JOURNAL OF NUMBER THEORY 6, 345–352 (1974)

On Polynomial Functions (mod m)

DAVID SINGMASTER

Department of Mathematics, Polytechnic of the South Bank, London, SE1 0AA, England

Communicated by H. B. Mann

Received February 16, 1972

In this paper, we obtain a canonical representation for those polynomials (with integer coefficients) which vanish (mod m), a canonical representation for each polynomial function (mod m) and an expression for the number of polynomial functions (mod m). This number turns out to be (weakly) multiplicative in m.

1. INTRODUCTION

In a previous paper [1], I have found the monic binomial of least degree which vanishes identically (mod m). The original motivation for that paper and the present one was to find the number of polynomial functions (mod m). In this paper, I am now able to present a canonical representation for those polynomials which vanish (mod m), a canonical representation for each polynomial function (mod m) and an expression for the exact number of polynomial functions (mod m), which turns out to be (weakly) multiplicative in m.

2. CONVENTIONS

Henceforth, we shall be concerned with several kinds of equality, so we shall pause briefly to consider them, in order to avoid future confusion. The symbol ($=$) will be used to denote ordinary equality. The symbol ($\equiv$) will be used to denote congruence (mod m), i.e., equality in $\mathbf{Z}_m$, the ring of residue classes (mod m). The modulus of a congruence will always be m unless otherwise specified.

We shall use capital letters F, G, S, etc. to represent elements of $\mathbf{Z}[X]$, the polynomial ring in X over $\mathbf{Z}$, the ring of integers. An equality $F = G$ or $F(X) = G(X)$ means that F and G are equal as elements of $\mathbf{Z}[X]$, i.e., they have corresponding coefficients equal. Any polynomial in $\mathbf{Z}[X]$ gives

rise to a polynomial in $\mathbf{Z}_m[X]$ and we shall use the same letter for this. Then a congruence $F \equiv G$ or $F(X) \equiv G(X)$ shall mean that F and G are equal as elements of $\mathbf{Z}_m[X]$, i.e., that F and G have corresponding coefficients congruent (mod m).

We shall use small letters f, g, s, etc. to represent functions from $\mathbf{Z}_m$ to $\mathbf{Z}$. Each such function gives rise to a function from $\mathbf{Z}_m$ to $\mathbf{Z}_m$, which we designate by the same letter. An equality $f(x) = g(x)$ will denote equality between the integers $f(x)$ and $g(x)$, while $f(x) \equiv g(x)$ will denote congruence between them. Then $f \equiv g$ will mean that f and g are equal as functions from $\mathbf{Z}_m$ to $\mathbf{Z}_m$, i.e., that $f(x) \equiv g(x)$ for all x in $\mathbf{Z}_m$.

Given a polynomial $F(X)$ in $\mathbf{Z}[X]$ or in $\mathbf{Z}_m[X]$, we can define a function $f\colon \mathbf{Z}_m \to \mathbf{Z}_m$ by setting $f(a) \equiv F(a)$ for all a in $\mathbf{Z}_m$. Such a function is called a polynomial function (mod m) and we say that f is determined by, or corresponds to, F and that F represents f. Henceforth, we shall always use corresponding large and small letters in this way. Clearly $F \equiv G$ implies $f \equiv g$ but not conversely.

3. Preliminaries

First we state a form of the division algorithm which is valid in $\mathbf{Z}_m[X]$. (We agree that the degree of the zero polynomial shall be $-\infty$.) [2, p. 30]

Lemma 1. *Let F and G be in $\mathbf{Z}_m[X]$ and let G be monic. Then*

$$F \equiv G \cdot Q + R \quad \text{and} \quad \deg R < \deg G, \tag{1}$$

where Q and R are uniquely determined elements of $\mathbf{Z}_m[X]$.

Definition 2. For a given positive integer m, let $n = n(m)$ be the least integer such that $m \mid n!$.

