5-2022

Strict Prime-Intersective Polynomials for a Fixed Prime Number

Rob Rexler Baello

Abstract

In this thesis, we examine intersective polynomials, which are polynomials with integer coefficients that have a root modulo any positive integer greater than 1. For any prime number p, a p-intersective polynomial is a polynomial with integer coefficients which has a root in $\mathbb{Z}_p$. We define a special type of p-intersective polynomial called *strict p-intersective polynomial* that can be factored as the product of a p-intersective polynomial and an irreducible polynomial mod p. The main results include methods of construction of strict p-intersective polynomials for certain prime numbers p and enumeration of such polynomials of certain degrees.

Chapter 1 gives the history and background of intersective polyomials. In Chapter 2, we explore irreducible polynomials over the field $\mathbb{Z}_p$, where p is prime. Those p-intersective polynomials of degree ≤ 5 for $p = 2,\ 3$ and 5 are investigated. In chapter 3, we analyze strict p-intersective polynomials with focus on counting the number of polynomials over $\mathbb{Z}_p$ that are strict p-intersective. The chapter ends with constructing and enumerating p-intersective polynomials with degrees 3,4, and 5. Lastly, we construct some special p-intersective and intersective polynomials in chapter 4.

Keywords: Intersective polynomial, p-intersective polynomial, Strict p-intersective polynomial, Irreducible polynomial.

MONTCLAIR STATE UNIVERSITY

Strict Prime-Intersective Polynomials For a Fixed Prime Number

by

Rob Rexler Baello

A Master's Thesis Submitted to the Faculty of

Montclair State University

In Partial Fulfillment of the Requirements

For the Degree of

Master of Science

May 2022

College of Science and Mathematics

Department of Mathematics

Thesis Committee:

[redacted]

Dr. Aihua Li

[redacted]

Committee Member

[redacted]

Dr. Jonathan Cutler
Committee Member

STRICT PRIME-INTERSECTIVE POLYNOMIALS FOR A FIXED PRIME NUMBER

A THESIS

Submitted in partial fulfillment of the requirements
for the degree of Master of Science

by

Rob Rexler Baello

Montclair State University

Montclair, NJ

2022

Acknowledgments

I would like to express my sincere gratitude to my advisor and thesis sponsor, Dr. Aihua Li, who has been my mentor since I was an undergraduate. She has provided me with invaluable knowledge and opened up plenty of opportunities for me to grow not only as a mathematician, but also as a teacher. I would also like to thank my committee members, Dr. Jonathan Cutler and Dr. Mark Korlie, for their support in writing the paper. Lastly, I would like to thank my family and friends for their unwavering support and guidance throughout my education.

Contents

List of Tables

Chapter 1

Introduction

Finding roots of a polynomial has massive applications in mathematics, science, and statistics. Often times finding roots of a polynomial helps determine when a function reaches zero, which may take many different forms and may be from various real applications. Another related problem is to figure out at what point(s) a polynomial reaches its maximum or minimum value. In Number Theory, a classical and popular problem is solving Diophantine equations. It is to search for integer solutions to a polynomial equation with integer coefficients. Equivalently, it is to search the roots of a polynomial with integer coefficients. The set $\mathbb{Z}[x]$ of all polynomials with integer coefficients forms an integral domain. If n is a positive integer greater than 1, the set of all integers modulo n is a ring, with the usual integer multiplication and addition, denoted $\mathbb{Z}_n$. An intersective polynomial $f(x)$ is a polynomial in $\mathbb{Z}[x]$ such that $f(x)$ has at least one root in $\mathbb{Z}_n$ for all positive integer $n > 1$. This research focuses on those intersective polynomials which favor prime numbers. We are particularly interested in a special type of p-intersective polynomial, where p is prime, that can be factored as the product of a p-intersective polynomial and an irreducible polynomial over $\mathbb{Z}_p$. Such a polynomial is called a strict p-intersective polynomial.

1.1 Useful Definitions

The irreducibility of a polynomial over a ring plays an important role in the study of polynomials. In this research, we focus on the ring of integers modulo a prime number p.

Definition 1. *Let R be a ring and $g(x)$ be a polynomial of degree $n > 1$ in $R[x]$. It is said to be reducible over R if $g(x)$ can be factored as $g(x) = f_1(x)f_2(x)$, where $f_i(x) \in R[x]$ and $0 < \deg(f_i(x)) < n$ for each $i = 1, 2$. A polynomial which is not reducible over R is called an irreducible polynomial over R.*

We denote the ring of integers by $\mathbb{Z}$ and for a positive integer $n > 1$, the ring of integers modulo n by $\mathbb{Z}_n$. The polynomial ring $\mathbb{Z}[x]$ is the set of all polynomials with integer coefficients equipped with the usual polynomial addition and multiplication. Similarly, $\mathbb{Z}_n[x]$ denotes the ring of polynomials with coefficients in $\mathbb{Z}_n$. Next, we introduce the concepts of intersective polynomials and m-intersective polynomials, where $m \in \mathbb{Z}$.

Definition 2. *A polynomial $f(x) \in \mathbb{Z}[x]$ is said to be intersective if for every positive integer $n > 1$, there exists an integer a such that $f(a) \equiv 0 \pmod{n}$. Let m be a positive integer at least 2. A polynomial $f(x) \in \mathbb{Z}[x]$ is called an m-intersective* *polynomial if for every positive integer k, there exists an integer a such that $f(a) \equiv 0 \pmod{m^k}$.*

In other words, an intersective polynomial is a polynomial in $\mathbb{Z}[x]$ that has a root in the ring $\mathbb{Z}_n$ for every positive integer $n > 1$. For a fixed integer $m > 1$, some polynomials with integer coefficients may have roots modulo all positive integer powers of m. They are called m-intersective polynomials.

Definition 3. *Let $\mathbf{P}$ be the set of all prime numbers and $S \subseteq \mathbf{P}$. A polynomial $f(x) \in \mathbb{Z}[x]$ is said to be S-intersective if for each $s \in S$, there is an integer solution to the equation $f(x) \equiv 0 \pmod{s^k}$ for all positive integers k. If the set $S = \{p\}$ is a singleton, then S-intersective means p-intersective. We denote by $N_d(p)$ the number of p-intersective polynomials in the polynomial ring $\mathbb{Z}_p[x]$.*

Of course, intersective polynomials are also m-intersective polynomials for every integer $m > 1$. A simple example of intersective polynomial is the linear polynomial $x - a$ with $a \in \mathbb{Z}$. Modulo every integer $n > 1$, a is a root of $x - a$. In general, if a polynomial in $\mathbb{Z}[x]$ has $x - a$ as a factor, it is also intersective. Assume $f(x) \in \mathbb{Z}[x]$ and $\deg(f(x)) > 1$. If a is a root of $f(x)$ in $\mathbb{Z}$ and $f(x) \equiv \overline{f}(x) \pmod{n}$, then a is a root of $\overline{f}(x)$ in $\mathbb{Z}_n$. With regard to polynomials in $\mathbb{Z}[x]$, some are called trivially intersective and some are called nearly intersective.

Definition 4. *A polynomial $g(x) \in \mathbb{Z}[x]$ is called trivially intersective if it has an integer root (so a root in $\mathbb{Z}_n$ for all n) and it is called nearly intersective if it has a rational root.*

In this research, we need to apply properties of quadratic residues modulo a positive integer $n \geq 2$. Special focus is on n being a prime number.

Definition 5. *An integer q is said to be a quadratic residue modulo n if there exists an $x \in \mathbb{Z}$ such that $x^2 \equiv q \pmod{n}$.*

For any odd prime p, the Legendre symbol is defined to characterize quadratic residues mod p.

Definition 6. [11] *Let $a \in \mathbb{Z}$ and p be an odd prime. The Legendre symbol $\left(\frac{a}{p}\right)$ is defined by*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \textit{if } p \nmid a \textit{ and } a \textit{ is a quadratic residue mod } p; \\ -1 & \textit{if } p \nmid a \textit{ and } a \textit{ is not a quadratic residue mod } p; \\ 0 & \textit{if } p \mid a. \end{cases}$$

Furthermore, the following properties of the Legendre symbol are useful in determining if an integer is a quadratic residue or not.

Theorem 1. [11] *Let p be an odd prime and $a, b \in \mathbb{Z}$.*

1. *If $a \equiv b \pmod{p}$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$;*

2. *$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$;*

3. *$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \textit{if } p \equiv 1 \pmod{4} \\ -1 & \textit{if } p \equiv 3 \pmod{4} \end{cases}$;*

4. $\left(\frac{2}{p}\right) = \begin{cases} 1 & \textit{if } p \equiv 1 \textit{ or } 7 \pmod 8 \\ -1 & \textit{if } p \equiv 3 \textit{ or } 5 \pmod 8 \end{cases}$;

5. $\left(\frac{3}{p}\right) = \begin{cases} 1 & \textit{if } p \equiv 1 \textit{ or } 11 \pmod{12} \\ -1 & \textit{if } p \equiv 5 \textit{ or } 7 \pmod{12} \end{cases}$;

6. $\left(\frac{p}{q}\right) = \begin{cases} -\left(\frac{q}{p}\right) & \textit{if } p \equiv 1 \pmod 4 \quad \textit{or} \quad q \equiv 1 \pmod 4 \\ \left(\frac{q}{p}\right) & \textit{if } p \equiv 3 \equiv q \pmod 4 \end{cases}$.

