Profinite Fibonacci Numbers

Alexander Braun

June 2026

Abstract. In this paper, we explore the extension of Fibonacci numbers to the profinite integers $\hat{\mathbb{Z}}$. We begin by defining the profinite integers through an inverse limit and describing their natural topology, then define profinite Fibonacci numbers by taking limits of ordinary Fibonacci numbers under this topology. We prove that the standard Fibonacci recurrence $F_p + F_{p+1} = F_{p+2}$ continues to hold for all profinite p, and prove the GCD identity $\gcd(F_a, F_b) = F_{\gcd(a,b)}$ for profinite a and b. Finally, we prove that the natural map $\mathbb{Z} \to \hat{\mathbb{Z}}$ is injective, and that distinct profinite integers represent distinct integers.

1 Introduction

Before defining profinite Fibonacci numbers, it is important to first define the profinite integers and the Fibonacci numbers.

Definition 1.1. The Fibonacci numbers are defined by $F_1 = 1, F_2 = 1$, and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 3$.

Definition 1.2. The profinite integers $\hat{\mathbb{Z}}$ are defined as the inverse limit

$$\hat{\mathbb{Z}} = \varprojlim_{n} \mathbb{Z}/n\mathbb{Z},$$

meaning that $\hat{\mathbb{Z}}$ consists of all sequences of residues compatible under the natural reduction maps $\mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ whenever $n|m$. We can topologize $\hat{\mathbb{Z}}$ as a subspace of the product $\prod_{n\geq 1} \mathbb{Z}/n\mathbb{Z}$, where each factor carries the discrete topology; by Tychonoff's theorem this makes $\hat{\mathbb{Z}}$ a compact, Hausdorff, totally disconnected topological ring.

Proposition 1.3. A profinite integer can be concretely represented as an infinite sequence $(c_1, c_2, \cdots)$ with $0 \leq c_i \leq i$, corresponding numerically to the formal sum $\sum_{i=1}^{\infty} c_i \cdot i!$. Although profinite integers are conventionally written as $\cdots a_3 a_2 a_1$ (right-to-left), we write them as $(a_1, a_2, \cdots)$ throughout this paper for the sake of simplicity.

Proposition 1.4. By the Chinese Remainder Theorem, there is an isomorphism of topological rings

$$\hat{\mathbb{Z}} \cong \prod_{p \text{ prime}} \mathbb{Z}_p,$$

where $\mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$ is the ring of p-adic integers. Concretely, a profinite integer q corresponds to $(x_2, x_3, \cdots)$ where $x_p \in \mathbb{Z}_p$ and $q \equiv x_p \pmod{p^n}$ for all $n \geq 1$.

Remark 1.5. Although it may seem like profinite integers have to be positive, negative profinite numbers exist, and for an integer that can be written as $(a_1, a_2, \cdots)$ in profinite form, its negative can be written as $(1 - a_1, 2 - a_2, 3 - a_3, 4 - a_4, 5 - a_5, \cdots) + 1$. This is because $-1 = \lim_{n\to\infty}(n+1)! - 1 = n \cdot n! + (n-1) \cdot (n-1)! + \cdots + 1 \cdot 1! = (1, 2, 3, 4, 5, \cdots)$, and any profinite integer $(a_1, a_2, \cdots)$ can be easily subtracted from this, as $0 \leq a_k \leq k$. Then, we add back the 1 to create the profinite integer $-(a_1, a_2, \cdots) = (1 - a_1, 2 - a_2, 3 - a_3, 4 - a_4, 5 - a_5, \cdots) + 1$.

Definition 1.6. For a profinite integer p, we define

$$F_p = \lim_{i\to\infty} F_{a_i} \quad \text{in } \hat{\mathbb{Z}},$$

where $a_i \equiv p \pmod{i!}$ with $0 \leq a_i < i!$, or equivalently, $a_i = (a_1, a_2, \cdots a_{i-1})$, the first $i - 1$ terms of p. This limit exists in $\hat{\mathbb{Z}}$ because for each fixed m, the Fibonacci sequence is eventually periodic $\pmod{m}$ (with Pisano period), so the sequence $F_{a_i} \pmod{m}$ is eventually constant.

In this paper, we will discuss the mapping between $\mathbb{Z}$ and $\hat{\mathbb{Z}}$, and explore identities and examples of profinite Fibonacci numbers.

