A GENERALIZATION OF FERMAT'S THEOREM

IVAN NIVEN AND LEROY J. WARREN

1. **Introduction.** There are various generalizations of Fermat's theorem that $a^{p-1} \equiv 1 \pmod{p}$ for any prime p and any integer a not divisible by p. The generalization that we present arises from looking at Fermat's result this way: given any prime p the congruence $x^p - x \equiv 0 \pmod{p}$ is satisfied by every integer x; moreover, if $f(x)$ is a polynomial with integral coefficients such that $f(x) \equiv 0 \pmod{p}$ is satisfied by every integer x, then $f(x)$ is a multiple of $x^p - x$. The problem that we raise and settle here is this: for any positive integer m characterize the class of polynomials $f(x)$ having the property that $f(x) \equiv 0 \pmod{m}$ is satisfied by every integer. It turns out that in general, unlike the Fermat case where m is a prime, these polynomials are not all multiples of a single polynomial. Nevertheless these polynomials form an ideal with a finite set of generators.

We now introduce a preferable notation to put the question in more tractable form. Let I denote the class of all integers, and I/m the finite ring of integers modulo m, so that I/m consists of elements $0, 1, 2, \cdots, m-1$ with addition and multiplication defined modulo m. In the ring R of polynomials $g(x)$ with coefficients in I/m, let $\mathfrak{g}(m)$ denote the subring of polynomials $f(x)$ such that $f(a) = 0$ for every element a in I/m. This subring $\mathfrak{g}(m)$ is an ideal in R, because (i) the difference of any two polynomials in $\mathfrak{g}(m)$ is again a polynomial in $\mathfrak{g}(m)$, and (ii) if $f(x)$ is any polynomial in $\mathfrak{g}(m)$ and $g(x)$ is any polynomial in R, then $f(x)g(x)$ is in $\mathfrak{g}(m)$. Our problem is to determine the structure of the ideal $\mathfrak{g}(m)$. In case m is a prime p, then as we remarked earlier, $\mathfrak{g}(p)$ is known to be the class of polynomials which are multiples of $x^p - x$. Thus $\mathfrak{g}(p)$ is a principal ideal with the single generator $x^p - x$. In case m is not a prime we prove that $\mathfrak{g}(m)$ is not a principal ideal, and we find a basis for $\mathfrak{g}(m)$.

2. **A prime power modulus.** First we solve the problem in case the modulus m has the form p^n, and then in the next section we use the theory of direct sums for the extension to the general case. For any positive integer k, define $t(k)$ as the highest exponent of the prime p that divides $(pk)!$, thus

$$p^{t(k)} \mid (pk)!, \quad p^{t(k)+1} \nmid (pk)!.$$

Let s be the integer, dependent on p and n, defined by the inequality

Received by the editors May 15, 1956.

$$t(s-1) < n \leqq t(s).$$

Finally, define the polynomials

$$(1)\qquad g_k(x) = p^{n-t(k)} \prod_{j=0}^{kp-1} (x-j), \qquad k = 1, 2, \cdots, s-1,$$
$$g_s(x) = \prod_{j=0}^{sp-1} (x-j),$$

with coefficients in I/p^n. We shall establish that these polynomials form a basis for the ideal $\mathfrak{g}(p^n)$.

LEMMA 1. *For any $a \in I/p^n$ and any k in the range $1 \leqq k \leqq s$, we have $g_k(a) = 0$.*

PROOF. When x is replaced by a, the product $\prod(x-j)$ in $g_k(x)$ becomes either zero or the product of kp consecutive integers, modulo p^n. But the product of kp consecutive integers is divisible by $(kp)!$, so the lemma follows from the definition of $t(k)$.

LEMMA 2. *Let j be one of the elements $0, 1, 2, \cdots, p^n-1$ of I/p^n. Then any polynomial $f(x)$ with coefficients in I/p^n can be written in the form*

$$f(x) = a_0 + a_1 x + a_2 x(x-1) + \cdots + a_{j-1} \prod_{i=0}^{j-2} (x-i)$$
$$+ q(x) \prod_{i=0}^{j-1} (x-i).$$

PROOF. Divide $f(x)$ by x, say with quotient $f_1(x)$ and remainder a_0, so that

$$f(x) = a_0 + x f_1(x).$$

Divide $f_1(x)$ by $x-1$, say with quotient $f_2(x)$ and remainder a_1, so that

$$f_1(x) = a_1 + (x-1) f_2(x), \qquad f(x) = a_0 + a_1 x + x(x-1) f_2(x).$$

Continuing this process by dividing $f_2(x)$ by $x-2$, then $f_3(x)$ by $x-3$, etc., we obtain the lemma by induction, $q(x)$ being the last quotient in the division process.

