PERIODS OF THE TRIBONACCI SEQUENCE MODULO A PRIME $\mathbf{p \equiv 1 \pmod 3}$

JIŘÍ KLAŠKA AND LADISLAV SKULA

Abstract. Let the Tribonacci polynomial $t(x) = x^3 - x^2 - x - 1$ be irreducible over the Galois field $\mathbb{F}_p$ where p is an arbitrary prime such that $p \equiv 1 \pmod 3$ and let τ be any root of $t(x)$ in the splitting field K of $t(x)$ over $\mathbb{F}_p$. We prove that $\tau^{(p^2+p+1)/3} = 1$. Using this identity we show that the period $h(p)$ of the sequence $(T_n \bmod p)_{n=0}^{\infty}$ where T_n is the nth Tribonacci number divides $(p^2 + p + 1)/3$. Similar results will also be obtained for $t(x)$ being reducible over $\mathbb{F}_p$. In this case we prove that the period $h(p)$ divides $(q - 1)/3$ where q is the number of elements of the splitting field of $t(x)$ over $\mathbb{F}_p$ if and only if 2 is a cubic residue of $\mathbb{F}_p$.

1. Introduction and Preliminaries

The Tribonacci sequence $(T_n)_{n=0}^{\infty}$ is defined by the third order linear recurrence $T_{n+3} = T_{n+2} + T_{n+1} + T_n$ with a triple of initial values $T_0 = 0$, $T_1 = 0$, and $T_2 = 1$. It is well-known, [9, Theorem 1] that $(T_n \bmod m)_{n=0}^{\infty}$ is simply periodic for any modulus $m > 1$. That is, the first three terms which are repeated in $(T_n \bmod m)_{n=0}^{\infty}$ are $0, 0, 1$. The least positive integer $h(m)$ satisfying $T_{h(m)} \equiv T_{h(m)+1} \equiv 0 \pmod m$ and $T_{h(m)+2} \equiv 1 \pmod m$ is called a period of $(T_n \bmod m)_{n=0}^{\infty}$. If $m = p$ is a prime, $h(p)$ depends in an essential way on the form of the factorization of the Tribonacci polynomial $t(x) = x^3 - x^2 - x - 1$ over the Galois field $\mathbb{F}_p$. Let K denote the splitting field of $t(x)$ over $\mathbb{F}_p$ and let α, β, γ be the roots of $t(x)$ in K. Since the discriminant of $t(x)$ is equal to $-2^2 \cdot 11$, for $p \neq 2, 11$, the roots α, β, γ are distinct. For any $0 \neq \xi \in K$, let $\mathrm{ord}_K(\xi)$ denote the order of ξ in the multiplicative group $K^{\times}$ of K. By [10, Section 8], the problem of determining $h(p)$ is equivalent to the problem of determining the orders of α, β, γ in $K^{\times}$. See also [1, 2, 7]. Let $I = \{3, 5, 23, 31, \dots\}$ be the set of all primes p for which $t(x)$ is irreducible over $\mathbb{F}_p$, $Q = \{7, 13, 17, 19, \dots\}$ be the set of all primes for which $t(x)$ splits over $\mathbb{F}_p$ into the product of a linear factor and an irreducible quadratic factor and let $L = \{2, 11, 47, 53, \dots\}$ be the set of all primes for which $t(x)$ completely splits over $\mathbb{F}_p$ into linear factors. Then we can state the following theorem.

Theorem 1.1. *Let $p \neq 2, 11$ be a prime. Then*

(i) $h(p) = \mathrm{lcm}(\mathrm{ord}_K(\alpha), \mathrm{ord}_K(\beta), \mathrm{ord}_K(\gamma))$.
(ii) *If $p \in I$, then $h(p) = \mathrm{ord}_K(\tau)$ where τ is any root of $t(x)$ in K.*
(iii) *$p \in I$ or $p \in L$ if and only if the Legendere-Jacobi symbol $(p/11) = 1$.*
(iv) *$p \in I$ if and only if $T_p^2 \equiv -4/11 \pmod p$.*
(v) *$p \in L$ if and only if $T_p \equiv 0 \pmod p$.*

The second author was supported by the Grant Agency of the Czech Republic (Algebraic, Analytic and Combinatorial Number Theory, 201/07/0191) and the result was acquired using the subsidization of the Ministry of Education, Youth and Sports of the Czech Republic, research plan MSM0021630518 "Simulation Modeling of Mechatronic Systems".

Statements (i) and (ii) are well-known. For example, see [1, p. 292], [7, p. 306] or consult [10, p. 161]. Statement (iii) is a consequence of more general results of L. Stickelberger [5] and G. Voronoï [8]. For details see [3]. Finally, statements (iv) and (v) are straightforward consequences of [6, Theorem 4.3].

The following theorem is due to A. Vince [7, Theorem 4].

