Mathematica Bohemica

Jiří Klaška

Tribonacci modulo p^t

Mathematica Bohemica, Vol. 133 (2008), No. 3, 267–288

Persistent URL: http://dml.cz/dmlcz/140617

TRIBONACCI MODULO p^t

Jiří Klaška, Brno

(Received February 16, 2007)

Abstract. Our research was inspired by the relations between the primitive periods of sequences obtained by reducing Tribonacci sequence by a given prime modulus p and by its powers p^t, which were deduced by M. E. Waddill. In this paper we derive similar results for the case of a Tribonacci sequence that starts with an arbitrary triple of integers.

Keywords: Tribonacci, modular periodicity, periodic sequence

MSC 2010: 11B50, 11B39

1. Introduction—known results

Let $(g_n)_{n=1}^{\infty}$ be a Tribonacci sequence $0, 0, 1, 1, 2, 4, 7, 13, 24, 44, 81, \ldots$ defined by the recurrence $g_{n+3} = g_{n+2} + g_{n+1} + g_n$ and the triple $[0, 0, 1]$ of initial values. Further, let $(G_n)_{n=1}^{\infty}$ be the Tribonacci sequence defined by an arbitrary triple of integers $[a, b, c]$. It is well known that the sequences $(g_n \bmod m)_{n=1}^{\infty}$ and $(G_n \bmod m)_{n=1}^{\infty}$ are periodical for an arbitrary modulus $m > 1$. We denote by $h(m)$ and $h(m)[a, b, c]$ the primitive periods of these sequences. In this paper we derive a relationship between the numbers $h(p)[a, b, c]$ and $h(p^t)[a, b, c]$ where p is an arbitrary prime, $p \neq 2, 11$ and $t \in \mathbb{N} = \{1, 2, 3, \ldots\}$. The case of the primes $p = 2, 11$ is solved in [2]. It can be proved that, if L is the splitting field of the Tribonacci polynomial $g(x) = x^3 - x^2 - x - 1$ over the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, $p \neq 2, 11$ and α, β, γ are the roots of $g(x)$ in L, then $h(p) = \operatorname{lcm}(\operatorname{ord}_L(\alpha), \operatorname{ord}_L(\beta), \operatorname{ord}_L(\gamma))$ where the numbers $\operatorname{ord}_L(\alpha)$, $\operatorname{ord}_L(\beta)$, $\operatorname{ord}_L(\gamma)$ are the orders of α, β, γ in the multiplicative group of L and lcm is their least common multiple. See [5]. Let T be a Tribonacci matrix where

$$(1.1)\qquad T = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix} \quad \text{and} \quad T^n = \begin{bmatrix} g_n & g_{n-1} + g_n & g_{n+1} \\ g_{n+1} & g_n + g_{n+1} & g_{n+2} \\ g_{n+2} & g_{n+1} + g_{n+2} & g_{n+3} \end{bmatrix} \quad \text{for } n > 1.$$

Clearly, for an arbitrary $n \in \mathbb{N}$ and an arbitrary modulus m, T^n assumes a unique form $T^n = B + mA$ where $A = [a_{ij}]$, $B = [b_{ij}]$ are integer matrices such that $0 \leqslant b_{ij} \leqslant m - 1$ and a_{ij} are nonnegative integers. Specifically, if $n = h(m)$, then $T^{h(m)} \equiv E \pmod m$ where E is the identity matrix. Thus, we can express $T^{h(m)}$ as $T^{h(m)} = E + mA$. We will use this fact in an alternative proof of Theorem 1.1 published by M. E. Waddill in 1978, see [6], p. 349. The proof that we will submit is based on matrix algebra. Its modification can also be used for the general case of linear recurrences of order k. This particularly applies to the case of Fibonacci sequences. For a proof of this, see [7], p. 527.

Theorem 1.1. *Let p be an arbitrary prime and $h(p) \neq h(p^2)$. Then*

$$h(p^t) = p^{t-1}h(p) \tag{1.2}$$

for all $t \in \mathbb{N}$.

Proof. We can write the matrix $T^{h(p^t)}$ as $T^{h(p^t)} = E + p^tA$. Using binomial expansion, we have

$$T^{ph(p^t)} = (E + p^tA)^p = \sum_{i=0}^{p} \binom{p}{i} E^{p-i}(p^tA)^i.$$

Passing from equality to congruence by the modulus p^{t+1}, we get

$$T^{ph(p^t)} \equiv E \pmod{p^{t+1}}.$$

Since $h(p^{t+1})$ is the primitive period, we have $h(p^{t+1}) \mid ph(p^t)$. Next, it is obvious that $h(p^t) \mid h(p^{t+1})$, which means that exactly one of the following equations is true:

$$h(p^{t+1}) = h(p^t) \quad \text{or} \quad h(p^{t+1}) = ph(p^t). \tag{1.3}$$

Now we use induction by t. For $t = 1$ the assertion is evident and for $t = 2$ it follows from the assumption. Assuming that $h(p^t) = ph(p^{t-1}) = p^{t-1}h(p)$ holds for a number $t \geqslant 1$, we will prove this equation for $t + 1$. The induction assumption $h(p^{t-1}) \neq h(p^t)$ implies $T^{h(p^{t-1})} = E + p^{t-1}A$ where $p \nmid A$. Thus we have

$$T^{ph(p^{t-1})} = (E + p^{t-1}A)^p = \sum_{i=0}^{p} \binom{p}{i} E^{p-i}(p^{t-1}A)^i.$$

Hence $T^{h(p^t)} = T^{ph(p^{t-1})} \not\equiv E \pmod{p^{t+1}}$ and $h(p^t) \neq h(p^{t+1})$. Next, from (1.3) we have $h(p^{t+1}) = ph(p^t)$ and $h(p^{t+1}) = p^th(p)$. □

Remark 1.2. The congruence $T^{ph(p^{t-1})} \equiv E + p^tA \pmod{p^{t+1}}$ does not hold for $p = 2$, $t = 2$. This fact, however, is irrelevant for the proof of 1.1. We omit the details.

Theorem 1.3. *Let $s \in \mathbb{N}$ satisfy $h(p) = h(p^2) = \ldots = h(p^s) \neq h(p^{s+1})$. Then, for an arbitrary $t \geqslant s$, we have $h(p^t) = p^{t-s}h(p)$.*

Proof. We proceed by analogy with 1.1. □

Problem 1.4. The question of whether the assumption $h(p) \neq h(p^2)$ is necessary or whether the equality $h(p) = h(p^2)$ never occurs is open. Up to the present, no instance of $h(p) = h(p^2)$ has been found. Neither is it proved that such an equality can never hold. However, for sequences defined by a general linear recurrence of order three, the condition $h(p) \neq h(p^2)$ need not be satisfied. If $(g_n)_{n=1}^{\infty}$ is a sequence defined by the recurrence $g_{n+3} = 2g_{n+2} - g_{n+1} + g_n$ and the triple of initial values $[0, 0, 1]$, then $h(2) = h(2^2) = 7$. A similar problem has been discussed in the case of a Fibonacci sequence. In [4] it is proved that the affirmative answer to the question whether $h(p) \neq h(p^2)$ holds for all primes implies the validity of the first case of Fermat's last theorem. However, questions related to the validity of the equation $h(p) = h(p^2)$ are not investigated in this paper. In the sequel, we will always assume $h(p) \neq h(p^2)$.

2. Elementary observations

The primary aim of this paper is to prove theorems similar to 1.1 for the case of a Tribonacci sequence beginning with an arbitrary triple $[a, b, c]$ of integers. Evidently, the relation $h(p^t)[a, b, c] = p^{t-1}h(p)[a, b, c]$ is generally not valid. We have, for instance, $h(p)[0, 0, 0] = h(p^t)[0, 0, 0] = 1$ for arbitrary p, t. Put $x_0 = [a, b, c]^\tau$ and $x_n = [G_{n+1}, G_{n+2}, G_{n+3}]^\tau$ where τ is the transposition. Then x_n can be expressed in terms of x_0 using the equation $x_n = T^n x_0$. If a Tribonacci sequence is determined by the triple $[0, 0, 1]$, then $h(m)$ is the smallest number h for which $T^h \equiv E \pmod{m}$. In the following example, we will show that, to an arbitrary triple $[a, b, c]$, this rule need not apply.

Example 2.1. Let $p = 7$ and $x_0 = [1, 3, 2]^\tau$. We can verify easily that $T^6 \not\equiv E$ (mod 7) while $T^6 x_0 \equiv x_0$ (mod 7). Since the congruence $T^h x_0 \equiv x_0$ (mod 7) holds for no $h < 6$, we have $h(7)[1, 3, 2] = 6$. Assuming results analogous to 1.1, one could expect that $h(7^2)[1, 3, 2] = 42$. However, $h(7^2)[1, 3, 2] = 336$.

The relationships between the numbers $h(p^t)[a, b, c]$ and $h(p)[a, b, c]$ clearly seem to be more complex and are worth closer study. First we will prove two simple but important lemmas.

Lemma 2.2. *Let p be an arbitrary prime. Then, for every $t \in \mathbb{N}$ and $1 \leqslant i \leqslant t$, we have*

$$h(p^t)[p^{t-i}a, p^{t-i}b, p^{t-i}c] = h(p^i)[a, b, c]. \tag{2.1}$$

Proof. (2.1) follows from the equality

$$(p^{t-i}G_n \bmod p^t)_{n=1}^{\infty} = p^{t-i} \cdot (G_n \bmod p^i)_{n=1}^{\infty}.$$

□

Using (2.1), the investigation of the periods for general triples $[a, b, c]$ can be reduced to the case with $[a, b, c] \not\equiv [0, 0, 0] \pmod p$. Particularly, for $i = 1$, (2.1) yields $h(p^t)[p^{t-1}a, p^{t-1}b, p^{t-1}c] = h(p)[a, b, c]$.

Lemma 2.3. *Let p be an arbitrary prime. For every triple $[a, b, c]$ and every $s, t \in \mathbb{N}$ where $s \leqslant t$ we have $h(p^s)[a, b, c] \mid h(p^t)[a, b, c]$. In particular, we have*

$$h(p)[a, b, c] \mid h(p^t)[a, b, c]. \tag{2.2}$$

Proof. Put $h = h(p^s)[a, b, c]$, $k = h(p^t)[a, b, c]$ and $x_0 = [a, b, c]^{\tau}$. Then, from $T^k x_0 \equiv x_0 \pmod{p^t}$, it follows that $T^k x_0 \equiv x_0 \pmod{p^s}$. This means that k is a period of the Tribonacci sequence beginning with the triple $[a, b, c]$ reduced by the modulus p^s. Since the primitive period divides an arbitrary period, we have $h \mid k$.

