ON TRIBONACCI-WIEFERICH PRIMES

JIŘÍ KLAŠKA

ABSTRACT. The problem of the existence of Fibonacci-Wieferich primes has already been investigated by many authors. In this paper we shall study a similar problem for the sequence of Tribonacci numbers. Using matrix algebra, we find certain equivalent formulations of this problem and also derive some criteria that can be used to effectively test particular primes. A computer search showed that the problem has no solution for primes $p \leq 10^9$.

1. INTRODUCTION

Let $(F_n)_{n=0}^{\infty}$ be the Fibonacci sequence defined by $F_{n+2} = F_{n+1} + F_n$ with $F_0 = 0$ and $F_1 = 1$. It is well-known [9, p. 525] that $(F_n \bmod m)_{n=0}^{\infty}$ is periodic for any modulus $m > 1$. Let $k(m)$ denote the period of $(F_n \bmod m)_{n=0}^{\infty}$. That is, $k(m)$ is the least positive integer such that $F_{k(m)} \equiv 0$ and $F_{k(m)+1} \equiv 1 \pmod m$. In 1960, D. D. Wall [9, Theorem 5] proved that for any prime p, we have: 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 [9, p. 528] asked whether $k(p) = k(p^2)$ is always impossible. This problem has not yet been resolved. The primes p satisfying the relation $k(p) = k(p^2)$ are often referred to as Wall-Sun-Sun primes [1] or as Fibonacci-Wieferich primes [5].

Finding an answer to Wall's question can be extremely difficult. In 1992, Zhi-Hong Sun and Zhi-Wei Sun [6] 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. From this point of view, there is a similarity to the well-known Wieferich primes. Recall that an odd prime p is called Wieferich if $2^{p-1} \equiv 1 \pmod{p^2}$. In 1909, A. Wieferich [10] proved that, if $p \nmid xyz$ and $x^p + y^p = z^p$, then $2^{p-1} \equiv 1 \pmod{p^2}$. The only Wieferich primes known are 1093 and 3511; this has been verified up to 1.25×10^{15} [3].

In this paper we focus on a similar problem related to the Tribonacci sequence. Recall that the Tribonacci sequence $(T_n)_{n=0}^{\infty}$ is defined by $T_{n+3} = T_{n+2} + T_{n+1} + T_n$ with $T_0 = 0$, $T_1 = 0, T_2 = 1$. It is well-known [8, Theorem 1] that $(T_n \bmod m)_{n=0}^{\infty}$ is periodic. Let $h(m)$ denote the period of $(T_n \bmod m)_{n=0}^{\infty}$. In [8, pp. 349–351], M. E. Waddill proved that, if $h(p) = h(p^s) \neq h(p^{s+1})$, then $h(p^t) = p^{t-s}h(p)$ for $t \geq s$. By analogy with the Fibonacci case, the primes p satisfying $h(p) = h(p^2)$ may be called Tribonacci-Wieferich primes. Up to the present, no instance of $h(p) = h(p^2)$ has been found, and it is an open question whether $h(p) = h(p^2)$ never appears.

2. MATRIX CHARACTERIZATION OF $h(p) = h(p^2)$

The Tribonacci numbers T_n can be computed by taking the powers of the Tribonacci companion matrix T. If

$$T = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}, \quad \text{then} \quad T^n = \begin{bmatrix} T_{n-1} & T_{n-2}+T_{n-1} & T_n \\ T_n & T_{n-1}+T_n & T_{n+1} \\ T_{n+1} & T_n+T_{n+1} & T_{n+2} \end{bmatrix} \quad \text{for } n > 1. \tag{2.1}$$

Clearly, $h(p)$ is the period of $(T_n \bmod p)_{n=0}^{\infty}$ if and only if $h(p)$ is the smallest positive integer h for which $T^h \equiv E \pmod p$ and $h(p^2)$ is the period of $(T_n \bmod p^2)_{n=0}^{\infty}$ if and only if $h(p^2)$ is the smallest positive integer k satisfying $T^k \equiv E \pmod{p^2}$ where E is the 3×3 identity matrix. For any prime p we define an integer matrix $A_p = [a_{ij}]$ such that

