Enumerating Annihilator Polynomials over $\mathbb{Z}_n$

Navin Kashyap[†] Alexander Vardy[†]

January 27, 2005

Abstract

In this paper, we present characterizations of annihilator polynomials over the ring, $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$, of integers modulo n. These characterizations are used to derive an expression for the number of annihilator polynomials of degree k over $\mathbb{Z}_n$, as well as one for the number of monic annihilators of degree k.

1 Introduction

Given the ring, $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$, of integers modulo n, and a polynomial, $f(x) \in \mathbb{Z}_n[x]$, over $\mathbb{Z}_n$, we say that $f(x)$ *annihilates* $\mathbb{Z}_n$ if $f(l) \equiv 0 \pmod{n}$ for all $l \in \mathbb{Z}_n$. A polynomial over $\mathbb{Z}_n$ that annihilates $\mathbb{Z}_n$ is called an *annihilator polynomial*. We shall denote the set of all annihilator polynomials of degree k over $\mathbb{Z}_n$ by $\mathcal{A}(n,k)$, and the cardinality of this set by $A(n,k)$. To allow for the zero polynomial ($f(x) \equiv 0$), we shall let $\mathcal{A}(n,0) = \{0\}$, so that $A(n,0) = 1$. We shall also be interested in *monic* polynomials, *i.e.*, polynomials $f(x) = \sum_{i=0}^{k} a_i x^i$ with $a_k = 1$, that annihilate $\mathbb{Z}_n$. The set of monic annihilator polynomials of degree k over $\mathbb{Z}_n$ shall be denoted by $\mathcal{M}(n,k)$, and we set $M(n,k) = |\mathcal{M}(n,k)|$.

If p is prime, then $\mathbb{Z}_p$ is a field, and it is well-known that annihilator polynomials over $\mathbb{Z}_p$ are precisely all the multiples of $x^p - x$. It follows that, for $k \geq p$, we have $A(p,k) = p^{k-p}(p-1)$ and $M(p,k) = p^{k-p}$, and for $1 \leq k < p$, $A(p,k) = M(p,k) = 0$. In this paper, we find characterizations of annihilator polynomials over $\mathbb{Z}_n$ for an arbitrary integer n, which we use to derive expressions for $A(n,k)$ and $M(n,k)$.

Given an integer $n > 0$, we shall find it useful to associate with it another integer $S(n)$, defined as the smallest integer $j > 0$ such that $n|j!$ (*i.e.* n divides $j!$). $S(n)$ is often called the nth *Smarandache number*. For example, we have $S(1) = 1$, $S(2) = 2$, $S(6) = 3$, $S(8) = 4$ and so on. It is not hard to see that $S(p) = p$ for any prime p, and if $n = \prod_{i=1}^{s} {p_i}^{m_i}$ is the prime factorization of n, then $S(n) = \max\{S({p_i}^{m_i}) \ : \ i = 1, 2, \ldots, s\}$.

The paper is organized as follows. We first show in Section 2 that the problem of analyzing annihilator polynomials over $\mathbb{Z}_n$, for an arbitrary integer n, can be reduced to one of characterizing such polynomials over $\mathbb{Z}_n$ with n a prime power, *i.e.* $n = p^m$ where p is prime and m is a positive integer. It turns out that the latter problem was independently solved by Sophie Frisch [1] in the far more general setting of polynomials over finite commutative local rings. In Section 3, we present Frisch's result in the special case of the ring $\mathbb{Z}_{p^m}$, and use the result to determine expressions for $A(n,k)$ and $M(n,k)$. Finally, in Section 4, we prove an alternative characterization of annihilators over $\mathbb{Z}_{p^m}$, which unfortunately only holds for $m \leq p$, but which is more in the spirit of the characterization of annihilators over $\mathbb{Z}_p$ mentioned above.

[†]Dept. of Electrical and Computer Engg., University of California, San Diego, CA 92093-0407.
Email: {nkashyap,vardy}@ece.ucsd.edu.

2 Reduction to the Case of n a Prime Power

In this section, we shall show that in order to characterize annihilator polynomials over $\mathbb{Z}_n$, it is sufficient to find a characterization of annihilator polynomials over $\mathbb{Z}_{p^m}$, where p is prime and m is some positive integer. Let $n = \prod_{i=1}^{s} {p_i}^{m_i}$ be the prime factorization of n, and let $q_i = {p_i}^{m_i}$, $i = 1, 2, \ldots, s$.

