THE CUBIC CHARACTER OF THE TRIBONACCI ROOTS

JIŘÍ KLAŠKA AND LADISLAV SKULA

Abstract. If τ is 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, $p \equiv 1 \pmod 3$, then

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

More generally, if χ is a root of $t(x)$ in any field extension $\mathbb{G}$ of $\mathbb{F}_p$, then 2χ is a cubic residue of the field $\mathbb{G}$.

1. Introduction

The quadratic character of the root $\theta = (1+\sqrt{5})/2$ of the Fibonacci polynomial $f(x) = x^2 - x - 1$ was examined by E. Lehmer in [2]. The way we understand Lehmer's Theorem 1 in [2, p. 137], which was written in a different form, is as follows. Let p be a prime in the form $p = a^2 + b^2$ where $a, b \in \mathbb{Z}$ and $a \equiv 1 \pmod 4$. Furthermore, suppose that θ is a root of f in the Galois field $\mathbb{F}_p$; then we have

$$\theta^{\frac{p-1}{2}} = \left(\frac{\theta}{p}\right) = \begin{cases} 1 & \text{if } p = 20m+1, b \equiv 0 \pmod 5 \text{ or } p = 20m+9, a \equiv 0 \pmod 5 \\ -1 & \text{if } p = 20m+1, a \equiv 0 \pmod 5 \text{ or } p = 20m+9, b \equiv 0 \pmod 5. \end{cases}$$

In this paper we let τ be an arbitrary 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, $p \equiv 1 \pmod 3$. The purpose of our article is to prove the following identity for the cubic character of τ and 2 in $\mathbb{F}_p$:

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

Moreover, if χ is a root of $t(x)$ in any field extension $\mathbb{G}$ of $\mathbb{F}_p$, then we show that 2χ is a cubic residue of the field $\mathbb{G}$, i.e. there exists $\omega \in \mathbb{G}$ such that $2\chi = \omega^3$.

2. Preliminaries

Let $\mathbb{F}$ be a field in which there exists an element $\varepsilon \neq 1$ such that $\varepsilon^3 = 1$. Then char $\mathbb{F} \neq 3$ and $\varepsilon^2 + \varepsilon + 1 = 0$. For $a, b, c \in \mathbb{F}$, put

$$\begin{aligned} w_1(x) &= x^3 + ax^2 + bx + c, \\ w_2(x) &= w_1(\varepsilon x) = x^3 + \varepsilon^2 ax^2 + \varepsilon bx + c, \\ w_3(x) &= w_1(\varepsilon^2 x) = x^3 + \varepsilon ax^2 + \varepsilon^2 bx + c. \end{aligned}$$

By direct calculation we get the following lemma.

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

Lemma 2.1. $w_1(x)w_2(x)w_3(x) = x^9 + (a^3 - 3ab + 3c)x^6 + (b^3 - 3abc + 3c^2)x^3 + c^3$.

For $c \in \mathbb{F}$ put

$$\begin{aligned} A(c) &= -18c^2 + 3, \\ B(c) &= -9c^2 - 27c - 24, \\ C(c) &= 9c^2 - 27c + 28, \\ f(x, c) &= x^3 + A(c)x^2 + B(c)x + C(c) \in \mathbb{F}[x]. \end{aligned}$$

Clearly, $f(x - 1) = x^3 - 15x^2 - 6x + 64 = (x - 2)g(x)$, where $g(x) = x^2 - 13x - 32$.

Furthermore, we shall consider the following polynomials over the field $\mathbb{F}$:

$$t(x) = x^3 - x^2 - x - 1, \quad u(x) = t(x^3) = x^9 - x^6 - x^3 - 1.$$

The polynomial $t(x)$ is the well-known Tribonacci polynomial. Let $c \in \{-1, -\varepsilon, -\varepsilon^2\}$. Using the identities $c^3 = -1$, $c^4 = -c$, $c^6 = 1$ and $c^{-1} = -c^2$, we obtain the following lemma.

Lemma 2.2. *For any $c \in \{-1, -\varepsilon, -\varepsilon^2\}$, $b \in \mathbb{F}$, $b \neq 0$, we have*

$$\frac{(b^3 + 3c^2 + 1)^3}{27b^3c^3} - \frac{b^3{+}3c^2{+}1}{c} + 3c + 1 = -\frac{b^9 + A(c)b^6 + B(c)b^3 + C(c)}{27b^3} = -\frac{f(b^3, c)}{27b^3}.$$

Theorem 2.3. *Let* $\operatorname{char} \mathbb{F} \neq 2, 7$*. Then we have $u(x) = w_1(x)w_2(x)w_3(x)$ if and only if*

$$c \in \{-1, -\varepsilon, -\varepsilon^2\}, \quad f(b^3, c) = 0, \quad b \neq 0 \quad \textit{and} \quad a = \frac{b^3 + 3c^2 + 1}{3bc}. \tag{2.1}$$

Proof. Using Lemma 2.1 we have $u(x) = w_1(x)w_2(x)w_3(x)$ if and only if

$$\begin{aligned} a^3 - 3ab + 3c &= -1, \\ b^3 - 3abc + 3c^2 &= -1, \\ c^3 &= -1. \end{aligned} \tag{2.2}$$

First, assume that the identities (2.2) are valid. Then $c \in \{-1, -\varepsilon, -\varepsilon^2\}$. If $b = 0$, then from the second identity in (2.2) we get $3c^2 = -1$ and thus $27 = -1$, which is a contradiction with $\operatorname{char} \mathbb{F} \neq 2, 7$. Consequently, $b \neq 0$ and $a = (b^3 + 3c^2 + 1)/3bc$. Substituting into the first identity in (2.2), we have

$$\frac{(b^3 + 3c^2 + 1)^3}{27b^3c^3} - \frac{b^3 + 3c^2 + 1}{c} + 3c + 1 = 0.$$

Combining Lemma 2.2 with $c^3 = -1$, we obtain $f(b^3, c) = 0$ and (2.1) follows.