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

From (2.1) it follows now that

$$A_p = \begin{bmatrix} a_{11} & a_{31}-a_{21} & a_{21} \\ a_{21} & a_{11}+a_{21} & a_{31} \\ a_{31} & a_{21}+a_{31} & a_{11}+a_{21}+a_{31} \end{bmatrix}. \tag{2.3}$$

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

Proof. This follows from (2.2). □

Lemma 2.2. *For any prime p, the elements a_{11}, a_{21}, a_{31} in (2.3) satisfy*

$$3a_{11} + 2a_{21} + a_{31} \equiv 0 \pmod p. \tag{2.4}$$

Proof. From (2.2) and (2.3), we obtain that

$$\det T^{h(p)} \equiv 1 + p(3a_{11} + 2a_{21} + a_{31}) \pmod{p^2}$$

and the lemma follows from $\det T = 1$. □

From (2.3) and (2.4) it follows that the elements of $A_p \bmod p$ can be expressed by means of a_{11}, a_{21} alone. Of course, if $A_p \equiv 0 \pmod p$, then $\det A_p \equiv 0 \pmod p$. On the other hand, we have the following proposition.

Proposition 2.3. *Let $p \neq 2$. If $\det A_p \equiv 0 \pmod p$ and $A_p \not\equiv 0 \pmod p$, then there is an $\varepsilon \in \mathbb{Z}$ such that*

$$7\varepsilon^3 + 29\varepsilon^2 + 39\varepsilon + 19 \equiv 0 \pmod p \quad \textit{and} \quad a_{21} \equiv a_{11}\varepsilon \pmod p.$$

Proof. Using (2.3) and (2.4), we obtain after some simplification

$$\det A_p \equiv -(38a_{11}^3 + 78a_{11}^2a_{21} + 58a_{11}a_{21}^2 + 14a_{21}^3) \pmod p. \tag{2.5}$$

Suppose $p|a_{11}$ and $p \nmid a_{21}$. Then from (2.5) we have $\det A_p \equiv -14a_{21}^3 \pmod p$ and thus $14 \equiv 0 \pmod p$. As $p \neq 2$, we have $p = 7$. We can verify that $h(7) = 48$. Then, for A_7, we have

$$A_7 = \frac{1}{7}(T^{48} - E) \equiv \begin{bmatrix} 4 & 2 & 0 \\ 0 & 4 & 2 \\ 2 & 2 & 6 \end{bmatrix} \pmod 7.$$

Hence, $a_{11} \equiv 4 \pmod 7$, which is a contradiction to $p|a_{11}$. Consequently, there is an $\varepsilon \in \mathbb{Z}$ such that $a_{21} \equiv a_{11}\varepsilon \pmod p$. From (2.5) it now follows that

$$\det A_p \equiv -a_{11}^3(14\varepsilon^3 + 58\varepsilon^2 + 78\varepsilon + 38) \pmod p. \tag{2.6}$$

Since $p \nmid a_{11}$, $p \neq 2$ and $p|\det A_p$, it follows from (2.6) that

$$7\varepsilon^3 + 29\varepsilon^2 + 39\varepsilon + 19 \equiv 0 \pmod{p}.$$

□

Let L_p be the splitting field of the Tribonacci characteristic polynomial $t(x) = x^3 - x^2 - x - 1$ over the field of p-adic numbers $\mathbb{Q}_p$ and let α, β, γ be the roots of $t(x)$ in L_p. Clearly, α, β, γ are in the ring O_p of integers of the field L_p. By a simple calculation we find that the discriminant of $t(x)$ is $\triangle t(x) = -44$. See also [7, p. 310]. This implies that $L_p/\mathbb{Q}_p$ does not ramify for $p \neq 2, 11$ and so the maximal ideal of O_p is generated by p. Finally, for a unit $u \in O_p$, we denote by $\mathrm{ord}_{p^t}(u)$ the least positive rational integer k such that $u^k \equiv 1 (\mathrm{mod}\ p^t)$. As $u^k \equiv 1 \pmod{p}$ implies $u^{pk} \equiv 1 \pmod{p^2}$, we have either $\mathrm{ord}_{p^2}(u) = \mathrm{ord}_p(u)$ or $\mathrm{ord}_{p^2}(u) = p \cdot \mathrm{ord}_p(u)$.

