# MORDELL'S EQUATION AND THE TRIBONACCI FAMILY

JIŘÍ KLAŠKA AND LADISLAV SKULA

Abstract. We define a Tribonacci family as the set $T$ of all cubic polynomials $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$ having the same discriminant as the Tribonacci polynomial $t(x) = x^3 - x^2 - x - 1$. Using integral solutions of Mordell's equation $Y^2 = X^3 + 297$, we establish explicit forms of all polynomials in $T$. As the main result we prove that all polynomials in $T$ have the same type of factorization over any Galois field $\mathbb{F}_p$ where $p$ is a prime.

## 1. Introduction

Mordell's equation

$$Y^2 = X^3 + k,\ 0 \neq k \in \mathbb{Z}, \tag{1.1}$$

has had a long and interesting history. A synopsis of the first discoveries concerning (1.1) is given in Dickson [1, pp. 533–539]. See also [6, pp. 1–5]. In 1909, A. Thue [9] showed that (1.1) has only a finite number of solutions in integers $X, Y$. Various methods for finding the integral solutions of (1.1) are known [3, 6, 7]. Extensive lists of further references related to (1.1) can be found in [3] and [6].

In this paper we show an interesting application of integral solutions of (1.1) with $k = 297$ to the theory of factorizations of the cubic polynomials $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$ with a discriminant $D_f = -44$ over a Galois field $\mathbb{F}_p$ where $p$ is a prime. In particular, we prove that the set

$$T = \{f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]; D_f = -44\}$$

contains infinitely many polynomials, which can be partitioned into eight pairwise disjoint classes such that the polynomials of each class are given by a simple formula that depends on some integral solution of $Y^2 = X^3 + 297$. Since the Tribonacci polynomial $t(x) = x^3 - x^2 - x - 1$ belongs to $T$, we call $T$ the Tribonacci family. As the main result we prove that, over any Galois field $\mathbb{F}_p$ where $p$ is a prime, all polynomials in $T$ have the same type of factorization and, consequently, the same number of roots in $\mathbb{F}_p$. We do this by combining the Stickelberger Parity Theorem [8] for the case of a cubic polynomial [10], a modification of the results presented in [5, pp. 229–230], and the relations between the cubic characters of certain elements of the field $\mathbb{F}_{p^2}$ corresponding to integral solutions of $Y^2 = X^3 + 297$. In general, we show that, for any $D \in \mathbb{Z}$, the set

$$C = \{f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]; D_f = D\}$$

can be obtained by means of integral solutions of Mordell's equation $Y^2 = X^3 - 432D$. This fact opens an interesting question, namely, for which $D \in \mathbb{Z}$ can our main result be generalized.

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".

## 2. Connection Between Mordel's Equation $Y^2 = X^3 - 432D$ and Cubic Polynomials with Discriminant $D$

Let $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Q}[x]$ and let $D_f = a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc$ be the discriminant of $f(x)$. Let $g_f(x) = f(x - a/3)$. Then $D_{g_f} = D_f$ and $g_f(x) = x^3 + rx + s \in \mathbb{Q}[x]$ where

$$r = b - \frac{a^2}{3} \quad \text{and} \quad s = \frac{2a^3}{27} - \frac{ab}{3} + c. \tag{2.1}$$

Next, let

$$d_f = \frac{r^3}{27} + \frac{s^2}{4}. \tag{2.2}$$

Then $D_f = -108d_f$ and $d_f = d_{g_f}$. If $f(x) \in \mathbb{Z}[x]$, then (2.1) implies

$$r, s \in \mathbb{Z} \iff 3|a. \tag{2.3}$$

On the other hand, for $f(x) \in \mathbb{Z}[x]$,

$$3 \nmid a \iff \text{there exists } \ u, v \in \mathbb{Z} : r = \frac{u}{3},\ s = \frac{v}{27},\ 3 \nmid uv. \tag{2.4}$$

Moreover, by (2.1), we obtain

$$u = 3b - a^2 \text{ and } v = 2a^3 - 9ab + 27c. \tag{2.5}$$

For $e \in \{0, 1, 2\}$, let $\mathbb{D}_e$ denote the set of all $d \in \mathbb{Q}$ for which there exists $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$ such that $a \equiv e \pmod 3$ and $d_f = d$. Some basic properties of $\mathbb{D}_e$ will be established in the following lemma.

**Lemma 2.1.** *For $\mathbb{D}_0$, $\mathbb{D}_1$ and $\mathbb{D}_2$ we have*

$$\mathbb{D}_0 = \left\{ d \in \mathbb{Q};\ d = \frac{4u^3 + 27v^2}{108}, u, v \in \mathbb{Z} \right\} \tag{2.6}$$

*and*

$$\mathbb{D}_1 = \mathbb{D}_2 = \left\{ d \in \mathbb{Q}; d = \frac{4u^3 + v^2}{2916}, u, v \in \mathbb{Z}, u \equiv 2 \pmod 3, 3u + v + 1 \equiv 0 \pmod{27} \right\}. \tag{2.7}$$

*Proof.* (i) Let $d \in \mathbb{D}_0$. Then there exists $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$ such that $3|a$ and $d_f = d$. By (2.3), $g_f(x) = x^3 + rx + s \in \mathbb{Z}[x]$. Let $u = r$, $v = s$. Then $u, v \in \mathbb{Z}$ and, by (2.2), $d = d_f = (4u^3 + 27v^2)/108$. Conversely, assume that $d = (4u^3 + 27v^2)/108$ where $u, v \in \mathbb{Z}$. For any $w \in \mathbb{Z}$, let

$$a = 3w,\ b = 3w^2 + u,\ c = w^3 + uw + v. \tag{2.8}$$

Then $f(x) = x^3+ax^2+bx+c \in \mathbb{Z}[x]$, $3|a$, and $g_f(x) = x^3+rx+s \in \mathbb{Z}[x]$. Substituting (2.8) into (2.1), we obtain $r = u$ and $s = v$, which together with (2.2) yields $d = d_f = (4u^3 + 27v^2)/108$. This proves (2.6).

