BULLETIN OF THE ICA
Volume **106** (2026), 82–94

Polynomial representation of functions on the integers modulo n

Nicholas Cotton, Gove Effinger, and Gary L. Mullen

Abstract. We define a polynomial index PI for any finite commutative ring with unity element. This index provides a measure of the distance the ring is from being a finite field (whose PI is 1). After proving a multiplicativity property for the ring $\mathbb{Z}_n$, we focus on the case of $\mathbb{Z}_{p^m}$ (p a prime). We determine the index for this ring using the concepts of annihilator polynomials and stopping point degrees. Finally, we give a specific formula for $PI(\mathbb{Z}_{p^m})$ in terms of p and m only, provided that $m \leq p$.

1 Introduction

In this paper we explore the extent to which functions from a finite commutative ring with unity to itself can be represented by polynomials over that ring, including defining an *index* to measure how close the ring is to being a finite field.

Let R denote a finite commutative ring with unity of cardinality r. Consider the set $P_r(R)$ of all polynomials with coefficients in R of degree $< r$, so there are a total of r^r such polynomials. We also note that there are r^r functions $f \colon R \to R$.

Let R^r denote the set of all r-tuples over the ring R. For a polynomial $p(x)$ with coefficients in R, let $S_p = (p(a_1), \ldots, p(a_r))$ where the elements a_i run through the r elements of the ring R, obtaining a vector of length r. Calculate these vectors S_p for each of the r^r polynomials over R and denote the resulting set of r^r vectors by the set T. Hence the set T contains all vectors—not necessarily distinct—that arise from the r^r polynomials of degree $< r$ with coefficients from R, and so $|T| \leq r^r$.

Key words and phrases: finite commutative ring, finite field, polynomials
Mathematics Subject Classifications: 12E20, 13M10
Corresponding author: Nicholas Cotton <nzc5354@psu.edu>

Received: 10 September 2024
Accepted: 22 February 2025

Definition 1.1. Define the *polynomial index* (*PI*) for the ring R by the ratio $|T|/r^r$. That is, it is the ratio of the number of distinct image vectors generated by all polynomials of degree less than r over R divided by the total number of possible vectors of length r over R.

The authors suspect that for a general ring R the polynomial index will be difficult to calculate. In what follows we do an examination of the case $R = \mathbb{Z}_n$, the ring of integers modulo n. First, however, we settle the question of the value of our index when R is a finite field.

Theorem 1.2. *If the ring R is a finite field, the polynomial index of R is* 1.

Proof. It is well known that the Lagrange Interpolation Formula holds over the finite field R (see [2], page 269). Over a finite field, every function can be represented by a polynomial, i.e., if $f\colon R \to R$ is a function over the finite field R of cardinality r, there is a unique polynomial $P_f(x)$ with coefficients in R of degree $< r$ with the property that $P_f(a) = f(a)$ for every element $a \in R$. In fact, the polynomial $P_f(x)$ can be written down as follows:

$$P_f(x) = \sum_{a \in R} f(a)(1 - (x-a)^{r-1}).$$

This polynomial is clearly of degree $< r$. Recall that the multiplicative group R^* of the field R is of order $r-1$, so for any non-zero element $y \in R$, we have $y^{r-1} = 1$. Hence for any $a \in R$, we get

$$P_f(a) = f(a)(1-0) + \sum_{b \neq a} f(b)(1-(a-b)^{r-1}) = f(a) + \sum_{b \neq a} f(b)(1-1) = f(a).$$

Since every function over the field R is represented by a polynomial of degree less than r, each of the r^r possible vectors will be obtained. But there are exactly r^r polynomials, so each vector will be picked up exactly once. Hence the polynomial index for the field R will be $r^r/r^r = 1$. □

Because of this beautiful fact about finite fields, we can use the polynomial index as a measure of how far away a given ring is from being a finite field.

2 The case $R = \mathbb{Z}_n$ and multiplicativity of V_n

We now turn our attention to the case where our ring R is of the form $\mathbb{Z}_n$; i.e., R is the ring of integers modulo n. We shall use the notation V_n to stand for the number of distinct image vectors of polynomials of degree less than n over $\mathbb{Z}_n$. Hence the polynomial index PI of $\mathbb{Z}_n$ is V_n/n^n, and we shall want to explore how to find the value of V_n. An initial step in doing this is to establish that it is sufficient to study $\mathbb{Z}_{p^m}$ where p is prime.