Theorem 1.2. *Let $p \neq 2, 11$ be a prime. Then*

(i) *If $p \in L$, then $h(p) | p - 1$.*
(ii) *If $p \in Q$, then $h(p) | p^2 - 1$.*
(iii) *If $p \in I$, then $h(p) | p^2 + p + 1$.*

In Theorem 4.1 of this paper, we strengthen Vince's result for $p \equiv 1 \pmod 3$ as follows:

(i) If $p \in L$, then $h(p) | \frac{p-1}{3}$ if and only if 2 is a cubic residue of the field $\mathbb{F}_p$.
(ii) If $p \in Q$, then $h(p) | \frac{p^2-1}{3}$ if and only if 2 is a cubic residue of the field $\mathbb{F}_p$.
(iii) If $p \in I$, then $h(p) | \frac{p^2+p+1}{3}$.

To prove this statement, we shall need the following result presented in [3].

Theorem 1.3. *Let p be an arbitrary prime such that $p \equiv 1 \pmod 3$ and let τ be any root of $t(x)$ in the field $\mathbb{F}_p$. Then*

$$\tau^{\frac{p-1}{3}} \equiv 2^{\frac{2(p-1)}{3}} \pmod p. \tag{1.1}$$

Moreover, if τ is any root of $t(x)$ in the splitting field K of $t(x)$ over $\mathbb{F}_p$, then 2τ is a cubic residue of K, i.e., there exists $\omega \in K$ such that $2\tau = \omega^3$.

2. A Way to Distinguish the Cases $p \in L$ and $p \in I$ For Primes $(p/11) = 1$, $p \equiv 1 \pmod 3$

Let $\mathbb{F}$ be a finite field with prime characteristic $p \equiv 1 \pmod 3$. Then $\mathbb{F} = \mathbb{F}_{p^n}$ for a positive integer n and there exists an $\varepsilon \in \mathbb{F}^\times$ with the property $\varepsilon^3 = 1$, $\varepsilon \neq 1$. Therefore, $\varepsilon^2+\varepsilon+1 = 0$. Let $\mathbb{F}^\times$ denote the multiplicative group of $\mathbb{F}$ with a generator g. For $e \in \{0, 1, 2\}$, put $C_e = \{\xi \in \mathbb{F}^\times; \xi = g^{3k+e}, k \in \mathbb{Z}, 0 \leq k < (p^n - 1)/3\}$. The sets C_e are called the cubic classes of $\mathbb{F}$ and the elements of C_0 the cubic residues of $\mathbb{F}$. The following lemma can be found in [3, Lemma 2.7].

Lemma 2.1. *Let $\alpha, \beta, \gamma \in \mathbb{F}$. If $\alpha\beta\gamma$ is the cubic residue of $\mathbb{F}$, then either α, β, γ belong to distinct cubic classes of $\mathbb{F}$ or α, β, γ belong to the same cubic class of $\mathbb{F}$.*

Let $f(x) = x^3 + rx + s \in \mathbb{F}[x]$, $r, s \neq 0$. Assume that $f(x)$ is irreducible over $\mathbb{F}$ or $f(x)$ has three distinct roots in $\mathbb{F}$. Put $d = \frac{s^2}{4} + \frac{r^3}{27}$. Since char $\mathbb{F} \neq 2, 3$, the element d is well defined. Next, assume that there exists a $\lambda \in \mathbb{F}$ such that $\lambda^2 = d$. Let

$$A = -\frac{s}{2} + \lambda \text{ and } B = -\frac{s}{2} - \lambda. \tag{2.1}$$

Then $AB = \frac{s^2}{4} - d = (-\frac{r}{3})^3$, which implies that

$$A \text{ is a cubic residue of } \mathbb{F} \text{ if and only if } B \text{ is a cubic residue of } \mathbb{F}. \tag{2.2}$$

The following lemma is essentially Cardano's formula for the field $\mathbb{F}$.

Lemma 2.2. *Let A, B be cubic residues of the field $\mathbb{F}$. Then there exist $\alpha, \beta \in \mathbb{F}$ such that $\alpha^3 = A$, $\beta^3 = B$, $\alpha\beta = -\frac{r}{3}$ and $\alpha + \beta$ is a root of $f(x)$ in $\mathbb{F}$.*

Proof. Since A, B are cubic residues of $\mathbb{F}$, there exist $\alpha, \gamma \in \mathbb{F}$ such that $\alpha^3 = A$, $\gamma^3 = B$. Then $(\alpha\gamma)^3 = AB = (-\frac{r}{3})^3$ and, consequently, there exists $e \in \{0,1,2\}$ such that $\alpha\gamma\varepsilon^e = -\frac{r}{3}$. Let $\beta = \gamma\varepsilon^e$. Then $\beta^3 = B$, $\alpha\beta = -\frac{r}{3}$ and $f(\alpha+\beta) = (\alpha+\beta)^3 + r(\alpha+\beta) + s = A + 3\alpha\beta(\alpha+\beta) + B + r\alpha + r\beta + s = -s - r(\alpha+\beta) + r\alpha + r\beta + s = 0$. □

Lemma 2.3. *Let $f(x)$ have three distinct roots in $\mathbb{F}$. Then A, B are cubic residues of $\mathbb{F}$.*