Theorem 2.4. *Let $p \neq 2, 11$. Then, for any $t \in \mathbb{N}$, we have*

$$h(p^t) = \mathrm{lcm}(\mathrm{ord}_{p^t}(\alpha), \mathrm{ord}_{p^t}(\beta), \mathrm{ord}_{p^t}(\gamma)). \tag{2.7}$$

Proof. Over L_p, we can write $T_n = A\alpha^n + B\beta^n + C\gamma^n$ for suitable $A, B, C \in L_p$. The coefficients A, B, C are uniquely determined by the system of equations $A + B + C = 0$, $A\alpha + B\beta + C\gamma = 0$ and $A\alpha^2 + B\beta^2 + C\gamma^2 = 1$ over L_p. The determinant of the matrix of this system is equal to $(\alpha - \beta)(\alpha - \gamma)(\gamma - \beta)$. As $\alpha \not\equiv \beta (\mathrm{mod}\ p)$, $\alpha \not\equiv \gamma (\mathrm{mod}\ p)$ and $\beta \not\equiv \gamma (\mathrm{mod}\ p)$, Cramer's rule gives $A = [(\alpha - \beta)(\alpha - \gamma)]^{-1}$, $B = [(\alpha - \beta)(\gamma - \beta)]^{-1}$, $C = -[(\alpha - \gamma)(\gamma - \beta)]^{-1}$. Moreover, A, B, C are units in O_p. Let $k = h(p^t)$. Then $[A\alpha^k + B\beta^k + C\gamma^k, A\alpha^{k+1} + B\beta^{k+1} + C\gamma^{k+1}, A\alpha^{k+2} + B\beta^{k+2} + C\gamma^{k+2}] \equiv [A + B + C, A\alpha + B\beta + C\gamma, A\alpha^2 + B\beta^2 + C\gamma^2] (\mathrm{mod}\ p^t)$. This system can be reduced to the equivalent form

$$\begin{bmatrix} 1 & 1 & 1 \\ \alpha & \beta & \gamma \\ \alpha^2 & \beta^2 & \gamma^2 \end{bmatrix} \begin{bmatrix} A(\alpha^k - 1) \\ B(\beta^k - 1) \\ C(\gamma^k - 1) \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} (\mathrm{mod}\ p^t). \tag{2.8}$$

As the determinant of the matrix in (2.8) is not divisible by p, (2.8) has only one solution

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

This implies $\alpha^k \equiv 1 \pmod{p^t}$, $\beta^k \equiv 1 \pmod{p^t}$ and $\gamma^k \equiv 1 \pmod{p^t}$. Thus, we have $\mathrm{ord}_{p^t}(\alpha) | k$, $\mathrm{ord}_{p^t}(\beta) | k$ and $\mathrm{ord}_{p^t}(\gamma) | k$, which implies

$$\mathrm{lcm}(\mathrm{ord}_{p^t}(\alpha), \mathrm{ord}_{p^t}(\beta), \mathrm{ord}_{p^t}(\gamma)) | k.$$

As A, B, C are not divisible by p, the periods of $(A\alpha^n \bmod p^t)_{n=0}^{\infty}$, $(B\beta^n \bmod p^t)_{n=0}^{\infty}$ and $(C\gamma^n \bmod p^t)_{n=0}^{\infty}$ are $\mathrm{ord}_{p^t}(\alpha)$, $\mathrm{ord}_{p^t}(\beta)$ and $\mathrm{ord}_{p^t}(\gamma)$. Consequently, the period k of $(A\alpha^n + B\beta^n + C\gamma^n \bmod p^t)_{n=0}^{\infty}$ divides $\mathrm{lcm}(\mathrm{ord}_{p^t}(\alpha), \mathrm{ord}_{p^t}(\beta), \mathrm{ord}_{p^t}(\gamma))$ and the theorem follows. □