Let $n = p^m q^k$ with p and q distinct primes and suppose $v = (a_0, a_1, \ldots, a_{n-1})$ is the image vector of $f(x) = c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$ over $\mathbb{Z}_n$. Let f_p and f_q be polynomials in which each coefficient c_i is replaced by $c_i \bmod p^m$ and $c_i \bmod q^k$, i.e., they are polynomials over $\mathbb{Z}_{p^m}$ and $\mathbb{Z}_{q^k}$, respectively. Finally, let the "combined" ordered pair of image vectors of (f_p, f_q) be

$$\big((a_0 \bmod p^m,\ a_0 \bmod q^k), \ldots, (a_{n-1} \bmod p^m,\ a_{n-1} \bmod q^k)\big).$$

By the Chinese Remainder Theorem, this set of ordered pairs uniquely represents the splitting of f into the pair (f_p, f_q). Said another way, the vector v in $\mathbb{Z}_n$ is uniquely represented by this ordered pair in $\mathbb{Z}_{p^m} \times \mathbb{Z}_{q^k}$.

Example 2.1. Suppose $f(x) = 5x^5$ over $\mathbb{Z}_{12}$. Its image vector is

$$v = f\big((0,1,2,3,4,5,6,7,8,9,10,11)\big) = (0,5,4,3,8,1,0,11,4,9,8,7).$$

Reducing f modulo 3 and 4 gives us $f_3(x) = 2x^5$ and $f_4(x) = x^5$. Reducing v modulo 3 (first entry) and 4 (second entry) gives us the following vector in $\mathbb{Z}_3 \times \mathbb{Z}_4$:

$$\big((0,0),\ (2,1),\ (1,0),\ (0,3),\ (2,0),\ (1,1),\ (0,0),\ (2,3),\ (1,0),\ (0,1),\ (2,0),\ (1,3)\big).$$

We note that the first (i.e., mod 3) entries are $(0,2,1,0,2,1,0,2,1,0,2,1)$ (i.e., four copies of $(0,2,1)$) and the second (i.e., mod 4) entries are $(0,1,0,3,0,1,0,3,0,1,0,3)$ (i.e., three copies of $(0,1,0,3)$). Finally, we can compute that $f_3((0,1,2)) = (0,2,1)$ and $f_4((0,1,2,3)) = (0,1,0,3)$.

We recall that, in general, the Euler-phi function $\phi(n)$ counts the number of elements a with $0 \leq a < n$ such that a is relatively prime to n. Because $\phi(p^m) = p^m - p^{m-1}$, Euler's Theorem says that if $\mathrm{GCD}(x,p) = 1$, then $x^{p^m - p^{m-1}} \equiv 1 \pmod{p^m}$, and likewise for q^k. This allows us to decrease (if necessary) the degree of each term of f_p and f_q so that the new reduced function f_p^* is of degree less than p^m, and likewise f_q^* is of degree less than q^k, while retaining the exact same combined image vector as (f_p, f_q). We can then show that the two vectors within the ordered pair are in fact image vectors of *allowable* polynomials in $\mathbb{Z}_{p^m} \times \mathbb{Z}_{q^k}$.

Example 2.2. Referring now to the example above and applying Euler's Theorem, since $\phi(3) = 2$ and $\phi(4) = 2$ also, we have

$$f_3^*(x) = 2x^5 = 2x^2x^2x \equiv 2(1)(1)x = 2x \pmod 3$$

(note that in this case we applied Euler's Theorem twice to get $\deg(f_3^*) < 3$), and we verify that $f_3^*\big((0,1,2)\big) = (0,2,1)$. Likewise, $f_4^*(x) = x^2x^3 \equiv x^3 \pmod 4$, and $f_4^*\big((0,1,2,3)\big) = (0,1,0,3)$.

