The Fibonacci Primes Under Modulo 4

Qing Zou[1] and Jun Steed Huang[2]

[1] Department of Mathematics, Suqian College, Yangzhou University, 399 South Huanghe, Jiangsu 223800, P.R. China,
[2] Suqian College, Jiangsu University, 399 South Huanghe, Jiangsu 223800, P.R. China,
Corresponding addresses
roronoaz@163.com, steedhuang@ujs.edu.cn

***Abstract*:** The research on prime numbers is an interesting topic in Analytic Number Theory. The Fibonacci sequence is one of the most popular sequences in mathematics. In this paper, we will discuss the prime numbers of the Fibonacci sequence, which we call Fibonacci primes. The goal of this paper is to prove that starting with $F_5 = 5$, all the Fibonacci primes p are satisfied with $p \equiv 1 \pmod 4$, on the basis of the Pythagorean theorem.

Keywords: Fibonacci sequence; Fibonacci primes; Pythagorean triple; Algebraic Number Theory.

1. Introduction

The Fibonacci sequence (sometimes called Fibonacci numbers), which is named after Leonardo Fibonacci (c.1170 – c.1250), are the numbers in the following integer sequence:

$$1,1,2,3,5,8,13,21,34,55,89,144,\cdots$$

In some cases [1], the first two numbers in the Fibonacci sequence are 0 and 1. It depends on the chosen starting point of the sequence. In this paper, we choose the first two numbers to be 1 and 1, since it relates immediately to the rabbit family size.

The constitution of the sequence is such that each subsequent number is the sum of the previous two. In mathematics terms, the sequence F_n of the Fibonacci numbers is defined by the recurrence formula

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

with initial values [2]

$$F_1 = 1, F_2 = 1.$$

There are some interesting identities on Fibonacci numbers. For example, since

$$\begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^n,$$

we have

$$F_{n+1}F_{n-1} - F_n^2 = (-1)^n.$$

Also, there exists

$$F_{n+3}^2 = 2F_{n+2}^2 + 2F_{n+1}^2 - F_n^2.$$

The common item equation of the Fibonacci sequence is

$$F_n = \frac{\sqrt{5}}{5}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right]$$

Several methods can be used to get this equation [3]. It is known that the Fibonacci sequence is closely related to golden ratio [4].

The Fibonacci numbers are also closely related to Lucas numbers, since they are a complementary pair of Lucas sequences [5], [6].

There are many applications of the Fibonacci sequence, including computer algorithms such as the Fibonacci heap [7] data structure, and graphs called Fibonacci cubes [8] used for interconnecting parallel and distributed systems. The Fibonacci numbers are also Nature's numbering system. They appear almost everywhere in Nature [9], from the leaf arrangement in plants, to the pattern of the florets of a flower, the bracts of a pinecone, or the scales of a pineapple [10]. The Fibonacci numbers are therefore applicable to the growth of every living thing, including a single cell, a grain of wheat, a hive of bees, and even mankind [10].

In light of the applications mentioned above, it is clear that the Fibonacci sequence plays an important role not only in mathematics but also in our daily lives, such as the obfuscation or encryption of the software code in C++ [11]. As such, research on the sequence becomes more and more important. Fibonacci primes are one of such topics.

A Fibonacci prime is a Fibonacci number that is prime. The few seeds are:

$$F_3 = 2, F_4 = 3, F_5 = 5, F_7 = 13, F_{11} = 89,$$
$$F_{13} = 233, F_{17} = 1597, \cdots$$

Although Fibonacci primes with thousands of digits have been found, it is not known whether there are infinitely many Fibonacci prime numbers [12]. It is one of the unsolved problems in mathematics. The divisibility of Fibonacci numbers by a prime, p, is related to the Legendre symbol $\left(\frac{p}{5}\right)$. If p is a prime number then

$$F_p \equiv \left(\frac{p}{5}\right) \pmod p,$$
$$F_{p-\left(\frac{p}{5}\right)} \equiv 0 \pmod p.$$

It is also not known whether there exists a prime, p, such that,

$$F_{p-\left(\frac{p}{5}\right)} \equiv 0 \pmod{p^2}.$$

Such primes (if there are any) would be called Wall-Sun-Sun primes or Fibonacci-Wieferich primes. Wall–Sun–Sun primes are named after Donald Dines Wall, Zhi Hong Sun and Zhi Wei Sun; Fibonacci-Wieferich primes are named after Arthur Wieferich.

It is not known whether there are an infinite number of Fibonacci primes, but we can determine the property of Fibonacci primes, which is the goal of this paper.