Remark 2.5. *If $p \neq 2, 11$ then $O_p/(p)$ is the field with $p^{[L_p:\mathbb{Q}_p]}$ elements where $[L_p : \mathbb{Q}_p] \in \{1, 2, 3\}$. Thus, for any $\lambda \in \{\alpha, \beta, \gamma\}$, $\mathrm{ord}_p(\lambda) | p^{[L_p:\mathbb{Q}_p]} - 1$, and by (2.7), we have $h(p) | p^{[L_p:\mathbb{Q}_p]} - 1$. This implies that, for any prime $p \neq 2, 11$, $h(p) \not\equiv 0 \pmod{p}$. If $p = 2, 11$, then $h(p) \equiv 0 \pmod{p}$. Exactly, $h(2^t) = 2^{t+1}$ and $h(11^t) = 10 \cdot 11^t$ for any $t \in \mathbb{N}$.*

Lemma 2.6. *For any prime $p \neq 2, 11$, we have $A_p \equiv 0 \pmod{p}$ if and only if $\mathrm{ord}_{p^2}(\lambda) \not\equiv 0 \pmod{p}$ for each $\lambda \in \{\alpha, \beta, \gamma\}$.*

Proof. From Lemma 2.1 it follows that $A_p \equiv 0 \pmod{p}$ if and only if $h(p) = h(p^2)$. As $p \neq 2, 11$, by Remark 2.5, we have $p \nmid h(p)$, which, together with (2.7), yields $h(p) = h(p^2)$ if and only if $\operatorname{lcm}(\operatorname{ord}_{p^2}(\alpha), \operatorname{ord}_{p^2}(\beta), \operatorname{ord}_{p^2}(\gamma)) \not\equiv 0 \pmod{p}$. □

Lemma 2.7. *Let $p \neq 2, 11$. Then $\operatorname{lcm}(\operatorname{ord}_{p^t}(\alpha), \operatorname{ord}_{p^t}(\beta)) = \operatorname{lcm}(\operatorname{ord}_{p^t}(\alpha), \operatorname{ord}_{p^t}(\gamma)) = \operatorname{lcm}(\operatorname{ord}_{p^t}(\beta), \operatorname{ord}_{p^t}(\gamma)) = \operatorname{lcm}(\operatorname{ord}_{p^t}(\alpha), \operatorname{ord}_{p^t}(\beta), \operatorname{ord}_{p^t}(\gamma))$ for any $t \in \mathbb{N}$.*

Proof. This follows from the Viète equation $\alpha\beta\gamma = 1$. □

Theorem 2.8. *Let $p \neq 2, 11$ and $A_p \not\equiv 0 \pmod{p}$. Then $\det A_p \equiv 0 \pmod{p}$ if and only if there is a unique $\lambda \in \{\alpha, \beta, \gamma\}$ for which $\operatorname{ord}_{p^2}(\lambda) \not\equiv 0 \pmod{p}$. Moreover, for this λ, we have $\lambda \in \mathbb{Z}_p$ where $\mathbb{Z}_p$ is the ring of p-adic integers.*

Proof. Over the field L_p, the Tribonacci matrix T is similar to the diagonal matrix D with α, β, γ on the diagonal. Thus, an invertible matrix H exists such that $T = HDH^{-1}$ and thus $T^h = HD^hH^{-1}$ where $h = h(p)$. On the other hand, $T^h = E + pA_p$ where $A_p \not\equiv 0 \pmod{p}$. If we combine these two expressions, we have $E + pA_p = HD^hH^{-1}$, which implies $pH^{-1}A_pH = D^h - E$. By the well-known properties of determinants, we easily obtain that

$$p^3 \cdot \det A_p = (\alpha^h - 1)(\beta^h - 1)(\gamma^h - 1). \tag{2.9}$$

Let $\det A_p \equiv 0 \pmod{p}$. From (2.7) and (2.9), it now follows that at least one of the differences $\alpha^h - 1, \beta^h - 1, \gamma^h - 1$ is divisible by p^2. Consequently, for at least one $\lambda \in \{\alpha, \beta, \gamma\}$, we have $\operatorname{ord}_{p^2}(\lambda) \not\equiv 0 \pmod{p}$. Since $A_p \not\equiv 0 \pmod{p}$, it follows from Lemmas 2.6 and 2.7 that this λ is unique. Without loss of generality, we can assume $\lambda = \alpha$. Suppose that $\alpha \notin \mathbb{Z}_p$. The Galois group $\operatorname{Gal}(L_p/\mathbb{Q}_p)$ is cyclic, generated by the Frobenius automorphism σ. Then $\alpha^\sigma \neq \alpha$ and so $\alpha^\sigma \in \{\beta, \gamma\}$, say $\alpha^\sigma = \beta$. Then $\operatorname{ord}_{p^2}(\beta) = \operatorname{ord}_{p^2}(\alpha) \not\equiv 0 \pmod{p}$, which is a contradiction as α is the unique root with this property.

