

Jiří Klaška

Short remark on Fibonacci-Wieferich primes

Acta Mathematica Universitatis Ostraviensis, Vol. 15 (2007), No. 1, 21--25

Persistent URL: <http://dml.cz/dmlcz/137492>

Terms of use:

© University of Ostrava, 2007

Institute of Mathematics of the Academy of Sciences of the Czech Republic provides access to digitized documents strictly for personal use. Each copy of any part of this document must contain these *Terms of use*.



This paper has been digitized, optimized for electronic delivery and stamped with digital signature within the project *DML-CZ: The Czech Digital Mathematics Library* <http://project.dml.cz>

Short remark on Fibonacci-Wieferich primes

Jiří Kláška

Abstract. This paper has been inspired by the endeavour of a large number of mathematicians to discover a Fibonacci-Wieferich prime. An exhaustive computer search has not been successful up to the present even though there exists a conjecture that there are infinitely many such primes. This conjecture is based on the assumption that the probability that a prime p is Fibonacci-Wieferich is equal to $1/p$. According to our computational results and some theoretical considerations, another form of probability can be assumed. This observation leads us to interesting consequences.

1 Introduction

A prime p is called a Fibonacci-Wieferich prime if

$$F_{p-(p/5)} \equiv 0 \pmod{p^2} \quad (1)$$

where F_n denotes the n -th Fibonacci number defined by $F_{n+2} = F_{n+1} + F_n$ with $F_0 = 0$, $F_1 = 1$, and (a/b) denotes the Legendere symbol of a and b . Fibonacci-Wieferich primes are mostly studied in relation to the first case of Fermat's last theorem. In 1992, Zhi-Hong Sun and Zhi-Wei Sun [8] showed that, if $p \mid xyz$ and $x^p + y^p = z^p$, then (1) is valid. Fibonacci-Wieferich primes are sometimes referred to as Wall-Sun-Sun primes. See [1].

Reducing F_n modulo m , we obtain the sequence $(F_n \pmod{m})_{n=1}^{\infty}$, which is periodic. A positive integer $k(m)$ is called the period of a Fibonacci sequence modulo m if it is the smallest positive integer for which $F_{k(m)} \equiv 0 \pmod{m}$ and $F_{k(m)+1} \equiv 1 \pmod{m}$. For a fixed prime p , D. D. Wall [9, Theorem 5] has proved that, if $k(p) = k(p^s) \neq k(p^{s+1})$, then $k(p^t) = p^{t-s}k(p)$ for $t \geq s$. Wall asked whether $k(p) = k(p^2)$ is always impossible. This is still an open question. It is well known (see e.g. [3]) that $k(p) = k(p^2)$ if and only if p satisfies (1). Consequently, no Fibonacci-Wieferich prime p is known. Fibonacci-Wieferich primes were studied by many authors. From an extensive list of references let us recall at least the

Received: October 25, 2007.

2000 Mathematics Subject Classification: 11B50, 11B39, 11A07, 11Y99 .

Key words and phrases: Fibonacci numbers, Wall's question, Wall-Sun-Sun prime, Fibonacci-Wieferich prime, modular periodicity, periodic sequence.

papers [3],[4], [7] and [10]. The problem of finding Fibonacci-Wieferich primes is in close analogy to the problem of finding Wieferich primes. See [1]. In 2007, R. McIntosh and E. L. Roettger [6] showed that there is no Fibonacci-Wieferich prime p for $p < 2 \times 10^{14}$. On the other hand, by statistical considerations

[1, p.447], in an interval $[x, y]$, there are expected to be

$$\sum_{x \leq p \leq y} \frac{1}{p} \approx \ln(\ln y / \ln x) \quad (2)$$

Fibonacci-Wieferich primes. By (2), this means that, in the interval $[2, 2 \times 10^{14}]$, we can expect about 3.86 Fibonacci-Wieferich primes. The results presented in this paper suggest that, for the number of Fibonacci-Wieferich primes in an interval $[x, y]$, a formula different from (2) is more likely to be valid. As we see, there exist two kinds of primes and, for each of these, the estimate is principally different.