Proof. Suppose that A and B are not cubic residues of $\mathbb{F}$ and let $\mathbb{G}$ be the splitting field of $x^3 - A$ over $\mathbb{F}$. Since A is a cubic residue of $\mathbb{G}$, B is a cubic residue of $\mathbb{G}$ by (2.2). Applying Lemma 2.2 to the field $\mathbb{G}$, we see that there exist $\alpha, \beta \in \mathbb{G}$ such that $\alpha^3 = A$, $\beta^3 = B$, $\alpha\beta = -\frac{r}{3}$ and $\alpha+\beta$ is a root of $f(x)$ in $\mathbb{G}$. As assumed, the roots of $f(x)$ belong to $\mathbb{F}$ and thus $\alpha+\beta \in \mathbb{F}$. Since $1, \alpha, \alpha^2$ is a basis of the extension $\mathbb{G}/\mathbb{F}$, there exist $a, b, c \in \mathbb{F}$ such that $\beta = a\alpha^2 + b\alpha + c$. Furthermore, $\alpha + \beta \in \mathbb{F}$ and $\alpha + \beta = a\alpha^2 + (b+1)\alpha + c$, implies $a = 0$, $b = -1$ and thus $\beta = -\alpha + c$. Then $B = \beta^3 = -\alpha^3 + 3\alpha^2 c - 3\alpha c^2 + c^3 = -A + 3\alpha^2 c - 3\alpha c^2 + c^3$, which implies $A + B = 3\alpha^2 c - 3\alpha c^2 + c^3$. Next, $A + B \in \mathbb{F}$ implies $c = 0$. Hence, $-\frac{s}{2} - \lambda = B = -A = \frac{s}{2} - \lambda$, which yields $s = 0$, and a contradiction follows. □

Combining (2.2), Lemma 2.2, and Lemma 2.3 we get the following theorem.

Theorem 2.4. *The following statements are equivalent:*

(i) *The polynomial $f(x) = x^3 + rx + s \in \mathbb{F}[x]$ has three distinct roots in $\mathbb{F}$.*
(ii) *$A = -\frac{s}{2} + \lambda$ is a cubic residue of $\mathbb{F}$.*
(iii) *$B = -\frac{s}{2} - \lambda$ is a cubic residue of $\mathbb{F}$.*

Now we apply Theorem 2.4 to a Tribonacci polynomial $t(x)$ and field $\mathbb{F} = \mathbb{F}_p$ where p is an arbitrary prime such that $p \equiv 1 \pmod 3$ and $(p/11) = 1$.

The assumption $(p/11) = 1$ implies, by Theorem 1.1, part (iii), that $t(x)$ is irreducible over $\mathbb{F}_p$, or $t(x)$ has three distinct roots in $\mathbb{F}_p$. Using the substitution $x = y + \frac{1}{3}$, we can easily convert $t(x)$ to the form $\bar{t}(y) = y^3 - \frac{4}{3}y - \frac{38}{27}$. Hence, $r = -\frac{4}{3}$, $s = -\frac{38}{27}$, and $d = \frac{11}{27}$. Since $(19/11) = -1$, we have $r, s, d \neq 0$ in the field $\mathbb{F}_p$ where $p \equiv 1 \pmod 3$ and $(p/11) = 1$. After some calculation, we find that $(d/p) = (33/p) = 1$ and thus there exists $\lambda \in \mathbb{F}_p$ such that $\lambda^2 = d$. Put $\varkappa = 9\lambda$. Then $\varkappa^2 = 33$ and (2.1) yields $A = \frac{1}{27}(19 + 3\varkappa)$ and $B = \frac{1}{27}(19 - 3\varkappa)$.

From this and from Theorem 2.4, we get the following criterion, which can be used for $t(x)$ and for a prime $p \equiv 1 \pmod 3$, $(p/11) = 1$ to decide whether $p \in L$ or $p \in I$.

Theorem 2.5. *Let p be a prime, $p \equiv 1 \pmod 3$ and let $(p/11) = 1$. Then the following statements are equivalent:*

(i) *The Tribonacci polynomial $t(x)$ has three distinct roots in $\mathbb{F}_p$.*
(ii) *$19 + 3\varkappa$ is a cubic residue of $\mathbb{F}_p$.*
(iii) *$19 - 3\varkappa$ is a cubic residue of $\mathbb{F}_p$.*

The following proposition will be needed in the next section.

Proposition 2.6. *Let p be a prime, $p \equiv 1 \pmod 3$ and let $(p/11) = 1$. Furthermore, let $\rho = (13 + 3\varkappa)/2$ and $\sigma = (13 - 3\varkappa)/2$ where $\varkappa \in \mathbb{F}_p$ such that $\varkappa^2 = 33$. Then the following statements are equivalent:*

(i) *The elements $2, \rho, \sigma$ belong to the same cubic class of $\mathbb{F}_p$.*
(ii) *$26 + 6\varkappa$ is a cubic residue of $\mathbb{F}_p$.*
(iii) *$26 - 6\varkappa$ is a cubic residue of $\mathbb{F}_p$.*

