University of Mississippi

eGrove

Electronic Theses and Dissertations | Graduate School

2011

Covering Systems of Polynomial Rings Over Finite Fields

Michael Wayne Azlin

Follow this and additional works at: https://egrove.olemiss.edu/etd

 Part of the Mathematics Commons

Recommended Citation

Azlin, Michael Wayne, "Covering Systems of Polynomial Rings Over Finite Fields" (2011). *Electronic Theses and Dissertations*. 39.
https://egrove.olemiss.edu/etd/39

This Thesis is brought to you for free and open access by the Graduate School at eGrove. It has been accepted for inclusion in Electronic Theses and Dissertations by an authorized administrator of eGrove. For more information, please contact egrove@olemiss.edu.

COVERING SYSTEMS OF POLYNOMIAL RINGS OVER FINITE FIELDS

A Thesis
presented in partial fulfillment of requirements for the degree
Master of Science in the Department of Mathematics
The University of Mississippi

by

Michael W. Azlin

May 2011

Copyright ©2011 by Michael W. Azlin
All rights reserved

ABSTRACT

In 1950 Paul Erdős observed that every integer belonged to a certain system of congruences with distinct moduli. He called such a systems of congruences *covering systems*. Utilizing his covering system, he disproved a conjecture of de Polignac asking, "for every odd k, is there a prime of the form $2^n + k$?"

Examples of covering systems of the integers are presented along with with some brief history and a sketch of the disproof by Erdős. Open conjectures concerning covering systems and best known results of attempts to prove these conjectures are given.

Analogies are drawn between the integers and $\mathbb{F}_q[x]$, and covering systems are defined in $\mathbb{F}_q[x]$. Examples of covering systems in the particular case of $\mathbb{F}_2[x]$ are presented along with some restrictions as to their construction. Also presented is a conjecture concerning covering systems of $\mathbb{F}_2[x]$ analogous to one of Erdős concerning covering systems of the integers.

DEDICATION

This thesis is dedicated to my mother, Linda O'Neal; my sister, Jonbeth Atib; my nephew, Tristan Harris; and lastly to the memory of my father, James Azlin.

ACKNOWLEDGEMENTS

I would first like to offer my most sincere and humble gratitude to my advisors, Drs. Micah Milinovich and Nathan Jones, for their tireless efforts in providing assistance, encouragement, and motivation (more than one kick in the pants) throughout this entire process.

I also wish to express great appreciation to Drs. William Staton and Sandra Spiroff, who not only served on my committee, but also expended valuable time answering questions of an often frustrated student along the way.

I bestow recognition on Susan Leake and Charlotte Alexander for helping me to rediscover my love for mathematics.

I salute the entire University of Mississippi Mathematics Department for their daily devotion to instill a greater knowledge of this wonderful subject.

Lastly, I am forever indebted to Evelyn Golden Sims. Although thirty years late, I extend to her my warmest and most heartfelt praise for teaching me the value of an education.

TABLE OF CONTENTS

1 COVERING SYSTEMS OF THE INTEGERS

Although the term *covering system* was not coined until the 1950's by Paul Erdős [4], the ideas underlying covering systems have been apparent since ancient times. In fact, in everyday life, we often think of the integers in terms of the most basic covering system:

$$0 \pmod 2 \quad \text{and} \quad 1 \pmod 2. \tag{1.1}$$

That is, we think of the integers in terms of even and odd. Clearly, every $b \in \mathbb{Z}$ satisfies one of these congruences, and in this case b is said to be *covered*. We call such a system a *covering*.

Definition 1.1. A ***covering system*** of the integers is a system of congruences

$$\mathcal{C} = \{a_i \pmod{m_i}\}_{i=1}^{k}$$

such that every $b \in \mathbb{Z}$ satisfies $b \equiv a_i \pmod{m_i}$ for some $i = 1, 2, \ldots, k$. In this case, we say that the integers are *covered* by $\mathcal{C}$.

System (1.1) is a trivial example, as are all covering systems of the integers with identical moduli. We want to expand the idea of covering systems beyond triviality. Hence our goal is to construct a non-trivial system of congruences which satisfies Definition (1.1). We will begin with a trivial system containing identical moduli meeting our definition and gradually modify it to the point that no *two* moduli are identical, yet our result will

remain a covering system of the integers. We see that

$$\begin{aligned} 0 \pmod 6 \\ 1 \pmod 6 \\ 2 \pmod 6 \\ 3 \pmod 6 \\ 4 \pmod 6 \\ 5 \pmod 6 \end{aligned} \tag{1.2}$$

satisfies Definition 1.1. We will now alter system (1.2) in such a way that it remains a covering system of the integers, yet each its moduli are distinct. First we note that $b \equiv 0, 2, 4 \pmod 6$ if and only if $b \equiv 0 \pmod 2$. Hence the system

$$\begin{aligned} 0 \pmod 2 \\ 1 \pmod 6 \\ 3 \pmod 6 \\ 5 \pmod 6 \end{aligned} \tag{1.3}$$

is still a covering system of the integers. Our next observation is that if $b \equiv 1 \pmod 6$, then $b \equiv 1 \pmod 3$. Therefore the system of congruences

$$\begin{aligned} 0 \pmod 2 \\ 1 \pmod 3 \\ 3 \pmod 6 \\ 5 \pmod 6 \end{aligned} \tag{1.4}$$

yet again satifies Definition 1.1. Next it remains to replace either $3 \pmod 6$ or $5 \pmod 6$ with congruences of moduli other than $2, 3$, or 6. We notice that if $b \equiv 5 \pmod 6$, then $b \equiv 5$ or $11 \pmod{12}$. We also make the observation that if $b \equiv 5 \pmod{12}$, then $b \equiv 1 \pmod 4$. Thus $b \equiv 5 \pmod 6$ implies that either $b \equiv 11 \pmod{12}$ or $b \equiv 1 \pmod 4$.

Thus the system of congruences

$$\begin{aligned} 0 \pmod 2 \\ 1 \pmod 3 \\ 1 \pmod 4 \\ 3 \pmod 6 \\ 11 \pmod{12} \end{aligned} \tag{1.5}$$

is a covering system of the integers where each of the moduli are distinct. This leads us to the following definition:

Definition 1.2. A ***distinct covering system*** of the integers is a system of congruences

$$\mathcal{C} = \{a_i \pmod{m_i}\}_{i=1}^{k}$$

such that every $b \in \mathbb{Z}$ satisfies $b \equiv a_i \pmod{m_i}$ for some $i = 1, 2, \ldots, k$ where the moduli m_i are distinct.

It can be shown that system (1.5) fulfills Definition 1.2 with largest modulus as small as possible (Krukenberg [10]); however, there is nothing special about the choice of a_i, and there are multiple ways to construct distinct covering systems of the integers with moduli $2, 3, 4, 6,$ and 12. For instance:

$$\begin{aligned} 0 \pmod 2 \\ 1 \pmod 3 \\ 3 \pmod 4 \\ 5 \pmod 6 \\ 9 \pmod{12} \end{aligned} \tag{1.6}$$

and

$$\begin{array}{rl} 1 & (\mathrm{mod}\ 2) \\ 2 & (\mathrm{mod}\ 3) \\ 0 & (\mathrm{mod}\ 4) \\ 0 & (\mathrm{mod}\ 6) \\ 10 & (\mathrm{mod}\ 12) \end{array} \tag{1.7}$$

are two examples of distinct covering systems of the integers with moduli $2, 3, 4, 6,$ and 12. In the next chapter we investigate how classical questions concerning prime numbers led to the concept of the covering system.