Definition 3. $S_0(X) = 1, S_1(X) = X + 1, S_2(X) = (X + 2)(X + 1),\ldots,$ $S_k(X) = (X + k)\, S_{k-1}(X),\ldots,$ and s_k is the function determined by S_k.

Lemma 4. *$bs_k \equiv 0$ iff $bs_k(-k - 1) \equiv 0$ iff $m/(k!, m) \mid b$, where $(k!, m)$ is the* GCD *of $k!$ and m.*

Proof. $bs_k \equiv 0$ certainly implies $bs_k(-k - 1) \equiv 0$. We observe that $s_k(-k - 1) = (-k)(-k + 1) \cdots (-1) = (-1)^k k!$. Hence $bs_k(-k - 1) \equiv 0 \Rightarrow m \mid bk! \Rightarrow m/(k!, m) \mid b$. Finally, note that $s_k(a)$ is a product of k consecutive integers, hence is divisible by $k!$ for any a. So if $m/(k!, m) \mid b$, then $mk!/(k!, m)$ divides $bs_k(a)$ and hence $bs_k \equiv 0$ as a function: $\mathbf{Z}_m \to \mathbf{Z}_m$.

Corollary 5. *$s_k \equiv 0$ iff $k \geqslant n$.*

4. The Polynomial Representations of the Zero Function

THEOREM 6. *Let F be a polynomial in $\mathbf{Z}_m[X]$. Then $f \equiv 0$ iff*

$$F \equiv F_n S_n + \sum_{k=0}^{n-1} a_k (m/(k!, m))\, S_k , \tag{2}$$

where $n = n(m)$ as given in Definition 1; F_n is an arbitrary polynomial in $\mathbf{Z}_m[X]$, which is uniquely determined by F; and a_k is an arbitrary integer, uniquely determined (mod$(k!, m)$) *by F.*

Proof. If F is as described in the theorem, then $f \equiv 0$ follows easily from Lemma 4 and Corollary 5.

Conversely, we inductively establish the following assertion for all i, $0 \leqslant i \leqslant n$.

$$F \equiv F_i S_i + \sum_{k=0}^{i-1} a_k (m/(k!, m))\, S_k , \tag{3}$$

where F_i is a uniquely determined polynomial in $\mathbf{Z}_m[X]$, and is such that $f_i s_i \equiv 0$; and a_k is uniquely determined (mod$(k!, m)$). When $i = n$, then $s_n \equiv 0$, so that f_n and F_n are arbitrary, so the case $i = n$ is our theorem.

The case $i = 0$ is trivial since $S_0 = 1$ and the sum is empty. We have $F_0 = F$.

Suppose that (3) has been established for some $i < n$. Apply Lemma 1 to F_i and $X + i + 1$ to obtain $F_i \equiv F_{i+1}(X + i + 1) + R_{i+1}$, where R_{i+1} is a constant. By the Lemma, F_{i+1} and R_{i+1} are unique (mod m). Substituting this into (3) and recalling that $(X + i + 1)\, S_i = S_{i+1}$, we have

$$F \equiv F_{i+1} S_{i+1} + R_{i+1} S_i + \sum_{k=0}^{i-1} a_k (m/(k!, m))\, S_k . \tag{4}$$

Evaluating this at $X = -i - 1$, we get

$$0 \equiv f(-i - 1) \equiv f_{i+1}(-i - 1) \cdot 0 + R_{i+1} s_i (-i - 1) + 0,$$

since the terms in the sum are zero by Lemma 4.

Hence $0 \equiv R_{i+1} s_i (-i - 1)$ and we have $m/(i!, m) \mid R_{i+1}$, by Lemma 4. Setting $R_{i+1} \equiv a_i m/(i!, m)$ determines a_i uniquely (mod$(i!, m)$). Hence we can rewrite (4) in the form

$$F \equiv F_{i+1} S_{i+1} + \sum_{k=0}^{i} a_k (m/(k!, m))\, S_k ,$$

which is (3) for the case $i + 1$. Again applying Lemma 4, we see that $0 \equiv f \equiv f_{i+1} s_{i+1}$, completing the induction and the proof.