□

Moreover, $T^{h(p^t)} \equiv E \pmod{p^t}$ implies $T^{h(p^t)}x_0 \equiv x_0 \pmod{p^t}$ for any $x_0 = [a, b, c]^{\tau}$ and $t \in \mathbb{N}$ and therefore $x_{h(p^t)} \equiv x_0 \pmod{p^t}$. Consequently, we have

$$h(p^t)[a, b, c] \mid h(p^t). \tag{2.3}$$

Lemma 2.3 together with (2.3) restricts the form of the numbers $h(p^t)[a, b, c]$. As we will see in the sequel, the relations between $h(p^t)[a, b, c]$ and $h(p)[a, b, c]$ also depend on the form of the factorization of the polynomial $g(x)$ over the field $\mathbb{F}_p$.

3. Irreducible case

In the investigation of primitive periods of Tribonacci sequences beginning with arbitrary triples $[a,b,c]$, the cubic form

$$D(a,b,c) = a^3 + 2b^3 + c^3 - 2abc + 2a^2b + 2ab^2 - 2bc^2 + a^2c - ac^2 \tag{3.1}$$

plays an important role. By means of $D(a,b,c)$, we can prove a theorem similar to 1.1 for the case of $g(x)$ being irreducible over $\mathbb{F}_p$. (3.1) was studied in other circumstances as well. See [1].

Theorem 3.1. *If a triple of initial values $[a,b,c]$ of a Tribonacci sequence $(G_n)_{n=1}^{\infty}$ satisfies $(D(a,b,c),m) = 1$, then $h(m)[a,b,c] = h(m)$.*

Proof. For $n \geqslant 1$, the sequences $(g_n)_{n=1}^{\infty}$ and $(G_n)_{n=1}^{\infty}$ satisfy

$$G_{n+3} = bg_{n+1} + (a+b)g_{n+2} + cg_{n+3}. \tag{3.2}$$

If we put $h(m)[a,b,c] = h$, we have $[G_{h+1}, G_{h+2}, G_{h+3}] \equiv [a,b,c] \pmod{m}$. By substituting into (3.2) and after some simplification, we get

$$\begin{bmatrix} c-b-a & b-a & a \\ a & c-b & b \\ b & a+b & c \end{bmatrix} \cdot \begin{bmatrix} g_{h+1} \\ g_{h+2} \\ g_{h+3} \end{bmatrix} \equiv \begin{bmatrix} a \\ b \\ c \end{bmatrix} \pmod{m}. \tag{3.3}$$

The system of congruences (3.3) can be further modified to the form

$$\begin{bmatrix} c-b-a & b-a & a \\ a & c-b & b \\ b & a+b & c \end{bmatrix} \cdot \begin{bmatrix} g_{h+1} \\ g_{h+2} \\ g_{h+3}-1 \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \pmod{m}, \tag{3.4}$$

where the determinant of the matrix of system (3.4) depends only on a, b, c and is equal to $D(a,b,c)$. System (3.4) has only one solution if and only if the numbers $D(a,b,c)$, m are coprime. In this case we have $[g_{h+1}, g_{h+2}, g_{h+3}] \equiv [0,0,1] \pmod{m}$ and thus $h(m) \mid h$. Since also $h \mid h(m)$, $h = h(m)$ follows. □

Corollary 3.2. *Let $u_1 = [a,b,c]$, $u_2 = [b,c,a+b+c]$, $u_3 = [c, a+b+c, a+2b+2c]$. Then u_1, u_2, u_3 are linearly independent over $\mathbb{F}_p$ if and only if $D(a,b,c) \not\equiv 0 \pmod{p}$. Moreover, the linear independence of u_1, u_2, u_3 implies $h(p)[a,b,c] = h(p)$.*

Proof. By elementary column transformations, the matrix of system (3.4) can be converted to the form

$$M = \begin{bmatrix} a & b & c \\ b & c & a+b+c \\ c & a+b+c & a+2b+2c \end{bmatrix} \quad \text{where } \det M = -D(a,b,c).$$

Hence, it follows that the rows of M are linearly independent over $\mathbb{F}_p$ if and only if $D(a,b,c) \not\equiv 0 \pmod{p}$. Now, from 3.1 it follows that $h(p)[a,b,c] = h(p)$. □

Remark 3.3. Generally, the equality of periods $h(p)[a,b,c] = h(p)$ does not imply linear independence of u_1, u_2, u_3 over $\mathbb{F}_p$.

Lemma 3.4. *A triple $[a,b,c]$ satisfies the congruence $D(a,b,c) \equiv 0 \pmod{p}$ if and only if the sequence $(G_n \bmod p)_{n=1}^{\infty}$ determined by $[a,b,c]$ can be defined by a first or second order recurrence formula.*

Proof. If $D(a,b,c) \equiv 0 \pmod{p}$, then it follows from 3.2 that u_1, u_2, u_3 are linearly dependent. Let first u_1, u_2 be linearly dependent. Then there is a $q \in \mathbb{Z}$ such that

$$q[a,b,c] \equiv [b,c,a+b+c] \pmod{p}. \tag{3.5}$$

Matching the terms, we obtain $G_n \equiv aq^{n-1} \pmod{p}$ from (3.5) by induction, which means that $(G_n \bmod p)_{n=1}^{\infty}$ can be defined over $\mathbb{F}_p$ by the first order recurrence $G_{n+1} \equiv qG_n \pmod{p}$ where $G_1 = a$. Suppose that u_1, u_2 are independent and u_1, u_2, u_3 dependent. This means that there are $q_1, q_2 \in \mathbb{Z}$ such that

$$q_1[a,b,c] + q_2[b,c,a+b+c] \equiv [c, a+b+c, a+2b+2c] \pmod{p}. \tag{3.6}$$

By analogy, it follows from (3.6) that $(G_n \bmod p)_{n=1}^{\infty}$ can be defined over $\mathbb{F}_p$ by a recurrence $G_{n+2} \equiv q_1 G_n + q_2 G_{n+1} \pmod{p}$ where $G_1 = a$, $G_2 = b$.

Conversely, suppose that $(G_n \bmod p)_{n=1}^{\infty}$ can be defined by a recurrence of order at most two. This implies that u_1, u_2, u_3 are dependent over $\mathbb{F}_p$ and, by 3.2, we have $D(a,b,c) \equiv 0 \pmod{p}$. □

Remark 3.5. There are sequences $(G_n \bmod p)_{n=1}^{\infty}$ that can be defined over $\mathbb{F}_p$ by a recurrence formula of order at most two and $h(p)[a,b,c] = h(p)$.

Let us now investigate the number of all solutions of the congruence

$$D(a,b,c) \equiv 0 \pmod{p}. \tag{3.7}$$

As we shall see in Lemmas 3.6 and 3.7, the number of solutions of (3.7) depends on the form of the factorization of $g(x) = x^3 - x^2 - x - 1$ over $\mathbb{F}_p$.

Lemma 3.6. *Let $g(x)$ be irreducible over $\mathbb{F}_p$. Then the only solution of* (3.7) *is* $[a,b,c] \equiv [0,0,0] \pmod p$.

Proof. Let L be the splitting field of $g(x)$ over $\mathbb{F}_p$. The irreducibility of $g(x)$ gives that $[L:\mathbb{F}_p] = 3$. The Galois group of $L/\mathbb{F}_p$ is generated by the Frobenius automorphism $\sigma\colon L \to L$ determined by $\sigma(t) = t^p$ for any $t \in L$. Let $\alpha \in L$ be a root of $g(x)$. Then $\beta = \sigma(\alpha)$ and $\gamma = \sigma(\beta)$ are the other roots of $g(x)$ and we have $\alpha^p = \beta$, $\beta^p = \gamma$, $\gamma^p = \alpha$. There are unique $A, B, C \in L$ such that

$$G_n \bmod p = A\alpha^n + B\beta^n + C\gamma^n \tag{3.8}$$

for each $n \in \mathbb{N}$. Moreover, $G_n \in \mathbb{Z}$, and so $A\alpha^n + B\beta^n + C\gamma^n = \sigma(A\alpha^n + B\beta^n + C\gamma^n) = \sigma(A)\beta^n + \sigma(B)\gamma^n + \sigma(C)\alpha^n$, which gives

$$B = \sigma(A) = A^p, \quad C = \sigma(B) = B^p, \quad A = \sigma(C) = C^p. \tag{3.9}$$

It follows from (3.9) that A, B, C are either all non-zero or $A = B = C = 0$. Hence by (3.8), the sequence $(G_n \bmod p)_{n=1}^{\infty}$ cannot be, with the exception of the sequence beginning with $[0,0,0]$, defined by a recurrence formula of the first or second order. Lemma 3.6 now follows from 3.4. □

Lemma 3.7. *Let $g(x)$ be factorized over $\mathbb{F}_p$, $p \neq 2, 11$, into the product of a linear factor and an irreducible quadratic factor. Then* (3.7) *has exactly $p^2 + p - 1$ solutions. Let $g(x)$ be factored over $\mathbb{F}_p$, $p \neq 2, 11$, into the product of linear factors. Then* (3.7) *has exactly $3p^2 - 3p + 1$ solutions.*

Proof. If $p \neq 2, 11$ then $g(x)$ has only simple roots in the splitting field L of $g(x)$ over $\mathbb{F}_p$, and so a Tribonacci sequence can be expressed in the form $G_n = c_1\alpha^n + c_2\beta^n + c_3\gamma^n$ where α, β, γ are the roots of $g(x)$ in L and $c_i \in L$. It is evident that $D(a,b,c) \equiv 0 \pmod p$ if and only if $c_i = 0$ for some $i = 1,2,3$. The assertion of the lemma can now be proved by a suitable use of the inclusion-exclusion principle. We leave the details to the reader. □

Corollary 3.8. *Let $p \neq 2, 11$. Then the number of all triples $[a,b,c]$ where $0 \leqslant a,b,c \leqslant p^t - 1$ such that $D(a,b,c) \not\equiv 0 \pmod p$ is equal to $p^{3(t-1)}(p^3-1)$ if $g(x)$ is irreducible over $\mathbb{F}_p$, $p^{3(t-1)}(p^3 - 3p^2 + 3p - 1)$ if $g(x)$ can be factorized over $\mathbb{F}_p$ into the product of linear factors, and $p^{3(t-1)}(p^3 - p^2 - p + 1)$ otherwise.*

Proof. Let $D(a_0,b_0,c_0) \not\equiv 0 \pmod p$ for $0 \leqslant a_0, b_0, c_0 \leqslant p-1$. Then also $D(a,b,c) \not\equiv 0 \pmod p$ for arbitrary $0 \leqslant a,b,c \leqslant p^t - 1$ such that $[a,b,c] \equiv [a_0,b_0,c_0] \pmod p$. The claim now follows from 3.6 and 3.7. □

Remark 3.9. The case of $g(x)$ having multiple roots over $\mathbb{F}_p$ leads to the investigation of the primes $p = 2, 11$ (see [2]). For $p = 2$, (3.7) has exactly 4 solutions and, for $p = 11$, it has exactly 231 solutions.