Lemma 2.3. *Suppose a polynomial $f(x)$ over $\mathbb{Z}_{p^m}$ contains a term of the form cx^d where $d \geq p^m$. Then $f(x)$ and $f^*(x) = \cdots + cx^{d-p^m+p^{m-1}} + \cdots$ have the same image vector in $\mathbb{Z}_{p^m}$.*

Proof. We suppose $d \geq p^m$ (since such a d needs to be reduced for our purposes). Euler's Theorem states that if $\mathrm{GCD}(x,p) = 1$, then

$$x^{\phi(p^m)} = x^{p^m - p^{m-1}} \equiv 1 \pmod{p^m}.$$

Hence if $\mathrm{GCD}(x,p) = 1$, then $x^d \equiv x^{d-p^m+p^{m-1}} \pmod{p^m}$. On the other hand, if $\mathrm{GCD}(x,p) \neq 1$ (i.e., if $x = pa$ for some a), then both x^d and $x^{d-p^m+p^{m-1}}$ are 0 since $d - p^m + p^{m-1} \geq p^{m-1} \geq m$ (for all p and m), and $(pa)^m$ is 0 modulo p^m. Thus $f(x)$ and $f^*(x)$ have the same image vector for all $x \in \mathbb{Z}_{p^m}$. □

Example 2.4. Suppose $f(x) = x^{10}$ over $\mathbb{Z}_9$. The image vector of f is $(0,1,7,0,4,4,0,7,1)$. Note that as long as the degree of this term is 2 or higher (since $9 = 3^2$), the image vector will contain 0 at the elements 0, 3, and 6 (i.e., all the elements that are not relatively prime to 9 and hence are not covered by Euler's Theorem). Now, $\phi(9) = 9 - 3 = 6$, so $f^*(x) = x^{10-6} = x^4$, and we confirm that its image vector is still $(0,1,7,0,4,4,0,7,1)$.

We are now ready for the main result of this section.

Theorem 2.5 (Multiplicativity). *Suppose $n = p^mq^k$ with p and q distinct primes. Let T_n be the set of all image vectors of polynomials of degree less than n over $\mathbb{Z}_n$ and, as above, let V_n be the cardinality of T_n. Define T_{p^m}, V_{p^m}, T_{q^k}, and V_{q^k} similarly. Then $V_n = V_{p^m}V_{q^k}$.*

Proof. ($V_n \leq V_{p^m}V_{q^k}$) We argue above that by the Chinese Remainder Theorem, every vector of T_n is in one-to-one correspondence with a unique ordered pair of vectors in $\mathbb{Z}_{p^m} \times \mathbb{Z}_{q^k}$, and, as in Lemma 2.3, we employ

Euler's Theorem to guarantee that those vectors are in fact in T_{p^m} and T_{q^k} (because they are image vectors of the polynomials of degree less than m and k, respectively). We do not, however, know if *all* ordered pairs of vectors of $T_{p^m} \times T_{q^k}$ are represented as we move through all the elements of T_n. Hence we can conclude that $V_n \leq V_{p^m} V_{q^k}$.

($V_n \geq V_{p^m} V_{q^k}$) Here we denote by $(cp)_i$, and $(cq)_j$ the coefficients of polynomials over $\mathbb{Z}_{p^m}$ and $\mathbb{Z}_{q^k}$, respectively. Likewise, we denote by $(ap)_i$ and $(aq)_j$ the first and second parts in an ordered pair in $T_{p^m} \times T_{q^k}$. Finally, by the Chinese Remainder Theorem, we denote the unique element of $\mathbb{Z}_n$ corresponding to the pair $\big((ap)_i, (aq)_j\big)$ by $\big[(ap)_i, (aq)_j\big]$. We assume without loss of generality that $p^m < q^k$.

Suppose $f_p(x) = (cp)_{m-1}x^{m-1} + \cdots + (cp)_0$ is a polynomial over $\mathbb{Z}_{p^m}$ whose image vector is $\big((ap)_0, \ldots, (ap)_{p^m-1}\big)$, and likewise suppose $f_q(x) = (cq)_{k-1}x^{k-1} + \cdots + (cq)_0$ is a polynomial over $\mathbb{Z}_{q^k}$ whose image vector is $\big((aq)_0, \ldots, (aq)_{q^k-1}\big)$ (so the ordered pairs of these vectors lie in $T_{p^m} \times T_{q^k}$). We note that for a power $d \geq m$, we have $(cp)_d = 0$. We now compute the unique (by the Chinese Remainder Theorem) vector a of length n of elements of $\mathbb{Z}_n$:

$$a = \Big(\big[(ap)_0, (aq)_0\big], \ldots, \big[(ap)_{p^m-1}, (aq)_{p^m-1}\big], \\ \big[(ap)_0, (aq)_{p^m}\big], \ldots, \big[(ap)_{p^m-1}, (aq)_{q^k-1}\big]\Big).$$