5. Corollaries to Theorem 6

Corollary 7. *If F is monic and $f \equiv 0$, then* $\deg F \geqslant n$.

Proof. If $F_n \equiv 0$ in (2), then the leading coefficient of F is $a_k m/(k!, m)$ for some k, so that F is not monic. Hence $F_n \not\equiv 0$ and $\deg F = \deg F_n S_n \geqslant \deg S_n = n$. Furthermore, S_n is a monic polynomial of degree n such that $s_n \equiv 0$, so that n is the best possible result.

Corollary 8. *There are $\prod_{k=0}^{n-1} (k!, m) = N_0(m)$ polynomials in $\mathbf{Z}_m[X]$ such that* $\deg F < n$ and $f \equiv 0$.

Proof. The hypotheses imply that F is of the form (2) where $F_n \equiv 0$. Any such F is uniquely determined by the choice of the constants a_k (mod$(k!, m)$). Clearly there are $(k!, m)$ ways to choose a_k (mod$(k!, m)$), so there are $\prod_{k=0}^{n-1} (k!, m)$ such polynomials.

Corollary 9. *There are $\prod_{k=0}^{n-1} m/(k!, m) = m^n/N_0(m) = N_1(m)$ distinct polynomial functions* (mod m).

Proof. Let the ring of polynomial functions be R. The mapping: $\mathbf{Z}_m[X] \to R$ given by $F \to f$ is a homomorphism with kernel $R_0 = \{F \mid f \equiv 0\}$. Hence $R = \mathbf{Z}_m[X]/R_0$. Let $S = (S_n)$ be the principal ideal generated by S_n. Then $S \subset R_0$, so we have $R = (\mathbf{Z}_m[X]/S)/(R_0/S)$. Since S_n is monic, it follows from Lemma 1 that $\mathbf{Z}_m[X]/S$ can be viewed as the ring of all polynomials F in $\mathbf{Z}_m[X]$ such that $\deg F < n$, where multiplication is taken (mod S_n). Under this representation, R_0/S is identified with the set of all polynomials F in $\mathbf{Z}_m[X]$ such that $\deg F < n$ and $f \equiv 0$. Let $\#(T)$ be the number of elements in the set T. Then we have $N_1(m) = \#(R) = \#(\mathbf{Z}_m[X]/S)/\#(R_0/S) = m^n/N_0(m) = \prod_{k=0}^{n-1} m/(k!, m) = \prod_{k=0}^{n-1} [k!, m]/k!$. This result can also be obtained from Theorem 10.

6. The Canonical Representation of a Polynomial Function

Theorem 10. *Let f be a polynomial function* (mod m). *Then f has a unique polynomial representation $F = \sum_{k=0}^{n-1} b_k X^k$ with $0 \leqslant b_k < m/(k!, m)$.*

Proof. Let G be any polynomial representing f. From Lemma 1, we may write $G \equiv Q \cdot S_n + G_0$, where $\deg G_0 < \deg S_n = n$. Then $f \equiv g \equiv q \cdot 0 + g_0 \equiv g_0$, so that G_0 also represents f. Write $G_0 = \sum_{k=0}^{n-1} c_k X^k$. Apply the division algorithm to the integers c_{n-1} and $m/((n-1)!, m)$, obtaining $c_{n-1} = q_{n-1} m/((n-1)!, m) + b_{n-1}$, where $0 \leqslant b_{n-1} < m/((n-1)!, m)$. Set $G_1 = G_0 - q_{n-1} m/((n-1)!, m) S_{n-1}$. The $(n-1)$st coefficient of G_1 is b_{n-1} and $g_1 \equiv g_0 - 0 \equiv f$.

Clearly, one can continue inductively, each time obtaining a G_i such that $g_i \equiv f$ and G_i has its i leading coefficients satisfying the conditions of the theorem. The step $i = n$ is the theorem, upon setting $F \equiv G_n$. The uniqueness of F follows easily from Theorem 6 by standard techniques.

