# Factorisation Properties of Integer-Valued Polynomials

Barbara Anne McClain

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

21 April 2004

THESIS ADVISOR

DEPARTMENT CHAIR

ASSOCIATE VICE PRESIDENT FOR
ACADEMIC AFFAIRS:
CURRICULUM AND STUDENT ISSUES

"God does not care about our mathematical difficulties. He integrates empirically."
– Albert Einstein

# Abstract

Let $S \subseteq \mathbb{Z}$. Polynomials in $\mathbb{Q}[x]$ mapping members of $S$ into the integers are called integer-valued over $S$. The ring of such polynomials is denoted $\mathrm{Int}(S, \mathbb{Z})$. Because $\mathrm{Int}(S, \mathbb{Z})$ does not constitute a unique factorisation domain, factorisation properties in this ring are especially appealing.

In this thesis, we present a criterion for irreducibility, a detailed analysis of factorisation lengths, and a class of polynomials that factor uniquely in $\mathrm{Int}(S, \mathbb{Z})$.

# Acknowledgements

An uncountably infinite set of gratitude goes out to Professor Chapman, "The Godfather." Dr. Chapman, you have been a fantastic academic and research advisor, as well as a generally great personality on campus throughout my stay at Trinity. If a garden variety commutative ring $R$ ever walks up to me in the supermarket and asks me who the most awesome professor I've known is, I will tell $R$ that its you.

Mrs. Bigler, you were the first lady I'd ever known to share your genuine appreciation and love for mathematics with your students. For as long as I've known you, you've been a model person and mathematician. You are the epitome of an effective educator and role model, and I thank you for your tireless work in LaVernia. You are still my favorite mathematician in the world.

Mom and Aunt Lue, you are the most lovely ladies in the world. Your love and support has been phenomenal. You are both role models for me and I love you from the bottom of my heart.

Amanda, you're my best friend in the whole world. Thanks for being such a great friend and a wonderful person. You rock more than David Bowie.

# Contents

**1 An Introduction to Int$(S, \mathbb{Z})$** **1**

1.1 The Generalised Binomial Polynomials . . . . . 2

**2 The Fixed Divisor** **5**

**3 The Structure of Irreducibles in Int$(S, \mathbb{Z})$** **14**

**4 Some Elements With Unique Factorisation in Int$(S, \mathbb{Z})$** **18**

**5 Elasticity in Int$(S, \mathbb{Z})$** **24**

# Chapter 1

# An Introduction to Int$(S, \mathbb{Z})$

Let $S \subseteq \mathbb{Z}$ and $f(x) \in \mathbb{Q}[x]$. We say that $f(x)$ is integer-valued over $S$ if $f(s) \in \mathbb{Z}$ for every $s \in S$. The set of all such polynomials is denoted $\text{Int}(S, \mathbb{Z})$:

$$\text{Int}(S, \mathbb{Z}) = \{f(x) \in \mathbb{Q}[x] \mid f(s) \in \mathbb{Z} \ \forall \ s \in S\}.$$

Notice that polynomials in $\mathbb{Z}[x]$ are integer-valued over $\mathbb{Z}$, as well as over every subset of the integers. For convenience, we use the notation $\text{Int}(\mathbb{Z}, \mathbb{Z}) = \text{Int}(\mathbb{Z})$. Furthermore, if a polynomial in $\mathbb{Q}[x]$ is integer-valued over all of $\mathbb{Z}$, it will be integer-valued over any subset $S$ of $\mathbb{Z}$. We observe:

$$\mathbb{Z}[x] \ \subseteq \ \text{Int}(\mathbb{Z}) \ \subseteq \ \text{Int}(S, \mathbb{Z}) \ \subseteq \ \mathbb{Q}[x],$$

and remark that although $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$ both constitute unique factorisation domains, $\text{Int}(\mathbb{Z})$ and $\text{Int}(S, \mathbb{Z})$ do not.

**Example 1.1.** $\frac{x}{2}$ is integer-valued over $2\mathbb{Z}$ but not over $\mathbb{Z}$.

**Example 1.2.** $\frac{x(x-1)}{2} \in \text{Int}(\mathbb{Z})$, although $\frac{x(x-1)}{2} \notin \mathbb{Z}[x]$. For every integer $x$, either $x$ or $x-1$ is even; hence, $2 \mid x(x-1)$.

**Definition 1.3 (See [5]).** Let $R$ be a ring. A (left) **R-module** is an additive abelian group $A$ together with a function $R \times A \to A$ (the image of $(r, a)$ denoted by $ra$) such that for every $r, s \in R$ and $a, b \in A$ the following hold:

(i) $r(a + b) = ra + rb$

(ii) $(r + s)a = ra + sa$

(iii) $r(sa) = (rs)a$,

and if $R$ has an identity element $1_R$ and

(iv) $1_R a = a \ \forall \ a \in A$,

then $A$ is said to be a **unitary R-module**.

Note that if $R$ is commutative, then every left $R$-module $A$ can be given the structure of a right $R$-module by defining $ra = ar$ for every $r \in R$ and $a \in A$. So every module $A$ over a commutative ring $R$ is said to be both a left and a right module with $ar = ra$ for all $r \in R$ and $a \in A$.

**Example 1.4.** If $S$ is a ring and $R$ is a subring, then $S$ is an $R$-module with $ra$ ($r \in R, a \in S$) being multiplication in $S$. In particular, $R[x_1, \ldots, x_m]$ is an $R$-module.

**Proposition 1.5.** *Int$(S, \mathbb{Z})$ is a unitary $\mathbb{Z}$-module.*

**Proof** Observe first that $\mathrm{Int}(S, \mathbb{Z})$ is an additive abelian group. Let $f(x), g(x) \in \mathrm{Int}(S, \mathbb{Z})$. Then $f(x) + g(x) \in \mathbb{Q}[x]$ and $\forall s \in S$, $f(s), g(s) \in \mathbb{Z}$ so $f(s) + g(s) \in \mathbb{Z}$. Hence, $f(x) + g(x) \in \mathrm{Int}(S, \mathbb{Z})$. Moreover, $\mathrm{Int}(S, \mathbb{Z})$ is closed under multiplication with the integers. Since for every integer $a$, $af(x) \in \mathbb{Q}[x]$, and $\forall z \in \mathbb{Z}$, $af(z) \in \mathbb{Z}$, we have $af(x) \in \mathrm{Int}(S, \mathbb{Z})$.

Thus, $\mathrm{Int}(S, \mathbb{Z})$, together with scalar multiplication in $\mathbb{Z}$ satisfies the requirements to be a unitary $\mathbb{Z}$-module, because for every $r, s \in \mathbb{Z}$ and $f(x), g(x) \in \mathrm{Int}(S, \mathbb{Z})$ we have the following:

(i) $r(f(x) + g(x)) = rf(x) + rg(x)$

(ii) $(r + s)f(x) = rf(x) + sf(x)$

(iii) $r(sf(x)) = (rs)f(x)$

where the properties (i) - (iii) follow from the properties of scalar multiplication in $\mathbb{Z}$. Finally, $\mathbb{Z}$ has an identity element 1, so that

(iv) $1f(x) = f(x)$ for every $f(x) \in \mathrm{Int}(S, \mathbb{Z})$. ■

**Definition 1.6 (See [6]).** Let $A$ be a module over a ring $R$ and let $H$ be a subset of $A$. We say that $H$ is a **basis** of $A$ if $H$ is not empty, if $H$ generates $A$, and if $H$ is linearly independent. If $H$ is a basis of $A$, then in particular $A \neq \{0\}$ if $R \neq \{0\}$ and every element of $A$ has a unique expression as a linear combination of elements in $H$. A module that admits such a basis is said to be a **free module**.

## 1.1 The Generalised Binomial Polynomials

By Proposition 1.5, we have that $\mathrm{Int}(S, \mathbb{Z})$ is a unitary $\mathbb{Z}$-module for subsets $S$ of the integers. In order to determine an appropriate $\mathbb{Z}$-basis for $\mathrm{Int}(S, \mathbb{Z})$, we turn to Bhargava and his generalisation of the Binomial Polynomials for subsets of $\mathbb{Z}$ (see [2]).

Let $S \subseteq \mathbb{Z}$, and fix a prime integer $p$. Bhargava details the construction of a *p-ordering* of $S$ as follows.

- Choose an element $a_0 \in S$ arbitrarily.
- Choose an element $a_1 \in S$ that minimizes the highest power of $p$ dividing $(a_1 - a_0)$.
- Choose an element $a_2 \in S$ minimizing the highest power of $p$ dividing $(a_2 - a_0)(a_2 - a_1)$.
- In general, at the $k$th step, choose $a_k \in S$ minimizing the highest power of $p$ dividing $(a_k - a_0)(a_k - a_1) \cdots (a_k - a_{k-1})$.

Bhargava argues that having obtained such a $p$-ordering $\{a_j\}_{j=0}^{\infty}$, then one obtains a monotone increasing sequence $\{\nu_k(S, p)\}_{k=0}^{\infty}$ of powers of $p$, where the $k$th element $\nu_k(S, p)$ is precisely the power of $p$ minimized at the $k$th step of the $p$-ordering process. So

$$\nu_k(S,p) = w_p((a_k - a_0)(a_k - a_1)\cdots(a_k - a_{k-1})),$$

where $w_p(z)$ is the highest power of $p$ dividing $z$. For example, $w_3(54) = 3^3 = 27$. The sequence $\{\nu_k(S,p)\}$ is known as the *associated p-sequence* of $S$ corresponding to the chosen $p$-ordering $\{a_j\}$ of $S$. We now define the generalised factorial function, denoted $k!_S$:

$$k!_S = \prod_p \nu_k(S,p).$$

**Example 1.7.** Let $S = 3\mathbb{Z} = \{3k \ : \ k \in \mathbb{Z}\}$. Then the natural ordering, $\{0, 3, 6, \dots\}$ also forms a $p$-ordering for every prime $p$. Then

$$k!_{3\mathbb{Z}} = (3k-0)(3k-3)\cdots(3k-(3k-3)) = 3^k k!.$$

In particular, $k!_{\mathbb{Z}} = k!$, where $k!$ represents the standard definition of the factorial function. We may now define the generalised binomial polynomials, denoted $B_{i,S}(x)$ for $S$:

$$B_{i,S}(x) = \binom{x}{i}_S = \frac{(x-a_{0,i})(x-a_{1,i})\cdots(x-a_{i-1,i})}{i!_S},$$

where $\{a_{j,k}\}_{j=0}^{\infty}$ is a sequence in $\mathbb{Z}$ that, for each prime $p$ dividing $k!_S$, is termwise congruent modulo $\nu_k(S,p)$ to some $p$-ordering of $S$. In the case that $S = \mathbb{Z}$, we have

$$B_{i,\mathbb{Z}}(x) = \binom{x}{i} = \frac{x(x-1)\cdots(x-i+1)}{i!},$$

which are the familiar Binomial Polynomials. We now have the tools to offer a basis for $\mathrm{Int}(S,\mathbb{Z})$.

**Theorem 1.8 (Theorem 23, [2]).** *The set $\{\binom{x}{i}_S\}_{i=1}^{\infty}$ forms a basis for the $\mathbb{Z}$-module Int$(S,\mathbb{Z})$.*

Hence, the familiar Binomial Polynomials form a basis for $\mathrm{Int}(\mathbb{Z})$.

Suppose that, given a polynomial $f(x) \in \mathrm{Int}(\mathbb{Z})$ of degree $n$, one wishes to find its unique expression explicitly as a linear combination of the Binomial Polynomials: $f(x) = f_0\binom{x}{0} + f_1\binom{x}{1} + \ldots + f_n\binom{x}{n}$, where $f_i \in \mathbb{Z}$ and $f_n \neq 0$. C. Long provides a method of finding these $f_j$ [8]. One first finds the set of images $\{f(0), f(1), \dots, f(n)\}$, and then creates a "difference table", denoting the entry in the $j$th row and $k$th column $D^j(k)$:

| 0 | 1 | 2 | $\cdots$ | n |
|---|---|---|---|---|
| f(0) | f(1) | f(2) | $\cdots$ | f(n) |
| $D^1(0) = f(1) - f(0)$ | $D^1(1) = f(2) - f(1)$ | $D^1(2) = f(3) - f(2)$ | $\cdots$ | $D^1(n) = f(n) - f(n-1)$ |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ |
| $D^n(0)$ | $D^n(1)$ | $D^n(2)$ | $\cdots$ | $D^n(n)$ |

Note that in general, $D^j(k) = D^{j-1}(k+1) - D^{j-1}(k)$. After having generated such a table, we have the following representation for $f(x)$:

$$f(x) = D^0(0)\binom{x}{0} + D^1(0)\binom{x}{1} + \ldots + D^n(0)\binom{x}{n}. \tag{1.1}$$

It is important to note that as a consequence of this construction, we have the following:

**Corollary 1.9.** *Let $f(x) \in \mathbb{Q}[x]$ have degree $r$. If $f(0), f(1), \ldots, f(r) \in \mathbb{Z}$, then $f(x)$ is integer-valued over all integers.*

**Proof** Assume that $f(0), f(1), \ldots, f(r) \in \mathbb{Z}$. Then applying the difference table construction, there are integers $f_0, f_1, \ldots, f_r$, with $f_r \neq 0$, so that

$$f(x) = f_0\binom{x}{0} + f_1\binom{x}{1} + \ldots + f_r\binom{x}{r}.$$

Since $\binom{x}{i}$ is integer-valued on $\mathbb{Z}$ for every $i \in [0, r]$, we have that $f(x)$ is integer-valued on $\mathbb{Z}$. ■

**Example 1.10.** Let $f(x) = 2x^2 + 3x + 5$. Notice that $f(0) = 5, f(1) = 10$, and $f(2) = 19$. We construct the difference table:

| f(0)=5 | f(1)=10 | f(2)=19 |
|---|---|---|
| 5 | 9 | |
| 4 | | |

so we have

$$\begin{aligned} f(x) &= 5\binom{x}{0} + 5\binom{x}{1} + 4\binom{x}{2} \\ &= 5 + 5x + 4\frac{x(x-1)}{2} \\ &= 5 + 3x + 2x^2. \end{aligned}$$

# Chapter 2

# The Fixed Divisor

**Definition 2.1.** 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 defined as

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

If $c(f) = 1$, we say that $f(x)$ is **primitive** over $\mathbb{Z}[x]$.

