FORMALIZED MATHEMATICS
Volume 12, Number **3**, 2004
University of Białystok

Some Properties of Fibonacci Numbers

Magdalena Jastrzębska
University of Białystok

Adam Grabowski[1]
University of Białystok

Summary. We formalized some basic properties of the Fibonacci numbers using definitions and lemmas from [7] and [23], e.g. Cassini's and Catalan's identities. We also showed the connections between Fibonacci numbers and Pythagorean triples as defined in [31]. The main result of this article is a proof of Carmichael's Theorem on prime divisors of prime-generated Fibonacci numbers. According to it, if we look at the prime factors of a Fibonacci number generated by a prime number, none of them have appeared as a factor in any earlier Fibonacci number. We plan to develop the full proof of the Carmichael Theorem following [33].

MML Identifier: `FIB_NUM2`.

The papers [26], [3], [4], [30], [24], [1], [28], [29], [2], [18], [13], [27], [32], [9], [10], [7], [12], [8], [17], [21], [19], [22], [25], [6], [20], [11], [23], [15], [31], [14], [16], and [5] provide the terminology and notation for this paper.

1. Preliminaries

In this paper n, k, r, m, i, j denote natural numbers.

We now state a number of propositions:

(1) For every non empty natural number n holds $(n -' 1) + 2 = n + 1$.

(2) For every odd integer n and for every non empty real number m holds $(-m)^n = -m^n$.

(3) For every odd integer n holds $(-1)^n = -1$.

(4) For every even integer n and for every non empty real number m holds $(-m)^n = m^n$.

[1]This work has been partially supported by the CALCULEMUS grant HPRN-CT-2000-00102.

ISSN 1426–2630

(5) For every even integer n holds $(-1)^n = 1$.

(6) For every non empty real number m and for every integer n holds $((-1) \cdot m)^n = (-1)^n \cdot m^n$.

(7) For every non empty real number a holds $a^{k+m} = a^k \cdot a^m$.

(8) For every non empty real number k and for every odd integer m holds $(k^m)^n = k^{m \cdot n}$.

(9) $((-1)^{-n})^{\mathbf{2}} = 1$.

(10) For every non empty real number a holds $a^{-k} \cdot a^{-m} = a^{-k-m}$.

(11) $(-1)^{-2 \cdot n} = 1$.

(12) For every non empty real number a holds $a^k \cdot a^{-k} = 1$.

Let n be an odd integer. One can verify that $-n$ is odd.

Let n be an even integer. Note that $-n$ is even.

One can prove the following two propositions:

(13) $(-1)^{-n} = (-1)^n$.

(14) For all natural numbers k, m, m_1, n_1 such that $k \mid m$ and $k \mid n$ holds $k \mid m \cdot m_1 + n \cdot n_1$.

One can check that there exists a set which is finite, non empty, and natural-membered and has non empty elements.

Let f be a function from $\mathbb{N}$ into $\mathbb{N}$ and let A be a finite natural-membered set with non empty elements. Note that $f \restriction A$ is finite subsequence-like.

One can prove the following proposition

(15) For every finite subsequence p holds $\operatorname{rng} \operatorname{Seq} p \subseteq \operatorname{rng} p$.

Let f be a function from $\mathbb{N}$ into $\mathbb{N}$ and let A be a finite natural-membered set with non empty elements. The functor $\operatorname{Prefix}(f, A)$ yields a finite sequence of elements of $\mathbb{N}$ and is defined as follows:

(Def. 1) $\operatorname{Prefix}(f, A) = \operatorname{Seq}(f \restriction A)$.

The following proposition is true

(16) For every natural number k such that $k \neq 0$ holds if $k + m \leqslant n$, then $m < n$.

Let us mention that $\mathbb{N}$ is lower bounded.

Let us mention that $\{1, 2, 3\}$ is natural-membered and has non empty elements.

Let us note that $\{1, 2, 3, 4\}$ is natural-membered and has non empty elements.

The following propositions are true:

(17) For all sets x, y such that $0 < i$ and $i < j$ holds $\{\langle i, x \rangle, \langle j, y \rangle\}$ is a finite subsequence.

