4-18-2007

Irreducible Polynomials and Factorization Properties of the Ring of Integer-Valued Polynomials

Megan Gallant
Trinity University

Irreducible Polynomials and Factorization Properties of the Ring of Integer-Valued Polynomials

Megan Gallant

A DEPARTMENTAL HONORS THESIS SUBMITTED TO THE
DEPARTMENT OF MATHEMATICS AT TRINITY UNIVERSITY
IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR GRADUATION WITH
DEPARTMENTAL HONORS

18 April 2007

THESIS ADVISOR

DEPARTMENTAL CHAIR

ASSOCIATE VICE PRESIDENT FOR
ACADEMIC AFFAIRS:
CURRICULUM AND STUDENT ISSUES

Contents

Chapter 1

Introduction

1.1 Definitions

The ring of integer-valued polynomials, denoted $\mathrm{Int}(\mathbb{Z})$, is the set of polynomials $f(x)$ in $\mathbb{Q}[x]$ such that $f(z) \in \mathbb{Z}$ for all $z \in \mathbb{Z}$:

$$\mathrm{Int}(\mathbb{Z}) = \{f(x) \in \mathbb{Q}[x] | f(z) \in \mathbb{Z}, \forall z \in \mathbb{Z}\}.$$

Notice that we get the following: $\mathbb{Z}[x] \subseteq \mathrm{Int}(\mathbb{Z}) \subseteq \mathbb{Q}[x]$. But while $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$ are unique factorization domains, $\mathrm{Int}(\mathbb{Z})$ is not.

Example 1.1. The product

$$x(x-1)(x-2) = 3 \cdot 2\Big(\frac{x(x-1)(x-2)}{3!}\Big)$$

represents 2 factorizations of the polynomial $g(x) = x^3 - 3x^2 + 2x$ into irreducible elements. From Cahen and Chabert [2, Corollary VI.3.5] we know that $\frac{x(x-1)\ldots(x-n+1)}{n!}$ is irreducible for every $n \geq 1$. Also, notice that a first degree polynomial with content 1 over $\mathbb{Z}$ is irreducible. That is, let $ax + b \in \mathbb{Z}[x]$ where $\gcd(a, b) = 1$. If $ax + b = u(x)v(x)$ for some $u(x), v(x) \in \mathbb{Z}[x]$ then we know that one of $u(x)$ or $v(x)$ has degree 1 and the other one has degree 0. Because if not, then the content would be greater than 1. So, a first degree polynomial in $\mathbb{Z}[x]$ with content=1 is irreducible in $\mathrm{Int}(\mathbb{Z})$.

Notice that $3!|x(x-1)(x-2)$ in Int($\mathbb{Z}$) because $\binom{x}{3}$ is integer-valued for every $x \in \mathbb{Z}$.

Definition 1.2. Let $f(x) = \sum_{i=0}^{n} a_i x^i \in \mathbb{Z}[x]$, where $a_i \in \mathbb{Z}$ and $a_n \neq 0$. The **content** of $f(x)$, denoted $c(f)$, is

$$c(f) = \gcd(a_0, a_1, ..., a_n).$$

We call $f(x)$ **primitive** over $\mathbb{Z}[x]$ if $c(f) = 1$.

Definition 1.3. Let $f(x) \in \text{Int}(\mathbb{Z})$. The **fixed divisor** of f in Int($\mathbb{Z}$), denoted $d(\mathbb{Z}, f)$ is

$$d(\mathbb{Z}, f) = \gcd\{f(z) : z \in \mathbb{Z}\}.$$

If $d(\mathbb{Z}, f) = 1$, then we call $f(x)$ **image primitive** over $\mathbb{Z}$.

Example 1.4. The polynomial

$$g(x) = \frac{x(x-1)(x-2)}{3!}$$

is image primitive over $\mathbb{Z}$ because $f(3) = 1$. Also notice that for the polynomial in the numerator $h(x) = x(x-1)(x-2)$, we have that $d(\mathbb{Z}, h) = 3!$.

Definition 1.5. Let $f(x) \in \text{Int}(\mathbb{Z})$. The **set of lengths of factorizations** of $f(x)$ into irreducible elements, denoted $\mathcal{L}(f(x))$, is

$$\mathcal{L}(f(x)) = \{m | f(x) = f_1(x)...f_m(x), f_i(x) \text{ is irreducible in Int}(\mathbb{Z})\}.$$

Example 1.6. From Example 1.1 the polynomial $g(x) = x^3 - 3x^2 + 2x$ can be factored into irreducibles as

$$x(x-1)(x-2) = 3 \cdot 2\Big(\frac{x(x-1)(x-2)}{3!}\Big).$$

Now, the factorization on the left has length 3, and the factorization on the right has length 3. The following also represents irreducible factorizations of $g(x)$ of length 3:

$$g(x) = 2\left(\frac{x(x-1)}{2}\right)(x-2),$$

$$g(x) = x \cdot 2\left(\frac{(x-1)(x-2)}{2}\right).$$

We claim these are the only irreducible factorizations of $g(x)$, so that $\mathcal{L}(g(x)) = \{3\}$.

Even though we have not discussed the properties of irreducibles in Int($\mathbb{Z}$) yet, a sketch of the argument is useful in beginning to understand the properties of Int($\mathbb{Z}$). Notice that if $h(x) = \frac{x(x-1)(x-2)}{z} \in \text{Int}(\mathbb{Z})$ where z is an integer, then $z \leq 3!$ by the results in the next section. If $z = 3$, then since $2|x(x-1)$ in Int($\mathbb{Z}$) the fraction is not irreducible. That is $h(x) = 2\left(\frac{x(x-1)(x-3)}{2\cdot 3}\right)$. By similar reasoning if $z = 2$ the fraction is not irreducible. So we get that $z = 3!$ which gives us a factorization already considered. Now all combinations that consider an irreducible polynomial of degree 2 multiplied by degree 1 have already been considered. Thus, $\mathcal{L}(g(x)) = \{3\}$.

1.2 Binomial Polynomials Form a Free Basis

For each positive integer n, let

$$B_n(x) = \frac{x(x-1)...(x-(n-1))}{n!} = \binom{x}{n}$$

Theorem 1.7. *Let $f(x) \in \text{Int}(\mathbb{Z})$ of degree n. Then, there exists unique integers $r_0, ..., r_n$ such that*

$$f(x) = r_0B_0(x) + r_1B_1(x) + ... + r_nB_n(x).$$

Proof. We will show this by induction on n. Let $f(x) \in \text{Int}(\mathbb{Z})$ be of degree 1. Then, $f(x) = ax + b$ for some $a, b \in \mathbb{Q}$. Now $f(x) \in \mathbb{Z}$ for every $x \in \mathbb{Z}$, so $f(0) = b \in \mathbb{Z}$. Then, $ax = c - b \in \mathbb{Z}$ so a must be an integer also. Then,

$$f(x) = a\binom{x}{1} + b\binom{x}{0}.$$

Now, let $f(x) \in \text{Int}(\mathbb{Z})$ be of degree $m+1$ and let the statement be true for all degree m polynomials. Now we can find a polynomial $h(x) \in \text{Int}(\mathbb{Z})$ where $\deg(h(x)) = m$ and $h(0) = f(0), ..., h(m) = f(m)$. Then by the induction hypothesis, $h(x) = \sum_{i=0}^{m} r_i\binom{x}{i}$ where $r_i \in \mathbb{Z}$ for every i. Now form a new polynomial, $g(x)$ of degree $m+1$ where $g(x) = h(x) + r_{m+1}\binom{x}{m+1}$ and $r_{m+1} = f(m+1) - h(m+1) \in \mathbb{Z}$. Now, $g(0) = f(0)$,...,$g(m) = f(m)$ since $\binom{x}{m+1} = 0$

when $0 \leq x \leq m$. Also, $g(m+1) = f(m+1)$ by construction. Thus we get that $g(x) = f(x)$ and,

$$f(x) = r_0 \binom{x}{0} + ... + r_m \binom{n}{m} + r_{m+1} \binom{x}{m+1}.$$

□

So every polynomial in Int($\mathbb{Z}$) can be written as a unique linear combination of the Binomial Polynomials. Now, given a polynomial $f(x) \in \text{Int}(\mathbb{Z})$, C. Long [7] outlines a method to determine its unique linear combination:

$$f(x) = f_0 \binom{x}{0} + ... + f_1 \binom{x}{n}$$

where $f_i \in \mathbb{Z}$ and $f_n \neq 0$. It is called the **"Difference Table Construction"**. Let $f(x) \in \text{Int}(\mathbb{Z})$ of degree n. We are going to set up the following "difference table".

