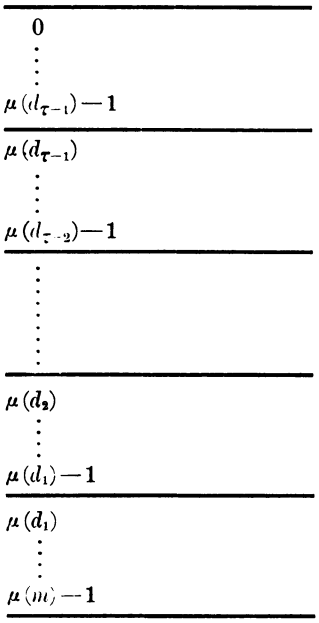

Fig. 3

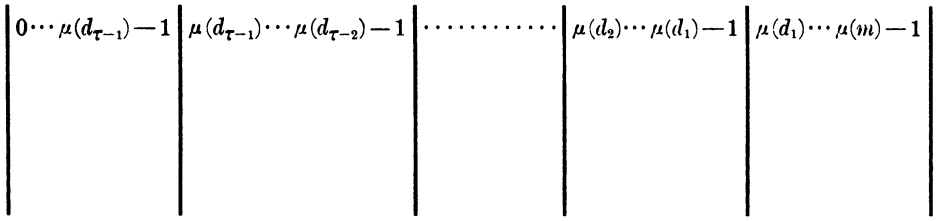

Fig. 2

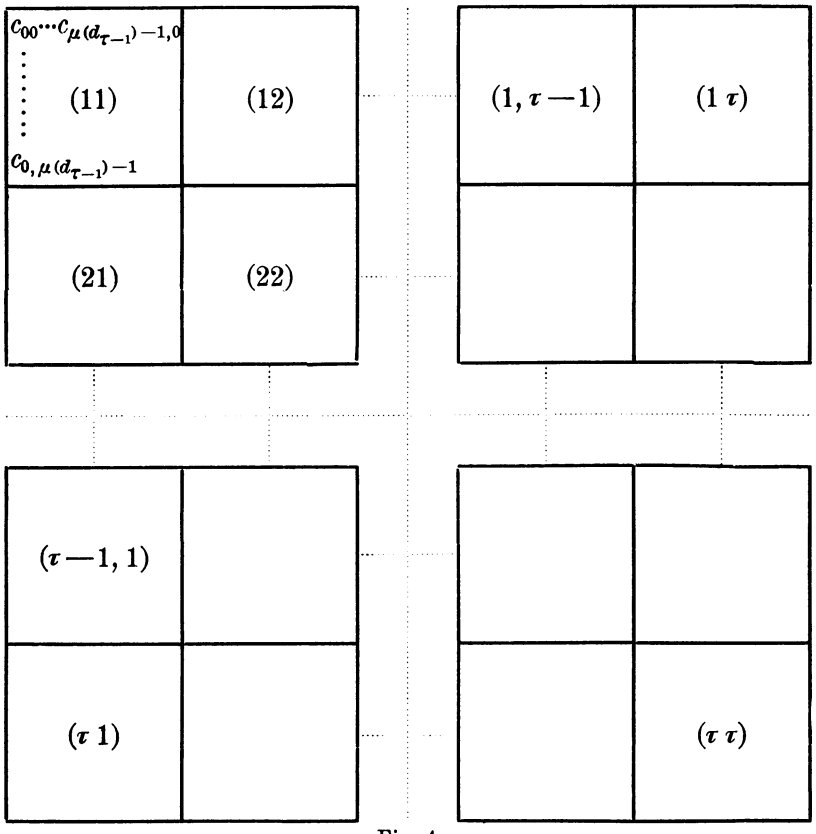

Fig. 4

In this figure we may expect the following state of affairs:

(1) all c_{ij} in (1, 1), i.e., all $c_{ij}(i, j = 0, \cdots, \mu(d_{\tau-1})-1)$ may unrestrictedly have any value $0, 1, \cdots, m-1$;

(2) all c_{ij} in (1, 2), (2, 2), (2, 1), i.e., all c_{ij} $(i, j = \mu(d_{\tau-1}), \cdots, \mu(d_{\tau-2})-1)$ may have any of certain $m/d_{\tau-1}$ values among $0, 1, \cdots, m-1$. The numbers from which these c_{ij} may be chosen may be expected to be determined by the choice of the c_{ij} of (1, 1);

(3) similarly for any "fringe" $(1, s)+(2, s)+\cdots+(s-1, s)+(s, s)+(s, s-1)+\cdots+(s, 1)$. For the arrangement, compare Fig. 1 and text.

