The Ideal of Vanishing Polynomials and the Ring of Polynomial Functions

Matvey Borodin, Ethan Liu, Justin Zhang

December 25, 2022

Abstract

We study the set of objects known as vanishing polynomials (the set of polynomials that annihilate all elements of the ring) over general commutative rings with identity. This set is an ideal of the ring of polynomials whose natural projection maps the ring of polynomials to the ring of polynomial functions. We present a new approach to finding the generating set of this ideal over the ring $\mathbb{Z}_n$ of residue classes modulo n. Generalizing this approach, we partially classify the vanishing polynomials over any general commutative ring with identity. We also establish a bijection between vanishing polynomials and polynomial functions over product rings and those of their constituent rings. Finally, we find some restrictions on how many roots polynomials can have over certain finite commutative rings.

1 Introduction

Polynomial rings are arguably one of the most fundamental and extensively studied objects in mathematics. While there has been a significant amount of research done regarding polynomials over fields and integral domains, less has been done investigating polynomials over rings with zero divisors. In particular, it is widely known that a polynomial of degree n can have at most n roots over a field, but when zero-divisors are introduced this result may fail. More specifically, a polynomial that vanishes for all $x \in R$ must be of degree at least $|R|$ if R is an integral domain, but if R has zero divisors the degree of this polynomial can be significantly smaller.

A complete description of such vanishing polynomials over the integers was given in [9, 10] while a more general result for multiple variables was found in [6]. We establish that the set of vanishing polynomials is an ideal and the quotient of the original polynomial ring by this ideal gives the ring of polynomial functions. Such a ring of polynomial functions over $\mathbb{Z}_n$, the ring of residue classes modulo n, was explored in [7, 12]. Throughout this paper, we build on these works and present various results regarding the structure of this ring. We then examine the structure of the ideal of vanishing polynomials and polynomial functions for more general rings.

In Section 2, we begin with definitions of essential terms followed by some background results that are used throughout the paper. In Section 3, we continue by studying the ring of polynomial functions over $\mathbb{Z}_n$ and find the number of zero divisors and units over this ring when n is a product of distinct primes. In Section 4, we look at the generating set of the ideal of vanishing polynomials over $\mathbb{Z}_n$. We present a new proof of the completeness of the generating set presented in [10] and generalize it to encompass results from various other works. In Section 5, the notion of a monic vanishing polynomial of minimal degree is developed and we study its properties over an infinite class of rings of a specific form. In Sections 6 and 7, we prove some results about vanishing polynomials for direct products of rings and rings of prime power, respectively. In Section 8 we find vanishing polynomials over arbitrary rings and apply these results to show that they give a complete classification for the integers modulo n. Finally, in Section 9 we examine what properties can be discerned about a ring when the polynomials over the ring have a finite number of roots, as well as provide a technique to limit the possible number of roots a polynomial has over a product ring.

2 Vanishing Polynomials

Throughout this paper, we assume rings to be commutative and with identity unless otherwise specified. Let R be a ring and let $R[x]$ denote the ring of polynomials with coefficients in R. We study objects in $R[x]$ known as *vanishing polynomials.*

Definition 1. A *polynomial* $F(x)$ in a polynomial ring $R[x]$ is a formal sum

$$a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$$

for some nonnegative integer n, where each $a_i \in R$ and x is an indeterminate.

Definition 2. A *vanishing polynomial* $F(x) \in R[x]$ is a polynomial such that $F(a) = 0$ for all $a \in R$. By definition, 0 itself is a vanishing polynomial.

Example 1. Consider the polynomial $F(x) = x^2 + x$ over $\mathbb{Z}_2$. Notice that $F(0) = 0$ and $F(1) = 0$. Therefore, $x^2 + x$ is a vanishing polynomial over $\mathbb{Z}_2$. Even infinite rings can have a finite nonzero vanishing polynomial: consider the ring $R = \Pi_{n=1}^{\infty}\mathbb{Z}_2$. Notice that $x^2 + x$ is vanishing in this ring as well. In fact, $ax^2 + ax$ is a vanishing polynomial for any $a \in R$.

The set of vanishing polynomials over a ring $R[x]$ is known to form an ideal. Thus, taking I to be the ideal of vanishing polynomials, it makes sense to consider the quotient $R[x]/I$. To understand the significance of this operation we must first consider the distinction between a *polynomial* and a *polynomial function.*

Definition 3. A *polynomial function* $f : R \to R$ is a function on R for which there exists a polynomial $F(x) \in R[x]$ such that $f(r) = F(r)$ for all $r \in R$.

When we need to distinguish between the two, we refer to the polynomial with an uppercase letter, such as $F(x)$, and the corresponding polynomial function with a lowercase letter, such as $f(x)$. Note that each polynomial $F(x)$ corresponds to a unique polynomial function $f(x)$, but as we will see later, any given polynomial function $f(x)$ must correspond to an infinite number of polynomials if there is a nonzero vanishing polynomial. The proposition below is a statement found in [5] connecting polynomials and polynomial functions.

Proposition 1. *The quotient $R[x]/I$, where I denotes the ideal of vanishing polynomials over $R[x]$, is the ring of polynomial functions $f : R \to R$.*

Finally, we present a well-known background result (a proof can be found in [4]) which we use in later sections.

Lemma 1. *Any function over a finite field $\mathbb{F}$ can be represented as a polynomial.*

In particular, every function over a finite field $\mathbb{Z}_p$ for a prime number p can be represented by a polynomial.

3 Polynomial Functions Over $\mathbb{Z}_n$

Let us now specifically look at the case where $R = \mathbb{Z}_n$, for an integer n, and consider the quotient ring $\mathbb{Z}_n[x]/I$. In the following theorems, we categorize the zero divisors and units of this ring for special types of n. We characterize polynomial functions using their evaluations which we represent as n-tuples with the ith entry corresponding to $f(i)$.

The first case that we will consider is when n has a prime factorization of the form $\prod_{i=1}^{k} p_i = p_1 p_2 \dots p_k$. It follows from the Chinese remainder theorem that any element $x \in \mathbb{Z}_n$ for an n of this form can be expressed as an element $(x_1, x_2, \dots, x_k)$ in the product ring $\mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \cdots \times \mathbb{Z}_{p_k}$. It can be easily seen that if $x \equiv y \pmod{p}$, then $f(x) \equiv f(y) \pmod{p}$ for any polynomial function f. In essence, this means that instead of considering a single n tuple over $\mathbb{Z}_n$ with the jth entry of the tuple corresponding to $f(j)$, we can consider k tuples corresponding to the values of the function over $\mathbb{Z}_{p_i}$, for $1 \leq i \leq k$, with the jth entry in each of those k tuples corresponding to $f(j)$ evaluated over the ring $\mathbb{Z}_{p_i}$. Hence, we see that if we can come up with a valid function for each of the tuples over the rings $\mathbb{Z}_{p_i}$ for $1 \leq i \leq k$, then we can use the Chinese remainder theorem to reconstruct a valid polynomial function in the product ring $\mathbb{Z}_{p_1} \times \mathbb{Z}_{p_2} \times \cdots \times \mathbb{Z}_{p_k}$. In fact, for n of this form, Lemma 1 states that in each ring $\mathbb{Z}_{p_i}$ for $1 \leq i \leq k$ the set of functions and the set of polynomial functions are identical, and thus the following theorem holds.

Definition 4. A tuple of integers is said to be m *cyclic* if whenever two indices are a multiple of m apart, then the values of the entries in those indices also differ by a multiple of m. For example, $(1, 4, 3, 2, 9, 8)$ is 2-cyclic.