THEOREM 1 *If $f(x) \in \mathbb{Z}_n[x]$ is an annihilator over $\mathbb{Z}_n$, then for $i = 1, 2, \ldots, s$, $f_i(x) = f(x) \bmod q_i$ is an annihilator over $\mathbb{Z}_{q_i}$. Conversely, given polynomials $f_i(x) \in \mathbb{Z}_{q_i}[x]$, $i = 1, 2, \ldots, s$, such that $f_i(x)$ annihilates $\mathbb{Z}_{q_i}$, there exists a unique $f(x) \in \mathbb{Z}_n[x]$ that annihilates $\mathbb{Z}_n$, such that $f(x) \equiv f_i(x) \pmod{q_i}$.*

Proof: If $f(x) \in \mathbb{Z}_n[x]$ annihilates $\mathbb{Z}_n$, then it is clear that $f_i(x) = f(x) \bmod q_i$ annihilates $\mathbb{Z}_{q_i}$. The converse statement in the theorem is a consequence of the Chinese remainder theorem (CRT). This is because if, for $i = 1, 2, \ldots, s$, $f_i(x) = \sum_{j \geq 0} a_{i,j} x^j$ with $a_{i,j} \in \mathbb{Z}_{q_i}$, then by the CRT, for each $j \geq 0$, there exists a unique $a_j \in \mathbb{Z}_n$ such that $a_j \equiv a_{i,j} \pmod{q_i}$, $i = 1, 2, \ldots, s$. Hence, $f(x) = \sum_{j \geq 0} a_j x^j$ is the unique polynomial in $\mathbb{Z}_n[x]$ such that $f(x) \equiv f_i(x) \pmod{q_i}$ for each i, and by the CRT again, $f(x)$ annihilates $\mathbb{Z}_n$ since for each i, $f_i(x)$ annihilates $\mathbb{Z}_{q_i}$. ■

Note that with $f(x)$ and $f_i(x)$, $i = 1, 2, \ldots, s$, as in the statement of the theorem, $f(x)$ is of degree k if and only if all the $f_i(x)$'s are of degree at most k, with at least one $f_i(x)$ being of degree exactly k. Thus, the above theorem shows that there is a one-to-one correspondence between $\mathcal{A}(n, k)$ and the set of all s-tuples $(f_1(x), f_2(x), \ldots, f_s(x))$ such that each $f_i(x)$ is of degree at most k and at least one $f_i(x)$ has degree exactly k. In other words, $\mathcal{A}(n, k)$ is in one-to-one correspondence with $\prod_{i=1}^{s} \cup_{j=0}^{k} \mathcal{A}(q_i, j) \setminus \prod_{i=1}^{s} \cup_{j=0}^{k-1} \mathcal{A}(q_i, j)$, from which we obtain the following result.

COROLLARY 2 *For any $k \geq 0$, $A(n, k) = \prod_{i=1}^{s} \sum_{j=0}^{k} A(q_i, j) - \prod_{i=1}^{s} \sum_{j=0}^{k-1} A(q_i, j)$.*

Thus, in order to determine $A(n, k)$ for arbitrary integers n and k, it is sufficient to restrict our attention to n's that are powers of primes.

The expression for $M(n, k)$, the number of monic annihilator polynomials of degree k over $\mathbb{Z}_n$, in terms of the number of annihilators over $\mathbb{Z}_{q_i}$ is considerably simpler. Observe that if $f(x)$ is in $\mathcal{M}(n, k)$, then for $i = 1, 2, \ldots, s$, $f_i(x) = f(x) \bmod q_i$ belongs to $\mathcal{M}(q_i, k)$. Conversely, if we are given polynomials $f_i(x) \in \mathcal{M}(q_i, k)$, $i = 1, 2, \ldots, s$, then it follows from the Chinese remainder theorem that there exists a unique polynomial $f(x) \in \mathcal{M}(n, k)$ such that $f(x) \equiv f_i(x) \pmod{q_i}$. Consequently, the sets $\mathcal{M}(n, k)$ and $\prod_{i=1}^{s} \mathcal{M}(q_i, k)$ have the same cardinality, which shows that $M(n, k)$ can be expressed in terms of the $M(q_i, k)$'s as follows.

COROLLARY 3 *For any $k \geq 0$, $M(n, k) = \prod_{i=1}^{s} M(q_i, k)$.*

So, to derive an expression for $M(n, k)$ for arbitrary n and k, it once again suffices to consider n's that are powers of primes. Much of the remainder of this paper is devoted to finding characterizations of annihilator polynomials over $\mathbb{Z}_{p^m}$, with p prime and m a positive integer.

3 Annihilators over $\mathbb{Z}_{p^m}$

As mentioned in the introduction, a characterization of annihilator polynomials over a fairly general class of finite commutative local rings, which includes $\mathbb{Z}_{p^m}$, was found by S. Frisch ([1],

Proposition 1). For the sake of completeness, we present a proof of this result in the case of the ring $\mathbb{Z}_{p^m}$.

