Profinite Number Theory

Bachelor's Thesis in Mathematics

Author:
David Hokken

Supervisor:
Prof. dr. Frits Beukers

June 9, 2018

Utrecht University

Abstract

In this thesis, we provide background and proofs of some of the results stated in the articles of H.W. Lenstra on profinite number theory [Len05, Len16]. We start by constructing the topological ring of profinite integers, known as $\hat{\mathbf{Z}}$ (pronounced "Zee-hat"), as the completion of the integers with respect to a certain metric in Chapter 3. This leads to an investigation of its connection to p-adic rings $\mathbf{Z}_p$ and the subsequent introduction of the profinite logarithm in Chapter 4. Aided by this machinery, we study the extension of the Fibonacci map to the ring of profinite integers and its fixed points in Chapter 5.

Contents

Acknowledgements

This thesis would not have been completed without the help of several individuals. First and foremost, I would like to thank prof. dr. Frits Beukers for his guidance and all insightful and encouraging meetings during the process, and for introducing me to this subject.

Secondly, I would like to thank my parents and sister for their continued support during the last few months.

1 Introduction

Although the so-called *profinite integers* form an important technical tool in various parts of arithmetic geometry and algebraic number theory, such as infinite Galois theory, their own virtues "have never been recognized" (Lenstra, [Len05]). Therefore, their little-known but remarkable properties have not been studied extensively. The present thesis serves as an introduction to profinite integers and some of their striking properties, which have been presented informally in the articles of H. W. Lenstra on the subject (see [Len05, Len16]).

Profinite integers may be defined in several equivalent ways. The following is the most straightforward approach. Note that every positive integer n has a unique representation – called the *factorial representation* – as

$$n = c_1 \cdot 1! + c_2 \cdot 2! + \cdots + c_{k-1} \cdot (k-1)! + c_k \cdot k! \stackrel{\text{def}}{=} (c_k \dots c_3 c_2 c_1)_!,$$

with $c_i \in \mathbf{Z}$, $0 \leq c_i \leq i$, for every positive integer $i \leq k$, and $c_k \neq 0$. For example, we can write $6 = (100)_!$ and $49 = (2001)_!$. The number k is, in the case of positive integers, always finite. However, permitting k to become arbitrarily large, we obtain the desired profinite integers, which are of the form

$$c_1 \cdot 1! + c_2 \cdot 2! + c_3 \cdot 3! + \cdots = (\dots c_3 c_2 c_1)_!.$$

These new numbers are not integers in the ordinary sense, and require a theoretical framework to be explored formally and in depth. This will be done in Chapter 3. There, the space of profinite integers $\hat{\mathbf{Z}}$ will be introduced as the Cauchy completion of $\mathbf{Z}$ with respect to a certain metric.

In Chapter 4, we prove that profinite integers can indeed be identified uniquely with their factorial representation. This representation, as the observant reader may note, is strongly reminiscent of the p-adic integers: these can be represented as $c_0 p^0 + c_1 p^1 + c_2 p^2 + \cdots = (\dots c_3 c_2 c_1)_p$ for some fixed prime number p and integers c_i with $0 \leq c_i \leq p-1$, for every i. Chapter 4 shows that this intuition is justified: we prove that there exists an isomorphism of topological rings between $\hat{\mathbf{Z}}$ and the product space of all p-adic rings. Lastly, Chapter 4 describes the p-adic and profinite logarithms, which we need in Chapter 5 of this thesis: a study of the extension of the Fibonacci map to the profinite integers and its fixed points.

As for prerequisites, although the reader may be helped with the extensive list of definitions and theorems in Chapter 2 (making the thesis almost self-contained), he may surely take advantage of any basic knowledge pertaining to topology and number theory.

2 Preliminaries

The content of this thesis resides in the domain of number theory and topology, where the latter is most often used to provide a foundation for the main results concerning the former. The notions recalled in the following subsections provide a starting point to the reader in his study of profinite integers. These definitions and results can be found (with proofs) in any elementary textbook, see for example Crainic [Cra16] for the topology and Beukers [Beu15] for the number theory part.

2.1 Topology

Definition 2.1. *Let X be a set and $\mathcal{T}$ a collection of subsets of X. Then $\mathcal{T}$ is a* ***topology*** *on X if*

(1). $\mathcal{T}$ contains the empty set and X.

(2). Any union of members of $\mathcal{T}$ is a member of $\mathcal{T}$.

(3). Any finite intersection of members of $\mathcal{T}$ is a member of $\mathcal{T}$.

The pair $(X, \mathcal{T})$ is called a ***topological space*** *and is often denoted simply by X. The members of $\mathcal{T}$ are called* ***open sets*** *or* ***opens****, and their complements are the* ***closed sets****.*

Definition 2.2. *Let X be a set and $\mathcal{B}$ a collection of subsets of X. Then $\mathcal{B}$ is called a* ***topology basis*** *if*

(1). For any $x \in X$, there exists a $B \in \mathcal{B}$ such that $x \in B$.

(2). For any $B_1, B_2 \in \mathcal{B}$ and $x \in B_1 \cap B_2$, there exists a $B \in \mathcal{B}$ such that $x \in B \subset B_1 \cap B_2$.

Furthermore, $\mathcal{B}$ induces a topology $\mathcal{T} = \mathcal{T}(\mathcal{B})$ given by the collection

$$\mathcal{T} \stackrel{\text{def}}{=} \{U \subset X : \exists\, \mathcal{B}' \subset \mathcal{B} : U = \cup_{B \in \mathcal{B}'} B\}.$$

Definition 2.3. *Let X and Y be topological spaces. Recall the following notions:*

(1). A map $f : X \to Y$ is ***continuous*** *if $f^{-1}(U)$ is open in X for any open $U \subset Y$.*

(2). X is called ***Hausdorff*** *if for any two distinct points $x, y \in X$ there exist opens U, V in X such that $x \in U$, $y \in V$ and $U \cap V = \varnothing$.*

(3). *Given a subset A of X, the* ***induced topology*** $\mathcal{T}|_A$ *on A consists of all subsets B of A such that $B = U \cap A$ for some $U \in \mathcal{T}$.*

(4). *X is called* ***connected*** *if it cannot be written as the union of two disjoint, nonempty opens. Furthermore, any $C \subset X$ is called connected if C, together with the induced topology, is connected.*

(5). *X is called* ***totally disconnected*** *if each connected subset $C \subset X$ is a singleton, i.e. $C = \{x\}$ for some $x \in X$.*

(6). *A* ***cover*** *of X is a family $\mathcal{U}$ of subsets of X, such that $\bigcup_{U \in \mathcal{U}} U = X$. The cover is* ***open*** *if each of the subsets $U \in \mathcal{U}$ is open. Furthermore, X is called* ***compact*** *if each of its open covers admits a finite open subcover; that is, if for any open cover $\mathcal{U}$ there is a finite subcollection $\mathcal{F} \subset \mathcal{U}$ such that $\bigcup_{U \in \mathcal{F}} U = X$.*

(7). *A sequence of elements $(x_n)_{n=1}^{\infty}$* ***converges*** *to $x \in X$ if for every open U, containing x, there exists an integer $N \geq 0$ such that $x_n \in U$ for all $n \geq N$. Furthermore, X is called* ***sequentially compact*** *if any sequence $(x_n)_{n=1}^{\infty} \in X$ has a convergent subsequence.*

(8). *We can construct a topology on $X \times Y$, known as the* ***product topology****, by declaring a subset $D \subset X \times Y$ to be open if and only if for all $(x, y) \in D$ there exist opens $U \subset X$ and $V \subset Y$ such that $x \in U$, $y \in V$ and $U \times V \subset D$.*

(9). *Given a subset A of X, we can form its* ***closure****, denoted $\overline{A}$, which is the smallest closed subset of X containing A. If the closure of A equals the whole space X, then A is called* ***dense*** *in X.*

Lemma 2.4. *Any continuous bijection from a compact space to a Hausdorff space is a homeomorphism.*

Definition 2.5. *Let (X, d) be a metric space. Recall that the* ***topology induced by d*** *is defined as the collection $\mathcal{T}_d$ of subsets of X given by*

$$\mathcal{T}_d \stackrel{\text{def}}{=} \{U \subset X : \forall x \in U \, \exists \epsilon > 0 : B_d(x, \epsilon) \subset U\}.$$

The pair $(X, \mathcal{T}_d)$ is a topological space.

Lemma 2.6. *Let X be a metric space. Then X is compact if and only if it is sequentially compact.*

Definition 2.7. *A metric space X is called* ***complete*** *if all Cauchy sequences converge (to a limit inside the space).*

Lemma 2.8 ([Sea06], p. 176)**.** *Any uniformly continuous function $X \to Y$ between metric spaces has a unique continuous extension $\hat{X} \to Y$, if X is dense in $\hat{X}$ and Y is complete.*

2.2 Rings and number theory

Let p be a prime number and n a positive integer.

Lemma 2.9. *Recall that we say that a and b are* ***congruent*** *modulo n and write $a \equiv b \pmod{n}$ if $a - b$ is divisible by n. Given integers a, a', b, b' and k such that $a \equiv a' \pmod{n}$ and $b \equiv b' \pmod{n}$, the mod operator, also called the congruence relation, satisfies the following properties:*

(1). It is an equivalence relation.

(2). $a + kb \equiv a' + kb' \pmod{n}$.

(3). $ab \equiv a'b' \pmod{n}$.

(4). $a^k \equiv (a')^k \pmod{n}$ if $k \geq 0$.

Lemma 2.10. *The equation $ax \equiv b \pmod{n}$ is solvable if $\gcd(a, n)$ divides b. In that case, the total number of solutions is $\gcd(a, n)$, and if s is some particular solution, the full set of solutions is given by*

$$\left\{ s + \frac{kn}{\gcd(a,n)} : k \in \mathbf{Z}, 0 \leq k < \gcd(a,n) \right\}. \tag{2.1}$$

Definition 2.11. *Recall that two integers a, b are said to be* ***coprime*** *if $\gcd(a, b) = 1$. The function that counts the number of positive integers less than a given integer n which are coprime to n, is known as the* ***Euler totient function*** *and denoted by $\varphi(n)$. In particular, $\varphi(p) = p - 1$.*

Theorem 2.12 (Euler)**.** *Let a be an integer coprime to n. Then $a^{\varphi(n)} \equiv 1 \pmod{n}$.*

Corollary 2.13 (Fermat's little theorem)**.** *Let a be any integer. Then $a^p \equiv a \pmod{p}$.*

Theorem 2.14 (Wilson)**.** *Let $n!$ denote the factorial of n. Then*

$$(p-1)! \equiv -1 \pmod{p}. \tag{2.2}$$

Corollary 2.15. *We have* $(p-2)! \equiv 1 \pmod{p}$.

Definition 2.16. *Recall that* a *is said to be a* ***quadratic residue (mod*** p***)*** *if there exists an* x *such that* $x^2 \equiv a \pmod{p}$. *The associated* ***Legendre symbol*** *is defined as*

$$\left(\frac{a}{p}\right) \stackrel{\text{def}}{=} \begin{cases} 1 & \text{if } a \text{ is a quadratic residue } \pmod{p} \text{ and } a \not\equiv 0 \pmod{p}, \\ -1 & \text{if } a \text{ is a quadratic nonresidue } \pmod{p}, \\ 0 & \text{if } a \equiv 0 \pmod{p}. \end{cases} \tag{2.3}$$

Lemma 2.17. *Let* a *be an integer. Then* $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$.

Lemma 2.18 (Quadratic reciprocity)**.** *Let* p *and* q *be prime numbers. Then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}. \tag{2.4}$$

Theorem 2.19 (Chinese Remainder Theorem)**.** *Let* $n = n_1 n_2 \cdots n_k$ *be a factorization of* n *into* k *coprime factors. Then the map*

$$\phi : \mathbf{Z}/n\mathbf{Z} \to \mathbf{Z}/n_1\mathbf{Z} \times \cdots \times \mathbf{Z}/n_k\mathbf{Z},$$
$$\phi(x \pmod{n}) \stackrel{\text{def}}{=} (x \pmod{n_1}, \ldots, x \pmod{n_k}),$$

is a ring isomorphism.

Definition 2.20. *Recall that the tuple* $(R, +, \cdot)$ *is called a* ***ring*** *when* $+$ *(addition) and* $\cdot$ *(multiplication) are binary operations on* R *such that*

(1). $(R, +)$ *is an abelian group.*

(2). Multiplication is associative, and there exist an element $1 \in R$ *such that* $1 \cdot r = r = r \cdot 1$ *for all* $r \in R$.

(3). Multiplication is (left and right) distributive with respect to addition.

A subset S *of a ring* R *is a* ***subring*** *of* R *when* S *with the addition and multiplication of* R *forms a ring itself, and has the same multiplicative identity as* R. *Furthermore, we say that* R *is a* ***topological ring*** *if it is a ring and the operations of addition and multiplication are continuous as maps* $R \times R \longrightarrow R$.

3 Construction of the topological ring of profinite integers

There are several ways to define the ring $\hat{\mathbf{Z}}$ of profinite integers. To avoid category-theoretical constructions, we will define a topology on $\mathbf{Z}$, which turns out to be induced by a metric; see section 3.1. Once this is done, we show in 3.2 that $\hat{\mathbf{Z}}$ can be defined as the Cauchy completion of $\mathbf{Z}$ with respect to this metric. The final section 3.3 of this chapter is a small investigation into the ring theoretic properties of $\hat{\mathbf{Z}}$.

3.1 A metric topology on the integers

The somewhat unconventional topology which forms the starting point of our study of profinite integers, is known as the **Furstenberg topology**, named after Hillen Furstenberg (who used the space to give an elegant topological proof of the infinitude of the primes (see [LM15, Fur55])), and is defined by means of the following basis.

Lemma 3.1. *Given integers $m > 0$ and a, let $a + m\mathbf{Z} = \{a + km : k \in \mathbf{Z}\}$ denote the associated arithmetic progression, and let $\mathcal{B} = \{a + m\mathbf{Z} : a, m \in \mathbf{Z},\, m > 0\}$ be the collection of all such progressions. Then $\mathcal{B}$ is a topology basis.*

Proof. Any $x \in \mathbf{Z}$ is contained in the basis member $x + m\mathbf{Z}$. Furthermore, if B_1 and B_2 are members of $\mathcal{B}$ and x an element in their intersection, then we can write $B_1 = x + m\mathbf{Z}$ and $B_2 = x + n\mathbf{Z}$ for some integers m and n greater than 0. Defining $B = x + mn\mathbf{Z}$ we obtain $x \in B \subset B_1 \cap B_2$. Hence $\mathcal{B}$ is a topology basis. ∎

The topology $\mathcal{T}$, induced by $\mathcal{B}$, is therefore given by the collection $\mathcal{B}$ together with the empty set and arbitrary unions of members of $\mathcal{B}$ (see Definition 2.2). The resulting topological space $(\mathbf{Z}, \mathcal{T})$ is often called the **Furstenberg space**. It has the property that any arithmetic progression $a + m\mathbf{Z}$ is open (by definition) as well as closed: it is the complement of

$$\bigcup_{b=1}^{m-1} (a + b) + m\mathbf{Z},$$

which is a union of opens.

The Furstenberg topology has the property that it is metrizable. An explicit metric that induces $\mathcal{T}$ arises from the following, somewhat peculiar function on $\mathbf{Z}$. Define

$$|\cdot| : \mathbf{Z} \longrightarrow \mathbf{R}_{\geq 0}, \quad |n| \overset{\text{def}}{=} \begin{cases} 0 & \text{if } n = 0, \\ 1/\max\{k \,:\, n \equiv 0 \pmod{k!}\} & \text{else.} \end{cases} \tag{3.1}$$

In short, $|\cdot|$ measures the divisibility of an integer by factorial numbers. (For some, this may seem reminiscent of the p-adic absolute value – and this is not entirely coincidental, as we shall see later on.) We shall refer to this function as 'the absolute value (on $\mathbf{Z}$)', even though it does not satisfy the usual multiplicative rule $|mn| = |m||n|$. Instead, it has the following properties.

Lemma 3.2. *The absolute value $|\cdot|$ satisfies the following properties, for all $m, n \in \mathbf{Z}$:*

(1). $|m| \geq 0$, *and* $|m| = 0$ *if and only if* $m = 0$.

