Profinite Fibonacci numbers

H. W. Lenstra, Jr.

Department of Mathematics
University of California
Berkeley, CA 94720
U. S. A.

Abstract. In this paper profinite integers and profinite Fibonacci numbers are described, and some of their properties are discussed. In particular, profinite integers s are considered that are equal to the sth Fibonacci number. There are precisely eleven such s.

Key words: Fibonacci numbers, profinite integers.

1980 Mathematics subject classification (1985): 11B39.

Acknowledgment. The author would like to thank the Institute for Advanced Study in Princeton for providing hospitality and support while this paper was being written. He was supported by NSF under Grant No. DMS 90-02939, and by NSA/MSP under Grant No. MDA90-H-4043.

The nth Fibonacci number is, for $n \geq 0$, inductively defined by $F_0 = 0$, $F_1 = 1$ and

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

for $n > 1$. It is well known that the definition can be extended to negative n by $F_n = (-1)^{n-1} F_{-n}$, and that many familiar identities, such as (1) and

$$F_n F_{m+1} - F_{n+1} F_m = (-1)^m \cdot F_{n-m}, \tag{2}$$

then hold for *all* integers n and m.

The definition of F_n can be extended to an even larger class of numbers, the *profinite integers*. To define profinite integers, recall that any positive integer n has a unique representation as

$$n = c_k \cdot k! + c_{k-1} \cdot (k-1)! + \ldots + c_2 \cdot 2! + c_1 \cdot 1!,$$

where the "digits" c_i are integers satisfying $c_k \neq 0$ and $0 \leq c_i \leq i$, for $1 \leq i \leq k$. In the *factorial number system*, the number n is then written as

$$n = (c_k c_{k-1} \ldots c_2 c_1)_!. \tag{3}$$

The exclamation mark distinguishes this representation from the decimal representation. For example, we have $5 = (21)_!$ and $25 = (1001)_!$.

If we allow the sequence of digits to extend indefinitely to the left, then we obtain a *profinite integer*:

$$(\ldots c_5 c_4 c_3 c_2 c_1)_!,$$

where we still require that $0 \leq c_i \leq i$ for each i. Usually, only a few of the digits are specified, depending on the accuracy that is required. In this paper, most profinite numbers are given to an accuracy of 24 digits. For example, we shall encounter the following profinite integer:

$$l = (\ldots {}^{1}{}_{6}04{}^{1}{}_{6}{}^{1}{}_{3}{}^{1}{}_{8}{}^{1}{}_{0}4768{}^{1}{}_{0}{}^{1}{}_{0}49000120100)_!. \tag{4}$$

In this number, the 19th digit has the value 18, but this is written ${}^{1}{}_{8}$ in order to make clear that it is a single digit. Note that by the 19th digit we mean the 19th digit *from behind*. Likewise, when we speak about the "first" digits or the "initial" digits of a profinite number, we always start counting from the right.

Each positive integer n as in (3) can be viewed as a profinite integer, by taking $c_i = 0$ for $i > k$. Also 0 is a profinite integer, with *all* digits equal to 0. The *negative* integers can be viewed as profinite integers as well, for example

$$-1 = (\ldots {}^{2}{}_{4}{}^{2}{}_{3}{}^{2}{}_{2}{}^{2}{}_{1}{}^{2}{}_{0}{}^{1}{}_{9}{}^{1}{}_{8}{}^{1}{}_{7}{}^{1}{}_{6}{}^{1}{}_{5}{}^{1}{}_{4}{}^{1}{}_{3}{}^{1}{}_{2}{}^{1}{}_{1}{}^{1}{}_{0}987654321)_!,$$

with $c_i = i$ for all i. In general, negative integers are characterized by the property that $c_i = i$ for all but finitely many i.

The ordinary arithmetic operations can be performed on profinite integers. To add two profinite integers, one adds them digitwise, proceeding from the right; when the sum of the ith digits is found to exceed i, one subtracts $i + 1$ from it and adds a carry of 1 to the sum of the $i + 1$st digits. The reader can check that in this way one finds that $1 + (-1) = 0$. Subtraction is performed in a similar manner. Multiplication can be done by means of a more elaborate scheme, but it is often more practical to compute products using the following rule: for each k, the first k digits of the product of two profinite numbers s

and t depend only on the first k digits of s and of t. (This rule is also valid for addition and subtraction.) Using this rule, one reduces the problem of computing products to the case of ordinary positive integers.