(18) For all sets x, y and for every finite subsequence q such that $i < j$ and $q = \{\langle i, x \rangle, \langle j, y \rangle\}$ holds $\operatorname{Seq} q = \langle x, y \rangle$.

Let n be a natural number. Observe that $\mathrm{Seg}\, n$ has non empty elements.

Let A be a set with non empty elements. Note that every subset of A has non empty elements.

Let A be a set with non empty elements and let B be a set. Observe that $A \cap B$ has non empty elements and $B \cap A$ has non empty elements.

We now state four propositions:

(19) For every natural number k and for every set a such that $k \geqslant 1$ holds $\{\langle k, a \rangle\}$ is a finite subsequence.

(20) Let i, k be natural numbers, y be a set, and f be a finite subsequence. If $f = \{\langle 1, y \rangle\}$, then $\mathrm{Shift}^i\, f = \{\langle 1 + i, y \rangle\}$.

(21) Let q be a finite subsequence and k, n be natural numbers. Suppose $\mathrm{dom}\, q \subseteq \mathrm{Seg}\, k$ and $n > k$. Then there exists a finite sequence p such that $q \subseteq p$ and $\mathrm{dom}\, p = \mathrm{Seg}\, n$.

(22) For every finite subsequence q there exists a finite sequence p such that $q \subseteq p$.

2. Fibonacci Numbers

In this article we present several logical schemes. The scheme *Fib Ind 1* concerns a unary predicate $\mathcal{P}$, and states that:

For every non empty natural number k holds $\mathcal{P}[k]$

provided the parameters have the following properties:

- $\mathcal{P}[1]$,
- $\mathcal{P}[2]$, and
- For every non empty natural number k such that $\mathcal{P}[k]$ and $\mathcal{P}[k+1]$ holds $\mathcal{P}[k+2]$.

The scheme *Fib Ind 2* concerns a unary predicate $\mathcal{P}$, and states that:

For every non trivial natural number k holds $\mathcal{P}[k]$

provided the parameters meet the following conditions:

- $\mathcal{P}[2]$,
- $\mathcal{P}[3]$, and
- For every non trivial natural number k such that $\mathcal{P}[k]$ and $\mathcal{P}[k+1]$ holds $\mathcal{P}[k+2]$.

Next we state a number of propositions:

(23) $\mathrm{Fib}(2) = 1$.

(24) $\mathrm{Fib}(3) = 2$.

(25) $\mathrm{Fib}(4) = 3$.

(26) $\mathrm{Fib}(n + 2) = \mathrm{Fib}(n) + \mathrm{Fib}(n + 1)$.

(27) $\mathrm{Fib}(n + 3) = \mathrm{Fib}(n + 2) + \mathrm{Fib}(n + 1)$.

(28) $\mathrm{Fib}(n + 4) = \mathrm{Fib}(n + 2) + \mathrm{Fib}(n + 3)$.

(29) $\mathrm{Fib}(n+5) = \mathrm{Fib}(n+3) + \mathrm{Fib}(n+4)$.

(30) $\mathrm{Fib}(n+2) = \mathrm{Fib}(n+3) - \mathrm{Fib}(n+1)$.

(31) $\mathrm{Fib}(n+1) = \mathrm{Fib}(n+2) - \mathrm{Fib}(n)$.

(32) $\mathrm{Fib}(n) = \mathrm{Fib}(n+2) - \mathrm{Fib}(n+1)$.

3. Cassini's and Catalan's Identities

The following propositions are true:

(33) $\mathrm{Fib}(n) \cdot \mathrm{Fib}(n+2) - \mathrm{Fib}(n+1)^{\mathbf{2}} = (-1)^{n+1}$.

(34) For every non empty natural number n holds $\mathrm{Fib}(n -' 1) \cdot \mathrm{Fib}(n+1) - \mathrm{Fib}(n)^{\mathbf{2}} = (-1)^n$.

(35) $\tau > 0$.

(36) $\overline{\tau} = (-\tau)^{-1}$.