(2). $|m+n| \leq \max\{|m|, |n|\}$, *and* $|m| > |n|$ *implies* $|m+n| = |m|$.

(3). $|mn| \leq \min\{|m|, |n|\}$.

(4). $|-m| = |m|$.

(5). $|n|$ *is equal to the reciprocal of some positive integer if* $n \neq 0$.

Proof. The properties (1), (4) and (5) hold by definition. If m or n equals 0, all statements hold trivially. Therefore, let m and n be integers different from 0. Then there exist m' and n', and maximal (positive) k_1 and k_2, such that $m = k_1! \cdot m'$ and $n = k_2! \cdot n'$. Assume without loss of generality that $k_1 \leq k_2$. Hence $|m| = 1/k_1 \geq 1/k_2 = |n|$. Then

$$m + n = k_1! \cdot (m' + (k_1 + 1) \cdot \ldots \cdot k_2 \cdot n').$$

If k_1 is strictly less than k_2, then $(k_1 + 1)!$ can't divide $m + n$, by maximality of k_1. If $k_1 = k_2$ then it may occur that $k_1 + 1$ divides the expression in the parenthesis on the right-hand side (for instance, take $m = n = 1$), hence the presence of the inequality sign is necessary. This proves (2). For (3), since

$$mn = k_2! \cdot k_1! m' n',$$

we have $|mn| \leq |n|$. The inequality may be strict when m' is divisible by $k_2 + 1$. ∎

The absolute value naturally gives rise to a metric on $\mathbf{Z}$, defined as $d : \mathbf{Z} \times \mathbf{Z} \longrightarrow \mathbf{R}_{\geq 0}$ by $d(x, y) = |x - y|$. Property (1) ensures that $d(x, y) = 0$ holds if and only if $x = y$, and the fourth property guarantees that $d(x, y) = d(y, x)$, so that d is, in fact, symmetric. Moreover, by property (2) we have $d(x, z) = |x - z| = |x - y + y - z| \leq \max\{|x - y|, |y - z|\}$. Hence d satisfies

$$d(x, z) \leq \max\{d(x, y), d(y, z)\},$$

which is the so-called **ultrametric inequality**, a stronger version of the triangle inequality. The map d, which we have just indeed proven to be a metric, is for this reason sometimes called **non-Archimedean**.

As mentioned before, we need the topology $\mathcal{T}_d$ induced by d to be the same as $\mathcal{T}$. It has the basis $\mathcal{B} = \{B_d(x,r) : x \in \mathbf{Z},\, r > 0\}$ of open balls, where each ball is defined as $B_d(x,r) \overset{\text{def}}{=} \{y \in \mathbf{Z} : d(x,y) = |x-y| < r\}$. By property (5) of Lemma 3.2, we might as well take r to be the reciprocal of a positive integer, so that we can redefine the basis to be the countable collection $\mathcal{B} = \{B_d(x,\, 1/n) : x, n \in \mathbf{Z},\, n > 0\}$.

The condition $d(x,y) < 1/n$ is equivalent to $\max\{k : x \equiv y \pmod{k!}\} > n$. This is satisfied by all $y \in \mathbf{Z}$ with $x \equiv y \pmod{(n+1)!}$; conversely, all y that satisfy the condition also satisfy $x \equiv y \pmod{(n+1)!}$. Hence

$$B_d(x, 1/n) = x + (n+1)!\mathbf{Z}.$$

Lemma 3.3. *The topology $\mathcal{T}_d$, induced by the metric d, coincides with $\mathcal{T}$.*

Proof. By the preceding observations, it is clear that $\mathcal{T}_d \subset \mathcal{T}$, since $\mathcal{T}$ contains all arithmetic progressions. For the other inclusion, let $a + b\mathbf{Z} \in \mathcal{T}$. If $b = 1$, the result is clear since $\mathbf{Z} = (1 + 2!\mathbf{Z}) \cup 2!\mathbf{Z}$. If $b > 1$, then we can write

$$a + b\mathbf{Z} = \bigcup_{k=0}^{(b-1)!-1} (a + kb) + b!\mathbf{Z},$$

which is a union of members of $\mathcal{T}_d$, so $a + b\mathbf{Z} \in \mathcal{T}_d$. ∎

From now on, $\mathbf{Z}$ will refer to the space $(\mathbf{Z}, \mathcal{T})$. To conclude this subsection, we state the following.

Lemma 3.4. $\mathbf{Z}$ *is a topological ring.*

Proof. We need to show that addition and multiplication are continuous. In fact, we will show that they are uniformly continuous. Assume that $a \equiv a' \pmod{k!}$ and $b \equiv b' \pmod{k!}$. Elementary properties of divisibility (see Lemma 2.9) imply that $ab \equiv a'b' \pmod{k!}$ and $a + b \equiv a' + b' \pmod{k!}$. This already shows that addition and multiplication are uniformly continuous: indeed, if $k > 1$, the assumptions imply that

$a' \in B_d(a, 1/(k-1))$ and $b' \in B_d(b, 1/(k-1))$, and hence we deduce that

$$a' + b' \in B_d\left(a+b, \frac{1}{k-1}\right), \quad a'b' \in B_d\left(ab, \frac{1}{k-1}\right). \qquad \blacksquare$$

See also [LM15] for more properties of the Furstenberg space.

3.2 The Cauchy completion of the integers

The Cauchy completion $\hat{X}$ of a metric space X can be regarded as the space X to which precisely those points are added that make all Cauchy sequences converge with a limit in $\hat{X}$. The space $\hat{X}$ is hence complete. The completion comes equipped with an isometric (that is, distance-preserving) embedding $\imath : X \hookrightarrow \hat{X}$, such that $\imath(X)$ is dense in $\hat{X}$. Hence, in some sense, $\hat{X}$ is the 'smallest' complete space containing an isometrically embedded copy of X.

In this context, Cauchy sequences in $\mathbf{Z}$ take the following form.

Lemma 3.5. *Let $(a_n)_{n=1}^{\infty}$ be a sequence in $\mathbf{Z}$. Then $(a_n)_{n=1}^{\infty}$ is Cauchy if and only if for all integers $N > 0$ there exists an $r > 0$, such that for all $n \geq r$,*

$$a_{n+1} \equiv a_n \pmod{N!}.$$

Proof. For $N = 1$, the statement is trivial. By definition, $(a_n)_{n=1}^{\infty}$ is Cauchy if and only if for all $N > 1$ there exists an $r = r(N)$ such that $d(a_m, a_n) = 1/(\max\{k : a_m \equiv a_n \pmod{k!}\}) < 1/(N-1)$ for all $m, n \geq r$; that is, if and only if $a_m \equiv a_n \pmod{N!}$. As a direct consequence we have that $a_{n+1} \equiv a_n \pmod{N!}$. On the other hand, if $a_{n+1} \equiv a_n \pmod{N!}$ for all $n \geq r$, then

$$\ldots \equiv a_{r+3} \equiv a_{r+2} \equiv a_{r+1} \equiv a_r \pmod{N!}.$$

In other words, $a_m \equiv a_n \pmod{N!}$ for all $m, n \geq r$. $\blacksquare$

Many Cauchy sequences do not converge in $\mathbf{Z}$. A generic example which shall occur as a motif in various places in this thesis, is the sequence $(a_n)_{n=1}^{\infty}$ given by $a_n = \sum_{k=1}^{n} k!$, for all n. In order to make this type of sequences converge, the space $\mathbf{Z}$ needs to be completed.

We will denote the space of Cauchy sequences in $\mathbf{Z}$ by $CS(\mathbf{Z})$. Let $x = (x_n)_{n=1}^{\infty}$ and $y = (y_n)_{n=1}^{\infty}$ be two Cauchy sequences. Define

$$d' : CS(\mathbf{Z}) \times CS(\mathbf{Z}) \to \mathbf{R}_{\geq 0}, \quad d'(x, y) \stackrel{\text{def}}{=} \lim_{n\to\infty} d(x_n, y_n).$$

Note that d' is well-defined since the sequence $(d(x_n, y_n))_{n=1}^{\infty}$ is a Cauchy sequence in the complete space $\mathbf{R}$, so the limit on the right-hand side exists.
However, d' can't be a metric: any two Cauchy sequences x and y that eventually coincide, satisfy $d'(x, y) = 0$, and, of course, we can easily manage for x and y to be distinct by letting the initial terms be different. So d' is degenerate.

In fact, d' is still symmetric and satisfies the ultrametric inequality, which follows immediately from the (similar) properties of d. Such a d' is often called a **pseudometric**. The failure of d' to be a metric shows that the space of Cauchy sequences needs some modification to suit our purposes. Luckily, we only need a small adjustment, consisting of modding out the 'right' sequences; the pseudometric d' then descends to the resulting quotient – which is defined to be $\hat{\mathbf{Z}}$ – where it transforms back to a full-fledged metric. Formally, we have an equivalence relation $\sim$ on $CS(\mathbf{Z})$, given by

$$x \sim y \Leftrightarrow d'(x, y) = 0,$$

and the space of **profinite integers** defined as the quotient

$$\hat{\mathbf{Z}} \stackrel{\text{def}}{=} CS(\mathbf{Z})/\sim,$$

which has elements $[x] = \{y \in CS(\mathbf{Z}) : x \sim y\}$, where $x \in [x]$ is an arbitrary representative. 'Having distance zero' is easily seen to be an equivalence relation, using the properties of d'. Clearly, $d'(x, x) = 0$, and if $d'(x, y) = 0$, then also $d'(y, x) = 0$ by symmetry. Furthermore, if $d'(x, y) = d'(y, z) = 0$, then $d'(x, z) = 0$ by the non-Archimedean property.
The equivalence relation $\sim$ resolves the degeneracy of d'. The metric on $\hat{\mathbf{Z}}$ can now be defined as

$$\hat{d} : \hat{\mathbf{Z}} \times \hat{\mathbf{Z}} \to \mathbf{R}_{\geq 0}, \quad \hat{d}([x], [y]) \stackrel{\text{def}}{=} d'(x, y).$$

Lemma 3.6. *The map $\hat{d}$ is a well-defined ultrametric.*

Proof. For the first part we have to check that any $x, x' \in [x]$ and $y, y' \in [y]$ satisfy

$d'(x,y) = d'(x',y')$. Note that $d'(x,x') = d'(y,y') = 0$. By the non-Archimedean property of d', we have $d'(x,y) \leq \max\{d'(x,x'),\, d'(x',y)\}$. Expanding this further (by again using the non-Archimedean property) yields

$$\begin{aligned} d'(x,y) &\leq \max\{d'(x,x'),\, \max\{d'(x',y'),\, d'(y',y)\}\}, \\ &= \max\{d'(x,x'),\, d'(x',y'),\, d'(y',y)\}, \\ &= d'(x',y'). \end{aligned}$$

Interchanging x with x' and y with y' gives $d'(x',y') \leq d'(x,y)$ in a similar fashion. Hence $d'(x,y) = d'(x',y')$, so $\hat{d}$ is well-defined.
The fact that $\hat{d}$ is an ultrametric follows immediately from the non-Archimedean property of d'. ■

As promised, we have the following:

Lemma 3.7. *Let $\imath$ be the canonical inclusion given by*

$$\imath : \mathbf{Z} \hookrightarrow \hat{\mathbf{Z}}, \quad n \mapsto [n] \stackrel{\text{def}}{=} [(n,n,n,\ldots)].$$

Then $\imath$ is an isometric embedding and $\imath(\mathbf{Z})$ is dense in $\hat{\mathbf{Z}}$.

Proof. Clearly,

$$\hat{d}(\imath(m),\imath(n)) = \hat{d}([m],[n]) = d'((m,m,\ldots),(n,n,\ldots)) = \lim_{i\to\infty} d(m,n) = d(m,n),$$

for any m and $n \in \mathbf{Z}$. Hence $\imath$ is an isometry. By nondegeneracy of d, we see that $\imath$ is injective: indeed, if $\imath(m) = \imath(n)$, then $d(m,n) = \hat{d}(\imath(m),\imath(n)) = 0$, and hence $m = n$.
To prove the second statement, let $[x] \in \hat{\mathbf{Z}}$, $(x_n)_{n=1}^{\infty} \in [x]$ and $N > 0$. Then $(x_n)_{n=1}^{\infty}$ is Cauchy. Hence there exists an $r > 0$ such that any $i,j \geq r$ satisfy $d(x_i,x_j) < N$. For the element $\imath(x_r) = [x_r]$ we have

$$\hat{d}([x_r],[x]) = d'((x_r),(x_n)_{n=1}^{\infty}) = \lim_{i\to\infty} d(x_r,x_i) < N.$$

It follows that $\imath(x_r) \in B_{\hat{d}}([x],N)$. So

$$\imath(\mathbf{Z}) \cap B_{\hat{d}}([x],N) \neq \varnothing,$$

that is, $\imath(\mathbf{Z})$ is dense in $\hat{\mathbf{Z}}$. ■

However, $\hat{\mathbf{Z}}$ is still 'much larger' than $\mathbf{Z}$, in the sense that it is uncountable; see Corollary 4.3 for a proof. Lemma 3.7 implies that $\hat{\mathbf{Z}}$ is a separable topological space, since it contains a countable, dense subset.

3.3 The profinite integers as a ring

In fact, the complete metric space $\hat{\mathbf{Z}}$ comes with a richer structure: it is a commutative ring. The ring operations are naturally inherited from those on $\mathbf{Z}$, by setting

$$[x] + [y] \stackrel{\text{def}}{=} [x + y] = [(x_1 + y_1, x_2 + y_2, \ldots)]$$

and

$$[x] \cdot [y] \stackrel{\text{def}}{=} [xy] = [(x_1 y_1,\, x_2 y_2, \ldots)].$$

Indeed, the elements $x+y$ and xy are Cauchy sequences: choose n large enough such that $d(x_{n+1}, x_n)$ and $d(y_{n+1}, y_n)$ are less than a given $N > 0$. Then $d(x_{n+1} + y_{n+1}, x_n + y_n)$ and $d(x_{n+1}y_{n+1}, x_n y_n)$ are less than N as well (by an argument similar to the one in the proof of Lemma 3.4). So the operations are well-defined. The commutativity of $\hat{\mathbf{Z}}$ is now an immediate consequence of this definition of addition.

The next lemma states that the ring operations are compatible with the topological structure of $\hat{\mathbf{Z}}$.

Lemma 3.8. $\hat{\mathbf{Z}}$ *is a topological ring.*

Proof. The argument is similar to the one in the proof of Lemma 3.4. Let $[x'] \in B_{\hat{d}}([x], 1/N)$ and $[y'] \in B_{\hat{d}}([y], 1/N)$. Then there exist $r(x)$ and $r(y)$ such that $x_n \equiv x'_n \pmod{(N+1)!}$ for all $n \geq r(x)$, and $y_n \equiv y'_n \pmod{(N+1)!}$ for all $n \geq r(y)$. Choose $r = \max\{r(x), r(y)\}$ and let $n \geq r$. Clearly, $x_n + y_n \equiv x'_n + y'_n \pmod{(N+1)!}$ and $x_n y_n \equiv x'_n y'_n \pmod{(N+1)!}$. Hence we obtain $[x' + y'] \in B_{\hat{d}}([x + y], 1/N)$ and $[x'y'] \in B_{\hat{d}}([xy], 1/N)$. ∎

4 Algebraic and topological aspects of $\hat{\mathbf{Z}}$

In this chapter, we state and prove some theorems that we need in the course of our study of profinite Fibonacci numbers in Chapter 5. Section 4.1 of this chapter is mainly devoted to the proof of Theorem 4.1, which provides a more intuitive way of thinking about profinite integers than as equivalence classes of Cauchy sequences. In section 4.2, we study the close relation between p-adic rings and $\hat{\mathbf{Z}}$, as described in Theorem 4.6. Introducing the group of units of $\hat{\mathbf{Z}}$ leads to section 4.3, where we define the logarithm on $\hat{\mathbf{Z}}$ and prove some of its properties.

4.1 The Representation Theorem

We have the following important representation of elements of $\hat{\mathbf{Z}}$.