7. Miscellaneous Further Results

Proposition 11. *$n(m) \leqslant m$ with equality iff m is a prime, $m = 1$ or $m = 4$.*

Proof. Straightforward.

Proposition 12. *$n(m) \leqslant \lambda(m) + N(m)$, where $\lambda(m)$ and $N(m)$ are as defined in* [1, p. 103].

Proof. In [1], I showed that if $F(X) = X^{\lambda(m)+N(m)} - X^{N(m)}$, then $f \equiv 0$. The proposition then follows from Corollary 7.

Proposition 13. *$N_0(m) = 1$ iff m is prime or $m = 1$.*

Proof. This follows from the definition of $N_0(m)$ given in Corollary 8 and from Definition 2.

Proposition 14. *$N_1(m) \leqslant m^n \leqslant m^m$, with both equalities holding simultaneously iff m is prime or $m = 1$.*

Proof. This follows from Corollary 9, Proposition 13 and Proposition 11.

Proposition 14 gives another proof of the result proven in [1], that every function $f\colon \mathbf{Z}_m \to \mathbf{Z}_m$ is a polynomial function if and only if m is a prime or $m = 1$.

Proposition 15. *$n(a) + n(b) \geqslant n(ab) \geqslant \max(n(a), n(b))$ and $(a, b) = 1$ is sufficient for equality on the right.*

Proof. We have $s_{n(a)} \equiv 0 \pmod{a}$ by Corollary 5. Hence $s_{n(a)}(n(b)) = (n(a) + n(b))!/n(b)! \equiv 0 \pmod{a}$ and so $(n(a) + n(b))! \equiv 0 \pmod{ab}$, i.e., $n(a) + n(b) \geqslant n(ab)$.

We have $ab \mid n(ab)! \Rightarrow a \mid n(ab)! \Rightarrow n(ab) \geqslant n(a)$. Similarly, $n(ab) \geqslant n(b)$, hence $n(ab) \geqslant \max(n(a), n(b))$.

Now assume $(a, b) = 1$. $a \mid n(a)!$ and $b \mid n(b)! \Rightarrow a \mid (\max(n(a), n(b)))!$ and $b \mid (\max(n(a), n(b)))!$. Since $(a, b) = 1$, this gives $ab \mid (\max(n(a), n(b)))!$, hence $n(ab) \leqslant \max(n(a), n(b))$.

PROPOSITION 16. $N_1(m) = \prod_{k=0}^{n-1} m/(k!, m)$ *is (weakly) multiplicative in* m.

Proof. First we observe that $k \geqslant n \Rightarrow m \mid k! \Rightarrow (k!, m) = m$, so $N_1(m) = \prod_{k=0}^{\infty} m/(k!, m)$, i.e., the dependence on $n(m)$ is only illusory. Next, if $m = rs$ with $(r, s) = 1$, then $(k!, rs) = (k!, r)(k!, s)$ for all k which gives $N_1(m) = N_1(r)\, N_1(s)$.

When m is a prime p, we know that

$$(*) \qquad X(X+1)\cdots(X+p-1) \equiv X^p - X.$$

The left-hand side is equal to $XS_{p-1} \equiv S_p$. The congruence (*) can be obtained from Theorem 6 as follows. Consider $F(X) = X^p - X$. Then $f \equiv 0$ by Fermat's Theorem. Hence F must be of the form (2) of Theorem 6. Since $\deg F = p$ and $n(p) = p$ and F is monic, we must have $F_p = F_n \equiv 1$. Further, $(k!, p) = 1$ and so $p/(k!, p) = 0 \pmod p$ for $p > k \geqslant 0$. Hence the expression (2) for F must reduce to simply S_p, i.e., we have shown that $X^p - X \equiv S_p \equiv X(X+1)\cdots(X+p-1)$. Using the relationship between our S_p and the Stirling numbers of the first kind, one can obtain congruences for the Stirling numbers of the first kind.