THEOREM 1. *The polynomials* (1) *form a basis, or set of generators, for the ideal $\mathfrak{g}(p^n)$ in the ring I/p^n.*

PROOF. Let $f(x)$ be any polynomial in $\mathfrak{g}(p^n)$, so that $f(a) = 0$ for all a in I/p^n. Expand $f(x)$ as in Lemma 2, with j replaced by sp,

$$f(x) = a_0 + a_1x + a_2x(x-1) + \cdots + a_{sp-1}\prod_{i=0}^{sp-2}(x-i) + q(x)\prod_{i=0}^{sp-1}(x-i). \tag{2}$$

By setting $x=0$, $x=1$, $\cdots$, $x=p-1$ in succession we conclude that $a_0=a_1=\cdots=a_{p-1}=0$. Next we set $x=p$ in (2) and conclude that $a_p(p!)=0$, whence a_p must have the form

$$a_p = p^{n-1}b_p = p^{n-t(1)}b_p.$$

Similarly from setting $x=p+1$, $x=p+2$, $\cdots$, $x=2p-1$ in succession we obtain

$$a_j = p^{n-1}b_j = p^{n-t(1)}b_j, \qquad j = p+1, p+2, \cdots, 2p-1.$$

The process continues with $x=2p$, $x=2p+1$, etc. In general when we set $x=kp+j$ with $0\leqq j<p$ in (2) we get

$$a_{kp+j}(kp+j)! = 0.$$

By definition the highest exponent of p dividing $(kp)!$, and so also $(kp+j)!$, is $t(k)$. Hence we have

$$a_{kp+j} = p^{n-t(k)}b_{kp+j}, \qquad j = 0, 1, \cdots, p-1.$$

Substituting these values in (2), we collect the terms in batches and use equations (1) to conclude that for $k<s$,

$$\sum_{j=0}^{p-1} a_{kp+j}\prod_{i=0}^{kp+j-1}(x-i) = \sum_{j=0}^{p-1} p^{n-t(k)}b_{kp+j}\prod_{i=0}^{kp+j-1}(x-i) = g_k(x)H_k(x).$$

Thus (2) becomes

$$f(x) = \sum_{k=1}^{s-1} g_k(x)H_k(x) + g_s(x)q(x),$$

and this proves the theorem.

EXAMPLE. Let $p^n=9$ so that $p=3$, $n=2$, $t(1)=1$, $t(2)=2$, $s=2$. Then $\mathfrak{g}(9)$ has a basis

$$g_1(x) = 3x(x-1)(x-2) = 3x^3 + 6x,$$

$$g_2(x) = \prod_{j=0}^{5}(x-j) = x^6 + 3x^5 + 4x^4 + 4x^2 + 6x.$$

In case $n=1$ the set (1) reduces to the single generator $x(x-1)\cdots$

$(x-p+1)$, and it is well-known that in the ring of integers I there exists a polynomial $q_1(x)$ such that

$$\prod_{j=0}^{p-1}(x-j) = x^p - x + pq_1(x),$$

so that in the ring I/p

$$\prod_{j=0}^{p-1}(x-j) = x^p - x.$$

This suggests the following simplification of part of the system (1).

The first few generators $g_1(x)$, $g_2(x)$, $\cdots$ in (1), specifically up to $p-1$ of these if there are that many, can be replaced by the simpler forms

$$h_k(x) = p^{n-k}(x^p - x)^k, \qquad 1 \leqq k \leqq p-1. \tag{3}$$

To sketch a proof of this we observe first that for these values of k the relation $t(k)=k$ holds. Then for $k=1$ the argument of the preceding paragraph shows that $g_1(x)=h_1(x)$ in I/p^n. Next we note that

$$\prod_{j=p}^{2p-1}(x-j) = \prod_{j=0}^{p-1}\{(x-j)-p\} = (x^p - x) + pq_2(x),$$

$$\prod_{j=0}^{2p-1}(x-j) = \{(x^p - x) + pq_1(x)\}\{(x^p - x) + pq_2(x)\}$$

$$= (x^p - x)^2 + p(x^p - x)\{q_1(x) + q_2(x)\} + p^2 q_1(x)q_2(x).$$

Hence in I/p^n we have

$$g_2(x) = h_2(x) + h_1(x)\{q_1(x) + q_2(x)\},$$

so that the generator $g_2(x)$ can be replaced by $h_2(x)$ in the presence of $h_1(x)$. Next it can be established that

$$\prod_{j=0}^{3p-1}(x-j) = (x^p - x)^3 + p(x^p - x)^2\{q_1 + q_2 + q_3\}$$

$$+ p^2(x^p - x)\{q_1q_2 + q_1q_3 + q_2q_3\} + p^3 q_1q_2q_3,$$

so that $g_3(x)$ can be replaced by $h_3(x)$ in the presence of $h_1(x)$ and $h_2(x)$. This argument can be continued by induction to obtain the result stated above; unfortunately the process stops at $k=p-1$.