Theorem 4.1 (Representation Theorem)**.** *Every element $[c] \in \hat{\mathbf{Z}}$ contains a uniquely determined element of the form*

$$(\dots c_3 c_2 c_1)_! \stackrel{\text{def}}{=} c_1 \cdot 1! + c_2 \cdot 2! + c_3 \cdot 3! + \cdots,$$

with $0 \leq c_i \leq i$, for all i, in the following sense: for all $a = (a_n)_{n=1}^{\infty} \in [c]$ and N greater than 0, there exists an $r = r(a, N)$ such that

$$a_n \equiv c_1 \cdot 1! + c_2 \cdot 2! + c_3 \cdot 3! + \cdots + c_{N-1}(N-1)! \pmod{N!},$$

for all $n \geq r$, such that the c_i's do not depend on the chosen representative $a \in [c]$.

Proof. Before starting this proof, we want to warn the reader that, for simplicity, it adopts a slight abuse of notation: the mod-operator is used for reduction (mod n) (in order to produce an integer between 0 and $n-1$), and to denote the equivalence class (mod n). However, from the context it should be clear which one is intended.

Let $a = (a_n)_{n=1}^{\infty} \in [c]$ and $N > 0$. Then there exists an $r = r(a, N)$ such that $a_m \equiv a_n \pmod{N!}$ for all $m, n \geq r$. Choose such an r. Define

$$\bar{a}_i \stackrel{\text{def}}{=} \frac{(a_r \pmod{(i+1)!}) - (a_r \pmod{i!})}{i!}, \tag{4.1}$$

for all $i \geq 1$. Note that the numerator of each $\bar{a}_i$ is always greater than or equal to 0, and strictly less than $(i+1)!$. Additionally, the numerator is divisible by $i!$ by construction.

It follows that $\bar{a}_i$ is an integer with $0 \leq \bar{a}_i \leq i$. Furthermore, the identity

$$1 \cdot 1! + 2 \cdot 2! + 3 \cdot 3! + \cdots + k \cdot k! = (k+1)! - 1$$

guarantees that $\bar{a}_1 \cdot 1! + \bar{a}_2 \cdot 2! + \bar{a}_3 \cdot 3! + \cdots + \bar{a}_n \cdot n! \pmod{N!} = \sum_{i=1}^{N-1} \bar{a}_i \cdot i!$ for all $n \geq N$, and

$$\sum_{i=1}^{N-1} \bar{a}_i \cdot i! = \sum_{i=1}^{N-1} (a_r \pmod{(i+1)!}) - (a_r \pmod{i!}) = a_r \pmod{N!}, \tag{4.2}$$

where the last equality holds since the summation in the middle is telescoping. Since the sequence a is Cauchy, it follows that $a_n \equiv a_r \pmod{N!}$ for all $n \geq r$ by Lemma 3.5. Hence we can choose $c_i = \bar{a}_i$, for all $i \leq N$.
Moreover, this choice of c_i's is unique for a. Namely, choose d_i's that also satisfy the conditions. Then for any $N > 0$, we have

$$c_1 \cdot 1! + c_2 \cdot 2! + c_3 \cdot 3! + \cdots + c_N \cdot N! = d_1 \cdot 1! + d_2 \cdot 2! + d_3 \cdot 3! + d_N \cdot N!.$$

Setting $N = 1$, we deduce that $c_1 = d_1$, and proceeding inductively (that is, choosing $N = 2$, 3, and so on) we see that $c_i = d_i$ for all i.

Strictly speaking, the element $c_1 \cdot 1! + c_2 \cdot 2! + \cdots$ is not really 'contained' in an element $[c] \in \hat{\mathbf{Z}}$, since it is not a Cauchy sequence. However, its partial sums almost trivially define a Cauchy sequence. We simply identify $(\ldots c_2 c_1)_!$ with this sequence, and then everything above goes through.

To conclude the proof, we still need to show that the c_i's do not depend on the chosen representative. To this end, let $(b_n)_{n=1}^{\infty}$ be another representative of $[c]$ and let i be given. By definition, $\lim_{n\to\infty} d(a_n, b_n) = 0$. Hence there exists an r such that $a_n \equiv b_n \pmod{i!}$ and $a_n \equiv b_n \pmod{(i+1)!}$ for all $n \geq r$. By virtue of their construction (see Equation (4.1)), we now see that the c_i's do not depend on the chosen representative. ■

From now on, we shall drop the brackets around c and, using Theorem 4.1, just say that $[c] = c = \sum_{i=0}^{\infty} c_i \cdot i! = (\ldots c_3 c_2 c_1)_!$. Any partial sum $c \pmod{N!} = \sum_{i=0}^{N-1} c_i \cdot i! = (\ldots 00 c_{N-1} \ldots c_2 c_1)_!$ identifies naturally with a positive integer. In fact, we can reduce c to any modulus n by calculating (in $\mathbf{Z}$) the reduction $c = \sum_{i=0}^{n!-1} c_i \cdot i! \pmod{n}$. We say that c is **divisible** by n if $c \equiv 0 \pmod{n}$. An element of $\hat{\mathbf{Z}}$ is called **even** or **odd** when $c_1 = 0$ or $c_1 = 1$, respectively, in accordance with the fact that $c \equiv c_1 \pmod{2}$.

The identification of $\imath(\mathbf{Z})$ with $\mathbf{Z}$ is consistent with earlier introduced notation – that is, for any integer n we recover $[n] = n$. We also have the following lemma.

Lemma 4.2. $\mathbf{Z}$ *is a subring of* $\hat{\mathbf{Z}}$*.*

Proof. The multiplicative identity of $\hat{\mathbf{Z}}$ is simply $1 = (\ldots 001)_!$ and is therefore contained in $\mathbf{Z}$. The operations of addition and multiplication on $\hat{\mathbf{Z}}$ coincide with the usual operations of addition and multiplication on $\mathbf{Z}$, which make the integers are ring. So $\mathbf{Z}$ must be a subring of $\hat{\mathbf{Z}}$ as well. ■

Using Theorem 4.1 we can now easily deduce the uncountability of $\hat{\mathbf{Z}}$.

Corollary 4.3. *The set* $\hat{\mathbf{Z}}$ *is uncountable.*

Proof. Looking at Theorem 4.1, we see that we may choose any c_i freely as long as $0 \leq c_i \leq i$, since each resulting sequence is Cauchy, and distinct from any sequence given by another choice of c_i's. Hence, as a set, $\hat{\mathbf{Z}}$ is in bijective correspondence with $\{0,1\} \times \{0,1,2\} \times \{0,1,2,3\} \times \ldots$, which is uncountable. ■

A limit that we shall often encounter in the course of this thesis, is the following.

Lemma 4.4. *The limit* $\lim_{n\to\infty} n!$ *exists and equals* 0*.*

Proof. Clearly, $\hat{d}(n!, 0) = 1/n!$, which converges to zero as n tends to infinity. ■

The sequence $(a_n)_{n=1}^{\infty}$ which we saw earlier, defined by $a_n = \sum_{k=1}^{n} k!$ for all n, is now almost trivially seen to converge to the element $(\ldots 111)_! \in \hat{\mathbf{Z}}$.

Although not strictly necessary for the remainder of the present thesis, it would be almost crude to exclude the following theorem. It justifies the thesis' title and could be considered as a tiny footstep into the large theoretical framework encompassing the study of profinite integers.

Theorem 4.5. $\hat{\mathbf{Z}}$ *is compact, Hausdorff and totally disconnected.*

Proof. Since any metric space is Hausdorff, the second statement follows directly. For the latter, first observe that any open ball $B = B_{\hat{d}}(x, r)$ is closed as well. Namely, assume that $y \notin B$, then by the ultrametric inequality, $B \cap B_{\hat{d}}(y, r)$ is empty. Hence the complement of B is open, so B is closed.
Now assume that two distinct elements a and b of $\hat{\mathbf{Z}}$ are given. Then there exists an $r > 0$ such that $\hat{d}(a, b) > r$. It follows that $b \notin B_{\hat{d}}(a, r)$. However, by the previous

claim, the complement of $B_{\hat{d}}(a,r)$ is open as well. Hence the connected components of $\hat{\mathbf{Z}}$ are the singletons, so $\hat{\mathbf{Z}}$ is totally disconnected.

To show that $\hat{\mathbf{Z}}$ is compact, we prove that it is sequentially compact, which is an equivalent statement for metric spaces. Let $(x_n)_{n=1}^{\infty}$ be a sequence in $\hat{\mathbf{Z}}$. If i is an integer and y an element of $\hat{\mathbf{Z}}$, then

$$y \in B_{i,N} \overset{\text{def}}{=} B_{\hat{d}}\left(i, \frac{1}{N-1}\right)$$

if there exists an $n_0 > 0$ such that $y_n \equiv i \pmod{N!}$ for all $n \geq n_0$. Hence for any $N > 1$, the collection

$$B_N \overset{\text{def}}{=} \{B_{i,N} : 0 \leq i \leq N! - 1\}$$

is a finite open cover of $\hat{\mathbf{Z}}$. Now let $N = 2$. Then at least one of the members of $B_N = B_2$ contains an infinite number of elements of $(x_n)_{n=1}^{\infty}$. Choose the smallest i such that this holds for $B_{i,2}$, and let

$$S_2 \overset{\text{def}}{=} \{m : x_m \in B_{i,2}\}.$$

Proceeding inductively, for any $N > 2$, one finds a smallest j such that $B_{j,N}$ contains an infinite number of x_m's with $m \in S_{N-1}$; again, the set of indices m such that $x_m \in B_{j,N}$ is called S_N. Note that there always exists such a $B_{j,N}$, because B_N contains only finitely many balls (and if each of these would only contain only finitely many elements of the sequence $(x_n)_{n=1}^{\infty}$, then the sequence would be finite, which is a contradiction).

By construction, $S_N \subset S_M$ for all $N \geq M$. Since each of the S_N's is infinite, we can choose elements $n_k \in S_k$, with $n_k < n_{k+1}$, for all $k \geq 2$. Let $i, j \geq k$, then it follows that $\hat{d}(x_{n_i}, x_{n_j}) < 1/(k-1)$. Hence the subsequence $(x_{n_k})_{k=1}^{\infty}$ is Cauchy in the complete space $\hat{\mathbf{Z}}$, so converges. It follows that $\hat{\mathbf{Z}}$ is sequentially compact. ■

Topological spaces such as $\hat{\mathbf{Z}}$ that are compact, Hausdorff, and totally disconnected are often called **profinite spaces**. Its additive group and group of invertible elements are examples of **profinite groups**, and when considered as a ring, the profinite integers form a so-called **profinite ring**. Profinite spaces find their origin in category theory, and have been studied extensively (see for example [RZ10]). The name of the research field studying number theoretic aspects of $\hat{\mathbf{Z}}$ is called **profinite number theory**, accordingly. This motivates the name of the present thesis.

4.2 p-adic rings and the unit group $\hat{\mathbf{Z}}^\times$

Let p be a prime number. In the course of introducing the absolute value on $\mathbf{Z}$, we briefly touched upon p-adic numbers. These numbers form an analogue of $\hat{\mathbf{Z}}$: there is an absolute value inducing a completion of $\mathbf{Z}$, which also carries the structure of a ring. For this reason, it is known as the **ring of p-adic numbers** and denoted by $\mathbf{Z}_p$. Any element $[c] = c \in \mathbf{Z}_p$ has a unique p-adic expansion given by $c = c_0 + c_1 p + c_2 p^2 + \cdots = (\ldots c_2 c_1 c_0)_p$ with every c_i an integer such that $0 \leq c_i \leq p-1$ (see [Len03]). Comparing this with Theorem 4.1 in particular, the resemblance with $\hat{\mathbf{Z}}$ can altogether hardly be overlooked. Although we won't delve deeply into the interesting properties of p-adic numbers and their analysis, the following theorem provides a connection between them and the ring of profinite integers, which forms an important tool in the forthcoming. The reader may find an informal outline of the construction and properties of $\mathbf{Z}_p$ in Appendix B, along with a few relevant references.

Theorem 4.6. *Let $b = (b_2, b_3, b_5, \ldots) \in \prod_p \mathbf{Z}_p$, where the product extends over all primes p. Write $\mathbf{Z}_p \ni b_p = (\ldots b_{p,2} b_{p,1} b_{p,0})_p$ with $0 \leq b_{p,i} \leq p-1$, for each p and i. Define the maps*

$$\psi : \hat{\mathbf{Z}} \to \prod_p \mathbf{Z}_p, \quad c \mapsto (\psi_2(c), \psi_3(c), \psi_5(c), \ldots), \tag{4.3}$$

$$\psi_p : \hat{\mathbf{Z}} \to \mathbf{Z}_p, \quad c \mapsto (\ldots b_{p,2} b_{p,1} b_{p,0})_p, \tag{4.4}$$

where $\prod_p \mathbf{Z}_p$ is equipped with the product topology and has the algebraic structure of a product ring, and set

$$b_{p,i} = b_{p,i}(c) \stackrel{\text{def}}{=} \frac{c \pmod{p^{i+1}} - c \pmod{p^i}}{p^i} \tag{4.5}$$

for any integer $i \geq 0$. Then ψ is a well-defined isomorphism of topological rings.

Proof. Let p be prime. We will start by showing that ψ is well-defined. An argument similar to the one in the proof of Theorem 4.1 shows that each $b_{p,i}$ is an integer satisfying $0 \leq b_{p,i} \leq p-1$. Hence any $c \in \hat{\mathbf{Z}}$ is indeed mapped to the ring $\mathbf{Z}_p$ under ψ_p, and ψ is well-defined. Actually, the map ψ_p is nothing more than 'writing c in base p'. Since addition and multiplication on $\hat{\mathbf{Z}}$ and $\mathbf{Z}_p$ are both inherited from the usual operations on $\mathbf{Z}$, it is clear that ψ_p is a homomorphism.
Note that $\sum_{i=0}^{m} b_{p,i} p^i = c \pmod{p^{m+1}}$. Let n be a positive integer. The prime factorizations $n! = p_1^{s_1} \cdots p_k^{s_k}$ and $(n+1)! = q_1^{t_1} \cdots q_l^{t_l}$ provide, invoking the Chinese Remainder

Theorem 2.19, ring isomorphisms

$$\mathbf{Z}/n!\mathbf{Z} \cong \mathbf{Z}/p_1^{s_1}\mathbf{Z} \times \cdots \times \mathbf{Z}/p_k^{s_k}\mathbf{Z}, \qquad \mathbf{Z}/(n+1)!\mathbf{Z} \cong \mathbf{Z}/q_1^{t_1}\mathbf{Z} \times \cdots \times \mathbf{Z}/q_l^{t_l}\mathbf{Z},$$

which guarantee the uniqueness of $c \pmod{(n+1)!}$ and $c \pmod{n!}$, given $b_{p_1,s_1}, \ldots, b_{p_k,s_k}$ and $b_{q_1,t_1}, \ldots, b_{q_l,t_l}$. These together determine c_n uniquely, by Theorem 4.1. As n gets larger, any prime power will eventually divide $n!$. It follows that ψ is a ring isomorphism. To show that the isomorphism is also topological, we first prove that ψ is continuous. Fix p and let $N > 0$ be an integer. Set $M = p^N$ and assume $x \equiv c \pmod{M!}$. Then $x \equiv c \pmod{p^i}$ for all $i \leq N$. Hence $b_{p,i}(x) = b_{p,i}(c)$ for all $i \leq N-1$. Hence $\psi_p(x) \equiv \psi_p(c) \pmod{p^N}$, so ψ_p is continuous. It follows that ψ is continuous. As $\hat{\mathbf{Z}}$ is compact (see Theorem 4.5) and $\mathbf{Z}_p$ is Hausdorff, ψ is a homeomorphism by Lemma 2.4. ■

Lemma 4.7. *The unit group of* $\mathbf{Z}_p$ *is* $\mathbf{Z}_p^\times = \mathbf{Z}_p - p\mathbf{Z}_p$.

