Jiří Klaška

Criteria for testing Wall's question

Czechoslovak Mathematical Journal, Vol. 58 (2008), No. 4, 1241–1246

Persistent URL: `http://dml.cz/dmlcz/140454`

Czechoslovak Mathematical Journal, 58 (133) (2008), 1241–1246

CRITERIA FOR TESTING WALL'S QUESTION

Jiří Klaška, Brno

(Received August 8, 2007)

Abstract. In this paper we find certain equivalent formulations of Wall's question and derive two interesting criteria that can be used to resolve this question for particular primes.

Keywords: Fibonacci numbers, Wall's question, Wall-Sun-Sun prime, Fibonacci-Wieferich prime, modular periodicity, periodic sequence

MSC 2010: 11B50, 11B39, 11A07

1. Introduction

In 1960, D. D. Wall published a well-known paper [6] concerning the modular periodicity of a Fibonacci sequence. In this paper an interesting problem was formulated, often referred to as Wall's question (see [6, p. 528]), which has remained unsolved up to the present. Let us outline this problem.

Let $(F_n)_{n=0}^{\infty}$ denote the Fibonacci sequence defined by $F_{n+2} = F_{n+1} + F_n$ with $F_0 = 0$, $F_1 = 1$. Let $m > 0$ be an arbitrary integer. Reducing F_n modulo m and taking the least nonnegative residues, we obtain the sequence $(F_n \bmod m)_{n=0}^{\infty}$, which is periodic. A positive integer $k(m)$ is called the period of the 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, Wall proved that, if $k(p) = k(p^s) \neq k(p^{s+1})$, then $k(p^t) = p^{t-s}k(p)$ for $t \geqslant s > 0$. Wall asked whether $k(p) = k(p^2)$ is possible. This is still an open question.

In [6] Wall noted that for $p < 10^4$, a counterexample of $k(p) \neq k(p^2)$ does not exist. According to [7], $k(p) \neq k(p^2)$ for $p < 10^9$. Using extensive search by computer, in [2] this result was extended to $p < 10^{14}$. Finally, according to the last report from 2007 (see [4]) there exists no such prime $p < 2 \times 10^{14}$. Finding the answer to Wall's question can be extremely difficult. In 1992, Zhi-Hong Sun and Zhi-Wei Sun [5] showed that, if $p \nmid xyz$ and $x^p + y^p = z^p$, then $k(p) = k(p^2)$. Consequently, an affirmative answer to Wall's question implies the first case of Fermat's last theorem.

It is well known that $k(p) = k(p^2)$ if and only if $F_{p-(5|p)} \equiv 0 \pmod{p^2}$ where $(a|b)$ denotes the Legendre symbol of a and b. Crandall, Dilcher, and Pomerance [1] called primes $p > 5$ satisfying $F_{p-(5|p)} \equiv 0 \pmod{p^2}$ the Wall-Sun-Sun primes. These are sometimes also called Fibonacci-Wieferich primes. See [4] for example. It has been conjectured that there are infinitely many Wall-Sun-Sun primes, but the conjecture remains unproven.

2. Wall's question and its equivalent formulations

It is well known that F_n can be computed by taking the powers of a matrix. Namely, if

$$F = \begin{bmatrix} F_0 & F_1 \\ F_1 & F_2 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \quad \text{then } F^n = \begin{bmatrix} F_{n-1} & F_n \\ F_n & F_{n+1} \end{bmatrix}. \tag{2.1}$$

Consequently, $k(p)$ is the period of $(F_n \bmod p)_{n=0}^{\infty}$ if and only if $k(p)$ is the smallest positive integer k for which $F^k \equiv E \pmod p$ and $k(p^2)$ is the period of $(F_n \bmod p^2)_{n=0}^{\infty}$ if and only if $k(p^2)$ is the smallest positive integer l satisfying $F^l \equiv E \pmod{p^2}$, where E is the 2×2 identity matrix. For any prime p, let us now define the integer matrix $A_p = [a_{ij}]$ such that

$$A_p = \frac{1}{p}(F^{k(p)} - E). \tag{2.2}$$

From (2.1) it follows that

$$A_p = \begin{bmatrix} a_{11} & a_{21} \\ a_{21} & a_{11} + a_{21} \end{bmatrix}. \tag{2.3}$$