A generalization of the Legendre symbol for non-prime moduli, called the Jacobi symbol, is defined.

Definition 7. *Assume n is an odd positive integer and its primary factorization is $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, where $p_1, p_2, \ldots, p_k$ are distinct primes. For any integer a, the Jacobi symbol $\left(\frac{a}{n}\right)$ is defined as follows:*

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{e_1} \left(\frac{a}{p_2}\right)^{e_2} \cdots \left(\frac{a}{p_k}\right)^{e_k}.$$

For an odd prime p, both the Legendre and Jacobi symbols help in determining whether an integer is a quadratic residue modulo p. In[10], cubic residue is defined and properties are explained.

Definition 8. *An integer $q \neq 0$ is said to be a cubic residue modulo a prime number*

p if there exists $a \in \mathbb{Z}$ such that $a^3 \equiv q \pmod{p}$.

$$\left(\frac{p}{q}\right)_3 = \begin{cases} 1 & \textit{if } p \textit{ is a cubic residue modulo } q \\ -1 & \textit{if } p \textit{ is not cubic residue modulo } q \end{cases}$$

Theorem 2. [10] *If $p \equiv 2 \pmod{3}$, then every integer is a cubic residue modulo p.*

Lastly, the famous möbius function is useful to help determining the number of irreducible polynomials.

Definition 9. *For any positive integer n, the möbius function, $\mu(n)$, is the sum of all the primitive nth roots of unity.*

The function $\mu(n)$ has values in $\{1, 0, 1\}$ depending on the factorization of n into prime factors: $\mu(n) = 1$ if n is a square-free positive integer with an even number of prime factors; $\mu(n) = -1$ if n is a square-free positive integer with an odd number of prime factors; $\mu(n) = 0$ if n has a squared prime factor. Also, $\mu(n)$ is multiplicative meaning $\mu(ab) = \mu(a)\mu(b)$ if a, b are relatively prime integers.

From this definition, $\mu(1) = 1$ because 1 has no prime divisors and it is square-free. If p is a prime number, $\mu(p) = -1$ because p has 1 prime divisor (itself) and is square-free. If k is a positive integer, $\mu(p^k) = (-1)^k$. in particular, the values of the möbius function is given by

Lemma 1. *Let n be a positive integer.*

$$\mu(n) = \begin{cases} 1 & \textit{if } n \textit{ is square-free with an even number of prime factors} ; \\ -1 & \textit{if } n \textit{ is square-free with an odd number of prime factors}; \\ 0 & \textit{if } n \textit{ has a squared prime factor.} \end{cases}$$

Next, we define a special kind of p-intersective polynomials.

Definition 10. *Consider a prime p. Let $f(x)$ and $g(x)$ be polynomials in $\mathbb{Z}_p$. We say that $f(x)$ is an associate of $g(x)$ if $f(x) = cg(x)$ for some $c \in \mathbb{Z}_p$.*

Definition 11. *Let p be a prime number and $f(x) \in \mathbb{Z}_p[x]$ with $\deg(f) = d \geq 3$. We say that $f(x)$ is strict p-intersective if it can be factored as $f(x) = g(x)h(x)$ where $g(x), h(x) \in \mathbb{Z}_p[x]$, $g(x)$ is p-intersective (treated as a polynomial in $\mathbb{Z}[x]$ and $h(x)$ is irreducible over $\mathbb{Z}_p$ with $\deg(h) \geq 2$. Denote the number of monic strict p-intersective polynomials of degree d mod p by $\nu_d(p)$.*

1.2 Existing Results

An example of non-trivial intersective polynomial is given in[2] which is proved by applying Galois Group Theory.

Proposition 1. [2] *The polynomial $f(x) = (x^3 - 19)(x^2 + x + 1)$ is an intersective polynomial.*

In this research, we first focus on classifying p-intersective polynomials and finding properties of such polynomials, where p is a prime number. Some theorems given in[1] are useful in identifying p-intersective polynomials.

Theorem 3. [1] *Let p be a prime number and $f(x) \in \mathbb{Z}[x]$.*

1. *If there exists $a \in \mathbb{Z}$ such that $p \mid f(a)$ but $p \nmid f'(a)$, then $f(x)$ is p-intersective.*

2. *Let $r \in \mathbb{Z}$ such that $p \nmid r$. Pick $m \in \mathbb{N} \cup \{0\}$ and let $f(x) = x^p - rp^m$. Then $f(x)$ is p-intersective if and only if $p \mid m$ and there exists $a \in \mathbb{Z}$ such that $a^p - r \equiv 0 \pmod{p^2}$.*

From Theorem 3(1), it is equivalent to say that for any prime p, if $f(a) = 0$ but $f'(a) \neq 0$ in $\mathbb{Z}_p$, then $f(x)$ is p-intersective. By the above theorem, we can easily find a 7-intersective polynomial.

Example 1. *Let $f(x) = x^2 + x + 1$. We have that $7 \mid f(2) = 7$ and $7 \nmid f'(2) = 5$. Thus $f(x)$ is 7-intersective.*

Note that $f(x) = x^2 + x + 1$ has no root modulo 2 because $f(0) = 1 \neq 0$ and $f(1) = 1 \neq 0$. Thus $f(x)$ is not 2-intersective and furthermore not intersective.

The results below shows the connection between p-intersective and regular intersective polynomials.

Proposition 2. *Let $\mathcal{P}$ be a set of prime numbers and $f(x)$ be $\mathcal{P}$-intersective. Then for any positive odd integer $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, where $p_1, \ldots, p_k \in P$ and $e_1, e_2, \cdots e_k$ are natural numbers, $f(x)$ has a root in $\mathbb{Z}_n$.*

Proposition 3. *Let $f(x)$ and $g(x)$ be polynomials in $\mathbb{Z}[x]$. Let $\mathcal{P}$ and $\mathcal{Q}$ be sets of prime numbers. If $f(x)$ is $\mathcal{P}$-intersective and $g(x)$ is $\mathcal{Q}$-intersective, then $f(x)g(x)$ is $(\mathcal{P} \cup \mathcal{Q})$-intersective.*

Recall that $\mathbf{P}$ is the set of all prime numbers.

Corollary 1. *Let $f(x)$ be in $\mathbb{Z}[x]$. If $f(x)$ is $\mathbf{P}$-intersective, then $f(x)$ is intersective.*

It is clear that an intersective polynomial is a p-intersective polynomial for every prime p. Thus we first focus on the construction of p-intersective polynomials for certain prime numbers p. The following result refers to the irreducibility of polynomials over $\mathbb{Z}_p$.

Theorem 4. *(Gauss' Formula) Let p be prime and $n > 1$ be a positive integer. The number $\eta_n(p)$ of all monic irreducible polynomials of degree n over the finite field $\mathbb{Z}_p$ of order p is given by*[12]

$$\eta_n(p) = \frac{1}{n}\sum_{d|n} \mu(n/d)p^{n/d},$$

where the $\mu(n)$ is the möbius function given in Definition 9.

If the degree of the irreducible polynomials in consideration is prime, the above formula can be simplified.

Corollary 2. *The number of monic irreducible polynomials of degree q, where q is prime, over the finite field $\mathbb{Z}_p$, is $\eta_q(p) = \frac{p^q - p}{q}$.*

Proof. Using the formula in Theorem 4, we calculate $\eta_q(p)$, where q is a prime number. The only positive divisors of q are 1 and q. By Lemma 1, $\eta_q(p) = \mu(q) = -1$ and $\mu(q/q) = \mu(1) = 1$. Thus,

$$\eta_q(p) = \frac{1}{q}\sum_{d|q} \mu(q/d)p^d = \frac{1}{q}\left(\mu(q)p + \mu(1)p^q\right) = \frac{p^q - p}{q}.$$

■

Lemma 2. [14] *Let p be any prime number and d be a positive integer. Then the number of monic irreducible polynomials for any degree d is bounded below by this formula:*

$$\eta_d(p) > \frac{p^d}{2d}.$$

The following result is a consequence of the famous Hensel's Lemma[9] and it is useful for determining whether a polynomial is p-intersective. We state it and give a simple proof.

Theorem 5. *Let p be an odd prime number and $a \in \mathbb{Z}_p$ with $p \nmid a$. Assume k is a positive integer. Then a is a quadratic residue mod p^k if and only if it is a quadratic residue mod p^{k+1}. Consequently, a is a quadratic residue mod p if and only if a is a quadratic residue mod p^k for all $k \in \mathbb{N}$.*

Proof. It is obvious that if a is a quadratic residue mod p^{k+1}, then a is a quadratic residue mod p^k.