(ii) Let $e \in \{1, 2\}$. First show

$$\mathbb{D}_e = \left\{ d \in \mathbb{Q}; d = \frac{4u^3+v^2}{2916}, u, v \in \mathbb{Z}, u \equiv 2 \pmod 3, e^3 + 3eu + v \equiv 0 \pmod{27} \right\}. \tag{2.9}$$

Let $d \in \mathbb{D}_e$. Then there exists $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$ such that $a \equiv e \pmod 3$ and $d_f = d$. By (2.4), $g_f(x) = x^3 + ux/3 + v/27 \in \mathbb{Q}[x]$ where $u, v \in \mathbb{Z}$, and $3 \nmid uv$. Hence, by (2.2), $d = d_f = (4u^3 + v^2)/2916$. Moreover, from (2.5) it follows that $u = 3b - a^2 \equiv -e^2 \equiv 2 \pmod 3$.

Since $a = 3w + e$ for some $w \in \mathbb{Z}$, the first identity of (2.1) yields $b = (a^2 + u)/3 = 3w^2 + 2ew + (u + e^2)/3$. Hence, by (2.5), $v \equiv 2(3w + e)^3 - 9(3w + e)(3w^2 + 2ew + (u + e^2)/3) \equiv -3eu - e^3 \pmod{27}$, and $e^3 + 3eu + v \equiv 0 \pmod{27}$ follows. Conversely, assume that $d = (4u^3 + v^2)/2916$ where $u, v \in \mathbb{Z}$ such that $u \equiv 2 \pmod 3$ and $e^3 + 3eu + v \equiv 0 \pmod{27}$. For any $w \in \mathbb{Z}$, let $a = 3w + e$, $b = (a^2 + u)/3$, $c = (-2a^3 + 9ab + v)/27$. Since $u \equiv 2 \pmod 3$, we have $a^2 + u \equiv e^2 + 2 \equiv 0 \pmod 3$. Hence, $b \in \mathbb{Z}$. Next, after some calculation, we obtain $-2a^3 + 9ab + v \equiv -2(3w + e)^3 + 9(3w + e)(3w^2 + 2ew + (u + e^2)/3) - e^3 - 3eu \equiv 0 \pmod{27}$. Hence, $c \in \mathbb{Z}$. Let $f(x) = x^3 + ax^2 + bx + c$. Using (2.1), we get $g_f(x) = x^3 + ux/3 + v/27$ and (2.2) yields $d_f = (4u^3 + v^2)/(4 \cdot 27^2) = d$ as required. This proves (2.9).

It remains to prove $\mathbb{D}_1 = \mathbb{D}_2$. Let $u$ be an integer, $u \equiv 2 \pmod 3$. Then $9u + 9 \equiv 0 \pmod{27}$, which implies

$$v + 3u + 1 \equiv 0 \pmod{27} \iff -v + 6u + 8 \equiv 0 \pmod{27} \tag{2.10}$$

for any $v \in \mathbb{Z}$. Clearly, if $d = d(u, v) = (4u^3 + v^2)/2916$, then $d(u, v) = d(u, -v)$. This, together with (2.9) and (2.10), yields (2.7). The proof is complete. $\square$

**Remark 2.2.** Let $\mathbb{D} = \mathbb{D}_1 = \mathbb{D}_2$. Then $\mathbb{D}_0 \cap \mathbb{D}$, $\mathbb{D}_0 - \mathbb{D}$, and $\mathbb{D} - \mathbb{D}_0$ are nonempty sets. For example, $23/108 \in \mathbb{D}_0 \cap \mathbb{D}$, $-13/108 \in \mathbb{D}_0 - \mathbb{D}$, and $11/27 \in \mathbb{D} - \mathbb{D}_0$.

For any $d \in \mathbb{Q}$ let

$$C(d) = \{f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]; d_f = d\}.$$

Then, $C(d) = \{f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]; D_f = -108d\}$. Furthermore, $C(d) = \emptyset$ if and only if $d \in \mathbb{Q} - (\mathbb{D}_0 \cup \mathbb{D})$. For $d \in \mathbb{D}_0 \cup \mathbb{D}$, the following theorem can be stated.