Conversely, let $c \in \{-1, -\varepsilon, -\varepsilon^2\}$, $f(b^3, c) = 0$, $b \neq 0$, and $a = (b^3 + 3c^2 + 1)/3bc$. Then $c^3 = -1$ and, from $a = (b^3{+}3c^2{+}1)/3bc$, we have $b^3 - 3abc + 3c^2 = -1$. Put $d = a^3 - 3ab + 3c$. Then by Lemma 2.2 we have

$$d = \frac{(b^3 + 3c^2 + 1)^3}{27b^3c^3} - \frac{b^3 + 3c^2 + 1}{c} + 3c = -\frac{f(b^3, c)}{27b^3} - 1 = -1$$

as required. □

Now we recall a well-known Stickelberger parity theorem [3] for the case of a cubic polynomial [5, p. 189]. See also Dickson's history [1, pp. 249–251] or consult [4, p. 42].

Theorem 2.4. *Let N be the number of solutions of $x^3 + Ax^2 + Bx + C \equiv 0 \pmod p$ where $A, B, C \in \mathbb{Z}$ and let*

$$D = A^2B^2 - 4B^3 - 4A^3C - 27C^2 + 18ABC \tag{2.3}$$

be the discriminant of the cubic polynomial $x^3 + Ax^2 + Bx + C$. If p is a prime, $p > 3$ and $p \nmid D$, we have:

$$\begin{aligned} &N = 1 \text{ if and only if } (D/p) = -1, \\ &N = 0 \text{ or } N = 3 \text{ if and only if } (D/p) = 1. \end{aligned} \tag{2.4}$$

Particularly, for the Tribonacci polynomial $t(x)$, we obtain the following corollary.

Corollary 2.5. *Let N be the number of distinct roots of the Tribonacci polynomial $t(x)$ in the field $\mathbb{F}_p$ where p is an arbitrary prime, $p \neq 2, 11$. Then $t(x)$ does not have multiple roots in $\mathbb{F}_p$, and we have:*

$$\begin{aligned} &N = 1 \text{ if and only if } (p/11) = -1, \\ &N = 0 \text{ or } N = 3 \text{ if and only if } (p/11) = 1. \end{aligned} \tag{2.5}$$

Proof. By (2.3), $D = -44 = -2^2 \cdot 11$. For $p = 3$, we have $(3/11) = 1$ and $N = 0$. Calculating the Legendre - Jacobi symbol, we get $(-44/p) = (p/11)$ and (2.5) follows from (2.4). □

Lemma 2.6. *For $c \in \{-1, -\varepsilon, -\varepsilon^2\}$, let D_c be the discriminant of $f(x, c)$. Then $D_c = 866052 = 2^2 \cdot 3^9 \cdot 11$ and $(D_c/p) = (p/11)$.*

Proof. For $c = -1$ we have $A(-1) = -15$, $B(-1) = -6$, $C(-1) = 64$ and, from (2.3), it follows that $D_{-1} = 866052$. For $c \in \{-\varepsilon, -\varepsilon^2\}$ we use the identity $c^2 - c + 1 = 0$ to determine D_c. From the quadratic reciprocity law and from further properties of the Legendre - Jacobi symbol it follows that

$$\begin{aligned} \left(\frac{866052}{p}\right) &= \left(\frac{3}{p}\right)\left(\frac{11}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)(-1)^{\frac{5(p-1)}{2}}\left(\frac{p}{11}\right) \\ &= (-1)^{3(p-1)}\left(\frac{1}{3}\right)\left(\frac{p}{11}\right) = \left(\frac{p}{11}\right). \end{aligned}$$

□

From now on, we will assume that p is an arbitrary prime such that $p \equiv 1 \pmod 3$ and $\mathbb{F}$ is an arbitrary finite field with characteristic p. Then there is an $n \in \mathbb{N}$ such that $\mathbb{F} = \mathbb{F}_{p^n}$. Let $\mathbb{F}^\times$ denote the multiplicative group of the field $\mathbb{F}$. This group is cyclic of order $p^n - 1$ and its generator will be denoted by g. For any $\xi \in \mathbb{F}^\times$, there is exactly one integer $\operatorname{ind} \xi$ such that $\xi = g^{\operatorname{ind} \xi}$ and $0 \leq \operatorname{ind} \xi \leq p^n - 2$. Clearly, for $\xi_1, \xi_2 \in \mathbb{F}^\times$, we have $\operatorname{ind} \xi_1\xi_2 \equiv \operatorname{ind} \xi_1 + \operatorname{ind} \xi_2 \pmod{p^n - 1}$. We can assume that $\varepsilon = g^{(p^n-1)/3}$. Then $\operatorname{ind} \varepsilon = (p^n - 1)/3$ and $\operatorname{ind} \varepsilon^2 = 2(p^n - 1)/3$. For $e \in \{0, 1, 2\}$ let

$$C_e = \{\xi \in \mathbb{F}^\times; \operatorname{ind} \xi \equiv e \pmod 3\} = \{\xi \in \mathbb{F}^\times; \xi = g^{3k+e}, k \in \mathbb{Z}, 0 \leq k < (p^n - 1)/3\}.$$

We will call the sets C_0, C_1, C_2 *the cubic classes of the field* $\mathbb{F}$. Clearly, $\{C_0, C_1, C_2\}$ is a partition of $\mathbb{F}^\times$. *For $\xi \in \mathbb{F}^\times$ we have $\xi \in C_0$ if and only if there exists $\omega \in \mathbb{F}^\times$ such that* $\omega^3 = \xi$. Let us call the elements $\xi's$ with this property *the cubic residues of the field* $\mathbb{F}$.

