DONALD DINES WALL'S CONJECTURE

JIŘÍ KLAŠKA

Abstract. Wall's conjecture is an interesting, not yet resolved number-theory problem concerning a Fibonacci sequence. The problem took on a new significance after its connection was discovered with Fermat's Last Theorem. What follows is a summary of all important discoveries and known facts related to Wall's conjecture made over 56 years of its existence.

Dedicated to Ladislav Skula on the occasion of his 80th birthday.

1. Wall's Question - State of Problem

The Fibonacci sequence $(F_n)_{n=0}^{\infty}$ was introduced by Italian mathematician Leonardo Fibonacci (1175 – 1250) in 1202. It is defined recursively: $F_0 = 0$, $F_1 = 1$, and $F_{n+2} = F_{n+1} + F_n$ for all $n \geq 0$. Fix a positive integer $m > 1$. It is well-known that, reducing $(F_n)_{n=0}^{\infty}$ modulo m and taking least positive residues, we obtain a sequence $(F_n \bmod m)_{n=0}^{\infty}$, which is periodic. The first related discovery concerning this property goes back to J. L. Lagrange [34, pp. 142–147]. See also Dickson's History [14, p. 393]. A positive integer $k(m)$ is called the period of Fibonacci sequence modulo m if it is the smallest positive integer for which $F_{k(m)} \equiv 0 \pmod{m}$ and $F_{k(m)+1} \equiv 1 \pmod{m}$. Various properties of $k(m)$ have been studied in great detail by many authors. For the basic properties of $k(m)$, see J. C. Kluyver [32], S. Täcklid [58], D. D. Wall [65], D. W. Robinson [49], and J. Vinson [61]. In 1928, J. C. Kluyver [32, p. 278] discovered that, if p is a prime, $p \equiv \pm 1 \pmod{10}$, then $k(p) | p-1$. If $p \equiv \pm 3 \pmod{10}$, then $k(p) | 2(p+1)$ but $k(p) \nmid p+1$. See also [65, p. 528]. In 1960, D. D. Wall [65, p. 527] proved that, if p is an arbitrary prime and $k(p) = k(p^s) \neq k(p^{s+1})$, then $k(p^t) = p^{t-s}k(p)$ for any positive integers $t \geq s$. Consequently, if $k(p^2) \neq k(p)$, then $k(p^t) = p^{t-1}k(p)$ for all t. Wall [65, p. 528] poses a question that has so far remained unanswered:

The most perplexing problem we have met in this study concerns the hypothesis $k(p^2) \neq k(p)$. We have run a test on a digital computer that shows $k(p^2) \neq k(p)$ for all p up to $10,000$; however, we cannot yet prove that $k(p^2) = k(p)$ is impossible. The question is closely related to another one, "can a number x have the same order mod p *and* mod p^2*?", for which rare cases give an affirmative answer (e.g., $x = 3$, $p = 11$; $x = 2$, $p = 1093$); hence, one might conjecture that equality may hold for some exceptional p.*

Note that the equality $k(m^2) = k(m)$ may be true if m is not a prime. For example, if $m = 12$, then $k(12^2) = k(12) = 24$, see [26, p. 347].

In 1997, R. E. Crandall, K. Dilcher, and C. Pomerance [12] called primes p satisfying the equality $k(p^2) = k(p)$ the Wall-Sun-Sun primes. In the literature, these primes are also often referred to as Fibonacci-Wieferich primes. This name was first used in 2005 by J. Knauer and J. Richstein [33].

This paper aims to summarize all important discoveries concerning Wall's conjecture made in the period 1960–2016.

2. First Partial Answer of S. E. Mamangakis

In 1961, S. E. Mamangakis [39] furnished a proof of the hypothesis $k(p^2) \neq k(p)$ under the following assumptions: If p is an arbitrary prime and, for some n, $F_n = cp$ with $(c,p) = 1$, then $k(p^2) \neq k(p)$ [39, Theorem 1]. Next, if $(c,p) = 1$, $t \leq s$, and $F_j = cp^s$ is the first multiple of p to occur in $(F_n)_{n=0}^{\infty}$, then $k(p^t) = k(p)$ if and only if F_{j-1} has the same order modulo p and modulo p^t [39, Theorem 2]. Furthermore, in [39, p. 649], Mamangakis posed the question whether [39, Theorem 1] can be strengthened as follows: If c and p are relatively prime, then cp occurs in $(F_n)_{n=0}^{\infty}$ and $k(p^2) \neq k(p)$. The generalization of [39, Theorem 1] for sequences $(G_n)_{n=0}^{\infty}$ defined by $G_{n+2} = aG_{n+1} + bG_n$ with $G_0 = 0$, $G_1 = 1$ where a, b are integers is given by C. C. Yalavigi [72, p. 125]. Yalavigi also claims [73] that the answer to the Mamangakis question is affirmative.

