THE INTEGER-VALUED POLYNOMIALS ON LUCAS NUMBERS

by

Amitabh Kumer Halder

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

at

Dalhousie University
Halifax, Nova Scotia
August 2017

Dedicated to my wife and kids

Table of Contents

Abstract

An integer-valued polynomial on a subset, S, of the set of integers, $\mathbb{Z}$, is a polynomial $f(x) \in \mathbb{Q}[x]$ such that $f(S) \subseteq \mathbb{Z}$. The collection, $Int(S, \mathbb{Z})$, of such integer-valued polynomials forms a ring with many interesting properties. The concept of p-ordering and the associated p-sequence due to Bhargava [2] is used for finding integer-valued polynomials on any subset, S, of $\mathbb{Z}$.

In this thesis, we concentrate on extending the work of Keith Johnson and Kira Scheibelhut [14] for the case $S = \mathfrak{L}$, the Lucas numbers, where they work on integer-valued polynomials on $S = \mathfrak{F}$, Fibonacci numbers. We also study integer-valued polynomials on the general 3 term recursion sequence, $\mathfrak{G}$, of integers for a given pair of initial values with some interesting properties. The results are well-agreed with those of [14].

List of Abbreviations and Symbols Used

$Int(S, \mathbb{Z})$	The set of integer-valued polynomials
$\binom{x}{k}$	The binomial polynomial
$\mathfrak{L}$	The sequence of Lucas numbers
$\mathfrak{L}_k$	The kth Lucas number
$\mathbb{Z}_{(p)}$	The p-local integers
$f_{S,p,k}(x)$	The $\mathbb{Z}_{(p)}$-basis elements
$b_{S,p,k}(x)$	The monic polynomials in $\mathbb{Z}[x]$
$\{\alpha_{S,p}(k)\}_{k=0}^{\infty}$	The associated p-sequence of S
$\nu_k(\mathbb{Z}, p)$	p-adic valuation of any element in $\mathbb{Z}$
D	A domain
F	The quotient field of D
R	A subring of D
D_p	A discrete valuation domain
E	A fractional subset of D
ν	An essential valuation of $\mathbb{Z}$
$ord_p a$	The highest power of p dividing an integer $a > 0$
$\lvert \cdot \rvert_p$	The p-adic norm on $\mathbb{Q}$
$\lvert\lvert \cdot \rvert\rvert$	A nontrivial norm on $\mathbb{Q}$
$\mathbb{Q}_p$	The p-adic numbers
$\mathbb{Z}_p$	The ring of p-adic integers
${\mathbb{Z}_p}^{\times}$	The p-adic units
$\omega(x)$	An arithmetic function on a ring R
$d(x, y)$	An ultradistance on a ring R
$\hat{R}$	The completion of a ring R
$\hat{P}$	The p-adic closure
$\mathbb{N}$	The positive integers
$\bar{S}$	The polynomial D-closure of S
f	A primitive polynomial

$d(S, f)$	The fixed divisor of f
$\mathbb{Z}/n\mathbb{Z}$	A factor ring
$\mathfrak{L}(n)$	First n-terms of Lucas numbers
τ	The Golden ratio $(1 + \sqrt{5})/2$
U	The units of $\mathbb{Z}_p$
$U(\sqrt{5})$	The units of $\mathbb{Z}_p(\sqrt{5})$
$U^0(\sqrt{5})$	The units of $\mathbb{Z}_p(\sqrt{5})$ with norm ± 1
$N(z)$	The norm of $z \in U(\sqrt{5})$
f_+, f_-	The functions in the Binet's formula of $\mathfrak{L}$
$< \tau >$	The group generated by τ
$\mathfrak{G}$	The general sequence for a given pair of integers
F_+, F_-	The functions used in the Binet's formula of $\mathfrak{G}$

Acknowledgements

I would like to thankfully acknowledge the fundings I received namely the Nova Scotia Graduate Scholarship, research grant from the project operated by Dr. Sara Faridi, departmental funding from the Department of Mathematics and Statistics in Dalhousie University, and Lett Bursary from the Lett family. I would like to express thanks to several people without whose help this thesis would not have been completed. In particular, I am very grateful to:

* my supervisor, Dr. Keith Johnson, for his cordial help, potential guidance, patience, passion, insight, and valuable suggestions;

* my readers, Dr. Robert Pare and Dr. Dorette Pronk, for their interest and suggestions;

* Dr. David Iron, for his academic help and sympathy;

* Dr. Sara Faridi, for her support and valuable advices that helped me to get an opportunity to study at the Department of Mathematics and Statistics in Dalhousie University;

* Dr. Keith Taylor and Dr. Karl Dilcher, for their help and suggestions;

* the faculty, staff, and students of the Department of Mathematics and Statistics in Dalhousie University for their help and assistance;

* my parents, wife, and kids, for their love, mental support, and sacrifice;

* and, my friends, especially Kunpeng Wang, Tom Potter, Giuseppe Pasqualino, and Bassemah Alhulaimi, for their homework help and company.

Chapter 1

Introduction

Let S be a subset of $\mathbb{Z}$, the set of integers. The ring of integer-valued polynomials on S, is given by
$Int(S,\mathbb{Z}) = Int(S) = \{f(x) \in \mathbb{Q}[x] : f(S) \subseteq \mathbb{Z}\}$.
This is a subring of $\mathbb{Q}[x]$ preserving many interesting properties. The study of the ring of integer-valued polynomials on the subsets of $\mathbb{Z}$ and its generalizations has been continuing for more than 100 years, as for examples [2] and [20]. The updated results up to 1997 are in [5].
In this thesis, we are interested in concentrating on the development of the work of Keith Johnson and Kira Scheibelhut [14] for the case $S = \mathfrak{L}$, the Lucas numbers.
In general, for the description of the $\mathbb{Z}$-module, $Int(S,\mathbb{Z})$, we wish to find a regular $\mathbb{Z}$-basis having polynomials $\{f_k(x) : k = 0, 1, 2, ...\}$ in $Int(S,\mathbb{Z})$ as basis elements such that $f_k(x)$ is a polynomial of degree k. Every element $f(x) \in Int(S)$ can be expressed uniquely as a $\mathbb{Z}$-linear combination of the polynomials $\{f_k(x) : k = 0, 1, 2, ...\}$.
We may consider certain suitable choices for S to form regular $\mathbb{Z}$-bases.
For example, every element in $Int(\mathbb{Z})$ is a $\mathbb{Z}$-linear combination of the binomial polynomials $\{f_k(x) : k = 0, 1, 2, ...\} = \{\binom{x}{k}\} = \{\prod_{i=0}^{k-1} \frac{x-i}{k-i}\}$.
Due to Pascal's triangle it is easy to show that the polynomials f_k are in $Int(\mathbb{Z})$. The polynomials $f_k(x)$ take values 0 at $x = 0, 1, 2, ..., k-1$ and 1 at $x = k$.
A similar result can be observed for $S = \{i^2 : i \in \mathbb{Z}\}$ due to [2] and $S = \{p : p \in \mathbb{Z}$ and p is positive prime $\}$ due to [6]. But no one has studied this construction for $S = \mathfrak{L}$, the Lucas numbers.
The set $\mathfrak{L} = \{\mathfrak{L}_k : k = 0, 1, 2, ...\}$ of Lucas numbers may be defined by the recurrence relation $\mathfrak{L}_{k+1} = \mathfrak{L}_k + \mathfrak{L}_{k-1}$ for $k \geq 1$ starting with $\mathfrak{L}_0 = 2$ and $\mathfrak{L}_1 = 1$.
We are interested in concentrating on the localization of the structure with respect to prime numbers and then deducing the general case from the localized structures, i.e., we require to first study $Int(S)_{(p)} = \{f(x) \in \mathbb{Q}[x] : f(S) \subseteq \mathbb{Z}_{(p)}\}$,

where $\mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Q} : gcd(p, b) = 1\}$ is the ring of p-local integers, and then to find the regular $\mathbb{Z}_{(p)}$-basis so that every element of $Int(S)$ can be written as a $\mathbb{Z}_{(p)}$-linear combination. We want to find the regular $\mathbb{Z}_{(p)}$-basis for all primes, p, with the polynomials of the form $f_{S,p,k}(x) = b_{S,p,k}(x)/p^{\alpha_S,p^{(k)}}$, where $b_{S,p,k}(x)$'s are monic polynomials in $\mathbb{Z}[x]$ and so $f_{S,p,k}(x)$'s are in $Int(S, \mathbb{Z})$ and $\alpha_S, p^{(k)}$ is nonzero for fixed k and for only finitely many primes. As for example, when $S = \mathbb{Z}$, we can see that $p^{\alpha_S,p^{(k)}}$ is exactly the power of p in the prime factorization of $k!$. In this case, $\alpha_{\mathbb{Z}}, p^{(k)}$ can be extracted by the well-known formulas

$$\nu_k(\mathbb{Z}, p) = \sum_{i\geq 1}[k/p^i] = (k - \sum_{i\geq 0} k_i)/(p - 1),$$

where k is a p-adic integer, i.e., $k = \sum_{i\geq 0} k_i p^i$.

For such given regular $\mathbb{Z}_{(p)}$-basis for each prime, p, the Chinese Remainder Theorem ensures that for each k there exists a $\mathbb{Z}$-linear combination $f_{S,k}(x)$, say, of $f_{S,p,k}(x)$'s so that we have $f_{S,k}(x) = b_{S,k}(x)/\prod p^{\alpha_S,p^{(k)}}$ with monic polynomials $b_{S,k}(x)$ in $\mathbb{Z}[x]$ for all primes such that $\alpha_S, p^{(k)}$ is positive. This shows that $f_{S,k}(x) \in Int(S, \mathbb{Z})$ and $f_{S,k}(x)$'s form regular $\mathbb{Z}_{(p)}$-basis of $Int(S, \mathbb{Z})$ and so form a regular $\mathbb{Z}$-basis.

In our investigation, we get a regular basis for $Int(\mathfrak{L}, \mathbb{Z})$ as
$\{1, (x-2), \frac{(x-2)(x-1)}{2}, \frac{(x-2)(x-1)(x-3)}{6}, \frac{(x-2)(x-1)(x-3)(x-4)}{120}, \frac{(x-2)(x-1)(x-3)(x-4)(x-207)}{240}, \cdots\}$.

We investigate a general sequence, $\mathfrak{G}$, of integers for any pair (A, B) of integers, in particular, $(A, B) = (0, 1)$ and $(A, B) = (2, 1)$ give the results of Keith Johnson and Kira Scheibelhut [14], and the results for Lucas numbers that are consistent. Also, we find regular $\mathbb{Z}$-basis for $Int(\mathfrak{G}, \mathbb{Z})$ at $(A, B) = (2, 5)$ given by
$\{1, (x-2), \frac{(x-2)(x-205)}{2}, \frac{(x-2)(x-205)(x-1119)}{6}, \frac{(x-2)(x-205)(x-1119)(x-356)}{24},$
$\frac{(x-2)(x-205)(x-1119)(x-356)(x-1243)}{240}, \cdots\}$.

Chapter 2

Algebraic Background

2.1 Properties of Local Rings

Definition 2.1.1. *([5], Definition I. 1. 8.) A subset S of the quotient field F of a domain D is said to be a fractional subset of D if there exists a nonzero element d of D such that $dS \subseteq D$. In particular, a subset S of $\mathbb{Q}$ is a fractional subset of $\mathbb{Z}$ if there exists a nonzero element d of $\mathbb{Z}$ such that $dS \subseteq \mathbb{Z}$.*

Definition 2.1.2. *Let D be a domain that is contained in a field F. A nonempty subset S of D is said to be a multiplicative subset of D if $0 \notin S$, $1 \in S$, and s_1, $s_2 \in S$ implies $s_1.s_2 \in S$.*

Theorem 1. *([5], Theorem I. 2. 1.) Let D be a domain that is contained in a field F, and let S be a multiplicative subset of D and $f(x) \in F[X]$ be a polynomial. Then $S^{-1} < f(D) >=< f(S^{-1}D) >$.*

Theorem 2. *([5], Proposition I. 2. 2.) Let S be a multiplicative subset of a domain D. Then $S^{-1}Int(D) \subseteq Int(S^{-1}D)$.*

Theorem 3. *([5], Theorem I. 2. 3.) Let S be a multiplicative subset of a Noetherian domain D. Then $S^{-1}Int(D) = Int(S^{-1}D)$.*

Lemma 1. *([5], Lemma I. 2. 4.) Let S be a multiplicative subset of a domain D and let E be a subset of the quotient field F of D. Then $S^{-1}Int(E, D) \subseteq Int(E, S^{-1}D)$.*

Theorem 4. *([5], Proposition I. 2. 5.) Let R be a subring of a domain D with the quotient field F of D, and let S be a multiplicative subset of R. Then $S^{-1}Int(R, D) \subseteq Int(R, S^{-1}D) = Int(S^{-1}R, S^{-1}D)$.*

In particular, for $R = D$, we have the following:

Corollary 1. *([5], Corollary I. 2. 6.) If S is a multiplicative subset of a domain D, then $S^{-1}Int(D) \subseteq Int(D, S^{-1}D) = Int(S^{-1}D)$.*

Theorem 5. *([5], Proposition I. 2. 7.)*
(i) Let S be a multiplicative subset and, let E be a fractional subset of a Noetherian domain D. Then $S^{-1}Int(E,D) = Int(E, S^{-1}D)$.
(ii) Let R be a Noetherian subring of a domain D, and let S be a multiplicative subset of R. Then $S^{-1}Int(R,D) = Int(R, S^{-1}D) = Int(S^{-1}R, S^{-1}D)$.

Definition 2.1.3. *A prime ideal of a domain D is said to be a height-one prime ideal if it is minimal among the nonzero prime ideals of D.*

Definition 2.1.4. *A domain D is said to be a Krull domain if following conditions are satisfied:*
(i) $D = \cap_p D_p$, where (p) runs over the height-one prime ideals of D,
(ii) D_p is a discrete valuation domain for each height-one prime ideal (p) of D,
(iii) for all height-one prime ideals of D, each element of D is invertible in D_p.

Theorem 6. *([5], Proposition I. 2. 8.) Let D be a Krull domain, let (p) be a height-one prime ideal, and let E be a fractional subset of D. Then $Int(E,D)_p = Int(E, D_p)$.*

Remark 1. *([5], Remark I. 2. 9.) The ring of integers, $\mathbb{Z}$, is both a Noetherian and a Krull domain. For any non-trivial multiplicative subset S of $\mathbb{Z}$, $S^{-1}\mathbb{Z}$ is not a fractional subset of $\mathbb{Z}$, and so by ([5], Proposition I. 1. 9), $S^{-1}Int(S^{-1}\mathbb{Z}, \mathbb{Z}) = S^{-1}\mathbb{Z}$, and on the other hand, $Int(S^{-1}\mathbb{Z}, S^{-1}\mathbb{Z}) = Int(S^{-1}\mathbb{Z})$. But in the case of Theorem 5 and Theorem 6, we must consider $S^{-1}\mathbb{Z}$ to be a fractional subset of $\mathbb{Z}$.*

Theorem 7. *([5], Proposition I. 2. 8.) Let S be a fractional subset of $\mathbb{Z}$. Then for any fixed prime p, $Int(S, \mathbb{Z}_p) = Int(S, \mathbb{Z})_p$.*

Proof. Due to Lemma 1 ([5], Lemma I. 2. 4.), we have $Int(S,\mathbb{Z})_p \subseteq Int(S, \mathbb{Z}_p)$.
For the reverse part, let $f \in Int(S, \mathbb{Z}_p)$, and let $d\mathbb{Z}$ be non-zero element such that $df \in \mathbb{Z}[X]$. Let V be a finite set of essential valuations v of $\mathbb{Z}$ with $v(d) > 0$ and v is not associated with (p). For any height-one prime ideal (q) such that $(p) \neq (q)$, there exists an element of (q) that is not in (p). We take a product of such elements to get an element $z \in \mathbb{Z}$ with $z \notin (p)$ such that $v(z) \geq v(d)$, for each $v \in V$. Thus. for each height-one prime ideal $(q) \neq (p)$, $zf \in \mathbb{Z}_q[X]$. Since S is a subset of $\mathbb{Z}$, due to ([5], Remark I. 1. 11.) $zf(S) \subseteq \mathbb{Z}_q$. Again, $zf(S) \subseteq \mathbb{Z}_p$ because $z \in \mathbb{Z}$ and $f \in Int(S, \mathbb{Z}_p)$ by hypothesis. Thus, $zf \in Int(S,\mathbb{Z})$ and so $f \in Int(S,\mathbb{Z})_p$ since $z \notin (p)$. Thus, $Int(S, \mathbb{Z}_p) \subseteq Int(S,\mathbb{Z})_p$. Hence $Int(S, \mathbb{Z}_p) = Int(S,\mathbb{Z})_p$.

2.2 Background for the p-adic Integers

Definition 2.2.1. *Let $p \geq 2$ be any prime. Then we define $ord_p a$ to be the highest power of p dividing a nonzero integer a, i.e., the greatest m for which $a \equiv 0 \ (mod\, p^m)$.*

For example, $ord_5 34 = 0$, $ord_7 28 = 1$, and if $a = 0$, then $ord_p a = \infty$. Note the multiplicative nature of $ord_p a$ is like a logarithm, such as $ord_p a_1 a_2 = ord_p a_1 + ord_p a_2$.

Definition 2.2.2. *For any prime $p \geq 2$, we define a map $|\ |_p$ on $\mathbb{Q}$ by*

$$|x|_p = \begin{cases} \frac{1}{p^{ord_p x}}, & \text{if } x \text{ is not } 0 \\ 0, & \text{if } x=0 \end{cases}.$$

Proposition 1. *([15], Chapter 1, Section 2, Proposition.) $|\ |_p$ is a norm on $\mathbb{Q}$.*

Definition 2.2.3. *Two metrics md_1 and md_2 on a set X are equivalent if the sequence is a Cauchy sequence with respect to the metric md_1 if and only if it is a Cauchy sequence with respect to md_2.*
Two norms are equivalent if they provide equivalent metrics.

Theorem 8. *([15], Chapter 1, Section 2, Theorem 1(Ostrowski).) Every nontrivial norm $||\cdot||$ on $\mathbb{Q}$ is equivalent to $|\ |_p$ for some prime p or for $p = \infty$.*

Definition 2.2.4. *Let $p \neq \infty$. Two Cauchy sequences $\{a_k\}_{k=1}^{\infty}$ and $\{b_k\}_{k=1}^{\infty}$ are said to be equivalent if $|a_k - b_k|_p \to 0$ as $k \to \infty$. We define $\mathbb{Q}_p$ to be the set of equivalence classes of Cauchy sequences. The elements of $\mathbb{Q}_p$ are called the p-adic numbers.*

Note that $\mathbb{Q}_p$ is a field and contains $\mathbb{Q}$. Also, each element $x \in \mathbb{Q}_p$ can be written as a series of the form:
$x = \frac{a_0}{p^k} + \frac{a_1}{p^{k-1}} + ... + \frac{a_{k-1}}{p} + a_k + a_{k+1}p + a_{k+2}p^2 + ...,$
which is known as the p-adic expansion of x.

Lemma 2. *([15], Section 4, Lemma, P.12.) Let $x \in \mathbb{Q}_p$ with $|x|_p \leq 1$. Then for any integer $k = 1, 2, 3, ...,$ there exists an integer $z \in \mathbb{Z}$ such that $|z - x|_p \leq p^{-k}$. The integer z can be taken in the set $\{0, 1, 2, ..., p^k - 1\}$.*

Definition 2.2.5. *The set $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$ consists of all elements of $\mathbb{Q}_p$ whose p-adic expansion does not contain negative powers of p. An element of $\mathbb{Z}_p$ is called a p-adic integer and the set $\mathbb{Z}_p$ is called the ring of p-adic integers. A p-adic integer in the set ${\mathbb{Z}_p}^{\times}$ is called a p-adic unit.*

2.3 Hensel's Lemma

We state the famous Hensel's Lemma.

Lemma 3. *(Hensel's Lemma)([15], Section 5, Theorem 3.) Let $f(x) \in \mathbb{Z}_p[X]$ be a polynomial and let $z_0 \in \mathbb{Z}_p$ such that $f(z_0) \equiv 0 \ (mod\ p)$ and $f'(z_0) \not\equiv 0 \ (mod\ p)$. Then there exists a unique element $z \in \mathbb{Z}_p$ such that $f(z) = 0$ and $z \equiv z_0 \ (mod\ p)$.*

Now we require to state and prove the generalization of Hensel's Lemma.

Lemma 4. *(Generalization of Hensel's Lemma.) Let $f(x) \in \mathbb{Z}_p[X]$ be a polynomial and let $z_0 \in \mathbb{Z}_p$ such that $f'(z_0) \equiv 0 \ (mod\ p^M)$ but $f'(z_0) \not\equiv 0 \ (mod\ p^{M+1})$, and $f(z_0) \equiv 0 \ (mod\ p^{2M+1})$ for some integer $M \geq 0$. Then there exists a unique element $z \in \mathbb{Z}_p$ such that $f(z) = 0$ and $z \equiv z_0 \ (mod\ p^{M+1})$.*

Proof. If $M = 0$, then we have the Hensel's Lemma.
Let $N \geq 2M + 1$. Then we have $f(z_0) \equiv 0 \pmod{p^N}$ with $f'(z_0) \equiv 0 \pmod{p^M}$ and $f'(z_0) \not\equiv 0 \pmod{p^{M+1}}$. If $z = z_0 + \lambda p^{N-M}$, then $f(z) \equiv f(z_0) \pmod{p^N}$ and $p^M | f'(z)$.
Now,

$$\begin{aligned} f(z) &= f(z_0 + \lambda p^{N-M}) \\ &= f(z_0) + \lambda p^{N-M} f'(z_0) + terms\ \ with\ \ p^{N+1} \\ &\equiv f(z_0) + \lambda p^{N-M} f'(z_0) \pmod{p^{N+1}} \\ &= f(z_0) + \lambda p^{N-M} f'(z_0). \end{aligned}$$

Since $f(z_0) \equiv 0 \pmod{P^N}$ and $p^{N-M} f'(z_0) \equiv 0 \pmod{P^N}$, $f(z) \equiv f(z_0) \equiv 0 \pmod{P^N}$. Now,

$$\begin{aligned} \frac{f(z)}{p^N} &\equiv \frac{f(z_0)}{p^N} + \frac{\lambda p^{N-M} f'(z_0)}{p^N} \pmod{p} \\ &\equiv \frac{f(z_0)}{p^N} + \frac{\lambda f'(z_0)}{p^M} \pmod{p}. \end{aligned}$$

Since $p^{M+1} \not| f'(z_0)$, $p \not| (\frac{f'(z_0)}{p^M})$ and so there exists a unique value of λ such that, taking $z = z_0 + \lambda p^{N-M}$ gives $\frac{f(z)}{p^N} \equiv 0 \pmod{p}$.
Also, $f'(z) \equiv f'(z_0) \pmod{p^{N-M}}$. Since $p^M | f'(z_0)$ but $p^{M+1} \not| f'(z_0)$, $p^{M+1} \not| f'(z)$.

