POLYNOMIALS THAT ARE INTEGER-VALUED ON THE FIBONACCI NUMBERS

by

Kira Scheibelhut

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

at

Dalhousie University
Halifax, Nova Scotia
August 2013

Table of Contents

List of Figures

Abstract

An integer-valued polynomial is a polynomial with rational coefficients that takes an integer value when evaluated at an integer. The polynomials $\{\binom{x}{n}\}_{n=0}^{\infty}$ form a regular basis for the $\mathbb{Z}$-module of all integer-valued polynomials. Using the idea of a p-ordering and a p-sequence, Bhargava describes a similar characterization for polynomials that are integer-valued on some subset of $\mathbb{Z}$. This thesis focuses on characterizing the polynomials that are integer-valued on the Fibonacci numbers.

For a certain class of primes p, we give a formula for the p-sequence of the Fibonacci numbers and an algorithm for finding a p-ordering by using Coelho and Parry's results on the distribution of the Fibonacci numbers modulo powers of primes. Knowing the p-sequence, we can then find a p-local regular basis for the polynomials that are integer-valued on the Fibonacci numbers using Bhargava's methods. A regular basis can be constructed from p-local bases for all primes p.

List of Abbreviations and Symbols Used

$\mathbb{F}_n$	The finite field of order n.	33
$\left(\frac{z}{p}\right)$	The Legendre symbol.	??
$(\mathbb{Z}/(p^k))^*$	The units of $\mathbb{Z}/(p^k)$.	36
$\langle\beta\rangle$	The group generated by β.	42
$\mathbf{i}(y)$	The number of solutions of $f(z) = y$.	42
$\mathbf{i}_+(y)$	The number of squares that are solutions of $f(z) = y$.	42
$\mathbf{i}_-(y)$	The number of non-squares that are solutions of $f(z) = y$.	42
Sq	The set of squares in $\mathbf{U}/\mathbf{U}_1$.	56
$\mathbb{F}_1$	The set $\{y \in \mathbb{F} \mid 5y^2 + 4 \not\equiv 0 \mod p \text{ and } 5y^2 - 4 \not\equiv 0 \mod p\}$.	56
$\mathbb{F}_2$	The set $\{y \in \mathbb{F} \mid 5y^2 + 4 \equiv 0 \mod p \text{ or } 5y^2 - 4 \equiv 0 \mod p\}$.	56

Acknowledgements

I would like to gratefully acknowledge the funding I received from the Natural Sciences and Engineering Research Council of Canada and the Dalhousie Department of Mathematics and Statistics.

On a more personal level, this thesis would not have been completed without the help of several people. In particular, I would like to thank:

- my supervisor, Dr. Keith Johnson, for his patience, passion, insight, and advice;
- my readers, Dr. Karl Dilcher and Dr. Dorette Pronk, for their interest and suggestions;
- Dr. Keith Taylor, for his guidance and for encouraging my initial desire to do research;
- the faculty, staff, and students of the Dalhousie Department of Mathematics and Statistics for their assistance and for making the department such a great place to be;
- my parents, Christie MacInnes and Tom Scheibelhut, for their love and support;
- Matthew Stephen, for all of the homework help and for making me feel calm in comparison;
- my family and friends, especially Kirk Scheibelhut, Brent Scheibelhut, Marie MacInnes, Carolyn Scheibelhut, John Scheibelhut, Jenny Wade, and Barbie Wade, for always being there;
- and, last, but certainly not least, Julien Ross , for more than I can write here.

Chapter 1

Introduction

An *integer-valued polynomial on* S, for $S \subseteq \mathbb{Q}$, is a polynomial with rational coefficients that takes an integer value when evaluated at an element of S. The set of all such polynomials is denoted by

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

Integer-valued polynomials on $\mathbb{Z}$ have long been known and used in calculus. In particular, it has been known that every integer-valued polynomial on $\mathbb{Z}$ can be uniquely expressed as an integer linear combination of the binomial polynomials

$$\left\{ \binom{x}{n} = \frac{x(x-1)\dots(x-n+1)}{n!} \right\}_{n=0}^{\infty}.$$

The polynomials $\binom{x}{n}$ are said to form a *regular basis*, that is, a basis consisting of one polynomial of each degree, for the ring $\mathrm{Int}(\mathbb{Z}, \mathbb{Z})$.

In a similar way, for a fixed prime integer p and $S \subseteq \mathbb{Q}$, we can consider

$$\mathrm{Int}(S, \mathbb{Z}_{(p)}) = \{f(x) \in \mathbb{Q}[x] | f(S) \subseteq \mathbb{Z}_{(p)}\},$$

where $\mathbb{Z}_{(p)} = \{a/b | a, b \in \mathbb{Z}, p \nmid b\}$ is the set of p-local integers . It has been shown, as in [5], that $\mathrm{Int}(S, \mathbb{Z}_{(p)}) = \mathrm{Int}(S, \mathbb{Z})_{(p)}$, the p-localization of $\mathrm{Int}(S, \mathbb{Z})$, so that by describing $\mathrm{Int}(S, \mathbb{Z}_{(p)})$ for all p, we can describe $\mathrm{Int}(S, \mathbb{Z})$. A regular basis for $\mathrm{Int}(S, \mathbb{Z})$ can be constructed from ones for $\mathrm{Int}(S, \mathbb{Z}_{(p)})$ for all primes p.

The question then arises whether such a basis can be found for $\mathrm{Int}(S, \mathbb{Z}_{(p)})$ with $S \neq \mathbb{Z}$. M. Bhargava, in [4], has shown that it is possible by constructing a "generalized binomial polynomial" using the idea of a p-ordering and a p-sequence. Associated to any subalgebra of $\mathbb{Q}[x]$ is a sequence of fractional ideals, called characteristic ideals, with the nth one consisting of 0 and the leading coefficients of elements of the subalgebra of degree less than or equal to n. The characteristic ideals we consider in this thesis are all principal ideals and the p-adic valuations of the generators of these ideals

form the characteristic sequence of the subalgebra. Given a regular basis for such a subalgebra, the leading coefficients of the basis elements generate the characteristic ideals and this property characterizes regular bases. For a fixed prime integer p, if the subalgebra is of the form $\mathrm{Int}(S, \mathbb{Z}_{(p)})$, then it is a theorem that the p-sequence coming from a p-ordering of S, defined by Bhargava, is the sequence of p-adic valuations of these characteristic ideals, so you can reconstruct the characteristic sequence if all of the p-sequences are known.

In this thesis, we show how to find the p-sequence of the set of Fibonacci numbers, denoted $\mathbb{F}$, for a certain class of primes. Then, from Bhargava's results, we obtain an algorithm for finding the characteristic sequence for $\mathrm{Int}(\mathbb{F}, \mathbb{Z}_{(p)})$ and constructing a p-local basis. With these p-local bases for all primes p, we can then show that

$$1, x, \frac{x^2 - x}{2}, \frac{x^3 - 3x^2 + 2x}{6}, \frac{x^4 - 6x^3 + 11x^2 - 6x}{24},$$

$$\frac{143x^5 - 2965x^4 + 14215x^3 - 24035x^2 + 12642x}{240},$$

$$\frac{269x^6 - 9255x^5 + 80285x^4 - 274545x^3 + 392126x^2 - 188880x}{720},$$

$$\frac{\begin{array}{c}245129x^7 - 18791962x^6 + 343262150x^5 \\ -2392639900x^4 + 7391778401x^3 - 10008680458x^2 + 4684826640x\end{array}}{443520},$$

$$\frac{\begin{array}{c}245129x^8 - 23406351x^7 + 605061912x^6 - 6640975530x^5 \\ +35440539981x^4 - 94265906679x^3 + 117015122578x^2 - 52130681040x\end{array}}{443520}, \text{ and}$$

$$\frac{\begin{array}{c}54687901x^9 - 31874521653x^8 + 7668792570894x^7 \\ -568782337259682x^6 + 9101305330342869x^5 - 58282598264258277x^4 \\ 171075685473526496x^3 - 224615295883995588x^2 + 103282048708907040x\end{array}}{103783680},$$

are the first 10 elements of a regular basis for $\mathrm{Int}(\mathbb{F}, \mathbb{Z})$ and, thus, give a method of testing whether or not a given polynomial of degree 9 or less is in $\mathrm{Int}(\mathbb{F}, \mathbb{Z})$. For example, we can show that

$$f(x) = \frac{x(x-1)(x-2)(x-3)(x-5)}{2^4}$$

is in $\mathrm{Int}(\mathbb{F}, \mathbb{Z})$, despite the fact that $f(x) \notin \mathrm{Int}(\mathbb{Z}, \mathbb{Z})$ since $f(4) = -\frac{3}{2}$.

Consider the recurrence relation

$$F_n = F_{n-1} + F_{n-2}, \quad n \geq 2.$$

If we set $F_0 = 0$ and $F_1 = 1$ we obtain the Fibonacci sequence. Each F_n is a Fibonacci number and, by Binet's formula, we can write

$$F_n = \frac{1}{\sqrt{5}} \left(\beta^n - \left(\frac{-1}{\beta} \right)^n \right),$$

where $\beta = \frac{1+\sqrt{5}}{2}$.

Although we would like to know the p-sequence of $\mathbb{F}$, for all prime integers p, we will restrict our attention to the primes for which β satisfies the following condition. (The methods we use, however, can be extended to include all primes.)

Condition 1.0.1.

1. *If 5 is a square mod p, then β is of order $p-1$ in the group of units of $\mathbb{Z}/(p)$ and $\beta^{p-1} \not\equiv 1$ in $\mathbb{Z}/(p^2)$.*

2. *If 5 is not a square mod p, then β is of order $2(p+1)$ in the group of units of $(\mathbb{Z} + \sqrt{5}\mathbb{Z})/(p)$ and $\beta^{2(p+1)} \not\equiv 1$ in $(\mathbb{Z} + \sqrt{5}\mathbb{Z})/(p^2)$.*

From here on, we will assume, unless otherwise stated, that all prime integers p appearing are ones for which β satisfies Condition 1.0.1. We will also assume that $p \neq 2$ or 5, since these two cases are handled separately in Chapter 5.

For a fixed prime p of this type, we can determine which residue classes are represented by the Fibonacci numbers modulo p, using some of the results from [6]. This information helps us find a subset T of the integers with $\mathbb{F} \subseteq T$ and $\mathbb{F}/(p^k) = T/(p^k), \forall k > 0$. For such a subset, $\mathrm{Int}(\mathbb{F}, \mathbb{Z}_{(p)}) = \mathrm{Int}(T, \mathbb{Z}_{(p)})$ and, thus, the p-sequence of $\mathbb{F}$ is the same as the p-sequence of T. We can then work with T instead of $\mathbb{F}$ when computing the p-sequence of the Fibonacci numbers.

The p-sequence of T can be found by decomposing T into simpler subsets, using known results to calculate their p-sequences, and then combining these p-sequences. Finding the p-sequence of T this way, we can give a formula for the p-sequence of $\mathbb{F}$ and an algorithm for finding a p-ordering and so a p-local regular basis, which is our main result.

To state the main result, we need the following notation:

Notation 1.0.2. *For a fixed prime integer p*

1. *The p-adic valuation of an element z of $\mathbb{Z}$ is the largest k for which p^k divides z and will be denoted $v_p(z)$.*

2. *For $a \in \mathbb{Z}$, the linear sequence with $a \cdot n$ as its n-th term will be denoted (an).*

3. *For $S \subseteq \mathbb{Z}$, the p-sequence of S will be denoted $\{\alpha_{S,p}(k)\}_{k=0}^{\infty}$.*

4. *The p-sequence of $\mathbb{Z}$ is*

$$\alpha_{\mathbb{Z},p}(k) = v_p(k!) = \sum_{i=0}^{\infty} \lfloor \frac{k}{p^i} \rfloor.$$

5. *The sum of two sequences σ and δ will be denoted $\sigma + \delta$ and has $\sigma(n) + \delta(n)$ as its n-th term.*

6. *The shuffle of two nondecreasing sequences σ and δ is the disjoint union of the elements of the two sequences sorted into nondecreasing order and will be denoted by $\sigma \wedge \delta$. The shuffle of k copies of a sequence σ with itself will be denoted $\sigma^{\wedge k}$.*

With this notation, our main result is:

Theorem 1.0.3. *For a fixed odd prime integer p for which β satisfies Condition 1.0.1,*

$$\alpha_{\mathbb{F},p} = (\alpha_{\mathbb{Z},p} + (k))^{\wedge a} \wedge (\alpha_{\gamma,p})^{\wedge b},$$

where γ is a set whose p-sequence, $\alpha_{\gamma,p}$, is determined completely by the equation

$$\alpha_{\gamma,p} = ((\alpha_{\mathbb{Z},p} + (k))^{\wedge \frac{p-1}{2}} \wedge \alpha_{\gamma,p}) + (2k),$$

and a and b are integers, with $0 \leq b \leq 4$, computed in a manner described in Section 9.2.

Note that the equation for $\alpha_{\gamma,p}$ does determine this sequence completely since $\alpha_{\gamma,p}(n)$ is expressed in terms of other known quantities and $\alpha_{\gamma,p}(m)$ for $m < n$. In fact, this theorem gives a quick algorithm for computing $\alpha_{\mathbb{F},p}$, since the only operations on sequences involved are sum, merge, and sort.

This thesis is organized as follows. In Chapter 2 we provide a basic overview of integer-valued polynomials and show that in order to describe $\mathrm{Int}(\mathbb{F}, \mathbb{Z})$ it is enough to describe, for all primes p, $\mathrm{Int}(T, \mathbb{Z}_{(p)})$ for some $\mathbb{F} \subseteq T \subseteq \mathbb{Z}$ such that $\mathbb{F}/(p^k) = T/(p^k), \forall k > 0$. Chapter 3 defines p-orderings and p-sequences and reviews results regarding their computation. With these definitions, we can then look, in Chapter 4, at the "generalized binomial polynomials" introduced by Bhargava in [4]. In Chapter 5 we provide a complete description of the distribution of the Fibonacci numbers mod 2^k and mod 5^k and show how this information can be used to calculate the 2-sequence and 5-sequence of the Fibonacci numbers. Chapter 6 introduces several interesting groups related to the p-adic integers which will be used in our analysis of Coelho and Parry's paper, and briefly discusses Hensel's Lemma. In Chapter 7 we show that, since β satisfies Condition 1.0.1, it generates certain groups that will be of interest in Chapter 8. Coelho and Parry's results are used in Chapter 8 to give a detailed account of how to determine which residue classes of $\mathbb{Z}/(p^k)$ are represented by Fibonacci numbers for the class of primes p we have restricted ourselves to. Finally, in Chapter 9 we describe how to create a visual representation of the results from Chapter 8 in the form of tree diagrams and prove our main result which gives a formula for calculating the p-sequence of the Fibonacci numbers for those primes p with β satisfying Condition 1.0.1. The conclusion suggests the value of the main result and describes how it may be extended to those primes p where β does not satisfy Condition 1.0.1 and to other second-order linear recurrence relations.

Chapter 2

Integer-Valued Polynomials

2.1 Integer-Valued Polynomials

Definition 2.1.1. *An integer-valued polynomial is a polynomial with rational coefficients that takes an integer value when evaluated at an integer. The set of all such polynomials is denoted by*

$$Int(\mathbb{Z}) = \{f(x) \in \mathbb{Q}[x] | f(\mathbb{Z}) \subseteq \mathbb{Z}\}.$$

Obviously, every polynomial with integer coefficients is integer-valued; however, it is also possible for an integer-valued polynomial to have rational non-integer coefficients. For example, the polynomial $f(x) = x(x-1)/2$ maps the integers to the integers, since one of x and $x-1$ must be even.

From our knowledge of Pascal's triangle we know that for all nonnegative integers m and n, the binomial coefficient $\binom{m}{n}$ is an integer. Hence, if we fix a nonnegative integer n, the binomial polynomial

$$\binom{x}{n} = \frac{x(x-1)\dots(x-n+1)}{n!}$$

is integer-valued for all nonnegative integers x, although its coefficients are not in $\mathbb{Z}$, since it evaluates to a binomial coefficient. Furthermore, it can easily be seen that $\binom{x}{n}$ is an integer for all integer values of x, not just the nonnegative ones.

Proposition 2.1.2. *Let $k \in \mathbb{Z}$. A polynomial f with coefficients in $\mathbb{Q}$ such that $f(n) \in \mathbb{Z}$ for $n \geq k$ is integer-valued.*

Proof. Let f be a polynomial with coefficients in $\mathbb{Q}$ such that $f(n) \in \mathbb{Z}$ for $n \geq k$. The proof is by induction on the degree d of f. If $d = 0$, then f is a constant function and the result holds trivially. Now, suppose that the result is true for $d = s$. Let f be of degree $s+1$ and let $a \in \mathbb{Z}$. Then there is a nonnegative integer b such that $(a+b) \geq k$ and, hence, $f(a+b) \in \mathbb{Z}$. Consider the polynomial $g(x) = f(x) - f(x+b)$.

Since f is of degree $s+1$, then g is of degree at most s, and it is easily seen that $g(n) \in \mathbb{Z}$ for $n \geq k$. Thus, $g \in \mathrm{Int}(\mathbb{Z})$. However, $f(a) = g(a) + f(a+b)$, and, so, $f(a) \in \mathbb{Z}$. Therefore, f is integer-valued. □

Thus, the polynomials $\binom{x}{n}$ are integer-valued, since $\binom{m}{n} \in \mathbb{Z}$ for $m \geq 0$. Using these polynomials, it is possible to characterize all integer-valued polynomials.

Theorem 2.1.3. *A polynomial is integer-valued on $\mathbb{Z}$ if and only if it can be written as a $\mathbb{Z}$-linear combination of the polynomials*

$$\left\{ \binom{x}{n} = \frac{x(x-1)\dots(x-n+1)}{n!} : n = 0, 1, 2, \dots \right\}.$$

In other words, this theorem states that the polynomials $\{\binom{x}{n}\}_{n=0}^{\infty}$ form a regular basis, i.e., a basis consisting of one polynomial of each degree, of the $\mathbb{Z}$-module $\mathrm{Int}(\mathbb{Z})$. The proof closely follows the one by Cahen and Chabert in [5].

Proof. Since there is one binomial polynomial for each degree, it is clear that the polynomials $\binom{x}{n}$ form a $\mathbb{Q}$-basis of the $\mathbb{Q}$-vector space $\mathbb{Q}[x]$. Furthermore, it was just seen that the polynomials $\binom{x}{n}$ are integer-valued. Thus, a $\mathbb{Z}$-linear combination of these polynomials is in $\mathrm{Int}(\mathbb{Z})$.

Conversely, let $f \in \mathrm{Int}(\mathbb{Z})$. Since the polynomials $\binom{x}{n}$ form a basis of the $\mathbb{Q}$-vector space $\mathbb{Q}[x]$, we can write

$$f(x) = a_0 + a_1 x + a_2 \binom{x}{2} \cdots + a_n \binom{x}{n},$$

where $a_0, a_1, \dots, a_n \in \mathbb{Q}$. The proof is by induction on the index j of the coefficients a_j of f. Note that $a_0 = f(0) \in \mathbb{Z}$. Let $k < n$ and suppose that $a_i \in \mathbb{Z}$ for $i \leq k$. Then $g_k(x) = f(x) - \sum_{i=0}^{k} a_i \binom{x}{i}$ is integer-valued. However,

$$g_k(x) = a_{k+1} \binom{x}{k+1} + \cdots + a_n \binom{x}{n}.$$

Thus, $a_{k+1} = g_k(k+1) \in \mathbb{Z}$. Therefore, f can be written as a $\mathbb{Z}$-linear combination of the polynomials $\binom{x}{n}$.

□

It is clear from this proof that it is sufficient for f to take integral values on the nonnegative integers $0, 1, \dots, n$, to be integer-valued on $\mathbb{Z}$. By considering the

polynomial h with $h(x) = f(x + a)$ for some integer a, we also have the following result.

Corollary 2.1.4. *A polynomial f of degree n is integer-valued if and only if it takes integral values on any $n + 1$ consecutive integers.*

In particular, for f to be in $\mathrm{Int}(\mathbb{Z})$ it is enough that $f(\mathbb{N}_0) \subseteq \mathbb{Z}$.

Now that we have seen that all of the polynomials that are integer-valued on $\mathbb{Z}$ are $\mathbb{Z}$-linear combinations of the binomial polynomials, it is natural to wonder to what generality this result can be extended. In particular, is it possible to come up with a similar characterization for polynomials that are integer-valued on some subset of $\mathbb{Z}$? For example, is there a characterization for polynomials such as $f(x) = x/2$, which are integer-valued on all even integers?

It turns out that it is possible. In order to create such a characterization, however, we must first define a generalized factorial function and a generalized "falling factorial". Once this has been done, a basis for polynomials that are integer-valued on a subset of $\mathbb{Z}$ that looks very similar to the one we have just described can be found.

Before continuing, we should define integer-valued polynomials on a subset of a domain.

Definition 2.1.5. *Let D be a domain with quotient field K and let $S \subseteq K$. An integer-valued polynomial on S is a polynomial with coefficients in K that takes a value in D when evaluated at an element of S. The set of all such polynomials is denoted by*

$$Int(S, D) = \{f \in K[X] | f(S) \subseteq D.\}$$

We are interested in integer-valued polynomials on $S \subseteq \mathbb{Q}$. The set of all such polynomials is denoted by

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

It is clear that $\mathrm{Int}(S, \mathbb{Z})$ is a ring contained in $\mathbb{Q}[x]$.

2.2 The Ring Int$(S, \mathbb{Z}_{(p)})$

Also of interest is the set

$$\mathrm{Int}(S, \mathbb{Z}_{(p)}) = \{f(x) \in \mathbb{Q}[x] | f(S) \subseteq \mathbb{Z}_{(p)}\},$$

where p is a fixed prime integer and $S \subseteq \mathbb{Q}$. We are particularly interested in its relationship to $\mathrm{Int}(S, \mathbb{Z})_{(p)}$. To describe this relationship, we first need another definition.

Definition 2.2.1. *A subset S of $\mathbb{Q}$ is said to be a fractional subset of $\mathbb{Z}$ if there exists a nonzero element d of $\mathbb{Z}$ such that $dS \subseteq \mathbb{Z}$.*

The following result is proved as Proposition I.2.7 in [5].