3. Rank of Appearance and the Fibonacci Quotient

In 1877, E. Lucas [38] discovered the following law of appearance of primes in the Fibonacci sequence: If p is a prime, $p \equiv \pm 1 \pmod{10}$, then $p | F_{p-1}$. If $p \equiv \pm 3 \pmod{10}$, then $p | F_{p+1}$. See also [14, p. 398]. Let (a/p) be the Legendere-Jacobi symbol. For $p \neq 2, 5$, using quadratic reciprocity law, we see that

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = 5^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } p \equiv \pm 1 \pmod{10}, \\ -1 & \text{if } p \equiv \pm 3 \pmod{10}. \end{cases}$$

Hence, for $p \neq 2$, we have $F_{p-(5/p)} \equiv 0 \pmod{p}$ and $F_{p-(5/p)}/p$ is a positive integer. Four different proofs of this fact have been given by G. H. Hardy and E. M. Wright [24], D. W. Robinson [49], J. H. Halton [22], and L. E. Somer [55]. The number $F_{p-(5/p)}/p$ is called the Fibonacci quotient.

Next, a positive integer $z(m)$ is called the rank of appearance (or also the rank of apparition) of Fibonacci sequence modulo m if it is the smallest positive integer such that $F_{z(m)} \equiv 0 \pmod{m}$. As has been pointed out by P. Ribenboim [48, p. 45], the term *"apparition"* stems from a bad translation of the French *"loi d'apparition"*, which means "law of appearance", not "law of apparition". The number $z(m)$ is also often called Fibonacci entry point or restricted period in the literature. Many interesting properties of $z(m)$ are known [22, 61, 62]. For example, if p is an odd prime and $z(p^2) \neq z(p)$, then $z(p^t) = p^{t-1} z(p)$ for all positive integers t. Moreover, we have $z(p) | p - (5/p)$ for any odd prime p. See [22, p. 223] or [61, p. 43].

The relationship of rank of appearance $z(m)$ to the period $k(m)$ is also well-known. D. D. Wall [65, p. 526] showed that $z(m) | k(m)$ and J. Vinson [61, p. 39] proved that, if p is an odd prime and t any positive integer, then

$$\begin{aligned} k(p^t) &= 4z(p^t) && \text{if} \quad z(p^t) \not\equiv 0 \pmod{2}, \\ k(p^t) &= z(p^t) && \text{if} \quad z(p^t) \equiv 2 \pmod{4}, \\ k(p^t) &= 2z(p^t) && \text{if} \quad z(p^t) \equiv 0 \pmod{4}. \end{aligned}$$

Combining the above properties [23, pp. 347–348], it can be shown that the following statements (i)-(v) are equivalent:

$$\text{(i) } k(p^2) = k(p), \quad \text{(ii) } z(p^2) = z(p), \quad \text{(iii) } F_{z(p)} \equiv 0 \pmod{p^2},$$

$$\text{(iv) } F_{p-(5/p)} \equiv 0 \pmod{p^2}, \quad \text{and} \quad \text{(v) } \mathrm{F_{p-1}F_{p+1}} \equiv 0 \pmod{\mathrm{p}^2}.$$

Unfortunately, there is no known way to resolve $F_{p-(5/p)} \pmod{p^2}$, other than through explicit computations. A detailed study of the Fibonacci quotient $F_{p-(5/p)}/p$ has yielded the following results:

In 1969, G. H. Andrews [2] proved the following, rather complicated, formulas for the Fibonacci quotient: If $p \equiv \pm 1 \pmod 5$, then

$$\frac{F_{p-1}}{p} \equiv 2(-1)^{\frac{p-1}{2}} \sum_{\substack{|m|<p \\ m \equiv 5,7 \ (\mathrm{mod}\ 10)}} \frac{\left(\frac{m+1}{5}\right)\left(\frac{-1}{m}\right)}{p-m} \pmod p$$

and, if $p \equiv \pm 2 \pmod 5$, then

$$\frac{F_{p+1}}{p} \equiv 2(-1)^{\frac{p-1}{2}} \sum_{\substack{|m|<p \\ m \equiv 1,5 \ (\mathrm{mod}\ 10)}} \frac{\left(\frac{m+1}{5}\right)\left(\frac{-1}{m}\right)}{p-m} \pmod p.$$

In 1982, H. C. Williams [70] showed that, if $p \neq 2, 5$ is an arbitrary prime and $[p/5]$ denotes the greatest integer not exceeding $p/5$, then

$$\frac{F_{p-(\frac{5}{p})}}{p} \equiv \frac{2}{5} \sum_{k=1}^{p-1-[p/5]} \frac{(-1)^k}{k} \pmod p.$$