Lemma 2.1. *For any prime p we have $k(p) \neq k(p^2)$ if and only if $A_p \not\equiv 0 \pmod p$.*

Proof. This follows from (2.2). ☐

Lemma 2.2. *Let $p \neq 5$. Then $A_p \equiv 0 \pmod p$ if and only if $\det A_p \equiv 0 \pmod p$.*

Proof. Let $p \neq 2$. Put $k = k(p)$. From (2.2) and (2.3) it follows that

$$\det F^k = 1 + p(2a_{11} + a_{21}) + p^2 \det A_p \quad \text{where } \det A_p = a_{11}^2 + a_{11}a_{21} - a_{21}^2. \tag{2.4}$$

Since $\det F = -1$, (2.4) implies $2a_{11} + a_{21} \equiv 0 \pmod p$ and $\det A_p \equiv -5a_{11}^2 \pmod p$. Consequently, we have $a_{11} \equiv 0 \pmod p$ if and only if $a_{21} \equiv 0 \pmod p$, and thus, $\det A_p \equiv 0 \pmod p$ implies $A_p \equiv 0 \pmod p$. The validity of the converse implication is evident. On the other hand, for $p = 2$ we can easily verify that $A_2 \not\equiv 0 \pmod 2$ and $\det A_2 \not\equiv 0 \pmod 2$. ☐

Remark 2.3. For $p = 5$ we have $A_5 \not\equiv 0 \pmod 5$ and $\det A_5 \equiv 0 \pmod 5$.

Our next considerations will take place in the following framework. Let L_p be the splitting field of the Fibonacci characteristic polynomial $f(x) = x^2 - x - 1$ over the field of p-adic numbers $\mathbb{Q}_p$ and let α, β be the roots of $f(x)$ in L_p. Denote by O_p the ring of integers of L_p. Clearly $\alpha, \beta \in O_p$. Since 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. Moreover, if $L_p = \mathbb{Q}_p$, then $\alpha, \beta \in \mathbb{Z}_p$, where $\mathbb{Z}_p$ is the ring of p-adic integers.

For a unit $\varepsilon \in O_p$ we denote by $\operatorname{ord}_{p^t}(\varepsilon)$ the least positive rational integer h such that $\varepsilon^h \equiv 1 \pmod{p^t}$. Since $\varepsilon^h \equiv 1 \pmod p$ implies $\varepsilon^{ph} \equiv 1 \pmod{p^2}$, we have

$$\text{either} \quad \operatorname{ord}_{p^2}(\varepsilon) = \operatorname{ord}_p(\varepsilon) \quad \text{or} \quad \operatorname{ord}_{p^2}(\varepsilon) = p \cdot \operatorname{ord}_p(\varepsilon). \tag{2.5}$$

Furthermore, it is not difficult to prove that if $p > 2$ and $\operatorname{ord}_p(\varepsilon) \neq \operatorname{ord}_{p^2}(\varepsilon)$, then for any $t \in \mathbb{N}$ we have $\operatorname{ord}_{p^t}(\varepsilon) = p^{t-1} \operatorname{ord}_p(\varepsilon)$. More generally, if $\varepsilon \neq \pm 1$ and $s \in \mathbb{N}$ is the largest integer such that $\operatorname{ord}_{p^s}(\varepsilon) = \operatorname{ord}_p(\varepsilon)$, then for any $t \geqslant s$, we have $\operatorname{ord}_{p^t}(\varepsilon) = p^{t-s} \operatorname{ord}_p(\varepsilon)$.