Theorem 1. *If $n = p_1 p_2 \dots p_k$, then the only condition for a tuple to be a valid polynomial function over $\mathbb{Z}_n$ is that each of the tuples over $\mathbb{Z}_{p_i}$ is p_i cyclic for $1 \leq i \leq k$.*

Proof. This follows from Lemma 1 and the Chinese remainder theorem. □

Using this theorem, the structure of the zero divisors and units of $\mathbb{Z}_n[x]/I$ for n of this form can be deduced.

Theorem 2. *The number of zero divisors of $\mathbb{Z}_n[x]/I$ where I is the ideal of vanishing polynomials and n is of the form $n = \prod_{i=1}^{k} p_i$ is given by:*

$$\prod_{i=1}^{k} p_i^{p_i} - \prod_{i=1}^{k} (p_i - 1)^{p_i}.$$

Proof. Consider the polynomial F and its corresponding polynomial function, denoted by the tuple $(f(0), f(1), \dots, f(n-1))$, where $f(i)$ is an element of $\mathbb{Z}_n$ for for $0 \le i \le n-1$. If we instead consider each of the n-tuples that are obtained when the tuple $(f(0), f(1), \dots, f(n-1))$ is considered over $\mathbb{Z}_{p_i}$, for $1 \le i \le k$, it follows from Theorem 1 that it is sufficient and necessary that each of these tuples be periodic every p_i elements for the original tuple over $\mathbb{Z}_n$ to be a valid polynomial function. It is sufficient because if two elements differ in position by a multiple of p, then the periodicity implies that the elements themselves must be in the same residue class over $\mathbb{Z}_p$. It is also necessary, as it follows from Theorem 1 that each of the following equality chains must hold, where all elements are considered over $\mathbb{Z}_{p_i}$:

$$\begin{gathered}
f(0) = f(p_i) = f(2p_i) = \ldots = f(n - p_i), \\
f(1) = f(p_i + 1) = f(2p_i + 1) = \ldots = f(n - p_i + 1), \\
f(2) = f(p_i + 2) = f(2p_i + 2) = \ldots = f(n - p_i + 2), \\
\vdots \\
\text{and } f(p_i - 1) = f(2p_i - 1) = f(3p_i - 1) = \ldots = f(n - 1).
\end{gathered}$$

Note that the last element in each chain is obtained from the fact that $p_i \mid n$.

For the polynomial function represented by $(f(0), f(1), \dots, f(n-1))$ to be a zero divisor, we consider the existence of a tuple $(g(0), g(1), \dots, g(n-1))$, where $g(i)$ for $0 \le i \le n-1$ are elements of $\mathbb{Z}_n$, such that

$$(f(0), f(1), \dots, f(n-1)) \cdot (g(0), g(1), \dots, g(n-1)) = (\underbrace{0, 0, \dots, 0}_{n \text{ zeros}}).$$

Here, the $\cdot$ denotes tuple multiplication, where multiplication is done separately in each index. The zero tuple $(g(0), g(1), \dots, g(n-1)) = (\underbrace{0, 0, \dots, 0}_{n \text{ zeros}})$ clearly satisfies the equation. The condition that $(f(0), f(1), \dots, f(n-1))$

is a zero divisor is equivalent to the stipulation that the zero tuple is not the only solution for $(g(0), g(1), \ldots, g(n-1))$ to the equation.

To count the number of zero divisors, we proceed with complementary counting and consider when the tuple $(g(0), g(1), \ldots, g(n-1))$ is forced to be 0 at all indices. If the tuple is forced to be 0 over $\mathbb{Z}_n$, this is an equivalent condition to the tuple being forced to be 0 at all indices when the polynomial function is considered over each of the $\mathbb{Z}_{p_i}$, for $1 \leq i \leq k$. The only way for the tuple $(g(0), g(1), \ldots, g(n-1))$ to be forced to be 0 at all indices over $\mathbb{Z}_{p_i}$ is if all indices in the tuple $(f(0), f(1), \ldots, f(n-1))$ evaluated over $\mathbb{Z}_{p_i}$ are relatively prime to p_i. This can be seen from considering each of the indices separately: it is well known that over $\mathbb{Z}_p$, for an arbitrary prime p, if $ab \equiv 0 \pmod{p}$, then either $a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$. In other words, either a is 0 in $\mathbb{Z}_p$, or if it is not, then b must be 0 in $\mathbb{Z}_p$.

Hence, to count the number of non-zero-divisors, we just have to choose the first p_i elements in the tuple $(f(0), f(1), \ldots, f(n-1))$ evaluated over $\mathbb{Z}_{p_i}$ to be relatively prime to p_i, as all functions are polynomial functions over a finite field; then the other elements would be determined from the periodicity previously discussed. Hence, there are $(p_i - 1)^{p_i}$ ways to construct the evaluation of $(f(0), f(1), \ldots, f(n-1))$ over $\mathbb{Z}_{p_i}$, and since $n = \prod_{i=1}^{k} p_i$, and each of the rings $\mathbb{Z}_{p_1}, \mathbb{Z}_{p_2}, \ldots, \mathbb{Z}_{p_n}$ are comaximal, it follows from the Chinese remainder theorem that there are

$$\prod_{i=1}^{k} (p_i - 1)^{p_i}$$

ways to construct polynomial functions which are non-zero-divisors over the ring of polynomial functions.

To count the number of total polynomial functions over $\mathbb{Z}_n$, we can just determine the evaluations of the tuple corresponding to the function over each of the $\mathbb{Z}_{p_i}$ for $1 \leq i \leq k$, again due to all functions over finite fields being polynomial functions. There are p_i choices for each of the first p_i values and then the rest of the elements of the tuple are determined by periodicity, so it follows from a similar application of the Chinese remainder theorem that there are

$$\prod_{i=1}^{k} p_i^{p_i}$$

possible polynomial functions over $\mathbb{Z}_n$. By complementary counting, it follows that the number of zero divisors over $\mathbb{Z}_n$ is given by

$$\prod_{i=1}^{k} p_i^{p_i} - \prod_{i=1}^{k} (p_i - 1)^{p_i},$$

as desired. □

Corollary 1. *Let I be the ideal of vanishing polynomials over $\mathbb{Z}_n$. Then there are*

$$\prod_{i=1}^{k} (p_i - 1)^{p_i}$$

units in $\mathbb{Z}_n[x]/I$ when n is of the form $n = \prod_{i=1}^{k} p_i$.

Proof. This follows easily from the fact that in a finite ring, all nonzero elements are either zero divisors or units. □

4 Vanishing Polynomials Over $\mathbb{Z}_n$

It was shown in [10] that any element of the ideal of vanishing polynomials over $\mathbb{Z}_n$ is of the form

$$G(x) = F(x)B_s(x) + \sum_{k=0}^{s-1} a_k \cdot \frac{n}{\gcd(k!, n)} \cdot B_k(x) \tag{1}$$

where $B_k(x) = (x+1)(x+2)\dots(x+k)$ with $B_0(x) = 1$, and s is the smallest integer such that $n \mid s!$, known as the Smarandache or Kempner function. $F(x)$ is a polynomial which is uniquely defined based on $G(x)$, and a_k's are integers also uniquely defined in the range $0 \leq a_k < \gcd(k!, n)$. Similar results were presented in [6, 9, 12] with slightly different definitions of $B_k(x)$, which we discuss later.

We propose a new method of finding vanishing polynomials with integer coefficients over $\mathbb{Z}_n$, inspired by [8]. It is well known that any integer-valued polynomial can be uniquely written as a linear sum with integer coefficients of functions of the form $\binom{x}{k} = x(x-1)(x-2)\dots(x-k+1)/k!$. If we want a polynomial to vanish modulo n, it must evaluate to an integer multiple of n for all integer inputs, so it must be n times an integer-valued polynomial. Therefore, any vanishing polynomial $F(x)$ corresponds to an integer-valued polynomial $G(x) = F(x)/n$. Conversely, for an integer-valued polynomial $G(x)$ to correspond to a polynomial $F(x) = nG(x)$, all resulting coefficients in $F(x)$ must be integers.

