TRIBONACCI MODULO 2^t AND 11^t

Jiří Klaška, Brno

(Received May 31, 2007)

Abstract. Our previous research was devoted to the problem of determining the primitive periods of the sequences $(G_n \bmod p^t)_{n=1}^{\infty}$ where $(G_n)_{n=1}^{\infty}$ is a Tribonacci sequence defined by an arbitrary triple of integers. The solution to this problem was found for the case of powers of an arbitrary prime $p \neq 2, 11$. In this paper, which could be seen as a completion of our preceding investigation, we find solution for the case of singular primes $p = 2, 11$.

Keywords: Tribonacci, modular periodicity, periodic sequence

MSC 2000: 11B50, 11B39

1. Introduction

Having a linear recurrence formula of order k with integer coefficients we can construct the corresponding characteristic polynomial $f(x)$. If $f(x)$ has no multiple roots then its discriminant is a non zero integer and so it is divisible by only a finite number of prime divisors. When investigating modular periodicity of the sequences defined by these formulas, the primes that divide the discriminant of $f(x)$ form exceptions and have to be considered separately. The exceptional primes p correspond to the cases of $f(x)$ having multiple roots over the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ of residue classes modulo p. In this paper, which could be seen as an extension of our previous paper [1], we focus on the Tribonacci case. It is well known, see for example [2, p. 310], that the primes $p = 2, 11$ are the only primes for which the Tribonacci characteristic polynomial $g(x) = x^3 - x^2 - x - 1$ has multiple roots.

Let us now review the notation introduced in [1]. Let $(g_n)_{n=1}^{\infty}$ denote a Tribonacci sequence defined by the recurrence formula $g_{n+3} = g_{n+2} + g_{n+1} + g_n$ and the triple of initial values $[0, 0, 1]$. Let further $(G_n)_{n=1}^{\infty}$ denote the generalized Tribonacci sequence defined by an arbitrary triple $[a, b, c]$ of integers. We will denote the primitive periods of the sequences $(g_n \bmod m)_{n=1}^{\infty}$ and $(G_n \bmod m)_{n=1}^{\infty}$ by $h(m)$ and $h(m)[a, b, c]$

respectively. In 1978, M. E. Waddill [3, Theorem 8] proved that for any prime p and $t \in \mathbb{N} = \{1, 2, 3, \ldots\}$, we have:

$$\text{If } \ h(p) \neq h(p^2), \text{ then } h(p^t) = p^{t-1}h(p). \tag{1.1}$$

This paper aims at determining the numbers $h(p^t)[a, b, c]$ and find the relationships between $h(p^t)[a, b, c]$ and $h(p)[a, b, c]$ for the primes $p = 2, 11$. The case of $p \neq 2, 11$ is solved in [1]. The methods used in proofs of this paper will mostly be based on matrix algebra. As usual, by T we will denote the Tribonacci matrix

$$T = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix} \quad \text{and} \quad T^n = \begin{bmatrix} g_n & g_{n-1} + g_n & g_{n+1} \\ g_{n+1} & g_n + g_{n+1} & g_{n+2} \\ g_{n+2} & g_{n+1} + g_{n+2} & g_{n+3} \end{bmatrix} \quad \text{for } \ n > 1. \tag{1.2}$$

Put $x_0 = [a, b, c]^\tau$ and $x_n = [G_{n+1}, G_{n+2}, G_{n+3}]^\tau$ where τ denotes transposition. Then the triple x_n may be expressed by means of x_0 as follows: $x_n = T^n x_0$. Thus the primitive period of the sequence $(G_n \bmod m)_{n=1}^\infty$ defined by a triple $[a, b, c]$ for an arbitrary module $m > 1$ is equal to the smallest number h for which $T^h x_0 \equiv x_0 \pmod m$. By [1, Lemma 2.1], the investigation of the primitive periods of Tribonacci sequences modulo p^t is restricted to sequences beginning with the triples $[a, b, c] \not\equiv [0, 0, 0] \pmod p$. In the opposite case, for any $t \in \mathbb{N}$ and $1 \leqslant i \leqslant t$, we have $h(p^t)[p^{t-i}a, p^{t-i}b, p^{t-i}c] = h(p^i)[a, b, c]$. For this reason, we will investigate only the triples satisfying $[a, b, c] \not\equiv [0, 0, 0] \pmod p$.