(37) $(-\tau)^{(-1)\cdot n} = ((-\tau)^{-1})^n$.

(38) $-\frac{1}{\tau} = \overline{\tau}$.

(39) $((\tau^r)^{\mathbf{2}} - 2 \cdot (-1)^r) + (\tau^{-r})^{\mathbf{2}} = (\tau^r - \overline{\tau}^r)^{\mathbf{2}}$.

(40) For all non empty natural numbers n, r such that $r \leqslant n$ holds $\mathrm{Fib}(n)^{\mathbf{2}} - \mathrm{Fib}(n+r) \cdot \mathrm{Fib}(n -' r) = (-1)^{n -' r} \cdot \mathrm{Fib}(r)^{\mathbf{2}}$.

(41) $\mathrm{Fib}(n)^{\mathbf{2}} + \mathrm{Fib}(n+1)^{\mathbf{2}} = \mathrm{Fib}(2 \cdot n + 1)$.

(42) For every non empty natural number k holds $\mathrm{Fib}(n+k) = \mathrm{Fib}(k) \cdot \mathrm{Fib}(n+1) + \mathrm{Fib}(k -' 1) \cdot \mathrm{Fib}(n)$.

(43) For every non empty natural number n holds $\mathrm{Fib}(n) \mid \mathrm{Fib}(n \cdot k)$.

(44) For every non empty natural number k such that $k \mid n$ holds $\mathrm{Fib}(k) \mid \mathrm{Fib}(n)$.

(45) $\mathrm{Fib}(n) \leqslant \mathrm{Fib}(n+1)$.

(46) For every natural number n such that $n > 1$ holds $\mathrm{Fib}(n) < \mathrm{Fib}(n+1)$.

(47) For all natural numbers m, n such that $m \geqslant n$ holds $\mathrm{Fib}(m) \geqslant \mathrm{Fib}(n)$.

(48) For every natural number k such that $k > 1$ holds if $k < n$, then $\mathrm{Fib}(k) < \mathrm{Fib}(n)$.

(49) $\mathrm{Fib}(k) = 1$ iff $k = 1$ or $k = 2$.

(50) Let k, n be natural numbers. Suppose $n > 1$ and $k \neq 0$ and $k \neq 1$ and $k \neq 1$ and $n \neq 2$ or $k \neq 2$ and $n \neq 1$. Then $\mathrm{Fib}(k) = \mathrm{Fib}(n)$ if and only if $k = n$.

(51) Let n be a natural number. Suppose $n > 1$ and $n \neq 4$. Suppose n is non prime. Then there exists a non empty natural number k such that $k \neq 1$ and $k \neq 2$ and $k \neq n$ and $k \mid n$.

(52) For every natural number n such that $n > 1$ and $n \neq 4$ holds if $\mathrm{Fib}(n)$ is prime, then n is prime.

4. Sequence of Fibonacci Numbers

The function FIB from $\mathbb{N}$ into $\mathbb{N}$ is defined as follows:

(Def. 2) For every natural number k holds $\mathrm{FIB}(k) = \mathrm{Fib}(k)$.

The subset $\mathbb{N}_{\mathrm{even}}$ of $\mathbb{N}$ is defined by:

(Def. 3) $\mathbb{N}_{\mathrm{even}} = \{2 \cdot k : k$ ranges over natural numbers$\}$.

The subset $\mathbb{N}_{\mathrm{odd}}$ of $\mathbb{N}$ is defined as follows:

(Def. 4) $\mathbb{N}_{\mathrm{odd}} = \{2 \cdot k + 1 : k$ ranges over natural numbers$\}$.

One can prove the following two propositions:

(53) For every natural number k holds $2 \cdot k \in \mathbb{N}_{\mathrm{even}}$ and $2 \cdot k + 1 \notin \mathbb{N}_{\mathrm{even}}$.

(54) For every natural number k holds $2 \cdot k + 1 \in \mathbb{N}_{\mathrm{odd}}$ and $2 \cdot k \notin \mathbb{N}_{\mathrm{odd}}$.