As mentioned previously, every such $G(x)$ can be uniquely represented as a sum $G(x) = \sum_{k=1}^{m} c_k \binom{x}{k}$ so every vanishing polynomial $F(x)$ over $\mathbb{Z}_n$ can be uniquely represented as

$$F(x) = \sum_{k=1}^{m} nc_k \binom{x}{k}$$

where c_k and m are integer values. Now we classify which sums of this form yield valid polynomials. First, we will show that each element of the sum must have integer coefficients.

Proposition 2. *If any term in the summation $\sum_{k=1}^{m} nc_k \binom{x}{k}$ has a non-integer coefficient then the resulting polynomial cannot have integer coefficients.*

Proof. Assume for contradiction that we can construct a polynomial of this form where one of the terms has a non-integer coefficient. If any term $nc_i \binom{x}{i} = \frac{nc_i}{i!} \cdot x(x-1)(x-2)\ldots(x-i+1)$ has a non-integer coefficient this means $i!$ does not divide nc_i and therefore the leading coefficient of this term, that is the coefficient on x^i, is also non-integer. Thus, if the sum is to have all integer coefficients, there must be a term of greater degree, say j, that has a non-integer coefficient on x^i. As before, this implies that the leading coefficient of this new term, that is the coefficient on x^j, is also non-integer. Inductively, we conclude that for every term with non-integer coefficients, there must be a term of greater degree with non-integer coefficients and therefore there is no term of maximal degree. We have reached a contradiction. □

For an element of the form $nc_k \cdot \binom{x}{k}$ to have integer coefficients, we must have $k! \mid nc_k$. The smallest such c_k is $k!/\gcd(n, k!)$ and any greater c_k would be a multiple of this, so any valid c_k can be written as $a_k \cdot (k!/\gcd(n, k!))$ for an arbitrary integer $0 \leq a_k < \gcd(n, k!)$. Note that any a_k outside this range gives a polynomial equivalent to having an a_k in this range by reduction modulo n. If we define s to be the smallest integer such that $n \mid s!$, any polynomial $na_k \cdot (k!/\gcd(k!, n)) \cdot \binom{x}{k}$ where $k \geq s$ is a polynomial multiple of $\binom{x}{s}$, therefore we have arrived at exactly the formulation in Equation 1 except with $B_k(x)$ defined as $k! \cdot \binom{x}{k}$.

An immediate consequence of this formula is that the generating set for the ideal of vanishing polynomials over $\mathbb{Z}_n$ is

$$\left\{\frac{n}{\gcd(k!,n)} \cdot B_k(x) \mid k \in \mathbb{Z}_{\geq 0}\right\}$$

for either definition of $B_k(x)$. Note that if k is less than the smallest prime divisor of n, we get the zero polynomial.

From this formulation, we can immediately find the degree of the minimal degree monic vanishing polynomial and minimal degree non-monic vanishing polynomial, which would be s and the smallest factor of n, respectively. Note that the minimal degree non-monic polynomial must be unique up to multiplication by a constant since the generating set only contains a single nonzero polynomial of that degree or lower.

There exists a far simpler description of this minimal-degree polynomial, namely $\frac{n}{p_1} \cdot x(x^{p_1-1} - 1)$ where p_1 is the smallest prime divisor of n. Fermat's little theorem states that $x^{p_1-1} - 1 = 0$ modulo p_1 for any x not divisible by p_1. To take care of the $p_1 \mid x$ case we multiply the whole polynomial by x. Thus, the polynomial $x(x^{p_1-1} - 1)$ is a multiple of p_1 for any input, and when multiplied by the leading coefficient n/p_1 it vanishes over $\mathbb{Z}_n$. Since the leading coefficient and degree matches the other formulation we have for the minimal degree monic polynomial they must be the same polynomial over $\mathbb{Z}_n$, which is an interesting identity.

While the generating set we found above is convenient in many ways because it uses linear combinations, if we consider it from the point of view of a generating set of an ideal, that is allow any coefficients in the ring, many of the elements become redundant. In particular, if we have two polynomials $a \cdot \binom{x}{i} \cdot i!$ and $a \cdot \binom{x}{j} \cdot j!$ for some integer a, and $i < j$ then the second polynomial is a polynomial multiple of the first and therefore redundant in a generating set. Thus, to minimize our generating set we can remove any polynomials $k! \cdot (n/\gcd(k!,n)) \cdot \binom{x}{k}$ for which k is not the minimal integer which gives the same value of $\gcd(k!,n)$.

Let us return to the varying definitions of $B_k(x)$ across multiple papers. In fact, $B_k(x)$ can be replaced with any sequence of terms such that the product is divisible by $\gcd(n,k!)$ and the set of generators will remain valid (for instance, $B_k(x) = (x+i)(x+i+1)\dots(x+i+k-1)$ for any integer i). The fact that a polynomial that uses any such $B_k(x)$ is vanishing is easy to prove. The coefficient on $B_k(x)$ must be a multiple of $n/\gcd(n,k!)$, thus the product is a multiple of n and the polynomial is vanishing. Furthermore, any polynomial $F(x)$ with degree d and integer coefficients can be uniquely decomposed as

$$F(x) = \sum_{k=0}^{d} b_k B_k(x) \tag{2}$$

using polynomial division as long as each $B_k(x)$ has degree k and is monic. It remains to show that every vanishing polynomial decomposed in this way has coefficients conforming with the required conditions, namely showing that $b_k = a_k \cdot n/\gcd(n, k!)$ for an integer a_k. We show this by polynomial division. Let our starting vanishing polynomial $F(x)$ have degree d. By Equation 1, we know the leading coefficient must be of the form $a_d \cdot \gcd(n, d!)$ for some integer a_d. When we take $F(x) - a_d \cdot \gcd(n, d!) \cdot B_d(x)$, we have the difference of two vanishing polynomials, giving another vanishing polynomial $F_1(x)$ with degree $d_1 < d$. Applying Equation 1 again, the leading coefficient of $F_1(x)$ must be of the form $a_{d_1} \cdot \gcd(n, d_1!)$ so we can repeat the procedure to get a new vanishing polynomial $F_2(x)$ with degree $d_2 < d_1$. Since the initial degree d is finite, the process must terminate with $d_m = 0$ at step m, showing that $b_k = a_k \cdot n/\gcd(n, k!)$ in Equation 2 for a vanishing polynomial $F(x)$, as desired.

5 Generalization of Monic Vanishing Polynomials

In Section 4, we discuss the notion of the monic vanishing polynomial of minimal degree over a ring of the form $\mathbb{Z}_n$. This can be extended to more general rings R: define $s(R)$ to be the minimum positive integer m such that there exists a polynomial $P(x) \in R[x]$ of degree less than m for which $P(r) = r^m$ for all elements $r \in R$. In other words, $s(R)$ denotes the minimal m for which the polynomial function $x \mapsto x^m$ corresponds to a polynomial in $R[x]$ of degree less than m. Note that the degree of the aforementioned minimal degree monic vanishing polynomial over $\mathbb{Z}_n$ corresponds exactly with $s(\mathbb{Z}_n)$.

We can similarly define an extension of this notion to subrings of $R[x]$. Define $s(S; R)$, where S is a subring of R, to equal the minimal degree m such that a polynomial $P(x) \in S[x]$ of degree less than m corresponds to the polynomial function $x \mapsto x^m$. In essence, the distinction between $s(S; R)$ and

$s(R)$ is that $s(S;R)$ includes the additional restriction that the coefficients of $P(x)$ must be in the subring S, in contrast to the more relaxed condition of being in R.