Proposition 2.2.2. *Let p be a fixed prime integer and let S be a fractional subset of $\mathbb{Z}$. Then*

$$Int(S, \mathbb{Z}_{(p)}) = Int(S, \mathbb{Z})_{(p)}.$$

Hence, as mentioned in the introduction, to describe $\mathrm{Int}(S, \mathbb{Z})$ it is enough to describe $\mathrm{Int}(S, \mathbb{Z}_{(p)})$ for all primes p. A regular basis for $\mathrm{Int}(S, \mathbb{Z})$ can be constructed from ones for $\mathrm{Int}(S, \mathbb{Z}_{(p)})$ for all p. For a given integer n, there are only a finite number of primes p for which the nth element of a regular $\mathbb{Z}_{(p)}$-basis for $\mathrm{Int}(S, \mathbb{Z}_{(p)})$ has a nonzero denominator. By the Chinese Remainder Theorem, there is an integer linear combination of these basis elements which will be the nth element of a $\mathbb{Z}$-basis of $\mathrm{Int}(S, \mathbb{Z})$. Thus, to find a regular basis for $\mathrm{Int}(\mathbb{F}, \mathbb{Z})$, we can now focus on constructing regular bases for $\mathrm{Int}(\mathbb{F}, \mathbb{Z}_{(p)})$. The next lemma makes this construction much simpler, by allowing us to work instead with $\mathrm{Int}(T, \mathbb{Z}_{(p)})$ for certain $\mathbb{F} \subseteq T \subseteq \mathbb{Z}$.

Lemma 2.2.3. *For a fixed prime integer p, if $S \subseteq T \subseteq \mathbb{Z}$ and $S/(p^k) = T/(p^k), \forall k > 0$, then $Int(S, \mathbb{Z}_{(p)}) = Int(T, \mathbb{Z}_{(p)})$.*

Proof. Suppose $S \subseteq T \subseteq \mathbb{Z}$ and $S/(p^k) = T/(p^k), \forall k > 0$. Clearly,

$$\begin{aligned}
\mathrm{Int}(T, \mathbb{Z}_{(p)}) &= \{f(x) \in \mathbb{Q}[x] | f(T) \subseteq \mathbb{Z}_{(p)}\} \\
&\subseteq \{f(x) \in \mathbb{Q}[x] | f(S) \subseteq \mathbb{Z}_{(p)}\} \\
&= \mathrm{Int}(S, \mathbb{Z}_{(p)}),
\end{aligned}$$

since $S \subseteq T$. Thus, it remains to show that $\text{Int}(S, \mathbb{Z}_{(p)}) \subseteq \text{Int}(T, \mathbb{Z}_{(p)})$. Let $f(x) = \sum_{i=0}^{n} a_i x^i \in \text{Int}(S, \mathbb{Z}_{(p)})$ and let $y \in T$. If $y \in S$, then $f(y) \in \mathbb{Z}_{(p)}$. So, suppose $y \notin S$. Now, $\forall i \in \{0, \ldots, n\}$, we have $a_i = \frac{c_i}{d_i}$, for some $c_i, d_i \in \mathbb{Z}$ with $d_i \neq 0$, since $a_i \in \mathbb{Q}$. Let $k_i = v_p(d_i), \forall i \in \{0, \ldots, n\}$ and let $k = \max\{k_0, \ldots, k_n\}$.

If $k = 0$, then $a_i \in \mathbb{Z}_{(p)}, \forall i \in \{0, \ldots, n\}$, and $f(y) \in \mathbb{Z}_{(p)}$ trivially. If $k > 0$, then $\exists z \in S$ such that $y \equiv z \mod p^k$, that is, such that $y = z + m \cdot p^k$ for some $m \in \mathbb{Z}$, since $S/(p^k) = T/(p^k)$. Note that $f(x) = \sum_{i=0}^{n} a_i x^i \in \text{Int}(S, \mathbb{Z}_{(p)})$ and $z \in S$, so $f(z) = \sum_{i=0}^{n} a_i z^i \in \mathbb{Z}_{(p)}$. Moreover, $\forall i \in \{0, \ldots, n\}$, we can write $a_i = \frac{b_i}{p^k}$, where $b_i = p^k a_i \in \mathbb{Z}_{(p)}$. Hence, $f(z) = \sum_{i=0}^{n} \frac{b_i}{p^k} z^i \in \mathbb{Z}_{(p)}$.

Now, consider

$$\begin{aligned} f(y) &= \sum_{i=0}^{n} \frac{b_i}{p^k} y^i \\ &= \sum_{i=0}^{n} \frac{b_i}{p^k} (z + m \cdot p^k)^i \\ &= \sum_{i=0}^{n} \frac{b_i z^i + b_i A_i}{p^k}, \end{aligned}$$

where A_i is an integer divisible by $p^k, \forall i \in \{0, \ldots, n\}$. Letting $A_i = p^k A_i'$ with $A_i' \in \mathbb{Z}$, $\forall i \in \{0, \ldots, n\}$, we have

$$\begin{aligned} f(y) &= \sum_{i=0}^{n} \frac{b_i z^i + b_i p^k A_i'}{p^k} \\ &= \sum_{i=0}^{n} \frac{b_i z^i}{p^k} + \sum_{i=0}^{n} b_i A_i' \\ &= f(z) + \sum_{i=0}^{n} b_i A_i'. \end{aligned}$$

From above, we know that $f(z) \in \mathbb{Z}_{(p)}$, and it is clear that $\sum_{i=0}^{n} b_i A_i' \in \mathbb{Z}_{(p)}$, since $b_i \in \mathbb{Z}_{(p)}$ and $A_i' \in \mathbb{Z}$. So, $f(y) \in \mathbb{Z}_{(p)}$. Thus, $f(x) \in \text{Int}(T, \mathbb{Z}_{(p)})$. Therefore, $\text{Int}(S, \mathbb{Z}_{(p)}) \subseteq \text{Int}(T, \mathbb{Z}_{(p)})$ and the result holds. □

So, to describe $\text{Int}(\mathbb{F}, \mathbb{Z}_{(p)})$ it is enough to describe $\text{Int}(T, \mathbb{Z}_{(p)})$ for some $\mathbb{F} \subseteq T \subseteq \mathbb{Z}$ such that $\mathbb{F}/(p^k) = T/(p^k), \forall k > 0$. Hence, we will look at $\mathbb{F}/(p^k)$, for different k, to determine an appropriate T.

If $\text{Int}(S, \mathbb{Z}_{(p)}) = \text{Int}(T, \mathbb{Z}_{(p)})$, then the p-sequence of S is the same as the p-sequence of T, since the regular bases of $\text{Int}(S, \mathbb{Z}_{(p)})$ and $\text{Int}(T, \mathbb{Z}_{(p)})$ are the same. Hence, if we

find a set T with $\mathbb{F} \subseteq T \subseteq \mathbb{Z}$ such that $\mathbb{F}/(p^k) = T/(p^k), \forall k > 0$, then the p-sequence of T will the same as the p-sequence of $\mathbb{F}$.

Chapter 3

p-Sequences

3.1 p-Orderings

As mentioned in the introduction, in order to find a regular basis for $\mathrm{Int}(\mathbb{F}, \mathbb{Z})$ we will construct a "generalized binomial polynomial" using the idea of a p-sequence. Before we define a p-sequence, we must first define a p-ordering.

Definition 3.1.1. *For an infinite subset S of $\mathbb{Z}$, an ordering of S is a bijective map $\psi : \mathbb{N}_0 \to S$.*

When we are only considering one ordering of a set, the familiar notation $\{a_i\}_{i=0}^{\infty}$ with $a_i = \psi(i)$ for an ordering will often be used instead.

Definition 3.1.2. *For a fixed prime integer p and an arbitrary infinite subset S of $\mathbb{Z}$, a p-ordering of S, as introduced in [4], is a sequence $\{a_i\}_{i=0}^{\infty}$ of elements of S such that a_0 is chosen randomly and, for each $n > 0$, the element a_n is chosen to minimize $v_p(\prod_{i=0}^{n-1}(s - a_i))$ over $s \in S$.*

Obviously, a p-ordering of S is not unique. In fact, the element a_0 is chosen randomly, and often several elements in S give the same desired minimum when searching for a_n when $n > 0$, in which case it is possible to choose any one of these elements. Moreover, each time an a_i is chosen, it affects the choices available in the future.

Although a_n is chosen to minimize $v_p(\prod_{i=0}^{n-1}(s - a_i))$ over $s \in S$ and S is an infinite set, we may restrict our search to $s \in S/(p^k)$ for an appropriate $k \in \mathbb{Z}$, making computations much easier. To prove this result, we must first recall two important properties of the p-adic valuation.

Lemma 3.1.3. *Let $c, d \in \mathbb{Z}$. Then*

1. *$v_p(c \cdot d) = v_p(c) + v_p(d)$ and*

2. $v_p(c+d) \geq min(v_p(c), v_p(d))$. *Moreover, if* $v_p(c) \neq v_p(d)$, *then* $v_p(c+d) = min(v_p(c), v_p(d))$.

Proof. First, note that, since $c, d \in \mathbb{Z}$, we can write $c = np^k$ and $d = mp^l$ for some $n, m, k, l \in \mathbb{Z}$ with $\gcd(n, p) = \gcd(m, p) = 1$.

1. Then

$$\begin{aligned} v_p(c \cdot d) &= v_p(np^k \cdot mp^l) \\ &= v_p(p^{k+l}nm) \\ &= k + l \\ &= v_p(c) + v_p(d). \end{aligned}$$

2. Suppose, without loss of generality, that $k \leq l$. That is, $v_p(c) \leq v_p(d)$. Then it is clear that

$$v_p(c+d) = v_p(p^k(n + mp^{l-k})) \geq v_p(c) = \min(v_p(c), v_p(d)),$$

with equality when $v_p(c) < v_p(d)$.

□

Remark 3.1.4. *The p-adic valuation gives rise to the p-adic norm of* $\mathbb{Q}$ *defined, for* $x \in \mathbb{Q}$, *by*

$$|x|_p = \begin{cases} p^{-v_p(x)}, & \text{if } x \neq 0 \\ 0, & \text{if } x = 0. \end{cases}$$

Note that $v_p(\frac{a}{b}) = v_p(a) - v_p(b)$ *for* $\frac{a}{b} \in \mathbb{Q}$. *A metric space can then be formed on* $\mathbb{Q}$ *with metric defined by* $d(x, y) = |x - y|_p$, *for* $x, y \in \mathbb{Q}$. *In fact, this metric forms an ultrametric structure on* $\mathbb{Q}$ *due to property 2 of Lemma 3.1.3.*

We may now prove the following lemma:

Lemma 3.1.5. *Let* S *be an arbitrary infinite subset of* $\mathbb{Z}$. *If* $\{a_0, a_1, \ldots, a_{n-1}\}$ *is the beginning of a p-ordering of* S, *then there is a* $k \in \mathbb{Z}$ *such that* a_n *can be computed by searching* $S/(p^k)$.

Proof. Let $\{a_0, a_1, \ldots, a_{n-1}\}$ be the beginning of a p-ordering of S. Let $a \in S$ and let $v_p(\prod_{i=0}^{n-1}(a - a_i)) = M$ for some $M \in \mathbb{Z}$. Let $b, b' \in S$ with $b \equiv b' \mod p^{M+1}$. That is, $b' = b + sp^{M+1}$ for some $s \in \mathbb{Z}$. Note that

$$\begin{aligned} v_p\left(\prod_{i=0}^{n-1}(b' - a_i)\right) &= v_p\left(\prod_{i=0}^{n-1}((b + sp^{M+1}) - a_i)\right) \\ &= v_p\left(\prod_{i=0}^{n-1}(sp^{M+1} + (b - a_i))\right) \\ &= \sum_{i=0}^{n-1} v_p(sp^{M+1} + (b - a_i)). \end{aligned}$$

Now, there are three cases to consider: $v_p(\prod_{i=0}^{n-1}(b-a_i)) = M$, $v_p(\prod_{i=0}^{n-1}(b-a_i)) > M$, and $v_p(\prod_{i=0}^{n-1}(b - a_i)) < M$. If $v_p(\prod_{i=0}^{n-1}(b - a_i)) = M$, then b is equivalent to a in our consideration of which element to choose next in our p-ordering. If $v_p(\prod_{i=0}^{n-1}(b-a_i)) > M$, however, then a is preferred to b in our consideration of which element to choose next in our p-ordering.

Finally, if $v_p(\prod_{i=0}^{n-1}(b - a_i)) = \sum_{i=0}^{n-1} v_p(b - a_i) < M$, then $v_p(b - a_i) < M$, $\forall i \in \{0, 1, \ldots, n-1\}$. Hence,

$$v_p(sp^{M+1} + (b - a_i)) = \min(v_p(sp^{M+1}), v_p(b - a_i)) = v_p(b - a_i)$$

since $v_p(b - a_i) \neq v_p(sp^{M+1})$, $\forall i \in \{0, 1, \ldots, n-1\}$, by Lemma 3.1.3. Thus,

$$\begin{aligned} v_p\left(\prod_{i=0}^{n-1}(b' - a_i)\right) &= \sum_{i=0}^{n-1} v_p(sp^{M+1} + (b - a_i)) \\ &= \sum_{i=0}^{n-1} v_p(b - a_i) \\ &= v_p\left(\prod_{i=0}^{n-1}(b - a_i)\right). \end{aligned}$$

So, if $v_p(\prod_{i=0}^{n-1}(b - a_i)) < M$, then b is equivalent to b' in our consideration of which element to choose next in our p-ordering and both b and b' are preferred to a. Therefore, when computing a_n, it is sufficient to consider an element $b \in S$ from each non-empty residue class modulo p^{M+1}. Thus, there is a $k \in \mathbb{Z}$ such that a_n can be computed by searching $S/(p^k)$. □

3.2 p-Sequences

Once a p-ordering has been constructed, we obtain a corresponding sequence of non-negative integers called the p-sequence of S.

Definition 3.2.1. *For a fixed prime integer p and an arbitrary infinite subset S of $\mathbb{Z}$ with p-ordering $\{a_i\}_{i=0}^{\infty}$, the p-sequence of S is the sequence of integers $\{\alpha_{S,p}(k)\}_{k=0}^{\infty}$ with $\alpha_{S,p}(0) = 0$ and $\alpha_{S,p}(k) = v_p(\prod_{i=0}^{k-1}(a_k - a_i))$, for $k > 0$.*

Now, it would seem, since there are many choices to be made when constructing a p-ordering, that the resulting p-sequence could be pretty much anything. Thus, it is surprising that the p-sequence of S is actually well-defined, in that it depends only on S and may be spoken of without reference to any particular p-ordering. This fact is Theorem 5 in [4].

Remark 3.2.2. *In [4] the p-sequence of S is the sequence of integers $\{v_k(S,p) = p^{\alpha_{S,p}(k)}\}_{k=0}^{\infty}$. It is clear, however, that if the sequence $\{v_k(S,p)\}_{k=0}^{\infty}$ is independent of the choice of p-ordering then so is the sequence $\{\alpha_{S,p}(k)\}_{k=0}^{\infty}$.*

The following lemma describes some of the properties of p-sequences that we will find useful.

Lemma 3.2.3. *Let S be an arbitrary infinite subset of $\mathbb{Z}$.*

1. *The p-sequence of S characterizes p-orderings of S in the sense that, if $\{a_i\}_{i=0}^{\infty}$ is an ordering of S such that $v_p(\prod_{i=0}^{k-1}(a_k - a_i)) = \alpha_{S,p}(k)$ for all $k \geq 0$, then $\{a_i\}_{i=0}^{\infty}$ is a p-ordering of S.*

2. *p-sequences are always nondecreasing.*

Proof. 1. The proof follows closely that of Lemma 3.3 (a) in [10]. Suppose $\{a_i\}_{i=0}^{\infty}$ is an ordering of S such that $v_p(\prod_{i=0}^{k-1}(a_k - a_i)) = \alpha_{S,p}(k)$ for all $k \geq 0$. If $\{a_i\}_{i=0}^{\infty}$ is not a p-ordering of S, then there must exist $m > 0$ and $b \in S$ such that $v_p(\prod_{i=0}^{k-1}(a_k - a_i))$ is minimal for $k < m$ and

$$v_p\left(\prod_{i=0}^{m-1}(b - a_i)\right) < v_p\left(\prod_{i=0}^{m-1}(a_m - a_i)\right) = \alpha_{S,p}(m).$$

This contradicts the fact that $\alpha_{S,p}(m)$ is the same for all p-orderings. Thus, $\{a_i\}_{i=0}^{\infty}$ is a p-ordering of S.

2. The proof follows closely that of Lemma 3.3 (b) of [10]. Suppose $\{a_i\}_{i=0}^{\infty}$ is a p-ordering of S with p-sequence $\{\alpha_{S,p}(k)\}_{k=0}^{\infty}$. The minimality of $v_p(\prod_{i=0}^{k-1}(a_k-a_i))$ implies

$$\alpha_{S,p}(k) = v_p\left(\prod_{i=0}^{k-1}(a_k - a_i)\right) \leq v_p\left(\prod_{i=0}^{k-1}(a_{k+1} - a_i)\right) \leq v_p\left(\prod_{i=0}^{k}(a_{k+1} - a_i)\right) = \alpha_{S,p}(k+1).$$

Thus, $\{\alpha_{S,p}(k)\}_{k=0}^{\infty}$ is always nondecreasing.

□

3.3 Computing p-Sequences

The next lemma is helpful for computation and will be used frequently in the material that follows.

Lemma 3.3.1. *Let S be an arbitrary infinite subset of $\mathbb{Z}$ with p-sequence $\{\alpha_{S,p}(k)\}_{k=0}^{\infty}$.*

1. *If $r \in \mathbb{Z}$, then the p-sequence of $r + S = \{r + s : s \in S\}$ is $\{\alpha_{S,p}(k)\}_{k=0}^{\infty}$ also.*
2. *If $r \in \mathbb{Z}$ such that p does not divide r, then the p-sequence of $r \cdot S = \{r \cdot s : s \in S\}$ is $\{\alpha_{S,p}(k)\}_{k=0}^{\infty}$ also.*
3. *If $m \in \mathbb{Z}^+$, then the p-sequence of $p^m \cdot S = \{p^m \cdot s : s \in S\}$ is $\{\alpha_{S,p}(k)+m \cdot k\}_{k=0}^{\infty}$. We denote this sequence $\alpha_{S,p} + (mk)$.*

Proof. The proofs follow closely that of Lemma 3.3 (c) in [10].

1. Let $r \in \mathbb{Z}$. Suppose $\{a_i\}_{i=0}^{\infty}$ is a p-ordering of S. Then $\alpha_{S,p}(0) = 0$ and $\alpha_{S,p}(k) = v_p(\prod_{i=0}^{k-1}(a_k - a_i))$, for $k > 0$.

   Consider the ordering $\{r + a_i\}_{i=0}^{\infty}$ of $r + S$. It is a p-ordering of $r + S$ if and only if, for each $k > 0$,

   $$v_p\left(\prod_{i=0}^{k-1}((r + a_k) - (r + a_i))\right) = v_p\left(\prod_{i=0}^{k-1}(a_k - a_i)\right)$$

   is minimal. Thus, $\{r + a_i\}_{i=0}^{\infty}$ is a p-ordering of $r + S$, since $\{a_i\}_{i=0}^{\infty}$ is a p-ordering of S. Moreover, the p-sequence is $\{\alpha_{S,p}(k)\}_{k=0}^{\infty}$ since $\alpha_{r+S,p}(0) = 0$ and, for $k > 0$,

   $$\alpha_{r+S,p}(k) = v_p(\prod_{i=0}^{k-1}((r + a_k) - (r + a_i))) = v_p(\prod_{i=0}^{k-1}(a_k - a_i)) = \alpha_{S,p}(k).$$

2. Let $r \in \mathbb{Z}$ such that p does not divide r. Suppose $\{a_i\}_{i=0}^{\infty}$ is a p-ordering of S. Then $\alpha_{S,p}(0) = 0$ and $\alpha_{S,p}(k) = v_p(\prod_{i=0}^{k-1}(a_k - a_i))$, for $k > 0$.

   Consider the ordering $\{r \cdot a_i\}_{i=0}^{\infty}$ of $r \cdot S$. It is a p-ordering of $r \cdot S$ if and only if, for each $k > 0$,

$$\begin{aligned} v_p\left(\prod_{i=0}^{k-1}((r \cdot a_k) - (r \cdot a_i))\right) &= v_p\left(\prod_{i=0}^{k-1} r(a_k - a_i)\right) \\ &= v_p\left(r^k \prod_{i=0}^{k-1}(a_k - a_i)\right) \\ &= v_p\left(r^k\right) + v_p\left(\prod_{i=0}^{k-1}(a_k - a_i)\right) \\ &= v_p\left(\prod_{i=0}^{k-1}(a_k - a_i)\right). \end{aligned}$$

   is minimal. Thus, $\{r \cdot a_i\}_{i=0}^{\infty}$ is a p-ordering of $r \cdot S$, since $\{a_i\}_{i=0}^{\infty}$ is a p-ordering of S. Moreover, the p-sequence is $\{\alpha_{S,p}(k)\}_{k=0}^{\infty}$ since $\alpha_{r \cdot S,p}(0) = 0$ and, for $k > 0$,

$$\alpha_{r \cdot S,p}(k) = v_p(\prod_{i=0}^{k-1}((r \cdot a_k) - (r \cdot a_i))) = v_p(\prod_{i=0}^{k-1}(a_k - a_i)) = \alpha_{S,p}(k).$$

3. Let $m \in \mathbb{Z}^+$. Suppose $\{a_i\}_{i=0}^{\infty}$ is a p-ordering of S. Then $\alpha_{S,p}(0) = 0$ and $\alpha_{S,p}(k) = v_p(\prod_{i=0}^{k-1}(a_k - a_i))$, for $k > 0$.

   Consider the ordering $\{p^m \cdot a_i\}_{i=0}^{\infty}$ of $p^m \cdot S$. It is a p-ordering of $p^m \cdot S$ if and only if, for each $k > 0$,

$$\begin{aligned} v_p\left(\prod_{i=0}^{k-1}((p^m \cdot a_k) - (p^m \cdot a_i))\right) &= v_p\left(\prod_{i=0}^{k-1} p^m(a_k - a_i)\right) \\ &= v_p\left(p^{mk} \prod_{i=0}^{k-1}(a_k - a_i)\right) \\ &= v_p\left(p^{mk}\right) + v_p\left(\prod_{i=0}^{k-1}(a_k - a_i)\right) \\ &= m \cdot k + v_p\left(\prod_{i=0}^{k-1}(a_k - a_i)\right). \end{aligned}$$

   is minimal. Thus, $\{p^m \cdot a_i\}_{i=0}^{\infty}$ is a p- ordering of $p^m \cdot S$, since $\{a_i\}_{i=0}^{\infty}$ is a p-ordering of S. Moreover, the p-sequence is $\{\alpha_{S,p}(k) + m \cdot k\}_{k=0}^{\infty}$ since $\alpha_{p^m \cdot S,p}(0) =$

0 and, for $k > 0$,

$$\alpha_{p^m \cdot S,p}(k) = v_p(\prod_{i=0}^{k-1}((p^m \cdot a_k) - (p^m \cdot a_i))) = m \cdot k + v_p\left(\prod_{i=0}^{k-1}(a_k - a_i)\right) = \alpha_{S,p}(k) + m \cdot k.$$

□

If a p-ordering of a set is known, it can be quite easy to determine p-orderings of certain subsets.