Proof. The equivalence of (ii) and (iii) follows from the equality $(26+6\varkappa)(26-6\varkappa) = (-8)^3$. We prove that (i) implies (ii). Since 2 and ρ belong to the same cubic class of $\mathbb{F}_p$, there exists $\omega \in \mathbb{F}_p$ such that $\rho = 2\omega^3$. Hence, $\omega^3 = \rho/2 = (13+3\varkappa)/4 = (26+6\varkappa)/8$, which proves that $26+6\varkappa$ is a cubic residue of $\mathbb{F}_p$. Conversely, assume (ii). Then $(26+6\varkappa)/8$ is a cubic residue of $\mathbb{F}_p$ and thus there exists $\omega \in \mathbb{F}_p$ such that $\omega^3 = (26+6\varkappa)/8$. Hence, we have $2\omega^3 = (13+3\varkappa)/2 = \rho$, which means that 2 and ρ belong to the same cubic class of $\mathbb{F}_p$. In a similar way, we can deduce that 2 and σ belong to the same cubic class of $\mathbb{F}_p$. Hence, (ii) implies (i). The proof is complete. ☐

3. The Existence and Properties of the Roots of the Polynomial $x^3 - \tau$ in the Field Extension $K/\mathbb{F}_p$ for a Prime $p \in I$

Let $p \in I$. Recall that K is the splitting field of $t(x)$ over $\mathbb{F}_p$ and α, β, γ are the roots of $t(x)$ in K. Then $\{\alpha, \beta, \gamma\} = \{\tau, \tau^p, \tau^{p^2}\}$ for any $\tau \in \{\alpha, \beta, \gamma\}$. Together with the Viète equation $\alpha\beta\gamma = 1$, this yields $\tau^{p^2+p+1} = 1$. Now we can prove the following lemma.

Lemma 3.1. *Let $p \in I$, $p \equiv 1 \pmod 3$ and let τ be an arbitrary root of $t(x)$ in K. Then there exist exactly three distinct roots ξ_1, ξ_2, ξ_3 of $x^3 - \tau$ in K.*

Proof. Since K is a finite field, the multiplicative group $K^\times$ is cyclic. Let g be a generator of $K^\times$. Then $\tau = g^t$ for a positive integer t. Since $1 = \tau^{p^2+p+1} = g^{t(p^2+p+1)}$, we have $p-1|t$. Hence, $3|t$. Set $\xi_i = g^{t/3+(i-1)(p^3-1)/3}$ for $i \in \{1,2,3\}$. Then ξ_1, ξ_2, ξ_3 are three distinct roots of $x^3 - \tau$ in K. ☐

The proofs of the following lemmas are easy to see.

Lemma 3.2. *Let $p \in I$, $p \equiv 1 \pmod 3$ and let τ be an arbitrary root of $t(x)$ in K. Furthermore, let ξ_1, ξ_2, ξ_3 be the roots of $x^3 - \tau$ in K. Then:*

(i) $\{\xi_1, \xi_2, \xi_3\} = \{\xi, \varepsilon\xi, \varepsilon^2\xi\}$ *for any* $\xi \in \{\xi_1, \xi_2, \xi_3\}$.
(ii) $\xi_1\xi_2\xi_3 = \tau$.
(iii) $\xi_1 + \xi_2 + \xi_3 = \xi_1^2 + \xi_2^2 + \xi_3^2 = \xi_1\xi_2 + \xi_1\xi_3 + \xi_2\xi_3 = 0$.

Let $p \in I$, $p \equiv 1 \pmod 3$ and let τ be an arbitrary root of $t(x)$ in K. Further, let ξ be an arbitrary root of $x^3 - \tau$ in K. Put $c(p) = -\xi^{p^2+p+1}$. It is easy to see that $c(p)$ does not depend on the choice of ξ and τ. Since $\xi^3 = \tau$ and $\tau^{p^2+p+1} = 1$, we have $c(p)^3 = -1$. Hence $c(p) \in \{-1, -\varepsilon, -\varepsilon^2\}$. Furthermore, let $w(x) = (x-\xi)(x-\xi^p)(x-\xi^{p^2})$. Then $w(x) \in \mathbb{F}_p[x]$ and $w(x)$ is irreducible over $\mathbb{F}_p$. For further considerations we will need the following polynomials defined in [3, Section 2]. For $c = c(p)$, put $f(x,c) = x^3 + A(c)x^2 + B(c)x + C(c) \in \mathbb{F}_p[x]$ where $A(c) = -18c^2 + 3$, $B(c) = -9c^2 - 27c - 24$, and $C(c) = 9c^2 - 27c + 28$. In particular, for $c = -1$ we have $f(x,-1) = x^3 - 15x^2 - 6x + 64$.

Lemma 3.3. *For any prime $p \in I$, $p \equiv 1 \pmod 3$, the following is true:*

(i) *$f(x, c(p))$ has three distinct roots in $\mathbb{F}_p$ belonging to distinct cubic classes of $\mathbb{F}_p$.*
(ii) *Let $c_1, c_2 \in \{-1, -\varepsilon, -\varepsilon^2\}$ and $b_1, b_2 \in \mathbb{F}_p$. If $f(b_1^3, c_1) = f(b_2^3, c_2) = 0$ then $c_1 = c_2$.*

For a proof of (i) see [3, Theorem 3.2] and for a proof of (ii) consult [3, Lemma 3.3]. The validity of the following lemma is easy to verify.