2 HISTORY AND EXAMPLES

An early question raised about primes was, "Are there infinitely many primes of the form 2^n-1?" It has long been known that in order for 2^n-1 to be prime, n must be prime. However, this is not sufficient. For example, $2^2-1=3,\ 2^3-1=7,$ and $2^5-1=31$ are all prime, but $2^{11}-1=2047=23\cdot 89$ is composite. Primes of the form 2^n-1 are known as *Mersenne primes.* As of May 2011, there are forty-seven known Mersenne primes with the largest being $2^{43,112,609}-1$ [7]. Historically, the interest in Mersenne primes comes from a famous theorem of Euclid: "If 2^n-1 is prime, then $N=2^{n-1}(2^n-1)$ is *perfect.*" That is, N is equal to the sum of its proper divisors. Euler proved the partial converse that if N is an even perfect number, then N is of Euclid's form. It is not known if there are any odd perfect numbers.

The next question we address is whether there are infinitely many primes of the form 2^n+1. Fermat showed that it is necessary for n to be a power of 2 in order for 2^n+1 to be prime. He also conjectured that this was a sufficient condition. Primes of the form $2^{2^k}+1$ are now known as *Fermat primes.* For example, $2^{2^0}+1=3,\ 2^{2^1}+1=5,\ 2^{2^2}+1=17,\ 2^{2^3}+1=257,$ and $2^{2^4}+1=65537$ are all prime. However, Euler showed that $2^{2^5}+1=641\cdot 6700417$ is composite, disproving Fermat's assertation that $2^{2^k}+1$ is prime for $k\geq 0$. No other Fermat primes are known, and it has been shown that for $k=5,6,\ldots,32$, and many larger values of k, that $2^{2^k}+1$ is composite. Moreover, Hardy and Wright have given a heuristic argument which suggests that only a finite number of them are prime [9].

Fermat's conjecture leads to the following: "For each odd k are there infinitely many primes of the form 2^n+k?" In 1849, de Polignac simplified this question with the following conjecture:

Conjecture 2.1. [13] *For each odd number k, there is at least one prime of the form $2^n + k$.*

Erdős disproved this conjecure using a distinct covering system of the integers. We will first use the idea of Erdős' proof to show that the conjecture holds for $k = 61$. That is, we will use a non-covering system of congruences to exhibit a prime of the form 2^n+61. Next we will present a sketch of Erdős' disproof of Conjecture 2.1.

In constructing our system of congruences, we are interested in the multiplicative order of 2 modulo each of the prime factors of $2^n + k$, and n modulo the multiplicative order of 2. First we consider $2^n + 61$ and the case of $n = 1$. Thus

$$2^1 + 61 = 63 = 3^2 \cdot 7.$$

Modulo 3, the multiplicative order of 2 is 2. So, $n \equiv 1 \pmod 2$ implies that

$$2^n + 61 \equiv 2 + 61 \equiv 0 \pmod 3.$$

Similarly, modulo 7, the multiplicative order of 2 is 3. So, $n \equiv 1 \pmod 3$ implies that

$$2^n + 61 \equiv 2 + 61 \equiv 0 \pmod 7,$$

as well. Thus 2^n+61 is composite provided n satisfies either of the following congruences:

$$n \equiv 1 \pmod 2, \text{ or}$$
$$n \equiv 1 \pmod 3.$$

Now we consider the case of $n = 2$. That is,

$$2^2 + 61 = 65 = 5 \cdot 13$$

Modulo 5, the multiplicative order of 2 is 4. So, $n \equiv 2 \pmod 4$ implies that

$$2^n + 61 \equiv 2^2 + 61 \equiv 0 \pmod 5.$$

Similarly, modulo 13, the multiplicative order of 2 is 12. So, $n \equiv 2 \pmod{12}$ implies that

$$2^n + 61 \equiv 2^2 + 61 \equiv 0 \pmod{13},$$

as well. We conclude that $2^n + 61$ is composite for n satisfying any of the following congruences:

$$\begin{aligned} n &\equiv 1 \pmod 2, \\ n &\equiv 1 \pmod 3, \\ n &\equiv 2 \pmod 4, \text{ or} \\ n &\equiv 2 \pmod{12}. \end{aligned} \tag{2.1}$$

Now we consider the integers $1, 2, \ldots, 12, \ldots$ to verify if they are covered. We observe that $1, 3, 5, 7, 9, 11, \ldots$ are in the congruence class $n \equiv 1 \pmod 2$. Similary, $1, 4, 7, 10, \ldots$ are in the congruence class $n \equiv 1 \pmod 3$; $2, 6, 10, \ldots$ are in the congruence class $n \equiv 2 \pmod 4$; and $2, 14, 26, \ldots$ are in the congruence class $n \equiv 2 \pmod{12}$. Hence the integers stricken in the list below:

$$\not{1}, \not{2}, \not{3}, \not{4}, \not{5}, \not{6}, \not{7}, 8, \not{9}, \not{10}, \not{11}, 12, \ldots$$

are covered by system (2.1). We see that 8 does not belong to any of our given congruence classes, making 2^8+61 a reasonable candidate to check for primality. Indeed, $2^8+61 = 317$ is prime. Thus, for $k = 61$, Conjecture 2.1 holds; moreover, we see that system (2.1) is not a covering system of the integers.

We now present a counterexample of Conjecture 2.1 due to Erdős. Our exposition follows Pomerance [13]. Erdős observed that every integer satisfies at least one of the

following congruences:

$$\begin{aligned} &1 \pmod 2,\\ &1 \pmod 3,\\ &2 \pmod 4,\\ &8 \pmod{12},\\ &4 \pmod 8, \text{ or}\\ &0 \pmod{24}. \end{aligned} \tag{2.2}$$

It is not difficult to show that system (2.2) satisfies Definition 1.2, and hence is a distinct covering system of the form

$$\mathcal{C} = \{a_i \pmod{m_i}\}_{i=1}^{k}.$$

Using the previous example as a guide, we want primes p_i such that $2^{m_i} \equiv 1 \pmod{p_i}$. Our primes p_i are presented in the following table:

$a_i \pmod{m_i}$	p_i, where $2^{m_i} \equiv 1 \pmod{p_i}$
$1 \pmod 2$	3
$2 \pmod 4$	5
$1 \pmod 3$	7
$8 \pmod{12}$	13
$4 \pmod 8$	17
$0 \pmod{24}$	241

If simultaneously, $k + 2^{a_i} \equiv 0 \pmod{p_i}$ for each i, that is:

$$\begin{aligned} k &\equiv -2^1 \pmod 3, \\ k &\equiv -2^2 \pmod 5, \\ k &\equiv -2^1 \pmod 7, \\ k &\equiv -2^8 \pmod{13}, \\ k &\equiv -2^4 \pmod{17}, \\ k &\equiv -2^0 \pmod{241}, \end{aligned} \tag{2.3}$$

and $k \equiv 1 \pmod 2$, then $2^n + k$ is composite for each n and k is odd. For example, take $n \equiv 8 \pmod{12}$. Since, modulo 13, the multiplicative order of 2 is 12, we have that $2^{8 \pmod{12}} + k \equiv 0 \pmod{13}$. A similar argument works for each of the other congruences in the covering system. Furthermore, the Chinese Remainder Theorem guarantees that (2.3) is equivalent to a single congruence $\pmod{\prod p_i}$. The solution to the simultaneous set of congruences in (2.3) is:

$$k \equiv 1518781 \pmod{11184810}.$$

Thus $2^n + 1518781$ is composite for all n. Therefore Conjecture 2.1 is false! Moreover, Erdős' construction actually gives an arithmetic progression of integers k where $2^n + k$ is composite for all n, e.g.

$$2^n + 1518781 + 11184810,\ 2^n + 1518781 + 2(11184810),\ 2^n + 1518781 + 3(11184810), \ldots$$

are also composite for all n.