3. **The general case.** In order to extend Theorem 1 to the case of modulus m, we use the concept of a direct sum. If m is expressed as a product of distinct prime powers

$$m = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r},$$

then the ring I/m can be represented as a direct sum of rings

$$I/m = I/p_1^{n_1} + I/p_2^{n_2} + \cdots + I/p_r^{n_r}. \tag{4}$$

This well-known representation[1] can be obtained readily as follows. To any element a of I/m there correspond elements $a_1, \cdots, a_r$ of $I/p_1^{n_1}, \cdots, I/p_r^{n_r}$ by the congruence relationships

$$a \equiv a_j \pmod{p_j^{n_j}}, \qquad j = 1, 2, \cdots, r. \tag{5}$$

Conversely, by a well-known result in elementary number theory, to any set of elements a_j in $I/p_j^{n_j}$ there corresponds exactly one element a in I/m satisfying the congruences (5). Thus to each element a in I/m there corresponds a unique r-tuple

$$a \leftrightarrow (a_1, a_2, \cdots, a_r), \tag{6}$$

with a_j in $I/p_j^{n_j}$. Addition and multiplication are defined componentwise for the r-tuples:

$$\begin{aligned}(a_1, a_2, \cdots, a_r) + (b_1, b_2, \cdots, b_r) &= (a_1 + b_1, a_2 + b_2, \cdots, a_r + b_r),\\ (a_1, a_2, \cdots, a_r)(b_1, b_2, \cdots, b_r) &= (a_1b_1, a_2b_2, \cdots, a_rb_r).\end{aligned} \tag{7}$$

With these definitions it can be verified that addition and multiplication are preserved under the correspondence (6). Thus these r-tuples comprise a ring isomorphic to I/m, as asserted in (4).

The direct sum extends from the rings to the corresponding ideals $\mathfrak{g}(m)$, $\mathfrak{g}(p_1^{n_1})$, etc. Let $f(x)$ be any polynomial in $\mathfrak{g}(m)$, say

$$f(x) = bx^t + cx^{t-1} + dx^{t-2} + \cdots. \tag{8}$$

Analogous to (6) the indeterminate x corresponds to an r-tuple $(x_1, x_2, \cdots, x_r)$, and so we can set up the correspondence

$$\begin{aligned}bx^t \leftrightarrow (b_1, b_2, \cdots, b_r)(x_1, x_2, \cdots, x_r)^t &= (b_1, b_2, \cdots, b_r)(x_1^t, x_2^t, \cdots, x_r^t)\\ &= (b_1x_1^t, b_2x_2^t, \cdots, b_rx_r^t).\end{aligned}$$

Using similar representations of the other terms of (8) as r-tuples, we have

$$\begin{aligned}&f(x) \leftrightarrow (f_1(x_1), f_2(x_2), \cdots, f_r(x_r)), \text{ where}\\ &f_j(x_j) = b_jx_j^t + c_jx_j^{t-1} + d_jx_j^{t-2} + \cdots.\end{aligned} \tag{9}$$

THEOREM 2. *Analogous to* (4), *the ideal* $\mathfrak{g}(m)$ *is a direct sum of ideals*

[1] Cf. N. H. McCoy, *Rings and ideals*, Carus Monograph No. 8, pp. 114–120.

$$g(m) = g(p_1^{n_1}) + g(p_2^{n_2}) + \cdots + g(p_r^{n_r}).$$

PROOF. If $f(x)$ belongs to $g(m)$ then $f(a)=0$ for every a in I/m. Hence the jth component of $f(x)$ in (9) has the property that $f_j(a_j)=0$ for every a_j in $I/p_j^{n_j}$. Conversely, suppose we have for $j=1, 2, \cdots, r$ a set of polynomials $f_j(x_j)$ with coefficients in $I/p_j^{n_j}$, such that $f_j(a_j)=0$ for every a_j in $I/p_j^{n_j}$. Then by (9) these polynomials define a unique polynomial $f(x)$ with coefficients in I/m, and it is clear that $f(a)=0$ for every a in I/m.

We now show that this direct sum gives us a basis for $g(m)$ from the known bases for $g(p_j^{n_j})$.