2 Basic observations

Let L_p be the splitting field of the Fibonacci characteristic polynomial $f(x)$ over the field of p -adic numbers \mathbb{Q}_p and α, β be the roots of $f(x)$ in L_p . Denote by O_p the ring of integers of L_p . As the discriminant of $f(x)$ is equal to 5, it follows that, for $p \neq 5$, L_p/\mathbb{Q}_p does not ramify and so the maximal ideal of O_p is generated by p . Put $q = |O_p/(p)|$. Then $q = p^t$ where $t = [L_p : \mathbb{Q}_p] \in \{1, 2\}$. If $f(x)$ is irreducible over \mathbb{Q}_p , then $O_p/(p)$ is a field with p^2 elements and $O_p/(p^2)$ is a ring with p^4 elements. If $f(x)$ is not irreducible over \mathbb{Q}_p , then $O_p/(p)$ is a field with p elements and $O_p/(p^2)$ has p^2 elements. For a unit $\xi \in O_p$, we denote by $\text{ord}_{p^t}(\xi)$ the least positive rational integer h such that $\xi^h \equiv 1 \pmod{p^t}$. Let us now recall some results derived in [5].

Lemma 2.1. *For any prime $p \neq 5$, we have*

- (i) $k(p^t) = \text{lcm}(\text{ord}_{p^t}(\alpha), \text{ord}_{p^t}(\beta))$ for any $t \in \mathbb{N}$.
- (ii) $\text{ord}_{p^t}(\alpha) = \text{ord}_{p^t}(\beta)$ or $\text{ord}_{p^t}(\alpha) = 2\text{ord}_{p^t}(\beta)$ or $2\text{ord}_{p^t}(\alpha) = \text{ord}_{p^t}(\beta)$.
- (iii) $k(p) \neq k(p^2)$ if and only if $\text{ord}_{p^2}(\alpha) \equiv 0 \pmod{p}$ and $\text{ord}_{p^2}(\beta) \equiv 0 \pmod{p}$.
- (iv) $\text{ord}_{p^2}(\alpha) \equiv 0 \pmod{p}$ if and only if $\text{ord}_{p^2}(\beta) \equiv 0 \pmod{p}$.

From (iii) and (iv), it now follows that p is a Fibonacci-Wieferich prime if and only if

$$\text{ord}_{p^2}(\alpha) \not\equiv 0 \pmod{p} \quad \text{and} \quad \text{ord}_{p^2}(\beta) \not\equiv 0 \pmod{p}. \quad (3)$$

Let I denote the set of all primes for which $f(x)$ is irreducible over \mathbb{Q}_p and $I(x)$ be the number of all $p \in I$, $p \leq x$. Similarly, let L denote the set of all primes p for which $f(x)$ is factorized over \mathbb{Q}_p into linear factors and $L(x)$ be the number of all $p \in L$, $p \leq x$. Clearly, $I \cap L = \emptyset$ and $I \cup L$ is the set of all primes. Hence, $I(x) + L(x) = \pi(x)$ where $\pi(x)$ is the number of all primes p not exceeding x .

The following beautiful characterization of the sets I and L is known. See [9, Theorems 6 and 7].

Lemma 2.2. For the sets I and L , we have:

- (i) $p \in I$ if and only if $p = 2, 5$ or $p \equiv 3 \pmod{10}$ or $p \equiv 7 \pmod{10}$.
- (ii) $p \in L$ if and only if $p \equiv 1 \pmod{10}$ or $p \equiv 9 \pmod{10}$.

Theorem 2.3. Let $q = p^{[L_p \cdot \mathbb{Q}_p]}$. Then, in the multiplicative group $[O_p/(p^2)]^\times$, there exist exactly $q - 1$ elements ξ satisfying $\xi^{q-1} \equiv 1 \pmod{p^2}$.

Proof: If $\varepsilon_1, \dots, \varepsilon_q$ is a complete residue system of $O_p/(p)$, then $\varepsilon_i + p\varepsilon_j$ where $i, j \in \{1, \dots, q\}$ is a complete residue system of $O_p/(p^2)$. Clearly, $\varepsilon_i + p\varepsilon_j$ is a unit in $O_p/(p^2)$ if and only if $\varepsilon_i \neq 0$. It follows that $[O_p/(p^2)]^\times$ has $(q - 1)q$ elements. Consequently, $[O_p/(p^2)]^\times \cong G \times H$ where G is a group of order $q - 1$ and H is a group of order q . For any $[u, v] \in G \times H$, we have $[u, v]^{q-1} = [1, v^{-1}]$. This implies that $[u, v]^{q-1} = [1, 1]$ if and only if $v = 1$ and u is arbitrary. As u can be chosen in $q - 1$ ways, there exist exactly $q - 1$ elements $\xi \in [O_p/(p^2)]^\times$ satisfying $\xi^{q-1} \equiv 1 \pmod{p^2}$. \square