2. Tribonacci modulo 2^t

We can easily calculate $h(2) = 4$ and $h(2^2) = 8$. By (1.1) we have $h(2^t) = 2^{t-1}h(2) = 2^{t+1}$ and so $h(2^t)[a, b, c] \mid 2^{t+1}$ for any $[a, b, c]$. For $p = 2$, the multiplicity of the root $\alpha = 1$ of the polynomial $g(x)$ is greater than $\operatorname{char}(\mathbb{F}_2) = 2$ and therefore $(G_n \bmod 2)_{n=1}^\infty$ cannot be expressed as $G_n \bmod 2 = c_1 + c_2 n + c_3 n^2$ as usual. The sequences $(1)_{n=1}^\infty, (n)_{n=1}^\infty$, $(n^2)_{n=1}^\infty$ are dependent over $\mathbb{F}_2$ and do not form a basis. Despite that, for some triples $[a, b, c] \not\equiv [0, 0, 0] \pmod 2$, the numbers $h(2^t)[a, b, c]$ can be determined using the results derived in [1]. In the first place, it is proved in [1, Theorem 3.1] that, if $(D(a, b, c), m) = 1$ where $D(a, b, c)$ is a cubic form defined by

$$D(a, b, c) = a^3 + 2b^3 + c^3 - 2abc + 2a^2b + 2ab^2 - 2bc^2 + a^2c - ac^2, \tag{2.1}$$

then $h(m)[a, b, c] = h(m)$ for any modulus $m > 1$. The following theorem is an easy consequence of the above assertions.

Theorem 2.1. *If $D(a,b,c)$ is an odd number, then $h(2^t)[a,b,c] = h(2^t) = 2^{t+1}$. Hence, we have $h(2^t)[a,b,c] = 2^{t-1} \cdot h(2)[a,b,c]$.*

It is easy to verify that the premise of Theorem 2.1 is true if and only if $[a,b,c]$ is congruent modulo 2 with some of the triples $[0,0,1]$, $[1,0,0]$, $[1,1,0]$, $[0,1,1]$. Therefore it suffices to investigate the cases of the triple $[a,b,c]$ being congruent modulo 2 with some of the triples $[0,1,0],[1,0,1],[1,1,1]$. The following assertions will be important for the proofs of the main theorems 2.4, 2.5 and 2.6.

Lemma 2.2. *For any modulus of the form 2^t where $t \geqslant 5$, the following congruences hold:*

$$\begin{aligned} g_{2^{t-1}-1} &\equiv -1 \pmod{2^t}, \\ g_{2^{t-1}} &\equiv 2^{t-2}+1 \pmod{2^t}, \\ g_{2^{t-1}+1} &\equiv 0 \pmod{2^t}, \\ g_{2^{t-1}+2} &\equiv 2^{t-2} \pmod{2^t}, \\ g_{2^{t-1}+3} &\equiv 2^{t-1}+1 \pmod{2^t}. \end{aligned}$$

Proof. Using methods of matrix algebra, we will prove all the congruences in (2.2) simultaneously. Let us consider a Tribonacci matrix T. Due to (1.2), it suffices to prove that for any $t \geqslant 5$ we have

$$\begin{aligned} T^{2^{t-1}} &\equiv \begin{bmatrix} 2^{t-2}+1 & 2^{t-2} & 0 \\ 0 & 2^{t-2}+1 & 2^{t-2} \\ 2^{t-2} & 2^{t-2} & 2^{t-1}+1 \end{bmatrix} \\ &\equiv E + 2^{t-2}A \pmod{2^t}, \text{ where } A = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 2 \end{bmatrix} \end{aligned}$$

and E is an identity matrix. Let us first prove the congruence for $t=5$. By direct calculation, we can verify that

$$T^{2^4} = \begin{bmatrix} 1705 & 2632 & 3136 \\ 3136 & 4841 & 5768 \\ 5768 & 8904 & 10609 \end{bmatrix} \equiv \begin{bmatrix} 2^3+1 & 2^3 & 0 \\ 0 & 2^3+1 & 2^3 \\ 2^3 & 2^3 & 2^4+1 \end{bmatrix} \pmod{2^5}.$$

Let us further assume that the congruence holds for $t \geqslant 5$. Since $AE = EA$, we have $T^{2^t} \equiv (E + 2^{t-2}A)^2 \equiv E + 2^{t-1}A \pmod{2^{t+1}}$, which proves (2.2). □

Consequence 2.3. *For any modulus of the form 2^t where $t \geqslant 3$, the following congruences hold:*

$$
\begin{aligned}
&g_{2^t-1} \equiv -1 \pmod{2^t}, \quad g_{2^t} \equiv 2^{t-1}+1 \pmod{2^t},\\
&g_{2^t+1} \equiv 0 \pmod{2^t}, \quad g_{2^t+2} \equiv 2^{t-1} \pmod{2^t},\\
&g_{2^t+3} \equiv 1 \pmod{2^t}.
\end{aligned}
\tag{2.3}
$$