2.4 P-adic Closures

Definition 2.4.1. *Let F be a quotient field of a domain D, and let ν be a (rank-one) discrete valuation on F. We define a distance d on F by $d(x,y) = e^{-v(x-y)}$. In general, if R is a ring and P is an ideal of R satisfying $\cap_{k=0}^{\infty} P^k = (0)$, we may define an arithmetic function w on R by*

$$w(x) = \begin{cases} sup\{k : x \in P^k\}, & \text{if } x \text{ is not } 0 \\ +\infty, & \text{if } x=0 \end{cases}.$$

It is important to note that w is not a valuation on R in general. Then employing the convention $e^{-\infty} = 0$ and considering $|x| = e^{-w(x)}$ and $d(x,y) = |x-y| = e^{-w(x-y)}$, we can easily check that d is an ultradistance on R:
(i) $d(x,y) = 0$ if and only if $x = y$,
(ii) $d(x,y) = d(y,x)$,
(iii) $d(x,z) \leq sup\{d(x,y), d(y,z)\}$.
For, (i) and (ii) are obvious; the third condition (iii) is immediate from the inequality $w(x,y) \geq inf\{w(x), w(y)\}$.

Definition 2.4.2. *The ultradistance d on R defines a topology called the P-adic topology. The clopen subsets of a topological space are the subsets that are both open and closed with respect to the corresponding topology.*

It is clear that the ideals P^k form a fundamental system of clopen neighborhoods of 0. Due to translation, each point meets a fundamental system of clopen neighborhoods that holds for ultrametric spaces. Finally, the addition and multiplication are continuous on R.
If F is a quotient field of a domain D, then the ultradistance function can be defined on F, and so F itself is a topological space and D is a clopen subspace with respect to the topology. Let D be a discrete valuation domain, then the topology defined by the valuation on D is clearly the m-adic topology for the maximal ideal m of D.

Definition 2.4.3. *Let R be a ring. The completion of R with respect to the metric associated with the P-adic topology is denoted by $\hat{R}$ that itself is the ultrametric space and a topological ring. If D is a discrete valuation ring in terms of valuation v on a*

field F, then $\hat{D}$ is the valuation ring in terms of the extended valuation $\hat{v}$ of v to the completion $\hat{F}$ to F.

Definition 2.4.4. *Let R be a ring, and let P be an ideal of R. The topological closure of P is denoted by $\hat{P}$ which is an ideal of the completion $\hat{R}$ of R.*

Remark 2. *The ideal P is contained in some maximal ideal of $\hat{R}$(see [[16], Theorem 8.2]). The closures $\hat{P^k}$ of the ideals P^k of R construct a fundamental system of clopen neighborhoods of 0 in $\hat{R}$ and $\hat{R}/\hat{P^k} \simeq R/P^k$ (see [[5], III. 1. Exercise3]).*
Let P be finitely generated, then $\hat{P^k} = \hat{P^k} = P^k\hat{R}$ (see [[18], (17. 4)]).

If R is a Noetherian ring, then we have the following:

Theorem 9. *([[16], Theorem 8.11], [[1], Theorem 10. 15. 8].) If R is a Noetherian ring, and P is an ideal of R satisfying $\cap_{k=0}^{\infty} P^k = (0)$, and if $\hat{R}$ is the completion of R in the P-adic topology, then*
(i) $\hat{R}$ is a Noetherian ring,
(ii) $(\hat{P})^k = (\hat{P^k}) = P^k\hat{R}$ for every k,
(iii) the topology of $\hat{R}$ is the $\hat{P}$-adic topology,
(iv) $\hat{R}/\hat{P^k} \simeq R/P^k$ for every k,
(v) if $P = m$ is a maximal ideal of R, then $\hat{R}$ is local with maximal ideal $\hat{m}$.

2.5 The Chinese Remainder Theorem

Let $d_1, d_2, ..., d_k$ be pairwise relatively prime integers. Then for any integers $x_1, x_2, ..., x_k$, the congruences $x \equiv x_i \pmod{d_i}$ have a simultaneous solution $x \in \mathbb{Z}$. Moreover, if x is one solution, then the other solutions are the integers of the form $x + md$ with $m \in \mathbb{Z}$ and $d = \prod d_i$.

We require to transfer the above statement in terms of ideals.
Note: Two integers m and n are relatively prime if and only if $(m, n) = \mathbb{Z}$, i.e., $(m) + (n) = \mathbb{Z}$. Thus, this inspires us to say that two ideals I_1 and I_2 of a ring R are relatively prime if $I_1 + I_2 = R$.
If $m_1, m_2, ..., m_k$ are integers and $m = lcm(m_1, m_2, ..., m_k)$, then $\prod(m_i) \subset \cap(m_i)$ and $\prod(m_i) = \cap(m_i)$ if the integers m_i's are pairwise relatively prime then $m = \prod m_i$.

Thus, for ideals $I_1, I_2, ..., I_k$, we have
$I_1 \cdot I_2 \cdots I_k \subset I_1 \cap I_2 \cap \cdots \cap I_k$, but the two ideals need not be equal.
In fact, for the ideals I_1, I_2, ..., I_k of a commutative ring R, $I_1 \cdot I_2 \cdots I_k = I_1 \cap I_2 \cap \cdots \cap I_k$ if and only if $Tor_1^R(\frac{R}{I_1}, \frac{R}{I_2}, \cdots, \frac{R}{I_k}) = 0$.
Regarding to the above discussion, we have

Theorem 10. *([17], Theorem 1. 14.) Let $I_1, I_2, ..., I_k$ be pairwise relatively prime ideals of a ring R. Then for any elements $x_1, x_2, ..., x_k$ of R, the congruences*
$x \equiv x_i \ (mod\ I_i)$
have a simultaneous solution $x \in R$. Moreover, if x is one solution, then the other solutions are the elements of the form $x + r$ with $r \in \cap I_i = \prod I_i$.
In other words, the natural maps provide an exact sequence
$0 \to I \to R \to \prod_{i=1}^{k} R/I_i \to 0$ *with* $I = \cap I_i = \prod I_i$.

Proof. First suppose that $k = 2$. Since I_1 and I_2 are relatively prime, $I_1 + I_2 = R$. Then there exist elements $a \in I_1$ and $a_2 \in I_2$ such that $a_1 + a_2 = 1$. So the element $x = a_1x_1 + a_2x_2$ has the required property.
For each i, we have $a_i \in I_1$ and $b_i \in I_i$ such that $a_i + b_i = 1$, for all $i \geq 2$.
Then $\prod_{i\geq 2}(a_i + b_i) = 1$ and so $1 \in I_1 + \prod_{i\geq 2} I_i$ and thus $I_1 + \prod_{i\geq 2} I_i = R$.
Now, for $k = 2$, we can apply the theorem to get an element $y_1 \in R$ such that $y_1 \equiv 1\ (modI_1)$ and $y_1 \equiv 0 \pmod{\prod_{i\geq 2} I_i}$.
These give that $y_1 \equiv 1 \pmod{I_1}$ and $y_1 \equiv 0 \pmod{I_j}$, for all $j > 1$. Thus, there exist elements $y_2, y_3, ..., y_k$ such that $y_i \equiv 1 \pmod{I_i}$ and $y_i \equiv 0 \pmod{I_j}$, for $i \neq j$.
Thus, the element $x = \sum x_i y_i$ has the required property.
Now, it remains to show that $\cap I_i = \prod I_i$. First suppose that $k = 2$. Let $a_1 \in I_1, a_2 \in I_2$ such that $a_1 + a_2 = 1$. Let $c \in I_1 \cap I_2$. Then we have $c = a_1c + a_2c$, which shows that $I_1 \cap I_2 = I_1.I_2$. By induction suppose that $\cap_{i\geq 2} I_i = \prod_{i\geq 2} I_i$. Since I_1 and $\prod_{i\geq 2} I_i$ are relatively prime, $I_1. \prod_{i\geq 2} I_i = I_1 \cap (\prod_{i\geq 2} I_i) = I_1 \cap (\cap_{i\geq 2} I_i) = \cap_i I_i$.

The above theorem extends to R-modules as follows:

Theorem 11. *([17], Theorem 1.15.) Let $I_1, I_2, ..., I_k$ be pairwise relatively prime ideals of a ring R, and let M be an R-module. Then there exists an exact sequence*
$0 \to IM \to M \to \prod_i M/I_iM \to 0$ *with* $I = \prod I_i = \cap I_i$.

2.6 Integer-Valued Polynomials

Definition 2.6.1. *A polynomial $f(x) \in \mathbb{Q}[X]$ is said to be an integer-valued polynomial if it gives an integer value while evaluating at an integer.*
The set of such integer-valued polynomials is denoted by
$Int(\mathbb{Z}) = \{f(x) \in \mathbb{Q}[X] : f(\mathbb{Z}) \subseteq \mathbb{Z}\}$.

It is clear that any polynomial $f(x) \in \mathbb{Z}[X]$ is integer-valued. However, the polynomials having rational coefficients may be integer-valued, as for example, $f(x) = x(x-1)/2$ is integer-valued since at any integer $x = k \in \mathbb{Z}$, k is even if and only if $(k-1)$ is odd and conversely.

Due to Pascal's triangle, we know that for any non-negative integers m and k, $\binom{m}{k}$ is an integer.
From which we have the following:

Lemma 5. *The binomial polynomials $\{f_k(x) : k = 0, 1, 2, ...\} = \{\binom{x}{k}\} = \{\prod_{i=0}^{k-1} \frac{x-i}{k-i}\}$ belong to $Int(\mathbb{Z})$.*

Proof. For $k = 0, 1, 2, ..., $ we have
$f_k(x) = \frac{x(x-1)(x-2)...(x-k+1)}{k!}$.
Now, for any $z \in \mathbb{Z}$ such that $0 \leq z < k$, $f_k(z) = 0 \in \mathbb{Z}$. Again, for any $z \in \mathbb{Z}$ such that $z \geq k$, we have $f_k(k+n) = \frac{(k+n)(k+n-1)(k+n-2)...(k+n-k+1)}{k!} = \binom{k+n}{k} \in \mathbb{Z}$ with $n = 0, 1, 2, ...$
Also, for any $z \in \mathbb{Z}$ such that $z < 0$, we have
$f_k(z) = (-1)^k \frac{(k-z-1)(k-z-2)(k-z-3)...(k-z-1-k+1)}{k!} = (-1)^k \binom{k-z-1}{k} \in \mathbb{Z}$.
Therefore, $f_k(\mathbb{Z}) \subseteq \mathbb{Z}$ for each $k = 0, 1, 2, ...$.

We have the following theorem:

Theorem 12. *([5], Proposition I. 1. 1.) Every element in $Int(\mathbb{Z})$ can be written uniquely as a $\mathbb{Z}$-linear combination of the binomial polynomials*
$\{f_k(x) : k = 0, 1, 2, ...\} = \{\binom{x}{k}\} = \{\prod_{i=0}^{k-1} \frac{x-i}{k-i}\}$.

Proof. Since for each $k = 0, 1, 2, ..., \binom{x}{k}$ is a polynomial of degree k, obviously $\{\binom{x}{k} : k = 0, 1, 2, ...\}$ forms a basis for the $\mathbb{Q}$-vector space $\mathbb{Q}[X]$. Lemma 5 shows that

$\{\binom{x}{k} : k = 0, 1, 2, ...\}$ are integer-valued polynomials. Thus, a $\mathbb{Z}$-linear combination of $\{\binom{x}{k} : k = 0, 1, 2, ...\}$ is in $Int(\mathbb{Z})$

Conversely, suppose that $f(x) \in Int(\mathbb{Z})$, and let $f(x) = \alpha_0 + \alpha_1 x + ... + \alpha_k \binom{x}{k}$, where $\alpha_i \in \mathbb{Q}$, $0 \leq i \leq k$.

Now, $f(0) = \alpha_0 \in \mathbb{Z}$. Suppose by induction on $l < k$ that $\alpha_i \in \mathbb{Z}$, for $i \leq l$. Then $g_l(x) = f(x) - \sum_{i=0}^{n} \alpha_i \binom{x}{i} \in Int(\mathbb{Z})$, and $g_l(x) = \alpha_{l+1}\binom{x}{l+1} + ... + \alpha_k \binom{x}{k}$.

Therefore, $\alpha_{l+1} = g_l(l+1) \in \mathbb{Z}$.

Therefore, f is a $\mathbb{Z}$-linear combination of $\binom{x}{k}$.

Hence the theorem.

2.7 Background about Integer-Valued Polynomials on a Subset

The ring $Int(S, D)$ is contained in $F[X]$. In spite of considering F as a quotient field of the domain D, we may choose a quotient field that contains S and smaller than F. In particular, if we assume S is a domain, then its quotient field, Q, (say) would be smaller than F. But the sizes of any two rings of integer-valued polynomials depend on the sizes of the two subsets of a quotient field with respect to which the polynomials are integer-valued. We make clear the fact by the following theorem:

Theorem 13. *([5], Proposition I. 1. 6 .) If $C \subseteq D$ are two domains having a quotient field F, and $S \subseteq T$ are two subsets of the quotient field F then $Int(T, C) \subseteq Int(S, D)$.*

From which, we have the following:

Corollary 2. *([5], Corollary I. 1. 7 .) If S is a subset of the quotient field F of the domain D then the following containments are equivalent:*
(i) $S \subseteq D$,
(ii) $Int(D) \subseteq Int(S, D)$,
(iii) $D[X] \subseteq Int(S, D)$.

Proof. Suppose that S is a subset of D. Then by Theorem 1, $D[X] \subseteq Int(D) \subseteq Int(S, D)$. Conversely suppose that $D[X] \subseteq Int(S, D)$. Then since the polynomials must have to be integer-valued on S, S is a subset of D.

2.8 Polynomial Closures

For any two distinct subsets S and T of the quotient field F of a domain D, the condition $Int(S, D) = Int(T, D)$ may hold. In particular, if S is a subset of the domain D, then the condition $Int(S, D) = Int(D)$ may hold. As for example, if we consider $S = \mathbb{N}$ and $D = \mathbb{Z}$ then $Int(\mathbb{N}, \mathbb{Z}) = Int(\mathbb{Z})$ (see [5], Corollary I.1.2).

It is very important to state the following lemma that points out some necessary definitions:

Lemma 6. *([5], Lemma IV.1.1.) Let S be a subset of the quotient field F of a domain D then $\bar{S} = \{x \in F : f(x) \in D \text{ for all } f \in Int(S, D)\}$ is the largest subset of F satisfying the condition $Int(S, D) = Int(\bar{S}, D)$.*

Definition 2.8.1. *(i) ([5], Definition IV.1.2.) Two subsets S and T of the quotient field F of a domain D are said to be polynomially D-equivalent or (simply polynomially equivalent) if $Int(S, D) = Int(T, D)$.*
(ii) Let S be a subset of the quotient field F of a domain D. Then the subset $\bar{S} = \{x \in F : f(x) \in D \text{ for all } f \in Int(S, D)\}$ of F is said to be the polynomial D-closure of S.
(iii) A subset S of the quotient field F of a domain D is called polynomially D-closed if $S = \bar{S}$, (where $Int(S, D) = Int(\bar{S}, D)$).
(iv) A subset S of a domain D is said to be a dense subset of D if $Int(S, D) = Int(D)$. Equivalently, a subset S of D is dense in D if and only if $\bar{S} = D$, where $\bar{S}$ is the polynomial D-closure of S.

Example 1. *([5], Example IV.1.3 .) If D is not a field then clearly the finite subsets of the quotient field F of D are polynomially closed whereas the cofinite subsets of D are dense in D (see [5], Proposition I.1.5).*

Remark 3. *([5], Remark IV.1.4.) Let $S \subseteq T \subseteq U$ be three subsets of the quotient field F of a domain D. Then $Int(S, D) = Int(U, D)$ if and only if $Int(S, D) = Int(T, D)$ and $Int(T, D) = Int(U, D)$. However, if T and U are domains then $Int(S, U) = Int(U)$ but $Int(S, T) \neq Int(T)$, i.e., S is polynomially dense in U but not in T.*

We mostly require to state the following basic properties of polynomial closure:

Theorem 14. *([5], Proposition IV. 1. 5.)*
(i) For each subset S of the quotient field F of a domain D, $\bar{\bar{S}} = \bar{S}$.
(ii) If S and T are two subsets of the quotient field F of a domain D such that $S \subseteq T$ then $\bar{S} \subseteq \bar{T}$.
(iii) For any family $\{S_k\}$ of subsets of the quotient field F of a domain D, $\overline{\bigcap_k S_k} \subseteq \bigcap_k \bar{S}_k$ and $\bigcup_k \bar{S}_k \subseteq \overline{\bigcup_k S_k}$.
(iv) For any subset S of F, $x\bar{S} = \overline{xS}$ and $x + \bar{S} = \overline{x+S}$, for all $x \in F$.

Example 2. *Let $S_1 = (2)$ and $S_2 = (3)$. Then $\bar{S}_1 = (\bar{2}) = (2) = S_1$ because $x/2 \in Int((2))$, and if k is odd then $k/2 \notin \mathbb{Z}$. Similarly, $\bar{S}_2 = (\bar{3}) = (3) = S_2$, and so $\bar{S}_1 \cup \bar{S}_2 = S_1 \cup S_2 \neq \mathbb{Z}$ since $7 \notin S_1 \cup S_2 = (2) \cup (3)$.*
Also, the 2-adic and 3-adic closures of $S_1 \cup S_2 = (2) \cup (3)$ are $\mathbb{Z}$.
We will show in section 2.9 that $Int((2) \cup (3)) = Int(\mathbb{Z})$.
Also, ([4], Remark 1.3.2), if we let $S_1 = \{z \in \mathbb{Z} : z \geq 0\}$ and $S_2 = \{z \in \mathbb{Z} : z \leq 0\}$. Then the polynomial closures of both S_1 and S_2 are $\mathbb{Z}$ and so their intersection is $\mathbb{Z}$. But the intersection of S_1 and S_2 is $\{0\}$ whose closure is also $\{0\}$.

Remark 4. *([5], Remark IV. 1. 6). The inclusions in (iii) are strict in general.*

2.9 Relation between Polynomial Closures and P-adic Closures

Definition 2.9.1. *Let R be a ring. The intersection of maximal ideals of R is called the Jacobson radical of R. A Noetherian ring equipped with P-adic topology R is called a Zariski ring if the ideal P of R is contained in the Jacobson radical of R.*

Theorem 15. *([5], Theorem IV. 1. 12.) If D is a Zariski domain, then the topological closure of a fractional subset S of R in the quotient field F of D is contained in the polynomial D-closure of S.*

Proof. Let S be a subset of D, and let $\bar{S}_t$ be the topological closure of S in the P-adic topology. Let $f \in Int(S, D)$, and let $x \in \bar{S}_t$. We need to show that $f(x) \in D$. Let $d \in D$ with $d \neq 0$ satisfying $df \in D[X]$. For every n, we have $y \in S$ satisfying $x - y \in P^n$. Since $(df(x) - df(y))$ is divisible by $x - y$ in D, then $(df(x) - df(y)) \in P^n$. Now, since $df(y) \in dD$, clearly $df(x) \in dD + P^n$. Thus, $df(x)$ belongs to the topological closure of the ideal dD, where the topological closure of dD is itself due to D being a Zariski ring. Therefore, $df(x) \in dD$ leaving $f(x) \in D$.

Corollary 3. *([5], Corollary IV. 1. 13.) Let D be a Zariski domain. Then*
(i) Every topological dense subset S of D is also a polynomially dense subset of D.
(ii) Every polynomially closed fractional subset S of D is also topologically closed in the quotient field F of D.

It is noted that Theorem 15 and Corollary 3 are applied in the case of D to be a Noetherian local ring with respect to the m-adic topology having m as maximal ideal of D.

2.10 p-Orderings and the Associated p-Sequences

p-Ordering ([2], section 4.) Let S be an arbitrary subset of $\mathbb{Z}$, and let p be a fixed prime number. A sequence $\{a_i\}_{i=0}^{\infty}$ of elements of S is said to be a p-ordering of S if it is constructed by maintaining the following steps:
Step 0: Pick an element $a_0 \in S$;
Step 1: Pick any element $a_1 \in S$ that minimizes the highest power of p dividing $a_1 - a_0$;
Step 2: Pick any element $a_2 \in S$ that minimizes the highest power of p dividing $(a_2 - a_0)(a_2 - a_1)$;
.
.
.
Step k: Pick the kth element $a_k \in S$ that minimizes the highest power of p dividing $(a_k - a_0)(a_k - a_1)...(a_k - a_{k-1})$.
It is necessary to note that the p-ordering of elements of S depends on the choices of initial element a_0 of the sequence $\{a_i\}_{i=0}^{\infty}$, i.e., for different choices of a_0 the p-orderings must be different.
The following examples illustrate the truth of the above statement:

Example 3. *Let $S = \{2z : z \in \mathbb{Z}\}$. Then at $a_0 = 2$ and $a_0 = 4$ the p-orderings of S are $\{2, 0, 4, 6, 8, 10, 12, \cdots\}$ and $\{4, 2, 0, 6, 8, 10, 12, \cdots\}$ respectively for all primes p simultaneously.*

Example 4. *Let $S = \{2^z : z \in \mathbb{Z}\}$. Then at $a_0 = 1$ and $a_0 = 2$ the p-orderings of S are $\{1, 2, 4, 8, \cdots\}$ and $\{2, 1, 4, 8, \cdots\}$ respectively for all primes p simultaneously.*

Example 5. *Let $S = \{z^2 : z \in \mathbb{Z}\}$. Then at $a_0 = 1$ and $a_0 = 4$ the p-orderings of S are $\{1, 0, 4, 9, \cdots\}$ and $\{4, 0, 1, 9, \cdots\}$ respectively for all primes p simultaneously.*

Example 6. *Let $S = \mathfrak{F} = \{1, 2, 3, 5, 8, 13, 21, ...\}$, the Fibonacci numbers, then at $a_0 = 3$ and $a_0 = 21$ with $p = 2$, the p-orderings of S are $\{3, 2, 1, 8, 5, 55, 34, 13, 89, 21, ...\}$ and $\{21, 2, 8, 55, 89, 3, 34, 1, 13, 5, ...\}$ respectively.*

The Associated p-Sequence([2], section 4.) If $\{a_i\}_{i=0}^{\infty}$ is a p-ordering of an arbitrary subset S of $\mathbb{Z}$ then the monotonically increasing sequence $\{\nu_k(S,p)\}_{k=0}^{\infty}$ of powers of p such that the kth element $\nu_k(S,p)$ is the power of p for which a_k minimizes $p^{\nu_k(S,p)}$ dividing $(a_k - a_0)(a_k - a_1)...(a_k - a_{k-1})$ in the p-ordering process is known as the associated p-sequence corresponding to the chosen p-ordering $\{a_i\}_{i=0}^{\infty}$ of S.
We feel more important to note that for any fixed prime p the associated p-sequence of a subset S is invariant to all p-orderings of S. For verification of this, we need to state and prove the following theorem:

Theorem 16. *(see [2], Theorem 5.) The associated p- sequence of S does not depend on the choice of p-ordering of S.*

Before proving the theorem, we need the following definition and the statements of some theorems:

Definition 2.10.1. *([2], Definition 7.) If S is a subset of $\mathbb{Z}$, then the factorial function of S is denoted by $K!_S$ and is defined by*
$k!_S = \prod_p \nu_k(S,p)$.