$f(0) = D^0(0)$	$f(1) = D^1(0)$	...	$f(n-1)$	$f(n)$
$f(1) - f(0) = D^1(0)$	$f(2) - f(1) = D^1(1)$	...	$D^{n-1}(n-1)$	-
$f(2) - 2f(1) + f(0) = D^1(1) - D^1(0) = D^2(0)$	$D^1(2) - D^1(1) = D^2(1)$	...	-	-
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$D^n(0)$	-	...	-	-

Where the entry in rth row and cth column is denoted $D^r(c)$. In general we have,

$$D^r(c) = D^{r-1}(c+1) - D^{r-1}(c).$$

Given the entries in the table, we get that

$$f(x) = D^0(0)\binom{x}{0} + D^1(0)\binom{x}{1} + ... + D^n(0)\binom{x}{n}.$$

Example 1.8. Let $f(x) = x^2 + 2x + 7$. The difference table is:

$f(0) = 7$	$f(1) = 10$	$f(2) = 15$
3	5	-
2	-	-

Which gives us that

$$f(x) = 7\binom{x}{0} + 3\binom{x}{1} + 2\binom{x}{2}$$
$$= 7 + 3x + 2\left(\frac{x(x-1)}{2}\right) = x^2 + 2x + 7.$$

1.3 Basic Properties

Here we present some basic facts properties about $\mathrm{Int}(\mathbb{Z})$. We will use many of these later on. We leave many of the proofs to the references provided.

First, notice that the difference table construction produces the following result.

Corollary 1.9. *Let $f(x) \in \mathbb{Q}[x]$ have degree n. If $f(0), f(1), ..., f(n) \in \mathbb{Z}$, then $f(x) \in \mathrm{Int}(\mathbb{Z})$.*

Since the binomial polynomials form a basis for $\mathrm{Int}(\mathbb{Z})$, it only makes sense that they would be irreducible in $\mathrm{Int}(\mathbb{Z})$.

Lemma 1.10. [2, Corollary VI.3.5] *For $n > 0$, every $B_n(x)$ is irreducible in $\mathrm{Int}(\mathbb{Z})$.*

From Gauss' Lemma, the content behaves nicely in $\mathrm{Int}(\mathbb{Z})$. That is, given two polynomials $f(x), g(x) \in \mathrm{Int}(\mathbb{Z})$, we have that $c(fg) = c(f)c(g)$. But the fixed divisor does not behave as nicely. In general, $d(\mathbb{Z}, fg) \neq d(\mathbb{Z}, f)d(\mathbb{Z}, g)$, but we can say the following.

Lemma 1.11. [3, Lemma 2.2] *Let $f(x) \in \mathrm{Int}(\mathbb{Z})$ be non-zero. Suppose $f_1(x)...f_k(x) \in \mathrm{Int}(\mathbb{Z})$ are non-zero with*

$$f(x) = f_1(x)...f_k(x)$$

then

1) $d(\mathbb{Z}, f_1) \cdots d(\mathbb{Z}, f_k) | d(\mathbb{Z}, f)$,

2) *if $f_1(x) = f_2(x) = ... = f_k(x)$, then $d(\mathbb{Z}, f) = d(\mathbb{Z}, (f_1)^k) = (d(\mathbb{Z}, f_1))^k$.*

Also, by knowing what the unique binomial expression is for a function in $\mathrm{Int}(\mathbb{Z})$, then we can determine the fixed divisor for that function.

Lemma 1.12. [3, Lemma 2.5] *Let $f(x) \in \mathrm{Int}(\mathbb{Z})$ have degree n, so that $f(x) = f_0 + f_1\binom{x}{1} + ... + f_n\binom{x}{n}$, where $f_i \in \mathbb{Z}$ and $f_n \neq 0$. Then*

$$d(\mathbb{Z}, f) = \gcd(f(0), f(1), ..., f(n)) = \gcd(f_0, f_1, ..., f_n).$$

The most useful application of this lemma is that by knowing the binomial expansion of a polynomial in $\mathrm{Int}(\mathbb{Z})$, then we can find its fixed divisor by taking the greatest common divisor of the binomial coefficients. Given a polynomial, knowing how to find its fixed divisor is very important. That is because the fixed divisor plays a key role in determining the irreducibility of an element in Int($\mathbb{Z}$).

Theorem 1.13. [3, Theorem 2.8] *Let $f(x)$ be a nonconstant primitive polynomial in $\mathbb{Z}[x]$. The following statements are equivalent.*

a) $\frac{f(x)}{d(\mathbb{Z},f)}$ *is irreducible in Int($\mathbb{Z}$).*

b) *Either $f(x)$ is irreducible in $\mathbb{Z}[x]$ or for every pair of nonconstant polynomials $f_1(x), f_2(x)$ in $\mathbb{Z}[x]$ with $f(x) = f_1(x)f_2(x)$, $d(\mathbb{Z}, f)) \nmid d(\mathbb{Z}, f_1)d(\mathbb{Z}, f_2)$.*

From [3, Lemma 2.7], it is known that every image primitive polynomial $f(x) \in \text{Int}(\mathbb{Z})$ can be expressed uniquely (up to associates) as

$$f(x) = \frac{f^*(x)}{n} \tag{1.1}$$

where $f^*(x) \in \mathbb{Z}[x]$ and $n \in \mathbb{Z}$. It is also known that $f(x) \in \mathbb{Z}[x]$ is irreducible in Int($\mathbb{Z}$) if and only if $f(x)$ is irreducible and image primitive in $\mathbb{Z}[x]$. So using these facts, Theorem 1.13 and [2] we can characterize the irreducibles of Int($\mathbb{Z}$).

Corollary 1.14. [3, Corollary 2.9] *Let $f(x)$ be a nonunit in* Int($\mathbb{Z}$)*. $f(x)$ is irreducible in* Int($\mathbb{Z}$) *if and only if*

1) $\deg(f(x)) = 0$ *and $f(x)$ is a prime integer.*

2) $\deg(f(x)) > 0$*, $f(x)$ is image primitive in* Int($\mathbb{Z}$)*, and when expressed in the form of* (1.1) *either*

- *$f^*(x)$ is irreducible in $\mathbb{Z}[x]$ and $n = d(\mathbb{Z}, f^*)$, or*
- *$n = d(\mathbb{Z}, f^*)$ and for every factorization $f^*(x) = f_1(x)f_2(x)$ into non-units of $\mathbb{Z}[x]$, $n \nmid d(\mathbb{Z}, f_1^*)d(\mathbb{Z}, f_2^*)$.*

While Int($\mathbb{Z}$) is not a unique factorization domain, there are elements in Int($\mathbb{Z}$) that have unique factorization.

Theorem 1.15. [3, Theorem 3.1] *Let $f(x) \in \mathbb{Z}[x]$ be of degree $d \geq 1$. If $f(x)$ is image primitive, then $f(x)$ factors uniquely as a product of irreducible elements of Int($\mathbb{Z}$).*

One way to explore the degree of non-unique factorization in Int($\mathbb{Z}$) is to consider the elasticity of polynomials in Int($\mathbb{Z}$) and the elasticity of Int($\mathbb{Z}$) itself.

Definition 1.16. Let $f(x) \in \text{Int}(\mathbb{Z})$. The **elasticity of** $f(x)$, denoted $\rho(f(x))$, is

$$\rho(f(x)) = \frac{\max \mathcal{L}(f(x))}{\min \mathcal{L}(f(x))}.$$

Now, $\rho(f(x))$ describes the character of non-unique factorizations of one polynomial. We can extend ρ to describe the global character of Int($\mathbb{Z}$).

Definition 1.17. The **elasticity of Int**($\mathbb{Z}$), denoted $\rho(\text{Int}(\mathbb{Z}))$, is

$$\rho(\text{Int}(\mathbb{Z})) = \sup\{\rho(f(x)) | f(x) \in \text{Int}(\mathbb{Z})\}.$$

Since n can be chosen to have as many prime factors as desired, notice the following shows that $\rho(\text{Int}(\mathbb{Z})) = \infty$:

$$n\binom{x}{n} = \binom{x}{n-1}(x-(n-1)).$$

Besides elasticity, there is another way to measure the global character of non-unique factorization in Int($\mathbb{Z}$). For a polynomial in Int($\mathbb{Z}$) we consider the differences between consecutive factorization lengths.