In 1992, Z.-H. Sun and Z.-W. Sun [56, p. 381] proved for any $p \neq 2, 5$ the following simple and beautiful formula

$$\frac{F_{p-(\frac{5}{p})}}{p} \equiv -2 \sum_{\substack{k=1 \\ k \equiv 2p \ (\mathrm{mod}\ 5)}}^{p-1} \frac{1}{k} \equiv 2 \sum_{\substack{k=1 \\ 5|p+k}}^{p-1} \frac{1}{k} \pmod p.$$

In 1996, A. Granville and Z.-W. Sun also discovered an interesting connection of Fibonacci quotient with Bernoulli numbers. See [19, p. 135].

4. Ward's Last Theorem

In 1640, P. de Fermat stated that, if p is any prime and a is any integer not divisible by p, then $a^p - 1$ is divisible by p. See [14, p. 59]. The quotient $q_p(a) = (a^{p-1} - 1)/p$ is called the Fermat quotient of p with base a. Let $\Phi_n(x) = x + x^2/2 + \cdots + x^n/n$, and let p be an arbitrary odd prime greater then 5. Then,

$$F_{z(p)} \equiv 0 \pmod{p^2} \text{ if and only if } \Phi_{\frac{p-1}{2}}\left(\frac{5}{9}\right) \equiv 2q_p\left(\frac{3}{2}\right) \pmod p.$$

This statement is often called Ward's Last Theorem in honour of Morgan Ward (1901-1963). It was posed by the late brilliant mathematician in [66]. For a proof, see the paper by L. Carlitz [9] and, for an alternative proof, consult the papers by J. H. Halton [23] and J. E. Desmond [13]. Since $F_{z(p)} \equiv 0 \pmod{p^2}$ if and only if $k(p^2) = k(p)$, Ward yields a new equivalent condition to Wall's question.

5. Further Discoveries Related to Wall's Conjecture

In 1975, A. J. Vince [64] stated the following problem. Prove or disprove: if $m^2|F_n$, then $m|n$. In 1976, D. E. Penney and C. Pomerance [44] showed that Vince's statement is the equivalent to Wall's conjecture that $k(p^2) \neq k(p)$ for all primes p.

In 1998, S. Jakubec [27, p. 376] discovered the following connection of Wall's conjecture to cyclotomic fields: Let q be an odd prime and let l, p be primes such that $p = 2l + 1$, $l \equiv 3 \pmod 4$ and $p \equiv -5 \pmod q$. Suppose that the order of q modulo l is $(l-1)/2$. If q divides the class number of the real cyclotomic field $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$, then q is a Wall-Sun-Sun prime.

In 1999, Hua–Chieh Li [35, p. 83] showed that, if p is an odd prime satisfying $(5/p) = 1$ and α is a solution to $x^2 - x - 1 \equiv 0 \pmod p$, then $k(p^2) = k(p)$ if and only if $2\alpha^{p+1} - \alpha^p - \alpha^2 - 1 \equiv 0 \pmod{p^2}$. Next, if $p > 2$, $(5/p) = -1$ and α is a solution $x^2 - x - 1 \equiv 0 \pmod p$ in the ring $\mathbb{Z}[(1+\sqrt{5})/2]$ modulo p, then $k(p^2) = k(p)$ if and only if $2\alpha^{p^2+1} - \alpha^{p^2} - \alpha^2 - 1 \equiv 0 \pmod{p^2}$.

In 2006, V. Andrejič [1, p. 42] proved that, if $(L_n)_{n=0}^{\infty}$ is the Lucas sequence defined by $L_0 = 2$, $L_1 = 1$, and $L_{n+2} = L_{n+1} + L_n$ for all $n \geq 0$, then p is a Wall-Sun-Sun prime if and only if $L_p \equiv 1 \pmod{p^2}$. Next, by [1],

$$k(p^2) = k(p) \quad \text{if and only if} \quad \sum_{k=1}^{(p-1)/2} \frac{5^k - 1}{k} \equiv 0 \pmod p.$$

Furthermore, it is well known [49] that the Fibonacci numbers can be computed by taking powers of a matrix. Namely, if

$$F = \begin{bmatrix} F_0 & F_1 \\ F_1 & F_2 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \quad \text{then} \quad F^n = \begin{bmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{bmatrix}.$$