Conversely, let α be the unique $\lambda \in \{\alpha, \beta, \gamma\}$ such that $\operatorname{ord}_{p^2}(\lambda) \not\equiv 0 \pmod{p}$. Consequently, we have $\operatorname{ord}_{p^2}(\alpha) = \operatorname{ord}_p(\alpha)$. Put $r = \operatorname{ord}_p(\alpha)$. Then we have $p^2 | \alpha^r - 1$ in O_p. From (2.7), it follows that $r | h$ and thus $p^2 | \alpha^h - 1$ in O_p. Further from (2.7), it follows that $p | \beta^h - 1$ and $p | \gamma^h - 1$. If we combine these facts, we obtain $p^4 | (\alpha^h - 1)(\beta^h - 1)(\gamma^h - 1)$. From (2.9), it now follows that $\det A_p \equiv 0 \pmod{p}$. □

Corollary 2.9. *Let $t(x)$ be irreducible over $\mathbb{Q}_p$. Then we have*

$$A_p \equiv 0 \pmod{p} \quad \text{if and only if} \quad \det A_p \equiv 0 \pmod{p}. \tag{2.10}$$

Proof. If $t(x)$ is irreducible over $\mathbb{Q}_p$, then there is no root of $t(x)$ in $\mathbb{Z}_p$. □

Corollary 2.10. *Let $p \neq 2, 11$. Then $\det A_p \equiv 0 \pmod{p}$ if and only if there is at least one $\lambda \in \{\alpha, \beta, \gamma\}$ such that $\operatorname{ord}_{p^2}(\lambda) \not\equiv 0 \pmod{p}$.*

Proof. This follows from Theorem 2.8 and Lemma 2.6. □

Our results can be summarized in the following theorem.

Theorem 2.11. *Let $p \neq 2, 11$ and let k be the number of roots α, β, γ of $t(x)$ in O_p whose order modulo p^2 is divisible by p. Then the following cases may occur:*

Case $k = 0$: $h(p) = h(p^2)$, or equivalently $A_p \equiv 0 \pmod{p}$.
Case $k = 1$: This case is impossible.
Case $k = 2$: $h(p) \neq h(p^2)$ and $\det A_p \equiv 0 \pmod{p}$.
Case $k = 3$: $h(p) \neq h(p^2)$ and $\det A_p \not\equiv 0 \pmod{p}$.

Proof. Theorem 2.4 gives that $k = 0$ if and only if $h(p) = h(p^2)$. Lemma 2.1 states that $h(p) = h(p^2)$ if and only if $A_p \equiv 0 \pmod{p}$. Using Lemma 2.7, we see that the case $k = 1$ is impossible and Theorem 2.8 distinguishes the remaining two cases. □

A natural question arises whether there is a prime p satisfying $k = 2$. Since the solution of this question seems to be as difficult as the question whether $h(p) \neq h(p^2)$ for all primes p, we state it as a problem.

Problem 2.12. *Decide whether there is a prime p for which $h(p) \neq h(p^2)$ and $\mathrm{ord}_p(\alpha) = \mathrm{ord}_{p^2}(\alpha)$ where $\alpha \in \mathbb{Z}$ is a solution of $x^3 - x^2 - x - 1 \equiv 0 \pmod{p^2}$. The prime p satisfying this condition may be called Tribonacci-Wieferich prime of the second kind.*

3. Criteria for testing Tribonacci-Wieferich primes

In this section we derive two interesting criteria that can be used, without computing the roots of $t(x)$ in O_p, to decide whether $h(p) = h(p^2)$ or not. Let $p \neq 2, 11$. Put $q = |O_p/(p)|$. By Remark 2.5, $q = p^t$ where $t = [L_p : \mathbb{Q}_p] \in \{1, 2, 3\}$. For proofs of our criteria, we shall need the following lemma.