It should be noted that the distinct covering system used in this example uses larger moduli than system (1.5) in the introduction. However, system (1.5) contains the moduli $2, 3,$ and 6. Since $2^2 - 1 = 3,\ 2^3 - 1 = 7,$ and $2^6 - 1 = 3^2 \cdot 7$, we are unable to use the Chinese Remainder Theorem if the moduli $2, 3,$ and 6 are all used. Therefore, system (1.5) cannot be used to disprove Conjecture 2.1 using Erdős' technique.

Distinct covering systems of the integers need not have a minimum modulus 2. For instance, I have found the following distinct covering system of minimum modulus 3:

$$\begin{aligned}
0 &\pmod 3\\
0 &\pmod 4\\
0 &\pmod 5\\
1 &\pmod 6\\
2 &\pmod 8\\
1 &\pmod{10}\\
5 &\pmod{12}\\
2 &\pmod{15}\\
3 &\pmod{20}\\
22 &\pmod{24}\\
29 &\pmod{30}\\
6 &\pmod{40}\\
14 &\pmod{60}\\
38 &\pmod{120}.
\end{aligned} \tag{2.4}$$

I leave the verification that this is a distinct covering of $\mathbb{Z}$ as an exercise for the reader; one need only check that (2.4) covers the integers n with $0 \leq n \leq 119$.

Mirroring Erdős' approach, I found primes p_i such that $2^{m_i} \equiv 1 \pmod{p_i}$ which are presented below:

$a_i \pmod{m_i}$	p_i
$0 \pmod 3$	7
$0 \pmod 4$	5
$0 \pmod 5$	31
$1 \pmod 6$	3
$2 \pmod 8$	17
$1 \pmod{10}$	11
$5 \pmod{12}$	13
$2 \pmod{15}$	151
$3 \pmod{20}$	41
$22 \pmod{24}$	241
$29 \pmod{30}$	331
$6 \pmod{40}$	61681
$14 \pmod{60}$	1321
$38 \pmod{120}$	4562284561

Solving the simultaneous equivalences:

$$\begin{aligned}
k &\equiv -2^0 \pmod 7,\\
k &\equiv -2^0 \pmod 5,\\
k &\equiv -2^0 \pmod{31},\\
k &\equiv -2^1 \pmod 3,\\
k &\equiv -2^2 \pmod{17},\\
k &\equiv -2^1 \pmod{11},\\
k &\equiv -2^5 \pmod{13},\\
k &\equiv -2^2 \pmod{151},\\
k &\equiv -2^3 \pmod{41},\\
k &\equiv -2^{22} \pmod{241},\\
k &\equiv -2^{29} \pmod{331},\\
k &\equiv -2^6 \pmod{61681},\\
k &\equiv -2^{14} \pmod{1321},\\
k &\equiv -2^{38} \pmod{4562284561}, \text{ and}\\
k &\equiv 1 \pmod 2
\end{aligned} \tag{2.5}$$

yields the value

$$k \equiv 78825751367790623790010350300 2689 \pmod{290541638422932431235804821919 2010}.$$

Thus $2^n + 78825751367790623790010350300 2689$ is composite for all n. It is not difficult to check that this value of k is not in the arithmetic progression exhibited by Erdős, and thus provides a genuinely new counterexample to Conjecture 2.1.

3 RESULTS AND CONJECTURES IN $\mathbb{Z}$

There are many conjectures dealing with covering systems of the integers. We present some of them here. The first and most famous of the conjectures is from Erdős in 1950, and is motivated by examples like system (2.4). Erdős has stated that, "This is my favourite problem" [5].

Conjecture 3.1. [5] *For any $N > 0$, there exists a distinct covering system*

$$\mathcal{C} = \{a_i \pmod{m_i}\}_{i=1}^{k}$$

for which $m_i \geq N$ for each $i = 1, 2, \ldots, k$.

In other words, there exists a distinct covering system of $\mathbb{Z}$ whose minimum modulus is arbitrarily large. Erdős offers \$1000.00 for a proof or disproof of this conjecture [5]. Attempts to prove the conjecture have led to the following results: Churchhouse found a system with minimum modulus $N = 9$ in 1968 [3]; Krukenberg with $N = 18$ in 1971 [10]; Choi with $N = 20$ in 1971 [2]; Morikawa with $N = 24$ in 1981 [11]; Gibson with $N = 25$ in 2006 [6]; and Nielson with $N = 40$ in 2008, which contains over 10^{50} congruences [12]. For the sake of conservation of time and natural resources, I will not list them here. Nielson has suggested that Conjecture 6.3 is false [12].

A second conjecture due to Erdős in 1960 is as follows:

Conjecture 3.2. [14] *There exists a distinct covering system with all moduli m_i odd, distinct, and greater than one.*

Erdős offers \$25.00 for a disproof of the conjecture [9]. It has been shown (Berger, Felzenbaum, and Fraenkel [1]) that the least common multiple of all the moduli of such a system must contain at least six prime factors. In 1970 Selfridge conjectured that no such covering system exists, and he offers \$900.00 for an explicit example of such a system [9].

Next is what is known as the *Strong Conjecture* of Erdős, stated in 1976 :

Conjecture 3.3. [14] *For all $N > 0$, there exists a distinct covering system,*

$$\mathcal{C} = \{a_i \pmod{m_i}\}_{i=1}^{k},$$

such that for all m_i and for every $p|m_i$, $p \geq N$ and all the m_i are squarefree.

We see that this conjecture implies both of the previous conjectures. If we demand that each modulus in a distinct covering system be odd and squarefree (as in Conjectures 3.2 and 3.3), then it has been shown (Guo, Sun [8]) that the least common multiple of all the moduli must contain at least twenty-two prime factors. This gives some indication of why finding examples of such covering systems (if they exist) is difficult.

4 ANALOGIES BETWEEN $\mathbb{Z}$ AND $\mathbb{F}_q[x]$

Consider a finite field $\mathbb{F}_q$ with q elements where q is the power of a prime p, and consider $\mathbb{F}_q[x]$, the polynomial ring over $\mathbb{F}_q$. We shall prove that $\mathbb{F}_q[x]$ has several properties in common with $\mathbb{Z}$, the ring of integers; namely:

1. Both rings are principal ideal domains
2. Both have finitely many units
3. Both have the property that the residue class ring of any non-zero ideal is finite, and
4. Both have infinitely many prime elements.