Lemma 3.3.2. *Let S be an arbitrary infinite subset of $\mathbb{Z}$. If $r \in \mathbb{Z}$ and $\{a_i\}_{i=0}^{\infty}$ is a p-ordering of S, then the subsequence of $\{a_i\}_{i=0}^{\infty}$ consisting of those $a_i \equiv r (mod\ p)$ is a p-ordering of $S \cap (r + p\mathbb{Z})$ and the corresponding subsequence of the p-sequence of S is the p-sequence of $S \cap (r + p\mathbb{Z})$.*

Proof. The proof follows closely that of Lemma 3.5 (a) in [10]. Let $r \in \mathbb{Z}$ and let $\{a_i\}_{i=0}^{\infty}$ be a p-ordering of S with p-sequence $\{\alpha_{S,p}(k)\}_{k=0}^{\infty}$. Let $S_r = S \cap (r + p\mathbb{Z})$ and suppose $a_k \in S_r$. If $a_i \in S \cap (t + p\mathbb{Z})$ for $r \not\equiv t (\mathrm{mod}\ p)$, then $v_p(a_k - a_i) = 0$. Hence,

$$\begin{aligned}\alpha_{S,p}(k) &= v_p\left(\prod_{i=0}^{k-1}(a_k - a_i)\right) \\ &= v_p\left(\prod_{\substack{i=0 \\ a_i \in S_r}}^{k-1}(a_k - a_i)\right).\end{aligned}$$

Furthermore, if $s \in S_r$, then

$$\begin{aligned}v_p\left(\prod_{\substack{i=0 \\ a_i \in S_r}}^{k-1}(s - a_i)\right) &= v_p\left(\prod_{i=0}^{k-1}(s - a_i)\right) \\ &\geq v_p\left(\prod_{i=0}^{k-1}(a_k - a_i)\right) \\ &= v_p\left(\prod_{\substack{i=0 \\ a_i \in S_r}}^{k-1}(a_k - a_i)\right).\end{aligned}$$

Thus, a_k minimizes

$$v_p\left(\prod_{\substack{i=0 \\ a_i \in S_r}}^{k-1}(s - a_i)\right)$$

for $s \in S_r$. Hence, $\{a_i\}_{i=0}^{\infty} \cap S_r$ is a p-ordering of S_r and $\{\alpha_{S,p}(k) : a_k \in S_r, k = 0, 1, 2, \dots\}$ is the p-sequence of S_r. □

Given the p-sequences of two sets, it can also be straightforward to compute the p-sequence of their union under certain conditions.

Lemma 3.3.3. *Let A and B be arbitrary infinite subsets of $\mathbb{Z}$ and let $\{a_i\}_{i=0}^{\infty}$ and $\{b_i\}_{i=0}^{\infty}$ be p-orderings of A and B, respectively, with associated p-sequences $\{\alpha_{A,p}(k) : k = 0, 1, 2, \dots\}$ and $\{\alpha_{B,p}(k) : k = 0, 1, 2, \dots\}$.*

If $v_p(a - b) = 0, \forall a \in A, b \in B$, then the p-sequence of $A \cup B$ is the disjoint union of $\{\alpha_{A,p}(k) : k = 0, 1, 2, \dots\}$ and $\{\alpha_{B,p}(k) : k = 0, 1, 2, \dots\}$ sorted into nondecreasing order. Moreover, the corresponding values of $\{a_i\}_{i=0}^{\infty}$ and $\{b_i\}_{i=0}^{\infty}$ sorted into the same order give a p-ordering of $A \cup B$.

Proof. Suppose that $\{a_i\}_{i=0}^{l-1}$ and $\{b_i\}_{i=0}^{m-1}$ together form the first $l + m$ terms of a p-ordering of $A \cup B$. The next element of a p-ordering will be one which minimizes

$$v_p\left((s - a_0) \dots (s - a_{l-1})(s - b_0) \dots (s - b_{m-1})\right)$$

over $s \in A \cup B$. By assumption, $v_p(a - b) = 0, \forall a \in A, b \in B$. Hence, for $s \in A$, the above valuation is $v_p\left((s - a_0) \dots (s - a_{l-1})\right)$ which is minimized by a_l, while for $s \in B$, this valuation is $v_p\left((s - b_0) \dots (s - b_{m-1})\right)$ which is minimized by b_m. Thus, the next term in a p-ordering of $A \cup B$ can be taken to be a_l if $v_p\left((a_l - a_0) \dots (a_l - a_{l-1})\right)$ is smaller than $v_p\left((b_m - b_0) \dots (b_m - b_{m-1})\right)$, and b_m if it is larger. Hence, the next term in the p-sequence of $A \cup B$ is $\alpha_{A,p}(l)$, if a_l is the next term in a p-ordering of $A \cup B$ and $\alpha_{B,p}(m)$, if b_m is. So, the p-sequence of $A \cup B$ is the disjoint union of the p-sequences of A and B sorted into nondecreasing order. It is clear from construction that the corresponding values of $\{a_i\}_{i=0}^{\infty}$ and $\{b_i\}_{i=0}^{\infty}$ give a p-ordering of $A \cup B$. □

The following definition will allow us to make the combination of sequences in Lemma 3.3.3 above precise.

Definition 3.3.4. *Let A and B be arbitrary infinite subsets of $\mathbb{Z}$ with p-sequences $\{\alpha_{A,p}(k) : k = 0, 1, 2, \dots\}$ and $\{\alpha_{B,p}(k) : k = 0, 1, 2, \dots\}$, respectively. The shuffle of the p-sequences of A and B is the disjoint union of the values of the two sequences sorted into nondecreasing order. We will denote this combination of sequences by $\alpha_{A,p} \wedge \alpha_{B,p}$.*

With this notation, we have the following corollary to Lemma 3.3.3.

Corollary 3.3.5. *Let S be an arbitrary infinite subset of $\mathbb{Z}$. If $r \not\equiv t (\mathrm{mod}\, p)$, then the p-sequence of $(S \cap (r + p\mathbb{Z})) \cup (S \cap (t + p\mathbb{Z}))$ is the shuffle of the p-sequences of $S \cap (r + p\mathbb{Z})$ and $S \cap (t + p\mathbb{Z})$.*

We can also generalize Lemma 3.3.3 as follows:

Corollary 3.3.6. *Let A and B be arbitrary infinite subsets of $\mathbb{Z}$ and let $\{a_i\}_{i=0}^{\infty}$ and $\{b_i\}_{i=0}^{\infty}$ be p-orderings of A and B, respectively, with associated p-sequences $\{\alpha_{A,p}(k) : k = 0, 1, 2, \dots\}$ and $\{\alpha_{B,p}(k) : k = 0, 1, 2, \dots\}$.*

If there is a non-negative integer m such that $v_p(a - b) = m, \forall a \in A, b \in B$, then the p-sequence of $A \cup B$ is the sum of the sequence $\{m \cdot k\}_{k=0}^{\infty}$ with the shuffle of $\{\alpha_{A,p}(k) - m \cdot k\}_{k=0}^{\infty}$ and $\{\alpha_{B,p}(k) - m \cdot k\}_{k=0}^{\infty}$. That is,

$$\alpha_{A\cup B,p} = ((\alpha_{A,p} - (mk)) \wedge (\alpha_{B,p} - (mk))) + (mk).$$

Moreover, this shuffle applied to $\{a_i\}_{i=0}^{\infty}$ and $\{b_i\}_{i=0}^{\infty}$ gives a p-ordering of $A \cup B$.

Proof. Fix $a_0 \in A$ and consider the sets $A - a_0$ and $B - a_0$. Let $a - a_0 \in A - a_0$ and $b - a_0 \in B - a_0$. Note that $v_p(a - a_0) \geq m$ since, $\forall c \in B$, we have

$$\begin{aligned} v_p(a - a_0) &= v_p(a - c + c - a_0)) \\ &\geq \min(v_p(a - c), v_p(c - a_0)), \text{by Lemma 3.1.3 (2)} \\ &= m, \text{ by assumption,} \end{aligned}$$

and $v_p(b - a_0) = m$, by assumption. Thus, $A - a_0 = p^m \cdot A'$ and $B - a_0 = p^m \cdot B'$, for some $A', B' \subseteq \mathbb{Z}$. So, $A = p^m A' + a_0$ and $B = p^m B' + a_0$.

Let $a' \in A'$ and $b' \in B'$. Then $p^m a' + a_0 \in A$ and $p^m b' + a_0 \in B$. Hence,

$$\begin{aligned} m &= v_p((p^m a' + a_0) - (p^m b' + a_0)), \text{ by assumption} \\ &= v_p(p^m(a' - b')) \\ &= v_p(p^m) + v_p(a' - b'), \text{by Lemma 3.1.3 (1)} \\ &= m + v_p(a' - b'), \end{aligned}$$

and so, $v_p(a' - b') = 0$. Thus, by Lemma 3.3.3 we have

$$\alpha_{A'\cup B',p} = \alpha_{A',p} \wedge \alpha_{B',p}.$$

Now, it is clear that $A \cup B = (p^m A' + a_0) \cup (p^m B' + a_0) = p^m(A' \cup B') + a_0$. Therefore, by Lemma 3.3.1,

$$\begin{aligned}\alpha_{A\cup B,p} &= \alpha_{p^m(A'\cup B')+a_0,p} \\ &= \alpha_{p^m(A'\cup B'),p} \\ &= \alpha_{A'\cup B',p} + (mk) \\ &= (\alpha_{A',p} \wedge \alpha_{B',p}) + (mk).\end{aligned}$$

Furthermore,

$$\begin{aligned}\alpha_{A,p} &= \alpha_{p^m A'+a_0,p} \\ &= \alpha_{p^m A',p} \\ &= \alpha_{A',p} + (mk),\end{aligned}$$

and similarly,

$$\alpha_{B,p} = \alpha_{B',p} + (mk).$$

Thus,

$$\begin{aligned}\alpha_{A\cup B,p} &= (\alpha_{A',p} \wedge \alpha_{B',p}) + (mk) \\ &= ((\alpha_{A,p} - (mk)) \wedge (\alpha_{B,p} - (mk))) + (mk).\end{aligned}$$

□

3.4 Examples for Computing p-Sequences

Let us look at some examples of how these lemmas can help us to compute the p-sequence of a set S. We begin by considering the 2-sequence of $S = \mathbb{Z}$.

Example: 2-Sequence of $\mathbb{Z}$

Let $S = \mathbb{Z}$. It is clear that we can write $S = \mathbb{Z} = 2\mathbb{Z} \cup (1 + 2\mathbb{Z})$. Now, by Lemma 3.3.1 (1), we know that $\alpha_{1+2\mathbb{Z},2} = \alpha_{2\mathbb{Z},2}$ and, by Lemma 3.3.1 (ii), we know that $\alpha_{1+2\mathbb{Z},2} = \alpha_{2\mathbb{Z},2} = \alpha_{\mathbb{Z},2} + (k)$. Note that $v_2(a - b) = 0 \ \forall a \in 2\mathbb{Z}, b \in (1 + 2\mathbb{Z})$. So, by Lemma 3.3.3,

$$\alpha_{\mathbb{Z},2} = (\alpha_{\mathbb{Z},2} + (k))^{\wedge 2}.$$

Since the p-sequence of $\mathbb{Z}$ is the shuffle of the same p-sequence with itself, the consecutive values $\alpha_{\mathbb{Z},2}(2k)$ and $\alpha_{\mathbb{Z},2}(2k+1)$ are equal. In fact, $\alpha_{\mathbb{Z},2}(2k) = \alpha_{\mathbb{Z},2}(2k+1) = \alpha_{\mathbb{Z},2}(k) + k$, by the equation above. Thus, $\alpha_{\mathbb{Z},2}(k) = \alpha_{\mathbb{Z},2}(\lfloor k/2 \rfloor) + \lfloor k/2 \rfloor$. Applying this equation repeatedly, a simple proof by inductions shows that

$$\begin{aligned}\alpha_{\mathbb{Z},2}(k) &= \alpha_{\mathbb{Z},2}(\lfloor k/2 \rfloor) + \lfloor k/2 \rfloor \\ &= (\alpha_{\mathbb{Z},2}(\lfloor k/4 \rfloor) + \lfloor k/4 \rfloor) + \lfloor k/2 \rfloor \\ &= \dots \\ &= \sum_{i=1}^{\infty} \lfloor \frac{k}{2^i} \rfloor.\end{aligned}$$

Moreover, it is a well-known theorem of Legendre's that $v_2(k!) = \sum_{i=1}^{\infty} \lfloor \frac{k}{2^i} \rfloor$. Hence, $\alpha_{\mathbb{Z},2}(k) = v_2(k!)$. Thus, the beginning of $\alpha_{\mathbb{Z},2}$ is:

$$\alpha_{\mathbb{Z},2} = \{0, 0, 1, 1, 3, 3, 4, 4, 7, 7, 8, 8, 10, 10, 11, 11, 15, 15, 16, 16, 18, 18, 19, 19, 22, 22, \dots\}.$$

Next, we will consider the 2-sequence of $S = \mathbb{Z} \setminus 4\mathbb{Z}$.

Example: 2-Sequence of $\mathbb{Z} \setminus 4\mathbb{Z}$

Let $S = \mathbb{Z} \setminus 4\mathbb{Z}$. It is clear that we can write $S = \mathbb{Z} \setminus 4\mathbb{Z} = (1 + 2\mathbb{Z}) \cup 2(1 + 2\mathbb{Z})$. Now, using the fact that $\alpha_{\mathbb{Z},2}(k) = v_2(k!)$, as shown after Proposition 3.5.1, we can calculate the beginning of $\alpha_{\mathbb{Z},2}$ to be:

$$\alpha_{\mathbb{Z},2} = \{0, 0, 1, 1, 3, 3, 4, 4, 7, 7, 8, 8, 10, 10, 11, 11, 15, 15, 16, 16, 18, 18, 19, 19, 22, 22, \dots\}.$$

Next, by Lemma 3.3.1 (1), we know that $\alpha_{1+2\mathbb{Z},2} = \alpha_{2\mathbb{Z},2}$ and, by Lemma 3.3.1 (ii), we know that $\alpha_{1+2\mathbb{Z},2} = \alpha_{2\mathbb{Z},2} = \alpha_{\mathbb{Z},2} + (k)$. Hence, the beginning of $\alpha_{1+2\mathbb{Z},2}$ is:

$$\alpha_{1+2\mathbb{Z},2} = \{0, 1, 3, 4, 7, 8, 10, 11, 15, 16, 18, 19, 22, 23, 25, 26, 31, 32, 34, 35, 38, 39, 41, \dots\}.$$

Similarly, by Lemma 3.3.1 (ii), we know that $\alpha_{2(1+2\mathbb{Z}),2} = \alpha_{1+2\mathbb{Z},2} + (k)$. Hence, the beginning of $\alpha_{2(1+2\mathbb{Z}),2}$ is:

$$\alpha_{2(1+2\mathbb{Z}),2} = \{0, 2, 5, 7, 11, 13, 16, 18, 23, 25, 28, 30, 34, 36, 39, 41, 47, 49, 52, 54, 58, 60, \dots\}.$$

Note that $v_2(a - b) = 0, \forall a \in (1 + 2\mathbb{Z}), b \in 2(1 + 2\mathbb{Z})$. So, by Lemma 3.3.3

$$\alpha_{\mathbb{Z}\setminus 4\mathbb{Z},2} = \alpha_{1+2\mathbb{Z},2} \wedge \alpha_{2(1+2\mathbb{Z}),2}.$$

Thus, the beginning of $\alpha_{\mathbb{Z}\setminus 4\mathbb{Z},2}$ is :

$$\alpha_{\mathbb{Z}\setminus 4\mathbb{Z},2}(k) = \{0, 0, 1, 2, 3, 4, 5, 7, 7, 8, 10, 11, 11, 13, 15, 16, 16, 18, 18, 19, 22, 23, 23, 25, \dots\}.$$

3.5 A p-Ordering of $\mathbb{Z}$

We just saw, in Section 3.4, that $\alpha_{\mathbb{Z},2}(k) = v_2(k!) = \sum_{i=1}^{\infty} \lfloor \frac{k}{2^i} \rfloor$. We will now find the p-sequence of $\mathbb{Z}$ for all of the other primes p, by first looking at a p-ordering of $\mathbb{Z}$.

Proposition 3.5.1. *The natural ordering* $0, 1, 2, \ldots$ *of the nonnegative integers forms a* p*-ordering of* $\mathbb{Z}$ *for all primes* p *simultaneously.*

Proof. Let p be a prime. The proof closely follows the proof of Proposition 6 in [4] and is by induction on the number of steps in the computation of a p-ordering. Clearly, 0 is a p-ordering for the 0th step, since the first element in a p-ordering is chosen randomly. Suppose $0, 1, 2, \ldots, k-1$ is a p-ordering for the first $k-1$ steps. Then at the kth step we need to pick a_k to minimize $v_p(\prod_{i=0}^{k-1}(s-a_i))$ over $s \in S$. Notice that $v_p(\prod_{i=0}^{k-1}(a_k - a_i)) = v_p[(a_k-0)(a_k-1)\ldots(a_k-(k-1))]$ and $(a_k-0)(a_k-1)\ldots(a_k-(k-1))$ is the product of k consecutive integers. Thus, $(a_k-0)(a_k-1)\ldots(a_k-(k-1)) = c \cdot k!$ for some $c \in \mathbb{Z}$. In particular, $(a_k-0)(a_k-1)\ldots(a_k-(k-1)) = k!$, if we choose $a_k = k$. Furthermore, it is clear that this value of a_k minimizes $v_p(\prod_{i=0}^{k-1}(a_k - a_i)) = v_p(c \cdot k!)$. Hence, at the kth step we choose $a_k = k$. Since p was arbitrarily chosen, the result holds.

□

Let p be a prime. Since the p-sequence is independent of the choice of p-ordering, we can calculate the p-sequence of $\mathbb{Z}$. For $k = 0$, we have $\alpha_{\mathbb{Z},p}(0) = 0$, and, for $k \in \{1, 2, 3, \ldots\}$, we have

$$\begin{aligned}
\alpha_{\mathbb{Z},p}(k) &= v_p\left(\prod_{i=0}^{k-1}(a_k - a_i)\right) \\
&= v_p((a_k - a_0)\ldots(a_k - a_{k-1})) \\
&= v_p((k-0)\ldots(k-(k-1))) \\
&= v_p(k!).
\end{aligned}$$

So, we get an expression with a factorial in it. In fact, if we multiply $p^{v_p(k!)}$ over all primes p, then we get exactly $k!$. That is,

$$k! = \prod_p p^{v_p(k!)} = \prod_p p^{\alpha_{\mathbb{Z},p}(k)}$$

Thus, the factorial function can be defined purely in terms of these invariants $\alpha_{\mathbb{Z},p}(k)$.

However, these invariants $\alpha_{S,p}(k)$ were defined not just for $\mathbb{Z}$ but for any subset S of $\mathbb{Z}$. This realization motivates the following definition:

Definition 3.5.2. *Let S be an arbitrary subset of $\mathbb{Z}$. Then the factorial function of S, denoted $k!_S$, is defined by*

$$k!_S = \prod_p p^{\alpha_{S,p}(k)}.$$

In particular, we have $k!_{\mathbb{Z}} = k!$.

Since we have unique factorization in $\mathbb{Z}$, we know that only finitely many of the factors in the product are not equal to 1. Thus, $k!_S$ is well-defined for all S and k.

This definition turns out to be an "appropriate" number-theoretic generalization of the factorial, in that many of the important number-theoretic properties of the usual factorial still hold for $k!_S$, even when $S \neq \mathbb{Z}$, as shown in [4].

Chapter 4

Generalized Characterization

4.1 Generalized "Falling Factorials"

Now, let us consider generalized "falling factorials." Typically, polynomials in $\mathbb{Q}[x]$ are written using the familiar basis $\{x^n : n \geq 0\}$. For many purposes, however, it is more convenient to use the "falling factorial" basis

$$\{x^{(n)} = x(x-1)\dots(x-n+1) : n = 0, 1, 2, \dots\}$$

Furthermore, note that for $n \in \{0, 1, 2, \dots\}$,

$$\binom{x}{n} = \frac{x(x-1)\dots(x-n+1)}{n!} = \frac{x^{(n)}}{n!}.$$

Thus, in order to characterize those polynomials that are integer-valued on a subset S of $\mathbb{Z}$ using generalized binomial polynomials, we must first generalize this notion of a "falling factorial".

Definition 4.1.1. *Let S be an arbitrary infinite subset of $\mathbb{Z}$ with p-ordering $\{a_i\}_{i=0}^{\infty}$. The generalized falling factorial of S, denoted $x^{(n)_{S,p}}$, is defined by*

$$x^{(n)_{S,p}} = (x-a_0)(x-a_1)\dots(x-a_{n-1}).$$

Note that when $S = \mathbb{Z}$ with p-ordering $\{0, 1, 2, \dots\}$, we have $x^{(n)_{\mathbb{Z},p}} = x^{(n)}$.

Taking this generalization one step further, we can construct a "global falling factorial."

Definition 4.1.2. *Let S be an arbitrary infinite subset of $\mathbb{Z}$. The global falling factorial of S, denoted $B_{k,S}(x)$, is defined by*

$$B_{k,S}(x) = (x-a_{0,k})(x-a_{1,k})\dots(x-a_{k-1,k}),$$

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

Note that such a sequence $\{a_{i,k}\}_{i=0}^{\infty}$ exists for any k as a result of the Chinese Remainder Theorem.

4.2 Generalized Basis

Recalling the basis for the integer-valued polynomials on $\mathbb{Z}$,

$$\left\{ \binom{x}{n} = \frac{x(x-1)\dots(x-n+1)}{n!} = \frac{x^{(n)}}{n!} : n = 0, 1, 2, \dots \right\},$$

the generalized basis for polynomials that are integer-valued on a subset S of $\mathbb{Z}$ is easily guessed. Namely, we expect, for each $n \in \{0, 1, 2, \dots\}$, the factorial in the denominator of $\binom{x}{n}$ to be replaced by the generalized factorial function of S, and the numerator to be replaced by the global falling factorial of S. Hence, we are led to the following result which was proved as Theorem 14 of [3].

Theorem 4.2.1. *A polynomial is integer-valued on a subset S of $\mathbb{Z}$ if and only if it can be written as a $\mathbb{Z}$-linear combination of the polynomials*

$$\left\{ \frac{B_{k,S}(x)}{k!_S} = \frac{(x-a_{0,k})(x-a_{1,k})\dots(x-a_{k-1,k})}{k!_S} : k = 0, 1, 2, .. \right\},$$

where $B_{k,S}$ is as defined in Definition 4.1.2.