These operations make the set of all profinite integers into a commutative ring with unit element 1. This ring is denoted $\hat{\mathbf{Z}}$, the *ring of profinite integers*.

For each profinite integer s, one can in a natural way define the sth Fibonacci number F_s, which is itself a profinite integer. Namely, given s, one can choose a sequence of positive integers n_1, n_2, n_3, … that have more and more initial digits in common with s, so that it may be said that n_i *converges* to s for $i \to \infty$. Then also the numbers F_{n_1}, F_{n_2}, F_{n_3}, … get more and more initial digits in common, and we define F_s to be their "limit" as $i \to \infty$. This does not depend on the choice of the sequence of numbers n_i.

For example, we can write $s = -1$ as the limit of the numbers $n_1 = (21)_! = 5$, $n_2 = (321)_! = 23$, $n_3 = (4321)_! = 119$, $n_4 = (54321)_! = 719$, …, so that F_{-1} is the limit of

$$\begin{aligned}
F_5 &= 5 = (21)_!,\\
F_{23} &= 28657 = (5444001)_!,\\
F_{119} &= 3311648143516982017180081\\
&= (5826{}^1_4{}^1_1 8{}^1_0{}^1_5{}^1_3 23418173200001)_!,\\
F_{719} &= (\ldots 3{}^1_6{}^1_6 98{}^1_6{}^1_2 51{}^1_1{}^1_4 3{}^1_1 49806000001)_!,\\
&\ldots,
\end{aligned}$$

which is consistent with the true value $F_{-1} = 1 = (\ldots 000001)_!$.

For each $k \geq 3$ the first k digits of F_s are determined by the first k digits of s. This rule makes it possible to compute profinite Fibonacci numbers, as we shall see below.

Many identities such as (1) and (2) are also valid for profinite Fibonacci numbers. In order to give a meaning to the sign that appears in (2), we call a profinite integer s *even* or *odd* depending on whether its first digit c_1 is even or odd, and we define $(-1)^s = 1$ or -1 accordingly. More generally, one defines a profinite integer s to be *divisible* by a positive integer b if the factorial number formed by the first $b-1$ digits of s is divisible by b. For many b, it suffices to look at far fewer than $b-1$ digits. For example, if k is a non-negative integer, then a profinite integer is divisible by $k!$ if and only if its $k-1$ initial digits are zero. Two profinite numbers s_1 and s_2 are called *congruent* modulo a positive integer b if their difference is divisible by b, notation: $s_1 \equiv s_2 \bmod b$.

The following method can be used to compute profinite Fibonacci numbers. Let s be a profinite number, and suppose that one wishes to compute the sth Fibonacci number F_s to an accuracy of k digits, for some $k \geq 3$. Then one first truncates s to k digits, which gives a non-negative integer n that is usually very large. By the rule mentioned above, F_s and F_n have at least k initial digits in common, so it suffices to calculate F_n to a precision of k digits. To this end, let ϑ be a symbol that satisfies the rule $\vartheta^2 = \vartheta + 1$. Then it is well known that $\vartheta^n = F_n\vartheta + F_{n-1}$. The left hand side can be quickly calculated by induction, even for very large n, if one uses that $\vartheta^{2m} = (\vartheta^m)^2$ and $\vartheta^{2m+1} = \vartheta^{2m} \cdot \vartheta$. All intermediate results are expressed in the form $a\vartheta + b$, where a and b are integers that are only computed to a precision of k digits in the factorial number system. Then in the end one knows F_n to a precision of k digits as well, as required.

The *Lucas numbers* L_n, which are defined by $L_0 = 2$, $L_1 = 1$, $L_n = L_{n-1} + L_{n-2}$ $(n > 1)$, can be generalized to profinite numbers in a completely similar manner. They can be expressed in Fibonacci numbers by $L_s = F_{s+1} + F_{s-1}$. It is also true that $F_sL_s = F_{2s}$ for all $s \in \hat{\mathbf{Z}}$; however, it is not necessarily meaningful to write $L_s = F_{2s}/F_s$, since division is not always possible in $\hat{\mathbf{Z}}$.