Theorem 3.10. *Let p be an arbitrary prime such that $g(x)$ is irreducible over $\mathbb{F}_p$. If $[a, b, c] \not\equiv [0, 0, 0] \pmod{p}$ and $h(p) \neq h(p^2)$, then*

$$h(p^t)[a, b, c] = p^{t-1}\, h(p)[a, b, c] = p^{t-1} h(p) \tag{3.10}$$

for an arbitrary $t \in \mathbb{N}$.

Proof. The proof follows imediately from 1.1, 3.1 and 3.6. □

If $g(x)$ is not irreducible, it is easy to find examples of triples $[a, b, c]$ for which (3.7) holds and $h(p^t)[a, b, c] = h(p^t)$. Consequently, the form $D(a, b, c)$ cannot be expected to enable us to describe the relationships between the primitive periods if $g(x)$ has at least one root over $\mathbb{F}_p$.

4. The case of an irreducible quadratic factor

Let us now deal with the case of a Tribonacci polynomial $g(x)$ having over $\mathbb{F}_p$ a factorization of the form

$$g(x) \equiv (x - \alpha_1)(x^2 - s_1 x - r_1) \pmod{p}, \tag{4.1}$$

where the polynomial $g_1(x) = x^2 - s_1 x - r_1$ is irreducible over $\mathbb{F}_p$. Since α_1 is a unique solution to $g(x) \equiv 0 \pmod{p}$, by Hensel's lemma there is a unique solution α_t to the congruence $g(x) \equiv 0 \pmod{p^t}$. Moreover, for α_t we have $\alpha_t \equiv \alpha_1 \pmod{p}$. This implies $(x - \alpha_t) \mid g(x)$ and there is a unique polynomial $g_t(x) = x^2 - s_t x - r_t \in \mathbb{Z}/p^t\mathbb{Z}[x]$ such that $g(x) \equiv (x - \alpha_t)(x^2 - s_t x - r_t) \pmod{p^t}$ where α_t, r_t, s_t are units of the ring $\mathbb{Z}/p^t\mathbb{Z}$ for which

$$s_t \equiv 1 - \alpha_t \pmod{p^t}, \quad r_t \equiv 1 + \alpha_t - \alpha_t^2 \pmod{p^t}. \tag{4.2}$$

Let us denote by $\operatorname{ord}_{p^t}(\alpha_t)$ the order of α_t in the group of units of the ring $\mathbb{Z}/p^t\mathbb{Z}$. Clearly, $\operatorname{ord}_{p^t}(\alpha_t) \mid p^{t-1}(p-1)$.

Lemma 4.1. *Let $(G_n)_{n=1}^{\infty}$ be the Tribonacci sequence determined by $[a, a\alpha_t, a\alpha_t^2]$. Then, for $(H_n)_{n=1}^{\infty}$ defined by $H_{n+1} = \alpha_t H_n$ and $H_1 = a$, we have $G_n \equiv H_n \pmod{p^t}$ for any $n \in \mathbb{N}$.*

Proof. Clearly, for $n = 1, 2, 3$ the claim holds. Let $n > 3$. Then $H_n = \alpha_t H_{n-1} \equiv \alpha_t^3 H_{n-3} \equiv (1 + \alpha_t + \alpha_t^2) H_{n-3} \equiv H_{n-3} + H_{n-2} + H_{n-1} \equiv G_n \pmod{p^t}$. □

Remark 4.2. Generally, the primitive period of a sequence $(a\alpha_t^n \bmod p^t)_{n=0}^{\infty}$ where $a \in \mathbb{N}$ does not depend only on the order of α_t in $\mathbb{Z}/p^t\mathbb{Z}$, but also on the coefficient a. If $p \nmid a$, then the primitive period of this sequence is equal to $\operatorname{ord}_{p^t}(\alpha_t)$. If $p^i \mid a$ where $0 \leqslant i \leqslant t-1$, then the primitive period equals $\operatorname{ord}_{p^{t-i}}(\alpha_{t-i})$.

Lemma 4.3. *Let $(G_n)_{n=1}^{\infty}$ be the Tribonacci sequence determined by $[a, b, r_t a + s_t b]$. Then for $(H_n)_{n=1}^{\infty}$ defined by $H_{n+2} = r_t H_n + s_t H_{n+1}$ with $H_1 = a$ and $H_2 = b$ we have $G_n \equiv H_n \pmod{p^t}$ for any $n \in \mathbb{N}$.*

Proof. For $n = 1, 2, 3$, the congruence $G_n \equiv H_n \pmod{p^t}$ holds. Let $n > 3$. Then

$$H_n \equiv r_t H_{n-2} + s_t H_{n-1} \equiv (r_t + s_t^2) H_{n-2} + r_t s_t H_{n-3} \pmod{p^t}. \tag{4.3}$$

The congruences (4.2) and $\alpha_t^3 \equiv \alpha_t^2 + \alpha_t + 1 \pmod{p^t}$ imply

$$r_t s_t \equiv 2 + \alpha_t - \alpha_t^2 \pmod{p^t}, \quad s_t^2 \equiv 1 - 2\alpha_t + \alpha_t^2 \pmod{p^t}. \tag{4.4}$$

By substituting (4.4) into (4.3) we obtain $H_n \equiv (2 - \alpha_t) H_{n-2} + (2 + \alpha_t - \alpha_t^2) H_{n-3} \equiv (1 + s_t) H_{n-2} + (1 + r_t) H_{n-3} \equiv H_{n-1} + H_{n-2} + H_{n-3} \equiv G_n \pmod{p^t}$. □

Remark 4.4. It is easy to find triples $[a, b, c]$ with $0 \leqslant a, b, c \leqslant p^t - 1$ and $t > 1$ such that $D(a, b, c) \equiv 0 \pmod{p^t}$ while $(G_n \bmod p^t)_{n=1}^{\infty}$ cannot be defined by a recurrence of order one or two. Thus, an analogue of Lemma 3.4 for the rings $\mathbb{Z}/p^t\mathbb{Z}$ cannot be proved. On the other hand, it is not difficult to prove that the sequences in 4.1 and 4.3 are the only ones that can be defined by lower order recurrences. In this case, of course, we have $D(a, b, c) \equiv 0 \pmod{p^t}$.

Theorem 4.5. *Let p be an arbitrary prime, $p \neq 2, 11$ and let $h = h(p) \neq h(p^2)$. Further, let $A = p^{-1}(T^h - E)$. The system*

$$T^{p^{t-2}h} x \equiv x \pmod{p^t} \tag{4.5}$$

has $p^{3(t-1)}$ trivial solutions $[a, b, c] \equiv [0, 0, 0] \pmod{p}$. If $p \nmid \det A$ then (4.5) has no nontrivial solution. If $p \mid \det A$ then (4.5) has $(p-1)p^{3(t-1)}$ non-congruent nontrivial solutions.

Proof. From $h(p) \neq h(p^2)$ and 1.1 we can show by induction that, for an arbitrary $t > 1$, we have

$$T^{p^{t-2}h} \equiv E \pmod{p^{t-1}}, \quad T^{p^{t-2}h} \equiv E + p^{t-1}A \pmod{p^t} \tag{4.6}$$

and $p \nmid A$. By (4.6), the system (4.5) is equivalent to the system $(E + p^{t-1}A)x \equiv x \pmod{p^t}$ and thus to the system $Ax \equiv 0 \pmod{p}$. Clearly, this system has a unique solution $x \equiv 0 \pmod{p}$ if and only if $p \nmid \det A$. In this case, the solution of (4.5) is formed exactly by triples of the form $[a, b, c] \equiv [0, 0, 0] \pmod{p}$ and the number of non-congruent solutions of this form is equal to $p^{3(t-1)}$.

Let $A = [a_{ij}]$. It follows form (4.6) that $\det T^{p^{t-2}h}$ can be written as

$$\det T^{p^{t-2}h} \equiv 1 + p^{t-1}(a_{11} + a_{22} + a_{33}) + p^{2(t-1)} \sum_{i=1}^{3} \det A_i + p^{3(t-1)} \det A \pmod{p^t},$$

where A_i is the submatrix of A obtained by deleting the i-th row and i-th column in A. For $t > 1$, this implies

$$\det T^{p^{t-2}h} \equiv 1 + p^{t-1}(a_{11} + a_{22} + a_{33}) \pmod{p^t}. \tag{4.7}$$

Since $\det T = 1$, by the Cauchy theorem we have $\det T^n = 1$ for an arbitrary $n \in \mathbb{N}$. This yields $\det T^{p^{t-2}h} \equiv 1 \pmod{p^t}$. Combining this with (4.7), we get

$$a_{11} + a_{22} + a_{33} \equiv 0 \pmod{p}. \tag{4.8}$$

From (1.1) it follows that each of the entries of $A = [a_{ij}]$ reduced by modulus p can be expressed using only the three values a_{11}, a_{21}, a_{31} so that

$$A \equiv \begin{bmatrix} a_{11} & a_{31} - a_{21} & a_{21} \\ a_{21} & a_{11} + a_{21} & a_{31} \\ a_{31} & a_{21} + a_{31} & a_{11} + a_{21} + a_{31} \end{bmatrix} \pmod{p}. \tag{4.9}$$

Now it follows from (4.8) that

$$3a_{11} + 2a_{21} + a_{31} \equiv 0 \pmod{p}. \tag{4.10}$$

Using (4.10) we can simplify (4.9) to

$$A \equiv \begin{bmatrix} a_{11} & -3a_{11} - 3a_{21} & a_{21} \\ a_{21} & a_{11} + a_{21} & -3a_{11} - 2a_{21} \\ -3a_{11} - 2a_{21} & -3a_{11} - a_{21} & -2a_{11} - a_{21} \end{bmatrix} \pmod{p}. \tag{4.11}$$

Suppose that $p \mid \det A$. Then the rows of A are linearly dependent over $\mathbb{F}_p$. Suppose first that the first two rows of A are dependent. Then there is $q \in \mathbb{Z}$ such that

$$q[a_{11}, -3a_{11} - 3a_{21}, a_{21}] \equiv [a_{21}, a_{11} + a_{21}, -3a_{11} - 2a_{21}] \pmod{p}. \tag{4.12}$$

Matching the terms and using $p \nmid A$, we obtain

$$3q^2 + 4q + 1 \equiv 0 \pmod{p} \text{ and } q^2 + 2q + 3 \equiv 0 \pmod{p}. \tag{4.13}$$

It follows from (4.13) that $2q + 8 \equiv 0 \pmod{p}$. As $p \neq 2$, we have $q \equiv -4 \pmod{p}$. Substituting into the second congruence in (4.13) yields $11 \equiv 0 \pmod{p}$. Hence $p = 11$, and we get a contradiction.