Proof. For $t = 3$, (2.3) can be verified by direct calculation. For $t \geqslant 4$, (2.3) follows from (2.2). □

Theorem 2.4. *If $[a, b, c] \equiv [0, 1, 0] \pmod 2$, then for $t > 1$ we have*

$$h(2^t)[a, b, c] = 2^{t+1}. \tag{2.4}$$

Proof. Clearly, it is sufficient to prove that $x_{2^t} \not\equiv x_0 \pmod{2^t}$, that is, that 2^t is not a period. The triple $[a, b, c]$ can be written as $x_0 = [2a_1, 1 + 2b_1, 2c_1]^\tau$ where $a_1, b_1, c_1 \in \mathbb{Z}$. For $t = 2$ we have

$$T^{2^2} x_0 = \begin{bmatrix} 1 & 2 & 2 \\ 2 & 3 & 4 \\ 4 & 6 & 7 \end{bmatrix} \begin{bmatrix} 2a_1 \\ 1 + 2b_1 \\ 2c_1 \end{bmatrix} \equiv \begin{bmatrix} 2 + 2a_1 \\ 3 + 2b_1 \\ 2 + 2c_1 \end{bmatrix} \pmod{2^2}.$$

Suppose that $T^{2^2} x_0 \equiv x_0 (\text{mod } 2^2)$. Then we have

$$[2 + 2a_1, 3 + 2b_1, 2 + 2c_1] \equiv [2a_1, 1 + 2b_1, 2c_1] (\text{mod } 2^2).$$

Hence $[2, 3, 2] \equiv [0, 1, 0] (\text{mod } 2^2)$, which is a contradiction. If $t \geqslant 3$, then by (2.3) we have

$$T^{2^t} x_0 \equiv \begin{bmatrix} 2^{t-1}+1 & 2^{t-1} & 0 \\ 0 & 2^{t-1}+1 & 2^{t-1} \\ 2^{t-1} & 2^{t-1} & 1 \end{bmatrix} \begin{bmatrix} 2a_1 \\ 1 + 2b_1 \\ 2c_1 \end{bmatrix} \equiv \begin{bmatrix} 2a_1 + 2^{t-1} \\ 1 + 2b_1 + 2^{t-1} \\ 2c_1 + 2^{t-1} \end{bmatrix} \pmod{2^t}.$$

Suppose that $T^{2^t} x_0 \equiv x_0 \pmod{2^t}$. Then we have

$$[2a_1 + 2^{t-1}, 2^{t-1}, 2c_1 + 2^{t-1}] \equiv [2a_1, 1 + 2b_1, 2c_1] \pmod{2^t}.$$

By matching terms, we obtain $2^{t-1} \equiv 0 \pmod{2^t}$ and thus a contradiction. □

It is not difficult to rephrase Theorem 2.4 to include the triples $[a, b, c] \equiv [1, 0, 1]$. Clearly, there is exactly one triple of the form $x_0 = [2(c_1 - a_1 - b_1), 1 + 2a_1, 2b_1]^\tau$ corresponding to each triple $x_1 = [1 + 2a_1, 2b_1, 1 + 2c_1]^\tau$. Since $Tx_0 = x_1$, the triples x_0 and x_1 define sequences with identical primitive periods. By 2.4, this primitive period equals 2^{t+1}. This proves the following theorem.

Theorem 2.5. *If* $[a,b,c] \equiv [1,0,1] \pmod 2$, *then for* $t > 1$ *we have*

$$h(2^t)[a,b,c] = 2^{t+1}. \tag{2.5}$$

We can also use the procedure from 2.4 to prove the following theorem:

Theorem 2.6. *If* $[a,b,c] \equiv [1,1,1] \pmod 2$, *then for* $t > 1$ *we have*

$$h(2^t)[a,b,c] = 2^t. \tag{2.6}$$

Proof. The triple $[a,b,c]$ can be written as $x_0 = [1+2a_1, 1+2b_1, 1+2c_1]^\tau$ where $a_1, b_1, c_1 \in \mathbb{Z}$. Suppose $t \geqslant 5$. Then by Lemma 2.2 we have $T^{2^t} x_0 \equiv x_0 \pmod{2^t}$ and so $h(2^t)[a,b,c] \mid 2^t$. It is now sufficient to prove that $x_{2^{t-1}} \not\equiv x_0 \pmod{2^t}$, that is, that 2^{t-1} is not a period. By (2.2) we have

$$x_{2^{t-1}} \equiv T^{2^{t-1}} x_0 \equiv \begin{bmatrix} 2^{t-2}+1 & 2^{t-2} & 0 \\ 0 & 2^{t-2}+1 & 2^{t-2} \\ 2^{t-2} & 2^{t-2} & 2^{t-1}+1 \end{bmatrix} \begin{bmatrix} 1+2a_1 \\ 1+2b_1 \\ 1+2c_1 \end{bmatrix} \pmod{2^t}.$$