**Definition 2.2 (See [2]).** Let $f(x) \in \mathrm{Int}(S, \mathbb{Z})$. The **fixed divisor** of $f$ over $S$, denoted $\mathrm{d}(S, f)$, is defined as

$$\mathrm{d}(S, f) = \gcd\{f(s) : s \in S\}.$$

**Definition 2.3.** Let $p(x) \in \mathrm{Int}(S, \mathbb{Z})$. If $\mathrm{d}(S, p) = 1$, we call $p(x)$ **image primitive** over $S$.

**Lemma 2.4.** *Let $f(x) \in Int(S, \mathbb{Z})$. Then $d(\mathbb{Z}, f) \mid d(S, f)$.*

**Proof** This result is clear since $S \subseteq \mathbb{Z}$. ■

**Example 2.5.** Each of the binomial polynomials $\binom{x}{i}$ is image primitive over $\mathbb{Z}$, since $\binom{i}{i} = 1$, for each $i \in \mathbb{N}$.

**Lemma 2.6.** *Let $F(x) \in Int(\mathbb{Z})$ have degree $r$, so that $F(x) = F_0 + F_1\binom{x}{1} + \ldots + F_r\binom{x}{r}$, where $F_i \in \mathbb{Z}$ and $F_r \neq 0$. The following are equivalent:*

*1* $d(\mathbb{Z}, F) = D$.

*2* $\gcd(F_0, F_1, \ldots, F_r) = D$.

*3* $\gcd(F(0), F(1), \ldots, F(r)) = D$.

**Proof**

**(1 ⇔ 2)** (⇒) Suppose that $\mathrm{d}(\mathbb{Z}, F) = D$. Now, amongst the coefficients $F_j$, there is a smallest $j$ for which $F_j \neq 0$. For such a $j$, $F(j) = F_j$. Since $\mathrm{d}(\mathbb{Z}, F) = D$, $D \mid F(j)$ implies that $D \mid F_j$. Assuming that $F_{j+1} \neq 0$, we see that $F(j+1) = (j+1)F_j + F_{j+1}$. Since $D \mid F(j+1)$ and $D \mid F_j$, we have $D \mid F_{j+1}$. We may proceed in this fashion to see that $D \mid F(j+2)$, implying that $D \mid F_{j+2}$, and so on until we see that $D \mid F_r$. So we have that $D \mid F_j$ for each $j$. Hence, we may write

$$F(X) = \sum_{i=0}^{r} F_i B_i(X) = D \sum_{i=0}^{r} F_i' B_i(X),$$

where each $F_i'$ is in $\mathbb{Z}$. Suppose that $\gcd(F_0', \ldots, F_r') = W > 1$. Then

$$F(X) = DW \sum_{i=0}^{r} F_i'' B_i(X),$$

where each $F_i''$ is in $\mathbb{Z}$. Hence,

$$\frac{F(X)}{DW} = \sum_{i=0}^{r} F_i'' B_i(X) \quad \in \mathrm{Int}(\mathbb{Z}),$$

implying that $\mathrm{d}(\mathbb{Z}, F) \geq DW$, a contradiction.

(⇐) Suppose $\gcd(F_0, \ldots, F_r) = D$. Then, as above, we may write $F(X) = \sum_{i=0}^{r} F_i B_i(X) = D \sum_{i=0}^{r} F_i' B_i(X)$, where $\gcd(F_0', \ldots, F_r') = 1$. Then $D \mid F(z)$ for every $z \in \mathbb{Z}$, implying that $D \leq \mathrm{d}(\mathbb{Z}, F)$. We apply an argument similar to that above. Among the coefficients, there is a smallest $j$ for which $F_j \neq 0$, and for such a $j$, $F(j) = F_j$. Then $\mathrm{d}(\mathbb{Z}, F) \mid F_j$. As above, it follows that $\mathrm{d}(\mathbb{Z}, F) \mid F_i$ for each $i$. Then $\mathrm{d}(\mathbb{Z}, F) \leq \gcd(F_0, \ldots, F_r) = D$. Combining $D \leq \mathrm{d}(\mathbb{Z}, F)$ and $\mathrm{d}(\mathbb{Z}, F) \leq D$ yields $D = \mathrm{d}(\mathbb{Z}, F)$.

**(1 ⇔ 3)** Suppose $\gcd(F(0), \ldots, F(r)) = M$. Recalling the Difference Table construction for polynomials in $\mathrm{Int}(\mathbb{Z})$ [8], we see immediately that $M \mid F_i$ for each $i$. Then, by the previous argument, $M \leq \gcd(F_0, \ldots, F_r)$ implies that $M \leq D$.

On the other hand, by definition, $D \mid F(0), \ldots, D \mid F(r)$. Hence, $D \leq \gcd(F(0), \ldots, F(r)) = M$. Thus $M = D$ and the result follows.

■

We remark that Narkiewicz found the following [9]:

**Theorem 2.7 (See [9], Thm. 3.4).** *If $f \in \mathbb{Z}[x]$ is a polynomial of degree $n$ and $d \in \mathbb{Z}$, then $f(\mathbb{Z}) \subseteq d\mathbb{Z}$ if and only if $d$ divides the numbers $f(i)$ for $i = 0, 1, \ldots, n$.*

Recall the familiar reducibility test for members of $\mathbb{Z}[x]$:

**Theorem 2.8 (Eisenstein's Criterion, See [5] III.6.15).** *Let $D$ be a unique factorisation domain with quotient field $F$. If $f = \sum_{i=0}^{n} a_i x^i \in D[x]$, $\deg(f) \geq 1$ and $p$ is an irreducible element of $D$ such that*

$$p \nmid a_n; \quad p \mid a_i \quad \text{for } i = 0, 1, \ldots, n-1; \quad p^2 \nmid a_0,$$

*then $f$ is irreducible in $F[x]$. If $f$ is primitive, then $f$ is irreducible in $D[x]$.*

**Example 2.9.** Let $f(X) = \frac{X^2+9X+6}{2}$. Noticing that $f(0) = 3, f(1) = 8$, and $f(2) = 14$, and applying Corollary 1.9, we have that $f(X) \in \text{Int}(\mathbb{Z})$. Further, notice that $3 \mid 6$; $3 \mid 9$; and $3^2 \not| 6$, so that $X^2 + 9X + 6$ is irreducible in $\mathbb{Z}[X]$ by Eisenstein's Criterion above.

**Theorem 2.10 (See [7], Thm. 3.13).** *For $m > 1$, a necessary and sufficient condition that the congruence*

$$ax \equiv b \pmod{m}$$

*be solvable is that $d \mid b$, where $d = \gcd(a, m)$. If this condition is satisfied, there is a unique solution modulo $\frac{m}{d}$, say $x_0$, and hence there are $d$ solutions modulo $m$, namely*

$$x \equiv x_0,\ x_0 + 1 \cdot \frac{m}{d},\ \ldots\ ,\ x_0 + (d-1)\frac{m}{d} \pmod{m}.$$

Notice that $\gcd(a, m) = 1$ implies $ax \equiv b \pmod{m}$ is solvable.

**Theorem 2.11.** *For every $m, n \in \mathbb{N}$, there are infinitely many irreducible polynomials $f(X) \in Int(\mathbb{Z})$ with leading coefficient $\frac{n}{m}$.*

**Proof** For ease of notation, let us write the falling factorial polynomials in the following manner:

$$X^{(n)} = X(X-1)\cdots(X-n+1) = \alpha_1^{(n)}X + \alpha_2^{(n)}X^2 + \ldots + \alpha_{n-1}^{(n)}X^{n-1} + \alpha_n^{(n)}X^n.$$

Note that since $X^{(n)}$ is monic for each $n$, we have $\alpha_i^{(i)} = 1$ for each $i$.

Observe that for every $m \in \mathbb{N}$, there is a least $r \in \mathbb{N}$ for which $m \mid r!$. Let us denote such a pair as $\{m, r\}$. Given any $m, n \in \mathbb{N}$, we find the pair $\{m, r\}$ and will construct a polynomial of degree $r$ fulfilling the theorem.

If $F(X)$ is an arbitrary integer-valued polynomial of degree $r$, then $F(X)$ can be written in the form

$$\begin{aligned} F(X) &= F_0 + F_1X + F_2B_2(X) + \ldots + F_{r-1}B_{r-1}(X) + F_rB_r(X) \\ &= F_0 + F_1X + F_2\tfrac{X^{(2)}}{2!} + \ldots + F_{r-1}\tfrac{X^{(r-1)}}{(r-1)!} + F_r\tfrac{X^{(r)}}{r!}. \end{aligned}$$

Since $m \mid r!$, we have $m\beta = r!$, some $\beta \in \mathbb{N}$. Let $F_2', \ldots, F_{r-1}'$ be nonnegative integers such that $F_2 = 2!F_2', \ldots, F_{r-1} = (r-1)!F_{r-1}'$ and set $F_r = n\beta$. Clearly, $F(X)$ may be written as

$$F(X) = F_0 + F_1X + F_2'X^{(2)} + \ldots + F_{r-1}'X^{(r-1)} + \frac{nX^{(r)}}{m}. \tag{2.1}$$

Now, we can rewrite Equation (2.1) as

$$F(X) = \frac{mF_0 + mF_1X + mF_2'X^{(2)} + \ldots + mF_{r-1}'X^{(r-1)} + nX^{(r)}}{m}.$$

Let us expand about the $X^{(i)}$, so that

$$F(X) = \frac{mF_0+mF_1X+mF_2'\left(\alpha_1^{(2)}X+\alpha_2^{(2)}X^2\right)+\ldots+mF_{r-2}'\left(\alpha_1^{(2)}X+\alpha_2^{(r-2)}X^2+\ldots+\alpha_{r-3}^{(r-2)}X^{r-3}+\alpha_{r-2}^{(r-2)}X^{r-2}\right)}{m}+\ldots$$
$$\ldots+\frac{mF_{r-1}'\left(\alpha_1^{(r-1)}X+\alpha_2^{(r-1)}X^2+\ldots+\alpha_{r-1}^{(r-1)}X^{(r-1)}\right)+n\left(\alpha_1^{(r)}X+\alpha_2^{(r)}X^2+\ldots+\alpha_{r-1}^{(r)}X^{r-1}+\alpha_r^{(r)}X^r\right)}{m}.$$

Recalling that $\alpha_i^{(i)}=1$ for each $i$ and combining like powers of $X$, we arrive at

$$F(X) = \frac{mF_0+X\left(mF_1+mF_2'\alpha_1^{(2)}+\ldots+mF_{r-1}'\alpha_1^{(r-1)}+n\alpha_1^{(r)}\right)+X^2\left(mF_2'+mF_3'\alpha_2^{(3)}+\ldots+mF_{r-2}'\alpha_2^{(r-2)}+mF_{r-1}'\alpha_2^{(r-1)}+n\alpha_2^{(r)}\right)}{m}$$
$$\ldots+\frac{X^{r-2}\left(mF_{r-2}'+mF_{r-1}'\alpha_{r-2}^{(r-1)}+n\alpha_{r-2}^{(r)}\right)+X^{r-1}\left(mF_{r-1}'+n\alpha_{r-1}^{(r)}\right)+nX^r}{m}.$$

Set $F_0=p$, for some prime integer $p$ such that $\gcd(p,nr!)=1$. Note that $\gcd(p,m)=1$ as well since $m \mid r!$, and that $\gcd(p,n\beta)=1$ since $n\beta \mid nr!$. Hence, $p \mid F_0$ while $p^2 \nmid F_0$ and $p \nmid F_r$. Consider the system of congruences:

$$\begin{aligned}
mF_{r-1}' &\equiv \left[-n\alpha_{r-1}^{(r)}\right] \pmod p && (2.2)\\
mF_{r-2}' &\equiv \left[-mF_{r-1}'\alpha_{r-2}^{(r-1)}-n\alpha_{r-2}^{(r)}\right] \pmod p && (2.3)\\
&\vdots\\
mF_2' &\equiv \left[-mF_3'\alpha_2^{(3)}-\ldots-mF_{r-2}'\alpha_2^{(r-2)}-mF_{r-1}'\alpha_2^{(r-1)}-n\alpha_2^{(r)}\right] \pmod p && (2.4)\\
mF_1 &\equiv \left[-mF_2'\alpha_1^{(2)}-\ldots-mF_{r-1}'\alpha_1^{(r-1)}-n\alpha_1^{(r)}\right] \pmod p. && (2.5)
\end{aligned}$$

Since $\gcd(p,m)=1$, Theorem 2.10 implies that Equation (2.2) has a solution $F_{r-1}'$. Using the value $F_{r-1}'$, we can now recursively solve Equation (2.3) for $F_{r-2}'$. Iterate this process to obtain integers $F_{r-1}', F_{r-2}', \ldots, F_1$ which solve the system. Now, set

$$\begin{aligned}
G_1 &= mF_1+mF_2'\alpha_1^{(2)}+\ldots+mF_{r-1}'\alpha_1^{(r-1)}+n\alpha_1^{(r)}\\
G_2 &= mF_2'+mF_3'\alpha_2^{(3)}+\ldots+mF_{r-2}'\alpha_2^{(r-2)}+mF_{r-1}'\alpha_2^{(r-1)}+n\alpha_2^{(r)}\\
&\vdots\\
G_{r-2} &= mF_{r-2}'+mF_{r-1}'\alpha_{r-2}^{(r-1)}+n\alpha_{r-2}^{(r)}\\
G_{r-1} &= mF_{r-1}'+n\alpha_{r-1}^{(r)},
\end{aligned}$$

so that

$$F(X)=\frac{mF_0+G_1X+G_2X^2+\ldots+G_{r-2}X^{r-2}+G_{r-1}X^{r-1}+nX^r}{m}.$$

By construction, $p \mid mF_0$, $p^2 \nmid mF_0$, $p \mid G_1$, …, $p \mid G_{r-1}$, and $p \nmid n$. Hence, the numerator of $F(X)$ is irreducible in $\mathbb{Z}[X]$ by an application of Eisenstein's Criterion.

To see that $\mathrm{d}(\mathbb{Z},F)=1$, recall that $F_r=n\beta$, and that $F_0=p$. Since we have chosen $p$ so that $\gcd(p,nr!)=1$, and $n\beta \mid nr!$, we have that $\gcd(F_0,F_r)=1$. Hence, $\gcd(F_0,F_1,\ldots,F_{r-1},F_r)=1$. By Lemma 2.6, we have $\mathrm{d}(\mathbb{Z},F)=1$.