Definition 2.10.2. *Let S be a subset of $\mathbb{Z}$, and let f be a primitive polynomial. Then the fixed divisor of f over S is denoted by $d(S,f)$, and is defined by*
$d(S,f) = gcd\{f(a) : a \in S\}$.

Theorem 17. *([2], Theorem 9.) If f is a primitive polynomial of degree k, and $d(S,f)$ is the fixed divisor of f over a subset S of $\mathbb{Z}$, then $d(S,f)|k!_S$.*

Theorem 18. *([2], Theorem 10.) If S is a subset of $\mathbb{Z}$, and $a_0, a_1, \cdots, a_n \in S$ are any $n+1$ integers, then the product $\prod_{i<j}(a_i - a_j)$ is a multiple of $0!_S 1!_S \cdots n!_S$.*

Theorem 19. *([2], Theorem 11.) Let S be a subset of $\mathbb{Z}$. Then $\prod_{k=0}^{n-1} \frac{n}{gcd(n, k!_S)}$ is the number of polynomial functions from S to $\mathbb{Z}/n\mathbb{Z}$.*

Proof. (Proof of Theorem 16). Since the Theorems 17 - 19 did not mention p-orderings except generalized factorials, the definition 2.10.1 of factorials can not have depended on any choices of p-ordering.

Theorem 20. *([2], Proposition 6.) The set $\{0, 1, 2, 3, ...\}$ of nonnegative integers forms a p-ordering of the set of integers, $\mathbb{Z}$, for all prime numbers p simultaneously.*

Proof. Suppose $a_{k-1} = k - 1$ minimizes the highest power of any prime p dividing $(a_{k-1} - 0)(a_{k-1} - 1)...(a_{k-1} - (k - 2))$. We want to show that $a_k = k$ minimizes the highest power of any prime p diving $(a_k - 0)(a_k - 1)...(a_k - (k - 1))$. For, since $E(x) = (x - 0)(x - 1)...(x - (k - 1))$ is the product of k consecutive integers, it must be a multiple of $k!$ by Pascal's triangle. Also, when $x = k$, $E(k) = k!$. Thus, $x = k$ minimizes the power of p dividing $E(k)$. Therefore, at the kth step we consider $a_k = k$ and the claim follows due to induction.

Corollary 4. *The sequence $[0, 0, 0, \cdots, p - terms, 1, 1, 1, \cdots, p - terms, 2, 2, 2, \cdots, p - terms, \cdots]$ is the associated p-sequence of $\mathbb{Z}$ corresponding to the p-ordering $\{0, 1, 2, 3, ...\}$.*

Example 7. *Let $S = \{2z : z \in \mathbb{Z}\}$. Suppose $a_{k-1} = 2(k - 1)$ minimizes the highest power of any prime p dividing $(a_{k-1} - 0)(a_{k-1} - 2)(a_{k-1} - 4) \cdots (a_{k-1} - 2(k - 2))$. Let $E(x) = (x - 0)(x - 2)(x - 4) \cdots (x - 2(k - 1))$. We see that $E(2k) = (2k - 0)(2k - 2) \cdots (2k - 2(k - 1)) = 2^k k!$, which is a product of k consecutive integers and so is a multiple of $k!$ by Pascal's triangle. Thus, $x = 2k$ minimizes the power of p dividing $E(2k)$. Therefore, $\{0, 2, 4, 6, ...\}$ is a p-ordering of S and the corresponding associated p-sequence is for all primes p simultaneously. The corresponding associated 2-sequence of S is $\{0, 1, 3, 4, 7, 8, 10, \cdots\}$.*

Example 8. *Let $S = \{2^z : z \in \mathbb{Z}\}$. Suppose $a_{k-1} = 2^{k-1}$ minimizes the highest power of any prime p dividing $(a_{k-1} - 1)(a_{k-1} - 2)(a_{k-1} - 4)(a_{k-1} - 8) \cdots (a_{k-1} - 2^{k-2})$. Let $E(x) = (x - 1)(x - 2)(x - 4)(x - 8) \cdots (x - 2^{k-1})$. We see that $E(2^k) = (2^k - 1)(2^k - 2)(2^k - 8) \cdots (2^k - 2^{k-1})$ is a product of k consecutive integers and so is a multiple of $k!$ by Pascal's triangle.Thus, $x = 2^k$ minimizes the power of p dividing $E(2^k)$. Therefore, $\{1, 2, 4, 8, ...\}$ is a p-ordering of S for all primes p simultaneously. The associated p-sequence of S is $\{0, 0, 0, \cdots (p-1)terms, 1, 1, 1, \cdots (p-1)terms, 2, 2, 2, \cdots (p-1)terms, \cdots\}$.*

Example 9. *Let* $S = \{z^2 : z \in \mathbb{Z}\}$. *Suppose* $a_{k-1} = (k-1)^2$ *minimizes the highest power of any prime* p *dividing* $(a_{k-1}-0)(a_{k-1}-1)(a_{k-1}-4)\cdots(a_{k-1}-(k-2)^2)$. *Let* $E(x) = (x-0)(x-1)(x-4)\cdots(x-(k-1)^2)$. *We see that* $E(k^2) = (k^2-0)(k^2-1)(k^2-4)\cdots(k^2-(k-1)^2)$, *which is a product of* k *consecutive integers and so is a multiple of* $k!$ *by Pascal's triangle. Thus,* $x = k^2$ *minimizes the power of* p *dividing* $E(k^2)$. *Therefore,* $\{0, 1, 4, 9, ...\}$ *is a* p*-ordering of* S *for all primes* p *simultaneously. The associated* 2*-sequence of* S *is* $\{0, 0, 2, 3, 6, 7, 9, 10, 14, \cdots\}$.

Maplecode 1 provides p-orderings as well as the corresponding associated p-sequences. As for example, we input the first 30-terms of the sequence of Lucas numbers, the initial element $a_0 = 2$, and a prime $p = 3$ as follows:
porder(L, 3, 1); and we get a p-ordering $[2, 1, 3, 4, 18, 521, 7, 123, 1364, 11, 76, 843, 199, 5778, 47, 322, 39603, 24476, 64079, 271443, 9349, 167761, 29, 439204, 2207, 15127, 1149851, 3571, 103682, 710647]$ and the associated p-sequence $[0, 0, 0, 1, 1, 1, 2, 2, 2, 4, 4, 4, 5, 5, 6, 6, 6, 7, 8, 8, 8, 9, 10, 11, 11, 13, 14, 16, 18, 20, 23]$.
A reasonable question at this point is how much the p-ordering of the finite sequence, $\{\mathfrak{L}_k\}$, the first k terms of Lucas numbers, of Lucas numbers agrees with that of $\mathfrak{L}$?

Definition 2.10.3. *The period of a periodic sequence* $\{A_n : n \geq 0\}$ *is the smallest* k *for which there exists an* m *such that* $A_{n+k} = A_n$ *for all* $n \geq m$.

Lemma 7. *If* $\{a_n\}$ *is defined by* $a_{n+1} = C_1 \cdot a_n + C_2 \cdot a_{n-1} + \cdots + C_k \cdot a_{n-k} mod\ p^l$, *then* $\{a_n\}$ *is periodic.*

Proof. Consider the set of k-tuples modulo p^l. Then the set is finite. So, some k-tuple must occur twice in the subsequences of length k in $\{a_n\}$. Suppose $\{a_{n_1+1}, a_{n_1+2}, \cdots a_{n_1+k}\}$ and $\{a_{n_2+1}, a_{n_2+2}, \cdots a_{n_2+k}\}$ are the same. Then, since the sequence is defined by a recurrence of length k, we must have $a_{n_1+i} = a_{n_2+i}$ for all i. Thus the sequence $\{a_n\}$ is periodic with period that divides $n_2 - n_1$.

Corollary 5. *For any prime* p *and integer* k *the Lucas sequence modulo* p^k *is periodic.*

Proof. For any prime p and integer k, there are p^{2k} possible pairs of Lucas numbers modulo p^k. Then by the pigeonhole principle, after $p^{2k}+1$ terms a pair must repeat. Also, if a pair repeats once, then it must repeat again.
Therefore, the Lucas sequence modulo p^k is periodic.

Lemma 8. *Let $\{\mathfrak{L}_k\}$ be a sequence of Lucas numbers, and let p be a prime number. If the sequence $\{\mathfrak{L}_k\}$ is periodic modulo p for $k \geq m$, then it is periodic modulo p for all $k \geq 0$, and similarly for the Fibonacci numbers.*

Proof. Since $\{\mathfrak{L}_k\}$ is periodic modulo p for $k \geq m$ with a period l (say), $\mathfrak{L}_k \equiv \mathfrak{L}_{k+l} \pmod{p}$ for $k \geq m$. Then $\mathfrak{L}_{k+1} \equiv \mathfrak{L}_{k+1+l} \pmod{p}$. By recurrence relation, we have $\mathfrak{L}_{k+1} = \mathfrak{L}_k + \mathfrak{L}_{k-1}$. So $\mathfrak{L}_{k-1} = \mathfrak{L}_{k+1} - \mathfrak{L}_k \equiv (\mathfrak{L}_{k+1+l} - \mathfrak{L}_{k+l}) \pmod{p} \equiv \mathfrak{L}_{k-1+l} \pmod{p}$. This shows that if the sequence $\{\mathfrak{L}_k\}$ is periodic modulo p for $k \geq m$, then it is also periodic modulo p for $k \geq m-1$. Now, $\mathfrak{L}_{k-2} = \mathfrak{L}_k - \mathfrak{L}_{k-1} \equiv (\mathfrak{L}_{k+l} - \mathfrak{L}_{k-1+l}) \pmod{p} \equiv \mathfrak{L}_{k-2+l} \pmod{p}$, showing $\{\mathfrak{L}_k\}$ is periodic modulo p for $k \geq m-2$. If we proceed m times in this way, then we get $\mathfrak{L}_{k-m} = \mathfrak{L}_{k-m+2} - \mathfrak{L}_{k-m+1} \equiv (\mathfrak{L}_{k-m+2+l} - \mathfrak{L}_{k-m+1+l}) \pmod{p} \equiv \mathfrak{L}_{k-m+l} \pmod{p}$, showing $\{\mathfrak{L}_k\}$ is periodic modulo p for $k \geq 0$. The proof for the Fibonacci numbers is similar. Hence this establishes the lemma.

Lemma 9. *Let $\{\mathfrak{F}_k\}$ be the sequence of Fibonacci numbers, and let $\{\mathfrak{L}_k\}$ be the sequence of Lucas numbers with integers $k \geq 0$. Then $\mathfrak{L}_k = \mathfrak{F}_{k-1} + \mathfrak{F}_{k+1}$ for all $k \geq 1$.*

Proof. We know that for all integers $k \geq 1$, $\mathfrak{F}_{k+1} = \mathfrak{F}_k + \mathfrak{F}_{k-1}$ with $\mathfrak{F}_0 = 0$, $\mathfrak{F}_1 = 1$. We will prove the lemma by induction on k. Let $k = 1$. Then $\mathfrak{F}_2 + \mathfrak{F}_0 = 1 + 0 = 1 = \mathfrak{L}_1$. Similarly, for $k = 2$, $\mathfrak{F}_3 + \mathfrak{F}_1 = \mathfrak{F}_2 + 2\mathfrak{F}_1 = 1 + 2 \cdot 1 = 3 = \mathfrak{L}_2$.
Suppose $\mathfrak{L}_n = \mathfrak{F}_{n+1} + \mathfrak{F}_{n-1}$ holds for all $n < k$. Then $\mathfrak{L}_k = \mathfrak{L}_{k-1} + \mathfrak{L}_{k-2} = (\mathfrak{F}_k + \mathfrak{F}_{k-2}) + (\mathfrak{F}_{k-1} + \mathfrak{F}_{k-3}) = (\mathfrak{F}_k + \mathfrak{F}_{k-1}) + (\mathfrak{F}_{k-2} + \mathfrak{F}_{k-3}) = \mathfrak{F}_{k+1} + \mathfrak{F}_{k-1}$ as required.
Therefore, $\mathfrak{L}_k = \mathfrak{F}_{k+1} + \mathfrak{F}_{k-1}$ for all $k \geq 1$.

Lemma 10. *Let $\{\mathfrak{F}_k\}$ be the sequence of Fibonacci numbers, and let $\{\mathfrak{L}_k\}$ be the sequence of Lucas numbers with integers $k \geq 0$. Then $\mathfrak{F}_k = \frac{\mathfrak{L}_{k-1} + \mathfrak{L}_{k+1}}{5}$ for all $k \geq 1$.*

Proof. The proof of this lemma is similar to lemma 9.

Lemma 11. *Let $\{\mathfrak{F}_k\}$ be the sequence of Fibonacci numbers, and let $\{\mathfrak{L}_k\}$ be the sequence of Lucas numbers with integers $k \geq 0$. If l is the period of $\{\mathfrak{L}_k\}$ mod p, then it is also the period of $\{\mathfrak{F}_k\}$ mod p with any prime p, and conversely.*

Proof. Since l is the period of the sequence of Lucas numbers mod p, $\mathfrak{L}_{l-1} \equiv \mathfrak{L}_0 \pmod{p}$ and $\mathfrak{L}_l \equiv \mathfrak{L}_1 \pmod{p}$. Then $\mathfrak{L}_{l+1} = \mathfrak{L}_l + \mathfrak{L}_{l-1} \equiv (\mathfrak{L}_1 + \mathfrak{L}_0) \pmod{p} \equiv \mathfrak{L}_2 \pmod{p}$ and

$\mathfrak{L}_{l+2} = \mathfrak{L}_{l+1} + \mathfrak{L}_l \equiv (\mathfrak{L}_2 + \mathfrak{L}_1) \pmod{p} \equiv \mathfrak{L}_3 \pmod{p}$. Due to lemma 10, $\mathfrak{F}_l = \frac{\mathfrak{L}_{l-1}+\mathfrak{L}_{l+1}}{5}$ for all $l \geq 1$. Now, $\mathfrak{F}_l = \frac{\mathfrak{L}_{l-1}+\mathfrak{L}_{l+1}}{5} \equiv (\frac{\mathfrak{L}_0+\mathfrak{L}_2}{5}) \pmod{p} \equiv (\frac{\mathfrak{L}_2+\mathfrak{L}_0}{5}) \pmod{p} \equiv \mathfrak{F}_1 \pmod{p}$ and $\mathfrak{F}_{l+1} = \frac{\mathfrak{L}_{l+2}+\mathfrak{L}_l}{5} \equiv (\frac{\mathfrak{L}_3+\mathfrak{L}_1}{5}) \pmod{p} \equiv \mathfrak{F}_2 \pmod{p}$. Therefore, l is the period of $\{\mathfrak{F}_k\}$ mod p. The proof of the converse part is straightforward.

Theorem 21. *If p is any prime and $a \equiv 1 \pmod{p}$, then $a^{p^k} \equiv 1 \pmod{p^{k+1}}$ for any integer $k \geq 0$.*

Proof. We will prove this theorem by induction on k. Since $a \equiv 1 \pmod{p}$, $a = 1 + zp$ for some $z \in \mathbb{Z}$. Then $a^p = (1 + zp)^p = 1 + zp^2 + \sum_{i=2}^{p-1} \binom{p}{i} (zp)^i \equiv 1 \pmod{p^2}$ since $p^2 | (zp)^i$ for $2 \leq i \leq p$. Thus $a^{p^k} \equiv 1 \pmod{p^{k+1}}$ holds for $k = 1$. Suppose this holds for $k = n$ with any integer $n > 1$, i.e., $a^{p^n} \equiv 1 \pmod{p^{n+1}}$. Then $a^{p^n} = 1 + z_1 p^{n+1}$ for some $z_1 \in \mathbb{Z}$. Now, $a^{p^{n+1}} = (a^{p^n})^p = (1 + z_1 p^{n+1})^p = 1 + \binom{p}{1} z_1 p^{n+1} + \sum_{i=2}^{p} \binom{p}{i} (z_1 p^{n+1})^i = 1 + z_1 p^{n+2} + \sum_{i=2}^{p} \binom{p}{i} (z_1 p^{n+1})^i \equiv 1 \pmod{p^{n+2}}$ since $p^{n+2} | (z_1 p^{n+1})^i$ for $2 \leq i \leq p$. Thus $a^{p^k} \equiv 1 \pmod{p^{k+1}}$ holds for $k = n + 1$. Hence the theorem follows by induction.

Corollary 6. *If p is any prime, and l is the period of $\{\mathfrak{F}_k\}$, the sequence of Fibonacci numbers, mod p, then the sequence is periodic with period dividing lp^{k-1} modulo p^k for any integer $k \geq 1$.*

Proof. Since l is the period of $\{\mathfrak{F}_k\}$ mod p, $\mathfrak{F}_l \equiv \frac{\tau^l - \bar{\tau}^l}{\sqrt{5}} \equiv \mathfrak{F}_0 \equiv 0 \pmod{p}$, and so $\tau^l \equiv \bar{\tau}^l \pmod{p}$. Since $\mathfrak{F}_l \equiv \mathfrak{F}_0 \pmod{p}$ and $\mathfrak{F}_{l+1} \equiv \mathfrak{F}_1 \pmod{p}$, $\mathfrak{F}_{l-2} \equiv \mathfrak{F}_0 \pmod{p}$ and $\mathfrak{F}_{l-1} \equiv \mathfrak{F}_1 \pmod{p}$, and so using $\tau^l \equiv \bar{\tau}^l \pmod{p}$, we have $\mathfrak{F}_l = \mathfrak{F}_{l+1} - \mathfrak{F}_{l-1} = \mathfrak{F}_{l+1} - \mathfrak{F}_1 = \frac{\tau^{l+1} - \bar{\tau}^{l+1}}{\sqrt{5}} - \frac{\tau - \bar{\tau}}{\sqrt{5}} = \frac{\tau(\tau^l - 1) - \bar{\tau}(\bar{\tau}^l - 1)}{\sqrt{5}} = \frac{\tau(\tau^l - 1) - \bar{\tau}(\tau^l - 1)}{\sqrt{5}} = (\tau^l - 1)\frac{(\tau - \bar{\tau})}{\sqrt{5}} = (\tau^l - 1)\mathfrak{F}_1 = (\tau^l - 1) \equiv 0 \pmod{p}$. Similarly, $\mathfrak{F}_l = (\bar{\tau}^l - 1) \equiv 0 \pmod{p}$. Thus $\tau^l \equiv \bar{\tau}^l \equiv 1 \pmod{p}$, and therefore by Theorem 21, $\tau^{lp^{k-1}} \equiv \bar{\tau}^{lp^{k-1}} \equiv 1 \pmod{p^k}$. Now, $\mathfrak{F}_{lp^{k-1}} = \frac{\tau^{lp^{k-1}} - \bar{\tau}^{lp^{k-1}}}{\sqrt{5}} \equiv 0 \pmod{p^k} \equiv \mathfrak{F}_0$, and $\mathfrak{F}_{lp^{k-1}+1} = \frac{\tau^{lp^{k-1}+1} - \bar{\tau}^{lp^{k-1}+1}}{\sqrt{5}} = \frac{\tau^{lp^{k-1}}\tau - \bar{\tau}^{lp^{k-1}}\tau + \bar{\tau}^{lp^{k-1}}\tau - \bar{\tau}^{lp^{k-1}}\bar{\tau}}{\sqrt{5}} = \frac{(\tau^{lp^{k-1}} - \bar{\tau}^{lp^{k-1}})\tau}{\sqrt{5}} + \bar{\tau}^{lp^{k-1}}\frac{\tau - \bar{\tau}}{\sqrt{5}} \equiv (0 \cdot \tau + 1 \cdot \mathfrak{F}_1) \pmod{p^k} \equiv \mathfrak{F}_1 \pmod{p^k}$. Therefore, the period of $\{\mathfrak{F}_k\}$ mod p^k divides lp^{k-1}.

Theorem 22. *Let p be a prime and $\{\mathfrak{L}_k\}$ be the sequence of Lucas numbers modulo p with period l. Then $\{\mathfrak{L}_k\}$ is periodic modulo p^k with period lp^{k-1} for $k \geq 1$.*

Proof. Since l is the period of the sequence of Lucas numbers, $\{\mathfrak{L}_k\}$, mod p, it is also the period of the sequence of Fibonacci numbers, $\{\mathfrak{F}_k\}$, mod p, by lemma 11. Then by Corollary 6, $\mathfrak{F}_{lp^{k-1}-1} \equiv \mathfrak{F}_0 \pmod{p^k}$ and $\mathfrak{F}_{lp^{k-1}} \equiv \mathfrak{F}_1 \pmod{p^k}$. Then $\mathfrak{F}_{lp^{k-1}+1} =$

$\mathfrak{F}_{lp^{k-1}} + \mathfrak{F}_{lp^{k-1}-1} \equiv \mathfrak{F}_1 + \mathfrak{F}_0 \pmod{p^k} \equiv \mathfrak{F}_2 \pmod{p^k}$ and $\mathfrak{F}_{lp^{k-1}+2} = \mathfrak{F}_{lp^{k-1}+1} + \mathfrak{F}_{lp^{k-1}} \equiv \mathfrak{F}_2 + \mathfrak{F}_1 \pmod{p^k} \equiv \mathfrak{F}_3 \pmod{p^k}$. But by lemma 9, we have $\mathfrak{L}_k = \mathfrak{F}_{k+1} + \mathfrak{F}_{k-1}$ for all $k \geq 1$. Then $\mathfrak{L}_{lp^{k-1}} = \mathfrak{F}_{lp^{k-1}+1} + \mathfrak{F}_{lp^{k-1}-1} \equiv \mathfrak{F}_2 + \mathfrak{F}_0 \pmod{p^k} \equiv \mathfrak{L}_1 \pmod{p^k}$ and $\mathfrak{L}_{lp^{k-1}+1} = \mathfrak{F}_{lp^{k-1}+2} + \mathfrak{F}_{lp^{k-1}} \equiv \mathfrak{F}_3 + \mathfrak{F}_1 \pmod{p^k} \equiv \mathfrak{L}_2 \pmod{p^k}$. Therefore, lp^{k-1} is the period of the sequence of Lucas numbers, $\{\mathfrak{L}_k\}$, mod p^k.