Proof. Let $\gamma = b_0 + b_1 p + b_2 p^2 + \cdots \in \mathbf{Z}_p$. If γ is invertible, then it must also be invertible mod p. Hence $b_0 \neq 0$. For the other inclusion, write $\gamma = b_0 + p\gamma'$ and note that $\gamma' \in \mathbf{Z}_p$. If $b_0 \neq 0$, then

$$(b_0 + p\gamma') \cdot b_0^{-2}(b_0 - p\gamma' + \cdots + (-1)^n(p\gamma')^n) = 1 + (-1)^n(p\gamma')^{n+1} \equiv 1 \pmod{p^{n+1}},$$

for every integer n. Hence after expanding we find coefficients c_i such that $b_0^{-1} + c_1 p + c_2 p^2 + \cdots$ is the inverse of γ. Hence $\gamma \in \mathbf{Z}_p^\times$. ■

Corollary 4.8. *The unit group of* $\hat{\mathbf{Z}}$ *is given by*

$$\hat{\mathbf{Z}}^\times \cong \prod_p (\mathbf{Z}_p - p\mathbf{Z}_p). \tag{4.6}$$

Proof. This is an immediate consequence of the fact that the unit group of a product ring is the product of the respective unit groups, Theorem 4.6, and Lemma 4.7. ■

The explicit isomorphism from Theorem 4.6 now shows that no unit $u \in \hat{\mathbf{Z}}^\times$ is divisible by any prime number p. Indeed, $c \pmod p = b_{p,0} \neq 0$. Therefore every unit is odd, and the only units contained in the subring $\mathbf{Z}$ are given by ± 1.

4.3 The logarithm on $\hat{\mathbf{Z}}^\times$

This section is devoted to the construction of the logarithm on $\hat{\mathbf{Z}}^\times$. Before we are ready to define the map (see Equation (4.13)) and prove some of its properties in Theorem 4.13, we define the p-adic logarithm which naturally induces the map in (4.13). In anticipation of that theorem, we will prove the following lemma.

Lemma 4.9. *Let $u \in 1 + p\mathbf{Z}_p$ and $n \geq 0$ be an integer. Then*

$$u^{p^n} \equiv \begin{cases} 1 \pmod{p^{n+1}} & \text{if } p \text{ is an odd prime,} \\ 1 \pmod{p^{n+2}} & \text{if } p = 2 \text{ and } n > 0. \end{cases}$$

Proof. Let $u \in 1 + p\mathbf{Z}_p$ and $n \geq 0$. Define

$$P_{p,n}(u) = P_n \overset{\text{def}}{=} \begin{cases} \frac{u^{p^n}-1}{p^{n+1}} & \text{if } p \text{ is an odd prime,} \\ \frac{u^{p^n}-1}{p^{n+2}} & \text{if } p = 2. \end{cases} \tag{4.7}$$

whenever it exists. We proceed by induction, starting with the case that p is an odd prime. Note that $u \equiv 1 \pmod{p}$. Assume the statement is true for some $n \geq 0$. Then $P_n(u)$ is p-adic and we can write $u^{p^n} = 1 + P_n(u)p^{n+1}$. Hence

$$\begin{aligned} u^{p^{n+1}} = (u^{p^n})^p &= (1 + P_n(u)p^{n+1})^p, \\ &= 1 + \sum_{k=1}^{p} \binom{p}{k} P_n(u)^k p^{(n+1)k}, \\ &= 1 + p^{n+2}P_n(u) + p^{2n+2} \sum_{k=2}^{p} \binom{p}{k} P_n(u)^k p^{(n+1)(k-2)}, \end{aligned}$$

and from here, the result is immediate. Also, it follows that

$$P_{n+1}(u) = P_n(u) + p^n \sum_{k=2}^{p} \binom{p}{k} P_n(u)^k p^{(n+1)(k-2)}$$

is again p-adic. Furthermore, $P_{n+1}(u) - P_n(u)$ is divisible by p^n.
If $p = 2$, then we can write $u = 1 + 2\gamma$ for some $\gamma \in \mathbf{Z}_p$. Hence $u^2 = 1 + 4\gamma(\gamma + 1) \equiv 1 \pmod{8}$. If $u^{2^n} = 1 + 2^{n+2}P_n(u)$ for some n and 2-adic $P_n(u)$, it follows that $u^{2^{n+1}} = (u^{2^n})^2 = (1+2^{n+2}P_n(u))^2 = 1+2^{n+3}P_n(u)+2^{2(n+2)}P_n(u)^2 \equiv 1 \pmod{2^{n+3}}$, so that $P_{n+1}(u)$ is again 2-adic and the result follows by induction. Furthermore, $P_{n+1}(u) - P_n(u) = 2^{n+1}P_n(u)^2$. ∎

We are now ready to define the p-adic logarithm, which is the subject of the following theorem.

Theorem 4.10. *The map*

$$\log_p : \begin{cases} 1 + p\mathbf{Z}_p \to p\mathbf{Z}_p & \text{if } p \text{ is an odd prime,} \\ 1 + 4\mathbf{Z}_2 \to 4\mathbf{Z}_2 & \text{if } p = 2, \end{cases} \qquad \log_p(u) \stackrel{\text{def}}{=} \lim_{n\to\infty} \frac{u^{p^n} - 1}{p^n}, \tag{4.8}$$

is a well-defined, continuous group homomorphism between the multiplicative group $1 + p\mathbf{Z}_p$ *(or* $1 + 4\mathbf{Z}_2$*) and the additive group* $p\mathbf{Z}_p$ *(or* $4\mathbf{Z}_2$*).*

Proof. Let $u \in 1 + p\mathbf{Z}_p$. The fraction on the right-hand side of Equation (4.8) exists for every p and n by virtue of the previous lemma. In its proof we saw that the sequence $P_{p,n}(u)$ (as a sequence with index n) satisfies $P_{p,n+1}(u) - P_{p,n}(u) \equiv 0 \pmod{p^n}$. By analogy of Lemma 3.5, we may deduce that the sequence is Cauchy in the complete space $\mathbf{Z}_p$. Hence the limit on the right-hand side of Equation (4.8) exists, and we can even say, as a consequence of the previous lemma, that

$$\log_p(u) = p \lim_{n\to\infty} \frac{u^{p^n} - 1}{p^{n+1}}, \quad \log_2(u) = 4 \lim_{n\to\infty} \frac{u^{2^n} - 1}{2^{n+2}},$$

where the prime p is odd. As each of these limits is an element of $\mathbf{Z}_p$, this proves that $\log_p$ maps to $p\mathbf{Z}_p$ if p is odd and to $4\mathbf{Z}_2$ if $p = 2$.

For the homomorphism property, write $T_n(u) = \frac{u^{p^n}-1}{p^n}$. Then $u^{p^n} = 1 + T_n(u)p^n$ and $v^{p^n} = 1 + T_n(v)p^n$, and we have $(uv)^{p^n} = 1 + (T_n(u) + T_n(v))p^n + T_n(u)T_n(v)p^{2n}$. Since $\lim_{n\to\infty} p^n = 0$, it follows that

$$\log_p(uv) = \lim_{n\to\infty} T_n(u) + T_n(v) + T_n(u)T_n(v)p^n = \log_p(u) + \log_p(v).$$

Hence $\log_p$ is a group homomorphism.

For continuity, let $p^N > 1$ be given. Set $M = p^N$. Let $x, u \in 1 + p\mathbf{Z}_p$ such that $x \equiv u \pmod{M}$. Then $x = u + \lambda p^N$ for some $\lambda \in \mathbf{Z}_p$. Since the logarithm is a homomorphism and u is invertible, we have $\log_p(x) - \log_p(u) = \log_p(xu^{-1}) = \log_p(1 + \lambda p^N u^{-1})$. We start by considering the case that p is odd. Adopting the previous notation, we have

$$T_{n+1} = \frac{(u^{p^n})^p - 1}{p^n},$$

$$= \frac{(1+T_n p^n)^p - 1}{p^n},$$
$$= \frac{1}{p^{n+1}} \sum_{k=1}^{p} \binom{p}{k} T_n^k p^{nk}.$$

Some rewriting gives

$$T_{n+1} = T_n \left(1 + T_n^{p-1} p^{n(p-1)-1} + \sum_{k=2}^{p-1} \frac{1}{k} \binom{p-1}{k-1} T_n^{k-1} p^{n(k-1)} \right). \tag{4.9}$$

Note that $\frac{1}{k}\binom{p-1}{k-1} = \frac{1}{p}\binom{p}{k}$ is an integer for all $2 \leq k \leq p-1$. Equation (4.9) shows that T_n divides T_{n+1} for all $n \geq 1$. In particular, since

$$T_1 = \frac{(1+\lambda p^N u^{-1})^p - 1}{p} = \lambda^p p^{(p-1)N} u^{-p} + \sum_{k=1}^{p-1} \frac{1}{k} \binom{p-1}{k-1} \lambda^k p^{kN} u^{-k}, \tag{4.10}$$

is divisible by p^N, it follows that p^N divides T_n for all $n \geq 0$.
If $p = 2$, then $T_{n+1} = \frac{(1+T_n 2^n)^2 - 1}{2^n} = T_n(2 + 2^n T_n)$. Again, we see that T_n divides T_{n+1} for all $n \geq 0$ so that we may immediately deduce that p^N divides T_n for all $n \geq 0$. ■

Lemma 4.11 and 4.12 provide some further insight into the p-adic logarithm. The first states that it is a group isomorphism, and gives its inverse: the p-adic exponential map. The second shows that the logarithm may be extended to a map on (the whole of) $\mathbf{Z}_p^\times$.

Lemma 4.11. *For every prime p, the map $\log_p$ as defined in Theorem 4.10 is a group isomorphism, with inverse*

$$\exp_p : \begin{cases} p\mathbf{Z}_p \to 1 + p\mathbf{Z}_p & \text{if } p \neq 2, \\ 4\mathbf{Z}_2 \to 1 + 4\mathbf{Z}_2 & \text{if } p = 2, \end{cases} \qquad \exp_p(x) = \sum_{k \geq 0} \frac{x^k}{k!}. \tag{4.11}$$

Proof. See [Rob00, p. 261] and [Kob84, p. 81]. ■

Lemma 4.12. *The p-adic logarithm can be extended to a continuous homomorphism $\mathrm{Log}_p : \mathbf{Z}_p^\times \cong \mathbf{Z}_p - p\mathbf{Z}_p \to \mathbf{Z}_p$, also known as the Iwasawa logarithm, with the same image as $\log_p$, by setting, for any $u \in \mathbf{Z}_p^\times$,*

$$\mathrm{Log}_p(u) \overset{\text{def}}{=} \frac{1}{p-1} \log_p(u^{p-1}). \tag{4.12}$$

Proof. See [Rob00, p. 260]. ■

In the forthcoming, we will simply denote the Iwasawa logarithm as $\log_p$ instead of Log_p and refer to it as the p-adic logarithm. Therefore, Lemma 4.11 should be read as '$\log_2|_{1+4\mathbf{Z}_2}$ and $\log_p|_{1+p\mathbf{Z}_p}$ are group isomorphisms for any odd prime p'.

In the following theorem, we will introduce the logarithm on $\hat{\mathbf{Z}}^\times$. Its definition, as the reader will see in (4.13), is much alike the p-adic logarithm. We basically prove that it has the same properties as the p-adic logarithm, and the (ideas of the) proofs are very similar.

Theorem 4.13. *The map*

$$\log : \hat{\mathbf{Z}}^\times \to \hat{\mathbf{Z}}, \quad \log(u) \stackrel{\text{def}}{=} \lim_{n\to\infty} \frac{u^{n!}-1}{n!}, \tag{4.13}$$

is a (1) well-defined, (2) continuous group homomorphism, with (3)

$$\ker\log = \overline{\{u \in \hat{\mathbf{Z}}^\times : \exists\, n \in \mathbf{Z}_{>0} : u^n = 1\}}, \quad \operatorname{im}\log = 2\mathrm{J},$$

where $\mathrm{J} = \bigcap_p p\hat{\mathbf{Z}} = \prod_p p\mathbf{Z}_p$ *is the so-called Jacobson radical of* $\hat{\mathbf{Z}}$.

For the proof of this theorem, we need the following lemma:

Lemma 4.14. *Let* $u \in \hat{\mathbf{Z}}^\times$ *be a unit. For all positive integers* n*, we have*

$$u^{n!} \equiv 1 \pmod{n!}. \tag{4.14}$$

Proof. We proceed by induction. The result is clear for $n = 1$. Assume the statement holds for some integer $n \geq 1$. Then we can define

$$A_n = A_n(u) \stackrel{\text{def}}{=} \frac{u^{n!}-1}{n!} \in \hat{\mathbf{Z}}, \tag{4.15}$$

so that $u^{n!} = 1 + A_n n!$. By the binomial theorem, we have

$$\begin{aligned} u^{(n+1)!} &= (1 + A_n n!)^{n+1}, \\ &= 1 + A_n^{n+1}(n!)^{n+1} + \sum_{k=1}^{n} \binom{n+1}{k} A_n^k (n!)^k, \\ &= 1 + A_n^{n+1}(n!)^{n+1} + \sum_{k=1}^{n} \frac{n+1}{k}\binom{n}{k-1} A_n^k (n!)^k, \\ &= 1 + A_n^{n+1}(n!)^{n+1} + (n+1)! \sum_{k=1}^{n} \binom{n}{k-1} A_n^k \frac{(n!)^{k-1}}{k}. \end{aligned} \tag{4.16}$$

The sum on the last line is in $\hat{\mathbf{Z}}$, since k divides $(n!)^{k-1}$ for all $1 \leq k \leq n$. Hence we obtain $u^{(n+1)!} \equiv 1 + (A_n n!)^{n+1} \pmod{(n+1)!}$. We need to show that $(A_n n!)^{n+1} \equiv 0 \pmod{(n+1)!}$, that is,

$$A_n^{n+1}(n!)^n \equiv 0 \pmod{n+1}. \tag{4.17}$$

In fact, we even show that

$$\begin{cases} A_n n! \equiv 0 \pmod{n+1} & \text{if } n+1 \neq 4, \\ (n!)^2 \equiv 0 \pmod{n+1} & \text{if } n+1 = 4. \end{cases} \tag{4.18}$$

There are three cases. First assume $n+1 \neq 4$ is composite. Then $n+1 = ab$ for some $2 \leq a, b \leq n$. If we can choose $a \neq b$, we are done. If not, then $n+1$ is the square of a prime q. Since $2q < q^2$ by the assumption $n+1 \neq 4$, it follows that both q and $2q$ divide $n!$. Therefore, $n! \equiv 0 \pmod{n+1}$.
When $n+1 = p$ is prime, the result is an easy consequence of Fermat's little theorem. Namely, since $p-1$ divides $p!$, we have

$$u^{p!} = (u^{p-1})^{p(p-2)!} \equiv 1^{p(p-2)!} \equiv 1 \pmod{p}.$$

That leaves the case $n+1 = 4$. We now find $(3!)^2 \equiv 0 \pmod{4}$ and hence we are done. ■

We are now ready to prove Theorem 4.13.

Proof of Theorem 4.13. We will treat the claims (1), (2) and (3) as stated in the theorem separately.