One of the interesting properties of profinite Fibonacci numbers is that they have *power series* expansions. If $s_0 \in \hat{\mathbf{Z}}$, then the power series expansion for F_s around s_0 takes the shape

$$\begin{aligned} F_s &= F_{s_0} + lL_{s_0}(s-s_0) + 5l^2F_{s_0}\frac{(s-s_0)^2}{2!} \\ &\qquad + 5l^3L_{s_0}\frac{(s-s_0)^3}{3!} + 5^2l^4F_{s_0}\frac{(s-s_0)^4}{4!} + \dots \\ &= \sum_{i=0}^{\infty}\Big(5^il^{2i}F_{s_0}\frac{(s-s_0)^{2i}}{(2i)!} + 5^il^{2i+1}L_{s_0}\frac{(s-s_0)^{2i+1}}{(2i+1)!}\Big), \end{aligned} \tag{5}$$

where l is a certain profinite integer that is given by (4). The number l is divisible by all prime numbers except 5. From this it follows that 5^il^{2i} and 5^il^{2i+1} are divisible by $(2i)!$ and $(2i+1)!$, respectively, so that the coefficients in the power series expansions are profinite integers.

No prime number p is known for which l is divisible by p^2. In fact, if p is a prime number, then the number of factors p in l is the same as the number of factors p in $F_{p-1}F_{p+1}$, and no prime number is known for which $F_{p-1}F_{p+1}$ is divisible by p^2. One may, however, conjecture that there exist infinitely many such primes.

An informal derivation of (5) can be given as follows. Let again ϑ be such that $\vartheta^2 = \vartheta + 1$, and put $\vartheta' = 1 - \vartheta$. It is well known that $F_n = (\vartheta^n - \vartheta'^n)/(\vartheta - \vartheta')$ and $L_n = \vartheta^n + \vartheta'^n$ for all integers n. This suggests that one also has $F_s = (\vartheta^s - \vartheta'^s)/(\vartheta - \vartheta')$ and $L_s = \vartheta^s + \vartheta'^s$ for all $s \in \hat{\mathbf{Z}}$, with a suitable interpretation of the powering operation. Now consider the Taylor series for F_s around s_0:

$$F_s = \sum_{j=0}^{\infty} F_{s_0}^{(j)} \frac{(s - s_0)^j}{j!},$$

where $F_s^{(j)} = \frac{d^j F_s}{ds^j}$ denotes the jth derivative. To calculate these higher derivatives, one first notes that from $\vartheta\vartheta' = -1$ it follows that

$$2(\log\vartheta + \log\vartheta') = 2\log(-1) = \log 1 = 0,$$

and therefore $\log\vartheta = -\log\vartheta'$. This leads to

$$\frac{dF_s}{ds} = \frac{d}{ds}\frac{\vartheta^s - \vartheta'^s}{\vartheta - \vartheta'} = \frac{\log\vartheta}{\vartheta - \vartheta'}\bigl(\vartheta^s + \vartheta'^s\bigr) = \frac{\log\vartheta}{\vartheta - \vartheta'}L_s,$$
$$\frac{dL_s}{ds} = \log\vartheta \cdot \bigl(\vartheta^s - \vartheta'^s\bigr) = \log\vartheta \cdot (\vartheta - \vartheta') \cdot F_s.$$

Combining this with $(\vartheta - \vartheta')^2 = 5$, one finds that

$$F_s^{(2i)} = 5^i l^{2i} F_s, \qquad F_s^{(2i+1)} = 5^i l^{2i+1} L_s$$

for each $i \geq 0$, where

$$l = \frac{\log\vartheta}{\vartheta - \vartheta'}. \tag{6}$$

This leads immediately to (5).

Making this informal argument rigorous involves, among other things, the development of an appropriate theory of logarithms, which I do not do here. In the end one finds that the precise meaning of (5) is a little more subtle than one might have expected. Namely, (5) means that for each positive integer b, the following is true for every profinite integer s that has enough initial digits in common with s_0: if k is any positive integer, then all but finitely many terms of the infinite sum are divisible by b^k, and the sum of the remaining terms is congruent to F_s modulo b^k. For example, if b divides $5! = 120$ then it suffices that s has three initial digits in common with s_0, and if b divides 36! six.