4.1 Principal Ideal Domain

Both the ring of integers $\mathbb{Z}$ and our polynomial ring $\mathbb{F}_q[x]$ are principal ideal domains.

Definition 4.1. An integral domain D is called a ***principal ideal domain*** if every ideal has the form $\langle a \rangle = \{ad |\ d \in D\}$ for some a in D.

Theorem 4.2. *$\mathbb{Z}$ is a principal ideal domain.*

Proof. Let I be an ideal of $\mathbb{Z}$. If $I = \{0\}$, then $I = \langle 0 \rangle$ and is a principal ideal as required. If $I \neq \{0\}$, then it contains a nonzero element x. Since $x, -x \in I$, we suppose that $x > 0$. Thus I contains at least one positive integer. Among the all the positive integers in I, we let m denote the least, thus $\langle m \rangle \subseteq I$. We will show that $\langle m \rangle = I$ by showing that $I \subseteq \langle m \rangle$. Let $a \in I$ be arbitrary. Upon division of a by m we get integers q and r such that $a = mq + r$; $0 \leq r < m$. We note that this is $r = a - mq$. Since $a \in I$ and $m \in I$, we have $r = a - mq \in I$. But this contradicts the minimality of m unless $r = 0$. Thus $a = mq$, and $I \subseteq \langle m \rangle$. Therefore $I = \langle m \rangle = m\mathbb{Z}$.

□

Before we can show that $\mathbb{F}_q[x]$ is a principal ideal domain, we must establish that it is an integral domain. We also need an analogous division algorithm for $\mathbb{F}_q[x]$.

Theorem 4.3. *$\mathbb{F}_q[x]$ is an integral domain.*

Proof. We claim that $\mathbb{F}_q[x]$ is commutative with unity and has no zero divisors. Obviously, the fact that $\mathbb{F}_q$ is commutative implies that $\mathbb{F}_q[x]$ is commutative. Clearly $p(x) = 1$ is the unity element of $\mathbb{F}_q[x]$. Now we suppose that $p(x), q(x) \in \mathbb{F}_q[x]$ and that

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

and

$$q(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0,$$

where $a_n \neq 0$ and $b_m \neq 0$. Thus $p(x)q(x) = a_n b_m x^{n+m} + \cdots + a_0 b_0$. Hence, since $\mathbb{F}_q$ is a field, $a_n b_m \neq 0$. Therefore $\mathbb{F}_q[x]$ is an integral domain.

□

Theorem 4.4. *Let $\mathbb{F}_q$ be a finite field of q elements and let $f(x), d(x) \in \mathbb{F}_q[x]$ with $d(x) \neq 0$. Then there exist unique polynomials $q(x), r(x) \in \mathbb{F}_q[x]$ such that $f(x) = q(x)d(x)+r(x)$ and either $r(x) = 0$ or deg $r(x) <$ deg $d(x)$.*

Proof. First we need to show the existence of $q(x)$ and $r(x)$. If $f(x) = 0$ or deg $f(x) <$ deg $d(x)$, then $q(x) = 0$ and $r(x) = f(x)$ and we are done. Thus it suffices to assume that $f(x) \neq 0$ and $n := \deg f(x) \geq \deg d(x) =: m$, say. Let

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

and

$$d(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0.$$

We will proceed by induction on n. Consider the base case of $n = 0$. Thus $f(x) = a_0 \in \mathbb{F}_q - \{0\}$, and $d(x) = b_0 \in \mathbb{F}_q - \{0\}$. In this case, $f(x) = (a_0 b_0^{-1})b_0 + 0$. Therefore

$f(x) = q(x)d(x) + r(x)$ where $q(x), r(x)$ have the desired properties. We assume that the result holds for deg $f(x) < n$. To complete the induction step let $f_1(x) = f(x) - a_n b_m^{-1} x^{n-m} d(x)$. Then $f_1(x) = 0$ or deg $f_1(x) < n$. Thus by our induction hypothesis, there exists $q_1(x), r_1(x) \in \mathbb{F}[x]$ such that $f_1(x) = q_1(x)d(x) + r_1(x)$, where $r_1(x) = 0$ or deg $r_1(x) <$ deg $d(x)$. Hence

$$\begin{aligned} f(x) =& a_n b_m^{-1} x^{n-m} d(x) + q_1(x)d(x) + r_1(x) \\ =& (q_1(x) + a_n b_m^{-1} x^{n-m})d(x) + r_1(x). \end{aligned}$$

Choosing $q(x) = q_1(x) + a_n b_m^{-1} x^{n-m}$ and $r(x) = r_1(x)$ we see that $f(x) = q(x)d(x) + r(x)$ as required, and the result holds by induction.

It remains to prove the uniqueness of $q(x), r(x)$. Suppose that

$$f(x) = q(x)d(x) + r(x) = \tilde{q}(x)d(x) + \tilde{r}(x),$$

where $r(x), \tilde{r}(x) = 0$ or deg $r(x)$, deg $\tilde{r}(x) <$ deg $d(x)$. Hence $\tilde{r}(x) - r(x) = d(x)[q(x) - \tilde{q}(x)]$. So, if $q(x) = \tilde{q}(x)$, then $r(x) = \tilde{r}(x)$; done. Similarly, if $r(x) = \tilde{r}(x)$, then $q(x) = \tilde{q}(x)$ and we are done. If $q(x) \neq \tilde{q}(x)$, then deg $[q(x) - \tilde{q}(x)]d(x) \geq$ deg $d(x)$. Thus deg $[\tilde{r}(x) - r(x)] \geq$ deg $d(x)$; a contradiction. Similarly, if $r(x) \neq \tilde{r}(x)$, then deg $[\tilde{r}(x) - r(x)] \leq$ deg $r(x)$, and hence deg $r(x) \geq$ deg $d(x)$; a contradiction. Thus $r(x)$ and $q(x)$ are unique as required. Therefore the theorem holds.

□

Now we are ready to show that $\mathbb{F}_q[x]$ is a principal ideal domain.

Theorem 4.5. *Let $\mathbb{F}_q$ be a finite field of q elements. Then $\mathbb{F}_q[x]$ is a principal ideal domain.*

Proof. Theorem 4.3 tells us that $\mathbb{F}_q[x]$ is an integral domain. Suppose I is an ideal of $\mathbb{F}_q[x]$. If $I = \{0\}$, then $I = \langle 0 \rangle$. We assume that $I \neq \{0\}$, thus I contains an element of minimum degree. Let $p(x) \in I$ be of minimum degree of all the elements in I. We will show that $I = \langle p(x) \rangle$. We let $q(x) \in I$. Thus, by Theorem 4.4, $q(x) = p(x)d(x) + r(x)$

where $r(x) = 0$ or $\deg r(x) < \deg p(x)$. But, $q(x) - p(x)d(x) = r(x) \in I$, and our choice of $p(x)$ of minimal degree implies that $r(x) = 0$. Hence $q(x) = p(x)d(x)$, and therefore $I = \langle p(x) \rangle$ and $\mathbb{F}_q[x]$ is a principal ideal domain.

