A NOTE ON THE CUBIC CHARACTERS OF TRIBONACCI ROOTS

JIŘÍ KLAŠKA AND LADISLAV SKULA

Abstract. In this paper we complete our preceding research concerning the cubic character of the roots of the Tribonacci polynomial $t(x) = x^3 - x^2 - x - 1$ over the Galois field $\mathbb{F}_p$ where p is an arbitrary prime, $p \equiv 1 \pmod 3$.

1. Introduction

Let τ be any root of the Tribonacci polynomial $t(x) = x^3 - x^2 - x - 1$ in the Galois field $\mathbb{F}_p$ where p is a prime, $p \equiv 1 \pmod 3$. In [1], we proved that

$$\tau^{\frac{p-1}{3}} = \left(\frac{\tau}{p}\right)_3 = 2^{\frac{2(p-1)}{3}}. \tag{1.1}$$

Next in [2], we showed that if $t(x)$ is irreducible over $\mathbb{F}_p$, $p \equiv 1 \pmod 3$ and τ is any root of $t(x)$ in the splitting field of $t(x)$ over $\mathbb{F}_p$, then

$$\tau^{\frac{p^2+p+1}{3}} = 1. \tag{1.2}$$

The number-theoretic results (1.1) and (1.2) were used in [2] to investigate the period $h(p)$ of the Tribonacci sequence $(T_n)_{n=0}^{\infty}$ reduced by a modulus p. Recall that $(T_n)_{n=0}^{\infty}$ is defined recursively by $T_{n+3} = T_{n+2} + T_{n+1} + T_n$ with $T_0 = T_1 = 0$, $T_2 = 1$ and that the period $h(p)$ of $(T_n \bmod p)_{n=0}^{\infty}$ is the least positive integer satisfying $T_{h(p)} \equiv T_{h(p)+1} \equiv 0 \pmod p$, $T_{h(p)+2} \equiv 1 \pmod p$. Let I be the set of all primes p for which $t(x)$ is irreducible over $\mathbb{F}_p$, Q 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 be the set of all primes for which $t(x)$ completely splits over $\mathbb{F}_p$ into linear factors. Furthermore, let $D = -2^2 \cdot 11$ be the discriminant of $t(x)$. By [1, Corollary 2.5], $p \in Q$ if and only if $\left(\frac{p}{11}\right) = -1$. Moreover, if $p \neq 2, 11$, then $p \in I \cup L$ if and only if $\left(\frac{p}{11}\right) = 1$. In [2], we established, for $p \equiv 1 \pmod 3$, the following properties of $h(p)$:

$$\begin{aligned} &\textit{If } p \in L, \textit{ then } h(p) \Big| \frac{p-1}{3} \textit{ if and only if } 2 \textit{ is a cubic residue of the field } \mathbb{F}_p. \\ &\textit{If } p \in Q, \textit{ then } h(p) \Big| \frac{p^2-1}{3} \textit{ if and only if } 2 \textit{ is a cubic residue of the field } \mathbb{F}_p. \\ &\textit{If } p \in I, \textit{ then } h(p) \Big| \frac{p^2+p+1}{3}. \end{aligned} \tag{1.3}$$

The second author was supported by the Ministry of Education, Youth and Sports of the Czech Republic, research plan MSM0021630518 “Simulation modeling of mechatronic systems”.

In the proofs of (1.1) – (1.3), which were presented in [1] and [2], a significant role is played by the cubic polynomials $f(x,c) = x^3 + A(c)x^2 + B(c)x + C(c) \in \mathbb{F}_p[x]$, $p \equiv 1 \pmod 3$ with

$$A(c) = -18c^2 + 3,\ B(c) = -9c^2 - 27c - 24,\ C(c) = 9c^2 - 27c + 28, \tag{1.4}$$

and $c \in \{-1, -\varepsilon, -\varepsilon^2\}$. Here, $\varepsilon \in \mathbb{F}_p$ denotes a primitive third root of unity so that $\varepsilon^2+\varepsilon+1 = 0$. Let D_c be the discriminant of $f(x,c)$. Then $D_c = 2^2 \cdot 3^9 \cdot 11$ for any $c \in \{-1, -\varepsilon, -\varepsilon^2\}$ and, by [1, Lemma 2.6], we have

$$\left(\frac{D_c}{p}\right) = \left(\frac{D}{p}\right) = \left(\frac{p}{11}\right). \tag{1.5}$$