Finally, to see that there are infinitely many such irreducible polynomials, notice that in Congruence (2.5) alone, there are infinitely many solutions $F_1$ that we might have chosen. (For, having found one such

solution, say $x_0$, there are infinitely many integers congruent to $x_0$ modulo $p$.) Translating this observation into infinitely many valid $G_1$ completes the claim.

■

Notice that by our method of constructive proof in Theorem 2.11, we make the following claim (which may be of greater intrinsic interest to the reader).

**Corollary 2.12.** *For every $m \in \mathbb{Z}$, there are infinitely-many irreducible polynomials $f(x) \in \mathbb{Z}[x]$ for which $d(\mathbb{Z}, f) = m$.*

**Proposition 2.13.** *Let $f(x) \in Int(\mathbb{Z})$ have degree $n$, and*

$$f^k(x) = \underbrace{f(x) \cdots f(x)}_{k \text{ factors}}$$

*in the usual polynomial multiplication. Then*

$$d(\mathbb{Z}, f^k) = \Big(d(\mathbb{Z}, f)\Big)^k. \tag{2.6}$$

**Proof** Recall that

$$\mathrm{d}(\mathbb{Z}, f) = \gcd(f(0), \ldots, f(n)), \tag{2.7}$$

and express $f(0), \ldots, f(n)$ in their prime decompositions:

$$\begin{aligned} f(0) &= p_1^{e_1^0} \cdots p_s^{e_s^0} \\ &\vdots \\ f(n) &= p_1^{e_1^n} \cdots p_s^{e_s^n}, \end{aligned}$$

where we slightly abuse notation: $e_j^i \in \mathbb{Z}$ is the power of the $j$th prime $p_j$ corresponding to $f(i)$.
By definition, $\gcd(f(0), \ldots, f(n)) = p_1^{m_1} \cdots p_s^{m_s}$, where $m_i = \min(e_i^0, \ldots, e_i^n)$, each $i$. Notice that

$$\begin{aligned} f^k(0) &= \Big(p_1^{e_1^0} \cdots p_s^{e_s^0}\Big)^k = p_1^{ke_1^0} \cdots p_s^{ke_s^0} \\ &\vdots \\ f^k(n) &= \Big(p_1^{e_1^n} \cdots p_s^{e_s^n}\Big)^k = p_1^{ke_1^n} \cdots p_s^{ke_s^n}. \end{aligned}$$

Again employing the definition of the greatest common divisor, we have

$$\gcd(f^k(0), \ldots, f^k(n)) = p_1^{r_1} \cdots p_s^{r_s}, \tag{2.8}$$

where $r_i = \min(ke_i^0, \ldots, ke_i^n)$, each $i$. But it is clear that

$$\begin{aligned} r_i &= \min(ke_i^0, \ldots, ke_i^n) \\ &= k\min(e_i^0, \ldots, e_i^n) \\ &= km_i \quad \text{(from above)}. \end{aligned}$$

Making this substitution into Equation (2.8), we find

$$\begin{aligned} \mathrm{d}(\mathbb{Z}, f^k(x)) &= p_1^{r_1} \cdots p_s^{r_s} \\ &= p_1^{km_i} \cdots p_s^{km_s} \\ &= (p_1^{m_1} \cdots p_s^{m_s})^k \\ &= \gcd(f(0), \ldots, f(n))^k \\ &= \mathrm{d}^k(\mathbb{Z}, f(x)), \end{aligned}$$

completing the proof. ■

**Lemma 2.14.** *Let $f(x) \in \mathbb{Z}[x]$ be such that $d(S, f) = 1$ over an infinite subset $S$ of $\mathbb{Z}$. The following hold.*

*(1) $f(x)$ is primitive in $\mathbb{Z}[x]$.*

*(2) If $f(x) \neq \pm 1$ and $f(x) = f_1(x)f_2(x)\cdots f_k(x)$, where each $f_i(x)$ is irreducible in $\mathbb{Z}[x]$, then $deg(f_i(x)) \geq 1$ for every $i \in [1, k]$.*

*(3) If $f(x) = q_1(x)\cdots q_r(x)$, where each $q_i(x)$ is irreducible in $\mathbb{Z}[x]$, then $d(S, q_i) = 1$ for every $1 \leq i \leq r$.*

**Proof** To see (1), suppose that $c(f) = m > 1$. Then $f(x) = mf'(x)$, where $f'(x)$ is primitive in $\mathbb{Z}[x]$, and $\frac{f(x)}{m} \in \mathrm{Int}(S, \mathbb{Z})$ implies $m = \pm 1$ since $\mathrm{d}(S, f) = 1$, a contradiction.
For (2), $f(x)$ image primitive over $S$ implies that $f(x)$ is primitive in $\mathbb{Z}[x]$ by (1) above. Assume without loss of generality that $f_1(x) = m \in \mathbb{Z}$. Then

$$\frac{f(x)}{m} = f_2(x)\cdots f_k(x),$$

and each $f_j(x)$, $j \geq 2$ is primitive and irreducible in $\mathbb{Z}[x]$. Since $f(x)$ is primitive, $\frac{f(x)}{m} \notin \mathbb{Z}[x]$, a contradiction.
Finally, for (3), suppose that $\mathrm{d}(S, q_i) = m > 1$ for some $i$. Then

$$f(x) = m\frac{q_i(x)}{m}q_1(x)\cdots q_r(x)$$

implies $\frac{f(x)}{m} \in \mathrm{Int}(S, \mathbb{Z})$. But $\mathrm{d}(S, f) = 1$ implies that $m = \pm 1$, a contradiction. ■

Notice that the converse of Lemma 2.14(1) is not necessarily true. Consider, for example, the familiar $f(x) = x(x-1)$ over $\mathbb{Z}$. Although $f(x)$ is primitive in $\mathbb{Z}[x]$, $f(x)$ is not image primitive over $\mathbb{Z}$, since $\mathrm{d}(\mathbb{Z}, f) = 2$.

**Lemma 2.15.** *Let $f(x) \in Int(S, \mathbb{Z})$ be of degree $r \geq 1$. The following hold.*

*(1) $f(x)$ irreducible in Int$(S,\mathbb{Z})$ implies d$(S,f)=1$.*

*(2) If $f(x)$ is image primitive over $S$, and $f(x)=f_1(x)f_2(x)\cdots f_w(x)$, with each $f_j(x)\in$ Int$(S,\mathbb{Z})$, then each $f_j(x)$ is also image primitive over $S$.*

**Proof** For (1), assume that $\mathrm{d}(S,f)=m$. Then

$$f(x)=\mathrm{d}(S,f)\frac{f(x)}{\mathrm{d}(S,f)}=m\frac{f(x)}{m},$$

with $\frac{f(x)}{m}\in \mathrm{Int}(S,\mathbb{Z})$. Then $f(x)$ irreducible in $\mathrm{Int}(S,\mathbb{Z})$ implies $m=\mathrm{d}(S,f)=\pm 1$.
For (2), let $\gamma_i=\mathrm{d}(S,f_i)$. Then for every $z\in S$, $\gamma_1\gamma_2\cdots\gamma_w$ divides $f(z)$. Since $\mathrm{d}(S,f)=1$, we have $\gamma_1\gamma_2\cdots\gamma_w=\pm 1$, implying $\gamma_i=\pm 1$ for each $i\in[1,w]$. Hence, $\mathrm{d}(S,f_i)=\pm 1$ for each $i$.

■

Note that the converse to Lemma 2.15(1) is not necessarily true. Consider $f(x)=x(x+2)$ over $\mathbb{Z}$. Since $f(0)=0$, $f(1)=3$, and $f(2)=8$, $\mathrm{d}(\mathbb{Z},f)=\gcd(0,3,8)=1$. Hence, $f(x)$ is image primitive, yet reducible in $\mathbb{Z}[x]$.

We present an interesting and somewhat surprising example of how the converse to Lemma 2.15(2) fails.

**Example 2.16.** Consider $f_3(x)=\frac{x(x-2)(x+2)}{3}$ and $f_2(x)=\frac{(x+1)(x+4)}{2}$ over $\mathbb{Z}$. Now,

$$\mathrm{d}(\mathbb{Z},f_3)=\gcd(f_3(0),f_3(1),f_3(2),f_3(3))=\gcd(0,-1,0,5)=1.$$

Similarly,

$$\mathrm{d}(\mathbb{Z},f_2)=\gcd(f_2(0),f_2(1),f_2(2))=\gcd(2,5,9)=1,$$

so both $f_3(x)$ and $f_2(x)$ are image primitive in $\mathrm{Int}(\mathbb{Z})$. Let $h(x)=f_2(x)f_3(x)$. Then

$$\mathrm{d}(\mathbb{Z},h)=\gcd(h(0),h(1),h(2),h(3),h(4),h(5))=\gcd(0,-5,0,70,320,945)=5,$$

so $h(x)=f_2(x)f_3(x)$ is not image primitive.

One may easily verify that several familiar polynomial properties (Thm 6.1, [5]) hold for $\mathrm{Int}(S,\mathbb{Z})$ as in $R[x_1,\ldots,x_n]$ (where $R$ is an integral domain). Let $f(x),g(x)\in\mathrm{Int}(S,\mathbb{Z})$. Then

- $\deg(f+g)\le\max(\deg f,\deg g)$
- $\deg(fg)=\deg(f)+\deg(g)$

Recall (Thm 6.2, [5]), that if $R$ is a ring with identity and $f,g\in R[x]$ are nonzero polynomials such that the leading coefficient of $g$ is a unit in $R$, then there exist unique polynomials $q,r\in R[x]$ such that

$$f=qg+r,\qquad \text{and } \deg(r)<\deg(g).$$

Furthermore, when $R = \mathbb{Q}$, every $q \in \mathbb{Q}$ is a unit. Notice that this division algorithm does not necessarily work for polynomials in $\text{Int}(\mathbb{Z})$.

**Example 2.17.** Consider $f(x) = \frac{(x-3)(x-4)(x-5)}{3}$ and $g(x) = \frac{(x-4)(x-5)}{2}$ over $\mathbb{Z}$. Notice that $f(x), g(x) \in \text{Int}(\mathbb{Z})$. Applying the above division algorithm, and treating $f(x)$ and $g(x)$ as members of $\mathbb{Q}[x]$, we have

$$\begin{aligned} \frac{(x-3)(x-4)(x-5)}{3} &= \left(\frac{2(x-3)}{3}\right)\left(\frac{(x-4)(x-5)}{2}\right), \quad \text{so that} \\ f(x) &= q(x)g(x) + r(x), \end{aligned}$$

where $q(x) = \frac{2(x-3)}{3}$ and $r(x) = 0$. Further, $q(x)$ and $r(x)$ are unique in $\mathbb{Q}[x]$ by the division algorithm. However, it is clear that $q(x) \notin \text{Int}(\mathbb{Z})$.

We may conclude that given two arbitrary polynomials $f(x)$ and $g(x)$ in $\text{Int}(\mathbb{Z})$, there is not necessarily a way to express them in the form $f(x) = g(x)q(x) + r(x)$ with $q(x)$ and $r(x)$ members of $\text{Int}(\mathbb{Z})$.

In the following Lemma, we present one specific case where a division algorithm may be applied for members of $\text{Int}(\mathbb{Z})$.

**Lemma 2.18.** *Let $f(x), g(x) \in$ Int$(\mathbb{Z})$. Write*

$$f(x) = \frac{f_1 f'(x)}{f_2} \qquad \text{and} \qquad g(x) = \frac{g_1 g'(x)}{g_2},$$

*where $f'(x), g'(x)$ are primitive in $\mathbb{Z}[x]$ and $\gcd(f_1, f_2) = 1 = \gcd(g_1, g_2)$. If $f'(x)$ and $g'(x)$ are monic, and if $\frac{f_1}{f_2}$ is an integer multiple of $\frac{g_1}{g_2}$, then there exist unique polynomials $q(x)$ and $r(x)$ in Int$(\mathbb{Z})$ ($\deg(r(x)) < \deg(g(x))$) such that*

$$f(x) = g(x)q(x) + r(x).$$

**Proof (Existence)** Proceed by induction on $n = \deg(f(x))$. Let us rewrite $f(x)$ and $g(x)$ for convenience:

$$f(x) = \sum_{i=0}^{n} a_i x^i \qquad \text{and} \qquad g(x) = \sum_{j=0}^{m} b_i x^i,$$

where in the notation of the above, $a_n = \frac{f_1}{f_2}$, and $b_m = \frac{g_1}{g_2}$. If $\deg(g(x)) > \deg(f(x))$ then $q(x) = 0$ and $r(x) = f(x)$ satisfies the result. Hence assume $\deg(g(x)) \leq \deg(f(x))$.

Now, if $n = 1$, then $f(x) \in \mathbb{Z}[x]$ may be written $f(x) = f_1 f'(x)$ where $f_1$ is the content of $f(x)$ and $f'(x)$ is primitive in $\mathbb{Z}[x]$. Then either $m = 1$ and $g(x)$ divides $f(x)$ or $g(x)$ fails to divide $f(x)$. In the former case, we need not proceed. In the latter, write $g(x) = g_1(x - g_0)$, and $f(x) = f_1(x - f_0)$. The assumption implies that $g_1$ divides $f_1$, say $g_1\beta = f_1$. In this case, $f(x) = \beta g(x) + \beta g_1(f_0 - g_0)$, which fulfills the lemma. Otherwise, $m = 0$, and the assumption of the lemma in this case implies that $g(x) \mid f_1$. We may write $g(x)\gamma = f_1$. Then $f(x) = f_1 f'(x) = g\gamma f'(x)$ and we have the desired result with $q(x) = \gamma f'(x)$ and $r(x) = 0$.