□

4.2 Finiteness of Units

Both the ring of integers $\mathbb{Z}$ and the polynomial ring $\mathbb{F}_q[x]$ have finitely many units.

Definition 4.6. An element u of a ring R is called a *unit* if there exists an element $v \in R$ such that $uv = 1$.

Theorem 4.7. *There are finitely many units in* $\mathbb{Z}$.

Proof. Suppose that $u \in \mathbb{Z}$ is a unit, $u \neq 0$. Then there exists a $v \in \mathbb{Z}$ such that $uv = 1$. Since v is a non-zero integer, $|v| \geq 1$. Thus $|1| = |uv| = |u| \cdot |v| \geq |u|$. Hence $u = \pm 1$. Therefore there are only two units in $\mathbb{Z}$, namely ± 1.

□

Theorem 4.8. *There are finitely many units in* $\mathbb{F}_q[x]$.

Proof. Suppose that $f(x) \in \mathbb{F}_q[x]$ is a unit. Then $f(x) \neq 0$ and there exists a $g(x) \in \mathbb{F}_q[x]$ such that $f(x) \cdot g(x) = 1$. Let $n = \deg f(x)$ and $m = \deg g(x)$. Thus

$$0 = \deg 1 = \deg f(x)g(x).$$

Hence $n = m = 0$ since degrees are non-negative. So $f \in \mathbb{F}_q^*$, the set of non-zero constants. Therefore there are only $q - 1$ units in $\mathbb{F}_q[x]$.

□

4.3 Residue Classes

Let R denote either $\mathbb{Z}$ or $\mathbb{F}_q[x]$, and let $I \subseteq R$ be any non-zero ideal. Then the residue class ring R/I is finite.

Theorem 4.9. *$\mathbb{Z}$ has finite residue class rings.*

Proof. Let I be an ideal in $\mathbb{Z}$. From Theorem 4.2 we know that $\mathbb{Z}$ is a principal ideal domain, and thus $I = \langle n \rangle = n\mathbb{Z}$. Therefore, since $|\mathbb{Z}/n\mathbb{Z}| = n, \mathbb{Z}$ has finite residue class rings.

□

Theorem 4.10. *Let $d(x) \in \mathbb{F}_q[x], d(x) \neq 0$. Then $\mathbb{F}_q[x]/d(x)\mathbb{F}_q[x]$ is a finite ring with $q^{\deg d(x)}$ elements.*

Proof. By Theorem 4.4, we have $\{r(x) \in \mathbb{F}_q[x] | \deg r(x) < \deg d(x)\}$ as a complete system of residue classes for $\mathbb{F}_q[x]/d(x)\mathbb{F}_q[x]$. The elements of $\mathbb{F}_q[x]/d(x)\mathbb{F}_q[x]$ have the form

$$r(x) = \alpha_0 x^{m-1} + \alpha_1 x^{m-2} + \cdots + \alpha_{m-1}$$

where $m = \deg d(x)$ and $\alpha_i \in \mathbb{F}_q$. Since there are q^m such polynomials, the proof is complete.

□

4.4 Infinitude of Primes

Both $\mathbb{Z}$ and $\mathbb{F}_q[x]$ have infinitely many prime elements.

Definition 4.11. A non-zero element a of an integral domain D is said to be *irreducible* if a is not a unit, and whenever there exist $b, c \in D$ such that $a = bc$, then either b or c is a unit.

Definition 4.12. A non-zero element a of an integral domain D is said to be *prime* if a is not a unit and $a|bc$ implies $a|b$ or $a|c$.

Lemma 4.13. *Every integer $n > 1$ is divisible by a prime.*

Proof. We proceed by strong induction on n. When $n = 2$, the lemma holds as 2 is prime and clearly $2|2$. We now assume it is true for all $n \leq k-1$ and show that k is divisible by a prime. If k is prime, then $k|k$ and we are done. If k is not prime, then it is composite.

Thus $k = ab$; $a, b \in \mathbb{Z}$, and $1 < a, b < k$. By the inductive hypothesis, a is divisible by a prime p, hence k is also divisible by the same prime p. Therefore the lemma holds by the principle of mathematical induction.

□

Theorem 4.14. *There are infinitely many prime numbers.*

Proof. (Euclid). We prove the theorem by contradiction. Assume that there are finitely many primes in $\mathbb{Z}$ and list them as $p_1, p_2, \ldots, p_n$, say. Now consider the integer $N = p_1 p_2 \ldots p_n + 1$. By Lemma 4.13 N has some prime factor, say p_k. Since $p_k | N$ and $p_k | p_1 p_2 \ldots p_n$, this implies that $p_k | 1$, which is absurd! Therefore the number of primes must be infinite. □

Lemma 4.15. *Every non-zero, non-unit $a(x) \in \mathbb{F}_q[x]$ has an irreducible factor.*

Proof. Suppose that $a(x) \in \mathbb{F}_q[x]$, $a(x) \neq 0$, and a non-unit. We proceed by induction on the degree of $a(x)$. If $\deg a(x) = 1$, then $a(x) = \alpha \cdot x + \beta$ for $\alpha, \beta \in \mathbb{F}_q$, which is irreducible. We now assume that all non-zero, non-unit polynomials of degree less than some $k \geq 2$ have an irreducible factor, and we show that every such degree k polynomial also has an irreducible factor. If $a(x)$ is irreducible, there is nothing to show. If $a(x)$ is reducible, then $a(x) = b(x)c(x)$; $b(x), c(x) \in \mathbb{F}_q[x]$, and $\deg b(x), \deg c(x) < k$. By the inductive hypothesis, $b(x)$ has an irreducible factor, hence $a(x)$ also has an irreducible factor. Therefore the result holds by the principle of mathematical induction.

□

Lemma 4.16. *In a principal ideal domain, an element is irreducible if and only if it is prime.*

Proof. Let D be a principal ideal domain. Suppose that $a \in D$ is prime and that $a = bc$. Thus $a | b$ or $a | c$. Without loss of generality, say $a | b$ and write $aq = b$. Thus $1b = b = aq = (bc)q = b(cq)$. Hence $1 = cq$. Thus c is a unit, and therefore a is irreducible. Conversely, suppose that $a \in D$ is irreducible and that $a | bc$. Consider the ideal $I = \{ax + by \mid x, y \in D\}$ and let $\langle d \rangle = I$. Since $a \in I$, we can write $a = dw$ for

some $w \in D$. So, d is a unit or w is a unit. If d is a unit, then $I = D$, and $ax + by = 1$ for some $x, y \in D$. Hence $c = cax + cby$, and since a divides both cax and bcy, a also divides c. On the other hand, if w is a unit, then $\langle a \rangle = \langle d \rangle = I$. Thus there exists an element $t \in D$ such that $at = b$. Hence a divides b, and therefore a is prime.

□

Theorem 4.17. *There are infinitely many prime elements in* $\mathbb{F}_q[x]$.