More information about these generalized binomial polynomials, along with examples, can be found in [3] and [4]. Thus, we have our desired generalization to subsets of $\mathbb{Z}$ of the characterization of integer-valued polynomials on $\mathbb{Z}$.

4.3 Generalized Basis Example

Let us look at these generalized basis polynomials for a subset of $\mathbb{Z}$. For our example, we will need one more result that will help us find the generalized factorial function.

In our previous example of the entire set $\mathbb{Z}$, we found that the natural ordering $0, 1, 2, \dots$ of the nonnegative integers is a sequence that is a p-ordering for all primes p simultaneously. It is very rare for there to exist such a sequence for a general subset S of $\mathbb{Z}$. There are, however, a few important subsets of $\mathbb{Z}$ for which this is the case, such as

$$\{q^n : n \geq 0\} \text{ for } q \in \mathbb{N}_0, \{n^2 : n \geq 0\}, \text{ and } \left\{ \frac{n(n+1)}{2} : n \geq 0 \right\}.$$

Further results on simultaneous p-orderings can be found in [1], [2], and [12]. In the special cases when a simultaneous p-ordering does exist, the generalized factorial functions become quite simple to compute.

Lemma 4.3.1. *Let S be an arbitrary subset of $\mathbb{Z}$ with $\{a_i\}_{i=0}^{\infty}$ a p-ordering of S for all primes p simultaneously. Then*

$$k!_S = |(a_k - a_0)(a_k - a_1)\dots(a_k - a_{k-1})|.$$

Proof. The proof follows trivially from the definitions, since we have

$$k!_S = \prod_p p^{\alpha_{S,p}(k)} = \prod_p p^{v_p(\prod_{i=0}^{k-1}(a_k - a_i))} = |(a_k - a_0)(a_k - a_1)\dots(a_k - a_{k-1})|.$$

□

Example Let S be the set of even integers $2\mathbb{Z}$ in $\mathbb{Z}$. Then, using the same method as when finding the p-ordering of $\mathbb{Z}$, we see that the natural ordering $0, 2, 4, 6, \dots$ of the nonnegative even integers forms a p-ordering of $2\mathbb{Z}$ for all primes p simultaneously. Thus, by Lemma 4.3.1, the generalized factorial function of S is

$$k!_{2\mathbb{Z}} = |(2k - 0)(2k - 2)\dots(2k - (2k - 2))| = 2^k k!.$$

Now, since the natural ordering $0, 2, 4, 6, \dots$ of the nonnegative even integers forms a p-ordering of $2\mathbb{Z}$ for all primes p simultaneously, we can use $\{a_{i,k} = 2i\}_{i=0}^{\infty}$, as the sequence described in Definition 4.1.2. So, the global falling factorial of S is

$$B_{k,S}(x) = (x - 0)(x - 2)\dots(x - 2(k - 1)).$$

Therefore, our generalized basis polynomials are

$$\left\{ \frac{B_{k,S}(x)}{k!_S} = \frac{(x - 0)(x - 2)\dots(x - 2(k - 1))}{2^k k!} : k = 0, 1, 2, \dots \right\}.$$

The similarity of these polynomials to the binomial polynomials is clear, since

$$\begin{aligned} \frac{B_{k,S}(x)}{k!_S} &= \frac{(x - 0)(x - 2)\dots(x - 2(k - 1))}{2^k k!} \\ &= \frac{(\frac{x}{2} - 0)(\frac{x}{2} - 1)\dots(\frac{x}{2} - (k - 1))}{k!} \\ &= \binom{x/2}{k}. \end{aligned}$$

Chapter 5

Distribution of $\mathbb{F} \mod 5^k$ and mod 2^k

Bhargava's results in the previous chapter show that we can construct "generalized binomial polynomials", which form a regular basis for $\mathrm{Int}(\mathbb{F}, \mathbb{Z})$, if we know the p-sequence of $\mathbb{F}$ for all primes p. We now need to consider how we can determine these p-sequences. We start by calculating the 5-sequence and the 2-sequence of $\mathbb{F}$, since these p-sequences can be calculated without considering Coelho and Parry's results in [6].

Recall that the Fibonacci sequence $\mathbb{F} = \{F_n\}$ is defined by the recurrence relation

$$F_n = F_{n-1} + F_{n-2}, \quad n \geq 2,$$

with $F_0 = 0$ and $F_1 = 1$. Thus, any two consecutive terms in the sequence completely determine the entire sequence. Consider $\mathbb{F}$ modulo $m \in \mathbb{Z}_+$. There are only m^2 possible pairs of residues. Hence, some pair of consecutive terms of $\mathbb{F} \mod m$ must eventually repeat. So, $\mathbb{F} \mod m$ is periodic.

Definition 5.0.2. *The period of* $\mathbb{F}$ *modulo* $m \in \mathbb{Z}_+$ *is the smallest* $n \in \mathbb{Z}_+$ *such that* $F_n \equiv 0 \mod m$ *and* $F_{n+1} \equiv 1 \mod m$.

Let $m \geq 2$ and let b be a residue modulo m. We will write $D(m, b)$ for the number of times b occurs as a residue in one period of $\mathbb{F} \mod m$.

It is well-known, as shown in [11], that the Fibonacci numbers are *uniformly distributed* modulo 5^k, for $k \in \mathbb{Z}_+$. In fact, the period of $\mathbb{F} \mod 5^k$ is $4 \cdot 5^k$, and $D(5^k, b) = 4$ for all residues $b \mod 5^k$. Thus, $\mathbb{F}/(5^k) = \mathbb{Z}/(5^k), \forall k \in \mathbb{Z}_+$, since the integers are also uniformly distributed modulo 5^k. So, by Lemma 2.2.3, $\mathrm{Int}(\mathbb{F}, \mathbb{Z}_{(5)}) = \mathrm{Int}(\mathbb{Z}, \mathbb{Z}_{(5)})$, which means that the 5-sequence of $\mathbb{F}$ and the 5-sequence of $\mathbb{Z}$ are the same. Therefore, the 5-sequence of $\mathbb{F}$ can easily be computed using the formula following Proposition 3.5.1 for $\alpha_{\mathbb{Z},p}$, that is, $\alpha_{\mathbb{Z},p}(k) = v_p(k!), \forall k \in \mathbb{Z}_+$. The beginning of $\alpha_{\mathbb{F},5}$ is:

$$\alpha_{\mathbb{F},5} = \alpha_{\mathbb{Z},5} = \{0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 2, 2, 2, 2, 2, 3, 3, 3, 3, 3, 4, 4, 4, 4, 4, 6, 6, 6, 6, 6, \dots\}.$$

Obviously, the fact that the Fibonacci numbers are uniformly distributed modulo 5^k made the calculation of $\alpha_{\mathbb{F},5}$ very simple. Unfortunately, the Fibonacci numbers are uniformly distributed only modulo p^k for $p = 5$. We are, however, also able to completely describe the function $D(2^k, b)$, for $k \in \mathbb{Z}_+$, due to a type of stability that occurs when $k \geq 5$. The following result was shown by Jacobson in [9]. Note that the values of $D(2^k, b)$ for $k = 1, 2, 3, 4$ can easily be checked by hand, but have been included for completeness.

Theorem 5.0.3. *For* $\mathbb{F} \mod 2^k$*, with* $k \in \mathbb{Z}_+$*, the following data appertain:*

For $1 \leq k \leq 4$*:*

$D(2, 0) = 1$,

$D(2, 1) = 2$,

$D(4, 0) = D(4, 2) = 1$,

$D(8, 0) = D(8, 2) = D(16, 0) = D(16, 8) = 2$,

$D(16, 2) = 4$,

$D(2^k, b) = 1$ *if* $b \equiv 3 \mod 4$ *and* $2 \leq k \leq 4$,

$D(2^k, b) = 3$ *if* $b \equiv 1 \mod 4$ *and* $2 \leq k \leq 4$, *and*

$D(2^k, b) = 0$ *in all other cases,* $1 \leq k \leq 4$.

For $k \geq 5$*:*

$$D(2^k, b) = \begin{cases} 1, & \text{if } b \equiv 3 \mod 4 \\ 2, & \text{if } b \equiv 0 \mod 8 \\ 3, & \text{if } b \equiv 1 \mod 4 \\ 8, & \text{if } b \equiv 2 \mod 32 \\ 0, & \text{for all other residues.} \end{cases}$$

The residue classes modulo 2 represented by the Fibonacci numbers can be visualized with the tree diagram in Figure 5.1.

A node in the tree diagram represents the residue class modulo the power of 2 aligned with the node on the left of the tree. A node is drawn if there is a Fibonacci number in that residue class and omitted if not. For instance there is a Fibonacci number in the residue class 2 modulo 2^3, but there is no Fibonacci number in the residue class 4 modulo 2^3. A triangle is used to depict the fact that there is a Fibonacci number in all of the residue classes below the node to which it is attached.

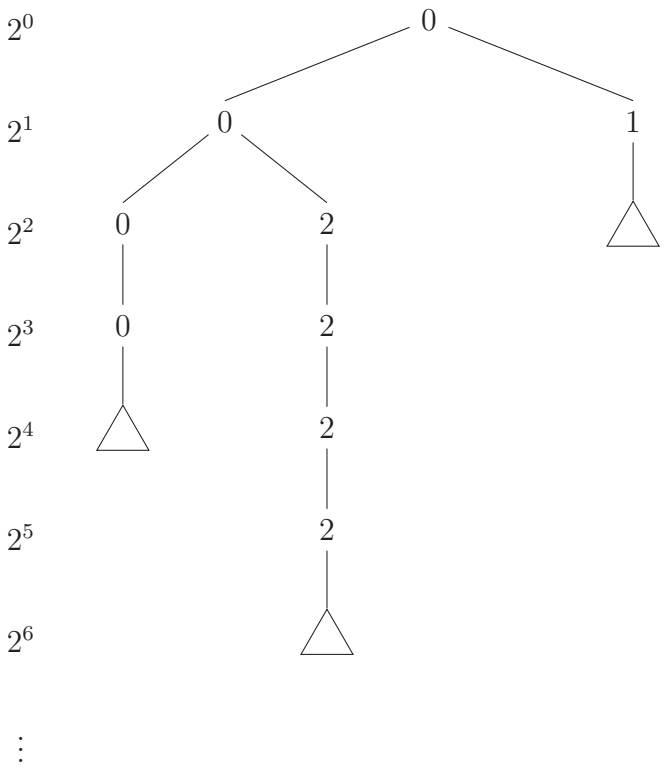

Figure 5.1: Tree diagram for $p = 2$.

For example, there is a Fibonacci number in each of the residue classes modulo 2^k, for $k \in \{4, 5, \dots\}$, that are equivalent to $0 \mod 2^3$.

Thus, $\forall k > 0$,

$$\frac{\mathbb{F}}{(2^k)} = \frac{(1 + 2\mathbb{Z}) \cup (0 + 8\mathbb{Z}) \cup (2 + 32\mathbb{Z})}{(2^k)}.$$

So, by Lemma 2.2.3,

$$\mathrm{Int}(\mathbb{F}, \mathbb{Z}_{(2)}) = \mathrm{Int}((1 + 2\mathbb{Z}) \cup (0 + 8\mathbb{Z}) \cup (2 + 32\mathbb{Z}), \mathbb{Z}_{(2)}),$$

which means that the 2-sequence of $\mathbb{F}$ and the 2-sequence of $(1 + 2\mathbb{Z}) \cup (0 + 8\mathbb{Z}) \cup (2 + 32\mathbb{Z})$ are the same. Using Lemma 3.3.1 and Lemma 3.3.6, the 2-sequence of $(1+2\mathbb{Z}) \cup (0+8\mathbb{Z}) \cup (2+32\mathbb{Z})$ can be calculated and it is the same as the 2-sequence of $\mathbb{F}$.

Proposition 5.0.4. *The 2-sequence of* $\mathbb{F}$ *is*

$$\alpha_{\mathbb{F},2} = (\alpha_{\mathbb{Z},2} + (k)) \wedge (((\alpha_{\mathbb{Z},2} + (2k)) \wedge (\alpha_{\mathbb{Z},2} + (4k))) + (k)).$$

Proof. We must first calculate the 2-sequence of $(0+8\mathbb{Z})\cup(2+32\mathbb{Z})$, using Lemma 3.3.1 and Lemma 3.3.6, as follows:

$$\alpha_{(0+8\mathbb{Z})\cup(2+32\mathbb{Z}),2} = (((\alpha_{\mathbb{Z},2} + (3k)) - (k)) \wedge ((\alpha_{\mathbb{Z},2} + (5k)) - (k))) + (k).$$

Then, using Lemma 3.3.1 and Lemma 3.3.6 again, we can compute the 2-sequence of $(1 + 2\mathbb{Z}) \cup (0 + 8\mathbb{Z}) \cup (2 + 32\mathbb{Z})$ to be:

$$\begin{aligned}\alpha_{(1+2\mathbb{Z})\cup(0+8\mathbb{Z})\cup(2+32\mathbb{Z}),2} &= \alpha_{(1+2\mathbb{Z}),2} \wedge \alpha_{(0+8\mathbb{Z})\cup(2+32\mathbb{Z}),2} \\ &= (\alpha_{\mathbb{Z},2} + (k)) \wedge (((\alpha_{\mathbb{Z},2} + (2k)) \wedge (\alpha_{\mathbb{Z},2} + (4k))) + (k)).\end{aligned}$$

Since, $\alpha_{\mathbb{F},2} = \alpha_{(1+2\mathbb{Z})\cup(0+8\mathbb{Z})\cup(2+32\mathbb{Z}),2}$, the result holds. □

The beginning of $\alpha_{\mathbb{F},2}$ is:

$$\alpha_{\mathbb{F},2} = \{0, 0, 1, 1, 3, 4, 4, 7, 7, 8, 9, 10, 11, 12, 15, 15, 16, 18, 18, 19, 21, 22, 22, \dots\}.$$

The computations involved can be seen in this table:

	(k)	0	1	2	3	4	5	6	7	8	9	10	11	12	13
	$\alpha_{\mathbb{Z},2}$	0	0	1	1	3	3	4	4	7	7	8	8	10	10
	$\alpha_{\mathbb{Z},2} + (k)$	0	1	3	4	7	8	10	11	15	16	18	19	22	23
(4)	$\alpha_{\mathbb{Z},2} + (2k)$	0	2	5	7	11	13	16	18	23	25	28	30	34	36
(5)	$\alpha_{\mathbb{Z},2} + (4k)$	0	4	9	13	19	23	28	32	39	43	48	52	58	62
(6)	$(4) \wedge (5)$	0	0	2	4	5	7	9	11	13	13	16	18	19	23
	$(6) + (k)$	0	1	4	7	9	12	15	18	21	22	26	29	31	36
	$\alpha_{\mathbb{F},2}$	0	0	1	1	3	4	4	7	7	8	9	10	11	12

In order to use Coelho and Parry's results from [6] to help us calculate the p-sequence of the Fibonacci numbers for the primes p different from 5 and 2, we will need some additional background material, which will be covered in the next two chapters.

Chapter 6

The p-adic Integers

For an odd prime p, we take $\mathbb{Z}_p$ to be the p-adic integers, whose elements are the sums $x = \sum_{n=0}^{\infty} x_n p^n$ that converge with respect to the p-adic metric, where $x_n \in \{0, \ldots, p-1\}$. Since many of our calculations are done modulo p, we note that x_0 is the reduction of $x \mod p$. The units, i.e., invertible elements, of $\mathbb{Z}_p$, which we denote by $\mathbf{U}$, consist of those $x \in \mathbb{Z}_p$ with $x_0 \neq 0$, i.e., $\mathbf{U} = \{x : p \nmid x\}$. That is, $\mathbf{U}$ is the multiplicative group $\mathbb{Z}_p^*$.

If $5 \in \mathbf{U}$ is not a square, $\mathbb{Z}_p(\sqrt{5}) = \mathbb{Z}_p + \sqrt{5}\mathbb{Z}_p$ is a ring with the obvious addition and multiplication. The units of $\mathbb{Z}_p(\sqrt{5})$, which we denote by $\mathbf{U}(\sqrt{5})$, consist of all $x + \sqrt{5}y$, with $x, y \in \mathbb{Z}_p$ and at least one of x, y in $\mathbf{U}$. Since the expression $x + \sqrt{5}y$ is unique, we can define the norm $N : \mathbf{U}(\sqrt{5}) \to \mathbf{U}$ by $N(x + \sqrt{5}y) = x^2 - 5y^2$. This is a multiplicative homomorphism and helps us to define the subgroup

$$\mathbf{U}^0(\sqrt{5}) = \{x + \sqrt{5}y \in \mathbf{U}(\sqrt{5}) : x^2 - 5y^2 = \pm 1\},$$

which will be of interest later.

For later results, we will define, for each $n \in \mathbb{Z}_+$, the subgroups $\mathbf{U}_n = 1 + p^n\mathbb{Z}_p$ of $\mathbf{U}$ and $\mathbf{U}_n(\sqrt{5}) = 1 + p^n(\mathbb{Z}_p(\sqrt{5}))$ of $\mathbf{U}(\sqrt{5})$, so that

$$\mathbf{U} \supseteq \mathbf{U}_1 \supseteq \mathbf{U}_2 \supseteq \ldots \text{ and } \cap_{n=1}^{\infty} \mathbf{U}_n = \{1\}$$

and

$$\mathbf{U}(\sqrt{5}) \supseteq \mathbf{U}_1(\sqrt{5}) \supseteq \mathbf{U}_2(\sqrt{5}) \supseteq \ldots \text{ and } \cap_{n=1}^{\infty} \mathbf{U}_n(\sqrt{5}) = \{1\}$$

It is easy to see that $\mathbf{U}/\mathbf{U}_1$ is isomorphic to the multiplicative group of $\mathbb{Z}/p\mathbb{Z}$ and $\mathbf{U}(\sqrt{5})/\mathbf{U}_1(\sqrt{5})$ is isomorphic to the multiplicative group of $\mathbb{F}_{p^2}$.

We will also need the following definitions:

Definition 6.0.5. *Let p be an odd integer prime and let S be a subset of a set T in $\mathbb{Z}_p$. If $\forall \epsilon > 0$ and $\forall t \in T$ $\exists s \in S$ such that $v_p(s - t) > \epsilon$, then S is p-adically dense in T.*

Definition 6.0.6. *Let p be an odd integer prime and let $g : \mathbb{Z}_p \to \mathbb{Z}_p$. The map g is p-adically continuous at the point $z_0 \in Z_p$, if $\forall \epsilon > 0$ $\exists \delta > 0$ such that $\forall z \in \mathbb{Z}_p$ with $v_p(z - z_0) > \delta$ we have $v_p(g(z) - g(z_0)) > \epsilon$. The map g is p-adically continuous if it is p-adically continuous at all points in $\mathbb{Z}_p$.*

Additionally, we can define similar concepts in $\mathbb{Z}_p(\sqrt{5})$, by replacing $\mathbb{Z}_p$ with $\mathbb{Z}_p(\sqrt{5})$.

The next theorem will be used extensively in the material that follows. A proof of this result can be found as Theorem 3.4.1 in [7].

Theorem 6.0.7. ***(Hensel's Lemma)*** *Let p be an odd integer prime and let $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ be a polynomial whose coefficients are in $\mathbb{Z}_p$. Let $f'(x) = a_1 + 2a_2x + \cdots + na_nx^{n-1}$ be its derivative. Suppose that there exists a p-adic integer $\alpha_0 \in \mathbb{Z}_p$ such that*

$$f(\alpha_0) \equiv 0 \mod p$$

and

$$f'(\alpha_0) \not\equiv 0 \mod p.$$

Then there exists a unique p-adic integer $\alpha \in \mathbb{Z}_p$ such that $\alpha \equiv \alpha_0 \mod p$ and $f(\alpha) = 0$.

We should note that the corresponding theorem with $\mathbb{Z}_p$ replaced by $\mathbb{Z}_p(\sqrt{5})$ also holds.

In many of the applications of Hensel's Lemma in this thesis, we will be using it in the form of an important corollary. To state this corollary, we need to define the Legendre symbol.

Definition 6.0.8. *Let p be an odd integer prime. The Legendre symbol of $z = \sum_{n=0}^{\infty} z_n p^n \in \mathbb{Z}_p$ is defined as follows:*

$$\left(\frac{z}{p}\right) = \begin{cases} 1, & \text{if } z_0 \text{ is congruent to a square modulo } p \text{ and } z_0 \not\equiv 0 \mod p \\ -1, & \text{if } z_0 \text{ is not congruent to a square modulo } p \\ 0, & \text{if } z_0 \equiv 0 \mod p. \end{cases}$$

Now, the corollary to Hensel's Lemma that we apply several times in this thesis is:

Corollary 6.0.9. *Let p be an odd integer prime and let $z \in \mathbb{Z}_p$ with $z \not\equiv 0 \mod p$. The square root of z is in $\mathbb{Z}_p$ if and only if $\left(\frac{z}{p}\right) = 1$.*

Proof. If the square root of z is in $\mathbb{Z}_p$ and $z \not\equiv 0 \mod p$, then $\left(\frac{z}{p}\right) = 1$.

Conversely, suppose $\left(\frac{z}{p}\right) = 1$ and let $f(x) = x^2 - z$. So, $f'(x) = 2x$. If $\alpha_0 \in \mathbb{Z}_p$ such that $\alpha_0 = \sqrt{z} \mod p$, then

$$f(\alpha_0) = \alpha_0^2 - z \equiv 0 \mod p$$

and

$$f'(\alpha_0) = 2\alpha_0 \not\equiv 0 \mod p,$$

where the second condition holds since p is odd. By Hensel's Lemma, there exists a unique p-adic integer $\alpha \in \mathbb{Z}_p$ such that $\alpha \equiv \alpha_0 \mod p$ and $f(\alpha) = 0$. Thus, the square root of z is in $\mathbb{Z}_p$. □

The existence of α can be seen by recursively constructing a sequence of integers $\{r_k\}$, starting from $r_1 = \alpha_0$, such that $r_{k+1} \equiv r_k \mod p^k$ and $r_k^2 \equiv z \mod p^k$. This sequence converges to α and we have $\alpha^2 = z$.

Using the law of quadratic reciprocity, we can easily test whether $\left(\frac{z}{p}\right) = 1$. Thus, we have a practical way to determine which p-adic numbers have a square root in $\mathbb{Z}_p$.

Chapter 7

Generators for $(\mathbb{Z}/(p^k))^*$

We must now show that if p is an odd prime integer and $k \in \mathbb{Z}_+$, then $(\mathbb{Z}/(p^k))^*$ is cyclic. In order to do so, we will need some definitions and the following sequence of elementary results, which are presented here as in Chapter 4 of [8].