**Theorem 2.3.** *Assume that* $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$.

(i) *Let* $d \in \mathbb{D}_0$. *Then* $f(x) \in C(d)$ *if and only if there exists* $u, v, w \in \mathbb{Z}$ *such that*

$$a = 3w,\ b = 3w^2 + u,\ c = w^3 + uw + v \text{ and } 4u^3 + 27v^2 = 108d. \tag{2.11}$$

(ii) *Let* $d \in \mathbb{D}_e$ *and* $e \in \{1, 2\}$. *Then* $f(x) \in C(d)$ *if and only if there exist* $u, v, w \in \mathbb{Z}$ *such that*

$$a = 3w + e,\ b = 3w^2 + 2ew + \frac{e^2 + u}{3},\ c = w^3 + ew^2 + \frac{e^2 + u}{3}w + \frac{e^3 + 3eu + v}{27} \tag{2.12}$$

*and*

$$4u^3 + v^2 = 2916d \text{ where } u \equiv 2 \pmod 3,\ e^3 + 3eu + v \equiv 0 \pmod{27}. \tag{2.13}$$

*Moreover, in* (i) *we have* $g_f(x) = x^3 + ux + v$ *and, in* (ii), $g_f(x) = x^3 + ux/3 + v/27$.

*Proof.* (i) Let $d \in \mathbb{D}_0$ and $f(x) \in C(d)$. Then there exist $w \in \mathbb{Z}$ such that $a = 3w$ and, by (2.3), $g_f(x) = x^3 + rx + s \in \mathbb{Z}[x]$. Let $u = r$ and $v = s$. By (2.2), $d = d_f = (4u^3 + 27v^2)/108$ and $4u^3 + 27v^2 = 108d$ follows. Since $a = 3w$, the first equation of (2.1) implies $b = 3w^2 + u$. Similarly, the second equation of (2.1) together with $a = 3w$ and $b = 3w^2 + u$ yields $c = w^2 + uw + v$. Hence, (2.11) follows. Conversely, assume that $a, b, c$ satisfy (2.11). Substituting $a = 3w$, $b = 3w^2 + u$ and $c = w^3 + uw + v$ into (2.1), after short calculation, we get, $r = u$ and $s = v$. Hence, by (2.2), $d_f = (4u^3 + 27v^2)/108 = d$ and $f(x) \in C(d)$ follows. This proves (i).

(ii) Let $d \in \mathbb{D}_e$, $e \in \{1, 2\}$, and $f(x) \in C(d)$. Then there exists $w \in \mathbb{Z}$ such that $a = 3w + e$ and, by (2.4), $g_f(x) = x^3 + ux/3 + v/27 \in \mathbb{Q}[x]$ where $u, v \in \mathbb{Z}$ and $3 \nmid uv$. By (2.2), $d = d_f = (4u^3 + v^2)/2916$ and $4u^3 + v^2 = 2916d$ follows. Substituting $a = 3w + e$ into the first equality of (2.1), we obtain, $b = 3w^2 + 2ew + (u + e^2)/3$. This together with the second equality of (2.1) yields $c = w^3 + ew^2 + (u + e^2)w/3 + (3eu + v + e^3)/27$ and (2.13) follows.

Conversely, assume that $a, b, c$ satisfy (2.12) and (2.13). Substituting (2.12) into (2.1), we get $r = u/3$ and $s = v/27$. Hence, $g_f(x) = x^3 + ux/3 + v/27$ and, by (2.2), we conclude that $d_f = (4u^3 + v^2)/2916 = d$. □

The following corollary states that both Diophantine equations $4u^3 + 27v^2 = 108d$ and $4u^3 + v^2 = 2919d$ can be reduced to the same Mordell equation $Y^2 = X^3 - 432D$ with $D = -108d$. Consequently, the coefficients $a, b, c$ from (2.12) and (2.13) can be given by the integral solutions of $Y^2 = X^3 - 432D$.

**Corollary 2.4.** (i) *Let $d \in \mathbb{D}_0$ and $D = -108d$. Then $f(x) = x^3 + ax^2 + bx + c \in C(d)$ if and only if there exist $w, X, Y \in \mathbb{Z}$ such that*

$$a = 3w,\ \ b = 3w^2 - \frac{X}{12},\ \ c = w^3 - \frac{X}{12}w + \frac{Y}{108} \tag{2.14}$$

*and*

$$Y^2 = X^3 - 432D \quad \textit{where} \quad 12|X, 108|Y.$$

(ii) *Let $d \in \mathbb{D}_e, e \in \{1,2\}$ and $D = -108d$. Then $f(x) = x^3 + ax^2 + bx + c \in C(d)$ if and only if there exist $w, X, Y \in \mathbb{Z}$ such that*

$$a=3w+e, b=3w^2+2ew+\frac{4e^2-X}{12}, c=w^3+ew^2+\frac{4e^2-X}{12}w+\frac{4e^3-3eX+Y}{108} \tag{2.15}$$

*and*

$$Y^2=X^3-432D \ \textit{where}\ 4|X, 4|Y, X\equiv 1 \pmod 3, 4e^3-3eX+Y\equiv 0 \pmod{27}.$$

Corollary 2.4 can be easily obtained from Theorem 2.3 by the substitutions $X = -12u$, $Y = 108v$ in case (i) and $X = -4u$, $Y = 4v$ in case (ii).

**Remark 2.5.** The coefficients $a, b, c$ given by (2.11), (2.12), (2.14) and (2.15) can be written using derivatives as follows: if $c = c(w)$, then $b = c'(w)$ and $a = c''(w)/2$.

**Remark 2.6.** A straightforward application of Corollary 2.4 with $d = 11/27$ leads to Mordell's equation (1.1) with $k = 19008$. In the following section, we show that the set $C(11/27)$ can also be obtained by means of integral solutions of (1.1) with $k = 297$.