Next we assume a is a quadratic residue mod p^k. Then $a = b^2 + mp^k$ for some $b, m \in \mathbb{Z}$ with $p \nmid b$. Since p is odd, we have $\mathrm{GCD}(2b, p) = 1$ and so the congruence equation $2bx - m \equiv 0 \pmod{p}$ has a solution in $\mathbb{Z}$. Let $c \in \mathbb{Z}$ satisfying $2bc - m \equiv 0 \pmod{p}$. Then $2bc = m + pn$ for some integer n and

$$\begin{aligned} (b + cp^k)^2 &= b^2 + 2bcp^k + c^2p^{2k} = (a - mp^k) + (m + pn)p^k + c^2p^{2k} \\ &= a + (n + c^2p^{k-1})p^{k+1} \Longrightarrow a \equiv (b + cp^k)^2 \pmod{p^{k+1}}. \end{aligned}$$

Thus, a is a quadratic residue mod p^{k+1}. The rest is straightforward. ■

1.3 Research Questions and Goals

Using to the definition of n-intersective, we will be focusing on the situation where n is prime. Let p be a prime number and $f(x) \in \mathbb{Z}[x]$. Since $f(x) \equiv \overline{f(x)} \pmod{p}$, for some $\overline{f(x)} \in \mathbb{Z}_p[x]$. If we identify $\overline{f(x)}$ as a polynomial with integer coefficients from 1 to $p-1$, it is also a p-intersective polynomial. Thus, from now on we concentrate on polynomials in $\mathbb{Z}_p[x]$. The following questions and/or goals are set for this research.

1. Identify or classify p-intersective polynomials in $\mathbb{Z}_p[x]$. In particular, for certain given prime p, develop methods of finding a set of p-intersective polynomials or strict p-intersective polynomials in $\mathbb{Z}_p[x]$.

2. At least how many (strict) p-intersective polynomials are there in $\mathbb{Z}_p[x]$?

3. Let p be a prime number. In the ring $\mathbb{Z}_p[x]$ and a given degree $d > 0$, how many p-intersective polynomials of degree d are there? In particular, how many quadratic or cubic p-intersective polynomials are there?

4. Find structural properties for strict p-intersective polynomials for certain prime numbers p.

5. Let p be a prime number. In the ring $\mathbb{Z}_p[x]$ and a given degree $d > 0$, how many strict p-intersective polynomials of degree d are there?

6. Construct intersective polynomials of certain degree.

1.4 Summary of Main Results

Chapter 1 gives the history and background of intersective polynomials. In Chapter 2, we explore irreducible polynomials over the field $\mathbb{Z}_p$, where p is prime. Furthermore, p-intersective polynomials in $\mathbb{Z}_p[x]$ of degree ≤ 5 for $p = 2, 3$ and 5 are investigated. In Chapter 3, we analyze strict p-intersective polynomials with focus on counting the number of polynomials that are strict p-intersective. The chapter ends with constructing and enumerating p-intersective polynomials with degrees 3, 4, and 5. Lastly, we construct some special p-intersective and intersective polynomials in Chapter 4.

Chapter 2

Preliminary Results and Examples

In this chapter, we state the basic properties of irreducible and reducible polynomials. We start with irreducible polynomials and explore the basic properties of quadratic and cubic irreducible polynomials and p-intersective polynomials. Consider a prime number p. It is well known that for any non-constant polynomial $f(x)$ of degree 1, 2, or 3, it is irreducible over $\mathbb{Z}_p$ if and only if $f(x)$ has a root in $\mathbb{Z}_p$.

2.1 Irreducible Polynomials Over $\mathbb{Z}_p$

Consider the finite field $\mathbb{Z}_p$, where p is prime. We first discuss irreducible polynomials of low degrees.

Example 2. *The polynomial $f(x) = x^2 + x + 1$ is irreducible over $\mathbb{Z}_2$ because it has no root in $\mathbb{Z}_2$. Consequently, it is not 2-intersective.*

We focus on monic irreducible polynomials and count the number of monic irreducible polynomials of degree $d > 0$ over $\mathbb{Z}_p$, where p is any prime. Obviously, there are p non-constant linear monic polynomials over $\mathbb{Z}_p$, which are irreducible. There is exactly one quadratic irreducible polynomial, $x^2 + x + 1$, in $\mathbb{Z}_2[x]$ and there are 2 monic quadratic irreducible polynomials over $\mathbb{Z}_3$. In[12], a formula is given to help calculating the number of monic irreducible polynomials of degree n by applying the famous Möbius function $\mu(n)$.

In the table below we give the numbers of irreducible polynomials of degrees 2 to 7 modulo prime numbers 2, 3, 5.

Table 2.1: Number of monic irreducible polynomials with small degrees

$p\backslash d$	2	3	4	5	6	7
$p = 2$	1	2	3	6	9	18
$p = 3$	3	8	18	48	116	312
$p = 5$	10	40	150	624	2580	11,160

In[13], irreducible polynomials of low degrees with the first 4 prime moduli are presented. Here we list the irreducible polynomials of degree 2, 3, 4 for $p = 2$.

Example 3. *Consider the field $\mathbb{Z}_2$. Over $\mathbb{Z}_2$,*[13]

1. *The only quadratic irreducible polynomial is $x^2 + x + 1$.*

2. *There are exactly 2 cubic irreducible polynomials: $x^3 + x + 1$ and $x^3 + x^2 + 1$;*

3. *There are exactly 3 irreducible polynomials of degree 4:*

$$x^4 + 1, \quad x^4 + x^2 + 1, \quad x^4 + x + 1.$$

For any prime p, Irreducible polynomials of degree 1, 2, or 3 in $\mathbb{Z}_p[x]$ can be similarly determined by checking the existence of a root in the field $\mathbb{Z}_p$. It helps to identify p-intersective polynomials. Since all non-constant linear polynomials are automatically p-intersective, we start with investigating quadratic p-intersective polynomials.

2.2 Quadratic p-Intersective Polynomials

When dealing with Quadratic polynomials, the famous quadratic formula is a useful tool.

Lemma 3. *Let p be a prime number and $a \in \mathbb{Z}$ with $\gcd(a, p) = 1$. Let $f(x) = (ax + b)g(x) \in \mathbb{Z}[x]$, where $g(x) \in \mathbb{Z}[x]$. Then $f(x)$ is p-intersective.*

Proof. For any positive integer k, $\gcd(a, p) = 1 \Longrightarrow \gcd(a, p^k) = 1$ as well. Thus, $a \not\equiv 0 \pmod{p^k}$ and so $a^{-1}b$ is a root of $f(x)$ in $\mathbb{Z}_{p^k}$. Thus $f(x)$ is p-intersective. ■

Next we give a criteria for a quadratic polynomial to be a p-intersective polynomial.

Lemma 4. *Let p be an odd prime number and $a \in \mathbb{Z}$ with $\gcd(a, p) = 1$. A quadratic polynomial $f(x) = ax^2 + bx + c \in \mathbb{Z}[x]$ is p-intersective if and only if $b^2 - 4ac$ is a quadratic residue modulo p.*

Proof. Let $k \in \mathbb{N}$. By the quadratic formula, any root of $f(x)$ in the ring $\mathbb{Z}_{p^k}$ must have the form of $(2a)^{-1}(-b \pm r)$, where $r^2 = b^2 - 4ac$ is a quadratic residue mod p^k. By Theorem 5, it is if and only if $b^2 - 4ac$ is a quadratic residue modulo p. Thus, $f(x)$ is p-intersective if and only if $b^2 - 4ac$ is a quadratic residue mod p. ■

Now we focus on monic polynomials over the ring $\mathbb{Z}_{p^k}$, where p is prime and $k \in \mathbb{N}$.

Corollary 3. *Let p be an odd prime and $f(x) = x^2 + c \in \mathbb{Z}_p[x]$ with $c \in \mathbb{Z}_p$. Then*

1. *$f(x)$ is p-intersective if and only if $-c$ is a quadratic residue mod p.*

2. *If c is a quadratic residue mod p, then $f(x)$ is p-intersective polynomial if and only if $p \equiv 1 \pmod 4$.*

Proof. (1) is obvious. For (2), by Lemma 4 and Theorem 5, $f(x)$ is p-intersectve iff $-4c$ is a quadratic residue modulo p iff -1 is a quadratic residue modulo p iff $p \equiv 1 \pmod 4$. ■

2.3 Classification of 2- or 3-Intersective Polynomials

In this section, we examine 2-intersective polynomials and 3-intersective polynomials in $\mathbb{Z}_p[x]$ of lower degrees. We focus on monic polynomials only.

Example 4. *Consider the prime number 2. There are eleven monic 2-intersective polynomials in $\mathbb{Z}_2[x]$ with degree at most 3 over $\mathbb{Z}_2$. Among them, 2 are linear, 3 are quadratic, and 6 are cubic. They are listed below:*

1. *Linear:*

x	$x+1$

;

2. *Quadratic:*

x^2	$x(x+1)$	$(x+1)^2$

;

3. *Cubic:*

x^3	$x^2(x+1)$	$x(x^2+x+1)$
$x(x+1)^2$	$(x+1)(x^2+x+1)$	$(x+1)^3$

.