Definition 1.18. Let $f(x) \in \text{Int}(\mathbb{Z})$ and order the elements of $\mathcal{L}(f(x)) = \{m_1, ..., m_k\}$ where $m_1 < ... < m_k$. The **delta set of** $f(x)$, denoted $\Delta(f(x))$, is

$$\Delta(f(x)) = \{n : (m_i - m_{i-1}) = n, 2 \leq i \leq k\}.$$

Definition 1.19. Let $\text{Int}(\mathbb{Z})^\bullet$ denote the subset of Int($\mathbb{Z}$) consisting of the nonzero nonunit elements of Int($\mathbb{Z}$). The **delta set of Int**($\mathbb{Z}$), denoted $\Delta(\text{Int}(\mathbb{Z}))$, is

$$\bigcup_{f(x) \in \text{Int}(\mathbb{Z})^\bullet} \Delta(f(x)).$$

So, $\Delta(\text{Int}(\mathbb{Z}))$ contains the magnitude of differences between consecutive factorization lengths of all integer-valued polynomials. In [3, Lemma 4.3] Chapman and McClain showed that $p-2 \in \Delta(\text{Int}(\mathbb{Z}))$ for every prime p. We show in Chapter 4 that $\Delta(\text{Int}(\mathbb{Z})) = \mathbb{N}$. That is, we can find a polynomial in $\text{Int}(\mathbb{Z})$ for every natural number n such that a difference between consecutive lengths of factorizations of that polynomial is n.

Before that, in Chapter 2 we briefly explore another measure of non-unique factorization in $\text{Int}(\mathbb{Z})$, the Omega Function. And in Chapter 3 we discuss properties of some polynomials in $\text{Int}(\mathbb{Z})$ that are formed from complete and incomplete sets of residues.

Chapter 2

The Omega Function

An interesting way to look at division and irreducible properties of an element in Int($\mathbb{Z}$) is to look at the omega function of an element. Let H be an atomic monoid and $u \in H$. The omega function of u with respect to H, denoted $\omega(H, u)$, is the smallest N such that whenever u divides a product of n things say $u|a_1...a_n$ then u divides a sub product of N factors say

$$u| \prod_{\imath \in \Omega} a_i, \qquad |\Omega| \leq N.$$

We start with an observation about the omega function.

Proposition 2.1. *Let H be an atomic monoid and p be a prime element in H. Then,* $\Omega(H, p) = 1$.

Proof. Let $p|a_1a_2...a_n$ where $a_i \in H$ for all i. If $p|a_1$ then we are done. If not, then because p is prime we know that $p|a_2...a_n$. Now, if $p|a_2$ then we are done. If not, then $p|a_3...a_n$. We can continue this process until we find $p|a_i$ for some $1 \leq i \leq n$. Thus, $\omega(H, p) = 1$. □

Hence, the Omega Function can be considered a measure of how far away an element is to being prime. In Int($\mathbb{Z}$), there are no prime elements. That is, there does not exist any element n such that when $n|ab$ we have that $n|a$ or $a|b$. Because there are no prime elements in Int($\mathbb{Z}$), studying the omega function of elements in Int($\mathbb{Z}$) yields interesting results. An exhaustive study of the omega function in other settings can be found in [4].

Lemma 2.2. *Suppose $p \nmid a$ where $f(x) = ax + b$. Then there exists a unique i with $0 \leq i < p$ where $p|f(i)$ and $p \nmid f(j)$ for $0 \leq j < p$ and $i \neq j$.*

Proof. Consider the set $F = \{f(0), f(1), ..., f(p-1)\}$. If $f(i) = f(j)$ for some i, j, then

$$ai + b \equiv aj + b \pmod p$$

$$ai \equiv aj \pmod p$$

$$i \equiv j \pmod p$$

since $gcd(a, p) = 1$. Thus, there is only one element in F for each residue class mod p. Since $|F| = p$, then F forms a complete set of residues modulo p and there exists a unique i with $0 \leq i < p$ for every x such that $p|f(i)$ and $p \nmid f(j)$ where $i \neq j$. □

Lemma 2.3. *Suppose $p \nmid b$ where $f(x) = ax + b$ and $p|a$. Then, $p \nmid f(x)$ for every x.*

Proof. let $p \nmid b$ and $p|a$. Then, $ax + b \equiv 0 + b \equiv b \pmod p$. Now $b \not\equiv 0 \pmod p$, thus $p|f(x)$ for ever x. □

Proposition 2.4. *Let $p \in \mathbb{Z}$ be a prime integer. Then, $\omega(Int(\mathbb{Z}), p) \geq p$.*

Proof. In $Int(\mathbb{Z})$, $p|x(x-1)...(x-p+1)$. But, since $\mathcal{I} = \{0, ..., p-1\}$ is a complete set of residues modulo p, $p \nmid \prod_{i \in \Omega}(x - i)$ where $\Omega \subset \mathcal{I}$ and $|\Omega| < p$. Thus, $\omega(Int(\mathbb{Z}), p) \geq p$. □

Proposition 2.5. *Let $f_k(x) = \binom{x-k}{n} + \binom{x-k}{n-1} + ... + \binom{x-k}{1} + \binom{x-k}{0}$. Then, $f_k(x)$ is irreducible in $Int(\mathbb{Z})$.*

Proof. Notice that $f_0(x) = \binom{x}{n} + ... + \binom{x}{0}$ is irreducible in $Int(\mathbb{Z})$ by Anderson, Cahen, Chapman and Smith [1, Corollary 2.2] because $a_n = 1$.

Let $k \in \mathbb{Z}$ and $k \geq 0$. Now if $f_k(x)$ is not irreducible, then it can be written as a product of two polynomials $s(x), r(x) \in Int(\mathbb{Z})$. So, $f_k(x) = s(x)r(x)$. Now, $f_k(x-k) = \binom{x}{n} + ... + \binom{x}{0} = s(x)r(x)$ which is a contradiction since $\binom{x}{n} + ... + \binom{x}{0}$ is irreducible by above. Thus, $f_k(x)$ is irreducible in $Int(\mathbb{Z})$. □

Proposition 2.6. $\omega(Int(\mathbb{Z}), 2) = \infty$.

Proof. Pick $k \in \mathbb{N}$. Let $2|f_0(x)...f_k(x)$. From above, $f_0(x), ..., f_k(x)$ are all irreducible polynomials in $Int(\mathbb{Z})$. Now consider the values of the polynomials $f_0(x), .., f_k(x)$ modulo 2 from 0 to k. It is displayed in the following table:

x	$f_0(x)$	$f_1(x)$	$f_2(x)$	$f_3(x)$	...	$f_k(x)$
0	1	0	0	0	...	0
1	0	1	0	0		0
2	0	0	1	0		0
3	0	0	0	1		0
⋮					⋮	
k	0	0	0	0	...	1

Notice that when $k = 0, ..., k$ then there is only 1 irreducible polynomial from $f_0(x), .., f_k(x)$ that is in the residue class equivalent to 1 modulo 2. So, in order for 2 to divide the whole product $f_0(x), ..., f_k(x)$ must form a complete set of residues modulo 2. So we could not remove any of the polynomials because then we would get an incomplete set of residues at some value of x. Thus, there is no smaller subgroup of irreducible polynomials that 2 divides from $f_0(x)...f_k(x)$. Now, the same thing can be done for $k+1, k+2, ...$ and so on. Thus, there exists a larger group of irreducibles that 2 would divide given any number of irreducible elements that 2 divides. Thus, $\omega(Int(\mathbb{Z}), 2) = \infty$. □

Chapter 3

Complete and Incomplete Sets of Residues from the Images of Polynomials

Chapman and McClain[3, Proposition 3.4] showed that given a prime p, there exists a set $\mathcal{I} = \{i_1, i_2, ..., i_t\}$ of integers such that the polynomial

$$f_p(x) = \frac{(x - i_1)(x - i_2)...(x - i_t)}{p}$$

is irreducible in $\mathrm{Int}(\mathbb{Z})$. The set $\mathcal{I}$ was found by using the Chinese Remainder Theorem. That is, we want to find a set of integers $\mathcal{I}$ that form a complete set of residues modulo the prime p, and that form an incomplete set of residues modulo every prime $q \neq p$. This can be done by setting up p systems of linear congruences.

We extend the idea behind this by considering different conditions on the set $\mathcal{I}$, and the polynomials formed by $(x - i_1)(x - i_2)...(x - i_t)$.