2 Examples and Identities

2.1 Examples

Since the method to figure out what a profinite Fibonacci number would look like seems obscure, we will work through an example to make the process more clear. Take the profinite integer $(1, 2, 3, \cdots)$. We can write each of its truncations as $(1) = 1 \cdot 1! = 1, (1, 2) = 2 \cdot 2! + 1 \cdot 1! = 5, (1, 2, 3) = 23, (1, 2, 3, 4) = 119, \cdots$. The Fibonacci representations of the numbers $1, 5, 23, 119, \cdots$ are $F_1 = 1, F_5 = 5, F_{23} = 28657, F_{119} = 3311648143516982017180081$. These numbers are then turned back into profinite integers, giving us $(1), (1, 2), (5, 4, 4, 4, 0, 0, 1)$, $(1, 0, 0, 0, 0, 2, 3, 7, 1, 8, 1, 4, 3, 2, 13, 15, 10, 8, 11, 14, 6, 2, 8, 5, 0, 0, 0), \cdots$. Notice that as these Fibonacci numbers get larger, we end up getting that $F_{(1,2,3,\cdots)} = (1, 0, 0, 0, \cdots) = 1$. Indeed, this is true with regular Fibonacci numbers, since $(1, 2, 3, \cdots) = -1$, and $F_{-1} = 1$. In short, the process to generate profinite Fibonacci numbers is to find the limit of the profinite integer, L, find F_L, and then turn F_L back into a profinite integer.

2.2 A Simple Identity

Theorem 2.1. For all profinite p, $F_p + F_{p+1} = F_{p+2}$.

Notice that if $F_p + F_{p+1} \equiv F_{p+2} \pmod{m}$ for all m, then this relation will hold generally. Since the Fibonacci sequence is periodic mod n for all n, if we let this period be q, then we simply must prove that $F_{p\text{mod } q} + F_{(p+1) \bmod q} \equiv F_{(p+2)\text{mod } q}\text{mod } m$ for all m. This is clearly true, since $F_r + F_{r+1} = F_{r+2}$ for finite r, so the identity $F_p + F_{p+1} = F_{p+2}$ must hold for profinite p.

3 GCD Theorem

In this section, we will prove one theorem. Before stating it, we first define GCD in $\hat{\mathbb{Z}}$. In $\hat{\mathbb{Z}}$, a divides b if and only if $k \in \hat{\mathbb{Z}}$ exists such that $a \cdot k = b$. The gcd of profinite integers $p = (x_p)_p$ and $q = (y_p)_p$, written in their p-adic components, is defined as

$$\gcd(p, q) = \prod_{p \text{ prime}} p^{\min(v_p(x_p), v_p(y_p))},$$

where v_p denotes the p-adic valuation.

Theorem 3.1. $\gcd(F_a, F_b) = F_{\gcd(a,b)}$ for profinite a and b.

To prove this, we will take the fact that this theorem holds in the integers for granted.

To start off, since $\hat{\mathbb{Z}} \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \cdots$, it suffices to show that $v_p(\gcd(F_a, F_b)) = v_p(F_{\gcd(a,b)})$ for every prime p, or equivalently $\min(v_p(F_a), v_p(F_b)) = v_p(F_{\gcd(a,b)})$.

Let $m(p)$ be the minimum value such that $p \mid F_{m(p)}$. Since $\gcd(F_a, F_b) = F_{\gcd(a,b)}$, we get that $\gcd(F_{m(p)}, F_b) = F_{\gcd(m(p),b)}$. We will now prove a lemma:

Lemma 3.2. p divides F_b if and only if $m(p)$ divides b. If p divides F_b, then $\gcd(F_{m(p)}, F_b)$ would be a multiple of p, so $F_{\gcd(m(p),b)}$ would need to be a multiple of p. Since $\gcd(m(p), b) \leq m(p), b$, and $m(p)$ is the smallest value such that $F_{m(p)}$ is a multiple of p, then $\gcd(m(p), b) = m(p)$, so b is a multiple of $m(p)$. In addition, if $m(p)$ divides b, then $\gcd(F_{m(p)}, F_b) = F_{m(p)}$, and since $F_{m(p)}$ is a multiple of p, so must F_b. Therefore, we have proven the statement.