Lemma 3.1. *Let $p \neq 2, 11$. Then, for a unit $u \in O_p$, we have*

$$\mathrm{ord}_{p^2}(u) \not\equiv 0 \pmod{p} \quad \text{if and only if} \quad u^{q-1} \equiv 1 \pmod{p^2}. \tag{3.1}$$

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

Now we are ready for the following theorem.

Theorem 3.2. *Let $p \neq 2, 11$, $u \in O_p$ such that $t(u) \equiv 0 \pmod{p}$. Let $t(x)$ be irreducible over $\mathbb{Q}_p$. Then the following statements are equivalent:*

(i) $h(p) = h(p^2)$,
(ii) $u^{3q} - u^{2q} - u^q - 1 \equiv 0 \pmod{p^2}$.

Proof. Let $u \in O_p$, $t(u) \equiv 0 \pmod{p}$. Then we have $u \equiv \alpha \pmod{p}$ or $u \equiv \beta \pmod{p}$ or $u \equiv \gamma \pmod{p}$. We can assume $u \equiv \alpha \pmod{p}$. Then $u^q \equiv \alpha^q \pmod{p^2}$. If $h(p) = h(p^2)$, then $u^q \equiv \alpha^q \equiv \alpha \pmod{p}^2$ and $u^{3q} - u^{2q} - u^q - 1 \equiv \alpha^3 - \alpha^2 - \alpha - 1 = 0 \pmod{p^2}$. On the other hand, assume $u^{3q} - u^{2q} - u^q - 1 \equiv 0 \pmod{p^2}$. Let $u^q = \alpha + pv$. Then $(\alpha + pv)^3 - (\alpha + pv)^2 - (\alpha + pv) - 1 \equiv pv(3\alpha^2 - 2\alpha - 1) \equiv pv \cdot t'(\alpha) \equiv 0 \pmod{p^2}$. Now $p \neq 2, 11$ implies $t'(\alpha) \not\equiv 0 \pmod{p}$ 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 3.1, yields $\mathrm{ord}_{p^2}(\alpha) \not\equiv 0 \pmod{p}$ and, by Corollary 2.10, we have $\det A_p \equiv 0 \pmod{p}$. As $t(x)$ is irreducible over $\mathbb{Q}_p$, Corollary 2.9 yields $A_p \equiv 0 \pmod{p}$ and $h(p) = h(p^2)$ follows using Lemma 2.1. □

Theorem 3.3. *Let $p \neq 2, 11$, $u \in O_p$ such that $t(u) \equiv 0 \pmod{p}$. Suppose that $t(x)$ is irreducible over $\mathbb{Q}_p$. Then the following statements are equivalent:*

(i) $h(p) = h(p^2)$,
(ii) $t(u) + (u^q - u)t'(u) \equiv 0 \pmod{p^2}$,
(iii) $3u^{q+2} - 2u^{q+1} - u^q - 2u^3 + u^2 - 1 \equiv 0 \pmod{p^2}$,

where t' is the derivative of the Tribonacci characteristic polynomial t.

Proof. Let α, β, γ be the roots of $t(x)$ in O_p and let $u \in O_p$, $t(u) \equiv 0 \pmod{p}$. We can assume $u \equiv \alpha \pmod{p}$. Let $u = \alpha + pw$. Then (ii) is equivalent to

$$(\alpha^q - \alpha)(t'(\alpha) + pw \cdot t''(\alpha)) \equiv 0 \pmod{p^2}. \tag{3.2}$$