It remains to show that the vector a lies in T_n; that is, a is the image vector of some polynomial over $\mathbb{Z}_n$ of degree less than n. Let

$$f(x) = \big[(cp)_{k-1}, (cq)_{k-1}\big]x^{k-1} + \big[(cp)_{k-2}, (cq)_{k-2}\big]x^{k-2} + \cdots + \big[(cp)_0, (cq)_0\big].$$

But now $f(x) \bmod p^m = f_p(x)$ and $f(x) \bmod q^k = f_q(x)$, as we defined above. We have shown then that an arbitrary ordered pair of vectors in $T_{p^m} \times T_{q^k}$ corresponds to a unique vector a of length n whose elements are in $\mathbb{Z}_n$, and we have shown that a is the image vector of a polynomial over $\mathbb{Z}_n$ whose degree is less than n. Hence a is in T_n, and so $V_n \geq V_{p^m} V_{q^k}$. Combined with our previous argument, we conclude that $V_n = V_{p^m} V_{q^k}$. □

Example 2.6. We illustrate this latter part of the proof; wherein, we start with image vectors in T_{p^m} and T_{q^k} and produce a corresponding, unique image vector in T_n. Suppose $f_3(x) = x^2$, whose image vector in T_3 is $(0, 1, 1)$, and $f_4(x) = x^3$, whose image vector in T_4 is $(0, 1, 0, 3)$. This results in the following combined vector in $T_3 \times T_4$:

$$\big((0,0),\ (1,1),\ (1,0),\ (0,3),\ (1,0),\ (1,1),\ (0,0),\ (1,3),\ (1,0),\ (0,1),\ (1,0),\ (1,3)\big).$$

By the Chinese Remainder Theorem, the unique vector in $\mathbb{Z}_{12}$ corresponding to this ordered pair of vectors is $(0, 1, 4, 3, 4, 1, 0, 7, 4, 9, 4, 7)$, and we need only show that this vector "belongs" to some polynomial of degree less than 12 over $\mathbb{Z}_{12}$. In reality it is the image vector of many, many such polynomials, but in particular, $f_{12}(x) = 9x^3 + 4x^2$ works (the reader can check). We note that $9x^3 + 4x^2 \equiv x^2 \pmod 3$ and $9x^3 + 4x^2 \equiv x^3 \pmod 4$.

Corollary 2.7. *If $n = p_1^{m_1} \dots p_s^{m_s}$ with $s \geq 2$, then $V_n = V_{p_1^{m_1}} \dots V_{p_s^{m_s}}$.*

This can be proved using induction on s. Theorem 2.2 handles the base case $s = 2$. Because the Chinese Remainder Theorem and Euler's Theorem can both be applied to an integer with multiple prime factors, the inductive step can be an argument similar to that used for the base case but now applied to $n/p_s^{m_s}$ and $p_s^{m_s}$. We leave the details of that inductive step to the reader.

We remark here that the polynomial index $PI(\mathbb{Z}_n) = V_n/n^n$ is not multiplicative. We have just proved that the numerator is multiplicative, but if $n = p^m q^k$, then $n^n = (p^m)^n (q^k)^n > (p^m)^{p^m} (q^k)^{q^k}$. However, the index remains the ratio of the number of functions produced by polynomials divided by the total number of possible functions; that is, if $n = p^m q^k$, then $PI(\mathbb{Z}_n) = V_{p^m} V_{q^k}/n^n$.

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

We have now shown that to investigate V_n it is sufficient to investigate V_{p^m}, where p is prime and $m \geq 0$.

Definition 3.1. A polynomial $a(x)$ of degree less than p^m over $\mathbb{Z}_{p^m}$ is called an *annihilator polynomial* (or simply an *annihilator*) if $a(x) = 0$ for all $x \in \mathbb{Z}_{p^m}$.