Lemma 2.4. *Let $p \neq 5$. We have either $\operatorname{ord}_{p^t}(\alpha) = \operatorname{ord}_{p^t}(\beta)$ or $\operatorname{ord}_{p^t}(\alpha) = 2\operatorname{ord}_{p^t}(\beta)$ or $2\operatorname{ord}_{p^t}(\alpha) = \operatorname{ord}_{p^t}(\beta)$.*

Proof. From Viète's equation $\alpha\beta = -1$ in L_p it follows that $\alpha = \pm 1$ if and only if $\beta = \pm 1$. Hence, if $\alpha^r = 1$, then $\beta^r = \pm 1$, and consequently, $\beta^{2r} = 1$. This implies $\operatorname{ord}_{p^t}(\beta) \mid 2\operatorname{ord}_{p^t}(\alpha)$. By analogy, we can obtain $\operatorname{ord}_{p^t}(\alpha) \mid 2\operatorname{ord}_{p^t}(\beta)$. $\square$

Corollary 2.5. *For any prime $p \neq 5$ we have*

$$\operatorname{ord}_{p^2}(\alpha) \equiv 0 \pmod p \quad \textit{if and only if} \quad \operatorname{ord}_{p^2}(\beta) \equiv 0 \pmod p. \tag{2.6}$$

Proof. This is a consequence of Lemma 2.4 if $p \neq 2$. For $p = 2$, the polynomial $f(x)$ is irreducible over $\mathbb{Q}_2$ and so $\operatorname{ord}_{2^t}(\alpha) = \operatorname{ord}_{2^t}(\beta)$. $\square$

In Theorem 2.6 we generalize [3, Lemma 2.4] also to the case of $f(x)$ being irreducible over $\mathbb{Q}_p$.

Theorem 2.6. *Let $p \neq 5$. Then $k(p^t) = \mathrm{lcm}(\mathrm{ord}_{p^t}(\alpha),\ \mathrm{ord}_{p^t}(\beta))$ for any $t \in \mathbb{N}$.*

Proof. Over L_p we can write $F_n = A\alpha^n + B\beta^n$ for suitable $A, B \in L_p$. The coefficients A, B are uniquely determined by the equations $A + B = 0$ and $A\alpha + B\beta = 1$ over L_p. The determinant of the matrix of this system is equal to $\beta - \alpha$. As $\alpha \not\equiv \beta \pmod p$, the Cramer rule gives $A = -(\beta-\alpha)^{-1}$, $B = (\beta-\alpha)^{-1}$. Moreover, A, B are units in O_p. Let $k = k(p^t)$. Then $[A\alpha^k + B\beta^k, A\alpha^{k+1} + B\beta^{k+1}] \equiv [A + B, A\alpha + B\beta] \pmod{p^t}$. This system can be reduced to an equivalent form

$$\begin{bmatrix} 1 & 1 \\ \alpha & \beta \end{bmatrix} \begin{bmatrix} A(\alpha^k - 1) \\ B(\beta^k - 1) \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 0 \end{bmatrix} \pmod{p^t}. \tag{2.7}$$

As the determinant of the matrix in (2.7) is not divisible by p, (2.7) has only one solution

$$A(\alpha^k - 1) \equiv 0 \pmod{p^t}, \quad B(\beta^k - 1) \equiv 0 \pmod{p^t}.$$

This implies $\alpha^k \equiv 1 \pmod{p^t}$ and $\beta^k \equiv 1 \pmod{p^t}$. Thus, we have $\mathrm{ord}_{p^t}(\alpha) \mid k$ and $\mathrm{ord}_{p^t}(\beta) \mid k$, which implies $\mathrm{lcm}(\mathrm{ord}_{p^t}(\alpha),\ \mathrm{ord}_{p^t}(\beta)) \mid k$. As A, B are not divisible by p, the periods of the sequences $(A\alpha^n \bmod p^t)_{n=0}^{\infty}$ and $(B\beta^n \bmod p^t)_{n=0}^{\infty}$ are $\mathrm{ord}_{p^t}(\alpha)$ and $\mathrm{ord}_{p^t}(\beta)$. Consequently, the period k of $(A\alpha^n + B\beta^n \bmod p^t)_{n=0}^{\infty}$ divides $\mathrm{lcm}(\mathrm{ord}_{p^t}(\alpha), \mathrm{ord}_{p^t}(\beta))$ and the theorem follows. $\square$