It follows that

$$x_{2^{t-1}} \equiv [1+2a_1+2^{t-1}(1+a_1+b_1), 1+2b_1+2^{t-1}(1+b_1+c_1), 1+2c_1+2^{t-1}(a_1+b_1)]^\tau.$$

Suppose $x_{2^{t-1}} \equiv x_0 \pmod{2^t}$. Matching the terms yields that

$$2^{t-1}(1+a_1+b_1) \equiv 0, \quad 2^{t-1}(1+b_1+c_1) \equiv 0, \quad 2^{t-1}(a_1+b_1) \equiv 0 \pmod{2^t}.$$

Hence $1 \equiv 0 \pmod 2$ and a contradiction follows. To prove the cases of $t = 2,3,4$ is easy and can be left to the reader. □

Remark 2.7. Theorems 2.4, 2.5, and 2.6 are true for $t > 1$. In particular, for $t = 1$ we have $h(2)[1,1,1] = 1$ and $h(2)[0,1,0] = h(2)[1,0,1] = 2$.

Corollary 2.8. *If a triple* $[a,b,c]$ *is congruent modulo 2 with some of the triples* $[0,1,0]$, $[1,0,1]$, $[1,1,1]$, *then for any* $t > 1$ *we have* $h(2^t)[a,b,c] = 2^t \cdot h(2)[a,b,c]$.

3. Tribonacci modulo 11^t

The determination of primitive periods modulo 11^t will be somewhat more complicated. We can directly verify that $h(11) = 110$ and $h(11^2) = 1210$. Now it follows from (1.1) that $h(11^t) = 10 \cdot 11^t$ for any $t \in \mathbb{N}$ and thus, for any triple $[a, b, c]$, we have $h(11^t)[a, b, c] \mid 10 \cdot 11^t$. As $x^3 - x^2 - x - 1 \equiv (x - 9)(x - 7)^2 \pmod{11}$ and $(9^n)_{n=1}^{\infty}$, $(7^n)_{n=1}^{\infty}$, $(n7^n)_{n=1}^{\infty}$ are linearly independent over $\mathbb{F}_{11}$, we have

$$G_n \equiv c_1 \cdot 9^n + (c_2 + c_3 n) \cdot 7^n \pmod{11}, \tag{3.1}$$

where the coefficients c_1, c_2, c_3 are uniquely determined by the triple $[a, b, c]$. Let $\mathrm{ord}_{11}(\varepsilon)$ denote the order of $\varepsilon \not\equiv 0 \pmod{11}$ in the multiplicative group of $\mathbb{F}_{11}$. It is easy to see that $\mathrm{ord}_{11}(9) = 5$ and $\mathrm{ord}_{11}(7) = 10$. Now yields (3.1) that for any $[a, b, c] \not\equiv [0, 0, 0] \pmod{11}$, $h(11)[a, b, c]$ is equal exactly to one of the numbers $5, 10$ and 110. This, together with $h(11)[a, b, c] \mid h(11^t)[a, b, c]$, implies that for $[a, b, c] \not\equiv [0, 0, 0] \pmod{11}$ the only forms of the periods $h(11^t)[a, b, c]$ are $5 \cdot 11^i$ and $10 \cdot 11^i$ where $i \in \{0, 1, \dots, t\}$. Consequently, there exists no triple $[a, b, c]$ for which $h(11^t)[a, b, c] = 2 \cdot 11^i$. In some cases, $h(11^t)[a, b, c]$ can be determined using the form $D(a, b, c)$. However, there are triples for which $h(11^t)[a, b, c] = h(11^t)$ and also $D(a, b, c) \equiv 0 \pmod{11}$. Thus $D(a, b, c)$ cannot be used to determine all the triples for which $h(11^t)[a, b, c] = h(11^t)$.