Proposition 3.1. *Let $\mathcal{I} = \{i_0, ..., i_{n-1}\}$ form a complete set of residues modulo the composite integer m, then $\mathcal{I}$ forms a complete set of residues modulo p where p is any prime divisor of m.*

Proof. Let $\mathcal{I} = \{i_0, i_1, ..., i_{m-2}, i_{m-1}\}$ form a complete set of residues modulo the integer $m = q_1^{r_1} q_2^{r_2} ... q_t^{r_t}$ where $q_1, q_2, ..., q_r$ are distinct primes and $r_1, r_2, ..., r_t \in \mathbb{N}$ and m is not prime.

Since $\mathcal{I}$ forms a complete set of residues modulo m, without loss of generality let $(x - i_j) \equiv j \pmod{m}$.

Consider the prime divisor q_k.

Now for $j < q_k$ consider $x - i_j \equiv j \pmod{m}$, so $x - i_j - j = mh_1 = (q_1^{r_1} q_2^{r_2} ... q_t^{r_t})h_1$ for some $h_1 \in \mathbb{Z}$. Thus, $q_k | (x - i_j) - j$ and $x - i_j \equiv j \pmod{q_k}$. Now $x - i_{j+q_k} \equiv j + q_k \pmod{q_k}$. So $x - i_{j+q_k} = mh_2 + j + q_k = (q_1^{r_1} q_2^{r_2} ... q_t^{r_t})h_2 + j + q_k$ for some $h_2 \in \mathbb{Z}$ and thus $q_k | (x - i_{j+q_k}) - j$. So, $x - i_j \equiv x - i_{j+q_k} \equiv j \pmod{q_k}$. This can be done with each subsequent multiple of q_k to show that $x - i_j \equiv x - i_{q_k+j} \equiv x - i_{2q_k+j} \equiv ... \equiv x - i_{m-q_k+j} \equiv j \pmod{q_k}$. Now there are q_k different $j's$, so the set $\{x - i_0, x - i_1, ..., x - i_{q_k-1}\}$ forms a complete residue class modulo q_k. So there exists a complete set of residues modulo every prime divisor of m. □

Corollary 3.2. *Let $\mathcal{I} = \{i_0, i_1, ..., i_{m-1}\}$ form a complete set of residues modulo the composite integer m. The polynomial*

$$f_m(x) = \frac{(x - i_0)(x - i_1)...(x - i_{m-1})}{m}$$

is reducible in $Int(\mathbb{Z})$.

Proof. Let the composite integer $m = q_1^{r_1} q_2^{r_2} ... q_t^{r_t}$ where $q_1, q_2, ..., q_r$ are distinct primes and $r_1, r_2, ..., r_t \in \mathbb{N}$. Now consider the smallest prime divisor of m, which without loss of generality is q_1. Let $k = \frac{m}{q_1} = q_1^{r_1-1} q_2^{r_2} ... q_t^{r_t}$. From the proof of Proposition 3.1 we can partition $\mathcal{I}$ into k distinct sets that form a complete set of residues modulo q_1. Now the set $\mathcal{I}' = \{i_{q_1}, i_{q_1+1}, ..., i_{m-1}\} = \mathcal{I} - \{i_0, ..., i_{q_1-1}\}$ must have $k - 1$ distinct sets that form a complete set of residues modulo r_1. Notice that $\mathcal{I}'$ is the set $\mathcal{I}$ minus 1 complete set of residues modulo q_1. Now notice that $r_1 \leq k = \frac{m}{q_1}$, because if $r_1 > \frac{m}{q_1}$ then $q_1 r_1 > m = q_1^{r_1} ... q_t^{r_t}$ which is a contradiction. So because $r_1 - 1 \leq k - 1$, $\mathcal{I}'$ forms a complete set of residues modulo $q_1^{r_1-1}$.

Now consider $q_j \neq q_1$. Once again by Proposition 3.1, we know that we can partition $\mathcal{I}$ into $k' = \frac{m}{q_j}$ distinct sets that form a complete set of residues modulo q_j. So the set $\mathcal{I}'$ can be partitioned into $k' - 1$ complete sets of residues modulo q_j since q_1 is the smallest prime divisor of m. Once again, notice that $r_j < \frac{m}{q_j} = k'$, because if $r_j \geq \frac{m}{q_j}$ then $q_j r_1 \geq m =$ which can't happen because $q_j \neq 2$. So because $r_j \leq k' - 1$ we have that the set $\mathcal{I}'$ forms a complete set of residues modulo $q_j^{r_j}$.

So, we can factor $f_m(x)$ as

$$f_m(x) = \left(\frac{(x - i_0)...(x - i_{q_1-1})}{q_1} \right) \left(\frac{(x - i_{q_1})...(x - i_{m-1})}{k} \right)$$

where the fraction on the left is irreducible by [3, Proposition 3.4]. Thus, $f_m(x)$ is reducible.

□

3.1 Complete and Incomplete Sets of Residues

Let $q_1 \leq q_2 \leq ... \leq q_k$ be primes, and $\mathbb{Q} = \{q_1, q_2, ..., q_k\}$. Since the primes in $\mathbb{Q}$ aren't necessarily distinct, let $\mathcal{W}$ denote the set of distinct primes from $\mathbb{Q}$. $\mathcal{W}$ is ordered so that $w_1 < w_2 < ... < w_t$. Now let p be a prime such that $p > w_1 + ... + w_t$. We will assume throughout section 3.1 that p is always greater than the sum of the distinct primes in $\mathcal{W}$. Now let $\mathcal{S}$ denote the set of primes less than p that are not in $\mathcal{W}$. Finally, let $\mathcal{I} = \{i_0, i_1, ..., i_{p-1}\}$ be a set of integers where $|\mathcal{I}| = p$. In the case that $\mathcal{I}$ forms a complete set of residues modulo any prime q_j or w_j we denote such a subset as Q_j or W_j.

Definition 3.3. A set $\mathcal{I}$ is **firm** for the prime p ($p > w_1 + ... + w_t$) and for the set of primes $\mathcal{Q}$ if:

1) $\mathcal{I}$ does not form a complete set of residues modulo p.

2) $\mathcal{I}$ forms a complete set of residues modulo w_i $\forall i$ where $w_i \in \mathcal{W}$.

3) $\mathcal{I}$ fails to form a complete set of residues modulo s_i $\forall i$ where $s_i \in \mathcal{S}$.

Firm sets can be constructed using p systems of linear congruences and the Chinese Remainder Theorem. We prove this and then give an example.

Proposition 3.4. *Given a set of primes $\mathbb{Q}$ and a prime p it is possible to construct a firm set $\mathcal{I}$.*

Proof. We need to construct p systems of linear congruences with solutions $x_0, x_1, ..., x_{p-1}$ as follows:

- For all i, $x_i \equiv 1 \pmod{p}$.
- For all i and all j, $x_i \equiv 1 \pmod{s_j}$.
- For all j and $0 \leq i \leq w_j - 1$, $x_i \equiv i \pmod{w_j}$.
- For all j and $w_j \leq i \leq p-1$, $x_i \equiv 1 \pmod{w_j}$.

This can be seen in a matrix form. Every row of the matrix refers to all linear congruences modulo the same prime. We will have a row for every prime less than or equal to p. Every column of the matrix refers to 1 system of linear congruences. To compute the $\mathcal{I}$ set, we use the Chinese Remainder Theorem p times, once for each column of the matrix.

Entry $c = (r, x_a)$, where r is a prime p, s_i or w_i, corresponds to the desired solution of the linear congruence $x_a \equiv c \pmod{r}$. The entry refers to the desired solution for the system of linear congruences whose column it is in modulo the prime whose row it is in.

	x_0	x_1	x_2	...	$w_1 - 1$	w_1	...	$w_{t-1} - 1$	w_{t-1}	...	$w_t - 1$	w_t	...	x_{p-1}
p	1	1	1	...	1	1	...	1	1	...	1	1	...	1
w_t	0	1	2	...	$w_1 - 1$	w_1	...	$w_{t-1} - 1$	w_{t-1}	...	$w_t - 1$	1	...	1
w_{t-1}	0	1	2	...	$w_1 - 1$	w_1	...	$w_{t-1} - 1$	1	...	1	1	...	1
$\vdots$				$\vdots$						$\vdots$			$\vdots$	
w_1	0	1	2	...	$w_1 - 1$	1	...	1	1	...	1	1	...	1
s_j	1	1	1	...	1	1	...	1	1	...	1	1	...	1

Since every solution to the systems of congruences is congruent to 1 modulo p, it is not possible for $\mathcal{I}$ to form a complete set of residues modulo p. Similarly, since every solution to the systems of congruences is congruent to 1 modulo s_i, $\forall\ s_i \in \mathcal{S}$, it is not possible for $\mathcal{I}$ to form a complete set of residues for any $s_i \in \mathcal{S}$.