Consequently, the Stickelberger parity theorem [1, Theorem 2.4] can be used to prove the following lemma:

Lemma 1.1. *Let p be an arbitrary prime, $p \equiv 1 \pmod 3$ such that $\left(\frac{p}{11}\right) = -1$. Then the Tribonacci polynomial $t(x)$ has exactly one root in the field $\mathbb{F}_p$ if and only if each of the polynomials $f(x,c)$, $c \in \{-1, -\varepsilon, -\varepsilon^2\}$ has exactly one root in $\mathbb{F}_p$.*

Since 2 is the root of $f(x,-1)$ in any Galois field $\mathbb{F}_p$, to find the further relations between the number of roots of $t(x)$ and $f(x,-1)$ is quite easy. The polynomial $f(x,-1)$ has three distinct roots in $\mathbb{F}_p$ if and only if $t(x)$ has no root or three distinct roots in $\mathbb{F}_p$. By means of the results derived in [1] and [2], these two cases may be distinguished as follows: The Tribonacci polynomial $t(x)$ has no root in $\mathbb{F}_p$ if and only if all three roots of $f(x,-1)$ belong to distinct cubic classes of $\mathbb{F}_p$. On the other hand, $t(x)$ has three distinct roots in $\mathbb{F}_p$ if and only if all three roots of $f(x,-1)$ belong to a single cubic class of $\mathbb{F}_p$.

In the present short note we complete what we know about the relations between the Tribonacci polynomial $t(x)$ and the polynomials $f(x,c)$, $c \in \{-\varepsilon, -\varepsilon^2\}$. In particular, we prove that in any Galois field $\mathbb{F}_p$ where $p \equiv 1 \pmod 3$, these polynomials have the same number of roots.

2. The Number of Roots of the Polynomials $t(x)$, $f(x,-\varepsilon)$, $f(x,-\varepsilon^2)$ Over the Galois Field $\mathbb{F}_p$ Where $p \equiv 1 \pmod 3$

For proof of our main result, we shall need the following two statements:

(i) Let p be a prime, $p \equiv 1 \pmod 3$ and let $g(x) = x^3 + rx + s \in \mathbb{F}_p[x]$, $r, s \neq 0$. Assume that there exists $\lambda \in \mathbb{F}_p$ such that $\lambda^2 = d$ where $d = \frac{s^2}{4} + \frac{r^3}{27}$. Further assume that $g(x)$ is irreducible over $\mathbb{F}_p$ or $g(x)$ has three distinct roots in $\mathbb{F}_p$. Then $g(x)$ is irreducible over $\mathbb{F}_p$ if and only if $A = -\frac{s}{2} + \lambda$ is not a cubic residue of $\mathbb{F}_p$.

(ii) For an arbitrary prime p, $p \equiv 1 \pmod 3$, there exists $\varkappa \in \mathbb{F}_p$ such that $\varkappa^2 = 33$. If $p \equiv 1 \pmod 3$ and $\left(\frac{p}{11}\right) = 1$, then $t(x)$ is irreducible over $\mathbb{F}_p$ if and only if $19 - 3\varkappa$ is not a cubic residue of $\mathbb{F}_p$.

Part (i) is a direct consequence of [2, Theorem 2.4]. For (ii), see [2, Theorem 2.5].