Lemma 3.4. *Let p be a prime, $p \equiv 1 \pmod 3$ and let $(p/11) = 1$. Then the polynomial $f(x,-1) = x^3 - 15x^2 - 6x + 64$ completely splits into linear factors over the field $\mathbb{F}_p$ and has three distinct roots $2, \rho = (13+3\varkappa)/2$, and $\sigma = (13-3\varkappa)/2$ where $\varkappa \in \mathbb{F}_p$ such that $\varkappa^2 = 33$.*

Now we are ready for the following theorem.

Theorem 3.5. *Let $p \in I$ and $p \equiv 1 \pmod 3$. Then $c(p) = -1$.*

Proof. By Theorem 2.5, $19-3\varkappa$ is not a cubic residue of the field $\mathbb{F}_p$. Since $(19-3\varkappa)(26+6\varkappa) = (-1+\varkappa)^3$, the element $26+6\varkappa$ is not a cubic residue of $\mathbb{F}_p$ either. By Lemma 3.4, the polynomial $f(x,-1)$ has three distinct roots $2, \rho, \sigma$ in $\mathbb{F}_p$ and Lemma 2.1, together with Proposition 2.6, yields that $2, \rho, \sigma$ belong to distinct cubic classes of $\mathbb{F}_p$. Hence, there exists a $b_2 \in \mathbb{F}_p$ such that $b_2^3 \in \{2, \rho, \sigma\}$ and $f(b_2^3, -1) = 0$. By Lemma 3.3, part (i), there exists $b_1 \in \mathbb{F}_p$ such that $f(b_1^3, c(p)) = 0$ and from Lemma 3.3, part (ii) we get $c(p) = -1$. □

Theorem 3.6. *Let $p \in I$, $p \equiv 1 \pmod 3$ and let τ be an arbitrary root of $t(x)$ in the splitting field K of $t(x)$ over $\mathbb{F}_p$. Furthermore, let ξ be any root of $x^3 - \tau$ in K. Then $\xi^{p^2+p+1} = 1$ and*

$$\tau^{\frac{p^2+p+1}{3}} = 1. \tag{3.1}$$

Proof. From Theorem 3.5 and the definition of $c(p)$ we immediately get $\xi^{p^2+p+1} = 1$. Since $\xi^3 = \tau$, we have $\tau^{(p^2+p+1)/3} = \xi^{p^2+p+1} = 1$ as required. □

Corollary 3.7. Let $p \in I$ and $p \equiv 1 \pmod 3$. Then $u(x) := t(x^3) = x^9 - x^6 - x^3 - 1$ factors over $\mathbb{F}_p$ into the product of three irreducible polynomials $w(x)$, $w(\varepsilon x)$, $w(\varepsilon^2 x)$ with constant terms equal to -1.

Remark 3.8. (i) Let $p \in I$ and τ be an arbitrary root of $t(x)$ in the splitting field K of $t(x)$ over $\mathbb{F}_p$. It is easy to prove by induction that

$$\tau^k = T_k\tau^2 + (T_{k-1} + T_{k-2})\tau + T_{k-1}, \ k > 1. \tag{3.2}$$

From equality (3.2) it follows for $k > 1$ that

$$\tau^k = \varepsilon \text{ if and only if } T_k \equiv T_{k+1} \equiv 0 \pmod p \text{ and } T_{k+2} \equiv \varepsilon \pmod p. \tag{3.3}$$

(ii) Put $H =< g^{p-1} >$ where g is the generator of $K^\times$. Then H is a cyclic group of order $p^2 + p + 1$. Since $\tau^{p^2+p+1} = 1$, we have $\tau \in H$ and $G =< \tau >$ is a subgroup of H. Let $p \equiv 1 \pmod 3$. Then in H, there exist exactly three elements belonging to $\mathbb{F}_p$. These are $1, \varepsilon, \varepsilon^2$. Moreover, together with $9 \nmid p^2 + p + 1$, (3.1) yields $\varepsilon, \varepsilon^2 \notin G$.

Theorem 3.9. *Let $p \in I$, $p \equiv 1 \pmod 3$ and let τ be an arbitrary root of $t(x)$ in the splitting field K of $t(x)$ over $\mathbb{F}_p$. Furthermore, let $\xi \in \{\xi_1, \xi_2, \xi_3\}$ be any root of $x^3 - \tau$ in K. Then $\mathrm{ord}_K(\xi) = \mathrm{ord}_K(\tau)$ or $\mathrm{ord}_K(\xi) = 3 \cdot \mathrm{ord}_K(\tau)$. Moreover, exactly one of the roots ξ_1, ξ_2, ξ_3 is of an order equal to $\mathrm{ord}_K(\tau)$ and two roots are of orders equal to $3 \cdot \mathrm{ord}_K(\tau)$.*

Proof. For brevity, put $\mathrm{ord}_K(\tau) = h$ and $\mathrm{ord}_K(\xi) = k$. We have $\xi^3 = \tau$ and so $\xi^{3h} = \tau^h = 1$, which means that $k | 3h$. On the other hand, $\xi^k = 1$ implies $\xi^{3k} = 1$. Together with $\xi^3 = \tau$ this yields $\tau^k = 1$ and $h | k$ follows. Consequently, there exist positive integers c_1, c_2 such that $c_1 \cdot k = 3 \cdot h$ and $k = c_2 \cdot h$. Hence, we have $c_1c_2 = 3$, which yields $c_1 = 1, c_2 = 3$ or $c_1 = 3, c_2 = 1$. Consequently, $\mathrm{ord}_K(\xi) = \mathrm{ord}_K(\tau)$ or $\mathrm{ord}_K(\xi) = 3 \cdot \mathrm{ord}_K(\tau)$.