Lemma 3.1. *Let $t \geqslant 3$ and $h = 10 \cdot 11^{t-2}$. Then we have the following congruences:*

$$\begin{aligned} g_{h-1} &\equiv 25 \cdot 11^{t-2} - 1 \pmod{11^t}, \\ g_h &\equiv 65 \cdot 11^{t-2} + 1 \pmod{11^t}, \\ g_{h+1} &\equiv 26 \cdot 11^{t-2} \pmod{11^t}, \\ g_{h+2} &\equiv 116 \cdot 11^{t-2} \pmod{11^t}, \\ g_{h+3} &\equiv 86 \cdot 11^{t-2} + 1 \pmod{11^t}. \end{aligned} \tag{3.2}$$

Proof. By (1.2), it is sufficient to prove that

$$T^{10 \cdot 11^{t-2}} \equiv \begin{bmatrix} 65 \cdot 11^{t-2} + 1 & 90 \cdot 11^{t-2} & 26 \cdot 11^{t-2} \\ 26 \cdot 11^{t-2} & 91 \cdot 11^{t-2} + 1 & 116 \cdot 11^{t-2} \\ 116 \cdot 11^{t-2} & 21 \cdot 11^{t-2} & 86 \cdot 11^{t-2} + 1 \end{bmatrix} \pmod{11^t},$$

i.e.

$$T^{10 \cdot 11^{t-2}} \equiv E + 11^{t-2} A \pmod{11^t}, \quad \text{where} \quad A = \begin{bmatrix} 65 & 90 & 26 \\ 26 & 91 & 116 \\ 116 & 21 & 86 \end{bmatrix}.$$

In the first induction step, we verify that the congruence is true for $t = 3$.

$$T^{10\cdot 11} \equiv \begin{bmatrix} 716 & 990 & 286 \\ 286 & 1002 & 1276 \\ 1276 & 231 & 947 \end{bmatrix} \equiv E + 11A \,(\mathrm{mod}\ 11^3).$$

Suppose now that the assertion is true for a fixed $t \geqslant 3$ and let us prove it for $t+1$. Since A, E commute, using the binomial expansion we obtain that

$$\begin{aligned} T^{10\cdot 11^{t-1}} &\equiv (E + 11^{t-2}A)^{11} \equiv \sum_{i=0}^{11} \binom{11}{i} (11^{t-2}A)^i \\ &\equiv E + 11^{t-1}A + 5\cdot 11^{2t-3}A^2 \,(\mathrm{mod}\ 11^{t+1}) \end{aligned}$$

and $A^2 \equiv 0 \,(\mathrm{mod}\, 11)$ proves (3.2). □

Consequence 3.2. *Let $t \geqslant 1$ and $h = 10 \cdot 11^{t-1}$. Then for any modulus of the form 11^t the following congruences hold:*

$$\begin{aligned} & g_{h-1} \equiv 3\cdot 11^{t-1} - 1 \pmod{11^t}, && g_h \equiv 10\cdot 11^{t-1} + 1 \pmod{11^t}, \\ & g_{h+1} \equiv 4\cdot 11^{t-1} \pmod{11^t}, && g_{h+2} \equiv 6\cdot 11^{t-1} \pmod{11^t}, \\ & g_{h+3} \equiv 9\cdot 11^{t-1} + 1 \pmod{11^t}. \end{aligned} \tag{3.3}$$

P r o o f. For $t = 1$, (3.3) can be easily verified by direct calculation. For $t \geqslant 2$, (3.3) follows from (3.2). □

Theorem 3.3. *For any $t \in \mathbb{N}$ we have $h(11^t)[a, b, c] \mid 10 \cdot 11^{t-1}$ if and only if $c \equiv 3a + 5b \pmod{11}$. Moreover, for any $t > 1$, if $h(11^t)[a, b, c] \mid 10 \cdot 11^{t-2}$ then $[a, b, c] \equiv [0, 0, 0] \pmod{11}$.*

P r o o f. Let $h(11^t)[a, b, c] \mid 10 \cdot 11^{t-1}$. Then (3.3) implies

$$\begin{bmatrix} 10\cdot 11^{t-1} + 1 & 2\cdot 11^{t-1} & 4\cdot 11^{t-1} \\ 4\cdot 11^{t-1} & 3\cdot 11^{t-1} + 1 & 6\cdot 11^{t-1} \\ 6\cdot 11^{t-1} & 10\cdot 11^{t-1} & 9\cdot 11^{t-1} + 1 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \end{bmatrix} \equiv \begin{bmatrix} a \\ b \\ c \end{bmatrix} \pmod{11^t}.$$

A simple modification of the system yields

$$\begin{bmatrix} 10 & 2 & 4 \\ 4 & 3 & 6 \\ 6 & 10 & 9 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \pmod{11}.$$

The congruences of this system are linearly dependent over $\mathbb{F}_{11}$ with the entire system being equivalent to the single congruence $10a + 2b + 4c \equiv 0 \pmod{11}$. Hence, we have $c \equiv 3a + 5b \pmod{11}$.

