A BASIS FOR RESIDUAL POLYNOMIALS IN n VARIABLES*

BY
MARIE LITZINGER

I. Introduction

Kempner† has established the existence of a basis for residual polynomials in one variable with respect to a composite modulus. A residual polynomial modulo m is by definition a polynomial $f(x)$ with integral coefficients which is divisible by m for every integral value of x, and a residual congruence is written $f(x)\equiv 0 \pmod{m}$. By a basis for a given modulus is meant a finite set of residual polynomials $p_i(x)$ which fulfills two requirements: (i) every residual polynomial modulo m is expressible as a sum of products of $p_i(x)$ by polynomials in x with integral coefficients; (ii) no member of the set $p_i(x)$ can be written identically equal to a sum of products of the remaining members of the set by polynomials in x with integral coefficients.

For this work, the following notation is used. The symbol $\mu(d)$ denotes the least positive integer for which d divides $\mu!$. A special set of divisors of m is chosen: separate all divisors of m which exceed 1 into groups such that $\mu(d)$ has the same value for all the d's of a group but different values for the d's of different groups; select the largest d of each group and denote this set by $d_1, \cdots, d_s$. Finally, $\Pi(\mu)=x(x-1)\cdots(x-\mu+1)$; when x is replaced by x_j, the product will be designated by $\Pi_j(\mu)$; $\Pi(1)$ is interpreted as 1. Employing this notation, Dickson‡ gave a brief proof of the theorem due to Kempner§:

Every residual polynomial $f(x)$ modulo m is a sum of products of m and $(m/d_i)\Pi(\mu(d_i))$ for $i=1, \cdots, s$ by polynomials in x with integral coefficients.

In a later paper, Kempner¶ considered the problem for n variables. In attempting to apply Dickson's method to the proof of the existence of a basis for residual polynomials in more than one variable, I found that Kempner had omitted from the set $p_i(x_1, \cdots, x_n)$ certain residual polynomials in

* Presented to the Society, February 23, 1935; received by the editors July 8, 1934.

† These Transactions, vol. 22 (1921), pp. 240–266.

‡ L. E. Dickson, *Introduction to the Theory of Numbers*, p. 26, Theorem 28.

§ These Transactions, vol. 22 (1921), p. 263.

¶ These Transactions, vol. 27 (1925), pp. 287–298.

several variables. This was brought to my attention by an example in two variables modulo 12. For this modulus, the $d_1, \cdots, d_s$ are $d_1=12$, $d_2=6$, $d_3=2$; the corresponding μ's are $\mu_1=4$, $\mu_2=3$, $\mu_3=2$. Write $q_i=m/d_i$. The part of the basis containing one variable is composed of

$$(1) \qquad 12, \quad q_i\Pi_1(\mu_i), \quad q_i\Pi_2(\mu_i) \qquad (i = 1, 2, 3).$$

Kempner would include in the basis $p_i(x_1, x_2)$ modulo 12 only the seven terms (1). However, the residual polynomial,

$$P = (m/(d_3\cdot d_3))\Pi_1(\mu_3)\Pi_2(\mu_3) = 3x_1(x_1 - 1)x_2(x_2 - 1),$$

must be added since, as is shown below, it is impossible to write the identity

$$(2) \qquad P = 12\cdot c + \sum_{i=1}^{3} q_i\Pi_1(\mu_i)f_i + \sum_{i=1}^{3} q_i\Pi_2(\mu_i)g_i,$$

where c, f_i, g_i are polynomials in x_1, x_2 with integral coefficients. By use of $(x_1, x_2)=(0, 0)$, $(2, 0)$, $(0, 2)$ we prove the constant terms of c, f_3, g_3 even. The pair $(x_1, x_2)=(2, 2)$ shows the right side of (2) divisible by 24 and the left side equal to 12.

II. Representation of residual polynomials

Dickson's method of establishing the existence of a basis for residual polynomials modulo m in one variable may be applied to the case of two variables and then by induction to n variables. Several preliminary steps are necessary. The first is the statement of two lemmas due to Dickson.

Lemma* 1. *If d is any divisor of m, $\mu(d)$ is the minimum degree of a residual polynomial $f(x)$ modulo m whose leading coefficient is m/d.*

Lemma† 2. *Any residual polynomial $f(x)$ modulo m is term by term congruent modulo m to the product of an integer prime to m by a residual polynomial whose leading coefficient is a divisor of m.*

The next step is to obtain a lemma similar to Lemma 2.