Lemma 2.7. *Let $\alpha, \beta, \gamma \in \mathbb{F}$ and $\alpha\beta\gamma \in C_0$. Then there exists $e \in \{0, 1, 2\}$ such that $\{\alpha, \beta, \gamma\} \subseteq C_e$ or α, β, γ belong to distinct cubic classes of the field $\mathbb{F}$.*

Proof. Suppose that there are $e_1, e_2 \in \{0,1,2\}$, $e_1 \neq e_2$ such that $\alpha, \beta \in C_{e_1}$, $\gamma \in C_{e_2}$. Then $\text{ind}\ \alpha\beta\gamma \equiv \text{ind}\ \alpha + \text{ind}\ \beta + \text{ind}\ \gamma \pmod{p^n - 1}$ and thus $\text{ind}\ \alpha\beta\gamma \equiv 2e_1 + e_2 \pmod 3$. On the other hand, we have $\text{ind}\ \alpha\beta\gamma \equiv 0 \pmod 3$, which implies $2e_1 + e_2 \equiv 0 \pmod 3$. Consequently, we have $e_1 = e_2$ and a contradiction follows. □

For the next theorem we need the following lemma which can be verified by direct computation.

Lemma 2.8. *The Tribonacci polynomial $t(x)$ has a unique root in $\mathbb{F}_7$ equal to 3. In the field $\mathbb{F}_{49}$, the polynomial $t(x)$ has three distinct roots $3, -1+5i, -1-5i$ where $i \in \mathbb{F}_{49}$, $i^2 = -1$. These roots belong to the same residue class of $\mathbb{F}_{49}$ and, for any $\chi \in \{3, -1+5i, -1-5i\}$, we have $(2\chi)^{(7^2-1)/3} = 1$. Consequently, if $t(x)$ has three distinct roots in an extension field $\mathbb{F}$ of $\mathbb{F}_7$, then $\mathbb{F}$ is an extension field of $\mathbb{F}_{49}$ and $3, -1+5i, -1-5i$ are roots of $t(x)$ in $\mathbb{F}$ belonging to the same cubic class of $\mathbb{F}$.*

Theorem 2.9. *Let $t(x)$ have three distinct roots $\alpha, \beta, \gamma \in \mathbb{F}$. Then*

(i) There is an $e_1 \in \{0,1,2\}$ such that $\{\alpha, \beta, \gamma\} \subseteq C_{e_1}$.

(ii) If $\text{char}\ \mathbb{F} \neq 7$, then, for each $c \in \{-1, -\varepsilon, -\varepsilon^2\}$, the polynomial $f(x,c)$ has three distinct roots in $\mathbb{F}$ belonging to the same cubic class C_{e_2} of $\mathbb{F}$ where $e_2 \in \{0,1,2\}$ and $e_1 + e_2 \equiv 0 \pmod 3$. In particular, for any $\tau \in \{\alpha, \beta, \gamma\}$, the element 2τ is a cubic residue of the field $\mathbb{F}$.

Proof. (i) For $p = 7$ the first part of the theorem follows from Lemma 2.8. Let $p \neq 7$. Suppose that for some $e \in \{0,1,2\}$ the inclusion $\{\alpha,\beta,\gamma\} \subseteq C_e$ is not valid. From the Viète equation $\alpha\beta\gamma = 1$ it follows that $\alpha\beta\gamma \in C_0$ and, by Lemma 2.7, the roots α, β, γ belong to distinct cubic classes of $\mathbb{F}$. We can assume that $\alpha \in C_0, \beta \in C_1, \gamma \in C_2$. Then there is $\xi_1 \in \mathbb{F}$ such that $\alpha = \xi_1^3$ and thus $t(x) = (x - \xi_1^3)(x-\beta)(x-\gamma)$. This implies that $\xi_1^3\beta\gamma = 1$.