These two characteristic numbers of a ring, $s(R)$ and $s(S;R)$, are introduced in [11]. In [11], the case when $S = R'$, where R' denotes the subring generated by 1, is specifically studied. Various number-theoretic and combinatorial bounds are given on the value of $s(R';R)$ if $s(R)$ is finite. In this section, we directly compute the value of $s(R)$ for an infinite class of rings that satisfy a specific form and use this to compute a bound on $s(R';R)$ for this class of rings.

Let U denote the set of all rings of the form $\mathbb{Z}_2[x]/(x^a + x^{a+1})$, where $a \geq 3$.

Lemma 2. *For all rings R in the set U, we have $s(R) \leq 4$.*

Proof. It suffices to show that for all $P \in \mathbb{Z}_2[x]$, it holds that

$$x^{a-2}P + (x^{a-3} + x^{a-2})P^2 + x^{a-3}P^4 \equiv 0 \pmod{x^a + x^{a+1}}. \qquad (3)$$

Consider when $P = x^k$ for a positive integer k. Equation 3 evaluates to

$$x^{a-2}(x^k)+(x^{a-3}+x^{a-2})(x^{2k})+x^{a-3}(x^{4k}) = x^{a+k-2}+x^{a+2k-3}+x^{a+2k-2}+x^{a+4k-3}.$$

To verify that this expression vanishes $\pmod{x^a + x^{a+1}}$, we do casework based on the value of k.

The cases when $k = 0$ and $k = 1$ are easy to verify manually. When $k = 0$, the expression is equal to $x^{a-2} + x^{a-3} + x^{a-2} + x^{a-3} \equiv 0 \pmod{x^a + x^{a+1}}$, and when $k = 1$, the expression is equal to $x^{a-1} + x^{a-1} + x^a + x^{a+1} \equiv 0 \pmod{x^a + x^{a+1}}$.

When $k \geq 2$, the expression can be greatly simplified by noting that $\pmod{x^a + x^{a+1}}$, we have that $x^a \equiv -x^{a+1}$. Since all the coefficients of the terms are in $\mathbb{Z}_2[x]/(x^a + x^{a+1})$, it follows that $-x^{a+1}$ is identically equal to x^{a+1}. Thus, we have that

$$x^a \equiv x^{a+1} \equiv x^{a+2} \equiv x^{a+3} \equiv \ldots.$$

If $k \geq 2$, then $a + k - 2, a + 2k - 3, a + 2k - 2$, and $a + 4k - 3$ are all at least a, so the expression evaluates to $x^a + x^a + x^a + x^a \equiv 0 \pmod{x^a + x^{a+1}}$.

Suppose Equation 3 vanishes for P_1 and P_2. Then, due to the additive properties of $\mathbb{Z}_2[x]$, we have

$$\begin{aligned} &x^{a-2}(P_1+P_2)+(x^{a-3}+x^{a-2})(P_1+P_2)^2+x^{a-3}(P_1+P_2)^4 \\ =&\sum_{i=1}^{2} x^{a-2}P_i+(x^{a-3}+x^{a-2})P_i^2+x^{a-3}P_i^4 \equiv 0 \pmod{x^a+x^{a+1}}, \end{aligned}$$

demonstrating that P_1+P_2 vanishes in Equation 3 as well. Thus, any additive combination of monomials vanishes in Equation 3, and since all polynomials in $\mathbb{Z}_2[x]$ can be expressed as the sum of monomials, we have shown that Equation 3 vanishes for all $P \in \mathbb{Z}_2[x]$, as desired. □

Lemma 3. *For all rings R in the set U, we have $s(R) \geq 4$.*

Proof. For the sake of contradiction, suppose that $s(R) \leq 3$. In other words, suppose that there exist coefficients $b_0, b_1, b_2, b_3 \in R$ (not necessarily nonzero) for which

$$b_0+b_1P+b_2P^2+b_3P^3 \equiv 0 \pmod{x^a+x^{a+1}} \tag{4}$$

for all $P \in \mathbb{Z}_2[x]$. Then, in particular, Equation 4 must vanish when $P = 0, 1, x, 1+x$.

When $P=0$, Equation 4 evaluates to b_0, so $b_0=0$.

Plugging in $P=1+x$, the expression can be simplified as follows:

$$\begin{aligned} &b_1(1+x)+b_2(1+x)^2+b_3(1+x)^3 \\ =&\, b_1(1+x)+b_2(1+x^2)+b_3(1+x+x^2+x^3) \equiv 0 \pmod{x^a+x^{a+1}}. \end{aligned} \tag{5}$$

We can also plug in $P=1$ and $P=x$ to yield the following equations:

$$b_1+b_2+b_3 \equiv 0 \pmod{x^a+x^{a+1}}, \tag{6}$$

$$b_1x+b_2x^2+b_3x^3 \equiv 0 \pmod{x^a+x^{a+1}}. \tag{7}$$

We can then subtract Equation 6 and Equation 7, respectively, from Equation 5, yielding $b_3(x+x^2) \equiv 0 \pmod{x^a+x^{a+1}}$.

As a result, b_3 is forced to be divisible by x^{a-1}, but since Equation 4 must be monic according to the definition of $s(R)$, this implies that $b_3=0$.

Equation 6 now simplifies to $b_1+b_2 \equiv 0 \pmod{x^a+x^{a+1}}$ and Equation 7 simplifies to $b_1x+b_2x^2 \equiv 0 \pmod{x^a+x^{a+1}}$. The former expression yields that $b_1=b_2$, and plugging this into the latter gives that $b_2(x+x^2) \equiv 0$

(mod $x^a + x^{a+1}$). Using analogous logic as we did to conclude that $b_3 = 0$, we see that $b_2 = b_1 = 0$.

So we have that $b_3 = b_2 = b_1 = b_0 = 0$, a contradiction (Equation 4 no longer has a well-defined degree), as desired.

□

Theorem 3. *For all rings R in the set U, we have $s(R) = 4$.*

Proof. This immediately follows from Lemma 2 and Lemma 3 □

We now obtain a corresponding upper bound for $s(R'; R)$ based on the value of $s(R)$. Let $\operatorname{lcm}(n)$ denote $\operatorname{lcm}[1, 2, \ldots, n]$. The theorem below is from [11].

Theorem 4 (Theorem 7, [11])**.** *Let $x = s(R)$. If x is finite, then the inequality $s(R'; R) \leq \operatorname{lcm}(n) + n$ holds, where $n = x!^{(2x)^x x}$.*

We can apply the above theorem to the rings in U.

Corollary 2. *We have $s(R'; R) \leq \operatorname{lcm}(24^{2^{14}}) + 24^{2^{14}}$ for all rings R in U.*

Although this bound may seem large for smaller values of a for R of the form $\mathbb{Z}_2[x]/(x^a + x^{a+1})$, an interesting property about this bound is that it does not depend on the value of a. In other words, as the value of a becomes increasingly larger and approaches infinity, the bound is not affected. Thus, even when the size of the ring approaches infinity, Corollary 2 provides a finite bound for the value of $s(R'; R)$.

6 Vanishing Polynomials Over Product Rings

The results in Section 4 can be generalized to direct products of multiple rings as follows.

Let $k \geq 2$ be an arbitrary positive integer, and let $R_1, \ldots, R_k$ be finite commutative rings. Let $R \cong R_1 \times \cdots \times R_k$, and let I be the vanishing polynomial ideal of $R[x]$, I_1 be the ideal of vanishing polynomials of $R_1[x]$, and so on. For any R_i, let $\pi_{R_i} : R \to R_i$ be the canonical projection mapping onto R_i.

First, we establish an isomorphism that maps vanishing polynomials in $R[x]$ to corresponding tuples of vanishing polynomials in $R_1[x], \ldots, R_k[x]$ and vice versa. The following well known lemma is found in [1], but we include the following proof as the notions developed in it are used in other results throughout this section.