Since the orders of the elements ξ_1, ξ_2, ξ_3 can only take on two values h and $3h$, at least two of them have the same order. Denote this order by h_0. Without loss of generality, we can assume $\mathrm{ord}_K(\xi_1) = \mathrm{ord}_K(\xi_2) = h_0$. Put $\xi_1 = \xi$. Since $\{\xi_1, \xi_2, \xi_3\} = \{\xi, \varepsilon\xi, \varepsilon^2\xi\}$, either $\mathrm{ord}_K(\xi) = \mathrm{ord}_K(\varepsilon\xi) = h_0$ or $\mathrm{ord}_K(\xi) = \mathrm{ord}_K(\varepsilon^2\xi) = h_0$. Hence, it easily follows that $3 | h_0$ and thus $h_0 = 3r$ for some positive integer r. Using Lemma 3.2, part (ii), we get

$\tau^{3r} = (\xi_1\xi_2\xi_3)^{h_0} = \xi_3^{h_0} = \tau^r$. Hence, $\tau^{2r} = 1$. Since $2 \nmid h$, we have $h|r$. This, together with $h_0 \in \{h, 3h\}$, yields $h_0 = 3h$. Consequently, we have either

$$\mathrm{ord}_K(\xi_1) = \mathrm{ord}_K(\xi_2) = \mathrm{ord}_K(\xi_3) = 3 \cdot \mathrm{ord}_K(\tau) = 3h \tag{3.4}$$

or

$$\mathrm{ord}_K(\xi_1) = \mathrm{ord}_K(\xi_2) = 3 \cdot \mathrm{ord}_K(\tau) \text{ and } \mathrm{ord}_K(\xi_3) = \mathrm{ord}_K(\tau). \tag{3.5}$$

In both cases, there exist $u, v \in \{\varepsilon, \varepsilon^2\}$ such that $\xi_1^h = u$, and $\xi_2^h = v$. First, assume that $u \neq v$. Then $\xi_1^h\xi_2^h = \varepsilon^3 = 1$, which yields $\xi_3^h = (\xi_1\xi_2\xi_3)^h = \tau^h = 1$. Hence, we have $\mathrm{ord}_K(\xi_3)|h$ and (3.5) follows. Further, assume that $u = v$. Since we have put $\xi_1 = \xi$, we have either $\xi^h = \varepsilon^h\xi^h$ or $\xi^h = \varepsilon^{2h}\xi^h$. Hence, $3|h$. Assume (3.4) is true. Then $\mathrm{ord}_K(\xi_3) = 3h$ and, thus, $9|\mathrm{ord}_K(\xi)$ for any $\xi \in \{\xi_1, \xi_2, \xi_3\}$. Since $9 \nmid p^2 + p + 1$, we have $\xi^{p^2+p+1} \neq 1$, which is a contradiction to Theorem 3.6. Hence, we have (3.5) and the theorem follows. □

Corollary 3.10. Let $p \in I$, $p \equiv 1 \pmod 3$ and let τ be an arbitrary root of $t(x)$ in the splitting field K of $t(x)$ over $\mathbb{F}_p$. Then $x^9 - \tau$ has exactly 9 distinct roots in K.

Proof. Since $\tau^{\frac{p^2+p+1}{3}} = 1$, the proof is a simple modification of the proof of Lemma 3.1. □

Example 3.11. Let $p = 37$. Then $p \equiv 1 \pmod 3$ and it can be verified that $p \in I$. Let K be the splitting field of $t(x)$ over $\mathbb{F}_{37}$ and let τ be any root of $t(x)$ in K. By Lemma 3.1, the polynomial $x^3 - \tau$ has three distinct roots ξ_1, ξ_2, ξ_3 in K. In the field $\mathbb{F}_{37}$ we have $\varepsilon = 10$, and Lemma 3.2, part (i), yields $\xi_2 = 10\xi_1$ and $\xi_3 = 15\xi_1$. Using the basis $1, \tau, \tau^2$ of the field extension $K/\mathbb{F}_p$, ξ_1, ξ_2, ξ_3 can be written in the form

$$\xi_1 = 2 + 16\tau + 24\tau^2,\ \xi_2 = 20 + 12\tau + 18\tau^2,\ \xi_3 = 15 + 9\tau + 32\tau^2.$$