Since $\beta \in C_1$, the polynomial $x^3 - \beta$ is irreducible over $\mathbb{F}$. Let K be the splitting field of $x^3 - \beta$ over $\mathbb{F}$. Then there is $\xi_2 \in K$ such that $\beta = \xi_2^3$ and $x^3 - \beta = (x-\xi_2)(x-\varepsilon\xi_2)(x-\varepsilon^2\xi_2)$. Let $\xi_3 = 1/(\xi_1\xi_2)$. As $\xi_1^3\beta\gamma = 1$, we have $\xi_3^3 = 1/(\xi_1^3\xi_2^3) = 1/(\xi_1^3\beta) = \gamma$ and thus $x^3 - \gamma = (x-\xi_3)(x-\varepsilon\xi_3)(x-\varepsilon^2\xi_3)$. Let $w_1(x) = (x-\xi_1)(x-\xi_2)(x-\xi_3)$, $w_2(x) = w_1(\varepsilon x) = (x-\varepsilon^2\xi_1)(x-\varepsilon^2\xi_2)(x-\varepsilon^2\xi_3)$, $w_3(x) = w_1(\varepsilon^2 x) = (x-\varepsilon\xi_1)(x-\varepsilon\xi_2)(x-\varepsilon\xi_3)$. In K we have $t(x) = (x-\xi_1^3)(x-\xi_2^3)(x-\xi_3^3)$. Hence $u(x) = w_1(x)w_2(x)w_3(x)$. Let $a = -\xi_1 - \xi_2 - \xi_3$, $b = \xi_1\xi_2 + \xi_1\xi_3 + \xi_2\xi_3$. Then $w_1(x) = x^3 + ax^2 + bx - 1$, $w_2(x) = x^3 + \varepsilon^2 ax^2 + \varepsilon bx - 1$, $w_3(x) = x^3 + \varepsilon ax^2 + \varepsilon^2 bx - 1$. Using Theorem 2.3 we get $b \neq 0$ and $f(b^3, -1) = 0$. After a short calculation we obtain

$$b^3 = \xi_1^3\xi_2^3 + \xi_1^3\xi_3^3 + \xi_2^3\xi_3^3 + 3(\xi_1^3\xi_2^2\xi_3 + \xi_1^3\xi_2\xi_3^2 + \xi_1^2\xi_2^3\xi_3 + \xi_1\xi_2^3\xi_3^2 + \xi_1^2\xi_2\xi_3^3 + \xi_1\xi_2^2\xi_3^3) + 6\xi_1^2\xi_2^2\xi_3^2.$$

Let $u = \xi_1^3\xi_2^3 + \xi_1^3\xi_3^3 + \xi_2^3\xi_3^3 + 6\xi_1^2\xi_2^2\xi_3^2$, $v = \xi_1^3\xi_2^2\xi_3 + \xi_1^3\xi_2\xi_3^2 + \xi_1^2\xi_2^3\xi_3 + \xi_1\xi_2^3\xi_3^2 + \xi_1^2\xi_2\xi_3^3 + \xi_1\xi_2^2\xi_3^3$. Then $b^3 = u + 3v$ and, for u, we have $u = \alpha\beta + \alpha\gamma + \beta\gamma + 6 = 5$. Clearly, $\xi_3 = \xi_2^2/(\xi_1\beta)$ and $\xi_3^2 = \xi_2/(\xi_1^2\beta)$. This implies that

$$v = \frac{\xi_1^3\xi_2^4}{\xi_1\beta} + \frac{\xi_1^3\xi_2^2}{\xi_1^2\beta} + \frac{\xi_1^2\beta\xi_2^2}{\xi_1\beta} + \frac{\xi_1\beta\xi_2}{\xi_1^2\beta} + \xi_1^2\xi_2\gamma + \xi_1\xi_2^2\gamma = \xi_2^2\left(\frac{\xi_1}{\beta} + \xi_1 + \xi_1\gamma\right) + \xi_2\left(\xi_1^2 + \frac{1}{\xi_1} + \xi_1^2\gamma\right).$$

Let $r = \xi_1/\beta + \xi_1 + \xi_1\gamma$, $s = \xi_1^2 + 1/\xi_1 + \xi_1^2\gamma$. Then $r, s \in \mathbb{F}$ and $b^3 = 3r\xi_2^2 + 3s\xi_2 + 5$. Since for $b^3 \neq 2$, we have $g(b^3) = 0$ and $[K : \mathbb{F}] = 3$, we obtain $b^3 \in \mathbb{F}$. Clearly, the elements $1, \xi_2, \xi_2^2 \in K$ are linear independent over $\mathbb{F}$ and thus we have $r = s = 5 - b^3 = 0$. Hence $b^3 = 5$. Consequently, $5 \equiv 2 \pmod p$ or 5 is a root of $g(x)$ in $\mathbb{F}$. As $g(5) = -2^3 \cdot 3^2 = 0$, we have a contradiction with $\text{char}\ \mathbb{F} \neq 2, 3$. This proves part (i).

(ii) According to (i) there exists $e_1 \in \{0,1,2\}$ such that $\{\alpha,\beta,\gamma\} \subseteq C_{e_1}$. Therefore, there exist $\omega_1, \omega_2 \in \mathbb{F}$ with the property $\beta = \alpha\omega_1^3$, $\gamma = \alpha\omega_2^3$ and $1 \neq \omega_1^3 \neq \omega_2^3 \neq 1$. Let $c \in \{-1,-\varepsilon,-\varepsilon^2\}$. Since $1 = \alpha\beta\gamma = \alpha^3\omega_1^3\omega_2^3$, we can choose the element ω_1 such that $\alpha\omega_1\omega_2 = -c$. Let K be the splitting field of $x^3-\alpha$ and let $\xi \in K$ such that $\xi^3 = \alpha$. Then $\xi^3\omega_1\omega_2 = -c$. Set $H_1 = \omega_1+\omega_2+\omega_1\omega_2$, $H_2 = \omega_1+\varepsilon\omega_2+\varepsilon^2\omega_1\omega_2$, $H_3 = \omega_1+\varepsilon^2\omega_2+\varepsilon\omega_1\omega_2$. Using $1 \neq \omega_1^3 \neq \omega_2^3 \neq 1$, we can prove $H_1^3 \neq H_2^3 \neq H_3^3 \neq H_1^3$. Furthermore, set