The system of residual congruences modulo m, as far as they are represented by our work up to the present point, will be the following:

$\mu(m)\cdot\tau$ congruences

$$\frac{m}{d_i}\left[c_{x+\mu(d_i),j}-\binom{\mu(d_i)}{1}c_{x+\mu(d_i)-1,j}+\binom{\mu(d_i)}{2}c_{x+\mu(d_i)-2,j}-\cdots\pm c_{xj}\right]\equiv 0 \pmod m$$

$$(i = 0, 1, \cdots, \tau-1;^{*}\ j = 0, 1, \cdots, \mu(m)-1);$$

* Since $i = \tau$ leads to a trivial congruence.

$\mu(m)\cdot\tau$ congruences

$$\frac{m}{d_j}\left[c_{i,x+\mu(d_j)}-\binom{\mu(d_j)}{1}c_{i,x+\mu(d_j)-1}+\binom{\mu(d_j)}{2}c_{i,x+\mu(d_j)-2}-\cdots\pm c_{ix}\right]\equiv 0 \pmod m$$
$$(j=0,1,\cdots,\tau-1;\ i=0,1,\cdots,\mu(m)-1).$$

We want next to show that this system of $2\mu(m)\cdot\tau$ congruences is complete in the sense that all other relations existing between the elements of a residue system are implied by it. The question of how far the $2\mu(m)\cdot\tau$ congruences are independent would be easily settled, but is not of interest for our purposes. That they are not independent is obvious.

We prove the completeness of the set of congruences in this manner (compare R. I, p. 43):

I. The number of residue systems must be $N(m)$;

II. The structure of the residue system, as determined by the chain of residual congruences above, gives exactly $N(m)$ systems (in block (1,1) there are $\mu^2 d_{\tau-1}$ numbers c_{ij}, each of which may assume independently m values; in blocks $(1,2)+(2,2)+(2,1)$ there are $\mu^2 d_{\tau-2}-\mu^2 d_{\tau-1}$ numbers, each of which has one of $m/d_{\tau-1}$ values, etc.; compare the argument of § 5).

9. **Three or more variables, $k\geqq 3$.** The work is extended in an obvious manner. We omit the details, because no new type of argument is used, while the notation grows cumbersome. The final result is contained in

THEOREM VI. *The following represent a set of necessary and sufficient conditions for a system of integers, $c_{i_1\cdots i_k}(i_1,i_2,\cdots,i_k=0,1,\cdots,m-1)$, $c_{i_1\cdots i_k}=$ smallest non-negative residue modulo m of $f(i_1,\cdots,i_k)$, to be a residue system modulo m of a polynomial $f(x_1,\cdots,x_k)$: Form the signature $S(m)$ and the characteristic $C(m)$; from $S(m)$ we read off k sets of $\tau\cdot\mu^{k-1}m^*$ residual congruences each, complete in the sense that all other residual congruences between elements of the residue system are implied by these. These sets of congruences are the following:*

$$\frac{m}{d_i}\left[c_{x+\mu(d_i),j_2,j_3,\cdots,j_k}-\binom{\mu(d_i)}{1}c_{x+\mu(d_i)-1,j_2,j_3,\cdots,j_k}+\cdots\pm c_{x,j_2,\cdots,j_k}\right]\equiv 0 \pmod m$$
$$(i=0,1,\cdots,\tau-1;\ j_2,j_3,\cdots,j_k=0,1,\cdots,\mu(m)-1);$$

$$\frac{m}{d_i}\left[c_{j_1,x+\mu(d_i),j_3,\cdots,j_k}-\binom{\mu(d_i)}{1}c_{j_1,x+\mu(d_i)-1,j_3,\cdots,j_k}+\cdots\pm c_{j_1,x,j_3,\cdots,j_k}\right]\equiv 0 \pmod m$$
$$(i=0,1,\cdots,\tau-1;\ j_1,j_3,\cdots,j_k=0,1,\cdots,\mu(m)-1);$$