If $h(p) = h(p^2)$, then by Lemmas 2.1 and 2.6 we have $\mathrm{ord}_{p^2}(\alpha) \not\equiv 0 \pmod{p}$ which, together with Lemma 3.1, yields $\alpha^q \equiv \alpha \pmod{p^2}$ and (3.2) follows. Conversely, assume (3.2). As $p \neq 2, 11$, we have $t'(\alpha)+pw\cdot t''(\alpha) = 3\alpha^2-2\alpha-1+6\alpha pw-2\alpha \equiv 3(\alpha+pw)^2-2(\alpha+pw)-1 \equiv f'(u) \not\equiv 0 \pmod{p}$. Consequently, (3.2) yields $\alpha^q - \alpha \equiv 0 \pmod{p^2}$. Using Lemma 3.1 and Corollary 2.10, we have $\det A_p \equiv 0 \pmod{p}$ and the irreducibility of $t(x)$ yields $A_p \equiv 0 \pmod{p}$ by (2.10). This, together with Lemma 2.1, implies $h(p) = h(p^2)$ as required. Finally, by expansion of (ii) we obtain (iii) and the proof is finished. □

Remark 3.4. *The result of Theorem 3.3, part (iii), is similar to that found by Li* [4, p. 83] *for a Fibonacci sequence.*

Remark 3.5. *Theorems 3.2 and 3.3 have been proved on the assumption that $t(x)$ is irreducible over $\mathbb{Q}_p$. Let us now discuss the case of this assumption not being fulfilled. Clearly, the proofs of the $(i) \Rightarrow (ii)$ implications of both theorems remain valid even if the assumption of irreducibility of $t(x)$ is omitted. When proving the reverse $(ii) \Rightarrow (i)$ implication, the following two cases may occur.*

If α is the unique root with the property $\mathrm{ord}_{p^2}(\alpha) \not\equiv 0 \pmod{p}$ then, by Lemma 2.6, we have $A_p \not\equiv 0 \pmod{p}$ and thus $h(p) \neq h(p^2)$. By Theorem 2.8, we have $\det A_p \equiv 0 \pmod{p}$. Consequently, p is a Tribonacci-Wieferich prime of the second kind. In the opposite case, Lemma 2.6 and Lemma 2.7 yield $A_p \equiv 0 \pmod{p}$, and $h(p) = h(p^2)$ follows.

4. Computer investigation of Tribonacci-Wieferich primes

In addition to the main result formulated in Theorem 4.3, our computer search for the Tribonacci-Wieferich primes brought an interesting discovery.

Let I denote the set of all primes for which $t(x)$ is irreducible over $\mathbb{Q}_p$ and $I(x)$ be the number of all $p \in I$, $p \leq x$. Further, let Q denote the set of all primes p for which $t(x)$ is factorized over $\mathbb{Q}_p$ into a product of a linear factor and a quadratic irreducible factor, and $Q(x)$ be the number of all $p \in Q$, $p \leq x$. Finally, let L denote the set of all primes p for which $t(x)$ is factorized over $\mathbb{Q}_p$ into linear factors and $L(x)$ be the number of all $p \in L$, $p \leq x$. Clearly, $I \cup Q \cup L$ is the set of all primes and I, Q, L are pairwise disjoint. Consequently, $I(x) + Q(x) + L(x) = \pi(x)$ where $\pi(x)$ is the number of all primes p not exceeding x. Note that $2 \in I$ and $11 \in Q$. The result of our computer examination of the exact values $I(x), Q(x), L(x)$ is summarized in the following table.

x	$I(x)$	$Q(x)$	$L(x)$	$\pi(x)$
10^2	11	12	2	25
10^3	59	84	25	168
10^4	412	616	201	1229
10^5	3212	4805	1575	9592
10^6	26135	39305	13058	78498
10^7	221524	332459	110596	664579
10^8	1920148	2881402	959905	5761455
10^9	16949462	25425162	8472910	50847534

(4.1)

Table 1.

From Table 1, we can see that, approximately, we have

$$I(x) : Q(x) : L(x) \approx 2 : 3 : 1. \tag{4.2}$$

Recall now that a subset A of the set of all primes has a natural density $d(A)$ if

$$d(A) = \lim_{x\to\infty} \frac{|\{p \in A; p \le x\}|}{\pi(x)}. \tag{4.3}$$

Using the Frobenius Density Theorem [2], we can prove that $d(I) = 1/3$, $d(Q) = 1/2$, and $d(L) = 1/6$. Thus we can formulate the following theorem.

Theorem 4.1. *For $d(I), d(Q), d(L)$ we have $d(I) : d(Q) : d(L) = 2 : 3 : 1$.*

This means that our computer observation (4.2) is a consequence of Theorem 4.1.