Here, the quadratic polynomials are obtained from multiplying two the linear polynomials and the cubic polynomials are obtained by multiplying a linear polynomial with a quadratic polynomial. Since each linear polynomial has a root in $\mathbb{Z}_p$, then the product is also p-intersective. Constructively, we obtain the number of monic 3-intersective polynomials with degree less than or equal to 3.

Example 5. *Consider the prime number 3. There are exactly 3 monic linear 3-intersective polynomials, 6 monic quadratic 3-intersective polynomials, and 19 monic cubic 3-intersective polynomials. They are listed below:*

1. *Three linear:* $x, x+1, x+2$;

2. *Six quadratic:* $x^2,\ x(x+1);\ x(x-1),\ (x+1)^2,\ (x-1)^2,\ (x+1)(x-1);$

3. Nineteen cubic:

x^3	$x^2(x+1)$	$x^2(x+2)$
$x(x+1)^2$	$x(x+1)(x-1)$	$x(x-1)^2$
$(x+1)^3$	$(x+1)^2(x-1)$	$(x+1)(x-1)^2$
$(x-1)^3$	$x(x^2+1)$	$x(x^2+x+2)$
$x(x^2+2x+2)$	$(x+1)(x^2+1)$	$(x+1)(x^2+x+2)$
$(x+1)(x^2+2x+2)$	$(x-1)(x^2+1)$	$(x-1)(x^2+x+2)$
$(x-1)(x^2+2x+2)$		

Proposition 4. *There are exactly 150 monic 3-intersective polynomials of degree 5.*

Proof. We count the 3-intersective polynomials by different types summarized below. Let $f(x)$, $g(x)$, $h(x)$, and $l(x)$ be irreducible polynomials over $\mathbb{Z}_3$ with $\deg(f(x)) = \deg(g(x)) = 2$, $\deg(h(x)) = 3$ and $\deg(l(x)) = 4$. Any 3-intersective polynomial of degree 5 must be in one of the following forms:

- There are 54 polynomials of the form $(x-a)l(x)$.
- There are 9 polynomials that are in the form of $(x-a)f(x)g(x)$.
- There are 9 polynomials of the form $(x-a)f(x)^2$.
- There are 24 polynomials of the form $(x-a)(x-b)h(x)$ with $a \neq b$.
- There are 3 polynomials of the form $(x-a)(x-b)(x-c)f(x)$ with a, b, c being distinct.

- There are 18 polynomials of the form $(x-a)^2(x-b)f(x)$ $(a \neq b)$.
- There are 24 polynomials of the form $(x-a)^2h(x)$.
- There are 9 polynomials of the form $(x-a)^3f(x)$.

The above gives all the possible 3-intersective polynomials of degree 5. Adding all the numbers up yields 150. ■

2.4 Quadractic 5-Intersctive Polynomials

Example 6. *The following quadratic polynomials are 5-intersective with leading coefficient 1:*

x^2	x^2+1	x^2+4
x^2+x	x^2+x+3	x^2+x+4
x^2+2x	x^2+2x+1	x^2+2x+2
x^2+3x	x^2+3x+1	x^2+3x+2
x^2+4x	x^2+4x+4	x^2+4x+4

.

Multiplying each of these polynomials with an integer would still result in a 5-intersective polynomial. If the polynomial $f(x)$ has a root in $\mathbb{Z}_5$, then $af(x)$ also has a root in $\mathbb{Z}_5$. Each of the above multiplied by 2, 3, and 4 will give a different 5-intersective polynomial of degree 2 and all quadratic 5-intersected polynomial are among them. That is, there are exactly 60 quadratic 5-intersective.

Proposition 5. *There are exactly* 105 *monic polynomials with degree 3 or less that are* 5*-intersective. Among them, 5 are linear, 15 are quadratic, and 85 are cubic.*

Proof. We count the 5-intersective polynomials by degree 1, 2, and 3 respectively.

- Obviously, there 5 monic polynomials in the form of $x+b$, where $b \in \mathbb{Z}_5$. These are all the 5-intersective polynomials of degree 1.

- There are 10 monic quadratic polynomials in the form of $(x-a)(x-b)$, where $a \neq b$. There are 5 polynomials of the form $(x-a)^2$. The total is 15.

- Cubic monic 5-intersective polynomials are counted by: 5 in the the form $(x-a)^3$, 20 in the form of $(x-a)(x-b)^2$ with $a \neq b$, $\frac{(5)(4)(3)}{6} = 10$ in the form of $(x-a)(x-b)(x-c)$ with a, b, c being distinct in $\mathbb{Z}_5$, and $50 = 5(10)$ polynomials of the form $(x-a)g(x)$ where $g(x)$ is a monic quadratic irreducible polynomial. Note that By Table 2.1, there are 10 monic quadratic irreducible polynomials mod 5. Adding all of those forms will give us 85 monic 5-intersective polynomials.

■

Below we give a summary for the enumeration of monic p-intersective polynomials for $p = 2, 3, 5$ of degree up to 5. Most of the numbers are from the examples from the previous results shown in this section.

Table 2.2: Number of monic p-intersective polynomials with small degrees

$p\backslash d$	1	2	3	4	5
$p=2$	2	3	6	12	24
$p=3$	3	6	19	54	150
$p=5$	5	15	85	420	2077

.

Chapter 3

Strict p-Intersective Polynomials of a Given Degree

Definition 11 defines a special type of p-intersective polynomials, called strict p-intersective polynomials. In this chapter, we classify, construct, and enumerate such polynomials of various degrees. For any prime number p, a strict p-intersective polynomial is a polynomial that is the product of a p-intersective polynomial and an irreducible polynomial of degree at least 2 over $\mathbb{Z}_p$. Below is an example of a strict 2-intersective polynomial.

Example 7. *The polynomial $(x+1)^3(x^2+x+1)$ is a strict 2-intersective polynomial with degree 5, where $(x+1)^3$ is 2-intersective and (x^2+x+1) is irreducible over $\mathbb{Z}_2$.*

Obviously, for any prime p, strict p-intersective polynomials exist and every strict p-polynomial is also p-intersective. For example, for any prime number p, a strict cubic monic p-intersective polynomial can be constructed as follows:

Example 8. *Let p be any prime, $a, b \in \mathbb{Z}_p$, and b is a quadratic non-residue mod p. Then $f(x) = (x-a)(x^2-b)$ is a cubic p-intersective polynomial over $\mathbb{Z}_p$.*

Note that $f(x)$ has a root a in $\mathbb{Z}_p$ and $x^2 - b$ has no root in $\mathbb{Z}_p$, so it is irreducible in $\mathbb{Z}_p[x]$. Thus $f(x)$ is strict p-intersective and also p-intersective.

Below are some questions that we would like to answer for this chapter:

1. For a fixed prime number p, how many (or at least how many) strict p-intersective polynomials do we have?

2. How do we construct strict p-intersective polynomials?

3. How to we determine if a given p-intersective polynomial is strict p-intersective?

4. For a given positive integer $d \geq 3$, does strict p-intersective polynomials of degree d exist and if yes, how many?

First, we will be looking at strict 2-intersective polynomials.

3.1 Classification of Strict 2-Intersective Polynomials of degree ≤ 5

In this section, we classify strict p-polynomials of degrees 3, 4, and 5 for any prime number p. As before, we focus on monic polynomials.

Proposition 6. *The following is the number of monic strict 2-intersective polynomials with the given degree.*

1. *There are exactly 2 strict 2-intersective polynomials of degree 3;*

2. There are exactly 7 strict 2-intersective polynomials of degree 4;

3. There are exactly 18 strict 2-intersective polynomials of degree 5.

Proof. 1. Two strict 2-intersective polynomials of degree 3 use the only irreducible polynomial $x^2 + x + 1$ and a polynomial of degree 1:

$$x(x^2 + x + 1), \quad (x + 1)(x^2 + x + 1).$$

2. A strict 2-intersective polynomial of degree 4 must have a quadratic irreducible factor or a cubic irreducible factor. The other factor(s) must have at least one of the factors $x, x + 1$. There are seven possible combinations:

$$x^2(x^2 + x + 1), \quad x(x + 1)(x^2 + x + 1), \quad (x + 1)^2(x^2 + x + 1)$$
$$x(x^3 + x + 1), \quad x(x^3 + x^2 + 1), \quad (x + 1)(x^3 + x + 1), \quad (x + 1)(x^3 + x^2 + 1).$$

3. We count strict p-intersective polynomials of degree 5 over $\mathbb{Z}_2$ by going through all possible cases.

(1) It is the product of an irreducible polynomial of degree 4 and a polynomial of degree 1; By Table 2.1 and Example 3, there are 3 irreducible polynomials of degree 4: $x^4 + x^3 + x^2 + x + 1$, $x^4 + x^3 + 1$, $x^4 + x + 1$. The table build 6 strict 2-intersective polynomials of degree 5 shown below:

$$x(x^4 + x^3 + x^2 + x + 1), \quad (x + 1)(x^4 + x^3 + x^2 + x + 1), \quad x(x^4 + x^3 + 1)$$
$$(x + 1)(x^4 + x^3 + 1), \quad x(x^4 + x + 1), \quad (x + 1)(x^4 + x + 1)$$

(2) Product of an irreducible polynomial of degree 3 and a reducible polynomial of degree 2. There are only two irreducible polynomials of degree 3: x^3+x^2+1 and x^3+x+1. Here 6 strict 2-intersective polynomials are constructed.