As for example, using Maplecode 2, we can verify the above Theorem.

Proposition 2. *For any k, the Lucas sequence, $\mathfrak{L}$, modulo p^k is periodic. Let the length of the period be $l(n)$. If $f(x) \in \mathbb{Q}[x]$, $f = \frac{g(x)}{p^k}$ with $g(x) \in \mathbb{Z}_p[x]$, and $f(x) \in \mathbb{Z}_p$ for all Lucas numbers $\mathfrak{L}_m$ for $m \leq l(n)$. Then $f(L) \subseteq \mathbb{Z}_p$.*

Proof. Let x and y be Lucas numbers such that $x \equiv y \pmod{p^k}$, and let $f(x) \in \mathbb{Z}_p$. We want to show that $f(y) \in \mathbb{Z}_p$. Since $x \equiv y \pmod{p^k}$, $y = x + p^k z$, for some $z \in \mathbb{Z}$. Now, for any n,

$$\begin{aligned} y^n &= (x + p^k z)^n \\ &= x^n + nx^{n-1}p^k z + \frac{n(n-1)}{2!}x^{n-2}p^{2k}z^2 + \frac{n(n-1)(n-2)}{3!}x^{n-3}p^{3k}z^3 + \cdots \\ &= x^n + p^k[nx^{n-1}z + \frac{n(n-1)}{2!}x^{n-2}p^k z^2 + \frac{n(n-1)(n-2)}{3!}x^{n-3}p^{2k}z^3 + \cdots]. \end{aligned}$$

This gives,

$$g(y) = g(x) + p^k[nx^{n-1}z + \frac{n(n-1)}{2!}x^{n-2}p^k z^2 + \frac{n(n-1)(n-2)}{3!}x^{n-3}p^{2k}z^3 + \cdots],$$

which implies

$$\frac{g(y)}{p^k} = \frac{g(x)}{p^k} + [nx^{n-1}z + \frac{n(n-1)}{2!}x^{n-2}p^k z^2 + \frac{n(n-1)(n-2)}{3!}x^{n-3}p^{2k}z^3 + \cdots]$$

with $[nx^{n-1}z + \frac{n(n-1)}{2!}x^{n-2}p^k z^2 + \frac{n(n-1)(n-2)}{3!}x^{n-3}p^{2k}z^3 + \cdots] \in \mathbb{Z}$.

Now, since $f(y) = \frac{g(y)}{p^k}$ and $f(x) = \frac{g(x)}{p^k}$, we have

$$f(y) = f(x) + [nx^{n-1}z + \frac{n(n-1)}{2!}x^{n-2}p^k z^2 + \frac{n(n-1)(n-2)}{3!}x^{n-3}p^{2k}z^3 + \cdots]$$

with $[nx^{n-1}z + \frac{n(n-1)}{2!}x^{n-2}p^k z^2 + \frac{n(n-1)(n-2)}{3!}x^{n-3}p^{2k}z^3 + \cdots] \in \mathbb{Z}$ and so $f(y) \in \mathbb{Z}_p$.

Problem 1. *Let $\mathfrak{L}(n)$ be the first n-terms of Lucas numbers $\mathfrak{L}$. The associated p-sequence of $\mathfrak{L}(n)$ is not necessarily the first n-terms of the associated p-sequence of $\mathfrak{L}$, but the sequence will agree for the first m-terms for some $m < n$. How is m related to n?*

Our answer is given below:

Remark 5. *Given any n, we compute the p-sequence of $\mathfrak{L}(n)$, say, $[a_0, a_1, \cdots, a_n]$. Then we pick the largest k for which $l(k) < n$, where $l(k)$ is the period of $\mathfrak{L}$ modulo p^k. Now, we pick m such that $a_m \leq k$, then the p-sequence $[a_0, a_1, \cdots, a_m]$ of $\mathfrak{L}(n)$ will agree with the p-sequence of $\mathfrak{L}$.*

As for example, the associated 5-sequence of $\mathfrak{L}(50)$ is $[0, 0, 0, 0, 1, 1, 1, 1, 2, 2, 2, 2, 4, 4, 4, 4, 5, 5, 5, 5, 7, 7, 7, 7, 8, 8, 8, 9, 9, 9, 10, 10, 11, 11, 12, 12, 12, 12, 13, 13, 14, 14, 15, 15, 15, 15, 16, 16, 17, 18]$, and $[\mathfrak{L} \bmod 5^2] = [2, 1, 3, 4, 7, 11, 18, 4, 22, 1, 23, 24, 22, 21, 18, 14, 7, 21, 3, 24, 2, 1, 3, 4, 7, 11, 18, 4, 22, 1, 23, 24, 22, 21, 18, 14, 7, 21, 3, 24]$, and so $l(k) = l(2) = 20 < 50$. We can pick $m = 11$ such that $a_{11} \leq k(= 2)$. Then the sequence $[0, 0, 0, 0, 1, 1, 1, 1, 2, 2, 2, 2]$ will agree with the 5-sequence of $\mathfrak{L}$.

2.11 Method for Computing p-Orderings and the Associated p-Sequences by Shuffling

We can employ the following lemma as the method of computing p-sequences and constructing p-orderings for a commutative ring R:

Lemma 12. *([13], Lemma 5.1.) Let S_1 and S_2 be two disjoint subsets of a commutative ring R satisfying the property that $\nu(s_1 - s_2) = 0$ for any $s_1 \in S_1$ and $s_2 \in S_2$, and let $\{a_i\}$ be a p-ordering of $S_1 \cup S_2$. Then the subsequence of the p-ordering of $S_1 \cup S_2$ consisting of those elements of S_1 is a p-ordering of S_1 and the similar case for S_2. Conversely, if $\{b_i\}$ and $\{c_i\}$ are p-orderings of S_1 and S_2 respectively with their respective associated p-sequences β_i and γ_i, then the shuffle of β_i and γ_i gives the p-sequence of $S_1 \cup S_2$ into nondecreasing order, and the shuffle of $\{b_i\}$ and $\{c_i\}$ gives a p-ordering of $S_1 \cup S_2$.*

Proof. ([11], Proof of Lemma 3.5(a).) Let $\{a_i\}_{i=1}^m$ be a p-ordering of $S_1 \cup S_2$. Suppose

that $a_k \in S_1$ and $a_j \in S_2$ such that $a_k - a_j \not\equiv 0 \pmod{p}$. Then $\nu(a_k - a_j) = 0$, and so

$$\begin{aligned} d_k &= \nu(\prod_{j<k}(a_k - a_j)) \\ &= \nu(\prod_{j<k, a_j \in S_1}(a_k - a_j)). \end{aligned}$$

Also, if for $s \in S_1 \cup S_2$ such that $s \in S_1$ then

$$\begin{aligned} \nu(\prod_{j<k, a_j \in S_1}(s - a_j)) &= \nu(\prod_{j<k}(s - a_j)) \\ &\geq \nu(\prod_{j<k}(a_k - a_j)) \\ &= \nu(\prod_{j<k, a_j \in S_1}(a_k - a_j)), \end{aligned}$$

and thus a_k minimizes $\nu(\prod_{j<k, a_j \in S_1}(s - a_j))$ for each $s \in S_1$. Therefore, $\{a_i\}_{i=1}^m \cap S_1$ is a p-ordering of S_1, and $\{d_k : a_k \in S_1\}$ is the corresponding associated p-sequence of S_1. Similarly for S_2.

The nondecreasing order in the p-sequence follows from ([11], Lemma 3.3(b)).

Example 10. *Let* $S_1 = \{0, 5, 10, 15, 20, 25\}$ *and* $S_2 = \{1, 6, 11, 16, 21, 26\}$ *be two disjoint subsets of* $\mathbb{Z}$*, where* $s_1 - s_2 \not\equiv 0 mod\ 5$ *with* $s_1 \in S_1$ *and* $s_2 \in S_2$*.*

A 5*-orderings of* S_1 *starting with* 5 *is* $\{5, 0, 10, 15, 20, 25\}$*, and the corresponding associated* 5*-sequence of* S_1 *is* $\{0, 1, 2, 3, 4, 6\}$*.*

A 5*-ordering of* S_2 *starting with* 11 *is* $\{11, 1, 6, 16, 21, 26\}$*, and the corresponding associated* 5*-sequence of* S_2 *is* $\{0, 1, 2, 3, 4, 6\}$*.*

Now, the associated 5*-sequence of* $S_1 \cup S_2$ *is* $\{0, 0, 1, 1, 2, 2, 3, 3, 4, 4, 6, 6\}$*, whereas* 5*-ordering of* $S_1 \cup S_2$ *is* $\{5, 11, 0, 1, 10, 6, 15, 16, 20, 21, 25, 26\}$*.*

Chapter 3

Background on Fibonacci Numbers, Lucas Numbers and Linear Recurrence Sequences

3.1 Golden Ratio

([9]) The Golden ratio is denoted by τ and is defined by $\tau = (1 + \sqrt(5))/2$ to be an irrational number having value 1.61803 ... .
Certain irrational numbers can be written in the following form:
$r_{ir} = (a + \sqrt{b})/c$,
from which we can get τ by substituting $a = 1$, $b = 5$, and $c = 2$, and the other irrational numbers can be obtained by putting the values of a, b, and c. However, the golden ratio provides a number of interesting and important properties that make it unique among the set of irrational numbers.

3.2 Fibonacci Numbers

The sequence of Fibonacci numbers satisfies the following linear recurrence relation:

$$\mathfrak{F}_{k+1} = \mathfrak{F}_k + \mathfrak{F}_{k-1}, \tag{3.1}$$

where $k = 1, 2, 3, ...$, and $\mathfrak{F}_0 = 0$, $\mathfrak{F}_1 = 1$.
Suppose a solution of (3.1) is of the form $A \cdot x^k$.
Then, using this, we get
$x^2 - x - 1 = 0$ that yields $x = \frac{1 \pm \sqrt{5}}{2}$. We verify that both choices of x do give solutions of (3.1), and that any linear combination of them does also.
Then the explicit formula for the Fibonacci numbers may be expressed as

$$\mathfrak{F}_k = a(\frac{1 + \sqrt{5}}{2})^k + b(\frac{1 - \sqrt{5}}{2})^k \tag{3.2}$$

On substitution $k = 0$, 1 in (3.2) and using $\mathfrak{F}_0 = 0$, $\mathfrak{F}_1 = 1$, we have $a + b = 0$, $a(\frac{1+\sqrt{5}}{2}) + b(\frac{1-\sqrt{5}}{2}) = 1$. Solving these, we have $a = \frac{1}{\sqrt{5}}$, $b = -\frac{1}{\sqrt{5}}$, and so

$\mathfrak{F}_k = \frac{1}{\sqrt{5}}(\frac{1+\sqrt{5}}{2})^k - \frac{1}{\sqrt{5}}(\frac{1-\sqrt{5}}{2})^k$.
Let $\tau_1 = \frac{1+\sqrt{5}}{2}$ and $\tau_2 = \frac{1-\sqrt{5}}{2}$ so that $(x-\tau_1)(x-\tau_2) = x^2 - x - 1$. Then $\tau_1\tau_2 = -1$ and so $\tau = \tau_1 = \frac{-1}{\tau_2}$.
Therefore, the Binet's formula for Fibonacci numbers is of the form

$$\mathfrak{F}_k = \frac{1}{\sqrt{5}}(\tau)^k - \frac{1}{\sqrt{5}}(\frac{-1}{\tau})^k = \begin{cases} \frac{1}{\sqrt{5}}\tau^k - \frac{1}{\sqrt{5}}\frac{1}{\tau^k}, & \text{if k is even} \\ \frac{1}{\sqrt{5}}\tau^k + \frac{1}{\sqrt{5}}\frac{1}{\tau^k}, & \text{if k is odd} \end{cases} = \begin{cases} f_+(\tau^k), & \text{if k is even} \\ f_-(\tau^k), & \text{if k is odd} \end{cases},$$

where $f_+(z) = \frac{1}{\sqrt{5}}(z - \frac{1}{z})$, $f_-(z) = \frac{1}{\sqrt{5}}(z + \frac{1}{z})$ and $\tau = \frac{1+\sqrt{5}}{2}$ with $z = \tau^k$.

For $k = 0, 1, 2, ...$, we have that $\mathfrak{F}_k = f(\tau^k)$,
where $f : U \to \mathbb{Z}_p$ or $f : U^0(\sqrt{5}) \to \mathbb{Z}_p$ such that
$f(z) = \frac{1}{\sqrt{5}}(z - \frac{N(z)}{z})$,
and the norm $N(z) = 1$ or -1 if z is a square or not in (U or $U^0(\sqrt{5})$) respectively whereas U is the set of p-units in $\mathbb{Z}_p$ and $U^0(\sqrt{5}) = \{x + \sqrt{5}y \in U(\sqrt{5}) : x^2 - 5y^2 = \pm 1\}$.

3.3 Lucas Numbers

The sequence of Lucas numbers satisfies the following equation

$$\mathfrak{L}_{k+1} = \mathfrak{L}_k + \mathfrak{L}_{k-1}, \tag{3.3}$$

where $k = 1, 2, 3, ...$, and $\mathfrak{L}_0 = 2, \mathfrak{L}_1 = 1$.
Suppose a solution of (3.3) is of the form $A \cdot x^k$.
Then, using this, we get
$x^2 - x - 1 = 0$ leaving $x = \frac{1\pm\sqrt{5}}{2}$. We verify that both choices of x do give solutions of (3.3), and that any linear combination of them does also.
Then the explicit formula for the Lucas numbers may be written as

$$\mathfrak{L}_k = a(\frac{1+\sqrt{5}}{2})^k + b(\frac{1-\sqrt{5}}{2})^k \tag{3.4}$$

Putting k = 0,1 in (3.4) and using $\mathfrak{L}_0 = 2$, $\mathfrak{L}_1 = 1$, we have $a + b = 2$, $a(\frac{1+\sqrt{5}}{2}) + b(\frac{1-\sqrt{5}}{2}) = 1$. Solving $a + b = 2$ and $a(\frac{1+\sqrt{5}}{2}) + b(\frac{1-\sqrt{5}}{2}) = 1$, we have $a = b = 1$, and so $\mathfrak{L}_k = (\frac{1+\sqrt{5}}{2})^k + (\frac{1-\sqrt{5}}{2})^k$.
Let $\tau_1 = \frac{1+\sqrt{5}}{2}$ and $\tau_2 = \frac{1-\sqrt{5}}{2}$ so that $(x-\tau_1)(x-\tau_2) = x^2 - x - 1$. Then $\tau_1\tau_2 = -1$

and so $\tau = \tau_1 = \frac{-1}{\tau_2}$.

Then, Binet's formula for Lucas numbers can be written as

$$\mathfrak{L}_k = (\tau)^k + (\tfrac{-1}{\tau})^k = \begin{cases} \tau^k + \frac{1}{\tau^k}, & \text{if k is even} \\ \tau^k - \frac{1}{\tau^k}, & \text{if k is odd} \end{cases} = \begin{cases} f_+(\tau^k), & \text{if k is even} \\ f_-(\tau^k), & \text{if k is odd} \end{cases},$$

where $f_+(z) = z + \frac{1}{z}$, $f_-(z) = z - \frac{1}{z}$ and $\tau = \frac{1+\sqrt{5}}{2}$ with $z = \tau^k$.

For $k = 0, 1, 2, ...$, we get $\mathfrak{L}_k = f(\tau^k)$,

where $f : U \to \mathbb{Z}_p$ or $f : U^0(\sqrt{5}) \to \mathbb{Z}_p$ with

$f(z) = (z - \frac{N(z)}{z})$,

and the norm $N(z) = 1$ or -1 depending on whether z is a square or not in (U or $U^0(\sqrt{5})$) respectively while U is the set of p-units in $\mathbb{Z}_p$ and $U^0(\sqrt{5}) = \{x + \sqrt{5}y \in U(\sqrt{5}) : x^2 - 5y^2 = \pm 1\}$.

Chapter 4

Lucas Numbers as Images of the Maps f_+ and f_-

4.1 Closures of Images of f_+ and f_-

The sequence of Lucas numbers can be obtained from Binet's formula:

$$\mathfrak{L}_k = \begin{cases} f_+(\tau^k), & \text{if k is even} \\ f_-(\tau^k), & \text{if k is odd} \end{cases},$$

where $f_+(z) = z + \frac{1}{z}$, $f_-(z) = z - \frac{1}{z}$ and $\tau = \frac{1+\sqrt{5}}{2}$ with $z = \tau^k$.

It is noted that $< \tau >= \{\tau^k : k \in \mathbb{Z}\}$ is a multiplicative group generated by τ. In fact, it is a subgroup of $\mathbb{Q}[\sqrt{5}]$.

Now, if we take the domains $D_{f_+} = \{\tau^0, \tau^2, \tau^4, ...\}$ and $D_{f_-} = \{\tau^1, \tau^3, \tau^5, ...\}$ for the functions f_+ and f_-, respectively, then the union of their images Im_{f_+} and Im_{f_-} is exactly $\mathfrak{L}$, the sequence of Lucas numbers, as shown below:

D_{f_+}	τ^0	τ^2	τ^4	τ^6	τ^8	$\cdots$
Im_{f_+}	2	3	7	18	47	$\cdots$

D_{f_-}	τ^1	τ^3	τ^5	τ^7	τ^9	$\cdots$
Im_{f_-}	1	4	11	29	76	$\cdots$

Due to [14], if p is an odd prime such that $p \equiv 1, -1 \pmod 5$, then $\tau \in \mathbb{Z}_p$ and τ generates a dense subgroup in $U(\mathbb{Z}_p)$, the set of units in $\mathbb{Z}_p$ (here $\mathbb{Z}_p$ denotes the p-adic integers), with conditions that the mod p reduction of τ generates $U(\mathbb{Z}/(p))$, and $\tau^{p-1} \not\equiv 1 \pmod{p^2}$, its reduction modulo p^k generates $U(\mathbb{Z}/(p^k))$ for all $k > 0$. Thus, we may extend the maps f_+ and f_- having their domains squares and non-squares of $U(\mathbb{Z}_p)$, respectively. In fact, these domains separate $U(\mathbb{Z}_p)$ into two disjoint open subsets with respect to the p-adic metric and the images of the extended maps are the closures, $\bar{\mathfrak{L}}$, of $\mathfrak{L}$ with respect to the p-adic metric having the property $\bar{\mathfrak{L}}/(p^k) = \mathfrak{L}/(p^k)$ for any k.

If $p \equiv 2, -2 \pmod 5$, then $\tau \notin \mathbb{Z}_p$ and we take a quadratic extension $\mathbb{Z}_p[\sqrt{5}]$ having members $\{x + \sqrt{5}y : x, y \in \mathbb{Z}_p\}$ with the usual addition and multiplication and possessing a norm $|x + \sqrt{5}y| = x^2 - 5y^2$. With respect to this norm and all elements of the subgroup generated by τ are of norm ± 1. If we denote the subgroup of units in $\mathbb{Z}_p$ with norm ± 1 by $U^0(\mathbb{Z}_p[\sqrt{5}])$, then the new version of the previous two conditions are the reduction of τ mod p generates $U^0(\mathbb{Z}[\sqrt{5}]/(p))$ and $\tau^{2(p+1)} \not\equiv 1 \pmod{p^2}$ and τ generates a dense subgroup of $U^0(\mathbb{Z}_p[\sqrt{5}])$ under these conditions. The squares and nonsquares in $U^0(\mathbb{Z}_p[\sqrt{5}])$ separate it into two disjoint open subsets with respect to the p-adic topology.

We describe $\bar{\mathfrak{L}}$ and $\bar{\mathfrak{L}}/(p^k)$ by applying Hensel's lemma (Lemma 3) or the Generalized Hensel's Lemma (Lemma 4) to the functions f_+ and f_-.
We restate the Hensel's Lemma and the Generalized Hensel's lemma as follows:

Lemma 13. *Let $f(x) \in \mathbb{Z}_p[x]$ or $\mathbb{Z}_p[\sqrt{5}][x]$ with formal derivative $f'(x)$, and z_0 is such that $f(z_0) \equiv 0 \pmod p$ and $f'(z_0) \not\equiv 0 \pmod p$, then there exists $z \in \mathbb{Z}_p$ or $\mathbb{Z}_p[\sqrt{5}]$ such that $z \equiv z_0 \pmod p$ and $f(z) = 0$.*

Lemma 14. *Let $f(x) \in \mathbb{Z}_p[x]$ or $\mathbb{Z}_p[\sqrt{5}][x]$ be a polynomial and let $z_0 \in \mathbb{Z}_p$ or $\mathbb{Z}_p[\sqrt{5}]$ such that $f'(z_0) \equiv 0 \pmod{p^M}$ but $f'(z_0) \not\equiv 0 \pmod{p^{M+1}}$, and $f(z_0) \equiv 0 \pmod{p^{2M+1}}$. Then there exists a unique element $z \in \mathbb{Z}_p$ or $\mathbb{Z}_p[\sqrt{5}]$ such that $z \equiv z_0 \pmod{p^{M+1}}$ and $f(z) = 0$.*

We compute $f_+(z_0)$ and $f_-(z_0)$ for primes p with $\mathbb{Z}_p$ by using Maplecode 3.
When $p = 7$, the length of a period of Lucas numbers modulo p is 16.

$2i$	0	2	4	6	8	10	12
$z_0 = \tau^{2i} \bmod 7$	1	$5 + 4\sqrt{5}$	$5\sqrt{5}$	$2 + 4\sqrt{5}$	6	$2 + 3\sqrt{5}$	$2\sqrt{5}$
$f_+(z_0) = f_+(\tau^{2i}) \bmod 7$	2	3	0	4	5	4	0
$f'_+(z_0) = f'_+(\tau^{2i}) \bmod 7$	0	$1 + 5\sqrt{5}$	2	$1 + 2\sqrt{5}$	0	$1 + 5\sqrt{5}$	2

$2i$	14
$z_0 = \tau^{2i} \bmod 7$	$5 + 3\sqrt{5}$
$f_+(z_0) = f_+(\tau^{2i}) \bmod 7$	3
$f'_+(z_0) = f'_+(\tau^{2i}) \bmod 7$	$1 + 2\sqrt{5}$

Since $f_+(z_0) \equiv 3 \pmod 7$ and $f'_+(z_0) \not\equiv 0 \pmod 7$ for $z_0 = \tau^{2i}$ with $2i = 2$ and 14, by Lemma 13, if $w \equiv 3 \pmod 7$, then there exists z with $z \equiv z_0 \pmod 7$ and $f_+(z) = w$ at $z_0 = \tau^{2i}$ for $2i = 2$ or 14. Similarly, $f_+(z_0) \equiv 0 \pmod 7$ and $f'_+(z_0) \not\equiv 0 \pmod 7$ for $z_0 = \tau^{2i}$ with $2i = 4$ and 12, so, if $w \equiv 0 \pmod 7$, then there exists z with $z \equiv z_0 \pmod 7$ and $f_+(z) = w$ at $z_0 = \tau^{2i}$ for $2i = 4$ or 12; $f_+(z_0) \equiv 4 \pmod 7$ and $f'_+(z_0) \not\equiv 0 \pmod 7$ for $z_0 = \tau^{2i}$ with $2i = 6$ and 10, hence, if $w \equiv 4 \pmod 7$, then there exists z with $z \equiv z_0 \pmod 7$ and $f_+(z) = w$ at $z_0 = \tau^{2i}$ for $2i = 4$ or 10. Therefore, the 7-adic closure of the images of f_+ contains the cosets $(3 + 7\mathbb{Z}) \cup (7\mathbb{Z}) \cup (4 + 7\mathbb{Z})$.