Suppose that the existence holds for polynomials of degree less than $n = \deg(f(x))$. Notice that the polynomial $(a_n b_m^{-1} x^{n-m})g(x)$ is a polynomial in $\text{Int}(\mathbb{Z})$ of degree $n$, with leading coefficient $a_n$. Hence,

$$f(x) - (a_n b_m^{-1} x^{n-m})g(x) = (a_n x^n + \ldots + a_0) - (a_n x^n + \ldots + a_n b_m^{-1} b_0 x^{n-m})$$

is an integer-valued polynomial of degree less than $n$. By the induction hypothesis, there are polynomials $q'(x)$ and $r(x)$ such that

$$f(x) - (a_n b_m^{-1} x^{n-m})g(x) = q'(x)g(x) + r(x) \qquad \deg(r(x)) < \deg(g(x)).$$

Therefore, if $q(x) = a_n b_m^{-1} x^{n-m} + q'(x) \in \mathrm{Int}(\mathbb{Z})$, then

$$f(x) = (a_n b_m^{-1} x^{n-m})g(x) + q'(x)g(x) + r(x) = q(x)g(x) + r(x).$$

**(Uniqueness)** Assume that $f(x) = q_1(x)g(x) + r_1(x) = q_2(x)g(x) + r_2(x)$, where $q_1(x), r_1(x), q_2(x)$ and $r_2(x)$ are members of $\mathrm{Int}(\mathbb{Z})$ and that $\deg(r_i(x)) < \deg(g(x))$ for $i = 1, 2$. In this case, we have

$$q_1(x)g(x) - q_2(x)g(x) = r_1(x) - r_2(x)$$

and hence

$$(q_1(x) - q_2(x))g(x) = r_1(x) - r_2(x).$$

But recall from the above that $\deg(r_1(x) - r_2(x)) < \deg(g(x))$. Furthermore, if $q_1(x) - q_2(x) \neq 0$, then $\deg((q_1(x) - q_2(x))g(x)) \geq \deg(g(x))$. Combining these observations necessitates that

$$q_1(x) - q_2(x) = 0 = r_1(x) - r_2(x),$$

or, equivalently, $q_1(x) = q_2(x)$ and $r_1(x) = r_2(x)$. ■

**Corollary 2.19.** *If $f(x), g(x)$ are irreducible in Int($\mathbb{Z}$), then the sufficient conditions in Lemma 2.18 above are reduced to: if $d(f) \mid d(g)$, then there exist unique polynomials $q(x)$ and $r(x)$ in Int($\mathbb{Z}$) ($\deg(r(x)) < \deg(g(x))$) such that*

$$f(x) = g(x)q(x) + r(x).$$

# Chapter 3

# The Structure of Irreducibles in Int$(S, \mathbb{Z})$

Let $f(x) \in \mathbb{Z}[x]$. Recall [5] that if $f(x)$ is primitive in $\mathbb{Z}[x]$ and is irreducible in $\mathbb{Z}[x]$, then $f(x)$ is irreducible in $\mathbb{Q}[x]$.

**Lemma 3.1.** *Let $f(x) \in Int(S, \mathbb{Z})$ be image primitive over $S$. Then there is a unique (up to associates) primitive polynomial $f'(x) \in \mathbb{Z}[x]$ and unique $n \in \mathbb{Z}$ such that*

$$f(x) = \frac{f'(x)}{n}. \tag{3.1}$$

**Proof** Write $f(x) = \frac{h(x)}{m}$, $h(x) \in \mathbb{Z}[x]$ and $m \in \mathbb{Z}$. If $h(x)$ is not primitive in $\mathbb{Z}[x]$, then write $h(x) = c(h)h_1(x)$, where $c(h)$ is the content of $h(x)$ in $\mathbb{Z}[x]$ and $h_1(x)$ is primitive in $\mathbb{Z}[x]$. Then

$$f(x) = \frac{c(h)h_1(x)}{m}.$$

Since $\mathrm{d}(S, f) = 1$, $\mathrm{d}(S, c(h)h_1(x)) = m$. Now, $\mathrm{d}(S, c(h)h_1(x)) = c(h)\mathrm{d}(S, h_1(x))$ so

$$f(x) = \frac{c(h)h_1(x)}{c(h)\mathrm{d}(S, h_1(x))} = \frac{h_1(x)}{\mathrm{d}(S, h_1)}.$$

Setting $f'(x) = h_1(x)$ and $n = \mathrm{d}(S, h_1)$ yields the desired representation.

Suppose

$$\frac{f'(x)}{n} = \frac{f''(x)}{n'},$$

with $f'(x), f''(x)$ primitive in $\mathbb{Z}[x]$ and $n, n' \in \mathbb{Z}$. Then unique factorisation in $\mathbb{Z}[x]$ and $n'f'(x) = nf''(x)$ yield $f'(x) = f''(x)$ and $n = n'$.

■

**Lemma 3.2.** *Let $f(x)$ be primitive in $\mathbb{Z}[x]$, with $deg(f) = r \geq 1$. If*

$$f(x) = f_1(x)f_2(x),$$

*where $f_1(x)$ and $f_2(x) \in \mathbb{Z}[x]$, then $d(S, f) \geq d(S, f_1)d(S, f_2)$.*

**Proof** Assume that $f(x) = f_1(x)f_2(x)$ and $\mathrm{d}(S, f) < \mathrm{d}(S, f_1)\mathrm{d}(S, f_2)$. Notice that $\frac{f_1(x)}{\mathrm{d}(S,f_1)}$ and $\frac{f_2(x)}{\mathrm{d}(S,f_2)}$ are members of $\mathrm{Int}(S, \mathbb{Z})$. Then $\mathrm{d}(S, f_1)\mathrm{d}(S, f_2) \mid f_1(x)f_2(x) = f(x)$ for every $x \in S$. By definition of the fixed divisor of $f$ over $S$, $\mathrm{d}(S, f) \geq \mathrm{d}(S, f_1)\mathrm{d}(S, f_2)$, a contradiction. ■

**Theorem 3.3.** *Let $f(x)$ be primitive in $\mathbb{Z}[x]$, and assume that $deg(f(x)) \geq 1$. The following conditions are equivalent:*

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

*(2) Either $f(x)$ is irreducible in $\mathbb{Z}[x]$ or $d(S, f) > d(S, f_1)d(S, f_2)$ for every pair of nonunit polynomials $f_1(x)$ and $f_2(x)$ such that $f(x) = f_1(x)f_2(x)$.*

**Proof** [(1) ⇒ (2)] Assume that $f(x)$ is not irreducible in $\mathbb{Z}[x]$. Assume that $\mathrm{d}(S, f) \leq \mathrm{d}(S, f_1)\mathrm{d}(S, f_2)$, where $\deg(f_1), \deg(f_2) \geq 1$, and $f_1(x)f_2(x) = f(x)$. Applying Lemma 3.2, we must have $\mathrm{d}(S, f) = \mathrm{d}(S, f_1)\mathrm{d}(S, f_2)$. Then

$$\begin{aligned}\frac{f(x)}{\mathrm{d}(S,f)} &= \frac{f_1(x)f_2(x)}{\mathrm{d}(S,f)} \\ &= \frac{f_1(x)f_2(x)}{\mathrm{d}(S,f_1)\mathrm{d}(S,f_2)} \\ &= \frac{f_1(x)}{\mathrm{d}(S,f_1)} \cdot \frac{f_2(x)}{\mathrm{d}(S,f_2)},\end{aligned}$$

so that $\frac{f(x)}{\mathrm{d}(S,f)}$ is reducible in $\mathrm{Int}(S, \mathbb{Z})$.

[(2) ⇒ (1)] Assume that

$$\frac{f(x)}{\mathrm{d}(S,f)} = h_1(x) \cdots h_r(x)$$

where each $h_i(x)$ is irreducible in $\mathrm{Int}(S, \mathbb{Z})$. Since $\frac{f(x)}{\mathrm{d}(S,f)}$ is image primitive, $\deg(h_i(x)) \geq 1$ for each $i$. By Lemma 3.1, we may write this product as

$$\frac{f(x)}{\mathrm{d}(S,f)} = \frac{h_1'(x)}{\mathrm{d}(S,h_1')} \cdots \frac{h_r'(x)}{\mathrm{d}(S,h_r')}$$

where each $h_i'(x)$ is primitive in $\mathbb{Z}[x]$. If $f(x)$ is irreducible in $\mathbb{Z}[x]$, then unique factorisation in $\mathbb{Z}[x]$ forces $r = 1$ and $\frac{f(x)}{\mathrm{d}(S,f)} = h_1(x)$ is irreducible. Otherwise, we obtain, using unique factorisation in $\mathbb{Z}[x]$, that

$$\mathrm{d}(S, f) = \mathrm{d}(S, h_1') \cdots \mathrm{d}(S, h_r'),$$

contradicting (2). ■

**Lemma 3.4.** *An element $z \in \mathbb{Z}$ is irreducible in Int$(S, \mathbb{Z})$ if and only if it is irreducible in $\mathbb{Z}$.*

**Proof** ($\Rightarrow$) Suppose $z \in \mathbb{Z}$ is irreducible in $\text{Int}(S, \mathbb{Z})$. Then $z = g(x)h(x)$, where $g(x), h(x) \in \text{Int}(S, \mathbb{Z})$, implies that either $g(x)$ or $h(x)$ is a unit in $\text{Int}(S, \mathbb{Z})$. Furthermore, the degree of both $h(x)$ and $g(x)$ must be zero as $\deg(z) = 0$. Since the units of $\text{Int}(S, \mathbb{Z})$ are $\pm 1$, $z = \pm c$, for some integer $c$, implying $z = c$ as $\mathbb{Z}$ is a unique factorisation domain. Hence, $z \in \mathbb{Z}$ is also irreducible.

($\Leftarrow$) Let us assume that $z = p(x)q(x)$ for $p(x), q(x) \in \text{Int}(S, \mathbb{Z})$. By the same argument as above, both $p(x)$ and $q(x)$ must be constants, so that $p(x) = \alpha$ and $q(x) = \beta$, and $\alpha, \beta \in \mathbb{Z}$. But since $z$ is irreducible in $\mathbb{Z}$, either $\alpha = \pm 1$ or $\beta = \pm 1$. Hence, $z$ is irreducible in $\text{Int}(S, \mathbb{Z})$, as $\pm 1$ are units for $\text{Int}(S, \mathbb{Z})$ as well as $\mathbb{Z}$.

■

The next Corollary characterizes the irreducible elements of $\text{Int}(S, \mathbb{Z})$ and follows directly from Theorem 3.3 and Lemma 3.4.

**Corollary 3.5.** *Let $f(x) = \frac{f'(x)}{n}$ be a non-unit image primitive polynomial in Int$(S, \mathbb{Z})$ expressed in the form of (3.1). $f(x)$ is irreducible in Int$(S, \mathbb{Z})$ if and only if*

*(1) $\deg(f(x)) = 0$ and $f(x)$ is a prime integer in $\mathbb{Z}$.*

*(2) $f'(x)$ is irreducible in $\mathbb{Z}[x]$ and $n = d(S, f')$.*

*(3) $n = d(S, f')$ and for every factorisation $f'(x) = f_1(x)f_2(x)$ into non-units of $\mathbb{Z}[x]$, $d(S, f') > d(S, f_1')d(S, f_2')$.*

We now apply the results of this chapter to construct some irreducible elements of $\text{Int}(S, \mathbb{Z})$ which will later be of interest.

**Corollary 3.6.** *Let the integers $i_1, i_2, \ldots, i_p$ form a complete set of residues modulo a prime $p$ and an incomplete set of residues modulo every prime $q \neq p$. Then the polynomial*

$$f_p(x) = \frac{(x - i_1)(x - i_2) \cdots (x - i_p)}{p}$$

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

Note for any prime $p$, such a sequence $\{i_j\}_{j=1}^{p}$ outlined above exists and may be chosen by the Chinese Remainder Theorem.

**Proof** Let $\mathcal{I}$ denote the set $\{i_1, \ldots, i_p\}$ outlined above, and $f(x) = (x - i_1)(x - i_2) \cdots (x - i_p)$. Note that $f(x)$ is primitive in $\mathbb{Z}[x]$ with $\deg(f(x)) = p$.

Claim: $\text{d}(\mathbb{Z}, f) = p$. For every integer $z$, $z \equiv i_j \pmod{p}$ for some $j \in [1, p]$. For such a $j$, $p \mid (z - i_j)$, so $p \mid \text{d}(\mathbb{Z}, f)$, and $p\alpha = \text{d}(\mathbb{Z}, f)$ for some $\alpha \in \mathbb{Z}$. Notice that for no prime $q \neq p$ does $q \mid \text{d}(\mathbb{Z}, f)$, since $\mathcal{I}$ fails to form a complete set of residues modulo every such $q$. Thus $\alpha = 1$ and $\text{d}(\mathbb{Z}, f) = p$.

Finally, by construction, any subset of $\mathcal{I}$ is also an incomplete set of residues modulo every prime $q \neq p$. It follows that for every polynomial $f_1(x)$ and $f_2(x)$ in $\mathbb{Z}[x]$ with $f(x) = f_1(x)f_2(x)$, we have $\text{d}(\mathbb{Z}, f_1) = \text{d}(\mathbb{Z}, f_2) = 1$ (recall $f(x)$ is primitive implies that $\deg(f_1(x))$ and $\deg(f_2(x)) \geq 1$). Hence $\text{d}(\mathbb{Z}, f) = p > \text{d}(\mathbb{Z}, f_1)\text{d}(\mathbb{Z}, f_2) = 1$ for every such $f_1(x)$ and $f_2(x)$. Applying Theorem 3.3 completes the proof.

■

**Theorem 3.7.** *For each $n \geq 1$, $B_{n,S}(x)$ is irreducible in Int$(S, \mathbb{Z})$.*

**Proof** Suppose that $B_{n,S}(x) = g(x)h(x)$, with $g(x), h(x) \in \mathrm{Int}(S, \mathbb{Z})$ such that $\deg(g(x)) = r$ and $\deg(h(x)) = s$. Then $n = r + s$. Because $\{\binom{x}{i}_S\}_{i=0}^{\infty}$ forms a basis for $\mathrm{Int}(S, \mathbb{Z})$, write

$$g(x) = g_0 B_{0,S}(x) + g_1 B_{1,S}(x) + \ldots + g_r B_{r,S}(x)$$

and

$$h(x) = h_0 B_{0,S}(x) + h_1 B_{1,S}(x) + \ldots + h_s B_{s,S}(x).$$

Then

$$r!_S g(x) = \left(\frac{r!_S}{0!_S}\right) g_0 B_{0,S}(x) + \left(\frac{r!_S}{1!_S}\right) g_1 B_{1,S}(x) + \ldots + g_r x_S^{(r)}$$

and

$$s!_S h(x) = \left(\frac{s!_S}{0!_S}\right) h_0 B_{0,S}(x) + \left(\frac{s!_S}{1!_S}\right) h_1 B_{1,S}(x) + \ldots + h_s x_S^{(s)}.$$

Now, $\frac{p!_S}{l!_S} \in \mathbb{Z}$ for every $l \leq p$ (see [2]), so

$$(r!_S g(x))(s!_S h(x)) = (r!_S s!_S)(g(x)h(x)) = (r!_S s!_S) B_{n,S} \in \mathbb{Z}[x]. \tag{3.2}$$

Then we must have

$$\frac{(r!_S s!_S)}{n!_S} = \frac{r!_S s!_S}{(r+s)!_S} \in \mathbb{Z}.$$

But (by Theorem 8, [2]) $r!_S s!_S \mid (r+s)!_S$. Hence, to avoid contradiction, we must have $s = n$ or $s = 0$. We are left with one of two cases:

(i) $s = 0 \Rightarrow h(x)$ is constant (or)

(ii) $s = n \Rightarrow r = n - s = 0 \Rightarrow g(x)$ is constant.