Next, suppose that the first two rows of A are independent and $p \mid \det A$. It follows from (4.11) and from $p \nmid A$ that at least one of the relations $p \nmid a_{11}$ and $p \nmid a_{21}$ is true. Suppose $p \mid a_{11}$ and $p \nmid a_{21}$. Then from (4.11) we have $\det A \equiv -14a_{21}^3 \pmod{p}$ and thus $14 \equiv 0 \pmod{p}$. As $p \neq 2$, we have $p = 7$. We can verify that $h(7) = 48$. Then for the corresponding matrix A we have

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

Hence $a_{11} \equiv 4 \pmod{7}$, which is a contradiction with $p \mid a_{11}$. It follows now from the above that there is $\varepsilon \in \mathbb{Z}$ such that

$$a_{21} \equiv a_{11}\varepsilon \pmod{p}. \tag{4.14}$$

Substituting (4.14) into (4.11) then yields

$$\det A \equiv a_{11}^3(14\varepsilon^3 + 58\varepsilon^2 + 78\varepsilon + 38) \pmod{p}. \tag{4.15}$$

Since $p \nmid a_{11}$, $p \neq 2$ and $p \mid \det A$, it follows from (4.15) that

$$7\varepsilon^3 + 29\varepsilon^2 + 39\varepsilon + 19 \equiv 0 \pmod{p}. \tag{4.16}$$

The facts that $p \mid \det A$ and that the two rows of A are independent prove the existence of a linear combination of the first and second rows of A which can be used to eliminate the third row. Using (4.14), $Ax \equiv 0 \pmod{p}$ can now be reduced to

$$\begin{gathered} a - 3(1+\varepsilon)b + \varepsilon c \equiv 0 \pmod{p}, \\ \varepsilon a + (1+\varepsilon)b - (3+2\varepsilon)c \equiv 0 \pmod{p}. \end{gathered} \tag{4.17}$$

Substituting $a \equiv 3(1+\varepsilon)b - \varepsilon c$ into the second congruence of (4.17) we have $(3\varepsilon^2 + 4\varepsilon + 1)b \equiv (\varepsilon^2 + 2\varepsilon + 3)c$. Using (4.16) and $p \neq 2, 11$ it is easy to show that p divides neither $3\varepsilon^2 + 4\varepsilon + 1$ nor $\varepsilon^2 + 2\varepsilon + 3$. This means that every solution of (4.17) is congruent modulo p to a solution of the form

$$[q(5\varepsilon^2 + 14\varepsilon + 9), q(\varepsilon^2 + 2\varepsilon + 3), q(3\varepsilon^2 + 4\varepsilon + 1)], \text{ where } q \in \mathbb{Z}. \tag{4.18}$$

Thus, exactly $p - 1$ non-congruent solutions $[a, b, c]$ exists to system (4.17) that satisfy $[a, b, c] \not\equiv [0, 0, 0] \pmod p$ and therefore $(p-1)p^{3(t-1)}$ noncongruent solutions satisfying $[a, b, c] \not\equiv [0, 0, 0] \pmod p$ exist to (4.5). □

For a $t \in \mathbb{N}$, denote by $\mathrm{S}_{p^t}(T)$ the set of roots of $g(x)$ in $\mathbb{Z}/p^t\mathbb{Z}$, i.e., the spectrum of the Tribonacci matrix T over $\mathbb{Z}/p^t\mathbb{Z}$. Next, for $\lambda \in \mathrm{S}_{p^t}(T)$ denote by $\mathrm{E}_{p^t}(\lambda) = \{[a, a\lambda, a\lambda^2], a \in \mathbb{Z}/p^t\mathbb{Z}\}$ the eigenspace corresponding to the eigenvalue λ. Specifically for this paragraph, due to Hensel's lemma, the spectrum T consists of a single element with $\mathrm{S}_{p^t}(T) = \{\alpha_t\}$. The elements of the spectrum $\mathrm{S}_{p^t}(T)$ play an important role in further considerations. Regarding their orders in the group of units of $\mathbb{Z}/p^t\mathbb{Z}$, the following lemma can easily be proved by modifying the proof of Theorem 1.1.

Lemma 4.6. *Let $p > 2$ be an arbitrary prime, $\lambda \in \mathbb{Z}$, $\lambda \neq \pm 1$ and $p \nmid \lambda$. If $\mathrm{ord}_p(\lambda) \neq \mathrm{ord}_{p^2}(\lambda)$, then, for any $t \in \mathbb{N}$,*

$$\mathrm{ord}_{p^t}(\lambda) = p^{t-1}\mathrm{ord}_p(\lambda). \tag{4.19}$$

More generally, if $s \in \mathbb{N}$ is the largest number such that $\mathrm{ord}_{p^s}(\lambda) = \mathrm{ord}_p(\lambda)$, then, for any $t \geqslant s$, $\mathrm{ord}_{p^t}(\lambda) = p^{t-s}\,\mathrm{ord}_p(\lambda)$.

Theorem 4.7. *Let p be an arbitrary prime, $p \neq 2, 11$ and $h = h(p) \neq h(p^2)$. The solution $[a, b, c]$ of the system $T^{p^{t-2}h}x \equiv x \pmod{p^t}$ for $t > 1$ satisfies $[a, b, c] \not\equiv [0, 0, 0] \pmod p$ if and only if $[a, b, c] \pmod p \in \mathrm{E}_p(\alpha_1)$ where $\alpha_1 \in \mathrm{S}_p(T)$.*

Proof. By 4.5 it is sufficient to prove that there exists a $q \in \mathbb{Z}$ such that $[q(5\varepsilon^2+14\varepsilon+9), q(\varepsilon^2+2\varepsilon+3), q(3\varepsilon^2+4\varepsilon+1)] \equiv [1, \alpha_1, \alpha_1^2] \pmod p$, where $\alpha_1 \in \mathrm{S}_p(T)$. Using (4.16) and $p \neq 2, 11$, it is easy to show that $p \nmid 5\varepsilon^2 + 14\varepsilon + 9$. This implies $q = (5\varepsilon + 9)^{-1}(\varepsilon + 1)^{-1}$ and $\alpha_1 = (5\varepsilon + 9)^{-1}(\varepsilon + 1)^{-1}(\varepsilon^2 + 2\varepsilon + 3)$. Let us now prove that $\alpha_1^2 = q(3\varepsilon^2 + 4\varepsilon + 1)$. As $\alpha_1^2 = (5\varepsilon + 9)^{-2}(\varepsilon + 1)^{-2}(\varepsilon^2 + 2\varepsilon + 3)^2$, it is sufficient to prove that

$$(5\varepsilon + 9)^{-2}(\varepsilon + 1)^{-2}(\varepsilon^2 + 2\varepsilon + 3)^2 \equiv (5\varepsilon + 9)^{-1}(\varepsilon + 1)^{-1}(3\varepsilon^2 + 4\varepsilon + 1) \pmod p.$$

However, this congruence is equivalent to (4.16) which holds. What remains to be proved is that $\alpha_1 \in \mathrm{S}_p(T)$. Now α_1^3 can be expressed in terms of α_1 and α_1^2 to derive the congruence $(5\varepsilon+9)^2(\varepsilon+1)(\alpha_1^3-\alpha_1^2-\alpha_1-1) \equiv -6(7\varepsilon^3+29\varepsilon^2+39\varepsilon+19) \pmod{p}$. Hence $\alpha_1^3 - \alpha_1^2 - \alpha_1 - 1 \equiv 0 \pmod{p}$ and thus $\alpha_1 \in \mathrm{S}_p(T)$. □

Let us denote by $\mathbb{Q}_p$ the field of p-adic numbers and by $\mathbb{Z}_p$ the ring of p-adic integers.

Theorem 4.8. *Let p be an arbitrary prime, $p \neq 2, 11$ and $h = h(p) \neq h(p^2)$. Further, let $g(x)$ be factorized over $\mathbb{F}_p$ into the product of a linear factor and an irreducible quadratic factor. Then $p \mid \det A$ if and only if $\mathrm{ord}_p(\alpha_2) = \mathrm{ord}_{p^2}(\alpha_2)$ where $\alpha_2 \in S_{p^2}(T)$.*