Let n be a natural number. The functor $\mathrm{EvenFibs}(n)$ yielding a finite sequence of elements of $\mathbb{N}$ is defined by:

(Def. 5) $\mathrm{EvenFibs}(n) = \mathrm{Prefix}(\mathrm{FIB}, \mathbb{N}_{\mathrm{even}} \cap \mathrm{Seg}\, n)$.

The functor $\mathrm{OddFibs}(n)$ yields a finite sequence of elements of $\mathbb{N}$ and is defined by:

(Def. 6) $\mathrm{OddFibs}(n) = \mathrm{Prefix}(\mathrm{FIB}, \mathbb{N}_{\mathrm{odd}} \cap \mathrm{Seg}\, n)$.

We now state a number of propositions:

(55) $\mathrm{EvenFibs}(0) = \emptyset$.

(56) $\mathrm{Seq}(\mathrm{FIB} \restriction \{2\}) = \langle 1 \rangle$.

(57) $\mathrm{EvenFibs}(2) = \langle 1 \rangle$.

(58) $\mathrm{EvenFibs}(4) = \langle 1, 3 \rangle$.

(59) For every natural number k holds $\mathbb{N}_{\mathrm{even}} \cap \mathrm{Seg}(2 \cdot k + 2) \cup \{2 \cdot k + 4\} = \mathbb{N}_{\mathrm{even}} \cap \mathrm{Seg}(2 \cdot k + 4)$.

(60) For every natural number k holds $\mathrm{FIB} \restriction (\mathbb{N}_{\mathrm{even}} \cap \mathrm{Seg}(2 \cdot k + 2)) \cup \{\langle\!\langle 2 \cdot k + 4, \mathrm{FIB}(2 \cdot k + 4) \rangle\!\rangle\} = \mathrm{FIB} \restriction (\mathbb{N}_{\mathrm{even}} \cap \mathrm{Seg}(2 \cdot k + 4))$.

(61) For every natural number n holds $\mathrm{EvenFibs}(2 \cdot n + 2) = \mathrm{EvenFibs}(2 \cdot n) \frown \langle \mathrm{Fib}(2 \cdot n + 2) \rangle$.

(62) $\mathrm{OddFibs}(1) = \langle 1 \rangle$.

(63) $\mathrm{OddFibs}(3) = \langle 1, 2 \rangle$.

(64) For every natural number k holds $\mathbb{N}_{\mathrm{odd}} \cap \mathrm{Seg}(2 \cdot k + 3) \cup \{2 \cdot k + 5\} = \mathbb{N}_{\mathrm{odd}} \cap \mathrm{Seg}(2 \cdot k + 5)$.

(65) For every natural number k holds $\mathrm{FIB} \restriction (\mathbb{N}_{\mathrm{odd}} \cap \mathrm{Seg}(2 \cdot k + 3)) \cup \{\langle\!\langle 2 \cdot k + 5, \mathrm{FIB}(2 \cdot k + 5) \rangle\!\rangle\} = \mathrm{FIB} \restriction (\mathbb{N}_{\mathrm{odd}} \cap \mathrm{Seg}(2 \cdot k + 5))$.

(66) For every natural number n holds $\mathrm{OddFibs}(2 \cdot n + 3) = \mathrm{OddFibs}(2 \cdot n + 1) \frown \langle \mathrm{Fib}(2 \cdot n + 3) \rangle$.

(67) For every natural number n holds $\sum \mathrm{EvenFibs}(2 \cdot n + 2) = \mathrm{Fib}(2 \cdot n + 3) - 1$.

(68) For every natural number n holds $\sum \mathrm{OddFibs}(2 \cdot n + 1) = \mathrm{Fib}(2 \cdot n + 2)$.

5. Carmichael's Theorem on Prime Divisors

One can prove the following three propositions:

(69) For every natural number n holds $\mathrm{Fib}(n)$ and $\mathrm{Fib}(n+1)$ are relative prime.

(70) For every non empty natural number n and for every natural number m such that $m \neq 1$ holds if $m \mid \mathrm{Fib}(n)$, then $m \nmid \mathrm{Fib}(n -' 1)$.