Let us first define the polynomials $f_0(x) = 1$ and $f_j(x) = \prod_{i=0}^{j-1}(x-i)$, for $j \geq 1$. It is a fact that any polynomial $f(x) \in \mathbb{Z}[x]$ can be *uniquely* written as a $\mathbb{Z}$-linear combination of these $f_j(x)$'s, *i.e.* $f(x)$ has a unique representation of the form $\sum_{j\geq 0} c_j f_j(x)$, for some choice of integers c_j. In other words, the $f_j(x)$'s form a basis for the $\mathbb{Z}$-module $\mathbb{Z}[x]$. This is because, as is easily verified, any monomial x^i can be written as a $\mathbb{Z}$-linear combination of the $f_j(x)$'s, and the polynomials $f_j(x)$ are linearly independent over $\mathbb{Z}$.

Annihilator polynomials over $\mathbb{Z}_{p^m}$ have a representation involving these polynomials $f_j(x)$, as shown in the following theorem.

THEOREM 4 *$f(x) \in \mathbb{Z}_{p^m}[x]$ annihilates $\mathbb{Z}_{p^m}$ if and only if*

$$f(x) \equiv \sum_{j\geq 1} a_j p^{m-\alpha(j)} f_j(x) \pmod{p^m}$$

for some $a_j \in \mathbb{Z}_{p^{\alpha(j)}}$, $j \geq 1$, where $\alpha(j)$ is defined to be the largest $\alpha \in \{0, 1, 2, \ldots, m\}$ such that $p^\alpha | j!$.

Proof: We first show that if $f(x) \equiv \sum_{j\geq 1} a_j p^{m-\alpha(j)} f_j(x) \pmod{p^m}$, then $f(x)$ annihilates $\mathbb{Z}_{p^m}$. We need to show that $f(t) \equiv 0 \pmod{p^m}$ for all $t \in \mathbb{Z}_{p^m}$. So, fix an arbitrary $t \in \mathbb{Z}_{p^m}$. It suffices to show that for any $j \geq 1$, $p^{m-\alpha(j)} f_j(t) \equiv 0 \pmod{p^m}$. Note that $f_j(t)$, when evaluated over $\mathbb{Z}$, is the product of j consecutive integers, and hence, $j! | f_j(t)$. Furthermore, by definition of $\alpha(j)$, $p^{\alpha(j)} | j!$, and so we see that $p^{\alpha(j)} | f_j(t)$. Therefore, p^m divides $p^{m-\alpha(j)} f_j(t)$, which means that $p^{m-\alpha(j)} f_j(t) \equiv 0 \pmod{p^m}$, as desired.

For the converse, suppose that $f(x) \in \mathbb{Z}[x]$ is a polynomial such that $f(x) \bmod p^m$ annihilates $\mathbb{Z}_{p^m}$. So, $f(t) \equiv 0 \pmod{p^m}$ for all $t \in \mathbb{Z}_{p^m}$. Since $f(x)$ has a representation of the form $\sum_{j\geq 0} c_j f_j(x)$ for some c_j's in $\mathbb{Z}$, we only need to show that $c_0 \equiv 0 \pmod{p^m}$, and for all $j \geq 1$, $c_j \equiv a_j p^{m-\alpha(j)} \pmod{p^m}$ for some $a_j \in \mathbb{Z}_{p^{\alpha(j)}}$.

Recall that $S(p^m)$ is the smallest integer $l > 0$ such that $p^m | l!$. Hence, for all $j \geq S(p^m)$, $\alpha(j) = m$, so that the congruence $c_j \equiv a_j p^{m-\alpha(j)} \pmod{p^m}$ is trivially satisfied for any $j \geq S(p^m)$. So, it is only the c_j's for $j < S(p^m)$ that need to be analyzed. Here, we shall show by induction on j that for $0 \leq j < S(p^m)$, $c_j \equiv 0 \pmod{p^{m-\alpha(j)}}$, so that $c_j \equiv a_j p^{m-\alpha(j)} \pmod{p^m}$ with $a_j \in \mathbb{Z}_{p^{\alpha(j)}}$.

Since $f(0) \equiv 0 \pmod{p^m}$, we have $\sum_{j\geq 0} c_j f_j(0) \equiv 0 \pmod{p^m}$. However, $f_j(0) = 0$ for $j > 0$, by definition of the f_j polynomials, and so we get $c_0 \equiv 0 \pmod{p^m}$.