Proof. By the previous lemma, it suffices to show that there are infinitely many irreducibles in $\mathbb{F}_q[x]$. We prove this by contradiction. Assume that there are finitely many irreducibles $g(x) \in \mathbb{F}_q[x]$, say n, and let $\mathbb{G} = \{g_1(x), g_2(x), \ldots, g_n(x)\}$ be the complete set of these irreducibles. Consider the polynomial $H(x) = g_1(x)g_2(x)\cdots g_n(x) + 1$. Since $H(x)$ is a polynomial of positive degree, by Lemma 4.15 it has an irreducible factor $g_k(x) \in \mathbb{G}$. Since $g_k(x)|H(x)$ and $g_k(x)|g_1(x)g_2(x)\cdots g_n(x)$, it follows that $g_k(x)|1$; a contradiction. Thus $\mathbb{G}$ is not the entire collection of irreducible polynomials in $\mathbb{F}_q[x]$. Hence there are infinitely many irredicibles in $\mathbb{F}_q[x]$.

□

These analogies between $\mathbb{Z}$ and $\mathbb{F}_q[x]$ lead us to ask if there are covering systems of $\mathbb{F}_q[x]$.

5 DEFINITION OF COVERING SYSTEMS OF $\mathbb{F}_q[x]$

In order to define a covering system of $\mathbb{F}_q[x]$, we first need a need a definition of what it means for polynomials in $\mathbb{F}_q[x]$ to be congruent.

Definition 5.1. Let $n(x)$ be a polynomial in $\mathbb{F}_q[x]$ such that $\deg n \geq 1$. We say that two polynomials $a(x)$ and $b(x)$ are ***congruent modulo n(x)*** if $n(x)|(a(x) - b(x))$ and we write $a(x) \equiv b(x) \pmod{n(x)}$.

Similar to the case in the ring of integers, we require that every $f(x) \in \mathbb{F}_q[x]$ satisfy at least one congruence in a system of congruences for $f(x)$ to be *covered*, and we say that $\mathbb{F}_q[x]$ is *covered*. Two such systems in $\mathbb{F}_2[x]$ are:

$$0 \pmod{x} \quad \text{and} \quad 1 \pmod{x}. \tag{5.1}$$

and

$$0 \pmod{x+1} \quad \text{and} \quad 1 \pmod{x+1}. \tag{5.2}$$

Definition 5.2. A ***covering system*** in $\mathbb{F}_q[x]$ is a system of congruences

$$\mathcal{C} = \{a_i(x) \pmod{m_i(x)}\}_{i=1}^{k}$$

such that every $f(x) \in \mathbb{F}_q[x]$ satisfies $f(x) \equiv a_i(x) \pmod{m_i(x)}$ for some $i = 1, 2, \ldots, k$. In this case, we say that $\mathbb{F}_q[x]$ is *covered*.

Systems (5.1) and (5.2) clearly satisfy Definition 5.2, yet they are trivial examples similar to systems (1.1) and (1.2) in the integers. We were able to exhibit covering systems with distinct moduli in $\mathbb{Z}$, and our goal is to construct a covering system of $\mathbb{F}_2[x]$ where each modulus is distinct and no two moduli are associates. In this setting, we call

elements $a(x), b(x) \in \mathbb{F}_q[x]$ associates if $a(x) = u \cdot b(x)$ where u is a non-zero element of $\mathbb{F}_q$.

Definition 5.3. A ***distinct covering system*** of $\mathbb{F}_q[x]$ is a system of congruences

$$\mathcal{C} = \{a_i(x) \pmod{m_i(x)}\}_{i=1}^{k}$$

such that every $f(x) \in \mathbb{F}_q[x]$ satisfies $f(x) \equiv a_i(x) \pmod{m_i(x)}$ for some $i = 1, 2, \ldots, k$ where the no two moduli are associates (and hence are distinct).

We claim that if all possible remainders of a polynomial modulo the least common multiple of the moduli in a system of congruences is covered, then all polynomials are covered.

Theorem 5.4. *Let $\mathcal{C} = \{a_i(x) \pmod{m_i(x)}\}_{i=1}^{k}$ be a system of congruences and let $M(x) = lcm\ (m_1(x), m_2(x), \ldots, m_k(x))$ If every polynomial $r(x) \in \mathbb{F}_q[x]$ with $\deg r(x) < \deg M(x)$ satisfies one of the congruences in $\mathcal{C}$, then $\mathcal{C}$ is a covering system of $\mathbb{F}_q[x]$.*

Proof. We need to show that every $f(x) \in \mathbb{F}_q[x]$ satisfies some congruence in $\mathcal{C}$. We write $f(x) = q(x)M(x) + r(x)$ where $\deg r(x) < \deg M(x)$ by Theorem 4.4. Thus $r(x) \equiv a_j(x) \pmod{m_j(x)}$ for some j; $1 \leq j \leq k$. Hence $q(x)M(x) + r(x) \equiv a_j(x) \pmod{m_j(x)}$. Since $m_j(x) | M(x)$ for every j, we have that $f(x) \equiv a_j(x) \pmod{m_j(x)}$. Therefore, $\mathcal{C}$ is a covering system of $\mathbb{F}_q[x]$.

□

With the previous theorem and definitions in place for $\mathbb{F}_q[x]$, we will exhibit examples of distinct covering systems of $\mathbb{F}_2[x]$ in the next chapter.

6 DISTINCT COVERING SYSTEMS OF $\mathbb{F}_2[x]$

Our first goal is to find a distinct covering system of $\mathbb{F}_2[x]$. Our first instinct is to employ a greedy approach and use both of the degree one polynomials in $\mathbb{F}_2[x]$. We claim that:

$$\begin{aligned} 0 \pmod{x} \\ 0 \pmod{x+1} \\ 1 \pmod{x^2+x} \end{aligned} \tag{6.1}$$

is a distinct covering system of $\mathbb{F}_2[x]$. To see that this is a distinct covering system it suffices by Theorem 5.4 to check only those elements of less degree than the least common multiple (lcm), i.e. $x^2 + x$. Each element of the set $\{0, 1, x, x+1\}$ satisfies at least one of the congruences in (6.1):

$$\begin{aligned} 0 &\equiv 0 \pmod{x} \\ 1 &\equiv 1 \pmod{x^2+x} \\ x &\equiv 0 \pmod{x} \\ x+1 &\equiv 0 \pmod{x+1}. \end{aligned}$$

We also see that:

$$\begin{aligned} 1 \pmod{x} \\ 1 \pmod{x+1} \\ 0 \pmod{x^2+x} \end{aligned} \tag{6.2}$$

is a distinct covering system, as the elements of $\mathbb{F}_2[x]$ of degree one or less satisfy at least

one of the congruences in (6.2):

$$\begin{aligned} 0 &\equiv 0 \pmod{x^2+x} \\ 1 &\equiv 1 \pmod{x} \\ x &\equiv 1 \pmod{x+1} \\ x+1 &\equiv 1 \pmod{x+1}. \end{aligned}$$