Lemma 3. *Any residual polynomial $f(x_1, \cdots, x_n)$ modulo m, written as a function of x_1 with coefficients containing $x_2, \cdots, x_n$, is term by term congruent modulo m to the product of an integer prime to m by a residual polynomial in which the greatest common divisor of the coefficients of the highest power of x_1 is a divisor of m.*

Let

$$f(x_1, \cdots, x_n) = cG(x_2, \cdots, x_n)x_1^r + \cdots,$$

* L. E. Dickson, *Introduction to the Theory of Numbers*, p. 25, V.

† Ibid., p. 25, VI.

where the coefficients of G have the greatest common divisor 1, and let g be the greatest common divisor of $c=gC$ and $m=gM$. Since C is prime to M, $CL\equiv 1 \pmod{M}$ has a unique solution L. Then every integer satisfying $Cz\equiv 1 \pmod{M}$ is of the form $z=L+My$, and y can be chosen so that z is prime to m. Consequently $zZ\equiv 1 \pmod{m}$ has a solution Z and $cz=gCz\equiv g \pmod{m}$, also

$$zf \equiv gG(x_2, \cdots, x_n)x_1^r + \cdots \pmod{m},$$
$$f \equiv Z[gG(x_2, \cdots, x_n)x_1^r + \cdots] \pmod{m}.$$

Finally, two properties of μ and divisors of m must be derived.

LEMMA 4. *If d and d' are divisors of m such that d' divides d, then $\mu(d')\leqq\mu(d)$.*

Write $d=p_1^{a_1}\cdot p_2^{a_2}\cdots p_k^{a_k}$ where $p_1, p_2, \cdots, p_k$ are distinct primes. Then $\mu(d)$ is the largest (or one of the largest in case several are equal)* of the numbers $\mu(p_1^{a_1}), \mu(p_2^{a_2}), \cdots, \mu(p_k^{a_k})$. Since d' divides d, $d'=p_1^{b_1}\cdot p_2^{b_2}\cdots p_k^{b_k}$ where $0\leqq b_i\leqq a_i$ for $i=1, 2, \cdots, k$. So $\mu(p_i^{b_i})\leqq\mu(p_i^{a_i})$ for $i=1, 2, \cdots, k$, and $\mu(d')$, the largest of the $\mu(p_1^{b_1}), \mu(p_2^{b_2}), \cdots, \mu(p_k^{b_k})$, is less than or equal to $\mu(d)$.

LEMMA 5. *If d_i is one of the set $d_1, \cdots, d_s$ for m, then d_i is divisible by every divisor of m which divides $\mu(d_i)!$.*

The assumption that a divisor d of m divides $\mu(d_i)!$ and does not divide d_i leads to a contradiction as follows. Denote by D the greatest common divisor of d_i and d so that $d_i=DD_i$ and $d=DD'$. Since $\mu(d_i)!$ is divisible by both d_i and d and since D_i and D' are relatively prime, $\mu(d_i)!$ is divisible by $N=DD_iD'$ and N divides m. As N divides $\mu(d_i)!$, $\mu(N)\leqq\mu(d_i)$; as N is divisible by d_i, by Lemma 4, $\mu(N)\geqq\mu(d_i)$; consequently $\mu(N)=\mu(d_i)$. But d_i is one of the set $d_1, \cdots, d_s$ and therefore is the maximum of all divisors d_j of m for which $\mu(d_j)=\mu(d_i)$. There is then a contradiction unless $D'=1$, therefore d divides d_i.

With the aid of these lemmas, it is possible to prove

THEOREM 1. *Every residual polynomial $f(x_1, x_2)$ modulo m is a sum of products of m and functions*

$$(m/(d_{i_1}\cdot d_{i_2}))\Pi_1(\mu(d_{i_1}))\Pi_2(\mu(d_{i_2})) \tag{3}$$

by polynomials in x_1, x_2 with integral coefficients, where d_{i_1}, d_{i_2} are divisors of m, at least one belongs to the set $d_1, \cdots, d_s$, and the product $d_{i_1}\cdot d_{i_2}$ divides m.