Proof. Let L_p be the splitting field of $g(x)$ over $\mathbb{Q}_p$ and let α, β, γ be the roots of $g(x)$ in L_p. Clearly, α, β, γ are in the ring O_p of integers of the field L_p. It follows from the form of the factorization of $g(x)$ over $\mathbb{F}_p$ that exactly one of the roots α, β, γ is in $\mathbb{Z}_p$. As the primes $p \neq 2, 11$ do not divide the discriminant $g(x)$, which is equal to -44, $L_p/\mathbb{Q}_p$ does not ramify and so the maximal ideal O_p is generated by p and α, β, γ are mutually different. Further, let $L = O_p/(p)$ be the residue field and α_1, β_1, γ_1 be the images of α, β, γ in L. Over the field L_p the Tribonacci matrix T is similar to D, whose diagonal is formed by α, β, γ. Thus, there exists an invertible matrix H such that $T = HDH^{-1}$ and thus $T^h = HD^hH^{-1}$. Next, $h(p) \neq h(p^2)$ implies that $T^h = E + pA$ where $p \nmid A$. Thus, over L_p we have $E + pA = HD^hH^{-1}$, which yields $pH^{-1}AH = D^h - E$. By the Cauchy theorem and other known properties of determinants we obtain

$$p^3 \cdot \det A = (\alpha^h - 1)(\beta^h - 1)(\gamma^h - 1). \tag{4.20}$$

As $h = \mathrm{lcm}(\mathrm{ord}_L(\alpha_1), \mathrm{ord}_L(\beta_1), \mathrm{ord}_L(\gamma_1))$, we have $\alpha_1^h = 1, \beta_1^h = 1, \gamma_1^h = 1$, which implies that p divides each of the differences $\alpha^h - 1$, $\beta^h - 1$, $\gamma^h - 1$ in O_p. Now using $p \mid \det A$ and equality (4.20) we deduce that at least one of such differences is divisible by p^2. Suppose that $\alpha \in \mathbb{Z}_p$ and $p^2 \nmid \alpha^h - 1$. Then p^2 divides at least one of the differences $\beta^h - 1$, $\gamma^h - 1$. Assume, without loss of generality, that $p^2 \mid \beta^h - 1$. Applying the Frobenius automorphism yields $p^2 \mid \gamma^h - 1$. From this fact it follows that $p^2 \mid \beta^h\gamma^h - 1$. Next, raising the Viète equation $\alpha\beta\gamma = 1$ to the h-th power in O_p yields $\alpha^h\beta^h\gamma^h = 1$. Since $p^2 \mid \beta^h\gamma^h - 1$, we have $p^2 \mid \alpha^h - 1$. Consequently, if $\alpha \in \mathbb{Z}_p$, then $p^2 \mid \alpha^h - 1$. Let us now denote by α_2 the image of α in $O_p/(p^2)$. As $\alpha \in \mathbb{Z}_p$, we have that $\alpha_2 \in \mathbb{Z}/p^2\mathbb{Z}$, which means $\alpha_2 \in \mathrm{S}_{p^2}(T)$. It follows from $p^2 \mid \alpha^h - 1$ in O_p that $p^2 \mid \alpha_2^h - 1$ in $\mathbb{Z}/p^2\mathbb{Z}$ and so $\mathrm{ord}_{p^2}(\alpha_2) \mid h$. Next we prove that $\mathrm{ord}_p(\alpha_2) = \mathrm{ord}_{p^2}(\alpha_2)$. By 4.6, exactly one of the equations

$\mathrm{ord}_{p^2}(\alpha_2) = p \cdot \mathrm{ord}_p(\alpha_2)$ and $\mathrm{ord}_{p^2}(\alpha_2) = \mathrm{ord}_p(\alpha_2)$ holds. Put $h_0 = \mathrm{ord}_p(\alpha_2)$ and suppose that $\mathrm{ord}_{p^2}(\alpha_2) = ph_0$. Then $ph_0 \mid h$. However, this is not possible because $p \nmid h$ for $p \neq 2, 11$. In this case, $p \nmid h$ because of the fact that h divides the order of the multiplicative group of L, which is equal to $p^2 - 1$.

Conversely, suppose that $\mathrm{ord}_p(\alpha_2) = \mathrm{ord}_{p^2}(\alpha_2)$. Since $\alpha_1 \equiv \alpha_2 \pmod{p}$, we have $\mathrm{ord}_p(\alpha_1) = \mathrm{ord}_p(\alpha_2)$. Moreover, it is evident that $\mathrm{ord}_p(\alpha_1) = \mathrm{ord}_L(\alpha_1)$. Combining it with $\mathrm{ord}_p(\alpha_2) = \mathrm{ord}_{p^2}(\alpha_2)$ we find that $\mathrm{ord}_{p^2}(\alpha_2) = \mathrm{ord}_L(\alpha_1)$. Therefore from $h = \mathrm{lcm}(\mathrm{ord}_L(\alpha_1), \mathrm{ord}_L(\beta_1), \mathrm{ord}_L(\gamma_1))$ it follows that $\mathrm{ord}_{p^2}(\alpha_2) \mid h$. Thus $p^2 \mid \alpha_2^h - 1$ in $O_p/(p^2)$ and $p^2 \mid \alpha^h - 1$ in O_p. Next, $h = \mathrm{lcm}(\mathrm{ord}_L(\alpha_1), \mathrm{ord}_L(\beta_1), \mathrm{ord}_L(\gamma_1))$ yields that $p \mid \beta^h - 1$ and $p \mid \gamma^h - 1$ in O_p. Combining $p^2 \mid \alpha^h - 1$, $p \mid \beta^h - 1$, $p \mid \gamma^h - 1$ with (4.20) we get $p \mid \det A$, as required. □

Lemma 4.9. *Let $g(x)$ be factorized over $\mathbb{F}_p$, into the product of a linear factor and an irreducible quadratic factor. If $h(p) = h(p^2)$ then $\mathrm{ord}_p(\alpha_2) = \mathrm{ord}_{p^2}(\alpha_2)$.*

Proof. Put $h_0 = \mathrm{ord}_p(\alpha_2)$ and suppose that $\mathrm{ord}_p(\alpha_2) \neq \mathrm{ord}_{p^2}(\alpha_2)$. Then, by 4.6, we have $\mathrm{ord}_{p^2}(\alpha_2) = ph_0$. Consider now any triple of the form $[a, a\alpha_2, a\alpha_2^2]$ where $p \nmid a$. Obviously, $h(p^2)[a, a\alpha_2, a\alpha_2^2] = ph_0$ and, by (2.3), $ph_0 \mid h(p^2)$. Hence, using the hypothesis $h(p) = h(p^2)$, we deduce that $p \mid h(p)$. However, this is not possible as $(h(p), p) = 1$. □

Problem 4.10. No prime p and $\lambda \in \mathrm{S}_{p^t}(T)$ where $t > 1$ are known such that (4.19) does not hold. Neither is there a proof of (4.19) holding for any $\lambda \in \mathrm{S}_{p^t}(T)$. However, 4.8 implies that (4.19) is not a consequence of $h(p) \neq h(p^2)$. It may be extremely difficult either to prove that (4.19) is generally true or find a counter-example. This means that we cannot even show a prime $p \neq 2, 11$ for which the system $Ax \equiv 0 \pmod{p}$ has a non-trivial solution. For $p = 2, 11$, however, $p \mid \det A$ and $Ax \equiv 0 \pmod{p}$ does have a non-trivial solution. Unfortunately, not even for $p = 2, 11$ there is a counter-example to (4.19). In the remaining part of this paper we shall no longer deal with issues whether (4.19) holds in general and, when formulating assertions, we will assume that (4.19) is true for any $\lambda \in \mathrm{S}_{p^t}(T)$.

Theorem 4.11. *Let $g(x)$ be factored over $\mathbb{F}_p$ as in* (4.1) *and let, for any $t \in \mathbb{N}$, $S_{p^t}(T) = \{\alpha_t\}$. Further, let $h_0 = \mathrm{ord}_p(\alpha_t)$. Then $h(p^t)[a, b, c] \mid p^{t-1}h_0$ if and only if $[a, b, c] \pmod{p^t} \in E_{p^t}(\alpha_t)$. Moreover, for $t > 1$, $h(p^t)[a, b, c] = p^{t-1}h_0$ if and only if $[a, b, c] \pmod{p^t} \in E_{p^t}(\alpha_t)$, $[a, b, c] \not\equiv [0, 0, 0] \pmod{p}$ and $\mathrm{ord}_p(\alpha_t) \neq \mathrm{ord}_{p^2}(\alpha_t)$.*

Proof. Let L be the splitting field of $g(x)$ over $\mathbb{F}_p$. Considering that $[L : \mathbb{F}_p] = 2$ and using the Frobenius automorphism we can prove, in a way similar to that used in 3.6, that the Tribonacci sequence $(G_n)_{n=1}^{\infty}$ defined by the initial conditions $[a, b, c]$

can be written over L as

$$G_n = A\alpha_1^n + B\beta_1^n + B^p(\beta_1^p)^n, \tag{4.21}$$

where α_1, β_1, β_1^p are different roots of $g(x)$ in L and the coefficients A, B are uniquely determined by $[a,b,c]$. Clearly, $A, \alpha_1 \in \mathbb{F}_p$ and $\beta_1 \in L$. Moreover, for the orders of α_1, β_1, β_1^p in the multiplicative group of L we have $\operatorname{ord}_L(\beta_1) = \operatorname{ord}_L(\beta_1^p)$ and $\operatorname{ord}_L(\alpha_1) \mid \operatorname{ord}_L(\beta_1)$ with $\operatorname{ord}_L(\alpha_1) < \operatorname{ord}_L(\beta_1)$ because the multiplicative group of L is cyclic. From $h(p) = \operatorname{lcm}(\operatorname{ord}_L(\alpha_1), \operatorname{ord}_L(\beta_1), \operatorname{ord}_L(\beta_1^p))$ it now follows that $h(p) = \operatorname{ord}_L(\beta_1)$. Further, we have from (4.21) that

$$h(p)[a,b,c] = \begin{cases} 1 & \text{if } A = 0,\ B = 0, \\ h_0 = \operatorname{ord}_p(\alpha_1) & \text{if } A \neq 0,\ B = 0, \\ h(p) = \operatorname{ord}_L(\beta_1) & \text{if } B \neq 0. \end{cases} \tag{4.22}$$

Thus the only primitive periods $(G_n \bmod p)_{n=1}^{\infty}$ possible are 1, h_0, and $h(p)$. From (4.21) and (4.22) we have that $h(p)[a,b,c] \mid h_0$ if and only if $[a,b,c] \equiv [0,0,0] \pmod p$ or $[a,b,c] \equiv [a, a\alpha_1, a\alpha_1^2] \pmod p$, i.e., if $[a,b,c] \pmod p \in E_p(\alpha_1)$.