2. Revisiting the Pythagorean Triple

A Pythagorean triple is made of three positive integers, x, y and z, such that $x^2+y^2=z^2$. Such a triple is often denoted as (x,y,z), and a well-known example found a few thousands years ago is (3,4,5). The name is due to the Pythagorean theorem (Chinese: Shang Gao Theorem), describing that any given right triangle has side lengths that satisfy the formula $x^2+y^2=z^2$. So, Pythagorean triples describe the relationship of the three integer side lengths of a right triangle.

Euclid's formula [13] is fundamental for generating Pythagorean triples when given an arbitrary pair of positive integers m and n with $m>n$. The formula states that integers

$$\begin{cases} x=m^2-n^2 \\ y=2mn \\ z=m^2+n^2 \end{cases}$$

form a Pythagorean triple. The triple generated by Euclid's formula is primitive if, and only if, m and n are coprime and $m-n$ is odd.

Euclid's formula does not generate all triples, but can generate all primitive triples. This can be remedied by inserting an additional parameter, k, into the formula. The following formula will generate all Pythagorean triples uniquely:

$$\begin{cases} x=k(m^2-n^2) \\ y=k(2mn) \\ z=k(m^2+n^2) \end{cases}$$

where m, n and k are positive integers with $m>n$, $m-n$ odd, and with m and n coprime.

The Euclidian formula is so prominent that the proof can be seen in almost every elementary number theory book [14]. So, we will not give the proof here.

3. The Parity Lemmas and Proofs

The Pythagorean triples can be used to prove the following lemma.

Lemma 1. Starting with $F_5=5$, every second Fibonacci number is the length of the hypotenuse of a right triangle with integer sides, or in other words, the largest number in a Pythagorean triple.

Proof. We can prove this lemma by the following table.

m	n	m^2-n^2	$2mn$	m^2+n^2
$F_3=2$	$F_2=1$	3	4	$F_5=5$
$F_4=3$	$F_3=2$	5	12	$F_7=13$
$F_5=5$	$F_4=3$	16	30	$F_9=34$
$F_6=8$	$F_5=5$	39	80	$F_{11}=89$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
F_{i+1}	F_i	$F_{i+1}^2-F_i^2$ $=F_{i+2}F_{i-1}$	$2F_iF_{i-1}$ $=F_{2i+2}^2-F_{i+1}^2$	F_{2i+1} $=F_i^2+F_{i+1}^2$

According to the table listed above, we can see

$$F_{2i+1}^2=(2F_iF_{i-1})^2+(F_{i+1}^2-F_i^2)^2.$$

That is to say, starting with $F_5=5$, every second Fibonacci number can be the largest number in a Pythagorean triple. □

Lemma 1 tells us that starting with $F_5=5$, the Fibonacci number with an odd index is the length of a right triangle with integer sides.

Lemma 2. Starting with $F_5=5$, Fibonacci primes have a prime index. In other words, starting with $F_5=5$, all Fibonacci primes have an odd index.

Proof. Suppose there exists a Fibonacci prime with a composite index m and a is a factor of m, then a divides m. For if a divides m, then F_a divides F_m, meaning that F_a is a factor of F_m. It is a contradiction. Therefore, lemma 2 is proved. □

What we need to point out is that though starting with $F_5=5$, Fibonacci primes have a prime index, not every prime larger than 5 is an example of a Fibonacci prime, $F_{19}=4181=37\times 113$ is a counter example.

4. The Modulo Theorem and Proof

By lemma 1 and lemma 2, we can easily get that, starting with $F_5=5$, all the Fibonacci primes can be the length of the hypotenuse of a right triangle with integer sides. Consequently, if we want to prove that, starting with $F_5=5$, all the Fibonacci primes satisfy $p\equiv 1(\mathrm{mod}\,4)$, we just need to prove that for all prime numbers p, if $p\equiv 1(\mathrm{mod}\,4)$, then $x^2+y^2=p^2$ has integer solutions.

Before we prove the proposition, we need to introduce another conclusion in Algebraic Number Theory.

Lemma 3. (1) If p is a prime number congruent to 1 modulo 4, then there exists a prime element a in $\mathbb{Z}[i]$ such that $p=a\bar{a}$ ($\bar{a}$ is also a prime element of $\mathbb{Z}[i]$).

(2) If p is a prime number congruent to 3 modulo 4, then p is a prime element in $\mathbb{Z}[\mathrm{i}]$.