By direct calculation we obtain $\mathrm{ord}_K(\tau) = 469$, $\mathrm{ord}_K(\xi_1) = \mathrm{ord}_K(\xi_2) = 1407$ and $\mathrm{ord}_K(\xi_3) = 469$. Consequently, by Theorem 1.1, part (ii), and Theorem 3.9, $h(37) = \mathrm{ord}_K(\tau) = \mathrm{ord}_K(\xi_3) = 469$. Furthermore, by Corollary 3.10, there exist 9 distinct roots of $x^9 - \tau$ in K:

$$\begin{array}{lllllllll}
\xi_{11} & = & 4 + 36\tau + 12\tau^2, & \xi_{12} & = & 3 + 27\tau + 9\tau^2, & \xi_{13} & = & 30 + 11\tau + 16\tau^2, \\
\xi_{21} & = & 21 + 4\tau + 26\tau^2, & \xi_{22} & = & 25 + 3\tau + \tau^2, & \xi_{23} & = & 28 + 30\tau + 10\tau^2, \\
\xi_{31} & = & 11 + 25\tau + 33\tau^2, & \xi_{32} & = & 27 + 21\tau + 7\tau^2, & \xi_{33} & = & 36 + 28\tau + 34\tau^2.
\end{array}$$

Moreover, for any $i, j \in \{1, 2, 3\}$, we have $\xi_{ij}^3 = \xi_i$. Let $w_1(x) = x^3 + 17x^2 + 31x - 1$, $w_2(x) = w_1(\varepsilon x) = x^3 + 22x^2 + 29x - 1$, and $w_3(x) = w_1(\varepsilon^2 x) = x^3 + 35x^2 + 14x - 1$. Then ξ_i, ξ_i^p, $\xi_i^{p^2}$, $i \in \{1, 2, 3\}$ are the roots of $w_i(x)$ and $x^9 - x^6 - x^3 - 1 \equiv w_1(x)w_2(x)w_3(x) \pmod{37}$ as required by Corollary 3.7.

4. Periods of the Tribonacci Sequence Modulo a Prime $p \equiv 1 \pmod 3$

Recall that, for a prime p, $h(p)$ denotes the period of $(T_n \bmod p)_{n=0}^{\infty}$. In this section we prove our main theorem extending Vince's result [7, Theorem 4].

Theorem 4.1. *Let p be an arbitrary prime, $p \equiv 1 \pmod 3$.*

(i) *If $p \in L$, then $h(p)|\frac{p-1}{3}$ if and only if 2 is a cubic residue of the field $\mathbb{F}_p$.*
(ii) *If $p \in Q$, then $h(p)|\frac{p^2-1}{3}$ if and only if 2 is a cubic residue of the field $\mathbb{F}_p$.*
(iii) *If $p \in I$, then $h(p)|\frac{p^2+p+1}{3}$.*

Proof. The congruence $p \equiv 1 \pmod 3$ implies $p \neq 2, 11$.

(i) Let $p \in L$ and let τ be any root of $t(x)$ in $\mathbb{F}_p$. If 2 is a cubic residue of $\mathbb{F}_p$, it follows from (1.1) that $\tau^{(p-1)/3} \equiv 1 \pmod p$. Hence, $\mathrm{ord}_{\mathbb{F}_p}(\tau) | \frac{p-1}{3}$ and Theorem 1.1, part (i), imply $h(p) | \frac{p-1}{3}$. On the other hand, if $h(p) | \frac{p-1}{3}$, then $\mathrm{ord}_{\mathbb{F}_p}(\tau) | \frac{p-1}{3}$ for any root τ of $t(x)$ in $\mathbb{F}_p$. Consequently, $\tau^{(p-1)/3} \equiv 1 \pmod p$ and (1.1) yields $2^{2(p-1)/3} \equiv 1 \pmod p$. This implies that either $2^{(p-1)/3} \equiv -1 \pmod p$ or 2 is a cubic residue of $\mathbb{F}_p$. Suppose that $2^{(p-1)/3} \equiv -1 \pmod p$. Then $1 \equiv 2^{p-1} \equiv (2^{(p-1)/3})^3 \equiv (-1)^3 \equiv -1$, which yields $2 \equiv 0 \pmod p$. Since $p \neq 2$, a contradiction follows.

(ii) Let $p \in Q$. Then the multiplicative group $K^\times$ of the splitting field K of $t(x)$ over $\mathbb{F}_p$ has $p^2 - 1$ elements. Let τ be any root of $t(x)$ in K. Then, by Theorem 1.3, there exists $\omega \in K$ such that $2\tau = \omega^3$. Let 2 be a cubic residue of $\mathbb{F}_p$. Then $2^{(p^2-1)/3} = 1$ in K and so $\tau^{(p^2-1)/3} = (2\tau)^{(p^2-1)/3} = \omega^{p^2-1} = 1$. This implies $\mathrm{ord}_K(\tau) | \frac{p^2-1}{3}$ and Theorem 1.1, part (i), yields $h(p) | \frac{p^2-1}{3}$. Conversely, assume that $h(p) | \frac{p^2-1}{3}$. Then $\mathrm{ord}_K(\tau) | \frac{p^2-1}{3}$ for any root τ of $t(x)$ in K and $\tau^{(p^2-1)/3} = 1$. From $2\tau = \omega^3$, we get $(2\tau)^{(p^2-1)/3} = \omega^{p^2-1} = 1$, which implies $2^{(p^2-1)/3} = 1$ in K. Clearly, $1 \equiv 2^{(p^2-1)/3} \equiv (2^{(p-1)/3})^{p+1} \equiv 2^{2(p-1)/3} \pmod p$. Using an argument similar to that in (i), we obtain $2^{(p-1)/3} \equiv 1 \pmod p$ and (ii) follows.