Since $f_+(z_0) \equiv 2 \pmod 7$ and $f'_+(z_0) \equiv 0 \pmod 7$ for $z_0 = \tau^0$, the image of f_+ will contain part of the coset $(2 + 7\mathbb{Z})$. Similarly, $f_+(z_0) \equiv 5 \pmod 7$ and $f'_+(z_0) \equiv 0 \pmod 7$ for $z_0 = \tau^8$, the image of f_+ will contain part of the coset $(5 + 7\mathbb{Z})$. We will examine this case more closely later.

$2i+1$	1	3	5	7	9
$z_0 = \tau^{2i+1} \bmod 7$	$4+4\sqrt{5}$	$2+\sqrt{5}$	$2+6\sqrt{5}$	$4+3\sqrt{5}$	$3+3\sqrt{5}$
$f_-(z_0) = f_-(\tau^{2i+1}) \bmod 7$	1	4	4	1	6
$f'_-(z_0) = f'_-(\tau^{2i+1}) \bmod 7$	$6+3\sqrt{5}$	$3+3\sqrt{5}$	$3+4\sqrt{5}$	$6+4\sqrt{5}$	$6+3\sqrt{5}$

$2i+1$	11	13	15
$z_0 = \tau^{2i+1} \bmod 7$	$5+6\sqrt{5}$	$5+\sqrt{5}$	$3+4\sqrt{5}$
$f_-(z_0) = f_-(\tau^{2i+1}) \bmod 7$	3	3	6
$f'_-(z_0) = f'_-(\tau^{2i+1}) \bmod 7$	$3+3\sqrt{5}$	$3+4\sqrt{5}$	$6+4\sqrt{5}$

The function $f_-(z_0)$ takes value 1mod 7 and $f'_-(z_0) \not\equiv 0 \pmod 7$ for $z_0 = \tau^{2i+1}$ with $2i+1 = 1$ and 7. Therefore, by lemma 13, if $w \equiv 1 \pmod 7$, then there exists z such that $z \equiv z_0 \pmod 7$ and $f_-(z) = w$ at $z_0 = \tau^{2i+1}$ for $2i+1 = 1$ or 7. Similarly, $f_-(z_0) \equiv 4 \pmod 7$ and $f'_-(z_0) \not\equiv 0 \pmod 7$ for $z_0 = \tau^{2i+1}$ with $2i+1 = 3$ and 5, so, if $w \equiv 4 \pmod 7$, then there exists z such that $z \equiv z_0 \pmod 7$ and $f_-(z) = w$ at $z_0 = \tau^{2i+1}$ for $2i+1 = 3$ or 5; $f_-(z_0) \equiv 6 \pmod 7$ and $f'_-(z_0) \not\equiv 0 \pmod 7$ for $z_0 = \tau^{2i+1}$ with $2i+1 = 9$ and 15, thus, if $w \equiv 6 \pmod 7$, then there exists z such that $z \equiv z_0 \pmod 7$ and $f_-(z) = w$ at $z_0 = \tau^{2i+1}$ for $2i+1 = 9$ or 15; $f_-(z_0) \equiv 3 \pmod 7$ and $f'_-(z_0) \not\equiv 0 \pmod 7$ for $z_0 = \tau^{2i+1}$ with $2i+1 = 11$ and 13, hence, if $w \equiv 3 \pmod 7$, then there exists z such that $z \equiv z_0 \pmod 7$ and $f_-(z) = w$

at $z_0 = \tau^{2i+1}$ for $2i+1 = 11$ or 13. Therefore, the 7-adic closure of the images of f_- contains the cosets $(1+7\mathbb{Z}) \cup (4+7\mathbb{Z}) \cup (6+7\mathbb{Z}) \cup (3+7\mathbb{Z})$.

When $p = 11$, the length of a period of Lucas numbers modulo p is 10.

$2i$	0	2	4	6	8
$z_0 = \tau^{2i} \bmod 11$	1	$7+6\sqrt{5}$	$9+7\sqrt{5}$	$9+4\sqrt{5}$	$7+5\sqrt{5}$
$f_+(z_0) = f_+(\tau^{2i}) \bmod 11$	2	3	7	7	3
$f'_+(z_0) = f'_+(\tau^{2i}) \bmod 11$	0	$3+7\sqrt{5}$	$5+5\sqrt{5}$	$5+6\sqrt{5}$	$3+4\sqrt{5}$

Since $f_+(z_0) \equiv 3 \pmod{11}$ at $z_0 = \tau^2$ and τ^8, and $f'_+(\tau^2), f'_+(\tau^8) \not\equiv 0 \pmod{11}$, by Lemma 13, if $w \equiv 3 \pmod{11}$, then there exists z with $z \equiv \tau^2$ or $\tau^8 \pmod{11}$ and $f_+(z) = w$. Similarly, $f_+(z_0) \equiv 7 \pmod{11}$ for $z_0 = \tau^4$ and τ^6, and $f'_+(\tau^4), f'_+(\tau^6) \not\equiv 0 \pmod{11}$, thus, if $w \equiv 7 \pmod{11}$, then there exists z with $z \equiv \tau^4$ or $\tau^6 \pmod{11}$ and $f_+(z) = w$. Therefore, the 11-adic closure of the images of f_+ contains the cosets $(3+11\mathbb{Z}) \cup (7+11\mathbb{Z})$.
Since $f_+(z_0) \equiv 2 \pmod{11}$ and $f'_+(z_0) \equiv 0 \pmod{11}$ for $z_0 = \tau^0$, the image of f_+ contains part of the coset $(2+11\mathbb{Z})$.

$2i+1$	1	3	5	7	9
$z_0 = \tau^{2i+1} \bmod 11$	$6+6\sqrt{5}$	$2+\sqrt{5}$	$8\sqrt{5}$	$9+\sqrt{5}$	$5+6\sqrt{5}$
$f_-(z_0) = f_-(\tau^{2i+1}) \bmod 11$	1	4	0	7	10
$f'_-(z_0) = f'_-(\tau^{2i+1}) \bmod 11$	$8+5\sqrt{5}$	$10+7\sqrt{5}$	2	$10+4\sqrt{5}$	$8+6\sqrt{5}$

Since $f_-(z_0) \equiv 1 \pmod{11}$ for $z_0 = \tau^1$ and $f'_-(\tau^1) \not\equiv 0 \pmod{11}$, by lemma 13, if $w \equiv 1 \pmod{11}$, then there exists z such that $z \equiv \tau^1 \pmod{11}$ and $f_-(z) = w$. Similarly, $f_-(z_0) \equiv 4 \pmod{11}$ for $z_0 = \tau^3$ and $f'_-(\tau^3) \not\equiv 0 \pmod{11}$, thus, if $w \equiv 4 \pmod{11}$, then there exists z such that $z \equiv \tau^3 \pmod{11}$ and $f_-(z) = w$; $f_-(z_0) \equiv 0 \pmod{11}$ for $z_0 = \tau^5$ and $f'_-(\tau^5) \not\equiv 0 \pmod{11}$, so, if $w \equiv 0 \pmod{11}$, then there exists z such that $z \equiv \tau^5 \pmod{11}$ and $f_-(z) = w$; $f_-(z_0) \equiv 7 \pmod{11}$ for $z_0 = \tau^7$ and $f'_-(\tau^7) \not\equiv 0 \pmod{11}$, hence, if $w \equiv 7 \pmod{11}$, then there exists z such that $z \equiv \tau^7 \pmod{11}$ and $f_-(z) = w$; $f_-(z_0) \equiv 10 \pmod{11}$ for $z_0 = \tau^9$ and $f'_-(\tau^9) \not\equiv 0 \pmod{11}$, so, if $w \equiv 10 \pmod{11}$, then there exists z such that $z \equiv \tau^9 \pmod{11}$ and $f_-(z) = w$. Therefore, the 11-adic closure of the images of f_- contains the cosets $(1+11\mathbb{Z}) \cup (4+11\mathbb{Z}) \cup (11\mathbb{Z}) \cup (7+11\mathbb{Z}) \cup (10+11\mathbb{Z})$.

When $p = 13$, the length of a period of Lucas numbers modulo p is 28.

$2i$	0	2	4	6	8
$z_0 = \tau^{2i} \bmod 13$	1	$8+7\sqrt{5}$	$10+8\sqrt{5}$	$9+4\sqrt{5}$	$4+4\sqrt{5}$
$f_+(z_0) = f_+(\tau^{2i}) \bmod 13$	2	3	7	5	8
$f'_+(z_0) = f'_+(\tau^{2i}) \bmod 13$	0	$4+8\sqrt{5}$	$10+4\sqrt{5}$	$9+7\sqrt{5}$	$9+6\sqrt{5}$

$2i$	10	12	14	16	18
$z_0 = \tau^{2i} \bmod 13$	$3+8\sqrt{5}$	$5+7\sqrt{5}$	12	$5+6\sqrt{5}$	$3+5\sqrt{5}$
$f_+(z_0) = f_+(\tau^{2i}) \bmod 13$	6	10	11	10	6
$f'_+(z_0) = f'_+(\tau^{2i}) \bmod 13$	$10+9\sqrt{5}$	$4+5\sqrt{5}$	0	$4+8\sqrt{5}$	$10+4\sqrt{5}$

$2i$	20	22	24	26
$z_0 = \tau^{2i} \bmod 13$	$4+9\sqrt{5}$	$9+9\sqrt{5}$	$10+5\sqrt{5}$	$8+6\sqrt{5}$
$f_+(z_0) = f_+(\tau^{2i}) \bmod 13$	8	5	7	3
$f'_+(z_0) = f'_+(\tau^{2i}) \bmod 13$	$9+7\sqrt{5}$	$9+6\sqrt{5}$	$10+9\sqrt{5}$	$4+5\sqrt{5}$

Since $f_+(z_0) \equiv 3 \pmod{13}$ for $z_0 = \tau^2$ and τ^{26} and $f'_+(\tau^2)$, $f'_+(\tau^{26}) \not\equiv 0 \pmod{13}$, by Lemma 13, if $w \equiv 3 \pmod{13}$, then there exists z such that $z \equiv \tau^2$ or $\tau^{26} \pmod{13}$ and $f_+(z) = w$. Similarly, $f_+(z_0) \equiv 7 \pmod{13}$ for $z_0 = \tau^4$ and τ^{24} and $f'_+(\tau^4)$, $f'_+(\tau^{24}) \not\equiv 0 \pmod{13}$, so, if $w \equiv 7 \pmod{13}$, then there exists z such that $z \equiv \tau^4$ or $\tau^{24} \pmod{13}$ and $f_+(z) = w$; $f_+(z_0) \equiv 5 \pmod{13}$ for $z_0 = \tau^6$ and τ^{22} and $f'_+(\tau^6)$, $f'_+(\tau^{22}) \not\equiv 0 \pmod{13}$, thus, if $w \equiv 5 \pmod{13}$, then there exists z such that $z \equiv \tau^6$ or $\tau^{22} \pmod{13}$ and $f_+(z) = w$; $f_+(z_0) \equiv 8 \pmod{13}$ for $z_0 = \tau^8$ and τ^{20} and $f'_+(\tau^8)$, $f'_+(\tau^{20}) \not\equiv 0 \pmod{13}$, hence, if $w \equiv 8 \pmod{13}$, then there exists z such that $z \equiv \tau^8$ or $\tau^{20} \pmod{13}$ and $f_+(z) = w$; $f_+(z_0) \equiv 6 \pmod{13}$ for $z_0 = \tau^{10}$ and τ^{18} and $f'_+(\tau^{10})$, $f'_+(\tau^{18}) \not\equiv 0 \pmod{13}$, so, if $w \equiv 6 \pmod{13}$, then there exists z such that $z \equiv \tau^{10}$ or $\tau^{18} \pmod{13}$ and $f_+(z) = w$; $f_+(z_0) \equiv 10 \pmod{13}$ for $z_0 = \tau^{12}$ and τ^{16} and $f'_+(\tau^{12})$, $f'_+(\tau^{16}) \not\equiv 0 \pmod{13}$, therefore, if $w \equiv 10 \pmod{13}$, then there exists z such that $z \equiv \tau^{12}$ or $\tau^{16} \pmod{13}$ and $f_+(z) = w$. Therefore, the 13-adic closure of the images of f_+ contains the cosets $(3+13\mathbb{Z}) \cup (7+13\mathbb{Z}) \cup (5+13\mathbb{Z}) \cup (8+13\mathbb{Z}) \cup (6+13\mathbb{Z}) \cup (10+13\mathbb{Z})$. Since $f_+(z_0) \equiv 2 \pmod{13}$ and $f'_+(z_0) \equiv 0 \pmod{13}$ for $z_0 = \tau^0$, the image of f_+ contains part of the coset $(2 + 13\mathbb{Z})$. Similarly, $f_+(z_0) \equiv 11 \pmod{13}$ and $f'_+(z_0) \equiv 0 \pmod{13}$ for $z_0 = \tau^{14}$, the image of f_+ contains part of the coset $(11 + 13\mathbb{Z})$.

$2i+1$	1	3	5	7	9
$z_0 = \tau^{2i+1} \bmod 13$	$7+7\sqrt{5}$	$2+\sqrt{5}$	$12+9\sqrt{5}$	8	$12+4\sqrt{5}$
$f_-(z_0) = f_-(\tau^{2i+1}) \bmod 13$	1	4	11	3	11
$f'_-(z_0) = f'_-(\tau^{2i+1}) \bmod 13$	$9+6\sqrt{5}$	$10+9\sqrt{5}$	$4+5\sqrt{5}$	0	$4+8\sqrt{5}$

$2i+1$	11	13	15	17
$z_0 = \tau^{2i+1} \bmod 13$	$2+12\sqrt{5}$	$7+6\sqrt{5}$	$6+6\sqrt{5}$	$11+12\sqrt{5}$
$f_-(z_0) = f_-(\tau^{2i+1}) \bmod 13$	4	1	12	9
$f'_-(z_0) = f'_-(\tau^{2i+1}) \bmod 13$	$10+4\sqrt{5}$	$9+7\sqrt{5}$	$9+6\sqrt{5}$	$10+9\sqrt{5}$

$2i+1$	19	21	23	25
$z_0 = \tau^{2i+1} \bmod 13$	$1+4\sqrt{5}$	5	$1+9\sqrt{5}$	$11+\sqrt{5}$
$f_-(z_0) = f_-(\tau^{2i+1}) \bmod 13$	2	10	2	9
$f'_-(z_0) = f'_-(\tau^{2i+1}) \bmod 13$	$4+5\sqrt{5}$	0	$4+8\sqrt{5}$	$10+4\sqrt{5}$

$2i+1$	27
$z_0 = \tau^{2i+1} \bmod 13$	$6+7\sqrt{5}$
$f_-(z_0) = f_-(\tau^{2i+1}) \bmod 13$	12
$f'_-(z_0) = f'_-(\tau^{2i+1}) \bmod 13$	$9+7\sqrt{5}$

Since $f_-(z_0) \equiv 1 (\text{mod } 13)$ for $z_0 = \tau^1$ and τ^{13} and $f'_-(\tau^1)$, $f'_-(\tau^{13}) \not\equiv 0 (\text{mod } 13)$, by lemma 13, if $w \equiv 1 (\text{mod } 13)$, then there exists z such that $z \equiv \tau^1$ or $\tau^{13} (\text{mod } 13)$ and $f_-(z) = w$. Similarly, $f_-(z_0) \equiv 4 (\text{mod } 13)$ for $z_0 = \tau^3$ and τ^{11} and $f'_-(\tau^3)$, $f'_-(\tau^{11}) \not\equiv 0 (\text{mod } 13)$, so, if $w \equiv 4 (\text{mod } 13)$, then there exists z such that $z \equiv \tau^3$ or $\tau^{11} (\text{mod } 13)$ and $f_-(z) = w$; $f_-(z_0) \equiv 11 (\text{mod } 13)$ for $z_0 = \tau^5$ and τ^9 and $f'_-(\tau^5)$, $f'_-(\tau^9) \not\equiv 0 (\text{mod } 13)$, thus, if $w \equiv 11 (\text{mod } 13)$, then there exists z such that $z \equiv \tau^5$ or $\tau^9 (\text{mod } 13)$ and $f_-(z) = w$; $f_-(z_0) \equiv 12 (\text{mod } 13)$ for $z_0 = \tau^{15}$ and τ^{27} and $f'_-(\tau^{15})$, $f'_-(\tau^{27}) \not\equiv 0 (\text{mod } 13)$, hence, if $w \equiv 12 (\text{mod } 13)$, then there exists z such that $z \equiv \tau^{15}$ or $\tau^{27} (\text{mod } 13)$ and $f_-(z) = w$; $f_-(z_0) \equiv 9 (\text{mod } 13)$ for $z_0 = \tau^{17}$ and τ^{25} and $f'_-(\tau^{17})$, $f'_-(\tau^{25}) \not\equiv 0 (\text{mod } 13)$, thus, if $w \equiv 9 (\text{mod } 13)$, then there exists z such that $z \equiv \tau^{17}$ or $\tau^{25} (\text{mod } 13)$ and $f_-(z) = w$; $f_-(z_0) \equiv 2 (\text{mod } 13)$ for $z_0 = \tau^{19}$ and τ^{23} and $f'_-(\tau^{19})$, $f'_-(\tau^{23}) \not\equiv 0 (\text{mod } 13)$, therefore, if $w \equiv 2 (\text{mod } 13)$, then there exists z such that $z \equiv \tau^{19}$ or $\tau^{23} (\text{mod } 13)$ and $f_-(z) = w$. Therefore, the 13-adic closure of the images of f_- contains the cosets $(1+13\mathbb{Z}) \cup (4+13\mathbb{Z}) \cup (11+13\mathbb{Z}) \cup (12+13\mathbb{Z}) \cup (9+13\mathbb{Z}) \cup (2+13\mathbb{Z})$.

Since $f_-(z_0) \equiv 3(\text{mod } 13)$ and $f'_-(z_0) \equiv 0(\text{mod } 13)$ for $z_0 = \tau^7$, the image of f_- will contain part of the coset $(3 + 13\mathbb{Z})$. Similarly, $f_-(z_0) \equiv 10(\text{mod } 13)$ and $f'_-(z_0) \equiv 0(\text{mod } 7)$ for $z_0 = \tau^{21}$, the image of f_- contains part of the coset $(10 + 13\mathbb{Z})$.

Now, a question arises what happens if the derivative of the function f_+ or f_- at any point is zero? To meet this situation, we use the Generalized Hensel's lemma 14. Now, since $f'_+(z) \equiv 0(\text{mod } p)$ if and only if $z \equiv \pm 1(\text{mod } p)$, we can consider that $z = 1(\text{mod } p)$, $z = -1(\text{mod } p)$, and the respective cases for f_- will be the same because $f_-(z) \equiv 0(\text{mod } p)$ if and only if $z = \pm 1(\text{mod } p)$. Now, if $z \equiv 1(\text{mod } p^M)$ for any integer $M > 0$, then $z = 1 + \lambda p^M$ for some $\lambda \in \mathbb{Z}_p$ or $\mathbb{Z}_p[\sqrt{5}]$ and so $f_+(z) = 1 + \lambda p^M + \frac{1}{\lambda p^M} = 1 + \lambda p^M + (1 - \lambda p^M + \lambda^2 p^{2M} - \lambda^3 p^{3M} + \cdots) = 2 + \lambda^2 p^{2M}(1 - \lambda p^M + \lambda^2 p^{2M} - \lambda^3 p^{3M} + \cdots) \equiv 2(\mu p^{2M})$, where $\mu = \lambda^2$ is a unit in $\mathbb{Z}_p$ or $\mathbb{Z}_p[\sqrt{5}]$. Due to the Generalized Hensel's lemma it can be shown that the converse holds letting $y = 2 + \mu p^{2M}$ with μ a unit square in $\mathbb{Z}_p$ or $\mathbb{Z}_p[\sqrt{5}]$ leaving $z \equiv 1(\text{mod } p)$ such that $f_+(z) = y$. For $z_0 = 1 + \lambda p^M$ with a unit λ such that $\mu = \lambda^2$ the conditions of Generalized Hensel's lemma are satisfied. In this situation, not all elements of the cosets $(2 + \mu p^{2M}) + (p^{2M+1})$ are Lucas numbers. We denote the union of the cosets $(2 + \mu p^{2M}) + (p^{2M+1})$ by T_1, where $M \geq 0$ is any integer and μ is a nonzero square modulo p. There are two possibilities: that $\mathfrak{L}$ may contain elements congruent to 2 modulo p or $T_1/(p^k) = (\mathfrak{L} \cap (2 + (p)))/(p^k)$ for all k. Considering the case $z \equiv -1(\text{mod } p)$, we get the corresponding result for a set T_{-1} by replacing 2 by -2. The critical points of z with respect to f_- are $\pm\sqrt{-1}(\text{mod } p)$ and the results are satisfied for the sets $T_{\pm\sqrt{-1}}$ changing $\pm 2\sqrt{-1}$ for 2.

Since the sets $T_{\pm 1}$ and $T_{\pm\sqrt{-1}}$ are constructed due to different cosets modulo p, the p-orderings and the associated p-sequences of $\mathfrak{L}$, when they happen, are shuffles of the p-orderings and the associated p-sequences of the T sets. Let the set of nonzero squares in $\mathbb{Z}/(p)$ be S_q with cardinality $(p-1)/2$, and let

$T'_1 = \cup_{M=2}^{\infty}(\cup_{\mu \in S_q}(2 + \mu p^{2M}) + (p^{2M+1}))$.

Then the set T_1 can be written as

$T_1 = (\cup_{\mu \in S_q}(2 + \mu p^2) + (p^3)) \cup T'_1$.