Remark 4.2. *An interesting question is whether for some primes, the chance that they are Tribonacci-Wieferich is greater than for the others. This is supported by the fact that the following assertion holds: If $q = p^{[L_p:\mathbb{Q}_p]}$, then in the multiplicative group $[O_p/(p^2)]^\times$ there exist exactly $q-1$ elements α satisfying $\alpha^{q-1} \equiv 1 \pmod{p^2}$. Consequently, the number of $\alpha \in [O_p/(p^2)]^\times$ satisfying $\alpha^{q-1} \equiv 1 \pmod{p^2}$ strongly depends on the form of factorization of $t(x)$ over $\mathbb{Q}_p$. Supposing that the images of the roots α, β, γ in $[O_p/(p^2)]^\times$ are randomly distributed (such as when rolling a die) the probability strongly depends on which of the sets I, Q, L the prime p belongs to. A similar reasoning for the case of a Fibonacci sequence would lead to an interesting conclusion that the probability of finding the first Fibonacci-Wieferich prime is much greater for primes ending with the digits 1 or 9.*

Now we state the main theorem. By means of an extensive computer search we have obtained the following two results.

Theorem 4.3.

(i) *There is no Tribonacci-Wieferich prime $p < 10^9$.*
(ii) *There is no Tribonacci-Wieferich prime of the second kind $p < 10^9$.*

Remark 4.4. *By analogy with Problem 2.12, we can consider a similar problem for a Tetranacci sequence $(M_n)_{n=0}^\infty$ defined by $M_{n+4} = M_{n+3} + M_{n+2} + M_{n+1} + M_n$ with $M_0 = M_1 = M_2 = 0$ and $M_3 = 1$. Now, let $h(m)$ denote a period of $(M_n \bmod m)_{n=0}^\infty$. Is there a prime p for which $h(p) \neq h(p^2)$ and $\mathrm{ord}_p(\alpha) = \mathrm{ord}_{p^2}(\alpha)$ where $\alpha \in \mathbb{Z}$ is a solution of $x^4 - x^3 - x^2 - x - 1 \equiv 0 \pmod{p^2}$? To this problem we find the following solution.*

Theorem 4.5. *For $p < 10^9$, there are exactly three Tetranacci-Wieferich primes of the second kind: $p_1 = 17$, $p_2 = 191$, and $p_3 = 11351$.*

References

[1] R. Crandall, K. Dilcher, and C. Pomerance, *A Search for Wieferich and Wilson Primes*, Math. Comp., **66** (1997), 443–449.

[2] F. G. Frobenius, *Über Beziehungen zwischen den Primidealen eines algebraischen Körpers und den Substitutionen seiner Gruppe*, Sitzungsberichte Königl. Preußisch. Akad. Wissenschaft. Berlin, (1896), 689–703; Gesammelte Abhandlungen II, Springer Berlin (1968), 719–733.

[3] J. Knauer and J. Richstein, *The Continuing Search for Wieferich Primes*, Math. Comp., **74** (2005), 1559–1563.

[4] H.-C. Li, *Fibonacci Primitive Roots and Wall's Question*, The Fibonacci Quarterly, **37** (1999), 77–84.

[5] R. J. McIntosh and E. L. Roettger, *A Search for Fibonacci-Wieferich and Wolstenholme Primes*, Math. Comp., **76** (2007), 2087–2094.

[6] Z.-H. Sun and Z.-W. Sun, *Fibonacci Numbers and Fermat's Last Theorem*, Acta Arith., **60** (1992), 371–388.
[7] A. Vince, *Period of a Linear Recurrence*, Acta Arith., **39** (1981), 303–311.
[8] M. E. Waddill, *Some Properties of a Generalized Fibonacci Sequence Modulo m*, The Fibonacci Quarterly, **16** (1978), 344–353.
[9] D. D. Wall, *Fibonacci Series Modulo m*, Amer. Math. Monthly, **67** (1960), 525–532.
[10] A. Wieferich, *Zum letzten Fermat'schen Theorem*, J. Reine Angew. Math., **136** (1909), 293–302.

MSC2000: 11B50, 11B39, 11A07

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