Suppose now that the assertion is true for any $t \geqslant 1$ and let us prove it for $t+1$. Let $h(p^{t+1})[a,b,c] \mid p^t h_0$. By 4.2 and 4.6, $h(p^{t+1})[a, a\alpha_{t+1}, a\alpha_{t+1}^2] \mid p^t h_0$ and so

$$h(p^{t+1})[0, b - a\alpha_{t+1}, c - a\alpha_{t+1}^2] \mid p^t h_0. \tag{4.23}$$

It also follows from $h(p^{t+1})[a,b,c] \mid p^t h_0$ that $h(p)[a,b,c] \mid h_0$. Therefore we have $[a,b,c] \pmod p \in E_p(\alpha_1)$. This yields $[a,b,c] \equiv [a, a\alpha_{t+1}, a\alpha_{t+1}^2] \pmod p$ and thus $[0, b - a\alpha_{t+1}, c - a\alpha_{t+1}^2] \equiv [0,0,0] \pmod p$. Hence $[0, p^{-1}(b - a\alpha_{t+1}), p^{-1}(c - a\alpha_{t+1}^2)] \in \mathbb{Z}^3$. From (4.23) we have $h(p^t)[0, p^{-1}(b - a\alpha_{t+1}), p^{-1}(c - a\alpha_{t+1}^2)] \mid p^t h_0$. As $h(p^t)[0, p^{-1}(b - a\alpha_{t+1}), p^{-1}(c - a\alpha_{t+1}^2)] \mid h(p^t)$ and $h(p^t) \mid p^{t-1}h(p)$, where $p \nmid h(p)$, we obtain $h(p^t)[0, p^{-1}(b - a\alpha_{t+1}), p^{-1}(c - a\alpha_{t+1}^2)] \mid p^{t-1}h_0$. By the induction hypothesis, $[0, p^{-1}(b - a\alpha_{t+1}), p^{-1}(c - a\alpha_{t+1}^2)] \pmod{p^t} \in E_{p^t}(\alpha_t)$. Thus, there is a $q \in \mathbb{Z}$ such that

$$\bigl[0, p^{-1}(b - a\alpha_{t+1}), p^{-1}(c - a\alpha_{t+1}^2)\bigr] \equiv q[1, \alpha_t, \alpha_t^2] \pmod{p^t}. \tag{4.24}$$

From (4.24) we obtain $q \equiv 0 \pmod{p^t}$ and so $p^{-1}(b - a\alpha_{t+1}) \equiv p^{-1}(c - a\alpha_{t+1}^2) \equiv 0 \pmod{p^t}$. This yields $b \equiv a\alpha_{t+1} \pmod{p^{t+1}}$, $c \equiv a\alpha_t^2 \pmod{p^{t+1}}$ and therefore $[a,b,c] \pmod{p^{t+1}} \in E_{p^{t+1}}(\alpha_{t+1})$.

Conversely, let $[a,b,c] \pmod{p^t} \in E_{p^t}(\alpha_t)$ for any $t \geqslant 1$. Then $[a,b,c] \equiv [a, \alpha_t, a\alpha_t^2] \pmod{p^t}$ and, by 4.1, for the sequence defined by this triple we have

$G_n \equiv a\alpha_t^{n-1} \pmod{p^t}$. From 4.2 it follows that $h(p^t)[a,b,c] \mid \mathrm{ord}_{p^t}(\alpha_t)$ and, by 4.6, this means that $h(p^t)[a,b,c] \mid p^{t-1}h_0$.

Let us now prove the second part of 4.11. Let $t > 1$ and $h(p^t)[a,b,c] = p^{t-1}h_0$. Suppose first that $[a,b,c] \equiv [0,0,0] \pmod p$. Then $[a/p, b/p, c/p] \in \mathbb{Z}^3$. From 2.2 and from $h(p^{t-1})[a,b,c] \mid p^{t-2}h(p)$ it follows that $h(p^t)[a,b,c] = h(p^{t-1})[a/p,b/p,c/p] \mid p^{t-2}h(p)$. Since $(h(p),p) = 1$, we get a contradiction. Suppose next that $\mathrm{ord}_p(\alpha_t) = \mathrm{ord}_{p^2}(\alpha_t)$. From $h(p^t)[a,b,c] = p^{t-1}h_0$ we have that $[a,b,c] \pmod{p^t} \in E_{p^t}(\alpha_t)$ and so, for any $n \in \mathbb{N}$, $G_n \equiv a\alpha_t^{n-1} \pmod{p^t}$. By 4.2, for a primitive period of this sequence we have $h(p^t)[a,b,c] \mid \mathrm{ord}_{p^t}(\alpha_t)$. Next, from 4.6 and from $\mathrm{ord}_p(\alpha_t) = \mathrm{ord}_{p^2}(\alpha_t)$ it follows that $\mathrm{ord}_{p^t}(\alpha_t) \mid p^{t-2}\,\mathrm{ord}_p(\alpha_t) = p^{t-2}h_0$, a contradiction.

Conversely, let $t > 1$, $[a,b,c] \pmod{p^t} \in E_{p^t}(\alpha_t)$, $[a,b,c] \not\equiv [0,0,0] \pmod p$ and $\mathrm{ord}_p(\alpha_t) \neq \mathrm{ord}_{p^2}(\alpha_t)$. From the hypothesis $[a,b,c] \pmod{p^t} \in E_{p^t}(\alpha_t)$ it follows that for the sequence determined by this triple, $G_n \equiv a\alpha_t^{n-1} \pmod{p^t}$ and $[a,b,c] \not\equiv [0,0,0] \pmod p$ implies $p \nmid a$. Thus, by 4.2, $h(p^t)[a,b,c] = \mathrm{ord}_{p^t}(\alpha_t)$. From 4.6 and from $\mathrm{ord}_p(\alpha_t) \neq \mathrm{ord}_{p^2}(\alpha_t)$ we now obtain $h(p^t)[a,b,c] = p^{t-1}h_0$. The proof is complete. □

Let us now formulate the main theorem of this section.

Theorem 4.12. *Let p be an arbitrary prime such that $g(x)$ is factorized over $\mathbb{F}_p$ into the product of a linear factor and an irreducible quadratic factor. Further, let $h(p) \neq h(p^2)$, $\mathrm{ord}_p(\alpha_2) \neq \mathrm{ord}_{p^2}(\alpha_2)$ and $[a,b,c] \not\equiv [0,0,0] \pmod p$. Then, for any $t \in \mathbb{N}$, the following assertions are true.*

If $[a,b,c] \pmod{p^t} \in E_{p^t}(\alpha_t)$ then

$$h(p^t)[a,b,c] = \mathrm{ord}_{p^t}(\alpha_t) = p^{t-1}\,\mathrm{ord}_p(\alpha_t). \tag{4.25}$$

If $[a,b,c] \pmod p \notin E_p(\alpha_1)$ then

$$h(p^t)[a,b,c] = p^{t-1}h(p) = p^{t-1}h(p)[a,b,c]. \tag{4.26}$$

If $[a,b,c] \pmod p \in E_p(\alpha_1)$ and $[a,b,c] \pmod{p^t} \notin E_{p^t}(\alpha_t)$ then

$$h(p^t)[a,b,c] = p^{t-1}h(p) \neq p^{t-1}h(p)[a,b,c]. \tag{4.27}$$

Proof. The validity of (4.25) follows from 4.11.

Let $[a,b,c] \pmod p \notin \mathrm{E}_p(\alpha_1)$. Then, by 4.11 and $[a,b,c] \not\equiv [0,0,0] \pmod p$, we have $h(p)[a,b,c] = h(p)$ and, by (2.2), we have $h(p) \mid h(p^t)[a,b,c]$. Next, from $h(p) \neq h(p^2)$, 1.1 and (2.3) it follows that $h(p^t)[a,b,c] \mid p^{t-1}h(p)$. Combining these equations yields $h(p^t)[a,b,c] = p^i h(p)$ for some $i \in \{0,1,\dots t-1\}$. Next, from

$\mathrm{ord}_p(\alpha_2) \neq \mathrm{ord}_{p^2}(\alpha_2)$ and 4.8 we have $p \nmid \det A$. Therefore, by 4.5, there exists no solution $[a,b,c] \not\equiv [0,0,0] \pmod{p}$ of $T^{p^{t-2}h(p)}x \equiv x \pmod{p^t}$ for $t > 1$, which implies that $h(p^t)[a,b,c] \nmid p^{t-2}h(p)$. Thus we conclude that (4.26) holds.

Let $[a,b,c] \pmod{p} \in \mathrm{E}_p(\alpha_1)$ and $[a,b,c] \pmod{p^t} \notin \mathrm{E}_{p^t}(\alpha_t)$. From 4.11 and $[a,b,c] \pmod{p^t} \notin \mathrm{E}_{p^t}(\alpha_t)$ it follows that $h(p^t)[a,b,c] \nmid p^{t-1}h_0$ where $h_0 = \mathrm{ord}_p(\alpha_t)$. Moreover, by 4.11, for $[a,b,c] \not\equiv [0,0,0] \pmod{p}$ exactly one of the equalities $h(p^t)[a,b,c] = p^i h(p)$ and $h(p^t)[a,b,c] = p^i h_0$ holds for some $i \in \{0,\dots,t-1\}$. Combining the above, we obtain $h(p^t)[a,b,c] = p^i h(p)$. We shall show that $h(p^t)[a,b,c] \nmid p^{t-2}h(p)$. Indeed, suppose that $h(p^t)[a,b,c] \mid p^{t-2}h(p)$. Theorem 4.5 and $[a,b,c] \not\equiv [0,0,0] \pmod{p}$ then give $p \mid \det A$. By 4.8 we have $\mathrm{ord}_p(\alpha_2) = \mathrm{ord}_{p^2}(\alpha_2)$, a contradiction. Since $h(p^t)[a,b,c] \mid p^{t-1}h(p)$, we obtain $h(p^t)[a,b,c] = p^{t-1}h(p)$. In addition, it follows from 4.11 and from $[a,b,c] \pmod{p} \in E_p(\alpha_1)$ that $h(p)[a,b,c] = \mathrm{ord}_L(\alpha_1) \neq \mathrm{ord}_L(\beta_1) = h(p)$, which, together with the preceding facts, proves (4.27). □

5. The case of factorization into the product of linear terms

What remains to be investigated is the case of the Tribonacci polynomial $g(x)$ being factorized over $\mathbb{F}_p$ into the product of linear terms, i.e.,

$$g(x) \equiv (x-\alpha_1)(x-\beta_1)(x-\gamma_1) \pmod{p} \quad \text{and} \quad \mathrm{S}_p(T) = \{\alpha_1, \beta_1, \gamma_1\}. \tag{5.1}$$

The assumption $p \neq 2, 11$ implies that $\alpha_1, \beta_1, \gamma_1$ are distinct, thus $g(x)$ has nonzero first derivatives over $\mathbb{F}_p$ at these points. From Hensel's lemma it follows that $g(x)$ can be factorized over $\mathbb{Q}_p$ as $g(x) = (x-\alpha)(x-\beta)(x-\gamma)$ where $\alpha, \beta, \gamma \in \mathbb{Z}_p$. Let us put $\alpha_t := \alpha \bmod p^t$, $\beta_t := \beta \bmod p^t$, $\gamma_t := \gamma \bmod p^t$ for every $t \in \mathbb{N}$. Thus, over the ring $\mathbb{Z}/p^t\mathbb{Z}$ we have $g(x) \equiv (x-\alpha_t)(x-\beta_t)(x-\gamma_t) \pmod{p^t}$ and $\mathrm{S}_{p^t}(T) = \{\alpha_t, \beta_t, \gamma_t\}$. Since $\mathbb{Z} \subset \mathbb{Z}_p \subset \mathbb{Q}_p$, the terms of the triple $[a,b,c]$ can be viewed as elements of the field $\mathbb{Q}_p$. Thus, over $\mathbb{Q}_p$, the terms of the Tribonacci sequence $(G_n)_{n=1}^{\infty}$ can be uniquely written as

$$G_n = A\alpha^n + B\beta^n + C\gamma^n, \quad \text{where } A, B, C \in \mathbb{Q}_p. \tag{5.2}$$

The equation (5.2) defines a 1-1 corespondence between the triples of initial values $[a,b,c] \in \mathbb{Q}_p^3$ and the triples of p-adic numbers $[A,B,C] \in \mathbb{Q}_p^3$.