Finally, notice that the first w_i solutions to the systems of congruences forms a complete set of residues modulo w_i, $\forall\ w_i \in \mathcal{W}$, so we have constructed a firm set. □

Example 3.5. Consider $\mathcal{Q} = \{3, 5, 7\}$ and $p = 17$.

$$\mathcal{I}_F = \{398685, 1, 11827, 393823, 335479, 72931, 218791, 510511, 1021021, 10531531,$$
$$2042041, 2552551, 3063061, 3573571, 4084081, 4594591, 5105101\}$$

is a firm set. This can be found by setting up the following 17 systems of linear congruences:

	x_0	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	x_{10}	x_{11}	x_{12}	x_{13}	x_{14}	x_{15}	x_{16}
17	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
13	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
11	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
7	0	1	2	3	4	5	6	1	1	1	1	1	1	1	1	1	1
5	0	1	2	3	4	1	1	1	1	1	1	1	1	1	1	1	1
3	0	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

There are many more ways to construct firm sets as mentioned above. The next set we construct is a specific type of Firm set. In this construction, we utilize the fact that $p > w_1 + ...w_t$.

Definition 3.6. A set $\mathcal{I}$ is **completely firm** for a prime p ($p > w_1 + ... + w_t$) and for the set of primes $\mathcal{Q}$ if:

1) $\mathcal{I}$ is firm.

2) Every subset in $\mathcal{I}$ of w_j elements that forms a complete set of residues modulo w_j fails to form a complete set of residues modulo w_i for every $i < j$.

3) There exists a complete set of residues modulo w_i in the subset $\mathcal{I} - \mathcal{W}_j$ for all $i \neq j$.

4) There does not exist a complete set of residues modulo w_i in the subset $\mathcal{I} - \mathcal{W}_i$ for all i.

Once again, to construct a completely firm set we need to use p systems of linear congruences and then utilize the Chinese Remainder Theorem. We prove the existence of such sets and then give an example.

Proposition 3.7. *Given a set of primes $\mathbb{Q}$ and a prime $p > w_1 + ... + w_t$ it is possible to construct a completely firm set $\mathcal{I}$.*

Proof. We need to construct p systems of linear congruences with solutions $x_0, x_1, ..., x_{p-1}$ as follows:

- For all i, $x_i \equiv 1 \pmod p$.
- For all i and all j, $x_i \equiv 1 \pmod{s_j}$.
- For $0 \leq i \leq w_t - 1$, $x_i \equiv i \pmod{w_t}$; for the remaining i, $x_i \equiv 1 \pmod{w_t}$.
- For $w_t \leq i \leq w_{t-1} - 1$, $x_i \equiv i - w_t \pmod{w_{t-1}}$; for the remaining i, $x_i \equiv 1 \pmod{w_{t-1}}$.

  $\vdots$

- For $w_t + ... + w_2 \leq i \leq w_t + ... + w_2 + w_1 - 1$, $x_i \equiv i - w_t - w_{t-1} - ... - w_2 \pmod{w_1}$; for the remaining i, $x_i \equiv 1 \pmod{w_1}$.

Basically the first w_t solutions to the congruences form a complete set of residues modulo w_t and are equivalent to 1 modulo every other prime less than p. Then the next w_{t-1} solutions to the congruences form a complete set of residues modulo w_{t-1} and are equivalent to 1 modulo every other prime less than p. This process is repeated for each subsequent prime in $\mathcal{W}$. You should notice that this is possible since $p > w_1 + ... + w_t$.

Once again, it can be seen more easily what's going on if we view it in matrix form.

	x_1	x_2	x_3	...	x_{w_t-1}	x_{w_t}	x_{w_t+1}	...	$x_{w_t+w_{t-1}-1}$	...	$x_{w_t+...+w_2}$	...	x_{p-1}
p	1	1	1	...	1	1	1	...	1	...	1	...	1
w_t	0	1	2	..	$w_t - 1$	1	1	...	1	...	1	...	1
w_{t-1}	1	1	1	...	1	0	1	...	$w_{t-1} - 1$	...	1	...	1
$\vdots$				$\vdots$					$\vdots$			$\vdots$	
w_1	1	1	1	...	1	1	1	...	1	...	0	...	1
s_j	1	1	1	...	1	1	1	...	1	...	1	...	1

Notice by our construction we have found a set satisfying all conditions to be completely firm. $\square$

Example 3.8. Consider $\mathcal{Q} = \{3, 5, 7\}$ and $p = 17$.

$$\mathcal{I}_{CF} = \{364651, 1, 145861, 291721, 437581, 72931, 218791, 204205, 510511, 306307, 102103, 408409, 340341, 1021021, 170171, 1531531, 2042041\}$$

is a completely firm set. This can be found by setting up the following 17 systems of linear congruences:

	x_0	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	x_{10}	x_{11}	x_{12}	x_{13}	x_{14}	x_{15}	x_{16}
17	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
13	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
11	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
7	0	1	2	3	4	5	6	1	1	1	1	1	1	1	1	1	1
5	1	1	1	1	1	1	1	0	1	2	3	4	1	1	1	1	1
3	1	1	1	1	1	1	1	1	1	1	1	1	0	1	2	1	1
2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

3.2 Firm Polynomials

Definition 3.9. Let $\mathcal{I} = \{i_0, ..., i_{p-1}\}$ be a completely-firm set with the set of primes $\mathcal{Q} = \{q_1, ..., q_k\}$. We can call the polynomial

$$C_k(x) = (x - i_0)...(x - i_{p-1})$$

a **completely-firm(CF) polynomial.**

Proposition 3.10. *Let $\mathcal{I}$, $\mathcal{Q}$, and $C_k(x)$ be as in* Definition 3.9. *We have*

$$\begin{aligned}\mathcal{L}(C_k(x)) = \{p\} & \\ & + \{p - q_{j_1} + 2 | 1 \leq j_1 \leq k\} \\ & + \{p - q_{j_1} - q_{j_2} + 4 | 1 \leq j_1 \leq k, 1 \leq j_2 \leq k, \text{ and } j_1 \neq j_2\} \\ & \vdots \\ & + \{p - q_{j_1} - ... - q_{j_z} + 2z | 1 \leq j_i \leq k \text{ and } j_1 \neq ... \neq j_z\}.\end{aligned}$$

Proof. For notation purposes let $q_j(x) = (x - q_{j_0})...(x - q_{j_{q_j-1}})$ where $Q_j = \{q_{j_0}, ..., q_{j_{q_j-1}}\}$ forms a complete set of residues modulo q_j. Notice that we can factor the polynomial in the following ways:

$$\begin{aligned} C_k(x) &= (x - i_0)...(x - i_p) \\ &= q_{j_1}\Big(\frac{q_{j_1}(x)}{q_{j_1}}\Big)(x - i_{q_{j_1}})...(x - i_{p-1}) \\ &= q_{j_1}q_{j_2}\Big(\frac{q_{j_1}(x)}{q_{j_1}}\Big)\Big(\frac{q_{j_2}}{q_{j_2}}\Big)(x - i_{q_{j_1}+q_{j_2}})...(x - i_{p-1}) \\ &\vdots \\ &= q_1...q_k\Big(\frac{q_1(x)}{q_1}\Big)...\Big(\frac{q_k(x)}{q_k}\Big)(x - i_{q_1+..+q_k})...(x - i_{p-1}) \end{aligned}$$

So, $\{p\} + \{p - q_{j_1} + 2 | 1 \le j_1 \le k\} + \{p - q_{j_1} - q_{j_2} + 4 | 1 \le j_1 \le k, 1 \le j_2 \le k\} + ... + \{p - q_{j_1} - ... - q_{j_z} + 2z | 1 \le j_i \le k\} \in \mathcal{L}(C_k(x))$.