$$w_{11}(x) = (x-\xi)(x-\xi\omega_1)(x-\xi\omega_2) = x^3+a_1x^2+b_1x+c,$$

$$w_{21}(x) = (x-\varepsilon\xi)(x-\varepsilon^2\xi\omega_1)(x-\xi\omega_2) = x^3+a_2x^2+b_2x+c,$$

$$w_{31}(x) = (x-\varepsilon^2\xi)(x-\varepsilon\xi\omega_1)(x-\xi\omega_2) = x^3+a_3x^2+b_3x+c,$$

and, for $i \in \{1,2,3\}$, set $w_{i2}(x) = w_{i1}(\varepsilon x)$, $w_{i3}(x) = w_{i1}(\varepsilon^2 x)$. Then $b_i = \xi^2 H_i$, $i \in \{1,2,3\}$. Since $\varepsilon^j\xi$, $\varepsilon^j\xi\omega_1$, $\varepsilon^j\xi\omega_2$, $j \in \{0,1,2\}$ are distinct roots of $u(x)$, we have $u(x) = w_{i1}(x)w_{i2}(x)w_{i3}(x)$ for each $i \in \{1,2,3\}$. Theorem 2.3 then implies $f(b_i^3, c) = 0$, $b_i \neq 0$. Thus, b_i^3, $i \in \{1,2,3\}$ are distinct roots of $f(x,c)$. Since $b_i^3\alpha = \xi^6 H_i^3\alpha = (\alpha H_i)^3$, $i \in \{1,2,3\}$, there exists $e_2 \in \{0,1,2\}$ such that $b_i \in C_{e_2}$ for each $i \in \{1,2,3\}$ and $e_1+e_2 \equiv 0 \pmod 3$. The theorem is proved. □

Remark 2.10. *The second part of the proof of Theorem 2.9 gives explicit formulas for the roots of the polynomial $f(x,c)$, namely $\alpha^2H_1^3$, $\alpha^2H_2^3$, $\alpha^2H_3^3$.*

3. The Cubic Character of the Tribonacci Roots

Let $t(x)$ be irreducible over $\mathbb{F}_p$ and $p \equiv 1 \pmod 3$. Let K be the splitting field of $t(x)$ over $\mathbb{F}_p$. Then $[K:\mathbb{F}_p] = 3$ and the multiplicative group $K^\times$ of the field K is of order $p^3-1 = (p-1)(p^2+p+1)$. We denote the generator of $K^\times$ by g. Let $\alpha,\beta,\gamma \in K$ satisfy $t(x) = (x-\alpha)(x-\beta)(x-\gamma)$. With respect to the automorphism $\xi \to \xi^p$ of the field K, we can assume that $\beta = \alpha^p$, $\gamma = \alpha^{p^2}$. Consequently, the roots α,β,γ are distinct. Let $\alpha = g^u$ where $u \in \mathbb{Z}$, $0 < u < p^3-1$. Then $1 = \alpha^{1+p+p^2} = g^{u(1+p+p^2)}$ and thus $u(1+p+p^2) \equiv 0 \pmod{p^3-1}$. This implies $p-1|u$ and thus there is a $k \in \mathbb{Z}$, $1 \leq k < p^2+p+1$ such that $u = k(p-1)$. We get $\alpha = g^{k(p-1)}$ and ind $\alpha = k(p-1)$ in K. Let

$$\xi_\alpha = g^{\frac{k(p-1)}{3}},\ \xi_\beta = \xi_\alpha^p = g^{\frac{kp(p-1)}{3}},\ \xi_\gamma = \xi_\beta^p = \xi_\alpha^{p^2} = g^{\frac{kp^2(p-1)}{3}}.$$

Then $\xi_\alpha,\xi_\beta,\xi_\gamma \in K^\times$, $\xi_\alpha^3 = \alpha$, $\xi_\beta^3 = \beta$, $\xi_\gamma^3 = \gamma$ and $(\xi_\alpha\xi_\beta\xi_\gamma)^3 = 1$. This implies that $\xi_\alpha\xi_\beta\xi_\gamma \in \{1,\varepsilon,\varepsilon^2\}$. Further, let $c(p) = -\xi_\alpha\xi_\beta\xi_\gamma = -\xi_\alpha^{1+p+p^2} \in \{-1,-\varepsilon,-\varepsilon^2\}$. It can be shown that $c(p)$ depends only on the prime p. By investigating the relation $C(c) = 0$ for $c \in \{-1,-\varepsilon,-\varepsilon^2\}$, we get the following lemma.

Lemma 3.1. *If $f(0,c) = 0$ for an element $c \in \{-1,-\varepsilon,-\varepsilon^2\}$ of $\mathbb{F}$, then* char $\mathbb{F} = 2$ *or* 7.