Lemma 5.1. *Let $g(x)$ be factorized over $\mathbb{F}_p$, $p \neq 2, 11$, into the product of linear terms. Then the terms of the sequence $(G_n \bmod p^t)_{n=1}^{\infty}$ defined by an arbitrary triple of initial values $[a, b, c]$ can be uniqely written as*

$$G_n \bmod p^t \equiv A_t\alpha_t^n + B_t\beta_t^n + C_t\gamma_t^n \pmod{p^t}, \tag{5.3}$$

where $0 \leqslant A_t, B_t, C_t \leqslant p^t - 1$ are nonnegative integers.

Proof. Let us first show that $[A, B, C] \in \mathbb{Z}_p^3$. By substituting $n = 1, 2, 3$ into (5.2) we obtain the system of equations over $\mathbb{Q}_p$

$$\begin{bmatrix} \alpha & \beta & \gamma \\ \alpha^2 & \beta^2 & \gamma^2 \\ \alpha^3 & \beta^3 & \gamma^3 \end{bmatrix} \begin{bmatrix} A \\ B \\ C \end{bmatrix} = \begin{bmatrix} a \\ b \\ c \end{bmatrix}. \tag{5.4}$$

The determinant of the matrix M of the system (5.4) is the well-known Vandermonde determinant, for which we have $\det M = \alpha\beta\gamma(\alpha - \beta)(\alpha - \gamma)(\gamma - \beta)$. Since α, β, γ are pairwise incongruent modulo p, none of the differences $\alpha - \beta$, $\alpha - \gamma$, $\gamma - \beta$ is divisible by p. From this fact and from $\alpha\beta\gamma = 1$, it follows that $p \nmid \det M$. Thus, $\det M$ is an invertible element of the ring $\mathbb{Z}_p$ and the matrix M is invertible over $\mathbb{Z}_p$. Multiplying (5.4) by M^{-1} we obtain $[A, B, C]$ as a $\mathbb{Z}_p$-linear combination of $[a, b, c]$ and so $[A, B, C] \in \mathbb{Z}_p^3$. Let us now put $A_t := A \bmod p^t$, $B_t := B \bmod p^t$, $C_t := C \bmod p^t$. It is not difficult to prove that $[A, B, C] \equiv [A', B', C'] \pmod{p^t}$ if and only if $[a, b, c] \equiv [a', b', c'] \pmod{p^t}$. Thus there exists a 1-1 corespondence between the triples $[a, b, c] \in (\mathbb{Z}/p^t\mathbb{Z})^3$ and the triples $[A_t, B_t, C_t] \in (\mathbb{Z}/p^t\mathbb{Z})^3$. Congruence (5.3) is now obtained by reducing (5.2) by p^t. □

Lemma 5.2. *Let the primitive periods of the sequences $(A_t\alpha_t^n \bmod p^t)_{n=1}^{\infty}$, $(B_t\beta_t^n \bmod p^t)_{n=1}^{\infty}$, $(C_t\gamma_t^n \bmod p^t)_{n=1}^{\infty}$ be k_1, k_2, k_3. Then the primitive period of the sequence $(A_t\alpha_t^n + B_t\beta_t^n + C_t\gamma_t^n \bmod p^t)_{n=1}^{\infty}$ is $\operatorname{lcm}(k_1, k_2, k_3)$.*

Proof. Clearly, $\operatorname{lcm}(k_1, k_2, k_3)$ is a period of $(A_t\alpha_t^n + B_t\beta_t^n + C_t\gamma_t^n \bmod p^t)_{n=1}^{\infty}$ and, therefore, it is sufficient to prove that this period is primitive. Suppose there is a primitive period $k < \operatorname{lcm}(k_1, k_2, k_3)$. Since k is a period, we have

$$\begin{aligned}&[A_t\alpha_t^{k+1} + B_t\beta_t^{k+1} + C_t\gamma_t^{k+1}, A_t\alpha_t^{k+2} + B_t\beta_t^{k+2} + C_t\gamma_t^{k+2}, A_t\alpha_t^{k+3} + B_t\beta_t^{k+3} + C_t\gamma_t^{k+3}] \\ &\quad \equiv [A_t\alpha_t + B_t\beta_t + C_t\gamma_t, A_t\alpha_t^2 + B_t\beta_t^2 + C_t\gamma_t^2, A_t\alpha_t^3 + B_t\beta_t^3 + C_t\gamma_t^3] \pmod{p^t}.\end{aligned}$$

This system of congruences can be reduced to the equivalent form

$$\begin{bmatrix} \alpha_t & \beta_t & \gamma_t \\ \alpha_t^2 & \beta_t^2 & \gamma_t^2 \\ \alpha_t^3 & \beta_t^3 & \gamma_t^3 \end{bmatrix} \begin{bmatrix} A_t(\alpha_t^k - 1) \\ B_t(\beta_t^k - 1) \\ C_t(\gamma_t^k - 1) \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix} \pmod{p^t}. \tag{5.5}$$

As the determinant of the system matrix of (5.5) is not divisible by p, (5.5) has only one solution

$$(5.6)\quad A_t(\alpha_t^k - 1) \equiv 0 \pmod{p^t},\ B_t(\beta_t^k - 1) \equiv 0 \pmod{p^t},\ C_t(\gamma_t^k - 1) \equiv 0 \pmod{p^t}.$$

Next, from (5.6) we have $A_t\alpha_t^{k+1} \equiv A_t\alpha_t \pmod{p^t}$, $B_t\beta_t^{k+1} \equiv B_t\beta_t \pmod{p^t}$, $C_t\gamma_t^{k+1} \equiv C_t\gamma_t \pmod{p^t}$. This implies that k is a period for each of the sequences $(A_t\alpha_t^n \bmod p^t)_{n=1}^{\infty}$, $(B_t\beta_t^n \bmod p^t)_{n=1}^{\infty}$, $(C_t\gamma_t^n \bmod p^t)_{n=1}^{\infty}$. Consequently, we have $k_1 \mid k$, $k_2 \mid k$, $k_3 \mid k$, which contradicts the hypothesis $k < \operatorname{lcm}(k_1, k_2, k_3)$. □

Lemma 5.3. *Let $p \neq 2, 11$ be an arbitrary prime and let $\mathrm{S}_p(T) = \{\alpha_1, \beta_1, \gamma_1\}$. Further, let $\operatorname{ord}_p(\alpha_1) = h_1$, $\operatorname{ord}_p(\beta_1) = h_2$ and $\operatorname{ord}_p(\gamma_1) = h_3$. Then*

$$(5.7)\qquad \operatorname{lcm}(h_1, h_2) = \operatorname{lcm}(h_1, h_3) = \operatorname{lcm}(h_2, h_3) = \operatorname{lcm}(h_1, h_2, h_3) = h(p).$$

Proof. Put $k = \gcd(h_1, h_2)$. Then there exist $r, s \in \mathbb{N}$ such that $h_1 = kr$, $h_2 = ks$ with $(r, s) = 1$. Thus, we have $\operatorname{lcm}(h_1, h_2) = krs$. Next, the Viète equation $\alpha_1\beta_1\gamma_1 \equiv 1 \pmod{p}$ yields $(\alpha_1\beta_1\gamma_1)^{krs} \equiv (\alpha_1^{kr})^s \cdot (\beta_1^{ks})^r \cdot \gamma_1^{krs} \equiv \gamma_1^{krs} \equiv 1 \pmod{p}$. Then we have $h_3 \mid krs$, which implies $\operatorname{lcm}(h_1, h_2) = \operatorname{lcm}(h_1, h_2, h_3)$. By analogy, we can prove that $\operatorname{lcm}(h_1, h_3) = \operatorname{lcm}(h_1, h_2, h_3)$ and $\operatorname{lcm}(h_2, h_3) = \operatorname{lcm}(h_1, h_2, h_3)$. Next, using (5.4) and Cramer's rule, we can show that, for the coefficients A_t, B_t, C_t corresponding to $[0, 0, 1]$, we have $A_t \equiv \varepsilon \cdot \beta\gamma(\gamma - \beta) \pmod{p^t}$, $B_t \equiv \varepsilon \cdot \alpha\gamma(\alpha - \gamma) \pmod{p^t}$, $C_t \equiv \varepsilon \cdot \alpha\beta(\beta - \alpha) \pmod{p^t}$, where $\varepsilon \equiv (\det M)^{-1} \pmod{p^t}$. Hence none of the coefficients A_t, B_t, C_t is divisible by p. Applying now (5.3) to the module p and the triple $[0, 0, 1]$, we can use Lemma 5.2 to show that $h(p) = \operatorname{lcm}(h_1, h_2, h_3)$. This proves (5.7). □

Remark 5.4. Investigating the orders h_1, h_2, h_3 for the first several hundreds of primes might lead to a hypothesis that there are always two of the orders h_1, h_2, h_3 that divide the third. That is, if $h_1 < h_2 < h_3$, all the terms in (5.7) are equal to h_3. The first counter-example that disproves this hypothesis is $p = 4481$. Over $\mathbb{F}_{4481}$, $g(x)$ can be written as $g(x) = (x - 2661)(x - 2677)(x - 3625)$. Denoting $\alpha_1 = 2661$, $\beta_1 = 2677$, $\gamma_1 = 3625$, we arrive at $\operatorname{ord}_p(\alpha_1) = 2240$, $\operatorname{ord}_p(\beta_1) = 640$, $\operatorname{ord}_p(\gamma_1) = 896$ and $h(p) = \operatorname{lcm}(2240, 640, 896) = 4480$. Further, if two of the roots $\alpha_1, \beta_1, \gamma_1$ are of the same order in the multiplicative group of $\mathbb{F}_p$ different from the order of the third root, the following two situations may, theoretically, occur:

$$\operatorname{ord}_p(\alpha_1) < \operatorname{ord}_p(\beta_1) = \operatorname{ord}_p(\gamma_1) \qquad \text{and} \qquad \operatorname{ord}_p(\alpha_1) = \operatorname{ord}_p(\beta_1) < \operatorname{ord}_p(\gamma_1).$$

Let us prove that the second case can never occur.