(71) Let n be a non empty natural number. Suppose m is prime and n is prime and $m \mid \mathrm{Fib}(n)$. Let r be a natural number. If $r < n$ and $r \neq 0$, then $m \nmid \mathrm{Fib}(r)$.

6. Fibonacci Numbers and Pythagorean Triples

We now state the proposition

(72) For every non empty natural number n holds $\{\mathrm{Fib}(n) \cdot \mathrm{Fib}(n+3), 2 \cdot \mathrm{Fib}(n+1) \cdot \mathrm{Fib}(n+2), \mathrm{Fib}(n+1)^{\mathbf{2}} + \mathrm{Fib}(n+2)^{\mathbf{2}}\}$ is a Pythagorean triple.

References

[1] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.
[2] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.
[3] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.
[4] Grzegorz Bancerek. Sequences of ordinal numbers. *Formalized Mathematics*, 1(**2**):281–290, 1990.
[5] Grzegorz Bancerek, Mitsuru Aoki, Akio Matsumoto, and Yasunari Shidama. Processes in Petri nets. *Formalized Mathematics*, 11(**1**):125–132, 2003.
[6] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[7] Grzegorz Bancerek and Piotr Rudnicki. Two programs for **scm**. Part I - preliminaries. *Formalized Mathematics*, 4(**1**):69–72, 1993.
[8] Józef Białas. Group and field definitions. *Formalized Mathematics*, 1(**3**):433–439, 1990.
[9] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[10] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[11] Czesław Byliński. The modification of a function by a function and the iteration of the composition of a function. *Formalized Mathematics*, 1(**3**):521–527, 1990.
[12] Czesław Byliński. The sum and product of finite sequences of real numbers. *Formalized Mathematics*, 1(**4**):661–668, 1990.
[13] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[14] Yoshinori Fujisawa, Yasushi Fuwa, and Hidetaka Shimizu. Public-key cryptography and Pepin's test for the primality of Fermat numbers. *Formalized Mathematics*, 7(**2**):317–321, 1998.
[15] Andrzej Kondracki. The Chinese Remainder Theorem. *Formalized Mathematics*, 6(**4**):573–577, 1997.
[16] Jarosław Kotowicz. Convergent real sequences. Upper and lower bound of sets of real numbers. *Formalized Mathematics*, 1(**3**):477–481, 1990.
[17] Rafał Kwiatek. Factorial and Newton coefficients. *Formalized Mathematics*, 1(**5**):887–890, 1990.

[18] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relative primes. *Formalized Mathematics*, 1(**5**):829–832, 1990.
[19] Yatsuka Nakamura and Andrzej Trybulec. A mathematical model of CPU. *Formalized Mathematics*, 3(**2**):151–160, 1992.
[20] Takaya Nishiyama and Yasuho Mizuhara. Binary arithmetics. *Formalized Mathematics*, 4(**1**):83–86, 1993.
[21] Konrad Raczkowski and Andrzej Nędzusiak. Real exponents and logarithms. *Formalized Mathematics*, 2(**2**):213–216, 1991.
[22] Piotr Rudnicki and Andrzej Trybulec. Abian's fixed point theorem. *Formalized Mathematics*, 6(**3**):335–338, 1997.
[23] Robert M. Solovay. Fibonacci numbers. *Formalized Mathematics*, 10(**2**):81–83, 2002.
[24] Andrzej Trybulec. Subsets of complex numbers. *To appear in Formalized Mathematics.*
[25] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**):115–122, 1990.
[26] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.
[27] Andrzej Trybulec. On the sets inhabited by numbers. *Formalized Mathematics*, 11(**4**):341–347, 2003.
[28] Andrzej Trybulec and Czesław Byliński. Some properties of real numbers. *Formalized Mathematics*, 1(**3**):445–449, 1990.
[29] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
[30] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[31] Freek Wiedijk. Pythagorean triples. *Formalized Mathematics*, 9(**4**):809–812, 2001.
[32] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.
[33] Minoru Yabuta. A simple proof of Carmichael's theorem of primitive divisors. *The Fibonacci Quarterly*, 39(5):439–443, 2001.

Received May 10, 2004