Without loss, let us take $s = n$, so that $g(x) = w \in \mathbb{Z}$. Then from Equation (3.2) we have
$n!_S wh(x) = n!_S B_{n,S} \in \mathbb{Z}[x]$. Since $n!_S B_{n,S}$ is monic in $\mathbb{Z}[x]$, $n!_S wh(x)$ must be monic in $\mathbb{Z}[x]$. Hence $w = \pm 1$.

Thus $B_{n,S}(x) = g(x)h(x)$ implies $B_{n,S}(x) = \pm h(x)$.

■

# Chapter 4

# Some Elements With Unique Factorisation in Int$(S, \mathbb{Z})$

**Theorem 4.1.** *Let $f(x) \in \mathbb{Z}[x]$ be of degree $d \geq 1$. If $d(S, f) = 1$, then $f(x)$ factors uniquely in Int$(S, \mathbb{Z})$.*

**Proof** $\mathbb{Z}[x]$ is a unique factorisation domain, so let $f(x) = q_1(x) \cdots q_t(x)$, with $q_i(x)$ irreducible in $\mathbb{Z}[x]$, be a unique factorisation up to order and multiplication by $\pm 1$. Since $\mathrm{d}(S, f) = 1$, $f(x)$ is primitive in $\mathbb{Z}[x]$ by Lemma 2.14(1), and $\mathrm{d}(S, q_i(x)) = 1$ for each $q_i(x)$. Assume $f(x)$ factors in $\mathrm{Int}(S, \mathbb{Z})$ as

$$f(x) = j_1(x) \cdots j_r(x),$$

where each $j_i(x)$ is irreducible in $\mathrm{Int}(S, \mathbb{Z})$.

Claim I: No $j_i(x)$ is a non-unit integer.

Proof of Claim I: Assume without loss that $j_1(x) = z \in \mathbb{Z}$ is not a unit. Then $f(x) = z j_2(x) \cdots j_r(x) \in \mathrm{Int}(S, \mathbb{Z})$ and thus $\frac{f(x)}{z} \in \mathrm{Int}(S, \mathbb{Z})$. Since $\mathrm{d}(S, f) = 1$, $z = \pm 1$, a contradiction.

Claim II: No $j_i(x) \in \mathbb{Q}[x] - \mathbb{Z}[x]$.

Proof of Claim II: Applying Lemma 3.1, $j_i(x) = \frac{j_i'(x)}{\mathrm{d}(S, j_i')}$. Then

$$f(x) = \frac{j_1'(x) \cdots j_r'(x)}{\mathrm{d}(S, j_1') \cdots \mathrm{d}(S, j_r')}.$$

Gauss's Lemma gives that the product of primitive polynomials in $\mathbb{Z}[x]$ is primitive, so the product $j_1'(x) \cdots j_r'(x)$ is a primitive polynomial. Since $\mathrm{d}(S, f) = 1$, $f(x)$ is primitive as well. Then $\mathrm{d}(S, j_1') \cdots \mathrm{d}(S, j_r')$ divides each coefficient of the polynomial $j_1'(x) \cdots j_r'(x)$, and so $\mathrm{d}(S, j_1') \cdots \mathrm{d}(S, j_r') = 1$ implies that $\mathrm{d}(S, j_i') = \pm 1$ for each $i \in [1, r]$. Hence, $j_i(x) = \pm j_i'(x) \in \mathbb{Z}[x]$ for each $i$, completing Claim II.

Finally, each $j_i(x)$ must be irreducible in $\mathbb{Z}[x]$, hence

$$f(x) = j_1(x) \cdots j_r(x) = q_1(x) \cdots q_t(x)$$

implies that $r = t$ and for some permutation of the $j_i$'s, each $j_i(x) = q_i(x)$. ■

**Example 4.2.** While image primitive polynomials in $\mathbb{Z}[x]$ factor uniquely in $\mathrm{Int}(S,\mathbb{Z})$, the same cannot be said for those in $\mathrm{Int}(S,\mathbb{Z})$. For example, let $f(x) = \frac{x(x-2)(x-4)}{3}$ and $g(x) = \frac{(x+1)(x+2)}{2}$ be polynomials in $\mathrm{Int}(\mathbb{Z})$. Since

$$\mathrm{d}(\mathbb{Z}, f) = \gcd(f(0), f(1), f(2), f(3)) = \gcd(0, 1, 0, -1) = 1$$

and

$$\mathrm{d}(\mathbb{Z}, g) = \gcd(f(0), f(1), f(2)) = \gcd(1, 3, 6) = 1,$$

we have that both $f(x)$ and $g(x)$ are image primitive on $\mathbb{Z}$. Let $h(x) = f(x)g(x)$. Since

$$\mathrm{d}(\mathbb{Z}, h) = \gcd(h(0), h(1), h(2), h(3), h(4), h(5)) = \gcd(0, 3, 0, -10, 0, 105) = 1,$$

we have $h(x)$ is image primitive over $\mathbb{Z}$. However,

$$h(x) = \frac{x(x-2)(x-4)}{3} \cdot \frac{(x+1)(x+2)}{2} = \frac{x(x-2)(x+2)}{3} \cdot \frac{(x+1)(x-4)}{2}$$

yields a non-unique factorisation in $\mathrm{Int}(\mathbb{Z})$.

**Theorem 4.3.** *Let $f(x) = \frac{f'(x)}{z} \in Int(\mathbb{Z})$, where $z \in \mathbb{Z}$ and $f'(x)$ is primitive in $\mathbb{Z}[x]$. $f(x)$ factors uniquely in $Int(\mathbb{Z})$ if the following hold:*

*(1) $deg(f(x)) = p$, where $p$ is a prime integer*

*(2) $p \mid d(\mathbb{Z}, f')$*

*(3) $p \nmid d(\mathbb{Z}, f)$*

**Proof** Assume that (1-3) hold. If $f(x)$ is irreducible in $\mathrm{Int}(\mathbb{Z})$, the claim is trivial. So assume that $f(x)$ is reducible in $\mathrm{Int}(\mathbb{Z})$. By (1), $z \leq p!$, and by (2) and (3), $p \mid z$, so $p\beta = z$ for some $\beta \in \mathbb{Z}$. Thus, $f(x) = \frac{f'(x)}{p\beta}$. By (3), say $\mathrm{d}(\mathbb{Z}, f) = r = p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$, where $p \nmid r$, and $f(x) = (p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r})\,\frac{f'(x)}{p\beta\left(p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}\right)}$. Now, either $\frac{f'(x)}{p\beta\left(p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}\right)}$ is irreducible in $\mathrm{Int}(\mathbb{Z})$ or can be factored into irreducibles. In either case,

$$f(x) = (p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r})\,\frac{f'(x)}{p\beta\,(p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r})} \tag{4.1}$$

yields a factorisation into irreducibles in $\mathrm{Int}(\mathbb{Z})$.
Suppose that $f(x) = f_1(x)f_2(x)\cdots f_j(x)$, where $f_i(x)$ is irreducible in $\mathrm{Int}(\mathbb{Z})$ for every $i$, so

$$f(x) = \frac{f'(x)}{p\beta} = q_1^{c_1}\cdots q_n^{c_n}\,\frac{f_1'(x)}{\mathrm{d}(\mathbb{Z}, f_1')}\cdots\frac{f_j'(x)}{\mathrm{d}(\mathbb{Z}, f_j')}, \tag{4.2}$$

where each $q_i$ is a prime integer, $1 \leq \deg(f_i'(x)) \leq p$ and $f_i'(x)$ is primitive in $\mathbb{Z}[x]$ for every $i$. Since $f'(x)$, $f_1'(x), \ldots, f_j'(x)$ are primitive in $\mathbb{Z}[x]$, unique factorisation in $\mathbb{Z}[x]$ implies that $p \mid \mathrm{d}(\mathbb{Z}, f_i')$ for some $i$.

Now suppose that $1 \leq \deg(f_i'(x)) < p$ for some $i$. Then $f_i'(x)$ divides $f'(x)$ in $\mathbb{Z}[x]$ and $\deg(f_1'(x)\cdots f_{i-1}'(x)f_{i+1}'(x)\cdots f_j'(x)) < p$. Then, $p \nmid \mathrm{d}(\mathbb{Z}, f_i')$ and $p \nmid \mathrm{d}(\mathbb{Z}, f_1'\cdots f_{i-1}'f_{i+1}'\cdots f_j')$ implying that $p \nmid \mathrm{d}(\mathbb{Z}, f_1')\cdots\mathrm{d}(\mathbb{Z}, f_{i-1}')\mathrm{d}(\mathbb{Z}, f_{i+1}')\cdots\mathrm{d}(\mathbb{Z}, f_j')$. Thus, $p \nmid \mathrm{d}(\mathbb{Z}, f_1')\cdots\mathrm{d}(\mathbb{Z}, f_i')\cdots\mathrm{d}(\mathbb{Z}, f_j')$, a contradiction.

Thus, $j = 1$ and Equation (4.2) is of the form

$$f(x) = \frac{f'(x)}{p\beta} = q_1^{c_1}\cdots q_n^{c_n}\frac{f_1'(x)}{\mathrm{d}(\mathbb{Z}, f_1')}. \tag{4.3}$$

Since $\frac{f_1'(x)}{\mathrm{d}(\mathbb{Z}, f_1')}$ is image primitive in $\mathbb{Z}$, it follows that

$$q_1^{c_1}\cdots q_n^{c_n} = \mathrm{d}(\mathbb{Z}, f) = p_1^{e_1}\cdots p_r^{e_r}.$$

Moreover, the primitive condition in $\mathbb{Z}[x]$ implies that $f'(x) = f_1'(x)$. Thus, the factorisation given in (4.3) is of the form

$$\begin{aligned} f(x) &= p_1^{e_1}\cdots p_r^{e_r}\frac{f'(x)}{\mathrm{d}(\mathbb{Z}, f')} && (4.4)\\ &= p_1^{e_1}\cdots p_r^{e_r}\frac{f'(x)}{p\beta p_1^{e_1}\cdots p_r^{e_r}}. && (4.5)\end{aligned}$$

Hence, the factorisation in (4.1) is actually an irreducible factorisation in $\mathrm{Int}(\mathbb{Z})$ and is obviously unique.

■

We consider a very interesting and well-known set of integer-valued polynomials named the Fermat polynomials (see [1]). If $p$ is any positive prime in $\mathbb{Z}$, let

$$\mathcal{F}_p(x) = \frac{x^p - x}{p}.$$

Fermat's Little Theorem implies that $\mathcal{F}_p(x) \in \mathrm{Int}(\mathbb{Z})$ for all positive primes $p$ in $\mathbb{Z}$. Chapman *et. al.* [1] showed that if $\mathcal{F}_p(x)$ factors non-trivially in $\mathrm{Int}(\mathbb{Z})$, then at least one factor must be a non-unit in $\mathbb{Z}$. In fact, it is shown in [1] that one possible irreducible factorisation of $\mathcal{F}_p(x)$ is

$$\left(\prod_{q\in T_p - \{p\}} q\right)\cdot\frac{x^p - x}{\left(\prod_{q\in T_p} q\right)} \tag{4.6}$$

where

$$T_p = \{q \mid q \geq 2 \text{ is prime and } q - 1 \text{ divides } p - 1\}.$$

**Corollary 4.4.** *For every prime $p$, $\mathcal{F}_p(x) = \frac{x^p - x}{p}$ factors uniquely in Int$(\mathbb{Z})$. Moreover, its unique irreducible factorsiation is given by (4.6).*

**Proof** Clearly $\mathcal{F}_p(x)$ satisfies conditions (1), (2) and (3) of Theorem 4.3, and hence has a unique factorisation in Int$(\mathbb{Z})$. The factorisation given in (4.6) follows from Corollary 2.9 in [1].

■

**Example 4.5.** Consider $\mathcal{F}_{53}(x) \in \text{Int}(\mathbb{Z})$. In this case, $T_{53} = \{2, 3, 5, 53\}$, and the unique irreducible factorisation of $\mathcal{F}_{53}(x)$ in Int$(\mathbb{Z})$ is

$$\mathcal{F}_{53}(x) = (2 \cdot 3 \cdot 5)\, \frac{x^{53} - x}{2 \cdot 3 \cdot 5 \cdot 53}.$$

Let $p \geq 2$ be a prime integer and $B_p(X)$ denote the usual $p$th Binomial Polynomial

$$B_p(X) = \frac{X(X-1)\cdots(X-p+1)}{p!}.$$

The following theorem is contained in a private communicate we obtained from Bullington [3]. Using the techniques and tools we have developed, we obtain a much more concise proof.