— Claim 1. *The logarithm is well defined; that is, the limit on the right-hand side of Equation (4.13) exists.*

Proof of Claim 1. Note that Lemma 3.5 and its proof still hold in the more general setting of sequences in $\hat{\mathbf{Z}}$, by replacing d with $\hat{d}$ throughout. Since $\hat{\mathbf{Z}}$ is complete, the Lemma offers a characterization of (general) convergent sequences. The limit on the right-hand side of Equation (4.13) henceforth exists if the profinite difference of succeeding terms tends to zero in the limit. Using (4.15), it follows that the limit exists if

$$\lim_{n \to \infty} \hat{d}(A_{n+1}, A_n) = 0. \tag{4.19}$$

We start by assuming $n \geq 2$. Since $1 + A_{n+1}(n+1)! = (1 + A_n n!)^{n+1}$, we have

$$\begin{aligned} A_{n+1} &= \frac{(1 + A_n n!)^{n+1} - 1}{(n+1)!}, \\ &= \sum_{k=1}^{n+1} \frac{1}{(n+1)!} \binom{n+1}{k} A_n^k (n!)^k, \\ &= A_n + \sum_{k=2}^{n+1} \frac{1}{(n+1)!} \frac{n+1}{k} \binom{n}{k-1} A_n^k (n!)^k, \\ &= A_n + A_n \sum_{k=2}^{n+1} \binom{n}{k-1} \frac{A_n^{k-1} (n!)^{k-1}}{k}. \end{aligned} \tag{4.20}$$

By Equation (4.18), we know that the slightly stronger $1/k \cdot (A_n^{k-1}(n!)^{k-2}) \in \hat{\mathbf{Z}}$ holds, when $k = n+1$. When $2 \leq k \leq n$, the fraction in the summation is clearly a profinite integer since k divides $n!$. Hence the equality (4.20) shows that A_n divides A_{n+1}. Note that this also holds for $n = 1$, since $A_2 = 1/2 \cdot A_1(A_1 + 2)$, and $A_1(u) = u - 1$ is even for any unit u. An immediate consequence of these facts is that A_n is even for all n. So, we may even assume that $n \geq 1$, and write

$$A_{n+1} - A_n = A_n n! \sum_{k=2}^{n+1} \binom{n}{k-1} \frac{A_n^{k-1} (n!)^{k-2}}{k}.$$

The preceding considerations show that the fraction in this summation is always a profinite integer. We therefore obtain $A_{n+1} \equiv A_n \pmod{n!}$. It follows that the limit (4.19) exists and equals 0. □

— Claim 2. *The logarithm is a continuous group homomorphism.*

Proof. This is almost entirely the same argument as in the proof of Theorem 4.10. Let u and v be units. Writing $u^{n!} = 1 + A_n n!$ and $v^{n!} = 1 + B_n n!$, we obtain $(uv)^{n!} = 1 + (A_n + B_n)n! + A_n B_n (n!)^2$. Hence

$$\log(uv) = \lim_{n \to \infty} A_n + B_n + A_n B_n n! = \log(u) + \log(v), \tag{4.21}$$

since $\lim_{n \to \infty} n! = 0$.

For continuity, let $N! > 0$ be given and set $M = N!$. Once again, let $x, u \in \hat{\mathbf{Z}}^\times$ such that $x \equiv u \pmod{M}$. Then there exists a $\lambda \in \hat{\mathbf{Z}}$ such that $\log(x) - \log(u) =$

$\log(1+\lambda N!u^{-1})$. Note that $A_1(1+\lambda N!u^{-1}) = \lambda N!u^{-1}$ is divisible by $N!$. In the proof of Claim 1 we saw that A_{n+1} is divisible by A_n for all $n \geq 1$. Hence A_n is divisible by $N!$, for all $n \geq 1$. Therefore $\log(1+\lambda N!u^{-1}) = \lim_{n\to\infty} A_n$ is divisible by $N!$. □

— Claim 3. *The logarithm has kernel and image given by*

$$\ker \log = \overline{\{u \in \hat{\mathbf{Z}}^\times : \exists\, n \in \mathbf{Z}_{>0} : u^n = 1\}}, \quad \operatorname{im} \log = 2\mathrm{J},$$

where $\mathrm{J} = \bigcap_p p\hat{\mathbf{Z}} = \prod_p p\mathbf{Z}_p$ is the so-called Jacobson radical of $\hat{\mathbf{Z}}$.

Proof. We will first look at the image of the logarithm. Fix a prime p. Consider $u = (u_2, u_3, \ldots)$ as an element of $\prod_p \mathbf{Z}_p$. Looking at the definition of the p-adic logarithm (4.12), we see that since $\log_p(u^m) = m\log_p(u)$ for any integer m, we have

$$\log_p(u) = \lim_{r\to\infty} \frac{u^{mp^r}-1}{mp^r}.$$

Choosing values m_r for any r such that $m_r p^r = (p^r)!$, we see that the p-th component

$$\left(\frac{u^{n!}-1}{n!}\right)_p \in \mathbf{Z}_p$$

must converge p-adically to $\log_p(u_p)$. Now $\log_p(u_p)$ maps onto $p\mathbf{Z}_p$ when p is odd and onto $4\mathbf{Z}_2$ when $p = 2$, by Lemma 4.11. Hence

$$\operatorname{im} \log = 4\mathbf{Z}_2 \times \prod_{p\neq 2} p\mathbf{Z}_p = 2\mathrm{J}.$$

For the kernel, by definition, the logarithm of any element of finite order vanishes. Since the logarithm is continuous and $\ker\log = \log^{-1}(0)$, the kernel must be closed, so it contains the closure of all units of finite order. To show the other inclusion, let $u \in \ker\log$, then for all $N > 0$ we have $\frac{u^{n!}-1}{n!} \equiv 0 \pmod{N!}$ for n large enough. Hence $u^{n!} \equiv 1 \pmod{N!}$. It follows that u is a limit point of $A = \{u \in \hat{\mathbf{Z}}^\times : \exists\, n \in \mathbf{Z}_{>0} : u^n = 1\}$, so $u \in \overline{A}$. □

Claim 1, 2 and 3 together prove the theorem. ■

Finally, we can state the following lemma.

Lemma 4.15. *The map* $\exp : 2\mathrm{J} \to 1 + 2\mathrm{J}$ *induced by the collection of maps* $\exp_p$ *for all* p*, is an isomorphism of topological rings, with inverse* $\log|_{1+2\mathrm{J}} : 1 + 2\mathrm{J} \to 2\mathrm{J}$.

Proof. This is a consequence of Theorem 4.13 (in particular, the proof of Claim 3) and Lemma 4.11. ■

5 Profinite Fibonacci numbers

In this chapter, we turn our attention to the well-known **Fibonacci numbers**. In $\mathbf{Z}$, these are given as usual by $F_0 = 0$, $F_1 = 1$ and

$$F_{n+1} \stackrel{\text{def}}{=} F_n + F_{n-1}$$

for all $n \geq 1$. The Fibonacci numbers have many interesting properties, which can be found in for instance [Luc78]. An important related sequence is formed by the **Lucas numbers**. It satisfies the same recurrence, but has starting values $L_0 = 2$ and $L_1 = 1$. The defining recurrence relation of the Fibonacci sequence can be used to extend the sequence to include negative indices quite naturally. Namely, considering that $F_{n+1} - F_n = F_{n-1}$, we may simply define $F_{-1} = F_1 - F_0 = 1$, $F_{-2} = F_0 - F_{-1} = -1$, and so on. The same can be done for the Lucas sequence. From this we can easily infer that $F_{-n} = (-1)^{n-1}F_n$ and $L_{-n} = (-1)^n L_n$, for all $n \geq 0$. In this chapter, we will henceforth consider the Fibonacci and Lucas sequences as sequences with indices ranging over the whole of $\mathbf{Z}$. If we regard F as a map $\mathbf{Z} \to \mathbf{Z} \subset \hat{\mathbf{Z}}$, defined as $n \mapsto F_n$, then it turns out that F admits a unique continuous extension to a function $\hat{\mathbf{Z}} \to \hat{\mathbf{Z}}$, called the Fibonacci map. The same holds for L.

The extended map F admits eight non-trivial fixed points (that is, they do not emerge from fixed points in $\mathbf{Z}$), which is the main result of this thesis (see 5.34). In section 5.1, we prove some relevant properties of the Fibonacci map and establish a suitable definition of F over $\hat{\mathbf{Z}}$. In sections 5.2 and 5.4, we develop an iterative method to obtain the fixed points of F, aided by the power series expansion of F found in section 5.3.

5.1 Defining the Fibonacci map

Many of the properties of the Fibonacci and Lucas sequence needed to comprehend the fixed points of the Fibonacci map, have elementary proofs and are therefore included in Appendix A so as not to distract the reader from the main discussion. Throughout this whole chapter, the symbols ϑ and $\bar{\vartheta}$ will be the roots in $\mathbf{Z}[\frac{1+\sqrt{5}}{2}]$ of the polynomial $x^2 - x - 1$, given by $\vartheta = \frac{1+\sqrt{5}}{2}$ and $\bar{\vartheta} = \frac{1-\sqrt{5}}{2}$. Recall that the Fibonacci and Lucas numbers are given by

$$F_n = \frac{\vartheta^n - \bar{\vartheta}^n}{\vartheta - \bar{\vartheta}} \quad \text{and} \quad L_n = \vartheta^n + \bar{\vartheta}^n, \tag{5.1}$$

respectively, see Lemma A.1. The Lucas numbers also satisfy $L_n = F_{n-1} + F_{n+1}$ for all integers n, see Lemma A.2. There is an addition law for Fibonacci numbers, see Lemma A.3, and the Fibonacci sequence is a **strong divisibility sequence** — it satisfies $\gcd(F_m, F_n) = F_{\gcd(m,n)}$ for all integers m and n, see Lemma A.4. These together reveal a lot of information regarding the divisibility of Fibonacci numbers.
A technical but essential part of the impending discussion is the fact that we now work over $\mathbf{Z}[\vartheta]$ instead of $\mathbf{Z}$, which could 'distort' the associated completion. Luckily the completion of $\mathbf{Z}[\vartheta]$ satisfies $\widehat{\mathbf{Z}[\vartheta]} = \hat{\mathbf{Z}}[\vartheta]$. The analysis of $\hat{\mathbf{Z}}[\vartheta]$ is strongly interlinked with the analysis of $\hat{\mathbf{Z}}$, and the main difference between the two actually boils down to the multiplicative order of the elements ϑ and $\bar{\vartheta}$ modulo p, which is considered in Lemma A.6.

Note that ϑ and $\bar{\vartheta}$ are units of $\hat{\mathbf{Z}}[\vartheta]$, since they both satisfy $x(x-1) = 1$. Analogous to Lemma 4.14, we have the following.

Lemma 5.1. *For every $n \geq 4$,*

$$\vartheta^{n!} \equiv 1 \pmod{n!}. \tag{5.2}$$

Proof. A calculation shows that

$$\vartheta^{4!} = 1 + 4! \cdot (2160 + 966\sqrt{5}) = 1 + 4! \cdot (1932\vartheta + 1194), \tag{5.3}$$

so the statement holds for $n = 4$. Assume the statement holds for some $n \geq 4$, then we can again write $\vartheta^{n!} = 1 + n!A_n$. Proceeding as in the proof of Lemma 4.14, once again we obtain the expression (4.16) and need to show (4.17). The proof given there in the case that $n+1$ is composite, is here exactly the same. However, if $n + 1 = p$ is prime, we need another argument. Using Equation (A.2), we obtain $\vartheta^{p^2-1} \equiv 1 \pmod{p}$ for all primes $p > 5$. Note that $p^2 - 1 = (p-1)(p+1)$ divides $(p-1)!$ when $p+1$ divides $(p-2)!$. Since $p+1$ is composite, and not a square, there exist distinct a and b such that $ab = p+1$. Hence $2 \leq a, b \leq \frac{p+1}{2}$, which is less than or equal to $p-2$ precisely when $p \geq 5$. Therefore $p^2 - 1$ divides $(p-1)!$ for all $p \geq 5$, so we obtain

$$\vartheta^{(p-1)!} = (\vartheta^{p^2-1})^{(p-1)!/(p^2-1)} \equiv 1 \pmod{p}. \tag{5.4}$$

Since $\vartheta^{(p-1)!} \equiv 1 \pmod{(p-1)!}$, it follows that $\vartheta^{p!} \equiv 1 \pmod{p!}$.
If $p = 5$, the identity (5.3) shows that $A_4^2 \equiv 0 \pmod{5}$. We have now shown (4.17), so the statement follows. ∎

Since

$$\bar{\vartheta}^{4!} = \overline{\vartheta^{4!}} = 1 + 4! \cdot (2160 - 966\sqrt{5}) = 1 + 4! \cdot (1932\bar{\vartheta} + 1194), \tag{5.5}$$

Lemma 5.1 also holds for $\bar{\vartheta}$ instead of ϑ. An immediate consequence is the following corollary.

Corollary 5.2. *For all integers $n \geq 4$, $k > 0$ and i,*

$$F_{kn!+i} \equiv F_i \pmod{n!}, \quad L_{kn!+i} \equiv L_i \pmod{n!}. \tag{5.6}$$

Proof. This follows directly by combining Lemma 5.1, Theorem A.1 and the remark preceding this corollary. ■

In fact, more is true when $i = 0$.

Lemma 5.3. *For all positive integers k and $n \geq 4$, we have*

$$L_{kn!} \equiv 2 \pmod{(n+1)!}, \tag{5.7}$$

$$F_{kn!} \equiv kF_{n!} \pmod{(n+1)!}. \tag{5.8}$$

Proof. If $n+1$ is prime, then (5.4) shows that $L_{kn!} \equiv 1^k + 1^k \equiv 2 \pmod{n+1}$. Combining this with Corollary 5.2 we obtain the claim. The proof when $n+1$ is composite is postponed until after the introduction of the power series of ϑ^s (see Lemma 5.13 and thereafter).
For (5.8), the statement is trivial when $k = 1$. If $k = 2$, using (5.7) and the well-known identity $F_{2n} = F_n L_n$ (which is a consequence of Lemma A.3), we obtain $F_{2n!} \equiv 2F_{n!} \pmod{(n+1)!}$. Proceeding by induction and assuming the statement to be true for some $k \geq 1$, we have

$$F_{(k+1)n!} = F_{kn!} \cdot \frac{L_{n!}}{2} + \frac{L_{kn!}}{2} \cdot F_{n!} \equiv kF_{n!} + F_{n!} \equiv (k+1)F_{n!} \pmod{(n+1)!}$$

by Lemma A.3. The claim follows. ■

Slightly more general than the congruence (5.8) when $k = n+1$, we can state the following lemma.

Lemma 5.4. *For all $n \geq 4$,*

$$F_{(n+1)!} \equiv 0 \pmod{(n+1)F_{n!}}. \tag{5.9}$$

Proof. Note that

$$\frac{F_{(n+1)!}}{F_{n!}} = \frac{\vartheta^{(n+1)!} - \bar{\vartheta}^{(n+1)!}}{\vartheta^{n!} - \bar{\vartheta}^{n!}} = \sum_{k=0}^{n} \vartheta^{kn!}\bar{\vartheta}^{(n-k)n!}. \tag{5.10}$$

If $n+1 = p$ is prime, then (5.4) shows that each summand of the summation on the right-hand side of Equation (5.10) is congruent to 1 (mod $n+1$). If $n+1 \neq 4$ is composite, the proof of (4.18) shows that $n! \equiv 0 \pmod{n+1}$. Combined with Lemma 5.1 and the remark before Corollary 5.2, we also obtain that each summand is congruent to 1 (mod $n+1$). In both cases, the total number of summands is $n+1$, and hence the whole summation is divisible by $n+1$. ■

Lemma 5.5. *For all $n \geq 4$, we have*

$$F_{n!} \equiv 0 \pmod{2n! \prod_{\substack{p \leq 2n + \left(\frac{p}{5}\right) \\ p \neq 5}} p}.$$

Proof. Let $p \neq 5$ be prime and $n \geq 4$. Note that $p - \left(\frac{p}{5}\right)$ divides $n!$ for all $n \geq \frac{1}{2} \cdot (p - \left(\frac{p}{5}\right))$. Hence in that case, $\gcd\left(F_{n!}, F_{p-\left(\frac{p}{5}\right)}\right) = F_{p-\left(\frac{p}{5}\right)}$. Since $F_{p-\left(\frac{p}{5}\right)} \equiv 0 \pmod{p}$ by Lemma A.5, it follows from the above that $F_{n!} \equiv 0 \pmod{p}$. Combining this with Corollary 5.2, we see that

$$\frac{F_{n!}}{n!} \equiv 0 \pmod{\prod_{\substack{n < p \leq 2n + \left(\frac{p}{5}\right) \\ p \neq 5}} p}.$$

Invoking Lemma 5.4 repeatedly, we obtain

$$\frac{F_{(n+i)!}}{(n+i)!} \equiv 0 \pmod{\prod_{\substack{i < p \leq 2(n+i) + \left(\frac{p}{5}\right) \\ p \neq 5}} p}$$

for all i such that $n+i \geq 4$. Fixing $i = 4$ and using that $F_{4!}/4! = 2^2 \cdot 3 \cdot 7 \cdot 23$, we obtain the desired result (by again using Lemma 5.4). ■

Theorem 5.6. *F admits a unique continuous extension to a function $F : \hat{\mathbf{Z}} \to \hat{\mathbf{Z}}$, defined by*

$$F(s) = F_s \stackrel{\text{def}}{=} \frac{\vartheta^s - \bar{\vartheta}^s}{\vartheta - \bar{\vartheta}}. \tag{5.11}$$

Proof. By Lemma 2.8, taking $X = \mathbf{Z}$ and $Y = \hat{\mathbf{Z}}$, there exists a unique continuous extension $F : \hat{\mathbf{Z}} \to \hat{\mathbf{Z}}$, since $\mathbf{Z}$ is dense in $\hat{\mathbf{Z}}$ and $\hat{\mathbf{Z}}$ is complete. This gives the desired result. For uniform continuity of (5.11), let $N \geq 4$. If $x \equiv s \pmod{N!}$, we have $F_x \equiv F_s \pmod{N!}$ by Corollary 5.2. ∎

Strictly speaking, we have not yet defined the powering operation when the exponent is an arbitrary profinite integer, but we will return to this question in a later section.