## 3. The Tribonacci Family

Let $t(x) = x^3 - x^2 - x - 1$ be the Tribonacci polynomial. First, observe that

$$D_t = -44,\ \ d_t = \frac{11}{27} \text{ and } g_t(x) = x^3 - \frac{4}{3}x - \frac{38}{27}.$$

Since

$$t(x) \in T = \{f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]; D_f = -44\} = C(11/27),$$

the set $T$ can be called the *Tribonacci family.* In this section, explicit forms of all polynomials in $T$ will be given.

**Lemma 3.1.** *Assume that $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$.*

(i) *We have $11/27 \notin \mathbb{D}_0$.*

(ii) *$f(x) \in T$ if and only if there exists $e \in \{1,2\}$ and $w, X, Y \in \mathbb{Z}$ such that*

$$a=3w+e,\ \ b=3w^2+2ew+\frac{e^2-X}{3},\ \ c=w^3+ew^2+\frac{e^2-X}{3}w+\frac{e^3-3eX+2Y}{27} \tag{3.1}$$

*and*

$$Y^2 = X^3 + 297 \text{ where } X \equiv 1 \pmod 3 \text{ and } e^3 - 3eX + 2Y \equiv 0 \pmod{27} \tag{3.2}$$

*Moreover,* $g_f(x) = x^3 + rx + s$ *where* $r = -X/3$, $s = 2Y/27$ *with* $X, Y$ *satisfying* (3.2).

*Proof.* (i) Suppose $11/27 \in \mathbb{D}_0$. Then, by (2.12), there exist $u, v \in \mathbb{Z}$ such that $4u^3 + 27v^2 = 44$. Hence, $2|v$ and $u^3 + 27k^2 = 11$ for some $k \in \mathbb{Z}$. Since $u^3 \equiv 11 \pmod{27}$ has no solution, we get a contradiction. Consequently, $11/27 \notin \mathbb{D}_0$ and $3 \nmid a$. Part (ii) can be obtained easily from Theorem 2.3 by substituting $u = -X$, $v = 2Y$. □

**Theorem 3.2.** *Mordell's equation* $Y^2 = X^3 + 297$ *has exactly eighteen integral solutions* $(X, Y)$*:* $(-6, \pm 9)$, $(-2, \pm 17)$, $(3, \pm 18)$, $(4, \pm 19)$, $(12, \pm 45)$, $(34, \pm 199)$, $(48, \pm 333)$, $(1362, \pm 50265)$, *and* $(93844, \pm 28748141)$.

See Table 3 in [2, p. 96] or consult [6, p. 127].

**Corollary 3.3.** *There exist exactly eight integral solutions* $(X, Y)$ *of* $Y^2 = X^3 + 297$ *satisfying* $X \equiv 1 \pmod 3$ *and* $e^3 - 3eX + 2Y \equiv 0 \pmod{27}$ *where* $e = 1$ *or* $e = 2$*:* $(-2, \pm 17)$, $(4, \pm 19)$, $(34, \pm 199)$, *and* $(93844, \pm 28748141)$.

Combining Lemma 3.1 and Corollary 3.3, we see that there exist exactly eight polynomials $g_j(x) = x^3 + r_j x + s_j \in \mathbb{Q}[x]$, $j \in \{1, \ldots, 8\}$ with $D_{g_j} = -44$:

$$\begin{array}{ll} g_1(x) = x^3 + \frac{2}{3}x - \frac{34}{27}, & g_2(x) = x^3 + \frac{2}{3}x + \frac{34}{27}, \\ g_3(x) = x^3 - \frac{4}{3}x - \frac{38}{27}, & g_4(x) = x^3 - \frac{4}{3}x + \frac{38}{27}, \\ g_5(x) = x^3 - \frac{34}{3}x - \frac{398}{27}, & g_6(x) = x^3 - \frac{34}{3}x + \frac{398}{27}, \\ g_7(x) = x^3 - \frac{93844}{3}x - \frac{57496282}{27}, & g_8(x) = x^3 - \frac{93844}{3}x + \frac{57496282}{27}. \end{array} \tag{3.3}$$

Next, letting $k = w$ in (3.1) and using Corollary 3.3, we find that $f(x) \in T$ if and only if $f(x) = t_j(x, k)$ for some $j \in \{1, \ldots, 8\}$ and $k \in \mathbb{Z}$ where

$$\begin{array}{l} t_1(x,k) = x^3 + (3k+1)x^2 + (3k^2+2k+1)x + k^3 + k^2 + k - 1, \\ t_2(x,k) = x^3 + (3k+2)x^2 + (3k^2+4k+2)x + k^3 + 2k^2 + 2k + 2, \\ t_3(x,k) = x^3 + (3k+2)x^2 + (3k^2+4k)x + k^3 + 2k^2 - 2, \\ t_4(x,k) = x^3 + (3k+1)x^2 + (3k^2+2k-1)x + k^3 + k^2 - k + 1, \\ t_5(x,k) = x^3 + (3k+2)x^2 + (3k^2+4k-10)x + k^3 + 2k^2 - 10k - 22, \\ t_6(x,k) = x^3 + (3k+1)x^2 + (3k^2+2k-11)x + k^3 + k^2 - 11k + 11, \\ t_7(x,k) = x^3 + (3k+1)x^2 + (3k^2+2k-31281)x + k^3 + k^2 - 31281k - 2139919, \\ t_8(x,k) = x^3 + (3k+2)x^2 + (3k^2+4k-31280)x + k^3 + 2k^2 - 31280k + 2108638. \end{array} \tag{3.4}$$

Consequently, $T$ can be written as $T = \bigcup_{j=1}^{8} \{t_j(x,k); k \in \mathbb{Z}\}$ where $\{t_j(x,k); k \in \mathbb{Z}\}$ are pairwise disjoint sets. Finally, by (3.4), $t(x) = t_3(x, -1)$.