Example 3.2. A machine search for annihilators of degree 4 over $\mathbb{Z}_{2^3}$ finds 28 such polynomials, for example $x^4 + 2x^3 + 3x^2 + 2x$.

Theorem 3.3. *If $A(p^m)$ is the total number of annihilator polynomials of degree less than p^m over $\mathbb{Z}_{p^m}$, then $V_{p^m} = (p^m)^{p^m}/A(p^m)$.*

Proof. Two polynomials $f(x)$ and $g(x)$ of degree less than p^m over $\mathbb{Z}_{p^m}$ have the same image vector if and only if they differ by an annihilator

$a(x)$. Hence the set of all polynomials having that fixed image vector is the set $f(x) + a(x)$ as $a(x)$ ranges over the set of annihilators. Since this set has cardinality $A(p^m)$, we get that the total number of *distinct* polynomial image vectors V_{p^m} is $(p^m)^{p^m}/A(p^m)$. □

So our task now is to determine the count $A(p^m)$. If k is any degree below p^m, we denote the number of annihilators of degree k over $\mathbb{Z}_{p^m}$ by $A(p^m, k)$. Clearly, $A(p^m) = \sum_{j=0}^{p^m-1} A(p^m, j)$.

We now need to introduce "the alpha function."

Definition 3.4. Over $\mathbb{Z}_{p^m}$, we let $\alpha(j)$ be the largest $\alpha \in \{0, 1, 2, \ldots, m\}$ such that p^α divides $j!$. In other words, $\alpha(j)$ is the total number times p appears in $j!$.

Example 3.5. In $\mathbb{Z}_{2^3}$, we have $\alpha(1) = 0$, and $\alpha(2) = \alpha(3) = 1$, and $\alpha(4) = \alpha(5) = \cdots = 3$ since the value of α cannot exceed $m = 3$.

The following theorem is proved as Corollary 5(i) in [1].

Theorem 3.6 (Kahyap and Vardy [1])**.** *The number of annihilators of degree $k < p^m$ over $\mathbb{Z}_{p^m}$ is $A(p^m, k) = (p^{\alpha(k)} - 1)p^{\alpha(1)+\alpha(2)+\cdots+\alpha(k-1)}$.*

Example 3.7. In $\mathbb{Z}_{2^3}$, this result says that

$$A(2^3, 4) = (2^3 - 1)2^{0+1+1} = (7)(4) = 28,$$

as confirmed by machine search in Example 3.2.

We can now, with a little more work, write down a simple expression for $A(p^m)$ in terms of the α-function. We observe that $A(p^m, 0) = 1$ (i.e., the zero polynomial) and that $A(p^m, 1) = 0$ (i.e., it is not possible to have a linear annihilator).

Theorem 3.8. *For all $k \geq 3$,*

$$1 + \sum_{j=2}^{k-1} A(p^m, j) = A(p^m, k)/(p^{\alpha(k)} - 1) = p^{\alpha(2)+\alpha(3)+\cdots+\alpha(k-1)}.$$

Proof. The second equality follows directly from Theorem 3.6, so we prove, by induction on the degree k, that the first and last quantities are equal. If $k = 3$, the first above is

$$1 + \sum_{j=2}^{2} A(p^m, j) = 1 + (p^{\alpha(2)} - 1)p^0 = p^{\alpha(2)};$$

whereas, the last is also $p^{\alpha(2)}$. Hence, we have established the base case.

We now assume for $j = k - 1$ that $1 + \sum_{j=2}^{k-2} A(p^m, j) = p^{\alpha(2)+\cdots+\alpha(k-2)}$. Then

$$\begin{aligned} 1 + \sum_{j=2}^{k-1} A(p^m, j) &= p^{\alpha(2)+\cdots+\alpha(k-2)} + A(p^m, k-1) \\ &= p^{\alpha(2)+\cdots+\alpha(k-2)} + (p^{\alpha(k-1)} - 1)p^{\alpha(2)+\cdots+\alpha(k-2)} \\ &= p^{\alpha(2)+\cdots+\alpha(k-2)} + p^{\alpha(2)+\cdots+\alpha(k-1)} - p^{\alpha(2)+\cdots+\alpha(k-2)} \\ &= p^{\alpha(2)+\cdots+\alpha(k-1)}, \end{aligned}$$

as desired. □

If we set $k = p^m$ in Theorem 3.8, we arrive at the following corollary.