By Lemma 3,

* Kempner, these Transactions, vol. 22 (1921), p. 243.

$$f(x_1, x_2) = m\phi(x_1, x_2) + ZF(x_1, x_2),$$

where Z and the coefficients of ϕ are integers, Z is prime to m and F is a residual polynomial modulo m of the form

$$(m/d)G(x_2)x_1^r + \cdots, \tag{4}$$

d being a divisor of m. If $d=1$, the terms containing m as a factor may be combined with $m\phi$ and the remaining portion considered the new ZF. So let $d>1$.

Case 1. Let $r \geqq \mu(d)$. Employ the relation*

$$(m/d)\Pi_1(\mu(d)) = (qm/d_{i_1})\Pi_1(\mu(d_{i_1})), \tag{5}$$

where d_{i_1} is one of the set $d_1, \cdots, d_s$ and q is an integer. The product of (5) by $G(x_2)x_1^{r-\mu(d_{i_1})}$ gives a function whose term in x_1^r is identical with that of F. The difference is a residual polynomial of degree less than r in x_1.

Case 2. Let $r<\mu(d)$. Consider F which is of the form (4). For a chosen value x_2' of x_2, by Lemma 2, F as a residual polynomial in x_1 is term by term congruent modulo m to the product of an integer prime to m by a residual polynomial whose leading coefficient is a divisor of m, that is,

$$F(x_1, x_2') = (m/d)G(x_2')x_1^r + \cdots \equiv z((m/d')x_1^r + \cdots) \pmod{m},$$

where z is prime to m and d' divides m. Then $(m/d)G(x_2')=z\cdot m/d'+km$ where k is integral. As m/d' divides m, $(m/d)G(x_2')$ is divisible by m/d'. Now $(m/d')x_1^r+\cdots$ is a residual polynomial whose leading coefficient is a divisor of m, consequently, by Lemma 1, $r \geqq \mu(d')$. Let d_i represent the divisor of the set $d_1, \cdots, d_s$ to which corresponds the largest μ which does not exceed r. Then $\mu(d_i) \geqq \mu(d')$, therefore d' divides $\mu(d_i)!$. By Lemma 5, d' divides d_i. Consequently m/d_i divides m/d' and must then divide $(m/d)G(x_2')$.

There is an important consequence of the divisibility of $(m/d)G(x_2')$ by m/d_i. Note first that m/d_i does not divide m/d, for if d divides d_i, by Lemma 4, $\mu(d) \leqq \mu(d_i)$; but by the definition of d_i, $\mu(d_i) \leqq r$; the conclusion $\mu(d) \leqq r$ contradicts the hypothesis of this second case, namely $r<\mu(d)$. Since m/d_i does not divide m/d, denote their greatest common divisor by M. Then

$$m/d_i = Mg, \quad m/d = Mv, \quad v\cdot m/d_i = g\cdot m/d, \tag{6}$$

where $g>1$ and prime to v. From the divisibility of $(m/d)G(x_2')$ by m/d_i, it follows that the quotient of $(m/d)G(x_2')$ by m/d_i, which equals $(v/g)G(x_2')$, is integral. As g is prime to v, g divides $G(x_2')$.

Consider $G(x_2)$ for other values of x_2. Although the coefficient correspond-

* L. E. Dickson, *Introduction to the Theory of Numbers*, p. 27, equation (34).

ing to m/d' varies with the choice of x_2, d_i by definition is determined by r and m and is independent of the value of x_2. Consequently g and v, determined by m/d_i and m/d, do not vary with x_2. So for every choice of x_2, the m/d' determined by it is such that it divides $(m/d)G(x_2)$ and is divisible by m/d_i; therefore $(m/d)G(x_2)$ is divisible by m/d_i and $G(x_2)$ is divisible by g.

Since $G(x_2)$ is divisible by g for every value of x_2, $G(x_2)\equiv 0 \pmod{g}$. Therefore $G(x_2)$ is expressible* as a sum of products of g and $(g/d_{i_2})\Pi_2(\mu(d_{i_2}))$ by polynomials in x_2 with integral coefficients, where the d_{i_2} represent the set of divisors of g selected as the set $d_1, \cdots, d_s$ was chosen from all divisors of m. As g divides m, for each d_{i_2}, $\mu(d_{i_2})=\mu(d_h)$ where d_h is one of the set $d_1, \cdots, d_s$ for m and, by Lemma 5, d_{i_2} equals or divides d_h.