(iii) Let $p \in I$ and let τ be any root of $t(x)$ in the splitting field K of $t(x)$ over $\mathbb{F}_p$. Then, by (3.1), we have $\tau^{(p^2+p+1)/3} = 1$. This implies $\mathrm{ord}_K(\tau) | \frac{p^2+p+1}{3}$ and part (ii) of Theorem 1.1 yields $h(p) | \frac{p^2+p+1}{3}$ as required. □

Remark 4.2. If $p \equiv 1 \pmod 3$, then 2 is a cubic residue of the field $\mathbb{F}_p$ if and only if there are integers u and v such that $p = u^2 + 27v^2$ [4, p. 119].

Let m be a positive integer, $m > 1$. In 1978, M. E. Waddill [9, Theorem 2] proved:

$$\text{if } \; T_k \equiv T_{k+1} \equiv 0 \pmod m, \; \text{ then } \; T_{k+2}^3 \equiv 1 \pmod m. \tag{4.1}$$

Moreover, if k is the least positive integer such that $T_k \equiv T_{k+1} \equiv 0 \pmod m$, then either $T_{k+2} \equiv 1 \pmod m$ or $T_{3k+2} \equiv 1 \bmod m$ and the period $h(m)$ of $(T_n \bmod m)_{n=0}^{\infty}$ is k or $3k$ [9, Theorem 10]. If $m = p \in I$, we can say more.

Proposition 4.3. *Let k be the least positive integer such that $T_k \equiv T_{k+1} \equiv 0 \pmod p$. If $p \in I$, then $h(p) = k$.*

Proof. By (4.1), the congruences $T_k \equiv T_{k+1} \equiv 0 \pmod p$ imply $T_{k+2}^3 \equiv 1 \pmod p$. Suppose that $T_{k+2} \not\equiv 1 \pmod p$. First, it is evident that, for $p \equiv 2 \pmod 3$, we have $T_{k+2}^3 \equiv 1 \pmod p$ if and only if $T_{k+2} \equiv 1 \pmod p$. Hence, $p \equiv 1 \pmod 3$ or $p = 3$. Let $p \equiv 1 \pmod 3$. Then $T_{k+2} \not\equiv 1 \pmod p$ implies $T_{k+2} \equiv \varepsilon \pmod p$ and (3.3) yields $\tau^k = \varepsilon$. Since, by Remark 3.8, we have $\varepsilon \notin G = <\tau>$, a contradiction follows. Finally, for $p = 3$, the proof can be done by direct calculation. □

Let $(t_n)_{n=0}^{\infty} = (a, b, c, a+b+c, a+2b+2c, \dots)$ be a generalized Tribonacci sequence beginning with an arbitrary triple of integers $t_0 = a, t_1 = b, t_2 = c$. In 2008, J. Klaška [2] investigated the period $h(m)[a, b, c]$ of the sequence $(t_n \bmod m)_{n=0}^{\infty}$ where the modulus m is a power of a prime. In particular, if $m = p \in I$, then, by [2, pp. 271–274], we have $h(p)[a, b, c] = h(p)$ if and only if $[a, b, c] \not\equiv [0, 0, 0] \pmod p$. Together with part (iii) of Theorem 4.1 this yields the following proposition.

Proposition 4.4. *Let a, b, c be arbitrary integers and $(t_n)_{n=0}^{\infty}$ the generalized Tribonacci sequence beginnig with $t_0 = a, t_1 = b, t_2 = c$. If p is a prime, $p \in I$, $p \equiv 1 \pmod 3$ then* $h(p)[a, b, c] \,\big|\, \frac{p^2+p+1}{3}$.

References

[1] W. Adams and D. Shanks, *Strong primality tests that are not sufficient*, Math. Comp. **39** (1982), 255–300.
[2] J. Klaška, *Tribonacci modulo p^t*, Math. Bohemica, **133.3** (2008), 267–288.
[3] J. Klaška and L. Skula, *The cubic character of the Tribonacci roots*, The Fibonacci Quarterly, **48.1** (2010), 21–28.
[4] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer, New York, 1992.
[5] L. Stickelberger, *Über eine neue Eigenschaft der Diskriminanten algebraischer Zahlkörper*, Verhand. I. Internat. Math. Kongress (1897), 182–193.
[6] Z.-H. Sun, *Cubic and quartic congruences modulo a prime*, J. Number Theory, **102** (2003), 41–89.
[7] A. Vince, *Period of a linear recurrence*, Acta Arith., **39** (1981), 303–311.
[8] G. Voronoï, *Sur une propriété du discriminant des fonctions entières*, Verhand. III. Internat. Math. Kongress, (1905), 186–189.
[9] M. E. Waddill, *Some properties of a generalized Fibonacci sequence modulo m*, The Fibonacci Quarterly **16.4** (1978), 344–353.
[10] M. Ward, *The characteristic number of a sequence of integers satisfying a linear recursion relation*, Trans. Amer. Math. Soc., **33** (1931), 153–165.

MSC2010: 11B50, 11B39, 11A07

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

Institute of Mathematics, Faculty of Mechanical Engineering, Brno University of Technology, Technická 2, 616 69 Brno, Czech Republic
E-mail address: `skula@fme.vutbr.cz`