Let $Q_p = (F^{k(p)} - I)/p$, where I is a 2×2 identity matrix. In 2008, J. Klaška [28] proved that $k(p^2) = k(p)$ if and only if $Q_p \equiv 0 \pmod{p^2}$. Moreover, if $p \neq 5$, then $Q_p \equiv 0 \pmod{p^2}$ if and only if $\det Q_p \equiv 0 \pmod{p^2}$. Let K_p be the splitting field of $f(x) = x^2 - x - 1$ over the field of p-adic numbers $\mathbb{Q}_p$ and let α, β be the roots of $f(x)$ in K_p. Denote by O_p the ring of integers of K_p and, for a unit $\varepsilon \in O_p$, denote by $\mathrm{ord}_{p^t}(\varepsilon)$, $t \in \mathbb{N}$ the least positive rational integer h such that $\varepsilon^h \equiv 1 \pmod{p^t}$. If $p \neq 5$, then, by [28, p. 1244], $k(p^t) = \mathrm{lcm}(\mathrm{ord}_{p^t}(\alpha), \mathrm{ord}_{p^t}(\beta))$ for any $t \in \mathbb{N}$ and we have $k(p^2) \neq k(p)$ if and only if $\mathrm{ord}_{p^2}(\alpha) \equiv 0 \pmod p$ and $\mathrm{ord}_{p^2}(\beta) \equiv 0 \pmod p$. Furthermore, by [28, p. 1245] we have: if $p \neq 5$, $u \in O_p$ and $f(u) \equiv 0 \pmod p$, then $k(p^2) = k(p)$ if and only if $u^{2q} - u^q - 1 \equiv 0 \pmod{p^2}$.

Some further results related to Wall's conjecture can be found in [21, p. 208], [25, p. 117], [36, p. 348], and [50, p. 82].

6. Wall's Conjecture and Fibonacci Perfect Power Problem

The following interesting statement is closely related to Wall's question: The only perfect powers in the Fibonacci sequence are $F_0 = 0$, $F_1 = F_2 = 1$, $F_6 = 8$ and, $F_{12} = 144$. By definition, F_n is a perfect power if there exist integers x, q such that $q > 1$ and $F_n = x^q$. The first attempt to prove the theorem was made by F. Buchanan [6] in 1964. Unfortunately, the proof presented in [6] was incorrect being later retracted by the author [7]. A mistake in Buchanan's proof consists in the false assumption that a formula $z(p^t) = p^{t-1}z(p)$ holds for an arbitrary prime p. We have $z(p^t) = p^{t-1}z(p)$ only for p satisfying $z(p^2) \neq z(p)$. Hence, if $k(p^2) \neq k(p)$ for all primes p, then the only perfect powers in the Fibonacci sequence are $0, 1, 8$ and, 144. A complete solution of $F_n = x^q$ was given for $q = 2$ by J. H. E. Cohn [10, 11] and by O. Wyler [71], and for $q = 3$ by H. London and R. Finkelstein [37]. The solution for $q = 5$ was found by A. Pethö [45] and for $q = 5, 7, 11, 13, 17$ by McLaughlin [41]. In general, the statement that 0, 1, 8 and, 144 are the only positive perfect powers in the Fibonacci sequence was proved in 2006 by Y. Bugeaud, M. Mignotte, and S. Siksek [8]. An extensive list of references concerning the Fibonacci perfect powers can be found in [1, 8, 45] and, for short historical surveys, see [8, pp. 973–975] or [1, pp. 38–39].

7. Wall's Conjecture and Fermat's Last Theorem

Around 1637, Pierre de Fermat (1601–1665) stated that the Diophantine equation $x^n+y^n=z^n$ has no integer solution when $n>2$ and $x,y,z\neq 0$. This proposition is known as Fermat's Last Theorem. In a marginal note, Fermat claimed to have discovered a truly remarkable proof. However, all the greatest mathematicians tried to find such proof without success over 350 years. The first accepted proof of Fermat's Last Theorem was published in 1995 by A. Wiles and R. Taylor [59, 68]. An extensive history of this problem can be found, for example, in [47]. It is well known that a solution of Fermat's problem can be reduced to the case of $n=p$ being an odd prime. Traditionally, two cases are then considered: case one if $p\nmid xyz$ and case two otherwise.

A central role in the study of the first case of Fermat's Last Theorem is played by Fermat quotients [1] $q_p(a)$ and the congruence $q_p(a)\equiv 0 \pmod{p}$, which can be written equivalently as $a^{p-1}\equiv 1 \pmod{p^2}$. In 1909, A. Wieferich [67] proved that, if there exists a solution of Fermat's equation $x^p+y^p=z^p$ such that $p\nmid xyz$ where p is an odd prime, then $a^{p-1}\equiv 1 \pmod{p^2}$ holds for $a=2$. This implication is known as the Wieferich criterion and the primes p satisfying $2^{p-1}\equiv 1 \pmod{p^2}$ are called Wieferich primes. At present, only two Wieferich primes are known: 1093 was found by W. Meissner in 1913 and 3511 was found by N. Beeger in 1922. The Wieferich's result has been extended by many authors. See, for example, [18, 42, 57, 60]. The last result due to J. Suzuki [57] stated that, if there exists a prime p satisfying $x^p+y^p=z^p$ where $p\nmid xyz$, then $a^{p-1}\equiv 1 \pmod{p^2}$ for any prime $a\leq 113$.