Now if $\mathcal{L}(C_k(x))$ is not equal to what's above, then there exists factorizations of other lengths of $C_k(x)$. Notice that the only integers that divide $C_k(x)$ are $q_1, ..., q_k$, so any new factorization of $C_k(x)$ must be in the form $C_k(x) = \frac{h_1(x)}{c}h_2(x)$ where $\frac{h_1(x)}{c}$ is irreducible in $\mathbb{Z}[x]$, $h_1(x), h_2(x) \in \mathbb{Z}[x]$, and c is composed of some of the primes $q_1, .., q_k$. The only factors in that form that are not above are $f_m(x) = \frac{h_1(x)}{c}\frac{h_3(x)}{c'}h_4(x)$ where $h_3(x), h_4(x) \in \mathbb{Z}[x]$ and c' shares a prime divisor with c, say q_t. But then $\mathcal{I} - \mathbb{Q}_t$ forms a complete set of residues modulo q_t, which is a contradiction. Thus, we have given all factorizations of $C_k(x)$ □

Notice that if $\mathcal{I}$ was a complete set of residues modulo p, then we could factor the polynomial as

$$C_k(x) = pq_1...q_k\Big(\frac{(x - i_0)...(x - i_{p-1})}{pq_1...q_k}\Big)$$

The factor length of this polynomial is $k + 2$. It is difficult to determine if $p - q_3 + 2 \ge k + 2$ adding another problem to taking the difference of consecutive lengths. Thus, we decided it best to have $\mathcal{I}$ an incomplete set of residues modulo p.

Proposition 3.11. *Let $q_1 \le q_2 \le q_3$ be primes, and $q_3 \ge q_1 + q_2 - 2$. Then $q_3 - q_1 - q_2 + 2 \in \triangle(C_3(x))$.*

Proof. From proposition 3.10 we can factor $C_3(x)$ as:

$$\begin{aligned} C_3(x) &= (x-i_0)...(x-i_{p-1}) \\ &= q_1\left(\frac{q_1(x)}{q_1}\right)(x-i_{q_1})...(x-i_{p-1}) \\ &= q_2\left(\frac{q_2(x)}{q_2}\right)(x-i_{q_2})...(x-i_{p-1}) \\ &= q_3\left(\frac{q_3(x)}{q_3}\right)(x-i_{q_3})...(x-i_{p-1}) \\ &= q_1q_2\left(\frac{q_1(x)}{q_1}\right)\left(\frac{q_2(x)}{q_2}\right)(x-i_{q_1+q_2})...(x-i_{p-1}) \\ &= q_1q_3\left(\frac{q_1(x)}{q_1}\right)\left(\frac{q_3(x)}{q_3}\right)(x-i_{q_1+q_3})...(x-i_{p-1}) \\ &= q_2q_3\left(\frac{q_2(x)}{q_2}\right)\left(\frac{q_3(x)}{q_3}\right)(x-i_{q_1+q_3})...(x-i_{p-1}) \\ &= q_1q_2q_3\left(\frac{q_1(x)}{q_1}\right)\left(\frac{q_2(x)}{q_2}\right)\left(\frac{q_3(x)}{q_3}\right)(x-i_{q_1+q_2+q_3})...(x-i_{p-1}) \end{aligned}$$

So $p, p-q_1+2, p-q_2+2, p-q_3+2, p-q_1-q_2+4, p-q_1-q_3+4, p-q_2-q_3+4, p-q_1-q_2-q_3+6 \in \mathcal{L}(C_3(x))$.

Now $q_1 > 2$, so $q_1 - 2 > 0$ and $p - q_1 + 2 < p$. Now $q_2 \geq q_1$, so $p - q_2 + 2 \leq p - q_1 + 2$. Now $q_1 > 2$, so $q_1 + q_2 > 2 + q_2$ and $p - q_1 - q_2 + 4 < p - q_2 + 2$. Now $q_3 \geq q_1 + q_2 - 2$, so $q_3 + 2 \geq q_1 + q_2$ and $p - q_3 + 2 \leq p - q_1 - q_2 + 4$. Now $q_1 > 2$, so $q_1 + q_3 > 2 + q_3$ and $p-q_1-q_3+4 < p-q_3+2$. Now $q_2 \geq q_1$, so $q_3+q_2 \geq q_3+q_1$ and $p-q_2-q_3+4 \leq p-q_1-q_3+4$. Now $q_1 > 2$, so $q_1 + q_2 + q_3 > q_2 + q_3 + 2$ and $p - q_2 - q_3 - q_1 + 6 < p - q_2 - q_3 + 4$.

Thus $p > p - q_1 + 2 \geq p - q_2 + 2 > p - q_1 - q_2 + 4 \geq p - q_3 + 2 > p - q_1 - q_3 + 4 \geq p - q_2 - q_3 + 4 > p - q_1 - q_2 - q_3 + 6$.

So by taking consecutive differences we find that $q_3 - q_1 - q_2 + 2 \in \triangle(C_3(x))$. □

We show that $q_3-q_1-q_2+2$ produces all odd numbers up to $3*10^{17}$ when $q_1 \leq q_2 \leq q_3$ are primes and $q_3 \geq q_1+q_2-2$. Since showing this relies on showing sums of primes equal natural numbers, we assume the Goldbach conjecture which is where we get the bound $3*10^{17}$.

Proposition 3.12. *Every natural odd number n such that $1 \leq n < 3*10^{17}$ can be written as $n = q_3 - q_1 - q_2$ where q_1, q_2, q_3 are primes such that $q_3 \geq q_1 + q_2 - 2$ and $q_1 \leq q_2 \leq q_3$.*

Proof. Proof by Induction on n. Let $n = 1$, $1 = 11 - 7 - 3$ and $11 \geq 7 + 3 - 2 = 8$ is true and $3 \leq 7 \leq 11$.

Let $n = q_3 - q_1 - q_2$ where $q_3 \geq q_1 + q_2 - 2$ and $q_1 \leq q_2 \leq q_3$. We show that there exists primes p_1, p_2, p_3 for $n + 2$ where $p_1 \leq p_2 \leq p_3$, and $p_3 \geq p_1 + p_2 - 2$. Now $n + 2 = q_3 - q_1 - q_2 + 2 = q_3 - (q_1 + q_2 - 2)$. Let $x = q_1 + q_2 - 2$. According to the Goldbach Conjecture, $x = p_1 + p_2$ where p_1, p_2 are primes. Now $n + 2 = q_3 - p_1 - p_2$. We know that $q_1 + q_2 - 2 = p_1 + p_2 \leq q_3$. Thus, $p_1 + p_2 - 2 \leq q_3$. Now if $p_2 \leq q_3$ then we are done since we have found our 3 primes $p_1, p_2, q_3 = p_3$ for $n+2$. If not, then $p_2 > q_3$. So, $p_2 > q_3 \geq p_1 + p_2 - 2$. Then $0 > q_3 - p_2 \geq p_1 - 2$, so $0 > p_1 - 2 \rightarrow 2 > p_1$ which is a contradiction since $2 \leq p_1$ because p_1 is prime.

Thus $n + 2 = q_3 - p_1 - p_2$ where $p_1 + p_2 - 2 \leq q_3$ and $p_1 \leq p_2 \leq q_3$. □

Corollary 3.13. *Every odd natural number less than* $3 * 10^{17}$ *is in* $\Delta(Int(\mathbb{Z}))$.

Chapter 4

The Delta Set of Int($\mathbb{Z}$)

We will improve the arguments of Chapter 3 and explicitly compute $\Delta(\text{Int}(\mathbb{Z}))$.

4.1 Incomplete Binomial Polynomials

Let $K = \{k_1, ..., k_n\}$ be a set of integers such that $0 \leq k_1 < k_2 < ... < k_n < m$ and

$$m_{K,n}(x) = x^{\alpha_0}(x-1)^{\alpha_1}(x-2)^{\alpha_2}...(x-m+1)^{\alpha_{m-1}}$$

with $\alpha_{k_1} = \alpha_{k_2} = ... = \alpha_{k_n} = 0$ and the rest of the α's equal 1.