Corollary 3.9. *The total number $A(p^m)$ of annihilator polynomials of degree less than p^m in $\mathbb{Z}_{p^m}$ (i.e., $A(p^m) = 1 + \sum_{j=2}^{p^m-1} A(p^m, j)$) is given by $p^{\alpha(2)+\alpha(3)+\cdots+\alpha(p^m-1)}$.*

This says that once you have computed the values of α up to the point where $\alpha(j) = m$, computing $A(p^m)$ is an easy process. We examine this “stabilization point” in the next section.

Example 3.10.
For $\mathbb{Z}_{2^3}$, we have $A(2^3) = 2^{\alpha(2)+\cdots+\alpha(7)} = 2^{1+1+3+3+3+3} = 2^{14}$.
For $\mathbb{Z}_{3^2}$, we have $A(3^2) = 3^{\alpha(2)+\cdots+\alpha(8)} = 3^{0+1+1+1+2+2+2} = 3^9$.

Corollary 3.11. *We have $V_{p^m} = (p^m)^{p^m} / \sum_{j=2}^{p^m-1} \alpha(j)$. Hence the polynomial index PI of $\mathbb{Z}_{p^m}$ is $1/\sum_{j=2}^{p^m-1} \alpha(j)$.*

Proof. The first statement is simply writing down that V_{p^m} is the total number of polynomials of degree less than m divided by the total number of annihilators. The second statement uses the first statement and the definition of the polynomial index:

$$PI(\mathbb{Z}_{p^m}) = \frac{V_{p^m}}{(p^m)^{p^m}} = \frac{(p^m)^{p^m}}{(p^m)^{p^m \sum_{j=2}^{p^m-1} \alpha(j)}} = \frac{1}{\sum_{j=2}^{p^m-1} \alpha(j)}. \qquad \square$$

Example 3.12.
Since $V_{2^3} = (2^3)^{2^3}/2^{14} = 2^{24}/2^{14} = 2^{10}$, we have $PI(\mathbb{Z}_{2^3}) = 1/2^{14}$.
Since $V_{3^2} = (3^2)^{3^2}/3^9 = 3^{18}/3^9 = 3^9$, we have $PI(\mathbb{Z}_{3^2}) = 1/3^9$.

4 Stopping points and computing V_{p^m}

When exploring the number V_{p^m} of distinct image vectors of polynomials over $\mathbb{Z}_{p^m}$, we look through all polynomials of degree less than p^m. It turns out, however, that it is not necessary to go up beyond a certain, smaller degree to find all the polynomial image vectors. Hence we make the following definition.

Definition 4.1. In $\mathbb{Z}_{p^m}$, the *stopping point* is the smallest degree $0 \leq s \leq p^m$ such that the full set of polynomial image vectors is generated by polynomials of degree less than s over $\mathbb{Z}_{p^m}$.

Theorem 4.2. *The stopping point $0 \leq s \leq p^m$ in $\mathbb{Z}_{p^m}$ is the smallest degree j for which $\alpha(j) = m$, i.e., by definition of the function α, it is the smallest j such that p^m divides $j!$.*

The degree s is known as the Kempner number for p^m (see [3], Sequence A002034).

Proof. By the definition of stopping point degree s, we have that the ratios $(p^m)^{p^m}/A(p^m)$ and $(p^m)^s/\big(1 + \sum_{j=2}^{s-1} A(p^m, j)\big)$ are equal since they both give the count V_{p^m}, and s is the smallest degree for which this equality holds. Applying Theorem 3.8, we obtain

$$\frac{(p^m)^{p^m}}{p^{\alpha(2)+\cdots+\alpha(p^m-1)}} = \frac{(p^m)^s}{p^{\alpha(2)+\cdots+\alpha(s-1)}},$$

and simplifying we get

$$(p^m)^{p^m-s} = p^{\alpha(s)+\cdots+\alpha(p^m-1)}.$$

On the left-hand side, the exponent on p is $(p^m - s)m$, i.e., it is the sum of $p^m - s$ copies of m. On the other hand, the right-hand side gives a summation of $p^m - s$ terms which can be no larger than m by definition of the α-function. We conclude then that $\alpha(s) = m$. Moreover, we must have $\alpha(s-1) < m$, for otherwise $s-1$ would make our ratios above equal, but s is the smallest degree with this property. □