Note. An element α in $\mathbb{Z}[\mathrm{i}]$ is a prime element if it satisfies:

(a) α is nonzero and not a unit (invertible element).
(b) If $a,b \in \mathbb{Z}[\mathrm{i}]$ and $ab \in \alpha\mathbb{Z}[\mathrm{i}]$, then $a \in \alpha\mathbb{Z}[\mathrm{i}]$ or $b \in \alpha\mathbb{Z}[\mathrm{i}]$.

Proof. (1) Let p be a prime number and $p \equiv 1 \pmod 4$, since

$$\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}=\begin{cases}1, & p\equiv 1 \pmod 4,\\ -1, & p \equiv 3 \pmod 4,\end{cases}$$

then $\left(\frac{-1}{p}\right)=1$, where $\left(\frac{a}{p}\right)$ represents Legendre symbol. Also, there exists an integer a such that $a^2 \equiv -1 \pmod p$. Since
$(a+\mathrm{i})(a-\mathrm{i})=a^2+1 \in p\mathbb{Z}[\mathrm{i}], \quad a+\mathrm{i} \notin p\mathbb{Z}[\mathrm{i}], \quad a-\mathrm{i} \notin p\mathbb{Z}[\mathrm{i}]$.
So, p is not a prime element in $\mathbb{Z}[\mathrm{i}]$.

On the other hand, because p is not a unit in $\mathbb{Z}[\mathrm{i}]$, it follows from the prime factorization of p in $\mathbb{Z}[\mathrm{i}]$ that there exists a prime element α in $\mathbb{Z}[\mathrm{i}]$ dividing p. Let $p=\alpha\beta, \beta \in \mathbb{Z}[\mathrm{i}]$. Because p is not a prime element, β is not a unit, we have

$$p^2=\alpha\beta\cdot\overline{\alpha\beta}=\alpha\bar{\alpha}\cdot\beta\bar{\beta},$$

and because both $\alpha\bar{\alpha}$ and $\beta\bar{\beta}$ are natural numbers, $\alpha\bar{\alpha}$ must be one of the divisors of p^2, i.e. $1, p, p^2$. If $\alpha\bar{\alpha}=1$, then α would be a unit and we will get a contradiction. If $\alpha\bar{\alpha}=p^2$, then β would be a unit, since $\beta\bar{\beta}=1$. Thus, there must be $p=\alpha\bar{\alpha}$.

(2) Let p be a prime number and $p \equiv 3 \pmod 4$, and let α be a prime element in $\mathbb{Z}[\mathrm{i}]$ dividing p. Let $p=\alpha\beta, \beta \in \mathbb{Z}[\mathrm{i}]$. Then, as is shown above, we have

$$p^2=\alpha\beta\cdot\overline{\alpha\beta}=\alpha\bar{\alpha}\cdot\beta\bar{\beta}.$$

Because $\alpha\bar{\alpha} \neq 1$ and we cannot write $p=x^2+y^2$ ($x,y \in \mathbb{Z}$) (since there exists $x,y \in \mathbb{Z}$ satisfying $p=x^2+y^2$ if and only if $p \equiv 1 \pmod 4$ or $p=2$), we can get that $p \neq \alpha\bar{\alpha}$. Thus, there must be $\alpha\bar{\alpha}=p^2, \beta\bar{\beta}=1$, and β is a unit. Hence $p=\alpha\beta$ is a prime element. □

Note. Moreover, we can prove that in the former part of this lemma, $\alpha\mathbb{Z}[\mathrm{i}]$ is not equal to $\bar{\alpha}\mathbb{Z}[\mathrm{i}]$.

By this lemma, we have

Theorem 1. Starting with $F_5=5$, all Fibonacci primes p satisfy $p \equiv 1 \pmod 4$.

Proof. Let's prove this conclusion in two steps.

Step 1. Let p be a prime number and $p \equiv 1 \pmod 4$, then there exists a right triangle with integer sides such that the length of hypotenuse is p.

Because $p \equiv 1 \pmod 4$, by lemma 3(1), p can be written as $p=\alpha\bar{\alpha}$, where α is a prime element in $\mathbb{Z}[\mathrm{i}]$. Suppose $\alpha^2=x+\mathrm{i}y, (x,y \in \mathbb{Z})$, we have

$$p^2=\alpha^2\bar{\alpha}^2=x^2+y^2.$$

If we show $x \neq 0, y \neq 0$, we see that p is the length of the hypotenuse of a right triangle whose three sides are $|x|,|y|$ and p. If $x=0$ or $y=0$, the argument of α is a multiple of $\frac{\pi}{4}$, and thus there exists an integer m such that

$$\alpha=m\beta, \quad \text{where } \beta \in \{1, 1+\mathrm{i}, \mathrm{i}, -1, -1+\mathrm{i}\}.$$

This contradicts the uniqueness of the prime factorization in $\mathbb{Z}[\mathrm{i}]$. It is obvious that the equation $2^2=x^2+y^2$ does not have a solution satisfying $x \neq 0, y \neq 0$.