**Theorem 4.6.** *For each $k \geq 1$, $B_p^k(X)$ factors uniquely in Int$(\mathbb{Z})$.*

**Proof** Let $k > 0$ be given. Notice

$$B_p^k(X) = \frac{X^k(X-1)^k \cdots (X-p+1)^k}{(p!)^k},$$

and since $B_p(X)$ is irreducible, $\mathrm{d}\left(\mathbb{Z}, B_p(X)\right) = 1$ and $\mathrm{d}\left(\mathbb{Z}, B_p^k(X)\right) = \left(\mathrm{d}(\mathbb{Z}, B_p(X))\right)^k = 1^k = 1$. Assume that

$$B_p^k(X) = f_1(X) f_2(X) \cdots f_r(X),$$

where $f_i(X)$ is irreducible in Int$(\mathbb{Z})$ for each $i$. Since $\mathrm{d}\big(\mathbb{Z}, B_p^k(X)\big) = 1$, $\deg(f_i(X)) > 1$ for each $i$.
By the unique factorisation of $\mathbb{Q}[X]$,

$$f_j(X) = \frac{X^{\alpha_1^{(j)}}(X-1)^{\alpha_2^{(j)}} \cdots (X-p+1)^{\alpha_p^{(j)}}}{\mathrm{d}\left(\mathbb{Z}, X^{\alpha_1^{(j)}}(X-1)^{\alpha_2^{(j)}} \cdots (X-p+1)^{\alpha_p^{(j)}}\right)},$$

where $0 \leq \alpha_i^{(j)} \leq k$ for each $i, j$. Recalling that $B_p(p) = \binom{p}{p} = 1$,

$$B_p^k(p) = f_1(p) f_2(p) \cdots f_r(p) = 1$$

implies that

$$f_j(p) = \frac{p^{\alpha_1^{(j)}}(p-1)^{\alpha_2^{(j)}}\cdots(1)^{\alpha_p^{(j)}}}{\mathrm{d}\left(\mathbb{Z}, X^{\alpha_1^{(j)}}(X-1)^{\alpha_2^{(j)}}\cdots(X-p+1)^{\alpha_p^{(j)}}\right)} = \pm 1.$$

Hence, $\mathrm{d}\left(\mathbb{Z}, X^{\alpha_1^{(j)}}(X-1)^{\alpha_2^{(j)}}\cdots(X-p+1)^{\alpha_p^{(j)}}\right) = \pm 1 p^{\alpha_1^{(j)}}(p-1)^{\alpha_2^{(j)}}\cdots(1)^{\alpha_p^{(j)}}$ for every $j$. So

$$f_j(X) = \pm\frac{X^{\alpha_1^{(j)}}(X-1)^{\alpha_2^{(j)}}\cdots(X-p+1)^{\alpha_p^{(j)}}}{p^{\alpha_1^{(j)}}(p-1)^{\alpha_2^{(j)}}\cdots(1)^{\alpha_p^{(j)}}}$$

for every $1 \leq j \leq r$. The set $\mathcal{P} = \{0, \ldots, p-1\}$ form a complete set of residues modulo the prime $p$, so every integer $z$ is congruent to exactly one member of $\mathcal{P}$. So, for example, if $z \equiv p-4 \pmod{p}$, $p$ will divide the $(X-p+4)$ term in the numerator of $f_j(X)$ evaluated at $X = z$.

We claim that $\alpha_1^{(j)} = \alpha_2^{(j)} = \ldots = \alpha_{p-1}^{(j)} = \alpha_p^{(j)}$ for every $j$. Notice that upon justifying the claim, the proof will be complete, for the irreducibility of each $f_j(X)$ implies that $\alpha_1^{(j)} = \alpha_2^{(j)} = \ldots = \alpha_{p-1}^{(j)} = \alpha_p^{(j)} = 1$ so each $f_j(X) = B_p(X)$ and $r = k$.

Assume that $\alpha_1^{(j)} > \alpha_m^{(j)}$ for some $2 \leq m \leq p$. Then $f_j(p+m-1) \notin \mathbb{Z}$. To see this, notice that $p+m-1 \equiv m-1 \pmod{p}$ in $\mathcal{P}$ uniquely, and

$$f_j(p+m-1) = \frac{(p+m-1)^{\alpha_1^{(j)}}\cdots(p)^{\alpha_m^{(j)}}\cdots(m)^{\alpha_p^{(j)}}}{p^{\alpha_1^{(j)}}\cdots(p-m+1)^{\alpha_m^{(j)}}\cdots(1)^{\alpha_p^{(j)}}}. \tag{4.7}$$

$p^{\alpha_m^{(j)}}$ is the only multiple of $p$ in the numerator of $f_j(p+m-1)$ in Equation (4.7), because $p+m-1 < p+p$. However, we have $p^{\alpha_1^{(j)}}$ in the numerator of $f_j(p+m-1)$ in Equation (4.7), and since $\alpha_1^{(j)} > \alpha_m^{(j)}$ by assumption, $f_j(p+m-1) \notin \mathbb{Z}$. Since $j$ was arbitrary, we conclude that $\alpha_1^{(j)} \leq \alpha_m^{(j)}$ for each $1 \leq j \leq r$ and $1 \leq m \leq p$.

Now, assume that $\alpha_1^{(j)} < \alpha_m^{(j)}$ for some $2 \leq m \leq p$. We write

$$\begin{aligned} B_p^k(X) &= f_j(X)g(X) \\ &= \left(\frac{X^{\alpha_1^{(j)}}(X-1)^{\alpha_2^{(j)}}\cdots(X-p+1)^{\alpha_p^{(j)}}}{p^{\alpha_1^{(j)}}(p-1)^{\alpha_2^{(j)}}\cdots(1)^{\alpha_p^{(j)}}}\right)\cdot\left(\frac{X^{k-\alpha_1^{(j)}}(X-1)^{k-\alpha_2^{(j)}}\cdots(X-p+1)^{k-\alpha_p^{(j)}}}{p^{k-\alpha_1^{(j)}}(p-1)^{k-\alpha_2^{(j)}}\cdots(1)^{k-\alpha_p^{(j)}}}\right). \end{aligned}$$

Since $\alpha_1^{(j)} < \alpha_m^{(j)}$, $k-\alpha_1^{(j)} > k-\alpha_m^{(j)}$, and this implies that $g(p+m-1) \notin \mathbb{Z}$ by the previous argument. Hence, $\alpha_1^{(j)} \geq \alpha_m^{(j)}$ for each $m, j$. Combining the two inequalities yields $\alpha_1^{(j)} = \ldots = \alpha_p^{(j)}$ for each $j$ completing the claim.

Finally, it is clear that $f_j(X)$ irreducible in $\mathrm{Int}(\mathbb{Z})$ implies that $\alpha_1^{(j)} = \ldots = \alpha_p^{(j)} = 1$ for every $j$, and so $f_j(X) = B_p(X)$ and $r = k$, as desired.

■

It may be tempting at this moment to conjecture that if $f(x)$ is irreducible in $\mathrm{Int}(\mathbb{Z})$, then $(f(x))^k$ factors uniquely in $\mathrm{Int}(\mathbb{Z})$. However, this is not the case.

**Example 4.7.** Let $f(x) = x^2 + 10x + 15$. Applying Eisenstein's Criterion for reducibility in $\mathbb{Z}[x]$, we see that $f(x)$ is irreducible in $\mathbb{Z}[x]$ and $\mathrm{d}(\mathbb{Z}, f) = 1$. Similarly, $g(x) = 5x^2 + 14x + 84$ is irreducible

in $\mathbb{Z}[x]$ and $\mathrm{d}(\mathbb{Z}, g) = 1$. Now, let $h(x) = g(x)f(x)$. Since $\mathrm{d}(\mathbb{Z}, h) = \gcd(h(0), h(1), h(2), h(3), h(4)) = \gcd(1260, 2678, 5148, 9234, 15620) = 2$, we have $p(x) = \frac{h(x)}{\mathrm{d}(\mathbb{Z},h)} = \frac{f(x)g(x)}{2}$ is irreducible in $\mathrm{Int}(\mathbb{Z})$. However, one can verify as above that $\mathrm{d}(\mathbb{Z}, f^2 g) = 4$, so

$$p^2(x) = \frac{f(x)g(x)}{2} \cdot \frac{f(x)g(x)}{2} = g(x)\frac{f^2(x)g(x)}{4}$$

is a non-unique factorisation in $\mathrm{Int}(\mathbb{Z})$.

# Chapter 5

# Elasticity in Int$(S, \mathbb{Z})$

**Definition 5.1 (See [6]).** A set $M$ with binary operation $\star$ is a monoid if

(1) $\forall a, b, c \in M$, $a \star (b \star c) = (a \star b) \star c$.

(2) $\exists\ e \in M$ such that $e \star a = a \star e = a$ for every $a \in M$.

$M$ satisfies the group axioms of closure, associativity, possesses an identity element, but may fail to possess inverses. In general terms, if $D$ is an integral domain and

$$D^* = D \backslash \{0\},$$

then $D^*$ is a monoid under multiplication.

All monoids throughout the remainder of this work are commutative (*i.e.*, $a \star b = b \star a$ for every $a, b \in M$).

**Definition 5.2 (See [6]).** Those elements of a ring which possess both a left and a right inverse are said to be **units** of the ring.

**Definition 5.3.** In a commutative monoid $M$, $x$ is **irreducible** if and only if whenever $x = yz$ then $y$ or $z$ is a unit in $M$ (with $x, y, z \in M$).

**Example 5.4.** Let $\mathbb{N}_0 = \{0, 1, \dots\}$. Then $\mathbb{N}_0$, together with the operation $+$ is an additive monoid.

**Definition 5.5.** Let $S \subset \mathbb{N}_0$ be a submonoid of $\mathbb{N}_0$. We call $S$ a **numerical monoid** generated by $z_1, z_2, \dots, z_k$ if:

$$S =< z_1, z_2, \dots, z_k >= \{x_1 z_1 + x_2 z_2 + \dots + x_k z_k \mid x_i \in \mathbb{N}_0\}.$$

The irreducible elements of $S$ are those in the minimal generating set of a numerical monoid.

**Example 5.6.** Consider the numerical monoid generated by 3, 5 and 7:

$$S =< 3, 5, 7 >= \{0, 3, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, \dots\}.$$

Note that we do not have unique factorisation in $S$:

$$\begin{aligned} 15 &= 3+3+3+3+3 \\ &= 5+5+5 \\ &= 3+5+7 \end{aligned}$$

**Definition 5.7.** Consider an element $n$ in a monoid $S$. We define the **set of Lengths of factorisations of $n$ into irreducibles, $\mathcal{L}(n)$,** as follows:

$$\mathcal{L}(n) = \{m \mid \exists\ \alpha_1, \alpha_2, \dots, \alpha_m \text{ irreducible in } S, \text{ with } n = \alpha_1 + \alpha_2 + \dots + \alpha_m\}.$$

Note that these $\alpha_i$ are not necessarily unique. In the context of Example 5.6, $\mathcal{L}(15) = \{3, 5\}$. For ease of notation, if $S$ is a monoid, then let $S^\bullet$ denote the set of nonunits of $S$.

**Definition 5.8.** The **elasticity of n**, denoted $\rho(n)$, for some element $n$ in a monoid $S$, is defined as follows:

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

Calling once again upon Example 5.6, we see that $\rho(15) = \frac{5}{3}$. Observe that the elasticity of elements within monoids is a local character. We may extend this local character to a **global character** for $S$ by setting:

$$\rho(S) = \sup\{\rho(n) \mid n \in S^\bullet\}.$$

**Definition 5.9.** The **set of elasticities of nonunits in S**, denoted $\mathcal{R}(\mathbf{S})$, is given as follows:

$$\mathcal{R}(S) = \{\rho(x) \mid x \in S^\bullet\}.$$

Chapman *et. al.* [4] concluded the following about the global character of elasticity for numerical monoids:

**Theorem 5.10 (See [4], Thm. 2.1).** *Let $S =< a_1, \dots, a_t >$ be a numerical monoid with $t > 1$, where $a_1 < a_2 < \dots < a_t$ is a minimal set of generators for $S$. Then $\rho(S) = \frac{a_t}{a_1}$.*

The following definition of full elasticity was also established by Chapman *et. al.,*:

**Definition 5.11 (See [4], Defn 1.2).** Let $M$ be a commutative cancellative monoid[1]. If $\rho(M) < \infty$, then $M$ is **fully elastic** if

[1] A monoid $(M, *)$ is cancellative if for all $a, b, c \in M$, $a * b = a * c$ always implies that $b = c$ and $b * a = c * a$ always implies that $b = c$.

$$\mathcal{R}(M) = \mathbb{Q} \cap [1, \rho(M)].$$

If $\rho(M) = \infty$, then $M$ is **fully elastic** if

$$\mathcal{R}(M) = \mathbb{Q} \cap [1, \infty).$$

We say that an integral domain $D$ is fully elastic if its multiplicative monoid $D^*$ is fully elastic.

Chapman *et. al.,* showed that any numerical monoid $S$ which requires more than one generator is not fully elastic [4, Thm 2.2]. Furthermore, in this same reference, it is shown that if $D$ is a ring of integers in finite extension of $\mathbb{Q}$ with class number $p^k$, where $p$ is a prime, then $D$ is fully elastic [4, Cor 3.10].

**Proposition 5.12.** *Let $S \subseteq \mathbb{Z}$ with $|S| = \infty$.*

***(1)*** *The elasticity of $Int(S, \mathbb{Z})$ is infinite (i.e., $\rho(Int(S, \mathbb{Z})) = \infty$).*

***(2)*** *For every $f(x) \in Int(S, \mathbb{Z})$ with $f(x) \neq \pm 1$ or 0, $1 \leq \rho(f(x)) < \infty$.*

**Proof** For **(1)**, see Proposition 1.7 of [1].

For **(2)**, any irreducible polynomial $p(x) \in \text{Int}(S, \mathbb{Z})$, has $\rho(p(x)) = 1$. What remains to be shown is that $\max \mathcal{L}(p(x)) < \infty$ for every polynomial $p(x)$ in $\text{Int}(S, \mathbb{Z})$. Let $p(x)$ be a polynomial in $\text{Int}(S, \mathbb{Z})$ of degree $m$, and let $p(x)$ be reducible. Then

$$p(x) = (z_1 \cdots z_k) p_1(x) \cdots p_t(x),$$

where each $z_i$ is a prime integer and each $p_j(x)$ is an irreducible member of $\text{Int}(S, \mathbb{Z})$ of degree greater than or equal to 1. So $\max \mathcal{L}(p(x)) \geq k + t$. For $\max \mathcal{L}(p(x)) = \infty$ to be true, either $\deg(p(x)) = \infty$ or $k = \infty$ or both $\deg(p(x)) = \infty$ and $k = \infty$ simultaneously. We know that the degree of $p(x)$ is defined as some finite number $m$; hence, $\deg(p(x)) < \infty$. If $k = \infty$, we would have that some positive integer could be written as an infinite product of primes, which contradicts the Fundamental Theorem of Arithmetic. Hence, $\max \mathcal{L}(p(x)) < \infty$ for every polynomial $p(x)$ in $\text{Int}(S, \mathbb{Z})$, and $\rho(p(x)) = \frac{\max \mathcal{L}(p(x))}{\min \mathcal{L}(p(x))} < \infty$.