Proposition 4.1. *For every* $1 \leq i \leq n$,

$$m_{K,n}(k_i) = k_i!(m-k_i-1)!(-1)^{m-k_i-1}\left[\prod_{j=1, j\neq i}^{n} \frac{1}{(k_i-k_j)}\right]$$

Proof. Proof by Induction on n. Let $n = 1$. Then, $K = \{k_1\}$ and

$$m_{K,1}(x) = x(x-1)...(x-k_1+1)(x-k_1-1)...(x-m+1),$$

and

$$m_{K,1}(k_1) = k_1(k_1-1)...(1)(-1)(-2)...(k_1-m+1)$$

$$m_{K,1}(k_1) = k_1!(-1)^{m-k_1-1}(1)(2)...(m-k_1-1) = k_1!(m-k_1-1)!(-1)^{m-k_1-1}.$$

Let $K = \{k_1, ..., k_n\}$ be a set of integers such that $0 \leq k_1 < ... < k_n < m$ and the statement be true for every $n-1$ subset of the integers. Then, using the induction hypothesis for every $0 \leq i \leq m-1$ and $\hat{K}_t = \{k_1, ..., k_{t-1}, k_{t+1}, ..., k_n\}$ for some $t \neq i$,

$$m_{K,n}(k_i) = \frac{m_{\hat{K}_t,n}(k_i)}{(k_i - k_t)}$$

$$= k_i!(m - k_i - 1)!(-1)^{m-k_i-1} \left[\prod_{j=1, j\neq i}^{n-1} \frac{1}{(k_i - k_j)} \right] \left[\frac{1}{(k_i - k_t)} \right].$$

$$= k_i!(m - k_i - 1)!(-1)^{m-k_i-1} \left[\prod_{j=1, j\neq i}^{n} \frac{1}{(k_i - k_j)} \right].$$

□

Proposition 4.2. *For every* $K = \{k_1, ..., k_n\}$,

$$gcd\big(m_{K,n}(k_1)...m_{K,n}(k_n)\big)|d\big(\mathbb{Z}, m_{K,n}(x)\big)$$

and

$$d\big(\mathbb{Z}, m_{K,n}(x)\big) \leq |m_{K,n}(k_1)|.$$

Proof. From above, we know $m_{K,n}(k_1)...m_{K,n}(k_n)$, and by construction $m_{K,n}(x) = 0$ for every $x \neq k_i$ for some $0 \leq i \leq m-1$. So, in the difference table construction of C. Long, we know

$$D^0(x) = 0 \qquad \text{where} \qquad 0 \leq x < k_1,$$

and

$$D^0(k_i) = m_{K,n}(k_i) \qquad \text{for every} \qquad 0 \leq i \leq m-1.$$

Now

$$D^j(0) = D^{j-1}(1) - D^{j-1}(0),$$

so

$$D^j(0) = 0 \qquad \text{for every} \qquad 0 \leq j < k_1.$$

Notice that $D^1(k_1 - 1) = D^0(k_1) - D^0(k_1 - 1) = D^0(k_1)$, and thus

$$D^2(k_1 - 2) = D^1(k_1 - 1) = D^0(k_1) = m_{K,n}(k_1).$$

We can continue this until we get that

$$D^{k_1}(0) = m_{K,n}(k_1).$$

Now

$$D^1(x) = D^0(x+1) + D^0(x) \qquad \text{for every} \qquad k_1 < x \leq m-1.$$

By our construction, for every $k_1 < x \leq m-1$, $D^0(x) = m_{K,n}(k_i)$ for some i or $D^0(x) = 0$. Thus, $D^1(x)$ for every $k_1 < j \leq m-1$ will either be 0, $m_{K,n}(k_{i1})$, $m_{K,n}(k_{i2}) - m_{K,n}(k_{i1})$. By doing this again for $D^2(x)$ and so on, we see that

$$D^j(0) = a_1 D^0(k_1) + a_2 D^0(k_2) + ... + a_n D^0(k_n) \qquad \text{for every} \qquad k_1 < j \leq m-1$$

where $a_1, a_2, ..., a_n \in \mathbb{Z}$. That is, $D^j(0)$ will be a linear combination of $m_{K,n}(k_1)...m_{K,n}(k_n)$ for every $k_1 < j \leq m-1$. Now,

$$d(m_{K,n}(x), \mathbb{Z}) = gcd\left(D^j(0)\right) \qquad \text{for every} \qquad 0 \leq j \leq m-1.$$

So,

$$d(m_{K,n}(x), \mathbb{Z}) = a_1 D^0(k_1) + a_2 D^0(k_2) + ... + a_n D^0(k_n)$$

for some $a_1, a_2, ..., a_n \in \mathbb{Z}$. Which means that

$$d(m_{K,n}(x), \mathbb{Z}) = a_1 m_{K,n}(k_1) + ... + a_n m_{K,n}(k_n).$$

Thus,

$$\gcd\big(m_{K,n}(k_1)...m_{K,n}(k_n)\big) | d\big(m_{K,n}(x), \mathbb{Z}\big),$$

and since $D^{k_1}(0) = m_{K,n}(k_1)$ we get that

$$d\big(\mathbb{Z}, m_{K,n}(x)\big) \leq |m_{K,n}(k_1)|.$$

□

Corollary 4.3. *Let $f(x) \in \mathbb{Q}[x]$ with $deg f(x) = m$. Suppose $f(j) \neq 0$ for $0 \leq j \leq m$ and $f(l) = 0$ for $l \neq j$, $0 \leq l \leq m$. Then, $d(\mathbb{Z}, f(x)) = |f(j)|$.*

Corollary 4.4. $d(\mathbb{Z}, m_1(x)) = |m_1(k_1)|$

4.2 The Delta Set

Pick $m \in \mathbb{N}$ and a prime $p > m$. Let

1) $\{0, ..., m-1\} \cup \{i_1, ..., i_{p-m}\}$ form a complete set of residues modulo p

2) $\{0, ..., m-1\} \cup \{i_1, ..., i_{p-m}\}$ not form a complete set of residues modulo any prime r such that $m < r < p$.

3) $i_1 \equiv ... \equiv i_{p-m} \equiv m-1 \pmod{q}$ for every prime $q < p$

Consider the polynomial

$$h(x) = x(x-1)...(x-m+1)(x-i_1)...(x-i_{p-m})$$

Proposition 4.5. *$d(\mathbb{Z}, h(x)) = m!p$.*

Proof. Since

$$m!|x(x-1)...(x-m+1) \qquad \text{and} \qquad p|h(x)$$

then

$$d(\mathbb{Z}, h(x)) \geq m!p \qquad \text{and} \qquad m!p|d(\mathbb{Z}, h(x)).$$

Notice that if $q \nmid m!$ and $q \neq p$, then $q \nmid d(\mathbb{Z}, h(x))$. Also, because of the conditions on i_j for every $i \leq j \leq p-m$ the only primes less than p that could divide $d(\mathbb{Z}, h(x))$ are the primes that also divide $m!$.

Let $m! = p_1^{r_1}...p_t^{r_t}$, $a(x) = x(x-1)...(x-m+1)$, and $b(x) = (x-i_1)...(x-i_{p-m})$.

If $x = m$, then $a(x) = m(m-1)...(1)$ and $p_k^{r_k}||a(x)$ for every $1 \leq k \leq t$. Also,

$$i_1 \equiv ... \equiv i_{p-m} \equiv 1 \pmod{p_k} \text{ for every } 1 \leq k \leq t.$$

So, $p_k^{r_k} \nmid b(m)$. Thus, for every power of prime that divides $m!$, that power exactly divides $a(m)$ and does not divide $b(m)$. Therefore, $d(\mathbb{Z}, h(x)) = m!p$. □

Let

$$f(x) = \frac{h(x)}{m!}.$$

Then we can write $f(x)$ as,

$$f(x) = \frac{x(x-1)...(x-m+1)}{m!}(x-i_1)...(x-i_{p-m}).$$

Now $\frac{x(x-1)...(x-m+1)}{m!} = \binom{x}{m}$ which is irreducible by Corollary 2.2 in Anderson, Cahen, Chapman, and Smith [1]. So the above factorization of $f(x)$ is an irreducible factorization of length $p-m+1$. Also,

$$f(x) = p\left(\frac{x(x-1)...(x-m+1)(x-i_1)...(x-i_{p-m})}{m!p}\right).$$

This is $f(x) = p\frac{h(x)}{d(\mathbb{Z},h(x))}$. Now $\frac{h(x)}{d(\mathbb{Z},h(x))}$ is irreducible if and only if $d(\mathbb{Z},h_1(x))d(\mathbb{Z},h_2(x)) < d(\mathbb{Z},h(x))$ for every $h_1(x)h_2(x) = h(x)$. Since $\{0,...,m-1\} \cup \{i_1,...,i_{p-m}\}$ forms a complete set of residues modulo p, then $p \nmid (\mathbb{Z},h_1(x))$ and $p \nmid (Z,h_2(x))$. Thus, $d(\mathbb{Z},h_1(x))d(\mathbb{Z},h_2(x)) < d(\mathbb{Z},h(x))$ and $f(x) = p\frac{h(x)}{d(\mathbb{Z},h(x))}$ is a factorization of $f(x)$ of length 2.