Now, suppose that $c_j \equiv 0 \pmod{p^{m-\alpha(j)}}$ for all $j < t$, t being some integer in $[0, S(p^m) - 1]$. To complete the induction step, we need to show that $c_t \equiv 0 \pmod{p^{m-\alpha(t)}}$. Note first that $f_k(t) = 0$ for all $k > t$, by definition of $f_k(x)$. Moreover, by the induction hypothesis, for all $j < t$, $c_j f_j(t) \equiv a_j p^{m-\alpha(j)} f_j(t) \pmod{p^m}$, for some $a_j \in \mathbb{Z}_{p^{\alpha(i)}}$. But, since $c_0 \equiv 0 \pmod{p^m}$, and as shown previously, $p^{m-\alpha(j)} f_j(t) \equiv 0 \pmod{p^m}$ for any $j \geq 1$ and $t \in \mathbb{Z}_{p^m}$, we therefore have $c_j f_j(t) \equiv 0 \pmod{p^m}$ for all $j < t$.

Therefore, $f(t) = \sum_{j\geq 0} c_j f_j(t) \equiv c_t f_t(t) \pmod{p^m}$. But since $f(t) \equiv 0 \pmod{p^m}$ for any $t \in \mathbb{Z}_{p^m}$, and $f_t(t) = t!$, we obtain $c_t(t!) \equiv 0 \pmod{p^m}$. Now, since $t < S(p^m)$, $\alpha(t)$ is the largest integer α such that $p^\alpha | t!$. Therefore, $c_t(t!) \equiv 0 \pmod{p^m}$ implies that $c_t \equiv 0 \pmod{p^{m-\alpha(t)}}$, thus completing the inductive step of the proof. ■

It should be noted that each $f(x) \in \mathbb{Z}_{p^m}[x]$ that annihilates $\mathbb{Z}_{p^m}$ has a unique representation of the form $\sum_{j\geq 1} a_j p^{m-\alpha(j)} f_j(x) \bmod p^m$ with $a_j \in \mathbb{Z}_{p^{\alpha(j)}}$. This is because we may regard

any polynomial with coefficients in $\mathbb{Z}_{p^m}$ as a polynomial having coefficients in $\mathbb{Z}$, with all the coefficients being restricted to the interval $[0, p^m - 1]$. As observed earlier, each polynomial with integer coefficients can be uniquely expressed as a $\mathbb{Z}$-linear combination of the polynomials $f_j(x)$, and this representation must remain unique upon reduction modulo p^m.

From the uniqueness of the representation in Theorem 4, it is clear that $A(p^m, k)$ is precisely the number of degree-k polynomials of the form $\sum_{j\geq 1} a_j p^{m-\alpha(j)} f_j(x)$ with $a_j \in \mathbb{Z}_{p^{\alpha(j)}}$. Similarly, $M(p^m, k)$ is the number of monic polynomials of degree k of this form, leading us to the following result.

COROLLARY 5 *Let $n = p^m$. (i) For all $k \geq 0$, $A(n,k) = (p^{\alpha(k)} - 1)\ p^{\sum_{j=1}^{k-1} \alpha(j)}$.*
(ii) For $0 \leq k < S(n)$, $M(n,k) = 0$. For $k \geq S(n)$, $M(n,k) = p^{m(k-S(n))}\ p^{\sum_{j=1}^{S(n)-1} \alpha(j)}$.

Proof: Since each polynomial $f_j(x)$ is monic of degree j, it follows from Theorem 4 that $f(x) \in \mathcal{A}(p^m, k)$ if and only if $f(x) \equiv \sum_{j=1}^{k} a_j p^{m-\alpha(j)} f_j(x) \pmod{p^m}$ for some $a_j \in \mathbb{Z}_{p^{\alpha(j)}}$, $j = 1, 2, \ldots, k$, with $a_k \neq 0$. The expression for $A(p^m, k)$ now follows by counting the number of ways of choosing the a_j's.

We next show that $M(p^m, k) = 0$ for $0 \leq k < S(p^m)$. If $0 \leq k < S(p^m)$, then for all $j \leq k$, $\alpha(j) < m$, so that $p | p^{m-\alpha(j)}$. Therefore, $p^{m-\alpha(j)} \equiv 0 \pmod{p}$ for all $j \leq k$, and hence if $f(x) \in \mathcal{A}(p^m, k)$, then $f(x) \equiv 0 \pmod{p}$. In particular, $f(x)$ cannot be monic, which shows that $M(p^m, k) = 0$.