Example 4.3. In $\mathbb{Z}_{2^3}$, since $\alpha(3) \neq 3$ (i.e., $8 \nmid 3!$) but $\alpha(4) = 3$ (i.e., $8 \mid 4!$) we see that 4 is the stopping point degree. In $\mathbb{Z}_{3^2}$, since $\alpha(5) = 1$ but $\alpha(6) = 2$, we see that 6 is the stopping point degree. For a more dramatic example, consider $\mathbb{Z}_{5^3}$. We have $\alpha(2)$ through $\alpha(4)$ are 0, $\alpha(5)$ through $\alpha(9)$ are 1, $\alpha(10)$ through $\alpha(14)$ are 2, and $\alpha(15) = 3$, so the stopping point is $s = 15$, which is far short of $5^3 = 125$. As both p and m increase, the gap between s and p^m grows rapidly.

We have already observed that the number of polynomials of degree less than p^m over $\mathbb{Z}_{p^m}$ that generate a fixed polynomial image vector is the total number of annihilators $A(p^m)$, so a formula for computing this number, making use of the stopping point, might be helpful.

Proposition 4.4. *If s is the stopping point for $\mathbb{Z}_{p^m}$, then*

$$A(p^m) = (p^m)^{p^m - s}(p^{\sum_{j=2}^{s-1} \alpha(j)})$$

Proof. We know from Corollary 3.9 that

$$A(p^m) = p^{\sum_{j=2}^{p^m-1} \alpha(j)}.$$

Moreover the proof of Theorem 4.2 uses the equality

$$\frac{(p^m)^{p^m}}{p^{\sum_{j=2}^{p^m-1} \alpha(j)}} = \frac{(p^m)^s}{p^{\sum_{j=2}^{s-1} \alpha(j)}}.$$

Solving for $A(p^m)$, the quantity in the left-hand denominator, gives the desired result. □

Example 4.5. We saw in Example 4.3 that $s = 4$ for $\mathbb{Z}_{2^3}$. Thus $A(2^3) = (2^3)^{8-4}2^2 = 2^{12+2} = 2^{14}$, as computed directly above. Again, the higher p and/or m goes, the greater computational advantage of the stopping degree. For another example, $s = 15$ for $\mathbb{Z}_{5^3}$, so $A(5^3) = (5^3)^{125-15}5^{5(1+2)} = 5^{330+15} = 5^{345}$ giving us that $V_{5^3} = (5^3)^{125}/5^{345} = 5^{375-345} = 5^{30}$.

Finally, let us return to the computation of V_{p^m}. We know that $V_{p^m} = (p^m)^{p^m}/A(p^m)$ and that it can also be computed with smaller quantities via $V_{p^m} = (p^m)^s/\big(p^{\sum_{j=2}^{s-1}\alpha(j)}\big)$. However, the former formula uses the α-function, and the latter uses both the α-function and the stopping point. It would be good to write down a formula for V_{p^m} that involves only p and m. The following is a start on that goal, with a restriction on these quantities. First, an example to hopefully "light the way."

Example 4.6. Consider V_{5^3}. Note that $s = 15 = (3)(5) = mp$. Also, $\sum_{j=2}^{14}\alpha(j) = 5(1+2) = p\big(1+\cdots+(m-1)\big) = p(m-1)(m)/2$. We thus conclude that $V_{5^3} = (5^3)^{(3)(5)}/5^{(5)(2)(3)/2} = 5^{45}/5^{15} = 5^{30}$, as computed in Example 4.5.