Lemma 5.5. *If* $\operatorname{ord}_p(\alpha_1) = \operatorname{ord}_p(\beta_1) = h$, *then* $\operatorname{ord}_p(\gamma_1) \mid h$.

Proof. By raising the Viète equation $\alpha_1\beta_1\gamma_1 \equiv 1 \pmod{p}$ to the h-th power we obtain $\gamma_1^h \equiv \alpha_1^h\beta_1^h\gamma_1^h \equiv 1 \pmod{p}$ and so $\operatorname{ord}_p \gamma_1 \mid h$. □

Remark 5.6. Without loss of generality we can denote the roots of $g(x)$ over $\mathbb{F}_p$ by α_1, β_1, γ_1 so that, for their orders h_1, h_2, h_3 and $h(p) = \operatorname{lcm}(h_1, h_2, h_3)$, exactly one of the four following cases occurs:

$$\begin{aligned} h_1 = h_2 = h_3 &= h(p), \quad p = 103,\\ h_1 < h_2 = h_3 &= h(p), \quad p = 47,\\ h_1 < h_2 < h_3 &= h(p), \quad p = 311,\\ h_1 < h_2 < h_3 &< h(p), \quad p = 4481. \end{aligned} \tag{5.8}$$

The values of the primes p shown in (5.8) are the least values for which the situation in question occurs.

Theorem 5.7. *Let* $g(x)$ *be factorized over* $\mathbb{F}_p$ *into the product of linear terms and let* $p \neq 2, 11$. *If* $h = h(p) \neq h(p^2)$, *then there is at most one eigenvalue* $\lambda \in S_{p^t}(T)$ *satisfying*

$$\operatorname{ord}_p(\lambda) = \operatorname{ord}_{p^2}(\lambda). \tag{5.9}$$

Proof. Supose that in $S_{p^t}(T)$ there are two eigenvalues satisfying (5.9). Without loss of generality, let $\operatorname{ord}_p(\alpha_t) = \operatorname{ord}_{p^2}(\alpha_t) = h_1$ and $\operatorname{ord}_p(\beta_t) = \operatorname{ord}_{p^2}(\beta_t) = h_2$. From (5.7) we obtain $\operatorname{lcm}(h_1, h_2) = h$ and thus $\operatorname{ord}_{p^2}(\alpha_2) = \operatorname{ord}_{p^2}(\beta_2) \mid h$. By raising the Viète equation $\alpha_2\beta_2\gamma_2 \equiv 1 \pmod{p^2}$ to the h-th power, we obtain $\alpha_2^h\beta_2^h\gamma_2^h \equiv 1 \pmod{p^2}$, which implies $\gamma_2^h \equiv 1 \pmod{p^2}$. Applying (5.3) to the triple $[0, 0, 1]$ and the module p^2, we obtain

$$\begin{aligned} &[G_{h+1}, G_{h+2}, G_{h+3}]\\ &\qquad \equiv [A_2\alpha_2 + B_2\beta_2 + C_2\gamma_2, A_2\alpha_2^2 + B_2\beta_2^2 + C_2\gamma_2^2, A_2\alpha_2^3 + B_2\beta_2^3 + C_2\gamma_2^3]\\ &\qquad \equiv [G_1, G_2, G_3] \pmod{p^2}. \end{aligned} \tag{5.10}$$

From (5.10) we conclude $h(p^2) \mid h$. By (2.2), also $h \mid h(p^2)$, which yields $h = h(p^2)$. □

Remark 5.8. By slightly modifying the proof of Theorem 4.8 we can show that $\operatorname{ord}_p(\lambda) = \operatorname{ord}_{p^2}(\lambda)$ if and only if $p \mid \det A$. We can also prove that it is not possible that $h(p) = h(p^2)$ if there is a $\lambda \in S_{p^t}(T) = \{\alpha_t, \beta_t, \gamma_t\}$ such that $\operatorname{ord}_p(\lambda) \neq \operatorname{ord}_{p^2}(\lambda)$. Thus, $h(p) = h(p^2)$ implies $\operatorname{ord}_p(\lambda) = \operatorname{ord}_{p^2}(\lambda)$ for every $\lambda \in S_{p^t}(T)$. The proof can be done by analogy with 4.9.

Theorem 5.9. *Let $g(x)$ be factorized over $\mathbb{F}_p$, where $p \neq 2, 11$, into the product of linear terms. Further, let $[a,b,c] \not\equiv [0,0,0] \pmod{p}$ and, for any $t \in \mathbb{N}$, let $S_{p^t}(T) = \{\alpha_t, \beta_t, \gamma_t\}$. If $\lambda \in S_{p^t}(T)$ and $[a,b,c] \pmod{p^t} \in E_{p^t}(\lambda)$ then*

$$h(p^t)[a,b,c] = \operatorname{ord}_{p^t}(\lambda). \tag{5.11}$$

Moreover, if, for $t > 1$, $\lambda \in S_{p^t}(T)$ fulfils the condition $\operatorname{ord}_p(\lambda) \neq \operatorname{ord}_{p^2}(\lambda)$, then

$$h(p^t)[a,b,c] = p^{t-1} \operatorname{ord}_p(\lambda) = p^{t-1} h(p)[a,b,c]. \tag{5.12}$$

If $[a,b,c] \pmod{p^t} \notin E_{p^t}(\alpha_t) \cup E_{p^t}(\beta_t) \cup E_{p^t}(\gamma_t)$ and, for every $\lambda \in S_{p^t}(T)$, $t > 1$, $\operatorname{ord}_p(\lambda) \neq \operatorname{ord}_{p^2}(\lambda)$, then

$$h(p^t)[a,b,c] = h(p^t) = p^{t-1} h(p). \tag{5.13}$$

Proof. By (5.3) we have $[a,b,c] \equiv [0,0,0] \pmod{p}$ if and only if $[A_t, B_t, C_t] \equiv [0,0,0] \pmod{p}$. Thus $[a,b,c] \not\equiv [0,0,0] \pmod{p}$ implies that at least one of the coefficients A_t, B_t, C_t is not divisible by p. If $[a,b,c] \pmod{p^t} \in E_{p^t}(\lambda)$ for some $\lambda \in S_{p^t}(T)$, then exactly two of the coefficients A_t, B_t, C_t are divisible by p^t. Now, from (5.3) it follows that $h(p^t)[a,b,c] = \operatorname{ord}_{p^t}(\lambda)$, which proves (5.11). Moreover, if $\operatorname{ord}_p(\lambda) \neq \operatorname{ord}_{p^2}(\lambda)$, then (4.19) implies (5.12).

Let $[a,b,c] \pmod{p^t} \notin E_{p^t}(\alpha_t) \cup E_{p^t}(\beta_t) \cup E_{p^t}(\gamma_t)$. Then at least two of the coefficients A_t, B_t, C_t in (5.3) are not divisible by p^t and at least one of them is not divisible by p. Without loss of generality we can denote $\alpha_t, \beta_t, \gamma_t$ so that $p \nmid A_t$ and $p^t \nmid B_t$. Hence (4.19) implies that the primitive period of $(A_t \alpha_t^n \bmod p^t)_{n=1}^{\infty}$ is $k_1 = \operatorname{ord}_{p^t}(\alpha_t) = p^{t-1} \operatorname{ord}_p(\alpha_t)$ and the primitive period of $(B_t \beta_t^n \bmod p^t)_{n=1}^{\infty}$ is $k_2 = p^i \operatorname{ord}_p(\beta_t)$ for some $i \in \{0, \ldots, t-1\}$. If we put $h_1 = \operatorname{ord}_p(\alpha_t)$, $h_2 = \operatorname{ord}_p(\beta_t)$, then $\operatorname{lcm}(k_1, k_2) = p^{t-1} \operatorname{lcm}(h_1, h_2)$. By (5.7) we have $\operatorname{lcm}(h_1, h_2) = h(p)$ and thus $\operatorname{lcm}(k_1, k_2) = p^{t-1} h(p) = h(p^t)$. Now, from 5.2 we conclude that $h(p^t)[a,b,c] = \operatorname{lcm}(k_1, k_2, k_3)$. As $\operatorname{lcm}(k_1, k_2) \mid \operatorname{lcm}(k_1, k_2, k_3)$, we have $h(p^t) \mid h(p^t)[a,b,c]$. This fact together with (2.3) yields (5.13). □

Remark 5.10. If $[a,b,c] \pmod{p} \notin E_p(\alpha_1) \cup E_p(\beta_1) \cup E_p(\gamma_1)$, then in (5.13) we have $h(p) = h(p)[a,b,c]$. In the opposite case, we have $h(p)[a,b,c] = \operatorname{ord}_p(\lambda)$ for some $\lambda \in S_{p^t}(T)$ and the equality $h(p)[a,b,c] = h(p)$ need not hold in general. See (5.8).

We will use the results obtained in this paper along with the results proved in [2] to solve a problem in combinatorics which is closely related to the modular periodicity of Tribonacci sequences. See [3].

References

[1] *M. Elia*: Derived sequences, the Tribonacci recurrence and cubic forms. The Fibonacci Quarterly *39.2* (2001), 107–115.

[2] *J. Klaška*: Tribonacci modulo 2^t and 11^t. To appear in Math. Bohem.

[3] *J. Klaška*: Tribonacci partition formulas modulo m. Preprint (2007).

[4] *Z.-H. Sun, Z.-W. Sun*: Fibonacci numbers and Fermat's last theorem. Acta Arith. *60* (1992), 371–388.

[5] *A. Vince*: Period of a linear recurrence. Acta Arith. *39* (1981), 303–311.

[6] *M. E. Waddill*: Some properties of a generalized Fibonacci sequence modulo m. The Fibonacci Quarterly *16* (Aug. 1978), no. 4, 344–353.

[7] *D. D. Wall*: Fibonacci series modulo m. Amer. Math. Monthly *67* (1960), no. 6, 525–532.

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`.