Jiří Klaška

A search for Tribonacci-Wieferich primes

Acta Mathematica Universitatis Ostraviensis, Vol. 16 (2008), No. 1, 15--20

Persistent URL: http://dml.cz/dmlcz/137497

A search for Tribonacci-Wieferich primes

Jiří Klaška

Abstract. Such problems as the search for Wieferich primes or Wall-Sun-Sun primes are intensively studied and often discused at present. This paper is devoted to a similar problem related to the Tribonacci numbers.

1 Introduction

Let T_n denote the n-th Tribonacci number defined by $T_{n+3} = T_{n+2}+T_{n+1}+T_n$ with $T_0 = 0$, $T_1 = 0$, and $T_2 = 1$. This number has been examined by many authors. First by A. Agronomof [1] in 1914 and subsequently by many others. See, for example, [2], [5], [7], [8], [9], [10]. It is well known that $(T_n \bmod m)_{n=0}^{\infty}$ is periodic for any modulus $m > 1$. The least positive integer h satisfying $[T_h, T_{h+1}, T_{h+2}] \equiv [T_0, T_1, T_2] \pmod{m}$ is called a period of $(T_n \bmod m)_{n=0}^{\infty}$ and denoted by $h(m)$.

Two problems remain open: 1. Is there a prime p satisfying $h(p) = h(p^2)$ (M. E. Waddill 1978, [10])? 2. Is there a prime p such that $h(p) \neq h(p^2)$ and $\mathrm{ord}_p(\alpha) = \mathrm{ord}_{p^2}(\alpha)$ where $\alpha \in \mathbb{Z}$ is a solution of $x^3 - x^2 - x - 1 \equiv 0 \pmod{p^2}$ (J. Klaška 2007, [5])? Here, $\mathrm{ord}_{p^t}(\alpha)$ denotes the order of α in the multiplicative group of the ring $\mathbb{Z}/p^t\mathbb{Z}$, $t \in \mathbb{N}$. See also [6, Problem 3.2]. In [6], the primes p satisfying $h(p) = h(p^2)$ are called Tribonacci-Wieferich primes and the primes for which $h(p^2) \neq h(p)$ and $\mathrm{ord}_p(\alpha) = \mathrm{ord}_{p^2}(\alpha)$ where $\alpha \in \mathbb{Z}$ is a solution of $x^3 - x^2 - x - 1 \equiv 0 \pmod{p^2}$ are called Tribonacci-Wieferich primes of the second kind. In [6] we proved that neither of this problems has a solution for $p < 10^9$. In the present paper we substantially extend these results focussing on the case of the Tribonacci characteristic polynomial $t(x) = x^3 - x^2 - x - 1$ being irreducible modulo p.

2 Tribonacci modulo p^2 – an irreducible case

Let $I = \{3, 5, 23, 31, \dots\}$ be the set of all primes p for which $t(x)$ is irreducible over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Let K be the splitting field of $t(x)$ over $\mathbb{F}_p$, $p \in I$ and α, β, γ the roots of $t(x)$ in K. Clearly, $K = GF(p^3)$ and the multiplicative group of K has $p^3 - 1$

2000 Mathematics Subject Classification: 11B50, 11B39
Key Words and Phrases: Tribonacci numbers, Tribonacci-Wieferich primes.

elements. Using the Frobenius authomorphism, we can easily prove that $\beta = \alpha^p$ and $\gamma = \alpha^{p^2}$. This implies that α, β, γ have the same order in the multiplicative group of K. It is well known, see e.g. [5], [6], [8], that for any prime $p \neq 2, 11$:

$$h(p) = \mathrm{lcm}(\mathrm{ord}_L(\alpha), \mathrm{ord}_L(\beta), \mathrm{ord}_L(\gamma)) \tag{2.1}$$

where L is the splitting field of $t(x)$ over $\mathbb{F}_p$ and $\mathrm{ord}_L(\alpha), \mathrm{ord}_L(\beta), \mathrm{ord}_L(\gamma)$ are the orders of α, β, γ in the multiplicative group of L. Consequently, for $p \in I$, we can state

Lemma 2.1. *Let $p \in I$. Then $h(p) = \mathrm{ord}_K(\alpha)$ where α is any root of $t(x)$ in a splitting field K of $t(x)$ over $\mathbb{F}_p$.*