The sets in the left part of the above union are all cosets of (p^3) and so the associated p-sequence is $\alpha_{\mathbb{Z},p} + (3n)$, whereas the set T'_1 is obtained from $p^2 T_1$ and thus its associated p-sequence is $\alpha_{T_{1,p}} + (2n)$. Then the equation $\alpha_{T_{1,p}} = ((\nu_n(\mathbb{Z}, p) + (n))^{(p-1)/2} \wedge \alpha_{T_{1,p}}) +$

$(2n)$ holds due to the associated p-sequence of T_1 from which α_{T_1} can be obtained because it expresses $\alpha_{T_{1,p}}(n)$ with respect to $\alpha_{T_{1,p}}(m)$ for $m < n$ and with respect to known sequences. Also, the sequence is satisfied due to the associated p-sequences of T_{-1} and $T_{\pm\sqrt{-1}}$. Therefore, we get a complete algorithm for computing $\alpha_{\mathfrak{L}}$.

We can apply this to $p = 7$.

Theorem 23. *([14], Proposition 4) The 7-sequence of $\mathfrak{L}$ can be written as*
$\alpha_{\mathfrak{L},7} = (\nu_k(\mathbb{Z}, 7) + (k))^{\wedge 5} \wedge (\alpha_{T_{1,7}})^2$
with the satisfing sequence $\alpha_{T_{1,7}}$ that can be determined by the equation
$\alpha_{T_{1,7}} = ((\nu_k(\mathbb{Z}, 7) + (k))^{\wedge 3} \wedge \alpha_{T_{1,7}}) + (2k)$.

Proof. The period of Lucas numbers modulo 7 is 16 and one period is given by

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\mathfrak{L}_k$	2	1	3	4	0	4	4	1	5	6	4	3	0	3	3	6

Separating these Lucas numbers modulo 7 into even and odd idex we can show that the image of f_+ modulo 7 is $\{0, 2, 3, 4, 5\}$ and that of f_- modulo 7 is $\{1, 3, 4, 6\}$. We have the critical points of f_+ and f_- by manipulating $y^2 - 4$ modulo 7 and $y^2 + 4$ modulo 7, respectively, as follows:

y	0	2	3	4	5
$y^2 - 4$	3	0	5	5	0

and

y	1	3	4	6
$y^2 + 4$	5	6	6	5

Therefore, considering T as the union of the cosets modulo 7 of $\{0, 1, 2, 3, 4, 5, 6\}$ together with T_1 and T_{-1} for $p = 7$, we can reach to the given equation.

Now, how do the results change when $U(\mathbb{Z}/(p))$ (respectively, $U^0(\mathbb{Z}[\sqrt{5}]/(p))$) is not generated by τ or the condition $\tau^{p-1} \equiv 1 (\text{mod } p^2)$ (respectively, $\tau^{2(p+1)} \equiv 1 (\text{mod } p^2)$) holds? When the order of τ, u, is strictly smaller than $p - 1$ or $2(p + 1)$, the group τ generates will meet u of the cosets of $U(\mathbb{Z}/(p))$ or $U^0(\mathbb{Z}[\sqrt{5}]/(p))$. Under the condition $\tau^u \not\equiv 1 (\text{mod } p^2)$, $< \tau >$ is dense in each of the cosets modulo p that

certainly occurs, and the outcomes remain unaltered when u is even. But, in the case that of u is odd, for any k the domains of f_+ and f_- modulo p^k will be the whole of $< \tau > /(p^k)$ instead of the square and nonsquare elements, respectively, because $\tau^i \equiv \tau^{i+up^{k-1}} (\text{mod } p^k)$, whereas i and $i + up^{k-1}$ are opposite parity. Therefore, the period of Lucas numbers modulo p will be $2u$ instead of u for this case, and the images of f_+ and f_- can each be formed due to all indices rather than selecting even and odd ones distinctly. The case $\tau^u \equiv 1(\text{mod } p^2)$ is very difficult to be found (see page 345, [14]). If this condition holds, then the said results with $U(\mathbb{Z}/(p))$ or $U^0(\mathbb{Z}[\sqrt{5}]/(p))$ will be transfered to those with $U(\mathbb{Z}/(p^a))$ or $U^0(\mathbb{Z}[\sqrt{5}]/(p^a))$ for the least integer a such that $\tau^u \not\equiv 1(\text{mod } p^{a+1})$.

4.2 Regular $\mathbb{Z}$-basis for $\mathfrak{L}$

We are ready to give part of a regular $\mathbb{Z}$-basis for $\mathfrak{L}$. Before doing that we set the following tables obtained from Maplecode 1 whereabouts p-orderings and the associated p-sequences are consistent with Remark 5:

2-ordering of $\mathbb{Z}$	$\{1, -6, -5, -4, -3, -2, -1, 0, -7, 2, 3, 4, 5, 6, 7\}$
2-ordering of $\mathfrak{L}$	$\{2, 1, 3, 4, 7, 29, 76, 18, 11, 521, 47, 322, 123, 199, 843\}$
3-ordering of $\mathbb{Z}$	$\{1, -7, -6, -5, -4, -3, -2, -1, 0, 2, 3, 4, 5, 6, 7\}$
3-ordering of $\mathfrak{L}$	$\{2, 1, 3, 4, 18, 521, 7, 123, 11, 76, 843, 47, 199, 322, 29\}$
5-ordering of $\mathbb{Z}$	$\{1, -7, -6, -5, -3, -4, -2, -1, 0, 2, 3, 4, 5, 6, 7\}$
5-ordering of $\mathfrak{L}$	$\{2, 1, 3, 4, 7, 11, 18, 199, 47, 123, 521, 29, 76, 322, 843\}$
7-ordering of $\mathbb{Z}$	$\{1, -7, -5, -4, -3, -2, -1, -6, 0, 2, 3, 4, 5, 6, 7\}$
7-ordering of $\mathfrak{L}$	$\{2, 1, 3, 4, 7, 47, 76, 11, 29, 322, 521, 18, 843, 123, 199\}$
11-ordering of $\mathbb{Z}$	$\{1, -7, -6, -5, -4, -3, -2, -1, 0, 2, 3, 4, 5, 6, 7\}$
11-ordering of $\mathfrak{L}$	$\{2, 1, 3, 4, 7, 11, 76, 18, 47, 199, 521, 29, 123, 322, 843\}$

2-sequence of $\mathbb{Z}$	$\{0,0,1,1,3,3,4,4,7,7,8,8,10,10,11\}$
2-sequence of $\mathfrak{L}$	$\{0,0,1,1,3,4,4,6,7,8,10,12,14,18,22\}$
3-sequence of $\mathbb{Z}$	$\{0,0,0,1,1,1,2,2,2,4,4,4,5,5,5\}$
3-sequence of $\mathfrak{L}$	$\{0,0,0,1,1,1,2,2,3,4,4,5,5,6,8\}$
5-sequence of $\mathbb{Z}$	$\{0,0,0,0,0,1,1,1,1,2,2,2,2,2\}$
5-sequence of $\mathfrak{L}$	$\{0,0,0,0,1,1,1,1,2,2,2,3,4,4,4\}$
7-sequence of $\mathbb{Z}$	$\{0,0,0,0,0,0,0,1,1,1,1,1,1,1,2\}$
7-sequence of $\mathfrak{L}$	$\{0,0,0,0,0,0,0,1,1,1,1,2,2,3,4\}$
11-sequence of $\mathbb{Z}$	$\{0,0,0,0,0,0,0,0,0,0,0,1,1,1,1\}$
11-sequence of $\mathfrak{L}$	$\{0,0,0,0,0,0,0,1,1,1,1,2,2,2,3\}$

Now, we manually check the p-orderings and p-sequence of Lucas numbers, and then we find the regular basis for $\mathfrak{L}$, the Lucas numbers.

Lucas numbers mod 2^k:

The length of a period of Lucas numbers mod 2 is 3, and the period is $[0,1,1]$.

The length of a period of Lucas numbers mod 4 is 6, and the period is $[2,1,3,0,3,3]$.

The length of a period of Lucas numbers mod 8 is 12, and the period is $[2,1,3,4,7,3,2,5,7,4,3,7]$.

There are no Lucas numbers congruent to 0 or 6 modulo 8, and hence $2,1,3,4,7,29$, will be the beginning of a 2-ordering with 2-sequence $0,0,1,1,3,4$.

The Lucas numbers modulo 8 are contained in $(1+2\mathbb{Z}) \cup (2+8\mathbb{Z}) \cup (4+8\mathbb{Z}) = (1+2\mathbb{Z}) \cup 2 \cdot ((1+4\mathbb{Z}) \cup (2+4\mathbb{Z}))$.

The 2-sequences of $1+4\mathbb{Z}$ and $2+4\mathbb{Z}$ are

$\alpha_{\mathbb{Z}} + (2n) = [0,0,1,1,3,3,\cdots] + [0,2,4,6,8,10,\cdots] = [0,2,5,7,11,13,\cdots]$.

The 2-sequence of $1+2\mathbb{Z}$ is

$\alpha_{\mathbb{Z}} + (n) = [0,0,1,1,3,3,\cdots] + [0,1,2,3,4,5,\cdots]$.

The 2-sequence of $(1+4\mathbb{Z}) \cup (2+4\mathbb{Z})$ is the shuffle $[0,0,2,2,5,5,7,7,\cdots]$, and that of $2 \cdot ((1+4\mathbb{Z}) \cup (2+4\mathbb{Z}))$ is $[0,0,2,2,5,5,7,7,\cdots] + [0,1,2,3,4,5,\cdots] = [0,1,4,5,9,12,\cdots]$.

Thus the 2-sequence of $(1+2\mathbb{Z}) \cup 2 \cdot ((1+4\mathbb{Z}) \cup (2+4\mathbb{Z}))$ is the shuffle

$[0,1,3,4,7,8,\cdots] \wedge [0,4,5,9,12,\cdots] = [0,0,1,1,3,4,4,5,7,8,\cdots]$.

The Lucas numbers mod 3^k:

The length of a period of Lucas numbers mod 3 is 8, and the period is $[2,1,0,1,1,2,0,2]$.

The length of a period of Lucas numbers mod 9 is 24, and the period is

$[2,1,3,4,7,2,0,2,2,4,6,1,7,8,6,5,2,7,0,7,7,5,3,8]$, and all residue classes mod 3^2 occur in $\mathfrak{L}$, and so its 3-sequence will begin with $[0,0,0,1,1,1,2,2,2,2,\cdots]$ with the first 9 elements of a 3-ordering having representation from all residue classes mod 9 $[2,1,3,4,18,521,7,123,1364]$.

The Lucas numbers mod 5^k:

The length of a period of Lucas numbers mod 5 is 4, and the period is $[2,1,3,4]$. Thus, no Lucas number is divisible by 5, and so the 5-sequence of Lucas numbers must start with $[0,0,0,0,1,1,1,1,\cdots]$, and a 5-ordering will start with $[2,1,3,4,7,11,\cdots]$.

Thus the p-sequences of $\mathfrak{L}$ begin:

k	0	1	2	3	4	5
$p=2$	0	0	1	1	3	4
$p=3$	0	0	0	1	1	1
$p=5$	0	0	0	0	1	1

Hence the denominators of a regular basis for Lucas numbers are

k	0	1	2	3
$d(k)$	$2^0\cdot 3^0\cdot 5^0=1$	$2^0\cdot 3^0\cdot 5^0=1$	$2^1\cdot 3^0\cdot 5^0=2$	$2^1\cdot 3^1\cdot 5^0=6$

k	4	5
$d(k)$	$2^3\cdot 3^1\cdot 5^1=120$	$2^4\cdot 3^1\cdot 5^1=240$

The regular basis will be of the form $\dfrac{\prod_{i=0}^{k}(x-a_i)}{d(i)}$, where the a_i's are picked using the Chinese remainder theorem to have the following residues:

	a_0	a_1	a_2	a_3	a_4	a_5
mod 2^3	2	1	3	4	7	5
mod 3^2	2	1	3	4	0	6
mod 5^2	2	1	3	4	7	11
	2	1	3	4	207	1181

Therefore, the regular $\mathbb{Z}$-basis for Lucas numbers is

$$\{1,(x-2),\frac{(x-2)(x-1)}{2},\frac{(x-2)(x-1)(x-3)}{6},\frac{(x-2)(x-1)(x-3)(x-4)}{120},$$

$$\frac{(x-2)(x-1)(x-3)(x-4)(x-207)}{240},\cdots\}.$$

Chapter 5

The General Sequences for a Given Pair of Initial Values

The aim of this chapter is to find a general sequence, $\mathfrak{G} = \{\mathfrak{G}_k\}$, of integers starting with any pair of integers, $(\mathfrak{G}_0, \mathfrak{G}_1) = (A, B)$. Also, we will find some interesting properties relating to this sequence.

5.1 Binet's Formula for the Sequence $\mathfrak{G}$

Suppose the sequence, $\{\mathfrak{G}_k\}$, of integers satisfies the equation

$$\mathfrak{G}_{k+1} = \mathfrak{G}_k + \mathfrak{G}_{k-1}, \tag{5.1}$$

where $k = 1, 2, 3, \cdots$, and $(\mathfrak{G}_0, \mathfrak{G}_1) = (A, B)$ with any integers A and B.
Suppose a solution of (5.1) is of the form $C \cdot X^k$.
Then using this as in the Fibonacci and Lucas cases, we obtain $X^2 - X - 1 = 0$ leaving $X = \frac{1 \pm \sqrt{5}}{2}$. We verify that both choices of X do give solutions of (5.1), and that any linear combination of them does also.
Then the explicit formula for the general sequence, $\{\mathfrak{G}_k\}$, is

$$\mathfrak{G}_k = C_1 \cdot (\frac{1+\sqrt{5}}{2})^k + C_2 \cdot (\frac{1-\sqrt{5}}{2})^k \tag{5.2}$$

Putting $k = 0, 1$ in (5.2), we get

$$C_1 + C_2 = A \tag{5.3}$$

and

$$C_1 \cdot \frac{1+\sqrt{5}}{2} + C_2 \cdot \frac{1-\sqrt{5}}{2} = B \tag{5.4}$$

Now, solving equations (5.3) and (5.4), we have
$C_1 = \frac{1}{\sqrt{5}}[\frac{\sqrt{5}-1}{2} \cdot A + B]$ and $C_2 = \frac{1}{\sqrt{5}}[\frac{1+\sqrt{5}}{2} \cdot A - B]$, and so
$\mathfrak{G}_k = \frac{1}{\sqrt{5}}[\frac{\sqrt{5}-1}{2} \cdot A + B](\frac{1+\sqrt{5}}{2})^k + \frac{1}{\sqrt{5}}[\frac{1+\sqrt{5}}{2} \cdot A - B](\frac{1-\sqrt{5}}{2})^k$.

Let $\tau_1 = \frac{1+\sqrt{5}}{2}$ and $\tau_2 = \frac{1-\sqrt{5}}{2}$ be such that $X^2 - X - 1 = (X - \tau_1)(X - \tau_2)$. Then $\tau_1\tau_2 = -1$ and so $\tau = \tau_1 = -\frac{1}{\tau_2}$.

Therefore, the Binet's formula for the general sequence can be written as

$$\mathfrak{G}_k = \begin{cases} F_+(\tau^k), & \text{if k is even} \\ F_-(\tau^k), & \text{if k is odd} \end{cases}$$

where $F_+(\tau^k) = C_1 \cdot (\tau)^k + C_2 \cdot (\frac{1}{\tau})^k$ and $F_-(\tau^k) = C_1 \cdot (\tau)^k - C_2 \cdot (\frac{1}{\tau})^k$ with $\tau = \frac{1+\sqrt{5}}{2}$, $C_1 = \frac{1}{\sqrt{5}}[\frac{1}{\tau} \cdot A + B]$, and $C_2 = \frac{1}{\sqrt{5}}[\tau \cdot A - B]$.

5.2 Closures of Images of F_+ and F_-

It is important to first note here that $< \tau >$ is a multiplicative group generated by τ, and is also a subgroup of $\mathbb{Q}[\sqrt{5}]$.
Now, when we take the set of squares and the set of nonsquares in the multiplicative group $< \tau >$ as the domains of F_+ and F_-, respectively, the union of their images will be $\mathfrak{G}$ or, after reduction, $\mathfrak{G}/(p^k)$, as for example, for the pairs $(A, B) = (0, 1)$ and $(A, B) = (2, 1)$, we see (section 3, [14]) and the corresponding result to the Lucas numbers in Chapter 4, respectively.
Now, we intend to concentrate on the localization at some prime p considering τ (and the group it generates) as an algebraic object instead of thinking of them in $\mathbb{R}$.
Due to [14], for any odd prime such that $p \equiv 1, -1 (\text{mod } 5)$, we have $\tau \in \mathbb{Z}_p$ and τ generates a dense subgroup of $U(\mathbb{Z}_p)$, the set of units in $\mathbb{Z}_p$ (here $\mathbb{Z}_p$ is the p-adic integers). Under conditions that the mod p reduction of τ generates $U(\mathbb{Z}/(p))$, and $\tau^{p-1} \not\equiv 1 (\text{mod } p^2)$, its reduction mod p^k generates $U(\mathbb{Z}/(p^k))$ for all $k > 0$. Then we can extend the maps F_+ and F_- such that their domains are squares and nonsquares of $U(\mathbb{Z}_p)$, respectively. These domains separate $U(\mathbb{Z}_p)$ into two disjoint open subsets with respect to the p-adic topology, and their images are the closures, $\bar{\mathfrak{G}}$, of $\mathfrak{G}$ with respect to the same topology with the property $\bar{\mathfrak{G}}/(p^k) = \mathfrak{G}/(p^k)$ for any k.

If p is an odd prime such that $p \equiv 2, -2 (\text{mod } 5)$, then we get the same results as in (section 3, [14] for $(A, B) = (0, 1)$), and the corresponding results for $(A, B) = (2, 1)$ in Chapter 4.

Now, to compute $F_+(Z_0)\text{mod } p$, $F'_+(Z_0)\text{mod } p$, $F_-(Z_0)\text{mod } p$, and $F'_-(Z_0)\text{mod } p$ for primes p, we use Maplecode 4.

For the pairs $(A, B) = (0, 1)$ and $(A, B) = (2, 1)$, and $p = 7, 11, 13$, we have the results in [14], and the results for the Lucas numbers in Chapter 4, respectively.

For finding the closures of images of F_+ and F_-, we use the Hensel's lemma and the generalized Hensel's lemma for pairs, (A, B), of integers such as $(A, B) = (2, 5)$ for primes p.

When $p = 7$, the length of a period of $\mathfrak{G}$ mod p is 16.

$2i$	0	2	4	6	8	10
$Z_0 = \tau^{2i}\text{mod } 7$	1	$5+4\sqrt{5}$	$5\sqrt{5}$	$2+4\sqrt{5}$	6	$2+3\sqrt{5}$
$F_+(Z_0) = F_+(\tau^{2i})\text{mod } 7$	2	0	5	1	5	0
$F'_+(Z_0) = F'_+(\tau^{2i})\text{mod } 7$	$3\sqrt{5}$	$2+3\sqrt{5}$	2	0	$3\sqrt{5}$	$2+3\sqrt{5}$

$2i$	12	14
$Z_0 = \tau^{2i}\text{mod } 7$	$2\sqrt{5}$	$5+3\sqrt{5}$
$F_+(Z_0) = F_+(\tau^{2i})\text{mod } 7$	2	6
$F'_+(Z_0) = F'_+(\tau^{2i})\text{mod } 7$	2	0

Since $F_+(Z_0) \equiv 2(\text{mod } 7)$ and $F'_+(Z_0) \not\equiv 0(\text{mod } 7)$ for $Z_0 = \tau^0$ and τ^{12}, by lemma 13, if $W \equiv 2(\text{mod } 7)$, then there exists Z such that $Z \equiv \tau^0$ or $\tau^{12}(\text{mod } 7)$ and $F_+(Z) = W$. Similarly, $F_+(Z_0) \equiv 0(\text{mod } 7)$ and $F'_+(Z_0) \not\equiv 0(\text{mod } 7)$ for $Z_0 = \tau^2$ and τ^{10}, so, if $W \equiv 0(\text{mod } 7)$, then there exists Z such that $Z \equiv \tau^2$ or $\tau^{10}(\text{mod } 7)$ and $F_+(Z) = W$; $F_+(Z_0) \equiv 5(\text{mod } 7)$ and $F'_+(Z_0) \not\equiv 0(\text{mod } 7)$ for $Z_0 = \tau^4$ and τ^8, so, if $W \equiv 5(\text{mod } 7)$, then there exists Z such that $Z \equiv \tau^4$ or $\tau^8(\text{mod } 7)$ and $F_+(Z) = W$. Therefore, the closure of the images of F_+ contains the cosets $(2+7\mathbb{Z})\cup(7\mathbb{Z})\cup(5+7\mathbb{Z})$. Since $F_+(Z_0) \equiv 1(\text{mod } 7)$ and $F'_+(Z_0) \equiv 0(\text{mod } 7)$ for $Z_0 = \tau^6$, the image of F_+ contains part of the coset $(1 + 7\mathbb{Z})$. Similarly, $F_+(Z_0) \equiv 6(\text{mod } 7)$ and $F'_+(Z_0) \equiv 0(\text{mod } 7)$ for $Z_0 = \tau^{14}$, and so the image of F_+ contains part of the coset $(6 + 7\mathbb{Z})$. We examined this type of case on page 37 in Chapter 4 by answering to the question "what happens if the derivative of a function at any point is zero?".