The two following results connecting the first case of Fermat's Last Theorem with Wall's conjecture are known. In 1972, G. Brückner [5] stated that, if $k(p^2)\neq k(p)$ for all primes p, then the Diophantine equation $\alpha^p+\beta^p+\gamma^p=0$ has no solution in integers α, β, γ of $\mathbb{Q}(\sqrt{5})$ such that $(\gamma,p)=1$ and $\alpha=a_1+a_2\sqrt{5}$, $\beta=b_1+b_2\sqrt{5}$ satisfy the condition $a_1b_2-a_2b_1\not\equiv 0 \pmod{p}$. Brückner also stated that γ^p may be replaced by $\varepsilon\gamma^p$, where ε is a unit in $\mathbb{Q}(\sqrt{5})$.

In 1992, Z.-H. Sun and Z.-W. Sun [56] proved that, if $k(p^2)\neq k(p)$ for all primes p, then $x^p+y^p=z^p$ has no integer solution with $p\nmid xyz$. Hence, the affirmative answer to Wall's question implies the first case of Fermat's Last Theorem.

8. A Computer Search for Fibonacci-Wieferich Primes

In this section, we recall the most important historical milestones in a computer search for Fibonacci-Wieferich primes. First, D. D. Wall [65] showed that $k(p^2)\neq k(p)$ for any prime $p<10.000$. In [23], J. H. Halton claims that $k(p^2)\neq k(p)$ has been verified thanks to Wunderlich's computations for $p\leq 28.837$. D. E. Penney and C. Pomerance [44] inform us that $k(p^2)\neq k(p)$ for $p\leq 177.409$. In [16], L. A. G. Dresel verified that $k(p^2)\neq k(p)$ for $p<10^6$. According to H. C. Williams [70, 69], $k(p)\neq k(p^2)$ for every prime $p<10^9$. By P. L. Montgomery [43], there is no Fibonacci-Wieferich prime less then 2^{32}. From a search conducted by R. J. McIntosh [12, p. 447], we learn that there are no Fibonacci-Wieferich primes $p<2\times 10^{12}$. An extensive computer search by A.-S. Elsenhans and J. Jahnel [17] leads to an extension of the bound up to 10^{14}. According to a report by R. J. McIntosh and E. L. Roettger [40], $k(p^2)\neq k(p)$ for $p<2\times 10^{14}$. F. G. Dorais and D. Klyve [15] proved that there exists no Fibonacci-Wieferich prime $p<9.7\times 10^{14}$.

[1] Note that the connection of the first case of Fermat's Last Theorem with the Fermat quotients has been extensively studied by Ladislav Skula, a Czechoslovak mathematician. See [51, 53, 54, 52].

Next, in December 2011, a PrimeGrid project [46] was started searching for Fibonacci-Wieferich primes. In 2011-2016, PrimeGrid extended the search limit to 1.9×10^{17} without finding any such primes. Finally, note that some computational results have been verified retrospectively. For example in [4, p. 228] for $p < 100.000$ and in [3, p. 62] for $p < 10^8$. Our short historical survey is summarized in Table 1.

Year	Author	Search limit
1960	D. D. Wall	$p < 10,000$
1967	J. H. Halton	$p \leq 28,837$
1976	D. E. Penny, C. Pomerance	$p \leq 177,409$
1977	L. A. G. Dresel	$p < 10^6$
1982	H. C. Williams	$p < 10^9$
1993	P. L. Montgomery	$p < 4,294,967,296 = 2^{32}$
1997	R. J. McIntosh	$p < 2 \times 10^{12}$
2004	A.– S. Elsenhans, J. Jahnel	$p < 10^{14}$
2007	R. J. McIntosh, E. L. Roettger	$p < 2 \times 10^{14}$
2011	F. G. Dorais, D. Klyve	$p < 9.7 \times 10^{14}$
2012	PrimeGrid	$p < 6 \times 10^{15}$
2014	PrimeGrid	$p < 2.8 \times 10^{16}$
2015	PrimeGrid	$p < 1.2 \times 10^{17}$
2016	PrimeGrid	$p < 1.9 \times 10^{17}$

Table 1

The computer search for Fibonacci-Wieferich primes is also closely related to the following statistical considerations. By the heuristic argument [12, pp. 446–447] and [40, p. 2091], the number N of Fibonacci-Wieferich primes in an interval $[x, y]$ is expected to be

$$N = \sum_{x \leq p \leq y} \frac{1}{p} \approx \sum_{n=x}^{y} \frac{1}{n \ln n} \approx \int_x^y \frac{dt}{t \ln t} = \ln(\ln y) - \ln(\ln x).$$

On the other hand, using the arguments presented in [30, p. 23], we have

$$N = \sum_{x \leq p \leq y} \frac{1}{q}, \quad \text{where} \quad \begin{cases} q = p^2, & \text{if} \quad p \equiv 3, 7 \pmod{10}, \\ q = p, & \text{if} \quad p \equiv 1, 9 \pmod{10}. \end{cases}$$

The mild conflict of these two heuristics is reconciled by G. Grell and W. Peng [20].