Theorem 2.1. *Let p be an arbitrary prime, $p \equiv 1 \pmod 3$ such that $\left(\frac{p}{11}\right) = 1$. Then the Tribonacci polynomial $t(x)$ is irreducible over the field $\mathbb{F}_p$ if and only if $f(x,-\varepsilon)$, $f(x,-\varepsilon^2)$ are irreducible over $\mathbb{F}_p$.*

Proof. After substituting $x = y - \frac{A(-\varepsilon)}{3}$, the polynomial $f(x,-\varepsilon)$ becomes a cubic polynomial $g(y) = y^3 + ry + s \in \mathbb{F}_p[y]$ with

$$r = \frac{1}{3}(3B(-\varepsilon) - A(-\varepsilon)^2) \ \text{ and } \ s = \frac{1}{27}(2A(-\varepsilon)^3 - 9A(-\varepsilon)B(-\varepsilon) + 27C(-\varepsilon)). \tag{2.1}$$

From (1.4), we obtain $A(-\varepsilon) = 18\varepsilon + 21$, $B(-\varepsilon) = 36\varepsilon - 15$, and $C(-\varepsilon) = 18\varepsilon + 19$. Substituting into (2.1) and using the identity $\varepsilon^2 + \varepsilon + 1 = 0$, r and s can be written in the form

$$r = -2 \cdot 3^3(2\varepsilon + 1), \quad s = 2 \cdot 3^3(6\varepsilon - 1). \tag{2.2}$$

We show that $r, s \neq 0$. Suppose $r = 0$. From (2.2) we have $2\varepsilon + 1 = 0$. This implies $9 = 0$, which yields a contradiction with $p \equiv 1 \pmod 3$. Next suppose $s = 0$. Then $6\varepsilon - 1 = 0$ and $215 = 5 \cdot 43 = 0$ follows. Since $5 \not\equiv 1 \pmod 3$ and $(\frac{43}{11}) = -1$, we have a contradiction.

By (ii), there exists $\varkappa \in \mathbb{F}_p$ such that $\varkappa^2 = 33$. Let $d = \frac{s^2}{4} + \frac{r^3}{27}$, $\mu = 2\varepsilon + 1$, $\nu = \frac{\varkappa}{\mu}$, $\lambda = 27\nu$, and $A = -\frac{s}{2} + \lambda$. Then $d = -3^6 \cdot 11$, $\lambda^2 = d$, and $A = (-3)^3(-4 + 3\mu - \nu)$.

It is evident that $f(x, -\varepsilon)$ and $g(y)$ have the same number of roots in $\mathbb{F}_p$. Hence, the assumption $\left(\frac{p}{11}\right) = 1$ implies that $g(y)$ is irreducible over $\mathbb{F}_p$ or has three distinct roots in $\mathbb{F}_p$. Moreover, according to (i),

$$g(y) \text{ is irreducible if and only if } -4 + 3\mu - \nu \text{ is not a cubic residue of } \mathbb{F}_p. \tag{2.3}$$

By direct calculation, we can verify that

$$(19 - 3\varkappa)(-4 + 3\mu - \nu) = (2 - \mu - \nu)^3. \tag{2.4}$$

By (ii), $t(x)$ is irreducible over $\mathbb{F}_p$ if and only if $19 - 3\varkappa$ is not a cubic residue of $\mathbb{F}_p$. From (2.4), it follows that $19 - 3\varkappa$ is not a cubic residue of $\mathbb{F}_p$ if and only if $-4 + 3\mu - \nu$ is not cubic residue of $\mathbb{F}_p$. Finally, using (2.3), we conclude that $g(y)$ and $f(x, -\varepsilon)$ are irreducible over $\mathbb{F}_p$. Since we can replace ε by ε^2, this is also true for $f(x, -\varepsilon^2)$. This completes the proof. □

Together with Lemma 1.1, Theorem 2.1 yields the desired result.

Theorem 2.2. *Let p be an arbitrary prime, $p \equiv 1 \pmod 3$. Then the polynomials $t(x)$, $f(x, -\varepsilon)$, $f(x, -\varepsilon^2)$ have the same number of roots over the field $\mathbb{F}_p$.*

References

[1] J. Klaška and L. Skula, *The cubic character of the tribonacci roots*, The Fibonacci Quarterly, **48.1** (2010), 21–28.

[2] J. Klaška and L. Skula, *Periods of the tribonacci sequence modulo a prime $p \equiv 1 \pmod 3$* (to appear).

MSC2010: 11B39, 11B50, 11D25

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