If $k \geq S(p^m)$, then Theorem 4 shows that $f(x) \in \mathcal{A}(p^m, k)$ if and only if

$$f(x) \equiv \sum_{j=1}^{S(p^m)-1} a_j p^{m-\alpha(j)} f_j(x) + \sum_{j=S(p^m)}^{k} a_j f_j(x) \pmod{p^m}$$

with $a_j \in \mathbb{Z}_{p^{\alpha(j)}}$ for $1 \leq j \leq S(p^m) - 1$ and $a_j \in \mathbb{Z}_{p^m}$ for $j \geq S(p^m)$, since $\alpha(j) = m$ for all $j \geq S(p^m)$. In particular, $f(x)$ is monic if and only if it is of the above form with $a_k = 1$, so the expression for $M(p^m, k)$ now follows by counting. ■

Corollaries 2, 3 and 5 together yield exact expressions for $A(n,k)$ and $M(n,k)$ for arbitrary integers n and k. In particular, it follows from Corollaries 3 and 5 that for an arbitrary integer n, $M(n,k) = 0$ if and only if $k < S(n)$, since as noted in Section 1, if $n = \prod_{i=1}^{s} {p_i}^{m_i}$ is the prime factorization of n, then $S(n) = \max\{S({p_i}^{m_i}) \ : \ i = 1, 2, \ldots, s\}$.

4 A Characterization of Annihilators over $\mathbb{Z}_{p^m}$ when $m \leq p$

As is well-known, since $\mathbb{Z}_p$ is a field, $f(x) \in \mathbb{Z}_p[x]$ annihilates $\mathbb{Z}_p$ if and only if $f(x) \equiv (x^p - x)g(x) \pmod{p}$ for some $g(x) \in \mathbb{Z}_p[x]$. This characterization of annihilator polynomials has a nice generalization that applies to annihilators over the ring $\mathbb{Z}_{p^m}$ with $m \leq p$. This characterization differs from the one in Theorem 4, and is stated in Theorem 8 below. Our derivation of this alternative characterization uses the notion of Hasse derivatives which we define next.

Given a polynomial $f(x) \in \mathbb{Z}[x]$, and an integer $j \geq 0$, let $D^j f(x)$ denote the jth formal derivative of $f(x)$. As usual, we take $D^0 f(x)$ to be $f(x)$ itself. We can then formally define the jth *Hasse derivative* of $f(x)$ to be $f^{(j)}(x) = \frac{1}{j!} D^j f(x)$. Now, the integers $1, 2, \ldots, p-1$ are all co-prime with p^m, and hence are all invertible in the ring $\mathbb{Z}_{p^m}$. Thus, if $f(x) \in \mathbb{Z}_{p^m}[x]$, then for $j = 0, 1, \ldots, p-1$, the Hasse derivatives $f^{(j)}(x)$, taken modulo p^m, are also polynomials in $\mathbb{Z}_{p^m}[x]$.

Our proof of Theorem 8 begins with the following lemma.

LEMMA 6 *Let $f(x), g(x)$ be polynomials in $\mathbb{Z}_p[x]$ such that $f(x) \equiv (x^p - x)^k g(x) \pmod{p}$, for some $k \in \{1, 2, \ldots, p-1\}$. Then, for all $r \in \mathbb{Z}_p$ and $j = k+1, k+2, \ldots, p-1$,*

$$f^{(j)}(r) \equiv (-1)^k g^{(j-k)}(r) \pmod{p}$$

Proof: We shall only prove the lemma for $k = 1$. The general result then easily follows by induction on k.

So, let $f(x) \equiv (x^p - x)g(x) \pmod{p}$. We need to show that for all $r \in \mathbb{Z}_p$, and $j = 1, 2, \ldots, p-1$, $f^{(j)}(r) \equiv -g^{(j-1)}(r) \pmod{p}$.

Let $h(x) = x^p - x$, so that $f(x) = g(x)h(x)$. Note that the product rule for Hasse derivatives is given by

$$f^{(j)}(x) = \sum_{l=0}^{j} g^{(j-l)}(x) h^{(l)}(x) \tag{1}$$

Now, for any $r \in \mathbb{Z}_p$, $h(r) = 0$ since $h(x)$ annihilates $\mathbb{Z}_p$. Furthermore, $h^{(1)}(r) = pr^{p-1} - 1 \equiv -1 \pmod{p}$, and for $l = 2, \ldots, p-1$, $h^{(l)}(r) = \binom{p}{l} r^{p-l} \equiv 0 \pmod{p}$, since $p | \binom{p}{l}$. The result for $k = 1$ now follows by plugging these into (1). ■

The above lemma is used to prove the following theorem, which is an important ingredient in our derivation of the alternative characterization of annihilator polynomials.