Theorem 3.2. *Let $t(x)$ be irreducible over $\mathbb{F}_p$. Then $f(x,c(p))$ has three distinct roots in $\mathbb{F}_p$ belonging to distinct cubic classes of the field $\mathbb{F}_p$.*

Proof. Let $w_1(x) = (x-\xi_\alpha)(x-\xi_\beta)(x-\xi_\gamma) = x^3+ax^2+bx+c$ where $a = -\xi_\alpha-\xi_\beta-\xi_\gamma$, $b = \xi_\alpha\xi_\beta+\xi_\alpha\xi_\gamma+\xi_\beta\xi_\gamma$, $c = c(p) = -\xi_\alpha\xi_\beta\xi_\gamma$. Since $a^p = a$, $b^p = b$, we have $a,b,c \in \mathbb{F}_p$ and $w_1(x), w_2(x), w_3(x) \in \mathbb{F}_p[x]$ where $w_2(x) = w_1(\varepsilon x)$ and $w_3(x) = w_1(\varepsilon^2 x)$. Furthermore, we have $w_2(x) = (x-\varepsilon^2\xi_\alpha)(x-\varepsilon^2\xi_\beta)(x-\varepsilon^2\xi_\gamma)$ and $w_3(x) = (x-\varepsilon\xi_\alpha)(x-\varepsilon\xi_\beta)(x-\varepsilon\xi_\gamma)$. Clearly, $\varepsilon^i\xi_\alpha$, $\varepsilon^i\xi_\beta$, $\varepsilon^i\xi_\gamma$, $i \in \{0,1,2\}$ are the distinct roots of $u(x)$ and $u(x) = w_1(x)w_2(x)w_3(x)$. By Theorem 2.3 we have $b \neq 0$ and $f(b^3, c(p)) = 0$. From Theorem 2.4 and Lemma 2.6 it follows that there exist $\rho, \sigma \in \mathbb{F}_p$ such that $\rho \neq b^3 \neq \sigma \neq \rho$, $f(\rho, c(p)) = f(\sigma, c(p)) = 0$. Suppose that there is $b' \in \mathbb{F}_p$, $b'^3 = \rho$. Let $w_1'(x) = x^3 + a'x^2 + b'x + c$, $c = c(p)$, where $a' = (b'^3 + 3c^2 + 1)/3b'c$, $w_2'(x) = w_1'(\varepsilon x)$, $w_3'(x) = w_1'(\varepsilon^2 x)$. By Theorem 2.3 we have $u(x) = w_1'(x)w_2'(x)w_3'(x)$. Since $b^3 \neq \rho = b'^3$, we have $\{w_1(x), w_2(x), w_3(x)\} \cap \{w_1'(x), w_2'(x), w_3'(x)\} = \emptyset$. Consequently, there exists $\tau \in \mathbb{F}_p$ such that $u(\tau) = 0$. Hence τ^3 is a root of $t(x)$ which is a contradiction. Therefore exactly one root of $f(x, c(p))$ is a cubic residue of $\mathbb{F}_p$. Since $C(-1) = 4^3$, $C(-\varepsilon) = 18\varepsilon + 19 = (\varepsilon + 3)^3$ and $C(-\varepsilon^2) = 18\varepsilon^2 + 19 = (\varepsilon^2 + 3)^3$, we get, using Lemma 2.7, that the roots of $f(x, c(p))$ belong to distinct cubic classes of $\mathbb{F}_p$. □

Lemma 3.3. *Let $t(x)$ be irreducible over $\mathbb{F}_p$, $c_1, c_2 \in \{-1, -\varepsilon, -\varepsilon^2\}$ and $b_1, b_2 \in \mathbb{F}_p$. If $f(b_1^3, c_1) = f(b_2^3, c_2) = 0$, then $c_1 = c_2$.*

Proof. For $i \in \{1, 2\}$, let $w_{i1}(x) = x^3 + a_i x^2 + b_i x + c_i$ where $a_i = (b_i^3 + 3c_i^2 + 1)/3b_i c_i$. Further, let $w_{i2}(x) = w_{i1}(\varepsilon x)$, $w_{i3}(x) = w_{i1}(\varepsilon^2 x)$. Then, by Theorem 2.3, we have $u(x) = w_{i1}(x)w_{i2}(x)w_{i3}(x)$, $i \in \{1, 2\}$. If $c_1 \neq c_2$, then $\{w_{11}(x), w_{12}(x), w_{13}(x)\} \cap \{w_{21}(x), w_{22}(x), w_{23}(x)\} = \emptyset$, and thus there is $\tau \in \mathbb{F}_p$ such that $u(\tau) = 0$. Since τ^3 is a root of $t(x)$ in $\mathbb{F}_p$, a contradiction follows. □

Theorem 3.4. *Let $c \in \{-1, -\varepsilon, -\varepsilon^2\}$ and let $f(x, c)$ have three distinct roots in $\mathbb{F}_p$ belonging to distinct cubic classes of $\mathbb{F}_p$. Then $t(x)$ is irreducible over $\mathbb{F}_p$ and $c = c(p)$.*

Proof. Let ρ be the root of $f(x, c)$ in $\mathbb{F}_p$ such that $\rho \in C_0$. Then there is $b \in \mathbb{F}_p$ such that $b^3 = \rho$. Let $a = (b^3 + 3c^2 + 1)/3bc$, $w_1(x) = x^3 + ax^2 + bx + c$, $w_2(x) = w_1(\varepsilon x)$, $w_3(x) = w_1(\varepsilon^2 x)$. By Theorem 2.3 we have $u(x) = w_1(x)w_2(x)w_3(x)$.