. . . . . .

$$\frac{m}{d_i}\left[c_{j_1,j_2,\cdots,j_{k-1},x+\mu(d_i)}-\binom{\mu(d_i)}{1}c_{j_1,\cdots,j_{k-1},x+\mu(d_i)-1}+\cdots\pm c_{j_1,\cdots,j_{k-1},x}\right]\equiv 0 \pmod m$$
$$(i=0,1,\cdots,\tau-1;\ j_1,j_2,\cdots,j_{k-1}=0,1,\cdots,\mu(m)-1).$$

* $\mu^{k-1}m=[\mu(m)]^{k-1}$.

The structure of the residue system is determined by these congruences and can be easily written down from the characteristic $C(m)$:

(1) *the* $\mu^k d_{\tau-1}$ *numbers* $c_{i_1,\cdots,i_k}(i_1, \cdots, i_k = 0, 1, \cdots, \mu(d_{\tau-1}) - 1)$ *may assume independently any of the values* $0, 1, \cdots, m-1$;

(2) *the* $\mu^k d_{\tau-2} - \mu^k d_{\tau-1}$ *numbers* $c_{i_1,\cdots,i_k}(i_1, \cdots, i_k = \mu(d_{\tau-1}), \cdots, \mu(d_{\tau-2}) - 1)$ *may then assume independently certain* $m/d_{\tau-1}$ *values among* $0, 1, \cdots, m-1$; *for each* c *the corresponding* $m/d_{\tau-1}$ *values over which it may range are determined by the congruences above*;

(3) *the* $\mu^k d_{\tau-3} - \mu^k d_{\tau-2}$ *numbers* $c_{i_1,\cdots,i_k}(i_1, \cdots, i_k = \mu(d_{\tau-2}), \cdots, \mu(d_{\tau-3}) - 1)$ *may still assume independently* any of* $m/d_{\tau-2}$ *values among* $0, 1, \cdots, m-1$;

. . . . . .

(4) *the* $\mu^k d_2 - \mu^k d_1$ *numbers* $c_{i_1,\cdots,i_k}(i_1, \cdots, i_k = \mu(d_2), \cdots, \mu(d_1) - 1)$ *may still each assume any of* m/d_1 *values*; *finally*

(5) *the remaining* $m^k - \mu^k d_1$ *numbers* $c_{i_1,\cdots,i_k}(i_1, \cdots, i_k = \mu(d_1), \cdots, \mu(m) - 1)$ *are then completely determined among the numbers* $0, 1, \cdots, m-1$.

The number of residue systems is $N(m)$.

In saying that our theorem represents necessary and sufficient conditions for a residue system, the word *necessary* must of course be understood in the sense that it is not required to select just the intersections of the first $\mu(d_{\tau-1})$ rows and columns—for the case of two variables, and *mutatis mutandis* for $k > 2$—for the unrestricted elements, etc. For example, the intersections of any $\mu(d_{\tau-1})$ consecutive rows and any $\mu(d_{\tau-1})$ consecutive columns may be chosen as the elements which are not restricted. On the other hand, it would not do to select arbitrarily $\mu(d_{\tau-1})$ rows and $\mu(d_{\tau-1})$ columns for the unrestricted elements.

---

* In this sense: After the numbers c of (1) and of (2) have been chosen, the congruences will leave for each c of (3) just $m/d_{\tau-2}$ values from $0, 1, \cdots, m-1$ which it may assume. Similarly in (4) and (5).

UNIVERSITY OF ILLINOIS,
URBANA, ILL.