The last identity we will be using is the Theorem of p-adic valuation of Fibonacci numbers, which states that $v_p(F_x) = v_p(x) + (v_p(F_{m(p)}) - v_p(m(p)))$ [Lengyel, 1995] when $p \neq 2, 5$. Since the concept of v_p is the same for profinite integers, this identity holds in $\hat{\mathbb{Z}}$.

Now, we will complete the proof. Let's split our proof into 4 cases.

Case 1: a and b are not both multiples of $m(p)$.

In this case, either $v_p(F_a)$ or $v_p(F_b)$ is 0, since by Lemma 3.2, if x isn't a multiple of $m(p)$, then F_x can't be a multiple of p. This means that $v_p(\gcd(F_a, F_b)) = 0$, since at least one of F_a, F_b isn't divisible by p. In addition, since at least one of a and b isn't a multiple of $m(p)$, then $\gcd(a, b)$ isn't a multiple of $m(p)$, so $F_{\gcd(a,b)}$ is not a multiple of p, meaning $v_p(F_{\gcd(a,b)}) = 0$. Therefore, if at least one of a and b isn't a multiple of $m(p)$, our identity holds.

Case 2: a and b are both multiples of $m(p)$, and $p \neq 2, 5$. In this case, we can use the theorem of p-adic valuation, which states $v_p(F_x) = v_p(x) + (v_p(F_{m(p)}) - v_p(m(p)))$. Then, $v_p(\gcd(F_a, F_b)) = \min(v_p(a) + (v_p(F_{m(p)}) - v_p(m(p))), v_p(b) + (v_p(F_{m(p)}) - v_p(m(p)))) = \min(v_p(a), v_p(b)) + v_p(F_{m(p)}) - v_p(m(p))$. In addition, $v_p(F_{\gcd(a,b)}) = v_p(\gcd(a, b)) + (v_p(F_{m(p)}) - v_p(m(p))) = \min(v_p(a), v_p(b)) + (v_p(F_{m(p)}) - v_p(m(p)))$. Therefore, $v_p(\gcd(F_a, F_b)) = v_p(F_{\gcd(a,b)})$.

Case 3: $p = 5$. Since $v_5(F_n) = v_5(n)$ for all n, $v_5(\gcd(F_a, F_b)) = \min(v_5(F_a), v_5(F_b)) = \min(v_5(a), v_5(b)) = v_5(\gcd(a, b)) = v_5(F_{\gcd(a,b)})$.

Case 4: $p = 2$. For all x, we know that $v_2(F_x) = 0$ if $x \equiv 1, 2 \pmod 3$, that $v_2(F_x) = 1$ if $x \equiv 3 \pmod 6$, that $v_2(F_x) = 3$ if $x \equiv 6 \pmod{12}$, and $v_2(F_x) = v_2(x) + 2$ if $x \equiv 0 \pmod{12}$. Now, in order to prove our identity that $\gcd(F_a, F_b) = F_{\gcd(a,b)}$, we can define a function $d(x)$, such that $d(x) = 0$ if $x \not\equiv 0 \pmod 3$, $d(x) = 1$ if $x \equiv 3 \pmod 6$, $d(x) = 2$ if $x \equiv 6 \pmod{12}$, and $d(x) = 3$ if $x \equiv 0 \pmod{12}$. Note that since $3 \mid 6 \mid 12$, $d(\gcd(x, y)) = \min(d(x), d(y))$. Now, if $d(a) \leq 2$ or $d(b) \leq 2$, then $v_2(F_x)$ is determined entirely by $d(x)$, so $v_2(\gcd(F_a, F_b)) = v_2(F_{\gcd(a,b)})$. To finish the proof, we just need to prove that $v_2(\gcd(F_a, F_b)) = v_2(F_{\gcd(a,b)})$ for a and b that are multiples of 12.

If a and b are both multiples of 12, then let $v_2(a) = x$ and $v_2(b) = y$. Then, $v_2(\gcd(F_a, F_b)) = \min(x + 2, y + 2) = \min(x, y) + 2$. In addition, $v_2(F_{\gcd(a,b)}) = \min(x, y) + 2$, since $\gcd(a, b)$ would still be a multiple of 12, and its power of 2 is $\min(x, y)$. Therefore, $v_2(\gcd(F_a, F_b)) = v_2(F_{\gcd(a,b)})$ for all a, b.