Lemma 2.2. *For any prime $p \in I$ we have $h(p) | p^2 + p + 1$.*

Proof. The Viète equation $\alpha\beta\gamma = 1$ together with $\beta = \alpha^p$ and $\gamma = \alpha^{p^2}$ yields $\alpha^{p^2+p+1} = 1$. This implies $\mathrm{ord}_K(\alpha) | p^2 + p + 1$ and the relation $h(p) | p^2 + p + 1$ follows from Lemma 2.1. □

Remark 2.3. *In the relation $h(p)|p^2 + p + 1$ it is often, but not always, true that $h(p) = p^2+p+1$. For example, $h(3) = 3^2+3+1 = 13$ but $h(31) = (31^2+31+1)/3 = 331$.*

In 1978, M. E. Waddill [10, Theorem 8] proved that for any prime p:

$$\text{If } \ h(p) \neq h(p^2), \text{ then } h(p^t) = p^{t-1} h(p) \text{ for any } t \in \mathbb{N}. \tag{2.2}$$

Consequently, we have either $h(p^2) = p \cdot h(p)$ or $h(p^2) = h(p)$. If we combine Waddill's result (2.2) with Lemma 2.2, we obtain

Lemma 2.4. *For any prime $p \in I$, $h(p) = h(p^2)$ if and only if $h(p^2)|p^2 + p + 1$.*

Now we show that to calculate the powers of α in the multiplicative group of K we need to calculate with Tribonacci numbers.

Lemma 2.5. *For any positive integer $n \geq 3$ we have the identity*

$$x^n = T_n x^2 + (T_{n-1} + T_{n-2})x + T_{n-1} + s_n(x)t(x) \ \text{ where } \ s_n(x) = \sum_{k=1}^{n} T_k x^{n-k}. \tag{2.3}$$

Proof. Using induction on n. □

Reducing the identity (2.3) by the double modulus $\mathrm{modd}(m, t(x))$ where $m > 1$ is an arbitrary positive integer, we obtain the congruence

$$x^n \equiv T_n x^2 + (T_{n-1} + T_{n-2})x + T_{n-1} (\mathrm{modd}\ m, t(x)). \tag{2.4}$$

From (2.4) now it follows that

$$x^n \equiv 1 (\mathrm{modd}\ m, t(x)) \ \text{ if and only if } \ [T_n, T_{n+1}, T_{n+2}] \equiv [0, 0, 1] (\mathrm{mod}\ m). \tag{2.5}$$

Particulary, if $m = p$, $p \in I$ and $x = \alpha$ where α is any root of $t(x)$ in K, (2.5) implies Lemma 2.1.

Example 2.6. *Let $p = 3$. Then $p^2 + p + 1 = 13$ and by (2.4) we have $x^{13} \equiv 504x^2 + 423x + 274 \equiv 4 \not\equiv 1(\text{modd } 3^2, t(x))$. From (2.5) now it follows that $h(3) \neq h(3^2)$ and thus $p = 3$ is not a Tribonacci-Wieferich prime. Moreover, from Lemma 2.2 and $h(3) \neq 1$, it follows that $h(3) = 13$ and by (2.2) we have $h(3^2) = 39$.*

Let $q \in I$. By I_q denote the set of all primes $p \in I$ not exceding q. Theoretically, we have two posibilites when searching for Tribonacci-Wieferich primes in I_q. First, we can calculate a finite sequence $(T_n)_{n=0}^{q^2+q+1}$ and, subsequently, for any particular primes $p \in I_q$, test whether $[T_{p^2+p+1}, T_{p^2+p+2}, T_{p^2+p+3}] \equiv [0, 0, 1] \pmod{p^2}$. Second, we compute the reduced sequences $(T_n \bmod p^2)_{n=0}^{p^2+p+1}$ for any $p \in I_q$.

Let us now show that the first possibility is virtually excluded as it uses an enormous amount of computer memory. It can be easily proved that the Tribonacci polynomial $t(x)$ has one real root

$$\tau = \frac{1}{3}\left(\sqrt[3]{19 + 3\sqrt{33}} + \sqrt[3]{19 - 3\sqrt{33}} + 1\right) \approx 1.839\,286\,755\,214\,161\,132\,\cdots \tag{2.6}$$

and two complex roots $\sigma, \overline{\sigma}$ ($\overline{\sigma}$ is the complex conjugate of σ) where

$$\sigma = \frac{1}{6}\left(2 - \sqrt[3]{19 + 3\sqrt{33}} - \sqrt[3]{19 - 3\sqrt{33}}\right) + \frac{\sqrt{3}i}{6}\left(\sqrt[3]{19 + 3\sqrt{33}} - \sqrt[3]{19 - 3\sqrt{33}}\right). \tag{2.7}$$