THEOREM 7 *Let $n = p^m$, $m \leq p$, p prime. If $f(x) \in \mathbb{Z}_n[x]$ annihilates $\mathbb{Z}_n$, then $f(x) \equiv (x^p - x)^m g(x) \pmod{p}$ for some $g(x) \in \mathbb{Z}_p[x]$.*

Proof: Let $f(x) \in \mathbb{Z}_n[x]$ be an annihilator for $\mathbb{Z}_n$. Our aim is to show by induction on j that for $j = 1, 2, \ldots, m$, $f(x) \equiv (x^p - x)^j g_j(x) \pmod{p}$ for some $g_j(x) \in \mathbb{Z}_p[x]$.

The fact that $f(x)$ annihilates $\mathbb{Z}_n$ shows that for any $a \in \mathbb{Z}_{p^{m-1}}$ and $r \in \mathbb{Z}_p$, $f(ap + r) \equiv 0 \pmod{p^m}$. Some straightforward manipulations modulo p^m show that $f(ap + r) \equiv \sum_{j=0}^{m-1} (ap)^j f^{(j)}(r) \pmod{p^m}$, so that we have

$$\sum_{j=0}^{m-1} (ap)^j f^{(j)}(r) \equiv 0 \pmod{p^m} \tag{2}$$

It should be kept in mind that the above equation holds for arbitrary $a \in \mathbb{Z}_{p^{m-1}}$ and $r \in \mathbb{Z}_p$.

Note first that as $f(x) \bmod p$ annihilates $\mathbb{Z}_p$, we must have $f(x) \equiv (x^p - x)g_1(x) \pmod{p}$ for some $g_1(x) \in \mathbb{Z}_p[x]$. This is because $\mathbb{Z}_p$ is a field, and so any annihilator for $\mathbb{Z}_p$ has to be a multiple of $(x^p - x)$.

Now, define $\mathcal{S}_k$ to be the following statement:

> For $j = 1, 2, \ldots, k$, $f(x) \equiv (x^p - x)^j g_j(x) \pmod{p}$ for some $g_j(x) \in \mathbb{Z}_p[x]$, and $f^{(k-j)}(r) \equiv 0 \pmod{p^j}$ for all $r \in \mathbb{Z}_p$.

As noted above, $\mathcal{S}_1$ is true. We shall show that if $\mathcal{S}_k$ is true for some $k \leq m-1$, then $\mathcal{S}_{k+1}$ is true as well.

So, suppose that $\mathcal{S}_k$ is true. Since $f(x) \equiv (x^p - x)^k g_k(x) \pmod{p}$, applying Lemma 6, we have for all $j = k+1, k+2, \ldots, p-1$, and any $r \in \mathbb{Z}_p$,

$$f^{(j)}(r) \equiv (-1)^k {g_k}^{(j-k)}(r) + pb_j \pmod{p^m}$$

for some $b_j \in \mathbb{Z}_{p^{m-1}}$, which may depend on r. Moreover, by the induction hypothesis, for any $r \in \mathbb{Z}_p$ and $j = 0, 1, \ldots, k-1$, $f^{(j)}(r) = p^{k-j}c_j$ for some integer c_j, which may also depend on r.

Plugging the above into (2), we get

$$\sum_{j=0}^{k-1}(ap)^j p^{k-j}c_j + \sum_{j=k}^{m-1}(ap)^j((-1)^k g_k{}^{(j-k)}(r) + pb_j) \equiv 0 \pmod{p^m} \tag{3}$$

Reducing the above equation modulo p^{k+1}, we get

$$p^k \sum_{j=0}^{k-1} a^j c_j + (ap)^k(-1)^k g_k(r) \equiv 0 \pmod{p^{k+1}}$$

Now, dividing the above congruence by p^k, we find that

$$\sum_{j=0}^{k-1} a^j c_j + a^k(-1)^k g_k(r) \equiv 0 \pmod{p} \tag{4}$$

Note that the above must hold for arbitrary $a \in \mathbb{Z}_{p^{m-1}}$ and $r \in \mathbb{Z}_p$.

Define the polynomial $h(x) = \sum_{j=0}^{k-1} c_j x^j + (-1)^k g_k(r)x^k$. From (4), we have $h(a) \equiv 0 \pmod{p}$ for all $a \in \mathbb{Z}_{p^{m-1}}$, so that $h(x) \bmod p$ annihilates $\mathbb{Z}_p$. However, $h(x)$ has degree $k \leq m-1 < p$, and so $h(x) \bmod p$ can annihilate $\mathbb{Z}_p$ only if $h(x) \equiv 0 \pmod{p}$. Therefore, $g_k(r) \equiv 0 \pmod{p}$. Since $r \in \mathbb{Z}_p$ is arbitrary, $g_k(x)$ annihilates $\mathbb{Z}_p$, and hence, $g_k(x) \equiv (x^p - x)g_{k+1}(x) \pmod{p}$ for some $g_{k+1}(x) \in \mathbb{Z}_p[x]$. Therefore, $f(x) \equiv (x^p - x)^k g_k(x) \equiv (x^p - x)^{k+1} g_{k+1}(x) \pmod{p}$.