■

Consider $f_p(X)$:

$$f_p(X) = \frac{(X - i_1)(X - i_2) \cdots (X - i_{p-1})(X - i_p)}{p}, \tag{5.1}$$

where $\mathcal{I} = \{i_1, i_2, \ldots, i_{p-1}, i_p\}$ form a complete set of residues modulo the prime $p$ and fail to form a complete set of residues modulo every prime $q < p$. To see that $f_p(X)$ is irreducible over $\text{Int}(\mathbb{Z})$, apply Theorem 3.3, and let $g(x)$ and $h(x) \in \mathbb{Z}[X]$ be such that $1 \leq \deg(g(x)), \deg(h(x)) < p$ and

$$g(X)h(X) = (X - i_1)(X - i_2) \cdots (X - i_{p-1})(X - i_p).$$

By the construction of $\mathcal{I}$, $\deg(h(x)) < p$ implies $\text{d}(\mathbb{Z}, h) = 1$, and a similar argument implies $\text{d}(\mathbb{Z}, g) = 1$. Hence, for every such $g(x)$ and $h(x)$, we have $\text{d}(\mathbb{Z}, g(x)h(x)) = p > \text{d}(\mathbb{Z}, g(x))\text{d}(\mathbb{Z}, h(x)) = 1$, implying $f_p(X)$ is irreducible in $\text{Int}(\mathbb{Z})$.

From Equation (5.1), let us denote $f_p(X) = \frac{h_p(X)}{p}$, so that $h_p(X) = (X - i_1)(X - i_2)\cdots(X - i_{p-1})(X - i_p)$ is monic in $\mathbb{Z}[X]$.

**Lemma 5.13.** *In Int*$(\mathbb{Z})$, $\mathcal{L}\left(h_p^k(X)\right) = \{2j + (k-j)p \quad : \quad 0 \leq j \leq k\}$.

**Proof** Let $h_p(X)$ be as above. We induct on $k$. Suppose that $k = 1$. Then

$$h_p(X) = (X - i_1)(X - i_2)\cdots(X - i_p) = p\left(\frac{(X - i_1)(X - i_2)\cdots(X - i_p)}{p}\right),$$

so that $p, 2 \in \mathcal{L}\left(h_p^1(X)\right)$. Assume that $h_p(X) = \frac{g(X)}{g_1}\frac{h(X)}{h_1}$, where $g(X), h(X) \in \mathbb{Z}[x]$ are such that $\deg(g(X)), \deg(h(X)) < p$, $g_1, h_1 \in \mathbb{Z}$, and $\frac{g(X)}{g_1}, \frac{h(X)}{h_1} \in \mathrm{Int}(\mathbb{Z})$. Since $\deg(g(X)), \deg(h(X)) < p$, by our construction of $\mathcal{I}$, $\mathrm{d}(\mathbb{Z}, g) = 1 = \mathrm{d}(\mathbb{Z}, h)$. Hence $g_1 = \pm 1 = h_1$, and we have exhausted all factorisations of $h_p(X)$. Then, $\mathcal{L}\left(h_p^1(X)\right) = \{2, p\}$ and the claim holds for the base case.

Suppose that the claim holds for every $k \leq n$. Then, by assumption,

$$\mathcal{L}\left(h_p^n(X)\right) = \{np, (n-1)p + 2, \ldots, p + 2(n-1), 2n\}. \tag{5.2}$$

Consider $h_p^{n+1}(X)$:

$$\begin{aligned} h_p^{n+1}(X) &= h_p^n(X) \cdot h_p(X) \\ &= \left(h_p^n(X)\right)\left[(X - i_1)\cdots(X - i_p)\right] \qquad (5.3) \\ &= \left(h_p^n(X)\right)\left[p\left(\frac{(X - i_1)\cdots(X - i_p)}{p}\right)\right]. \qquad (5.4) \end{aligned}$$

Combining Equations (5.3) and (5.4), we see that for every $z \in \mathcal{L}\left(h_p^n(X)\right)$, both $z + p$ and $z + 2 \in \mathcal{L}\left(h_p^{n+1}(X)\right)$. Hence, $\{2j + (n+1-j)p \quad : \quad 0 \leq j \leq n+1\} \subseteq \mathcal{L}(h_p^{n+1}(X))$. To complete the proof, we must show that $\mathcal{L}(h_p^{n+1}(X)) \subseteq \{2j + (n+1-j)p \quad : \quad 0 \leq j \leq n+1\}$.

Suppose that

$$h_p^{n+1}(X) = \alpha g(X), \tag{5.5}$$

where $g(X) \in \mathrm{Int}(\mathbb{Z})$ and $\alpha \in \mathbb{Z}$. Then $\alpha \mid \mathrm{d}(\mathbb{Z}, h_p^{n+1}) = p^{n+1}$. We have two cases to consider.

*Case 1*: $\alpha > 1$. Then $\alpha = p^r$, some $r$ $(1 \leq r \leq n+1)$. Notice that we may write $g(X) = \frac{g'(X)}{\tilde{g}}$, where $g'(X)$ is primitive in $\mathbb{Z}[X]$ and $\tilde{g} \in \mathbb{Z}$. Then

$$h_p^{n+1}(X) = p^r \frac{g'(X)}{\tilde{g}}. \tag{5.6}$$

By unique factorisation in $\mathbb{Z}[x]$, we have $g'(X) = (X - i_1)^{n+1}\cdots(X - i_p)^{n+1}$, and by our choice of the congruence system $\mathcal{I}$, we have $\tilde{g} = p^s$, some s $(1 \leq s \leq n+1)$. We rewrite Equation (5.6) so that

$$h_p^{n+1}(X) = \frac{p^r g'(X)}{p^s},$$

and since $h_p^{n+1}(X)$ is monic in $\mathbb{Z}[X]$, we have $r = s$ and hence

$$h_p^{n+1}(X) = p^r \frac{g'(X)}{p^r} = p^r \frac{(X-i_1)^{n+1}\cdots(X-i_p)^{n+1}}{p^r}, \tag{5.7}$$

where $1 \leq r \leq n+1$. Since we consider lengths of factorisations of $h_p^{n+1}(X)$ as products of irreducibles in $\mathrm{Int}(\mathbb{Z})$, we rewrite Equation (5.7):

$$\begin{aligned} h_p^{n+1}(X) &= p^r \left( \frac{(X-i_1)^r \cdots (X-i_p)^r}{p^r} \right) (X-i_1)^{n+1-r} \cdots (X-i_p)^{n+1-r} \\ &= p^r \left(f_p(X)\right)^r (X-i_1)^{n+1-r} \cdots (X-i_p)^{n+1-r}. \end{aligned}$$

We have constructed the above set of factorisations in the only ways possible given the constraints of $\mathcal{I}$, and the length of such a factorisation is $2r + (n+1-r)p \in \{2j + (n+1-j) \quad : \quad 0 \leq j \leq n+1\}$.

*Case 2*: $\alpha = 1$. Then

$$h_p^{n+1}(X) = \frac{g_1(X)}{z_1} \cdots \frac{g_m(X)}{z_m},$$

where $g_j(X)$ is primitive in $\mathbb{Z}[X]$ for each $j$. Then the product $g_1(X)\cdots g_m(X)$ is also primitive in $\mathbb{Z}[X]$, so it must be that $(z_1 \cdots z_m) = \pm 1$. This factorisation is just a factorisation in $\mathbb{Z}[X]$, with length (regardless of the value of $m$, for $\mathcal{L}(h_p^{n+1}(X))$ concerns factorisations into *irreducibles*), of

$$(n+1)p \in \{2j + (n+1-j) \quad : \quad 0 \leq j \leq n+1\}.$$

Hence, $\mathcal{L}\left(h_p^{n+1}(X)\right) \subseteq \{2j + (n+1-j) \quad : \quad 0 \leq j \leq n+1\}$, and the induction is complete.

■

**Lemma 5.14.** *In Int($\mathbb{Z}$), $\mathcal{L}\left(h_p^k(X) f_p^s(X)\right) = \{2j + (k-j)p + s \quad : \quad 0 \leq j \leq k\}$, for natural numbers $k$ and $s$.*

**Proof** Let $h_p(X)$ and $f_p(X)$ be as prescribed. Having Lemma 5.13, we induct on $s$.

Suppose $s = 1$. Then

$$h_p^k(X) f_p(X) = (X-i_1)^k \cdots (X-i_p)^k \left( \frac{(X-i_1)\cdots(X-i_p)}{p} \right).$$

Recall that $\mathcal{L}(h_p^k(X)) = \{2j + (k-j)p \quad : \quad 0 \leq j \leq k\}$. Since $f_p(X)$ is irreducible in $\mathrm{Int}(\mathbb{Z})$, we know that for every factorisation of $h_p^k(X)$, we may add 1 to its length, so that $\{2j + (k-j)p + 1 \quad 0 \leq j \leq k\} \subseteq \mathcal{L}(h_p^k(X) f_p(X))$. We must show that $\mathcal{L}(h_p^k(X) f_p(X)) \subseteq \{2j + (k-j)p + 1 \quad 0 \leq j \leq k\}$. Suppose that

$$h_p^k(X) f_p(X) = \alpha g_1(X) g_2(X) \cdots g_m(X), \tag{5.8}$$

where $g_j(X)$ is irreducible in $\mathrm{Int}(S, \mathbb{Z})$ and $\alpha \in \mathbb{Z}$. By Lemma 3.1, we have $g_j(X) = \frac{g_j'(X)}{\mathrm{d}(\mathbb{Z}, g_j')}$ for each $j$, where $g_j'(X)$ is primitive in $\mathbb{Z}[X]$. Then $\alpha \mid \mathrm{d}(\mathbb{Z}, h_p^k(X) f_p(X)) = p^k$. We consider two cases.

*Case 1a*: $\alpha = 1$. Then

$$h_p^k(X)f_p(X) = \frac{g_1'(X)}{\mathrm{d}(\mathbb{Z}, g_1')} \cdots \frac{g_m'(X)}{\mathrm{d}(\mathbb{Z}, g_m)},$$

and the product $g_1'(X) \cdots g_m'(X)$ is primitive in $\mathbb{Z}[X]$. By the unique factorisation in $\mathbb{Q}[X]$, $\mathrm{d}(\mathbb{Z}, g_1') \cdots \mathrm{d}(\mathbb{Z}, g_m') = p$, implying that $\mathrm{d}(\mathbb{Z}, g_j') = p$ for some $j$ and that $\mathrm{d}(\mathbb{Z}, g_i') = \pm 1$ for each $i \neq j$. Moreover, $g_1'(X) \cdots g_m'(X) = (X - i_1)^{k+1} \cdots (X - i_p)^{k+1}$. By construction of $\mathcal{I}$, $\mathrm{d}(\mathbb{Z}, g_j') = p$ and $\frac{g_j'(X)}{\mathrm{d}(\mathbb{Z}, g_j')}$ irreducible in $\mathrm{Int}(\mathbb{Z})$ implies that $\frac{g_j'(X)}{\mathrm{d}(\mathbb{Z}, g_j')} = f_p(X)$. Hence, the length of such a factorisation is $pk + 1 \in \{2j + (k - j)p + 1 \quad 0 \leq j \leq k\}$.

*Case 1b*: $\alpha > 1$. Then $\alpha = p^r$, some $r$ $(1 \leq r \leq k)$, and

$$h_p^k(X)f_p(X) = p^r \frac{g_1'(X)}{\mathrm{d}(\mathbb{Z}, g_1')} \cdots \frac{g_m'(X)}{\mathrm{d}(\mathbb{Z}, g_m)}. \tag{5.9}$$

By unique factorisation in $\mathbb{Q}[X]$, we have that $g_1'(X) \cdots g_m'(X) = (X - i_1)^{k+1} \cdots (X - i_p)^{k+1}$, and by our choice of $\mathcal{I}$, we have $\mathrm{d}(\mathbb{Z}, g_i') \mid p^{k+1}$, for each $i$. Hence, $\mathrm{d}(\mathbb{Z}, g_i') = p^{\alpha_i}$, where $0 \leq \alpha_i \leq k + 1$. We rewrite Equation (5.9):

$$h_p^k(X)f_p(X) = p^r \frac{g_1'(X)}{p^{\alpha_1}} \cdots \frac{g_m'(X)}{p^{\alpha_m}}, \tag{5.10}$$

and for $g_i(X)$ to be integer-valued over $\mathbb{Z}$, we rewrite Equation (5.10):

$$h_p^k(X)f_p(X) = p^r \left( \frac{(X - i_1)^{\alpha_1} \cdots (X - i_p)^{\alpha_1}}{p^{\alpha_1}} \right) \cdots \left( \frac{(X - i_1)^{\alpha_m} \cdots (X - i_p)^{\alpha_m}}{p^{\alpha_m}} \right). \tag{5.11}$$

Notice that this is the only way to write Equation (5.10) as a product of irreducibles in $\mathrm{Int}(\mathbb{Z})$ given our construction of $\mathcal{I}$. For ease of representation, we condense Equation (5.11):

$$h_p^k(X)f_p(X) = p^r \left( \frac{(X - i_1)^r \cdots (X - i_p)^r}{p^r} \right) \left( \frac{(X - i_1)^1 \cdots (X - i_p)^1}{p} \right) ((X - i_1) \cdots (X - i_p))^{k-r},$$

and the length of such a factorisation is $2r + (k - r)p + 1 \in \{2j + (k - j)p + 1 \quad 0 \leq j \leq k\}$. Hence, $\mathcal{L}(h_p^k(X)f_p(X)) \subseteq \{2j + (k - j)p + 1 \quad 0 \leq j \leq k\}$, and the hypothesis holds for the base case.