Put $\varepsilon = \tau^2/|\tau - \sigma|^2 \approx 0.618\,419\,922\,319\,392\,550\cdots$. In [7], W. R. Spickerman proved that for T_n we have

$$T_n = [\varepsilon \cdot \tau^n + 0.5]. \tag{2.8}$$

Here $[x]$ denotes the greatest integer not exceeding x. Clearly, if x is positive, then $[x]$ is simply the integer part of x. Note that, in [7], σ is incorrect. See [7, p. 119]. From (2.8) it follows that, for $\log T_n$, we have

$$\log T_n \approx n \cdot \log \tau \quad \text{where} \quad \log \tau = 0.264\,649\,443\,484\,250\,871\cdots. \tag{2.9}$$

Evidently, T_n has exactly k digits for $n > 1$ if and only if $k - 1 \leq \log T_n < k$. This, together with (2.9) yields an estimate for the number of digits of T_n. The following example may provide a more precise idea of the greatness of Tribonacci numbers T_n.

Example 2.7. *The Tribonacci number T_{100} has 26 digits, T_{1000} has 264 digits, and T_{10000} has 2646 digits. Consider now the greatest prime p from the interval $[2, 10^9]$ for which $t(x)$ is irreducible modulo p. This p is equal to 999999929. To test whether $h(p) = h(p^2)$ we need to find $[T_q, T_{q+1}, T_{q+2}]$ where $q = p^2 + p + 1 = 999999859000004971$. Since, by (2.9), T_q has more than $5 \cdot 10^{15}$ digits, we need about 10^6 GB of memory for T_q, assuming that one byte is needed for one digit.*

In this paper, we use a method based on matrix algebra to search for Tribonacci-Wieferich primes on a given set I_q using a computer. It is well known (see e.g. [5],

[9]) that Tribonacci numbers can be computed by powers of the Tribonacci matrix T where

$$T = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix} \quad \text{and} \quad T^{n+1} = \begin{bmatrix} T_n & T_{n-1} + T_n & T_{n+1} \\ T_{n+1} & T_n + T_{n+1} & T_{n+2} \\ T_{n+2} & T_{n+1} + T_{n+2} & T_{n+3} \end{bmatrix} \quad \text{for} \quad n \in \mathbb{N}. \tag{2.10}$$

Clearly, $h(m)$ is the period of $(T_n \bmod m)_{n=0}^{\infty}$ if and only if $h(m)$ is the smallest positive integer h for which $T^h \equiv E \pmod{m}$ where E is the 3×3 identity matrix. This, together with Lemma 2.4, yields

Lemma 2.8. *For any $p \in I$ we have $h(p) = h(p^2)$ if and only if $T^{p^2+p+1} \equiv E \pmod{p^2}$ where E is the 3×3 identity matrix.*

Now we briefly describe the algorithm used to prove the main theorem of this section.

Algorithm for testing $h(p) = h(p^2)$ for $p \in I$

First, we find a 2-adic expansion of $p^2 + p + 1 = c_0 + 2c_1 + 2^2 c_2 + \cdots + 2^k c_k$.

Second, we define the matrix $T \bmod p^2$ and, subsequently, we compute k matrices $T^{2^i} \bmod p^2$ for $i = 1, \ldots, k$.

Third, we compute the matrix

$$T^{p^2+p+1} \bmod p^2 = \prod_{i=0}^{k} (T^{2^i} \bmod p^2)^{c_i}. \tag{2.11}$$

Finally, we test whether $T^{p^2+p+1} \bmod p^2$ is equal to the identity matrix E.

This process is repeated for every prime $p \in I$.

Implementing this algorithm in Pari GP, we have obtained the following result:

Theorem 2.9. *For any prime $p \in I$, $p < 10^{11}$ we have $h(p) \neq h(p^2)$.*

Let us remark that, achieving this result takes about 1500 hours of CPU time on a 1.6 GHz processor computer.