In the work which follows, write d_{i_1} for d_i to indicate its association with x_1. The term of F containing the highest power of x_1 may be expressed as follows:

$$(m/d)G(x_2)x_1^r = g(m/d)(1/g)G(x_2)x_1^r = v(m/d_{i_1})(t/m)G(x_2)x_1^r,$$

where t is defined by the equation $tg=m$, and g and v are defined by (6). Note that d_{i_1} divides t from the following considerations: $t/d_{i_1}=(m/g)g/(dv)=m/(dv)$ which is integral since v divides m/d. As d_{i_1} divides t and each d_{i_2} is a factor of g, for every d_{i_2}, the product $d_{i_1}d_{i_2}$ divides m. From its definition, d_{i_1} is one of the set $d_1, \cdots, d_s$ for m. The product of $v(m/d_{i_1})\Pi_1(\mu(d_{i_1}))$ by $(t/m)G(x_2)x_1^{r-\mu(d_{i_1})}$ gives a function whose term in x_1^r is identical with that of F. The difference is a residual polynomial of degree less than r in x_1.

This process, continued for the resulting polynomials considered as functions of x_1 or x_2, lowers the degree in x_1 or x_2 at each step and leads to a difference zero. Finally $f(x_1, x_2)$ is expressed in the manner described in Theorem 1.

A similar theorem for n variables is readily proved by induction.

THEOREM 2. *Every residual polynomial $f(x_1, \cdots, x_n)$ modulo m is a sum of products of m and functions*

$$(7) \qquad (m/(d_{i_1}\cdots d_{i_n}))\Pi_1(\mu(d_{i_1}))\cdots\Pi_n(\mu(d_{i_n}))$$

by polynomials in $x_1, \cdots, x_n$ with integral coefficients where the d_{i_j} are divisors of m, at least one of the $d_{i_1}, \cdots, d_{i_n}$ belongs to the set $d_1, \cdots, d_s$, and the product $d_{i_1}\cdots d_{i_n}$ divides m.

The theorem has been established for the case $n=2$. Assume that it holds for $n-1$ variables and show that it must then be true for n. By Lemma 3,

$$f(x_1, \cdots, x_n) = m\phi(x_1, \cdots, x_n) + ZF(x_1, \cdots, x_n),$$

where Z and the coefficients of ϕ are integers, Z is prime to m, and F is a resid-

* L. E. Dickson, *Introduction to the Theory of Numbers*, p. 26, Theorem 28.

ual polynomial modulo m of the form

$$(8)\qquad (m/d)G(x_2, \cdots, x_n)x_1^r + \cdots,$$

d being a divisor of m. If $d=1$, the terms containing m as a factor may be combined with $m\phi$ and the remaining portion considered the new ZF. So let $d>1$.

Case 1. Let $r \geqq \mu(d)$. Employ relation (5). The product of (5) by $G(x_2, \cdots, x_n)x_1^{r-\mu(d_{i1})}$ gives a function whose term in x_1^r is identical with that of F. The difference is a residual polynomial modulo m of degree less than r in x_1.

Case 2. Let $r<\mu(d)$. Consider F which is of the form (8). For a chosen set of values $x_2', \cdots, x_n'$, by Lemma 2, F as a residual polynomial in x_1 modulo m is term by term congruent modulo m to the product of an integer prime to m by a residual polynomial whose leading coefficient is a divisor of m, that is,

$$\begin{aligned} F(x_1, x_2', \cdots, x_n') &= (m/d)G(x_2', \cdots, x_n')x_1^r + \cdots \\ &\equiv z((m/d')x_1^r + \cdots) \qquad \pmod{m}, \end{aligned}$$

where z is prime to m and d' divides m. For the chosen set $x_2', \cdots, x_n'$, $(m/d)G(x_2', \cdots, x_n') = z\cdot m/d' + km$ where k is integral. As m/d' divides m, m/d' divides $(m/d)G(x_2', \cdots, x_n')$. Now $(m/d')x_1^r + \cdots$ is a residual polynomial whose leading coefficient is a divisor of m, consequently, by Lemma 1, $r \geqq \mu(d')$.