The fact that $h(x) \equiv 0 \pmod{p}$ also implies that for $j = 0, 1, \ldots, k-1$, $c_j \equiv 0 \pmod{p}$. As a result, $f^{(j)}(r) = p^{k-j}c_j = p^{k+1-j}a_j$ for some integer a_j. Equivalently, for $j = 1, 2, \ldots, k$, $f^{(k+1-j)}(r) \equiv 0 \pmod{p^j}$. Moreover, this congruence holds for $j = k+1$ as well, since $f(r) \equiv 0 \pmod{p^m}$ implies that $f(r) \equiv 0 \pmod{p^{k+1}}$.

Thus, we have shown that if $\mathcal{S}_k$ is true for some $k \leq m-1$, then so is $\mathcal{S}_{k+1}$. Since $\mathcal{S}_1$ is true, by induction, $\mathcal{S}_m$ is true as well, which proves the theorem. ■

We are now ready to prove the following theorem.

THEOREM 8 *Let $n = p^m$, $m \leq p$. $f(x) \in \mathbb{Z}_n[x]$ annihilates Z_n if and only if*

$$f(x) \equiv \sum_{j=1}^{m} p^{m-j}(x^p - x)^j g_j(x) \pmod{p^m}$$

for some $g_1(x), g_2(x), \ldots, g_m(x) \in \mathbb{Z}_p[x]$. Moreover, the above representation of $f(x)$ is unique, i.e. *if $f(x) \equiv \sum_{j=1}^{m} p^{m-j}(x^p - x)^j g_j(x) \equiv \sum_{j=1}^{m} p^{m-j}(x^p - x)^j h_j(x) \pmod{p^m}$ for some $g_j(x)$, $h_j(x) \in \mathbb{Z}_p[x]$, $j = 1, 2, \ldots, m$, then $g_j(x) = h_j(x)$ for all j.*

Proof: We first show that if $f(x) \in \mathbb{Z}_{p^m}[x]$ has a representation of the form $\sum_{j=1}^{m} p^{m-j}(x^p - x)^j g_j(x)$, with $g_j(x) \in \mathbb{Z}_p[x]$, then the representation is unique. It suffices to show that if $g_1(x)$, $g_2(x), \ldots, g_m(x) \in \mathbb{Z}_p[x]$ are such that

$$\sum_{j=1}^{m} p^{m-j}(x^p - x)^j g_j(x) \equiv 0 \pmod{p^m} \tag{5}$$

then $g_j(x) = 0$ for $j = 1, 2, \ldots, m$.

So, let $g_j(x) \in \mathbb{Z}_p[x]$, $j = 1, 2, \ldots, m$, satisfy the congruence in (5). Reducing the congruence modulo p, we obtain $(x^p - x)^m g_m(x) \equiv 0 \pmod{p}$. This shows that $g_m(x) \equiv 0 \pmod{p}$, so that $g_m(x) = 0$ since $g_m(x) \in \mathbb{Z}_p[x]$.

Now, suppose that $g_j(x) = 0$ for $j = m, m-1, \ldots, m-k+1$, for some integer $k < m$. Equation (5) now becomes

$$\sum_{j=1}^{m-k} p^{m-j}(x^p - x)^j g_j(x) \equiv 0 \pmod{p^m}$$

Dividing this congruence by p^k, we get

$$\sum_{j=1}^{m-k} p^{m-k-j}(x^p - x)^j g_j(x) \equiv 0 \pmod{p^{m-k}}$$

Reducing this modulo p, we obtain $(x^p - x)^{m-k} g_{m-k}(x) \equiv 0 \pmod{p}$, which implies that $g_{m-k}(x) \equiv 0 \pmod{p}$, or equivalently, $g_{m-k}(x) = 0$ since $g_{m-k}(x) \in \mathbb{Z}_p[x]$. It now follows by induction that $g_j(x) = 0$ for $j = 1, 2, \ldots, m$.