3 Searching for Tribonacci-Wieferich primes $p \notin I$

In the case of $p \notin I$ we can use the criteria derived in [6] to search for Tribonacci-Wieferich primes. Moreover, when dealing with this case, Tribonacci-Wieferich primes of the second kind may also be found easily. Indeed, by [5], from $h(p) = h(p^2)$, we have $\text{ord}_p(\xi) = \text{ord}_{p^2}(\xi)$ for any solution $\xi \in \mathbb{Z}$ of $t(x) \equiv 0 \pmod{p^2}$. Next, acording to [6], if $\alpha \in \mathbb{Z}$ is the unique root of $t(x)$ modulo p with the property

$$3\alpha^{p+2} - 2\alpha^{p+1} - \alpha^p - 2\alpha^3 + \alpha^2 - 1 \equiv 0 \pmod{p^2} \tag{3.1}$$

or, equivalently, with the property

$$\alpha^{3p} - \alpha^{2p} - \alpha^p - 1 \equiv 0 \pmod{p^2} \tag{3.2}$$

then p is the Tribonacci-Wieferich prime of the second kind. It should be stressed that the criteria (3.1) and (3.2) make it possible to find Tribonacci-Wieferich primes of the second kind and thus also Tribonacci-Wieferich primes p with $p \notin I$ without having to calculate with Tribonacci numbers. The following result has been obtained using (3.1) in Pari GP.

Theorem 3.1. *There is no prime $p \notin I$, $p < 10^{11}$ satisfying $\mathrm{ord}_p(\xi) = \mathrm{ord}_{p^2}(\xi)$ where $\xi \in \mathbb{Z}$ is a solution of $t(x) \equiv 0 \pmod{p^2}$. Consequently, there is no Tribonacci-Wieferich prime of the second kind less than 10^{11}.*

Note that, as compared with Theorem 2.9, only about 700 hours of CPU time are needed to obtain Theorem 3.1 on the same computer.

Corollary 3.2. *For any prime $p \notin I$, $p < 10^{11}$, we have $h(p) \neq h(p^2)$.*

If we combine Corollary 3.2 with Theorem 2.9, we obtain the main theorem of this paper:

Theorem 3.3. *There is no Tribonacci-Wieferich prime $p < 10^{11}$.*

Moreover, based on (2.2), we can now state

Corollary 3.4. *For any prime $p < 10^{11}$ and for any $t \in \mathbb{N}$, we have $h(p^t) = p^{t-1}h(p)$.*

Remark 3.5. *Like in the problem of finding Fibonacci-Wieferich primes (see [3], [4]) also in the Tribonacci case a question may be raised whether the probability of some primes being Tribonacci-Wieferich is greater than that of others. Using a reasoning similar to that used in [4], we can conclude that further search of the set I for $p > 10^{11}$ will virtually not increase the probability of finding a Tribonacci-Wieferich prime. Consequently, the chances of finding Tribonacci-Wieferich primes on a computer seem to be greater for primes not in I, particulary, for those for which $t(x)$ can be factorized into linear terms over $\mathbb{F}_p$.*

References

[1] A. Agronomof, *Une série récurrente,* Mathesis **4** (1914), 125–126.

[2] M. Feinberg, *Fibonacci-Tribonacci,* The Fibonacci Quarterly **1.3** (1963), 70, 71–74.

[3] J. Klaška, *Criteria for testing Wall's question,* to appear in Czechoslovak Math. Journal **58.4** (2008).

[4] J. Klaška, *Short remark on Fibonacci-Wieferich primes,* Acta Math. Univ. Ostrav. **15** (2007), 21–25.

[5] J. Klaška, *Tribonacci modulo p^t,* Mathematica Bohemica, **133.3** (2008), 267–288.

[6] J. Klaška, *On Tribonacci-Wieferich primes,* submitted for publication in The Fibonacci Quarterly.

[7] W. R. Spickerman, *Binet's Formula for the Tribonacci Sequence,* The Fibonacci Quarterly **20.2** (1982), 118–120.

[8] A. Vince, *Period of a Linear Recurrence,* Acta Arith. **39** (1981), 303–311.

[9] M. E. Waddill, L. Sacks, *Another Generalized Fibonacci Sequence,* The Fibonacci Quarterly **5.3** (1967), 209–222.

[10] M. E. Waddill, *Some Properties of a Generalized Fibonacci Sequence Modulo m*, The Fibonacci Quarterly **16.4** (1978), 344–353.

Author(s) Address(es):
Department of Mathematics, Brno University of Technology, Technická 2, 616 69 Brno, Czech Republic

E-mail Address: klaska@fme.vutbr.cz