Let $h(11^t)[a, b, c] \mid 10 \cdot 11^{t-2}$. The validity of the implication for $t = 2$ is not difficult to verify by direct calculation. If $t \geqslant 3$, then by (3.2) we have

$$\begin{bmatrix} 65 \cdot 11^{t-2} + 1 & 90 \cdot 11^{t-2} & 26 \cdot 11^{t-2} \\ 26 \cdot 11^{t-2} & 91 \cdot 11^{t-2} + 1 & 116 \cdot 11^{t-2} \\ 116 \cdot 11^{t-2} & 21 \cdot 11^{t-2} & 86 \cdot 11^{t-2} + 1 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \end{bmatrix} \equiv \begin{bmatrix} a \\ b \\ c \end{bmatrix} \pmod{11^t}.$$

This system is equivalent to

$$\begin{bmatrix} 65 & 90 & 26 \\ 26 & 91 & 116 \\ 116 & 21 & 86 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \pmod{11^2}.$$

The last system has exactly 121 non-congruent solutions over $\mathbb{Z}/11^2\mathbb{Z}$ that can be written as $[11r, 11s, 11(3r + 5s)]$ where r, s are integers. $\square$

Remark 3.4. It follows from 3.3 that, if $t \geqslant 1$ and $[a, b, c] \not\equiv [0, 0, 0] \pmod{11}$, then $h(11^t)[a, b, c]$ is equal to some of the numbers $5 \cdot 11^{t-1}, 10 \cdot 11^{t-1}, 5 \cdot 11^t, 10 \cdot 11^t$. The following lemmas will help us to determine which of the cases will occur for a given $[a, b, c]$. We will also prove that there exists no triple for which $h(11^t)[a, b, c] = 5 \cdot 11^t$.

Lemma 3.5. *For any $t \in \mathbb{N}$ we have*

$$T^{5 \cdot 11^t} \equiv A \pmod{11} \quad \text{where} \quad A = \begin{bmatrix} 7 & 4 & 6 \\ 6 & 2 & 10 \\ 10 & 5 & 1 \end{bmatrix}. \tag{3.4}$$

Moreover, $A^{2t} \equiv E \pmod{11}$.

Proof. For $t = 1$, (3.4) is true since

$$T^{55} = \begin{bmatrix} 35731770264967 & 55158741162067 & 65720971788709 \\ 65720971788709 & 101452742053676 & 120879712950776 \\ 120879712950776 & 186600684739485 & 222332455004452 \end{bmatrix} \equiv \begin{bmatrix} 7 & 4 & 6 \\ 6 & 2 & 10 \\ 10 & 5 & 1 \end{bmatrix}.$$

Let now (3.4) be true for a fixed $t \geqslant 1$. Then $T^{5 \cdot 11^{t+1}} = (T^{5 \cdot 11^t})^{11} \equiv A^{11} \pmod{11}$ and it suffices to prove that $A^{11} \equiv A \pmod{11}$. Since $A^2 \equiv E \pmod{11}$, we have $A^{2t} \equiv (A^2)^t \equiv E^t \equiv E \pmod{11}$ for any $t \in \mathbb{N}$. Consequently, $A^{11} \equiv A \pmod{11}$, which proves 3.5. $\square$

Lemma 3.6. *For any $t \in \mathbb{N}$ we have* $\det(T^{5\cdot 11^t} - E) \equiv 0 \pmod{11^{t+1}}$.

Proof. If $t = 1$, then

$$\det(T^{55} - E) = 2 \cdot 11^2 \cdot 397 \cdot 3742083511 \equiv 0 \pmod{11^2}.$$

Let the assertion be true for a fixed $t \geqslant 1$. First, it is evident that $T^{5\cdot 11^{t+1}} - E$ can be written as

$$T^{5\cdot 11^{t+1}} - E = (T^{5\cdot 11^t} - E) \cdot (E + T^{5\cdot 11^t} + T^{2\cdot 5\cdot 11^t} + \ldots + T^{10\cdot 5\cdot 11^t}). \tag{3.5}$$

Now it follows from the induction hypothesis, from (3.5) and from Cauchy's theorem that it suffices to prove that

$$\det(E + T^{5\cdot 11^t} + T^{2\cdot 5\cdot 11^t} + \ldots + T^{10\cdot 5\cdot 11^t}) \equiv 0 \pmod{11}.$$

From (3.4) it follows that

$$E + T^{5\cdot 11^t} + T^{2\cdot 5\cdot 11^t} + \ldots + T^{10\cdot 5\cdot 11^t} \equiv E + A + A^2 + \ldots + A^{10} \equiv 6E + 5A \pmod{11}.$$