- $x^2(x^3+x+1)$, $x^2(x^3+x^2+1)$
- $x(x+1)(x^3+x+1)$, $x(x+1)(x^3+x^2+1)$
- $(x+1)^2(x^3+x+1)$, $(x+1)^2(x^3+x^2+1)$

(3) The last case the product of a cubic 2-intersective polynomial with a quadratic irreducible polynomial x^2+x+1. This case includes the situation when $(x^2+x+1)^2$ is used.

- $x^3(x^2+x+1)$, $x^2(x+1)(x^2+x+1)$
- $x(x^2+x+1)^2$, $x(x+1)^2(x^2+x+1)$
- $(x+1)(x^2+x+1)^2$, $(x+1)^3(x^2+x+1)$

Taking all of these polynomials into account gives 18 strict 2-intersective polynomials of degree 5. ■

3.2 Classification of Strict 3-Intersective Polynomials of Degree ≤ 5

After classifying strict 2-intersective polynomials in the previous section, we investigate the situation for $p=3$. Similar as in the previous section, we examine strict 3-intersective polynomials of degree 3, 4, 5.

Proposition 7. *There are exactly* 9*, 42, and 150 monic strict* 3*-intersective polynomials of degree 3, 4, 5 respectively.*

Proof. 1. Any monic strict 3-intersective polynomial of degree 3 can only be in the form of $(x-a)f(x)$ where $a \in \mathbb{Z}_3$ and $f(x)$ is one of the 3 quadratic irreducible polynomial over $\mathbb{Z}_3$: x^2+1, x^2+x+2, and x^2+2x+2. It gives 9 monic strict 3-intersective polynomials of degree 3.

2. Monic strict 3-intersective polynomials of degree 4 can only be in two forms;

(1) The first form is $(x-a)f(x)$ where $f(x)$ is an irreducible polynomial of degree 3 and $a \in \mathbb{Z}_3$. There are 8 irreducible polynomials which can be $f(x)$ and 3 from $x-a$. Thus, there is a total of 24 in this form. Below is the list of this form. $(a = 0, 1, 2)$

$(x-a)(x^3+2x+1)$	$(x-a)(x^3+2x+2)$	x^3+x^2+2
$(x-a)(x^3+x^2+x+2)$	$(x-a)(x^2+x^2+2x+1)$	$(x-a)(x^2+2x^2+1)$
$(x-a)(x^3+2x^2+x+1)$	$(x-a)(x^3+2x^2+2x+2)$	

(2) The second form is $(x-a)(x-b)f(x)$ where $f(x)$ is one of the 3 quadratic irreducible polynomials, x^2+1, x^2+x+2, x^2+2x+2, and $a, b \in \mathbb{Z}_3$. There

are 18 such polynomials listed below.

$(x^2)(x^2+1)$	$(x^2)(x^2+x+2)$	$(x^2)(x^2+2x+2)$
$(x+1)^2(x^2+1)$	$(x+1)^2(x^2+x+2)$	$(x+1)^2(x^2+2x+2)$
$(x+2)^2(x^2+1)$	$(x+2)^2(x^2+x+2)$	$(x+2)^2(x^2+2x+2)$
$(x)(x+1)^2(x^2+1)$	$(x)(x+1)^2(x^2+x+2)$	$(x)(x+1)^2(x^2+2x+2)$
$(x+1)(x+2)(x^2+1)$	$(x+1)(x+2)(x^2+x+2)$	$(x+1)(x+2)(x^2+2x+2)$
$(x)(x+2)(x^2+1)$	$(x)(x+2)(x^2+x+2)$	$(x)(x+2)(x^2+2x+2)$

Adding both forms together gives 42 monic strict 3-intersective polynomials of degree 4.

3. There are 3 types of monic strict 3-intersective polynomial of degree 5.

   - 54 polynomials of the form $(x-a)f(x)$ with $\deg(f(x)) = 4$.
   - 48 polynomials of the form $(x-a)(x-b)f(x)$ with $\deg(f(x)) = 3$.
   - 48 polynomials of the form $(x-a)(x-b)(x-c)f(x)$ with $\deg(f(x)) = 2$.

   In the above, a, b, c are in $\mathbb{Z}_3$ and $f(x)$ is a monic irreducible polynomial over $\mathbb{Z}_3$. In total, there are exactly 150 monic strict 3-intersective polynomials of degree 5.

■

3.3 Enumeration of Certain Strict p-Intersective Polynomials

Enumeration of strict p-intersective polynomials for prime numbers greater than 3 of higher degree is more complicated. We next investigate degree 3 for any prime p.

Theorem 6. *For any prime p, there are exactly $\frac{p^2(p-1)}{2}$ many monic strict p-intersective polynomials of degree 3. That is, $\nu_3(p) = \frac{1}{2}p^2(p-1)$.*

Proof. Any strict p-intersective polynomial of degree 3 can only be in the form $(x-a)g(x)$ where $g(x)$ is an irreducible polynomial of degree 2. There are p polynomials of the form $(x-a)$ and $\eta_2(p) = \frac{p^2-p}{2}$ irreducible polynomials over $\mathbb{Z}_p$ (Corollary 2). Multiplying them together we obtain

$$\nu_3(p) = \frac{p^2(p-1)}{2},$$

the number of polynomials that are strict p-intersective polynomials of degree 3. ■

Similarly, we develop the formula for the strict p-intersective polynomials of degree 4.

Theorem 7. *For any prime p, the number of strict monic p-intersective polynomials of degree 4 is given by*

$$\nu_4(p) = \frac{7p^2(p^2-1)}{12} = \frac{7}{12}\left(p^4 - p^2\right).$$

Proof. Any monic strict p-intersective polynomials only has 2 forms: (1) $(x-a)g(x)$ where $a \in \mathbb{Z}_p$ and $g(x)$ is an irreducible polynomial of degree 3, and (2) $(x-a)(x-b)g(x)$ where $a, b \in \mathbb{Z}_p$ and $g(x)$ is an irreducible polynomial of degree 2. The number of monic strict p-intersective polynomials is the sum of the produced polynomials in both forms.

(1) Polynomials in the form of $(x-a)g(x)$. By Corollary 2, there are $\frac{p^3-p}{3}$ many such $g(x)$. Thus $\frac{p^4-p^2}{3}$ polynomials of this form can be produced.

(2) Polynomials in the form of $(x-a)(x-b)g(x)$. By Corollary 2 again, there are $\frac{1}{2}(p^2-p)$ many quadratic irreducible polynomials. There are p quadratic polynomials in the form of $(x-a)^2$ with $a \in \mathbb{Z}_p$. There are $p(p-1)/2$ many quadratic polynomials in the form of $(x-a)(x-b)$ with $a \neq b$ and $a, b \in \mathbb{Z}_p$. Altogether, the number of polynomials in the form of $(x-a)(x-b)g(x)$, where $g(x)$ is irreducible over $\mathbb{Z}_p$, is

$$p \cdot \frac{p^2-p}{2} + \frac{p(p-1)}{2} \cdot \frac{p(p-1)}{2} = \frac{p^2(p^2-1)}{4} = \frac{p^4-p^2}{4}.$$

Adding the number from case (1), we have

$$\nu_4(p) = \frac{p^4-p^2}{3} + \frac{(p^4-p^2)}{4} = \frac{7}{12}\left(p^4-p^2\right).$$

■

Lastly, we develop a formula for the number of (monic) strict p-intersective polynomials of degree 5.

Theorem 8. *For any prime number p, the number of monic strict p-intersective* *polynomials of degree 5 is given by*

$$\nu_5(p) = \frac{1}{24}\left(15p^5 + 2p^4 - 3p^3 - 14p^2\right).$$

Proof. We consider 4 cases. Below is the number of polynomials that are strict p-intersective with the given forms.

1. There are $(\frac{p^4-p^2}{4})p = \frac{p^3(p^2-1)}{4}$ polynomials of the form $(x-a)g(x)$ where $g(x)$ is an irreducible polynomial of degree 4 over $\mathbb{Z}_p$.

2. There are $(\frac{p(p-1)}{2}+p)(\frac{p^3-p}{3}) = \frac{p^2(p^2-1)(p+1)}{6}$ polynomials of the form $(x-a)(x-b)g(x)$ where $g(x)$ is an irreducible polynomial of degree 3 in $\mathbb{Z}_p[x]$.