Therefore, since $v_p(\gcd(F_a, F_b)) = v_p(F_{\gcd(a,b)})$ for all primes p, $\gcd(F_a, F_b) = F_{\gcd(a,b)}$.

4 $\mathbb{Z}$ and $\hat{\mathbb{Z}}$

Theorem 4.1. The mapping from $\mathbb{Z}$ to $\hat{\mathbb{Z}}$ is injective.

To do this, we must prove that each integer can be written as a profinite integer.

We will prove this by showing that $\mathbb{Z}$ is completely covered by the profinite integers, by induction. More specifically, we will prove that the truncated profinite integer $(a_1, a_2, \cdots a_{k-1})$ can take any value from 0 to $k! - 1$, proving that it covers $\mathbb{Z}_{\geq 0}$, and then we will use this result to prove it also covers all the negative numbers.

First, our base case is simple, since $(a_1) = a_1$ can be either 0 or $1 = 2! - 1$. Now, if the truncated profinite integer $(a_1, a_2, \cdots a_{k-1})$ can be any integer from 0 to $k! - 1$, then the integer $(a_1, a_2, \cdots a_k) = a_k \cdot k! + (a_1, a_2, \cdots a_{k-1})$ can take any value in $[0, k! - 1] \cup [k!, 2 \cdot k! - 1] \cup \cdots \cup [k \cdot k!, (k+1) \cdot k! - 1]$, so it can take any value from 0 to $(k+1) \cdot k! - 1 = (k+1)! - 1$. Therefore, $(a_1, a_2, \cdots a_k)$ can take any value from 0 to $(k+1)! - 1$, and we have proven our inductive step, meaning our proof is finished.

Since $(a_1, a_2, \cdots a_k)$ can take any value from 0 to $k! - 1$, any profinite integer $(a_1, a_2, \cdots)$ can take any value ≥ 0. In addition, since $-1 = (1, 2, 3, \cdots)$, we can write $-(a_1, a_2, \cdots)$ as $(1 - a_1, 2 - a_2, 3 - a_3, \cdots) + 1$, meaning that each negative integer can be written as a profinite integer.

Therefore, each integer can be expressed as a profinite integer, so the mapping from $\mathbb{Z} \to \hat{\mathbb{Z}}$ is injective.

Theorem 4.2. No two distinct profinite integers map to the same integer.

To prove that no two distinct profinite integers can map to the same integer, we will assume for the sake of contradiction that $(a_1, a_2, \cdots)$ and $(b_1, b_2, \cdots)$ map to the same integer. We will prove that the first n terms of these profinite integers must be the same, and we will induct on n. Since the sum of the terms after a_1 and b_1 will be divisible by 2, we get that $a_1 \equiv b_1 \pmod 2$, and since $a_1, b_1 \in \{0, 1\}$, $a_1 = b_1$, so our base case is proven. Now, assume that $a_1 = b_1, a_2 = b_2, \cdots, a_{k-1} = b_{k-1}$. We know that $(a_1, a_2, \cdots a_k) \equiv (b_1, b_2, \cdots b_k) \pmod{(k+1)!}$, since each subsequent term is divisible by $(k+1)!$. Since $(a_1, a_2, \cdots a_{k-1}) = (b_1, b_2, \cdots b_{k-1})$, meaning that

$(a_1, a_2, \cdots a_{k-1}) \equiv (b_1, b_2, \cdots b_{k-1}) \pmod{(k+1)!}$,

and

$(a_1, a_2, \cdots a_k) \equiv (b_1, b_2, \cdots b_k) \pmod{(k+1)!}$,

then

$$(a_1, a_2, \cdots a_k) - (a_1, a_2, \cdots a_{k-1}) \equiv (b_1, b_2, \cdots b_k) - (b_1, b_2, \cdots b_{k-1}) \pmod{(k+1)!},$$

or

$$a_k \cdot k! \equiv b_k \cdot k! \pmod{(k+1)!}.$$

Since $0 \leq a_k \leq k$ and $a_k \equiv b_k \pmod{k+1}$, we get that $a_k = b_k$, proving our inductive step. Therefore, no two distinct profinite integers map to the same integer.