By Theorem 2.3, the number of $\xi \in [O_p/(p^2)]^\times$ satisfying $\xi^{p-1} \equiv 1 \pmod{p^2}$ strongly depends on the form of the factorization of $f(x)$ over \mathbb{Q}_p . Put $Q(p) = \{\xi \in [O_p/(p^2)]^\times; \xi^{q-1} \equiv 1 \pmod{p^2}\}$. Clearly, $Q(p)$ is a subgroup of order $q - 1$ of $[O_p/(p^2)]^\times$. Let α, β be the roots of $f(x)$ in O_p and let α_2, β_2 be the images of α, β in $[O_p/(p^2)]^\times$. By (3), we have $\alpha_2 \in Q(p)$ if and only if $\beta_2 \in Q(p)$. Moreover, the Viète equation $\alpha_2\beta_2 = -1$ implies that $\beta_2 = -\alpha_2^{-1}$ in $[O_p/(p^2)]^\times$.

Remark 2.4. *In my opinion, the results of Theorem 2.3 rather indicate that the probability P of inclusion $\{\alpha_2, \beta_2\} \subseteq Q(p)$ is equal to*

$$P = \begin{cases} 1/p^2, & \text{if } p \in I, \\ 1/p, & \text{if } p \in L. \end{cases} \quad (4)$$

For this reason, the sum in (2) should be replaced by

$$\sum_{x \leq p \leq y} \frac{1}{q}, \quad \text{where } \begin{cases} q = p^2, & \text{if } p \in I, \\ q = p, & \text{if } p \in L. \end{cases} \quad (5)$$

Of course, one knows in advance which of the cases $\{\alpha_2, \beta_2\} \subseteq Q(p)$ and $\{\alpha_2, \beta_2\} \not\subseteq Q(p)$ will occur as the roots α_2, β_2 are uniquely determined for any prime p .

3 Statistical consequences

Let us now consider the series

$$R = \sum_{p \in I} \frac{1}{p^2} = \frac{1}{4} + \frac{1}{9} + \frac{1}{25} + \frac{1}{49} + \frac{1}{169} + \frac{1}{289} + \dots \quad (6)$$

and

$$S = \sum_{p \in L} \frac{1}{p} = \frac{1}{11} + \frac{1}{19} + \frac{1}{29} + \frac{1}{31} + \frac{1}{41} + \frac{1}{59} + \dots \quad (7)$$

Since $\sum_{p \in I} \frac{1}{p^2} < \sum_p \frac{1}{p^2} = \zeta_p(2)$, we have

Lemma 3.1. *The series R converges.*

Remark 3.2. *The convergence of $\zeta_p(2) = \sum_p \frac{1}{p^2}$ is logarithmic and therefore extremely slow. The estimate $\zeta_p(2) = 0.45224\dots$ comes from Euler (1748). On the other hand, we have $0.42151\dots < \sum_{p \in I}^{p < 10} \frac{1}{p^2}$. Computing yields*

$$R = \sum_{p \in I} \frac{1}{p^2} = 0.43648\dots \quad (8)$$

which is a good match with $0.42151\dots < \sum_{p \in I} \frac{1}{p^2} < 0.45224\dots$.

The probability P of finding a Fibonacci-Wieferich prime ending with digits 3 or 7 will virtually not increase as the search set becomes larger. Consequently, the existence of a Fibonacci-Wieferich prime $p \in I$, $p > 2 \times 10^{14}$ is very improbable. As the following lemma is valid by Dirichlet's theorem on primes in arithmetic progression, for a prime that ends with 1 or 9, the situation is more optimistic.