Theorem 4.7. *If $1 \le m \le p$, then $V_{p^m} = p^{pm(m+1)/2}$.*

Proof. For $m = 1$, we know that $V_p = p^p$, so the result holds. Otherwise, since

$$\begin{aligned}
\alpha(p) = \cdots = \alpha(2p-1) &= 1,\\
\alpha(2p) = \cdots = \alpha(3p-1) &= 2,\\
&\vdots\\
\alpha\big((m-1)p\big) = \cdots = \alpha(mp-1) &= m-1,\\
\alpha(mp) &= m,
\end{aligned}$$

we see that the stopping degree s is mp. Moreover,

$$\begin{aligned}
\alpha(2)+\cdots+\alpha(s-1) &= \alpha(2)+\cdots+\alpha(mp-1)\\
&= p + 2p + \cdots + (m-1)p\\
&= p(1+2+\cdots+(m-1))\\
&= p(m-1)(m)/2.
\end{aligned}$$

We have then

$$\begin{aligned}
V_{p^m} &= \frac{p^{m^2p}}{p^{p(m-1)(m)/2}}\\
&= p^{m^2p-p(m-1)(m)/2}\\
&= p^{p(2m^2-m^2+m)/2}\\
&= p^{pm(m+1)/2}.
\end{aligned}$$

□

Corollary 4.8.

- (a) *For all primes p, we have $V_{p^2} = p^{3p}$.*
- (b) *For all odd primes p, we have $V_{p^3} = p^{6p}$.*

Example 4.9.

- (a) $V_{3^2} = 3^9$; $V_{101^2} = 101^{303}$.
- (b) $V_{5^3} = 5^{30}$; $V_{101^3} = 101^{606}$.

Finding a formula for V_{p^m} in terms of p and m when m exceeds p is more complicated because of the behavior of the α-function. For example, for $\mathbb{Z}_{2^4}$, we have $\alpha(2) = \alpha(3) = 1$; but then $\alpha(4)$ jumps by 2 rather than 1; and later $\alpha(8)$ jumps by 3; etc. Thus the general case requires much closer examination than the $m \leq p$ case above.

We have one more result, which follows from Theorem 4.7 and the fact that, by definition, $PI(\mathbb{Z}_{p^m}) = V_{p^m}/(p^m)^{p^m}$.

Corollary 4.10. *If $m \leq p$, then $PI(\mathbb{Z}_{p^m}) = \dfrac{1}{p^{mp^m - p(m)(m+1)/2}}$.*

Example 4.11.
$PI(\mathbb{Z}_{2^2}) = 1/2^{(2)(4)-(2)(2)(3)/2} = 1/2^2$.
$PI(\mathbb{Z}_{3^2}) = 1/3^{(2)(9)-(3)(2)(3)/2} = 1/3^9$ (as computed in Example 3.12).
$PI(\mathbb{Z}_{5^3}) = 1/5^{(3)(125)-(5)(3)(4)/2} = 1/5^{375-30} = 1/5^{345}$.

While this index PI is difficult to determine for an arbitrary ring, we end by noting that there are exactly four non-isomorphic rings of order 4: the finite field of order 4, whose PI is 1 (as proved at the start); the ring $\mathbb{Z}_4$ of integers modulo 4, whose PI is 1/4; the ring L of 2×2 matrices $\left(\begin{smallmatrix} a & b \\ 0 & a \end{smallmatrix}\right)$ over $\mathbb{Z}_2$, whose PI (by machine calculation) is 1/4; and the ring $M = \mathbb{Z}_2 \times \mathbb{Z}_2$, whose PI (again by machine calculation) is 1/16.

Acknowledgments

The authors would like to thank the referee for their comments and corrections that improved our draft.

References

[1] N. Kashyap and A. Vardy, Enumerating annihilator polynomials over $\mathbb{Z}_n$, (2005), preprint, `https://ece.iisc.ac.in/~nkashyap/Papers/annihilators.pdf`.

[2] R. Lidl and H. Niederreiter, *Finite Fields, Second edition*, Cambridge University Press, 1997.

[3] N. J. A. Sloane, The On-line Encyclopedia of Integer Sequences, 1964. `https//oeis.org`.

Nicholas Cotton
661 W. Chestnut Street, Lancaster, PA 17603
nzc5354@psu.edu

Gove Effinger
Department of Mathematics and Statistics, Skidmore College
Saratoga Springs NY 12866
effinger@skidmore.edu

Gary L. Mullen
Department of Mathematics, The Pennsylvania State University
University Park, PA 16802
g4m@psu.edu