The power series development can be used to determine l to any desired number of digits. Namely, put $s_0 = 0$, so that $F_{s_0} = 0$ and $L_{s_0} = 2$. Then the power series development reads

$$F_s = 2ls + \frac{2{\cdot}5{\cdot}l^3{\cdot}s^3}{3!} + \frac{2{\cdot}5^2{\cdot}l^5{\cdot}s^5}{5!} + \dots . \tag{7}$$

Suppose that one wishes to determine the first 35 digits of l, or, equivalently, the residue class of l modulo 36!. Modulo any power of 36!, the expansion is valid for profinite numbers s of which the first six digits are zero. Choose

$$s = 2^{16} \cdot 3^8 \cdot 5^4 \cdot 7 = (168133000000000)_!.$$

Using that l is divisible by all prime numbers except 5, one easily sees that in (7) each term on the right beyond the first term is divisible by $2s \cdot 36!$. Calculating F_s modulo $2s \cdot 36!$ by means of the technique explained earlier, and dividing by $2s$, one finds l modulo 36!:

$$l = (\dots {}^{2}_{6}{}^{3}_{3}51{}^{1}_{3}{}^{1}_{7}{}^{1}_{1}{}^{2}_{3}471{}^{1}_{6}04{}^{1}_{6}{}^{1}_{3}{}^{1}_{8}{}^{1}_{0}4768{}^{1}_{0}{}^{1}_{0}49000120100)_!.$$

One can also compute l directly from (6), but this is significantly more laborious, since the logarithm has a rather circuitous definition.

The power series expansion also comes in when one wishes to determine the *fixed points* of the Fibonacci sequence, i. e. the numbers s for which $F_s = s$. It is very easy to see that among the ordinary integers the only examples are $F_0 = 0$, $F_1 = 1$, $F_5 = 5$. Using the power series, one can show that in $\hat{\mathbf{Z}}$ there are exactly eight additional fixed points, namely the following profinite numbers:

$$z_{1,-5} = (\ldots 7{}^{1}_{1}548{}^{1}_{6}{}^{1}_{7}86{}^{1}_{0}65657871411001)_{!},$$

$$z_{1,-1} = (\ldots {}^{1}_{8}{}^{2}_{1}300813{}^{1}_{5}180733953122001)_{!},$$

$$z_{1,0} = (\ldots {}^{1}_{3}{}^{1}_{6}507{}^{1}_{6}{}^{1}_{4}7{}^{1}_{1}68{}^{1}_{1}133471411001)_{!},$$

$$z_{1,5} = (\ldots {}^{1}_{9}{}^{2}_{1}4{}^{1}_{8}6{}^{1}_{6}{}^{1}_{1}6{}^{1}_{6}2{}^{1}_{1}290{}^{1}_{0}071411001)_{!},$$

$$z_{5,-5} = (\ldots {}^{1}_{2}{}^{1}_{4}08206177{}^{1}_{0}2{}^{1}_{0}48800000021)_{!},$$

$$z_{5,-1} = (\ldots {}^{2}_{3}{}^{2}_{3}{}^{2}_{1}3{}^{1}_{4}{}^{1}_{1}8{}^{1}_{4}{}^{1}_{5}{}^{1}_{4}{}^{1}_{1}{}^{1}_{1}{}^{1}_{1}24871411021)_{!},$$

$$z_{5,0} = (\ldots {}^{1}_{8}{}^{1}_{9}041030{}^{1}_{2}3{}^{1}_{2}8524400000021)_{!},$$

$$z_{5,1} = (\ldots 52{}^{1}_{8}3{}^{1}_{4}37{}^{1}_{1}0{}^{1}_{3}3{}^{1}_{1}3{}^{1}_{1}0916244021)_{!}.$$

The notation $z_{a,b}$, for $a \in \{1,\ 5\}$, $b \in \{-5,\ -1,\ 0,\ 1,\ 5\}$ is chosen because we have

$$z_{a,b} \equiv a \bmod 6^k, \qquad z_{a,b} \equiv b \bmod 5^k$$

for all positive integers k; this uniquely determines $z_{a,b}$ as a fixed point of the Fibonacci sequence. (For $a = b \in \{1,\ 5\}$ one may take $z_{a,b} = a$.)

The eight fixed points $z_{a,b}$ have, imprecisely speaking, the tendency to approximately inherit properties of a, b. For example, each of $a = 1$ and $b = 0$ is equal to its own square, and, correspondingly, $z_{1,0}$ is quite close to its own square, in the sense that the nine initial digits are the same:

$$z_{1,0}^2 = (\ldots {}^{1}_{3}66{}^{2}_{0}407953{}^{1}_{0}2255471411001)_{!}.$$

Each of $a = 1$, $b = -1$ has square equal to 1, and this is almost true for $z_{1,-1}$:

$$z_{1,-1}^2 = (\ldots {}^{2}_{2}{}^{1}_{7}{}^{1}_{0}{}^{1}_{0}00000000000000000001)_{!}.$$