Theorem 2.7. *Let $p \neq 5$. Then $k(p) \neq k(p^2)$ if and only if*

$$\mathrm{ord}_{p^2}(\alpha) \equiv 0 \pmod p \quad \textit{and} \quad \mathrm{ord}_{p^2}(\beta) \equiv 0 \pmod p. \tag{2.8}$$

Proof. It follows from (2.8) that $\mathrm{lcm}(\mathrm{ord}_{p^2}(\alpha), \mathrm{ord}_{p^2}(\beta)) \equiv 0 \pmod p$ and, by Theorem 2.6, we have $k(p^2) \equiv 0 \pmod p$. Using Theorem 2.6 for $t = 1$ and recalling that (p) is the maximal ideal of O_p, we have $k(p) \not\equiv 0 \pmod p$, which together with $k(p^2) \equiv 0 \pmod p$, gives $k(p) \neq k(p^2)$.

Conversely, if $k(p) \neq k(p^2)$, then $k(p^2) = p \cdot k(p)$. From Theorem 2.6 it now follows that $\mathrm{lcm}(\mathrm{ord}_{p^2}(\alpha), \mathrm{ord}_{p^2}(\beta)) \equiv 0 \pmod p$. This implies that $\mathrm{ord}_{p^2}(\alpha) \equiv 0 \pmod p$ or $\mathrm{ord}_{p^2}(\beta) \equiv 0 \pmod p$, which together with (2.6) proves (2.8). $\square$

Remark 2.8. If $p = 5$, then $k(p) \neq k(p^2)$ and $k(5^t) = 4 \cdot 5^t$ for any $t \in \mathbb{N}$. See [6].

Our results can be summarized in the following theorem.

Theorem 2.9. *Let $p \neq 5$ and let s be the number of roots α, β of $f(x)$ in O_p whose order modulo p^2 is divisible by p. Then there are the following possibilities:*

Case $s = 0$: $k(p) = k(p^2)$, or equivalently $A_p \equiv 0 \pmod{p}$.

Case $s = 1$: This case is impossible.

Case $s = 2$: $k(p) \neq k(p^2)$, or equivalently $\det A_p \not\equiv 0 \pmod{p}$.

Proof. By Theorem 2.6 we have that $s = 0$ if and only if $k(p) = k(p^2)$. Lemma 2.1 states that $k(p) = k(p^2)$ if and only if $A_p \equiv 0 \pmod{p}$, which is equivalent to $\det A_p \equiv 0 \pmod{p}$ by Lemma 2.2. By Corollary 2.5 we see that the case of $k = 1$ is impossible. The proof is complete. □

Our results reduce Wall's question to solving the following equivalent problem. Is there at least one root $\alpha \in O_p$ of $f(x)$ for which $\operatorname{ord}_{p^2}(\alpha) \not\equiv 0 \pmod{p}$ or is this never possible?

Now we derive two interesting criteria that can be used, without computing the roots of $f(x)$ in O_p, to decide whether $k(p) = k(p^2)$ or not. Let $p \neq 5$. 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. If $f(x)$ is not irreducible over $\mathbb{Q}_p$, then $f(x)$ has both roots in the ring $\mathbb{Z}_p$ and $O_p/(p)$ is a field with p elements. For the proof of our criteria, we shall need the following lemma.

Lemma 2.10. *We have $\operatorname{ord}_{p^2}(\alpha) \not\equiv 0 \pmod{p}$ if and only if $\alpha^{q-1} \equiv 1 \pmod{p^2}$.*

Proof. Put $s = \operatorname{ord}_{p^2}(\alpha)$. Clearly, $[O_p/(p^2)]^\times$ has $q(q-1)$ elements and so $s \mid q(q-1)$. Let $p \nmid s$. As $q = p^t$, we have $s \mid q-1$, and $\alpha^{q-1} \equiv 1 \pmod{p^2}$ follows. On the other hand, let $\alpha^{q-1} \equiv 1 \pmod{p^2}$. Then $s \mid q-1$. As $p \nmid q-1$, we have $\operatorname{ord}_{p^2}(\alpha) \not\equiv 0 \pmod{p}$. □