We notice that any congruence modulo a degree one polynomial covers exactly half of $\mathbb{F}_2[x]$, although there are some overlapping terms, and we observe that by using both of the degree one polynomials, we cover 75% of $\mathbb{F}_2[x]$. In essence, the degree one polynomials in $\mathbb{F}_2[x]$ "act like" the number 2 in the integers, and by using both, our solution is simplistic in nature. To refine the problem, we impose the additional restriction that we use only a single degree one polynomial from $\mathbb{F}_2[x]$. We claim that:

$$\begin{aligned} 0 &\pmod{x} \\ 1 &\pmod{x^2} \\ 1 &\pmod{x^2+x} \\ x+1 &\pmod{x^3+x^2} \end{aligned} \tag{6.3}$$

is a distinct covering system. Once again, by Theorem 5.4, it suffices to check that only those elements in $\mathbb{F}_2[x]$ of degree less than the degree of x^3+x^2, or 3, are covered. We observe that the elements of $\mathbb{F}_2[x]$ of degree two or less satisfy at least one of the

congruences in (6.3):

$$\begin{aligned} 0 &\equiv 0 \pmod{x} \\ 1 &\equiv 1 \pmod{x^2} \\ x &\equiv 0 \pmod{x} \\ x+1 &\equiv 1 \pmod{x^3+x^2} \\ x^2 &\equiv 0 \pmod{x} \\ x^2+1 &\equiv 1 \pmod{x^2} \\ x^2+x &\equiv 0 \pmod{x} \\ x^2+x+1 &\equiv 1 \pmod{x^2+x}. \end{aligned}$$

Additional distinct covering systems restricted to the use of only one degree one polynomial in $\mathbb{F}_2[x]$ such that x^3+x^2 is our lcm are as follows:

$$\begin{aligned} 0 &\pmod{x} \\ 1 &\pmod{x^2} \\ x+1 &\pmod{x^2+x} \\ x^2+x+1 &\pmod{x^3+x^2}, \end{aligned} \tag{6.4}$$

$$\begin{aligned} 1 &\pmod{x} \\ 0 &\pmod{x^2} \\ x &\pmod{x^2+x} \\ x^2+x &\pmod{x^3+x^2}, \end{aligned} \tag{6.5}$$

$$\begin{aligned} 1 &\pmod{x} \\ 0 &\pmod{x^2} \\ 0 &\pmod{x^2+x} \\ x &\pmod{x^3+x^2}, \end{aligned} \tag{6.6}$$

$$\begin{aligned} 0 &\pmod{x+1} \\ 1 &\pmod{x^2} \\ x &\pmod{x^2+x} \\ x^2+x+1 &\pmod{x^3+x^2}, \end{aligned} \tag{6.7}$$

$$\begin{aligned} 1 &\pmod{x+1} \\ x+1 &\pmod{x^2} \\ 0 &\pmod{x^2+x} \\ x^2+1 &\pmod{x^3+x^2}. \end{aligned} \tag{6.8}$$

We also find that the following are distinct covering systems in $\mathbb{F}_q[x]$ where we use

only one degree one polynomial and where our lcm is $x^3 + x$:

$$\begin{aligned} 0 &\pmod{x+1} \\ 1 &\pmod{x^2+1} \\ 1 &\pmod{x^2+x} \\ x &\pmod{x^3+x}, \end{aligned} \tag{6.9}$$

$$\begin{aligned} 0 &\pmod{x+1} \\ 1 &\pmod{x^2+1} \\ x &\pmod{x^2+x} \\ x^2+x+1 &\pmod{x^3+x}, \end{aligned} \tag{6.10}$$

$$\begin{aligned} 1 &\pmod{x+1} \\ 0 &\pmod{x^2+1} \\ 0 &\pmod{x^2+x} \\ x+1 &\pmod{x^3+x}, \end{aligned} \tag{6.11}$$

$$\begin{aligned} 1 &\pmod{x+1} \\ 0 &\pmod{x^2+1} \\ x+1 &\pmod{x^2+x} \\ x^2+x &\pmod{x^3+x}, \end{aligned} \tag{6.12}$$

$$\begin{aligned} 0 &\pmod{x} \\ x+1 &\pmod{x^2+1} \\ 1 &\pmod{x^2+x} \\ x^2+1 &\pmod{x^3+x}, \end{aligned} \tag{6.13}$$

$$\begin{aligned} 1 &\pmod{x} \\ 1 &\pmod{x^2+1} \\ 0 &\pmod{x^2+x} \\ x &\pmod{x^3+x}. \end{aligned} \tag{6.14}$$

We now impose the restriction that we are only allowed at most one degree one and at most one degree two polynomial in our attempt to discover a distinct cover. We consider

$x^2(x+1)^2$ as our lcm. We find that:

$$\begin{aligned} 0 &\pmod{x} \\ x+1 &\pmod{x^2} \\ x^2+1 &\pmod{x^3+x^2} \\ 1 &\pmod{x^3+x} \\ x^3+x^2+1 &\pmod{x^4+x^2} \end{aligned} \tag{6.15}$$

is a distinct covering system. It can be checked that all polynomials of degree less than or equal to three satisfy at least one of the six congruences in (6.15). We next ask the question, "Can we exhibit a distinct covering system of $\mathbb{F}_2[x]$ using at most one polynomial of each degree?" We claim no.

Lemma 6.1. *Let $0 < d \leq D$ be integers and $m(x) \in \mathbb{F}_2[x]$ of degree d. Then for any $a(x) \in \mathbb{F}_2[x]$, the residue class $a(x) \pmod{m(x)}$ covers exactly $\frac{2^D}{2^d}$ polynomials in $\mathbb{F}_2[x]$ of degree $< D$.*

Proof. Let $S_D = \{p(x) \in \mathbb{F}_2[x] : \deg p(x) < D, \text{ or } p(x) = 0\}$. Any $p(x) \in S_D$ is of the form $a_0 + a_1x + \cdots + a_{D-1}x^{D-1}$, and thus $|S_D| = 2^D$. Now, by the Division Algorithm for $\mathbb{F}_2[x]$ (Theorem 4.4), for every $p(x) \in S_D$, $p(x) \equiv a(x) \pmod{m(x)}$ if and only if $r_p(x) = r_a(x)$; where $r_f(x)$ denotes the remainder of $f(x)$ upon division by $m(x)$. Hence

$$|\{p(x) \in S_D : p(x) \equiv a(x) \pmod{m(x)}\}| = |\{p(x) \in S_D : r_p(x) = r_a(x)\}|$$

$$= |\{p(x) \in S_D : p(x) = m(x)q(x) + r_a(x) \text{ for some } q(x) \in \mathbb{F}_2[x] \text{ such that } \deg q(x) < D-d\}|$$

$$= |\{q(x) : \deg q(x) < D - d\}| = 2^{D-d}.$$

Therefore, for any $a(x) \in \mathbb{F}_2[x]$, the residue class $a(x) \pmod{m(x)}$ covers exactly $\frac{2^D}{2^d}$ polynomials in $\mathbb{F}_2[x]$ of degree $< D$.

□

Theorem 6.2. *There is no distinct covering system of $\mathbb{F}_2[x]$ using at most one polyno-*

mial of each degree ≥ 1.