Suppose that $t(x)$ is not irreducible over $\mathbb{F}_p$. Since $f(x, c)$ has three distinct roots in $\mathbb{F}_p$, then by Theorem 2.4 and Lemma 2.6, we have $(p/11) = 1$. By (2.5), there are distinct elements $\tau_1, \tau_2, \tau_3 \in \mathbb{F}_p$ such that $t(x) = (x - \tau_1)(x - \tau_2)(x - \tau_3)$ and thus $u(x) = (x^3 - \tau_1)(x^3 - \tau_2)(x^3 - \tau_3)$. For any $i \in \{1, 2, 3\}$, there is $k = k(i) \in \{1, 2, 3\}$ such that $1 \leq \deg(\gcd(x^3 - \tau_i, w_k(x))) \leq 2$. Thus there is $\xi_i \in \mathbb{F}_p$ which is the root of $x^3 - \tau_i$. Since $\varepsilon\xi_1$, $\varepsilon^2\xi_i$ are also the roots of $x^3 - \tau_i$, we have $x^3 - \tau_i = (x - \xi_i)(x - \varepsilon\xi_i)(x - \varepsilon^2\xi_i)$ for $i \in \{1, 2, 3\}$. This implies that $u(x)$ completely splits over $\mathbb{F}_p$ into the product of the linear terms $x - \varepsilon^i\xi_j$, $i \in \{0, 1, 2\}$, $j \in \{1, 2, 3\}$. We can assume

$$w_1(x) = (x - \xi_1)(x - \xi_2)(x - \xi_3),$$
$$w_2(x) = w_1(\varepsilon x) = (x - \varepsilon^2\xi_1)(x - \varepsilon^2\xi_2)(x - \varepsilon^2\xi_3),$$
$$w_3(x) = w_1(\varepsilon^2 x) = (x - \varepsilon\xi_1)(x - \varepsilon\xi_2)(x - \varepsilon\xi_3).$$

It follows that $b = \xi_1\xi_2 + \xi_1\xi_3 + \xi_2\xi_3$ and $c = -\xi_1\xi_2\xi_3$. Let

$$\overline{w}_1(x) = (x - \varepsilon\xi_1)(x - \varepsilon^2\xi_2)(x - \xi_3),$$
$$\overline{w}_2(x) = \overline{w}_1(\varepsilon x) = (x - \xi_1)(x - \varepsilon\xi_2)(x - \varepsilon^2\xi_3),$$
$$\overline{w}_3(x) = \overline{w}_1(\varepsilon^2 x) = (x - \varepsilon^2\xi_1)(x - \xi_2)(x - \varepsilon\xi_3).$$

Letting $\overline{a} = -\varepsilon\xi_1 - \varepsilon^2\xi_2 - \xi_3$ and $\overline{b} = \xi_1\xi_2 + \varepsilon\xi_1\xi_3 + \varepsilon^2\xi_2\xi_3$, we get $\overline{w}_1(x) = x^3 + \overline{a}x^2 + \overline{b}x + c$. Since $u(x) = \overline{w}_1(x)\overline{w}_2(x)\overline{w}_3(x)$, it follows from Theorem 2.3 that $f(\overline{b}^3, c) = 0$.

We prove that $b \notin \{\overline{b}, \varepsilon\overline{b}, \varepsilon^2\overline{b}\}$. Suppose that $b = \overline{b}$. Then $\xi_1\xi_2 + \xi_1\xi_3 + \xi_2\xi_3 = \xi_1\xi_2 + \varepsilon\xi_1\xi_3 + \varepsilon^2\xi_2\xi_3$ and thus $\xi_2\xi_3(\varepsilon^2 - 1) + \xi_1\xi_3(\varepsilon - 1) = 0$. Hence $\xi_2(\varepsilon + 1) = -\xi_1$. Since $(\varepsilon + 1)^3 = -1$ we have $\tau_2 = \xi_2^3 = \xi_1^3 = \tau_1$, which is a contradiction. Similarly we can prove that $b \neq \varepsilon\overline{b}$ and $b \neq \varepsilon^2\overline{b}$. Hence $b \notin \{\overline{b}, \varepsilon\overline{b}, \varepsilon^2\overline{b}\}$, and thus $b^3 \neq \overline{b}^3$. Consequently, the roots $b^3, \overline{b}^3$ of $f(x, c)$

belong to the same cubic class and a contradiction follows. Thus $t(x)$ is irreducible over $\mathbb{F}_p$. From Theorem 3.2 we get that $f(x, c(p))$ has a root b_1^3 where $b_1 \in \mathbb{F}_p$ and Lemma 3.3 implies $c = c(p)$. □

Theorem 3.5. *Let $t(x)$ have exactly one root τ in the field $\mathbb{F}_p$ and $p \neq 7$. Then, for any $c \in \{-1, -\varepsilon, -\varepsilon^2\}$, there exists the unique $\rho = \rho(c) \in \mathbb{F}_p$ such that $f(\rho, c) = 0$. Furthermore, $\rho\tau$ is a cubic residue of the field $\mathbb{F}_p$.*

Proof. According to Corollary 2.5 we have $(p/11) = -1$. Let $\mathbb{F} = \mathbb{F}_{p^2}$. Then $t(x)$ has three distinct roots $\tau, \alpha, \beta \in \mathbb{F}$ and $t(x) = (x-\tau)(x-\alpha)(x-\beta)$. Let $c \in \{-1, -\varepsilon, -\varepsilon^2\}$. Using Theorem 2.9, we get that τ, α, β belong to the same cubic class C_{e_1} of the field $\mathbb{F}$ and $f(x, c)$ has three distinct roots in $\mathbb{F}$ which belong to the same cubic class C_{e_2}, $e_2 \in \{0, 1, 2\}$ of $\mathbb{F}$ and $e_1 + e_2 \equiv 0 \pmod 3$.