Corollary 5.7. *For each $k \geq 3$ and $s \in \hat{\mathbf{Z}}$, the first k digits of F_s and L_s are determined by the first k digits of s.*

Proof. Let $n \geq 4$. Set $t = (\ldots s_{n+1}s_n 0 \ldots 0)_!$ and $t' = (\ldots 0 s_{n-1} \ldots s_1)_!$. Then

$$F_s = F_{t+t'} = F_{t+1}F_{t'} + F_t F_{t'-1} \equiv F_1 F_{t'} + F_0 F_{t'-1} \equiv F_{t'} \pmod{n!}, \tag{5.12}$$

by Corollary 5.2 and Lemma A.3. Of course, the same holds for L, since $L_s = F_{s-1} + F_{s+1}$. ∎

5.2 Fixed points of the Fibonacci map: an iterative approach (I)

Of particular interest are the fixed points of F, given by numbers $s \in \hat{\mathbf{Z}}$ that satisfy $F_s = s$. It is easy to see that apart from $F_0 = 0$, $F_1 = 1$ and $F_5 = 5$, no integer examples exist. However, $\hat{\mathbf{Z}}$ contains eight other fixed points which exhibit some quite remarkable behaviour, as we shall see further on.

By Corollary 5.2, $F_{n!}/n!$ is in $\hat{\mathbf{Z}}$ for all $n \geq 4$. Note that

$$\frac{F_{n!}}{n!} = \frac{\vartheta^{n!} - \bar{\vartheta}^{n!}}{n!(\vartheta - \bar{\vartheta})} = \frac{\vartheta^{n!} - 1}{n!(\vartheta - \bar{\vartheta})} - \frac{\bar{\vartheta}^{n!} - 1}{n!(\vartheta - \bar{\vartheta})} = \frac{1}{\vartheta - \bar{\vartheta}} \left(\frac{\vartheta^{n!} - 1}{n!} - \frac{\bar{\vartheta}^{n!} - 1}{n!} \right). \tag{5.13}$$

Hence

$$\lim_{n \to \infty} \frac{F_{n!}}{n!} = \frac{1}{\vartheta - \bar{\vartheta}} (\log(\vartheta) - \log(\bar{\vartheta})),$$

which exists since ϑ and $\bar{\vartheta}$ are units. Since $\log(\vartheta) + \log(\bar{\vartheta}) = \log(\vartheta\bar{\vartheta}) = \log(-1) = 0$, it follows that $\log(\vartheta) = -\log(\bar{\vartheta})$. Define

$$l \stackrel{\text{def}}{=} \frac{\log(\vartheta)}{\vartheta - \bar{\vartheta}} = \lim_{n \to \infty} \frac{F_{n!}}{2n!}. \tag{5.14}$$

By Lemma 5.5, l is divisible by all primes $p \neq 5$; more precisely, the number of factors p in l is equal to the number of factors p in $F_{p-1}F_{p+1}$. When $p = 5$, we have the following.

Lemma 5.8. *We have* $F_{n!}/n! \equiv 2 \pmod 5$ *for all* $n \geq 4$.

Proof. Adopting the notation from (4.15), a simple check shows that $A_n(\vartheta) = \frac{\vartheta^{n!}-1}{n!} \equiv \sqrt{5} \pmod 5$ and $A_n(\bar{\vartheta}) = \frac{\bar{\vartheta}^{n!}-1}{n!} \equiv -\sqrt{5} \pmod 5$ for $n = 4$ and $n = 5$. Let u be a unit in $\hat{\mathbf{Z}}[\vartheta]$. Since $A_{n+1}(u) \equiv A_n(u) \pmod{n!}$ for all $n \geq 4$ we have $A_n(u) \equiv A_5(u) \pmod 5$. It follows that $A_n(\vartheta) \equiv \sqrt{5} \pmod 5$ and $A_n(\bar{\vartheta}) \equiv -\sqrt{5} \pmod 5$. Hence $F_{n!}/n! = \frac{A_n(\vartheta)-A_n(\bar{\vartheta})}{\vartheta-\bar{\vartheta}} \equiv \frac{2\sqrt{5}}{\sqrt{5}} \equiv 2 \pmod 5$ for all $n \geq 4$. ∎

The eight other profinite fixed points can be computed by means of an iteration. Note that s is a fixed point of F_s if and only if $F_s \equiv s \pmod{n!}$ for all $n \geq 4$, by Corollary 5.7. The idea is to find for any $n \geq 4$ an $s_n \in \mathbf{Z}$ such that $F_{s_n} \equiv s_n \pmod{n!}$. Therefore, start by fixing $n = 4$. We then have to determine iteratively a $k = k(n)$ such that $s_{n+1} = s_n + kn!$. We should have $F_{s_{n+1}} \equiv s_{n+1} \equiv s_n + kn! \pmod{(n+1)!}$. Hence

$$\begin{aligned} F_{s_{n+1}} = F_{s_n+kn!} &= \frac{1}{2}\left(F_{s_n}L_{kn!} + F_{kn!}L_{s_n}\right), \\ &\equiv \frac{1}{2}\left(2F_{s_n} + kF_{n!}L_{s_n}\right) \pmod{(n+1)!}, \end{aligned}$$

where we used the addition law A.3 on the first line and Lemma 5.3 on the second. It follows that

$$\frac{F_{s_n} - s_n}{n!} + kL_{s_n}\frac{F_{n!}}{2n!} \equiv k \pmod{n+1},$$

and hence

$$\frac{F_{s_n} - s_n}{n!} \equiv k\left(1 - L_{s_n}\frac{F_{n!}}{2n!}\right) \pmod{n+1}. \tag{5.15}$$

This equation has a unique solution for k if $\gcd\left(n+1, 1 - L_{s_n}\frac{F_{n!}}{2n!}\right) = 1$. If $n+1$ is not divisible by 5, this follows immediately from Lemma 5.5. However, when $n+1$ is divisible by 5, we encounter the following problem.

Lemma 5.9. *If* $n \equiv -1 \pmod 5$, *then* $\gcd\left(n+1, 1 - L_{s_n}\frac{F_{n!}}{2n!}\right) = 5^k$ *for some positive integer* k.

Proof. The first few values of the Lucas sequence $(2, 1, 3, 4, 7, 11, \ldots)$ show that it is

periodic modulo 5, with

$$L_m \equiv \begin{cases} 2 \pmod 5 & \text{if } m \equiv 0 \pmod 4, \\ 1 \pmod 5 & \text{if } m \equiv 1 \pmod 4, \\ 3 \pmod 5 & \text{if } m \equiv 2 \pmod 4, \\ 4 \pmod 5 & \text{if } m \equiv 3 \pmod 4. \end{cases} \tag{5.16}$$

Let s be a fixed point of F. Corollary 5.7 shows that the first k digits of F_s are determined by the first k digits of s, for each $k \geq 3$. Hence, for example, $F_s \equiv s \pmod{4!}$. Modulo $4! = 24$, the only fixed points of F are 0, 1 and 5. Hence for any $n \geq 4$, either $s_n = (\ldots 000)_!$, $s_n = (\ldots 001)_!$ or $s_n = (\ldots 021)_!$. However, there are no even fixed points except 0, as we will prove in Lemma 5.10. It follows from (5.16) that $s_n \equiv 1 \pmod 4$ and hence $L_{s_n} \equiv 1 \pmod 5$. Hence by Lemma 5.8 we have $1 - L_{s_n} \frac{F_{n!}}{2n!} \equiv 0 \pmod 5$. By Theorem 5.5 the expression $1 - L_{s_n} \frac{F_{n!}}{2n!}$ is not divisible by any other prime less than $2n$. Obviously, all prime factors of $n+1$ are less than $2n$, so it follows that $\gcd\left(n+1, 1 - L_{s_n} \frac{F_{n!}}{2n!}\right) = 5^k$ for some $k \geq 1$. ■

We still need to prove the claim made in the previous lemma.

Lemma 5.10. *F has no nontrivial even fixed points.*

Proof. Let s be an even fixed point. The argument in the proof of the previous lemma shows that the last three digits of s must equal zero. Let $n \geq 4$ be given. If $s_n = 0$, then $F_{s_n} - s_n = 0$. Equation (5.15) shows that $k = 0$ is a solution for the next digit. Assuming that $n \not\equiv -1 \pmod 5$, it is the only solution, since $\gcd\left(n+1, 1 - L_{s_n} \frac{F_{n!}}{2n!}\right) = 1$. Now assume $n \equiv -1 \pmod 5$. Since $s_n \equiv 0 \pmod 4$, the periodicity of L (see (5.16)) shows that $L_{s_n} \equiv 2 \pmod 5$. Hence

$$1 - L_{s_n} \frac{F_{n!}}{2n!} \equiv -1 \pmod 5.$$

Again, Lemma 5.5 shows that $\gcd\left(n+1, 1 - L_{s_n} \frac{F_{n!}}{2n!}\right) = 1$, so $k = 0$ is the only solution. Hence $s = 0$. ■

5.3 The power series expansion for the Fibonacci map

Lemma 5.9 shows that a given starting value for the iteration alone is not sufficient to determine a unique digit of a fixed point s at each step. Intuitively, we would like to have a 'stronger' congruence than (5.15), in order to retain uniqueness of k, even when

$n \equiv -1 \pmod 5$. Ideally, we would like to have the same congruence as (5.15), but with $\pmod{n+1}$ replaced by $\pmod{5^r(n+1)}$ for some suitable r: the exponent satisfying $5^r = \gcd(1 - L_{s_n}\frac{F_{n!}}{2n!}, n+1)$. This turns out to be true, and establishing that fact (see Theorem 5.15) is the main goal of this chapter. However, we need some more machinery to prove this, to which this section is devoted, starting with the following theorem.

Theorem 5.11. *Let $P = \{p_1, \ldots, p_t\}$ be a set of prime numbers. Define*

$$a_p \overset{\text{def}}{=} \begin{cases} p-1 & \text{if } (\frac{p}{5}) = 1, \\ 2(p+1) & \text{if } (\frac{p}{5}) = -1, \\ 20 & \text{if } p = 5, \end{cases} \tag{5.17}$$

for any $p \in P$, and $n_P \overset{\text{def}}{=} \operatorname{lcm}\{a_p : p \in P\}$. Let $s \in \hat{\mathbf{Z}}$ be divisible by n_P and m an integer whose prime factors are contained in P. Then

$$\vartheta^s \equiv \sum_{k \geq 0} \frac{(l^* s)^k}{k!} \pmod m, \tag{5.18}$$

where $l^* = \log(\vartheta) = l\sqrt{5}$ (as defined in (5.14)).

Proof. Let $p \in P$. Then there exists an $\eta = \eta(p) \in \mathbf{Z}_p[\vartheta]$ such that

$$\vartheta^{a_p} = 1 + p\eta \tag{5.19}$$

by Lemma A.6. Since a_p divides s, we obtain $\vartheta^s = (1+p\eta)^{s/a_p}$. Hence $\log_p(1+p\eta) = \log_p(\vartheta^{a_p}) = a_p \log_p(\vartheta)$. Note that l_p, the p-th component of l as defined in (5.14), equals $\log_p(\vartheta)/(\vartheta - \bar{\vartheta})$ and is hence divisible by p by Lemma 5.5, if $p \neq 5$. Write $l_p^* = \log_p(\vartheta) = l_p\sqrt{5}$. Then we have

$$\begin{aligned} \vartheta^s &= (1+p\eta)^{s/a_p}, \\ &= \exp_p(\log_p((1+p\eta)^{s/a_p})), \\ &= \exp_p(l_p^* s), \\ &= 1 + l_p^* s + \frac{(l_p^* s)^2}{2!} + \frac{(l_p^* s)^3}{3!} + \cdots, \end{aligned}$$

which is a p-adic power series. Hence we obtain the congruence

$$\vartheta^s \equiv 1 + l^* s + \frac{(l^* s)^2}{2!} + \frac{(l^* s)^3}{3!} + \cdots \pmod{p^k} \tag{5.20}$$

for any integer $k \geq 0$. Using the Chinese Remainder Theorem, we obtain Equation (5.18). ■

Note that $\log_p(\vartheta) = -\log_p(\bar{\vartheta})$ for all p. Hence a similar argument would give

$$\bar{\vartheta}^s \equiv 1 - l^* s + \frac{(l^* s)^2}{2!} - \frac{(l^* s)^3}{3!} + \cdots \pmod{m}, \tag{5.21}$$

where s and m satisfy the same properties as in the previous theorem.

Using Theorem 5.11, we establish the following power series for F in the point s, around s_0.

Lemma 5.12. *Let P, a_p, n_P and m be as in Theorem 5.11. Let $s - s_0 \in \hat{\mathbf{Z}}$ be divisible by n_P. Then*

$$F_s \equiv \sum_{k \geq 0} 5^k l^{2k+1} L_{s_0} \frac{(s-s_0)^{2k+1}}{(2k+1)!} + 5^k l^{2k} F_{s_0} \frac{(s-s_0)^{2k}}{(2k)!} \pmod{m}. \tag{5.22}$$

Proof. Let $t \in \hat{\mathbf{Z}}$ be divisible by n_P. From Theorem 5.11 and the remark above, we obtain

$$\begin{aligned} F_t = \frac{\vartheta^t - \bar{\vartheta}^t}{\vartheta - \vartheta} &\equiv \frac{1}{\sqrt{5}} \left(2l^* t + 2\frac{(l^* t)^3}{3!} + \cdots \right), \\ &\equiv 2 \sum_{k \geq 0} 5^k l^{2k+1} \frac{t^{2k+1}}{(2k+1)!} \pmod{m}, \end{aligned} \tag{5.23}$$

and

$$\begin{aligned} L_t = \vartheta^t + \bar{\vartheta}^t &\equiv 2 + (l^* t)^2 + \frac{(l^* t)^4}{12} + \cdots, \\ &\equiv 2 \sum_{k \geq 0} 5^k l^{2k} \frac{t^{2k}}{(2k)!} \pmod{m}. \end{aligned} \tag{5.24}$$

Hence, writing $F_s = F_{s-s_0+s_0}$ and substituting $s - s_0$ for t, we obtain

$$\begin{aligned} F_s = F_{s-s_0+s_0} &= \frac{1}{2}(F_{s-s_0} L_{s_0} + L_{s-s_0} F_{s_0}), \\ &\equiv \sum_{k \geq 0} 5^k l^{2k+1} L_{s_0} \frac{(s-s_0)^{2k+1}}{(2k+1)!} + 5^k l^{2k} F_{s_0} \frac{(s-s_0)^{2k}}{(2k)!} \pmod{m}, \end{aligned}$$

which is the desired expression. ■

We can now conclude the proof of Lemma 5.3, using the following technical lemma.

Lemma 5.13. *Let $P_k = \{p : p \leq k\}$ be the set of primes less than or equal to k, and let $k \geq 12$. Adopting the notation from Theorem 5.11, we have*

$$\left\lfloor \frac{k}{2} \right\rfloor ! \equiv 0 \pmod{n_{P_k}} \text{ if } k \text{ is composite or } \left(\frac{k}{5}\right) = 1, \tag{5.25}$$

$$\left\lfloor \frac{k+1}{2} \right\rfloor ! \equiv 0 \pmod{n_{P_k}} \text{ if } \left(\frac{k}{5}\right) = -1, \tag{5.26}$$

where $\lfloor x \rfloor$ denotes the greatest integer less than or equal to x.