Step 2. If p is a prime number and $p \equiv 3 \pmod 4$, then there will be no right triangle that the length of the hypotenuse is p.

Let $p^2=x^2+y^2 (x,y \in \mathbb{Z})$. If we set $\alpha=x+\mathrm{i}y$, then we have $p^2=\alpha\bar{\alpha}$. By lemma 3(2), p is a prime element in $\mathbb{Z}[\mathrm{i}]$. It follows from the uniqueness of factorization that

$$\alpha=p\times(\pm 1, \text{or} \pm \mathrm{i}).$$

This implies $x=0$ or $y=0$.

According to the two steps shown above, lemma 1 and lemma 2, the theorem is proved. □

5. Conclusion

In this paper, we have studied the Fibonacci numbers that are prime and started with the simple seed 1 and 1. We have proven that, in this case, modulo 4 be 1 can be used to offer a quick judgment and if the number obtained during the computer program iteration belongs to a prime. This operation saves the complicated computation time for finding a prime that fits well for applications like obfuscation of intellectual property protected code. The applications of this new finding will not be limited.

6. Acknowledgement

This work was partially supported by GenieView subsidiary M2M Technology 331.7.49 Project, and the Suqian Excellence Expert Allowance 2013.18.14.5.9.2.

We are grateful to following individuals for their immeasurable helps and contributions to this research work: Jiangyong Gu, Runping Ye, from our university.

6.1 Author Contributions

The manuscript was written through contributions of all authors. All authors have given approval to the final version of the manuscript. Qing Zou conceived and designed the original work that led to this submission, and played an important role in proof of the results. Jun S. Huang improved the manuscript, collected some references and discussed the applications with Qing Zou during the process of the writing.

6.2 Conflict of Interests

The authors declare no Conflicts of Interest.

References

[1] Beck, Matthias, Geoghegan, Ross, The Art of Proof: Basic Training for Deeper Mathematics, New York: *Springer*, 2010.

[2] M. A. Khan, Harris Kwong, "On Sums of Products of Fibonacci-Type Recurrences", *The Fibonacci Quarterly*, vol.52,pp.20-26, 2014.

[3] Binet's Fibonacci Number Formula. http://mathworld.wolfram.com/BinetsFibonacciNumberFormula.html

[4] Helmut Prodinger, Two Families of Series for the Generalized Golden Ratio, *The Fibonacci Quarterly*, vol.53,pp.74-77, 2015.

[5] Leonid Bedratyuk, "Derivations and Identitites for Fibonacci and Lucas Polynomials", *The Fibonacci Quarterly*, vol.51,pp.351-366, 2013.

[6] Mohamed Taoufiq Damir, Bernadette Faye, Florian Luca, Amadou Tall, "Members of Lucas Sequences Whose Euler Function Is a Power of 2", *The Fibonacci Quarterly*, vol.52,pp.3-9, 2014.

[7] Brodal G. S. L., Lagogiannis G., Tarjan R. E., "Strict Fibonacci Heaps", *Proceedings of the 44th Symposium on Theory of Computing - STOC '12*, 2012, pp. 1177.

[8] Dedó, Ernesto, Torri, Damiano, Salvi, Norma Zagaglia, "The observability of the Fibonacci and the Lucas cubes", *Discrete Mathematics*, vol.255(1-3),pp. 55-63, 2002.

[9] Douady S., Couder Y., "Phyllotaxis as a Dynamical Self Organizing Process". *Journal of Theoretical Biology*, vol.178 ,pp. 255-74, 1996.

[10] S. L. Basin, "The Fibonacci sequence as it appears in nature", *The Fibonacci Quarterly*, vol.1,pp.53-56, 1993.

[11] K. Donald, The Art of Computer Programming 1, *Addison Wesley*, 1968.

[12] List of unsolved problems in mathematics. http://en.wikipedia.org/wiki/List_of_unsolved_problems_in_mathematics

[13] Joyce, D. E., Book X, Proposition XXIX, Euclid's Elements, *Clark University*, 1997.

[14] Burton, David M., Elementary Number Theory (Sixth Edition), *McGraw-Hill College*, 2005.