We claim that these are the only two irreducible factorizations of $f(x)$.

Proposition 4.6. $\mathcal{L}(f(x)) = \{2, p-m+1\}$.

Proof. Since $d(\mathbb{Z},h(x)) = m!p$, we can not take out any other integers from $h(x)$ than $m!p$. So, there does not exist any factorizations of $f(x)$ where $f(x) = c\frac{h(x)}{m!c}$ where $c \neq p$.

Thus, we only need to consider factorizations of $f(x)$ such that

$$f(x) = w(x)v(x) \qquad \text{where} \qquad w(x) = \frac{s(x)}{d_1} \qquad \text{and} \qquad v(x) = \frac{r(x)}{d_2}$$

where $d_1 | d(s(x),\mathbb{Z})$, $d_2 | d(r(x),\mathbb{Z})$ and $d_1, d_2 \in \mathbb{Z}$. Notice that $d_1 = d(s(x),\mathbb{Z})$ and $d_2 = d(r(x),\mathbb{Z})$. Because if $d_1 \neq d(s(x),\mathbb{Z})$ then $\alpha d_1 = d(s(x),\mathbb{Z})$ for some $\alpha > 1$. Thus,

$$f(x) = \alpha\left(\frac{s(x)}{\alpha d_1}\right)\left(\frac{r(x)}{d_2}\right)$$

which is a contradiction since $\alpha \neq p$. The same argument can be used to show that $d_2 = d(r(x),\mathbb{Z})$.

Therefore,

$$f(x) = \frac{s(x)}{d(\mathbb{Z},s(x))}\frac{r(x)}{d(\mathbb{Z},r(x))}$$

.

Also notice that $s(x)$ and $r(x)$ are primitive. If $s(x)$ is not primitive, then

$$\frac{s(x)}{d_1} = \frac{s_1 s'(x)}{d_1} = \frac{s'(x)}{d_1'}$$

for some polynomial $s'(x)$ and integers s_1 and $d_1' \neq d_1$. But then, $d_1' = d(s(x), \mathbb{Z})$ which is a contradiction. A similar argument can also be used to show that $r(x)$ is primitive also.

Now, notice that

$$\frac{h(x)}{m!} = \frac{s(x)}{d(\mathbb{Z}, s(x))} \frac{r(x)}{d(\mathbb{Z}, r(x))},$$

so $h(x)d(\mathbb{Z}, s(x))d(\mathbb{Z}, r(x)) = s(x)r(x)m!$. And because $h(x), s(x), r(x)$ are primitive we get that $d(\mathbb{Z}, s(x))d(\mathbb{Z}, r(x)) = m!$.

Now $h(x) = s(x)r(x)$, so $s(x)$ and $r(x)$ are composed of some terms from $a(x)$ and $b(x)$. Remember, $a(x) = x(x-1)...(x-m+1)$, and $b(x) = (x-i_1)...(x-i_{p-m})$. Notice that neither $s(x)$ or $r(x)$ can have all the terms from $a(x)$ or all the terms from $b(x)$. Because without loss of generality let $s(x) = a(x)b'(x)$ where $b'(x)$ is composed of some terms of $b(x)$. Then, $d(\mathbb{Z}, s(x)) = m!$ and $d(\mathbb{Z}, r(x)) = 1$ and we get a factorization of length $p - m + 1$. Thus, $s(x)$ and $r(x)$ are composed of some of the terms of $a(x)$ and $b(x)$, but neither one has all the terms from $a(x)$.

That is, $s(x) = a_1(x)b_1(x)$ and $r(x) = a_2(x)b_2(x)$. Where $a_1(x), a_2(x)$ are composed of some terms from $a(x)$ but $a_1(x) \neq 1$ and $a_2(x) \neq 1$. Also, $b_1(x), b_2(x)$ are composed of some terms from $b(x)$. So,

$$f(x) = \frac{s(x)}{d(\mathbb{Z}, s(x))} \frac{r(x)}{d(\mathbb{Z}, r(x))} = \frac{a_1(x)b_1(x)}{d(\mathbb{Z}, s(x))} = \frac{a_2(x)b_2(x)}{d(\mathbb{Z}, r(x))}$$

Now, $d(\mathbb{Z}, a_1(x))d(\mathbb{Z}, a_2(x)) < m!$. If $d(\mathbb{Z}, a_1(x))d(\mathbb{Z}, a_2(x)) = m!$, then

$$\binom{x}{m} = \left(\frac{a_1(x)}{d(\mathbb{Z}, a_1(x))}\right)\left(\frac{a_2(x)}{d(\mathbb{Z}, a_2(x))}\right)$$

which contradicts the fact that $\binom{x}{m}$ is irreducible. Thus, $d(\mathbb{Z}, a_1(x))d(\mathbb{Z}, a_2(x)) < m!$.

Now

$$s(x) = \frac{a_1(x)b_1(x)}{d(\mathbb{Z}, s(x))} = \frac{a_1(x)b_1(x)}{kd(\mathbb{Z}, a_1(x))d(\mathbb{Z}, b_1(x))}$$

where $k \in \mathbb{Z}$. Consider the case when $x = m$, then $b_1(m) \equiv 1 \pmod{q}$ for every prime $q|m$. So, $d(\mathbb{Z}, b_1(x)) \nmid s(m)$. So, $d(\mathbb{Z}, s(x)) = kd(\mathbb{Z}, a_1(x))$ and $d(\mathbb{Z}, a_1(x))||s(m)$.

Now, $d(\mathbb{Z}, s(x)) = kd(\mathbb{Z}, a_1(x))$ where $k \in \mathbb{Z}$. Let q be a prime, $q < p$, $q \nmid a_1(m)$, and $q|b_1(m)$. Now $i_1 \equiv ... \equiv i_{p-m} \equiv m - 1 \pmod{q}$. So, $b_1(m) \equiv m - i_j \equiv m - (m-1) \equiv 1 \pmod{q}$ for every $1 \leq j \leq p - m$. So, $q \nmid b_1(m)$ which is a contradiction. Thus, there does not exist any prime $q < p$ such that $q \nmid a_1(m)$ and $q|b_1(m)$. Therefore, $d(\mathbb{Z}, s(x)) = d(\mathbb{Z}, a_1(x)$. A similar argument can be used to show that $d(\mathbb{Z}, r(x)) = d(\mathbb{Z}, a_2(x))$.

But then $m! = d(\mathbb{Z}, s(x))d(\mathbb{Z}, r(x)) = d(\mathbb{Z}, a_1(x))d(\mathbb{Z}, a_2(x)) < m!$ which is a contradiction, so the only factorizations of $f(x)$ are the ones of length 2 and length $p - m + 1$. Therefore, $\mathcal{L}(f(x)) = \{2, p - m + 1\}$ □

Corollary 4.7. $\Delta(Int(\mathbb{Z})) = \mathbb{N}$

Acknowledgements

Dr. Chapman, thank you for everything. I know I would not have had most of my great experiences these past 4 years without you encouraging me to go for them. You are one of the reasons that I enjoyed and learned so much at Trinity. You are an amazing advisor and more than that, I would not be this person today without you. Hopefully, you'll find someone else to come by your office and "annoy" you when I'm gone.

Bibliography

[1] D.F. Anderson, P-J. Cahen, S.T. Chapman and W.W. Smith, *Some Factorization Properties of the Ring of Integer-Valued Polynomials*, Lecture Notes in Pure and Applied Mathematics, Marcel Dekker, **171** (1995), 125-142.

[2] P.-J. Cahen and J.-L. Chabert. "Integer Valued-Polynomials", Amer. Math Soc. Surverys and Monographs, **58** (1997), American Mathematical Society, Providence.

[3] S.T. Chapman and B. McClain. *Irreducible Polynomials and full elasticity in rings of integer-valued polynomials*, J. Algebra, **293** (2005), 595-610.

[4] A. Gaeroldinger and W. Hassler. *Local Tameness of v-Noetherian Monoids*, Preprint.

[5] R. Gilmer and W.W. Smith. *Finitely Generated Ideals of the Ring of Integer-Valued Polynomials*, J. Algebra, **81** (1983), 150-164.

[6] Thomas W. Hungerford. *Algebra*. Holt, Rinehart and Winston, Inc. 1974.

[7] Calvin Long. *Pascal's Triangle, Difference Tables and Arithmetic Sequences of Order N*, College Math Journal, **15** (1984), 290-298.