## 4. The Cubic Character of the Field $\mathbb{F}_{p^2}$

We start this section with a more general theorem.

**Theorem 4.1.** *Let* $\mathbb{H}$ *be a subfield of the field* $\mathbb{G}$, $[\mathbb{G} : \mathbb{H}] = 2$, $\operatorname{char} \mathbb{H} \neq 2, 3$ *and let* $g(x) = x^3 + rx + s \in \mathbb{H}[x]$ *with* $r \neq 0$. *Assume that* $g(x)$ *is irreducible over* $\mathbb{H}$ *or* $g(x)$ *has three distinct roots in* $\mathbb{H}$. *Further let* $d_g = r^3/27 + s^2/4$ *and* $\varepsilon, \lambda \in \mathbb{G}$ *be such that* $\varepsilon^2 + \varepsilon + 1 = 0$ *and* $\lambda^2 = d_g$. *Then the following statements are equivalent:*

(i) $g(x)$ *has three distinct roots in* $\mathbb{H}$.
(ii) $g(x)$ *has three distinct roots in* $\mathbb{G}$.

(iii) $A = -s/2 - \lambda$ *is a cubic residue of* $\mathbb{G}$.
(iv) $B = -s/2 + \lambda$ *is a cubic residue of* $\mathbb{G}$.

*Proof.* Clearly, (i) implies (ii). Assume (ii) and suppose that $g(x)$ is irreducible over $\mathbb{H}$. Then $\mathbb{G}$ is a splitting field of $g(x)$ over $\mathbb{H}$. Hence, $[\mathbb{G} : \mathbb{H}] = 3$ which is a contradiction. This proves that (i) and (ii) are equivalent. Next, a simple calculation yields $AB = (-r/3)^3$. Since $r \neq 0$, it follows that (iii) and (iv) are equivalent.

Let $\mathbb{K}$ be an arbitrary over-field of $\mathbb{G}$ such that $A, B$ are cubic residues of $\mathbb{K}$. Then there exists $\alpha, \gamma \in \mathbb{K}$ satisfying $\alpha^3 = A$, $\gamma^3 = B$. Since $(\alpha\gamma)^3 = AB = (-r/3)^3$ there exist $i \in \{0, 1, 2\}$ such that $\alpha\gamma\varepsilon^i = -r/3$. Let $\beta = \gamma\varepsilon^i$. Then $\beta^3 = B$ and $\alpha\beta = -r/3$. Since $A + B = -s$, we have $g(\alpha + \beta) = A + B + (\alpha + \beta)(3\alpha\beta + r) + s = 0$.

Hence, it follows for $\mathbb{K} = \mathbb{G}$ that (iii) implies (ii). Finally, assume (ii) and suppose that $A$ is not a cubic residue of $\mathbb{G}$. Let $\mathbb{S}$ be a splitting field of $x^3 - A$ over $\mathbb{G}$. Then $A$ is a cubic residue of $\mathbb{S}$ and $AB = (-r/3)^3$ yields that $B$ is a cubic reside of $\mathbb{S}$, too. By what was proved above, in the field $\mathbb{K} = \mathbb{S}$, there exist $\alpha, \beta$ such that $g(\alpha + \beta) = 0$. Since $g(x)$ has three distinct roots in $\mathbb{G}$, we have $\alpha + \beta \in \mathbb{G}$. Let $\eta = \alpha + \beta$. Then $-s = A + B = \alpha^3 + (\eta - \alpha)^3 = 3\alpha^2\eta - 3\alpha\eta^2 + \eta^3$. Since $1, \alpha, \alpha^2$ is a base of the extension $\mathbb{S}/\mathbb{G}$, we have $\eta = 0$ and $s = 0$. Let $\rho = -3\lambda/r$. Then $\rho \in \mathbb{G}$ and $\lambda^2 = d_g = r^3/27$ yields $\rho^3 = -27\lambda^3/r^3 = -\lambda = A$, a contradiction. Hence, (ii) implies (iii) as required. The proof is complete. □

Note that Theorem 4.1 generalizes the results obtained in [5, pp. 229–230]. The following statement which is an easy consequence of Theorem 4.1 will be used in proving the main result presented in Section 5.

**Theorem 4.2.** *Let $p$ be a prime, $p > 3$ and let $g(x) = x^3 + rx + s \in \mathbb{F}_p[x]$ with $r \neq 0$. Assume that $g(x)$ is irreducible over $\mathbb{F}_p$ or $g(x)$ has three distinct roots in $\mathbb{F}_p$. Then the following statements are equivalent:*

(i) $g(x)$ *has three distinct roots in* $\mathbb{F}_p$.
(ii) $g(x)$ *has three distinct roots in* $\mathbb{F}_{p^2}$.
(iii) $A = -s/2 - \lambda$ *is a cubic residue of* $\mathbb{F}_{p^2}$.
(iv) $B = -s/2 + \lambda$ *is a cubic residue of* $\mathbb{F}_{p^2}$.