3. The number of strict p-intersective polynomials of degree 5 in the form of $(x-a)(x-b)(x-c)g(x)$, where $g(x)$ is an quadratic irreducible polynomial over $\mathbb{Z}_p$, is given by

$$\left(\frac{p(p-1)(p-2)}{6} + p(p-1) + p\right) \cdot \frac{p^2-p}{2} = \frac{1}{12}(p^5 + 2p^4 - p^3 - 2p^2).$$

4. The number of strict p-intersective polynomials of degree 5 in the form of $(x-a)g(x)h(x)$, where $g(x)$ and $h(x)$ are quadratic irreducible polynomials over $\mathbb{Z}_p$, is given by

$$p\left[\frac{(\frac{p^2-p}{2})(\frac{p^2-p}{2}-1)}{2} + \frac{p^2-p}{2}\right] = \frac{1}{8}(p^5 - 2p^4 + 3p^3 - 2p^2).$$

The above four cases cover all the possible strict p-intersective polynomials of degree 5 over $\mathbb{Z}_p$. By adding all of the expressions from the the above and simplify the result, we obtain the exact number $\nu_5(p)$ of all strict p-intersective polynomials of degree 5:

$$\nu_5(p) = \frac{p^2(p-1)(15p^2+17p+14)}{24} = \frac{1}{24}(15p^5+2p^4-3p^3-14p^2).$$

■

Remark 1. *Note that $\nu_5(2) = 18$ and $\nu_5(3) = 150$ which confirms our earlier results for the number of strict 2-intersective or 3-intersective polynomials. Theorems 13, 7, 8 give formulas for $\nu_d(p)$ for any prime p and for $d = 3, 4, 5$. In sections 3.1 and 3.2, we provided the numbers $\nu_d(2)$ and $\nu_d(3)$ for $d = 3, 4, 5$. Those results confirm the formulas given in the above theorems. The following table shows the comparison.*

Table 3.1: Values of $\nu_d(2)$ and $\nu_d(3)$ for $d = 3, 4, 5$

	$p = 2$	$p = 3$
$d = 3$	$\frac{2^2(2-1)}{2} = 2$	$\frac{3^2(3-1)}{2} = 9$
$d = 4$	$\frac{7(2^4-2^2)}{12} = 7$	$\frac{7(3^4-3^2)}{12} = 42$
$d = 5$	$\frac{2^2(15(2)^3+2(2)^2-3(2)-14)}{24} = 18$	$\frac{3^2(15(3)^3+2(3)^2-3(3)-14)}{24} = 150$

Recall that $\eta_d(p)$ is the number of monic irreducible polynomials of degree d and $\nu_d(p)$ is the number of strict p-intersective polynomials mod p. Below we show that the $\nu_d(p)$ can be obtained by counting the number of p-intersective polynomials and irreducible polynomials of lower degrees.

Theorem 9. *Let p be prime and d be a positive integer at least 3. Then the number of strict p-intersective polynomials with degree d is given by*

$$\nu_d(p) = \sum_{k=2}^{d-1} N_{d-k}(p)\eta_k(p),$$

where $N_{d-k}(p)$ is the number of p-intersective polynomials over $\mathbb{Z}_p$ of degree k and $\eta_k(p)$ is the number of monic irreducible polynomials over $\mathbb{Z}_p$ of degree k.

Proof. For $2 \leq k \leq d-1$, choose any irreducible polynomial $f(x)$ of degree k and any p-intersective polynomial $g(x)$ of degree $d-k$. Then $f(x)g(x)$ is a strict p-intersective polynomial of degree d. Thus, the formula is true. ■

3.4 Strict p-Intersective Polynomials of Higher Degrees

In this section, we explore strict p-intersective polynomials for any prime number p for any degree d. As seen above, the calculation for the number of monic strict p-intersective polynomials gets more complex as the degree gets higher. Theorem 9 gives only a general formula for the counting but since there is no well-developed formulas for $\nu_d(p)$ in general, it is not easy to apply. We then approach to give a lower bound for the number $\nu_d(p)$.

Theorem 10. *Let p be any prime number. For a specific degree $d > 3$, the number of* *monic strict p-intersective polynomial of degree is bounded from below by the formula:*

$$\nu_d(p) > \frac{p^{d-2}}{12}\left[(10p^2+3p+2)d^2 - \left(45p^2+9p+10\right)d + \left(47p^2+6p+7\right)\right].$$

Proof. Just like in the previous sections, we will be looking at each form one by one and add them all together. We count the number of monic p-intersective polynomials in the forms of the product of an irreducible polynomial and exactly one linear factor, two linear factors, or three linear factors. Refer to Lemma 2, we have

1. There are more than $\frac{p^d}{2(d-1)}$ many monic strict p-intersective polynomials of the form $(x-a)g(x)$, where $g(x)$ is irreducible of degree $d-1$.

2. There are more than $\frac{p^{d-2}}{2(d-2)}$ monic irreducible polynomials of degree $d-2$. There are $p(p-1)/2+p$ many polynomials of the form $(x-a)(x-b)$. Thus there are in total $\frac{p^{d-1}(p+1)}{4d-8}$ many monic strict p-intersective polynomials of degree d in the form of $(x-a)(x-b)g(x)$ with $g(x)$ being irreducible.

3. Similarly, there are $\frac{p^{d-1}(p+1)(p+2)}{12(d-3)}$ monic strict p-intersective polynomials of the form $(x-a)(x-b)(x-c)f(x)$ where $\deg((f(x)) = d-3$.

Adding all of them together will obtain;

$$\nu_d(p) > \frac{p^d}{2(d-1)} + \frac{p^{d-1}(p+1)}{4(d-2)} + \frac{p^{d-2}(p+1)(p+2)}{12(d-3)}$$

$$= \frac{p^{d-2}}{12}\left[(10p^2+3p+2)d^2 + (-45p^2-9p-10)d + (47p^2+6p+7)\right].$$

■

To get a better estimation of the number of monic polynomials that are p-intersective, we would have to continue adding each forms, adding 1 linear factor and reducing the degree of the irreducible polynomial by 1 until we get to the form $(x-a_1)(x-a_2)...(x-a_{d-2})f(x)$ where $\deg(f(x)) = 2$.

Lemma 5. *Let p be any prime and r be a positive integer. Assume d is a positive integer with $d-r$ being a prime number. Then the number of strict monic p-intersective polynomials of degree d in the form of $f(x)g(x)$, where $f(x)$ is a p-intersective polynomial of degree r and $g(x)$ is an irreducible polynomial of degree $d-r$, is*

$$v_r(p)\eta_{d-r}(p) = v_r(p) \cdot \frac{p^{d-r}-p}{d-r}.$$

Proof. The proof is straightforward by Lemma 2. ■

Theorem 11. *The number of strict p-intersective polynomials of degree 6 can be calculated by the formula:*

$$\nu_6(p) = \frac{1}{60}\left(47p^6 - 20p^5 - 35p^4 + 20p^3 - 12p^2\right).$$

Proof. These are the numbers of each polynomials for each form with degree 6:

1. There are $\left(\frac{p^6-p^2}{5}\right)$ polynomials of the form $(x-a)g(x)$ where $g(x)$ is an irreducible polynomial of degree 5. Given that $N_5(p) = \frac{p^5-p}{5}$ and there are p elements for a in $\mathbb{Z}_p$.

2. There are $\frac{p(p+1)}{2}\left(\frac{p^4-p^2}{4}\right)$ of the form $(x-a)(x-b)g(x)$ where $g(x)$is an irreducible polynomial of degree 4. Given that $N_4(p) = \frac{p^4-p^2}{4}$ and $\frac{p(p+1)}{2}$ strict p-intersective polynomials of degree 2.

3. There are $\frac{p^2(p-1)}{2}\left(\frac{p^3-p}{3}\right)$ polynomials of the form $(x-a)(x-b)(x-c)g(x)$ where $g(x)$ is an irreducible polynomials of degree 3. Given that $N_3(p) = \frac{p^3-p}{3}$ and $\frac{p^2(p-1)}{2}$ strict p-intersective polynomials of degree 3.

4. There are $\frac{7(p^4-p^2)(p^2-p)}{24}$ polynomials of the form $(x-a)(x-b)(x-c)(x-d)g(x)$ where $g(x)$ is an irreducible polynomial of degree 2. Given $N_2(p) = \frac{p^2-p}{2}$ and $\frac{7}{12}(p^4-p^2)$strict p-intersective polynomials of degree 4.

Adding all of the forms together will yield:

$$\begin{aligned}\nu_6(p) &= \frac{p^6-p^2}{5} + \frac{p^2+p}{2}\cdot\frac{p^4-p^2}{4} + \frac{p^2(p-1)}{2}\cdot\frac{p^3-p}{3} + \frac{7(p^4-p^2)(p^2-p)}{24} \\ &= \nu_6(p) = \frac{1}{60}\left(47p^6 - 20p^5 - 35p^4 + 20p^3 - 12p^2\right).\end{aligned}$$

■

Table 3.2: Values of $\nu_d(2), \nu_d(3), \nu_d(5)$, and $\nu_d(7)$ for $d = 3, 4, 5, 6$.

$d\backslash p$	2	3	5	7
$d = 3$	2	9	50	147
$d = 4$	7	42	350	1,372
$d = 5$	18	150	1,975	10,633
$d = 6$	32	450	10,870	85,260

From the results from this chapter, we are now able to find the number of monic strict p-intersective polynomials with degrees 3,4,5, and 6. Above is a table for some of the values with a specific prime p.