Using Theorem 2.4 and Lemma 2.6, we get that there exists exactly one element $\rho = \rho(c) \in \mathbb{F}_p$ such that $f(\rho, c) = 0$. Since $\tau \in C_{e_1}$ and $\rho \in C_{e_2}$, there exists $\omega \in \mathbb{F} = \mathbb{F}_{p^2}$ such that $\rho\tau = \omega^3$. The element $\rho\tau$ belongs to $\mathbb{F}_p$ and $[\mathbb{F} : \mathbb{F}_p] = 2$, thus $\omega \in \mathbb{F}_p$ and the result follows. □

The case $p = 7$ will be investigated separately. The polynomial $t(x)$ has only one root $\tau = 3$ in the field $\mathbb{F}_7$. The set $\{-1, -\varepsilon, -\varepsilon^2\} = \{3, 5, 6\}$ and the polynomials $f(x, c)$, $c = 3, 5, 6$ have the following roots in $\mathbb{F}_7$:

c	$\rho = \rho(c)$	$\rho^{(p-1)/3} = \rho^2$	$(\rho\tau)^{(p-1)/3} = (\rho\tau)^2$
3	0	0	0
5	5	4	1
6	2	4	1

where $\rho = \rho(c)$ is the only root of $f(x, c)$ in $\mathbb{F}_7$. Therefore, we can state the following proposition.

Proposition 3.6. *Let $p = 7$. Then the Tribonacci polynomial $t(x)$ has a unique root $\tau = 3$ in $\mathbb{F}_7$ and, for $c \in \{-1, -\varepsilon, -\varepsilon^2\} - \{3\}$, there exists a unique $\rho = \rho(c) \in \mathbb{F}_7$ with $f(\rho, c) = 0$ and $\rho\tau$ is a cubic residue in $\mathbb{F}_7$.*

Combining Theorem 3.5 with Proposition 3.6, we obtain the following theorem.

Theorem 3.7. *Let $t(x)$ have a unique root τ in the field $\mathbb{F}_p$. Then 2τ belongs to the cubic class C_0 of $\mathbb{F}_p$ and therefore*

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

Using Theorem 2.9 we get the following theorem.

Theorem 3.8. *Let $t(x)$ have three distinct roots $\alpha, \beta, \gamma \in \mathbb{F}_p$. Then there exists $e_1 \in \{0, 1, 2\}$ such that $\{\alpha, \beta, \gamma\} \subseteq C_{e_1}$ and any polynomial $f(x, c)$, $c \in \{-1, -\varepsilon, -\varepsilon^2\}$ has three distinct roots in $\mathbb{F}_p$ which belong to the same cubic class C_{e_2} of $\mathbb{F}_p$ where $e_2 \in \{0, 1, 2\}$ and $e_1 + e_2 \equiv 0 \pmod 3$. In particular, for any $\tau \in \{\alpha, \beta, \gamma\}$, the element 2τ belongs to the cubic class C_0 of $\mathbb{F}_p$ and thus*

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

4. Conclusion

In conclusion, we prove a theorem on the relation between the roots of $t(x)$ and the number 2 in any extension of the field $\mathbb{F}_p$.

Theorem 4.1. *Let $\mathbb{G}$ be an arbitrary extension of the field $\mathbb{F}_p$ and $\chi \in \mathbb{G}$ be a root of $t(x)$ in $\mathbb{G}$. Then there exists $\omega \in \mathbb{G}$ such that $2\chi = \omega^3$.*

Proof. We will discuss three cases. (i) Let $t(x)$ be irreducible over $\mathbb{F}_p$. Then $t(x)$ has three distinct roots α, β, γ in the splitting field K over $\mathbb{F}_p$. Thus $K \subseteq \mathbb{G}$ and $\chi \in \{\alpha, \beta, \gamma\}$. Using Theorem 2.9, we see that 2χ is a cubic residue of the field K and the result follows.

(ii) Let $t(x)$ have the unique root τ in the field $\mathbb{F}_p$. By Theorem 3.7, the element 2τ is a cubic residue of the field $\mathbb{F}_p \subseteq \mathbb{G}$. Thus, for $\chi = \tau$, the theorem is valid. If $\chi \neq \tau$, then $\chi \in \mathbb{F}_{p^2}$. Since $\mathbb{F}_{p^2} \subseteq \mathbb{G}$, we obtain the result from Theorem 2.9 provided that $p \neq 7$. For $p = 7$, we get the assertion from Lemma 2.8.

(iii) Let $t(x)$ have three distinct roots in $\mathbb{F}_p$. According to Theorem 3.8, the element 2χ is a cubic residue of the field $\mathbb{F}_p$ and hence $2\chi = \omega^3$ for an element $\omega \in \mathbb{F}_p \subseteq \mathbb{G}$. The proof is complete. □

References

[1] L. E. Dickson, *History of the Theory of Numbers*, Vol. I, Chelsea, New York, 1952.

[2] E. Lehmer, *On the quadratic character of the Fibonacci root*, The Fibonacci Quarterly, **4.2** (1966), 135–138.

[3] L. Stickelberger, *Über eine neue Eigenschaft der Diskriminanten algebraischer Zahlkörper*, Verhand. I. Internat. Math. Kongress, (1897), 182–193.

[4] Z.-H. Sun, *Cubic and quartic congruences modulo a prime*, Journal of Number Theory, **102**, (2003), 41–89.

[5] G. Voronoï, *Sur une propriété du discriminant des fonctions entirès*, Verhand. III. Internat. Math. Kongress, (1905), 186–189.

MSC2000: 11B39, 11A15

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