**Remark 4.3.** Theorems 4.1 and 4.2 also hold in the case of $r = 0$ if we let $A = B = s$.

Let $\mathbb{F}_{p^2}^\times$ denote the multiplicative group of the Galois field $\mathbb{F}_{p^2}$ where $p$ is a prime, $p > 3$. Recall that the cubic character $\chi$ of $\mathbb{F}_{p^2}$ is a mapping $\chi : \mathbb{F}_{p^2}^\times \to \mathbb{F}_{p^2}^\times$ defined by $\chi(\xi) = \xi^{(p^2-1)/3}$ for any $\xi \in \mathbb{F}_{p^2}^\times$. Let $\varepsilon \in \mathbb{F}_{p^2}^\times$ be such that $\varepsilon^2 + \varepsilon + 1 = 0$. Then $\varepsilon^3 = 1$ and $\varepsilon \neq 1$. Clearly, if $\xi \in \mathbb{F}_{p^2}^\times$, then $\chi(\xi) = \varepsilon^i$ for some $i \in \{0, 1, 2\}$. Next, recall the following familiar properties of $\chi$:

*If $\xi_1, \xi_2 \in \mathbb{F}_{p^2}^\times$, then $\chi(\xi_1 \cdot \xi_2) = \chi(\xi_1) \cdot \chi(\xi_2)$.*
*If $\xi \in \mathbb{F}_{p^2}^\times$, then $\chi(\xi) = 1$ if and only if $\xi$ is a cube in the field $\mathbb{F}_{p^2}$.*
*If $\xi \in \mathbb{F}_p^\times$ and $\chi(\xi) = 1$, then $\xi$ is a cube in the field $\mathbb{F}_p$.*

Let $\lambda \in \mathbb{F}_{p^2}$ be such that $\lambda^2 = d_t = 11/27 \in \mathbb{F}_p$ and $g_j(x) = x^3 + r_j x + s_j$, $j \in \{1, \ldots, 8\}$ be the cubic polynomials established in (3.3) considered as polynomials in $\mathbb{F}_p[x]$. For any $j \in \{1, \ldots, 8\}$, we define the elements $A(y_j), B(y_j) \in \mathbb{F}_{p^2}$ as follows:

$$A(y_j) = -\frac{y_j}{27} - \frac{1}{9}\varkappa, \; B(y_j) = -\frac{y_j}{27} + \frac{1}{9}\varkappa \;\text{ where }\; y_j = \frac{27}{2}s_j \text{ and } \varkappa = 9\lambda.$$

Let $\mathbb{Y}=\{y_j, j=1,\dots,8\}$. Then $\mathbb{Y}=\{\pm 17, \pm 19, \pm 199, \pm 28748141\}$ and $A(y)$, $B(y)\neq 0$ in $\mathbb{F}_{p^2}$ for any $y\in\mathbb{Y}$ and $p\neq 17, 29, 809$. Furthermore, it is easy to verify that

$$\chi(A(y))=\chi(B(-y)) \text{ and } \chi(A(y))\cdot\chi(A(-y))=1 \text{ for any } y\in\mathbb{Y}. \tag{4.1}$$

Let

$$\begin{aligned} R&=\{A(17), B(-17), A(-19), B(19), A(-199), B(199), A(28748141), B(-28748141)\},\\ S&=\{A(-17), B(17), A(19), B(-19), A(199), B(-199), A(-28748141), B(28748141)\}.\end{aligned}$$

The fundamental relations between the cubic characters of the elements of $R$ and $S$ will be stated in the following lemma.

**Lemma 4.4.** *Let $p$ be an arbitrary prime, $p\neq 2, 3, 17, 29, 809$. Then*
(i) *All elements of $R$ have the same cubic character in $\mathbb{F}_{p^2}$.*
(ii) *All elements of $S$ have the same cubic character in $\mathbb{F}_{p^2}$.*
(iii) *If $\rho\in R$ and $\sigma\in S$, then $\chi(\rho)\cdot\chi(\sigma)=1$.*

*Proof.* By direct calculation we can easily verify that

$$\begin{aligned} &(19+3\sqrt{33})\cdot(17+3\sqrt{33})=(5+\sqrt{33})^3,\\ &(19+3\sqrt{33})\cdot(199-3\sqrt{33})=(13+\sqrt{33})^3,\\ &(19+3\sqrt{33})\cdot(28748141+3\sqrt{33})=(692+56\sqrt{33})^3.\end{aligned} \tag{4.2}$$