Definition 7.0.10. *The order of an element g of a group G is the smallest positive integer k such that $g^k = e$, where e denotes the identity element of G and g^k denotes the product of k copies of g. If no such k exists, g is said to have infinite order.*

Definition 7.0.11. *Let $n \in \mathbb{Z}$. An element g of a group G is a primitive root modulo n if it generates the group of units of G modulo n.*

With these definitions, we can now look at the results which will help us prove that $(\mathbb{Z}/(p^k))^*$ is cyclic.

Lemma 7.0.12. *If p is a prime integer and $k \in \mathbb{Z}_+$ with $k < p$, then the binomial coefficient $\binom{p}{k}$ is divisible by p*

Proof. By definition, $\binom{p}{k} = \frac{p!}{k!(p-k)!}$. Thus, $p! = k!(p-k)!\binom{p}{k}$. Now, p divides $p!$, but p does not divide $k!(p-k)!$, since this expression is a product of integers less than, and thus relatively prime to, p. Hence, p must divide $\binom{p}{k}$. □

Lemma 7.0.13. *If $a, b \in \mathbb{Z}$ and $k \in \mathbb{Z}_+$ and $a \equiv b \mod p^k$, then $a^p \equiv b^p \mod p^{k+1}$.*

Proof. Since $a \equiv b \mod p^k$, we may write $a = b + cp^k, c \in \mathbb{Z}$. By the binomial theorem, $a^p = b^p + \binom{p}{1}b^{p-1}cp^k + A$, where A is an integer divisible by p^{k+2}. The second term is clearly divisible by p^{k+1}. Thus, $a^p \equiv b^p \mod p^{k+1}$. □

Corollary 7.0.14. *If p is an odd prime integer and $k \in \mathbb{Z}_+, k \geq 2$, then $(1+ap)^{p^{k-2}} \equiv 1 + ap^{k-1} \mod p^k, \forall a \in \mathbb{Z}$.*

Proof. The proof is by induction on k. For $k = 2$, the assertion is trivial. Suppose the result holds for some $k \geq 2$. We will show that it then also holds for $k+1$. By the inductive hypothesis and Lemma 7.0.13, we have $(1+ap)^{p^{k-1}} \equiv (1+ap^{k-1})^p \mod p^{k+1}$. Applying the binomial theorem, $(1+ap^{k-1})^p = 1 + \binom{p}{1}ap^{k-1} + B$, where B is the sum of $p-1$ terms. Using Lemma 7.0.12, it is clear that all of these terms are divisible by $p^{1+2(k-1)}$, except perhaps for the last term, $a^p p^{p(k-1)}$. Now, since $k \geq 2$, $1+2(k-1) \geq k+1$, and since also $p \geq 3$, $p(k-1) \geq k+1$. Thus, $p^{k+1}|B$ and $(1+ap)^{p^{k-1}} \equiv 1 + ap^k \mod p^{k+1}$, which is as required. □

Corollary 7.0.15. *If p is an odd prime integer, $a \in \mathbb{Z}$ such that $p \nmid a$, and $k \in \mathbb{Z}_+, k \geq 2$, then p^{k-1} is the order of $1+ap \mod p^k$.*

Proof. By Corollary 7.0.14, we know $(1+ap)^{p^{k-1}} \equiv 1 + ap^k \mod p^{k+1}$. Thus, $(1+ap)^{p^{k-1}} \equiv 1 \mod p^k$. So, $1+ap$ has order dividing p^{k-1}. Now, by assumption, $p \nmid a$ and, from Corollary 7.0.14, we have $(1+ap)^{p^{k-2}} \equiv 1 + ap^{k-1} \mod p^k$, which shows that p^{k-2} is not a multiple of the order of $1+ap$. Therefore, p^{k-1} is the order of $1+ap \mod p^k$. □

With these results, we may now prove the desired result.

Theorem 7.0.16. *If p is an odd prime integer and $k \in \mathbb{Z}_+$, then $(\mathbb{Z}/(p^k))^*$ is cyclic. In fact, if*

1. *$g \in \mathbb{Z}$ is a primitive root mod p (i.e., $p-1$ is the least positive integer k for which $g^k \equiv 1 \mod p$) and*
2. *$g^{p-1} \not\equiv 1 \mod p^2$,*

then g generates $(\mathbb{Z}/(p^k))^*, \forall k \in \mathbb{Z}_+$. Moreover, such a g always exists.

Proof. Suppose p is an odd prime integer and $k \in \mathbb{Z}_+$. It is sufficient to prove the second and third statements. It is well-known that there exist primitive roots mod p. If $g \in \mathbb{Z}$ is a primitive root mod p, then $g+p$ is also. If $g^{p-1} \equiv 1 \mod p^2$, then $(g+p)^{p-1} \equiv g^{p-1} + (p-1)g^{p-2}p \equiv 1 + (p-1)g^{p-2}p \not\equiv 1 \mod p^2$. Thus, $\exists g \in \mathbb{Z}$ such that g is a primitive root mod p and $g^{p-1} \not\equiv 1 \mod p^2$.

We will now show that such a g is a primitive root mod p^k. It is enough to prove that if $g^n \equiv 1 \mod p^k$, then $\phi(p^k) = p^{k-1}(p-1)|n$, i.e., that the order of g is $\phi(p^k)$.

Suppose $g^n \equiv 1 \mod p^k$. We chose g such that $g^{p-1} = 1 + ap$, for some $a \in \mathbb{Z}$ such that $p \nmid a$. By Corollary 7.0.15, the order of $1 + ap \mod p^k$ is p^{k-1}. Since $(1 + ap)^n = (g^{p-1})^n \equiv 1^{p-1} \equiv 1 \mod p^k$, we have $p^{k-1}|n$.

Let $n = p^{k-1}n'$. Then $g^n = (g^{p^{k-1}})^{n'} \equiv g^{n'} \mod p$ and, since $g^n \equiv 1 \mod p^k$, we have $g^{n'} \equiv 1 \mod p$. Therefore, $p - 1|n'$, since g is a primitive root mod p. Hence, $p^{k-1}(p - 1)|n$ and g generates $(\mathbb{Z}/(p^k))^*$. □

Theorem 7.0.16 shows that if $g \in \mathbb{Z}$ is a primitive root mod p and $g^{p-1} \not\equiv 1 \mod p^2$, then g generates $(\mathbb{Z}/(p^k))^*, \forall k \in \mathbb{Z}_+$. We need to know, however, what happens if a p-adic integer, g, satisfies those same conditions. For this case, we have the following corollary:

Corollary 7.0.17. *For p an odd prime integer, if*

1. *$g \in \mathbb{Z}_p$ is a primitive root mod p (i.e., $p - 1$ is the least positive integer k for which $g^k \equiv 1 \mod p$) and*

2. *$g^{p-1} \not\equiv 1 \mod p^2$,*

then g generates $(\mathbb{Z}/(p^k))^*, \forall k \in \mathbb{Z}_+$.

Proof. Let p be an odd prime integer and $k \in \mathbb{Z}_+$. Suppose $g \in \mathbb{Z}_p$ is a primitive root mod p and $g^{p-1} \not\equiv 1 \mod p^2$. We can choose $h \in \mathbb{Z}$ such that $h \equiv g \mod p^k$. Then h is a primitive root mod p and $h^{p-1} \not\equiv 1 \mod p^2$, since g is. Hence, by Theorem 7.0.16, h generates $(\mathbb{Z}/(p^n))^*, \forall n \leq k$, and so, g does also. Since k was chosen arbitrarily, g generates $(\mathbb{Z}/(p^k))^*, \forall k \in \mathbb{Z}_+$. □

We will need a similar result for $g \in \mathbf{U}^0(\sqrt{5})$. Thus, we will need results similar to Lemma 7.0.13 and its corollaries, for when $a, b \in \mathbb{Z}_p(\sqrt{5})$. These results are stated below, but the proofs are not shown as they are almost identical to the ones with $a, b \in \mathbb{Z}$.

Lemma 7.0.18. *If $a, b \in \mathbb{Z}_p(\sqrt{5})$ and $k \in \mathbb{Z}_+$ and $a \equiv b \mod p^k$, then $a^p \equiv b^p \mod p^{k+1}$.*

Corollary 7.0.19. *If p is an odd prime integer and $k \in \mathbb{Z}_+, k \geq 2$, then $(1+ap)^{p^{k-2}} \equiv 1 + ap^{k-1} \mod p^k, \forall a \in \mathbb{Z}_p(\sqrt{5})$.*

Corollary 7.0.20. *If p is an odd prime integer, $a \in \mathbb{Z}_p(\sqrt{5})$ such that $p \nmid a$, and $k \in \mathbb{Z}_+, k \geq 2$, then p^{k-1} is the order of $1 + ap \mod p^k$.*

Before we prove the result similar to Corollary 7.0.17 for $g \in \mathbf{U}^0(\sqrt{5})$, note that the cardinality of $\mathbf{U}(\sqrt{5}) \mod p$ is p^2-1, since $\mathbf{U}(\sqrt{5}) \mod p$ consists of all $x+\sqrt{5}y$, with $x, y \in \{0, 1, \ldots, p-1\}$ and at least one of x and y not equal to 0. Next, note that the cardinality of $\mathbf{U}^0(\sqrt{5}) \mod p$ is $2(p+1)$. To see this fact, we observe that each element of $\mathbb{F}_p^\times$ is the mod p norm of some element of $\mathbf{U}(\sqrt{5}) \mod p$, which is shown as Lemma 11 of [6]. It is, then, not hard to see that for any $k \in \mathbb{F}_p^\times$ there is a one-to-one correspondence between $\{x \in \mathbf{U}(\sqrt{5}) \mod p : N(x) = k\}$ and $\{x \in \mathbf{U}(\sqrt{5}) \mod p : N(x) = 1\}$, due to the multiplicative property of the norm. Thus, each of these sets has cardinality $(p^2-1)/(p-1) = p+1$. Since $\mathbf{U}^0(\sqrt{5}) \mod p$ is the union of two such sets, namely, those with $k = \pm 1$, $\mathbf{U}^0(\sqrt{5}) \mod p$ has order $2(p+1)$. Moreover, as a subgroup of the multiplicative group $\mathbf{U}(\sqrt{5}) \mod p$ of a finite field $\mathbb{Z}_p(\sqrt{5}) \mod p$, we see that $\mathbf{U}^0(\sqrt{5}) \mod p$ is cyclic.

We can now prove the result for $g \in \mathbf{U}^0(\sqrt{5})$.

Theorem 7.0.21. *For p an odd prime integer, if*

1. *$g \in \mathbf{U}^0(\sqrt{5})$ is a primitive root mod p (i.e., $2(p+1)$ is the least positive integer k for which $g^k \equiv 1 \mod p$) and*
2. *$g^{2(p+1)} \not\equiv 1 \mod p^2$,*

then g generates $\mathbf{U}^0(\sqrt{5})/\mathbf{U}_k(\sqrt{5}), \forall k \in \mathbb{Z}$.

Proof. Suppose p is an odd prime integer and $k \in \mathbb{Z}_+$. Note that the cardinality of $\mathbf{U}(\sqrt{5}) \mod p^k$ is $(p^k)^2 - (p^{k-1})^2 = p^{2k} - p^{2k-2} = p^{2k-2}(p^2-1)$ and recall that the cardinality of $\mathbf{U}/\mathbf{U}_k = (\mathbb{Z}/(p^k))^* = \phi(p^k) = p^{k-1}(p-1)$. Also, in a similar manner as above, note that each element of $\mathbf{U}/\mathbf{U}_k$ is the mod p^k norm of some element of $\mathbf{U}(\sqrt{5})$ mod p^k and it is not difficult to see that there is a one-to-one correspondence between $\{x \in \mathbf{U}(\sqrt{5}) \mod p^k : N(x) = m\}$ and $\{x \in \mathbf{U}(\sqrt{5}) \mod p^k : N(x) = 1\}$. For this reason each of these sets has cardinality $(p^{2k-2}(p^2-1))/(p^{k-1}(p-1)) = p^{k-1}(p+1)$, and, therefore, $\mathbf{U}^0(\sqrt{5}) \mod p^k$ has order $2(p+1)p^{k-1}$.

We will now show that if $g \in \mathbf{U}^0(\sqrt{5})$ is a primitive root mod p and $g^{2(p+1)} \not\equiv 1$ mod p^2, then g generates $\mathbf{U}^0(\sqrt{5})/\mathbf{U}_k(\sqrt{5})$. It is enough to prove that if $g^n \equiv 1$ mod p^k, then $2(p+1)p^{k-1}|n$.

Suppose $g^n \equiv 1 \mod p^k$. Then $g^n \equiv 1 \mod p$ and $2(p+1)|n$, since g is a primitive root mod p. Now, we chose g such that $g^{2(p+1)} = 1 + ap$, for some $a \in \mathbb{Z}_p(\sqrt{5})$ such that $p \nmid a$. By Corollary 7.0.20, the order of $1 + ap \mod p^k$ is p^{k-1}. So, since $(1 + ap)^n = (g^{2(p+1)})^n \equiv 1^{2(p+1)} \equiv 1 \mod p^k$, we have $p^{k-1}|n$. Hence, $2(p + 1)p^{k-1}|n$, since $\gcd(2(p + 1), p^{k-1}) = 1$. Therefore, g generates $\mathbf{U}^0(\sqrt{5})/\mathbf{U}_k(\sqrt{5})$. □

Chapter 8

The Fibonacci Sequence

8.1 Coelho and Parry

For the primes p for which β satisfies Condition 1.0.1, β also satisfies either Corollary 7.0.17, if $\beta \in \mathbb{Z}_p$, or Theorem 7.0.21, if $\beta \in \mathbf{U}^0(\sqrt{5})$. In [6], Coelho and Parry use this fact to determine, for these primes, which residue classes of $\mathbb{Z}/(p^k)$ are represented by Fibonacci numbers. In fact, by requiring p to satisfy a slightly stronger condition, they are able to give a complete description of the distribution of the Fibonacci numbers modulo prime powers. We can use this information on which residue classes of $\mathbb{Z}/(p^k)$ are represented by Fibonacci numbers to find $T \subseteq \mathbb{Z}$ with $\mathbb{F} \subseteq T$ and $\mathbb{F}/(p^k) = T/(p^k), \forall k \geq 0$, so that we may apply Lemma 2.2.3. Then, as shown in Section 2.2, the p-sequence of T will be the same as the p-sequence of $\mathbb{F}$. Moreover, the set T we find will be of a form that makes it easier to apply the results on computing p-sequences from Section 3.3.

Recall that the Fibonacci sequence $\mathbb{F} = \{F_n\}$ is defined by the recurrence relation

$$F_n = F_{n-1} + F_{n-2}, n \geq 2,$$

with $F_0 = 0$ and $F_1 = 1$, and that, by Binet's formula, we can write

$$F_n = \frac{1}{\sqrt{5}} \left(\beta^n - \left(\frac{-1}{\beta} \right)^n \right),$$

where $\beta = \frac{1+\sqrt{5}}{2}$. We see that $\forall n = 0, 1, 2, \ldots$, we have $F_n = f(\beta^n)$, where $f : \mathbf{U} \to \mathbb{Z}_p$ or $f : \mathbf{U}^0(\sqrt{5}) \to \mathbb{Z}_p$ is given by

$$f(z) = \frac{1}{\sqrt{5}} \left(z - \frac{N(z)}{z} \right)$$

and $N(z) = 1$ or -1 according to whether z is a square or not (in $\mathbf{U}$ or $\mathbf{U}^0(\sqrt{5})$). Note that for $z \in \mathbf{U}^0(\sqrt{5})$, $N(z)$ is simply the norm defined in Chapter 6 and the map N distinguishes between the even and the odd powers of β.

Since Binet's formula gives $\mathbb{F} = \{f(\beta^n) : n = 0, 1, 2, \dots\} = f(\langle\beta\rangle)$, the residue classes of $\mathbb{Z}/(p^k)$ represented by the Fibonacci numbers are exactly those in the image of the function f. Thus, $\mathbb{F}/(p^k) = f(\langle\beta\rangle)/(p^k), \forall k > 0$. Hence, to determine which residue classes are represented by the Fibonacci numbers modulo various primes p, we just need to consider for which $y \in \mathbb{Z}_p$ the equation

$$f(z) = \frac{1}{\sqrt{5}}\left(z - \frac{N(z)}{z}\right) = y,$$

is solvable for z in terms of y.

The domain of f depends on which group contains β, which is determined by the prime p.

Lemma 8.1.1. *Let p be an odd integer prime different from 5. The square root of 5 is in $\mathbb{Z}_p$ if and only if $p \equiv \pm 1 \mod 5$.*

Proof. The square root of 5 is in $\mathbb{Z}_p$ if and only if $\left(\frac{5}{p}\right) = 1$, by Corollary 6.0.9. By the law of quadratic reciprocity,

$$\left(\frac{5}{p}\right)\left(\frac{p}{5}\right) = (-1)^{(5-1)(p-1)/4} = (-1)^{p-1} = 1.$$

Hence, by the multiplicative property of the Legendre symbol, $\left(\frac{5}{p}\right) = 1$ if and only if $\left(\frac{p}{5}\right) = 1$. Now, $\left(\frac{p}{5}\right) = 1$ if and only if $p \equiv \pm 1 \mod 5$. Thus, the result holds. □

By Lemma 8.1.1, if $p \equiv \pm 1 \mod 5$, then the square root of 5 is in $\mathbb{Z}_p$. Thus, $\beta \in \mathbf{U}$ and the domain of f is $\mathbf{U}$. On the other hand, if $p \equiv \pm 2 \mod 5$, then the square root of 5 is not in $\mathbb{Z}_p$. Hence, $\beta \in \mathbf{U}^0(\sqrt{5})$ and the domain of f is $\mathbf{U}^0(\sqrt{5})$. We consider these two cases separately. Before we look at the first case with $p \equiv \pm 1 \mod 5$, we must introduce some additional notation.

We write $\mathbf{i}(y)$ for the total number of solutions of $f(z) = y$, with $\mathbf{i}(y) = \mathbf{i}_+(y) + \mathbf{i}_-(y)$, where $\mathbf{i}_+(y)$ is the number of squares that are solutions of $f(z) = y$ and $\mathbf{i}_-(y)$ is the number of non-squares that are solutions of $f(z) = y$.

Proposition 8.1.2. *If $\mathbf{i}_+(y)$ and $\mathbf{i}_-(y)$ are defined as above, then*

1. *$\mathbf{i}_+(y)$ is the number of squares of the form $(\sqrt{5}y \pm \sqrt{5y^2 + 4})/2$ and*
2. *$\mathbf{i}_-(y)$ is the number of non-squares of the form $(\sqrt{5}y \pm \sqrt{5y^2 - 4})/2$.*

Proof. When $f(z) = y$, we have

$$\begin{aligned} \frac{1}{\sqrt{5}}\left(z - \frac{N(z)}{z}\right) - y &= 0 \\ \frac{z^2 - N(z)}{\sqrt{5}z} - y &= 0 \\ z^2 - \sqrt{5}yz - N(z) &= 0. \end{aligned}$$

Thus, by the quadratic formula,

$$z = \frac{\sqrt{5}y \pm \sqrt{5y^2 + 4N(z)}}{2}.$$

Since $N(z) = 1$ or -1 according to whether z is a square or not (in $\mathbf{U}$ or $\mathbf{U}^0(\sqrt{5})$), $\mathbf{i}_+(y)$ is the number of squares of the form $(\sqrt{5}y \pm \sqrt{5y^2+4})/2$ and $\mathbf{i}_-(y)$ is the number of non-squares of the form $(\sqrt{5}y \pm \sqrt{5y^2-4})/2$. □

The actual value of $\mathbf{i}(y)$ is important for Coelho and Parry's results on the distribution of the Fibonacci numbers modulo prime powers. We only need to know, however, whether or not $\mathbf{i}(y)$ is zero in order to determine which residue classes of $\mathbb{Z}/(p^k)$ are represented by the Fibonacci numbers.

We are now ready to look at the first case with $p \equiv \pm 1 \mod 5$.

8.2 Case I: $p \equiv \pm 1 \mod 5$

When $p \equiv \pm 1 \mod 5$, we have two subcases to consider. Before looking at these subcases, recall that $y \in \mathbb{Z}_p$ is a sum $y = \sum_{n=0}^{\infty} y_n p^n$, with $y_n \in \{0, \ldots, p-1\}$, whose convergence is assured with respect to the p-adic metric, and that y_0 is the reduction of $y \mod p$.

8.2.1 Case I (a): $5y_0^2 \pm 4 \not\equiv 0 \mod p$

Proposition 8.2.1. *When $5y_0^2 + 4 \not\equiv 0 \mod p$, $\mathbf{i}_+(y) = \mathbf{i}_+(y_0)$ depends only on y_0, and when $5y_0^2 - 4 \not\equiv 0 \mod p$, $\mathbf{i}_-(y) = \mathbf{i}_-(y_0)$ depends only on y_0.*

Proof. Suppose $5y_0^2 + 4 \not\equiv 0 \mod p$. Recall that $\mathbf{i}_+(y)$ is the number of squares of the form $(\sqrt{5}y \pm \sqrt{5y^2+4})/2$. Note that $5y^2 + 4 \in \mathbb{Z}_p$ with $5y^2 + 4 \equiv 5y_0^2 + 4 \not\equiv 0 \mod p$. Thus, by Corollary 6.0.9, the square root of $5y^2 + 4$ is in $\mathbb{Z}_p$ if and only if

$5y^2+4$ is a square mod p if and only if $5y_0^2+4$ is a square mod p. So, if $5y_0^2+4$ is a not square mod p, then the square root of $5y^2+4$ is not in $\mathbb{Z}_p$ and $\mathbf{i}_+(y)=0$. Assume $5y_0^2+4$ is a square mod p. then the square root of $5y^2+4$ is in $\mathbb{Z}_p$ and we have $(\sqrt{5}y \pm \sqrt{5y^2+4})/2 \in \mathbb{Z}_p$ with $(\sqrt{5}y \pm \sqrt{5y^2+4})/2 \equiv (\sqrt{5}y_0 \pm \sqrt{5y_0^2+4})/2 \neq 0$ mod p. Thus, by Corollary 6.0.9, the square root of $(\sqrt{5}y \pm \sqrt{5y^2+4})/2$ is in $\mathbb{Z}_p$ if and only if $(\sqrt{5}y \pm \sqrt{5y^2+4})/2$ is a square mod p, which is the case if and only if $(\sqrt{5}y_0 \pm \sqrt{5y_0^2+4})/2$ is a square mod p. Thus, $\mathbf{i}_+(y)$ depends only on y_0. The case when $5y_0^2-4 \not\equiv 0 \mod p$ follows similarly. □

Furthermore, we have the following result.