We next show that $f(x) \in \mathbb{Z}_{p^m}$ annihilates $\mathbb{Z}_{p^m}$ if and only if it is of the form $\sum_{j=1}^{m} p^{m-j}(x^p - x)^j g_j(x)$. It is easy to see that if $f(x) \equiv \sum_{j=1}^{m} p^{m-j}(x^p - x)^j g_j(x) \pmod{p^m}$ for some $g_j(x) \in \mathbb{Z}_p[x]$, $j = 1, 2, \ldots, m$, then $f(x)$ annihilates $\mathbb{Z}_{p^m}$. The reason for this is that for any integer r, $p | (r^p - r)$ by Fermat's (little) theorem, and hence, $p^j | (r^p - r)^j$ for any $j \geq 1$. As a result, for any $r \in \mathbb{Z}_n$, $p^{m-j}(r^p - r)^j \equiv 0 \pmod{p^m}$ for any $j \geq 0$, from which we see that $f(r) \equiv 0 \pmod{p^m}$.

We prove the converse by induction on $m = 1, 2, \ldots, p$. When $m = 1$, $\mathbb{Z}_p$ is a field, and so any polynomial that annihilates $\mathbb{Z}_p$ must be a multiple of $(x^p - x)$, modulo p.

So, suppose that the desired result is true for $m = 1, 2, \ldots, s-1$, with $s \leq p$. Consider $m = s$, and let $f(x)$ be an annihilator over $\mathbb{Z}_{p^s}$.

From Theorem 7, $f(x) \equiv (x^p - x)^s g(x) \pmod{p}$, for some $g(x) \in \mathbb{Z}_p[x]$. As noted above, for any integer r, $p^s | (r^p - r)^s$. Hence, it follows that $(x^p - x)^s g(x)$ is also an annihilator for $\mathbb{Z}_{p^s}$.

Now, since $f(x) \equiv (x^p - x)^s g(x) \pmod{p}$, we can write

$$f(x) \equiv (x^p - x)^s g(x) + p\, h(x) \pmod{p^s} \tag{6}$$

for some $h(x) \in \mathbb{Z}_{p^{s-1}}[x]$. Since both $f(x)$ and $(x^p - x)^s g(x)$ annihilate $\mathbb{Z}_{p^s}$, so must $p\, h(x)$. But, writing an arbitrary $x \in \mathbb{Z}_{p^s}$ as $x = ap^{s-1} + r$ for $r \in \mathbb{Z}_{p^{s-1}}$, it is easily seen that $p\, h(x)$ can annihilate $\mathbb{Z}_{p^s}$ if and only if $h(x)$ annihilates $\mathbb{Z}_{p^{s-1}}$.

So, applying the induction hypothesis, we find

$$h(x) \equiv \sum_{j=1}^{s-1} p^{s-1-j}(x^p - x)^j g_j(x) \pmod{p^{s-1}}$$

for some $g_j(x) \in \mathbb{Z}_p[x]$, $j = 1, 2, \ldots, s-1$. Plugging this into (6) proves the required statement for $m = s$, thus completing the induction step of the proof. ■

We can obtain expressions for $A(p^m, k)$ and $M(p^m, k)$, $m \leq p$, from the above theorem in much the same way as from Theorem 4. In this case, to obtain an expression for $A(p^m, k)$, we need to count the number of ways of choosing the $g_j(x)$'s so that the resultant $f(x)$ is of degree k. It is not hard to show that for $f(x)$ to be of degree $k \geq mp$, each $g_j(x)$ must be of degree

$k - jp$ or less, with at least one $g_j(x)$ being of degree exactly $k - jp$. Similarly, for $f(x)$ to be an annihilator of degree $k < mp$, we must have $g_j(x) = 0$ for $j > \lfloor k/p \rfloor$, and for $1 \leq j \leq \lfloor k/p \rfloor$, $g_j(x)$ must have degree at most $k - jp$, with at least one of these $g_j(x)'s$ having degree exactly $k - jp$. Counting arguments now show that when $m \leq p$, $A(p^m, k) = (p^l - 1)p^{lk - p\frac{l(l+1)}{2}}$, where $l = \min(\lfloor k/p \rfloor, m)$. Some algebraic manipulations are needed to show that this agrees with the result of part (i) of Corollary 5.

Finally, for $f(x)$ to be a monic annihilator of degree k, the $g_j(x)$'s must satisfy the above conditions, and moreover, $g_l(x)$ must be monic of degree exactly $k - lp$, where $l = \min(\lfloor k/p \rfloor, m)$ as above. From this, we obtain for $m \leq p$, $M(p^m, k) = p^{lk - p\frac{l(l+1)}{2}}$, which agrees with part (ii) of Corollary 5.

References

[1] S. Frisch, "Polynomial functions on finite commutative rings," *Advances in commutative ring theory (Fez, 1997)*, pp. 323–336, Lecture notes in Pure and Appl. Math., 205, New York: Dekker, 1999.