Lemma 3.3. *The series S diverges.*

Remark 3.4. *It is well known (see e.g. [2, p.57]) that*

$$\sum_{\substack{p \leq x \\ p \equiv l \pmod{k}}} \frac{1}{p} = \frac{1}{\phi(k)} \ln \ln x + A(k, l) + O((\ln x)^{-1}) \quad (9)$$

where ϕ is the Euler function. From (9) it follows that

$$\sum_{p \in L \cap [x, y]} \frac{1}{p} \approx \frac{1}{2} \sum_{p \in [x, y]} \frac{1}{p} \approx \frac{1}{2} \ln(\ln y / \ln x) \quad (10)$$

Moreover, for $I(x)$ and $L(x)$, we have

$$\lim_{x \rightarrow \infty} \frac{I(x)}{L(x)} = 1. \quad (11)$$

Put $S(x) = \sum_{\substack{p \leq x \\ p \in L}} \frac{1}{p}$. A certain idea of the above functions can be obtained from Table 1.

x	$I(x)$	$L(x)$	$\pi(x)$	$I(x) : L(x)$	$S(x)$
10^2	15	10	25	1.50000	0.30599
10^3	90	78	168	1.15384	0.49500
10^4	620	609	1229	1.01806	0.63822
10^5	4815	4777	9592	1.00795	0.74875
10^6	39288	39210	78498	1.00198	0.83970
10^7	332443	332136	664579	1.00092	0.91673
10^8	2880971	2880484	5761455	1.00016	0.98342

Table 1.

From the results derived, it seems to be worthwhile to direct attention only to the primes ending with the digits 1 or 9. In this case, to decide whether p is a Fibonacci-Wieferich prime, we can use some of the criteria derived in [5, Theorem 2.11]. The main advantage of such criteria is that they do not involve calculating with

Fibonacci numbers but rather with the solution of the congruence $f(x) \equiv 0 \pmod{p}$. We have

Theorem 3.5. *Let $p \equiv 1 \pmod{10}$ or $p \equiv 9 \pmod{10}$. Further, let a be any solution of $f(x) \equiv 0 \pmod{p}$ and let f' be a derivative of the Fibonacci characteristic polynomial f . Then the following statements are equivalent:*

- (i) p is Fibonacci-Wieferich prime,
- (ii) $a^{2p} - a^p - 1 \equiv 0 \pmod{p^2}$,
- (iii) $f(a) + (a^p - a)f'(a) \equiv 0 \pmod{p^2}$.

Proof: If $p \equiv 1 \pmod{10}$ or $p \equiv 9 \pmod{10}$, then by Lemma 2.2, part (ii), we have $p \in L$ and $|O_p/(p)| = p$. The equivalence of (i),(ii), and (iii) is now a straightforward consequence of [5, Theorem 2.11]. \square

Anyone searching for a Fibonacci-Wieferich prime using a computer is facing an immediate problem of completing the search of the interval $[2 \times 10^{14}, 10^{15}]$. By (9), theoretically, there should be about 0.02 Fibonacci-Wieferich primes within this interval ending with 1 or 9. In the following interval $[10^{15}, 10^{16}]$ then, there should be about 0.03 primes. Even though the odds are not much favourable, there is still hope that a Fibonacci-Wieferich prime will be discovered.

References

- [1] R. Crandall, K. Dilcher, C. Pomerance *A search for Wieferich and Wilson primes* Math. Comp. **66** (1997) 443-449
- [2] H. Davenport *Multiplicative Number Theory* Springer-Verlag New York 3rd ed. (2000)
- [3] A. - S. Elsenhans, J. Jahnel *The Fibonacci sequence modulo p^2 - An investigation by computer for $p < 10^{14}$* The On-Line Encyclopedia of Integer Sequences (2004) 27 p
- [4] Hua-Chieh Li *Fibonacci primitive roots and Wall's question* The Fibonacci Quarterly **37** (1999) 77-84
- [5] J. Klaka *Criteria for Testing Wall's Question* preprint (2007)
- [6] R. J. McIntosh, E. L. Roettger *A search for Fibonacci-Wieferich and Wolstenholme primes* Math. Comp. **76** (2007) 2087-2094
- [7] *A note on some relations among special sums of reciprocals modulo p* L. Skula to appear in Math. Slovaca (2008)
- [8] *Fibonacci Numbers and Fermat's Last Theorem* Zhi-Hong Sun, Zhi-Wei Sun Acta Arith. **60** (1992) 371-388
- [9] D. D. Wall *Fibonacci Series Modulo m* Amer. Math. Monthly **67** no. 6, (1960) 525-532
- [10] H. C. Williams *A Note on the Fibonacci Quotient $F_{p-\epsilon}/p$* Canad. Math. Bull. **25** (1982) 366-370

Author(s) Address(es):

DEPARTMENT OF MATHEMATICS, BRNO UNIVERSITY OF TECHNOLOGY, TECHNICK 2, 616
69 BRNO, CZECH REPUBLIC

E-mail address: klaskafme.vutbr.cz