Proposition 8.2.2.

1. *If* $5y_0^2+4 \not\equiv 0 \mod p$ *is not a square then* $\mathbf{i}_+(y)=0$. *If* $5y_0^2+4 \not\equiv 0 \mod p$ *is a square and* -1 *is a square, then*

$$\mathbf{i}_+(y) = \begin{cases} 2, & \text{if } (\sqrt{5}y+\sqrt{5y^2+4})/2 \text{ is a square} \\ 0, & \text{if } (\sqrt{5}y+\sqrt{5y^2+4})/2 \text{ is not a square.} \end{cases}$$

   If $5y_0^2+4 \not\equiv 0 \mod p$ *is a square and* -1 *is not a square, then* $\mathbf{i}_+(y)=1$.

2. *If* $5y_0^2-4 \neq 0$ *mod* p *is not a square then* $\mathbf{i}_-(y)=0$. *If* $5y_0^2-4 \not\equiv 0 \mod p$ *is a square, then*

$$\mathbf{i}_-(y) = \begin{cases} 0, & \text{if } (\sqrt{5}y+\sqrt{5y^2-4})/2 \text{ is a square} \\ 2, & \text{if } (\sqrt{5}y+\sqrt{5y^2-4})/2 \text{ is not a square.} \end{cases}$$

Proof.

1. It is clear that if $5y_0^2+4 \not\equiv 0 \mod p$ is not a square then $\mathbf{i}_+(y)=0$, since $\sqrt{5y^2+4} \notin \mathbb{Z}_p$. If $5y_0^2+4 \not\equiv 0 \mod p$ is a square then $\sqrt{5y^2+4} \in \mathbb{Z}_p$ and we must consider the product

$$\left(\frac{\sqrt{5}y+\sqrt{5y^2+4}}{2}\right)\left(\frac{\sqrt{5}y-\sqrt{5y^2+4}}{2}\right) = -1.$$

   Let

$$\alpha_+ = \left(\frac{\sqrt{5}y+\sqrt{5y^2+4}}{2}\right) \text{ and } \alpha_- = \left(\frac{\sqrt{5}y-\sqrt{5y^2+4}}{2}\right).$$

When -1 is a square, we have

$$\left(\frac{-1}{p}\right) = 1.$$

Thus, by the multiplicativity of the Legendre symbol,

$$\left(\frac{\alpha_+}{p}\right) = \left(\frac{\alpha_-}{p}\right).$$

Hence, either both α_+ and α_- are squares or neither is. That is,

$$\mathbf{i}_+(y) = \begin{cases} 2, & \text{if } (\sqrt{5}y + \sqrt{5y^2+4})/2 \text{ is a square} \\ 0, & \text{if } (\sqrt{5}y + \sqrt{5y^2+4})/2 \text{ is not a square.} \end{cases}$$

By a similar argument, when -1 is not a square, we have

$$\left(\frac{-1}{p}\right) = -1$$

and

$$\left(\frac{\alpha_+}{p}\right) \neq \left(\frac{\alpha_-}{p}\right).$$

Hence, $\mathbf{i}_+(y) = 1$.

2. The proof follows closely that of part 1. It is clear that if $5y_0^2 - 4 \not\equiv 0 \mod p$ is not a square then $\mathbf{i}_+(y) = 0$, since $\sqrt{5y^2-4} \notin \mathbb{Z}_p$. If $5y_0^2 - 4 \not\equiv 0 \mod p$ is a square then $\sqrt{5y^2-4} \in \mathbb{Z}_p$ and we must consider the product

$$\left(\frac{\sqrt{5}y + \sqrt{5y^2-4}}{2}\right)\left(\frac{\sqrt{5}y - \sqrt{5y^2-4}}{2}\right) = 1.$$

Let

$$\beta_+ = \left(\frac{\sqrt{5}y + \sqrt{5y^2-4}}{2}\right) \text{ and } \beta_- = \left(\frac{\sqrt{5}y - \sqrt{5y^2-4}}{2}\right).$$

Since 1 is always a square, we have

$$\left(\frac{1}{p}\right) = 1.$$

Thus, by the multiplicativity of the Legendre symbol,

$$\left(\frac{\beta_+}{p}\right) = \left(\frac{\beta_-}{p}\right).$$

Hence, either both β_+ and β_- are squares or neither is. That is,

$$\mathbf{i}_-(y) = \begin{cases} 0, & \text{if } (\sqrt{5}y + \sqrt{5y^2-4})/2 \text{ is a square} \\ 2, & \text{if } (\sqrt{5}y + \sqrt{5y^2-4})/2 \text{ is not a square.} \end{cases}$$

□

With the above proposition we may compute $\mathbf{i}(y)$ when $5y_0^2 \pm 4 \not\equiv 0 \mod p$. The situation is more complicated when $5y_0^2 \pm 4 \equiv 0 \mod p$.

8.2.2 Case I (b): $5y_0^2 \pm 4 \equiv 0 \mod p$

Proposition 8.2.3. *When $5y_0^2+4 \equiv 0 \mod p$, we can write $5y_0^2+4 = \lambda p^k$, for some $k \geq 1, \lambda \in \mathbf{U}$. Thus, $5y_0^2+4$ is not a square, and $\mathbf{i}_+(y) = 0$, if k is odd. If k is even, $5y^2+4$ is a square if and only if λ_0 is a square mod p.*

Supposing k is even, since the squaring function is two-to-one mod p on $\mathbf{U}$ except at 0, there are $(p-1)/2$ values of λ_0 for which it is a square mod p and $(p-1)/2$ values for which it is not. When λ_0 is not a square, we have $\mathbf{i}_+(y) = 0$, and when λ_0 is a square, we have

$$\mathbf{i}_+(y) = \begin{cases} 2, & \text{if } (\sqrt{5}y + \sqrt{5y^2+4})/2 \text{ is a square} \\ 0, & \text{if } (\sqrt{5}y + \sqrt{5y^2+4})/2 \text{ is not a square,} \end{cases}$$

for the same reasons as in Proposition 8.2.2. Unlike in Proposition 8.2.2, however, -1 is always a square, since $5y_0^2 + 4 \equiv 0 \mod p$, that is, since $y_0^2 \equiv -\frac{4}{5} \mod p$ has a solution only if -1 is a square because 4 and 5 are both squares.

Similarly, we have the following:

Proposition 8.2.4. *When $5y_0^2-4 \equiv 0 \mod p$, we can write $5y_0^2-4 = \lambda p^k$, for some $k \geq 1, \lambda \in \mathbf{U}$. Thus, $5y_0^2-4$ is not a square, and $\mathbf{i}_-(y) = 0$, if k is odd. If k is even, $5y^2-4$ is a square if and only if λ_0 is a square mod p.*

Thus, supposing k is even, when λ_0 is not a square, we have $\mathbf{i}_-(y) = 0$, and when λ_0 is a square, we have

$$\mathbf{i}_-(y) = \begin{cases} 0, & \text{if } (\sqrt{5}y + \sqrt{5y^2-4})/2 \text{ is a square} \\ 2, & \text{if } (\sqrt{5}y + \sqrt{5y^2-4})/2 \text{ is not a square,} \end{cases}$$

for the same reasons as in Proposition 8.2.2.

Additionally, we have the following result, which simplifies computation.

Theorem 8.2.5.

1. *Let* $5y_0^2 + 4 \equiv 0 \mod p$. *If* $5y^2 + 4$ *is a square and* -1 *is a fourth power, then* $\mathbf{i}_+(y) = 2$. *Otherwise,* $\mathbf{i}_+(y) = 0$.

2. *Let* $5y_0^2 - 4 \equiv 0 \mod p$. *If* $5y^2 - 4$ *is a square and* $\sqrt{5}y_0/2 (= \pm 1)$ *is not a square* $\mod p$, *then* $\mathbf{i}_-(y) = 2$. *Otherwise,* $\mathbf{i}_-(y) = 0$.

Proof. 1. If $\mathbf{i}_+(y) \neq 0$, then $5y^2 + 4$ must be a square, so that $\sqrt{5y^2+4} \in \mathbb{Z}_p$. Thus, we can write $5y^2 + 4 = \lambda^2 p^{2k}$, for some $k \geq 1, \lambda \in \mathbf{U}$. Rearranging, we get

$$\begin{aligned} 5y^2 &= \lambda^2 p^{2k} - 4 \\ \frac{5y^2}{4} &= \frac{\lambda^2 p^{2k}}{4} - 1 \\ \frac{\sqrt{5}y}{2} &= \pm \left(\frac{\lambda^2 p^{2k}}{4} - 1 \right)^{1/2} \\ \frac{\sqrt{5}y}{2} &= \pm (-1)^{1/2} \left(1 - \frac{\lambda^2 p^{2k}}{4} \right)^{1/2}. \end{aligned}$$

Since $k \geq 1$, we know that $1 - \frac{\lambda^2 p^{2k}}{4} \equiv 1 \mod p$ and so, $(1 - \frac{\lambda^2 p^{2k}}{4})^{1/2} \equiv \pm 1 \mod p$. Thus,

$$\begin{aligned} \frac{\sqrt{5}y + \sqrt{5y^2+4}}{2} &= \pm (-1)^{1/2} \left(1 - \frac{\lambda^2 p^{2k}}{4} \right)^{1/2} + \frac{\lambda p^k}{2} \\ &\equiv \pm (-1)^{1/2} \mod p. \end{aligned}$$

Since $(-1)^{1/2} \not\equiv 0 \mod p$, it has a square root in $\mathbb{Z}_p$ if and only if it has one mod p, by Corollary 6.0.9. For the same reason, $(\sqrt{5}y + \sqrt{5y^2+4})/2$ has a square root in $\mathbb{Z}_p$ if and only if it has one mod p. Hence, for $(\sqrt{5}y + \sqrt{5y^2+4})/2$ to be a square it is necessary and sufficient that $(-1)^{1/2}$ exist and be a square mod p, that is, that -1 be a fourth power mod p. Moreover, it is obvious that if $(\sqrt{5}y + \sqrt{5y^2+4})/2$ is a square, then so is $(\sqrt{5}y - \sqrt{5y^2+4})/2$. Therefore, $\mathbf{i}_+(y) = 2$ if and only if $5y^2 + 4$ is a square and -1 is a fourth power.

2. Similarly, if $\mathbf{i}_-(y) \neq 0$, then $5y^2 - 4$ must be a square, so that $\sqrt{5y^2-4} \in \mathbb{Z}_p$. Thus, we can write $5y^2 - 4 = \lambda^2 p^{2k}$, for some $k \geq 1, \lambda \in \mathbf{U}$. Rearranging, we

get

$$\begin{aligned} 5y^2 &= \lambda^2 p^{2k} + 4 \\ \frac{5y^2}{4} &= \frac{\lambda^2 p^{2k}}{4} + 1 \\ \frac{\sqrt{5}y}{2} &= \pm\left(1 + \frac{\lambda^2 p^{2k}}{4}\right)^{1/2}. \end{aligned}$$

Since $k \geq 1$, we know that $1 + \frac{\lambda^2 p^{2k}}{4} \equiv 1 \mod p$ and so, $(1 + \frac{\lambda^2 p^{2k}}{4})^{1/2} \equiv \pm 1 \mod p$. Thus,

$$\begin{aligned} \frac{\sqrt{5}y + \sqrt{5y^2 - 4}}{2} &= \pm\left(1 + \frac{\lambda^2 p^{2k}}{4}\right)^{1/2} + \frac{\lambda p^k}{2} \\ &\equiv \pm 1 \mod p. \end{aligned}$$

Hence, for $(\sqrt{5}y + \sqrt{5y^2 - 4})/2$ to be a square it is necessary and sufficient that $\sqrt{5}y_0/2 (= \pm 1)$ be a square $\mod p$. Moreover, it is obvious that if $(\sqrt{5}y + \sqrt{5y^2 - 4})/2$ is a square, then so is $(\sqrt{5}y - \sqrt{5y^2 - 4})/2$. Therefore, $\mathbf{i}_-(y) = 2$ if and only if $5y^2 - 4$ is a square and $\sqrt{5}y_0/2 (= \pm 1)$ is not a square $\mod p$.

□

Example Let $p = 11$. Then $p \equiv \pm 1 \mod 5$, so $\sqrt{5} \in \mathbb{Z}_{11}$. As seen in the table below, $\sqrt{5} \equiv 4$ or $7 \mod 11$. When $\sqrt{5} \equiv 4 \mod 11$, we have $\beta = \frac{5}{2} \equiv 8 \mod 11$ and β is a primitive root mod p with $\beta^{p-1} \not\equiv 1 \mod p^2$. Hence, we are in the situation described above.

Consider the following table where numbers are written mod 11 and boxed numbers are non-zero squares. Note that $-1 \equiv 10 \mod 11$ is not a square in $\mathbb{Z}_{11}$.

y_0	0	1	2	3	4	5	6	7	8	9	10
y_0^2	0	1	4	9	5	3	3	5	9	4	1
$5y_0^2$	0	5	9	1	3	4	4	3	1	9	5
$5y_0^2 + 4$	$\boxed{4}$	$\boxed{9}$	2	$\boxed{5}$	7	8	8	7	$\boxed{5}$	2	$\boxed{9}$
$5y_0^2 - 4$	7	$\boxed{1}$	$\boxed{5}$	8	10	0	0	10	8	$\boxed{5}$	$\boxed{1}$

(a) If $y_0 = 2, 4, 5, 6, 7, 9$, then $\mathbf{i}_+(y) = 0$, since $5y_0^2 + 4 \not\equiv 0 \mod 11$ is not a square. When $y_0 = 0, 1, 3, 8, 10$, we have $\mathbf{i}_+(y) = 1$, since $5y_0^2 + 4 \not\equiv 0 \mod 11$ is a square and -1 is not a square.

(b) If $y_0 = 0, 3, 4, 7, 8$, then $\mathbf{i}_-(y) = 0$, since $5y_0^2 - 4 \not\equiv 0 \mod 11$ is not a square. When $5y_0^2 - 4 \not\equiv 0 \mod 11$ is a square, we have $\mathbf{i}_-(y) = 2$ for $y_0 = 1, 2$, since $(\sqrt{5}y + \sqrt{5y^2 - 4})/2$ is not a square, and $\mathbf{i}_-(y) = 0$ fo $y_0 = 9, 10$, since $(\sqrt{5}y + \sqrt{5y^2 - 4})/2$ is a square.

To evaluate $\mathbf{i}_-(y)$ for $y_0 = 5$ or 6 we must consider all the cases when $5y^2 - 4 = \lambda^2 p^{2k}$, where $\lambda \in \mathbf{U}$ and $k \geq 1$, since if y does not satisfy this equation, then $\mathbf{i}_-(y) = 0$. When $y_0 = 5$ and y satisfy such an equation, $\mathbf{i}_-(y) = 2$, since $\sqrt{5} \cdot 5/2 \equiv 10 \mod 11$ is not a square mod 11. On the other hand, when $y_0 = 6$, then $\mathbf{i}_-(y) = 0$, since $\sqrt{5} \cdot 6/2 \equiv 12 \mod 11 \equiv 1 \mod 11$ is a square mod 11.

We have in total:

y_0	0	1	2	3	4	5	6	7	8	9	10
$\mathbf{i}_+(y)$	1	1	0	1	0	0	0	0	1	0	1
$\mathbf{i}_-(y)$	0	2	2	0	0	2	0	0	0	0	0
$\mathbf{i}(y)$	1	3	2	1	0	2	0	0	1	0	1

8.3 Case II: $p \equiv \pm 2 \mod 5$

When $p \equiv \pm 2 \mod 5$, we have $\sqrt{5} \notin \mathbb{Z}_p$. In this case, it is possible to give a formula for $\mathbf{i}(y)$, which makes calculations somewhat simpler.

Note that $\langle \beta \rangle = \mathbf{U}^0(\sqrt{5})/\mathbf{U}_1$, since β is a primitive root mod p. So, $z \in \mathbf{U}^0(\sqrt{5})$ can be written $z \equiv \beta^k \mod p$, for some $k \in \mathbb{Z}$. Now, for $z, w \in \mathbf{U}^0(\sqrt{5})$, if $z \equiv w \mod p$, then $N(z) \equiv N(w) \mod p$. Furthermore, $N(\beta) = \frac{1}{4} - 5 \cdot \frac{1}{4} = -1$. Thus, since the norm is multiplicative, we have

$$N(z) = N(\beta^k) = \begin{cases} 1, & \text{if } k \text{ is even} \\ -1, & \text{if } k \text{ is odd.} \end{cases}$$

That is,

$$N(z) = \begin{cases} 1, & \text{if } z \text{ is a square in } \mathbf{U}^0(\sqrt{5})/\mathbf{U}_1 \\ -1, & \text{otherwise.} \end{cases}$$

Hence, if $N(z) = 1$, then $x^2 = z$ is solvable mod p in $\mathbf{U}^0(\sqrt{5})$. Since the solution is in $\mathbf{U}^0(\sqrt{5})/\mathbf{U}_1$, it is a unit. So, the derivative of x^2 at this point is not 0 mod p.

Then, by Hensel's Lemma, $x^2 = z$ is solvable in $\mathbf{U}^0(\sqrt{5})$. That is,

$$N(z) = \begin{cases} 1, & \text{if } z \text{ is a square in } \mathbf{U}^0(\sqrt{5}) \\ -1, & \text{otherwise.} \end{cases}$$

When $5y^2+4$ is a square, $N((\sqrt{5}y \pm \sqrt{5y^2+4})/2) = \frac{5y^2+4}{4} - 5 \cdot \frac{y^2}{4} = 1$. Thus, $(\sqrt{5}y \pm \sqrt{5y^2+4})/2$ are squares in $\mathbf{U}^0(\sqrt{5})$. Similarly, when $5y^2-4$ is a square, $N((\sqrt{5}y \pm \sqrt{5y^2-4})/2) = \frac{5y^2-4}{4} - 5 \cdot \frac{y^2}{4} = -1$. Thus, $(\sqrt{5}y \pm \sqrt{5y^2-4})/2$ are not squares in $\mathbf{U}^0(\sqrt{5})$.

Hence, we have $\mathbf{i}_+(y) = N(5y^2+4)+1$ (i.e., 2 when $5y^2+4$ is a square and 0 otherwise) and $\mathbf{i}_-(y) = N(5y^2-4)+1$, by the same reasoning.

Theorem 8.3.1. *When* $5y_0^2+4 \not\equiv 0 \mod p$, $\mathbf{i}_+(y) = \mathbf{i}_+(y_0)$ *depends only on* y_0 *and when* $5y_0^2-4 \not\equiv 0 \mod p$, $\mathbf{i}_-(y) = \mathbf{i}_-(y_0)$ *depends only on* y_0. *If* $5y^2+4 \equiv 0 \mod p$, *then*

$$\mathbf{i}_+(y) = \begin{cases} 2, & \text{if } 5y^2+4 = \lambda^2 p^{2k} \text{ for some } k \geq 1, \lambda \in \mathbf{U} \\ 0, & \text{otherwise.} \end{cases}$$

For all cases,

$$\mathbf{i}(y) = N(5y^2+4) + N(5y^2-4) + 2.$$

Proof. It was shown above that $\mathbf{i}_+(y) = N(5y^2+4)+1$ and $\mathbf{i}_-(y) = N(5y^2-4)+1$. Thus, $\mathbf{i}(y) = \mathbf{i}_+(y) + \mathbf{i}_-(y) = N(5y^2+4) + N(5y^2-4) + 2$.

By Hensel's Lemma, it is easy to see that $\mathbf{i}_+(y)$ and $\mathbf{i}_-(y)$ depend only on y_0 when, respectively, $5y_0^2+4 \not\equiv 0 \mod p$, $5y_0^2-4 \not\equiv 0 \mod p$. Furthermore, when $5y_0^2+4 \equiv 0 \mod p$, $5y^2+4$ is a square if and only if $5y^2+4 = \lambda^2 p^{2k}$ for some $k \geq 1, \lambda \in \mathbf{U}$. Thus, since $\mathbf{i}_+(y) = N(5y^2+4)+1$, $\mathbf{i}_+(y)$ is 2 when $5y^2+4$ is a square and 0 otherwise, i.e., $\mathbf{i}_+(y)$ is 2 when $5y^2+4 = \lambda^2 p^{2k}$ for some $k \geq 1, \lambda \in \mathbf{U}$ and 0 otherwise. □

If $5y^2+4 \equiv 0 \mod p$, then $y^2 \equiv -\frac{4}{5} \mod p$. Since 4 is a square mod p and 5 is not, this equation has a solution if and only if -1 is also not a square mod p, by the multiplicative property of the Legendre symbol. Thus, this equation has a solution if and only if $p \equiv 3 \mod 4$, by the law of quadratic reciprocity. By the same argument, the equation $5y^2-4 \equiv 0 \mod p$ never has a solution.

Thus, if $p \equiv 1 \mod 4$, then $5y^2 \pm 4 \equiv 0 \mod p$ has no solutions and $\mathbf{i}(y)$ is determined by $y_0 \equiv y \mod p$. If $p \equiv 3 \mod 4$, then $5y^2+4 \equiv 0 \mod p$ has 2

solutions and $5y^2 - 4 \equiv 0 \mod p$ has no solutions. So, $\mathbf{i}_-(y)$ is determined by $y_0 \equiv y \mod p$, but for $\mathbf{i}_+(y)$ there are 2 residue classes for which $5y^2 + 4 \equiv 0 \mod p$ and so $5y^2 + 4 = \lambda p^k$, for some $k \geq 1, \lambda \in \mathbf{U}$. Thus, $\mathbf{i}_+(y)$ is determined by λ_0 and the parity of k.

Example Let $p = 13$. Then $p \equiv \pm 2 \mod 5$, so $\sqrt{5} \notin \mathbb{Z}_{13}$. We have $\beta = \frac{1+\sqrt{5}}{2} \equiv 7 + 7\sqrt{5} \mod 13$ and β is a primitive root mod p with $\beta^{2(p+1)} \not\equiv 1 \mod p^2$. Also, $5y_0^2 \pm 4$ is never $0 \mod 13$. Hence, it is straightforward to apply Theorem 8.3.1.