Below we give some values for $n(m)$, $N_0(m)$, $N_1(m)$.

m	$n(m)$	$N_0(m)$	$N_1(m)$
1	0	1	1
p prime	p	1	p^p
4	4	4	64
6	3	2	108
8	4	4	1024
9	6	27	19683
10	5	8	12500
12	4	12	1728
14	7	32	3294172
16	6	256	65536
18	6	432	8728
20	5	16	200000

8. ADDED IN TYPESCRIPT (April 3, 1973)

I have recently discovered some related previous work. The polynomials F such that $f \equiv 0$ are clearly an ideal in $\mathbf{Z}_m[X]$. Niven and Warren [3] showed that polynomials similar to my S_k form a basis of this ideal when

$m = p^e$. They then used the direct sum representation of $\mathbf{Z}_m$ and $\mathbf{Z}_m[X]$ to describe a basis in general. Keller and Olson [4] considered the case $m = p^e$ and obtained a result like Theorem 10 and a recursion for $N_1(p^e)(= r_e$ in their notation) but did not obtain anything like Corollary 9. Following their observation, one can compute: $n(p^2) = 2p$, $N_0(p^2) = p^p$ and $N_1(p^2) = p^{3p}$. Redei and Szele [5] obtained Corollary 9 and Proposition 16.

Following a suggestion of H. Tverberg, one can prove Theorem 6 in a much different manner. Let F be in $\mathbf{Z}[X]$ and let $\deg F = d$. If $f \equiv 0$, then $G(X) = F(X)/m$ is a polynomial in $\mathbf{Q}[X]$ such that $G(a)$ is an integer whenever a is. Applying Newton's formula, we have

$$G(X) = \sum_{k=0}^{d} (\Delta^k G)(0) \binom{X}{k}.$$

But $(\Delta^k G)(0)$ is an integral combination of the values $G(0), G(1),..., G(k)$ and hence is an integer which we denote as c_k. Since

$$mG(X) = F(X) = \sum_{k=0}^{d} mc_k \binom{X}{k}$$

has integral coefficients, we see that $mc_k/k!$ are all integers, by proceeding from $k = d$ to $k = 0$. Hence $k!/(k!, m)$ divides c_k and we can write $a_k = c_k(k!, m)/k!$. If we consider F as in $\mathbf{Z}_m[X]$, then the coefficients $mc_k/k! = a_k(m/(k!, m))$ are uniquely determined (mod m), so that a_k is uniquely determined (mod$(k!, m)$). Separating our expression for $F(X)$ into the terms with $k \geqslant n$ and with $k < n$, we obtain Theorem 6, except that we now have the polynomials $1, X, X(X-1),...$ instead of $1, X+1, (X+2)(X+1),...$. However, the choice of polynomial sequence is fairly arbitrary and does not affect the actual content of the theorem or any of its consequences.

ACKNOWLEDGMENTS

In closing, I would like to thank Dr. Steven Bryant for originally posing the problem of determining $N_1(m)$ and Prof. R. M. Robinson for pointing out Proposition 16.

REFERENCES

1. DAVID SINGMASTER, A maximal generalization of Fermat's Theorem, *Math. Mag.* **39** (1966), 103–7.
2. O. ZARISKI AND P. SAMUEL, "Commutative Algebra," Vol. 1. Van Nostrand, Princeton, 1958.

3. IVAN NIVEN AND LEROY J. WARREN. A generalization of Fermat's theorem. *Proc. Amer. Math. Soc.* **8** (1957), 306–313.
4. GORDON KELLER AND F. R. OLSON. Counting polynomial functions (mod p^n). *Duke Math. J.* **35** (1968), 835–838.
5. L. REDEI AND T. SZELE. Algebraisch–Zahlentheoretische Betrachtungen über Ringe, II. *Acta Math.* **82** (1950), 209–241.