Proof. Let $m_1(x), m_2(x), \ldots m_n(x) \in \mathbb{F}_2[x]$ be polynomials with distinct degrees and consider the system $\mathcal{C} = \{a_i(x) \pmod{m_i(x)}\}_{i=1}^n$. Our claim is that there exists some $f(x) \in \mathbb{F}_2[x]$ not covered by $\mathcal{C}$. We assume the contrary and suppose that every $f(x) \in \mathbb{F}_2[x]$ is covered by $\mathcal{C}$. Let $M(x) = \text{lcm}(\{m_i(x)\}_{i=1}^n)$. By Theorem 5.4, $\mathcal{C}$ covers $\mathbb{F}_2[x]$ if $\mathcal{C}$ covers every $f(x)$ with $\deg f(x) < \deg M(x) = D$. Let $S_D = \{f(x) \in \mathbb{F}_2[x] : \deg f(x) < D, \text{ or } f(x) = 0\}$ and $S_D^i = \{f(x) \in S_D : f(x) \equiv a_i(x) \pmod{m_i(x)}\}$. Thus $|S_D| = 2^D$ and, by Lemma 6.1, $|S_D^i| = 2^{D-d_i}$ where $d_i = \deg m_i(x)$. Hence

$$2^D = |S_D| \leq \sum_{i=1}^{n} |S_D^i| = \sum_{i=1}^{n} \frac{2^D}{2^{d_i}} = 2^D \sum_{i=1}^{n} \frac{1}{2^{d_i}} < 2^D \sum_{k=1}^{\infty} \frac{1}{2^k} = 2^D;$$

a contradiction. Therefore our claim holds, and there is no distinct covering of $\mathbb{F}_2[x]$ using at most one polynomial of each degree ≥ 1 .

□

Our results in $\mathbb{F}_2[x]$ have led us to the following conjecture analogous to Erdős' favorite problem (Conjecture 6.3):

Conjecture 6.3. *For any degree* $D > 0$*, there exists a distinct covering system*

$$\mathcal{C} = \{a_i(x) \pmod{m_i(x)}\}_{i=1}^k$$

for which $\deg m_i(x) \geq D$ *for each* $i = 1, 2, \ldots, k$.

In other words, there exist distinct covering systems of $\mathbb{F}_2[x]$ where the minimum degree of the moduli is arbitrarily large. We will now present a system of congruences which is a distinct covering system of $\mathbb{F}_2[x]$ where the minimum degree of the moduli is two. We choose $x^2(x+1)^2 = x^4+x^2$ as the least common multiple of our moduli. We make this choice to maximize the number of pairs of non-coprime moduli, thus maximizing the number of polynomials in $\mathbb{F}_2[x]$ which we can cover. The factors of $x^2(x+1)^2$ of degree

≥ 2 are $x^2,\ (x+1)^2,\ x(x+1),\ x(x+1)^2,\ x^2(x+1),$ and $x^2(x+1)^2$. We claim that:

$$\begin{aligned} 0 &\pmod{x^2} \\ x &\pmod{x^2+1} \\ x+1 &\pmod{x^2+x} \\ 1 &\pmod{x^3+x} \\ x^2+x &\pmod{x^3+x^2} \\ x^3+x^2+x &\pmod{x^4+x^2} \end{aligned} \tag{6.16}$$

is a distinct covering system of $\mathbb{F}_2[x]$. Recall, by Theorem 5.4, we need only check those elements of degree ≤ 3. We exhibit below that each element of the set

$$\{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1, x^3, x^3+1, x^3+x, \ldots \\ \ldots, x^3+x^2, x^3+x^2+1, x^3+x^2+x, x^3+x^2+x+1\}$$

satisfies at least one of the congruences in (6.16) since

$$\begin{aligned} 0,\ x^2,\ x^3,\ x^3+x^2 &\equiv 0 && \pmod{x^2}, \\ x,\ x^2+x+1,\ x^3,\ x^3+x^2+1 &\equiv x && \pmod{x^2+1}, \\ x+1,\ x^2+1,\ x^3+x^2+x+1,\ x^3+1 &\equiv x+1 && \pmod{x^2+x}, \\ 1,\ x^3+x+1 &\equiv 1 && \pmod{x^3+x}, \\ x^2+x,\ x^3+x &\equiv x^2+x && \pmod{x^3+x^2}, \text{ and} \\ x^3+x^2+x &\equiv x^3+x^2+x && \pmod{x^4+x^2}. \end{aligned}$$

Emulating Erdős and Selfridge, I offer \$3.00 for a disproof of Conjecture 6.3, Micah Milinovich offers \$5.00 for a proof, and Nathan Jones offers \$4.00 for either.

References

[1] M. A. Berger, A. Felzenbaum, and A. S. Fraenkel, *Necessary condition for the existence of an incongruent covering system with odd moduli II*, Acta Arith. 48 (1987), no. 1, 73-79. MR 893463 (88j:11002)

[2] S. L. G. Choi, *Covering the set of integers by congruence classes of distinct moduli*, Math. Comp. **25** (1971), 885-895. MR 0297692 (45 #6744)

[3] R. F. Churchhouse, *Covering sets and systems of congruences*, Computers in Mathematical Research, North-Holland, Amsterdam, 1968, pp. 20-36. MR 0240045 (39 #1399)

[4] P. Erdős, *On integers of the form* $2^k + p$ *and some related problem*, Summa Brasil. Math. **2** (1950), 113-123. MR 0044558 (13,437i)

[5] P. Erdős, *On some of my problems in number theory I would most like to see solved*, Number theory (Ootacamund, 1984), Lecture Notes in Math., vol. 1122, Springer, Berlin, 1985, pp. 74-84. MR797781

[6] D. J. Gibson, *A covering system with least modulus 25*, Math. Comp. **78** (2009), 1127-1146. MR2476575 (2010a:11019)

[7] GIMPS, *Great Internet Mersenne Prime Search*, `http://www.mersenne.org/`

[8] S. Guo and Z.-W. Sun, *On odd covering systems with distinct moduli*, Adv. in Appl. Math. **35** (2005), no. 2, 182187. MR2152886 (2006e:11018)

[9] R. K. Guy, *Unsolved problems in number theory*, Third Edition, Problem Books in Mathematics, Springer-Verlag, New York, 2004. MR2076335 (2005h:11003)

[10] C. E. Krukenberg, *Covering sets of the integers*, Ph.D. thesis, University of Illinois at Urbana-Champaign (1971).

[11] R. Morikawa, *On a method to construct covering sets*, Bull. Fac. Liberal Arts Nagasaki Univ. **22** (1981), no. 1, 1-11. MR 639636 (84i:10057)

[12] P. Nielsen, *A covering system whose smallest modulus is 40*, J. Number Theory,**129** (2009), no. 3, 640-666. MR2488595 (2010d:11014)

[13] C. Pomerance, *The covering congruences of Paul Erdős*, MAA Invited Address, Joint Math Meetings, San Diego, CA, January 8, 2008.

[14] Š. Porubský and J. Schönheim, *Covering systems of Paul Erdős. Past, present and future*, Paul Erdős and his mathematics, I (Budapest, 1999), Bolyai Soc. Math. Stud., vol. 11, János Bolyai Math. Soc., Budapest, 2002, pp. 581627. MR1954716 (2004d:11006)

VITA

Michael W. Azlin was born in Memphis, Tennessee. After completing his work at Southaven High School in Southaven, Mississippi in 1984, he served in the United States Navy from 1984 to 1990. He enrolled at Nortwest Mississippi Community College in Senatobia, Mississippi in 2004. He received an Associate of Arts degree in Mathematics and was elected to the school's Hall of Fame in May, 2007. In the fall of 2007, he entered the University of Mississippi. He received the degree of Bachelor of Science, *cum laude*, in Mathematics in May, 2009. In August, 2009, he entered the Graduate School at the University of Missisippi.