Repeat the argument given in Theorem 1 for Case 2, defining d_i as the divisor of the set $d_1, \cdots, d_s$ for m to which corresponds the largest μ not exceeding r, and replacing the phrase "value of x_2'" by "set of values $x_2', \cdots, x_n'$," and $G(x_2')$ by $G(x_2', \cdots, x_n')$. Exactly as in the first two paragraphs of Case 2, Theorem 1, m/d_i divides m/d' and therefore divides $(m/d)G(x_2', \cdots, x_n')$; but m/d_i does not divide m/d. Let M denote the greatest common divisor of m/d_i and m/d, and obtain (6). Then the quotient of $(m/d)G(x_2', \cdots, x_n')$ by m/d_i, which equals $(v/g)G(x_2', \cdots, x_n')$, is integral. Since g is prime to v, g divides $G(x_2', \cdots, x_n')$.

Consider $G(x_2, \cdots, x_n)$ for other values of $x_2, \cdots, x_n$. Although the coefficient corresponding to m/d' varies with the choice of $x_2, \cdots, x_n$, d_i is determined by r and m and is independent of the values of $x_2, \cdots, x_n$. Consequently g and v, determined by m/d_i and m/d, do not vary with $x_2, \cdots, x_n$. So for every choice of $x_2, \cdots, x_n$, the m/d' determined by it is such that it divides $(m/d)G(x_2, \cdots, x_n)$ and is divisible by m/d_i; therefore $(m/d)G(x_2, \cdots, x_n)$ is divisible by m/d_i and $G(x_2, \cdots, x_n)$ is divisible by g.

Since $G(x_2, \cdots, x_n)$ is divisible by g for every set of values $x_2, \cdots, x_n$, $G(x_2, \cdots, x_n) \equiv 0 \pmod{g}$. According to the hypothesis, G as a residual polynomial in $n-1$ variables is expressible as a sum of products of g and

$$(g/(d_{i_2}\cdots d_{i_n}))\Pi_2(\mu(d_{i_2}))\cdots\Pi_n(\mu(d_{i_n}))$$

by polynomials in $x_2, \cdots, x_n$ with integral coefficients, where the d_{i_j} (for $j=2, \cdots, n$) represent divisors of g and $d_{i_2}\cdots d_{i_n}$ divides g. Since g divides m, for each d_{i_j}, $\mu(d_{i_j})=\mu(d_h)$ where d_h is one of the set $d_1, \cdots, d_s$ for m, and, by Lemma 5, d_{i_j} equals or divides d_h.

For the following work, write d_{i_1} in place of d_i to indicate its association with x_1. The term of F which contains the highest power of x_1 may be expressed as follows:

$$(m/d)G(x_2, \cdots, x_n)x_1^r = v(m/d_{i_1})(t/m)G(x_2, \cdots, x_n)x_1^r,$$

where t is defined by the equation $tg=m$, and g and v are defined by (6). As in the fifth paragraph of Case 2, Theorem 1, d_{i_1} divides t. Since each product $d_{i_2}\cdots d_{i_n}$ divides g, then $d_{i_1}d_{i_2}\cdots d_{i_n}$ divides m. The product of $v(m/d_{i_1})$ $\Pi_1(\mu(d_{i_1}))$ by $(t/m)G(x_2, \cdots, x_n)x_1^{r-\mu(d_{i_1})}$ gives a function whose term in x_1^r is identical with that of F. The difference is a residual polynomial of degree less than r in x_1.

This process, continued for the resulting polynomials considered as functions of x_j for $j=1, 2, \cdots, n$, lowers the degree in x_j at each step and leads to a difference zero. Finally $f(x_1, \cdots, x_n)$ is expressed in the manner described in Theorem 2.

Theorems 1 and 2 contain one interesting difference from the theorem for one variable. Of the divisors of m appearing in a term (3) or (7), only one is necessarily chosen from $d_1, \cdots, d_s$.

III. Selection of a basis

It is now essential to establish a basis for residual polynomials in n variables modulo m. By Theorem 2, the set composed of m and all terms (7) fulfills the first requirement for a basis. It remains to select from m and (7) a reduced set $p_i(x_1, \cdots, x_n)$ such that no member of p_i can be written identically equal to a sum of products of the remaining p_i by polynomials in $x_1, \cdots, x_n$ with integral coefficients, and such that each of the terms of m and (7) not included among the p_i can be written identically equal to a sum of products of p_i by polynomials in $x_1, \cdots, x_n$ with integral coefficients. The terms p_i form a basis and will be called independent. All other terms m and (7) will be called dependent.