$2i+1$	1	3	5	7	9
$Z_0 = \tau^{2i+1} \bmod 7$	$4+4\sqrt{5}$	$2+\sqrt{5}$	$2+6\sqrt{5}$	$4+3\sqrt{5}$	$3+3\sqrt{5}$
$F_-(Z_0) = F_-(\tau^{2i+1}) \bmod 7$	5	5	3	4	2
$F'_-(Z_0) = F'_-(\tau^{2i+1}) \bmod 7$	$1+4\sqrt{5}$	$5+5\sqrt{5}$	$1+6\sqrt{5}$	$4+5\sqrt{5}$	$1+4\sqrt{5}$

$2i+1$	11	13	15
$Z_0 = \tau^{2i+1} \bmod 7$	$5+6\sqrt{5}$	$5+\sqrt{5}$	$3+4\sqrt{5}$
$F_-(Z_0) = F_-(\tau^{2i+1}) \bmod 7$	2	4	3
$F'_-(Z_0) = F'_-(\tau^{2i+1}) \bmod 7$	$5+5\sqrt{5}$	$1+6\sqrt{5}$	$4+5\sqrt{5}$

Since $F_-(Z_0) \equiv 5 (\text{mod } 7)$ and $F'_-(Z_0) \not\equiv 0 (\text{mod } 7)$ for $Z_0 = \tau^1$ and τ^3, by lemma 13, if $W \equiv 5 (\text{mod } 7)$, then there exists Z such that $Z \equiv \tau^1$ or $\tau^3 (\text{mod } 7)$ and $F_-(Z) = W$. Similarly, $F_-(Z_0) \equiv 3 (\text{mod } 7)$ and $F'_-(Z_0) \not\equiv 0 (\text{mod } 7)$ for $Z_0 = \tau^5$ and τ^{15}, so, if $W \equiv 3 (\text{mod } 7)$, then there exists Z such that $Z \equiv \tau^5$ or $\tau^{15} (\text{mod } 7)$ and $F_-(Z) = W$; $F_-(Z_0) \equiv 4 (\text{mod } 7)$ and $F'_-(Z_0) \not\equiv 0 (\text{mod } 7)$ for $Z_0 = \tau^7$ and τ^{13}, hence, if $W \equiv 4 (\text{mod } 7)$, then there exists Z such that $Z \equiv \tau^7$ or $\tau^{13} (\text{mod } 7)$ and $F_-(Z) = W$; $F_-(Z_0) \equiv 2 (\text{mod } 7)$ and $F'_-(Z_0) \not\equiv 0 (\text{mod } 7)$ for $Z_0 = \tau^9$ and τ^{11}, thus, if $W \equiv 2 (\text{mod } 7)$, then there exists Z such that $Z \equiv \tau^9$ or $\tau^{11} (\text{mod } 7)$ and $F_-(Z) = W$. Therefore, the closure of the images of F_- contains the cosets $(5 + 7\mathbb{Z}) \cup (3 + 7\mathbb{Z}) \cup (4 + 7\mathbb{Z}) \cup (2 + 7\mathbb{Z})$.

When $p = 11$, the length of a period of $\mathfrak{G}$ modulo p is 10.

$2i$	0	2	4	6	8
$Z_0 = \tau^{2i} \bmod 11$	1	$7+6\sqrt{5}$	$9+7\sqrt{5}$	$9+4\sqrt{5}$	$7+5\sqrt{5}$
$F_+(Z_0) = F_+(\tau^{2i}) \bmod 11$	2	7	8	6	10
$F'_+(Z_0) = F'_+(\tau^{2i}) \bmod 11$	$6\sqrt{5}$	$8+4\sqrt{5}$	$7+7\sqrt{5}$	$3+8\sqrt{5}$	$9+\sqrt{5}$

Since $F_+(Z_0) \equiv 2 (\text{mod } 11)$ and $F'_+(Z_0) \not\equiv 0 (\text{mod } 11)$ for $Z_0 = \tau^0$, by lemma 13, if $W \equiv 2 (\text{mod } 11)$, then there exists Z such that $Z \equiv \tau^0 (\text{mod } 11)$ and $F_+(Z) = W$. Similarly, $F_+(Z_0) \equiv 7 (\text{mod } 11)$ and $F'_+(Z_0) \not\equiv 0 (\text{mod } 11)$ for $Z_0 = \tau^2$, so, if $W \equiv 7 (\text{mod } 11)$, then there exists Z such that $Z \equiv \tau^2 (\text{mod } 11)$ and $F_+(Z) = W$; $F_+(Z_0) \equiv 8 (\text{mod } 11)$ and $F'_+(Z_0) \not\equiv 0 (\text{mod } 11)$ for $Z_0 = \tau^4$, thus, if $W \equiv 8 (\text{mod } 11)$, then there exists Z such that $Z \equiv \tau^4 (\text{mod } 11)$ and $F_+(Z) = W$; $F_+(Z_0) \equiv 6 (\text{mod } 11)$ and $F'_+(Z_0) \not\equiv 0 (\text{mod } 11)$ for $Z_0 = \tau^6$, hence, if $W \equiv 6 (\text{mod } 11)$, then there exists

Z such that $Z \equiv \tau^6 (\text{mod } 11)$ and $F_+(Z) = W$; $F_+(Z_0) \equiv 10(\text{mod } 11)$ and $F'_+(Z_0) \not\equiv 0(\text{mod } 11)$ for $Z_0 = \tau^8$, therefore, if $W \equiv 10(\text{mod } 11)$, then there exists Z such that $Z \equiv \tau^8(\text{mod } 11)$ and $F_+(Z) = W$. Therefore, the closure of the images of F_+ contains the cosets $(2 + 11\mathbb{Z}) \cup (7 + 11\mathbb{Z}) \cup (8 + 11\mathbb{Z}) \cup (6 + 11\mathbb{Z}) \cup (10 + 11\mathbb{Z})$.

$2i+1$	1	3	5	7	9
$Z_0 = \tau^{2i+1} \text{mod } 11$	$6+6\sqrt{5}$	$2+\sqrt{5}$	$8\sqrt{5}$	$9+\sqrt{5}$	$5+6\sqrt{5}$
$F_-(Z_0) = F_-(\tau^{2i+1}) \text{mod } 11$	5	1	9	4	3
$F'_-(Z_0) = F'_-(\tau^{2i+1}) \text{mod } 11$	$10+9\sqrt{5}$	$4+5\sqrt{5}$	2	$5+2\sqrt{5}$	$6+10\sqrt{5}$

The function $F_-(Z_0)$ takes value $5(\text{mod } 11)$ for $Z_0 = \tau^1$ and $F'_-(Z_0) \not\equiv 0(\text{mod } 11)$ for $Z_0 = \tau^0$, then by lemma 13, if $W \equiv 5(\text{mod } 11)$, then there exists Z such that $Z \equiv \tau^1(\text{mod } 11)$ and $F_-(Z) = W$. Similarly, $F_-(Z_0) \equiv 1(\text{mod } 11)$ and $F'_-(Z_0) \not\equiv 0(\text{mod } 11)$ for $Z_0 = \tau^3$, so, if $W \equiv 1(\text{mod } 11)$, then there exists Z such that $Z \equiv \tau^3(\text{mod } 11)$ and $F_-(Z) = W$; $F_-(Z_0) \equiv 9(\text{mod } 11)$ and $F'_-(Z_0) \not\equiv 0(\text{mod } 11)$ for $Z_0 = \tau^5$, thus, if $W \equiv 9(\text{mod } 11)$, then there exists Z such that $Z \equiv \tau^5(\text{mod } 11)$ and $F_-(Z) = W$; $F_-(Z_0) \equiv 4(\text{mod } 11)$ and $F'_-(Z_0) \not\equiv 0(\text{mod } 11)$ for $Z_0 = \tau^7$, then, if $W \equiv 4(\text{mod } 11)$, then there exists Z such that $Z \equiv \tau^7(\text{mod } 11)$ and $F_-(Z) = W$; $F_-(Z_0) \equiv 3(\text{mod } 11)$ and $F'_-(Z_0) \not\equiv 0(\text{mod } 11)$ for $Z_0 = \tau^9$, therefore, if $W \equiv 3(\text{mod } 11)$, then there exists Z such that $Z \equiv \tau^9(\text{mod } 11)$ and $F_-(Z) = W$. Therefore, the closure of the images of F_- contains the cosets $(5+11\mathbb{Z}) \cup (1+11\mathbb{Z}) \cup (9+11\mathbb{Z}) \cup (4+11\mathbb{Z}) \cup (3+11\mathbb{Z})$.

When $p = 13$, the length of a period of $\mathfrak{G}$ modulo p is 28.

$2i$	0	2	4	6	8
$Z_0 = \tau^{2i} \text{mod } 13$	1	$8+7\sqrt{5}$	$10+8\sqrt{5}$	$9+4\sqrt{5}$	$4+4\sqrt{5}$
$F_+(Z_0) = F_+(\tau^{2i}) \text{mod } 13$	2	7	6	11	1
$F'_+(Z_0) = F'_+(\tau^{2i}) \text{mod } 13$	$12\sqrt{5}$	$11+9\sqrt{5}$	$7+8\sqrt{5}$	$7+4\sqrt{5}$	$11+3\sqrt{5}$

$2i$	10	12	14	16	18
$Z_0 = \tau^{2i} \text{mod } 13$	$3+8\sqrt{5}$	$5+7\sqrt{5}$	12	$5+6\sqrt{5}$	$3+5\sqrt{5}$
$F_+(Z_0) = F_+(\tau^{2i}) \text{mod } 13$	5	1	11	6	7
$F'_+(Z_0) = F'_+(\tau^{2i}) \text{mod } 13$	0	$10+6\sqrt{5}$	$12\sqrt{5}$	$11+9\sqrt{5}$	$7+8\sqrt{5}$

$2i$	20	22	24	26
$Z_0 = \tau^{2i} \bmod 13$	$4+9\sqrt{5}$	$9+9\sqrt{5}$	$10+5\sqrt{5}$	$8+6\sqrt{5}$
$F_+(Z_0) = F_+(\tau^{2i}) \bmod 13$	2	12	8	12
$F'_+(Z_0) = F'_+(\tau^{2i}) \bmod 13$	$7+4\sqrt{5}$	$11+3\sqrt{5}$	0	$10+6\sqrt{5}$

Since $F_+(Z_0) \equiv 2 (\text{mod } 13)$ and $F'_+(Z_0) \not\equiv 0 (\text{mod } 13)$ for $Z_0 = \tau^0$ and τ^{20}, by lemma 13, if $W \equiv 2 (\text{mod } 13)$, then there exists Z such that $Z \equiv \tau^0$ or $\tau^{20} (\text{mod } 13)$ and $F_+(Z) = W$. Similarly, $F_+(Z_0) \equiv 7 (\text{mod } 13)$ and $F'_+(Z_0) \not\equiv 0 (\text{mod } 13)$ for $Z_0 = \tau^2$ and τ^{18}, so, if $W \equiv 7 (\text{mod } 13)$, then there exists Z such that $Z \equiv \tau^2$ or $\tau^{18} (\text{mod } 13)$ and $F_+(Z) = W$; $F_+(Z_0) \equiv 6 (\text{mod } 13)$ and $F'_+(Z_0) \not\equiv 0 (\text{mod } 13)$ for $Z_0 = \tau^4$ and τ^{16}, hence, if $W \equiv 6 (\text{mod } 13)$, then there exists Z such that $Z \equiv \tau^4$ or $\tau^{16} (\text{mod } 13)$ and $F_+(Z) = W$; $F_+(Z_0) \equiv 11 (\text{mod } 13)$ and $F'_+(Z_0) \not\equiv 0 (\text{mod } 13)$ for $Z_0 = \tau^6$ and τ^{14}, so, if $W \equiv 11 (\text{mod } 13)$, then there exists Z such that $Z \equiv \tau^6$ or $\tau^{14} (\text{mod } 13)$ and $F_+(Z) = W$; $F_+(Z_0) \equiv 1 (\text{mod } 13)$ and $F'_+(Z_0) \not\equiv 0 (\text{mod } 13)$ for $Z_0 = \tau^8$ and τ^{12}, hence, if $W \equiv 1 (\text{mod } 13)$, then there exists Z such that $Z \equiv \tau^8$ or $\tau^{12} (\text{mod } 13)$ and $F_+(Z) = W$; $F_+(Z_0) \equiv 12 (\text{mod } 13)$ and $F'_+(Z_0) \not\equiv 0 (\text{mod } 13)$ for $Z_0 = \tau^{22}$ and τ^{26}, therefore, if $W \equiv 12 (\text{mod } 13)$, then there exists Z such that $Z \equiv \tau^{22}$ or $\tau^{26} (\text{mod } 13)$ and $F_+(Z) = W$. Therefore, the closure of the images of F_+ contains the cosets $(2+13\mathbb{Z}) \cup (7+13\mathbb{Z}) \cup (6+13\mathbb{Z}) \cup (11+13\mathbb{Z}) \cup (1+13\mathbb{Z}) \cup (12+13\mathbb{Z})$. Since $F_+(Z_0) \equiv 5 (\text{mod } 13)$ and $F'_+(Z_0) \equiv 0 (\text{mod } 13)$ for $Z_0 = \tau^{10}$, the image of F_+ contains part of the coset $(5 + 13\mathbb{Z})$. Similarly, $F_+(Z_0) \equiv 8 (\text{mod } 13)$ and $F'_+(Z_0) \equiv 0 (\text{mod } 13)$ for $Z_0 = \tau^{24}$, then the image of F_+ contains part of the coset $(8 + 7\mathbb{Z})$.

$2i+1$	1	3	5	7	9
$Z_0 = \tau^{2i+1} \bmod 13$	$7+7\sqrt{5}$	$2+\sqrt{5}$	$12+9\sqrt{5}$	8	$12+4\sqrt{5}$
$F_-(Z_0) = F_-(\tau^{2i+1}) \bmod 13$	5	12	5	3	4
$F'_-(Z_0) = F'_-(\tau^{2i+1}) \bmod 13$	$11+3\sqrt{5}$	0	$10+6\sqrt{5}$	$12\sqrt{5}$	$11+9\sqrt{5}$

$2i+1$	11	13	15	17
$Z_0 = \tau^{2i+1} \bmod 13$	$2+12\sqrt{5}$	$7+6\sqrt{5}$	$6+6\sqrt{5}$	$11+12\sqrt{5}$
$F_-(Z_0) = F_-(\tau^{2i+1}) \bmod 13$	9	10	8	1
$F'_-(Z_0) = F'_-(\tau^{2i+1}) \bmod 13$	$7+8\sqrt{5}$	$7+4\sqrt{5}$	$11+3\sqrt{5}$	0

$2i+1$	19	21	23	25	27
$Z_0 = \tau^{2i+1} \bmod 13$	$1+4\sqrt{5}$	5	$1+9\sqrt{5}$	$11+\sqrt{5}$	$6+7\sqrt{5}$
$F_-(Z_0) = F_-(\tau^{2i+1}) \bmod 13$	8	10	9	4	3
$F'_-(Z_0) = F'_-(\tau^{2i+1}) \bmod 13$	$10+6\sqrt{5}$	$12\sqrt{5}$	$11+9\sqrt{5}$	$7+8\sqrt{5}$	$7+4\sqrt{5}$

The function $F_-(Z_0)$ yields value $5 (\text{mod } 13)$ and $F'_-(Z_0) \not\equiv 0 (\text{mod } 13)$ for $Z_0 = \tau^1$ and τ^5, by lemma 13, if $W \equiv 5 (\text{mod } 13)$, then there exists Z such that $Z \equiv \tau^1$ or $\tau^5 (\text{mod } 13)$ and $F_-(Z) = W$. Similarly, $F_-(Z_0) \equiv 3 (\text{mod } 13)$ and $F'_-(Z_0) \not\equiv 0 (\text{mod } 13)$ for $Z_0 = \tau^7$ and τ^{27}, so, if $W \equiv 3 (\text{mod } 13)$, then there exists Z such that $Z \equiv \tau^7$ or $\tau^{27} (\text{mod } 13)$ and $F_-(Z) = W$; $F_-(Z_0) \equiv 4 (\text{mod } 13)$ and $F'_-(Z_0) \not\equiv 0 (\text{mod } 13)$ for $Z_0 = \tau^9$ and τ^{25}, thus, if $W \equiv 4 (\text{mod } 13)$, then there exists Z such that $Z \equiv \tau^9$ or $\tau^{25} (\text{mod } 13)$ and $F_-(Z) = W$; $F_-(Z_0) \equiv 9 (\text{mod } 13)$ and $F'_-(Z_0) \not\equiv 0 (\text{mod } 13)$ for $Z_0 = \tau^{11}$ and τ^{23}, hence, if $W \equiv 9 (\text{mod } 13)$, then there exists Z such that $Z \equiv \tau^{11}$ or $\tau^{23} (\text{mod } 13)$ and $F_-(Z) = W$; $F_-(Z_0) \equiv 10 (\text{mod } 13)$ and $F'_-(Z_0) \not\equiv 0 (\text{mod } 13)$ for $Z_0 = \tau^{13}$ and τ^{21}, so, if $W \equiv 10 (\text{mod } 13)$, then there exists Z such that $Z \equiv \tau^{13}$ or $\tau^{21} (\text{mod } 13)$ and $F_-(Z) = W$; $F_-(Z_0) \equiv 8 (\text{mod } 13)$ and $F'_-(Z_0) \not\equiv 0 (\text{mod } 13)$ for $Z_0 = \tau^{15}$ and τ^{19}, therefore, if $W \equiv 8 (\text{mod } 13)$, then there exists Z such that $Z \equiv \tau^{15}$ or $\tau^{19} (\text{mod } 13)$ and $F_-(Z) = W$. Therefore, the closure of the images of F_- contains the cosets $(5+13\mathbb{Z}) \cup (3+13\mathbb{Z}) \cup (4+13\mathbb{Z}) \cup (9+13\mathbb{Z}) \cup (10+13\mathbb{Z}) \cup (8+13\mathbb{Z})$.
Since $F_-(Z_0) \equiv 12 (\text{mod } 13)$ and $F'_-(Z_0) \equiv 0 (\text{mod } 13)$ for $Z_0 = \tau^3$, the image of F_- contains part of the coset $(12+13\mathbb{Z})$. Similarly, $F_-(Z_0) \equiv 1 (\text{mod } 13)$ and $F'_-(Z_0) \equiv 0 (\text{mod } 13)$ for $Z_0 = \tau^{17}$, hence the image of F_- contains part of the coset $(1+13\mathbb{Z})$.

5.3 Regular $\mathbb{Z}$-basis for $\mathfrak{G}$

We study a p-ordering for the general sequence $\mathfrak{G}$ at any pair, (A, B), of integers.

Theorem 24. *Let $\{\mathfrak{F}_k\}$ be the sequence of Fibonacci numbers, and let (A, B) be a pair of any integers. Then the general sequence, $\{\mathfrak{G}_k\}$, of integers can be expressed as $\mathfrak{G}_k = A\mathfrak{F}_{k-1} + B\mathfrak{F}_k$ for all $k \geq 1$.*

Proof. The sequence, $\{\mathfrak{F}_k\}$, of Fibonacci numbers can be written as $\mathfrak{F}_{k+1} = \mathfrak{F}_k + \mathfrak{F}_{k-1}$ for all $k \geq 1$ with $\mathfrak{F}_0 = 0$, $\mathfrak{F}_1 = 1$. Then $\mathfrak{F}_k = \mathfrak{F}_{k-1} + \mathfrak{F}_{k-2}$ and $\mathfrak{F}_{k-1} = \mathfrak{F}_{k-2} + \mathfrak{F}_{k-3}$.

We prove our result by induction on k. If $k = 1, 2$, then $\mathfrak{G}_1 = A\mathfrak{F}_0 + B\mathfrak{F}_1 = B$ and $\mathfrak{G}_2 = A\mathfrak{F}_1 + B\mathfrak{F}_2 = A + B$.
Suppose $\mathfrak{G}_n = A\mathfrak{F}_{n-1} + B\mathfrak{F}_n$ holds for all $n < k$. Then $\mathfrak{G}_k = \mathfrak{G}_{k-1} + \mathfrak{G}_{k-2} = A\mathfrak{F}_{k-2} + B\mathfrak{F}_{k-1} + A\mathfrak{F}_{k-3} + B\mathfrak{F}_{k-2} = A(\mathfrak{F}_{k-2} + \mathfrak{F}_{k-3}) + B(\mathfrak{F}_{k-1} + \mathfrak{F}_{k-2}) = A\mathfrak{F}_{k-1} + B\mathfrak{F}_k$ as required. Hence the lemma.

The following corollary follows from the above theorem.

Corollary 7. *Let $\{\mathfrak{F}_k\}$ be the sequence of Fibonacci numbers, and let (A, B) be a pair of any integers. Then a p-ordering of general sequence, $\{\mathfrak{G}_k\}$, of integers is exactly some p-ordering of the sequence $\{A\mathfrak{F}_{k-1} + B\mathfrak{F}_k\}_{k=1}^{\infty}$, and similarly for the p-sequence.*

Now, we need to give a regular $\mathbb{Z}$-basis for $\mathfrak{G}$. For this, we need to find some p-orderings and the associated p-sequences. We replace Maplecode 5 in Maplecode 1 instead of the portion of Lucas numbers for calculating p-orderings and the associated p-sequences.
It is important to note that we already have the results for Fibonacci numbers and Lucas numbers since these sequences are obtained at $(A, B) = (0, 1)$ and $(A, B) = (2, 1)$, respectively.
For $(A, B) = (2, 5)$, p-orderings and the associated p-sequences in the following tables obtained by using the Maplecode 1 after the Maplecode 5 has been inserted in it are consistent with Remark 5:

2-ordering of $\mathbb{Z}$	$\{1, -6, -5, -4, -3, -2, -1, 0, -7, 2, 3, 4, 5, 6, 7\}$
2-ordering of $\mathfrak{G}$	$\{2, 5, 7, 12, 19, 81, 212, 50, 31, 1453, 555, 898, 131, 343, 2351\}$
3-ordering of $\mathbb{Z}$	$\{1, -7, -6, -5, -4, -3, -2, -1, 0, 2, 3, 4, 5, 6, 7\}$
3-ordering of $\mathfrak{G}$	$\{2, 7, 12, 5, 19, 81, 31, 555, 50, 1453, 2351, 343, 131, 898, 212\}$
5-ordering of $\mathbb{Z}$	$\{1, -7, -6, -5, -3, -4, -2, -1, 0, 2, 3, 4, 5, 6, 7\}$
5-ordering of $\mathfrak{G}$	$\{2, 5, 19, 31, 343, 7, 50, 898, 2351, 12, 1453, 81, 555, 212, 131\}$
7-ordering of $\mathbb{Z}$	$\{1, -7, -5, -4, -3, -2, -1, -6, 0, 2, 3, 4, 5, 6, 7\}$
7-ordering of $\mathfrak{G}$	$\{2, 5, 7, 31, 50, 81, 2351, 12, 212, 343, 19, 131, 1453, 555, 898\}$
11-ordering of $\mathbb{Z}$	$\{1, -7, -6, -5, -4, -3, -2, -1, 0, 2, 3, 4, 5, 6, 7\}$
11-ordering of $\mathfrak{G}$	$\{2, 5, 7, 12, 19, 31, 50, 81, 131, 212, 343, 555, 898, 1453, 2351\}$

2-sequence of $\mathbb{Z}$	$\{0,0,1,1,3,3,4,4,7,7,8,8,10,10,11\}$
2-sequence of $\mathfrak{G}$	$\{0,0,1,1,3,4,4,6,7,8,10,13,14,16,19\}$
3-sequence of $\mathbb{Z}$	$\{0,0,0,1,1,1,2,2,2,4,4,4,5,5,5\}$
3-sequence of $\mathfrak{G}$	$\{0,0,0,1,1,1,2,2,3,4,6,7,8,8,12\}$
5-sequence of $\mathbb{Z}$	$\{0,0,0,0,1,1,1,1,2,2,2,2\}$
5-sequence of $\mathfrak{G}$	$\{0,0,0,0,0,1,1,1,1,2,2,3,3,4,5\}$
7-sequence of $\mathbb{Z}$	$\{0,0,0,0,0,0,0,1,1,1,2,3,3,4,7\}$
7-sequence of $\mathfrak{G}$	$\{0,0,0,0,0,0,0,1,1,1,1,2,2,3,4\}$
11-sequence of $\mathbb{Z}$	$\{0,0,0,0,0,0,0,0,0,0,0,1,1,1,1\}$
11-sequence of $\mathfrak{G}$	$\{0,0,0,0,0,0,0,0,0,0,1,1,1,1,1\}$

Now, we will check the p-orderings and p-sequence of $\mathfrak{G}$ manually to get a regular $\mathbb{Z}$-basis for $\mathfrak{G}$.