Lemma 4. *Given $R \cong R_1 \times \cdots \times R_k$, we have*

$$R[x] \cong R_1[x] \times \cdots \times R_k[x].$$

Proof. We define a mapping ϕ from $R[x]$ to $R_1[x] \times \cdots \times R_k[x]$ which breaks down a polynomial $P(x) \in R[x]$ of degree m into a k-tuple of polynomials by splitting up the components in the coefficients. More specifically, let

$$P(x) = \sum_{i=0}^{m} a_i x^i.$$

Then,

$$\phi(P(x)) = \left(\sum_{i=0}^{m} \pi_{R_1}(a_i)x^i, \sum_{i=0}^{m} \pi_{R_2}(a_i)x^i, \dots, \sum_{i=0}^{m} \pi_{R_k}(a_i)x^i \right).$$

Notice that ϕ is a homomorphism because for any arbitrary polynomials $P(x), Q(x)$ in $R[x]$, $\phi(P(x) + Q(x))$ is the componentwise sum of $\phi(P(x))$ and $\phi(Q(x))$, and $\phi(P(x)Q(x))$ is the componentwise product of $\phi(P(x))$ and $\phi(Q(x))$. In addition, we define ϕ^{-1} from $R_1[x] \times \cdots \times R_k[x]$ to $R[x]$ mapping k polynomials $P_1(x) \in R_1[x], \dots, P_k(x) \in R_k[x]$ with highest degree m to a polynomial $P(x) \in R[x]$. For any integer j from 1 to k, let

$$P_j = \sum_{i=1}^{m} a_{i,j} x^i.$$

Then,

$$\phi^{-1}((P_1(x), \dots, P_k(x))) = \sum_{i=1}^{m} (a_{i,1}, a_{i,2}, \dots, a_{i,k}) x^i.$$

We now note that for any polynomial $P(x) \in R[x]$, $\phi(\phi^{-1}(P(x))) = P(x)$ Therefore ϕ is invertible, so it is an isomorphism. □

Theorem 5. *The ideal I of vanishing polynomials in $R[x]$ is isomorphic to the direct products of the ideals $I_1, \dots, I_k$ of vanishing polynomials in $R_1[x], \dots, R_k[x]$, respectively. In other words,*

$$I \cong I_1 \times \cdots \times I_k.$$

Proof. Consider a vanishing polynomial $P(x)$ in $R[x]$. Let $P_i(x) = \pi_{R_i}(\phi(P(x)))$ be the canonical projection of $P(x)$ onto $R_i[x]$ for all integers i from 1 to k, as defined prior. Then, each $P_i(x)$ must be a vanishing polynomial in $R_i[x]$. Therefore any vanishing polynomial in R has vanishing polynomials in $R_1[x], \ldots, R_k[x]$.

Going in the other direction, suppose we have a k-tuple of vanishing polynomials $(P_1(x), \ldots, P_k(x))$, where $P_i(x)$ is in polynomial ring $R_i[x]$ for $1 \leq i \leq k$. It then follows that there exists a polynomial $P(x)$ in $R[x]$ such that $P(x) = \phi^{-1}((P_1(x), \ldots, P_k(x)))$. It follows that $P(x)$ is a vanishing polynomial. Therefore, if we have a k-tuple of vanishing polynomials in each of $R_1[x], \ldots, R_k[x]$, we can construct a vanishing polynomial in $R[x]$. Thus, I is isomorphic to $I_1 \times \cdots \times I_k$. □

Now we consider an isomorphism between the rings of polynomial functions over R and over $R_1 \times R_2 \times \cdots \times R_k$.

Theorem 6. *Let R be the direct product of k rings $R_1, \ldots, R_k$. Then, the ring of polynomial functions on R is isomorphic to the direct product of the rings of polynomial functions on $R_1, \ldots, R_k$. In other words,*

$$R[x]/I \cong R_1[x]/I_1 \times \cdots \times R_k[x]/I_k.$$

Proof. We have already established that $R[x]/I$ is the ring of polynomial functions over R. Similarly, $R_1[x]/I_1$ is the ring of polynomial functions over R_1, and so on.

Now, consider a polynomial function over R. Each polynomial function f is in essence a mapping of every possible input k-tuple to an output k-tuple. If we consider only the ith component of each k-tuple, we construct a mapping β_i which maps a polynomial function $f \in R[x]/I$ to a function f_i over R_i such that for any $r \in R$,

$$\pi_{R_i}(f(r)) = f_i(\pi_{R_i}(r)).$$

Notice that given any two polynomial functions $f \mapsto f_i$ and $g \mapsto g_i$, we have

$$\pi_{R_i}(f(r)) + \pi_{R_i}(g(r)) = f_i(\pi_{R_i}(r)) + g_i(\pi_{R_i}(r)).$$

Therefore, by the definition π_{R_i},

$$\pi_{R_i}(f(r) + g(r)) = (f_i + g_i)(\pi_{R_i}(r)).$$

This means that

$$\beta_i(f+g) = \beta_i(f) + \beta_i(g).$$

A similar argument holds over multiplication, so β_i is a homomorphism.

Now we must show that f_i is a polynomial function (note that not all functions can be expressed as polynomials). Let F be a polynomial in $R[x]$ that corresponds to the polynomial function f. Then, take only the i-th component of each coefficient in F. We now have a polynomial F_i in $R_i[x]$ that evaluates to f_i. Therefore f_i is a polynomial function, so every f over R can be split into $f_1, \ldots, f_k$ over $R_1, \ldots, R_k$, respectively.

On the other hand, suppose we have a tuple of k polynomial functions $f_1, \ldots, f_k$ over $R_1, \ldots, R_k$, respectively. We construct a function f over R that maps any input tuple $(a_1, \ldots, a_k)$ to an output tuple $(f_1(a_1), \ldots, f_k(a_k))$.

We now show that f is a polynomial function. Let $F_1, \ldots, F_k$ be polynomials in $R_1[x], \ldots, R_k[x]$ which evaluate to $f_1, \ldots, f_k$, respectively, and $G_1, \ldots, G_k$ their extensions in R. Let $F = (1, \ldots, 0)G_1 + \ldots + (0, \ldots, 1)G_k$, where every G_i is multiplied by an k-tuple whose ith component is 1 and whose other components are 0. This polynomial F evaluates to the function f. Therefore for all sets of k polynomial functions $f_1, \ldots, f_k$ over $R_1, \ldots, R_k$, respectively, we have a polynomial function f over R. Thus, the ring of polynomial functions over R is isomorphic to the direct product of the rings of polynomial functions over $R_1, \ldots, R_k$, respectively. □

We can extend our results to polynomial functions in multiple indeterminates using the following theorem.

Theorem 7. *Suppose R is a finite ring such that any function $R \to R$ can be expressed as a polynomial in R. Then, any function $R^n \to R$ for any integer $n \geq 2$ can be expressed as a polynomial F in $R[x_1, x_2, \ldots, x_n]$.*

Proof. Let r be an element in the ring R, and let $F_r(x)$ be a polynomial in $R[x]$ such that for all $x \neq r$, $F_r(x) = 0$, and $F_r(r) = 1$. Let $r_1, r_2, \ldots, r_n$ be elements of R, and let us define $f_{r_1,r_2,\ldots,r_n}(x_1, x_2, \ldots, x_n) : R^n \to R$ to be a function such that if $(x_1, x_2, \ldots, x_n) \neq (r_1, r_2, \ldots, r_n)$, then we have $f_{r_1,r_2,\ldots,r_n}(x_1, x_2, \ldots, x_n) = 0$, and $f_{r_1,r_2,\ldots,r_n}(r_1, r_2, \ldots, r_n) = 1$. For any choice of elements $r_1, r_2, \ldots, r_n, x_1, x_2, \ldots, x_n$ in R, f satisfies the equation $f_{r_1,r_2,\ldots,r_n}(x_1, x_2, \ldots, x_n) = F_{r_1}(x_1)F_{r_2}(x_2) \ldots F_{r_n}(x_n)$, and so it follows that $f_{r_1,r_2,\ldots,r_n}(x_1, x_2, \ldots, x_n)$ can be expressed as a polynomial for any choice of $r_1, r_2, \ldots, r_n$ in R. Clearly, any function $f : R^n \to R$ can be expressed as a finite sum of $f_{r_1,r_2,\ldots,r_n}(x_1, x_2, \ldots, x_n)$, so any function $f : R^n \to R$ can be expressed as a polynomial with coefficients in R and n indeterminates, as desired. □

7 Vanishing Polynomials Over Rings of Prime Power Order

In Section 6 we established that if a ring R is a direct product of rings $R_1, R_2, \ldots, R_n$, then its vanishing polynomial ideal I is a direct product of the vanishing polynomial ideals of $R_1, R_2, \ldots, R_n$. As a consequence, if we have a unique representation of all vanishing polynomials over R_1 and R_2 and so on, we have a unique representation of all vanishing polynomials over R.