A term $k\cdot\Pi_1(\mu(d_{i_1}))\cdots\Pi_n(\mu(d_{i_n}))$ of (7) whose coefficient k is a multiple of that of another term (7) containing $\Pi_1(\mu(d_{i_1}))\cdots\Pi_n(\mu(d_{i_n}))$ is obviously dependent. Discard such terms and represent the remaining terms (7) by

(9) $$P(d_{i_1}, \cdots, d_{i_n}).$$

Denote by S the set composed of m and all terms (9). Throughout the discussion, an element of the set S will be termed simple or compound according as it contains one variable or more than one variable. The phrase "member related to (9)" will be used to designate any term of the set S, simple or compound, which contains not more than $\mu(d_{i_j})$ factors in x_j for each $j=1, \cdots, n$.

The following theorem establishes a basis.

THEOREM 3. *For the general modulus m, a basis for residual polynomials in n variables is composed of m, all simple terms and all compound terms* (9) *such that $\mu(d_{i_1}), \cdots, \mu(d_{i_n})$ are all multiples of the same prime factor of m.*

Example. For the modulus $3^3\cdot 5$, the set S in two variables contains terms which are not members of the basis. The $d_1, \cdots, d_s$ for this modulus are $d_1=3^3\cdot 5$, $d_2=3^2\cdot 5$, $d_3=3\cdot 5$, $d_4=3$; the corresponding μ's are $\mu_1=9$, $\mu_2=6$, $\mu_3=5$, $\mu_4=3$. The basis is composed of $3^3\cdot 5$, all simple terms, and the compound terms $P(d_4, d_4)$, $P(d_4, d_2)$, $P(d_2, d_4)$. The dependent compound terms of S are expressible in terms of the basis as follows:

$$P(d_4, d_3) = 2(x_2-3)(x_2-4)P(d_4, d_4) - 3x_1(x_1-1)(x_1-2)q_3\Pi_2(\mu_3),$$
$$P(d_3, d_4) = 2(x_1-3)(x_1-4)P(d_4, d_4) - 3x_2(x_2-1)(x_2-2)q_3\Pi_1(\mu_3).$$

The part of Theorem 3 concerned with simple terms is readily established. Kempner* proved that m and $(m/d_i)\Pi(\mu(d_i))$ for $i=1, \cdots, s$ form a basis for residual polynomials modulo m in one variable. It follows that m as well as each simple term of S is independent of all other members of the set S. For instance, to show the independence of a simple term in x_j, set the remaining $n-1$ variables equal to zero.

The proof of the portion of Theorem 3 which deals with compound terms will be divided into two parts. First it will be shown that each of the compound terms listed in the theorem is independent of all other members of the set S. Then it will be shown by means of an auxiliary theorem that these are the only independent compound terms.

It is not difficult to prove the independence of the compound terms described in Theorem 3. Suppose it were possible to write the identity

(10) $$P(d_{i_1}, \cdots, d_{i_n}) = m\cdot c + \sum_i P_i\cdot f_i,$$

where c and f_i are polynomials in $x_1, \cdots, x_n$ with integral coefficients and the P_i represent all members of the set S, simple and compound, except

(11) $$P(d_{i_1}, \cdots, d_{i_n}).$$

* These Transactions, vol. 22 (1921), pp. 263–264.

By hypothesis each μ on the left side of (10) is a multiple of a prime p which divides m. That each term on the right contains one more factor p than appears on the left for $x_1=\mu(d_{i_1}), \cdots, x_n=\mu(d_{i_n})$ may be shown as follows. Substitute successively for each x_j the values 0, $\mu(d_{i_k})$ for all $k=1, \cdots, n$ such that $\mu(d_{i_k}) \leqq \mu(d_{i_j})$. Under this substitution, terms P_i not related to (11) disappear, and the constant term of c and each remaining f_i associated with a member of the basis containing only μ's which are multiples of p is proved congruent to zero modulo p. Related members not included among the latter present no difficulty since for the values listed above each will contain p to a power at least one greater than that exhibited in the modulus, p^s. For instance, consider the simple term $(m/d_i)\Pi((\mu(d_i))$ which lies between terms whose variable parts are $\Pi(rp)$ and $\Pi((r+1)p)$ and contain respectively rp and $(r+1)p$ factors. This implies $rp<\mu(d_i)<(r+1)p$. For $x=rp$, $(m/d_i) \cdot\Pi(\mu(d_i))$ is zero; for $x=\mu(d_i)$ it is divisible by exactly p^s. The sequence $\Pi(\mu(d_i))=x(x-1) \cdots (x-\mu(d_i)+1)$ contains at least one higher power of p for $x=(r+1)p$ than for $x=\mu(d_i)$ since one additional factor p is thus introduced at the beginning of the sequence when $(r+1)p$ is substituted for x, and none is lost at the end as the sequence contains more than rp factors. The same reasoning holds for members of the set S formed by compounding $(m/d_i)\Pi(\mu(d_i))$ with other terms; however it will be shown in the Auxiliary Theorem that such members are dependent. The independence of (11) follows immediately; substitute for each x_j the value $\mu(d_{i_j})$. The left side of (10) is divisible by exactly p^s, the right side by p^{s+1}.