Looking at $z_{1,5}$ and $z_{5,1}$ one sees that for each i with $4 < i \leq 24$ their ith digits add up to i. This is due to the remarkable relation

$$z_{1,5} + z_{5,1} = (\ldots 000000000000000000000100)_{!},$$

which reflects that $5 + 1 = 6 = (100)_{!}$. Likewise, $5 \cdot 1 = 5 = (21)_{!}$ is reflected in

$$z_{1,5} \cdot z_{5,1} = (\ldots 000000000000000000000021)_{!}.$$

However, if one uses greater precision then one finds that $z_{1,5} + z_{5,1} \neq 6$ and $z_{1,5} \cdot z_{5,1} \neq 5$:

$$\begin{aligned}
z_{1,5} &= (\ldots 2\,{}^{2}{}_{9}\,{}^{2}{}_{6}\,{}^{2}{}_{6}\,{}^{2}{}_{4}\,{}^{1}{}_{6}\,3\,{}^{1}{}_{9}\,{}^{2}{}_{1}\,4\,{}^{1}{}_{8}\,6\,{}^{1}{}_{6}\,{}^{1}{}_{1}\,6\,{}^{1}{}_{6}\,2\,{}^{1}{}_{1}\,290\,{}^{1}{}_{0}\,071411001)_{!},\\
z_{5,1} &= (\ldots 26323\,{}^{1}{}_{0}\,{}^{2}{}_{2}\,52\,{}^{1}{}_{8}\,3\,{}^{1}{}_{4}\,37\,{}^{1}{}_{1}\,0\,{}^{1}{}_{3}\,3\,{}^{1}{}_{1}\,3\,{}^{1}{}_{1}\,0916244021)_{!},\\
z_{1,5} + z_{5,1} &= (\ldots 5500000000000000000000000000100)_{!},\\
z_{1,5} \cdot z_{5,1} &= (\ldots {}^{2}{}_{5}\,{}^{2}{}_{5}\,00000000000000000000000000021)_{!}.
\end{aligned}$$

The number $z_{5,-5}$ has the most astonishing property of all. One would expect that its square is close to $5^2 = (-5)^2 = 25$, and indeed $z_{5,-5}^2$ does not differ from $25 = (1001)_{!}$ until the *four hundredth* digit:

$$z_{5,-5}^2 - 25 = (\ldots {}^{3}{\scriptstyle 8}{}_{6}\,{}^{3}{\scriptstyle 3}{}_{1}\,{}^{1}{\scriptstyle 8}{}_{5}\,{}^{3}{\scriptstyle 7}{}_{0}\,{}^{3}{\scriptstyle 7}{}_{0}\,00000000 \ldots 00000000)_{!},$$

with 399 initial zeros!

There are several techniques that can be used to calculate the profinite numbers $z_{a,b}$ to any required precision. The first is to start from any number x_0 that satisfies $x_0 \equiv a \bmod 24$, $x_0 \equiv b \bmod 5^k$, where k is at least one quarter of the required number of digits, and $k \geq 2$, and next to apply the iteration $x_{i+1} = F_{x_i}$. This converges to $z_{a,b}$ in the required precision, but the convergence is not very fast. This method can be accelerated by starting from a value x_0 for which $x_0 - a$ has more factors 2 and 3. The second method is to apply a Newton iteration to find a zero of the function $F_s - s$:

$$x_{i+1} = x_i - \frac{F_{x_i} - x_i}{lL_{x_i} - 1}.$$

This requires some care with the division that is involved, and one needs to know l to the same precision. However, it converges much faster, even if the starting value x_0 only satisfies $x_0 \equiv a \bmod 24$, $x_0 \equiv b \bmod 25$.

If one investigates in a similar manner the fixed points of the Lucas sequence, one finds that there are exactly three of them, namely 1, -1, and a profinite integer that is divisible by infinitely many factors 3.

Further experimentation is left to the reader, who may also enjoy finding rigorous formulations and proofs of the statements made in this paper. The bibliography below lists two books that are useful in this context. Mahler's book develops the theory of g-adic and p-adic numbers, which are closely related to profinite numbers. In the book by Cassels one can find a treatment of power series and logarithms that are similar to the power series and logarithms considered above. Cassels' book also contains numerous applications to number theory.

Bibliography.

1. J. W. S. Cassels, *Local fields*, Cambridge University Press, Cambridge, 1986.
2. K. Mahler, *Introduction to p-adic numbers and their functions*, Cambridge University Press, Cambridge, 1973; second edition, 1981.