Consider the following table where numbers are written mod 13 and boxed numbers are non-zero squares.

y_0	0	1	2	3	4	5	6	7	8	9	10	11	12
y_0^2	0	1	4	9	3	12	10	10	12	3	9	4	1
$5y_0^2$	0	5	7	6	2	8	11	11	8	2	6	7	5
$5y_0^2 + 4$	$\boxed{4}$	$\boxed{9}$	11	$\boxed{10}$	6	$\boxed{12}$	2	2	$\boxed{12}$	6	$\boxed{10}$	11	$\boxed{9}$
$5y_0^2 - 4$	$\boxed{9}$	$\boxed{1}$	$\boxed{3}$	2	11	$\boxed{4}$	7	7	$\boxed{4}$	11	2	$\boxed{3}$	$\boxed{1}$

It is now very easy to find the values of $\mathbf{i}(y)$ using the formula from Theorem 8.3.1. We have in total:

y_0	0	1	2	3	4	5	6	7	8	9	10	11	12
$\mathbf{i}(y)$	4	4	2	2	0	4	0	0	4	0	2	2	4

Example Let $p = 7$. Then $p \equiv \pm 2 \mod 5$, so $\sqrt{5} \notin \mathbb{Z}_{13}$. We have $\beta = \frac{1+\sqrt{5}}{2} \equiv 4 + 4\sqrt{5} \mod 7$ and β is a primitive root mod p with $\beta^{2(p+1)} \not\equiv 1 \mod p^2$. Hence, we are in the situation described above. Note that $5y_0^2 + 4 \equiv 0 \mod 7$ for $y_0 = 3$ and 4. Thus, in these cases, we must consider all the cases when $5y^2 + 4 = \lambda^2 p^{2k}$, where $\lambda \in \mathbf{U}$ and $k \geq 1$.

Consider the following table where numbers are written mod 7 and boxed numbers are non-zero squares.

y_0	0	1	2	3	4	5	6
y_0^2	0	1	4	2	2	4	1
$5y_0^2$	0	5	6	3	3	6	5
$5y_0^2 + 4$	$\boxed{4}$	$\boxed{2}$	3	0	0	3	$\boxed{2}$
$5y_0^2 - 4$	3	$\boxed{1}$	$\boxed{2}$	6	6	$\boxed{2}$	$\boxed{1}$

It is now very easy to find the values of $\mathbf{i}(y)$ using the formula from Theorem 8.3.1. We have in total:

y_0	0	1	2	3	4	5	6
$\mathbf{i}(y)$	2	4	2	2	2	2	4

Chapter 9

Tree Diagrams and Main Result

9.1 Tree Diagrams

Once we have calculated $\mathbf{i}(y)$, for all $y \in \mathbb{Z}_p$, we can represent the data in a tree diagram similar to the one we used for the residue classes modulo 2 represented by the Fibonacci numbers. It will have the same shape as the one in Figure 9.1.

In this tree, a node aligned with p^k on the left of the tree corresponds to the coefficient y_{k-1} of p^{k-1} in the p-adic expansion, $\sum_{i=0}^{\infty} y_i \cdot p^i$, of a Fibonacci number. Note that we have written c_i^j for $(y_i)_{a+1,j}$ and d_i^j for $(y_i)_{a+b,j}$, where the j's are indices and not exponents, in an effort to conserve space. Observe that, although $c_i^j \neq c_i^l$ for any $j \neq l$ with $j, l \in \{1, .., \frac{p-1}{2} + 1\}$, and $d_i^m \neq d_i^n$ for any $m \neq n$ with $m, n \in \{1, .., \frac{p-1}{2} + 1\}$, we may still have $c_i^s = d_i^t$ for some $s, t \in \{1, .., \frac{p-1}{2} + 1\}$.

A node is drawn if there is a Fibonacci number with that p-adic expansion and omitted if not. For instance there is a Fibonacci number whose p-adic expansion starts $(y_0)_{a+1} + c_1^1 \cdot p + c_2^{\frac{p-1}{2}+1} \cdot p^2 + c_3^1 \cdot p^3 + c_4^{\frac{p-1}{2}+1} \cdot p^4 + c_5^1 \cdot p^5 + \ldots$, but there is no Fibonacci number whose p-adic expansion starts $(y_0)_{a+1} + c_1^2 \cdot p + \ldots$, where $c_1^2 \in \{0, \ldots, p-1\}$ and $c_1^2 \neq c_1^1$. A triangle is used to depict the fact that there is a Fibonacci number with p-adic expansion corresponding to each of the branches below the node to which it is attached. For example, there is a Fibonacci number with p-adic expansion $(y_0)_1 + \sum_{i=1}^{\infty} y_i \cdot p^i$ with $y_i \in \{0, \ldots, p-1\}, \forall i \geq 1$.

To draw such a tree using the calculations from Chapter 8, first add a branch for each of the y_0's with $\mathbf{i}(y) \neq 0$. If $\mathbf{i}(y) \neq 0$ and both $5y_0^2 + 4 \not\equiv 0 \mod p$ and $5y_0^2 - 4 \not\equiv 0 \mod p$, draw a triangle after the y_0, since $\mathbf{i}(y)$ depends only on y_0. If $\mathbf{i}(y) \neq 0$ and either $5y_0^2 + 4 \equiv 0 \mod p$ or $5y_0^2 + 4 \equiv 0 \mod p$, we must consider when $5y^2 + 4 = \lambda^2 p^{2k}$ or $5y^2 - 4 = \lambda^2 p^{2k}$, respectively, where $\lambda \in \mathbf{U}$ and $k \geq 1$. Thus, every two levels, i.e., for every even power of p, we have $\frac{p-1}{2}$ branches stabilize in triangles, since there are $\frac{p-1}{2}$ values of λ_0 for which it is a square mod p. As we will only be concerned with the shape of the branches, it is enough to draw this repeating pattern,

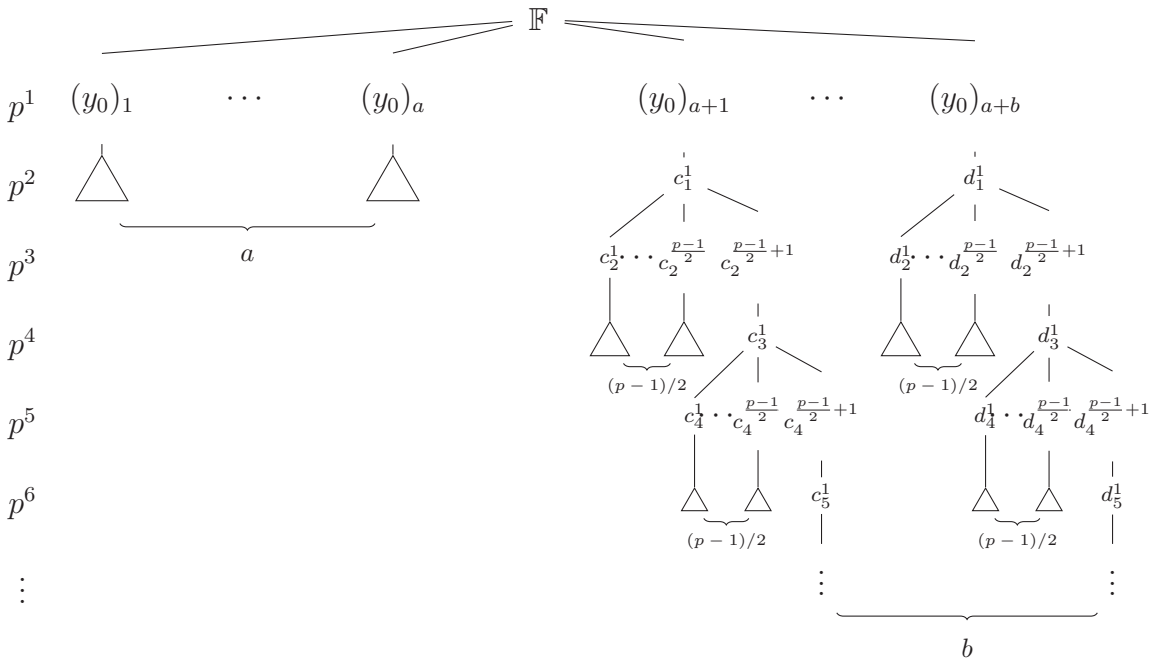

Figure 9.1: Generalized tree diagram.

although the node values can easily be calculated using Hensel's Lemma.

Example For $p = 11$, recall that

y_0	0	1	2	3	4	5	6	7	8	9	10
$\mathbf{i}_+(y)$	1	1	0	1	0	0	0	0	1	0	1
$\mathbf{i}_-(y)$	0	2	2	0	0	2	0	0	0	0	0
$\mathbf{i}(y)$	1	3	2	1	0	2	0	0	1	0	1

The associated tree diagram is shown in Figure 9.2.

Example For $p = 13$, recall that

y_0	0	1	2	3	4	5	6	7	8	9	10	11	12
$\mathbf{i}(y)$	4	4	2	2	0	4	0	0	4	0	2	2	4

The associated tree diagram is shown in Figure 9.3.

Example For $p = 7$, recall that

y_0	0	1	2	3	4	5	6
$\mathbf{i}(y)$	2	4	2	2	2	2	4

The associated tree diagram is shown in Figure 9.4.

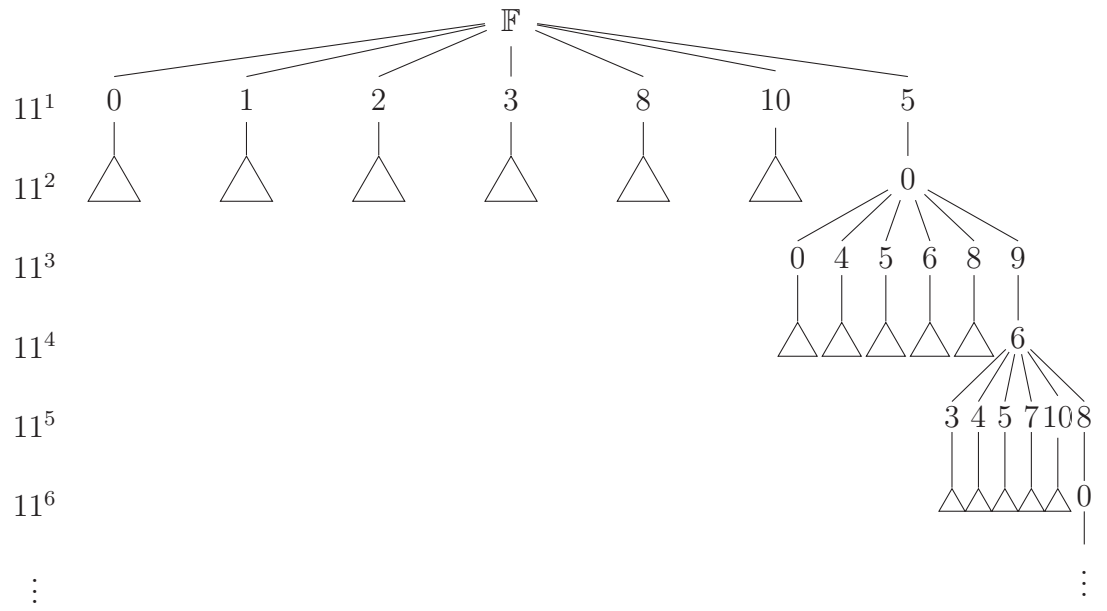

Figure 9.2: Tree diagram for $p = 11$.

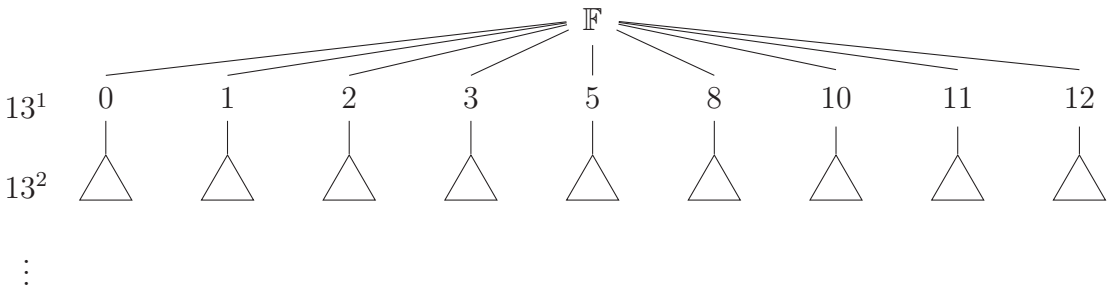

Figure 9.3: Tree diagram for $p = 13$.

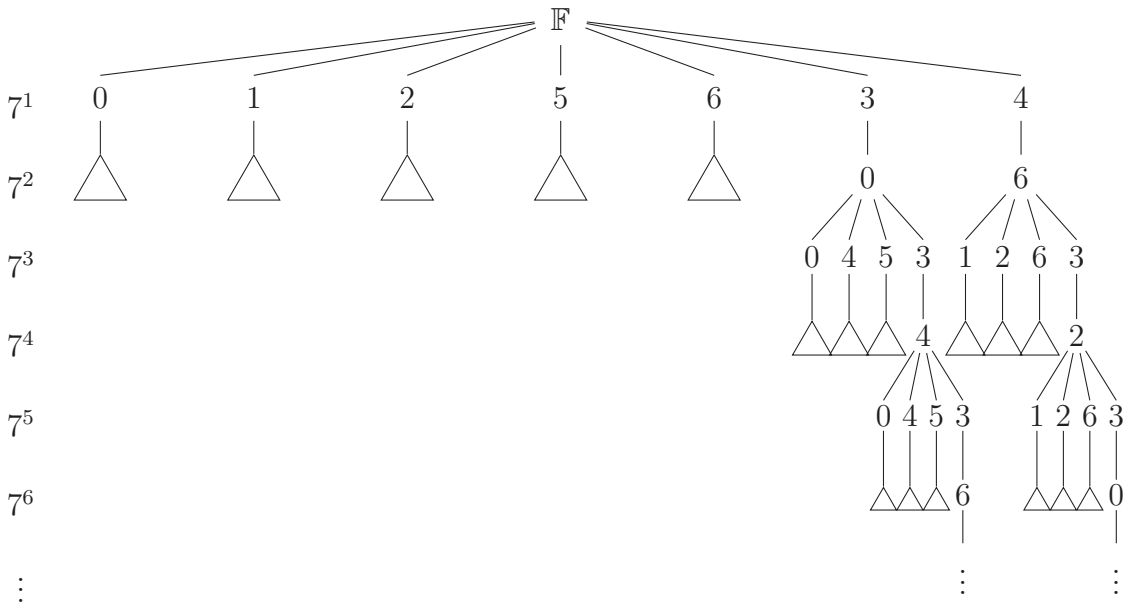

Figure 9.4: Tree diagram for $p = 7$.

9.2 Main Result

Using the results in Chapter 8, it is possible to determine which residue classes are represented by the Fibonacci numbers modulo various prime powers when the prime is such that β satisfies Condition 1.0.1. In such cases, we can calculate the p-sequence of the Fibonacci numbers.

Before stating the main result, we will need a bit more notation.

Notation 9.2.1.

1. *Let Sq be the set of squares in $\mathbf{U}/\mathbf{U}_1$.*
2. *Let $\mathbb{F}_1 = \{y \in \mathbb{F} | 5y^2 + 4 \not\equiv 0 \mod p$ and $5y^2 - 4 \not\equiv 0 \mod p\}$ and $\mathbb{F}_2 = \{y \in \mathbb{F} | 5y^2 + 4 \equiv 0 \mod p$ or $5y^2 - 4 \equiv 0 \mod p\}$.*

We will also need the following proposition.

Proposition 9.2.2. *We have the following equality:*

$$\{\lambda^2 p^{2k} | \lambda \in \mathbf{U}, k \geq 1\} = \bigcup_{k \geq 1} \left(\bigcup_{s \in Sq} (sp^{2k} + p^{2k+1}\mathbb{Z}_p) \right).$$

Proof. It is clear that

$$\{\lambda^2 p^{2k} | \lambda \in \mathbf{U}, k \geq 1\} \subseteq \bigcup_{k \geq 1} \left(\bigcup_{s \in Sq} (sp^{2k} + p^{2k+1}\mathbb{Z}_p) \right).$$

The converse is a consequence of Hensel's Lemma. Let

$$x \in \bigcup_{k \geq 1} \left(\bigcup_{s \in Sq} (sp^{2k} + p^{2k+1}\mathbb{Z}_p) \right).$$

So, $x = sp^{2k} + p^{2k+1}z$ for some $k \geq 1, s \in Sq$, and $z \in \mathbb{Z}_p$. Note that $s + pz \in \mathbb{Z}_p$ with $s + pz \not\equiv 0 \mod p$ and $(\frac{s}{p}) = 1$, since $s \in Sq$. Thus, by Corollary 6.0.9, the square root of $s + pz$, say λ, is in $\mathbb{Z}_p$. In fact, $\lambda \in \mathbf{U}$, since $p \nmid \lambda$ because $s \in Sq$. Hence, $\lambda^2 = s + pz$ and $\lambda^2 p^{2k} = sp^{2k} + p^{2k+1}z = x$ for $\lambda \in \mathbf{U}, k \geq 1$. Therefore,

$$\bigcup_{k \geq 1} \left(\bigcup_{s \in Sq} (sp^{2k} + p^{2k+1}\mathbb{Z}_p) \right) \subseteq \{\lambda^2 p^{2k} | \lambda \in \mathbf{U}, k \geq 1\}.$$

□

With this information, we can now prove our main result.

Theorem 9.2.3. *Let $f : \mathbf{U} \to \mathbb{Z}_p$ or $f : \mathbf{U}^0(\sqrt{5}) \to \mathbb{Z}_p$ be given by*

$$f(z) = \frac{1}{\sqrt{5}} \left(z - \frac{N(z)}{z} \right),$$

where $N(z) = 1$ or -1 according to whether z is a square or not (in $\mathbf{U}$ or $\mathbf{U}^0(\sqrt{5})$).

For a fixed odd prime integer p for which β satisfies Condition 1.0.1, we have

$$\alpha_{\mathbb{F},p} = (\alpha_{\mathbb{Z},p} + (k))^{\wedge a} \wedge (\alpha_{\gamma,p})^{\wedge b},$$

where γ is a set whose p-sequence, $\alpha_{\gamma,p}$, is determined completely by the equation

$$\alpha_{\gamma,p} = ((\alpha_{\mathbb{Z},p} + (k))^{\wedge \frac{p-1}{2}} \wedge \alpha_{\gamma,p}) + (2k),$$

$$a = \text{number of images of } \langle \beta_0 \rangle \text{ in } \mathbb{Z}/(p) \text{ under } f \text{ with } f' \text{ not equal to } 0,$$

and

$$b = \text{number of images of } \langle \beta_0 \rangle \text{ in } \mathbb{Z}/(p) \text{ under } f \text{ with } f' \text{ equal to } 0,$$

Furthermore, b is determined by the number of solutions of $1 \mp \frac{1}{z^2} \equiv 0 \mod p$. Thus, $0 \leq b \leq 4$.

Proof. Let p be a fixed odd prime integer for which β satisfies Condition 1.0.1. Using Proposition 8.2.2, Theorem 8.2.5, and Theorem 8.3.1, we are able to calculate the number of solutions of $f(z) = y$, that is, $\mathbf{i}(y), \forall y \in \mathbb{Z}_p$. With this information, we can create a tree diagram, as in the previous section.

Since a node is drawn if there is a Fibonacci number with that p-adic expansion and omitted if not, there is a branch for each of the y_0's with $\mathbf{i}(y) \neq 0$. Thus, the total number of branches is equal to the total number of images of $\langle \beta_0 \rangle$ in $\mathbb{Z}/(p)$ under f, i.e., $a + b$.

It is clear that

$$f'(z) = \frac{1}{\sqrt{5}} \left(1 \mp \frac{1}{z^2} \right).$$

Thus,

$$\begin{aligned} f'(z) = 0 &\iff 1 \mp \frac{1}{z^2} = 0 \\ &\iff 1 = \pm \frac{1}{z^2} \\ &\iff z^2 = \pm 1 \\ &\iff z = \pm 1, \pm\sqrt{-1}. \end{aligned}$$

Since b is the number of images of $\langle \beta_0 \rangle$ in $\mathbb{Z}/(p)$ under f with f' equal to 0, b is determined by the number of solutions of $1 \mp \frac{1}{z^2} \equiv 0 \mod p$. Thus, $0 \leq b \leq 4$.

Clearly, $\mathbb{F} = \mathbb{F}_1 \cup \mathbb{F}_2$ and $v_p(u_1 - u_2) = 0, \forall u_1 \in \mathbb{F}_1, u_2 \in \mathbb{F}_2$. Thus, by Lemma 3.3.3, the p-sequence of $\mathbb{F}$ is

$$\alpha_{\mathbb{F},p} = \alpha_{\mathbb{F}_1,p} \wedge \alpha_{\mathbb{F}_2,p}.$$

To determine $\alpha_{\mathbb{F},p}$, we will use the information from the tree diagram to find $S \subseteq \mathbb{Z}$ with $\mathbb{F}_1 \subseteq S$ and $\mathbb{F}_1/(p^k) = S/(p^k), \forall k \geq 0$, and to find $T \subseteq \mathbb{Z}$ with $\mathbb{F}_2 \subseteq T$ and $\mathbb{F}_2/(p^k) = T/(p^k), \forall k \geq 0$, so that we can apply Lemma 2.2.3.

Consider $\mathbb{F}_1/(p)$. Any $y_0 \in \mathbb{F}_1/(p)$ will have $5y_0^2 + 4 \not\equiv 0 \mod p$ and $5y_0^2 - 4 \not\equiv 0 \mod p$. In this case, $\mathbf{i}(y) = \mathbf{i}(y_0)$ depends only on y_0. Thus, the y_0's in $\mathbb{F}_1/(p)$ with $\mathbf{i}(y) \neq 0$ start the branches that stabilize. Since $5y_0^2 + 4 \not\equiv 0 \mod p$ and $5y_0^2 - 4 \not\equiv 0 \mod p$ if and only if f' is not equal to 0, the number of such y_0's is a. The branches that stabilize represent sets of the form $y_0 + p\mathbb{Z}$, since they include all p-adic numbers with initial coefficient y_0. Thus, their p-sequences are easily calculated, using Lemma 3.3.1, to be $\alpha_{\mathbb{Z},p} + (k)$. There are a such branches and, for any two of them, say C and D,

$v_p(c-d)=0, \forall c \in C, d \in D$. Thus, Lemma 3.3.3 applies to all of them and we get

$$\alpha_{\mathbb{F}_1,p} = (\alpha_{\mathbb{Z},p} + (k))^{\wedge a}.$$

Now, consider $\mathbb{F}_2/(p)$. Any $y_0 \in \mathbb{F}_2/(p)$ will have $5y_0^2+4 \equiv 0 \mod p$ or $5y_0^2-4 \equiv 0 \mod p$. In this case, as described in Theorem 8.2.5 and Theorem 8.3.1, to determine $\mathbf{i}(y)$ we must consider all of the instances when $5y^2 \pm 4 = \lambda^2 p^{2k}$, where $\lambda \in \mathbf{U}$ and $k \geq 1$. Thus, the y_0's in $\mathbb{F}_2/(p)$ with $\mathbf{i}(y) \neq 0$ start the branches that repeat. Since $5y_0^2 + 4 \equiv 0 \mod p$ or $5y_0^2 - 4 \equiv 0 \mod p$ if and only if f' is equal to 0, the number of such y_0's is b. Note that there are at most four different y_0's in $\mathbb{F}_2/(p)$, since $\mathbb{F}_2/(p)$ contains at most four residue classes depending on p, namely, $\pm\frac{2}{\sqrt{5}}, \pm\frac{2\sqrt{-1}}{\sqrt{5}} \mod p$, which again shows us that $0 \leq b \leq 4$.