Since the mapping $H:\mathbb{Z}[\sqrt{33}]\to\mathbb{F}_{p^2}$ defined by $H(\alpha+\beta\sqrt{33})=\alpha+\beta\varkappa$ is a homomorphism of $\mathbb{Z}[\sqrt{33}]$ into $\mathbb{F}_{p^2}$, (4.2) yields $\chi(19+3\varkappa)\cdot\chi(17+3\varkappa)=\chi(19+3\varkappa)\cdot\chi(199-3\varkappa)=\chi(19+3\varkappa)\cdot\chi(28748141+3\varkappa)=1$. Multiplying by $\chi(19-3\varkappa)$ and using the second equality of (4.1) for $y=19$ we get $\chi(B(-17))=\chi(A(-199))=\chi(B(-28748141))=\chi(A(-19))$. This together with the first equality of (4.1) implies that all elements of $R$ have the same cubic character. Since $S$ can be written in the form $S=\{A(-y); A(y)\in R\}\cup\{B(-y); B(y)\in R\}$, the second equality of (4.1) implies that all elements of $S$ have the same cubic character and $\chi(\rho)\cdot\chi(\sigma)=1$ for any $\rho\in R$ and $\sigma\in S$. □

## 5. The Main Theorem

There exist five types of factorization of the cubic polynomial $f(x)=x^3+ax^2+bx+c\in\mathbb{Z}[x]$ over the Galois field $\mathbb{F}_p$ with $p$ a prime:

Type I: *$f(x)$ is irreducible over $\mathbb{F}_p$, i.e., $f(x)$ has no root in $\mathbb{F}_p$.*
Type II: *$f(x)$ splits over $\mathbb{F}_p$ into a linear factor and an irreducible quadratic factor.*
Type III: *$f(x)$ has three distinct roots in $\mathbb{F}_p$.*
Type IV: *$f(x)$ has a double root in $\mathbb{F}_p$.*
Type V: *$f(x)$ has a triple root in $\mathbb{F}_p$.*

Cases I–V can partially be distinguished using the quadratic character of $D_f$. Let $(D_f/p)$ denote the Legendre–Jacobi symbol. By the Stickelberger Parity Theorem [8] for the case of a cubic polynomial [10, p. 189], we can distinguish case II from cases I and III as follows.

*Let $N$ be the number of distinct roots of $f(x)=x^3+ax^2+bx+c\in\mathbb{Z}[x]$ over the Galois field $\mathbb{F}_p$ with $p$ a prime, $p>3$ and $p\nmid D_f$. Then*

$$\begin{aligned} &N=1 \textit{ if and only if } (D_f/p)=-1,\\ &N=0 \textit{ or } N=3 \textit{ if and only if } (D_f/p)=1.\end{aligned} \tag{5.1}$$

For distinguishing types I and III, we can use the cubic character and the field $\mathbb{F}_{p^2}$ by Theorem 4.2 as follows: Let $p > 3$ and $(D_f/p) = 1$. Set $r = b - a^2/3$, $s = 2a^3/27 - ab/3 + c$, $d = r^3/27 + s^2/4$ and let $\lambda \in \mathbb{F}_{p^2}$ with $\lambda^2 = d$. Further let $A = -s/2 - \lambda$, $B = -s/2 + \lambda$ if $a^2 \not\equiv 3b \pmod{p}$ and $A = B = s$ if $a^2 \equiv 3b \pmod{p}$. Then

*$f(x)$ is of type* III *if and only if $A$ and $B$ are cubic residues of $\mathbb{F}_{p^2}$.*

Furthermore, for an arbitrary prime $p$, $f(x)$ has a multiple root in $\mathbb{F}_p$ if and only if $p|D_f$. Clearly, for $p > 2$, the condition $p|D_f$ is equivalent to $(D_f/p) = 0$. Moreover, if $p > 2$ and $p|D_f$, then using Viètes relations between the roots and coefficients of $f(x)$, it is easy to see that

$$f(x) \text{ is of the type } \begin{cases} \text{IV} & \text{if and only if } p \nmid ab - 9c \text{ or } p \nmid a, p|b, p|c, \\ \text{V} & \text{otherwise.} \end{cases}$$

Our next considerations will be restricted to polynomials $f(x)$ belonging to the Tribonacci family $T$. In this case, $D_f = -44$ and, for any prime $p \neq 2, 11$, we have $(D_f/p) = (-44/p) = (p/11)$. See also [4, p. 23]. To prove the main theorem, we will need the following proposition.

**Proposition 5.1.** *Let $p$ be a prime, $p > 3$ and $(p/11) = 1$. Then all polynomials in $T$ have the same type of factorization over $\mathbb{F}_p$.*

*Proof.* It is evident that, for any fixed $j \in \{1, \dots, 8\}$, the polynomials $g_j(x)$ and $t_j(x, k)$, $k \in \mathbb{Z}$ defined by (3.3) and (3.4) have the same type of factorization over an arbitrary Galois field $\mathbb{F}_p$ with $p$ a prime, $p > 3$. Hence, it follows that all polynomials in $T$ have the same type of factorization over $\mathbb{F}_p$ if and only if the polynomials $g_j(x) = x^3 + r_j x + s_j \in \mathbb{F}_p[x]$, $j \in \{1, \dots, 8\}$ have the same type of factorization over $\mathbb{F}_p$. Now we show that, if $p > 3$ and $(p/11) = 1$, then $r_j \neq 0$ in $\mathbb{F}_p$ for any $g_j(x)$. Suppose that $r_j = 0$ for some $j$. Then it follows from (3.4) that $p \in \{17, 29, 809\}$. Since $(p/11) = -1$ for any $p \in \{17, 29, 809\}$, a contradiction follows. Furthermore, if $p > 3$ and $(p/11) = 1$, then, by (5.1), any $g_j(x)$, $j \in \{1, \dots, 8\}$ is of type I or type III. By Lemma 4.4, for any $\tau_1, \tau_2 \in R \cup S$, we have $\chi(\tau_1) = 1$ if and only if $\chi(\tau_2) = 1$. This together with Theorem 4.2 concludes the proof. □

Now we can to prove our main theorem.