Theorem 2.11. *Let $p \neq 5$, $u \in O_p$ be such that $f(u) \equiv 0 \pmod{p}$. Then $k(p) = k(p^2)$ if and only if*

$$u^{2q} - u^q - 1 \equiv 0 \pmod{p^2}, \tag{2.9}$$

or equivalently

$$f(u) + (u^q - u)f'(u) \equiv 0 \pmod{p^2}, \tag{2.10}$$

where f' is the derivative of the Fibonacci characteristic polynomial f.

Proof. Let $u \in O_p$, $u^2 - u - 1 \equiv 0 \pmod{p}$. Then we have $u \equiv \alpha \pmod{p}$ or $u \equiv \beta \pmod{p}$. We can assume $u \equiv \alpha \pmod{p}$. Then $u^q \equiv \alpha^q \pmod{p^2}$. If $k(p) = k(p^2)$, then $u^q \equiv \alpha^q \equiv \alpha \pmod{p^2}$ and $u^{2q} - u^q - 1 \equiv \alpha^2 - \alpha - 1 = 0 \pmod{p^2}$.

On the other hand, assume $u^{2q} - u^q - 1 \equiv 0 \pmod{p^2}$. Let $u^q = \alpha + pv$. Then $(\alpha + pv)^2 - (\alpha + pv) - 1 \equiv pv(2\alpha - 1) \equiv 0 \pmod{p^2}$. Now $p \neq 5$ implies $2\alpha - 1 \not\equiv 0 \pmod{p}$ and so $v \equiv 0 \pmod{p}$. Consequently, $u^q \equiv \alpha \pmod{p^2}$ and $\alpha^{q-1} \equiv u^{q(q-1)} \equiv 1 \pmod{p^2}$. This, together with Lemma 2.10, yields $\mathrm{ord}_{p^2}(\alpha) \not\equiv 0 \pmod{p}$ and $k(p) = k(p^2)$ follows by Theorem 2.7 and Corollary 2.5.

Furthermore, let $u = \alpha + pw$. Then (2.10) is equivalent to

$$(\alpha^q - \alpha)(2\alpha + 2pw - 1) \equiv 0 \pmod{p^2}. \tag{2.11}$$

If $k(p) = k(p^2)$, then $\alpha^q \equiv \alpha \pmod{p^2}$ and (2.11) follows.

Conversely, assume (2.11). As $p \neq 5$, we have $2\alpha + 2pw - 1 \equiv 2u - 1 \equiv f'(\alpha) \not\equiv 0 \pmod{p}$. Consequently, (2.11) gives $\alpha^q - \alpha \equiv 0 \pmod{p^2}$. This, together with Lemma 2.10, implies $k(p) = k(p^2)$ as required. □

References

[1] *R. Crandall, K. Dilcher and C. Pomerance*: A search for Wieferich and Wilson primes. Math. Comp. *66* (1997), 443–449.
[2] *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.
[3] *H. Ch. Li*: Fibonacci primitive roots and Wall's question. Fibonacci Quart. *37* (1999), 77–84.
[4] *R. J. McIntosh and E. L. Roettger*: A search for Fibonacci-Wieferich and Wolstenholme primes. Math. Comp. *76* (2007), 2087–2094.
[5] *Z.-H. Sun and Z.-W. Sun*: Fibonacci numbers and Fermat's Last Theorem. Acta Arith. *60* (1992), 371–388.
[6] *D. D. Wall*: Fibonacci series modulo m. Amer. Math. Monthly *67* (1960), no. 6, 525–532.
[7] *H. C. Williams*: A Note on the Fibonacci quotient $F_{p-\varepsilon}/p$. Canad. Math. Bull. *25* (1982), 366–370.

Author's address: Jiří Klaška, Department of Mathematics, Brno University of Technology, Technická 2, 616 69 Brno, Czech Republic, e-mail: klaska@fme.vutbr.cz.