It is possible to select from the set S certain dependent terms. If the coefficient of a compound member is the greatest common divisor of the coefficients of related terms, it is expressible as a linear homogeneous function of them with integral coefficients. Since the related terms by definition contain no more factors in any one variable than appear in the given term, the latter may be expressed by means of the related members in the manner described in Theorem 3.

That these are the only dependent terms follows from the

AUXILIARY THEOREM. *For a compound term* (11) *of the set S for n variables modulo m, if*

$$m/(d_{i_1} \cdots d_{i_n}) \tag{12}$$

is not the greatest common divisor of the coefficients of all related members of the set S, each $\mu(d_{i_j})$ for $j=1, \cdots, n$ is a multiple of the same prime factor of the modulus.

Adopt the following notation to designate terms related to (11): let d_{i_j}' represent any of the divisors of m such that $\mu(d_{i_j}') < \mu(d_{i_j})$ for $j=1, \cdots, n$.

Then the coefficient of any term related to (11) is of the form

$$m/(d_{k_1} \cdots d_{k_n}), \tag{13}$$

where at least one $d_{k_t} = d'_{i_t}$ if all of them are greater than 1; for one possible type of coefficients (13), each $d_{k_t} = d'_{i_t}$.

From the manner in which the set S is constructed, (12) divides the coefficients of all related terms. Since by hypothesis (12) is not the greatest common divisor of all coefficients (13), denote their greatest common divisor by the product of k by (12), where k is a divisor of m greater than 1 which may or may not be prime to (12). Then for $j = 1, \cdots, n$, each m/d'_{i_j} contains a higher power of k than appears in m/d_{i_j}. Otherwise one of the combinations (13) would equal (12) and (12) would be the greatest common divisor of all coefficients of related terms. In other words, the coefficient of every simple term of the set S which exceeds m/d_{i_j} contains a higher power of k than does m/d_{i_j}. Since for each j, the largest $\Pi_j(\mu(d'_{i_j}))$ has a coefficient which divides all the other m/d'_{i_j}, its coefficient contains the product of k by (12). So for each j, $\Pi_j(\mu(d_{i_j}))$ differs from the largest $\Pi_j(\mu(d'_{i_j}))$ in that it is divisible by a higher power of k than $\Pi_j(\mu(d'_{i_j}))$ for all values of x_j. Therefore if k is a prime p, for each j, $\mu(d_{i_j})$ is a multiple of p; if k is composite, for each j, $\mu(d_{i_j})$ is a multiple of the same prime factor of k.

There are two corollaries to Theorem 3.

COROLLARY 1. *For a modulus composed of the product of distinct primes, a basis is composed of m and all simple terms.*

Write the modulus m as $p_1p_2 \cdots p_c$ where the p's are distinct primes arranged in descending order. The set $d_1, \cdots, d_s$ for m is composed of $p_1p_2p_3 \cdots p_c$, $p_2p_3 \cdots p_c$, $\cdots$, $p_{c-1}p_c$, p_c; the corresponding μ's are p_1, $p_2, \cdots, p_{c-1}$, p_c. No product of two or more of the d's listed above will divide m since each contains p_c. Even when all possible divisors of m are considered, as each one associated with $\mu = p_j$ contains p_j as a factor, the product of two or more such divisors, if it divides m, divides one of the d's given above. Consequently a residual polynomial whose coefficient is m divided by this product is expressible as a single variable member of the set S multiplied by a polynomial with integral coefficients.

COROLLARY 2. *For a modulus equal to the power of a prime, a basis is composed of all terms m and* (9).

The divisors of $m = p^k$ are powers of p, and the μ's are all multiples of p.

MOUNT HOLYOKE COLLEGE,
SOUTH HADLEY, MASS.