**Main Theorem 5.2.** Let $p$ be an arbitrary prime. Then all polynomials in $T$ have the same type of factorization over the Galois field $\mathbb{F}_p$.

*Proof.* If $p > 3$ and $(p/11) = -1$, then the Stickelberger Parity Theorem says that each polynomial in $T$ is of the type II over $\mathbb{F}_p$. If $p > 3$ and $(p/11) = 1$, then all polynomials in $T$ have the same type of factorization over $\mathbb{F}_p$ by Proposition 5.1. Moreover, by the Stickelberger Parity Theorem, this type is either I or III.

Let $p = 2$. Substituting $k = 0, 1$ into (3.4), we obtain the following identities over $\mathbb{F}_2[x]$: $t_1(x,0) = t_2(x,1) = t_3(x,1) = t_4(x,0) = t_5(x,1) = t_6(x,0) = t_7(x,0) = t_8(x,1) = (x-1)^3$, and $t_1(x,1) = t_2(x,0) = t_3(x,0) = t_4(x,1) = t_5(x,0) = t_6(x,1) = t_7(x,1) = t_8(x,0) = x^3$. This proves that each polynomial in $T$ is of type V over $\mathbb{F}_2$. Let $p = 3$. Substituting $k = 0, 1, 2$

into (3.4), we get the following identities over $\mathbb{F}_3[x]$:

$$\begin{aligned}
t_1(x,0) = t_4(x,1) = t_6(x,0) = t_7(x,2) &= x^3 + x^2 + x + 2,\\
t_1(x,1) = t_4(x,2) = t_6(x,1) = t_7(x,0) &= x^3 + x^2 + 2,\\
t_1(x,2) = t_4(x,0) = t_6(x,2) = t_7(x,1) &= x^3 + x^2 + 2x + 1,\\
t_2(x,0) = t_3(x,2) = t_5(x,0) = t_8(x,1) &= x^3 + 2x^2 + 2x + 2,\\
t_2(x,1) = t_3(x,0) = t_5(x,1) = t_8(x,2) &= x^3 + 2x^2 + 1,\\
t_2(x,2) = t_3(x,1) = t_5(x,2) = t_8(x,0) &= x^3 + 2x^2 + x + 1.
\end{aligned} \tag{5.2}$$

By direct calculation, it is easy to verify that all polynomials in (5.2) are irreducible over $\mathbb{F}_3$. This means that each polynomial in $T$ is of type I over $\mathbb{F}_3$.

Finally, let $p = 11$. Then the polynomials $g_j(x)$, $j \in \{1, \dots, 8\}$ established in (3.3), have the following factorizations over $\mathbb{F}_{11}$:

$$\begin{aligned}
g_1(x) &= (x+10)^2(x+2), & g_2(x) &= (x+1)^2(x+9),\\
g_3(x) &= (x+8)^2(x+6), & g_4(x) &= (x+3)^2(x+5),\\
g_5(x) &= (x+4)^2(x+3), & g_6(x) &= (x+7)^2(x+8),\\
g_7(x) &= (x+9)^2(x+4), & g_8(x) &= (x+2)^2(x+7).
\end{aligned} \tag{5.3}$$

From (5.3) it follows that each polynomial in $T$ is of type IV over $\mathbb{F}_{11}$. The proof is complete. □

## 6. Conclusion

The results presented in Theorem 2.3 and Corollary 2.4 make it possible to find the set of all cubic polynomials $f(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$ with a given discriminant $0 \neq D \in \mathbb{Z}$ if all integral solutions of Mordell's equation $Y^2 = X^3 + k$, $k = 432D$ are known. Thanks to the computations made by Gebel, Pethö and Zimmer [3], all integral solutions of this equation are determined for any $0 \neq |k| \leq 10^5$ and thus, for any $0 \neq |D| \leq 231$. Consequently, the method used in proving the Main Theorem 5.2 can actually be applied to any particular $0 \neq |D| \leq 231$. These facts open a new and interesting question, namely, for which $D \in \mathbb{Z}$ can the Main Theorem 5.2 be generalized. However, to determine all such $D$'s can be a difficult problem.

## References

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

[2] O. Hemer, *On the Diophantine Equation $y^2 - k = x^3$*, Doctoral Dissertation, Uppsala, (1952).

[3] J. Gebel, A. Pethö, and G. H. Zimmer, *On Mordell's equation*, Compositio Mathematica, **110** (1998), 335–367.

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

[5] J. Klaška and L. Skula, *Periods of the Tribonacci sequence modulo a prime $p \equiv 1 \pmod 3$*, The Fibonacci Quarterly, **48.3** (2010), 228–235.

[6] J. London and M. Finkelstein, *On Mordell's Equation $y^2 - k = x^3$*, Bowling Green, Ohio Bowling Green State University, (1973).

[7] L. J. Mordell, *The Diophantine equation $y^2 - k = x^3$*, London Math. Soc., **13** (1913), 60–80.

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

[9] A. Thue, *Über Annährungswerte algebraischer Zahlen*, Reine u. Angew. Math., **135** (1909), 284–305.

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

MSC2010: 11B39, 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