To see the form of the sets represented by the branches that repeat, consider the class of $\frac{2}{\sqrt{5}} \mod p$, that is, the positive solutions of $5y^2 - 4 \equiv 0 \mod p$. The other three classes are similar. Suppose $\mathbb{F}_2/(p)$ contains the residue class $\frac{2}{\sqrt{5}} \mod p$. As mentioned above, when $5y_0^2 - 4 \equiv 0 \mod p$, we must consider all of the cases when $5y^2 - 4 = \lambda^2 p^{2k}$, where $\lambda \in \mathbf{U}$ and $k \geq 1$. If $5y^2 = 4 + \lambda^2 p^{2k}$ for $\lambda \in \mathbf{U}$ and $k \geq 1$, then we have $5y^2 \in \mathbb{Z}_p$ with $5y^2 \not\equiv 0 \mod p$ and $(\frac{5y^2}{p}) = 1$, so the square root of $5y^2$ is in $\mathbb{Z}_p$, by Corollary 6.0.9. Moreover, it must be of the form $2 + \mu^2 p^{2k}$ for $\mu \in \mathbf{U}$ with $\mu \equiv \pm\frac{\lambda}{2} \mod p$, since $5y^2 = 4 + \lambda^2 p^{2k}$. So, $5y^2 = (2 + \mu^2 p^{2k})^2$ and, thus, $y = \pm\frac{1}{\sqrt{5}}(2 + \mu^2 p^{2k})$. Since we are considering only the class of $\frac{2}{\sqrt{5}} \mod p$, we have $y = \frac{1}{\sqrt{5}}(2 + \mu^2 p^{2k})$. All elements of this form are in the image of f and we denote the set of all such y, for $\mu \in \mathbf{U}$ and $k \geq 1$, by γ. By Condition 1.0.1, the group generated by β is p-adically dense in $\mathbf{U}$ or $\mathbf{U}^0(\sqrt{5})$, and f is p-adically continuous; hence, the image of the subgroup generated by β is p-adically dense in γ. The set γ can be expressed as a union in the following way.

$$\begin{aligned}
\gamma &= \frac{1}{\sqrt{5}}(2 + \{\mu^2 p^{2k} | \mu \in \mathbf{U}, k \geq 1\}) \\
&= \frac{2}{\sqrt{5}} + \frac{1}{\sqrt{5}} \left(\bigcup_{k \geq 1} \left(\bigcup_{s \in Sq} sp^{2k} + p^{2k+1}\mathbb{Z}_p \right) \right), \qquad \text{by Proposition 9.2.2.}
\end{aligned}$$

Rearranging we get

$$\sqrt{5}\gamma - 2 = \bigcup_{k\geq 1}\left(\bigcup_{s\in Sq} sp^{2k} + p^{2k+1}\mathbb{Z}_p\right),$$
$$p^2(\sqrt{5}\gamma - 2) = \bigcup_{k\geq 2}\left(\bigcup_{s\in Sq} sp^{2k} + p^{2k+1}\mathbb{Z}_p\right).$$

Hence,

$$\begin{aligned}\gamma &= \frac{2}{\sqrt{5}} + \frac{1}{\sqrt{5}}\left(\left(\bigcup_{s\in Sq} sp^2 + p^3\mathbb{Z}_p\right)\bigcup\left(\bigcup_{k\geq 2}\left(\bigcup_{s\in Sq} sp^{2k} + p^{2k+1}\mathbb{Z}_p\right)\right)\right)\\ &= \frac{2}{\sqrt{5}} + \frac{1}{\sqrt{5}}\left(\left(\bigcup_{s\in Sq} sp^2 + p^3\mathbb{Z}_p\right)\bigcup p^2(\sqrt{5}\gamma - 2)\right)\\ &= \frac{2}{\sqrt{5}} + \frac{1}{\sqrt{5}}\left(\gamma_1 \bigcup \gamma_2\right),\end{aligned}$$

where $\gamma_1 = \bigcup_{s\in Sq} sp^2 + p^3\mathbb{Z}_p$ and $\gamma_2 = p^2(\sqrt{5}\gamma - 2)$.

Since Lemma 3.3.1 holds for $r \in \mathbb{Z}_p(\sqrt{5})$ as well as $r \in \mathbb{Z}$, to compute $\alpha_{\gamma,p}$, we see that we may ignore the translation by $\frac{2}{\sqrt{5}}$ and the scaling by $\frac{1}{\sqrt{5}}$ because they do not change the p-sequence. We are left with the union of two sets to which Corollary 3.3.6 applies, since $v_p(x-y) = 2, \forall x \in \gamma_1, y \in \gamma_2$. Therefore,

$$\begin{aligned}\alpha_{\gamma,p} &= \alpha_{\gamma_1\cup\gamma_2,p}\\ &= ((\alpha_{\gamma_1,p} - (2k)) \wedge (\alpha_{\gamma_2,p} - (2k))) + (2k).\end{aligned}$$

Since $\gamma_1 = \bigcup_{s\in Sq} sp^2 + p^3\mathbb{Z}_p$ and $|Sq| = \frac{p-1}{2}$, γ_1 is a union of $\frac{p-1}{2}$ sets of the form $sp^2 + p^3\mathbb{Z}_p$, for $s \in Sq$. A set of this form has p-sequence $\alpha_{\mathbb{Z},p} + (3k)$, by Lemma 3.3.1, since $\mathbb{Z}_p/(p) = \mathbb{Z}/(p)$. Thus,

$$\alpha_{\gamma_1,p} = (\alpha_{\mathbb{Z},p} + (3k))^{\wedge\frac{p-1}{2}}.$$

Now, consider $\gamma_2 = p^2(\sqrt{5}\gamma - 2)$.

$$\begin{aligned}\alpha_{\gamma_2,p} &= \alpha_{p^2(\sqrt{5}\gamma-2),p}\\ &= \alpha_{\sqrt{5}\gamma-2,p} + (2k), && \text{by Lemma 3.3.1}\\ &= \alpha_{\gamma,p} + (2k), && \text{by Lemma 3.3.1.}\end{aligned}$$

Using these results, we then get

$$\begin{aligned}\alpha_{\gamma,p} &= ((\alpha_{\gamma_1,p} - (2k)) \wedge (\alpha_{\gamma_2,p} - (2k))) + (2k) \\ &= (((\alpha_{\mathbb{Z},p} + (3k))^{\wedge\frac{p-1}{2}} - (2k)) \wedge ((\alpha_{\gamma,p} + (2k)) - (2k))) + (2k) \\ &= ((\alpha_{\mathbb{Z},p} + (k))^{\wedge\frac{p-1}{2}} \wedge \alpha_{\gamma,p}) + (2k).\end{aligned}$$

Note that, as mentioned in the introduction, the equation for $\alpha_{\gamma,p}$ does determine this sequence completely since $\alpha_{\gamma,p}(n)$ is expressed in terms of other known quantities and $\alpha_{\gamma,p}(m)$ for $m < n$.

Although we used γ to denote the repeating branch with $\frac{2}{\sqrt{5}}$ as its first node, we can use the same name for all repeating branches since we are only interested in their p-sequences, which are all the same. Their p-sequences are the same by Lemma 3.3.1, because the only differences between the branches are in scaling or translation by a unit. Since there are b repeating branches, as shown above,

$$\alpha_{\mathbb{F}_2,p} = (\alpha_{\gamma,p})^{\wedge b} = (((\alpha_{\mathbb{Z},p} + (k))^{\wedge\frac{p-1}{2}} \wedge \alpha_{\gamma,p}) + (2k))^{\wedge b}.$$

Finally,

$$\begin{aligned}\alpha_{\mathbb{F},p} &= \alpha_{\mathbb{F}_1,p} \wedge \alpha_{\mathbb{F}_2,p} \\ &= (\alpha_{\mathbb{Z},p} + (k))^{\wedge a} \wedge (((\alpha_{\mathbb{Z},p} + (k))^{\wedge\frac{p-1}{2}} \wedge \alpha_{\gamma,p}) + (2k))^{\wedge b}.\end{aligned}$$

□

We now have a simple and fast algorithm for computing $\alpha_{\mathbb{F},p}$ for the primes for which β satisfies Condition 1.0.1, since the only operations required to apply Theorem 9.2.3 are sum, merge, and sort.

9.3 Examples

Let us now look at how we can apply Theorem 9.2.3 to calculate the p-sequence of the Fibonacci numbers for the primes $p = 11, 13$, and 17.

Example For $p = 11$, recall that the associated tree diagram is as shown in Figure 9.2.

Let

$$C = 11\mathbb{Z} \cup (1 + 11\mathbb{Z}) \cup (2 + 11\mathbb{Z}) \cup (3 + 11\mathbb{Z})) \cup (8 + 11\mathbb{Z})) \cup (10 + 11\mathbb{Z})) \cup \gamma,$$

where γ is the set represented by the repeating branch. From this diagram, we see that, $\forall k > 0$,

$$\frac{\mathbb{F}}{(11^k)} = \frac{C}{(11^k)}.$$

Hence, by Lemma 2.2.3,

$$\mathrm{Int}(\mathbb{F}, \mathbb{Z}_{(11)}) = \mathrm{Int}(C, \mathbb{Z}_{(11)}),$$

which means that the 11-sequence of $\mathbb{F}$ and the 11-sequence of C are the same.

Note that there are six branches that stabilize and one that repeats. Thus, we can apply Theorem 9.2.3 with $a = 6$ and $b = 1$. We then see that

$$\alpha_{\mathbb{F},11} = (\alpha_{\mathbb{Z},11} + (k))^{\wedge 6} \wedge \alpha_{\gamma,11},$$

where

$$\alpha_{\gamma,11} = ((\alpha_{\mathbb{Z},11} + (k))^{\wedge 5} \wedge \alpha_{\gamma,11}) + (2k).$$

The beginning of $\alpha_{\mathbb{F},11}$ is:

$\alpha_{\mathbb{F},11}$

$\{0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 2, 2, 2, 2, 2, 2, 2, 2, 3, 3, 3, 3, 3, 3, 4, 4, 4, 4, 4, 4, 4, 5, 5, 5, 5, 5,$
$5, 5, 6, 6, 6, 6, 6, 6, 6, 7, 7, 7, 7, 7, 7, 8, 8, 8, 8, 8, 8, 8, 9, 9, 9, 9, 9, 9, 10, 10, 10, 10, 10, 10,$
$10, 12, 12, 12, 12, 12, 12, 13, 13, 13, 13, 13, 13, 13, 14, 14, 14, 14, 14, 14, 15, 15, 15, 15,$
$15, 15, 15, 16, 16, 16, 16, 16, 16, 17, 17, 17, 17, 17, 17, 17, 18, 18, 18, 18, 18, 18, 19, \ldots\}$

Example For $p = 13$, recall that the associated tree diagram is as shown in Figure 9.3.

Let

$$\begin{aligned} C =& 13\mathbb{Z} \cup (1 + 13\mathbb{Z}) \cup (2 + 13\mathbb{Z}) \cup (3 + 13\mathbb{Z}) \cup (5 + 13\mathbb{Z}) \\ & \cup (8 + 13\mathbb{Z}) \cup (10 + 13\mathbb{Z}) \cup (11 + 13\mathbb{Z}) \cup (12 + 13\mathbb{Z}). \end{aligned}$$

From this diagram, we see that, $\forall k > 0$,

$$\frac{\mathbb{F}}{(13^k)} = \frac{C}{(13^k)}.$$

Hence, by Lemma 2.2.3,

$$\mathrm{Int}(\mathbb{F}, \mathbb{Z}_{(13)}) = \mathrm{Int}(C, \mathbb{Z}_{(13)}),$$

which means that the 13-sequence of $\mathbb{F}$ and the 13-sequence of C are the same.

Note that there are nine branches that stabilize and none that repeat. Thus, we can apply Theorem 9.2.3 with $a = 9$ and $b = 0$. We then see that

$$\alpha_{\mathbb{F},13} = (\alpha_{\mathbb{Z},13} + (k))^{\wedge 9}.$$

The beginning of $\alpha_{\mathbb{F},13}$ is:

$\alpha_{\mathbb{F},13} =$

$\{0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 1, 1, 1, 1, 1, 1, 2, 2, 2, 2, 2, 2, 2, 2, 2, 3, 3, 3, 3, 3, 3, 3, 3, 3, 4,$
$4, 4, 4, 4, 4, 4, 4, 5, 5, 5, 5, 5, 5, 5, 5, 5, 6, 6, 6, 6, 6, 6, 6, 6, 6, 7, 7, 7, 7, 7, 7, 7, 7, 7, 8, 8,$
$8, 8, 8, 8, 8, 8, 9, 9, 9, 9, 9, 9, 9, 9, 9, 10, 10, 10, 10, 10, 10, 10, 10, 10, 11, 11, 11, 11, 11,$
$11, 11, 11, 11, 12, 12, 12, 12, 12, 12, 12, 12, 12, 14, 14, 14, 14, 14, 14, 14, 14, 14, 15, \ldots\}$

Example For $p = 7$, recall that the associated tree diagram is as shown in Figure 9.4.

Let

$$C = 7\mathbb{Z} \cup (1 + 7\mathbb{Z}) \cup (2 + 7\mathbb{Z}) \cup (5 + 7\mathbb{Z}) \cup (6 + 7\mathbb{Z}) \cup \gamma \cup \delta,$$

where γ is the set represented by the repeating branch with 3 as its first node and δ is the set represented by the repeating branch with 4 as its first node. From this diagram, we see that, $\forall k > 0$,

$$\frac{\mathbb{F}}{(7^k)} = \frac{C}{(7^k)}.$$

Hence, by Lemma 2.2.3,

$$\mathrm{Int}(\mathbb{F}, \mathbb{Z}_{(7)}) = \mathrm{Int}(C, \mathbb{Z}_{(7)}),$$

which means that the 7-sequence of $\mathbb{F}$ and the 7-sequence of C are the same.

Note that there are five branches that stabilize and two that repeat. As mentioned in the proof of Theorem 9.2.3, we can use the same name for all repeating branches since we are only interested in their p-sequences, which are all the same. Thus, $\gamma = \delta$. We can now apply Theorem 9.2.3 with $a = 5$ and $b = 2$. We then see that

$$\alpha_{\mathbb{F},7} = (\alpha_{\mathbb{Z},7} + (k))^{\wedge 5} \wedge (\alpha_{\gamma,7})^{\wedge 2},$$

where

$$\alpha_{\gamma,7} = ((\alpha_{\mathbb{Z},7} + (k))^{\wedge 3} \wedge \alpha_{\gamma,7}) + (2k).$$

The beginning of $\alpha_{\mathbb{F},7}$ is:

$\alpha_{\mathbb{F},7} =$

$\{0,0,0,0,0,0,0,1,1,1,1,1,2,2,2,2,2,2,2,3,3,3,3,3,4,4,4,4,4,4,4,5,5,5,5,5,6,$
$6,6,6,6,6,6,8,8,8,8,8,9,9,9,9,9,9,9,10,10,10,10,10,11,11,11,11,11,11,11,$
$12,12,12,12,12,13,13,13,13,13,13,13,14,14,14,14,14,16,16,16,16,16,16,16,$
$17,17,17,17,17,18,18,18,18,18,18,18,19,19,19,19,19,20,20,20,20,20,20,\ldots\}$

With the p-sequences calculated in this thesis, together with the p-sequences for $p = 3$ and $p = 13$, we can calculate the first 10 elements in a regular basis for $\mathrm{Int}(\mathbb{F}, \mathbb{Z})$. They are:

$$1, x, \frac{x^2 - x}{2}, \frac{x^3 - 3x^2 + 2x}{6}, \frac{x^4 - 6x^3 + 11x^2 - 6x}{24},$$

$$\frac{143x^5 - 2965x^4 + 14215x^3 - 24035x^2 + 12642x}{240},$$

$$\frac{269x^6 - 9255x^5 + 80285x^4 - 274545x^3 + 392126x^2 - 188880x}{720},$$

$$\frac{\begin{array}{c}245129x^7 - 18791962x^6 + 343262150x^5 \\ -2392639900x^4 + 7391778401x^3 - 10008680458x^2 + 4684826640x\end{array}}{443520},$$

$$\frac{\begin{array}{c}245129x^8 - 23406351x^7 + 605061912x^6 - 6640975530x^5 \\ +35440539981x^4 - 94265906679x^3 + 117015122578x^2 - 52130681040x\end{array}}{443520}, \text{ and}$$

$$\frac{\begin{array}{c}54687901x^9 - 31874521653x^8 + 7668792570894x^7 \\ -568782337259682x^6 + 9101305330342869x^5 - 58282598264258277x^4 \\ 171075685473526496x^3 - 224615295883995588x^2 + 103282048708907040x\end{array}}{103783680},$$

as stated in Chapter 1.

Chapter 10

Conclusion

By using Coelho and Parry's results on the distribution of the Fibonacci numbers modulo powers of primes, we now have, for the primes p for which β satisfies Condition 1.0.1, a formula for the p-sequence of the Fibonacci numbers and an algorithm for finding a p-ordering. Once we know the p-sequence, we can then find a p-local regular basis for the polynomials that are integer-valued on the Fibonacci numbers using Bhargava's methods. A regular basis can be constructed for $\mathrm{Int}(\mathbb{F}, \mathbb{Z})$ from p-local regular bases for all primes p.

For the primes p for which β does not satisfy Condition 1.0.1 the distribution of the Fibonacci numbers modulo powers of these primes can be described using methods analogous to those above, with some of the differences clarified in Section 9 of [6]. This case is complicated by the fact that the domain of f cannot always be divided modulo p into squares and non-squares. Once we have determined which residue classes of $\mathbb{Z}/(p^k)$ are represented by the Fibonacci numbers for these primes, we can apply methods similar to those in this thesis to find a formula for the p-sequence of the Fibonacci numbers that has only slight modifications to the one given in our main result. We will then be able to find p-local regular bases for all primes p. Thus, as mentioned in the previous paragraph, we will be able to construct a regular basis for $\mathrm{Int}(\mathbb{F}, \mathbb{Z})$. Hence, our results provide a new and interesting example of a set $S \subseteq \mathbb{Z}$ for which we can describe $\mathrm{Int}(S, \mathbb{Z})$. Furthermore, our results are a step on the way to a general description of $\mathrm{Int}(S, \mathbb{Z})$ for sets $S \subseteq \mathbb{Z}$ determined by linear recurrence relations.

One such set, which is described in Section 10 of Coelho and Parry's paper, is quite similar to the Fibonacci numbers. For a prime integer p, consider the recurrence relation

$$u_n = Au_{n-1} + u_{n-2}, n \geq 2,$$

where A is an integer such that p does not divide $A(A^2 + 4)$. If we set $u_0 = 0$ and

$u_1 = 1$, we obtain a sequence to which we can directly extend Coelho and Parry's results for the Fibonacci numbers. This extension is possible because this sequence also satisfies Binet's formula, that is, we can write

$$u_n = \frac{1}{\sqrt{D}}\left(\beta^n - \left(\frac{-1}{\beta}\right)^n\right),$$

where $D = A^2 + 4$ is the discriminant of $P(x) = x^2 - Ax - 1$ and $\beta = (A + \sqrt{D})/2$ is the dominant root of P. The condition that p does not divide $A(A^2 + 4)$ ensures that β is a unit in $\mathbb{Z}_p$ if D is a square and that β is a unit in $\mathbb{Z}_p(\sqrt{D})$ if D is not a square. Thus, basically all of the results of the earlier chapters hold in this case by replacing 5 with D and replacing the β used for the Fibonacci numbers by this more general one in our presentation. Hence, we will also be able to construct a regular basis for $\mathrm{Int}(S, \mathbb{Z})$, where S is the set determined by the linear recursion described above.

It is now natural to wonder to what further generality these results can be extended. For instance, it would be interesting to consider whether or not the initial conditions required in the previous paragraph are necessary to apply Coelho and Parry's methods. Even more generally, we would like to be able to describe $\mathrm{Int}(S, \mathbb{Z})$ for sets S determined by a second-order linear recurrence relation of the form

$$u_n = A \cdot u_{n-1} + B \cdot u_{n-2}, n \geq 2$$

where A, B, u_0, and u_1 are integers. An alternative approach will be necessary for this result. From there, we would want to find a general description of $\mathrm{Int}(S, \mathbb{Z})$ for any set $S \subseteq \mathbb{Z}$ determined by a linear recurrence relation.

Bibliography

[1] David Adam and Paul-Jean Cahen, *Newtonian and Schinzel quadratic fields*, Journal of Pure and Applied Algebra **215** (2011), 1902–1918.

[2] David Adam, Jean-Luc Chabert, and Youssef Fares, *Subsets of $\mathbb{Z}$ with simultaneous orderings*, Integers **10** (2010), 437–451.

[3] Manjul Bhargava, *P-orderings and polynomial functions on arbitrary subsets of Dedekind rings*, Journal für die reine und angewandte Mathematik **490** (1997), 101–127.

[4] ———, *The factorial function and generalizations*, The American Mathematical Monthly **107** (2000), no. 9, 783–799.

[5] Paul-Jean Cahen and Jean-Luc Chabert, *Integer-valued polynomials*, American Mathematical Society, Providence, Rhode Island, 1997.

[6] Zaqueu Coelho and William Parry, *Ergodicity of p-adic multiplications and the distribution of Fibonacci numbers*, American Mathematical Society Translation **202** (2001), 51–70.

[7] Fernando Q. Gouvêa, *p-adic numbers: An introduction*, second ed., Universitext, Springer-Verlag, Berlin, 1997.

[8] Kenneth Ireland and Michael I. Rosen, *Elements of number theorey: Including an introduction to equations over finite fields*, Bogden & Quigley, Inc., Publishers, Tarrytown-on-Hudson, New York, 1972.

[9] Eliot T. Jacobson, *Distribution of the Fibonacci numbers mod 2^k*, The Fibonacci Quarterly **30** (1992), 211–215.

[10] Keith Johnson, *P-orderings of finite subsets of Dedekind domains*, Journal of Algebraic Combinatorics **30** (2009), 233–253.

[11] Harald Niederreiter, *Distribution of Fibonacci numbers mod 5^k*, The Fibonacci Quarterly **10** (1972), no. 4, 373–374.

[12] Melanie Wood, *P-orderings: a metric viewpoint and the non-existence of simultaneous orderings*, Journal of Number Theory **99** (2003), 36–56.