As congruent matrices have congruent determinants, we have

$$\det(E + T^{5\cdot 11^t} + T^{2\cdot 5\cdot 11^t} + \ldots + T^{10\cdot 5\cdot 11^t}) \equiv \det(6E + 5A) = 132 \equiv 0 \pmod{11}.$$

This proves 3.6. □

Theorem 3.7. *For any $t \in \mathbb{N}$, the system of congruences*

$$(T^{5\cdot 11^t} - E)x \equiv 0 \pmod{11^{t+1}} \tag{3.6}$$

has exactly 11^{t+1} solutions and the number of solutions satisfying $x \not\equiv 0 \pmod{11}$ is equal to $10 \cdot 11^t$. Moreover, if α_{t+1} is a solution of $g(x) \equiv 0 \pmod{11^{t+1}}$, then each solution of (3.6) can be expressed as $[q, q\alpha_{t+1}, q\alpha_{t+1}^2]$, where $q \in \mathbb{Z}$.

Proof. Put $W = T^{5\cdot 11^t} - E \pmod{11^{t+1}}$. From (3.4) it follows that all the entries of W, except for w_{33}, are units of the ring $\mathbb{Z}/11^{t+1}\mathbb{Z}$. Since $11 \nmid \det \begin{bmatrix} 6 & 4 \\ 6 & 1 \end{bmatrix}$, there are coefficients r, s that are also units of the ring $\mathbb{Z}/11^{t+1}\mathbb{Z}$, for which

$$r(w_{11}, w_{12}) + s(w_{21}, w_{22}) \equiv (w_{31}, w_{32}) \pmod{11^{t+1}}.$$

Thus there is a linear combination of the first and second rows of W transforming $Wx \equiv 0 \pmod{11^{t+1}}$ to an equivalent form

$$(3.7)\qquad \begin{bmatrix} w_{11} & w_{12} & w_{13} \\ w_{21} & w_{22} & w_{23} \\ 0 & 0 & w'_{33} \end{bmatrix} \begin{bmatrix} a \\ b \\ c \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \pmod{11^{t+1}}.$$

Let us now prove that $w'_{33} \equiv 0 \pmod{11^{t+1}}$. Multiplying the first row in (3.7) by a suitable unit and, subsequently, adding it to the second row yields

$$(3.8)\qquad \begin{bmatrix} w_{11} & w_{12} & w_{13} \\ 0 & w'_{22} & w'_{23} \\ 0 & 0 & w'_{33} \end{bmatrix} \begin{bmatrix} a \\ b \\ c \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \pmod{11^{t+1}}.$$

The determinant of the matrix of (3.8) is $w_{11}w'_{22}w'_{33}$ and, by Lemma 3.6, we have $w_{11}w'_{22}w'_{33} \equiv 0 \pmod{11^{t+1}}$. Now it follows from (3.4) that w_{11} and w'_{22} are units of $\mathbb{Z}/p^{t+1}\mathbb{Z}$ and thus $w'_{33} \equiv 0 \pmod{11^{t+1}}$. This implies that the system $Wx \equiv 0 \pmod{11^{t+1}}$ is equivalent to the system

$$(3.9)\qquad \begin{aligned} w_{11}a + w_{12}b + w_{13}c &\equiv 0 \pmod{11^{t+1}}, \\ w_{21}a + w_{22}b + w_{23}c &\equiv 0 \pmod{11^{t+1}}, \end{aligned}$$

in which all the coefficients are units of $\mathbb{Z}/p^{t+1}\mathbb{Z}$. As no subdeterminant of the system matrix of (3.9) is divisible by 11, any of the unknowns a, b, c can be chosen as a parameter to express the other unknowns in a unique manner. Thus, each solution of $Wx \equiv 0 \pmod{11^{t+1}}$ can be written as $[qu_1, qu_2, qu_3]$ for a fixed triple of units u_1, u_2, u_3 and a parameter $q \in \mathbb{Z}$. Therefore the number of non-congruent solutions to (3.6) is equal to the number of elements of the ring $\mathbb{Z}/11^{t+1}\mathbb{Z}$, which is 11^{t+1}, and the number of solutions of the form $x \not\equiv 0 \pmod{11}$ is equal to the number of units of this ring, which is $10 \cdot 11^t$.