We want to find unique representations of all vanishing polynomials over all rings, and one big step is to find such representations for all finite commutative rings with identity. We also know that every finite commutative ring with identity can be expressed as the direct product of local commutative rings with identity of prime power order, as given in [2]. Therefore, if we find unique representations of all vanishing polynomials over all commutative rings of prime power orders with identity, we have such representations over all finite commutative rings with identity.

7.1 Rings of order p

Naturally, we begin by considering rings of prime order p, since proving or disproving a property for all rings of prime order will cover a large portion of the general case. Because p is prime, we know that all commutative rings of prime order with identity are isomorphic to $\mathbb{Z}_p$, over which we already have a description of all the vanishing polynomials.

7.2 Rings of order p^2

We can now consider rings of order p^2, where p is prime. This case is more nuanced than the last, but still within reach: every ring of order p^2 is isomorphic to either $\mathbb{Z}_p \times \mathbb{Z}_p$, $\mathbb{Z}_{p^2}$, $\mathrm{GF}(p^2)$, or $\mathbb{Z}_p[x]/(x^2)$. We examine these subcases one by one.

First, $\mathbb{Z}_p \times \mathbb{Z}_p$ is a direct product of two rings that we already have desired representations for, so we have such a representation for $\mathbb{Z}_p \times \mathbb{Z}_p$.

Second, $\mathbb{Z}_{p^2}$ is a ring of integers modulo an integer, so we already have a unique representation for its vanishing polynomials.

The third subcase is $\mathrm{GF}(p^2)$ (the finite field of p^2 elements), whose elements we represent as $f_1, \ldots, f_{p^2}$. We analyze this case presently.

Let $V(x) = (x - f_1)(x - f_2) \ldots (x - f_{p^2})$, where $\{f_1, f_2, \ldots, f_{p^2}\}$ are all the elements of $\mathrm{GF}(p^2)$. Then, $V(x)$ is a vanishing polynomial, so all multiples of $V(x)$ are vanishing polynomials. Also, since there are no zero divisors in $\mathrm{GF}(p^2)$, all vanishing polynomials are necessarily multiples of $(x - f_1), (x - f_2), \ldots, (x - f_{p^2})$. Therefore, all vanishing polynomials are necessarily multiples of $V(x)$. Thus, there exists a one-to-one correspondence between vanishing polynomials and multiplies of $V(x)$, so any vanishing polynomial $G(x)$ in $\mathrm{GF}(p^2)$ can be uniquely represented as

$$G(x) = F(x)V(x)$$

where $F(x)$ is a polynomial which is uniquely defined based on $G(x)$.

The fourth subcase $\mathbb{Z}_p[x]/(x^2)$ is the trickiest. To summarize the structure of the ring, it can be interpreted as the ring $\mathbb{Z}_p$ adjoined with a square nilpotent element. Because x appears as an element of $\mathbb{Z}_p[x]/(x^2)$, we will use the indeterminate y when dealing with polynomials over $\mathbb{Z}_p[x]/(x^2)$. For example, $F(y) = yx$ is a polynomial $F(y) \in (\mathbb{Z}_p[x]/(x^2))[y]$, and it maps 1 to x and x to 0.

Definition 5. Let polynomial $P(y) = a_n y^n + \cdots + a_1 y + a_0$, where $n \geq 2$. Then, the *formal derivative* is $P'(y) = n a_n y^{n-1} + \cdots + 2a_2 y + a_1$.

Proposition 3. *Let J and K be vanishing polynomials over $\mathbb{Z}_p$. Then, the polynomial*

$$G(y) = J(y) + xK(y)$$

vanishes in $\mathbb{Z}_p[x]/(x^2)$ if and only if J' vanishes over $\mathbb{Z}_p$.

Proof. Let $G(y)$ be a vanishing polynomial in $\mathbb{Z}_p[x]/(x^2)$. Then,

$$G(y) = \sum_{i=0}^{n} C_i y^i.$$

Substituting $y = Ax + B$ and $C_i = D_i x + E_i$ we have

$$\begin{aligned} G(y) &= \sum_{i=0}^{n} (D_i x + E_i)(Ax + B)^i \\ &= \sum_{i=1}^{n} (D_i x + E_i)(Ax + B)^i + D_0 x + E_0 \\ &= \sum_{i=1}^{n} (D_i x + E_i)(iAB^{i-1}x + B^i) + D_0 x + E_0 \\ &= \sum_{i=1}^{n} E_i B^i + E_0 + x \sum_{i=1}^{n} (D_i B^i) + D_0 x + xA \sum_{i=1}^{n} iB^{i-1} E_i \\ &= \sum_{i=0}^{n} E_i B^i + x \sum_{i=0}^{n} (D_i B^i) + xA \sum_{i=0}^{n} (i+1) E_{i+1} B^i \\ &= J(B) + xK(B) + xAJ'(B) \end{aligned}$$

where $J(B)$ and $K(B)$ are polynomials in $\mathbb{Z}_p$. We immediately see that $J(B)$ is vanishing, and if we plug in $A = 0$ we get that $K(B)$ is vanishing. If we now plug in $A = 1$ we get that $J'(B)$ is also vanishing. Now, if we plug in $B = y$ and $A = 0$ we get $G(y) = J(y) + xK(y)$.

The opposite is clear: let A, B be elements of $\mathbb{Z}_p$ and $y = Ax + B$, and suppose J, K, J' are vanishing over $\mathbb{Z}_p$. Then, the polynomial given by $G(y) = J(B) + xK(B) + xAJ'(B)$ evaluates to 0. Therefore, since all elements of $\mathbb{Z}_p[x]/(x^2)$ can be represented as $Ax + B$, G is vanishing on $\mathbb{Z}_p[x]/(x^2)$. □

Example 2. To illustrate this theorem, we will now consider some examples over $\mathbb{Z}_2[x]/(x^2)$.

1. Suppose $J(y) = 0$ and $K(y) = y(y + 1)$. Then, both J and K vanish over $\mathbb{Z}_2$. In addition, $J'(y) = 0$ vanishes over $\mathbb{Z}_2$. Now, notice that $G(y) = J(y) + xK(y) = xy(y + 1)$ vanishes over $\mathbb{Z}_2[x]/(x^2)$.

2. Suppose $J(y) = y^4 + y^2$ and $K(y) = 0$. Then, both J and K vanish over $\mathbb{Z}_2$. In addition, $J'(y) = 4y^3 + 2y = 0$ vanishes over $\mathbb{Z}_2$. Now, notice that $G(y) = J(y) + xK(y) = y^4 + y^2$ vanishes over $\mathbb{Z}_2[x]/(x^2)$.

3. Suppose $J(y) = y(y + 1)$ and $K(y) = 0$. Then, both J and K vanish over $\mathbb{Z}_2$. However, $J'(y) = 2y + 1 = 1$ does not vanish over $\mathbb{Z}_2$. Now, notice that $G(y) = J(y) + xK(y) = y(y + 1)$ does not vanish over $\mathbb{Z}_2[x]/(x^2)$: for a counterexample, see $K(x) = x \neq 0$.