$\mathfrak{G}$mod 2^k:

The length of a period of $\mathfrak{G}$ mod 2 is 3, and the period is $[0,1,1]$.

The length of a period of $\mathfrak{G}$ mod 4 is 6, and the period is $[2,1,3,0,3,3]$.

The length of a period of $\mathfrak{G}$ mod 8 is 12, and the period is $[2,5,7,4,3,7,2,1,3,4,7,3]$.

There are no numbers in $\mathfrak{G}$ that are congruent to 0 or 6 modulo 8, and hence $2,5,7,12,19,81$ will be the beginning of a 2-ordering with the associated 2-sequence $[0,0,1,1,3,4,4]$.

The numbers in $\mathfrak{G}$ modulo 8 are contained in $(1+2\mathbb{Z}) \cup (2+8\mathbb{Z}) \cup (4+8\mathbb{Z}) = (1+2\mathbb{Z}) \cup 2 \cdot ((1+4\mathbb{Z}) \cup (2+4\mathbb{Z}))$.

The 2-sequences of $1+4\mathbb{Z}$ and $2+4\mathbb{Z}$ are

$\alpha_{\mathbb{Z}} + (2n) = [0,0,1,1,3,3,\cdots] + [0,2,4,6,8,10,\cdots] = [0,2,5,7,11,13,\cdots]$.

The 2-sequence of $1+2\mathbb{Z}$ is

$\alpha_{\mathbb{Z}} + (n) = [0,0,1,1,3,3,\cdots] + [0,1,2,3,4,5,\cdots]$.

The 2-sequence of $(1+4\mathbb{Z}) \cup (2+4\mathbb{Z})$ is the shuffle

$[0,0,2,2,5,5,7,7,\cdots]$, and that of $2 \cdot ((1+4\mathbb{Z}) \cup (2+4\mathbb{Z}))$ is $[0,0,2,2,5,5,7,7,\cdots] + [0,1,2,3,4,5,\cdots] = [0,1,4,5,9,12,\cdots]$.

Thus the 2-sequence of $(1+2\mathbb{Z}) \cup 2 \cdot ((1+4\mathbb{Z}) \cup (2+4\mathbb{Z}))$ is the shuffle

$[0,1,3,4,7,8,\cdots] \wedge [0,4,5,9,12,\cdots] = [0,0,1,1,3,4,4,5,7,8,\cdots]$.

$\mathfrak{G}$mod 3^k:

The length of a period of $\mathfrak{G}$ mod 3 is 8, and the period is $[2,2,1,0,1,1,2,0]$.

The length of a period of $\mathfrak{G}$ mod 9 is 24, and the period is
$[2, 5, 7, 3, 1, 4, 5, 0, 5, 5, 1, 6, 7, 4, 2, 6, 8, 5, 4, 0, 4, 4, 8, 3]$, and all residue classes mod 3^2 occur in $\mathfrak{G}$, and so its 3-sequence will begin $[0, 0, 0, 1, 1, 1, 2, 2, 2, \cdots]$ with the first 9 elements of a 3-ordering having representation from all residue classes mod 9 $[2, 7, 12, 5, 19, 81, 31, 555, 6155]$.

$\mathfrak{G}$ mod 5^k:

The length of a period of $\mathfrak{G}$ mod 5 is 20, and the period is
$[2, 0, 2, 2, 4, 1, 0, 1, 1, 2, 3, 0, 3, 3, 1, 4, 0, 4, 4, 3]$.

The length of a period of $\mathfrak{G}$mod 5^2 is 100, and the period is
$[2, 5, 7, 12, 19, 6, 0, 6, 6, 12, 18, 5, 23, 3, 1, 4, 5, 9, 14, 23, 12, 10, 22, 7, 4, 11, 15, 1, 16, 17, 8, 0, 8, 8, 16, 24, 15, 14, 4, 18, 22, 15, 12, 2, 14, 16, 5, 21, 1, 22, 23, 20, 18, 13, 6, 19, 0, 19, 19, 13, 7, 20, 2, 22, 24, 21, 20, 16, 11, 2, 13, 15, 3, 18, 21, 14, 10, 24, 9, 8, 17, 0, 17, 17, 9, 1, 10, 11, 21, 7, 3, 10, 13, 23, 11, 9, 20, 4, 24, 3]$, and all residue classes modulo 5 and 5^2 are in $\mathfrak{G}$. The 5-sequence of $\mathfrak{G}$ must starts with $[0, 0, 0, 0, 0, 1, 1, 1, \cdots]$, and a 5-ordering will start with $[2, 5, 19, 31, 343, 7, \cdots]$.

Thus the p-sequences of $\mathfrak{G}$ begin:

k	0	1	2	3	4	5	6
$p = 2$	0	0	1	1	3	4	4
$p = 3$	0	0	0	1	1	1	2
$p = 5$	0	0	0	0	0	1	1

Then, we have the denominators of a regular basis for $\mathfrak{G}$ as

k	0	1	2	3
$d(k)$	$2^0 \cdot 3^0 \cdot 5^0 = 1$	$2^0 \cdot 3^0 \cdot 5^0 = 1$	$2^1 \cdot 3^0 \cdot 5^0 = 2$	$2^1 \cdot 3^1 \cdot 5^0 = 6$

k	4	5	6
$d(k)$	$2^3 \cdot 3^1 \cdot 5^0 = 24$	$2^4 \cdot 3^1 \cdot 5^1 = 240$	$2^4 \cdot 3^2 \cdot 5^1 = 720$

The regular basis will be of the form $\dfrac{\prod_{i=0}^{k}(x - a_i)}{d(i)}$, where the a_i's are picked using Chinese remainder theorem to have the following residues:

	a_0	a_1	a_2	a_3	a_4	a_5
mod 2^3	2	5	7	4	3	1
mod 3^2	2	7	3	5	1	0
mod 5^2	2	5	19	6	18	7
	2	205	1119	356	1243	657

Therefore, the regular basis for $Int(\mathfrak{G}, \mathbb{Z})$ is
$\{1, (x-2), \frac{(x-2)(x-205)}{2}, \frac{(x-2)(x-205)(x-1119)}{6}, \frac{(x-2)(x-205)(x-1119)(x-356)}{24},$
$\frac{(x-2)(x-205)(x-1119)(x-356)(x-1243)}{240},$
$\frac{(x-2)(x-205)(x-1119)(x-356)(x-1243)(x-657)}{720}, \cdots\}.$

Chapter 6

Conclusion

By using the method of finding p-orderings and the associated p-sequences of a subset S of $\mathbb{Z}$ due to Bhargava, we develop the results of Keith Johnson and Kira Scheibelhut on the Lucas numbers $\mathfrak{L}$, and we find the regular basis for $Int(\mathfrak{L}, \mathbb{Z})$. For doing this, we find the linear recurrence relation $\mathfrak{L}_{k+1} = \mathfrak{L}_k + \mathfrak{L}_{k-1}$ for $k = 1, 2, 3, \cdots$ with $\mathfrak{L}_0 = 2, \mathfrak{L}_1 = 1$ together with Binet's formula $\mathfrak{L}_k = (\tau)^k + (-\frac{1}{\tau})^k$ with $k = 0, 1, 2, \cdots$ for Lucas numbers having the functions f_+ and f_- whose domains are positive even and odd integers, respectively, extending the functions with their domains to squares and nonsquares of $U(\mathbb{Z}_p)$, respectively, under conditions that the mod p of reduction of τ generates $U(\mathbb{Z}_p)$, and $\tau^{p-1} \not\equiv 1 (\text{mod } p^2)$, its reduction mod p^k generates $U(\mathbb{Z}/(p^k))$. The images of extended maps are the closures, $\bar{\mathfrak{L}}$ of $\mathfrak{L}$ with respect to p-adic topology under the condition $\bar{\mathfrak{L}}/(p^k) = \mathfrak{L}/(p^k)$ for any k. The closures due to images of f_+ and f_- are obtained using the Hensel's lemma for the normal case and the Generalized Hensel's lemma when the tangent of the functions are parallel to the x-axis at some point. We find p-sequences for primes p by applying Maplecodes keeping the consistency with reality how many terms of them we can calculate to get the denominators $d(k)$ of the regular basis, and then using Chinese remainder theorem to the integers modulo p^k, we get a p-ordering $a_0, a_1, a_2, \cdots$, to get the regular basis $\frac{\prod_{i=0}^{k}(x-a_i)}{d(i)}$.

We study the general sequence $\mathfrak{G}$ of integers for any pair (A, B) of integers leaving linear recurrence relation $\mathfrak{G}_{k+1} = \mathfrak{G}_k + \mathfrak{G}_{k-1}$ with $\mathfrak{G}_0 = A$, $\mathfrak{G}_1 = B$ for $k = 1, 2, 3, \cdots$, together with Binet's formula $\mathfrak{G}_k = \frac{1}{\sqrt{5}}[\frac{\sqrt{5}-1}{2} \cdot A + B] \cdot (\tau)^k + \frac{1}{\sqrt{5}}[\frac{1+\sqrt{5}}{2} \cdot A - B] \cdot (\frac{-1}{\tau})^k$ for $k = 0, 1, 2, \cdots$. The results for $(A, B) = (0, 1)$, $(A, B) = (2, 1)$ of sequence $\{\mathfrak{G}_k\}$ are consistent with the results of Keith Johnson and Kira Scheibelhut, and the corresponding results for Lucas numbers. We find the a relation $\mathfrak{G}_k = A\mathfrak{F}_{k-1} + B\mathfrak{F}_k$ for all integers $k \geq 1$ that gives general p-orderings and the p-sequences. For justification, we find regular basis for $Int(\mathfrak{G}, \mathbb{Z})$ taking other particular pair $(A, B) = (2, 5)$.

Bibliography

[1] M. F. Atiyah, I. G. MacDonald, *Introduction to Commutative Algebra*, Addison-Wesley 1969.

[2] M. Bhargava, *The factorial function and generalizations*, Amer. Math. Monthly **107** (2000) 783–799.

[3] J. Boulanger, J.-L. Chabert, S. Evrard, G. Gerbound, *The characteristic sequence of integer-valued polynomials on a subset*, Lect. Notes Pure Appl. Math. **205** (1999) 161–174.

[4] P. -J. Cahen, *Polynomial Closure*, Journal of Number Theory **61** (1996) 226–247.

[5] P. -J. Cahen, J.-L. Chabert, *Integer-Valued Polynomials*, Amer. Math. Soc., Providence, RI, 1997.

[6] J.-L. Chabert, S. Chapman, W. Smith, *Algebraic properties of the ring of integer-valued polynomials on prime numbers*, Commun. Alg. **25** (1997) 1945–1959.

[7] Z. Coelho, W. Parry, *Ergodicity of p-adic multiplications and distribution of Fibonacci numbers*, Amer. Math. Soc. Transl. Ser. 2 **202** (2001) 51–70.

[8] S. T. Chapman, V. Ponomarenko, W. Smith, *Robert Gilmer's Contributions to the Theory of Integer-Valued Polynomials*. Richard A, Dunlap

[9] R. A. Dunlap, *The Golden Ratio and Fibonacci Numbers*, World Scientific Publishing Co. Pte. Ltd, 1997.

[10] E. T. Jacobson, *Distribution of Fibonacci numbers modulo* 2^k, Fibonacci Quart.**30** (1992) 211–215.

[11] K. Johnson, *P-orderings of finite subsets of Dedekind domains*, J. Algebraic Combin. **30(2)** (2009) 233–253.

[12] K. Johnson, *Limits of characteristic sequences of integer-valued polynomials on homogeneous sets*, J. Number Theory **129** (2009) 2933–2942.

[13] K. Johnson, *P-orderings of noncommutative rings*, Proc. AMS **143(8)** (2015) 3265–3279.

[14] K. Johnson, K. Scheibelhut, *Rational Polynomials That Take Integer Values at the Fibonacci Numbers*, The Math. Asso. of Amer. Monthly **123** (2016) 338–346.

[15] N. Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta Functions*, Springer-Verlag, New York, 1984.

[16] M. Matsumara, *Commutative Ring Theory*, Cambridge University Press, Cambridge 1986.

[17] J. S. Milne, *Algebraic Number Theory*, Copyright©2009.

[18] M. Nagata, *Local Rings*, Interscience, New York 1962.

[19] H. Niederreiter, *Distribution of Fibonacci numbers modulo* 5^k, Fibonacci Quart. **4** (1972) 373–374.

[20] A. Ostrowski, *Über Ganzwertige Polynome in Algebraischen Zahlkorper*, J. Reine Angew. Math. **149** (1919) 117–124.

[21] G. Polya, *Über Ganzwertige Polynome in Algebraischen Zahlkorper*, J. Reine Angew. Math. **149** (1919) 97–116.

[22] D. D. Wall, *Fibonacci Series Modulo m*, Am. Math. Monthly 67(6) 525–532.

Appendix

Maplecode 1.

```
with(ListTools):
with(LinearAlgebra):
# The proceedure, "A", calculates the highest power, k, of a prime
# number, p, dividing any number n.
A := proc (n, p) local m, k;
if n = 0 then k := 10000 else
m := n:  k := 0:
while irem(m, p) = 0 do
k := k+1:  m := m/p end do end if:
k:
end:
# The proceedure, "porder", calculates a p-ordering and the
# corresponding associated p-sequence while inputing a sequence of
# integers, L, a prime, p, and the position, l, of an element in
# L such that L[l] is the initial element of a p-ordering of L.
# It is important to note that L1, M, D2, and P1 in th procedure,
# "porder", have the same number of elements after each execution
# of the while loop.
porder:=proc(L,p,l) local Ord,Seq,L1,D1,D2,M,P1,mp,Ps,pm,a,b;
Ord:=[L[l]];Seq:=[0];a:=L[l];L1:=subsop(l=NULL, L);D1:=1:
while (nops(L1) ≠ 0) do
# D2 represents the sequences of differences of element of L1
# and the initial element a_0 and the elements a_l with l ≥ 1 that
# minimize the highest powers of p dividing
# (a_l − a_0)(a_l − a_1) ··· (a_l − a_{l−1}) while finding a p-ordering of L
# until it becomes an empty set.
D2:=[seq(i-a, i=L1)]:
```

```
# M's represent the sequences of products (a_l − a_0)(a_l − a_1) ··· (a_l − a_{l−1}).
M:=[op(D1*∼ D2)]:
# P1's represent the sequences of highest powers of prime p dividing
# (a_l − a_0)(a_l − a_1) ··· (a_l − a_{l−1}).
P1:=[seq(A(i, p), i=M)]:
# mp represents the minimal element in P1 together with its position.
mp:=[FindMinimalElement(P1,position)]:
# Ps is the minimal element of P1.
Ps:=op(1, mp);Seq:=[op(Seq),Ps]:
# pm is the position of the minimal element of P1.
pm:=op(2, mp);Ord:=[op(Ord),L1[pm]]:
b:=L1[pm]:
D2:=subsop(pm=NULL, D2):  M:=subsop(pm=NULL, M):
# D1 is replaced by M after each execution of the while loop in
# the program.
D1:=M:
# L1's represent the sequences of all elements of L excluding the
# initial element a_0 and the elements a_l with l ≥ 1 that minimize the
# highest powers of p dividing (a_l − a_0)(a_l − a_1) ··· (a_l − a_{l−1}) while
# finding a p-ordering of L until it becomes an empty set.
L1:=subsop(pm=NULL, L1):
a:=b:
od;
# Seq is the p-sequence and Ord is a p-ordering of L.
[Ord, Seq]:
end:
```

Maplecode 2.

```
# p is any prime, k ≥ 1 is any integer.
# The proceedure, "Period", yields a period of the sequence of
# Lucas numbers modulo p^k.
Period:=proc(p, k)local L;
# Initialization of the sequence of Lucas numbers modulo p^k.
```

```
L := [2, 1, 3]:
# The while loop executes until the period is obtained.
while [L[nops(L) − 1], L[nops(L)]] ≠ [2, 1] do
L := [op(L), (L[nops(L)] + L[nops(L) − 1])mod p^k] od:
# this L is the period of the sequence of Lucas numbers modulo p^k.
L:
# "ifactor(nops(L) − 2)" calculates the length of a period.
ifactor(nops(L) − 2):
end:
```

Maplecode 3.

```
with(ListTools):
with(LinearAlgebra):
# The proceedure, "Period", calculates the length of a period of
# Lucas numbers mod p.
Period := proc(p) local Lp, lp;
Lp := [2, 1, 3]:
while [Lp[nops(Lp) − 1], Lp[nops(Lp)]] ≠ [2, 1] do
Lp := [op(Lp), (Lp[nops(Lp)] + Lp[nops(Lp) − 1]mod p)] od:
# Lp is a period of Lucas numbers mod p.
Lp:
# lp is the length of Lp.
lp := nops(Lp)-2:
end:
# The proceedure, "LHenfp", calculates images of f_+(z_0)mod p.
LHenfp := proc (p) local L, i, t;
t := 1/2 + (1/2) ∗ sqrt(5):
L := []:  for i from 0 by 2 to Period(p)-1 do
L :=[op(L), (simplify(t^i + rationalize(1/t^i))mod p)]:
od:
# L is the image of f_+(z_0)mod p.
L:
end:
```

```
# The proceedure, "LHendfp", calculates images of f'+(z0)mod p.
LHendfp := proc (p) local L, i, t;
t := 1/2 + (1/2) * sqrt(5):
L := []:  for i from 0 by 2 to Period(p)-1 do
L :=[op(L), (simplify(1 - rationalize(1/t^(2*i)))mod p)]:
od:
# L is the image of f'+(z0)mod p
L:
end:
# The proceedure, "LHenfn", calculates images of f-(z0)mod p.
LHenfn := proc (p) local L, i, t;
t := 1/2 + (1/2) * sqrt(5):
L := []:  for i from 1 by 2 to Period(p)-1 do
L := [op(L), (simplify(t^i - rationalize(1/t^i))mod p)]:
od:
# L is the image of f-(z0)mod p.
L:
end:
# The proceedure, "LHendfn", calculates images of f'-(z0)mod p.
LHendfn := proc (p) local L, i, t;
t := 1/2 + (1/2) * sqrt(5):
L :=[]; for i from 1 by 2 to Period(p)-1 do
L := [op(L), (simplify(1 + rationalize(1/t^(2*i)))mod p)]:
od:
# L is the image of f'-(z0)mod p.
L:
end:
```

Maplecode 4.

```
with(ListTools):
with(LinearAlgebra):
# The proceedure, "Period", calculates the length of a period of
# 𝔊 mod p.
```

```
Period := proc(p) local A, B, Gp, C, Lp;
C := A+B:
Gp := [A, B, C]:
while [Gp[nops(Gp) − 1], Gp[nops(Gp)]] ≠ [A, B] do
Gp :=[op(Gp), (Gp[nops(Gp)] + Gp[nops(Gp) − 1])mod p]:
od:
# Gp is a period of 𝔊mod p.
Gp:
# Lp is the length of Gp.
Lp := nops(Gp)-2:
end:
# The proceedure, "GHenFp", calculates the images of F+(Z0) mod p
# for any pair, (A, B), of integers, t = τ, p is any odd prime, and
# C1 and C2 are constants of Binet's formula due to the General
# sequence.
GHenFp := proc (p, A, B) local G, i, t, C1, C2;
t := 1/2 + (1/2) ∗ sqrt(5):
C1 := (rationalize(1/t) ∗ A + B)/sqrt(5):
C2 := (t ∗ A − B)/sqrt(5):
G := []:
for i from 0 by 2 to Period(p)-1 do
G := [op(G), simplify(C1 ∗ t^i + C2 ∗ rationalize(1/t^i))mod p]:
od:
# G is the image of F+(Z0) mod p.
G:
end:
# The proceedure, "GHendFp", calculates the images of F'+(Z0)
# mod p for any pair, (A, B), of integers.
# Other variables bear the same meanings as before.
GHendFp := proc (p, A, B) local G, i, t, C1, C2;
t :=1/2 + (1/2) ∗ sqrt(5):
C1 :=(rationalize(1/t) ∗ A + B)/sqrt(5):
```

```
C2 :=(t * A - B)/sqrt(5):
G := []:
for i from 0 by 2 to Period(p)-1 do
G := [op(G), simplify(C1 - C2 * rationalize(1/t^(2*i)))mod p]:
od:
# G is the image of F'_+(Z_0) modp.
G:
end:
# The proceedure, "GHenFn", calculates the images of F_-(Z_0)
# mod p for any pair, (A, B), of integers.
# Other variables bear the same meanings as before.
GHenFn := proc (p, A, B) local G, i, t, C1, C2;
t := 1/2 + (1/2) * sqrt(5):
C1 := (rationalize(1/t) * A + B)/sqrt(5):
C2 := (t * A - B)/sqrt(5):
G := []:
for i from 1 by 2 to Period(p)-1 do
G := [op(G), simplify(C1 * t^i - C2 * rationalize(1/t^i))mod p]:
od:
# G is the image of F_-(Z_0)mod p.
G:
end:
# The proceedure, "GHendFn", calculates the images of F'_-(Z_0) mod p
# for any pair, (A, B), of integers.
# Other variables bear the same meanings as before.
GHendFn := proc (p, A, B) local G, i, t, C1, C2;
t :=1/2 + (1/2) * sqrt(5) :
C1 := (rationalize(1/t) * A + B)/sqrt(5):
C2 := (t * A - B)/sqrt(5):
G := []:
for i from 1 by 2 to Period(p)-1 do
G := [op(G), simplify(C1 + C2 * rationalize(1/t^(2*i)))mod p]:
```

```
od:
# G is the image of F'_(Z_0)mod p.
G:
end:
```

Maplecode 5.

```
# The proceedure, "Fibo", finds the sequence of Fibonacci numbers
Fibo := proc (n) local F, i;
F := [0, 1]:
for i from 2 to n do
F := [op(F), F[-1]+F[-2]]:
od:
F:
end:
# The proceedure, "GSeq", finds the general sequence of integers at
# any pair, (A, B), of integers.
GSeq := proc (m, A, B) local G, i, Fb;
Fb := Fibo(m):
G := [A, B]:
for i from 3 to m do G := [op(G), A*Fb[i-1]+B*Fb[i]]:
od:
G:
end:
```