Chapter 4

Construction and Enumeration of p-Intersective Polynomials

In this chapter, We focus on p-intersective polynomials where p is any fixed prime number. It is obvious that every polynomial of degree 1 over $\mathbb{Z}_p$ is p-intersective. We start with small prime numbers p and lower degree p-intersective polynomials.

In order to construct an intersective polynomial, one idea is to first construct a P_i-intersective polynomial $f_i(x)$ for each subset $P_i \subseteq \mathcal{P}$, where $i = 1, 2, \ldots, r$, with $P_1 \cup \cdots \cup P_r = \mathcal{P}$. The product $h(x) = f_1(x) \cdot \cdots \cdot f_r(x)$ is then a $\mathcal{P}$-intersectionve polynomial. Thus, it is important to investigate methods of creating p-intersective polynomials for a fixed prime number p. We first count the number of linear and quadratic p-intersective polynomials in $\mathbb{Z}_p[x]$.

4.1 Linear and Quadratic P-Intersective Polynomials

In this section, we focus on monic p-intersective polynomials in the ring $\mathbb{Z}_p[x]$ for a given prime number p. Recall that $N_d(p)$ denotes the number of p-intersective polynomials in $\mathbb{Z}_p[x]$.

Theorem 12. *Let p be any prime. In the ring $\mathbb{Z}_p[x]$, there are exactly p monic linear p-intersective polynomials and $\frac{p(p+1)}{2}$ many monic quadratic p-intersective polynomials. That is, $N_1(p) = p$ and $N_2(p) = p(p+1)/2$.*

Proof. Every momnic polynomial of degree 1 is in the form of $x + a$, where $a \in \mathbb{Z}_p$. Therefore, there are exactly p monic linear p-intersective polynomials.

For a monic quadratic polynomial to be p-intersective, it must be the product of two monic polynomials of degree 1 and so it can be written in the form of $(x-a)(x-b)$, where $a, b, \in \mathbb{Z}_p$. There are p of them in the form of $(x-a)^2$ $(a = b)$. There are $p(p-1)/2$ polynomials in the form of $(x-a)(x-b)$, where $a \neq b$. We obtain

$$N_2(p) = p + \frac{p(p-1)}{2} = \frac{p(p+1)}{2}$$

many monic quadratic p-intersective polynomials. ■

Next we construct a quadratic S-intersective polynomial for some special sets S.

Proposition 8. *Let p be an odd prime number.*

1. *The polynomial $x^2+x+1 \in \mathbb{Z}[x]$ is P_1-intersective where*

$$P_1 = \{\, p \in \mathbf{P} \mid p \equiv 1 \text{ or } 7 \pmod{12} \,\}.$$

2. *If $p \equiv 5 \pmod{12}$, then the polynomial $f(x) = x^2+2x+2$ is p-intersective.*

3. *If $p \equiv 11 \pmod{12}$, then the polynomial $f(x) = x^2+2x-2$ is P_1-intersective.*

Proof. By Lemma 4, it is sufficient to prove that $1^2 - 4(1)(1) = -3$ is a quadratic residue.

For (1), there are two cases: $p \equiv 1 \pmod{12}$ or $p \equiv 7 \pmod{12}$.

Case 1. $p \equiv 1 \pmod{12}$. *Then 3 is a quadratic residue by Theorem 1(5). Also, $p \equiv 1 \pmod{12}$ implies $p \equiv 1 \pmod 4$, so -1 is a quadratic residue. Therefore -3 is a quadratic residue.*

Case 2. $p \equiv 7 \pmod{12}$. *Then $p \equiv 3 \pmod 4$. Again by Theorem 1, both -1 and 3 are quadratic non-residues, thus -3 is a quadratic residue.*

Therefore, $f(x)$ is p-intersective.

For (2), the discriminate for x^2+2x+2 is -4. Since $p \equiv 1 \pmod 4$, -1 is a quadratic residue mod p and so is -4. By Lemma 4, x^2+2x+2 is p-intersective.

For (3), the discriminant of x^2+2x-2 is $12 = 3 \cdot 4$. Since $p \equiv 11 \pmod{12}$, 3 is a quadratic residue mod p, and so does 12. Thus, x^2+2x-2 is p-intersective. ■

Proposition 9. *The polynomial $f(x) = x^2 - (2\beta+1)x + \beta(1+\beta)$ for any $\beta \in \mathbb{Z}$ is intersective and has two consecutive roots in $\mathbb{Z}_p$.*

Proof. Let p be any prime. We apply Theorem 3 to determine if the given polynomial f is p-intersective. It is obvious that the polynomial can be factored as $f(x) = (x-\beta)(x-\beta-1)$, therefore both β and $\beta+1$ are roots. Next,

$$f'(x) = 2x - (2\beta+1) \Rightarrow f'(\beta) = 2\beta - (2\beta+1) = -1 \neq 0 \quad \text{in } \mathbb{Z}_p.$$

This proves that $f(x)$ is p-intersective for every prime p, therefore it is intersective.

■

4.2 Cubic p-Intersective Polynomials

Now we focus on p-intersective polynomials of degree 3 which are also monic.

Theorem 13. *Let p be a prime number. The number of monic cubic p-intersective polynomials in $\mathbb{Z}_p[x]$ is given by*

$$N_3(p) = \frac{p(2p^2+1)}{3}.$$

Proof. We need to count all of the polynomials with degree 3 that are p-intersective. Below is the list of all possible forms of monic cubic polynomials that have a root in $\mathbb{Z}_p$ and the number of them:

1. There are p cubic polynomials that are in the form of $(x-a)^3$, $a \in \mathbb{Z}_p$.

2. There are $p(p-1)$ polynomials that are in the form of $(x-a)^2(x-b)$ where $a, b \in \mathbb{Z}_p$ and $a \neq b$.

3. There are $\frac{p(p-1)(p-2)}{6}$ polynomials that are in the form of $(x-a)(x-b)(x-c)$ where $a \neq b \neq c$.

4. There are $\frac{p(p^2-p)}{2}$ polynomials that are in the form of $(x-a)g(x)$ where $g(x)$ is an irreducible polynomial of degree 2 in $\mathbb{Z}_p[x]$. Refer to Corollary 2 for the number of quadratic irreducible polynomials over $\mathbb{Z}_p$.

Adding all of the polynomials will give us,

$$N_3(p) = p + p(p-1) + \frac{p(p-1)(p-2)}{6} + \frac{p(p^2-p)}{2} = \frac{p(2p^2+1)}{3}.$$

■

For small primes, we immediately obtain the following results which confirms the numbers in Examples 4, 5, and Proposition 5.

Corollary 4. *There are exactly 6 monic cubic 2-intersective polynomials, 19 monic cubic 3-intersective polynomials, and 85 monic 5-intersective polynomials in* $\mathbb{Z}_2[x], \mathbb{Z}_3[x]$, *and* $\mathbb{Z}_5[x]$ *respectively. That is,*

$$N_3(2) = 6, \quad N_3(3) = 19, \quad \textit{and} \quad N_3(5) = 85.$$

Proof. By evaluating the formula $p(p^2+1)/3$ obtained from Theorem 13 at $p = 2, 3, 5$, we obtain the values 6, 19, and 85. ■

Note that there are 1, 2, and 4 non-zero quadratic residues modulo 2, 3, 5 respectively. The product of a non-zero quadratic residue and a p-intersect polynomial is also p-intersective. Thus, there are 6, 38, and 340 2,3,5-intersective polynomials respectively, including the non-monic ones.

4.3 Construction of Special Intersective Polynomials

The polynomial $(x^3-19)(x^2+x+1)$ in Proposition 1 was proven to be intersective using advanced Galois Theory. We create a similar intersective polynomial.

Theorem 14. *The polynomial $(x^3-19)(x^2+3)$ is intersective.*

Proof. In order to prove that the polynomial is intersective, we need to show that modulo any prime number p, either (x^3-19) or (x^2+3) has a root in $\mathbb{Z}_p$.

Case 1. *If $p \equiv 5$ or $11 \pmod{12}$, x^2+x+1 is irreducible over $\mathbb{Z}_p$ because the discriminant is -3 which is a quadratic non-residue mod p and so mod p^k for all positive integer k. It implies that x^2+x+1 has no root in $\mathbb{Z}_{p^k}$ where $k \in \mathbb{N}$. When $p=2$, x^2+x+1 is irreducible over $\mathbb{Z}_2$ so does in $\mathbb{Z}_{p^k}$ for all positive integers k. By Proposition 8, the polynomial x^3-19 must have a root in $\mathbb{Z}_{p^k}$ for all $k \in \mathbb{N}$ and therefore it is p-intersective. Thus, $(x^3-19)(x^2+3)$ is p-intersective.*

Case 2. *If $p \equiv 1$ or $7 \pmod{12}$, the discriminant of x^2+3 is -3 which is a quadratic residue mod p because both -1 and 3 are so. Thus, x^2+3 is p-intersective, so it has a root in $\mathbb{Z}_p$.*

Therefore, the polynomial $f(x)$ is $\mathbf{P}$-intersective. Then, by Corollary 1, it is intersective. ■

Theorem 15. *The polynomial* $f(x) = (x^2+x+1)(x^2+2x-2)(x^2+2x+2)$ *is* P_o*-intersective, where* $P_o = \mathbf{P} \setminus \{2\}$.