9. Some Analogical Problems

Analogies to the equality $k(p^2) = k(p)$ have also been examined for other linear recurrence sequences. Let $K(m)$ be the period of $(G_n \bmod m)_{n=0}^{\infty}$ where $G_0 = 0$, $G_1 = 1$, and $G_{n+2} = aG_{n+1} + bG_n$ for all $n \geq 0$, i.e. $K(m)$ is the least positive integer satisfying $[G_{K(m)}, G_{K(m)+1}] \equiv [0, 1](\bmod m)$. For example, if $[a, b] = [2, 1]$, we get the Pell sequence. In this case, all primes

$p \leq 10^8$ for which $K(p^2) = K(p)$ are 13; 31; and $1,546,463$. See [69, p. 86]. In general, $K(p^t) = K(p)$ can also be true for $t > 2$. If $[a, b] = [5, 1]$, then $K(3^3) = K(3^2) = K(3) = 8$. Consult [63, p. 305].

Similarly, let us denote by $h(m)$ the period of $(T_n \mod m)_{n=0}^{\infty}$ where $T_0 = T_1 = 0$, $T_2 = 1$, and $T_{n+3} = T_{n+2} + T_{n+1} + T_n$, i.e. $h(m)$ is the least positive integer satisfying $[T_{h(m)}, T_{h(m)+1}, T_{h(m)+2}] \equiv [0, 0, 1](\mod m)$. A prime p is called Tribonacci-Wieferich [31] if $h(p^2) = h(p)$. By J. Klaška [29, p. 19], no Tribonacci-Wieferich prime exists below 10^{11}. Up to the present, no instance of $h(p^2) = h(p)$ has been found and it is an open question whether $h(p^2) = h(p)$ never appears. Finally, some results for Tetranacci-Wieferich primes are also known [31, p. 296].

10. Concluding Remarks

The long failure to find Wall-Sun-Sun primes supports the original conjecture of Donald Dines Wall, namely, that $k(p^2) \neq k(p)$ holds for all primes p. Therefore, the attention of the mathematicians should focus on finding a proof of this conjecture rather than on searching for a counterexample. However, it is evident that, until the proof of Wall's conjecture is found, the computer search for Wall-Sun-Sun primes will continue.

References

[1] V. Andrejič, *On Fibonacci powers*, Univ. Beograd. Publ. Elektroteh. Fak. Ser. Math., **17** (2006), 38–44.

[2] G. H. Andrews, *Some formulae for the Fibonacci sequence with generalizations*, The Fibonacci Quarterly, **7.2** (1969), 113–130.

[3] H. Aydin, R. Dikici, and G. C. Smith, *Wall and Vinson revisited*, Applications of Fibonacci Numbers, **5** (1993), 61–68.

[4] R. A. Bateman, E. A. Clark, M. L. Hancock, and C. A. Reiter, *The period of convergents modulo m of reduced quadratic irrationals*, The Fibonacci Quarterly, **29.3** (1991), 220–229.

[5] G. Brückner, *Die Fermatsche Vermutung über $Q(\sqrt{5})$ und die Fibonacci-Folge*, Math. Nachr., **52** (1972), 255–257.

[6] F. Buchanan, *N-th powers in the Fibonacci series*, Amer. Math. Monthly, **71** (1964), 647–649.

[7] F. Buchanan, *Retraction of "N-th powers in the Fibonacci series"*, Amer. Math. Monthly, **71** (1964), 1112.

[8] Y. Bugeaud, M. Mignotte, and S. Siksek, *Classical and modular approaches to exponential Diophantine equations I. Fibonacci and Lucas perfect powers*, Annals of Math., **163** (2006), 969–1018.

[9] L. Carlitz, *Solution of advanced problem* H-24, The Fibonacci Quarterly, **2.3** (1964), 205–207.

[10] J. H. E. Cohn, *On square Fibonacci numbers*, J. London Math. Soc., **39** (1964), 537–540.

[11] J. H. E. Cohn, *Square Fibonacci numbers, etc.*, The Fibonacci Quarterly, **2.2** (1964), 109–113.