THEOREM 3. *For each generator $g_j(x_j)$ of $g(p_j^{n_j})$ define a polynomial $g(x)$ by the correspondence, similar to* (9),

$$g(x) \leftrightarrow (0, 0, \cdots, 0, g_j(x_j), 0, \cdots, 0), \tag{10}$$

where all components except the jth are zero. The totality of such $g(x)$ constitutes a basis for $g(m)$. Thus if we have say s_1 generators of type (1) *for $g(p_1^{n_1})$, s_2 for $g(p_2^{n_2})$, $\cdots$, s_r for $g(p_r^{n_r})$, then we have in all $\sum_{i=1}^{r} s_i$ generators* (10) *for $g(m)$.*

PROOF. Any polynomial $f(x)$ of I/m can be represented in the r-tuple form (9), and this in turn can be written as a sum

$$(f_1(x_1), 0, \cdots, 0) + (0, f_2(x_2), 0, \cdots, 0) + \cdots + (0, 0, \cdots, 0, f_r(x_r)).$$

Now $f_j(a_j)=0$ for every a_j in $I/p_j^{n_j}$, and hence each term of this sum can be expressed in terms of the generators (10).

This theorem can be stated in the language of number theory, without any direct sum notation, as follows.

THEOREM 3 (2D FORMULATION). *Let $m=p_1^{n_1}p_2^{n_2}\cdots p_r^{n_r}$ be the representation of m as a product of powers of distinct primes. For each generator*

$$g(x) = a_q x^q + a_{q-1}x^{q-1} + \cdots + a_0$$

of $g(p_j^{n_j})$, define a polynomial

$$G(x) = A_q x^q + A_{q-1}x^{q-1} + \cdots + A_0,$$

where the coefficients A_k satisfy the congruence relations

$$A_k \equiv 0 \pmod{p_i^{n_i}}, \qquad i = 1, 2, \cdots, r, i \neq j,$$
$$A_k \equiv a_k \pmod{p_j^{n_j}}.$$

The totality of such $G(x)$ constitutes a basis for $g(m)$.

EXAMPLE. $m=45$. We have seen earlier that $g(9)$ has the generators

$3x^3+6x$ and $x^6+3x^5+4x^4+4x^2+6x$. Now $\mathfrak{g}(5)$ has the single generator x^5+4x. Using the second formulation of Theorem 3 we see that $\mathfrak{g}(45)$ has a basis

$$30x^3 + 15x, \quad 10x^6 + 30x^5 + 40x^4 + 40x^2 + 15x, \quad 36x^5 + 9x.$$

REMARKS. We have stated Theorem 2 for the special direct sum (4). It could have been stated for any direct sum of commutative rings

$$R = R_1 \dotplus R_2 \dotplus \cdots \dotplus R_r.$$

Thus let S be the ideal of all polynomials $f(x)$ over R such that $f(a)=0$ for every a in R. Let $S_1, S_2, \cdots, S_r$ be the corresponding ideals for $R_1, R_2, \cdots, R_r$. Then the obvious generalization of Theorem 2 is that

$$S = S_1 \dotplus S_2 \dotplus \cdots \dotplus S_r.$$

A similar generalization holds for Theorem 3.

4. Nonprincipal ideals.

THEOREM 4. *The ideal $\mathfrak{g}(m)$ is principal if and only if m is a prime.*

PROOF. If m is a prime p then $\mathfrak{g}(p)$ has a single generator by Theorem 1. Conversely, assume that $\mathfrak{g}(m)$ is a principal ideal for some value of m. Then for any prime divisor p of m the polynomial

$$f(x) = \frac{m}{p} \prod_{j=0}^{p-1} (x - j)$$

belongs to $\mathfrak{g}(m)$. Hence the generator of the ideal is either $f(x)$ or some divisor of $f(x)$. But no proper divisor of $f(x)$ is in the ideal, because (i) the proper divisor $f(x)/(x-j)$ does not vanish at $x=j$, and (ii), if m_1 is a proper divisor of m/p, then the polynomial

$$m_1 \prod_{j=0}^{p-1} (x - j)$$

does not vanish at $x=p$. Hence the generator of the ideal $\mathfrak{g}(m)$ is $f(x)$.

Next we observe that m cannot have more than one prime factor. For if m had another prime factor besides p, say p_1, then by the argument of the last paragraph the polynomial

$$f_1(x) = \frac{m}{p_1} \prod_{j=0}^{p_1-1} (x - j)$$

would also be a generator, contrary to the assumption that $\mathfrak{g}(m)$ is a principal ideal.

Thus m has the form p^n, and the single generator is

$$f(x) = p^{n-1} \prod_{j=0}^{p-1} (x - j).$$

If $n > 1$, then the polynomial

$$\prod_{j=0}^{p^n-1} (x - j)$$

is also in the ideal, but this polynomial is not a multiple of $f(x)$. Hence $n = 1$ and $m = p$.

UNIVERSITY OF OREGON AND
SAN DIEGO STATE COLLEGE