Proof. It is immediate from Proposition 8 ■

Chapter 5

Conclusions and Future Directions

In this paper, we first examined and enumerated irreducible polynomials over $\mathbb{Z}_p$, where p is prime. We investigated and enumerated the polynomials in $\mathbb{Z}_p[x]$ that are p-intersective with certain degrees. Furthermore, we introduced the concept of "strict p-intersective polynomial," for any fixed prime number p. The main results include the classification of strict p-intersective polynomials, an iterative formula for counting such polynomials, and the exact number for those of small degrees. Several polynomials in $\mathbb{Z}[x]$ that are intersective are constructed.

Below is a list of things that could be done in the future:

1. Find explicit formulas for the number of p-intersective or strict p-intersective polynomials over $\mathbb{Z}_p[x]$ with higher degrees.
2. Get a bound for the number of strict p-intersective polynomials over $\mathbb{Z}_p[x]$ of a certain degree.

3. Develop different methods of constructing strict p-intersective polynomials over $\mathbb{Z}_p[x]$.

4. Find real-life applications for strict p-intersective polynomials.

Bibliography

[1] Gegner E. *Notes on Intersective Polynomials.*[master's thesis].Columbus, OH: The Ohio State University; 2018.

[2] Daniel B, Yuri B. Polynomials With Roots Modulo Every Integer, *Proc. Amer. Math. Soc.*.1996; 124(6); 1663-1670

[3] Bergelson V, Leibman A, Lesigne E. Intersective polynomials and the polynomial Szemerédi theorem. *Adv in Math*. 2008;219(1);369-88.

[4] Brandl R. Integer polynomials with roots mod p for all primes p. *J. of Alg*. 2001;240(2);822-35.

[5] Garonzi M, Lucchini A. Covers and normal covers of finite groups. *J. of Algebra*. 2015;422148-65.

[6] Sonn J. Polynomials with roots in $\mathbb{Q}_p$ for All p Proceedings of the *Am. Math. Soc*. 2008;136(6):1955-60.

[7] Sonn, Jack.Sonn J. Two remarks on the inverse Galois problem for in-

tersective polynomials. *J. de théo. des nom. de Bod.* 2009;21(2):435-7.doi: 10.5802/jtnb.680.

[8] Soule MM. A classification and study of intersective polynomials.[Doctoral dissertation]. 2013

[9] Hyde AM, Lee PD, Spearman BK. Polynomials $(x^3-n)(x^2+3)$ solvable modulo any integer. *The Am. Math. Mth.* 2014;121(4);355-358.

[10] Lemmermeyer F. *Reciprocity laws: from Euler to Eisenstein.*Berlin, Germany:" Springer Science & Business Media; 2013 Mar 14.

[11] Rosen KH. Elementary number theory. London: Pearson Education; 2011.

[12] Chebolu SK, Mináč J. Counting Irreducible Polynomials Over Finite Fields Using the Inclusion-Exclusion Principle. *Math. mag.*. 2011;84(5);369-71.

[13] Church R. Tables of irreducible polynomials for the first four prime moduli. *Annals of Math.* 1935:198-209. https://doi.org/10.2307/1968675.

[14] Childs LN.Chapter 27: Irreducible Polynomials.In:Childs LN,ed. *A concrete introduction to higher algebra.* New York, NY: Springer; 2009:557-567.

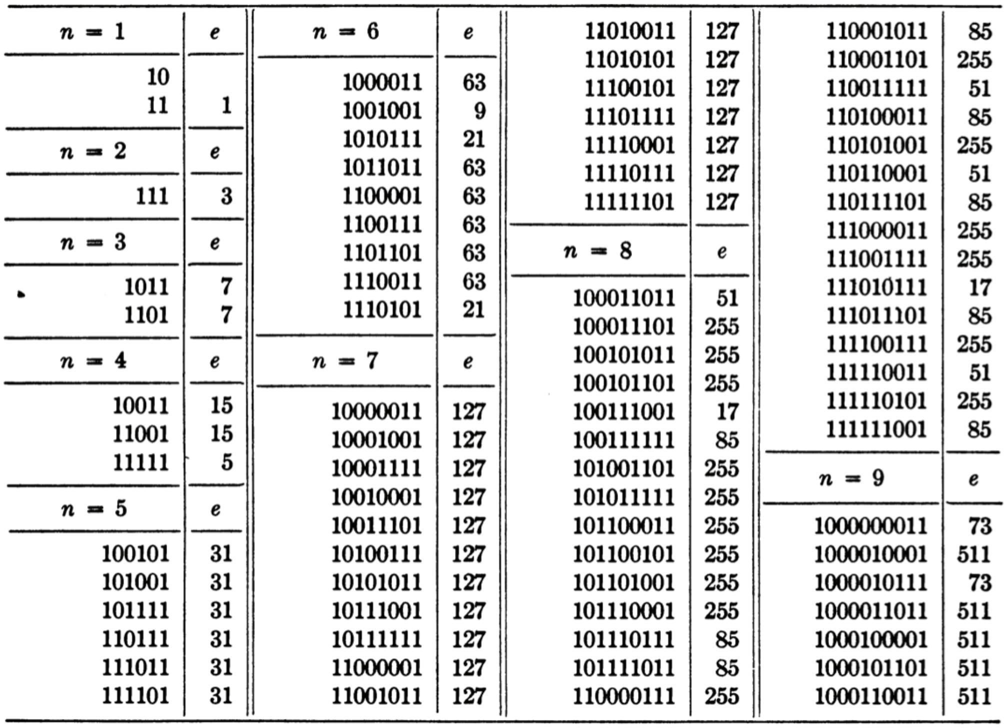
[15] Hyde A. Intersective polynomials and Hensel's Lemma.[master's thesis].Vancouver, CAN: University of British Columbia;2014

[16] Lehmer DN. Certain theorems in the theory of quadratic residues. *The Am. Math. Mth.* 1913;20(5):151-7. https://doi.org/10.2307/2972413.

Appendix

Below are the polynomials that are irreducible in $\mathbb{Z}_p$ with degree n. The number corresponds to the coefficients of the terms from the highest power decreasing into the constant term. For example, in modulus 2 and $n = 3$, 1011 means that $x^3 + x + 1$ is irreducible in $\mathbb{Z}_2$[13].

Irreducible Polynomials for the Modulus 2



$n = 1$	e
10	
11	1
$n = 2$	e
111	3
$n = 3$	e
1011	7
1101	7
$n = 4$	e
10011	15
11001	15
11111	5
$n = 5$	e
100101	31
101001	31
101111	31
110111	31
111011	31
111101	31
$n = 6$	e
1000011	63
1001001	9
1010111	21
1011011	63
1100001	63
1100111	63
1101101	63
1110011	63
1110101	21
$n = 7$	e
10000011	127
10001001	127
10001111	127
10010001	127
10011101	127
10100111	127
10101011	127
10111001	127
10111111	127
11000001	127
11001011	127
11010011	127
11010101	127
11100101	127
11101111	127
11110001	127
11110111	127
11111101	127
$n = 8$	e
100011011	51
100011101	255
100101011	255
100101101	255
100111001	17
100111111	85
101001101	255
101011111	255
101100011	255
101100101	255
101101001	255
101110001	255
101110111	85
101111011	85
110000111	255
110001011	85
110001101	255
110011111	51
110100011	85
110101001	255
110110001	51
110111101	85
111000011	255
111001111	255
111010111	17
111011101	85
111100111	255
111110011	51
111110101	255
111111001	85
$n = 9$	e
1000000011	73
1000010001	511
1000010111	73
1000011011	511
1000100001	511
1000101101	511
1000110011	511

Irreducible Polynomials for the Modulus 3

$n = 1$	e
10	
11	2
12	1
$n = 2$	e
101	4
112	8
122	8
$n = 3$	e
1021	26
1022	13
1102	13
1112	13
1121	26
1201	26
1211	26
1222	13
$n = 4$	e
10012	80
10022	80
10102	16
10111	40
10121	40
10202	16
11002	80
11021	20
11101	40
11111	5
11122	80
11222	80
12002	80
12011	20
12101	40
12112	80
12121	10
12212	80
$n = 5$	e
100021	242
100022	121
100112	121
100211	242
101011	242
101012	121
101102	121
101122	121
101201	242
101221	242
102101	242
102112	121
102122	11
102202	121
102211	242
102221	22
110002	121
110012	121
110021	242
110101	242
110111	242

Irreducible Polynomials for the Modulus 5

$n = 1$	e
10	
11	2
12	4
13	4
14	1
$n = 2$	e
102	8
103	8
111	3
112	24
123	24
124	12
133	24
134	12
141	6
142	24
$n = 3$	e
1011	62
1014	31
1021	62
1024	31
1032	124
1033	124
1042	124
1043	124
1101	62
1102	124
1113	124
1114	31
1131	62
1134	31
1141	62
1143	124
1201	62
1203	124
1213	124