[12] R. E. Crandall, K. Dilcher, and C. Pomerance, *A search for Wieferich and Wilson primes*, Math. Comp., **66** (1997), 433–449.

[13] J. E. Desmond, *On the equality of periods of different moduli in the Fibonacci sequence*, The Fibonacci Quarterly, **16.1** (1978), 86–87, 96.

[14] L. E. Dickson, *History of the Theory of Numbers*, Vol. I, Chelsea, New York, 1952.

[15] F. G. Dorais and D. Klyve, *A Wieferich prime search up to* 6.7×10^{15}, Journal of Integer Sequences, **14** (2011), Article 11.9.2.

[16] L. A. G. Dresel, *Letter to the editor*, The Fibonacci Quarterly, **15.4** (1977), 346.

[17] A.-S. Elsenhans and 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.

[18] A. Granville and M. B. Monagan, *The first case of Fermat's Last Theorem is true for all prime exponents up to* $714,591,416,091,389$, Trans. Amer. Math. Soc., **306** (1988), 329–359.

[19] A. Granville and Z.-W. Sun, *Values of Bernoulli polynomials*, Pacific J. Math., **172** (1996), 117–137.

[20] G. Grell and W. Peng, *Wall's conjecture and the ABC conjecture*, arXiv:1511.01210v1 [math. NT], (2015).

[21] Ch. Guo and A. Koch, *Bounds for Fibonacci period growth*, Involve, **2.2** (2009), 195–210.

[22] J. H. Halton, *On the divisibility properties of Fibonacci numbers*, The Fibonacci Quarterly, **4.3** (1966), 217–240.

[23] J. H. Halton, *Some properties associated with square Fibonacci numbers*, The Fibonacci Quarterly, **5.4** (1967), 347–355.
[24] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, Clarendon Press, Oxford, (1960), 148–150, 221–223.
[25] J. J. Heed, *Wieferichs and the problem $z(p^2) = z(p)$*, The Fibonacci Quarterly, **22.2** (1984), 116–118.
[26] V. E. Hoggatt and C. Smith, *Primitive periods of generalized Fibonacci sequences*, The Fibonacci Quarterly, **14.4** (1976), 343–347.
[27] S. Jakubec, *On divisibility of the class number h^+ of the real cyclotomic fields of prime degree l*, Math. Comp., **67** (1998), 369–398.
[28] J. Klaška, *Criteria for testing Wall's question*, Czechoslovak Math. Journal, **58.4** (2008), 1241–1246.
[29] J. Klaška, *A search for Tribonacci-Wieferich primes*, Acta Math. Univ. Ostrav, **16** (2008), 15–20.
[30] J. Klaška, *Short remark on Fibonacci-Wieferich primes*, Acta Math. Univ. Ostrav., **15** (2007), 21–25.
[31] J. Klaška, *On Tribonacci-Wieferich primes*, The Fibonacci Quarterly, **46/47.4** (2008/2009), 290–297.
[32] J. C. Kluyver, *Vraagstuk CXXXIX, CXL*, Wiskundige Opgaven, **14** (1928), 278–281.
[33] J. Knauer and J. Richstein, *The continuing search for Wieferich primes*, Math. Comp., **74** (2005), 1559–1563.
[34] J. L. Lagrange, *Oeuvres de LaGrange*, Vol. 7, §78-79, Gauthier Villars, Paris, 1877.
[35] H.-C. Li, *Fibonacci primitive roots and Wall's question*, The Fibonacci Quarterly, **37.1** (1999), 77–84.
[36] H.-C. Li, *On second-order linear recurrence sequences: Wall and Wyler revisited*, The Fibonacci Quarterly, **37.4** (1999), 342–349.
[37] H. London and R. Finkelstein, *On Fibonacci and Lucas numbers which are perfect powers*, The Fibonacci Quarterly, **7.5** (1969), 476–481 & 487 (errata ibid) **8.3** (1970), 248.
[38] E. Lucas, *Théorie des fonctions numériques simplement périodiques*, Amer. J. Math., **1** (1878), 184–240, 289–321.
[39] S. E. Mamangakis, *Remarks on the Fibonacci series modulo m*, Amer. Math. Monthly, **68** (1961), 648–649.
[40] R. J. McIntosh and E. L. Roettger, *A search for Fibonacci-Wieferich and Wolstenholme primes*, Math. Comp., **76** (2007), 2087–2094.
[41] J. McLaughlin, *Small prime powers in the Fibonacci sequence*, arXiv:math.NT/0110150v2, (2002).
[42] D. Mirimanoff, *Zum letzter Fermat'schen Theorem*, J. Reine Angew. Math., **139** (1911), 309–324.
[43] P. L. Montgomery, *New solutions of $a^{p-1} \equiv 1 \pmod{p^2}$*, Math. Comp., **61** (1993), 361–363.
[44] D. E. Penny and C. Pomerance, *Solution to problem* E 2539, Amer. Math. Monthly, **83** (1976), 742–743.
[45] A. Pethö, *Perfect powers in second order recurrences*, Topics in Classical Number Theory, **2** (Budapest 1981), 1217–1227.
[46] PrimeGrid, *Wall-Sun-Sun prime search*, `http://www.primegrid.com`.
[47] P. Ribenboim, 13 *Lectures on Fermat's Last Theorem*, Springer-Verlag, New York (1979).
[48] P. Ribenboim, *The Little Book of Big Primes*, Springer-Verlag, New York (1991).
[49] D. W. Robinson, *The Fibonacci matrix modulo m*, The Fibonacci Quarterly, **1.2** (1963), 29–36.
[50] A. Saha and C. S. Karthik, *A few equivalences of Wall-Sun-Sun prime conjecture*, International Journal of Mathematics & Applications, **4.1** (2011), 77–86.
[51] L. Skula, *A remark on Mirimanoff polynomials*, Commentarii Math. Univ. Sancti Pauli (Tokyo), **31** (1982), 89–97.
[52] L. Skula, *Fermat's Last Theorem and the Fermat quotients*, Commentarii Math. Univ. Sancti Pauli (Tokyo), **41** (1992), 35–54.
[53] L. Skula, *On the Kummer's system of congruences*, Commentarii Math. Univ. Sancti Pauli (Tokyo), **35** (1986), 137–163.
[54] L. Skula, *Some consequences of the Kummer system of congruences*, Commentarii Math. Univ. Sancti Pauli (Tokyo), **39** (1990), 19–40.
[55] L. E. Somer, *The Fibonacci group and a new proof that $F_{p-(5/p)} \equiv 0 \pmod{p}$*, The Fibonacci Quarterly, **10.4** (1972), 345–348, 354.
[56] Z.-H. Sun and Z.-W. Sun, *Fibonacci numbers and Fermat's Last Theorem*, Acta Arith., **60** (1992), 371–388.
[57] J. Suzuki, *On the generalized Wieferich criteria*, Proc. Japan Acad. Ser. A Math. Sci., **70** (1994), 230–234.
[58] S. Täcklind, *Über die Periodiziät der Lösungen von Differenzenkongruenzen*, Ark. Math. Astr. Fys., **30A.22** (1944), 1–9.
[59] R. L. Taylor and A. Wiles, *Ring theoretic properties of certain Hecke algebras*, Annals of Math., **141** (1995), 553–572.