Proof. Note that $n_{P_{12}} = \operatorname{lcm}\{6, 8, 20, 16, 10\} = 2^4 \cdot 3 \cdot 5 = 240$, which divides $6! = 720$, and $n_{P_{13}} = \operatorname{lcm}\{6, 8, 20, 16, 10, 28\} = 2^4 \cdot 3 \cdot 5 \cdot 7 = 1680$, which divides $7! = 5040$. Now assume that the statements holds for some $k-1$ and k, with $k \geq 13$, and $k+1$ is not prime. Then $n_{P_{k+1}} = n_{P_k}$, and since we have $\left\lfloor \frac{k+1}{2} \right\rfloor ! \equiv 0 \pmod{n_{P_k}}$ by the induction hypothesis, it follows that $\left\lfloor \frac{k+1}{2} \right\rfloor ! \equiv 0 \pmod{n_{P_{k+1}}}$, so that Equation (5.25) holds.

If $k+1$ is prime, then k is even and hence composite. Therefore $n_{P_k} = n_{P_{k-1}}$, so that $n_{P_{k+1}} = \operatorname{lcm}\{n_{P_k}, a_{k+1}\} = \operatorname{lcm}\{n_{P_{k-1}}, a_{k+1}\}$. Again, we have two cases.

(1). If $\left(\frac{k}{5}\right) = -1$, then $a_{k+1} = 2(k+2) = 4 \cdot \frac{k+2}{2}$. Hence

$$n_{P_{k+1}} = \operatorname{lcm}\left\{ n_{P_{k-1}}, 4 \cdot \frac{k+2}{2} \right\}.$$

Since 4 divides $n_{P_{k-1}}$, using the induction hypothesis, it follows that $n_{P_{k+1}}$ is a divisor of

$$\frac{k+2}{2} \cdot \left\lfloor \frac{k}{2} \right\rfloor ! = \left\lfloor \frac{k+2}{2} \right\rfloor !,$$

which agrees with Equation (5.26).

(2). If $\left(\frac{k}{5}\right) = 1$, then $a_{k+1} = k = 2 \cdot \frac{k}{2}$. Hence

$$n_{P_{k+1}} = \operatorname{lcm}\left\{ n_{P_{k-1}}, 2 \cdot \frac{k}{2} \right\}.$$

Since 2 divides $n_{P_{k-1}}$, again using the induction hypothesis, it follows that $n_{P_{k+1}}$ is a divisor of

$$\frac{k}{2} \cdot \left\lfloor \frac{k-1}{2} \right\rfloor ! = \left\lfloor \frac{k}{2} \right\rfloor !,$$

if $k-1$ is not prime or $\left(\frac{k-1}{5}\right) = 1$. Once again, this agrees with Equation (5.25). However, we still need to consider the case that $\left(\frac{k-1}{5}\right) = -1$. In that case, $a_{k+1} = k$ and $a_{k-1} = 2k$, so their least common multiple is simply a_{k-1}. Hence $n_{P_{k+1}} = n_{P_{k-1}}$, which divides $\left\lfloor \frac{k}{2} \right\rfloor !$ by the induction hypothesis.

The claims (1) and (2) together conclude the proof of this lemma. ■

Proof of Lemma 5.3. Adopting the notation of the previous lemma, we see that n_{P_k} divides $k!$ for all $k \geq 12$. A simple calculation shows that this even holds for all $k \geq 5$. Hence choosing $n \geq 5, P = P_n, s = rn!$ for some integer $r > 0$ and $m = (n!)^2$ in Theorem 5.11, then the previous lemma shows that s divides n_{P_n}. Hence Equation (5.24) shows that

$$L_{rn!} \equiv 2 \sum_{k \geq 0} 5^k l^{2k} \frac{(rn!)^{2k}}{(2k)!} \equiv 2 \pmod{(n!)^2}. \tag{5.27}$$

If $n+1$ is not prime, then it is a divisor of $n!$ (see also the proof of Lemma 4.14). Hence $L_{rn!} \equiv 2 \pmod{(n+1)!}$, which was to be shown. ■

5.4 Fixed points of the Fibonacci map: an iterative approach (II)

In this section, we will state and prove the announced refinement of the congruence (5.15), see Theorem 5.15. Lemma 5.14 provides an essential technical tool for the proof of Theorem 5.15. In the course of its proof, we use the map

$$v_p : \hat{\mathbf{Z}} \to \mathbf{Z}_{\geq 0}, \quad v_p(s) \stackrel{\text{def}}{=} \max\{k : s \equiv 0 \pmod{p^k}\},$$

which counts the number of times a given profinite integer is divisible by some fixed prime number p.

Lemma 5.14. *Let $s \neq 0$ be a fixed point of F. Then*

$$v_5(1 - lL_s) = j, \tag{5.28}$$

for some $1 \leq j \leq 3$.

Proof. By Lemma 5.9, the j in the theorem is larger than or equal to 1. Therefore, we have to show that $1 - lL_s \not\equiv 0 \pmod{5^4}$. Note that if we know the first 19 digits of l (or equivalently, $l \pmod{20!}$), then we also know $l \pmod{5^4}$, since 5^4 divides $20!$.
One particularly nice application of the power series is the determination of l to any desired precision. Namely, set $s_0 = 0$, then $F_{s_0} = 0$ and $L_{s_0} = 2$. For suitable m and s, the power series now reads

$$\begin{aligned} F_s &\equiv \sum_{k\geq 0} 5^k l^{2k+1} \frac{2s^{2k+1}}{(2k+1)!}, \\ &\equiv 2ls + \frac{2\cdot 5\cdot l^3\cdot s^3}{3!} + \frac{2\cdot 5^2\cdot l^5\cdot s^5}{5!} + \cdots \pmod{m}. \end{aligned} \tag{5.29}$$

To determine l to an accuracy of 19 digits, we have to find an $s \in \hat{\mathbf{Z}}$ and put $m = 2s\cdot 20!$, in such a way that $F_s \equiv 2ls \pmod{m}$. Then $F_s/2s$ would be congruent to $l \pmod{20!}$. Note that $20! = 2^{18}\cdot 3^8\cdot 5^4\cdot 7^2\cdot 11\cdot 13\cdot 17\cdot 19$. Let P be the set of prime numbers less than or equal to 19. Then $n_P = \operatorname{lcm}(6,8,20,16,10,28,36,18) = 2^4\cdot 3^2\cdot 5\cdot 7$.
Recall that l is divisible by any prime number except 5. Hence $(2\cdot 5\cdot l^3\cdot s^3)/6$ is divisible by $s^3\cdot(2^3\cdot 3^2\cdot 5\cdot 7^3\cdot 11^3\cdot\ldots)$. This is congruent to 0 $\pmod{m}$ if $2^{16}\cdot 3^6\cdot 5^3$ divides s^2. Pick $s = 2^8\cdot 3^3\cdot 5^2\cdot 7$ (the factor 7 is included so that n_P divides s). Since all prime factors of m are contained in P, it now follows that $(2\cdot 5\cdot l^3\cdot s^3)/6$ – and therefore all subsequent terms of the power series development (5.29) – are congruent to 0 $\pmod{m}$. Hence $F_s/2s \equiv l \pmod{20!}$. A computer calculation shows that the first 19 digits of l are therefore given by

$$l = (\ldots, 18, 10, 4, 7, 6, 8, 10, 10, 4, 9, 0, 0, 0, 1, 2, 0, 1, 0, 0)_!, \tag{5.30}$$

where we denote $(\ldots, c_1, c_0)_! = (\ldots c_1 c_0)_!$.

We now return to the proof of the lemma. Since $n!$ is divisible by 5^4 for all $n \geq 20$, using (5.30), we can calculate that $l \equiv 591 \pmod{5^4}$. Assume by contradiction that $1 - lL_s \equiv 0 \pmod{5^4}$. Then $L_s \equiv 591^{-1} \equiv 386 \pmod{5^4}$. Note that L is also periodic modulo 5^4, with a period of 500, as one may verify computationally. We can now use a computer calculation to show that no nonnegative integer $n < 500$ satisfies $L_n \equiv 386 \pmod{5^4}$. Therefore, no profinite integer s (in particular, no fixed point s of F) satisfies $L_s \equiv 386 \pmod{5^4}$. This concludes the proof. ∎

We are now ready to prove the main result of this chapter.

Theorem 5.15. *Let $n \geq 5$ be an integer and $1 \leq j \leq 3$ be the integer satisfying $j = v_5(1 - lL_{s_n})$. Then*

$$\frac{F_{s_n} - s_n}{5^j n!} \equiv k \frac{1 - lL_{s_n}}{5^j} \pmod{n+1}. \tag{5.31}$$

for all $n \geq 5j$. Furthermore, if we take $n \geq 15$, then k is uniquely determined by this congruence.

Proof. Recall that $s_{n+1} = s_n + kn!$, and we need to determine k so that $F_{s_{n+1}} \equiv s_{n+1} \pmod{(n+1)!}$; however, let us now impose the stricter congruence $F_{s_{n+1}} \equiv s_{n+1} \pmod{5^j(n+1)!}$. Set $P = P_{n+1}$, the set of primes less than or equal to $n+1$, and $m = 5^j(n+1)!$ in Lemma 5.12. Note that $s_{n+1} - s_n = kn!$ is divisible by n_P by Lemma 5.13. Looking at the associated power series for F,

$$F_{s_{n+1}} = \sum_{t \geq 0} 5^t l^{2t+1} L_{s_n} \frac{(kn!)^{2t+1}}{(2t+1)!} + 5^t l^{2t} F_{s_n} \frac{(kn!)^{2t}}{(2t)!} \pmod{5^j(n+1)!}, \tag{5.32}$$

it is clear that all terms beyond the third vanish when $j = 3$, and therefore also when $j < 3$. Hence, it reads

$$F_{s_{n+1}} \equiv lL_{s_n} kn! + F_{s_n} + A + B \pmod{5^j(n+1)!},$$

with

$$A = 5l^3 L_{s_n} \frac{(kn!)^3}{6} + 5l^2 F_{s_n} \frac{(kn!)^2}{2}, \quad B = 25l^5 L_{s_n} \frac{(kn!)^5}{120} + 25l^4 F_{s_n} \frac{(kn!)^4}{24}.$$

Note that both A and B are divisible by $5l(kn!)^2$. Some elementary rewriting shows that $5l(kn!)^2 \equiv 0 \pmod{5^j(n+1)!}$ if $n \geq 5j$. Hence

$$F_{s_{n+1}} \equiv lL_{s_n} kn! + F_{s_n} \pmod{5^j(n+1)!}$$

for all $n \geq 5j$, and therefore,

$$\frac{1 - lL_{s_n}}{5^j} kn! \equiv \frac{kn! + F_{s_n} - F_{s_{n+1}}}{5^j} \equiv \frac{F_{s_n} - s_n}{5^j} \pmod{(n+1)!}, \tag{5.33}$$

since $F_{s_{n+1}} \equiv s_n + kn! \pmod{5^j(n+1)!}$. Dividing by $n!$ yields the desired congruence (5.31). Furthermore, since $\gcd(1 - lL_{s_n}, n+1)$ is a power of 5 by Lemma 5.9 and at

most 5^j, we have

$$\gcd\left(\frac{1-lL_{s_n}}{5^j}, n+1\right) = 1,$$

for all $n \geq 15 \geq 5j$. Therefore, there is a unique k satisfying (5.31). ■

Theorem 5.15 shows that the fixed points of F are uniquely determined, once the first 14 digits of s are known. This means (by combining with the uniqueness of k when $n \not\equiv -1 \pmod 5$) that we only have to make choices for the fourth, ninth, and fourteenth digit, each admitting five options for k that satisfy the congruence (5.15). Computationally, we find eleven possibilities for the first 14 digits, namely

$$\begin{aligned}
z_1 &= (\ldots, 0,0,0,0,0,0,0,0,0,0,0,0,0,0)_!,\\
z_2 &= (\ldots, 0,0,0,0,0,0,0,0,0,0,0,0,0,1)_!,\\
z_3 &= (\ldots, 0,0,0,0,0,0,0,0,0,0,0,0,2,1)_!,\\
z_{1,5} = z_4 &= (\ldots, 11,2,9,0,10,0,7,1,4,1,1,0,0,1)_!,\\
z_{1,0} = z_5 &= (\ldots, 8,11,1,3,3,4,7,1,4,1,1,0,0,1)_!,\\
z_{1,-5} = z_6 &= (\ldots, 6,5,6,5,7,8,7,1,4,1,1,0,0,1)_!,\\
z_{1,-1} = z_7 &= (\ldots, 8,0,7,3,3,9,5,3,1,2,2,0,0,1)_!,\\
z_{5,0} = z_8 &= (\ldots, 12,8,5,2,4,4,0,0,0,0,0,0,2,1)_!,\\
z_{5,-5} = z_9 &= (\ldots, 10,2,10,4,8,8,0,0,0,0,0,0,2,1)_!,\\
z_{5,-1} = z_{10} &= (\ldots, 11,11,11,2,4,8,7,1,4,1,1,0,2,1)_!,\\
z_{5,1} = z_{11} &= (\ldots, 3,11,3,11,0,9,1,6,2,4,4,0,2,1)_!.
\end{aligned} \tag{5.34}$$

There are 52 other integers s satisfying $F_s \equiv s \pmod{15!}$. Of those, 32 can be constructed as follows: Pick a z_i with $4 \leq i \leq 11$ from the list above. Change its last (i.e. leftmost) digit to another number between 0 and 15, such that the new digit is congruent to the old digit, modulo 3. Since there are four options of those, this gives $4 \cdot 8 = 32$ options. However, none of these options satisfies (5.31) with $n = 15$, for any k, as one may check computationally.

The other twenty options are profinite numbers that already differ from the ones given above at an earlier digit. None of these satisfies the congruence (5.31) with $n = 14$, for any k, as a straightforward computation shows.

Since no nontrivial even fixed points exist, z_1 must be 0. Lastly, when i is 2 or 3, then $F_{z_i} = z_i$. Hence $k = 0$ is always a solution for the next digit of the congruence (5.31). By uniqueness, no other solutions exist. Hence $z_2 = 1$ and $z_3 = 5$. The eight other fixed points are the nontrivial ones. In Appendix C, where they are given to fifty digits, one also finds the first hundred digits of l.

The alternative indices of the fixed points are chosen because we have the following conjecture.

Conjecture 5.16 (Lenstra)**.** *Let $a \in \{1, 5\}$ and $b \in \{-5, -1, 0, 1, 5\}$, then*

$$z_{a,b} \equiv a \pmod{6^k}, \quad z_{a,b} \equiv b \pmod{5^k}, \tag{5.35}$$

for all positive integers k. (For $a = b \in \{1, 5\}$, one may take $z_{a,b} = a$.) Furthermore, the fixed points are uniquely determined by these congruences.

According to Lenstra ([Len05]), the fixed points $z_{a,b}$ have "the tendency to approximately inherit properties of a, b." The exact outcome of these tendencies may be found in the cited article. Among those, we have $z_{1,0}^2 \equiv z_{1,0} \pmod{10!}$, by analogy of the fact that both 0 and 1 satisfy $x^2 = x$; likewise, $z_{1,-1}^2 \equiv 1 \pmod{21!}$ is reminiscent of the property that both 1 and -1 satisfy $x^2 = 1$; furthermore, $z_{1,5} + z_{5,1} \equiv 6 \pmod{30!}$ and $z_{1,5} \cdot z_{5,1} \equiv 5 \pmod{30!}$ are similar to the equalities $1 + 5 = 6$ and $1 \cdot 5 = 5$; and quite stunningly,

$$z_{5,-5}^2 \equiv 25 \pmod{201!},$$

which reflects $(\pm 5)^2 = 25$. Further investigations into the realm of profinite integers shall have to account for this now seemingly inexplicable behaviour.