Suppose that the claim holds for every $s \leq n$. Then

$$\mathcal{L}(h_p^k(X)f_p^n(X)) = \{2j + (k - j)p + n \quad : \quad 0 \leq j \leq k\}.$$

Consider $h_p^k(X)f_p^{n+1}(X)$:

$$\begin{aligned} h_p^k(X)f_p^{n+1}(X) &= \left(h_p^k(X)f_p^n(X)\right) f_p(X) \\ &= h_p^k(X)f_p^n(X) \left( \tfrac{(X - i_1) \cdots (X - i_p)}{p} \right). \end{aligned}$$

Hence, for every $z \in \mathcal{L}(h_p^k(X)f_p^n(X))$, $z+1 \in \mathcal{L}(h_p^k(X)f_p^{n+1}(X))$. Thus,
$\{2j+(k-j)p+(n+1) \quad : \quad 0 \leq j \leq k\} \subseteq \mathcal{L}(h_p^k(X)f_p^{n+1}(X))$. As in the base case, we need to show that $\mathcal{L}(h_p^k(X)f_p^{n+1}(X)) \subseteq \{2j+(k-j)p+(n+1) \quad : \quad 0 \leq j \leq k\}$.
As above, suppose that

$$h_p^k(X)f_p^{n+1}(X) = \alpha g_1(X)\cdots g_m(X), \tag{5.12}$$

where $g_i(X)$ is irreducible in $\mathrm{Int}(\mathbb{Z})$ and $\alpha \in \mathbb{Z}$. By Lemma 3.1, we have $g_j(X) = \frac{g_j'(X)}{\mathrm{d}(\mathbb{Z},g_j')}$ for each $j$, where $g_j'(X)$ is primitive in $\mathbb{Z}[X]$. Then $\alpha \mid \mathrm{d}(\mathbb{Z}, h_p^k(X)f_p^{n+1}(X)) = p^k$. We consider two cases.
*Case 2a*: $\alpha = 1$. Then

$$h_p^k(X)f_p^{n+1}(X) = \frac{g_1'(X)}{\mathrm{d}(\mathbb{Z},g_1')}\cdots\frac{g_m'(X)}{\mathrm{d}(\mathbb{Z},g_m')}, \tag{5.13}$$

and the product $g_1'(X)\cdots g_m'(X)$ is primitive in $\mathbb{Z}[X]$. By the unique factorisation of $\mathbb{Q}[X]$, $\mathrm{d}(\mathbb{Z},g_1')\cdots\mathrm{d}(\mathbb{Z},g_m') = p^{n+1}$, implying that $\mathrm{d}(\mathbb{Z},g_j') = p^\beta$ $(0 \leq \beta \leq n+1)$. Further,
$g_i'(X) = (X-i_1)^{b_1}\cdots(X-i_p)^{b_p}$ for $0 \leq b_j \leq k+n+1$, by unique factorisation in $\mathbb{Z}[X]$. Then

$$\frac{g_j'(X)}{\mathrm{d}(\mathbb{Z},g_j')} = \frac{(X-i_1)^{b_1}\cdots(X-i_p)^{b_p}}{p^\beta}$$

irreducible in $\mathrm{Int}(\mathbb{Z})$ implies that, given our construction of $\mathcal{I}$, either $\frac{g_j'(X)}{\mathrm{d}(\mathbb{Z},g_j')} = f_p(X)$
(with $b_1 = \ldots = b_p = \beta = 1$), or $g_j'(X)$ is irreducible in $\mathbb{Z}[X]$ with $\mathrm{d}(\mathbb{Z},g_j') = 1$. But such a factorisation can be reduced to

$$h_p^k(X)f_p^{n+1}(X) = (X-i_1)^k\cdots(X-i_p)^k\left(\frac{(X-i_1)\cdots(X-i_p)}{p}\right)^{n+1},$$

whose length is $pk+n+1 \in \{2j+(k-j)p+(n+1) \quad : \quad 0 \leq j \leq k\}$.
*Case 2b*: $\alpha > 1$. Then $\alpha = p^r$, some $r$ $(1 \leq r \leq k)$. In Equation (5.12), have

$$h_p^k(X)f_p^{n+1}(X) = p^r\frac{g_1'(X)}{\mathrm{d}(\mathbb{Z},g_1')}\cdots\frac{g_m'(X)}{\mathrm{d}(\mathbb{Z},g_m')}. \tag{5.14}$$

By the unique factorisation of $\mathbb{Q}[X]$, we have $(g_1'(X))\cdots(g_m'(X)) = (X-i_1)^{k+n+1}\cdots(X-i_p)^{k+n+1}$, and by our choice of $\mathcal{I}$, we have $\mathrm{d}(\mathbb{Z},g_i') \mid p^{k+n+1}$ for each $i$. Hence, $\mathrm{d}(\mathbb{Z},g_i') = p^{\alpha_i}$, where $0 \leq \alpha_i \leq k+n+1$ for each $i$. We rewrite Equation (5.14):

$$h_p^k(X)f_p^{n+1}(X) = p^r\frac{g_1'(X)}{p^{\alpha_1}}\cdots\frac{g_m'(X)}{p^{\alpha_m}}, \tag{5.15}$$

and for $g_i(X)$ to be integer-valued over $\mathbb{Z}$, and given our choice of $\mathcal{I}$, we rewrite Equation (5.15):

$$h_p^k(X)f_p^{n+1}(X) = p^r\left(\frac{(X-i_1)^{\alpha_1}\cdots(X-i_m)^{\alpha_1}}{p^{\alpha_1}}\right)\cdots\left(\frac{(X-i_1)^{\alpha_m}\cdots(X-i_m)^{\alpha_m}}{p^{\alpha_m}}\right), \tag{5.16}$$

Notice that this is the only way to write Equation (5.15) as a product of irreducibles given our construction of $\mathcal{I}$. For ease of representation, we condense Equation (5.16):

$$h_p^k(X)f_p^{n+1}(X) = p^r\left(\frac{(X-i_1)^{r}\cdots(X-i_m)^{r}}{p^r}\right)\cdots\left(\frac{(X-i_1)\cdots(X-i_p)}{p}\right)^{n+1}(X-i_1)^{k-r}\cdots(X-i_p)^{k-r},$$

and the length of such a factorisation is $2r + p(k-r) + n + 1 \in \{2j + (k-j)p + (n+1) \quad : \quad 0 \leq j \leq k\}$. Hence, $\mathcal{L}(h_p^k(X)f_p^{n+1}(X)) \subseteq \{2j + (k-j)p + (n+1) \quad : \quad 0 \leq j \leq k\}$, and the induction is complete.

■

**Corollary 5.15.** *In Int($\mathbb{Z}$), for all primes $p$ and $k, s \in \mathbb{N}$,*

$$\rho(h_p^k(X)f_p^s(X)) = \frac{kp+s}{2k+s}.$$

**Lemma 5.16.** *Every rational number larger than 1, written in lowest terms, can be written in the form $\frac{kp+s}{2k+s}$, for $k > s \geq 0 \in \mathbb{Z}$ and $p > 2$ a prime integer.*

**Proof** Let $t > u \geq 2$ be given, so that $\gcd(t,u) = 1$. We wish to show that there are integers $k > s \geq 0$, and a prime integer $p$ for which we can write

$$\frac{kp+s}{2k+s} = \frac{t}{u}.$$

Set $k = t - u$ and $s = up - 2t$, and choose $p$ so that $s \geq 0$. In this case,

$$\begin{aligned}\frac{kp+s}{2k+s} &= \frac{(t-u)p + up - 2t}{(t-u)2 + up - 2t} \\ &= \frac{tp-2t}{up-2u} \\ &= \frac{t(p-2)}{u(p-2)} \\ &= \frac{t}{u},\end{aligned}$$

since $p > 2$.

■

**Theorem 5.17.** *Int($\mathbb{Z}$) is fully elastic.*

**Proof** For every $q \in \mathbb{Q}$ larger than 1, we may write $q = \frac{t}{u}$, where $\gcd(t,u) = 1$. Further, by Lemma 5.16, there are integers $k > s \geq 0$ and a prime $p > 2$ for which $q = \frac{t}{u} = \frac{kp+s}{2k+s}$. For such $k, s$ and $p$,

$$\rho\left(h_p^k(X) f_p^s(X)\right) = \frac{kp+s}{2k+s} = \frac{t}{u},$$

by Lemma 5.14. Hence, $\forall q \in \mathbb{Q}$ larger than 1, there is an $f(X) \in \text{Int}(\mathbb{Z})$ for which $\rho(f(X)) = q$.

■

We now proceed to show (analogously) that $\text{Int}(S,\mathbb{Z})$ is fully elastic for every $S \subseteq \mathbb{Z}$, $|S| = \infty$.

**Definition 5.18.** Let $S \subseteq \mathbb{Z}$ and $p$ a prime integer. Define

$$\text{CRS}_S(p) = \{m_1, \ldots, m_r\} \text{ with the properties that}$$

- $m_j \equiv m_i \pmod{p} \Rightarrow j = i$, and
- $s \equiv m_j \pmod{p}$ for every $s \in S$ and some $1 \leq j \leq r$.

**Lemma 5.19.** *Let $S \subseteq \mathbb{Z}$ with $|S| = \infty$. For every $m \in \mathbb{N}$, there is a prime $p \in \mathbb{Z}$ for which $|CRS_S(p)| \geq m$.*

**Proof** Let $m > 0$ be given, and suppose that $|\text{CRS}_S(p)| < m$ for every prime $p \in \mathbb{Z}$. Since $S \subseteq \mathbb{Z}$, $S$ is countable and so we may list the members of $S$: $\{s_i\}_{i=1}^{\infty}$.

Either

i infinitely many $s_i \leq 0$, or

ii infinitely many $s_i \geq 0$.

Without loss, suppose that $S$ is such that (ii) holds. We may order the positive $\{s_i\}_{i=1}^{\infty}$ such that

$$s_1 \leq s_2 \leq \cdots \leq s_m \leq s_{m+1} \leq \cdots$$

Choose a prime $q > s_m$. Then there are at least $m$ (mutually incongruent) elements of $S$ less than $q$, so $|\text{CRS}_S(q)| \geq m$, a contradiction.

■

**Lemma 5.20.** *For every $n \in \mathbb{N}$ there is an irreducible polynomial $p(x) \in Int(S,\mathbb{Z})$ of degree $\geq n$ which is a product of linear factors in $\mathbb{Q}[x]$.*

**Proof** Let $n \in \mathbb{N}$ be given. We construct an irreducible polynomial $p(x) \in \text{Int}(S,\mathbb{Z})$ such that $\deg(f) \geq n$. By Lemma 5.19, there is a prime $p$ such that $|\text{CRS}_S(p)| = j \geq m$. Let

$$\text{CRS}_S(p) = \{a_1, \ldots, a_j\}.$$

Then $f(x) = \frac{(x-a_1)\cdots(x-a_j)}{p} \in \text{Int}(S,\mathbb{Z})$, since for every $x \in S$, $x \equiv a_i \pmod{p}$ (some $1 \leq i \leq j$). Let $\{b_1, \ldots, b_j\}$ be such that

$$\begin{aligned} b_1 &\equiv a_1 \pmod{p} \\ &\vdots \\ b_j &\equiv a_j \pmod{p} \end{aligned}$$

and $\{b_1, \ldots, b_j\}$ does not form (or contain) any $\mathrm{CRS}_S(q)$ for any other prime $q$. (This is possible by the Chinese Remainder Theorem). Let

$$g(x) = \frac{(x-b_1)\cdots(x-b_j)}{p}.$$

Then $\mathrm{d}(S, g) = 1$, and since any proper subset of $\{b_1, \ldots, b_j\}$ does not constitute $\mathrm{CRS}_S(p)$, $\frac{l(x)}{p} \notin \mathrm{Int}(S, \mathbb{Z})$ for any $l(x)$ that properly divides $(x-b_1)\cdots(x-b_j)$ in $\mathbb{Z}[x]$. Hence, applying Theorem 3.3, $g(x)$ is irreducible in $\mathrm{Int}(S, \mathbb{Z})$.

■

**Theorem 5.21.** *Let $q = \frac{t}{u} \in \mathbb{Q}$, $t > u \geq 2 \in \mathbb{N}$ be given. Then there is a polynomial $f(x) \in Int(S, \mathbb{Z})$ for which $\rho(f(x)) = \frac{t}{u}$. Equivalently, $Int(S, \mathbb{Z})$ is fully elastic for $S \subseteq \mathbb{Z}$, $|S| = \infty$.*

**Proof** Let $q = \frac{t}{u}$ be given as above. Set $k = t - u$, $s = up - 2t$, and choose the prime $p$ large enough so that $s \geq 0$. Then, as in Lemma 5.16, $\frac{kp+s}{2k+s} = \frac{t}{u}$.

Notice that for any choice of $p' \in \mathbb{N}$, $p' > p$, and $k = t - u$, $s = up' - 2t$, we will still have $\frac{kp'+s}{2k+s} = \frac{t}{u}$.

So by Lemma 5.19, find a prime $p' > p$ such that $|\mathrm{CRS}_S(p')| = j > p$. As in the constructive proof of Lemma 5.20, let

$$g_{p'}(x) = \frac{(x-b_1)\cdots(x-b_j)}{p'},$$

where $\mathcal{I} = \{b_1, \ldots, b_j\}$ forms a $\mathrm{CRS}_S(p')$ and fails to form a $\mathrm{CRS}_S(q)$ for primes $q \neq p'$. Notice that by our choice of $p'$, $j > p$. Then $g_{p'}(x)$ is irreducible in $\mathrm{Int}(S, \mathbb{Z})$. Set $h_{p'}(x) = (x-b_1)\cdots(x-b_j)$, and $f_{p'}(x) = \frac{(x-b_1)\cdots(x-b_j)}{p'}$. It is then straightforward to verify that if one replaces $h_p(x)$ and $f_p(x)$ with $h_{p'}(x)$ and $f_{p'}(x)$, respectively, in Lemmas 5.13 and 5.14, we have the following results:

$$\mathcal{L}(h_{p'}^k(x)) = \{2i + (k-i)j \ : \ 0 \leq i \leq k\}$$

and

$$\mathcal{L}(h_{p'}^k(x) f_{p'}^s(x)) = \{2i + (k-i)j + s \ : \ 0 \leq i \leq k\}$$

since no steps in the proof of either of the Lemmas 5.13 or 5.14 were specific to $\mathrm{Int}(\mathbb{Z})$. Moreover, one may freely replace $\mathrm{d}(\mathbb{Z}, f)$ with $\mathrm{d}(S, f)$ when necessary as they behave identically in such a context.

Hence, we conclude that

$$\rho(h_{p'}^k(x) f_{p'}^s(x)) = \frac{kj+s}{2k+s}.$$

Recalling our initial analysis and choice of $p'$ so that $j > p$, we have

$$\rho(h_{p'}^k(x) f_{p'}^s(x)) = \frac{t}{u}.$$

■

# 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] Manjul Bhargava. *The Factorial Function and Generalisations*. The Mathematical Association of America (Monthly **107**) November 2000.

[3] Grady Bullington, private communication.

[4] S. T. Chapman, et al. *Full Elasticity in Atomic Monoids and Integral Domains*. To appear: Rocky Mountain J. Math.

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

[6] Serge Lang. *Algebra*. 2nd Ed. Addison-Wesley Publishing Company, Inc. 1984.

[7] William J. LeVeque. *Fundamentals of Number Theory*. Dover Publications, Inc. 1996.

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

[9] W. Narkiewicz, *Polynomial mappings, Lecture Notes in Mathematics,* Springer-Verlag. 1995.