8 Vanishing Polynomials Over General Rings

We can apply a generalization of the method used in Section 4 to find vanishing polynomials over an arbitrary commutative ring R with identity. Given an element $r \in R$, we denote the ideal generated by r as $(r) = \{qr \mid q \in R\}$. We begin with a definition that simplifies the construction.

Definition 6. Given an element $y \in R$ such that the quotient $R/(y)$ partitions R into a finite number of equivalence classes of the form $a_1 + (y), a_2 + (y), \ldots, a_n + (y)$, let $F_y(x) = (x - a_1)(x - a_2) \ldots (x - a_n)$. If $R/(y)$ is not finite we say $F_y(x)$ is not defined.

We claim that $F_y(x)$ evaluates to a multiple of y for any input $x \in R$. Note that x must fall into some equivalence class $a_i + (y)$, so $x - a_i \in (y)$. Since $F_y(x)$ contains the factor $(x - a_i) \in (y)$ and (y) is an ideal, $F_y(x) \in (y)$ so $F_y(x)$ is a multiple of y.

Theorem 8. *Consider a set of zero divisors $\{y_1, y_2, \ldots, y_n\}$ which satisfies $y_1 y_2 \ldots y_n = 0$. Let $N \subset \mathbb{N}$ be an indexing set which can contain i if $F_{y_i}(x)$ is defined (but does not necessarily contain i if $F_{y_i}(x)$ is defined). Let $M \subset \mathbb{N}$ contain all integers $1 \leq j \leq n$ such that $j \notin N$. Then the polynomial*

$$G(x) = \left(\prod_{j \in M} y_j \right) \left(\prod_{i \in N} F_{y_i}(x) \right)$$

is vanishing.

Proof. This follows directly from the definition of $F_y(x)$. For any input x, $G(x)$ evaluates to a multiple of $y_1 y_2 \ldots y_n = 0$ so it is vanishing. □

Observe that if all quotients $R/(y_1), R/(y_2), \ldots, R/(y_n)$ are finite, we can take the subset of y_i's to be the whole set in which case we get a monic polynomial. Also, if R is finite, setting $y_1 = 0$ gives us the monic vanishing polynomial $F_0(x)$ whose degree is $|R|$ (such as for a finite field which has no other zero divisors).

Example 3. This method allows us to find vanishing polynomials not only for finite rings but also for infinite ones. For instance, in the ring $\prod_{n=1}^{\infty} \mathbb{Z}_2$, consider the pair of zero divisors $(0, 1, 1, 1, 1, \ldots)$ and $(1, 0, 0, 0, 0, \ldots)$. Since the quotient of this ring by the ideal generated by $(0, 1, 1, 1, 1, \ldots)$ is finite (it is isomorphic to $\mathbb{Z}_2$), there exists a degree 2 vanishing polynomial for this ring. Furthermore, since we can pick any representatives from the cosets in the quotient there exists an infinite number of degree 2 vanishing polynomials for this ring.

Note that a polynomial generated in this way will often have a lot of redundant terms since if we have two finite quotients $R/(y_i)$ and $R/(y_j)$, there will often be pairs of factors $(x-c) = (x-d)$ with c chosen from one of the cosets of $R/(y_i)$ and d chosen from one of the cosets of $R/(y_k)$. To remove such redundancies we can create groups of identical factors with the additional condition that factors corresponding to quotients $R/(y_i)$ and $R/(y_j)$ can only be grouped together if being a multiple of both y_i and y_j implies being a multiple of $y_i y_j$ (analogous to y_i and y_j being coprime over the integers). Once such a grouping is carried out in a way minimizing the number of groups (including picking representatives from cosets to facilitate this process), we simply keep a single factor from each of the groups.

Example 4. Consider $(x-1)(x-2)\cdot(x-1)(x-2)\cdot(x-1)(x-2)(x-3)$, a polynomial over the ring $\mathbb{Z}_{12}$ using the zero divisors $2\cdot 2\cdot 3 = 0$. We cannot group terms corresponding to the two instances of $\mathbb{Z}_{12}/(2)$ but we can group terms corresponding to $\mathbb{Z}_{12}/(2)$ with terms corresponding to $\mathbb{Z}_{12}/(3)$. We can also replace one of the terms $(x-1)$ with $(x-3)$ as it belongs to the same equivalence class modulo 2. Thus, we get the grouping pairs $(x-1)(x-1)\cdot(x-2)(x-2)\cdot(x-3)(x-3)\cdot(x-2)$, giving the final reduced polynomial $(x-1)(x-2)(x-3)(x-2)$.

Proposition 4. *If $R = \mathbb{Z}_n$, this description is sufficient to classify all vanishing polynomials when we take $y_1 \dots y_k = n$ to be the prime factorization of n.*

Proof. This is essentially the proof found at the end of Section 4. Let us define N such that $\prod_{i\in N} y_i = \gcd(n, k!)$. Then $G(x)$ as defined in Theorem 8 behaves identically to $\frac{n}{\gcd(k!,n)} B_k(x)$ in Equation 1. In particular, note that we get the same leading coefficients.

Thus, to completely reuse the proof in Section 4 it simply remains to show that this $G(x)$ has degree less than or equal to k after removing duplicate terms. Let us define $z_1^{e_1} z_2^{e_2} \dots z_l^{e_l} = \gcd(n, k!)$ to be the prime factorization of $\gcd(n, k!)$. Using the method above we can chose representatives to get $F_{z_i}(x)F_{z_i}(x)\dots F_{z_i}(x) = (x-1)(x-2)\dots(x-z_i e_i)$ for each $z_i^{e_i}$. After performing the grouping as described, we simply get $(x-1)(x-2)\dots(x-z_j e_j)$

for whichever $z_j e_j$ was maximal (since all z_i are coprime). Now, if $k!$ has the factor $z_i^{e_i}$, k is at least $z_i e_i$ so the polynomial we get has degree less than or equal to k. From this point, the proof is identical, except with $\frac{n}{\gcd(k!,n)} B_k(x)$ replaced by an appropriate $G(x)$ for each value of k. □

This is not the case in general. For instance, the polynomial $x(x + (1,1,1,1,\ldots))$ is vanishing over $\prod_{n=1}^{\infty} \mathbb{Z}_2$ but does not correspond to any pair zero divisors as described previously. This gap, however, can be easily fixed by noticing that if a ring R can be represented as a direct product of a ring S with itself and some other ring T, namely $R = S \times S \times T$, a vanishing polynomial for the ring $S \times T$ can be trivially generalized to a vanishing polynomial for the ring R by replacing any terms (s,t) with (s,s,t). In particular, doing this infinitely for $S = \mathbb{Z}_2$, we get the polynomial $x(x + (1,1,1,1,\ldots))$ over $\prod_{n=1}^{\infty} \mathbb{Z}_2$.

With this generalization, we do not currently know if this gives a complete description of vanishing polynomials but do not have any examples suggesting otherwise.

9 Counting Roots of Polynomials

Before considering the problem of counting and bounding the number of roots of polynomials over rings, we start by considering a weaker notion, namely, considering whether the number of roots of these polynomials is finite.

More specifically, we aim to study what characteristics we can discern about a commutative nonzero ring (not necessarily with identity) with the property that every polynomial has a finite number of roots. In the case where the ring is finite, it easily follows that every polynomial has a finite number of roots as there are only a finite number of elements in the ring. In the case where the ring is infinite, the following theorem provides a characterization of rings that satisfy the desired property. A similar result was given in [3], but we extend their proof to include rings that don't necessarily have an identity element.