A Identities of the Fibonacci and Lucas sequences

Lemma A.1. *Let $\vartheta = \frac{1+\sqrt{5}}{2}$ and $\bar{\vartheta} = \frac{1-\sqrt{5}}{2}$ be the roots in $\mathbf{Z}[\frac{1+\sqrt{5}}{2}]$ of $x^2 - x - 1$. Define*

$$\tilde{F}_n \stackrel{\text{def}}{=} \frac{\vartheta^n - \bar{\vartheta}^n}{\vartheta - \bar{\vartheta}}, \quad \tilde{L}_n \stackrel{\text{def}}{=} \vartheta^n + \bar{\vartheta}^n,$$

for all integers n. Then $\tilde{F}_n = F_n$ and $\tilde{L}_n = L_n$.

Proof. We proceed by induction. A simple check shows that $\tilde{F}_0 = 0$, $\tilde{F}_1 = 1$, $\tilde{L}_0 = 2$ and $\tilde{L}_1 = 1$. Now assume the statements hold for $n = k-1$ and $n = k$. Since ϑ and $\bar{\vartheta}$ satisfy $x^2 = x + 1$, we obtain

$$\begin{aligned}\tilde{F}_{k+1} &= \frac{\vartheta^{k+1} - \bar{\vartheta}^{k+1}}{\vartheta - \bar{\vartheta}} = \frac{\vartheta^k + \vartheta^{k-1} - (\bar{\vartheta}^k + \bar{\vartheta}^{k-1})}{\vartheta - \bar{\vartheta}}, \\ &= \frac{\vartheta^k - \bar{\vartheta}^k}{\vartheta - \bar{\vartheta}} + \frac{\vartheta^{k-1} - \bar{\vartheta}^{k-1}}{\vartheta - \bar{\vartheta}} = \tilde{F}_k + \tilde{F}_{k-1}.\end{aligned}$$

Similarly, $\tilde{L}_{k+1} = \tilde{L}_k + \tilde{L}_{k-1}$. Hence $\tilde{F}_n$ and $\tilde{L}_n$ satisfy the same recurrence relation as F_n and L_n and have the same starting values, so $\tilde{F}_n = F_n$ and $\tilde{L}_n = L_n$ for all n. ■

Lemma A.2. *The Lucas numbers satisfy $L_n = F_{n-1} + F_{n+1}$ for all integers n.*

Proof. Note that $F_{-1} + F_1 = L_0 = 2$ and $F_0 + F_2 = L_1 = 1$. Furthermore, the sequence defined by $K_n = F_{n-1} + F_{n+1}$ for all n clearly satisfies $K_{n+1} = K_n + K_{n-1}$. Hence the result follows by induction. ■

Lemma A.3 (Addition law of Fibonacci numbers)**.** *The Fibonacci numbers satisfy*

$$F_{m+n} = F_m \cdot \frac{L_n}{2} + \frac{L_m}{2} \cdot F_n = F_{n+1}F_m + F_nF_{m-1}.$$

Proof. We start by proving the first equality. Using Lemma A.1, we have

$$F_m \cdot L_n = \frac{\vartheta^{m+n} - \bar{\vartheta}^{m+n} + \vartheta^m\bar{\vartheta}^n - \bar{\vartheta}^m\vartheta^n}{\vartheta - \bar{\vartheta}}.$$

Interchanging m and n gives a similar formula for $L_m \cdot F_n$, and adding them gives

$$F_m \cdot L_n + L_m \cdot F_n = 2 \cdot \frac{\vartheta^{m+n} - \bar{\vartheta}^{m+n}}{\vartheta - \bar{\vartheta}} = 2 \cdot F_{m+n}.$$

For the second equality, we have

$$\begin{aligned} F_m \cdot L_n + L_m \cdot F_n &= F_m \cdot (F_{n-1} + F_{n+1}) + (F_{m-1} + F_{m+1}) \cdot F_n, \\ &= F_m \cdot (F_{n-1} + F_{n+1}) + (2F_{m-1} + F_m) \cdot F_n, \\ &= F_m \cdot (F_{n-1} + F_n) + F_m \cdot F_{n+1} + 2F_n \cdot F_{m-1}, \\ &= 2\,(F_{n+1}F_m + F_nF_{m-1}). \end{aligned}$$

where the equality on the first line follows by Lemma A.2. ■

Lemma A.4. *The Fibonacci sequence is a* ***strong divisibility sequence****; that is, it satisfies*

$$\gcd(F_m, F_n) = F_{\gcd(m,n)},$$

for all integers m and n.

Proof. See [Luc78, p. 206]. ■

Lemma A.5. *For any prime $p \neq 5$, we have*

$$F_{p-\left(\frac{p}{5}\right)} \equiv 0 \pmod{p}, \quad F_p \equiv \left(\frac{p}{5}\right) \pmod{p}, \quad \text{and} \quad F_{p+\left(\frac{p}{5}\right)} \equiv 1 \pmod{p}.$$

Proof. Note that the statements hold for $p = 2$. If $p \neq 2$, a straightforward calculation shows that, in $\mathbf{Z}[\vartheta]$,

$$\vartheta^p \equiv \left(\frac{1+\sqrt{5}}{2}\right)^p \equiv \frac{1+\sqrt{5}^p}{2} \equiv \frac{1+5^{\frac{p-1}{2}}\sqrt{5}}{2} \pmod{p}. \tag{A.1}$$

and similarly for $\bar{\vartheta}$. Note that $5^{\frac{p-1}{2}} = \left(\frac{5}{p}\right) \pmod{p}$ and $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$ by quadratic reciprocity. Recall that

$$\left(\frac{p}{5}\right) = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod 5, \\ -1 & \text{if } p \equiv \pm 2 \pmod 5, \\ 0 & \text{if } p = 5. \end{cases}$$

Since $p \neq 5$, we won't consider the last case. It follows that

$$\vartheta^p \equiv \begin{cases} \vartheta \pmod p & \text{if } \left(\frac{p}{5}\right) = 1, \\ \bar{\vartheta} \pmod p & \text{if } \left(\frac{p}{5}\right) = -1, \end{cases} \quad \text{and} \quad \bar{\vartheta}^p \equiv \begin{cases} \bar{\vartheta} \pmod p & \text{if } \left(\frac{p}{5}\right) = 1, \\ \vartheta \pmod p & \text{if } \left(\frac{p}{5}\right) = -1. \end{cases} \tag{A.2}$$

Putting things back together, we obtain $\vartheta^p - \bar{\vartheta}^p \equiv (\vartheta - \bar{\vartheta}) \cdot \left(\frac{p}{5}\right)$ and hence $F_p \equiv \left(\frac{p}{5}\right) \pmod{p}$. We also deduce that

$$\vartheta^{p-\left(\frac{p}{5}\right)} - \bar{\vartheta}^{p-\left(\frac{p}{5}\right)} \equiv \vartheta^{1-1} - \bar{\vartheta}^{1-1} \equiv 0,$$

if $\left(\frac{p}{5}\right) = 1$, and

$$\vartheta^{p-\left(\frac{p}{5}\right)} - \bar{\vartheta}^{p-\left(\frac{p}{5}\right)} \equiv \bar{\vartheta} \cdot \vartheta - \vartheta \cdot \bar{\vartheta} = 0,$$

if $\left(\frac{p}{5}\right) = -1$. Hence we obtain $F_{p-\left(\frac{p}{5}\right)} \equiv 0 \pmod{p}$. Finally, using that $F_{n+1} = F_n + F_{n-1}$, again separating the two cases, we get $F_{p+\left(\frac{p}{5}\right)} \equiv 1 \pmod{p}$. ■

Lemma A.6. *For all primes $p \neq 5$, the order of ϑ and $\bar{\vartheta}$ in $\mathbf{Z}/p\mathbf{Z}[\vartheta]$ is a divisor of either $p-1$ (if $\left(\frac{p}{5}\right) = 1$) or of $2(p+1)$ (if $\left(\frac{p}{5}\right) = -1$). Furthermore, when $p = 5$, the order of ϑ and $\bar{\vartheta}$ equals 20.*

Proof. The expressions in (A.2) show that $\vartheta^{p-1} \equiv 1 \pmod{p}$ and $\bar{\vartheta}^{p-1} \equiv 1 \pmod{p}$ if $\left(\frac{p}{5}\right) = 1$. When $\left(\frac{p}{5}\right) = 1$, we see that $\vartheta^{p+1} \equiv -1 \pmod{p}$ and $\bar{\vartheta}^{p+1} \equiv -1 \pmod{p}$. Hence squaring yields the result in both cases. When $p = 5$, a straightforward calculation shows that the order of ϑ and $\bar{\vartheta}$ equals 20 (as a consequence of the fact that $\vartheta^5 = 5\vartheta + 3 \equiv 3 \pmod{5}$ – and the same holds for $\bar{\vartheta}$). ■

B The ring $\mathbf{Z}_p$ of p-adic integers

Here, we will present a short and informal overview of the construction of the p-adic ring $\mathbf{Z}_p$, for a given prime p, along with some theorems. Define $|n|_p = p^{-\max\{k : n \equiv 0 \pmod{p^k}\}}$ if $n \neq 0$, and zero otherwise. Completely analogous to the construction of $\hat{\mathbf{Z}}$ (see Chapter 3), we may now define a metric d_p on $\mathbf{Z}$ by setting $d_p(x, y) = |x - y|_p$. Once again, this induces a metric on the space $CS(\mathbf{Z})$ of Cauchy sequences (with respect to d_p). Using (mutatis mutandis) the same equivalence relation $\sim$ as before, we construct $\mathbf{Z}_p$ as $CS(\mathbf{Z})/\sim$, and endow it with a metric also induced by d_p. This space and its associated maps satisfy analogues of many basic properties that also hold for the ring of profinite integers. Among these are Lemmas 3.5, 3.6, 3.7, 3.8, and Theorems 4.1 and 4.5.

The reader may find proofs of these statements and more on p-adic integers in (for example) [Kob84, Rob00].

C Fixed points up to fifty digits

Using the methods described in the last chapter, we calculated the eight nontrivial fixed points up to 50 digits, which are given by

$$\begin{aligned}
z_{1,5} = z_4 &= (\ldots, 32, 35, 20, 16, 39, 40, 34, 6, 30, 18, 12, 17, 28, 21, 20, 2, 3, 6, 29, 2, 29, 26,\\
&\quad 26, 24, 16, 3, 19, 21, 4, 18, 6, 16, 11, 6, 16, 2, 11, 2, 9, 0, 10, 0, 7, 1, 4, 1, 1, 0, 0, 1)_!,\\
z_{1,0} = z_5 &= (\ldots, 6, 49, 13, 0, 18, 39, 15, 19, 7, 32, 27, 38, 14, 9, 6, 12, 15, 10, 15, 27, 19, 4,\\
&\quad 28, 14, 8, 23, 13, 16, 5, 0, 7, 16, 14, 7, 11, 6, 8, 11, 1, 3, 3, 4, 7, 1, 4, 1, 1, 0, 0, 1)_!,\\
z_{1,-5} = z_6 &= (\ldots, 32, 13, 5, 31, 44, 37, 41, 31, 28, 5, 2, 18, 38, 34, 29, 22, 27, 14, 2, 20, 8, 13,\\
&\quad 1, 4, 1, 17, 7, 11, 5, 4, 8, 16, 17, 8, 6, 10, 6, 5, 6, 5, 7, 8, 7, 1, 4, 1, 1, 0, 0, 1)_!,\\
z_{1,-1} = z_7 &= (\ldots, 25, 4, 1, 30, 29, 14, 24, 18, 15, 28, 29, 35, 8, 24, 30, 19, 28, 10, 25, 17, 10,\\
&\quad 25, 16, 27, 26, 1, 18, 21, 3, 0, 0, 8, 1, 3, 15, 1, 8, 0, 7, 3, 3, 9, 5, 3, 1, 2, 2, 0, 0, 1)_!,\\
z_{5,0} = z_8 &= (\ldots, 25, 13, 41, 31, 25, 44, 26, 12, 20, 14, 15, 20, 24, 25, 23, 10, 12, 3, 19, 24, 20,\\
&\quad 8, 1, 17, 19, 19, 18, 19, 0, 4, 1, 0, 3, 0, 12, 3, 12, 8, 5, 2, 4, 4, 0, 0, 0, 0, 0, 0, 2, 1)_!,\\
z_{5,-5} = z_9 &= (\ldots, 50, 27, 34, 15, 4, 43, 7, 24, 40, 28, 31, 1, 10, 13, 9, 20, 24, 7, 6, 17, 9, 16,\\
&\quad 3, 7, 12, 13, 12, 14, 0, 8, 2, 0, 6, 1, 7, 7, 10, 2, 10, 4, 8, 8, 0, 0, 0, 0, 0, 0, 2, 1)_!,\\
z_{5,-1} = z_{10} &= (\ldots, 7, 49, 12, 19, 24, 31, 14, 43, 24, 11, 30, 25, 9, 0, 30, 28, 5, 31, 10, 9, 6, 28, 19,\\
&\quad 3, 9, 23, 23, 23, 21, 3, 14, 11, 8, 14, 15, 14, 11, 11, 11, 2, 4, 8, 7, 1, 4, 1, 1, 0, 2, 1)_!,\\
z_{5,1} = z_{11} &= (\ldots, 22, 7, 18, 19, 14, 10, 14, 2, 1, 30, 23, 14, 20, 18, 33, 23, 15, 33, 23, 2, 6, 3,\\
&\quad 2, 3, 10, 22, 5, 2, 18, 3, 14, 3, 7, 11, 0, 13, 3, 11, 3, 11, 0, 9, 1, 6, 2, 4, 4, 0, 2, 1)_!.
\end{aligned}$$

Furthermore, the first 100 digits of l are

$$\begin{aligned}
l = (\ldots, &57, 88, 83, 84, 84, 49, 90, 16, 67, 83, 22, 83, 71, 65, 0, 26, 69, 45, 21, 69, 13, 63, 17, 59,\\
&51, 62, 56, 29, 35, 4, 64, 4, 11, 25, 39, 24, 63, 51, 48, 54, 5, 0, 52, 36, 1, 32, 22, 1, 16, 11, 37,\\
&2, 31, 14, 40, 31, 42, 27, 41, 24, 27, 13, 19, 8, 4, 26, 33, 5, 1, 13, 17, 11, 23, 4, 7, 1, 16, 0, 4, 16,\\
&13, 18, 10, 4, 7, 6, 8, 10, 10, 4, 9, 0, 0, 0, 1, 2, 0, 1, 0, 0)_!.
\end{aligned}$$

References

[Beu15] F. Beukers, *Getaltheorie - Een inleiding*, Epsilon Editions, Utrecht 2015.

[Cra16] M. Crainic (2016), *Inleiding Topologie 2015/2016*. Retrieved from URL = <http://www.staff.science.uu.nl/ crain101/topologie2015/ aaa-main-2015-2016.pdf>.

[Fur55] H. Furstenberg (1955), *On the Infinitude of Primes,* The American Mathematical Monthly, 62(5), 353-353. doi:10.2307/2307043

[HW08] G. H. Hardy & E. M. Wright (2008), *An Introduction to the Theory of Numbers,* sixth edition. Oxford: Oxford University Press.

[Kob84] N. Koblitz (1984), *p-adic Numbers, p-adic Analysis, and Zeta-Functions,* second edition. New York: Springer Verlag.

[Len03] H. W. Lenstra (2003), *Profinite Groups,* lecture notes available on the web. Retrieved from URL = <http://www.mat.unb.br/~ zapata/Research/Files/lenstra-profinite.pdf>.

[Len05] H. W. Lenstra (2005), *Profinite Fibonacci numbers,* Nieuw Arch. Wisk. (5)6, 297–300.

[Len16] H. W. Lenstra (2016), *Profinite Number Theory,* EMS Newsletter June 2016 (100), 14-18.

[LM15] R. Lovas & I. Mezo (2015), *Some observations on the Furstenberg topological space,* Elemente der Mathematik, 70, 103–116. doi:10.4171/EM/283

[Luc78] E. Lucas (1878), *Théorie des Fonctions Numériques Simplements Périodiques,* [Continued]. American Journal of Mathematics, 1(3), 197-240. doi:10.2307/2369311

[Rob00] A. M. Robert (2000), *A Course in p-adic Analysis.* New York: Springer Verlag.

[RZ10] L. Ribes & P. Zalesskii (2010), *Profinite Groups,* second edition. Berlin: Springer Verlag.

[Sea06] O'Searcoid, M. (2006), *Metric spaces,* Springer Science & Business Media.