[60] H. S. Vandiver, *Extension of the criteria of Wieferich and Mirimanoff in connection with Fermat's Last Theorem*, J. Reine Angew. Math., **144** (1914), 314–318.
[61] J. Vinson, *The relation of the period modulo m to the rank of apparition of m in the Fibonacci sequence*, The Fibonacci Quarterly, **1.2** (1963), 37–45.
[62] A. Vince, *The Fibonacci sequence modulo n*, The Fibonacci Quarterly, **16.5** (1978), 403–407.
[63] A. Vince, *Period of a linear recurrence*, Acta Arith., **39** (1981), 303–311.
[64] A. Vince, *Problem* E 2539, Amer. Math. Monthly, **82** (1975), p. 521.
[65] D. D. Wall, *Fibonacci series modulo m*, Amer. Math. Monthly, **67.6** (1960), 525–532.
[66] M. Ward, *Advanced problem* H-24, The Fibonacci Quarterly, **1.4** (1963), 47.
[67] A. Wieferich, *Zum letzten Fermat'schen Theorem*, J. Reine Angew. Math., **136.6** (1909), 293–302.
[68] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Annals of Math., **141** (1995), 443–551.
[69] H. C. Williams, *The influence of computers in the development of number theory*, Comput. Math. Appl., **8** (1982), 75–93.
[70] H. C. Williams, *A note on the Fibonacci quotient $F_{p-\varepsilon}/p$*, Canad. Math. Bull., **25.3** (1982), 366–370.
[71] O. Wyler, *Solution of advanced problem* 5080, Amer. Math. Monthly, **71** (1964), 220–222.
[72] C. C. Yalavigi, *A conjecture of J. H. Halton*, Math. Education, Ser. A, **4.4** (1970), 125–126.
[73] C. C. Yalavigi, *A note on remarks of S. E. Mamangakis*, Math. Stud., **34** (1966), 37.

MSC2010: 11B50, 11B39, 01A60, 97A30

Institute of Mathematics, Faculty of Mechanical Engineering, Brno University of Technology, Technická 2, 616 69 Brno, Czech Republic
E-mail address: klaska@fme.vutbr.cz