Theorem 9. *The only infinite rings R which satisfy the property that all polynomials in $R[x]$ have finitely many roots are rings with no nonzero zero divisors.*

Proof. Suppose that the infinite ring R satisfies the given property. We wish to show that this implies that R has no nonzero zero divisors.

Suppose for contradiction that R does have a zero divisor, call it a. Then the roots of the polynomial ax over R are by definition the annihilator of a over R (denoted $\mathrm{Ann}(a)$), which is well known to be an ideal of R. By our assumption that all polynomials with coefficients in R have a finite number of roots, we have that the size of $\mathrm{Ann}(a)$ is finite.

Let a nonzero element in $\mathrm{Ann}(a)$ be denoted by y. It follows that yR is finite because $yR \subseteq \mathrm{Ann}(a)$, and we have already shown that $\mathrm{Ann}(a)$ is finite. Consider the R-module homomorphism $\phi : R \to yR$ given by $\phi(r) = yr$. Because yR is finite and R is infinite, it follows that there is an element yr in yR that has infinitely many elements of R mapping to it. Denote the set of elements in R mapping to yr by M. If M is countably infinite, then denote the elements in M by $\{r_1, r_2, r_3, \ldots\}$. Otherwise, we can choose a countably infinite subset of M, and denote the elements in this subset by $\{r_1, r_2, r_3, \ldots\}$. This follows directly from the axiom of choice.

Thus, for all $n \geq 2$, we have that $yr_1 = yr_n$, and so $y(r_1 - r_n) = 0$. But because all the elements in $\{r_1, r_2, r_3, \ldots\}$ are distinct, it follows that all the elements in $\{r_1 - r_n\}_{n=2}^{\infty}$ are also distinct, so there are an infinite number of roots to the equation $yx = 0$. But since $yx \in R[x]$, it is supposed to have a finite number of roots, a contradiction.

Thus, infinite rings which have zero divisors do not satisfy the condition that all polynomials in the ring have a finite number of roots.

We now show that if a ring has no zero divisors, then all polynomials over the ring have a finite number of roots. Suppose that R has no zero divisors, and suppose $F(x)$ is a polynomial in the ring $R[x]$. Note that the set $K = \{\frac{a}{b} \mid a, b \in R, b \neq 0\}$ is a field. $F(x)$ is an element of $R[x]$, which is contained in $K[x]$. Since every polynomial over a field has a finite number of roots, it follows that $F(x)$ has a finite number of roots over $R[x]$, as desired. □

We now present a result that allows us to limit the number of roots a polynomial could have over a commutative ring that can be represented as a ring product. In contrast to the previous theorem, this result allows us to restrict the possible number of roots of a polynomial, not just determine whether this number is finite or infinite.

Consider a finite commutative ring R with identity which can be written as $R \cong R_1 \times R_2 \times \cdots \times R_k$. Thus, each element $x \in R$ can be represented as some tuple $(x_1, x_2, \ldots, x_k)$ where each x_i is an element of R_i. Let us also call $n = |R|$ and $n_1 = |R_1|, n_2 = |R_2|, \ldots, n_k = |R_k|$. Take any polynomial $F : R \to R$. Equivalently, we can view F as a set of k polynomials $F_1, F_2, \ldots, F_k$ over $R_1, R_2, \ldots R_k$, respectively, as described by Lemma 4. Note that if an element x is a root of F, that is $F(x) = 0$, it must be a root of $F_1, F_2, \ldots, F_k$ in each of $R_1, R_2, \ldots R_k$. However, rather than counting roots, we count elements that are not roots. Let us define $0 \leq a_i$ to be the number of elements that are not roots of F_i in each of the rings R_i. To find the number of non-roots of F over R, we must find the number of tuples $(F_1(x_1), F_2(x_2), \ldots, F_k(x_k))$ where not all elements are 0.

We can use the principle of inclusion-exclusion to calculate this number. Each set of a_i non-roots over R_i contributes $(n/n_i) \cdot a_i$ tuples that are non-zero. However, all tuples where two entries are non-zero are double counted so we must subtract $(n/(n_i n_j)) \cdot (a_i a_j)$ for every pair of i, j. Now all tuples that contain three non-zero entries have been added three times and subtracted three times so they must be added back. Continuing in this way we find that the number of non-roots of F over R is

$$\sum_{i=1}^{k} \sum_{j_1 < j_2 < \ldots < j_i \leq k} (-1)^{k+1} \cdot \frac{n a_{j_1} a_{j_2} \ldots a_{j_i}}{n_{j_1} n_{j_2} \ldots n_{j_i}}.$$

Thus, we can conclude that if a number cannot be represented in this way for any set of $a_1, a_2, \ldots, a_k$, a polynomial cannot have that number of non-roots. The converse is not necessarily true since it is not necessarily true that any value of a_i is possible over the ring R_i. Note that since we know $|R|$, if we know a polynomial can't have q non-roots over R, it directly follows that a polynomial cannot have $|R| - q$ roots.

In the case of the squarefree integers, however, any function is possible over a field such as $\mathbb{Z}_p$ for prime p, so all a_i's are possible and the converse of the above statement holds.

For example, consider $\mathbb{Z}_6 = \mathbb{Z}_3 \times \mathbb{Z}_2$. In this case every polynomial must have $2a_1 + 3a_2 - a_1 a_2$ non-roots for some integers $0 \leq a_1 \leq 3$ and $0 \leq a_2 \leq 2$. Thus, one may easily verify that a polynomial over $\mathbb{Z}_6$ cannot have exactly 1 non-root but can have 0, 2, 3, 4, 5, or 6 non-roots. By complimentary counting, we can conclude that a polynomial over $\mathbb{Z}_6$ can have 0, 1, 2, 3, 4, or 6 roots but cannot have 5 roots.

10 Acknowledgements

We would like to thank our research advisor, Prof. James Barker Coykendall, for mentoring us throughout this research process. We would also like to thank Dr. Felix Gotti and Dr. Tanya Khovanova for reviewing the paper and providing many helpful comments for revision. Finally, we would like to express our gratitude to Dr. Pavel Etingof, Dr. Slava Gerovitch, and the MIT PRIMES program for making this project possible.

References

[1] Malik Tusif Ahmed, Tiberiu Dumitrescu, and M Azeem Khadam. Commutative rings with absorbing factorization. *Communications in Algebra*, 48(12):5067–5075, 2020.

[2] G. Bini and F. Flamini. *Finite commutative rings and their applications*, volume 680. Springer Science & Business Media, 2002.

[3] Drike, MooS, and Dan. For which rings does a polynomial in r have finitely many roots? *Mathematics Stack Exchange*, Feb 2016.

[4] A. Eskandarian. Counting polynomial functions over rings. *College of William and Mary*, May 2015.

[5] R. Gilmer. The ideal of polynomials vanishing on a commutative ring. *Proceedings of the American Mathematical Society*, 127(5):1265–1267, 1999.

[6] G.-M. Greuel, F. Seelisch, and O. Wienand. The gröbner basis of the ideal of vanishing polynomials. *Journal of Symbolic Computation*, 46(5):561–570, 2011. Groebner Bases and Applications.

[7] A. Guha and A. Dukkipati. A faster algorithm for testing polynomial representability of functions over finite integer rings. *Theoretical Computer Science*, 579:88–99, 2015.

[8] D.J. Newman. *A Problem Seminar*. Springer New York, 1982.

[9] I.M. Niven and L.J. Warren. A generalization of fermat's theorem. 1957.

[10] D. Singmaster. On polynomial functions (mod m). *Journal of Number Theory*, 6(5):345–352, 1974.

[11] E. Specker, N. Hungerbühler, and M. Wasem. Polyfunctions over general rings. *arXiv preprint arXiv:2111.14573*, 2021.

[12] E. Specker, N. Hungerbühler, and M. Wasem. The ring of polyfunctions over $\mathbb{Z}/n\mathbb{Z}$. 2021.