Let us now prove that the solutions to (3.6) are exactly the triples $[q, q\alpha_{t+1}, q\alpha_{t+1}^2]$ where $q \in \mathbb{Z}$. As the number of non-congruent triples $[q, q\alpha_{t+1}, q\alpha_{t+1}^2]$ is equal to 11^{t+1}, it suffices to show that $h(11^{t+1})[q, q\alpha_{t+1}, q\alpha_{t+1}^2] \mid 5 \cdot 11^t$. As $\alpha = 9$ is a simple root of $g(x) \equiv 0 \pmod{11}$, we obtain by Hensel's lemma, that for each $t \in \mathbb{N}$ there is α_t, which is uniquely determined modulo 11^t, satisfying $g(x) \equiv 0 \pmod{11^t}$ and such that $\alpha_1 = \alpha$ and $\alpha_t \equiv \alpha_{t-1} \pmod{11^{t-1}}$. Let $\mathrm{ord}_{11^t}(\varepsilon)$ for $\varepsilon \not\equiv 0 \pmod{11}$ denote the order of ε in the multiplicative group of $\mathbb{Z}/11^t\mathbb{Z}$. Clearly, $h(11^{t+1})[q, q\alpha_{t+1}, q\alpha_{t+1}^2] = \mathrm{ord}_{11^{t+1}}(\alpha_{t+1})$ for any $q \in \mathbb{Z}$ where $q \not\equiv 0 \pmod{11}$. From $\mathrm{ord}_{11}(\alpha_1) = 5$ and $\alpha_{t+1} \equiv \alpha_1 \pmod{11}$ it now follows $\alpha_{t+1}^5 \equiv 1 \pmod{11}$ for any $t \in \mathbb{N}$ and thus $\alpha_{t+1}^{5\cdot 11^t} \equiv 1 \pmod{11^{t+1}}$. Hence $\mathrm{ord}_{11^{t+1}}(\alpha_{t+1}) \mid 5 \cdot 11^t$. □

According to Theorem 3.7, the set of all non-congruent solutions to (3.6) can be written as $E(\alpha_{t+1}) = \{[q, q\alpha_{t+1}, q\alpha_{t+1}^2], q \in \mathbb{Z}/p^{t+1}\mathbb{Z}\}$ and viewed as the eigenspace associated with the eigenvalue α_{t+1}.

R e m a r k 3.8. The equality $\operatorname{ord}_{11^t}(\alpha_t) = 5 \cdot 11^{t-1}$ is a non-trivial consequence of 3.3 and 3.7 for each $t \in \mathbb{N}$. See also Lemma 4.6 in [1].

Lemma 3.9. *There exists no triple $[a, b, c]$ for which $h(11^t)[a, b, c] = 5 \cdot 11^t$.*

P r o o f. It suffices to prove that the systems $(T^{5\cdot 11^{t-1}} - E)x \equiv 0 \pmod{11^t}$ and $(T^{5\cdot 11^t} - E)x \equiv 0 \pmod{11^t}$ have identical solution sets for any $t \geqslant 1$. Denote by X the set of all solutions of $(T^{5\cdot 11^{t-1}} - E)x \equiv 0 \pmod{11^t}$ and by Y the set of all solutions of $(T^{5\cdot 11^t} - E)x \equiv 0 \pmod{11^t}$. The inclusion $X \subseteq Y$ follows immediately from the equality

$$T^{5\cdot 11^t} - E = (E + T^{5\cdot 11^{t-1}} + T^{2\cdot 5\cdot 11^{t-1}} + \ldots + T^{10\cdot 5\cdot 11^{t-1}}) \cdot (T^{5\cdot 11^{t-1}} - E).$$

Modifying the proof of 3.7, we can determine that $(T^{5\cdot 11^t} - E)x \equiv 0 \pmod{11^t}$ has 11^t solutions, thus the same number as $(T^{5\cdot 11^{t-1}} - E)x \equiv 0 \pmod{11^t}$. The equality of the sets X and Y follows from their finiteness. $\square$

Now we can summarize our results in the main theorem:

Theorem 3.10. *For any triple $[a, b, c] \not\equiv [0, 0, 0] \pmod{11}$, we have:*
If $[a, b, c] \notin E(\alpha_t)$ and $c \equiv 3a + 5b \pmod{11}$, then $h(11^t)[a, b, c] = 10 \cdot 11^{t-1}$.
If $[a, b, c] \notin E(\alpha_t)$ and $c \not\equiv 3a + 5b \pmod{11}$, then $h(11^t)[a, b, c] = 10 \cdot 11^t$.
If $[a, b, c] \in E(\alpha_t)$, then $h(11^t)[a, b, c] = \operatorname{ord}_{11^t}(\alpha_t) = 5 \cdot 11^{t-1}$.

References

[1] *J. Klaška*: Tribonacci modulo p^t. Math. Bohem. *133* (2008), 267–288.
[2] *A. Vince*: Period of a linear recurrence. Acta Arith. *39* (1981), 303–311.
[3] *M. E. Waddill*: Some properties of a generalized Fibonacci sequence modulo m. The Fibonacci Quarterly *16* (Aug. 1978), 344–353.

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.